High-bandwidth Digital Content Protection System v1.3

Amendment for DisplayPort

Revision 1.1

15 January, 2010

Notice

THIS DOCUMENT IS PROVIDED "AS IS" WITH NO WARRANTIES WHATSOEVER, INCLUDING ANY WARRANTY OF MERCHANTABILITY, NONINFRINGEMENT, FITNESS FOR ANY PARTICULAR PURPOSE, OR ANY WARRANTY OTHERWISE ARISING OUT OF ANY PROPOSAL, SPECIFICATION OR SAMPLE. Intel Corporation disclaims all liability, including liability for infringement of any proprietary rights, relating to use of information in this specification. No license, express or implied, by estoppel or otherwise, to any intellectual property rights is granted herein.

The cryptographic functions described in this specification may be subject to export control by the United States, Japanese, and/or other governments.

Acknowledgement

Advanced Micro Devices, Nvidia and STMicroelectronics have contributed to the development of this specification.

Intellectual Property

Implementation of this specification requires a license from the Digital Content Protection LLC.

Contact Information

Digital Content Protection LLC
C/O Vital Technical Marketing, Inc.
3855 SW 153rd Drive
Beaverton, OR 97006 USA

Email: info@digital-cp.com

Web: www.digital-cp.com

Revision History

1 Introduction

1.1 Scope

This specification describes the amendment of the High-bandwidth Digital Content Protection (HDCP) system for DisplayPort, Revision 1.10, referred to as DisplayPort-HDCP 1.1. It is based on the High-bandwidth Digital Content Protection (HDCP) system, Revision 1.30, referred to as HDCP 1.3.

DisplayPort-HDCP 1.1 is designed for protecting Audiovisual content over the DisplayPort interface. For specific details of the DisplayPort interface, consult the References section of this specification. This specification defines the required behavior for Multi-stream Transport (MST) mode and Single-stream Transport (SST) mode DisplayPort implementations. In an HDCP System, two or more HDCP Devices are interconnected through an HDCP-protected Interface. The Audiovisual Content protected by HDCP, referred to as HDCP Content, flows from the Upstream Content Control Function into the HDCP System at the most upstream HDCP Transmitter. From there, the HDCP Content, encrypted by the HDCP System, flows through a tree-shaped topology of HDCP Receivers over HDCP-protected Interfaces. This specification describes a content protection mechanism for: (1) authentication of HDCP Receivers to their immediate upstream connection (i.e., an HDCP Transmitter), (2) revocation of HDCP Receivers that are determined by the Digital Content Protection, LLC, to be invalid, and (3) HDCP Encryption of Audiovisual Content over the HDCP-protected Interfaces between HDCP Transmitters and their downstream HDCP Receivers. HDCP Receivers may render the HDCP Content in audio and visual form for human consumption. HDCP Receivers may be HDCP Repeaters that serve as downstream HDCP Transmitters emitting the HDCP Content further downstream to one or more additional HDCP Receivers.

Except when specified otherwise, DisplayPort-HDCP 1.1-compliant Devices must interoperate with other DisplayPort-HDCP 1.1-compliant Devices attached to their HDCP-protected Interface Ports using the same protocol. HDCP Transmitters must support HDCP Repeaters.

The state machines in this specification define the required behavior of HDCP Devices. The link-visible behavior of HDCP Devices implementing the specified state machines must be identical, even if implementations differ from the descriptions. The behavior of HDCP Devices implementing the specified state machines must also be identical from the perspective of an entity outside of the HDCP System.

Implementations must include all elements of the content protection system described herein, unless the element is specifically identified as informative or optional. Adopters must also ensure that implementations satisfy the robustness and compliance rules described in the technology license. Additionally, HDCP Transmitters may be subject to additional robustness and compliance rules associated with other content protection technologies.

1.2 Definitions

The following terminology, as used throughout this specification, is defined as herein:

Audiovisual Content. Audiovisual works (as defined in the United States Copyright Act as in effect on January 1, 1978), text and graphic images, are referred to as *AudioVisual Content*.

Authorized Device. An HDCP Device that is permitted access to HDCP Content is referred to as an *Authorized Device*. An HDCP Transmitter may test if an attached HDCP Receiver is an Authorized Device by successfully completing the first and, when applicable, second part of the authentication protocol. If the authentication protocol successfully results in establishing authentication, then the other device is considered by the HDCP Transmitter to be an Authorized Device.

Device Key Set. Each HDCP Device has a *Device Key Set*, which consists of a set of Device Private Keys along with the associated Key Selection Vector.

Device Private Keys. A set of Device Private Keys consists of 40 different 56-bit values. These keys are to be protected from exposure outside of the HDCP Device. A set of Device Private Keys is associated with a unique Key Selection Vector.

DisplayPort Encryption Signaling (DPES). DPE*S*, further described in Section 5 and Section 6, is a protocol for signaling whether encryption is enabled or disabled for the main link.

DisplayPort-HDCP 1.0. DisplayPort-*HDCP 1.0* refers to, specifically, the variant of the amendment of HDCP for DisplayPort described by Revision 1.00 of this specification along with its associated errata, if applicable.

DisplayPort-HDCP 1.0-compliant Device. A DisplayPort-HDCP Device that is designed in adherence to DisplayPort-HDCP 1.0 is referred to as a *DisplayPort-HDCP 1.0-compliant Device*.

DisplayPort-HDCP 1.1. DisplayPort-*HDCP 1.1* refers to, specifically, the variant of the amendment of HDCP for DisplayPort described by Revision 1.10 of this specification along with its associated errata, if applicable.

DisplayPort-HDCP 1.1-compliant Device. A DisplayPort-HDCP Device that is designed in adherence to DisplayPort-HDCP 1.1 is referred to as a *DisplayPort-HDCP 1.1-compliant Device*.

downstream. The term, *downstream*, is used as an adjective to refer to being towards the sink of the HDCP Content stream. For example, when an HDCP Transmitter and an HDCP Receiver are connected over an HDCP-protected Interface, the HDCP Receiver can be referred to as the *downstream* HDCP Device in this connection. For another example, on an HDCP Repeater, the HDCP-protected Interface Port(s) which can emit HDCP Content can be referred to as its *downstream* HDCP-protected Interface Port(s). See also, *upstream*.

frame. For purposes of the application of HDCP onto DisplayPort in the SST mode, a frame consists of the link symbol data between successive scrambler reset (SR/CPSR) link symbols, which are inserted every 512 blank start (BS/CPBS) link symbols. There is no implicit relationship between this definition of a frame and the concept of a video frame or, in the case of interlaced video formats, a video field.

HDCP. *HDCP* is an acronym for High-bandwidth Digital Content Protection. This term refers to this content protection system as described by any revision of this specification and its errata.

HDCP 1.2. *HDCP 1.2* refers to, specifically, the variant of HDCP described by Revision 1.20 along with its associated errata, if applicable.

HDCP 1.2-compliant Device. An HDCP Device that is designed in adherence to HDCP 1.2 is referred to as an *HDCP 1.2-compliant Device*.

HDCP 1.3. *HDCP 1.3* refers to, specifically, the variant of HDCP described by Revision 1.30 along with its associated errata, if applicable.

HDCP 1.3-compliant Device. An HDCP Device that is designed in adherence to HDCP 1.3 is referred to as an *HDCP 1.3-compliant Device*.

HDCP Content. *HDCP Content* consists of Audiovisual Content that is protected by the HDCP System. *HDCP Content* includes the Audiovisual Content in encrypted form as it is transferred from an HDCP Transmitter to an HDCP Receiver over an HDCP-protected Interface, as well as any translations of the same content, or portions thereof. For avoidance of doubt, Audiovisual Content that is never encrypted by the HDCP System is not *HDCP Content*.

HDCP Device. Any device that contains one or more HDCP-protected Interface Port and is designed in adherence to HDCP is referred to as an *HDCP Device*.

HDCP Encryption. *HDCP Encryption* is the encryption technology of HDCP when applied to the protection of HDCP Content in an HDCP System.

HDCP-protected Interface. An interface for which HDCP applies is described as an *HDCP-protected Interface*.

HDCP-protected Interface Port. A connection point on an HDCP Device that supports an HDCP-protected Interface is referred to as an *HDCP-protected Interface Port*.

HDCP Receiver. An HDCP Device that can receive and decrypt HDCP Content through one or more of its HDCP-protected Interface Ports is referred to as an *HDCP Receiver*.

HDCP Repeater. An HDCP Device that can receive and decrypt HDCP Content through one or more of its HDCP-protected Interface Ports, and can also re-encrypt and emit said HDCP Content through one or more of its HDCP-protected Interface Ports, is referred to as an *HDCP Repeater*. An *HDCP Repeater* may also be referred to as either an HDCP Receiver or an HDCP Transmitter when referring to either the upstream side or the downstream side, respectively.

HDCP System. An *HDCP System* consists of an HDCP Transmitter, zero or more HDCP Repeaters and one or more HDCP Receivers connected through their HDCP-protected interfaces in a tree topology; whereas the said HDCP Transmitter is the HDCP Device most upstream, and receives the HDCP Content from one or more Upstream Content Control Functions. All HDCP Devices connected to other HDCP Devices in an *HDCP System* over HDCP-protected Interfaces are part of the *HDCP System*.

HDCP Transmitter. An HDCP Device that can encrypt and emit HDCP Content through one or more of its HDCP-protected Interface Ports is referred to as an *HDCP Transmitter*.

Key Selection Vector (KSV). Each HDCP Device contains a set of Device Private Keys. A set of Device Private Keys is associated with a *Key Selection Vector* (*KSV*). Each HDCP Transmitter has assigned to it a unique *KSV* from all other HDCP Transmitters. Also, each HDCP Receiver has assigned to it a unique *KSV* from all other HDCP Receivers.

link frame. In the MST mode, a frame consists of the link symbol data between successive SR link symbols, which occur regularly every 1024 MTPs or 2^16 timeslots.

link line boundary. In the MST mode a link line boundary is not explicitly demarcated but determined by counting as each link line consists of a fixed 2^13 timeslots, with 8 link lines per link frame aligned to the link frame boundary.

upstream. The term, *upstream*, is used as an adjective to refer to being towards the source of the HDCP Content stream. For example, when an HDCP Transmitter and an HDCP Receiver are connected over an HDCP-protected Interface, the HDCP Transmitter can be referred to as the *upstream* HDCP Device in this connection. For another example, on an HDCP Repeater, the HDCP-protected Interface Port(s) which can receive HDCP Content can be referred to as its *upstream* HDCP-protected Interface Port(s). See also, *downstream*. This term should not be confused as referring to the Upstream Specification.

Upstream Content Control Function. The HDCP Transmitter most upstream in the HDCP System receives HDCP Content from the *Upstream Content Control Function*. The *Upstream*

Content Control Function is not part of the HDCP System, and the methods used, if any, by the *Upstream Content Control Function* to determine for itself the HDCP System is correctly authenticated or permitted to receive the Audiovisual Content, or to transfer the Audiovisual Content to the HDCP System, are beyond the scope of this specification. On a personal computer platform, an example of an *Upstream Content Control Function* may be software designed to emit Audiovisual Content to a display or other presentation device that requires HDCP.

In addition, terms such as *AUX CH, DPCD, Enhanced Framing, Symbol, K-codes, Link Symbol Clock, HPD pulse, DisplayPort Converter, Secondary data and VB-ID* are further explained in the DisplayPort Specification (see references).

1.3 Overview

HDCP is designed to protect the transmission of Audiovisual Content between an HDCP Transmitter and an HDCP Receiver. The system also allows for HDCP Repeaters that support downstream HDCP-protected Interface Ports. Figure 1-1 illustrates an example connection topology for HDCP Devices. The HDCP System allows up to seven levels of HDCP Repeaters and as many as 128 total HDCP Devices, including HDCP Repeaters, to be attached to an HDCP-protected Interface Port.

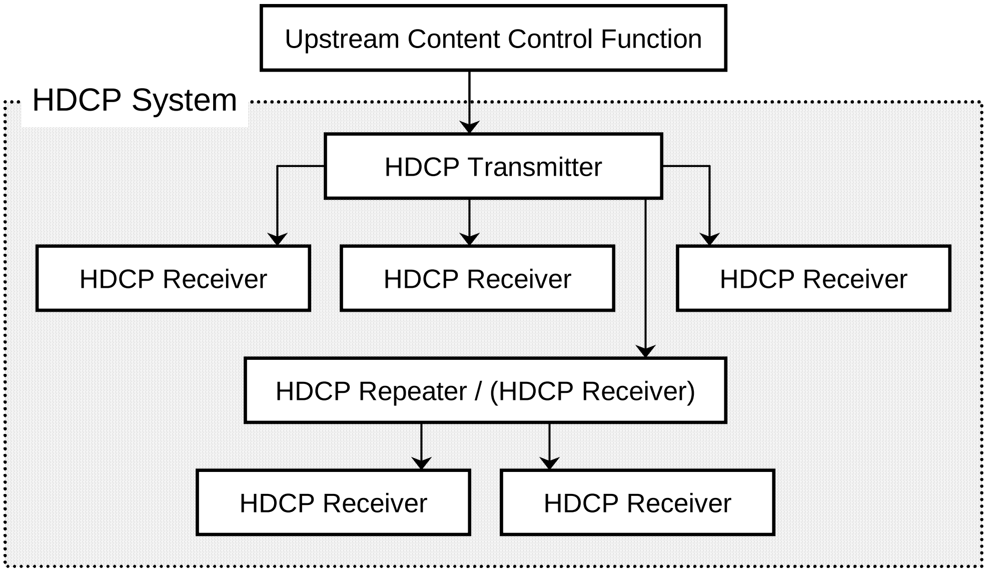

Figure 1-1. Sample Connection Topology of an HDCP System

There are three elements of the content protection system. Each element plays a specific role in the system. First, there is the authentication protocol, through which the HDCP Transmitter verifies that a given HDCP Receiver is licensed to receive HDCP Content. With the legitimacy of the HDCP Receiver determined, encrypted HDCP Content is transmitted between the two devices based on shared secrets established during the authentication protocol. This prevents eavesdropping devices from utilizing the content. Finally, in the event that legitimate devices are compromised to permit unauthorized use of HDCP Content, renewability allows a HDCP Transmitter to identify such compromised devices and prevent the transmission of HDCP Content.

This document contains chapters describing in detail the requirements of each of these elements. In addition, a chapter is devoted describing the cipher that is used in both the authentication protocol and in the encryption of the HDCP Content. All aspects of HDCP map easily onto the existing DisplayPort specification.

1.4 Terminology

Throughout this specification, names that appear in italic refer to values that are exchanged during the HDCP cryptographic protocol. Names that appear in CAPS refer to status values from the receiver. C-style notation is used throughout the state diagrams and protocol diagrams, although the logic functions AND, OR, and XOR are written out where a textual description would be more clear.

The concatenation operator ‘||’ combines two values into one. For eight-bit values *a* and *b*, the result of (*a* || *b*) is a 16-bit value, with the value *a* in the most significant eight bits and *b* in the least significant eight bits.

1.5 References

Video Electronics Standards Association (VESA), DisplayPort Proposed Standard Version 1.2, 2009

National Institute of Standards and Technology (NIST), *Digital Signature Standard (DSS)*, FIPS Publication 186-1, December 15, 1998.

National Institute of Standards and Technology (NIST), *Secure Hash Standard (SHS)*, FIPS Publication 180-1, April 17, 1995.

2 Authentication

The HDCP Authentication protocol is an exchange between an HDCP Transmitter and an HDCP Receiver that affirms to the HDCP Transmitter that the HDCP Receiver is authorized to receive HDCP Content. This affirmation is in the form of the HDCP Receiver demonstrating knowledge of a valid set of secret device keys. Each HDCP Device is provided with a unique set of secret device keys, referred to as the Device Private Keys, from the Digital Content Protection LLC. The communication exchange, which allows for the receiver to demonstrate knowledge of such secret device keys, also provides for both HDCP Devices to generate a shared secret value that cannot be determined by eavesdroppers on this exchange. By having this shared secret formation melded into the demonstration of authorization, the shared secret can then be used as a symmetric key to encrypt HDCP Content intended only for the Authorized Device. Thus, a communication path is established between the HDCP Transmitter and HDCP Receiver that only Authorized Devices can access.

2.1 Overview

Each HDCP Device contains an array of 40, 56-bit secret device keys which make up its Device Private Keys, and a corresponding identifier, received from the Digital Content Protection LLC. This identifier is the Key Selection Vector (KSV) assigned to the device. The KSV is a 40-bit binary value.

An HDCP Device with multiple inputs can share the same keys (Receiver keys) across all its inputs. Similarly, an HDCP Device with multiple outputs can share the keys (Transmitter keys) across all its outputs.

The HDCP Authentication Protocol consists of two parts. The first part establishes shared values between the two HDCP Devices if both devices have a valid Device Key Set from the Digital Content Protection LLC. The second part allows an HDCP Repeater to report the KSVs of attached HDCP Receivers.

After successful completion of the first part of authentication, HDCP Encryption is enabled by the HDCP Transmitter. Once encryption is enabled, a periodic Link Integrity Check is performed to ensure cipher synchronization between the transmitter and the receiver. The Link Integrity Check process is explained in Section 2.2.3 and Section 2.2.4.

2.2 Protocol

2.2.1 First Part of Authentication Protocol

Figure 2-1 illustrates the first part of the authentication exchange. The HDCP Transmitter (*Device A*) can initiate authentication at any time, even before a previous authentication exchange has completed. Authentication is initiated by the HDCP Transmitter by sending an initiation message containing a 64-bit pseudo-random value (*An*) generated by the HDCP Cipher function hdcpRngCipher (Section 4.5) and its KSV (*Aksv*) to the HDCP Receiver (*Device B*). The HDCP Transmitter initiates an HDCP session by sending the *An* and *Aksv* to the HDCP Receiver. The HDCP Transmitter then uses the native AUX-CH to read the HDCP Receiver's KSV (*Bksv*) and REPEATER bit (*Bcaps[1]).* The REPEATER bit in the *Bcaps* register indicates if the receiver is an HDCP Repeater. The HDCP Transmitter verifies that the HDCP Receiver's KSV has not been revoked (Section 7), and that the received KSV contains 20 ones and 20 zeros.

The HDCP Transmitter can also initiate authentication by first reading the receiver's *Bksv* and the REPEATER bit before sending its *An* and *Aksv* value to the HDCP Receiver. However, throughout this specification it is assumed that the transmitter initiates authentication by first sending it's *An* and *Aksv* value to the HDCP Receiver.

After the HDCP Transmitter has written *An* and *Aksv* and read the receiver's *Bksv* and the REPEATER bit, it sets the REAUTHENTICATION_ENABLE_IRQ_HPD bit in the Ainfo register if the REPEATER bit is set and the transmitter determines that the downstream HDCP Repeater supports DPCD Revision 1.2 or higher.

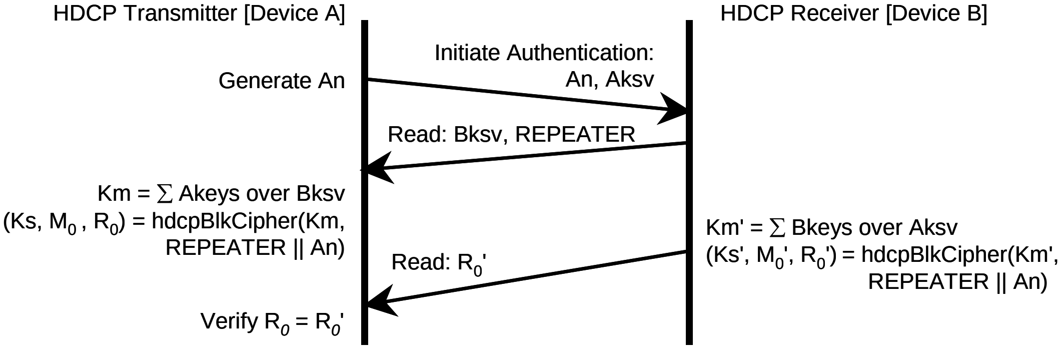

Figure 2-1. First Part of Authentication Protocol

At this point, if both HDCP Devices have a valid array of secret device keys and corresponding KSV from the Digital Content Protection LLC, then they can each calculate a 56-bit shared secret value, *Km* (*Km*' in the HDCP Receiver). Each device calculates *Km* (*Km*' in the HDCP Receiver) by adding a selection of its private device keys described by the other device's KSV, using 56-bit binary addition (i.e. unsigned addition modulo 2^{56}). The selection of secret device keys that are added together consists of those corresponding to the bit indexes of all of the 1-bits of the binary representation of the KSV.

For example, suppose *Bksv* equals 0x5A3. For the binary representation of 0x5A3, bit positions 0, 1, 5, 7, 8, and 10 are ones and all other bit positions are zeros. Therefore, *Device A* will add it's own secret device keys at array indexes 0, 1, 5, 7, 8, and 10 together to calculate the shared secret value, *Km*. *Device B* will perform an analogous calculation using its own private key array and *Aksv* to get *Km*'.

If either device has an invalid set of secret device keys or corresponding KSV, then *Km* will not be equal to *Km*'.

The HDCP Cipher function hdcpBlockCipher (Section 4.5) is then used to calculate three values, *Ks,* M_0, and R_0. The cipher initialization values for this calculation are *Km* (or *Km*'), and the 65-bit concatenation of REPEATER with *An*. The HDCP Receiver's status bit REPEATER indicates that the HDCP Receiver supports retransmission of HDCP Content to additional HDCP Receivers. The session key *Ks* is a 56-bit secret key for the HDCP Cipher. M_0 is a 64-bit secret value used in the second part of the authentication protocol, and as a supplemental HDCP Cipher initialization value. R_0' is a 16-bit response value that the HDCP Receiver returns to the HDCP Transmitter to provide an indication as to the success of the authentication exchange. R_0' must be available for the HDCP Transmitter to read within 100 milliseconds from the time that the HDCP Transmitter finishes writing *Aksv* to the HDCP Receiver. The HDCP Transmitter must not read the R_0' value sooner than 100ms after writing *Aksv*.

As soon as R_0' is available, the HDCP Receiver must set the R_0'_AVAILABLE bit in the *Bstatus* register and generate CP_IRQ interrupt. If the HDCP Transmitter chooses to field the CP_IRQ interrupt, it must read the R_0'_AVAILABLE bit in the *Bstatus* register. If this bit is set, it must read R_0'. The CP_IRQ interrupt must be generated by the HDCP Receiver within 100ms after writing *Aksv*. The HDCP Transmitter can optionally choose to ignore the CP_IRQ interrupt and read R_0' after 100ms. It must not read R_0' sooner than 100ms in this case.

If authentication was successful, then R_0' will be equal to R_0. If there is a mismatch between R_0 and R_0', the HDCP Transmitter must re-read R_0' for comparison against R_0 two additional times (for a total of three consecutive comparisons) in order to account for the possibility of link errors. The authentication protocol is deemed to have failed on three consecutive mismatches between R_0 and R_0'. Authentication can be reattempted with the transmission of new *An* and *Aksv* on failure of the first part of authentication.

The HDCP Transmitter enables HDCP Encryption when the first part of the authentication protocol successfully completes. Section 5 and Section 6 explain in detail the encryption signaling protocol that is used to enable / disable HDCP Encryption.

2.2.2 Second Part of Authentication Protocol

Figure 2-2 illustrates second part of the authentication protocol. The HDCP Transmitter executes the second part of the protocol only when the REPEATER bit is set, indicating that the attached HDCP Receiver is an HDCP Repeater. The second part of the authentication protocol may be implemented in parallel with the Link Integrity Check process. The Link Integrity Check process is explained in Section 2.2.3 and Section 2.2.4. This part of the protocol assembles a list of all downstream KSVs attached to the HDCP Repeater through a permitted connection tree, enabling revocation support upstream.

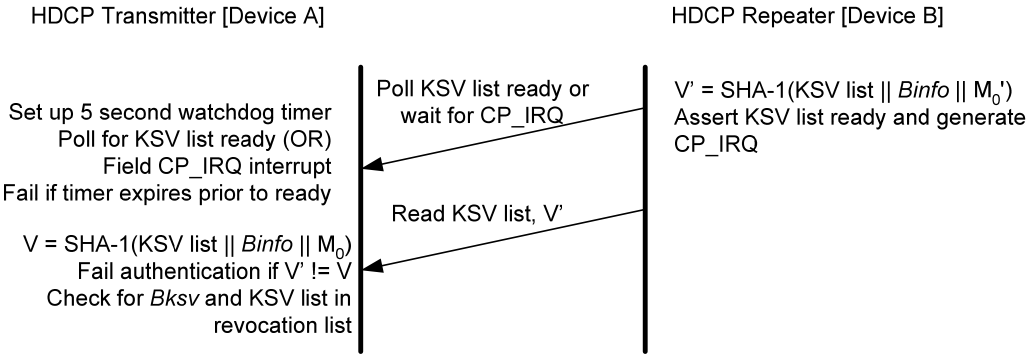
HDCP Transmitter [Device A]
HDCP Repeater [Device B]
Set up 5 second watchdog timer
Poll for KSV list ready (OR)
Field CP_IRQ interrupt
Fail if timer expires prior to ready
Poll KSV list ready or wait for CP_IRQ
V' = SHA-1(KSV list || *Binfo* || M_0')
Assert KSV list ready and generate CP_IRQ
Read KSV list, V'
V = SHA-1(KSV list || *Binfo* || M_0)
Fail authentication if V' != V
Check for *Bksv* and KSV list in revocation list

Figure 2-2. Second Part of Authentication Protocol

HDCP Repeaters assemble the list of all attached downstream HDCP Receivers as the downstream HDCP-protected Interface Ports of the HDCP Repeater complete the authentication protocol with attached HDCP Receivers. The list is represented by a contiguous set of bytes, with each KSV occupying five bytes stored in little-endian order. The total length of the KSV list is five bytes times the total number of attached and active downstream HDCP Devices, including downstream HDCP Repeaters. An HDCP-protected Interface Port with no active device attached adds nothing to the list. Also, the KSV of the HDCP Repeater itself at any level is not included in its own KSV list. An HDCP-protected Interface Port connected to an HDCP Receiver that is not an HDCP Repeater adds the *Bksv* of the attached HDCP Receiver to the list. HDCP-protected Interface Ports that have an HDCP Repeater attached add the KSV list read from the attached downstream HDCP Repeater, plus the *Bksv* of the attached downstream HDCP Repeater itself. In order to add the KSV list of the attached HDCP Repeater, it is necessary for the HDCP Repeater to verify the integrity of the list by computing *V* and checking this value against *V*' received from the attached HDCP Repeater. If *V* does not equal *V*', the downstream KSV list integrity check fails, and the HDCP Repeater must not assert its READY status and must not assert CP_IRQ. Upstream HDCP Transmitters will detect this failure by the expiration of a watchdog timer set in the HDCP Transmitter.

When the HDCP Repeater has assembled the complete list of attached HDCP Devices' KSVs, it computes the verification value *V'*. This value is the SHA–1 hash of the concatenation of the KSV list, *Binfo*, and the secret value M_0'. When constructing the byte stream for the SHA-1 input, the

KSV list is in the same little-endian byte order in which it is transmitted over the link, *Binfo* is appended in little-endian order, and M_0 is also appended in little-endian order. When both the KSV list and *V'* are available, the HDCP Repeater asserts its READY status indicator and asserts the CP_IRQ interrupt.

The HDCP Transmitter, having determined that the REPEATER bit read earlier in the protocol is set, sets a five-second watchdog timer. It may either poll the HDCP Repeater's READY status bit or alternatively check the READY bit when a CP_IRQ interrupt is received. When READY is set, the HDCP Transmitter reads the KSV list and *V'* from the HDCP Repeater. The HDCP Transmitter verifies the integrity of the KSV list by computing the SHA–1 hash value *V* and comparing this value to *V'*. If *V* is not equal to *V'*, the HDCP Transmitter must re-read the KSV list, *Binfo* and *V'* two additional times (for a total of three consecutive *V'* checks) to account for the possibility of link errors. The authentication protocol is aborted on three consecutive mismatches between *V* and *V'* and authentication can be reattempted with the transmission of new *An* and the *Aksv*.

If the asserted READY status is not received by the HDCP Transmitter within a maximum-permitted time of five seconds, authentication of the HDCP Repeater fails. With this failure, the HDCP Transmitter aborts the authentication protocol with the HDCP Repeater. Authentication can be reattempted with the transmission of a new *An* and the *Aksv*.

In addition to assembling the KSV list, an HDCP Repeater propagates topology information upward through the connection tree to the HDCP Transmitter. An HDCP Repeater reports the topology status variables DEVICE_COUNT and DEPTH. The DEVICE_COUNT for an HDCP Repeater is equal to the total number of attached downstream HDCP Receivers and HDCP Repeaters. The value is calculated as the sum of the number of attached downstream HDCP Receivers and HDCP Repeaters plus the sum of the DEVICE_COUNT read from all attached HDCP Repeaters. The DEPTH status for an HDCP Repeater is equal to the maximum number of connection levels below any of the downstream HDCP-protected Interface Ports. The value is calculated as the maximum DEPTH reported from downstream HDCP Repeaters plus one (accounting for the attached downstream HDCP Repeater).

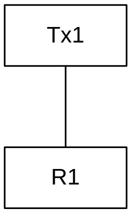

Figure 2-3. DEPTH and DEVICE_COUNT for HDCP Repeater

In Figure 2-3 above, R1 has zero downstream HDCP Devices and reports a value of zero for both the DEPTH and the DEVICE_COUNT.

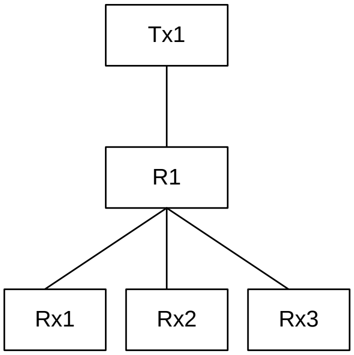

Figure 2-4. DEPTH and DEVICE_COUNT for HDCP Repeater

In Figure 2-4 above, R1 has three downstream HDCP Receivers connected to it. It reports a DEPTH of one and a DEVICE_COUNT of three.

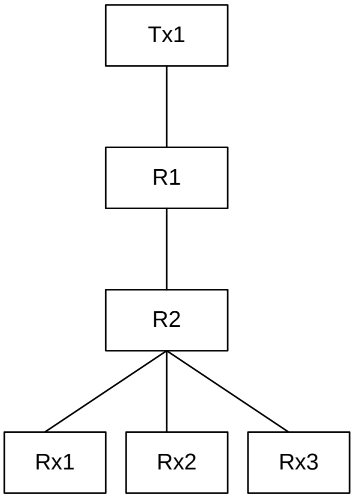

Figure 2-5. DEPTH and DEVICE_COUNT for HDCP Repeater

In Figure 2-5 above, R1 reports a DEPTH of two and a DEVICE_COUNT of four.

HDCP Repeaters must be capable of supporting DEVICE_COUNT values less than or equal to 127 and DEPTH values less than or equal to 7. If the computed DEVICE_COUNT for an HDCP Repeater exceeds 127, the HDCP Repeater must assert the MAX_DEVS_EXCEEDED status bit. If the computed DEPTH for an HDCP Repeater exceeds seven, the HDCP Repeater must assert the MAX_CASCADE_EXCEEDED status bit. When an HDCP Repeater receives a MAX_DEVS_EXCEEDED or a MAX_CASCADE_EXCEEDED status from a downstream HDCP Repeater, it must assert the corresponding status bits to the upstream HDCP Transmitter, assert the READY bit and assert the CP_IRQ interrupt.

In a dual link HDCP Repeater (e.g. Dual Link DisplayPort Converters), the repeater combines the topology information for both links in to a single KSV list. DisplayPort converters must remove duplicate KSV information in the list. Duplicate KSV values may result from downstream dual link HDCP devices sharing the same KSV on both links. In this case, the DisplayPort converter increments DEVICE_COUNT by one to account for the downstream dual link device. If a downstream dual link HDCP device contains different sets of KSVs on both links, the DisplayPort converter increments DEVICE_COUNT by two to account for the downstream dual link device and sets the MAX_DEVS_EXCEEDED bit when the total number of KSVs received by the DisplayPort converter exceeds 127.

For example, consider a dual link DisplayPort converter that has 65 downstream dual link HDCP devices connected to it and each device shares the same set of KSV across both its links. The converter removes duplicate KSVs from its KSV list resulting in 65 unique KSVs and sets DEVICE_COUNT to 65. Consider the case where a dual link DisplayPort converter has 65 downstream dual link HDCP devices connected to it and each device contains different KSVs on both its links. The DisplayPort converter receives 130 unique KSVs and sets the MAX_DEVS_EXCEEDED bit.

Authentication fails if the topology maximums are exceeded. The top-level HDCP Transmitter checks to see if the KSV of any attached device is found in the current revocation list, and, if present, the authentication fails. The HDCP Transmitter verifies the integrity of the current revocation list by checking the signature of the system renewability message (SRM) using the

Digital Content Protection LLC public key. Failure of this integrity check constitutes an authentication failure.

The top-level HDCP Transmitter must complete the second phase of authentication within 1 minute after the assertion of READY by the downstream HDCP Repeater. When a new SRM version is received, the top-level HDCP Transmitter must complete SRM updates (see Section 7.2) and must complete verification of KSVs of attached devices against the revocation list within 1 minute after the new SRM is received.

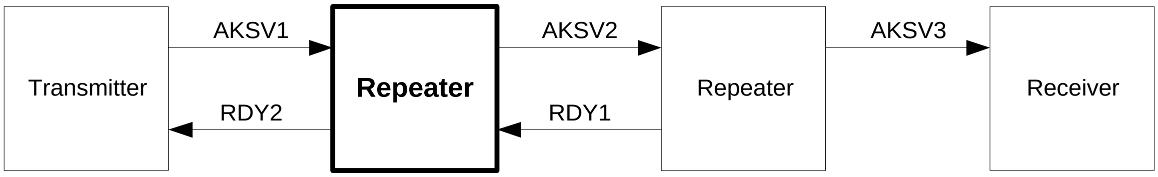

Figure 2-6. Multi-level Repeater Protocol Signals

From	To	Max Delay	Conditions and Comments
AKSV1 Upstream HDCP Transmitter *Aksv* received	AKSV2 HDCP Repeater's *Aksv* transmitted downstream	100 ms	Downstream propagation time. To latest *Aksv* transmission when more than one HDCP Receiver is attached.
AKSV3 *Aksv* transmitted to all downstream HDCP-protected Interface Ports	RDY1 Upstream READY asserted	500 ms	Upstream propagation time when no downstream HDCP Repeaters are attached. (no downstream KSV lists to process)
RDY1 Downstream READY asserted	RDY2 Upstream READY asserted	500 ms	Upstream propagation time when one or more HDCP Repeaters are attached. From latest downstream READY. (downstream KSV lists must be processed)
AKSV1 Upstream HDCP Transmitter transmits *Aksv*	RDY2 Upstream HDCP Transmitter polls asserted READY	4.2 seconds	For the Maximum of seven repeater levels, 7 * (100 ms + 500 ms)

Table 2-1. HDCP Repeater Protocol Timing Requirements

Table 2-1 specifies HDCP Repeater timing requirements that bound the worst-case propagation time for the KSV list. Note that because each HDCP Repeater does not know the number of downstream HDCP Repeaters, it must use the same five-second timeout used by the upstream HDCP Transmitter when polling for downstream READY.

2.2.3 Link Integrity Check in MST Mode

After successful completion of the first part of authentication, HDCP Encryption is enabled by the HDCP Transmitter. Once encryption is enabled, a periodic Link Integrity Check is performed to maintain cipher synchronization between the HDCP Transmitter and the HDCP Receiver. This section describes the link integrity check implemented in the MST mode.

To perform link integrity check, two MTPH timeslots immediately following SR are used to transmit a known 16-bit pattern, 0x531F, from the transmitter to the receiver. This pattern is referred to as LINK_VERIFICATION_PATTERN and is transmitted least significant byte first. . The LINK_VERIFICATION_PATTERN is duplicated per lane on 2-lane and 4-lane Main Links. The transmitter sets the two MTPH timeslots following a given SR symbol to the corresponding byte of the pattern, encrypts the MTPHs and sends the MTPHs to the receiver. The receiver decrypts the MTPHs and compares the decrypted byte values to the corresponding byte in the LINK_VERIFICATION_PATTERN. If the received pattern, which is transmitted least significant byte first, matches the LINK_VERIFICATION_PATTERN at the receiver, it indicates that the ciphers are in sync. An error is determined to have occurred if the decrypted byte does not match the corresponding byte in the LINK_VERIFICATION_PATTERN. No error correction techniques (e.g., majority voting) should be applied to the MTPH timeslots used to transmit the LINK_VERIFICATION_PATTERN. HDCP Encryption is only applied to the MTPH timeslots used to transmit LINK_VERIFICATION_PATTERN, other MTPH timeslots must not be encrypted.

A link integrity failure is determined to have occurred if pattern mismatches at the receiver are detected for three successive link frame periods. Three successive link frame periods are checked to enable recovery from simple transient synchronization errors (e.g., random bit error bursts). If a failure is detected within three successive link frames then the receiver has experienced a non-recoverable loss of cipher synchronization.

On detecting an unrecoverable loss of cipher synchronization , the HDCP Receiver must assert the LINK_INTEGRITY_FAILURE bit in the *Bstatus* register and generate a CP_IRQ interrupt. On receiving a CP_IRQ interrupt, the HDCP Transmitter is required to read the *Bstatus* register to determine the cause of the interrupt. The HDCP Transmitter must disable HDCP Encryption at the SR boundary as soon as feasible after receiving the CP_IRQ interrupt from the HDCP Receiver if the LINK_INTEGRITY_FAILURE bit is set and must initiate re-authentication with the transmission of a new *An* and *Aksv.*

2.2.4 Link Integrity Check in SST Mode

This section describes the link integrity check implemented in the SST mode.

To perform link integrity check, Bit 5 of VB-ID is used to transmit a known 16-bit pattern, 0x531F, from the transmitter to the receiver one bit at a time. This pattern is referred to as LINK_VERIFICATION_PATTERN. The VB-ID is transmitted on all lanes after every BS/SR/CPBS/CPSR symbol, as described in the DisplayPort Specification. It is transmitted once per lane for 4-lane Main Link, twice per lane for 2-lane Main Link, and four times for 1-lane Main Link, resulting in a total of four VB-ID's following each CPSR. The LINK_VERIFICATION_PATTERN is continuously and repeatedly transmitted least significant bit first. All four VB-ID's following each CPSR shall carry the same Bit 5 value. After every CPSR symbol the pattern transmission is restarted, inserting the LSB of the pattern in all VB-IDs associated with the CPSR symbol. The transmitter sets Bit 5 of the VB-ID symbol associated with a given CPBS/CPSR symbol to the corresponding pattern bit value, encrypts the VB-ID and sends the VB-ID to the receiver. The receiver decrypts the VB-ID and compares Bit 5 of VB-ID to the corresponding bit value in the LINK_VERIFICATION_PATTERN. If the received pattern, which is transmitted one bit at a time, matches the LINK_VERIFICATION_PATTERN at the receiver, it indicates that the ciphers are in sync. An error is determined to have occurred if the bit pattern in any of the VB-ID symbols is found to not match the expected bit of the LINK_VERIFICATION_PATTERN. No error correction techniques (e.g., majority voting) should be applied to Bit 5 of the VB-ID symbols associated with a given CPBS/CPSR symbol.

A link integrity failure is determined to have occurred if three consecutive pattern mismatches at the receiver (in 16 * 3 = 48 VB-ID transmissions) are detected within two successive frame periods. Two successive frame periods are checked to enable recovery from simple transient synchronization errors (e.g., random bit error bursts). If a failure is detected within two successive frames then the receiver has experienced a non-recoverable loss of cipher synchronization. The state machine shown in Figure 2-7 illustrates the expected HDCP Receiver link integrity check behavior.

On detecting an unrecoverable loss of cipher synchronization (e.g., transition from "Check 2nd Frame" to "Disable Pending" in Figure 2-7), the HDCP Receiver must assert the LINK_INTEGRITY_FAILURE bit in the *Bstatus* register and generate a CP_IRQ interrupt. On receiving a CP_IRQ interrupt, the HDCP Transmitter is required to read the *Bstatus* register to determine the cause of the interrupt. The HDCP Transmitter must disable HDCP Encryption at the CPSR/SR transmission boundary as soon as feasible after receiving the CP_IRQ interrupt from the HDCP Receiver if the LINK_INTEGRITY_FAILURE bit is set and must initiate re-authentication with the transmission of a new *An* and *Aksv*.

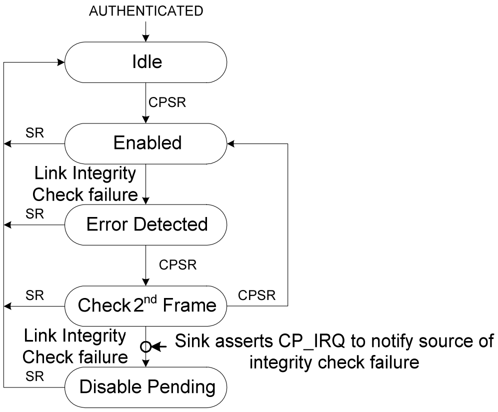

Figure 2-7. HDCP Receiver Link Integrity Check State Machine

2.3 HDCP Transmitter State Diagram

The HDCP Transmitter Link State Diagram and HDCP Transmitter Authentication Protocol State Diagram (Figure 2-8 and Figure 2-9) illustrate the operation states of the authentication protocol for an HDCP Transmitter that is not an HDCP Repeater. For HDCP Repeaters, the downstream (HDCP Transmitter) side is covered in Section 2.5.3.

Transmitter's decision to begin authentication is dependent on events such as hot plug detection of an HDCP Receiver, availability of premium content or other implementation dependent details in the transmitter. HDCP Receivers are not required to authenticate unless the main link is initialized. An HDCP Receiver must be ready to authenticate when it responds with its *Bcaps* register value upstream. In the event of authentication failure, it must be prepared to process subsequent authentication attempts. The HDCP Transmitter should not attempt to authenticate until it has successfully obtained the contents of the receiver's *Bcaps* register. In the case of an authentication failure, authentication can be reattempted with the transmission of new *An* and *Aksv*. The HDCP Transmitter may cease to attempt authentication for transmitter-specific reasons, which include fielding hot plug detach.

The HDCP Transmitter reads HDCP registers of the HDCP Receiver using AUX transactions. It handles HDCP register read failures (in terms of re-try attempts) in a manner consistent with other DPCD register read failures.

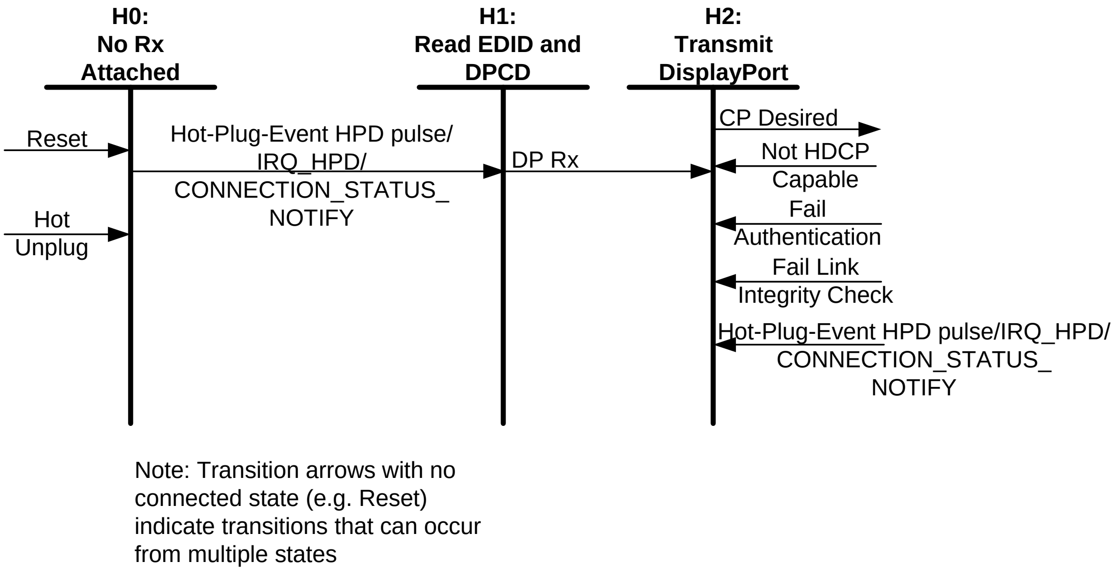

Figure 2-8. HDCP Transmitter Link State Diagram

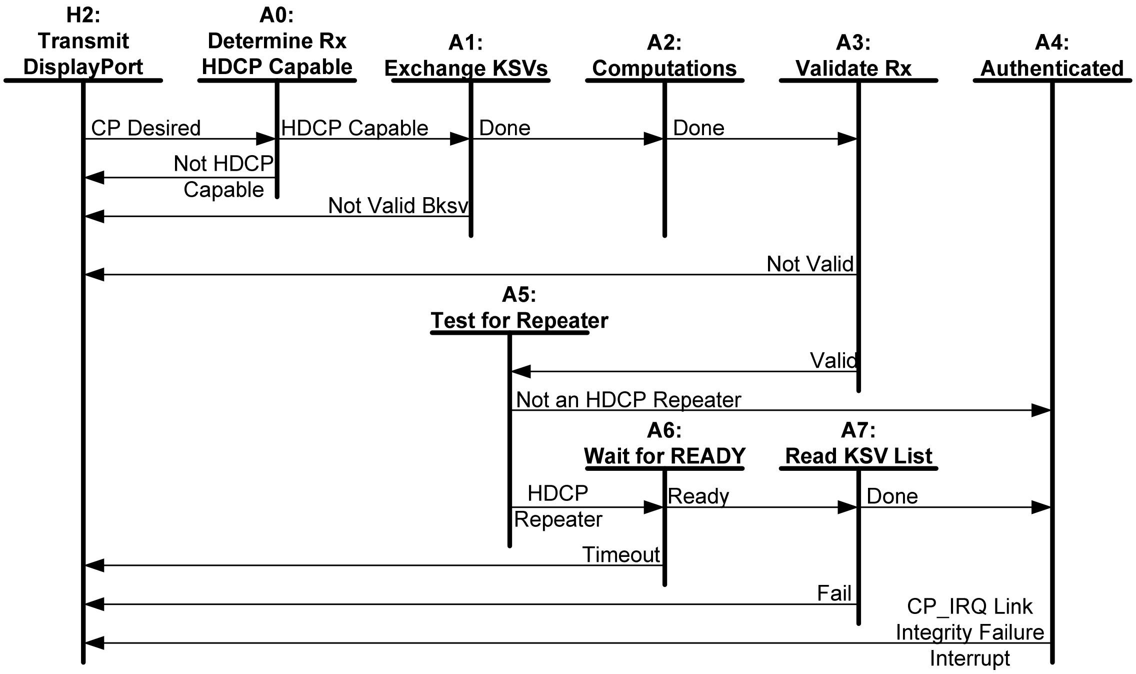

Figure 2-9. HDCP Transmitter Authentication Protocol State Diagram

Transition Any State:H0. Reset conditions at the HDCP Transmitter or hot unplug of all HDCP capable receivers cause the HDCP Transmitter to enter the No Receiver Attached state.

Transition H0:H1. The detection of a sink device (through Hot-Plug-Event HPD pulse or IRQ_HPD or CONNECTION_STATUS_NOTIFY message) indicates to the transmitter that a sink device is attached and that the EDID ROM and DPCD are available for reading. This is sufficient indication to the transmitter that the receiver is available and active (ready to display received content). When the receiver is no longer active, the transmitter is notified through hot unplug.

State H1: Read EDID and DPCD. The HDCP Transmitter reads the EDID to determine the type of sink device attached. EDID and DPCD contain information about the sink device capabilities. Additionally, the HDCP Transmitter also initializes the main link by performing link training.

Transition H1:H2. The transmitter enters the Transmit DisplayPort state only after determining that the attached sink device is a Display Port sink device.

State H2: Transmit DisplayPort. In this state the transmitter should begin sending an unencrypted signal with HDCP Encryption disabled after the receiver is made active. In some types of transmitters, the transmitted signal can be a low value content or informative on-screen display, and it could be available immediately, while in other types of transmitters, there may be an additional step of making the connected receiver active before any content is displayed. If video signal is being transmitted by the HDCP Transmitter, this will ensure that a valid video signal is displayed to the user before and during authentication.

The transmitter transitions to this state from any state whenever it determines using mechanisms provided in the DisplayPort specification that the received IRQ_HPD, Hot-Plug-Event HPD pulse or CONNECTION_STATUS_NOTIFY message was due to the connection of an HDCP Receiver that was previously not authenticated and that HDCP Content is to be transmitted to that HDCP Receiver. The transmitter may transition to this state when it determines that the received IRQ_HPD, CONNECTION_STATUS_NOTIFY message or Hot-Plug-Event HPD pulse was due to re-connect of a previously authenticated HDCP Receiver to which HDCP Content is to be transmitted. This transition also occurs when an IRQ_HPD is received in response to a re-authentication event.

Transition H2:A0. If content protection is desired by the Upstream Content Control Function, then the HDCP Transmitter should immediately attempt to determine whether the receiver is HDCP capable.

State A0: Determine Rx HDCP Capable. In this state, the transmitter reads the HDCP_CAPABLE bit in the receiver's *Bcaps* register. If this bit is set to 1, it indicates that the receiver is HDCP capable. Since state A0 is reached when content protection is desired by the Upstream Content Control Function, authentication must be started immediately by the transmitter. If video signal is being transmitted by the HDCP Transmitter, a valid video screen is displayed to the user with encryption disabled during this time.

Transition A0:H2. If *Bcaps* HDCP_CAPABLE bit is zero or unavailable, it indicates that the receiver is not HDCP capable. The transmitter continues to transmit low value content or informative on-screen display.

Transition A0:A1. If *Bcaps* HDCP_CAPABLE bit is set to 1, the transmitter initiates the authentication protocol.

State A1:Exchange KSVs. In this state, the HDCP Transmitter generates a 64-bit pseudo-random value (*An*) and writes that value to the HDCP Receiver. The transmitter also writes its KSV (*Aksv)*. It reads the HDCP Receiver's KSV (*Bksv*) and the REPEATER status bit necessary for cipher initialization. Generation of *An* using the HDCP Cipher is described in Section 4.5. After the HDCP Transmitter has written *An* and *Aksv* and read the receiver's *Bksv* and the REPEATER bit, it sets the REAUTHENTICATION_ENABLE_IRQ_HPD bit in the Ainfo register if the REPEATER bit is set and the transmitter determines that the downstream HDCP Repeater supports DPCD Revision 1.2 or higher.

Transition A1:H2. Failure to read *Bksv* containing 20 zeros and 20 ones is considered a protocol failure and causes this state transition to State H2.

Transition A1:A2. The random value *An* and HDCP Transmitter KSV have been written, and a valid HDCP Receiver *Bksv* and REPEATER bit have been read. HDCP Transmitter has confirmed that *Bksv* contains 20 ones and 20 zeros.

State A2: Computations. In this state, the HDCP Transmitter computes the values *Km*, *Ks*, $M_{0,}$ and R_0, using the HDCP Transmitter's Device Private Keys, *Bksv* read during State A1, and the random number *An* written to the HDCP Receiver during state A1.

Transition A2:A3. When the computed results from State A2 are available, the HDCP Transmitter proceeds to State A3.

State A3: Validate Receiver. The HDCP Transmitter reads R0' from the HDCP Receiver and compares it with the corresponding R0 produced by the HDCP Transmitter during the computations of State A2. If R0 is equal to R0', then HDCP Encryption is immediately enabled. The HDCP Transmitter must allow the HDCP Receiver at least 100 ms to make R0' available from the time that Aksv is written although the HDCP Receiver can generate notify availability of R0' using the CP_IRQ interrupt sooner than this 100 ms time period. The HDCP Transmitter also checks the current revocation list for the HDCP Receiver's KSV Bksv. If Bksv is in the revocation list, then the HDCP Receiver is considered to have failed the authentication. Note: checking the revocation list for Bksv may begin as soon as the Bksv has been read in State A1, asynchronously to the other portions of the protocol. The HDCP Transmitter must complete verification of the Bksv against the revocation list within 1 minute after the Bksv has been read by the HDCP Transmitter. However, if an HDCP Repeater is attached to the transmitter, the transmitter may defer revocation checking until the second phase of the authentication protocol.

The integrity of the current revocation list must be verified by checking the signature of the SRM using the Digital Content Protection LLC public key, as specified in Section 7.

Transition A3:H2. The link integrity message R_0' received from the HDCP Receiver does not match the value calculated by the HDCP Transmitter, or *Bksv* is in the current revocation list.

Transition A3:A5. The link integrity message R_0' received from the HDCP Receiver matches the expected value calculated by the HDCP Transmitter and *Bksv* is not in the current revocation list.

State A4: Authenticated. The HDCP Transmitter has completed the authentication protocol. At this time, and at no time prior, the HDCP System makes available to the Upstream Content Control Function upon request, information that indicates that the HDCP System is fully engaged and able to deliver HDCP Content, which means (a) HDCP Encryption is operational on each downstream HDCP-protected Interface Port attached to an HDCP Receiver, (b) processing of valid received SRMs, if any, has occurred, as defined in this Specification, and (c) there are no HDCP Receivers on HDCP-protected Interface Ports, or downstream, with KSVs in the current revocation list.

State A5: Test for Repeater. The HDCP Transmitter evaluates the state of the HDCP Repeater capability bit (REPEATER) that was read in State A1.

Transition A5:A4. The REPEATER bit is not set (the HDCP Receiver is not an HDCP Repeater).

Transition A5:A6. The REPEATER bit is set (the HDCP Receiver is an HDCP Repeater).

State A6: Wait for Ready. The HDCP Transmitter sets up a five-second watchdog timer and either polls the HDCP Receiver's READY bit or resumes further processing based on the CP_IRQ interrupt.

Transition A6:H2. The watchdog timer expires before the READY indication is received.

Transition A6:A7. READY is asserted and is detected by the HDCP Transmitter when polling, or when *Bstatus* register is read while processing a CP_IRQ interrupt.

State A7: Read KSV List. The watchdog timer is cleared. The HDCP Transmitter reads the list of attached KSVs from the KSV FIFO, reads *V'*, computes *V,* and verifies *V* == *V'*, and the KSVs from the list are compared against the current revocation list.

The integrity of the current revocation list must be verified by checking the signature of the SRM using the Digital Content Protection LLC public key, as specified in Section 7.

The above operations must be completed by the HDCP Transmitter within 1 minute after the assertion of READY by the downstream HDCP Repeater.

Transition A7:H2. This transition is made if *V* != *V'*, verification of the SRM fails, or if any of the KSVs in the list are found in the current revocation list. If *V* is not equal to *V'*, the HDCP Transmitter must re-read the KSV list, *Binfo* and *V'* two additional times (for a total of three consecutive *V'* checks) to account for the possibility of link errors. Two additional status bits cause this transition when asserted. These are MAX_CASCADE_EXCEEDED and MAX_DEVS_EXCEEDED.

Transition A7:A4. If *V* == *V'*, the SRM is valid, none of the reported KSVs are in the current revocation list, and the downstream topology does not exceed specified maximums.

Transition A4:H2. On receiving a CP_IRQ interrupt, the HDCP Transmitter reads the *Bstatus* register to determine the cause of the interrupt. The HDCP Transmitter must disable HDCP Encryption at the link frame boundary in MST mode and at the CPSR/SR transmission boundary in the SST mode as soon as feasible after receiving the CP_IRQ interrupt from the HDCP Receiver if the LINK_INTEGRITY_FAILURE bit is set and must initiate re-authentication with the transmission of a new *An* and *Aksv.*

2.4 HDCP Receiver State Diagram

The operation states of the authentication protocol for an HDCP Receiver that is not an HDCP Repeater are illustrated in Figure 2-10. For HDCP Repeaters, the upstream (HDCP Receiver) side is covered in Section 2.5.4.

The HDCP Receiver must be ready to re-authenticate with the HDCP Transmitter at any point in time. In particular, the only indication to the HDCP Receiver of a re-authentication attempt by the HDCP Transmitter is the reception of *An* and *Aksv* from the HDCP Transmitter.

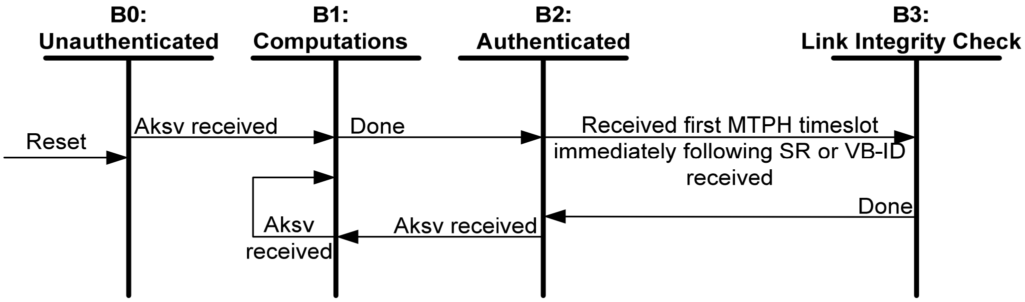

Figure 2-10. HDCP Receiver Authentication State Diagram

Transition Any State:B0. Reset conditions at the HDCP Receiver cause the HDCP Receiver to enter the unauthenticated state.

State B0: Unauthenticated. The HDCP Receiver is awaiting the reception of *An* and *Aksv* from the HDCP Transmitter to trigger the authentication protocol.

Transition B0:B1. The final byte of *Aksv* is received from the HDCP Transmitter.

State B1: Computations. In this state, the HDCP Receiver calculates the values *Km*', *Ks*', M_0', and R_0' using the HDCP Receiver's Device Private Keys and the received values of *An* and *Aksv*. The HDCP Receiver must complete the computations within 100 milliseconds and make R_0' available to the HDCP Transmitter.

Transition B1: B1. Should the HDCP Transmitter write a new *An* and its *Aksv* while the HDCP Receiver is in State B1, the HDCP Receiver abandons intermediate results and restarts the computations.

Transition B1:B2. The computations are complete and the results are available for reading by the HDCP Transmitter. The HDCP Receiver must set the R_0'_AVAILABLE bit in the *Bstatus* register and generate the CP_IRQ interrupt.

State B2: Authenticated. The HDCP Receiver has completed the authentication protocol and is ready to generate the first frame key when signaled by the HDCP Transmitter.

Transition B2:B1. A new authentication is forced any time a new *An* and the *Aksv* are written by the attached HDCP Transmitter.

Transition B2:B3. This transition is made when the first MTPH timeslot immediately following SR is received in the MST mode or a VB-ID is received in the SST mode. The receiver proceeds to check for loss of cipher synchronization.

State B3: Link Integrity Check. The receiver performs link integrity check as explained in Section 2.2.3 and Section 2.2.4 after it has received the two MTPH timeslots immediately following SR in the MST mode or when a VB-ID is received in the SST mode. If a loss of cipher synchronization is detected, the receiver sets the *Bstatus* LINK_INTEGRITY_FAILURE bit and generates a CP_IRQ interrupt.

Transition B3:B2. After the link integrity check, the receiver returns to the authenticated state.

2.5 HDCP Repeater State Diagrams

The HDCP Repeater has one HDCP-protected Interface connection to an upstream HDCP Transmitter and one or more HDCP-protected Interface connections to downstream HDCP Receivers as permitted in the Digital Content Protection LLC license. The state diagram for each downstream connection (Figure 2-13 and Figure 2-14) is substantially the same as that for the host HDCP Transmitter (Section 2.3), with two exceptions. First, the HDCP Repeater is not required to check for downstream KSVs in a revocation list. Second, the HDCP Repeater initiates authentication downstream when it receives an authentication request from upstream, rather than at detection of an HDCP Receiver on the downstream HDCP-protected Interface Port.

The HDCP Repeater signals the detection of an active downstream HDCP Receiver to the upstream HDCP Transmitter by either propagating the CONNECTION_STATUS_NOTIFY message to indicate plug of an active HDCP Receiver when the most upstream HDCP Transmitter is capable of operating in the MST mode (MST-capable) or by pulsing IRQ_HPD when the most upstream HDCP Transmitter is capable of operating only in the SST mode (SST-capable only).

HDCP Repeaters that have no active downstream HDCP devices must be considered. The HDCP Repeater may authenticate as an HDCP Receiver with *Bcaps* REPEATER bit set to 0 if it wishes to receive HDCP Content, but may not pass HDCP Content to downstream devices. If an HDCP Transmitter encounters a downstream HDCP Repeater reporting zero DEVICE_COUNT and sends it HDCP Content, it must complete the second phase of authentication successfully, computing V over an empty KSV list.

2.5.1 Propagation of Topology Errors

MAX_DEVS_EXCEEDED and MAX_CASCADE_EXCEEDED: If the computed DEVICE_COUNT for an HDCP Repeater exceeds 127, the HDCP Repeater must assert the MAX_DEVS_EXCEEDED status bit. If the computed DEPTH for an HDCP Repeater exceeds seven, the HDCP Repeater must assert the MAX_CASCADE_EXCEEDED status bit. When an HDCP Repeater receives a MAX_DEVS_EXCEEDED or a MAX_CASCADE_EXCEEDED status from a downstream HDCP Repeater, it is required to assert the corresponding status bits to the upstream HDCP Transmitter, set the READY bit and raise the CP_IRQ interrupt.

2.5.2 Propagation of Re-authentication Events and Topology Changes

2.5.2.1 Topology Change Due to Receiver Connection

When an active HDCP Receiver that was previously not authenticated is connected to the downstream side, the most upstream HDCP Transmitter must be immediately notified of the resulting topology change.

The downstream side must initiate authentication with the HDCP Receiver only after it receives an Upstream Authentication Request.

If the upstream HDCP Device is not MST-capable and has not enabled IRQ_HPD for upstream notification as described in the DisplayPort specification, the HDCP Repeater propagates a Hot-Plug-Event HPD pulse in response to a new receiver connection.

If the most upstream HDCP Transmitter is MST-capable, a CONNECTION_STATUS_NOTIFY message to indicate the receiver plug event must immediately be propagated to the most upstream HDCP Transmitter.

If the most upstream HDCP Transmitter is SST-capable only and has enabled IRQ_HPD for upstream notification by the HDCP Repeater, an IRQ_HPD signal must immediately be propagated to the most upstream HDCP Transmitter. When an HDCP Repeater receives an IRQ_HPD from the downstream HDCP Repeater, it must immediately pulse the IRQ_HPD upstream.

If the most upstream HDCP Transmitter determines using mechanisms provided in the DisplayPort specification that the received CONNECTION_STATUS_NOTIFY, IRQ_HPD or Hot-Plug-Event HPD pulse was due to the connection of an HDCP Receiver that was previously not authenticated and that HDCP Content is to be transmitted to that HDCP Receiver, it must initiate re-authentication.

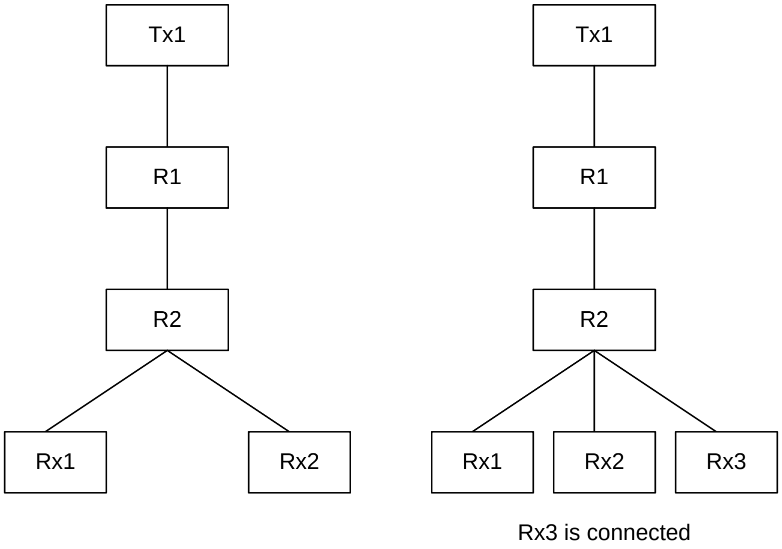

Figure 2-11. HPD Propagation on Connection of Active HDCP Receiver

In Figure 2-11, all the devices are authenticated and HDCP Content is flowing. Connection of an active HDCP Receiver Rx3 must result in an IRQ_HPD pulse to Tx1 if Tx1 is SST-capable only or a CONNECTION_STATUS_NOTIFY message to Tx1 if Tx1 is MST-capable. Tx1 must immediately initiate re-authentication if it determines that the IRQ_HPD or CONNECTION_STATUS_NOTIFY message was due to a new HDCP Receiver plug event and that HDCP Content is to be transmitted to that HDCP Receiver.

2.5.2.2 Topology Change Due to Disconnect or Reconnect of a Receiver

The authenticated upstream connection of the HDCP Repeater must not enter an unauthenticated state if an authenticated HDCP Receiver is disconnected from the downstream HDCP-protected Interface Port of the repeater. Also, if an authenticated HDCP Receiver attached to the downstream side of the repeater is disconnected and reconnected (i.e. the downstream HDCP Repeater side sees the same KSV stored in its KSV list at the HDCP protected interface port), the upstream side of the repeater must not become unauthenticated. The downstream side is required to only re-authenticate the attached HDCP Receiver.

Topology change notification to indicate disconnect or re-connect of the receiver must immediately be propagated to the most upstream HDCP Transmitter. When the most upstream HDCP Transmitter receives a topology change notification, it must determine using mechanisms provided in the DisplayPort specification that the topology change notification was due to an unplug event, it must not initiate re-authentication. If it determines that the topology change was due to re-connect of an active, authenticated HDCP Receiver attached to the downstream HDCP Repeater side and that HDCP Content is to be transmitted to that HDCP Receiver, it may initiate re-authentication. The topology change notification must be a CONNECTION_STATUS_NOTIFY message if the most upstream HDCP Transmitter is MST-capable and an IRQ_HPD generated in response to a topology change if the most upstream HDCP Transmitter is SST-capable only and has enabled IRQ_HPD for upstream notification by the HDCP Repeater.

If the upstream HDCP Device is not MST-capable and has not enabled IRQ_HPD for upstream notification as described in the DisplayPort specification, the HDCP Repeater propagates a Hot-Plug-Event HPD pulse in response to the unplug or re-connect event.

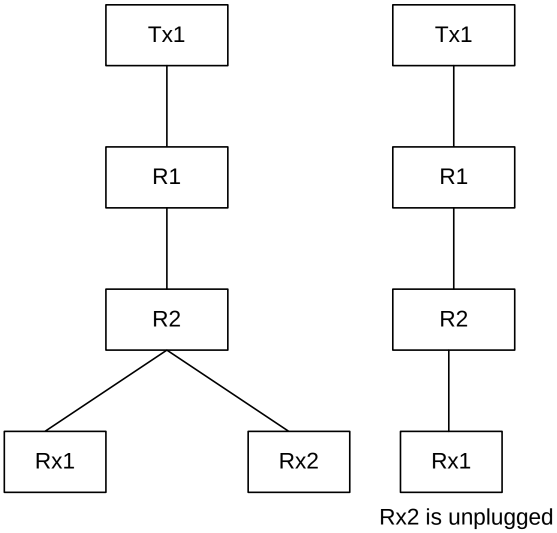

Figure 2-12. HPD Propagation on Unplug or Re-connect

In Figure 2-12, all the devices are authenticated and HDCP Content is flowing. Tx1 must not initiate re-authentication when it receives a CONNECTION_STATUS_NOTIFY message or an IRQ_HPD as a result of unplug of Rx2 and may initiate re-authentication on re-connect of Rx2 if HDCP Content is to be transmitted to Rx2.

2.5.2.3 Re-Authentication Events

The upstream side of the HDCP Repeater becomes unauthenticated when any downstream side enters the unauthenticated state due to authentication failures. Authentication failures on the downstream side of the HDCP Repeater are indicated by state transitions F1:P2, F3:P2, F6:P2 and F7:P2. When the upstream side becomes unauthenticated it signals the upstream HDCP Transmitter to initiate re-authentication.

When the upstream (HDCP Receiver) side of the HDCP Repeater becomes unauthenticated and the REAUTHENTICATION_ENABLE_IRQ_HPD is set to one by the upstream HDCP Transmitter, the upstream side of the HDCP Repeater asserts the REAUTHENTICATION_REQUEST bit in the *Bstatus* register, sets CP_IRQ status bit and generates IRQ_HPD upstream. On receiving a CP_IRQ interrupt, the upstream HDCP Transmitter is required to read the *Bstatus* register to determine the cause of the interrupt. The downstream HDCP Repeater side transitions into an unauthenticated state when a re-authentication request is received from the downstream repeater. The most upstream HDCP Transmitter must initiate re-authentication on reception of a CP_IRQ interrupt with the REAUTHENTICATION_REQUEST bit asserted in the *Bstatus* register.

When the upstream (HDCP Receiver) side of the HDCP Repeater becomes unauthenticated and the REAUTHENTICATION_ENABLE_IRQ_HPD is not set to one by the upstream HDCP Transmitter, the Hot-Plug-Event HPD pulse is used for upstream notification of re-authentication events.

On a new authentication request from the upstream HDCP Transmitter, the downstream side of the HDCP Repeater need not initiate re-authentication of all its authenticated downstream ports provided there have been no changes to the topology during the current HDCP session (i.e. downstream side of the HDCP Repeater has not received an IRQ_HPD pulse, Hot-Plug-Event HPD Pulse or CONNECTION_STATUS_NOTIFY) and all the downstream ports are either in an authenticated or unconnected state. The upstream HDCP Repeater connection may reuse the KSV list and topology information collected during the previous authentication session to complete the second part of authentication with the upstream HDCP Transmitter.

2.5.3 HDCP Repeater Downstream State Diagram

In this state diagram and its following description, the downstream (HDCP Transmitter) side refers to the HDCP Transmitter functionality within the HDCP Repeater for its corresponding downstream HDCP-protected Interface Port.

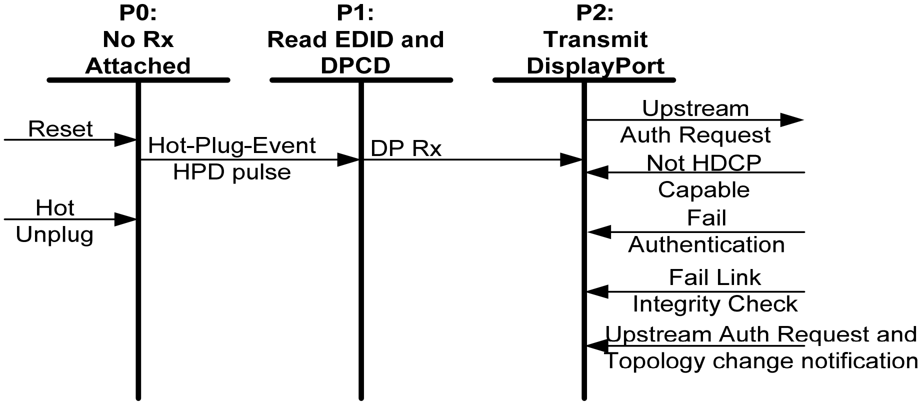

Figure 2-13. HDCP Repeater Downstream Link State Diagram

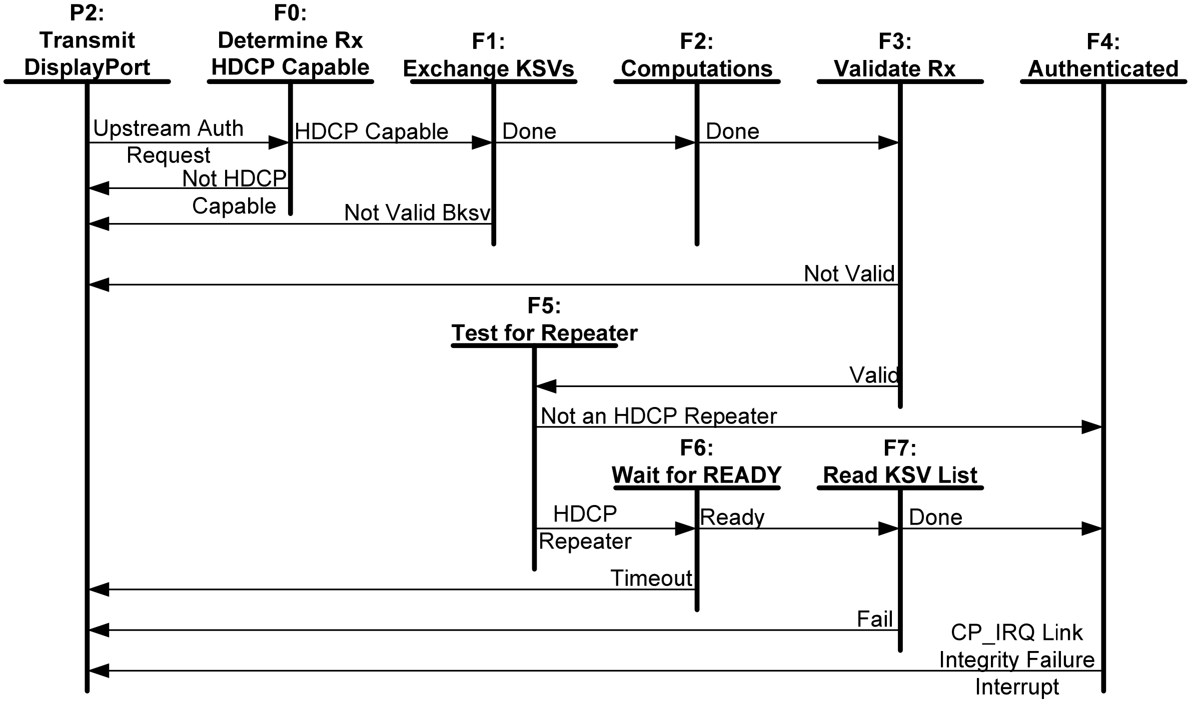

Figure 2-14. HDCP Repeater Downstream Authentication Protocol State Diagram

Transition Any State:P0. Reset conditions at the HDCP Repeater or hot unplug of all HDCP capable receivers cause the HDCP Repeater to enter the No Receiver Attached state.

Transition P0:P1. The detection of Hot Plug Detect indicates that a sink device is attached and that the EDID ROM and DPCD are available for reading. Reception of an HPD is sufficient indication that the receiver is available and active (ready to display received content). When the receiver is no longer active, the downstream (HDCP Transmitter) side is notified through hot unplug.

State P1: Read EDID and DPCD. The downstream side reads the EDID to determine the type of sink device attached. EDID and DPCD contain information about the sink device capabilities. Additionally, the downstream side also performs link training in this state.

Transition P1:P2. The downstream side enters the Transmit DisplayPort state only after determining that the attached sink device is a Display Port sink device.

State P2: Transmit DisplayPort. In this state the downstream side should begin sending the unencrypted video signal received from the upstream HDCP Transmitter with HDCP Encryption disabled.

The downstream side transitions to this state from any state when it receives an Upstream Authentication Request and downstream topology changes have occurred during the current HDCP session. In this case, the downstream side must transition to State F0 from State P2.

Transition P2:F0. Upon an Upstream Authentication Request, the downstream side should immediately attempt to determine whether the receiver is HDCP capable.

State F0: Determine Rx HDCP Capable. In this state, the downstream side reads the HDCP_CAPABLE bit in the receiver's *Bcaps* register. If this bit is set to 1, it indicates that the receiver is HDCP capable. Since state F0 is reached upon an Upstream Stream Authentication Request, authentication should be started immediately by the downstream side. If video signal is being transmitted by the HDCP Transmitter, a valid video screen is displayed to the user with encryption disabled during this time.

Transition F0:P2. If *Bcaps* HDCP_CAPABLE bit is zero, it indicates that the receiver is not HDCP capable. The downstream continues to transmit low value content or informative on-screen display received from the upstream HDCP Transmitter.

Transition F0:F1. If *Bcaps* HDCP_CAPABLE bit is set to 1, the downstream side initiates the authentication protocol.

State F1:Exchange KSVs. In this state, the downstream side generates a 64-bit pseudo-random value (*An*) and writes that value to the HDCP Receiver. The downstream side also writes its KSV (*Aksv)*. It reads the HDCP Receiver's KSV (*Bksv*) and the REPEATER status bit necessary for cipher initialization. Generation of *An* using the HDCP Cipher is described in Section 4.5. After the downstream side has written *An* and *Aksv* and read the receiver's *Bksv* and the REPEATER bit, it sets the REAUTHENTICATION_ENABLE_IRQ_HPD bit in the Ainfo register if the REPEATER bit is set and the downstream side determines that the downstream HDCP Repeater supports DPCD Revision 1.2 or higher.

Transition F1:P2. Failure to read *Bksv* containing 20 zeros and 20 ones is considered a protocol failure and causes this state transition to State P2.

Transition F1:F2. The random value *An* and downstream side (HDCP Transmitter) KSV have been written, and a valid HDCP Receiver *Bksv* and REPEATER bit have been read. The downstream side has confirmed that *Bksv* contains 20 ones and 20 zeros.

State F2: Computations. In this state, the downstream side computes the values *Km*, *Ks*, M_0, and R_0, using the its Device Private Keys, *Bksv* read during State F1, and the random number *An* written to the HDCP Receiver during State F1.

Transition F2:F3. When the computed results from State F2 are available, the downstream side proceeds to State F3.

State F3: Validate Receiver. The downstream side reads R_0' from the HDCP Receiver and compares it with the corresponding R_0 produced by the HDCP Transmitter during the computations of State F2. If R_0 is equal to R_0', then HDCP Encryption is immediately enabled. The downstream side must allow the HDCP Receiver at least 100 ms to make R_0' available from the time that *Aksv* is written although the HDCP Receiver can generate notify availability of R_0' using the CP_IRQ interrupt sooner than this 100msec time period. The HDCP Receiver's *Bksv* is added to the KSV list for this HDCP Repeater.

Transition F3:P2. The link integrity message R_0' received from the HDCP Receiver does not match the value calculated by the downstream side.

Transition F3:F5. The link integrity message R_0' received from the HDCP Receiver matches the expected value calculated by the downstream side.

State F4: Authenticated. At this time, and at no prior time, the downstream side has completed the authentication protocol and is fully operational, able to deliver HDCP Content.

State F5: Test for Repeater. The downstream side evaluates the state of the HDCP Repeater capability bit (REPEATER) that was read in State F1.

Transition F5:F4. The REPEATER bit is not set (the HDCP Receiver is not an HDCP Repeater).

Transition F5:F6. The REPEATER bit is set (the HDCP Receiver is an HDCP Repeater).

State F6: Wait for Ready. The downstream side sets up a five-second watchdog timer and either polls the HDCP Receiver's READY bit or resumes further processing based on the CP_IRQ interrupt.

Transition F6:P2. The watchdog timer expires before the READY indication is received.

Transition F6:F7. READY is asserted and is detected by the HDCP Transmitter when polling, or when *Bstatus* register is read while processing a CP_IRQ interrupt.

State F7: Read KSV List. The watchdog timer is cleared. The downstream side reads the list of attached KSVs through the KSV FIFO, reads *V'*, computes *V*, and verifies *V* == *V'*, and the KSVs from this port are added to the KSV list for this HDCP Repeater. Additional status bits (MAX_CASCADE_EXCEEDED and MAX_DEVS_EXCEEDED) from the downstream HDCP Repeater are read and if asserted, cause the HDCP Repeater to also assert them upstream.

Transition F7:P2. This transition is made if *V* != *V'*. It is also made if either MAX_CASCADE_EXCEEDED or MAX_DEVS_EXCEEDED are asserted.

Transition F7:F4. This transition is made if *V* == *V'*, the downstream topology does not exceed specified maximums and all downstream devices are HDCP Capable.

Transition F4:P2. On receiving a CP_IRQ interrupt, the downstream side reads the *Bstatus* register to determine the cause of the interrupt. The downstream side must disable HDCP Encryption at the link frame boundary in MST mode and at the CPSR/SR transmission boundary in SST mode as soon as feasible after receiving the CP_IRQ interrupt from the HDCP Receiver if the LINK_INTEGRITY_FAILURE bit is set and must initiate re-authentication with the transmission of a new *An* and *Aksv*.

2.5.4 HDCP Repeater Upstream State Diagram

The HDCP Repeater upstream state diagram, illustrated in Figure 2-15, makes reference to states of the HDCP Repeater downstream state diagram. A link integrity check failure on a downstream HDCP-protected Interface Port should not cause the upstream HDCP-protected Interface Port to move into an unauthenticated state.

In this state diagram and its following description, the upstream (HDCP Receiver) side refers to the HDCP Receiver functionality within the HDCP Repeater for its corresponding upstream HDCP-protected Interface Port

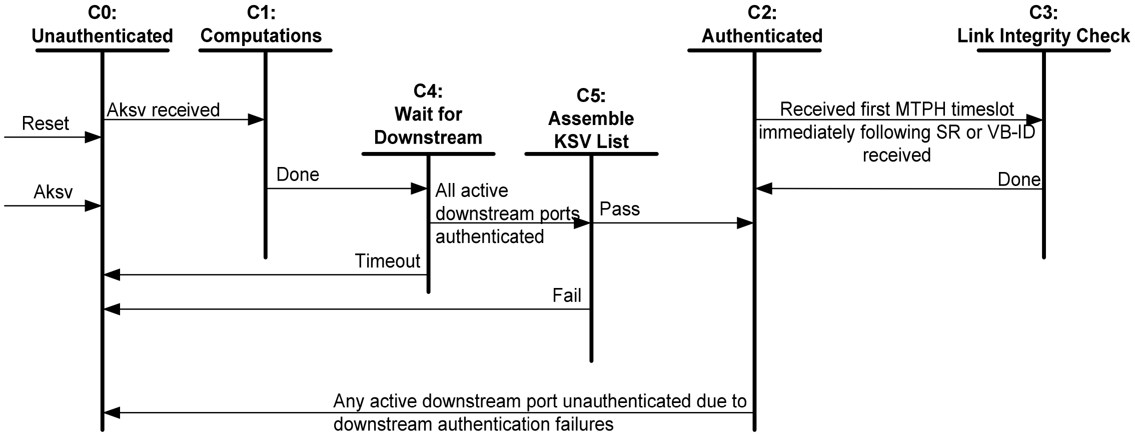

Figure 2-15. HDCP Repeater Upstream Authentication Protocol State Diagram

Transitions Any State:C0. Reset conditions at the HDCP Repeater cause the HDCP Repeater to enter the unauthenticated state. Re-authentication is forced any time the *Aksv* is written by the attached HDCP Transmitter, with a transition through the unauthenticated state.

State C0: Unauthenticated. The device is idle, awaiting the reception of *An* and *Aksv* from the HDCP Transmitter to trigger the authentication protocol. The READY status bit, in the HDCP-protected Interface Port, is de-asserted.

Transition C0:C1. The final byte of *Aksv* is received from the HDCP Transmitter.

State C1: Computations. In this state, the upstream (HDCP Receiver) side of the HDCP Repeater calculates the values *Km*', *Ks*', M_0', and R_0' using its Device Private Keys and the received values of *An* and *Aksv*. The upstream side is allowed a maximum time of 100 milliseconds to complete the computations and make R_0' available to the HDCP Transmitter. Should the HDCP Transmitter write the *Aksv* while the HDCP Repeater is in this state (State C1), the HDCP Repeater abandons intermediate results and restarts the computations.

Transition C1:C5. The computations are complete and the results are available for reading by the HDCP Transmitter. The upstream side must set the R_0'_AVAILABLE bit in the *Bstatus* register and generate the CP_IRQ interrupt.

State C2: Authenticated. The upstream side has completed the authentication protocol and is ready to generate the first frame key when signaled by the HDCP Transmitter. The READY status bit is asserted.

Transition C2:C0. The upstream side becomes unauthenticated when any downstream side enters the unauthenticated state due to downstream authentication failures. Authentication failures on the downstream side of the HDCP Repeater are indicated by state transitions F1:P2, F3:P2, F6:P2 and F7:P2. When the upstream side becomes unauthenticated it signals the upstream HDCP Transmitter to initiate re-authentication by generating a CP_IRQ interrupt for re-authentication events as explained in Section 2.5.2.3.

Transition C2:C3. This transition is made when the first timeslot immediately following SR is received in the MST mode or a VB-ID is received in the SST mode. The upstream side proceeds to check for loss of cipher synchronization.

State C3: Verify VB-ID. The upstream side performs link integrity check as explained in Section 2.2.3 and Section 2.2.4 after it has received the two MTPH timeslots immediately following SR in the MST mode or a VB-ID in the SST mode. If a loss of cipher synchronization is detected, the receiver sets the *Bstatus* LINK_INTEGRITY_FAILURE bit and generates a CP_IRQ interrupt.

Transition C3:C2. After the link integrity check, the upstream side returns to the authenticated state.

State C4: Wait for Downstream. The upstream state machine waits for all downstream HDCP-protected Interface Ports of the HDCP Repeater to enter either the unconnected (State P0), inactive (State P2), or the authenticated state (State F4).

Transition C4:C0. The watchdog timer expires before all downstream HDCP-protected Interface Ports enter the authenticated or unconnected state.

Transition C4:C5. All downstream HDCP-protected Interface Ports with attached HDCP Receivers have reached the state of authenticated or unconnected.

State C5: Assemble KSV List. The upstream side assembles the list of all attached downstream topology HDCP Devices as the downstream HDCP-protected Interface Ports reach terminal states of the authentication protocol. An HDCP-protected Interface Port that advances to State P0, the unconnected state, or P2, the inactive state, does not add to the list. A downstream HDCP-protected Interface Port that arrives in State F4 that has an HDCP Receiver that is not an HDCP Repeater attached, adds the *Bksv* of the attached HDCP Receiver to the list. Downstream HDCP-protected Interface Ports that arrive in State F4 that have an HDCP Repeater attached will cause the KSV list read from the attached HDCP Repeater, plus the *Bksv* of the attached HDCP Repeater itself, to be added to the list.

When the KSV list for all downstream HDCP Receivers has been assembled, the upstream side computes the upstream *V'*. When an HDCP Repeater receives a MAX_DEVS_EXCEEDED or MAX_CASCADE_EXCEEDED status from a downstream HDCP Repeater, it is required to assert its corresponding upstream status bit.

Transition C5:C0. If any downstream HDCP-protected Interface Port should transition to the unauthenticated state due to authentication failures, the upstream connection transitions to the unauthenticated state. This transition is also made when the KSV list integrity check for a downstream HDCP Repeater fails.

Transition C5:C2. The KSV list and *V'*, as well as DEVICE_COUNT and DEPTH, are ready for reading by the upstream HDCP Transmitter.

2.6 HDCP Port

HDCP Transmitter and the HDCP Receiver communicate HDCP register values over the AUX channel. The HDCP Receiver and HDCP Repeaters must support these HDCP registers. Within the DPCD address space, addresses from 0x68000 to 0x68fff are reserved for HDCP. Table 2-2 specifies the usage of these HDCP registers. Multi-byte values are stored in little-endian format.

Offset (hex)	**Name**	**Size in Bytes**	**Rd/ Wr**	**Function**
0x68000	*Bksv*	5	Rd	HDCP Receiver KSV. Valid KSVs contain 20 ones and 20 zeros, a characteristic that must be verified by HDCP Transmitters before main link encryption is enabled. This value must be available any time the HDCP Receiver's HDCP hardware is ready to operate.
0x68005	*R_0'*	2	Rd	*R_0'* is generated by the HDCP Receiver during the first part of the authentication protocol. *R_0'* must be available less than 100 ms after *Aksv* is received.
0x68007	*Aksv*	5	Wr	HDCP Transmitter KSV. Writes to this multi-byte value are written least significant byte first.
0x6800C	*An*	8	Wr	Session random number. This multi-byte value must be written by the HDCP Transmitter before the KSV is written.
0x68014	*V'.H0*	4	Rd	H0 part of SHA–1 hash value used in the second part of the authentication protocol for HDCP Repeaters. (NOTE: DPCD address 0x68114 is the least significant byte of the H0 value, as all addresses are little-endian byte order).
0x68018	*V'.H1*	4	Rd	H1 part of SHA-1 hash value *V'*.
0x6801C	*V'.H2*	4	Rd	H2 part of SHA-1 hash value *V'*.
0x68020	*V'.H3*	4	Rd	H3 part of SHA-1 hash value *V'*.
0x68024	*V'.H4*	4	Rd	H4 part of SHA-1 hash value *V'*.
0x68028	*Bcaps*	1	Rd	Bits 7-2: Reserved (must be zero) Bit 1: REPEATER, HDCP Repeater capability. When set to one, this HDCP Receiver supports downstream connections as permitted by the Digital Content Protection LLC license. This bit does not change while the HDCP Receiver is active. Bit 0: HDCP_CAPABLE. When set to 1, indicates that the receiver is HDCP capable. This bit does not change while the HDCP Receiver is active.
0x68029	*Bstatus*	1	Rd	Refer to Table 2-3 for definitions.
0x6802A	*Binfo*	2	Rd	Refer to Table 2-4 for definitions.
0x6802C	KSV FIFO	15	Rd	Key selection vector FIFO. Used to pull downstream KSVs from HDCP Repeaters using auto-incrementing access. All bytes read as 0x00 for HDCP Receivers that are not HDCP Repeaters (REPEATER == 0). Refer to Section 2.6.1 for details.
0x6803B	Ainfo	1	Wr	Bits 7-1: Reserved (must be zero) Bit 0: REAUTHENTICATION_ENABLE_IRQ_HPD. When set to one, this bit enables upstream notification using IRQ_HPD for re-authentication events as explained in Section 2.5.2.3. This bit resets to a default zero when the HDCP Receiver becomes attached or active, or is reset, or the last byte of Aksv is written. When this bit is zero, the Hot-Plug-Event HPD pulse is used for upstream notification of re-authentication events. The HDCP Transmitter sets this bit to one if the REPEATER bit is set and the transmitter determines that the

				repeater supports DPCD Revision 1.2 or higher.
0x6803C	Rsvd	132	Rd	All bytes read as 0x00
0x680C0	dbg	64	Rd/ Wr	Implementation-specific debug registers. Confidential values must not be exposed through these registers.

Table 2-2. HDCP Addresses in DPCD

Name	Bit Field	Rd/ Wr	Description
Rsvd	7:4	Rd	Reserved. Read as zero
REAUTHENTICATION_REQUEST	3	Rd	When set to one, indicates that the upstream side of the HDCP Repeater has become unauthenticated and a re-authentication must be initiated by the most upstream HDCP Transmitter. This value must be reset to zero by the upstream (HDCP Receiver) side on every new authentication request by the HDCP Transmitter as indicated by a write of the *Aksv*. This bit must never to set to one by HDCP Receivers that are not HDCP Repeaters.
LINK_INTEGRITY_FAILURE	2	Rd	When set to one, indicates that loss of cipher synchronization was detected at the HDCP Receiver during a link integrity check. This value must be reset by the HDCP Receiver on every new authentication request by the HDCP Transmitter as indicated by a write of the *Aksv*.
R0'_AVAILABLE	1	Rd	When set to one, indicates that R_0' is available for reading at the HDCP Receiver. This value must be reset by the HDCP Receiver as soon as R_0' is read by the HDCP Transmitter.
READY	0	Rd	When set to one, this HDCP Repeater has built the list of attached KSVs and computed the verification value *V'*. This value must be reset by the HDCP Repeater as soon as *Binfo* has been read by the HDCP Transmitter. This value is always zero during the computation of *V'*.

Table 2-3. *Bstatus* Register Bit Field Definitions

Name	Bit Field	Rd/ Wr	Description
Rsvd	15:12	Rd	Reserved. Read as zero
MAX_CASCADE_EXCEEDED.	11	Rd	Topology error indicator. When set to one, more than seven levels of repeater have been cascaded together.
DEPTH	10:8	Rd	Three-bit repeater cascade depth. This value gives the number of attached levels through the connection topology.
MAX_DEVS_EXCEEDED	7	Rd	Topology error indicator. When set to one, more than 127 downstream devices are attached.
DEVICE_COUNT	6:0	Rd	Total number of attached downstream devices. Always zero for HDCP Receivers. This count does not include the HDCP Repeater itself, but only devices downstream from the HDCP Repeater.

Table 2-4. *Binfo* Register Bit Field Definitions

2.6.1 KSV FIFO Reading

All (DEVICE_COUNT * 5) bytes within the KSV FIFO are read using an auto-incrementing 15B window represented by the DPCD address range 0x6802C-0x6803A. Figure 2-16 depicts the mapping of KSV bytes to DPCD addresses within the KSV FIFO window. When all 15B have been read successfully (i.e., read request was ACKed by the HDCP Repeater), the KSV FIFO offset values increment by 15 and the next three KSVs are mapped within the window (e.g., KSV_{i+3}, KSV_{i+4}, and KSV_{i+5}). Note that out-of-order or repeated reads of the bytes within a window are allowed so long as all 15B have not already been successfully read.

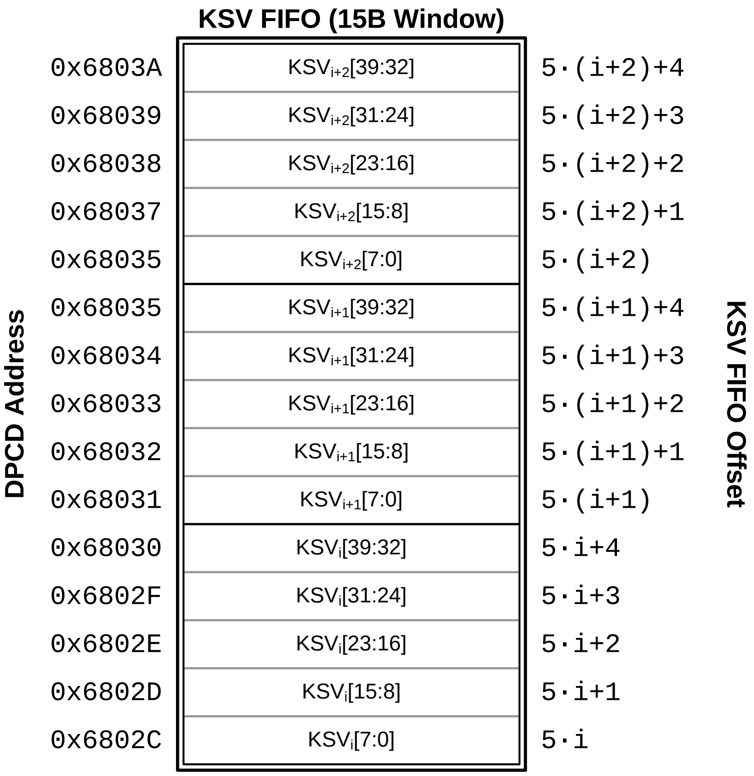
KSV FIFO (15B Window)
DPCD Address
KSV FIFO Offset
0x6803A KSV_{i+2}[39:32] 5·(i+2)+4
0x68039 KSV_{i+2}[31:24] 5·(i+2)+3
0x68038 KSV_{i+2}[23:16] 5·(i+2)+2
0x68037 KSV_{i+2}[15:8] 5·(i+2)+1
0x68035 KSV_{i+2}[7:0] 5·(i+2)
0x68035 KSV_{i+1}[39:32] 5·(i+1)+4
0x68034 KSV_{i+1}[31:24] 5·(i+1)+3
0x68033 KSV_{i+1}[23:16] 5·(i+1)+2
0x68032 KSV_{i+1}[15:8] 5·(i+1)+1
0x68031 KSV_{i+1}[7:0] 5·(i+1)
0x68030 KSV_i[39:32] 5·i+4
0x6802F KSV_i[31:24] 5·i+3
0x6802E KSV_i[23:16] 5·i+2
0x6802D KSV_i[15:8] 5·i+1
0x6802C KSV_i[7:0] 5·i

Figure 2-16. KSV FIFO address/offset mapping

Attempts to read beyond the last KSV (i.e., reading KSV FIFO offsets ≥ DEVICE_COUNT*5) return zero values.

When a KSV FIFO read results in a NACK/DEFER, or returns less than the expected number of bytes, the KSV FIFO offset must not be auto-incremented by the HDCP Repeater to allow the HDCP Transmitter to attempt a re-read of the current KSV FIFO window.

The window's KSV FIFO offset is reset to 0 whenever the HDCP Transmitter successfully reads the DPCD address 0x68014 (i.e., V'.H0[7:0]). This allows the HDCP Transmitter to reset the KSV FIFO explicitly in the event of attempting to re-read the KSV when V != V', or if an unforeseen AUX-CH error causes the HDCP Transmitter to lose track of where it is within the KSV list read back.

2.7 CP_IRQ Interrupt Processing

HDCP Transmitters have the option of not using the CP_IRQ. They may directly read R_0' after 100 ms during first part of authentication and poll for READY during the second part of authentication. However, generation of CP_IRQ is not optional for the HDCP Repeaters and HDCP Receivers. The HDCP Transmitters that choose not to use the CP_IRQ interrupt must continue to field the HPD interrupt and ignore the CP_IRQ bit during interrupt processing.

The HDCP Transmitter uses the following steps when processing HPD interrupts:

1. If CP_IRQ is not set, process the interrupt as specified in DisplayPort Specification and exit
2. Read *Bstatus* register
3. If LINK_INTEGRITY_FAILURE, abort HDCP session
4. If REAUTHENTICATION_REQUEST, abort HDCP session
5. If the transmitter is not relying on CP_IRQ for READY and R_0' check, it can exit the interrupt service routine at this time
6. If (READY bit is set)
    a. Read *Binfo* register
    b. If MAX_DEVS_EXCEEDED, abort authentication
    c. If MAX_CASCADE_EXCEEDED, abort authentication
    d. Continue with the second part of authentication: process the KSV_FIFO, compute V and verify whether $V = V'$
7. If (R_0'_AVAILABLE bit is set)
    a. Read R_0'
    b. Verify whether $R_0 = R_0'$
8. Else ignore interrupt and continue HDCP session without aborting

Note that since the HDCP Transmitter sends premium content in parallel with second part of authentication, multiple link integrity checks would occur at the downstream HDCP Repeater and HDCP Receiver while the second part of authentication is in progress. So it is important that HDCP Transmitters that rely on polled method for READY still enable CP_IRQ processing before polling for READY starts.

3 Data Encryption

HDCP Encryption is applied in the DisplayPort transmitter at the input of the PHY layer before inter-lane skewing is applied, and in the DisplayPort receiver at the output of the data scrambler after inter-lane de-skewing has been applied (Figure 3-1 and Figure 3-2). HDCP Encryption consists of a bit-wise exclusive-OR (XOR) of the 32-bit HDCP Content with a 32-bit block of pseudo-random bits produced by the HDCP Cipher. The HDCP Cipher produces a new 32-bit block of pseudo-random bits for every input HDCP Cipher clock pulse.

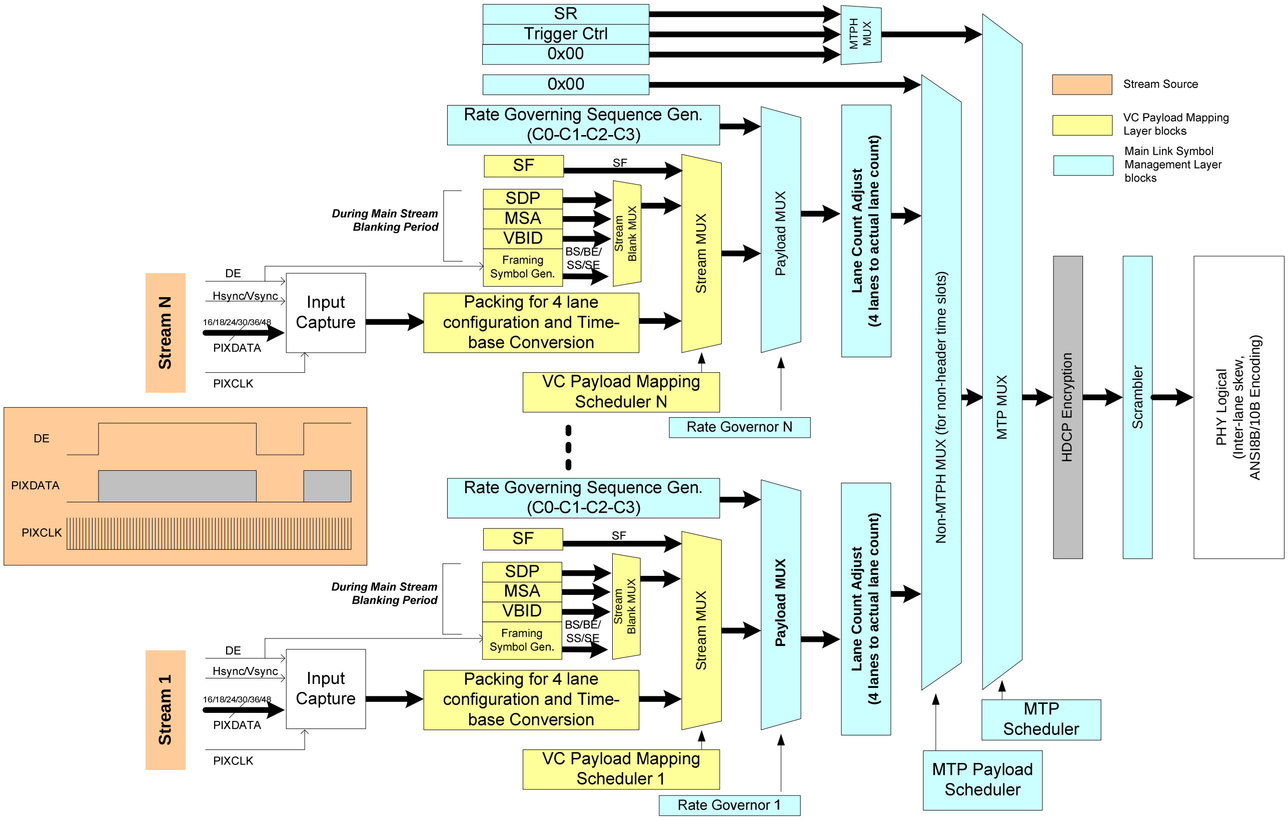
SR
Trigger Ctrl
0x00
MTPH MUX
0x00
Stream Source
VC Payload Mapping Layer blocks
Main Link Symbol Management Layer blocks
Rate Governing Sequence Gen. (C0-C1-C2-C3)
SF
SF
During Main Stream Blanking Period
SDP
MSA
VBID
Framing Symbol Gen.
BS/BE/ SS/SE
Stream Blank MUX
Stream MUX
Payload MUX
Lane Count Adjust (4 lanes to actual lane count)
Non-MTPH MUX (for non-header time slots)
MTP MUX
HDCP Encryption
Scrambler
PHY Logical (Inter-lane skew, ANSI8B/10B Encoding)
Stream N
DE
Hsync/Vsync
16/18/24/30/36/48
PIXDATA
PIXCLK
Input Capture
Packing for 4 lane configuration and Time-base Conversion
VC Payload Mapping Scheduler N
Rate Governor N
DE
PIXDATA
PIXCLK
Rate Governing Sequence Gen. (C0-C1-C2-C3)
SF
SF
During Main Stream Blanking Period
SDP
MSA
VBID
Framing Symbol Gen.
BS/BE/ SS/SE
Stream Blank MUX
Stream MUX
Payload MUX
Lane Count Adjust (4 lanes to actual lane count)
Stream 1
DE
Hsync/Vsync
16/18/24/30/36/48
PIXDATA
PIXCLK
Input Capture
Packing for 4 lane configuration and Time-base Conversion
VC Payload Mapping Scheduler 1
Rate Governor 1
MTP Scheduler
MTP Payload Scheduler

Figure 3-1. HDCP Encryption in the DisplayPort Transmitter

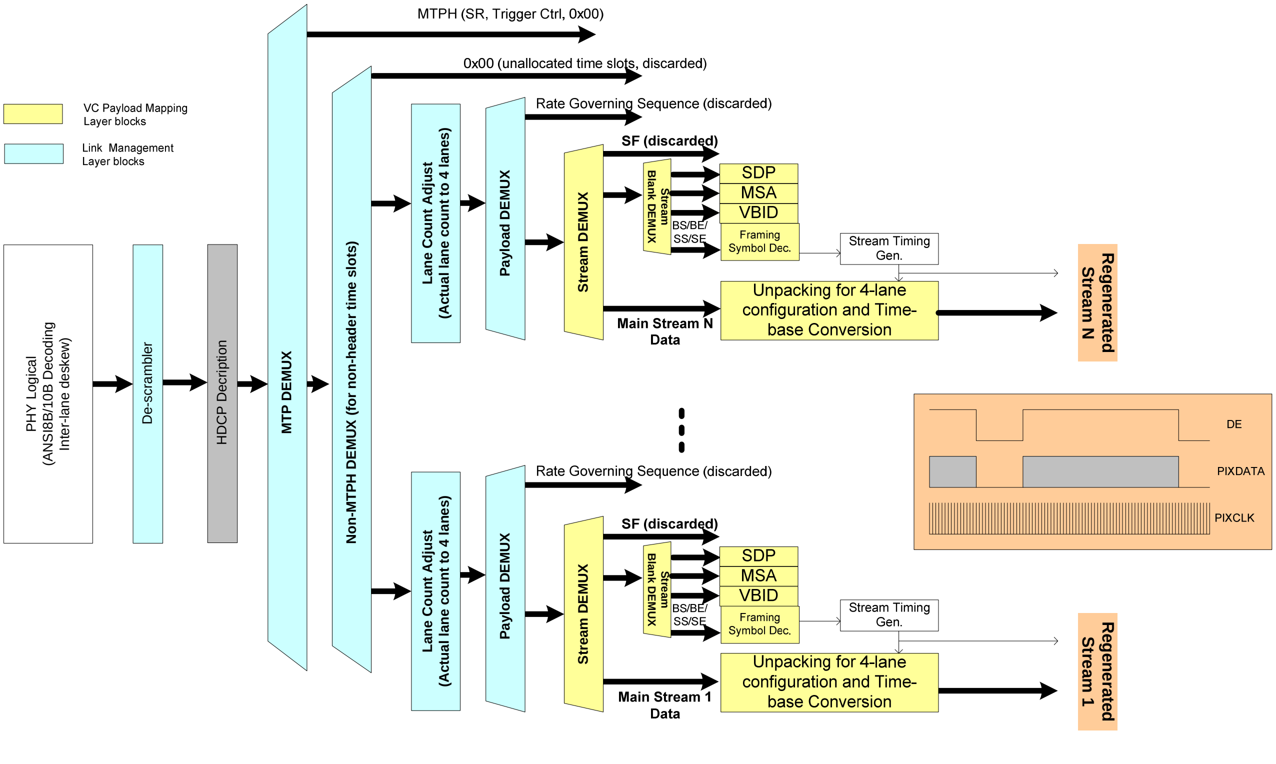
VC Payload Mapping Layer blocks
Link Management Layer blocks
PHY Logical (ANSI8B/10B Decoding Inter-lane deskew)
De-scrambler
HDCP Decription
MTP DEMUX
MTPH (SR, Trigger Ctrl, 0x00)
Non-MTPH DEMUX (for non-header time slots)
0x00 (unallocated time slots, discarded)
Lane Count Adjust (Actual lane count to 4 lanes)
Payload DEMUX
Rate Governing Sequence (discarded)
Stream DEMUX
SF (discarded)
Stream Blank DEMUX
BS/BE/ SS/SE
SDP
MSA
VBID
Framing Symbol Dec.
Stream Timing Gen.
Unpacking for 4-lane configuration and Time-base Conversion
Main Stream N Data
Regenerated Stream N
DE
PIXDATA
PIXCLK
Lane Count Adjust (Actual lane count to 4 lanes)
Payload DEMUX
Rate Governing Sequence (discarded)
Stream DEMUX
SF (discarded)
Stream Blank DEMUX
BS/BE/ SS/SE
SDP
MSA
VBID
Framing Symbol Dec.
Stream Timing Gen.
Unpacking for 4-lane configuration and Time-base Conversion
Main Stream 1 Data
Regenerated Stream 1

Figure 3-2. HDCP Decryption in the DisplayPort Receiver

When HDCP Encryption is applied to a timeslot in the MST mode or when HDCP Encryption is enabled in the SST mode, all data symbols (including video data, secondary data and dummy symbols) must be encrypted and K-codes must not be encrypted. Section 5 and Section 6 explains in detail the encryption signaling protocol that is used to enable/disable HDCP Encryption.

The HDCP Cipher is clocked at the following rates.

- For 4-lane Main link configurations, the HDCP Cipher is clocked for every link symbol clock (LS_CLK)
- For 2-lane Main link configurations, the HDCP Cipher is clocked at LS_CLK/2
- For 1-lane Main link configurations, the HDCP Cipher is clocked LS_CLK/4

Unless otherwise specified, all references to clock in this specification denote the HDCP Cipher clock. The clock is applied regardless of K-codes or data symbols.

For 2-lane Main Link configuration, there are two phase relationships between LS_CLK and HDCP Cipher clock. For 1-lane Main Link configuration, there are four. This phase relationship must be re-synchronized at the first LS_CLK following the SR symbol at the link frame boundary in the MST mode[1] or following the CPSR symbol in the SST mode when HDCP Encryption is enabled. Refer to **Error! Reference source not found.** and Appendix E for detailed timing diagrams.

[1] In the MST mode, once phase is aligned, the constant SR interval should not result in subsequent phase mis-alignment during normal link operation

The mappings of the 32-bit HDCP Cipher output to the DisplayPort Lanes are shown in Table 3-1, Table 3-2 and Table 3-3.

Cipher Output	**DisplayPort Lane**	**Symbol**
31:24	3	3
23:16	2	2
15:8	1	1
7:0	0	0

Table 3-1. Encryption Stream Mapping for 4-lane Main Link Configuration

Cipher Output	**DisplayPort Lane**	**Symbol**
31:24	1	3
23:16	0	2
15:8	1	1
7:0	0	0

Table 3-2. Encryption Stream Mapping for 2-lane Main Link Configuration

Cipher Output	**DisplayPort Lane**	**Symbol**
31:24	0	3
23:16	0	2
15:8	0	1
7:0	0	0

Table 3-3. Encryption Stream Mapping for 1-lane Main Link Configuration

4 HDCP Cipher

4.1 Overview

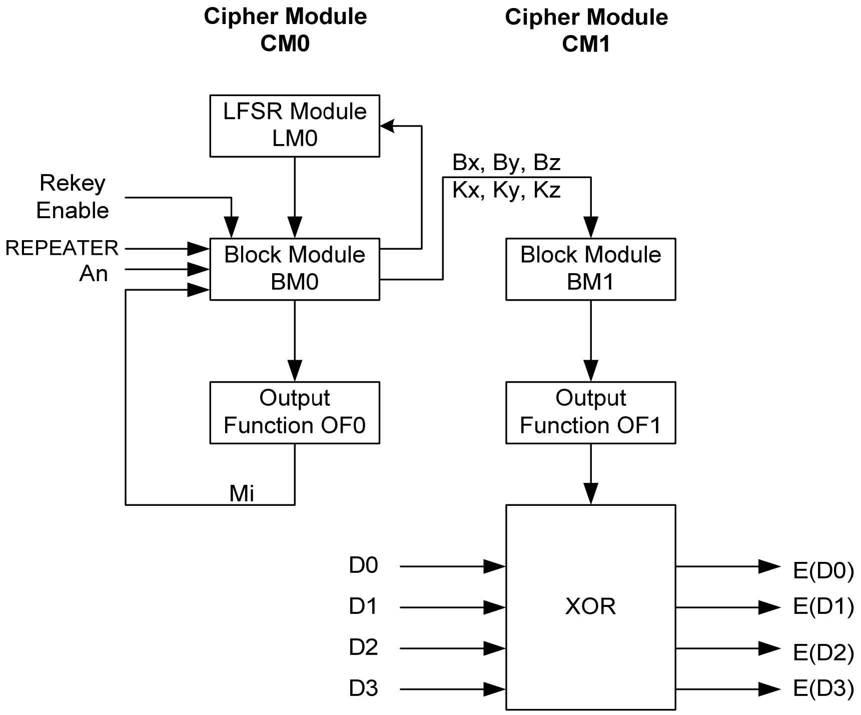

Figure 4-1. HDCP Cipher Structure

The HDCP Cipher structure is illustrated in Figure 4-1. There are two cipher modules – CM0 and CM1. CM0 consists of three layers. The first layer (LM0) consists of a set of four Linear Feedback Shift Registers that are combined to one bit. This one bit feeds into the middle Block Module (BM0) layer when enabled via the rekey enable signal. The middle layer consists of two halves that are very similar in design. One half, *Round Function B*, performs one round of a block cipher using three 28-bit registers, *Bx*, *By*, and *Bz*. The other half, *Round Function K*, is similar in structure to Round Function B, but provides the output of latch *Ky* as a stream of 28-bit round keys to Round Function B at the rate of one 28-bit round key for every clock pulse. The final layer takes four 28-bit register outputs from the round functions, *By*, *Bz*, *Ky*, and *Kz*, through a compression function (OF0) to produce a 32-bit block of pseudo-random bits for every clock pulse.

CM1 consists of two layers – Block Module (BM1) and the Output Function (OF1) - which are similar in design to BM0 and OF0 of CM0 respectively. OF1 produces a 32-bit block of pseudo-random bits for every clock pulse. The 32-bit block of pseudo-random bits produced by OF1 is XORed with the 32-bit HDCP Content as explained in Section 3.

The hdcpBlockCipher, hdcpStreamCipher and hdcpRekeyCipher operations are implemented in CM0. The 32-bit block of pseudo-random bits from OF0 is not used for HDCP Encryption. The 8 MSBs (i.e. [31:24]) of OF0's output are never used. The 24 LSBs (i.e. [23:0]) of OF0's output are used to produce R_i and M_i values during the hdcpBlockCipherOperation. A one-way data path connects BM0 to BM1. The B and K register contents are transferred from BM0 to BM1 at the end of the hdcpBlockCipher and hdcpRekeyCipher operations. The hdcpStreamCipher operation is implemented in CM1. Section 4.5 explains hdcpBlockCipher, hdcpStreamCipher and hdcpRekeyCipher operations.

The following sections explain the structure of LFSR, Block Module and Output Function in detail.

4.2 Linear Feedback Shift Register Module

The linear feedback shift register module in CM0 consists of four LFSRs of different lengths and a combining function that produces a single bit stream from them. The combining function takes three taps from each LFSR. The generator polynomials and combining function taps for the LFSRs are specified in Table 4-1.

LFSR	Polynomial	Combining Function Taps		
		0	1	2
3	$x^{17}+x^{15}+x^{11}+x^{5}+1$	5	11	16
2	$x^{16}+x^{15}+x^{12}+x^{8}+x^{7}+x^{5}+1$	5	9	15
1	$x^{14}+x^{11}+x^{10}+x^{7}+x^{6}+x^{4}+1$	4	8	13
0	$x^{13}+x^{11}+x^{9}+x^{5}+1$	3	7	12

Table 4-1. LFSR Generation and Tapping

Figure 4-2 illustrates the tap locations of LFSR0 as well as the XOR term feedback into the least significant bit of LFSR0.

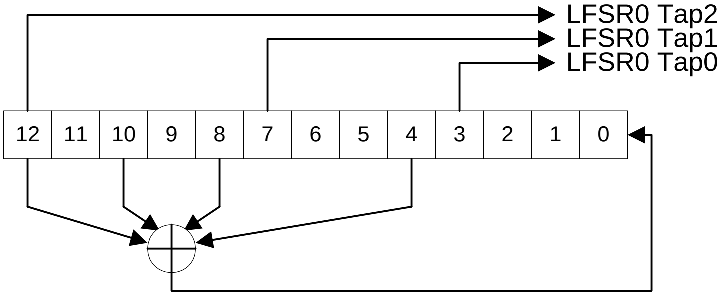

Figure 4-2. LFSR0

The combining function contains four cascaded shuffle networks, each of which includes two state bits. One tap from each of the four LFSRs is XORed together to form the data input to the first shuffle network. One tap from each of the four LFSRs is used as the select input to one of the four shuffle networks. The output of the fourth shuffle network is XORed together with one tap from each of the LFSRs. The Combiner Function illustrated in Figure 4-3.

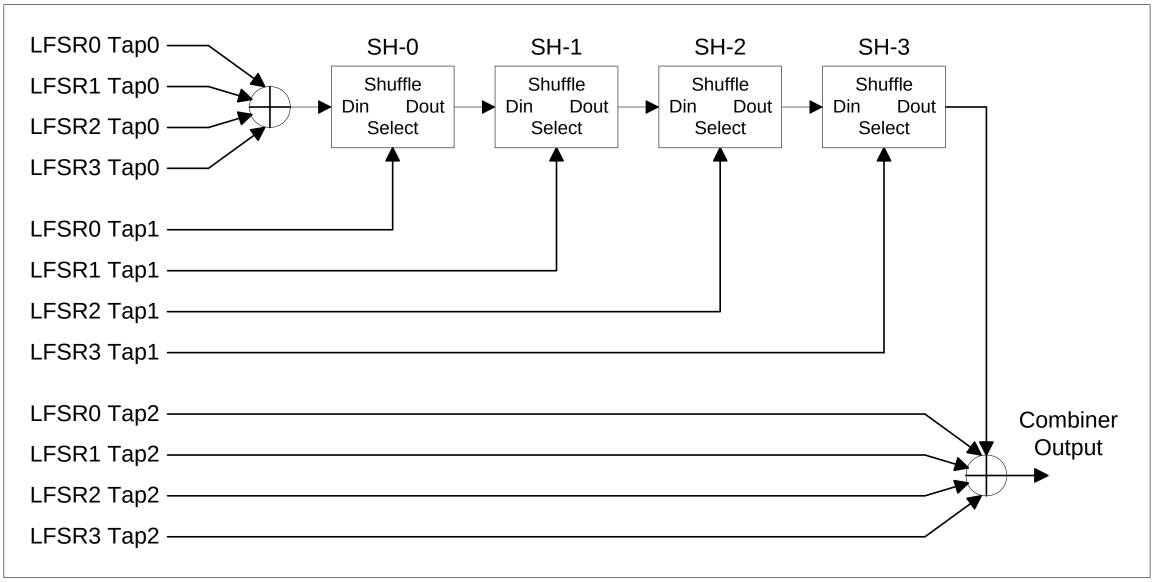

Figure 4-3. LFSR Module Combiner Function

The shuffle network is represented schematically in Figure 4-4. If the shuffle network contains the ordered pair of boolean values (A, B) and has boolean data input D and selection input S, the S value controls the next state. If S is zero, it outputs A and assumes state (B, D). If S is one, it outputs B and assumes state (D, A).

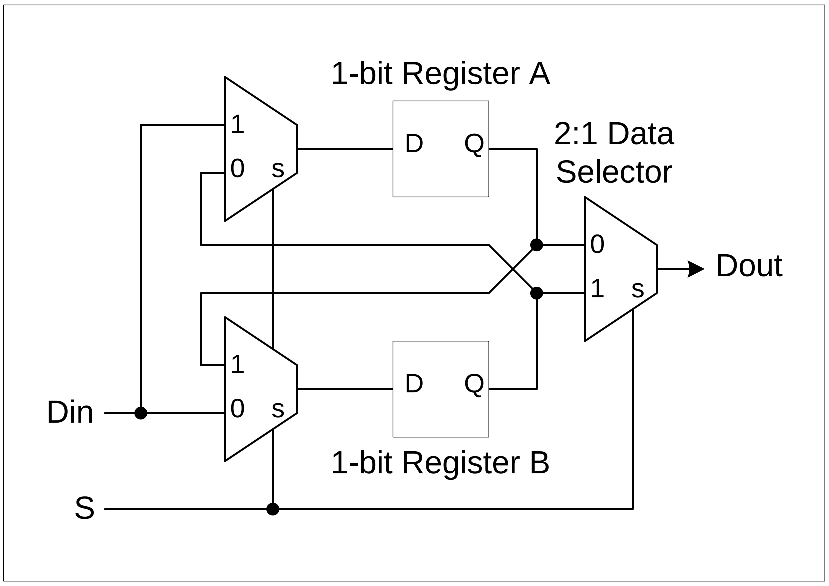

Figure 4-4. Shuffle Network

In all modes of operation the LFSRs and combining function are initialized by a 56-bit value. The 60 bits of LFSR state use these 56 bits directly plus the complements of four of the bits. The shuffle networks are each initialized with the same constant value. The initialization of the LFSR module is specified in Table 4-2 for a 56-bit initialization value.

	Bit Field	Initial Value
LFSR3	[16]	Complement of input bit 47
	[15:0]	Input bits [55:40]
LFSR2	[15]	Complement of input bit 32
	[14:0]	Input bits [39:25]
LFSR1	[13]	Complement of input bit 18
	[12:0]	Input bits [24:12]
LFSR0	[12]	Complement of input bit 6
	[11:0]	Input bits [11:0]
Shuffle Networks	Register A	0
	Register B	1

Table 4-2. LFSR Module Initialization

This one-bit stream output of the combining function is the only output from the LFSR module. This bit stream provides key material to the block module BM0 when the rekey enable signal is active.

4.3 Block Module

The structure of the block modules BM0 and BM1 are similar with one exception. Bit 13 of Ky register in BM0 takes its input from LM0 when rekey enable signal is asserted. BM1 does not receive inputs from the LFSR module. The B and K register states in BM1 are initialized using the corresponding register states in BM0 at the end of the hdcpBlockCipher and hdcpRekeyCipher operation. Section 4.5 explains hdcpBlockCipher and hdcpRekeyCipher operations.

The block module consists of two separate "round function" components. One of these components, *Round Function K*, provides a key stream for the other component, *Round Function B*. Each of these two components operates on a corresponding set of three 28-bit registers. The structure of the block module is diagrammed in Figure 4-5.

For Round Function K, bit 13 of the Ky register in BM0 takes its input from the LM0 module output stream when the external rekey enable signal is asserted.

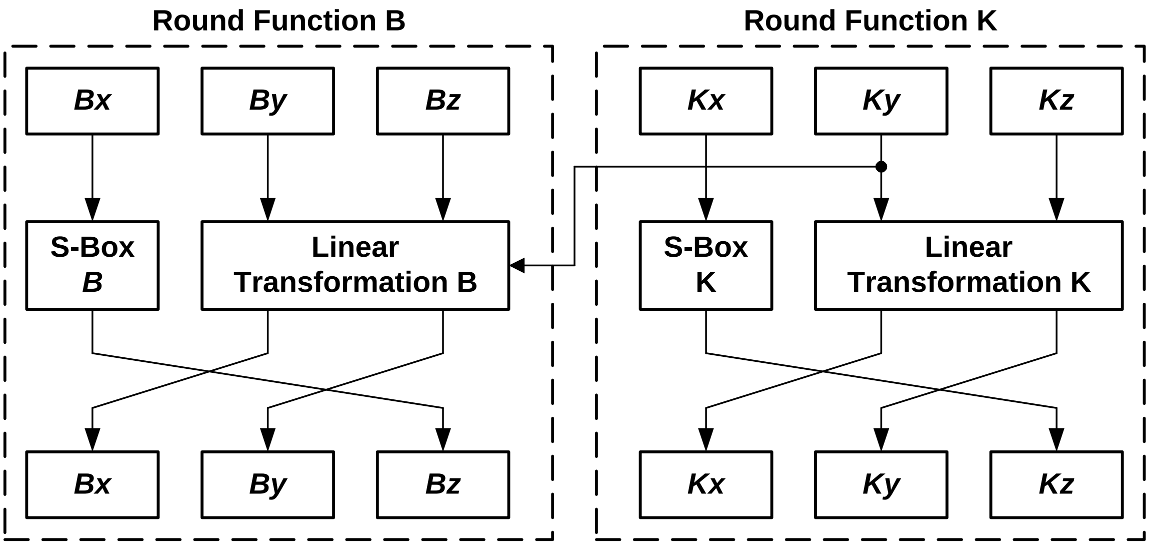

Figure 4-5. Block Module

The S-Boxes for both round functions consist of seven 4 input by 4 output S-boxes. Round function K S-Boxes are labeled SK0 through SK6 and round function B S-Boxes are labeled SB0 through SB6. The Ith input to box J is bit I*7+J from the round x register (*Bx* or *Kx*), and output I of box J goes to bit I*7+J of register z of the round function (*Bz* or *Kz*). Bit 0 is the least significant bit. The S-box permutations of round functions K and B are specified in Table 4-3.

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
SK0	8	14	5	9	3	0	12	6	1	11	15	2	4	7	10	13
SK1	1	6	4	15	8	3	11	5	10	0	9	12	7	13	14	2
SK2	13	11	8	6	7	4	2	15	1	12	14	0	10	3	9	5
SK3	0	14	11	7	12	3	2	13	15	4	8	1	9	10	5	6
SK4	12	7	15	8	11	14	1	4	6	10	3	5	0	9	13	2
SK5	1	12	7	2	8	3	4	14	11	5	0	15	13	6	10	9
SK6	10	7	6	1	0	14	3	13	12	9	11	2	15	5	4	8
SB0	12	9	3	0	11	5	13	6	2	4	14	7	8	15	1	10
SB1	3	8	14	1	5	2	11	13	10	4	9	7	6	15	12	0
SB2	7	4	1	10	11	13	14	3	12	15	6	0	2	8	9	5
SB3	6	3	1	4	10	12	15	2	5	14	11	8	9	7	0	13
SB4	3	6	15	12	4	1	9	2	5	8	10	7	11	13	0	14
SB5	11	14	6	8	5	2	12	7	1	4	15	3	10	13	9	0
SB6	1	11	7	4	2	5	12	9	13	6	8	15	14	0	3	10

Table 4-3. Block Module S-Box Values

Both linear transformation K and linear transformation B produce 56 output values. These values are the combined outputs from eight diffusion networks that each produces seven outputs. The diffusion network function is specified in Table 4-4. Each diffusion network has seven data inputs labeled I_0 - I_6, seven outputs $O_0 – O_6$, plus an additional seven optional key inputs $K_0 – K_6$.

The diffusion networks of round function K are specified in Table 4-5. Note that none of the round function K diffusion networks have the optional key inputs. The diffusion units of round function B are specified in Table 4-6. Half of these diffusion networks have key inputs that are driven from the Ky register of round function K. A dash in the table indicates that the key input is not present.

	Diffusion Network Logic Function
O_0	$K_0 \oplus I_1 \oplus I_2 \oplus I_3 \oplus I_4 \oplus I_5 \oplus I_6$
O_1	$K_1 \oplus I_0 \oplus I_2 \oplus I_3 \oplus I_4 \oplus I_5 \oplus I_6$
O_2	$K_2 \oplus I_0 \oplus I_1 \oplus I_3 \oplus I_4 \oplus I_5 \oplus I_6$
O_3	$K_3 \oplus I_0 \oplus I_1 \oplus I_2 \oplus I_4 \oplus I_5 \oplus I_6$
O_4	$K_4 \oplus I_0 \oplus I_1 \oplus I_2 \oplus I_3 \oplus I_5 \oplus I_6$
O_5	$K_5 \oplus I_0 \oplus I_1 \oplus I_2 \oplus I_3 \oplus I_4 \oplus I_6$
O_6	$K_6 \oplus I_0 \oplus I_1 \oplus I_2 \oplus I_3 \oplus I_4 \oplus I_5 \oplus I_6$

Table 4-4. Diffusion Network Logic Function

	K1	**K2**	**K3**	**K4**	**K5**	**K6**	**K7**	**K8**
I_0	Kz0	Kz7	Kz10	Kz13	Kz16	Ky16	Ky20	Ky24
I_1	Kz1	Kz8	Kz11	Kz14	Kz17	Ky17	Ky21	Ky25
I_2	Kz2	Kz9	Kz12	Kz15	Kz18	Ky18	Ky22	Ky26
I_3	Kz3	Ky0	Ky3	Ky6	Ky9	Ky19	Ky23	Ky27
I_4	Kz4	Ky1	Ky4	Ky7	Ky10	Kz19	Kz22	Kz25
I_5	Kz5	Ky2	Ky5	Ky8	Ky11	Kz20	Kz23	Kz26
I_6	Kz6	Ky12	Ky13	Ky14	Ky15	Kz21	Kz24	Kz27
O_0	Kx0	Ky0	Ky1	Ky2	Ky3	Kx1	Kx2	Kx3
O_1	Kx4	Ky4	Ky5	Ky6	Ky7	Kx5	Kx6	Kx7
O_2	Kx8	Ky8	Ky9	Ky10	Ky11	Kx9	Kx10	Kx11
O_3	Kx12	Ky12	Ky13	Ky14	Ky15	Kx13	Kx14	Kx15
O_4	Kx16	Ky16	Ky17	Ky18	Ky19	Kx17	Kx18	Kx19
O_5	Kx20	Ky20	Ky21	Ky22	Ky23	Kx21	Kx22	Kx23
O_6	Kx24	Ky24	Ky25	Ky26	Ky27	Kx25	Kx26	Kx27

Table 4-5. K Round Input and Output Mapping

	B1	**B2**	**B3**	**B4**	**B5**	**B6**	**B7**	**B8**
$\mathbf{I_0}$	Bz0	Bz7	Bz10	Bz13	Bz16	By16	By20	By24
$\mathbf{I_1}$	Bz1	Bz8	Bz11	Bz14	Bz17	By17	By21	By25
$\mathbf{I_2}$	Bz2	Bz9	Bz12	Bz15	Bz18	By18	By22	By26
$\mathbf{I_3}$	Bz3	By0	By3	By6	By9	By19	By23	By27
$\mathbf{I_4}$	Bz4	By1	By4	By7	By10	Bz19	Bz22	Bz25
$\mathbf{I_5}$	Bz5	By2	By5	By8	By11	Bz20	Bz23	Bz26
$\mathbf{I_6}$	Bz6	By12	By13	By14	By15	Bz21	Bz24	Bz27
$\mathbf{K_0}$	Ky0	–	–	–	–	Ky7	Ky14	Ky21
$\mathbf{K_1}$	Ky1	–	–	–	–	Ky8	Ky15	Ky22
$\mathbf{K_2}$	Ky2	–	–	–	–	Ky9	Ky16	Ky23
$\mathbf{K_3}$	Ky3	–	–	–	–	Ky10	Ky17	Ky24
$\mathbf{K_4}$	Ky4	–	–	–	–	Ky11	Ky18	Ky25
$\mathbf{K_5}$	Ky5	–	–	–	–	Ky12	Ky19	Ky26
$\mathbf{K_6}$	Ky6	–	–	–	–	Ky13	Ky20	Ky27
$\mathbf{O_0}$	Bx0	By0	By1	By2	By3	Bx1	Bx2	Bx3
$\mathbf{O_1}$	Bx4	By4	By5	By6	By7	Bx5	Bx6	Bx7
$\mathbf{O_2}$	Bx8	By8	By9	By10	By11	Bx9	Bx10	Bx11
$\mathbf{O_3}$	Bx12	By12	By13	By14	By15	Bx13	Bx14	Bx15
$\mathbf{O_4}$	Bx16	By16	By17	By18	By19	Bx17	Bx18	Bx19
$\mathbf{O_5}$	Bx20	By20	By21	By22	By23	Bx21	Bx22	Bx23
$\mathbf{O_6}$	Bx24	By24	By25	By26	By27	Bx25	Bx26	Bx27

Table 4-6. B Round Input and Output Mapping

4.4 Output Function

The output function structure explained below applies to both OF0 and OF1.

The Ky, Kz, By, and Bz registers drive the final output function. Each of the 32 outputs consists of the XOR of nine terms given by the following formula:

$(B0 \bullet K0) \oplus (B1 \bullet K1) \oplus (B2 \bullet K2) \oplus (B3 \bullet K3) \oplus (B4 \bullet K4) \oplus (B5 \bullet K5) \oplus (B6 \bullet K6) \oplus B7 \oplus K7$

Where "$\oplus$" represents a logical XOR function and "$\bullet$" represents a logical AND function. Table 4-7 specifies the input values B and K to the 32 logic functions.

For example, output bit 0 is computed as
$(Bz17 \bullet Kz3) \oplus (Bz26 \bullet Kz6) \oplus (Bz22 \bullet Kz0) \oplus (Bz27 \bullet Kz9) \oplus (Bz21 \bullet Kz4) \oplus (Bz18 \bullet Kz22) \oplus (Bz2 \bullet Kz5) \oplus By5 \oplus Ky10$.

Input	**B0**	**B1**	**B2**	**B3**	**B4**	**B5**	**B6**	**B7**	**K0**	**K1**	**K2**	**K3**	**K4**	**K5**	**K6**	**K7**
Origin	**Bz**	**Bz**	**Bz**	**Bz**	**Bz**	**Bz**	**Bz**	**By**	**Kz**	**Kz**	**Kz**	**Kz**	**Kz**	**Kz**	**Kz**	**Ky**
Output bit																
0	17	26	22	27	21	18	2	5	3	6	0	9	4	22	5	10
1	5	20	15	24	2	25	0	16	20	18	7	23	15	5	3	25
2	22	5	14	16	25	17	20	11	7	19	2	10	22	4	13	21
3	19	3	15	11	21	16	27	1	6	14	9	8	17	18	12	24
4	19	6	17	18	22	7	9	12	25	6	5	2	10	15	21	8
5	3	7	4	8	16	6	5	17	27	14	2	4	24	19	1	12
6	8	21	27	2	11	24	12	3	17	26	4	16	27	7	22	11
7	9	5	7	4	8	13	3	15	9	10	19	11	7	6	8	23
8	26	13	23	10	11	7	15	19	13	12	18	24	15	23	7	16
9	1	0	19	11	13	16	24	18	0	5	20	25	1	24	9	27
10	26	13	9	14	10	4	1	2	14	23	27	25	17	19	1	22
11	21	15	5	3	13	25	16	27	6	21	17	15	26	11	16	7
12	20	7	18	12	17	1	16	0	11	22	20	0	26	23	17	2
13	14	23	1	12	24	6	18	9	8	4	3	14	20	26	23	15
14	19	6	21	25	23	1	10	8	19	0	18	2	13	8	24	14
15	3	0	27	23	19	8	4	7	16	21	24	25	12	27	15	18
16	6	5	14	22	24	18	2	21	3	5	8	25	7	27	2	26
17	3	4	2	6	22	14	12	26	11	14	23	17	22	13	19	4
18	25	21	19	9	10	15	13	22	1	16	14	11	12	6	10	19
19	23	11	10	20	1	12	14	4	21	1	10	20	18	26	9	13
20	11	26	20	17	8	23	0	24	20	21	9	25	12	3	15	0
21	9	17	26	4	27	0	15	6	18	12	21	27	1	16	24	20
22	22	12	2	10	7	20	25	13	13	0	3	16	22	11	26	9
23	27	24	26	8	0	9	18	23	2	0	13	5	4	8	10	3
24	5	18	27	23	17	7	8	14	23	24	0	19	1	13	25	17
25	26	11	9	24	21	15	6	25	16	21	15	27	3	26	11	1
26	19	4	20	16	22	3	14	20	4	10	14	5	9	20	22	6
27	2	12	25	13	10	1	0	10	6	17	7	8	18	2	12	5
28	12	21	2	1	18	3	13	5	23	0	22	20	12	25	24	20
29	16	5	7	4	15	10	27	2	7	8	6	3	19	9	11	19
30	26	6	23	14	11	22	17	4	4	15	26	10	14	2	13	15
31	19	25	20	8	9	24	0	8	16	18	21	1	27	5	17	27

Table 4-7. Output Function Input and Output Mapping

4.5 Operation

The HDCP Cipher is used in four different ways during operation: hdcpBlockCipher, hdcpStreamCipher, hdcpRekeyCipher, and hdcpRngCipher.

hdcpBlockCipher

This operation is performed in CM0. The sequence is used during the first part of authentication to establish the session key, *Ks*, and after detection of SR at the link frame boundary when HDCP Encryption is enabled in the MST mode or after detection of CPSR during the interval preceding encrypted frames in the SST mode to establish the frame key, *Ki* (Refer to Section 5 and Section 6). Table 4-8 and Table 4-9 describe this sequence. Note that the 8 MSBs (i.e., [31:24]) of OF0's output are never used.

The initial value for the B round register in CM0 is specified with the concatenation operator "||". For eight-bit values *a* and *b*, the result of (*a* || *b*) is a 16-bit value, with the value *a* in the most significant eight bits and *b* in the least significant eight bits.

Step	Activity
1	Load B and K registers of BM0
2	Apply 48 clocks to BM0 registers
3	Save the least significant 56 bits of the B register for future use as Ks/K_i
4	Transfer 84-bit B register values to the K registers
5	Reload B registers
6	Initialize LM0
7	Assert rekey enable
8	Apply 56 clocks to LM0 and BM0, saving the 64-bit M_i value during the last four clocks as specified in Table 4-11.
9	De-assert rekey enable

Table 4-8. hdcpBlockCipher Sequence

	Steps	clocks	LFSR (LM0) init (56 bits)	K init	B init (65 bits)	B output (84 bits)	Output Function (OF0)
hdcpBlockCipher at Authentication	1-3	48	–	*Km* (56 bits)	REPEATER || *An*	*Ks*	–
	6-9	56	*Ks*	*Ks* (84 bits)	REPEATER || *An*	–	R_0, M_0
hdcpBlockCipher on detection of SR when HDCP Encryption is enabled in the MST mode or on detection of CPSR in the SST mode	1-3	48	–	*Ks* (56 bits)	REPEATER || M_{i-1}	K_i	–
	6-9	56	K_i	K_i (84 bits)	REPEATER || M_{i-1}	–	R_i, M_i

Table 4-9. hdcpBlockCipher Initial Values and Outputs

For both the B and K round functions, the x, y, and z registers may be viewed as comprising a single register 84 bits in length, identified by B[83:0] and K[83:0]. The mapping of the x, y, and z registers into the full round register is specified by Table 4-10.

Round Register	B[83:56]	B[55:28]	B[27:0]	K[83:56]	K[55:28]	K[27:0]
Sub Register	Bz[27:0]	By[27:0]	Bx[27:0]	Kz[27:0]	Ky[27:0]	Kx[27:0]

Table 4-10. Round Register Bit Precedence

When fewer than 84 bits of output of a round register are required, the least significant bits are used. When fewer than 84 bits are available for initialization, the least significant bits are filled and the most significant bits are set to zero. For example, the 65-bit concatenation of REPEATER with *An* will be loaded into the Bx and By registers, plus the least significant nine bits of the Bz register, and the most significant 19 bits of the Bz register are set to zero. Similarly, the 56 bits from the Bx and By registers are saved as *Ks* or K_i during hdcpBlockCipher.

The origin of the M_i bits from the output function is specified by Table 4-11.

Warm-up Clock (Step 8)	Output Function Bits 23……16	Output Function Bits 15 ………… 0
53	–	M_i [63:48]
54	–	M_i [47:32]
55	R_i [15:8]	M_i [31:16]
56	R_i [7:0]	M_i [15:0]

Table 4-11. hdcpBlockCipher Output Function Bit Map

While the hdcpBlockCipher operation is being implemented in CM0, CM1 performs hdcpStreamCipher operation in parallel. At the end of the hdcpBlockCipher operation, contents are transferred from BM0 to BM1. Refer to Section 5.1 and Section 6.1 for an overview of the operations of CM0 and CM1 during hdcpBlockCipher, hdcpStreamCipher and hdcpRekeyCipher computations.

hdcpStreamCipher

hdcpStreamCipher operation is implemented in CM0 and CM1. For every input clock pulse, hdcpStreamCipher produces 32-bits of output data from the output functions OF0 and OF1. The 32-bit data output from OF0 is not used for HDCP Encryption.

In the MST mode, the 32-bit data output from OF1 is used for HDCP Encryption of the LINK_VERIFICATION_PATTERN (as explained in Section 2.2.3) and HDCP Encryption of data symbols when the XOR Enable/Disable Indicator bits indicate HDCP Encryption must be applied to the corresponding timeslots as explained in Section 5. Control symbols are not encrypted. When control symbols are detected or when the XOR Enable/Disable Indicator bits indicate HDCP Encryption must not be applied to the corresponding timeslots, the 32-bit output data from OF1 is not used for HDCP Encryption, but the CM1 cipher module continues to be clocked. The block module BM1 is clocked. In parallel, LM0 and BM0 are also clocked with the rekey enable signal de-asserted.

In the SST mode, the 32-bit data output from OF1 is used for HDCP Encryption of data symbols. Control symbols are not encrypted. The block module BM1 is clocked. In parallel, LM0 and BM0 are also clocked with the rekey enable signal de-asserted.

Thus, in both the MST and SST modes, the B and K register states in CM0 and CM1 are in sync until the next hdcpBlockCipher or hdcpRekeyCipher operations are initiated in CM0. Refer to Section 5.1 and Section 6.1 for an overview of the operations of CM0 and CM1 during hdcpBlockCipher, hdcpStreamCipher and hdcpRekeyCipher computations.

hdcpRekeyCipher

hdcpRekeyCipher operation is implemented in CM0. At the link line boundary when HDCP Encryption is enabled in the MST mode or on detection of CPBS in the SST mode, hdcpRekeyCipher moves new key material from LM0 into BM0. No other initialization of the cipher state is made, and no outputs are taken from the cipher during re-keying. Both LM0 and BM0 are clocked 56 times. The rekey enable signal is asserted.

While the hdcpRekeyCipher operation is being implemented in CM0, CM1 performs hdcpStreamCipher operation in parallel. At the end of the hdcpRekeyCipher operation, contents are transferred from BM0 to BM1. Refer to Section 5.1 and Section 6.1 for an overview of the operations of CM0 and CM1 during hdcpBlockCipher, hdcpStreamCipher and hdcpRekeyCipher computations.

hdcpRngCipher

The HDCP Cipher must be used as defined in Figure 4-6 to produce the value *An* required for the authentication protocol. This state diagram references HDCP Transmitter states from Figure 2-9.

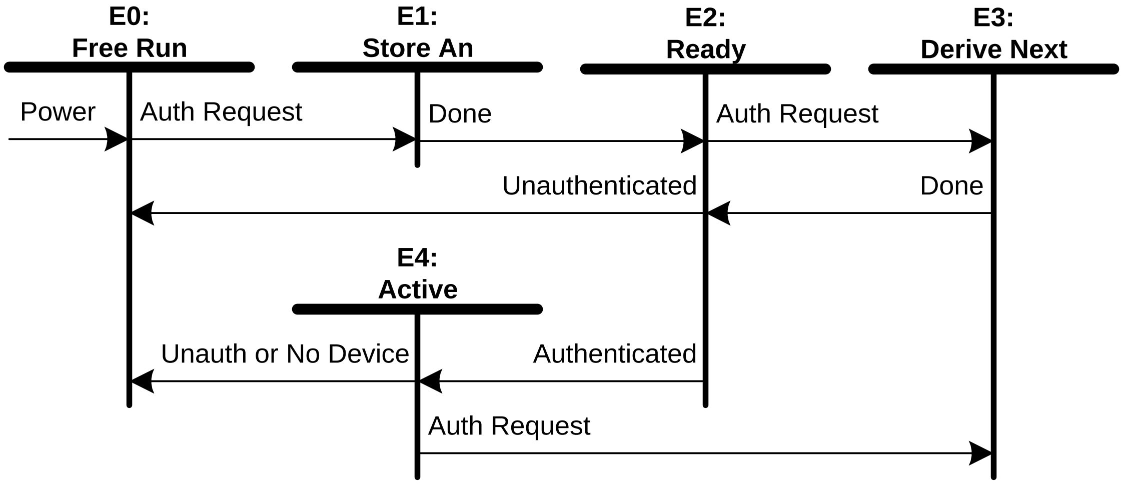

Figure 4-6. hdcpRngCipher State Diagram

Transition Any State:E0. On power up the HDCP Cipher is allowed to free run from its initial state, clocked by the pixel clock.

State E0: Free Run. The HDCP Cipher is clocked from its current state.

Transition E0:E1. An authentication request to the HDCP Transmitter causes this transition. Authentication requests are identified by an HDCP Transmitter state transition to State:A1.

State E1: Store An. *An* is taken from the HDCP Cipher output function bits that are ordinarily used to produce *Mi*. This requires four clocks.

Transition E1:E2. This transition is made immediately upon storage of *An*.

State E2: Ready. The *An* value is available for the authentication protocol.

Transition E2:E0. This transition is made if the current authentication fails, as indicated by an HDCP Transmitter state transition to State:A0.

Transition E2:E3. A new authentication request causes a new *An* value to be derived.

Transition E2:E4. The authentication protocol using the derived *An* is successful, as indicated by an HDCP Transmitter state transition to State:A4.

State E3: Derive Next. A new *An* is derived using the hdcpBlockCipher sequence, using the current values stored in the *Mi* and *Ki* registers.

Transition E3:E2. This transition is made immediately upon storage of *An.*

State E4: Active. The HDCP Transmitter is authenticated with a HDCP Receiver.

Transition E4:E0. This transition is made whenever the HDCP Transmitter becomes unauthenticated or if the HDCP Receiver is detached or goes inactive.

Transition E4:E3. An authentication request to the HDCP Transmitter causes this transition.

This pseudorandom number generator must implement a method to receive bits of outside influence. This method must mix the input influence bits into the values of the block register without replacement. That is, there must no way to determine the value--only change it from whatever it is to another value. For example, one can exclusive-or the influence values into the state. However, any 1-to-1 operation that does not reduce the number possible values or skew the otherwise uniform probability distribution of possible values is acceptable.

The bits of influence shall come from a source of reasonable variability or entropy. A reasonable level of variability or entropy is established if, given 1,000,000 different power up cycles on the HDCP Transmitter logic such that the amount of time from power up to the initial authentication were controlled precisely enough to eliminate any variability from the free running of the cipher before initial authentication (i.e. the number of clocks applied to the cipher in State E0 remains unchanged between different tests), and the An values from the first authentication attempt after the additional influence has been applied (using different content streams if this influence comes from the content stream), the probability of there being any duplicates in this list of 1,000,000 An values collected is less than 50%. This corresponds to about 40 (considering one million is about 2^20) random bits out of the 64 (or equivalent if the bits are biased).

An (incomplete) list of sources of entropy might include:

a) a true Random Number Generator or analog noise source, even if a poor (biased) one
b) a pseudo-random number generator (PRNG) where the state is stored in non-volatile memory after each use. (That is, every power on continues the sequence--it does produce not the same sequence each time). Flash memory or even disk is usable for this purpose as long as it is reasonably secure from tampering. The hdcpRngCipher combined with tamper-resistant non-volatile memory is one such solution.
c) timers, network statistics, error correction information, radio/cable television signals, disk seek times, etc.
d) Since the random number An is not used for secret material, a reliable (not manipulatable by the user) calendar and time-of-day clock can be used as seed. For example, some broadcast content sources may give reliable date and time information.

Different product environments have different resources available to them. There is generally no one source that is available in all environments.

The initial state of the hdcpRngCipher is not defined and is left to the implementer. Ideally, one would prefer that the initial value be different for each device power-on, though this is not possible in many environments. In addition, the Rekey enable signal may but need not be enabled during hdcpRngCipher operation.

The An values do not have to be secret, but must be fresh. That is, the method of producing new values must have integrity.

While each An value is already required to be fresh, HDCP Devices that have multiple inputs or outputs must ensure that each downstream link receives a distinct An value. This ensures that each link between HDCP devices that have multiple inputs or outputs sharing the same device keys will produce distinct session keys (Ks), encryption keystreams, and authentication values.

5 Encryption Status Signaling in MST Mode

An HDCP Transmitter signals a downstream device that encryption is enabled or disabled and indicates whether or not encryption must be applied to a given timeslot using the DisplayPort Encryption Signaling (DPES) protocol. HDCP Encryption must be enabled by the HDCP Transmitter only when it is in an authenticated state, at all other times HDCP Encryption must be disabled. Authenticated state for an HDCP Transmitter is State A4. Authenticated states for HDCP Receivers are State B2 and State B3. Authenticated states for HDCP Repeaters are State C2 and C3. For interoperability with a DisplayPort-HDCP 1.0-compliant HDCP Receiver, a DisplayPort-HDCP 1.1-compliant HDCP Transmitter must support and implement DisplayPort-HDCP 1.0-compliant behavior.

This section describes the DPES protocol implemented in the MST mode.

The DPES protocol in MST mode uses an HDCP Encryption Indicator bit to indicate whether HDCP Encryption is enabled or disabled. XOR Enable/Disable Indicator bits are used to indicate whether HDCP Encryption must be applied to a specific MTP timeslot during hdcpStreamCipher operation. Section 4.5 explains hdcpStreamCipher operation.

HDCP Encryption is enabled or disabled at link frame boundaries using an HDCP Encryption Indicator bit in the MTP Header.

A multi-stream link may be comprised of different content streams where some content streams may require HDCP Encryption to be applied and some for which HDCP Encryption is not required. An XOR Enable/Disable indication, corresponding to each of the 63 MTP timeslots, contained in MTP Header bits indicates whether or not HDCP Encryption must be applied to each timeslot during hdcpStreamCipher operation. Section 4.5 explains hdcpStreamCipher operation. XOR Enable/Disable indication is valid only when HDCP Encryption is enabled as indicated by the HDCP Encryption Indicator bit. When HDCP Encryption is disabled as indicated by the HDCP Encryption Indicator bit, any further XOR Enable/Disable indication must be ignored.

The HDCP Encryption Indicator bit and the bits used for XOR Enable/Disable indication are represented by a 64-bit data structure referred to as HDCP_Encryption_Control, where

> HDCP_Encryption_Control[0] = HDCP Encryption Indicator bit. When HDCP Encryption is disabled, the HDCP Encryption Indicator bit is set to 0. When HDCP Encryption is enabled, the HDCP Encryption Indicator bit is set to 1.
>
> HDCP_Encryption_Control[1..63] = XOR Enable/Disable Indicator bits. HDCP_Encryption_Control[1] corresponds to XOR Enable/Disable indication for timeslot 1 and so on. XOR Enable/Disable Indicator bits are set to 0 (XOR Disabled) when HDCP Encryption must not be applied to the corresponding timeslots during hdcpStreamCipher operation. They are set to 1 (XOR Enabled) when HDCP Encryption must be applied to the corresponding timeslots during hdcpStreamCipher operation.

The 64-bit HDCP_Encryption_Control is contained in the Encryption_Control_Field which is described in the DisplayPort Specification (see References). The HDCP_Encryption_Control occupies eight MTP Headers.

The HDCP_Encryption_Control is transmitted in the Encryption_Control_Field as explained in the DisplayPort specification (see References). The HDCP_Encryption_Control consists of an 8 (scrambled) data code sequence spanning consecutive MTPH's. The data code sequence is identical per-lane, regardless of lane count. The HDCP_Encryption_Control is repeated four consecutive times, resulting in a total sequence length of 32 MTPs. HDCP Receivers apply majority voting to the repeated sequence for error correction, as described in DisplayPort specification. Unless otherwise noted, references in the HDCP specification to receiver use of the HDCP_Encryption_Control refer to the post-error corrected result.

The HDCP_Encryption_Control must be transmitted starting exactly 36 MTPs prior to each link frame boundary SR signal, and immediately prior to any standalone ACT[2] sequence. A single HDCP_Encryption_Control must be transmitted immediately preceding any (optional) back to back ACT/SR sequence.

The HDCP_Encryption_Control starting 36 MTPs before the SR is used to enable or disable HDCP Encryption in addition to indicating XOR Enable/Disable status for timeslots. The HDCP Encryption Indicator bit is valid only at link frame boundaries and HDCP Encryption is enabled/disabled only at link frame boundaries.

The HDCP_Encryption_Control preceding a standalone ACT must not be used to enable or disable HDCP Encryption. It is only used to indicate XOR Enable/Disable status for every timeslot. The HDCP Encryption Indicator bit in the HDCP_Encryption_Control preceding a standalone ACT must be ignored.

In cases of the (optional) back-to-back ACT/SR sequence an HDCP Transmitter must transmit a single HDCP_Encryption_Control sequence preceding the ACT/SR pair. The HDCP_Encryption_Control preceding an ACT/SR pair is used to enable/disable HDCP Encryption in addition to indicating XOR Enable/Disable status for timeslots.

A link line is a fixed 2^13 timeslots, resulting in eight link lines per link frame. hdcpRekeyCipher operation is initiated immediately following the 2^13th timeslot.

Devices compliant with DisplayPort-HDCP 1.0 and higher must support and use Enhanced Framing Mode. Refer to the DisplayPort Specification for more details regarding enhanced framing mode (see References).

5.1 Encryption Status Signaling and HDCP Cipher Operations

[2] For this section, a *standalone ACT* is defined as an ACT not part of a back-to-back ACT/SR sequence

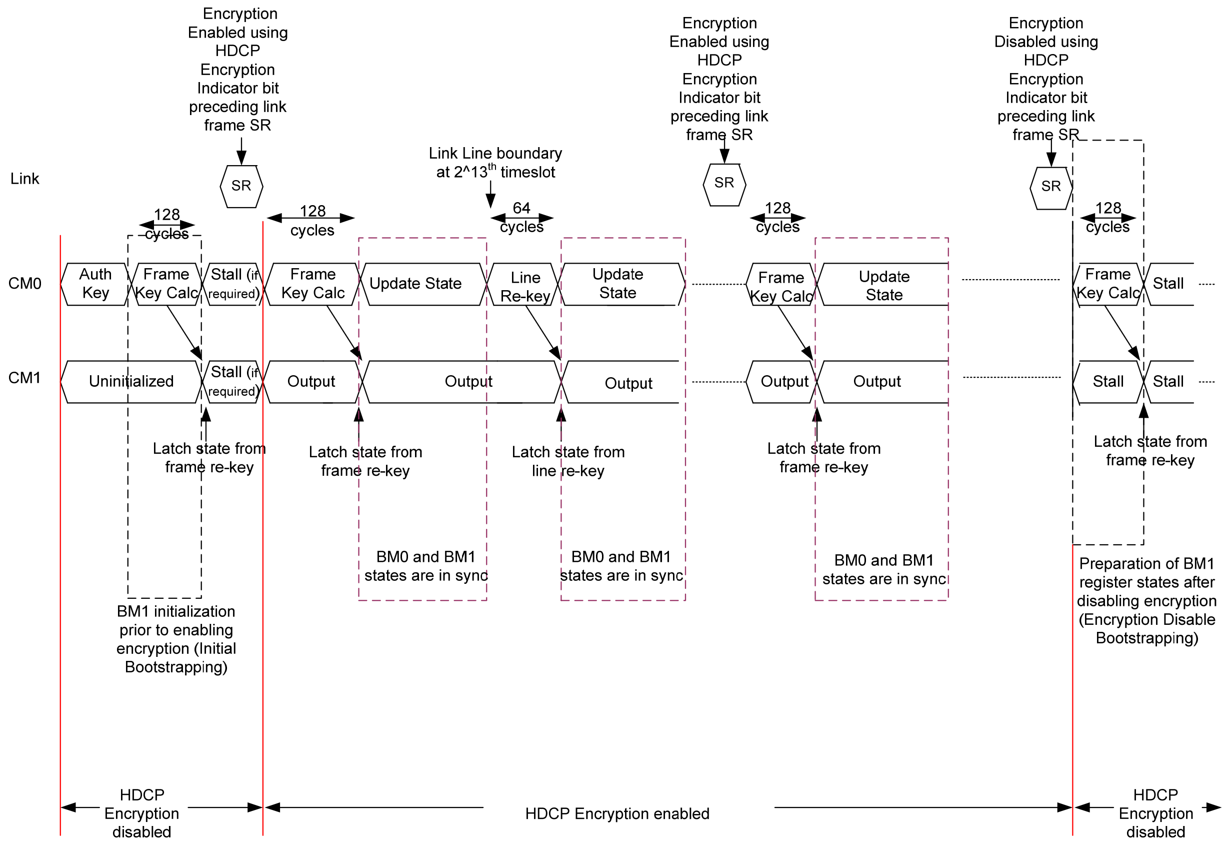
Encryption Enabled using HDCP Encryption Indicator bit preceding link frame SR
Link Line boundary at 2^13th timeslot
Encryption Enabled using HDCP Encryption Indicator bit preceding link frame SR
Encryption Disabled using HDCP Encryption Indicator bit preceding link frame SR
Link
SR
SR
SR
128 cycles
128 cycles
64 cycles
128 cycles
128 cycles
CM0
Auth Key
Frame Key Calc
Stall (if required)
Frame Key Calc
Update State
Line Re-key
Update State
Frame Key Calc
Update State
Frame Key Calc
Stall
CM1
Uninitialized
Stall (if required)
Output
Output
Output
Output
Output
Stall
Stall
Latch state from frame re-key
Latch state from frame re-key
Latch state from line re-key
Latch state from frame re-key
Latch state from frame re-key
BM0 and BM1 states are in sync
BM0 and BM1 states are in sync
BM0 and BM1 states are in sync
BM1 initialization prior to enabling encryption (Initial Bootstrapping)
Preparation of BM1 register states after disabling encryption (Encryption Disable Bootstrapping)
HDCP Encryption disabled
HDCP Encryption enabled
HDCP Encryption disabled

Figure 5-1. Encryption Status Signaling and HDCP Cipher Operations

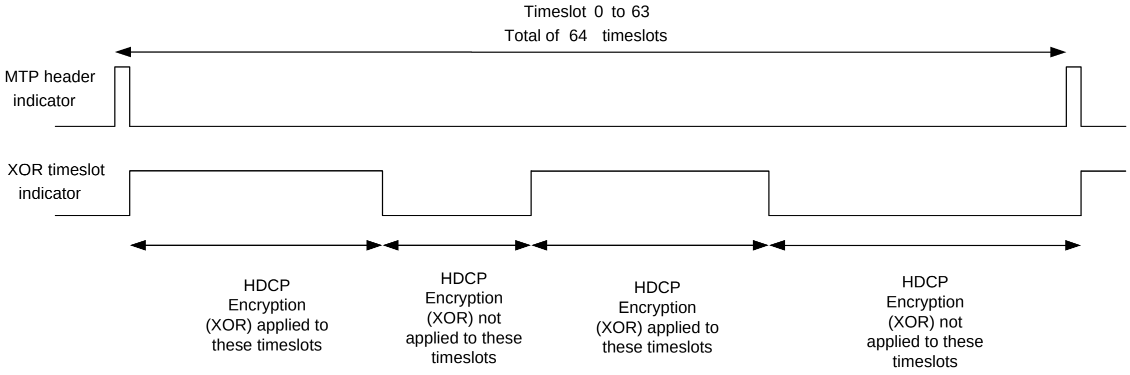
Timeslot 0 to 63
Total of 64 timeslots
MTP header indicator
XOR timeslot indicator
HDCP Encryption (XOR) applied to these timeslots
HDCP Encryption (XOR) not applied to these timeslots
HDCP Encryption (XOR) applied to these timeslots
HDCP Encryption (XOR) not applied to these timeslots

Figure 5-2. HDCP Encryption Applied Based on HDCP_Encryption_Control Bits 1:63

Figure 5-1 references the HDCP Cipher structure from Figure 4-1. As illustrated in the figure, hdcpRekeyCipher (line re-key), hdcpStreamCipher and hdcpBlockCipher (frame key calculation) operations are performed in CM0 and hdcpStreamCipher operations are performed in CM1. When HDCP Encryption is enabled, hdcpRekeyCipher operation must be completed within 64 clocks immediately following the link line boundary and hdcpBlockCipher operation must be completed within 128 clocks immediately following the transmission/reception of SR at the link frame boundary. A series of dummy cycles are inserted during the 64 clock period and the 128 clock period since both hdcpRekeyCipher and hdcpBlockCipher operations take less than 64 clocks and 128 clocks respectively to implement. CM0 is not clocked during the dummy cycle period.

Completion of the R_0 and M_0 computations during the first phase of authentication triggers frame key calculation using the hdcpBlockCipher operation in CM0. This is done to initialize the BM1 module prior to enabling HDCP Encryption. This is referred to as the Initial Bootstrapping operation. After HDCP Encryption is enabled, as indicated by the transmission of the HDCP_Encryption_Control starting 36 MTPs before an SR or immediately preceding a back-to-back ACT/SR sequence with HDCP Encryption Indictor bit set to 1, subsequent SR transmissions and link line boundaries are followed by hdcpBlockCipher and hdcpRekeyCipher operations respectively in CM0. hdcpBlockCipher operation must be completed within 128 clocks and hdcpRekeyCipher operation must be completed within 64 clocks. hdcpStreamCipher operations are implemented in parallel in CM1 during both the 64 clock period and the 128 clock period. The hdcpStreamCipher operations are implemented as explained in Section 4.5. The B and K register contents are transferred from BM0 to BM1 immediately at the end of the 64 clock period and the 128 clock period.

After the transfer of B and K register contents, hdcpStreamCipher operation is performed in CM0. LM0 and BM0 are clocked with the re-key enable signal de-asserted. The 32-bit output data from OF0 is not used for HDCP Encryption. BM1 is also clocked and performs hdcpStreamCipher computations as explained in Section 4.5. Thus, the cipher states in CM0 and CM1 are in sync until the next hdcpBlockCipher or hdcpRekeyCipher operations are initiated in CM0, as illustrated in Figure 5-1.

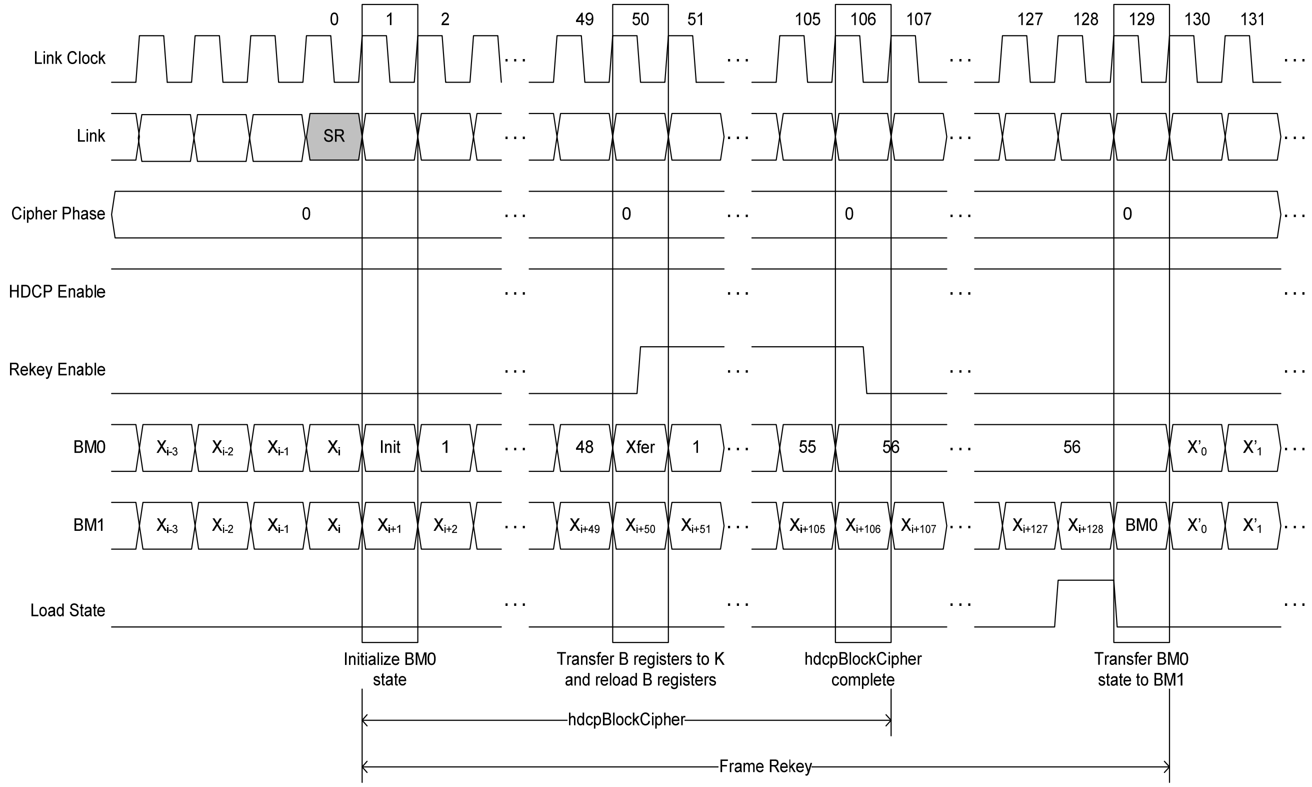

Figure 5-3. 4-Lane Frame Key Calculation Timing Diagram

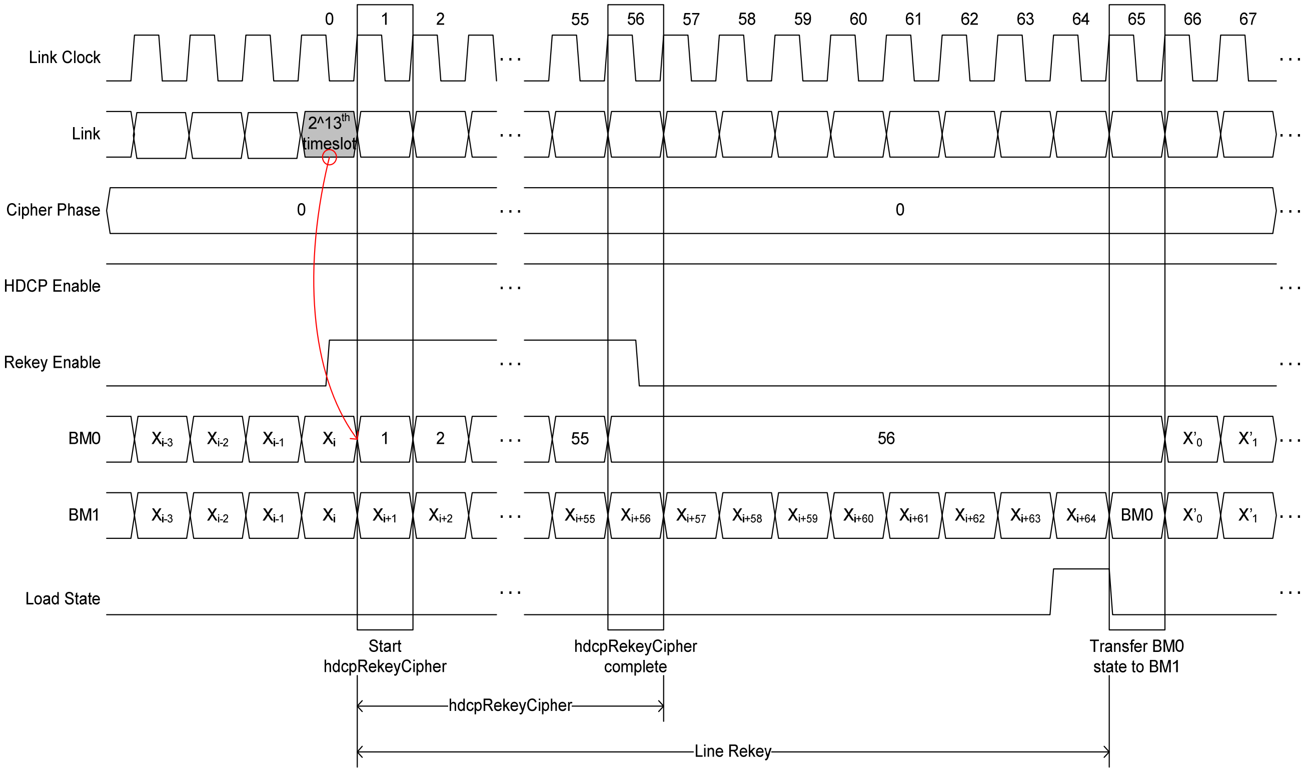

Figure 5-4. 4-Lane Line Re-key Timing Diagram

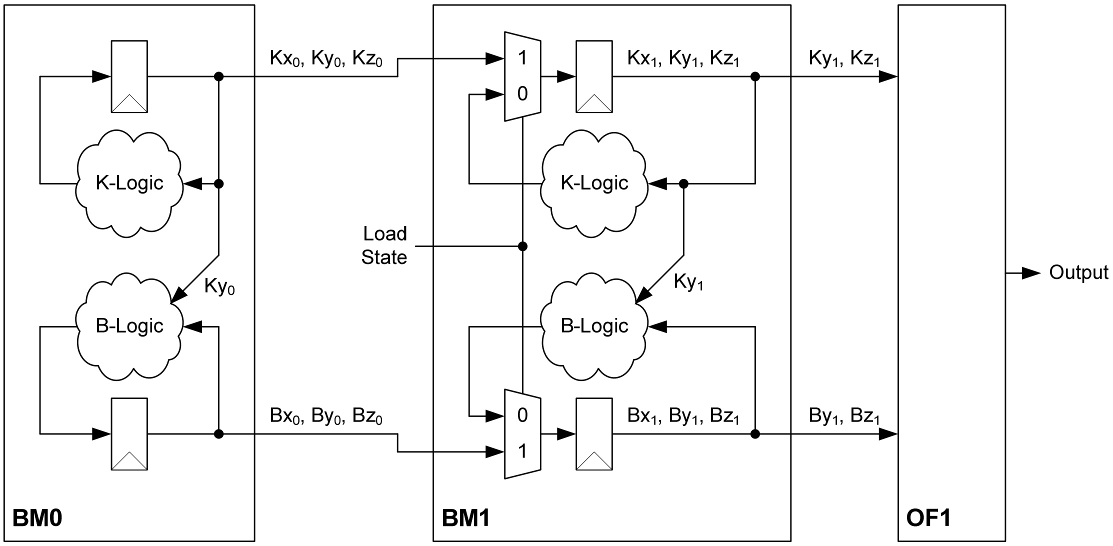

Figure 5-5. BM0/BM1 State Transfer Schematic

HDCP Encryption is disabled at the link frame boundary by the transmission of the HDCP_Encryption_Control starting 36 MTPs before an SR or immediately preceding a back-to-back ACT/SR sequence with HDCP Encryption Indictor bit set to 0. As illustrated in Figure 5-1, when encryption is enabled, transmission of the HDCP_Encryption_Control starting 36 MTPs before an SR or immediately preceding a back-to-back ACT/SR sequence with HDCP Encryption

Indictor bit set to 0 causes the hdcpBlockCipher operation to be implemented within 128-clocks following an SR. The B and K register contents are transferred from BM0 to BM1 immediately at the end of the 128 clock period. This serves to prepare the register states in BM1 so that encryption may be applied seamlessly when it is re-enabled provided there were no intervening hot plugs or hot unplugs between the time encryption was disabled and re-enabled. This operation is referred to as Encryption Disable Bootstrapping. Following the transfer, the CM0 and CM1 modules transition into an idle state until encryption is re-enabled.

Encryption disable bootstrapping must be implemented by HDCP Receivers when HDCP Encryption is disabled. In the case of HDCP Transmitters, encryption disable bootstrapping must not be implemented if encryption was disabled due to the detection of a hot plug, hot unplug, link errors (e.g. link integrity check failure) or any other event that causes the link to be unauthenticated. In all other cases where encryption is disabled while the link is still active and authenticated, encryption disable bootstrapping can be implemented by the HDCP Transmitter. If the HDCP Transmitter chooses to not implement encryption disable bootstrapping, it must initiate re-authentication with the HDCP Receiver before transmitting HDCP Content when encryption is re-enabled.

Detection of any intervening hot plugs or hot unplugs during the time encryption is disabled will require re-authentication.

5.2 Encryption/Decryption State Diagrams

Figure 5-6 and Figure 5-7 illustrate the state transitions of CM0 and CM1 while using DPES encryption signaling. This diagram is applicable to both HDCP Transmitters and HDCP Receivers. As illustrated in Figure 5-6, detection of an SR symbol during a line key calculation will result in the line key calculation to be abandoned and the frame key calculation to begin (Transition G5:G2). Section 3 explains the HDCP Cipher clock rate relative to the link symbol clock rate.

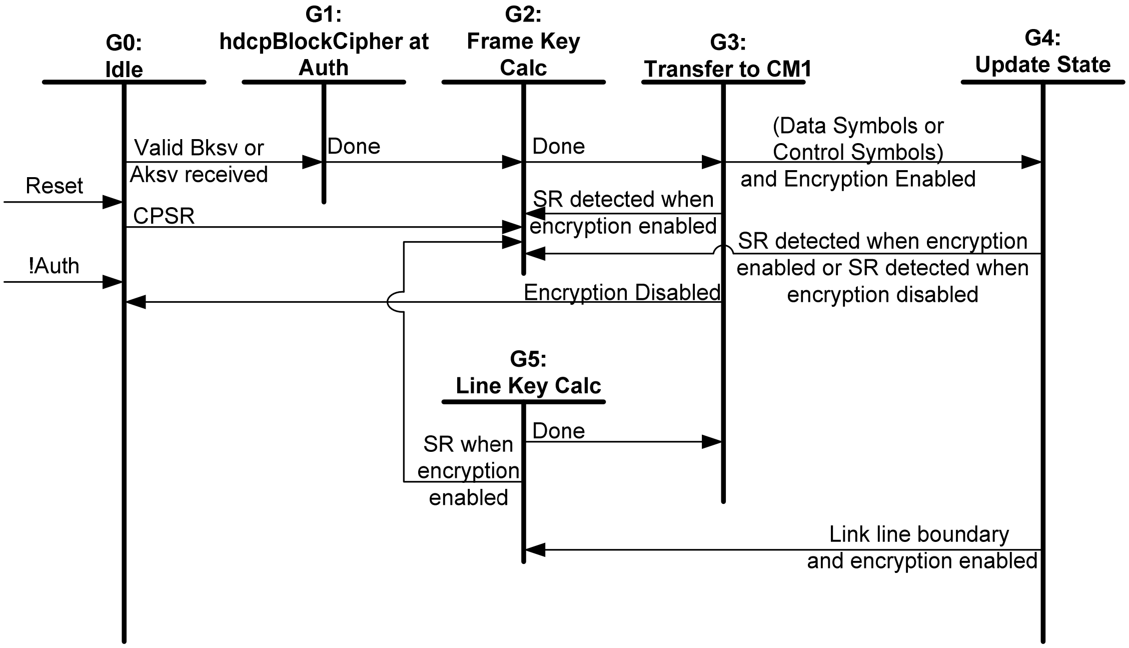

Figure 5-6. CM0 Encryption/Decryption State Diagram (DPES)

Transition Any State:G0. Reset conditions or transitions into the unauthenticated state at the HDCP Device cause the CM0 encryption state machine to transition to the idle state.

State G0:Idle. The HDCP Cipher is free running and available for use as hdcpRngCipher. Refer to Section 4.5 for an explanation of hdcpRngCipher.

Transition G0:G1. When a valid *Bksv* or *Aksv* is received by the HDCP Transmitter or HDCP Receiver it begins the hdcpBlockCipher at authentication operation. Refer to Section 4.5 for an explanation of hdcpBlockCipher operation.

State G1:hdcpBlockCipher At Authentication. The R_0 and M_0 values are computed as explained in Section 4.5 using the hdcpBlockCipher.

Transition G1:G2. Successful completion of first phase of authentication transitions the CM0 state machine into the frame key calculation state to perform the Initial Bootstrapping operation.

State G2:Frame Key Calculation. M_i is computed in this state and a frame key is calculated using hdcpBlockCipher as explained in Section 4.5. This operation is initiated at the end of hdcpBlockCipher at Authentication or on detecting an SR at the link frame boundary when HDCP Encryption is enabled as indicated by the transmission of the HDCP_Encryption_Control starting 36 MTPs before an SR or immediately preceding a back-to-back ACT/SR sequence with HDCP Encryption Indictor bit set to 1. It must be completed within 128-clocks starting immediately after hdcpBlockCipher at Authentication or after transmission/reception of SR symbol.

Transition G2:G3. The frame key is calculated within 128 clocks. At the end of the 128 clock period, contents are transferred from BM0 to BM1.

State G3:Transfer to CM1. In this state register contents are transferred from BM0 to BM1.

Transition G3:G2. Detection of an SR when encryption is enabled causes frame key calculation using hdcpBlockCipher as explained in Section 4.5.

Transition G3:G0. After transfer to CM1, if encryption is currently disabled, the state machine transitions to the idle state.

Transition G3:G4. Detection of valid data symbols or control symbols when encryption is enabled causes this transition.

State G4:Update State. In this state, hdcpStreamCipher operation is implemented in CM0. LM0 and BM0 are clocked with the re-key enable signal de-asserted thus causing their register states to change for every clock. The 32-bit output from the output function OF0 is not used.

Transition G4:G2. Detection of an SR when HDCP Encryption is enabled or disabled causes frame key calculation using hdcpBlockCipher as explained in Section 4.5. Frame key calculation is performed on detection of an SR when encryption is disabled to prepare the register states in BM1 so that encryption may be applied seamlessly when it is re-enabled. This is referred to as the Encryption Disable Bootstrapping operation (see Figure 5-1). This operation is implemented by HDCP Receivers after detection of SR when encryption is disabled. This operation may be implemented by HDCP Transmitters as soon as encryption is disabled and the link is still active and authenticated. If the link is unauthenticated, the CM0 state machine in HDCP Transmitters transition into the Idle state.

Transition G4:G5. When encryption is enabled, line key calculation is implemented using hdcpRekeyCipher at the link line boundary as explained in Section 4.5.

State G5:Line Key Calculation. A line key is calculated using hdcpRekeyCipher as explained in Section 4.5. This operation is initiated at the link line boundary. It must be completed within 64-clocks starting at the link line boundary.

Transition G5:G3. The line key is calculated within 64 clocks. At the end of the 64 clock period, contents are transferred from BM0 to BM1.

Transition G5:G2. Detection of an SR when encryption is enabled causes frame key calculation using hdcpBlockCipher as explained in Section 4.5.

Transition G0:G2. Detection of an SR when encryption is enabled causes frame key calculation using hdcpBlockCipher as explained in Section 4.5. This transition occurs when encryption is re-enabled after it has been disabled and the Encryption Disable Bootstrapping operation has been implemented.

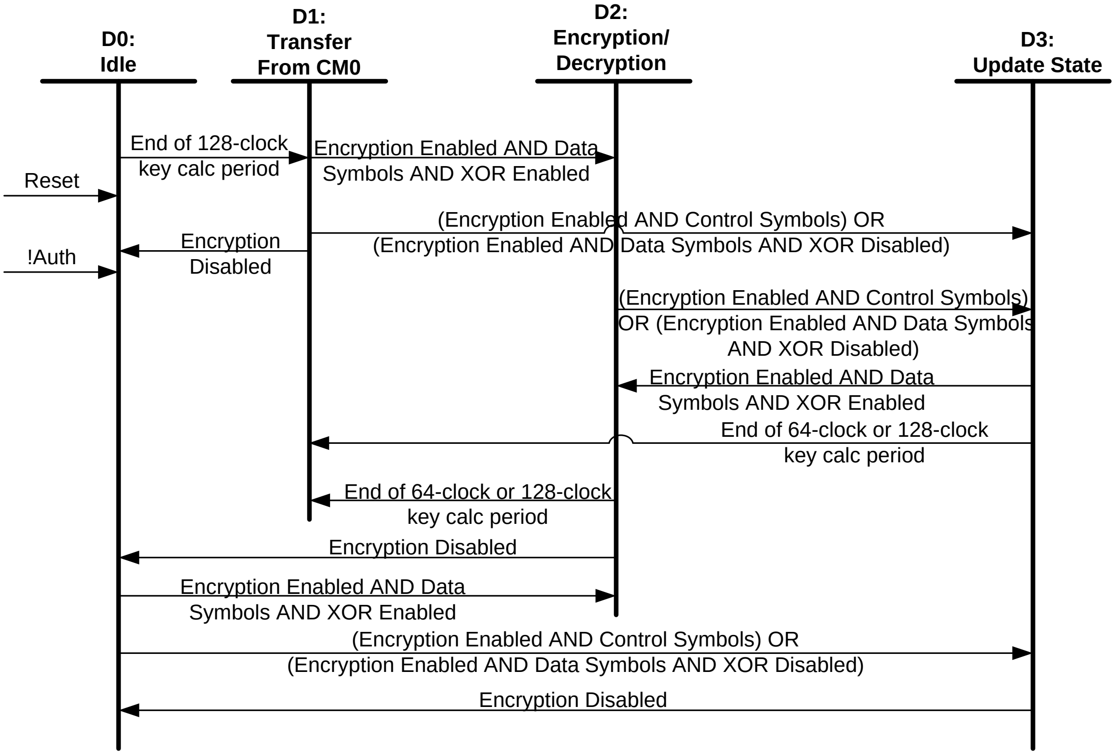
D0:
Idle
D1:
Transfer
From CM0
D2:
Encryption/
Decryption
D3:
Update State
Reset
!Auth
End of 128-clock key calc period
Encryption Enabled AND Data Symbols AND XOR Enabled
Encryption Disabled
(Encryption Enabled AND Control Symbols) OR (Encryption Enabled AND Data Symbols AND XOR Disabled)
(Encryption Enabled AND Control Symbols) OR (Encryption Enabled AND Data Symbols AND XOR Disabled)
Encryption Enabled AND Data Symbols AND XOR Enabled
End of 64-clock or 128-clock key calc period
End of 64-clock or 128-clock key calc period
Encryption Disabled
Encryption Enabled AND Data Symbols AND XOR Enabled
(Encryption Enabled AND Control Symbols) OR (Encryption Enabled AND Data Symbols AND XOR Disabled)
Encryption Disabled

Figure 5-7. CM1 Encryption/Decryption State Diagram (DPES)

Transition Any State:D0. Reset conditions or transitions into the unauthenticated state at the HDCP Device cause the CM1 encryption state machine to transition to the idle state.

Transition D0:D1. End of the 128-clock frame key calculation period in CM0 causes the transfer of block module register contents from CM0 to CM1.

State D1:Transfer From CM0. Contents are transferred from BM0 to BM1.

Transition D1:D0. When encryption is disabled as indicated by the transmission of the HDCP_Encryption_Control starting 36 MTPs before an SR or immediately preceding a back-to-back ACT/SR sequence with HDCP Encryption Indictor bit set to 0, the CM1 encryption state machine transitions to the idle state.

Transition D1:D2. When encryption is enabled, detection of valid data symbols in timeslots for which XOR is enabled initiates encryption / decryption.

State D2:Encryption/Decryption. In this state, the data symbols are encrypted/decrypted using hdcpStreamCipher operation which is explained in Section 4.5.

Transition D2:D3. Detection of control symbols when encryption is enabled causes this transition. The transition also occurs when encryption is enabled and data symbols are detected in timeslots for which XOR is disabled.

State D3:Update State. In this state CM1 performs hdcpStreamCipher computations which is explained in Section 4.5; BM1 is clocked thus causing its register states to change. HDCP Encryption is not applied in this state.

Transition D3:D2. When encryption is enabled, detection of valid data symbols in timeslots for which XOR is enabled causes this transition. hdcpStreamCipher operation is implemented in CM1 as explained in Section 4.5 and the output data from OF1 is used for HDCP Encryption of data symbols only.

Transition D1:D3. Detection of control symbols when encryption is enabled causes this transition. The transition also occurs when encryption is enabled and data symbols are detected in timeslots for which XOR is disabled.

Transition D3:D1. End of the 128-clock frame key calculation period or 64-clock line key calculation period in CM0 causes the transfer of block module register contents from CM0 to CM1.

Transition D2:D1. End of the 128-clock frame key calculation period or 64-clock line key calculation period in CM0 causes the transfer of block module register contents from CM0 to CM1.

Transition D0:D2. When encryption is enabled, detection of valid data symbols in timeslots for which XOR is enabled causes this transition. This transition occurs when encryption is re-enabled after it has been disabled and the Encryption Disable Bootstrapping operation has been implemented. The BM1 register states have been prepared as a result of the Encryption Disable Bootstrapping operation and encryption may be applied seamlessly when it is re-enabled.

Transition D0:D3. Detection of control symbols when encryption is enabled causes this transition. The transition also occurs when encryption is enabled and data symbols are detected in timeslots for which XOR is disabled. This transition occurs when encryption is re-enabled after it has been disabled and the Encryption Disable Bootstrapping operation has been implemented.

Transition D2:D0. When encryption is disabled, the CM1 encryption state machine transitions to the idle state.

Transition D3:D0. When encryption is disabled, the CM1 encryption state machine transitions to the idle state.

6 Encryption Status Signaling in SST Mode

HDCP Encryption must be enabled by the HDCP Transmitter only when it is in an authenticated state, at all other times HDCP Encryption must be disabled. Authenticated state for an HDCP Transmitter is State A4. Authenticated states for HDCP Receivers are State B2 and State B3. Authenticated states for HDCP Repeaters are State C2 and C3.

This section describes the DPES protocol implemented in the SST mode.

The DisplayPort transmitter inserts a blanking start (BS) symbol after each line of video is transmitted including the last line of a frame. For audio only transmissions, a BS symbol is transmitted every 8192 symbols per lane. Every 512th BS symbol is replaced by a scrambler reset (SR) symbol. When encryption is currently disabled, BS and SR control symbols are transmitted. When encryption is currently enabled, BS and SR control symbols are replaced by CPBS and CPSR control symbols respectively.

Thus in DPES in the SST mode, detection of SR indicate that encryption is disabled and detection of CPSR indicates that encryption is enabled. The decision to enable or disable encryption is made by the downstream device on detection of a valid CPSR or SR respectively.

Devices compliant with DisplayPort-HDCP 1.0 and higher must support and use Enhanced Framing Mode. Refer to the DisplayPort Specification for more details regarding enhanced framing mode (see References).

6.1 Encryption Status Signaling and HDCP Cipher Operations

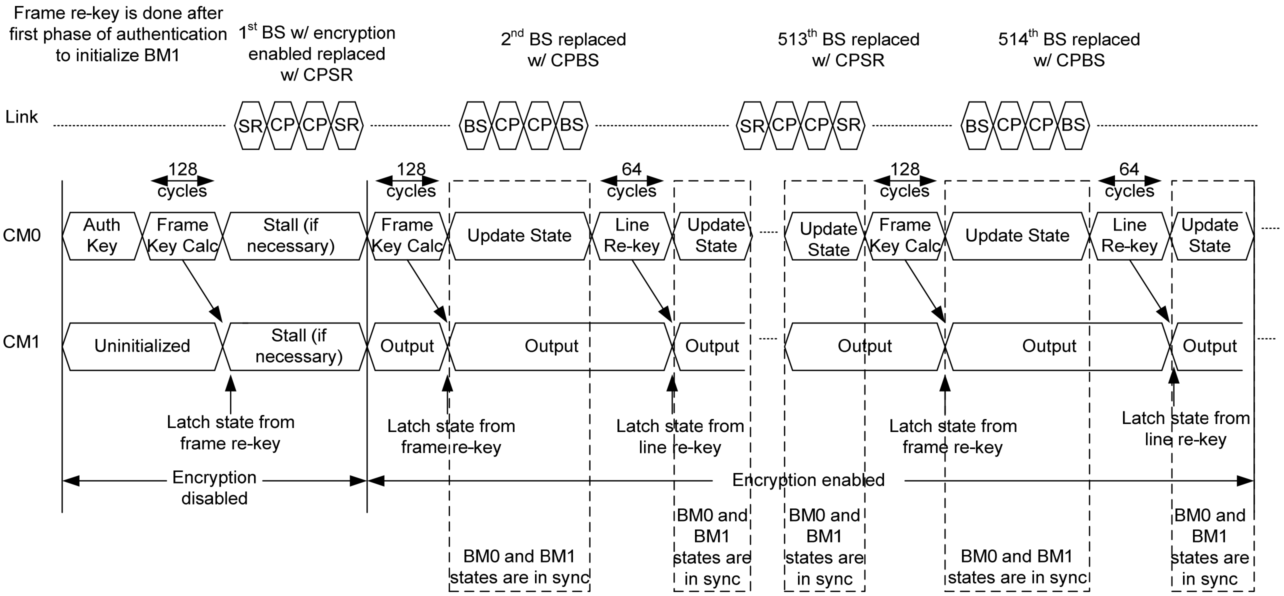
Frame re-key is done after first phase of authentication to initialize BM1
1st BS w/ encryption enabled replaced w/ CPSR
2nd BS replaced w/ CPBS
513th BS replaced w/ CPSR
514th BS replaced w/ CPBS
Link
SR CP CP SR
BS CP CP BS
SR CP CP SR
BS CP CP BS
128 cycles
128 cycles
64 cycles
128 cycles
64 cycles
CM0
Auth Key
Frame Key Calc
Stall (if necessary)
Frame Key Calc
Update State
Line Re-key
Update State
Update State
Frame Key Calc
Update State
Line Re-key
Update State
CM1
Uninitialized
Stall (if necessary)
Output
Output
Output
Output
Output
Output
Latch state from frame re-key
Latch state from frame re-key
Latch state from line re-key
Latch state from frame re-key
Latch state from line re-key
Encryption disabled
Encryption enabled
BM0 and BM1 states are in sync
BM0 and BM1 states are in sync
BM0 and BM1 states are in sync
BM0 and BM1 states are in sync
BM0 and BM1 states are in sync

Figure 6-1. Encryption Status Signaling and HDCP Cipher Operations

Figure 6-1 references the HDCP Cipher structure from Figure 4-1. As illustrated in the figure, hdcpRekeyCipher (line re-key), hdcpStreamCipher and hdcpBlockCipher (frame key calculation) operations are performed in CM0 and hdcpStreamCipher operations are performed in CM1. hdcpRekeyCipher operation must be completed within 64 clocks immediately following the transmission/reception of CPBS and hdcpBlockCipher operation must be completed within 128 clocks immediately following the transmission/reception of CPSR. A series of dummy cycles are inserted during the 64 clock period and the 128 clock period since both hdcpRekeyCipher and hdcpBlockCipher operations take less than 64 clocks and 128 clocks respectively to implement. CM0 is not clocked during the dummy cycle period.

Completion of the R_0 and M_0 computations during the first phase of authentication triggers frame key calculation using the hdcpBlockCipher operation in CM0. This is done prior to enabling HDCP Encryption to initialize the BM1 module. This is referred to as the Initial Bootstrapping operation. Subsequent CPSR and CPBS transmissions are followed by hdcpBlockCipher and hdcpRekeyCipher operations respectively in CM0. hdcpBlockCipher operation must be completed within 128 clocks and hdcpRekeyCipher operation must be completed within 64 clocks. hdcpStreamCipher operations are implemented in parallel in CM1 during both the 64 clock period and the 128 clock period and the 32-bit output data from OF1 is used for HDCP Encryption. The B and K register contents are transferred from BM0 to BM1 immediately at the end of the 64 clock period and the 128 clock period. Figure 6-2 and Figure 6-3 illustrate the 4-lane frame key calculation and 4-lane line re-key operations respectively using the BM0/BM1 functions and interconnections depicted in Figure 6-4. Appendix A illustrates 2-Lane Frame Key Calculation and Line Re-key timing diagrams for Phase 0 and 1 and 1-Lane Frame Key Calculation and Line Re-key timing diagrams for Phase 0, 1, 2 and 3.

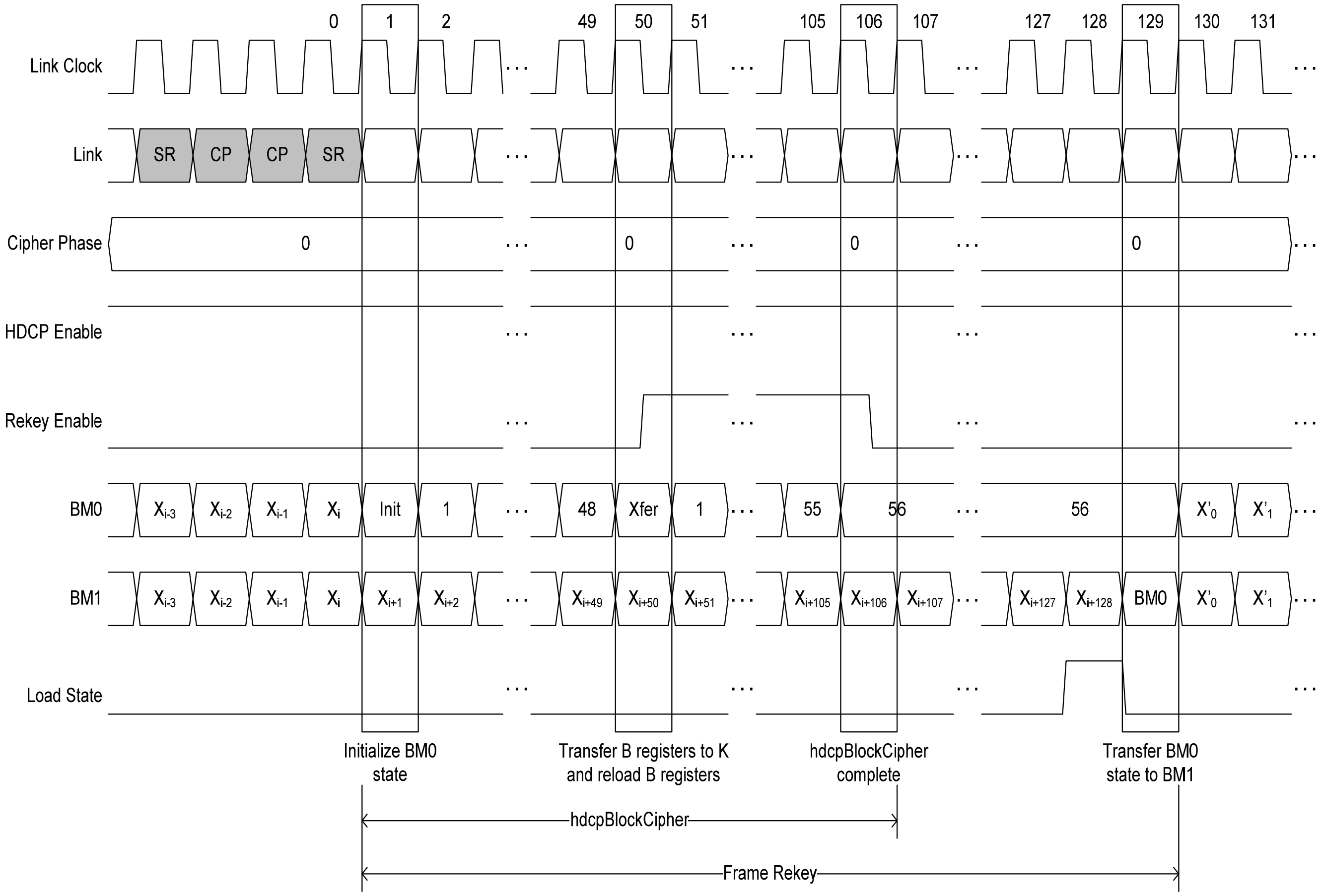

Figure 6-2. 4-Lane Frame Key Calculation Timing Diagram

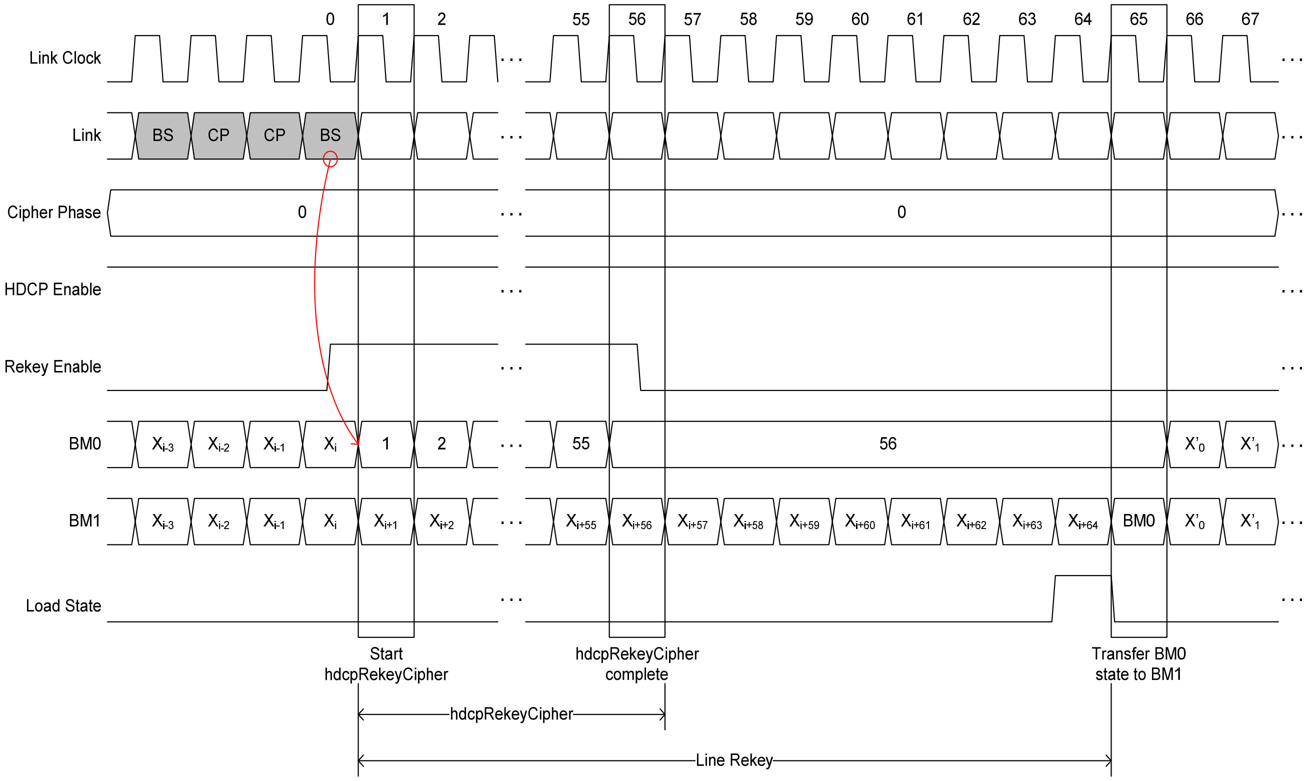
0 1 2 55 56 57 58 59 60 61 62 63 64 65 66 67
Link Clock
Link
BS CP CP BS
Cipher Phase
0
0
HDCP Enable
Rekey Enable
BM0
X_{i-3} X_{i-2} X_{i-1} X_i 1 2 55 56 X'_0 X'_1
BM1
X_{i-3} X_{i-2} X_{i-1} X_i X_{i+1} X_{i+2} X_{i+55} X_{i+56} X_{i+57} X_{i+58} X_{i+59} X_{i+60} X_{i+61} X_{i+62} X_{i+63} X_{i+64} BM0 X'_0 X'_1
Load State
Start hdcpRekeyCipher
hdcpRekeyCipher complete
Transfer BM0 state to BM1
hdcpRekeyCipher
Line Rekey

Figure 6-3. 4-Lane Line Re-key Timing Diagram

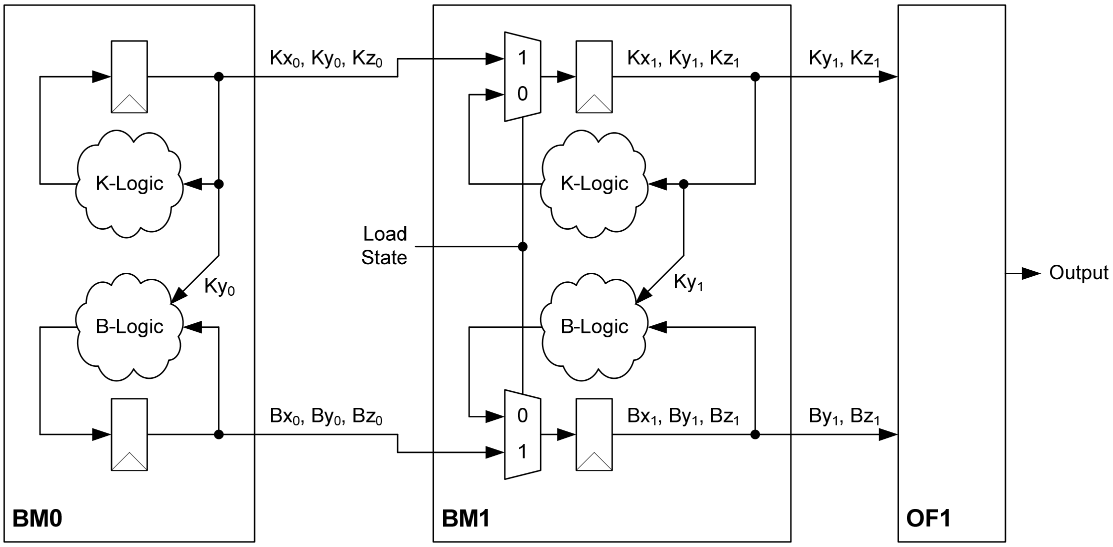

Figure 6-4. BM0/BM1 State Transfer Schematic

After the transfer of B and K register contents, hdcpStreamCipher operation is performed in CM0. LM0 and BM0 are clocked with the re-key enable signal de-asserted. The 32-bit output data from OF0 is not used for HDCP Encryption. BM1 is also clocked and performs hdcpStreamCipher computations. Thus, the cipher states in CM0 and CM1 are in sync until the next hdcpBlockCipher or hdcpRekeyCipher operations are initiated in CM0, as illustrated in Figure 5-1.

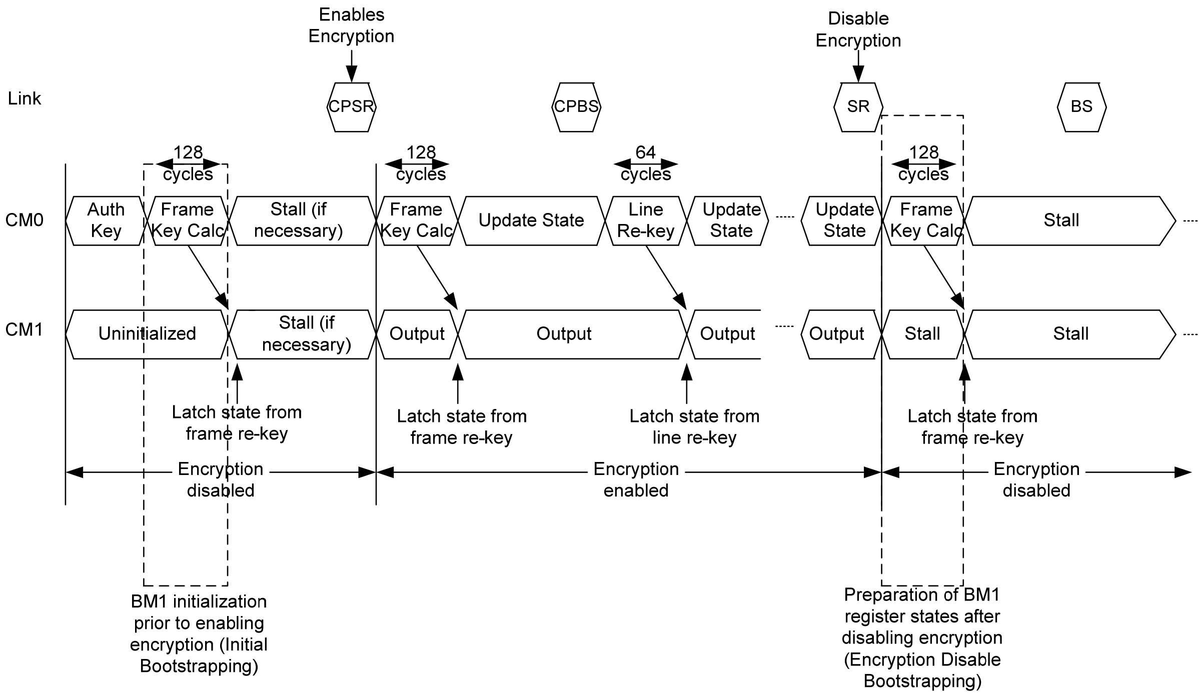

Figure 6-5. Preparation of BM1 Register States

Detection of SR causes encryption to be disabled. As illustrated in Figure 6-5, when encryption is currently enabled, detection of SR causes the hdcpBlockCipher operation to be implemented within 128-clocks following an SR. The B and K register contents are transferred from BM0 to BM1 immediately at the end of the 128 clock period. This serves to prepare the register states in BM1 so that encryption may be applied seamlessly on detection of a CPSR (i.e. when encryption is re-enabled) provided there were no intervening hot plugs or hot unplugs between the time encryption was disabled and re-enabled. This operation is referred to as Encryption Disable Bootstrapping. Following the transfer, the CM0 and CM1 modules transition into an idle state until encryption is re-enabled.

Encryption disable bootstrapping must be implemented by HDCP Receivers on detection of an SR. In the case of HDCP Transmitters, encryption disable bootstrapping must not be implemented if encryption was disabled due to the detection of a hot plug, hot unplug, link errors (e.g. link integrity check failure) or any other event that causes the link to be unauthenticated. In all other cases where encryption is disabled while the link is still active and authenticated, encryption disable bootstrapping can be implemented by the HDCP Transmitter. If the HDCP Transmitter chooses to not implement encryption disable bootstrapping, it must initiate re-authentication with the HDCP Receiver before transmitting HDCP Content when encryption is re-enabled. Some example scenarios where encryption disable bootstrapping may be applied include:

- Video format changes at the HDCP Transmitter when protected content is flowing cause the HDCP Transmitter to temporarily disable HDCP Encryption for a few frames.

- The HDCP Transmitter disables HDCP Encryption when instructed by the Upstream Content Control Function and re-enables HDCP Encryption when CP is desired by the Upstream Content Control Function.

In both these cases, encryption disable bootstrapping operation enables HDCP Encryption to be applied seamlessly when it is re-enabled by the HDCP Transmitter without requiring any re-authentication. Detection of any intervening hot plugs or hot unplugs during the time encryption is temporarily disabled will require re-authentication.

6.2 Encryption/Decryption State Diagrams

Figure 6-6 and Figure 6-7 illustrate the state transitions of CM0 and CM1 while using DPES encryption signaling. This diagram is applicable to both HDCP Transmitters and HDCP Receivers. As illustrated in Figure 6-6, detection of a CPSR symbol during a line key calculation will result in the line key calculation to be abandoned and the frame key calculation to begin (Transition G5:G2). A CPBS symbol detected during frame key calculation is ignored. Section 3 explains the HDCP Cipher clock rate relative to the link symbol clock rate.

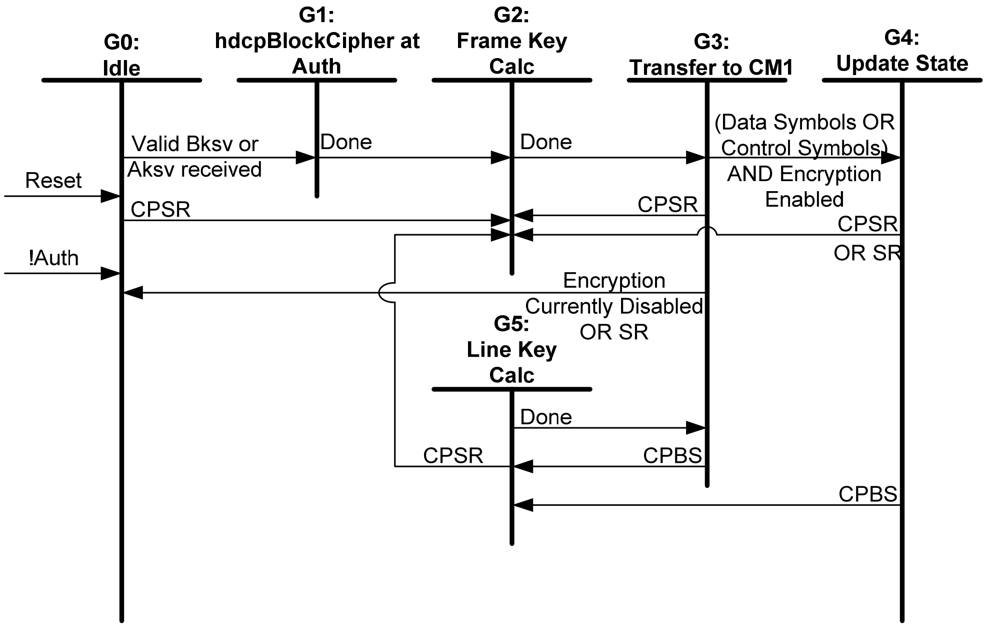

Figure 6-6. CM0 Encryption/Decryption State Diagram (DPES)

Transition Any State:G0. Reset conditions or transitions into the unauthenticated state at the HDCP Device cause the CM0 encryption state machine to transition to the idle state.

State G0:Idle. The HDCP Cipher is free running and available for use as hdcpRngCipher. Refer to Section 4.5 for an explanation of hdcpRngCipher.

Transition G0:G1. When a valid *Bksv* or *Aksv* is received by the HDCP Transmitter or HDCP Receiver it begins the hdcpBlockCipher at authentication operation. Refer to Section 4.5 for an explanation of hdcpBlockCipher operation.

State G1:hdcpBlockCipher At Authentication. The R_0 and M_0 values are computed as explained in Section 4.5 using the hdcpBlockCipher.

Transition G1:G2. Successful completion of first phase of authentication transitions the CM0 state machine into the frame key calculation state to perform the Initial Bootstrapping operation.

State G2:Frame Key Calculation. M_i is computed in this state and a frame key is calculated using hdcpBlockCipher as explained in Section 4.5. This operation is initiated at the end of hdcpBlockCipher at Authentication or on detecting a valid CPSR. It must be completed within 128-clocks starting immediately after hdcpBlockCipher at Authentication or after transmission/reception of CPSR symbol.

Transition G2:G3. The frame key is calculated within 128 clocks. At the end of the 128 clock period, contents are transferred from BM0 to BM1.

State G3:Transfer to CM1. In this state register contents are transferred from BM0 to BM1.

Transition G3:G5. Detection of a valid CPBS causes line key calculation using hdcpRekeyCipher as explained in Section 4.5.

Transition G3:G2. Detection of a valid CPSR causes frame key calculation using hdcpBlockCipher as explained in Section 4.5.

Transition G3:G0. After transfer to CM1, if encryption is currently disabled or SR is detected, the state machine to transitions to the idle state.

Transition G3:G4. Detection of valid data symbols or control symbols when encryption is enabled causes this transition.

State G4:Update State. In this state, hdcpStreamCipher operation is implemented in CM0. LM0 and BM0 are clocked with the re-key enable signal de-asserted thus causing their register states to change for every clock. The 32-bit output from the output function OF0 is not used.

Transition G4:G2. Detection of a valid CPSR or SR causes frame key calculation using hdcpBlockCipher as explained in Section 4.5. Frame key calculation is performed on detection of an SR to prepare the register states in BM1 so that encryption may be applied seamlessly on detection of a CPSR. This is referred to as the Encryption Disable Bootstrapping operation (see Figure 6-5). This operation is implemented by HDCP Receivers as soon as encryption is disabled after detection of SR. This operation may be implemented by HDCP Transmitters as soon as encryption is disabled and the link is still active and authenticated. If the link is unauthenticated, the CM0 state machine in HDCP Transmitters transition into the Idle state.

Transition G4:G5. Detection of a valid CPBS causes line key calculation using hdcpRekeyCipher as explained in Section 4.5.

State G5:Line Key Calculation. A line key is calculated using hdcpRekeyCipher as explained in Section 4.5. This operation is initiated on detecting a valid CPBS symbol. It must be completed within 64-clocks starting immediately after transmission/reception of the CPBS symbol.

Transition G5:G3. The line key is calculated within 64 clocks. At the end of the 64 clock period, contents are transferred from BM0 to BM1.

Transition G5:G2. Detection of a valid CPSR causes frame key calculation using hdcpBlockCipher as explained in Section 4.5.

Transition G0:G2. Detection of a valid CPSR causes frame key calculation using hdcpBlockCipher as explained in Section 4.5. This transition occurs when encryption is re-enabled after it has been temporarily disabled and the Encryption Disable Bootstrapping operation has been implemented.

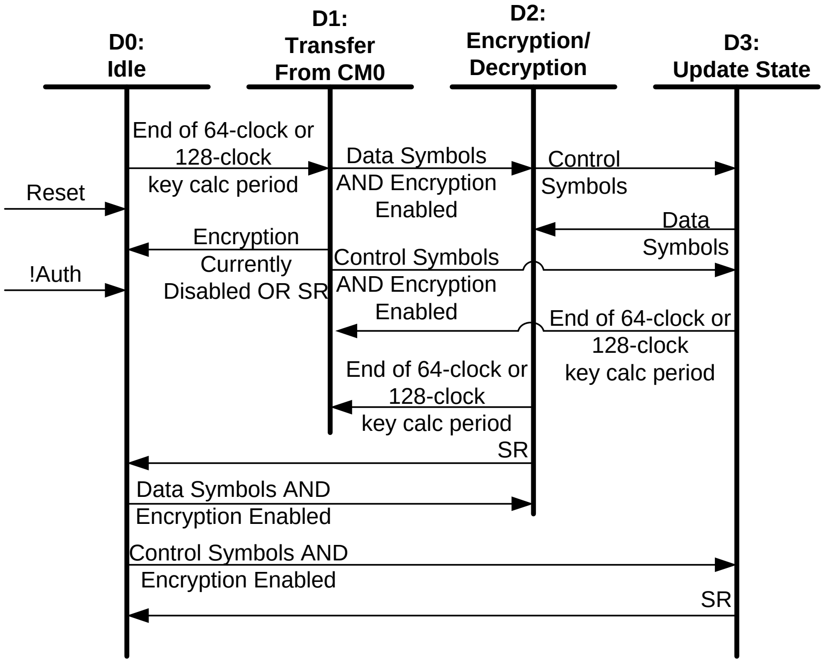
D0:
Idle
D1:
Transfer
From CM0
D2:
Encryption/
Decryption
D3:
Update State
End of 64-clock or 128-clock key calc period
Data Symbols AND Encryption Enabled
Control Symbols
Reset
Data Symbols
Encryption Currently Disabled OR SR
Control Symbols AND Encryption Enabled
!Auth
End of 64-clock or 128-clock key calc period
End of 64-clock or 128-clock key calc period
SR
Data Symbols AND Encryption Enabled
Control Symbols AND Encryption Enabled
SR

Figure 6-7. CM1 Encryption/Decryption State Diagram (DPES)

Transition Any State:D0. Reset conditions or transitions into the unauthenticated state at the HDCP Device cause the CM1 encryption state machine to transition to the idle state.

Transition D0:D1. End of the 128-clock frame key calculation period or the 64-clock line key calculation period in CM0 causes the transfer of block module register contents from CM0 to CM1.

State D1:Transfer From CM0. Contents are transferred from BM0 to BM1.

Transition D1:D0. When encryption is currently disabled or SR is detected, the CM1 encryption state machine transitions to the idle state.

Transition D1:D2. Detection of valid data symbols when encryption is enabled initiates encryption / decryption.

State D2:Encryption/Decryption. In this state, the data symbols are encrypted/decrypted using hdcpStreamCipher operation which is explained in Section 4.5.

Transition D2:D3. Detection of control symbols causes this transition.

State D3:Update State. Transition to this state happens on detection of valid control symbols. In this state CM1 performs hdcpStreamCipher computations; BM1 is clocked thus causing its register states to change. Control symbols are not encrypted and therefore HDCP Encryption is not applied in this state.

Transition D3:D2. Detection of data symbols causes this transition. hdcpStreamCipher operation is implemented in CM1 and the output data from OF1 is used for HDCP Encryption of any data symbols only.

Transition D1:D3. Detection of control symbols when encryption is enabled causes this transition.

Transition D3:D1. End of the 128-clock frame key calculation period or 64-clock line key calculation period in CM0 causes the transfer of block module register contents from CM0 to CM1.

Transition D2:D1. End of the 128-clock frame key calculation period or 64-clock line key calculation period in CM0 causes the transfer of block module register contents from CM0 to CM1.

Transition D0:D2. Detection of data symbols when encryption is enabled causes this transition. This transition occurs when encryption is re-enabled after it has been temporarily disabled and the Encryption Disable Bootstrapping operation has been implemented. The BM1 register states have been prepared as a result of the Encryption Disable Bootstrapping operation and encryption may be applied seamlessly when it is re-enabled.

Transition D0:D3. Detection of control symbols when encryption is enabled causes this transition. This transition occurs when encryption is re-enabled after it has been temporarily disabled and the Encryption Disable Bootstrapping operation has been implemented.

Transition D2:D0. When SR is detected, the CM1 encryption state machine transitions to the idle state.

Transition D3:D0. When SR is detected, the CM1 encryption state machine transitions to the idle state.

7 Renewability

It is contemplated that an authorized participant in the authentication protocol may become compromised so as to expose the Device Private Keys it possesses for misuse by unauthorized parties. In consideration of this, each HDCP Receiver is issued a unique set of Device Private Keys, matched with a non-secret identifier (the KSV), referred to collectively as the Device Key Set. Through a process defined in the HDCP Adopter's License, the Digital Content Protection LLC may determine that a set of Device Private Keys has been compromised. If so, it places the corresponding KSV on a revocation list that the HDCP Transmitter checks during authentication. Other authorized HDCP Receivers are not affected by this revocation because they have different sets of Device Private keys.

The HDCP Transmitter is required to manage system renewability messages (SRMs) carrying the KSV revocation list. The validity of an SRM is established by verifying the integrity of its signature with the Digital Content Protection LLC public key, which is specified by the Digital Content Protection LLC.

The SRMs are delivered with content and must be checked when available. The KSVs must immediately be checked against the SRM when a new version of the SRM is received. Additionally, devices compliant with HDCP 1.2 and higher must be capable of storing at least 5kB of the SRM in their non-volatile memory. The process by which a device compliant with HDCP 1.2 or higher updates the SRM stored in its non-volatile storage when presented with a newer SRM version is explained in Section 7.2.

7.1 SRM Size and Scalability

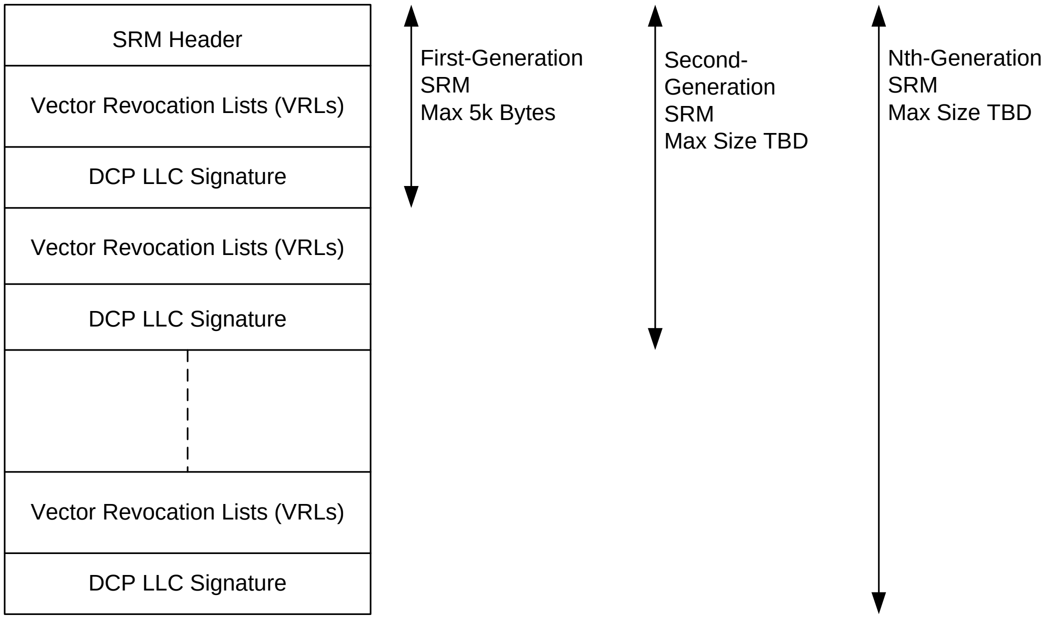
SRM Header
Vector Revocation Lists (VRLs)
DCP LLC Signature
Vector Revocation Lists (VRLs)
DCP LLC Signature
Vector Revocation Lists (VRLs)
DCP LLC Signature
First-Generation SRM Max 5k Bytes
Second-Generation SRM Max Size TBD
Nth-Generation SRM Max Size TBD

Figure 7-1. SRM Generational Format

As illustrated in Figure 7-1 , the size of the First-Generation HDCP SRM will be limited to a maximum of 5kB. The actual size of the First-Generation SRM is 5116 bytes. For scalability of the SRM, the SRM format supports next-generation extensions. By supporting generations of SRMs, an HDCP SRM can, if required in future, grow beyond the 5kB limit to accommodate more KSVs. Next-generation extensions are appended to the current-generation SRM in order to ensure backward compatibility with devices that support only previous-generation SRMs.

Table 7-1 gives the format of the HDCP SRM. All values are stored in big endian format.

Name	Size (bits)	Function
SRM ID	4	A value of 0x8 signifies that the message is for HDCP. All other values are reserved
Reserved	12	Reserved for future definition. Must be 0x000
SRM Version	16	Sequentially increasing unique SRM numbers. Higher numbered SRMs are more recent
SRM Generation Number	8	Indicates the generation of the SRM. The generation number starts at 1 and increases sequentially
VRL Length	24	Specifies the combined length of all vector revocation lists contained in this SRM. The length is in bytes and includes the three bytes of this field, the combined size of the vector revocation lists (only those contained in the first-generation SRM), and the 40 bytes of the Digital Content Protection LLC signature in the first-generation SRM
VRLs	Variable. Max 40544 (5068 bytes)	One or more VRLs, each in the format specified in the HDCP VRL format table below
DCP LLC Signature	320	A cryptographic signature of the SRM as defined by the Digital Signature Algorithm (DSA), as described in FIPS Publication 186-1 dated December 15, 1998. The first 160 bits is the big endian representation of the "r" value of the signature and the trailing 160 bits is the big endian representation of the "s" value produced by DSA

Table 7-1. System Renewability Message Format

The SRM contains the vector revocation list, variable-length list of KSVs that belong to compromised devices. The format of the revocation list is specified in Table 7-2.

Name	Size (bits)	Function
Reserved	1	Set to 0.
Number of Devices	7	Specifies the number KSVs N in this list.
Device KSVs	40 * N	Forty-bit KSVs follow the type/number byte. The first byte following the type byte is the most significant byte of the first KSV in the list.

Table 7-2. Vector Revocation List Format

Each subsequent next-generation extensions to the first-generation SRM will have the following fields.

Name	Size (bits)	Function
VRL Length	16	Specifies the combined length in bytes of all VRLs in this generation extension, the 2 bytes of this field and the 40 bytes of the DCP LLC signature
VRLs	Variable	One or more VRLs, each in the format specified in the HDCP VRL format table below
DCP LLC Signature	320	A cryptographic signature of the SRM as defined by the Digital Signature Algorithm (DSA), as described in FIPS Publication 186-1 dated December 15, 1998. The first 160 bits is the big endian representation of the "r" value of the signature and the trailing 160 bits is the big endian representation of the "s" value produced by DSA. The signature field is calculated over all preceding fields of the SRM

Table 7-3. Next-generation extension format

Table 7-4 gives the cryptographic parameters used to verify the digital signature of the SRM.

Parameter	Value (hexadecimal)
Prime Modulus	d3c3f5b2fd1761b7018d75f79343786b17395b355a52c7b8a1a24fc36a7058ff8e7fa164f5 00e0dca0d284821d969e4b4f34dc0cae7c7667b844c747d4c6b983e52ba70e5447cf35f40 4a0bcd1974c3a10715509b3721530a73f3207b99820495c7b9c143275733b028a49fd968 919542a39951c46edc2118c59802bf3287527
Prime Divisor	ee8af2ce5e6db56acd6d14e297ef3f4df9c708e7
Generator	92f85d1b6a4d52131ae43e2445de1ab502afdeaca9bed7315d56d766cd2786118f5db14ab deca9d25162977da83effa88eedc6bfeb37e1a90e29cd0ca03d799e92dd2945f778585ff7c8 35642c21ba7fb1a0b6be81c8a5e3c8ab69b21da54242c98e9b8aab4a9dc251fa7dac29216f e8b93f185b2f67405b69462442c2ba0bd9
Public Key	c70600526ba0b0863a80fbe0a3acff0d4f0d76658a1754a8e7654755f15ba78d56950e4865 4f0bbde16804de1b541874db22e14f031704db8d5cb2a417c4566c27ba973c43d84e0da2 a70856fe9ea48d87259038b16553e662435ff7fd5206e27bb7ffbd886c241095c8dc8d66f6 62cbd88f9df7e9b3fb8362a9f7fa36e53799

Table 7-4. Cryptographic Parameters for Verifying SRM

7.2 Updating SRMs

The stored HDCP SRM must be updated when a newer version of the SRM is delivered with the content. The procedure for updating an SRM is as follows:

1. Verify that the version number of the new SRM is greater than the version number of the SRM currently stored in the device's non-volatile storage

2. If the version number of the new SRM is greater (implying that it is a more recent version), verify the signature on the new SRM

On successful signature verification, replace the current SRM in the device's non-volatile storage with the new SRM. If, for instance, the device supports only second-generation SRMs and the new SRM is a third-generation SRM, the device is not required to store the third-generation extension.

Devices compliant with HDCP 1.2 or higher must be capable of storing at least 5kB of the SRM (First-Generation SRM).

Appendix A. Timing Diagrams in MST Mode

Figure A-1 depict the frame key calculation timing for a 2-lane configuration. Figure A-2 depict the frame key calculation timing for a 1-lane configuration.

Figure A-3 depict the 2-Lane line re-key timing diagrams. Figure A-4 depict 1-Lane line re-key timing diagrams.

Figure A-5, Figure A-6 and Figure A-7 depict the initial frame key calculation timing for 1-lane, 2-lane and 4-lane configurations respectively. In this situation both BM0 and BM1 are initially stalled after completing the initial authentication bootstrap operation.

Note: The states X_i, X_{i+1} etc in the timing diagrams indicate the BM0 and BM1 register states at the beginning of a particular cycle and are directly used to generate the corresponding encrypted output at each cycle.

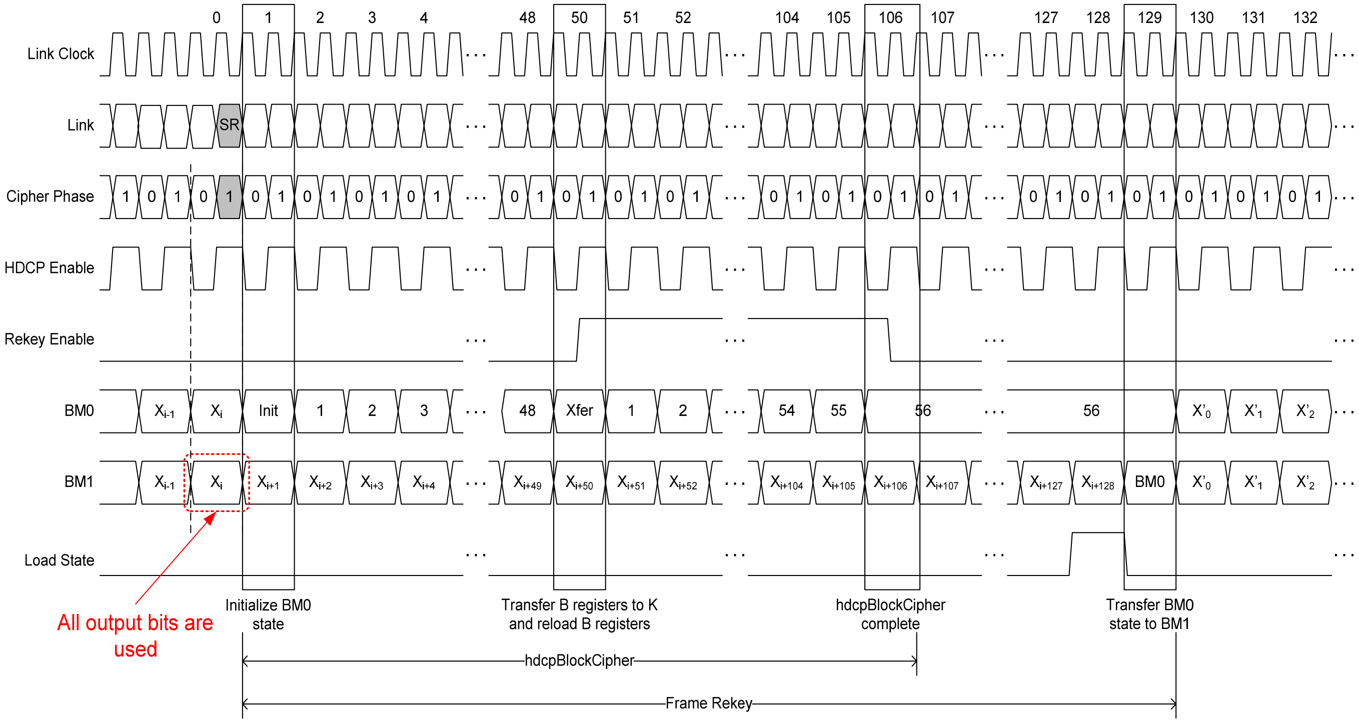

Figure A-1. 2-Lane Frame Key Calculation Timing Diagram (Phase 1)

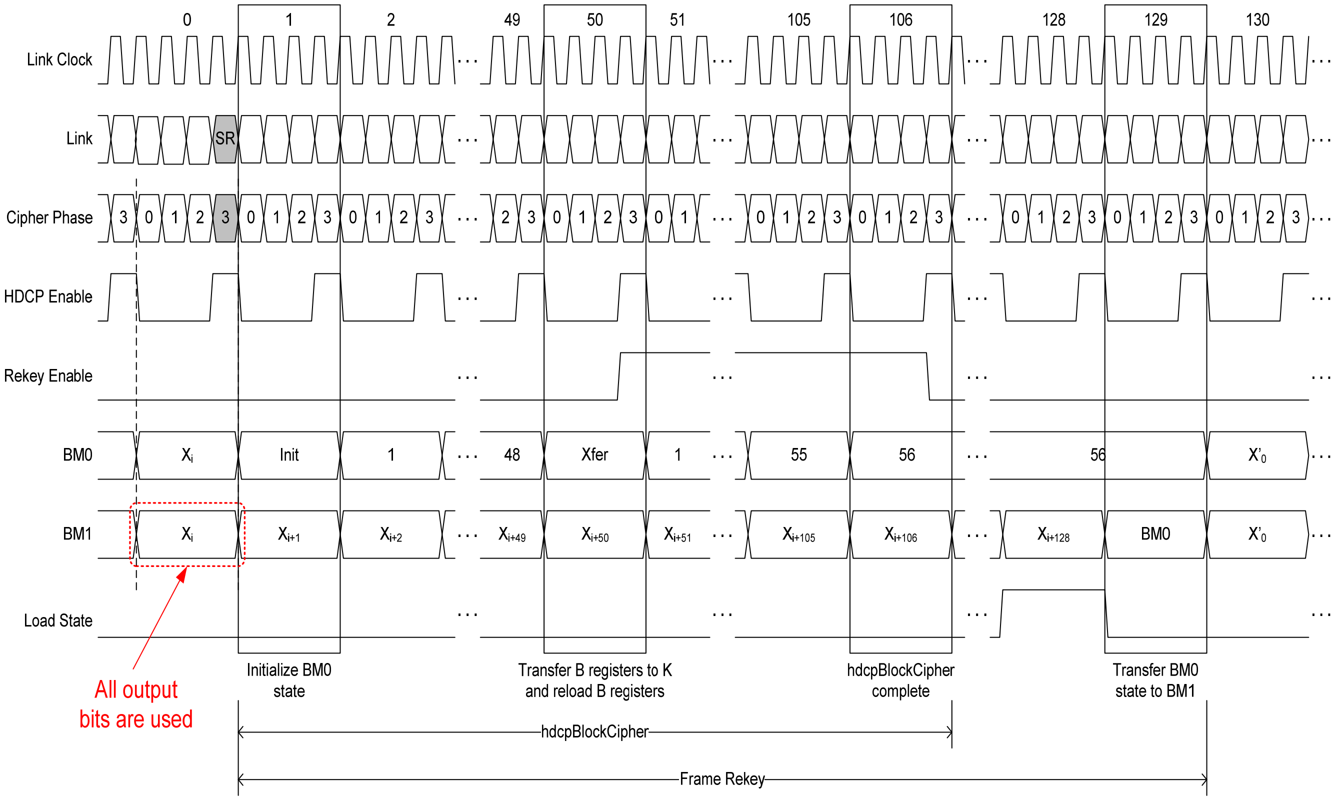

Figure A-2. 1-Lane Frame Key Calculation Timing Diagram (Phase 3)

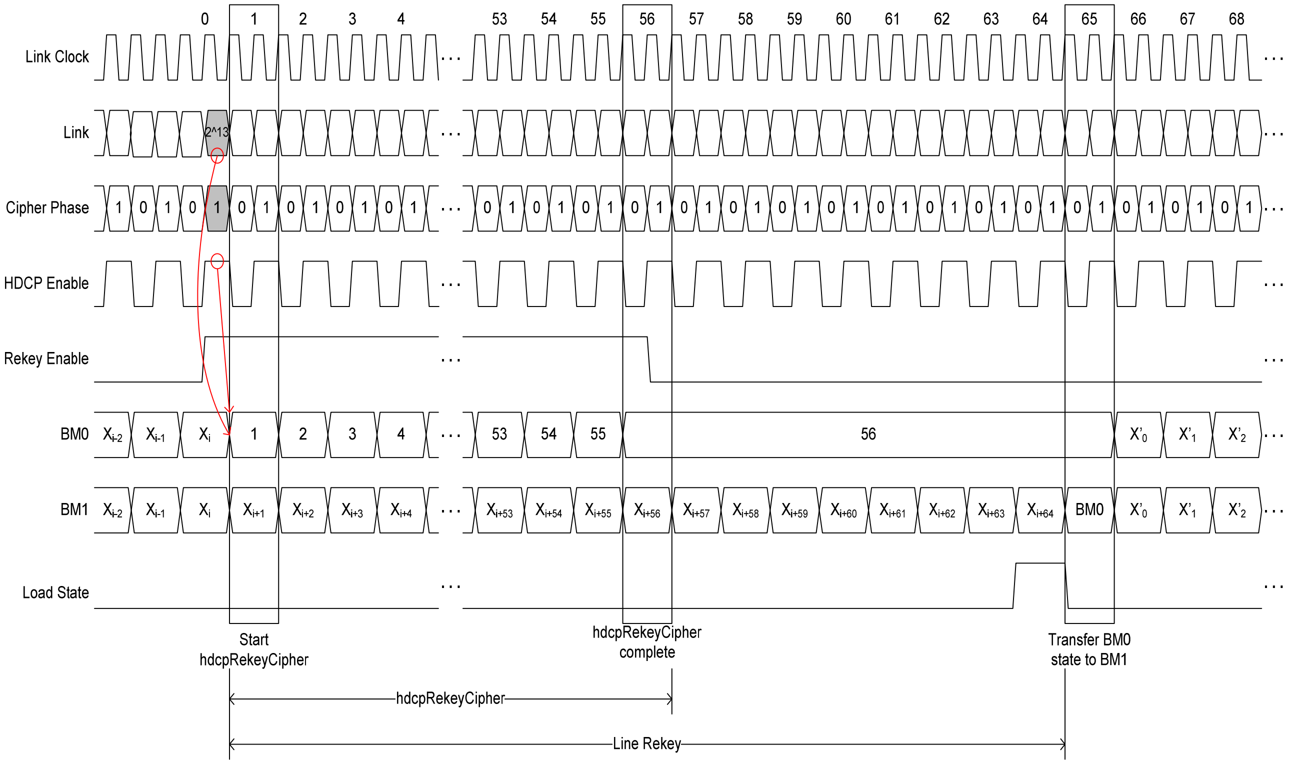

Figure A-3. 2-Lane Line Re-Key Calculation Timing Diagram (Phase 1)

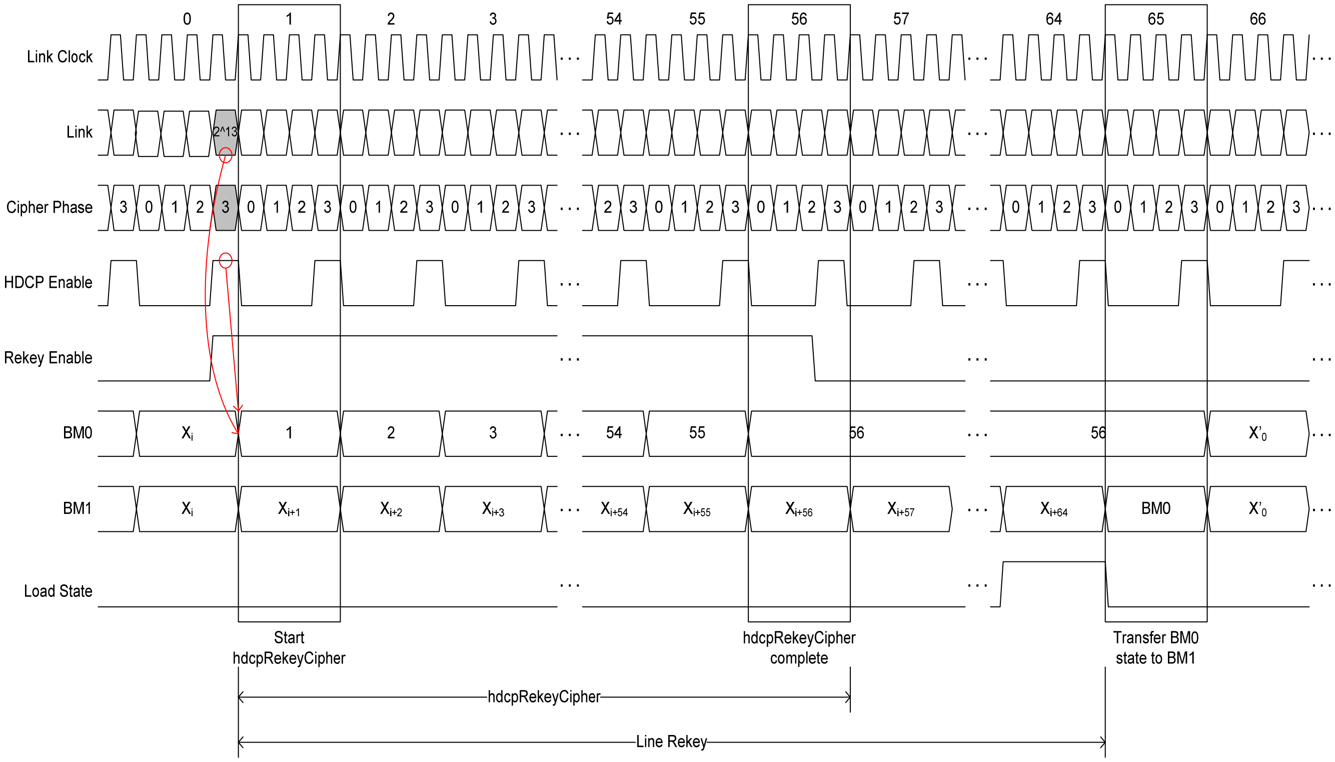

Figure A-4. 1-Lane Line Re-Key Timing Diagram (Phase 3)

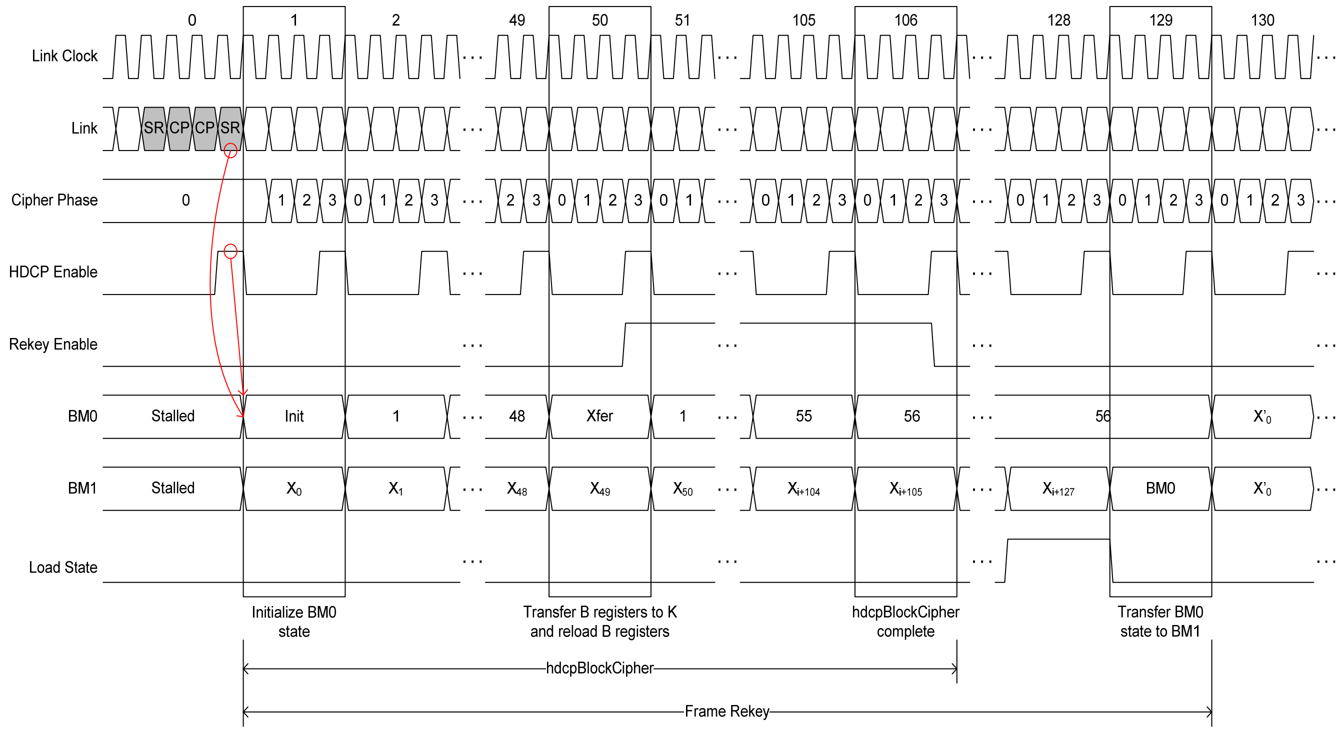

Figure A-5. 1-Lane Initial Frame Key Calculation Timing Diagram

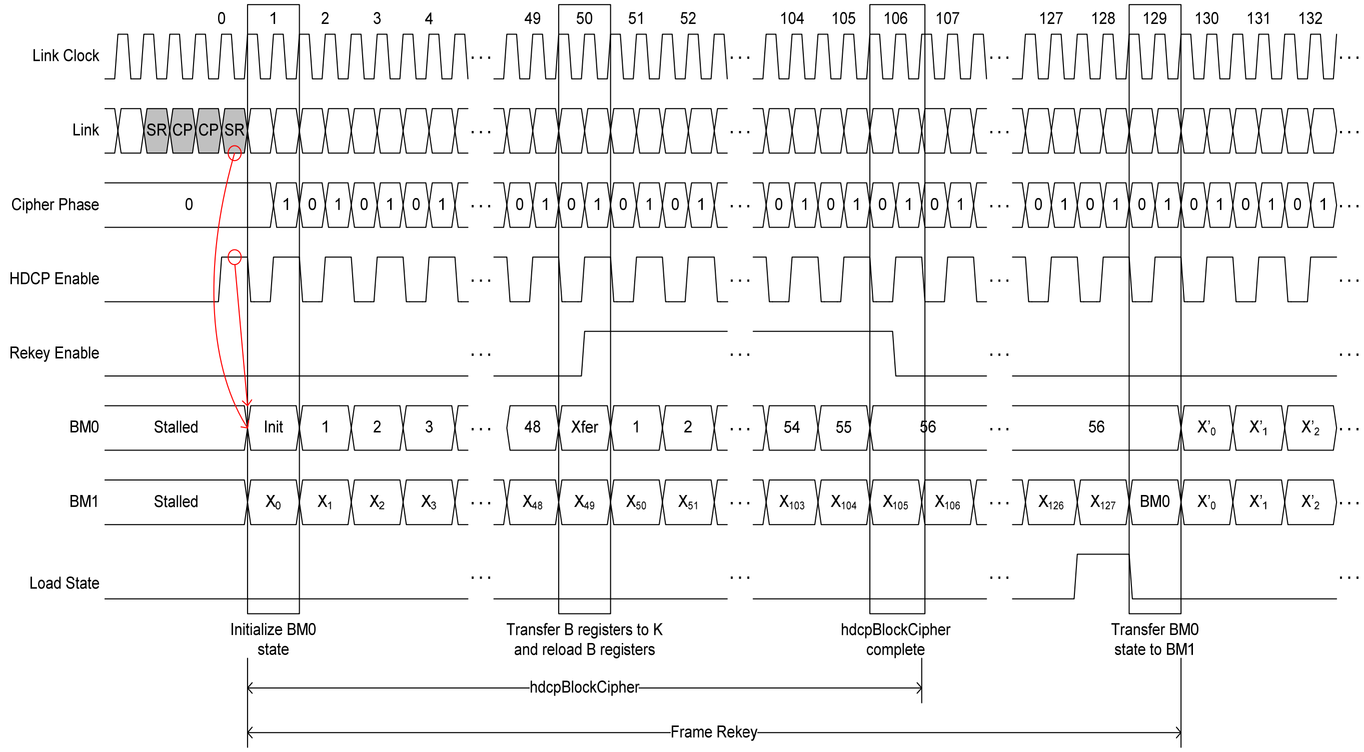

Figure A-6. 2-Lane Initial Frame Key Calculation Timing Diagram

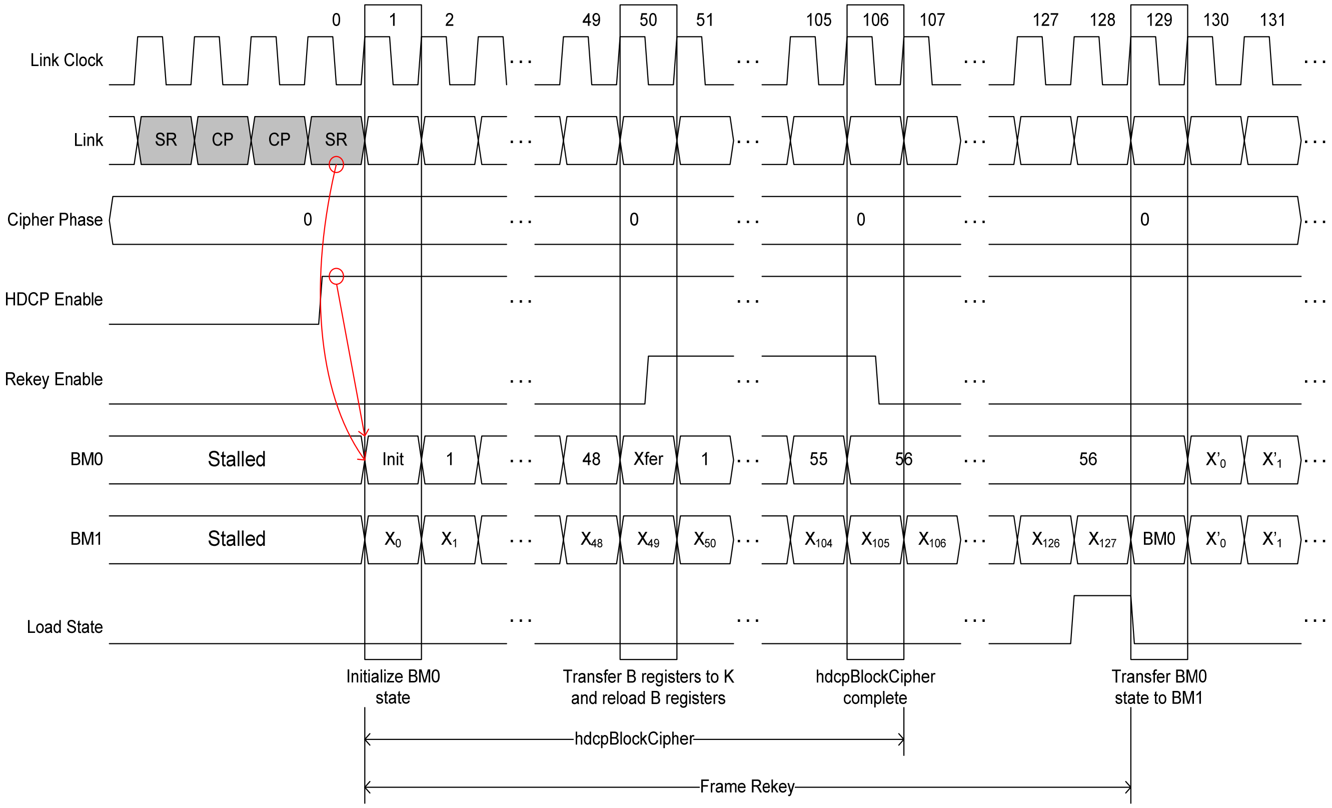

Figure A-7. 4-Lane Initial Frame Key Calculation Timing Diagram

Appendix B. Test Vectors

Table B-1 gives facsimile key information for test purposes.

	Transmitter A1	Transmitter A2	Receiver B1	Receiver B2
Key Selection Vector	b70361f714	43f72d5066	511ef21acd	e72697f401
Key 0	4da4588f131e69	9aaba1f9ef907c	bc13e0c75bf0fd	93afe1ff4ca0ed
Key 1	1f823558e65009	34a0407731d1d0	ae0d2c7f76443b	efb49d4a25a4e4
Key 2	8a6a47abb9980d	97c682992dc5d9	24bf2185a36c60	e822d8a9335346
Key 3	f3181b52cbc5ca	da80caca68ed15	f4bc6cbcd7a32f	8812c3004e23d2
Key 4	fb147f6896d8b4	1866d9b51462a6	a72e69c5eb6388	dc63ba78d94263
Key 5	e08bc978488f81	d9fc9599bb7498	7fa2d27a37d9f8	47ebdf52776fd5
Key 6	a0d064c8112c41	7a062ac883f528	32fd3529dea3d1	4bce49472e0464
Key 7	b39d5a28242044	f5938c662af454	485fc240cc9bae	0479bed7732682
Key 8	b928b2bdad566b	ec3075e82d3ef2	3b9857797d5103	c5f800fad716d5
Key 9	91a47b4a6ce4f6	536e376e7ffc49	0dd170be615250	f53fd67ba9b9ec
Key 10	5600f8205e9d58	51c83a6cbeb116	1a748be4866bb1	6fb3901e5867f2
Key 11	8c7fb706ee3fa0	79d44ae1bd5f50	f9606a7c348cca	24c46f520f1be5
Key 12	c02d8c9d7cbc28	674b2563e27393	4bbb037899eea1	2038176d369ed7
Key 13	561261e54b9f05	7a1357efc538a2	190ecf9cc095a9	9ba9cd6a077a57
Key 14	74f0de8ccac1cb	6486e57ea46b02	a821c46897447f	5f2764b35c5591
Key 15	3bb8f60efcdb6a	Bdf27a1ce8a299	1a8a0bc4298a41	ee32f1171f5356
Key 16	a02bbb16b22fd7	dc8bd1fa5b46b9	aefc0853e62082	d20a9e2f4d57fa
Key 17	482f8e46785498	27ef71efef9b73	f75d4a0c497ba4	439eb96d2daff0
Key 18	66ae2562274738	187599f603c947	ad6495fc8a06d8	1c68df6f868aaf
Key 19	3d4952a323ddf2	023ae9da303ecb	67c2020c2b2e02	dd50d7551dc6fb
Key 20	e2d231767b3a54	3d1cf6533dea8e	8f116b18f4ae8d	50b85379165c5f
Key 21	4d581aede66125	34dd5525f1890c	e3053fa3e9fa69	f45d64b097d6b5
Key 22	326082bf7b22f7	367dd774a07f4c	37d8002881c7d1	a1a154e07adb4d
Key 23	f61b463530ce6b	cdc34c8a6f56d1	c3a5fd1c15669c	0755ea83e47e71
Key 24	360409f0d7976b	de3413927363a8	9e93d41e0811f7	e1dca26293efe4
Key 25	a1e105618d49f9	21b11c739f45b3	2c4074509eec6c	e1092507ab8f45
Key 26	c98e9dd1053406	84440fadd281ac	8b7fd819279b61	3d56680db98e15
Key 27	20c36794426190	10f7900c65fef4	d7caada0a06ce9	0a49af413de66b
Key 28	964451ceac4fc3	30070704c8aa06	9297dca1f8c1db	90a814bbf971a0
Key 29	3e904504e18c8a	f287cb4063cb9d	5d1aaa99dea489	626b121ca0504f
Key 30	290010579c2dfc	97033445a4d587	60cb56ddbaa1d9	00f9bb7a94a1a7
Key 31	d7943b69e5b180	8051045091c10b	85d4ad5e5ff2e0	f485290cc5c1ba
Key 32	54c7ea5bdd7b43	d18f282074da20	1280161221df6d	baa873c54fdedf
Key 33	74fb5887c790ba	f2679a98828400	ca31a5f2406589	2d6a56233b8aba
Key 34	935cfa364e1de0	a6f0b6042a3dd7	1d30e8cb198e6f	a60d0379512312
Key 35	03075e159a11ae	3e5ddad097f5e1	d1c18bed07d3fa	942582078dadb8
Key 36	05d3408a78fb01	3ad1f8a2e5958f	cec7ec09245b43	8395a4b022082f
Key 37	0059a5d7a04db3	f025bb1c085d4f	b08129efedd583	cb12fe97842b60
Key 38	373b634a2c9e40	0864213d6d50c1	2134cf4ce286e5	282ffe78f2f95c
Key 39	2573bbb4562041	9018b0ff3ab170	edeef9d099b78c	f6491f33c7ef53

Table B-1. Sample Device Keys

Transmitter Device #1 examines the KSV of Receiver Device #1 and combines its own secret device keys that correspond to the bit positions of all of the ones in the KSV. Receiver Device #1 examines the KSV of Transmitter Device #1 and combines its own secret device keys that correspond to the bit positions of all of the ones in the KSV. Table B-2 shows the 56-bit binary addition of keys performed by Transmitter Device #1 and Receiver Device #1, and the corresponding equivalent values derived for Km and Km'.

Transmitter Device #1 Sum of Keys Calculation		**Receiver Device #1 Sum of Keys Calculation**	
Key 0	4da4588f131e69	Key 2	24bf2185a36c60
Key 2	8a6a47abb9980d	Key 4	a72e69c5eb6388
Key 3	f3181b52cbc5ca	Key 8	3b9857797d5103
Key 6	a0d064c8112c41	Key 9	0dd170be615250
Key 7	b39d5a28242044	Key 10	1a748be4866bb1
Key 9	91a47b4a6ce4f6	Key 12	4bbb037899eea1
Key 11	8c7fb706ee3fa0	Key 13	190ecf9cc095a9
Key 12	c02d8c9d7cbc28	Key 14	a821c46897447f
Key 17	482f8e46785498	Key 15	1a8a0bc4298a41
Key 20	e2d231767b3a54	Key 16	aefc0853e62082
Key 21	4d581aede66125	Key 21	e3053fa3e9fa69
Key 22	326082bf7b22f7	Key 22	37d8002881c7d1
Key 23	f61b463530ce6b	Key 24	9e93d41e0811f7
Key 25	a1e105618d49f9	Key 25	2c4074509eec6c
Key 26	c98e9dd1053406	Key 32	1280161221df6d
Key 27	20c36794426190	Key 33	ca31a5f2406589
Key 28	964451ceac4fc3	Key 34	1d30e8cb198e6f
Key 32	54c7ea5bdd7b43	Key 36	cec7ec09245b43
Key 36	05d3408a78fb01	Key 37	b08129efedd583
Key 38	373b634a2c9e40	Key 39	edeef9d099b78c
RESULT (*Km*):	**5309c7d22fcecc**	**RESULT (*Km*')**	**5309c7d22fcecc**

Table B-2. Sample Km Calculation

Sequence	LFSR 0	LFSR 1	LFSR 2	LFSR 3	SH 0	SH 1	SH 2	SH 3
Load								
1								
2								
3								
…								
47								
48								
Load	0x01e35	0x00040	0x025be	0x15429	01	01	01	01
1	0x01c6b	0x00081	0x04b7c	0x0a853	10	10	10	10
2	0x018d6	0x00102	0x096f8	0x150a7	00	01	11	01
3	0x011ac	0x00204	0x02df0	0x0a14e	00	00	11	11
4	0x00358	0x00409	0x05be0	0x1429c	00	00	10	11
5	0x006b0	0x00812	0x0b7c0	0x08539	00	00	01	10
6	0x00d60	0x01024	0x06f81	0x10a72	00	00	00	01
7	0x01ac0	0x02049	0x0df03	0x014e4	01	00	00	00
8	0x01581	0x00093	0x0be07	0x029c9	10	01	00	00
…	…	…	…	…	…	…	…	…
49	0x01cbc	0x03218	0x05712	0x0ab75	10	10	01	11
50	0x01979	0x02431	0x0ae24	0x156eb	11	00	10	11
51	0x012f3	0x00863	0x05c48	0x0add7	10	01	01	10
52	0x005e6	0x010c6	0x0b891	0x15bae	01	10	10	01
53	0x00bcc	0x0218d	0x07122	0x0b75c	10	01	01	10
54	0x01799	0x0031a	0x0e245	0x16eb8	01	00	11	00
55	0x00f32	0x00634	0x0c48b	0x0dd70	10	10	01	10
56	0x01e65	0x00c69	0x08917	0x1bae1	00	01	11	01

Table B-3. LFSR Module (LM0) States During A1 - B1 Authentication (REPEATER = 0)

Sequence	Kx	Ky	Kz	Bx	By	Bz	Output ([23:0])
Load	0x22fcecc	0x5309c7d	0x0000000	0xc070403	0x271c130	0x0000034	
1	0x000084c	0xf458fff	0x7f722dc	0xa5d4b70	0x8ea8888	0x9f6066d	0xbe70ee
2	0x0ed9f8a	0xb444236	0x3b62e76	0x8fa5383	0x5d17cd7	0x2e71e83	0x007023
3	0x70ef0ef	0x9aa103f	0x8aa659d	0x49d0347	0xe71b545	0xd39af92	0xdd51b7
4	0xc8f3da5	0x8bbb85f	0x58047e6	0x05add47	0xaf2ff95	0x4371447	0xeae10f
5	0x6b68710	0x1826042	0xc20a675	0x5693206	0xd034757	0x71f4c59	0xe0e624
6	0xd4c9cf4	0x0014506	0x6c11733	0xf679cf3	0xbe06351	0x412aafc	0x6104f9
7	0x2ff2231	0x059031a	0xd84c367	0x7c6878b	0x735a2d2	0x2d4fba7	0x12c5e4
8	0x1c13406	0x516f805	0x3e231f5	0x61f3f4d	0xccb03b9	0x3030a78	0x9f08dc
…	…	…	…	…	…	…	…
41	0x7dc29a3	0x5895932	0x26047a5	0x12b9cbd	0xe40581a	0xc892f27	0x1cfd71
42	0xba7d2b0	0xf1cfeac	0x36eb45d	0xa8bab0f	0x083213e	0x38fd0ef	0xb90f28
43	0xdd26650	0x29e8ca4	0xbf0109c	0x04a0c9b	0xf8cd136	0xb6b8827	0xf32344
44	0xf928c5b	0xc70cecd	0xcc71bb9	0x004c69f	0xf8cfb57	0x20d8664	0xff2c26
45	0x491d801	0xf630446	0x43655f6	0x26727b8	0xb6866b1	0x48253f0	0xead81d
46	0x9281463	0x891c25b	0x2c40a10	0xe2e3627	0xce25f1d	0x6fd76d2	0x7cb35d
47	0x37ef335	0xbb8429b	0xfad91c5	0x8bb8770	0x94322d6	0xbc24e18	0x4ac7aa
48	0x7bd96ba	0xee950f7	0x749f3d9	0xc040e35	0x54294b7	0x1c61d8e	0x37d937
Load	0xc040e35	0x54294b7	0x1c61d8e	0xc070403	0x271c130	0x0000034	
1	0x3772e0b	0x6595cd5	0x93d46aa	0xf5f1bea	0x8ea8888	0x9f6066d	0x5d74aa
2	0xfcdc369	0x18f685a	0x22626f1	0x48ec1f7	0x5d17cd7	0x083878b	0x1e60bc
3	0x67f044d	0xd5eb45a	0x8ca9144	0x034b338	0x3ac66a8	0xdc9e6f6	0x4c29b4
4	0x046af2c	0x992df09	0xd7b21a9	0x845e47f	0xce06983	0xc50059e	0x1c3d69
5	0x1a7c13c	0x6aed6fb	0x57ba318	0xea50517	0xc09dcdf	0xcdbf157	0x2d0855
6	0x82ff268	0xfd00a63	0xf4c6f06	0x00bc25d	0xb24cd67	0xa94407a	0xddb851
7	0xe602372	0xe4f1798	0x6487e18	0x47a81d0	0x3ca6b73	0x90eea67	0x5605dd
8	0xa251408	0x26ca144	0x2c8a821	0x700ece4	0x1f2ccf5	0x575dec4	0x44236d
…	…	…	…	…	…	…	…
49	0xade5581	0x026eead	0x58676ad	0x19978d8	0x207678c	0x552b693	0x65e697
50	0xc1cdfad	0x29eb9e5	0x85864c6	0x3a260ed	0xd817a5a	0xf2e4743	0xa341ef
51	0x75114c3	0x6923621	0xc5367fa	0x4c7b24b	0x4c7ad96	0x4bf179e	0x6c2f44
52	0x5e00de1	0x31ba2ec	0x9352a05	0x21f7177	0x1ce1a8a	0x5fe9127	0xdce5b0
53	0xa8a8b05	0x470ad68	0x35c28f6	0x3eaf43f	0x194bf81	0xb8d5477	0x14a02b
54	0x56a5801	0x5bd1d70	0xd724992	0xf41fb7d	0x6aafc2c	0x3fbf3ef	0x54c815
55	0x6c30c38	0xf15bf0e	0xfc5799d	0xb673b37	0x921be44	0x956fe75	0x8ae73d
56	0x8451307	0x58cff28	0x9ee2338	0x346ebe6	0x189def7	0xf04cb0e	0xe0001c

Table B-4. Block Module (BM0) States During A1 - B1 Authentication (REPEATER = 0)

Note that the 8 MSBs (i.e., [31:24]) of OF0's output are never used and hence are not provided in this table and subsequent tables that provide BM0 states during authentication.

Sequence	LFSR 0	LFSR 1	LFSR 2	LFSR 3	SH 0	SH 1	SH 2	SH 3
Load								
1								
2								
3								
…								
47								
48								
Load	0x018b1	0x03d0e	0x06ca0	0x14e60	01	01	01	01
1	0x01162	0x03a1d	0x0d941	0x09cc1	00	10	11	00
2	0x002c4	0x0343b	0x0b282	0x13983	01	00	11	10
3	0x00588	0x02876	0x06504	0x07307	10	01	01	11
4	0x00b10	0x010ed	0x0ca09	0x0e60f	01	10	10	10
5	0x01620	0x021db	0x09413	0x1cc1e	10	00	11	00
6	0x00c40	0x003b7	0x02826	0x1983c	01	10	10	10
7	0x01881	0x0076e	0x0504d	0x13078	11	01	00	11
8	0x01103	0x00edd	0x0a09a	0x060f0	11	10	01	10
…	…	…	…	…	…	…	…	…
49	0x005c3	0x016e4	0x0917e	0x1efbd	01	00	00	01
50	0x00b86	0x02dc8	0x022fd	0x1df7a	00	01	00	00
51	0x0170d	0x01b90	0x045fb	0x1bef4	00	00	10	00
52	0x00e1b	0x03721	0x08bf6	0x17de9	00	00	00	10
53	0x01c36	0x02e42	0x017ed	0x0fbd3	01	00	00	01
54	0x0186d	0x01c84	0x02fda	0x1f7a6	11	00	00	00
55	0x010db	0x03909	0x05fb4	0x1ef4d	10	01	00	00
56	0x001b6	0x03212	0x0bf68	0x1de9b	01	00	10	00

Table B-5. LFSR Module (LM0) States During A1 – B2 Authentication (REPEATER = 0)

Sequence	Kx	Ky	Kz	Bx	By	Bz	Output ([23:0])
Load	0x089c923	0xf6aee46	0x0000000	0xad10fe5	0x5e62a53	0x0000044	
1	0x000ace8	0x2bbe222	0xa84ba32	0xf8ee8f0	0x4c79444	0x649180e	0xb24463
2	0xbe2db4d	0xced43e8	0x6cf4c5d	0xb0bccb3	0xcd48ee4	0xfbde86b	0x0ff14d
3	0x59aaa16	0x420acae	0x948ddf1	0x4f31d66	0x5e99939	0x8945bd4	0x5a7c22
4	0x6716e27	0xc71eabf	0x728216a	0x948e7ab	0xb5980ca	0x3969dfa	0xe29870
5	0x2b8be74	0xc7b7cd8	0x1896efd	0xdd99072	0xdd8b36e	0x9005894	0x252d85
6	0x417f923	0xf719e90	0xd5c1459	0xdc0bba0	0x6178407	0x066cb0a	0x5195fa
7	0x6c1faa9	0xf7175fd	0x50bb276	0xcafbc7c	0x32a2ec3	0xa479ab9	0xced7d1
8	0x90a1447	0xad4dd26	0x59afdb6	0xfa48546	0x6ebb9cf	0x890acc2	0xd92360
…	…	…	…	…	…	…	…
41	0x456a8de	0x218a73d	0xefe8143	0xdb40d6f	0x8adb81b	0x7f17e90	0x4b21a1
42	0x5bb75c0	0x9e32509	0xcd4d66f	0x94b2edc	0x91aaaf6	0x3894216	0x537e81
43	0x692b31d	0x40c7b06	0xeb692c8	0x5b4a26a	0x7c0b63f	0xb5e23ed	0x71f997
44	0x4ac7e44	0x584dad4	0x2606dca	0xb41c724	0xde66448	0x90f07c0	0x9b4c0f
45	0x995c381	0xe782e99	0x500545a	0x296761d	0x33b5aa8	0xd7c96dd	0xcce274
46	0x2a39ef6	0xb3509f9	0xbd26dfe	0xf7d1275	0xd7972de	0xa1c5513	0xa9e21a
47	0xe937d30	0x7910780	0x03575d7	0x0e9e5a9	0x235c870	0x246431c	0x8d7b49
48	0xb9af224	0x04c8a5f	0x49c96b1	0x1d0e8b1	0x4e60d94	0x072bad0	0x1cfb41
Load	0x1d0e8b1	0x4e60d94	0x072bad0	0xad10fe5	0x5e62a53	0x0000044	
1	0x8adc6e8	0xb659c1e	0x70ae5ce	0x4c36286	0x4c79444	0x649180e	0xfeaeeb
2	0xe647934	0x7ec73a0	0xae21cfc	0x57c3737	0xcd48ee4	0x131ec75	0xe6e976
3	0xfa28037	0x602e4c5	0xcc87a66	0x1fe7698	0xf433b91	0x990c71a	0x47ee81
4	0x0d609b0	0x76b0413	0xbb909ab	0xc160202	0x2e4b770	0xd5b0319	0x09463e
5	0x8f2b473	0x00b1039	0x54e4007	0xf914da7	0xbd17a23	0x9746424	0x341d4a
6	0x91fb8aa	0x6445ea6	0x8649c97	0x623f7e9	0xf5e67b9	0xb986c8a	0x61be45
7	0x88d8719	0x4f9ea67	0x5195717	0x2f6bf08	0x42af423	0x0f517b2	0x38c278
8	0x4e72913	0x5e4a60f	0xef64d8e	0xa7afa70	0x46d5f5f	0x8599680	0x366d9f
…	…	…	…	…	…	…	…
49	0x4dda715	0x5cf4582	0x66dc877	0x4e69fc3	0x6790add	0x692ce89	0x40f21c
50	0x4db2b7f	0xfb2f397	0x76dedec	0x20ef253	0x81e7d6b	0xf0b76f9	0x9c8062
51	0x6f8bf8a	0x0579c7f	0xa79d4cc	0xf23684b	0x79e04b8	0x71c4515	0xef455b
52	0x57b4273	0x7cc013c	0x4a37fd9	0xa63e183	0x13f3943	0xaf26eed	0x9b00a8
53	0x6a718ef	0x43667bb	0x91c7a99	0x9383356	0x3f262d4	0xda416b4	0xbee7d2
54	0x5764f30	0xca377a9	0x61cb7fc	0x75526c2	0x5439e56	0xc8e2a8a	0x168b9b
55	0x1aac873	0xf9340e8	0x0ce402a	0x8504037	0x18ad8b4	0xb818ef9	0xfb2f46
56	0x365eb8d	0x02468c0	0x31071ef	0x01c71f2	0xc7ac9e7	0xc1ffc01	0x65c49d

Table B-6. Block Module (BM0) States During A1 – B2 Authentication (REPEATER = 0)

Sequence	LFSR 0	LFSR 1	LFSR 2	LFSR 3	SH 0	SH 1	SH 2	SH 3
Load								
1								
2								
3								
…								
47								
48								
Load	0x0192e	0x01df7	0x077b8	0x02c9b	01	01	01	01
1	0x0125c	0x03bef	0x0ef71	0x05936	11	00	10	10
2	0x004b8	0x037df	0x0dee3	0x0b26c	11	10	01	01
3	0x00970	0x02fbf	0x0bdc7	0x164d8	01	11	00	11
4	0x012e0	0x01f7f	0x07b8e	0x0c9b0	11	01	01	10
5	0x005c1	0x03eff	0x0f71d	0x19360	01	10	10	11
6	0x00b82	0x03dfe	0x0ee3b	0x126c1	00	01	11	10
7	0x01705	0x03bfd	0x0dc76	0x04d82	00	00	11	01
8	0x00e0b	0x037fb	0x0b8ed	0x09b04	00	00	10	10
…	…	…	…	…	…	…	…	…
49	0x016ef	0x004ea	0x08ffb	0x18374	01	11	11	10
50	0x00dde	0x009d4	0x01ff7	0x106e8	10	11	11	01
51	0x01bbd	0x013a9	0x03fee	0x00dd0	01	01	11	11
52	0x0177b	0x02753	0x07fdd	0x01ba0	00	10	11	11
53	0x00ef6	0x00ea6	0x0ffbb	0x03740	01	01	01	11
54	0x01dec	0x01d4d	0x0ff77	0x06e81	10	11	00	11
55	0x01bd9	0x03a9b	0x0feef	0x0dd02	01	01	10	01
56	0x017b3	0x03537	0x0fddf	0x1ba04	10	11	01	00

Table B-7. LFSR Module (LM0) States During A2 – B1 Authentication (REPEATER = 0)

Sequence	Kx	Ky	Kz	Bx	By	Bz	Output ([23:0])
Load	0xbec1205	0x4afe34d	0x0000000	0x1c66e07	0xbec2bb0	0x0000083	
1	0x888e2ea	0x414b444	0x97a0589	0xf087578	0x3d5b332	0x610f071	0x001a91
2	0x4625e41	0xcd48c5f	0x3a77722	0x17b01a9	0x0638644	0xb71a3c5	0x892758
3	0xc9402d8	0x5ce2e8b	0x2d46dd1	0xcba2da3	0x45c8159	0x0c27e9f	0xd3c6e1
4	0x9f4f7b0	0x4c9fc33	0x7975e63	0xb1a5c1f	0x37140d4	0x78f6cfb	0x916ff8
5	0xa52c6b9	0x0ab1bea	0x3f59b80	0x66c7c4e	0xef8a601	0xd5f6819	0x21475c
6	0xe828e8c	0x1f4fe28	0xf9ae9ca	0xa6e1944	0x11989fd	0x4338020	0x729008
7	0x3d9656f	0x9313d6c	0xd525839	0x3d3cf97	0x2d456aa	0x5592482	0x2c2762
8	0x0b5904f	0xe168c0e	0x8549a6c	0x8e384cb	0xfd25ff0	0x40578b4	0xa66b25
…	…	…	…	…	…	…	…
41	0xf907779	0x8add56d	0xa2bf28b	0xb6d2591	0x8cbe163	0x1db3ce9	0x55f6f1
42	0xbb149e8	0x34b44fe	0xe899a28	0x7ec27a0	0xbdae914	0xbcc46bf	0xb1c490
43	0x852bc22	0x30c541b	0x4ba8ad0	0xbacaa81	0xf2df6bc	0x7796efa	0x134543
44	0xe0dcc66	0x3380692	0x2f59c16	0x5875f9a	0x03ea16f	0x80bc2ab	0xf8b3c8
45	0xbd69a67	0x11e9f3b	0xb0d15db	0xcd318e7	0xbcace72	0x5aa586f	0x49d410
46	0x992aba4	0x79ccd6c	0x374d0da	0x4a507c8	0xd761f3d	0x3849c30	0x4d30b7
47	0x02d7a9c	0x69e0827	0x75c491b	0x1c3734c	0x1ebaf33	0x8e6e1e4	0x9df48b
48	0x28d5897	0x4f55c34	0x1bf2686	0x1df792e	0x2c9bef7	0x07b1c9f	0xebdeef
Load	0x1df792e	0x2c9bef7	0x07b1c9f	0x1c66e07	0xbec2bb0	0x0000083	
1	0xfd88a6c	0x1aec3ba	0x548b6d5	0xfb705c6	0x3d5b332	0x610f071	0x636064
2	0x0876369	0x710f070	0x03a9952	0x68afa97	0x0638644	0x2a048b2	0x3a375c
3	0xfdcf763	0x64400d6	0x6888c5c	0x81f7bc9	0xab26acb	0x5146df0	0x1b8dbf
4	0x0cb1f80	0x6710244	0xd810320	0x8a558ef	0xc4934bb	0xfcbe390	0x2fba5d
5	0x7a77bb1	0x545b44d	0xacc6c17	0xefc1031	0x8a7bd55	0x6f02498	0x66bde4
6	0x629697d	0xdc585bb	0x5b8f82d	0x9e3cd09	0xe34bee9	0xad76510	0x9b04a5
7	0x2d0fd29	0x6095002	0x10fd4d1	0x161afae	0x9356147	0xf76daf9	0x9467c6
8	0x7745ff4	0xddcd316	0x042bd5c	0x9cc0fc2	0x7262896	0x73c7ad4	0xa7a735
…	…	…	…	…	…	…	…
49	0x3e266d1	0xc895108	0x65cffa5	0xbbf95cd	0x063edad	0x9f1843e	0xd2a1f8
50	0x1aff812	0xc8cc3bb	0x2e34b69	0x548d48b	0x0fc340a	0x7ca499b	0xdeebe6
51	0xeb214ef	0x067b1f8	0x19c630a	0xe7c0a44	0x66f4697	0x541cbf6	0x4420a7
52	0x2403450	0x5331c01	0x59f99e8	0xa39e281	0x8971df1	0x4c21780	0x9f6e12
53	0x96b81f7	0xc44f275	0x3e91d6c	0x644040d	0xd338e4e	0x0afa6f2	0xd38e1e
54	0xaf435aa	0x8ba5ab2	0x90519f8	0x72a4777	0xc552143	0x2630971	0x6c91f6
55	0x011f064	0x0a7aa39	0x072d48d	0x2802af7	0x15041a9	0xea862e3	0x34d8ae
56	0x7532414	0x0a296c3	0xa5510c1	0x6891e10	0x5316410	0x45e1c10	0x354c25

Table B-8. Block Module (BM0) States During A2 – B1 Authentication (REPEATER = 0)

Sequence	LFSR 0	LFSR 1	LFSR 2	LFSR 3	SH 0	SH 1	SH 2	SH 3
Load								
1								
2								
3								
…								
47								
48								
Load	0x01e82	0x0399e	0x0ef5b	0x11963	01	01	01	01
1	0x01d04	0x0333c	0x0deb7	0x032c7	00	10	10	10
2	0x01a09	0x02678	0x0bd6f	0x0658e	00	01	01	00
3	0x01413	0x00cf0	0x07adf	0x0cb1c	01	10	10	00
4	0x00827	0x019e1	0x0f5bf	0x19638	11	00	11	00
5	0x0104e	0x033c2	0x0eb7e	0x12c71	10	10	10	01
6	0x0009d	0x02785	0x0d6fd	0x058e3	01	11	01	00
7	0x0013b	0x00f0b	0x0adfb	0x0b1c7	10	11	10	10
8	0x00276	0x01e17	0x05bf7	0x1638e	00	11	01	01
…	…	…	…	…	…	…	…	…
49	0x0055e	0x02e73	0x08f69	0x07085	11	00	11	10
50	0x00abd	0x01ce7	0x01ed3	0x0e10b	11	01	01	01
51	0x0157b	0x039cf	0x03da6	0x1c217	11	11	00	11
52	0x00af6	0x0339f	0x07b4c	0x1842f	10	11	01	10
53	0x015ed	0x0273f	0x0f699	0x1085e	01	01	10	01
54	0x00bdb	0x00e7f	0x0ed32	0x010bc	00	10	11	00
55	0x017b6	0x01cff	0x0da64	0x02179	00	00	11	01
56	0x00f6c	0x039fe	0x0b4c8	0x042f3	10	00	01	11

Table B-9. LFSR Module (LM0) States During A2 – B2 Authentication (REPEATER = 0)

Sequence	Kx	Ky	Kz	Bx	By	Bz	Output ([23:0])
Load	0xb8676a7	0xa423d78	0x0000000	0x406a74d	0x51f7175	0x0000003	
1	0x666e2c6	0x1fb7111	0x802f1c8	0xf7f1edb	0x7052777	0x0f40723	0xf05140
2	0x222564c	0xeacf83b	0x56392e2	0xf8c5faf	0x9e2408b	0x787caa9	0x91937d
3	0x3a7d9e3	0x39004ba	0x11f7a6a	0xd50bb43	0x88db561	0x91040c2	0x026852
4	0x47614d8	0x6494d8a	0x3b4f25b	0x4395a00	0x53d0514	0xe2e383d	0x3bc587
5	0xdb4e14e	0x845a7cc	0xbf7698d	0xbeab442	0xbe1b11f	0x6a72f32	0xb649af
6	0x9f50e9a	0x72b9f8a	0xe83d832	0x2446aa1	0x2711b9c	0xcdda1d2	0x76b8c5
7	0x3ea1bc9	0x2ef84ca	0x8b460ed	0xff20d53	0x0d6ac1d	0x45a75c4	0x1cfba1
8	0x16166f2	0xaa7c2ef	0x1d92ed2	0x962b376	0x2b810f5	0x085c932	0x34494d
…	…	…	…	…	…	…	…
41	0x2b7a4ee	0x76aaca6	0x990b686	0xe19348b	0xfea6035	0xa9afaf0	0x37e446
42	0x2420fda	0xc71cbcb	0xd3a43cf	0x3b01c23	0xa98bd4f	0x4c62274	0x58a13f
43	0x1b38c46	0x7b286a6	0x1d6e079	0x7fd5dd1	0xd04a459	0x7c16c08	0xd854bb
44	0x9ecc174	0xa97266e	0xa162b3f	0xbab8ead	0xff58f91	0x7740eea	0x5b3ceb
45	0x039d3b7	0x039e9b4	0xbc7dd68	0xfa0a1ce	0xb752298	0xb13d8cf	0xdf6e53
46	0x5096513	0xc3ac236	0x4adda17	0xdc0290a	0xff95916	0x9f7e6f6	0x1dbde4
47	0xc0f65b9	0x566da3d	0x55dab36	0x179735f	0x586589a	0xba7cd32	0xc580c5
48	0x83f87f0	0xd6f60e1	0xb0ffacc	0x799ee82	0x1963deb	0xd2ecfc7	0x531799
Load	0x799ee82	0x1963deb	0xd2ecfc7	0x406a74d	0x51f7175	0x0000003	
1	0xc4e8ff1	0x68b3b95	0x5a86976	0x3729648	0x7052777	0x0f40723	0xda19ca
2	0xf2c964d	0x2f49256	0x8ec9541	0xb06dc21	0x9e2408b	0x11e91dc	0xa8a0b8
3	0x26464e7	0xab964b8	0xc6112c9	0x72cfc92	0x4417ad5	0xc11c247	0xe28985
4	0x3b7c3f4	0x20c212b	0x5a8464d	0x235fdd1	0xc5a1984	0x7152f6d	0x8d3851
5	0x0c23381	0x1700053	0xf79219e	0x593da63	0xc18c5f2	0xaec1bce	0xb484bf
6	0x6c9733a	0xaa9fab7	0x3ff3223	0x3295feb	0x8e7c3b9	0x394597d	0x30ed7d
7	0xf811f2c	0x5e2ced9	0x7d2aca5	0xe469c78	0xacc10da	0xba93ae2	0xa60a41
8	0x1ed5c78	0xc42186b	0xc39983c	0x0c80d4e	0xccbafe1	0x235ff24	0x25ab7f
…	…	…	…	…	…	…	…
49	0x7d252c0	0x081db0e	0x329083e	0x3036a4c	0x4c638fc	0x9042db0	0x9c7024
50	0xba0eaa9	0x1c0b139	0x9f56b08	0x4771510	0x4f22c73	0x6321faf	0x4732f1
51	0x531015d	0xe8cd792	0xceb6a51	0x9327e2f	0xd768e6e	0x5ca36be	0x45edc6
52	0xd1a375c	0xd925c31	0xc37b8b1	0xb098639	0x8316b0f	0x7e66ad9	0x62404c
53	0xb0a7396	0xd77e370	0xc279e10	0x0b2b48e	0x3e28ad6	0xbb19243	0xc8d05d
54	0xd5c53b3	0x9fb7633	0xb69eb4a	0x88af562	0x5c2925d	0x8b95f94	0x5c8c26
55	0x33dc74d	0x9b22ce5	0xfd6ece8	0x2de6f79	0xab859d1	0x9fbbcfb	0x4f378a
56	0x96549f5	0x5e909b2	0xcd1638f	0x7ed9156	0x95fcf36	0xa455e43	0xd5126e

Table B-10. Block Module (BM0) States During A2 – B2 Authentication (REPEATER = 0)

Sequence	LFSR 0	LFSR 1	LFSR 2	LFSR 3	SH 0	SH 1	SH 2	SH 3
Load								
1								
2								
3								
…								
47								
48								
Load	0x01e97	0x01d48	0x03d90	0x1bc60	01	01	01	01
1	0x01d2f	0x03a91	0x07b21	0x178c0	10	10	11	00
2	0x01a5f	0x03522	0x0f642	0x0f180	01	01	11	10
3	0x014be	0x02a45	0x0ec85	0x1e301	11	00	11	01
4	0x0097d	0x0148b	0x0d90a	0x1c602	11	01	10	11
5	0x012fa	0x02916	0x0b215	0x18c05	11	11	00	11
6	0x005f4	0x0122d	0x0642a	0x1180a	01	11	10	01
7	0x00be9	0x0245b	0x0c855	0x03015	10	11	01	10
8	0x017d3	0x008b6	0x090ab	0x0602b	01	10	11	00
…	…	…	…	…	…	…	…	…
49	0x01f26	0x01ba1	0x004d1	0x01eb1	01	10	01	00
50	0x01e4d	0x03742	0x009a3	0x03d62	11	01	10	00
51	0x01c9a	0x02e84	0x01346	0x07ac5	11	10	01	10
52	0x01935	0x01d09	0x0268d	0x0f58b	11	01	10	11
53	0x0126b	0x03a12	0x04d1b	0x1eb16	10	10	11	10
54	0x004d7	0x03424	0x09a37	0x1d62d	00	01	11	11
55	0x009ae	0x02849	0x0346f	0x1ac5b	00	10	01	11
56	0x0135d	0x01093	0x068df	0x158b7	00	00	11	01

Table B-11. LFSR Module (LM0) States During A1 – B1 Authentication (REPEATER = 1)

Sequence	Kx	Ky	Kz	Bx	By	Bz	Output ([23:0])
Load	0x22fcecc	0x5309c7d	0x0000000	0xc070403	0x271c130	0x0000134	
1	0x000084c	0xf458fff	0x7f722dc	0xa5d4b70	0x9fb9989	0x9f6066d	0xbe70ee
2	0x0ed9f8a	0xb444236	0x3b62e76	0x614bd63	0x1d52893	0x2e71e83	0x102031
3	0x70ef0ef	0x9aa103f	0x8aa659d	0xe37a3ed	0x6e17dcd	0x861926f	0xff57a7
4	0xc8f3da5	0x8bbb85f	0x58047e6	0x0ed0c42	0xe3299e6	0xb4a6b97	0xb351be
5	0x6b68710	0x1826042	0xc20a675	0x7e45c24	0xc398d39	0xa08a2f8	0x785499
6	0xd4c9cf4	0x0014506	0x6c11733	0x1395270	0xf15cafa	0x1e1176c	0xe2b59c
7	0x2ff2231	0x059031a	0xd84c367	0x2769c98	0x7d0946d	0x0bf1b6a	0xaaa109
8	0x1c13406	0x516f805	0x3e231f5	0xe99e086	0xde5a665	0x22dff84	0x2ce1f3
…	…	…	…	…	…	…	…
41	0x7dc29a3	0x5895932	0x26047a5	0x0755719	0x935cfbf	0xb95d7e0	0x24e15b
42	0xba7d2b0	0xf1cfeac	0x36eb45d	0x2a92c58	0x699d93d	0x0eb7293	0x87309b
43	0xdd26650	0x29e8ca4	0xbf0109c	0xfa8cac0	0x1e322dc	0x01e0bb2	0xb0f7f3
44	0xf928c5b	0xc70cecd	0xcc71bb9	0x9b0f0e5	0x89e6139	0x613ba0b	0x800977
45	0x491d801	0xf630446	0x43655f6	0x4b35863	0x06237ac	0xca3aa9e	0x4fdd1d
46	0x9281463	0x891c25b	0x2c40a10	0xd0db4ac	0x07ca5ad	0x3745ef1	0x4fd875
47	0x37ef335	0xbb8429b	0xfad91c5	0x1f0f4dc	0xcb0f7af	0x9858087	0x08d905
48	0x7bd96ba	0xee950f7	0x749f3d9	0x1d48e97	0xbc607b2	0x98d9b45	0x2247f5
Load	0x1d48e97	0xbc607b2	0x98d9b45	0xc070403	0x271c130	0x0000134	
1	0x371f49a	0x53afa6d	0x1648023	0x7f3108b	0x9fb9989	0x9f6066d	0x7ccafe
2	0x3271b4e	0x7c7ab77	0x269baee	0x879d9dd	0x1d52893	0x40ef6b9	0xf3e3bb
3	0x76928cd	0x3c0c41e	0x3ddb777	0x56aff98	0x80f974f	0x6ed848c	0x387685
4	0xcb38955	0x45f4b5a	0x44b09f0	0x84f827e	0xd8421d6	0x756a06d	0xcac318
5	0x7e05951	0x7b4b7ce	0x77213e7	0x8a65060	0x41308c0	0x172f316	0xbba079
6	0xf43b422	0x63ba5f7	0x15664df	0xa546f91	0x6e221b2	0x5b52502	0x15723b
7	0x02539f7	0x43b1c83	0xc6fba6e	0x8c6d674	0x4234c5a	0x64478ee	0x6d962d
8	0xf69c689	0xc41f360	0x04591c2	0xde7e4f0	0x803e2ed	0x532a599	0xa8de7e
…	…	…	…	…	…	…	…
49	0x7bf9fa7	0x1a284c6	0x739fd87	0x461f4a1	0xf717fe1	0x32b1a29	0xf7f563
50	0xd779ca4	0xef3a891	0x60780be	0xaa1ce2e	0x9754a31	0x0b0bbfc	0x664b98
51	0x900446f	0x80e9401	0xc3bf1fb	0xfebca94	0x4e6d371	0xe3b1944	0xd1dc3b
52	0x83b3ab9	0x66e50bb	0xe8c834c	0xea84947	0x53787ed	0xd15995d	0xc6c650
53	0xd17e23d	0xfd8c2ef	0x618168a	0x5091ea5	0x9e567a1	0x6b37e87	0x49372d
54	0x6cc9afa	0x560a656	0x3dd0e24	0xc214d9d	0x71be498	0x3040f5e	0x0e3dce
55	0xcb2c184	0xdc614f7	0x5d3ee63	0x0bba955	0xaa48398	0xaf781e4	0x6438bb
56	0x692a85f	0xde2a833	0xff731e2	0xafa1960	0xc8a6055	0xbcc4562	0x85e78f

Table B-12. Block Module (BM0) States During A1 – B1 Authentication (REPEATER = 1)

Sequence	LFSR 0	LFSR 1	LFSR 2	LFSR 3	SH 0	SH 1	SH 2	SH 3
Load								
1								
2								
3								
…								
47								
48								
Load	0x01aaa	0x0154c	0x0278b	0x0b789	01	01	01	01
1	0x01555	0x02a99	0x04f17	0x16f13	10	10	10	11
2	0x00aaa	0x01533	0x09e2f	0x0de26	01	01	11	01
3	0x01554	0x02a66	0x03c5e	0x1bc4c	00	10	11	10
4	0x00aa8	0x014cc	0x078bd	0x17898	00	00	11	11
5	0x01550	0x02999	0x0f17a	0x0f131	00	00	10	11
6	0x00aa0	0x01332	0x0e2f4	0x1e262	01	00	00	11
7	0x01540	0x02664	0x0c5e9	0x1c4c4	10	10	00	10
8	0x00a81	0x00cc9	0x08bd2	0x18989	01	01	01	00
…	…	…	…	…	…	…	…	…
49	0x00c45	0x01b77	0x08130	0x052e4	00	01	00	01
50	0x0188b	0x036ef	0x00260	0x0a5c9	01	00	01	10
51	0x01117	0x02dde	0x004c1	0x14b93	00	01	00	01
52	0x0022f	0x01bbc	0x00982	0x09727	01	00	01	00
53	0x0045e	0x03779	0x01304	0x12e4f	11	00	10	00
54	0x008bc	0x02ef2	0x02608	0x05c9e	10	10	01	00
55	0x01179	0x01de5	0x04c10	0x0b93d	01	00	10	10
56	0x002f3	0x03bcb	0x09821	0x1727b	10	00	00	11

Table B-13. LFSR Module (LM0) States During A1 – B2 Authentication (REPEATER = 1)

Sequence	Kx	Ky	Kz	Bx	By	Bz	Output ([23:0])
Load	0x089c923	0xf6aee46	0x0000000	0xad10fe5	0x5e62a53	0x0000144	
1	0x000ace8	0x2bbe222	0xa84ba32	0xf8ee8f0	0x5d68545	0x649180e	0xb24463
2	0xbe2db4d	0xced43e8	0x6cf4c5d	0x5e52253	0x8d0daa0	0xfbde86b	0x1fa15f
3	0x59aaa16	0x420acae	0x948ddf1	0xe59bdcc	0xd7951b1	0x092c03c	0x787a32
4	0x6716e27	0xc71eabf	0x728216a	0x84926be	0xcaad80c	0xec3a8a5	0xf27cef
5	0x2b8be74	0xc7b7cd8	0x1896efd	0x7d66727	0x5c571f8	0x8069a85	0x88a3ad
6	0x417f923	0xf719e90	0xd5c1459	0x76bb30d	0x5333af4	0xa18c913	0xd01f1b
7	0x6c1faa9	0xf7175fd	0x50bb276	0xd91bfa4	0x1a7d561	0x456e67c	0xdc6f7c
8	0x90a1447	0xad4dd26	0x59afdb6	0xa59b390	0x1794cd7	0x3453dff	0x9276f6
…	…	…	…	…	…	…	…
41	0x456a8de	0x218a73d	0xefe8143	0x4705e66	0xa0ab473	0x77d249d	0x40cba0
42	0x5bb75c0	0x9e32509	0xcd4d66f	0x4d4a0e2	0x02b580f	0x2b49a78	0x1a3445
43	0x692b31d	0x40c7b06	0xeb692c8	0x0d36661	0x3a20c13	0x8cf85c3	0x02f684
44	0x4ac7e44	0x584dad4	0x2606dca	0xb39da54	0xc47d057	0xdca5d5d	0xf7ef88
45	0x995c381	0xe782e99	0x500545a	0x0710574	0x54607a7	0x42e8a1e	0xf1a5cc
46	0x2a39ef6	0xb3509f9	0xbd26dfe	0x284e17f	0x439d9e4	0x4dd18ce	0x23402b
47	0xe937d30	0x7910780	0x03575d7	0xdf9ad7d	0x3c7791a	0x6ddd61f	0x95dc64
48	0xb9af224	0x04c8a5f	0x49c96b1	0x754caaa	0xb7894f1	0xfcce020	0xcdaa1d
Load	0x754caaa	0xb7894f1	0xfcce020	0xad10fe5	0x5e62a53	0x0000144	
1	0x1cfb5dd	0xce2b088	0x2eec032	0x93dabe7	0x5d68545	0x649180e	0x4bbc20
2	0xfa0338f	0xdd9d11d	0x26e8f45	0x91d34c5	0x8d0daa0	0xa42f29f	0x0c1351
3	0x11ffc1e	0xd8fc06f	0x846a9c2	0x575d169	0x5f1d290	0xd8d250e	0x14f5d7
4	0x004ea3a	0xb8ae70e	0x00f25c3	0x807911a	0x442cc5a	0x1f6d6e5	0xa0c9b8
5	0xffd1f46	0x63fcef9	0x59e2583	0x0965cff	0x912f65a	0x9fad256	0x28067a
6	0x86aa27f	0x1bfc986	0x7559055	0xd307ffb	0x11af6d1	0x4d14ec4	0xa73184
7	0xe438d81	0x2f72c2a	0x065bebb	0x2c48a34	0x00ed16b	0xb2430a6	0x62d500
8	0xdc88b2a	0x1b83e3e	0xc719f35	0x3530afd	0x2435827	0x62edd40	0xe4b982
…	…	…	…	…	…	…	…
49	0x6e1ecc7	0x2126ced	0xa7ac884	0x0a7c511	0x278da73	0x3c52476	0x2afbb7
50	0x9b7983d	0xd61a93c	0x560de7f	0x47467e0	0xf5c27f1	0x56257fb	0xbf090b
51	0x1848c4a	0x6946104	0x97436c5	0x0ac81df	0xac47979	0x84c004f	0x6fffc7
52	0xb9ff03e	0xfafd4f8	0x030217e	0xb570368	0x4a63c44	0x8c9e6ff	0x8f5af2
53	0x031fbfa	0x20c4236	0x7181797	0xa99940c	0x810cdc7	0x6eb5e1a	0xda43d6
54	0xc67ef5d	0xdee5ece	0xb3296c2	0xd4f4edd	0xe33bd04	0xcbee012	0xc409c6
55	0xa8244d2	0x3aef4b0	0x5c7f3ad	0x7eb9d86	0xa72a66e	0x5527b8c	0x3f82c9
56	0xe3a9d07	0xce2e311	0xa20cd64	0xe15b166	0x74e9482	0x6a048e0	0x6856e1

Table B-14. Block Module (BM0) States During A1 – B2 Authentication (REPEATER = 1)

Sequence	LFSR 0	LFSR 1	LFSR 2	LFSR 3	SH 0	SH 1	SH 2	SH 3
Load								
1								
2								
3								
…								
47								
48								
Load	0x01bb1	0x012f3	0x00be0	0x1fe37	01	01	01	01
1	0x01763	0x025e7	0x017c1	0x1fc6e	10	11	00	10
2	0x00ec7	0x00bce	0x02f82	0x1f8dd	01	11	10	01
3	0x01d8f	0x0179d	0x05f04	0x1f1bb	00	11	11	00
4	0x01b1f	0x02f3b	0x0be08	0x1e377	10	01	11	01
5	0x0163f	0x01e77	0x07c10	0x1c6ef	01	10	11	11
6	0x00c7f	0x03cee	0x0f821	0x18ddf	11	00	11	11
7	0x018fe	0x039dd	0x0f043	0x11bbf	10	01	10	11
8	0x011fc	0x033bb	0x0e087	0x0377e	11	00	01	11
…	…	…	…	…	…	…	…	…
49	0x00d13	0x03c38	0x09f02	0x16ea7	00	11	11	01
50	0x01a27	0x03870	0x03e04	0x0dd4f	00	10	11	10
51	0x0144f	0x030e1	0x07c09	0x1ba9e	01	00	11	11
52	0x0089e	0x021c3	0x0f812	0x1753c	11	00	10	11
53	0x0113d	0x00386	0x0f024	0x0ea78	01	10	00	11
54	0x0027b	0x0070d	0x0e048	0x1d4f0	11	01	00	01
55	0x004f7	0x00e1b	0x0c091	0x1a9e0	10	10	01	10
56	0x009ee	0x01c37	0x08122	0x153c1	01	00	11	01

Table B-15. LFSR Module (LM0) States During A2 – B1 Authentication (REPEATER = 1)

Sequence	Kx	Ky	Kz	Bx	By	Bz	Output ([23:0])
Load	0xbec1205	0x4afe34d	0x0000000	0x1c66e07	0xbec2bb0	0x0000183	
1	0x888e2ea	0x414b444	0x97a0589	0xf087578	0x2c4a233	0x610f071	0x001a91
2	0x4625e41	0xcd48c5f	0x3a77722	0xf95ef49	0x467d200	0xb71a3c5	0x99774a
3	0xc9402d8	0x5ce2e8b	0x2d46dd1	0x6108d09	0xccc49d1	0x9c06127	0xf1c0f1
4	0x9f4f7b0	0x4c9fc33	0x7975e63	0xe5ed94e	0xa6cfafe	0x2632b27	0x3ce478
5	0xa52c6b9	0x0ab1bea	0x3f59b80	0xc0165ea	0xb0c5a07	0x52300a1	0x8091f8
6	0xe828e8c	0x1f4fe28	0xf9ae9ca	0x7849ad5	0x5c4c5dc	0x8ba6a57	0xa1cf90
7	0x3d9656f	0x9313d6c	0xd525839	0xb882808	0xaf4cb4e	0xe0eb86a	0xd6d500
8	0x0b5904f	0xe168c0e	0x8549a6c	0x720eb74	0xe3f004a	0xbab4d22	0x1000c1
…	…	…	…	…	…	…	…
41	0xf907779	0x8add56d	0xa2bf28b	0x170a7c3	0x35dc444	0x8e8c9fa	0xa24983
42	0xbb149e8	0x34b44fe	0xe899a28	0x298b048	0x32b7742	0xd005cfd	0xea1835
43	0x852bc22	0x30c541b	0x4ba8ad0	0x3eae65f	0x158d372	0xcadc45a	0xe1162f
44	0xe0dcc66	0x3380692	0x2f59c16	0xe406ae7	0x605aa2c	0x37ac1ab	0x9e5a09
45	0xbd69a67	0x11e9f3b	0xb0d15db	0xedd1223	0x38397e2	0xa9aeec0	0xb5955f
46	0x992aba4	0x79ccd6c	0x374d0da	0x50ca3ca	0x24fe7c5	0xab2ac15	0x8680ef
47	0x02d7a9c	0x69e0827	0x75c491b	0xc2e075e	0x27ef684	0x5569487	0x2f26b1
48	0x28d5897	0x4f55c34	0x1bf2686	0x12f3bb1	0xfe3717c	0x4903692	0x490497
Load	0x12f3bb1	0xfe3717c	0x4903692	0x1c66e07	0xbec2bb0	0x0000183	
1	0xa4b6650	0x0726307	0x51cb288	0x775f7b9	0x2c4a233	0x610f071	0xc6a91b
2	0xb19afdf	0x140ae14	0x6402f81	0xe318db4	0x467d200	0xbf592b0	0x5dcbb5
3	0x9159d90	0x4dec573	0xca5821f	0xc90434c	0x333bc3a	0x8fd699e	0x93cd20
4	0x958e6ac	0x17a4c19	0x95d7367	0xf18d3a1	0xa0182d7	0x0608db9	0xa81d43
5	0x5637028	0x7fd4c2b	0x235d32a	0x012244a	0x760a344	0x856619e	0x73e788
6	0x30b4ded	0x6cf793e	0x75d7724	0x29dc723	0x363fbe6	0xc615e74	0x18faae
7	0x0be6fa2	0x96a92c7	0x013fcf0	0x40c3e38	0x693a50c	0x2c0f81f	0x429d33
8	0x302975b	0x762a198	0x0e1b7f2	0x0b403f5	0x1493775	0x0326946	0x743991
…	…	…	…	…	…	…	…
49	0xaf2d2bb	0xe13c1bf	0xd5bf725	0xa861b70	0x30baed9	0x595a054	0xaee82d
50	0xd6b547a	0xbcc8c65	0xaf1fe4b	0x5e1ed44	0x3bdcf3f	0x775ef00	0x574a8e
51	0x8e47e11	0x1a9467f	0xc074e74	0xf94ad69	0x78cca09	0x3f48c38	0x6d424b
52	0x819e9c2	0xed51704	0x9cd77e9	0x03dd484	0x3b38f11	0x9e92103	0xbcdd40
53	0x274fca5	0x50dde0a	0xe25ca16	0x462e7d7	0xa603ab6	0x48da00f	0x97536d
54	0x910b283	0x5dcf83d	0x3a4f75f	0xecacd6b	0x7c0fb7b	0x1b60ea8	0x0eee1e
55	0xea791f3	0x92b86cf	0x3be152b	0xe0f4dc5	0xd3e247e	0x6996c21	0xdd44a5
56	0xcb67cb7	0xab75038	0xf8a92f2	0x754b3d8	0x47f242a	0x5d3f58c	0x9b8bf4

Table B-16. Block Module (BM0) States During A2 – B1 Authentication (REPEATER = 1)

Sequence	LFSR 0	LFSR 1	LFSR 2	LFSR 3	SH 0	SH 1	SH 2	SH 3
Load								
1								
2								
3								
…								
47								
48								
Load	0x002d0	0x0281a	0x08a38	0x0aac4	01	01	01	01
1	0x005a1	0x01034	0x01471	0x15588	00	11	00	10
2	0x00b42	0x02069	0x028e2	0x0ab11	00	10	01	00
3	0x01685	0x000d2	0x051c5	0x15623	01	00	11	00
4	0x00d0a	0x001a5	0x0a38b	0x0ac47	00	01	10	01
5	0x01a14	0x0034b	0x04716	0x1588f	01	00	11	00
6	0x01428	0x00697	0x08e2c	0x0b11e	10	00	01	10
7	0x00850	0x00d2e	0x01c58	0x1623d	01	01	00	01
8	0x010a1	0x01a5d	0x038b1	0x0c47b	11	00	01	10
…	…	…	…	…	…	…	…	…
49	0x017d1	0x002a0	0x0c549	0x10b2f	10	00	00	11
50	0x00fa2	0x00540	0x08a93	0x0165f	11	00	00	01
51	0x01f44	0x00a80	0x01526	0x02cbe	01	10	00	10
52	0x01e89	0x01501	0x02a4c	0x0597c	10	00	01	01
53	0x01d12	0x02a03	0x05498	0x0b2f8	01	00	00	10
54	0x01a24	0x01406	0x0a931	0x165f1	11	00	00	00
55	0x01449	0x0280d	0x05263	0x0cbe2	10	01	00	00
56	0x00892	0x0101a	0x0a4c6	0x197c5	01	11	00	00

Table B-17. LFSR Module (LM0) States During A2 – B2 Authentication (REPEATER = 1)

Sequence	Kx	Ky	Kz	Bx	By	Bz	Output ([23:0])
Load	0xb8676a7	0xa423d78	0x0000000	0x406a74d	0x51f7175	0x0000103	
1	0x666e2c6	0x1fb7111	0x802f1c8	0xf7f1edb	0x6143676	0x0f40723	0xf05140
2	0x222564c	0xeacf83b	0x56392e2	0x162b14f	0xde614cf	0x787caa9	0x81c36f
3	0x3a7d9e3	0x39004ba	0x11f7a6a	0x7fa1be9	0x01d7de9	0x01b5c18	0x206e42
4	0x47614d8	0x6494d8a	0x3b4f25b	0x25cec72	0x4a836ae	0x2534ecb	0xeaf263
5	0xdb4e14e	0x845a7cc	0xbf7698d	0x4a208a3	0x30e92d8	0xa659bcf	0x84539a
6	0x9f50e9a	0x72b9f8a	0xe83d832	0xe5d510e	0x442ab7d	0x3cd4cd1	0xc822c1
7	0x3ea1bc9	0x2ef84ca	0x8b460ed	0x1b4eb4a	0xd2f25b6	0xeb1adbf	0x37ed7a
8	0x16166f2	0xaa7c2ef	0x1d92ed2	0x1b5c7a1	0x25d261d	0xf639672	0x0312ca
…	…	…	…	…	…	…	…
41	0x2b7a4ee	0x76aaca6	0x990b686	0x7b9285b	0xcea3e3a	0xf0550a8	0xab9a38
42	0x2420fda	0xc71cbcb	0xd3a43cf	0xaca9532	0xf5455b6	0xd465e50	0x6ccddb
43	0x1b38c46	0x7b286a6	0x1d6e079	0xf25ba51	0xad5a148	0xbbb5468	0x0532d5
44	0x9ecc174	0xa97266e	0xa162b3f	0x3954aab	0xc8cae06	0xe9ffa6a	0x59de69
45	0x039d3b7	0x039e9b4	0xbc7dd68	0x76e0d88	0xf667013	0x5ca7484	0xa81811
46	0x5096513	0xc3ac236	0x4adda17	0x96a7579	0xccfde0b	0x56352ce	0x1d33c5
47	0xc0f65b9	0x566da3d	0x55dab36	0x6ff16c4	0x198a2d8	0x97f7aef	0x1ad8fa
48	0x83f87f0	0xd6f60e1	0xb0ffacc	0x081a2d0	0xaac4147	0x7734dfc	0xd23a1e
Load	0x081a2d0	0xaac4147	0x7734dfc	0x406a74d	0x51f7175	0x0000103	
1	0x1ace2d1	0x14061ea	0x0c44875	0xd086746	0x6143676	0x0f40723	0x4e6747
2	0xd88d8d4	0xdb895bd	0x7e74e49	0x413ed54	0xde614cf	0xdb03edb	0x8d2332
3	0x95561d4	0xe90f704	0xfe35448	0x1cdbacf	0xcd1bfeb	0xbe705ef	0xb7c367
4	0x6aabee2	0xeb64c24	0xb674c2a	0xef4f673	0xd302546	0x75b8516	0x1c6484
5	0xfe3250b	0xb039351	0x4a14ff3	0x5a879c9	0xd849947	0xa65f3bb	0xb37177
6	0x7a6f7cc	0xfbd0e84	0xce6bee1	0x0ad85e1	0x7a6282a	0x7f78db0	0xe41787
7	0x581bf9a	0xf637058	0x06205c2	0x0ff292e	0x7d65bcc	0x84473cb	0x85be3b
8	0x662ea9c	0x99bf90a	0x290e00f	0xbad8a31	0x94d72cc	0xb929192	0x5857cf
…	…	…	…	…	…	…	…
49	0x68a55fc	0x5bc6412	0x5ca2595	0x14cc21e	0x30c7bd6	0xb826f67	0x06a265
50	0xb7cd0f6	0x33813a4	0x7b3e868	0x78c9a94	0x94e586f	0x1ea87f3	0x18c4db
51	0x3cb03ff	0xcb86820	0x7fa96de	0x71c1620	0x7c602e4	0x60688eb	0xc9abf0
52	0x1fee845	0x0a02783	0x371bc65	0x7d3cf2c	0xcf8006d	0x3206d1e	0xb00bfa
53	0x8b4c9c9	0x8c51ea6	0xd91c1db	0xec51ba3	0x5652523	0x36ba88d	0xb238b5
54	0xb5a6da8	0x7caf32e	0x1724577	0x1a1a940	0xf96eb52	0x8929566	0x1c7ad3
55	0x8bde531	0xcbd6c1e	0x0f35c36	0xc66fea6	0x0c3c692	0x6561bba	0x79cdd1
56	0x6138d30	0x09b02ea	0x3d45fab	0x81c0f48	0xaa5211b	0xbc2973b	0x30b266

Table B-18. Block Module (BM0) States During A2 – B2 Authentication (REPEATER = 1)

The A1-B1 test key pair is used to derive values in Table B-19 and Table B-20.

Ksv0	0x35796a172e
Ksv1	0x478e71e20f
Ksv2	0x74e85397a6
Binfo	0x0203
M_0	0x372d3dce38bbe78f
SHA-1 transform input	2e 17 6a 79 35 0f e2 71 8e 47 a6 97 53 e8 74 03 02 8f e7 bb 38 ce 3d 2d 37 80 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 c8
SHA-1 H0	0x0fcbd586
SHA-1 H1	0xefc107ef
SHA-1 H2	0xccd70a1d
SHA-1 H3	0xb1186dda
SHA-1 H4	0x1fb3ff5e
KSV FIFO (DPCD Address 0x6802C)	2e 17 6a 79 35 0f e2 71 8e 47 a6 97 53 e8 74
DPCD Addresses 0x6802A, 0x6802B	03 02
DPCD Addresses 0x68014 - 0x68017	86 d5 cb 0f
DPCD Addresses 0x68018 - 0x6801B	ef 07 c1 ef
DPCD Addresses 0x6801C - 0x6801F	1d 0a d7 cc
DPCD Addresses 0x68020 - 0x68023	da 6d 18 b1
DPCD Addresses 0x68024 - 0x68027	5e ff b3 1f

Table B-19. V/V' computation for an HDCP Repeater with DEVICE_COUNT = 3 and DEPTH = 2

Ksv0	0x23a19cbe4d
Ksv1	0x0d7e993570
Ksv2	0xd3458d7d09
Ksv3	0xe2a2dce946
Ksv4	0xf3148e499d
Ksv5	0x9345e95ca3
Ksv6	0xda8cb307c5
Ksv7	0x9901fa75ac
Ksv8	0x697f3a3c20
Ksv9	0xc89758ed19
Ksv10	0x2de3a8e869
Ksv11	0xe0d9295af2
Ksv12	0x6cde88a8b3
Ksv13	0x6e219499f5
Ksv14	0x31e3e1a572
Binfo	0x030f
M_0	0x372d3dce38bbe78f
First SHA-1 transform input	4d be 9c a1 23 70 35 99 7e 0d 09 7d 8d 45 d3 46 e9 dc a2 e2 9d 49 8e 14 f3 a3 5c e9 45 93 c5 07 b3 8c da ac 75 fa 01 99 20 3c 3a 7f 69 19 ed 58 97 c8 69 e8 a8 e3 2d f2 5a 29 d9 e0 b3 a8 88 de
Second SHA-1 transform input	6c f5 99 94 21 6e 72 a5 e1 e3 31 0f 03 8f e7 bb 38 ce 3d 2d 37 80 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 02 a8
SHA-1 H0	0x6dad1995
SHA-1 H1	0x7c0a62fc
SHA-1 H2	0x1b98fff2
SHA-1 H3	0x0159cbb7
SHA-1 H4	0xeae604fe
KSV FIFO (DPCD Address 0x6802C)	4d be 9c a1 23 70 35 99 7e 0d 09 7d 8d 45 d3 46 e9 dc a2 e2 9d 49 8e 14 f3 a3 5c e9 45 93 c5 07 b3 8c da ac 75 fa 01 99 20 3c 3a 7f 69 19 ed 58 97 c8 69 e8 a8 e3 2d f2 5a 29 d9 e0 b3 a8 88 de 6c f5 99 94 21 6e 72 a5 e1 e3 31
DPCD Addresses 0x6802A, 0x6802B	0f 03
DPCD Addresses 0x68014 - 0x68017	95 19 ad 6d
DPCD Addresses 0x68018 -	fc 62 0a 7c

0x6801B	
DPCD Addresses 0x6801C - 0x6801F	f2 ff 98 1b
DPCD Addresses 0x68020 - 0x68023	b7 cb 59 01
DPCD Addresses 0x68024 - 0x68027	Fe 04 e6 ea

Table B-20. V/V' computation for an HDCP Repeater with DEVICE_COUNT = 15 and DEPTH = 3

Table B-21 provides cryptographic parameters for verifying the facsimile SRM provided in Table B-22. These parameters are not used in production devices or SRMs. Refer to Table 7-4 for the cryptographic parameters used in production SRMs.

Parameter	Value (hexadecimal)
Prime Modulus	See Table 7-4
Prime Divisor	See Table 7-4
Generator	See Table 7-4
Public Key	8d13e19f340e11ceb0db95eb3eb0743195dfc402b7dc8caac7752e47ded8e8c00b115f8e5e08c7a664cbbba39786efd71c012e8394af79cd01f722a0926952e8de857cbd2e7295e6b1d88cc0ff5dcc0ab16d14fa11a48eb50fca83a37ed18de16d973565df8a784e854296ac700b2e030fd2a98183aa7b22a63b57bee5c2b946

Table B-21. Cryptographic Parameters for Verifying Facsimile SRMs

KSVs Revoked	SRM Version	Value (sequence of hexadecimal bytes)
511ef21acd, e72697f401	0005	80 00 00 05 01 00 00 36 02 51 1e f2 1a cd e7 26 97 f4 01 97 10 19 92 53 e9 f0 59 95 a3 7a 3b fe e0 9c 76 dd 83 aa c2 5b 24 b3 36 84 94 75 34 db 10 9e 3b 23 13 d8 7a c2 30 79 84

Table B-22. Facsimile SRMs

Table B-23 provides the intermediate results for DSA signature verification of the facsimile SRM provided in Table B-22. This uses the facsimile public key provided in Table B-21.

Message	80 00 00 05 01 00 00 36 02 51 1e f2 1a cd e7 26 97 f4 01
SHA-1 digest	f1be46b62fb9e0c155269fd7a293c4d823777b9d
w	6cdb2497316d6c4ece12b5c96058e3da5c53062c
u1	95f8e7790ff871c19d5f709075496206257 20a35
u2	5fae5a63e0d5c63d5e717f51ce2b85d6b5a81f06
G^u1	ace4b82012f02e73a0ec6d338a7159ef17534e0956e6d00606b26ba193fc33a7ccd4d39741a2b290dc1b1792453f3f41633fe9c455e4720012a61f698453207f579544ebf0307c4697c32c452dc0e2f66da2eb2260a16ff8e9a83cc34eae149397298e7db5a9bc8edf5b51b4a98c32cb5350b4ecf016651ab44cc091990275e5
Y^u2	6838025b95c5ac360a698c091b2ea6f7f68e8b8edcac43d251e9c8f46301b1291dcdf79041fb82b33170857ca3d9b5a42cf38ad7514bcef7db06fe1c1fbb3e120ac260d0dd29d53afa0f7ab86eb57dfd6da95504cc8f9518013ee74c85d3e2fb3b9e9fe140724b4ae476924d37b62c1fb73fc9644b438a2e532fd841c4d26f21
Product	915ec8e51d9314583b2b73b337dba961d87b0081b9a306ca9588cc3eed7bc051a0380a4a48dd28e322d5f238b990a72530fd0183114d20a820354204d9ceee265841e898cbc193aca330a002128003bfcc58f3195f5c4a95bf5c87eb9a60866ee0577d43a170872102fce784a095a9b0612440d9ff4194e4ea25b72567c5b25c
v	9710199253e9f05995a37a3bfee09c76dd83aac2

Table B-23. Facsimile SRM Verification Test Vectors

The encrypted output is derived in the SST mode. The A1-B1 test key pair is used to derive the test vectors given below. 4-Lane Main Link configuration is assumed and the input to the HDCP Cipher is assumed to be an all zero input (0x00000000). The HDCP Receiver does not support downstream connections (REPEATER = 0). S0, S1, S2 and S3 denote Symbol 0, Symbol 1, Symbol 2 and Symbol 3 respectively.

Km		5309c7d22fcecc
REPEATER || *An*		034271c130c070403
Ks		54294b7c040e35
M_0		a02bc815e73d001c
R_0		8ae0
K_1		d692b7ee1d40e8
M_1		1dbf44e50f523e56
Encrypted output generated during the 128-clock frame key calculation period. It is assumed that 128 32-bit symbols are encrypted during the 128-clock period. Frame key calculation is implemented in BM0. The 32-bit pseudo-random bits from OF1 are used to generate the encrypted output	1	S3 b7 S2 9e S1 e5 S0 fe
	2	S3 28 S2 9a S1 f9 S0 19
	3	S3 d2 S2 5b S1 5d S0 6c
	4	S3 ed S2 55 S1 dc S0 de
	5	S3 e4 S2 e5 S1 87 S0 63
	6	S3 f3 S2 be S1 fc S0 c7
	7	S3 a4 S2 a1 S1 b5 S0 65
	8	S3 7c S2 c3 S1 53 S0 b3
	9	S3 9c S2 ea S1 8e S0 38
	10	S3 ee S2 0a S1 a3 S0 3e
	11	S3 6c S2 13 S1 c2 S0 35
	12	S3 cb S2 40 S1 e9 S0 94
	13	S3 20 S2 0b S1 f7 S0 8b
	14	S3 e1 S2 13 S1 37 S0 6d
	15	S3 bd S2 7d S1 19 S0 0c
	16	S3 35 S2 22 S1 09 S0 92
	17	S3 b7 S2 80 S1 43 S0 ee
	18	S3 be S2 6b S1 9a S0 6c
	19	S3 51 S2 80 S1 fd S0 62
	20	S3 18 S2 27 S1 13 S0 54
	…	…
	109	S3 d4 S2 bd S1 6f S0 59
	110	S3 30 S2 f5 S1 c3 S0 21
	111	S3 79 S2 6e S1 95 S0 f3
	112	S3 78 S2 b3 S1 1d S0 f0
	113	S3 c6 S2 c7 S1 87 S0 82
	114	S3 6e S2 0c S1 e2 S0 3d
	115	S3 86 S2 33 S1 af S0 af
	116	S3 56 S2 69 S1 6c S0 0b
	117	S3 9d S2 81 S1 3c S0 11
	118	S3 62 S2 cb S1 43 S0 5b
	119	S3 a5 S2 37 S1 ed S0 94
	120	S3 bb S2 0e S1 3f S0 9f
	121	S3 55 S2 b5 S1 b4 S0 96
	122	S3 a8 S2 5a S1 1e S0 e9
	123	S3 39 S2 ad S1 0a S0 b2
	124	S3 ae S2 ee S1 7c S0 03
	125	S3 ee S2 62 S1 9a S0 59
	126	S3 0d S2 25 S1 40 S0 8d
	127	S3 c0 S2 7e S1 ce S0 76
	128	S3 ed S2 f0 S1 8a S0 f9
K_2		ea7c2988bb82fe

M_2		6a42b1dbd7a3b0f9
Encrypted symbols generated after the 128-clock frame key calculation		S3 b8 S2 62 S1 84 S0 bb
		S3 b8 S2 74 S1 39 S0 a6
		S3 f7 S2 01 S1 f1 S0 ed
		S3 52 S2 3d S1 12 S0 1c
		S3 f9 S2 6f S1 47 S0 ae
		S3 ba S2 69 S1 5c S0 5b
		S3 11 S2 63 S1 a5 S0 e9
		S3 27 S2 2f S1 1b S0 d1
CPBS is detected. Control symbols are not encrypted, however the BM0 and BM1 states are updated		
Encrypted output generated during the 64-clock line re-key period. It is assumed that 64 32-bit symbols are encrypted during the 64-clock period. Line Re-key is implemented in BM0. The 32-bit pseudo-random bits from OF1 are used to generate the encrypted output	1	S3 36 S2 12 S1 a0 S0 78
	2	S3 88 S2 d7 S1 37 S0 bf
	3	S3 db S2 de S1 a5 S0 97
	4	S3 3e S2 5d S1 dc S0 8a
	5	S3 06 S2 c2 S1 1d S0 b5
	6	S3 b3 S2 27 S1 75 S0 75
	7	S3 da S2 54 S1 ce S0 58
	8	S3 98 S2 62 S1 1d S0 74
	9	S3 b1 S2 a7 S1 ac S0 af
	10	S3 07 S2 b6 S1 05 S0 a2
	11	S3 7a S2 6e S1 58 S0 7b
	12	S3 09 S2 c7 S1 b3 S0 a7
	13	S3 e9 S2 9f S1 1a S0 b9
	14	S3 e0 S2 c2 S1 ba S0 e1
	15	S3 9f S2 bc S1 da S0 80
	16	S3 8d S2 7a S1 f8 S0 dc
	17	S3 7e S2 5e S1 fd S0 24
	18	S3 9f S2 43 S1 e2 S0 69
	19	S3 36 S2 e8 S1 71 S0 ed
	20	S3 fb S2 a3 S1 6c S0 bd
	…	…
	45	S3 e8 S2 b7 S1 ea S0 1e
	46	S3 ac S2 7e S1 0e S0 bc
	47	S3 23 S2 3b S1 f0 S0 c3
	48	S3 16 S2 20 S1 8c S0 84
	49	S3 2a S2 cb S1 e0 S0 6b
	50	S3 e8 S2 56 S1 01 S0 9a
	51	S3 e2 S2 96 S1 61 S0 45
	52	S3 81 S2 51 S1 e9 S0 2c
	53	S3 e2 S2 28 S1 cf S0 c1
	54	S3 68 S2 1b S1 90 S0 8d
	55	S3 37 S2 92 S1 bb S0 c6
	56	S3 58 S2 07 S1 ee S0 8e
	57	S3 62 S2 b4 S1 c1 S0 ae
	58	S3 c7 S2 65 S1 13 S0 57
	59	S3 6e S2 06 S1 59 S0 78
	60	S3 22 S2 d4 S1 ef S0 52
	61	S3 5d S2 e8 S1 20 S0 db
	62	S3 b9 S2 a4 S1 63 S0 92
	63	S3 62 S2 5c S1 b1 S0 28
	64	S3 a7 S2 e5 S1 86 S0 26
Encrypted symbols generated after 64-clock line re-key.		S3 69 S2 b1 S1 7a S0 6b
		S3 01 S2 f5 S1 e4 S0 17

		S3 9d S2 36 S1 3f S0 8f
		S3 d5 S2 3e S1 c7 S0 44
		S3 26 S2 17 S1 c2 S0 cc
		S3 21 S2 fe S1 67 S0 dd
		S3 be S2 c5 S1 e6 S0 b8
		S3 db S2 1f S1 b3 S0 ae

Table B-24. Sample Authentication and Encryption Values in SST Mode(REPEATER = 0)

Note: In all following tables, BM0 and BM1 values are indicated in the following format: Kx_Ky_Kz_Bx_By_Bz. LFSR[59:0] consists of concatenating the four LFSR states as follows (in Verilog format) LFSR[59:0] = {$LFSR_3$[16:0], $LFSR_2$[15:0], $LFSR_1$[13:0], $LFSR_0$[12:0]}. A1-B1 test key pair is used to generate values. The HDCP Receiver does not support downstream connection (REPEATER = 0)

Table B-25 provides test vectors during initial bootstrapping operation.

clk	LFSR[59:0]	BM0[167:0]	OF0 [23:16]	OF0 [15:0]	BM1[167:0]	OF1[31:0]	
1	--	0xc040e35_54294b7_0000000_73d001c_2bc815e_00000a0	--	--	--	--	
2	--	0x6666a4e_47b5444_93d46aa_d7c5eca_9caf998_7873596	--	--	--	--	
3	--	0x1232d67_ef6a7a5_6055678_43891a5_b7d9124_7008035	--	--	--	--	
4	--	0x811566c_da14697_66f89db_4af668e_adaaeaa_0436d93	--	--	--	--	
5	--	0xf7027a4_dc24164_29716cf_9955abb_7dad788_4553445	--	--	--	--	
6	--	0x53d886c_f8fb474_17d4aa3_a07973a_bf711b5_dd26c84	--	--	--	--	
7	--	0x7419dcc_03a4969_85b3011_6c4f773_8fe986f_ef5c652	--	--	--	--	
8	--	0xcebeca9_b5bc937_051e959_68c856a_7c60a3d_2155239	--	--	--	--	
9	--	0xce97863_e1dfa92_baefb5b_e40b97e_5e7ee1d_eebe872	--	--	--	--	
10	--	0xfb44568_c4b4338_6846ab1	--	--	--	--	

		_0dea6c2_09ab4ec_8357c78					
…	…	…	…	…	…	…	
40	--	0x95b2a05_05a1e0e_912d9df_e255290_c0d7412_b22dd49	--	--	--	--	
41	--	0xecfdbdb_3aa95c2_7f54b9c_13f9cc6_77c7185_e9f1773	--	--	--	--	
42	--	0x5b824bd_37e7a4a_c805dcc_082d7b6_fabe465_6b941d4	--	--	--	--	
43	--	0x3f304df_6e78415_08d38da_2d06e23_cf49c95_566cc4b	--	--	--	--	
44	--	0x0435ef2_76d6d5a_a122ea4_8813b14_f61e31d_e19da09	--	--	--	--	
45	--	0x8b0a742_b70da1c_2307640_9cf82dd_be90cd3_a6fd504	--	--	--	--	
46	--	0x57dd199_d4f7e9b_b85862b_5bcef9f_b34e561_01ba53c	--	--	--	--	
47	--	0xc9472f7_c4371c6_667db05_07ecff1_60e32f8_d709882	--	--	--	--	
48	--	0x2aeaf01_beef443_e0cd9a0_8375c35_cea2aed_1729ccc	--	--	--	--	
49	--	0x5cfb3bd_bb2e5ca_6f52793_e1d40e8_d692b7e_db36d8f	--	--	--	--	Ki : 0x00d692b7ee1d40e8
50	0x06b492dfb83a80e8	0xe1d40e8_d692b7e_db36d8f_73d001c_2bc815e_00000a0	--	--	--	--	
51	0x0d692dbf787521d0	0x86835d3_0f3c0ff_13b5646_61e28a1_9caf998_7873596	--	--	--	--	
52	0x0ad2537ef8ea63a0	0x7553201_a9df960_1cdac9c_4c9a9f6_b7d9124_d190726	--	--	--	--	

53	0x05a4a6fdf9d4e741	0x512a6d3_4a4086b_16267c8_4771001_434455e_69e04a1	--	--	--	--	
54	0x0b4945fbfba9ee82	0x88cd2c8_7d606a0_cb6197b_f82fcb2_fa4977c_5cc7724	--	--	--	--	
55	0x069283f7f753fd05	0x879d635_75bddc7_beb4e50_886ed86_258c974_8a55931	--	--	--	--	
56	0x0d2507efeea7fa0b	0xea1c240_d00ac37_d9dffdf_0ee9427_0f24a78_fe3d63f	--	--	--	--	
57	0x0a4a07dfd54fd417	0x86b1191_c77d3b3_cc45864_68238e8_391d4f9_1cfd76e	--	--	--	--	
58	0x049407bfa29fa82f	0x7a3f811_9fe23f9_95f0a96_9b64234_ec09134_39319a3	--	--	--	--	
59	0x0928077f4d3f505e	0xb9c5cc7_711aede_1d46299_c1e2509_cbece75_d38311a	--	--	--	--	
60	0x025006fe9a7e80bc	0x9fc8116_a3563ef_39dc1d0_6395c37_7cda563_465b745	--	--	--	--	
…	…	…	…	…	…	…	
97	0x03ddbed3211267e0	0x576981a_c96d5eb_0bc0716_d25e6a7_5ba1ffc_2df8d50	--	--	--	--	
98	0x07bb75a64224cfc0	0x714bc43_bd6c2a9_1c58407_117dcd7_3cddf89_92c078c	--	--	--	--	
99	0x0f76e34c8c49bf80	0x9dd5e24_753eb7d_bb541d6_2f043a3_d1164ce_09959c4	--	--	--	--	
100	0x0eedc69910935f01	0x8e18536_87a50d1_d5931d5_d53f441_01d6279_42fb792	--	--	--	--	
101	0x0ddb853221269e03	0xc6b69a9_88eda95_d1c0f1d_30c8c77_022ff9f_c88fb35	--	--	--	--	
102	0x0bb70264424d3	0xa09598b_3a58a01_a6d	--	0x1dbf	--	--	

	c06	7e5f_8b44a26_2fd9556_b253d49					
103	0x076e0cc88c9a580c	0x44b179f_a2a11c4_95bcf96_ddb2553_41f0e7a_e7a3410	--	0x44e5	--	--	Mi : 0x1dbfc815e73d001c
104	0x0edc11911934b019	0xdfa7c2d_50130ae_de7ba1d_af4583f_398d1b5_c24bb03	0xc0	0x0f52	--	--	Mi : 0x1dbf44e5e73d001c
105	0x0db8232232696032	0x4815d4f_edbe142_6d74db1_230f58f_5234a61_eb5ee8d	0x8b	0x3e56	--	--	Mi : 0x1dbf44e50f52001c Ri : 0x0000c0e0
106	0x0b70464464d2e065	0xd20317a_3725bc8_256af5e_6b9cc06_7d7aa18_87f9092	0x59	0xc03e	--	--	Mi : 0x1dbf44e50f523e56 Ri : 0x0000c08b
107	0x0b70464464d2e065	0xd20317a_3725bc8_256af5e_6b9cc06_7d7aa18_87f9092	0x59	0xc03e	--	--	
108	0x0b70464464d2e065	0xd20317a_3725bc8_256af5e_6b9cc06_7d7aa18_87f9092	0x59	0xc03e	--	--	
109	0x0b70464464d2e065	0xd20317a_3725bc8_256af5e_6b9cc06_7d7aa18_87f9092	0x59	0xc03e	--	--	
110	0x0b70464464d2e065	0xd20317a_3725bc8_256af5e_6b9cc06_7d7aa18_87f9092	0x59	0xc03e	--	--	
…	…	…	…	…	…	…	
128	0x0b70464464d2e065	0xd20317a_3725bc8_256af5e_6b9cc06_7d7aa18_87f9092	0x59	0xc03e	--	--	
129	0x0b70464464d2e065	0xd20317a_3725bc8_256af5e_6b9cc06_7d7aa18_87f9092	0x59	0xc03e	0xd20317a_3725bc8_256af5e_6b9cc06_7d7aa18_87f9092	0x6559c03e	
130	0x0b70464464d2e065	0xd20317a_3725bc8_256af5e_6b9cc06_7d7aa18_87f9092	0x59	0xc03e	0xd20317a_3725bc8_256af5e_6b9cc06_7d7aa18_87f9092	0x6559c03e	
131	0x0b70464464d2e065	0xd20317a_3725bc8_256af5e_6b9cc06_7d7aa18_87f9092	0x59	0xc03e	0xd20317a_3725bc8_256af5e_6b9cc06_7d7aa18_87f9092	0x6559c03e	

Table B-25. Initial Bootstrapping

Test Vectors for 4-Lane Main Link Configuration in SST Mode (Inter-BS spacing = 130, CPSR Interval = 3)

Authentication

Table B-3 and Table B-4 provide the LFSR and Block module states during the first part of authentication.

Initial Bootstrapping

Table B-25 provides test vectors during the initial bootstrapping operation.

After start of encryption

Table B-26 provides test vectors generated after the start of encryption (beginning with the first CPSR symbol set that triggers encryption). The main link stream is indicated for the initial transmissions. Table B-27 provides encrypted cipher outputs.

clk	Sym clk	LFSR[59:0]	BM0[167:0]	OF0[23:16]	OF0[15:0]	BM1[167:0]	Stream	OF1[31:0]
Frame key calc started								
-3	--	--	0xd20317a_3725bc8_256af5e_6b9cc06_7d7aa18_87f9092	--	--	0xd20317a_3725bc8_256af5e_6b9cc06_7d7aa18_87f9092	0x1c1c1c1c (SR)	0x6559c03e
-2	--	--	0xd20317a_3725bc8_256af5e_6b9cc06_7d7aa18_87f9092	--	--	0xd20317a_3725bc8_256af5e_6b9cc06_7d7aa18_87f9092	0x3c3c3c3c (CP)	0x6559c03e
-1	--	--	0xd20317a_3725bc8_256af5e_6b9cc06_7d7aa18_87f9092	--	--	0xd20317a_3725bc8_256af5e_6b9cc06_7d7aa18_87f9092	0x3c3c3c3c (CP)	0x6559c03e
0	0	--	0xd20317a_3725bc8_256af5e_6b9cc06_7d7aa18_87f9092	--	--	0xd20317a_3725bc8_256af5e_6b9cc06_7d7aa18_87f9092	0x1c1c1c1c (SR)	0x6559c03e
1	1	--	0xc040e35_54294b7_0000000_f523e56_bf44e50_000001d	--	--	0x9b48c65_3f7de85_4cfb937_50d9c10_5d7fbdc_6a03908	0x39393939 (VB-ID)	0xb79ee5fe
2	2	--	0x6666a4e_47b5444_93d46aa_a1a9cb4_a206aaa_cacfa30	--	--	0x94ede66_8141634_5f900d1_5f7a0f0_f291dcb_5a0ce6e	0x00000000	0x289af919
3	3	--	0x1232d67_ef6a7a5_6055678_533e54c_e4b418a_91fbcbb	--	--	0x1f69314_9a31990_c4b92db_31a6525_6ab1304_928c3d8	0x00000000	0xd25b5d6c
4	4	--	0x811566c_da14697_66f89db_d9ce46b_c89e263_9e3097e	--	--	0x7f0a70c_d1bda54_34c9929_7df4b37_d8d588c_855d111	0x00000000	0xed55dcde
5	5	--	0xf7027a4_dc24164_29716cf_27efca7_312e38b_d8d6	--	--	0x54bed7a_7e5b947_444b969_dc62d4f_90db7c1_70de92f	0x00000000	0xe4e58763

			121					
…	…	…	…	…	…	...	…	…
45	45	--	0x8b0a742_b70da1c_2307640_f0093a0_6c69ad6_2dfc26d	--	--	0x4736b27_c7ebca1_aa86bef_4539c7b_6c6bdec_c4b1f11	0x00000000	0x10f21d66
46	46	--	0x57dd199_d4f7e9b_b85862b_5cc55f4_2b5efea_85611ff	--	--	0x2789d57_f53ee8a_3cfeaf5_817480c_c30af76_2f49767	0x00000000	0x37affe86
47	47	--	0xc9472f7_c4371c6_667db05_9e19673_1fcfb80_9e1665f	--	--	0xfa07250_f725212_9bc279d_76fe61a_e1521fc_fb331b7	0x00000000	0x49152bc4
48	48	--	0x2aeaf01_beef443_e0cd9a0_d83548d_480c50a_5d4ed0e	--	--	0xcaf5121_1129806_3836e0a_9051c5e_34551ae_7f7b35a	0x00000000	0x1f068148
49	49	--	0x5cfb3bd_bb2e5ca_6f52793_8bb82fe_ea7c298_d9a59fa	--	--	0x62e765a_09101ee_f92cab1_4cfd7ca_f8ad063_1f97804	0x00000000	0xb79cb954
50	50	0x0f53e0a6257702fe	0x8bb82fe_ea7c298_d9a59fa_f523e56_bf44e50_000001d	--	--	0x960d99e_e9b8b0f_782d158_645c7a9_312615f_ca46465	0x00000000	0xfe492f2a
51	51	0x0ea7c94c42ee05fd	0xb486149_cca6e3d_0355dff_2262329_a206aaa_cacfa30	--	--	0xb72431d_495f294_aba13a4_c1a5edc_d8ea59b_2cbcad0	0x00000000	0x53331e18
52	52	0x0d4f929885dc0bfb	0x120ec20_a1030d1_4c72806_a00fb45_e4b418a_75af954	--	--	0xe94a5e8_bad382a_b516ee3_2aea12a_04f35e9_6a44723	0x00000000	0x5c0e4039
…	…	…	…	…	…	...	…	…
104	104	0x02a4d3a938e782d8	0x924eb87_b7a728b_8f829c6_35dd971_63da5b0_486ff01	0x97	0xd7a3	0x398cfb0_51408ef_9500162_a935d4f_835f420_da99144	0x00000000	0x1d74baa3
105	105	0x0549af5279cf05b1	0x711d28b_ffa6fca_923e67b_15707a7_42a4bb2_2deda6d	0xbb	0xb0f9	0xde9d7c1_83df898_1e55332_ddc9add_a82acb2_2885c03	0x00000000	0xd8835587
106	106	0x0a935ea4f39e2b63	0xeff1213_e232b20_0064b82_ae1968a_4a3cba4_40cb306	0x62	0x84bb	0xd887f8b_5d37e0d_fe4d145_6a55c77_9369bfb_5028d20	0x00000000	0xaf70715f
107	107	0x0a935ea4f39e2b63	0xeff1213_e232b20_0064b82_ae1968a_4a3cba4_40cb306	0x62	0x84bb	0xb77f694_6fed836_ec5fbda_befa034_2c5d690_ae478e9	0x00000000	0xc861665f
108	108	0x0a935ea4f39e2b63	0xeff1213_e232b20_0064b82_ae1968a_4a3cba4_40cb	0x62	0x84bb	0xa67d45e_0b30f7d_2bb93be_e09b5f5_22ca847_b849198	0x00000000	0x2bbcf09a

			306					
…	…	…	…	…	…	...	…	…
128	128	0x0a935ea4f39e2b63	0xeff1213_e232b20_0064b82_ae1968a_4a3cba4_40cb306	0x62	0x84bb	0x9359a39_d450a12_51ce5bc_d3062b6_2c9cca3_c74edc4	0x3c3c3c3c (CP)	0xedf08af9
129	129	0x0a935ea4f39e2b63	0xeff1213_e232b20_0064b82_ae1968a_4a3cba4_40cb306	0x62	0x84bb	0xeff1213_e232b20_0064b82_ae1968a_4a3cba4_40cb306	0x3c3c3c3c (CP)	0xb86284bb
Line Rekey Started								
clk	**Sym clk**	**LFSR[59:0]**	**BM0[167:0]**	**OF0[23:16]**	**OF0[15:0]**	**BM1[167:0]**		**OF1[31:0]**
-3	--	0x0a935ea4f39e2b63	0xeff1213_e232b20_0064b82_ae1968a_4a3cba4_40cb306	--	--	0x6886c93_2065e45_773f684_82237f8_df3ef7a_cae90a7	0xbcbcbcbc (BS)	0xc07ece76
-2	--	0x0a935ea4f39e2b63	0xeff1213_e232b20_0064b82_ae1968a_4a3cba4_40cb306	--	--	0x9359a39_d450a12_51ce5bc_d3062b6_2c9cca3_c74edc4	0x3c3c3c3c (CP)	0xedf08af9
-1	--	0x0a935ea4f39e2b63	0xeff1213_e232b20_0064b82_ae1968a_4a3cba4_40cb306	--	--	0xeff1213_e232b20_0064b82_ae1968a_4a3cba4_40cb306	0x3c3c3c3c (CP)	0xb86284bb
0	130	0x0526b549e73c76c7	0xddd552f_3d3bac2_fb230d5_83a2d78_5a1da41_8fed1d6	--	--	0xddd552f_3d3bac2_fb230d5_83a2d78_5a1da41_8fed1d6	0xbcbcbcbc (BS)	0xb87439a6
1	131	0x0a4d6293ce78ed8e	0xc258963_5d097d0_e50aa7c_fc50f00_a2a747b_a45b784	--	--	0xc258963_5d097d0_e50aa7c_fc50f00_a2a747b_a45b784	0x39393939 (VB-ID)	0xf701f1ed
2	132	0x049ac5279cf1fb1c	0xb06e6b7_c8209e8_82982f7_4bc1a13_8a3f797_9f0446e	--	--	0xb06e6b7_c8209e8_82982f7_4bc1a13_8a3f797_9f0446e	0x00000000	0x523d121c
3	133	0x09358a4f31e3d639	0xefd27df_0e46509_e0b63da_cb3dc05_af53ae8_4436e20	--	--	0xefd27df_0e46509_e0b63da_cb3dc05_af53ae8_4436e20	0x00000000	0xf96f47ae
4	134	0x026b1c9e63c7ac73	0xc479a9c_8c09955_e4b84bc_f4d23b6_286c3cc_fbefcbb	--	--	0xc479a9c_8c0b955_e4b84bc_f4d23b6_286c3cc_fbefcbb	0x00000000	0xba695c5b
5	135	0x04d6313ccf8f58e6	0x6f9b366_49610cf_895c70f_eaf2c27_410aaa3_e0e83bf	--	--	0x6f9b366_6b432ed_895c70f_caf2c27_410aaa3_e0e83bf	0x00000000	0x1163a5e9
…	…	…	…	…	…	...	…	…
51	181	0x0934a6387ba6fed0	0xb39166a_8c1b092_9679527_b34e394_86a9ea3_8c0	--	--	0x01eab39_3961796_96cf800_65550a2_286c641_1cf5ec3		0xcdd5ddb2

			2b91					
52	182	0x02694c70f74ddda1	0x014c513_1161f8b_41c9b49_a64a8b3_0ad9135_6c6337b	--	--	0x88eca24_fa0719b_0e475ea_fd01238_77fac9c_2a2fe35		0x241e4836
53	183	0x04d290e1ee9bbb43	0x5f74778_7bae847_3858c2e_6d9a242_bc9a02f_e4fdf87	--	--	0x276fafa_fb8c5a8_95210b1_8d295f2_09e27e6_b737720		0x673be722
54	184	0x09a529c3d5375686	0x41c3db8_7e60b5d_ade6c26_0335bb1_0313ffb_ce6d556	--	--	0xde83510_f93dd7e_8f09cca_fd7e979_439879a_5870c89		0x0e661a04
55	185	0x034a5387aa6ead0c	0xda39225_0d2f8e6_487e46d_14adaff_c23321e_7e5a780	--	--	0x9fd4127_873eeab_d443857_d7bc533_04fa8ab_a4eee09		0xe8b7ea1e
56	186	0x0694af0f54dd7a18	0xb6bee9e_b0ef775_f7d10ad_5dce396_89b2597_acef7ea	--	--	0xd5858aa_e4354ca_b52fefd_c3e62de_3960ed5_cbc6aa5		0xac7e0ebc
57	187	0x0694af0f54dd7a18	0xb6bee9e_b0ef775_f7d10ad_5dce396_89b2597_acef7ea	--	--	0xed3734d_00d67e7_eb76874_e2d404c_09ed965_dc23211		0x233bf0c3
…	…	…	…	…	…	...		…
63	193	0x0694af0f54dd7a18	0xb6bee9e_b0ef775_f7d10ad_5dce396_89b2597_acef7ea	--	--	0x5b908ab_b2fdadc_ab7f84a_88d8992_bb6fc94_30a7b52		0xe228cfc1
64	194	0x0694af0f54dd7a18	0xb6bee9e_b0ef775_f7d10ad_5dce396_89b2597_acef7ea	--	--	0x9f12b63_096eeec_28e9b90_a572681_09e03f4_85a8ee3		0x681b908d
65	195	0x0694af0f54dd7a18	0xb6bee9e_b0ef775_f7d10ad_5dce396_89b2597_acef7ea	--	--	0xb6bee9e_b0ef775_f7d10ad_5dce396_89b2597_acef7ea		0xabaaaf5a
66	196	0x0d29561ea1bad430	0x0beb3a9_cb616c5_ce7a6d6_3ab9bdb_c93d31b_c325019	--	--	0x0beb3a9_cb616c5_ce7a6d6_3ab9bdb_c93d31b_c325019		0x0b6d3310
67	197	0x0a52a43d4b758861	0x6a3ad12_ba76634_6c93fda_c14a23d_fbc4d3f_cceecdf	--	--	0x6a3ad12_ba76634_6c93fda_c14a23d_fbc4d3f_cceecdf		0xcd7c74f2
…	…	…	…	…	…	...		…
124	254	0x0c4022556ebc0341	0x1b667c4_58eb259_02f8446_b23b297_c215fed_fd22fda	0x0e	0x12bc	0x1b667c4_58eb259_02f8446_b23b297_c215fed_fd22fda		0x7a0e12bc
125	255	0x08804caadd780683	0x7751c4f_88a7402_a3288f8_b80ca9b_4b8b5f3_b08	0xb0	0xb3e3	0x7751c4f_88a7402_a3288f8_b80ca9b_4b8b5f3_b08538d		0xe6b0b3e3

			538d					
126	256	0x01009955baf02d07	0xcf53cec_11815b0_a352099_3f388c8_06f5351_d175ff0	0x30	0x90f2	0xcf53cec_11815b0_a352099_3f388c8_06f5351_d175ff0		0xf23090f2
127	257	0x02013aab7de05a0e	0xfd6cff2_ca2c4c1_c6a57bd_3b7f137_153caea_632dfe8	0x78	0x7fea	0xfd6cff2_ca2c4c1_c6a57bd_3b7f137_153caea_632dfe8		0xa2787fea
128	258	0x04027d56f3c0b41d	0x7e0ae16_884db5b_0bb4b68_0a1e5f8_6c38195_ff4c09b	0x05	0x6ff8	0x7e0ae16_884db5b_0bb4b68_0a1e5f8_6c38195_ff4c09b		0xb1056ff8
129	259	0x0804f2adef81483b	0x9eb4b99_b784a43_554b033_5068a0a_3652f72_45e1b03	0x9b	0xb233	0x9eb4b99_b784a43_554b033_5068a0a_3652f72_45e1b03		0xe29bb233

Line Rekey Started

clk	Sym clk	LFSR[59:0]	BM0[167:0]	OF0[23:16]	OF0[15:0]	BM1[167:0]		OF1[31:0]
-3	--	0x02013aab7de05a0e	0xfd6cff2_ca2c4c1_c6a57bd_3b7f137_153caea_632dfe8	--	--	0xfd6cff2_ca2c4c1_c6a57bd_3b7f137_153caea_632dfe8		0xa2787fea
-2	--	0x04027d56f3c0b41d	0x7e0ae16_884db5b_0bb4b68_0a1e5f8_6c38195_ff4c09b	--	--	0x7e0ae16_884db5b_0bb4b68_0a1e5f8_6c38195_ff4c09b		0xb1056ff8
-1	--	0x0804f2adef81483b	0x9eb4b99_b784a43_554b033_5068a0a_3652f72_45e1b03	--	--	0x9eb4b99_b784a43_554b033_5068a0a_3652f72_45e1b03		0xe29bb233
0	260	0x0009e55bdf02b077	0x4f1e099_a2b74ae_ff04407_120488a_b50700b_222457c	--	--	0x4f1e099_a2b74ae_ff04407_120488a_b50700b_222457c		0x79a5b695
1	261	0x0013cab7b60560ee	0xb571a48_de0dd9f_5a6ff73_952d3a1_aab9a78_7471e75	--	--	0xb571a48_de0fd9f_5a6ff73_952d3a1_aab9a78_7471e75		0x17dd6489
2	262	0x00279d6f640ae1dc	0x7a6bb2e_a75b55c_37c1770_b0d6b2f_4e6afee_d50e89c	--	--	0x7a6bb2e_857b77e_37c1770_90d6b2f_4e6afee_d50e89c		0x755fc807
3	263	0x004f32dec015c3b8	0xfc07939_af0c1b8_71cb433_0779577_1ecf574_9025607	--	--	0x12e9737_16afa03_71cb433_06fd76f_1ecf574_b025617		0x8c8946a0
4	264	0x009e65bd882b8770	0x4ff8091_6006860_c4e3076_d086ea6_bc1f879_593445c	--	--	0xc77e8b5_7f6e971_e2fba8b_ae32d0c_bc1f879_82c76e5		0xc4b18b1c
5	265	0x013cc37b1857	0x7e07ee7_e4e846a_78e	--	--	0x19b4fec_f1da052_13fc123_5		0xa741e1

		0ee1	8ba2_37bd58e_6c416ac_fec4e39			af2f44_82af3cf_ec01ca2		6f
…	…	…	…	…	…	...		…
52	312	0x04b9d2c7b47e816b	0xf59c95c_6c60114_a0ea2c9_eee35b9_890c00c_bff87ce	--	--	0x9ffba7d_188e1c3_34acde5_0103c0b_d184884_a89b6be		0x79245d7b
53	313	0x0973a58f68fd02d7	0x3396d92_7255af2_45f81f1_e0d765a_0102d9b_ac54493	--	--	0x45a254d_26776d1_d2d9587_a82a8f2_185161e_a7f1a15		0x0870a024
54	314	0x02e74b1ed9fa25af	0x0b70acb_82f4411_565a3d6_4a7d35e_59a6d1e_ef722f1	--	--	0xf7df80c_00ede1b_ffe42ee_8b99e3f_8932320_d9d3dd1		0xf67191d1
55	315	0x05ce963db3f46b5e	0x6e3c514_ee4d3f3_890a5bc_03084a8_e35c763_d6bb076	--	--	0xd23eeed_19aa8d0_617d112_91d2beb_aca2095_a1f7124		0xa7a328be
56	316	0x0b9d2c7b67e8f6bc	0x071dfc0_354e724_e40ff24_0b318b0_ca51a40_42bfa96	--	--	0xa03ca96_b3df563_2ef6e35_7792de2_fe9e523_b833612		0x3dd32f99
57	317	0x0b9d2c7b67e8f6bc	0x071dfc0_354e724_e40ff24_0b318b0_ca51a40_42bfa96	--	--	0x27d81ed_ca59522_9b74336_b710ce3_53c46db_fa8cfee		0x14ffa1ea
58	318	0x0b9d2c7b67e8f6bc	0x071dfc0_354e724_e40ff24_0b318b0_ca51a40_42bfa96	--	--	0x8f943da_ac3a372_953b5a0_1f78ebd_55aa026_788de8d		0xa0123a84
…	…	…	…	…	…	...		…
63	323	0x0b9d2c7b67e8f6bc	0x071dfc0_354e724_e40ff24_0b318b0_ca51a40_42bfa96	--	--	0x0a5d925_9000dab_7d7b782_417ba72_a7d8586_76c45aa		0xf288b02a
64	324	0x0b9d2c7b67e8f6bc	0x071dfc0_354e724_e40ff24_0b318b0_ca51a40_42bfa96	--	--	0x79bf76f_974a606_8407397_ffb7192_eb3e6bd_9a15f60		0xda55bcea
…	…	…	…	…	…	...		…
125	385	0x0370a27349c2fa0d	0xcdaa576_8acd1db_09b8cc0_5d1e37e_1eca0aa_ac189e9	0x67	0xf889	0xcdaa576_8acd1db_09b8cc0_5d1e37e_1eca0aa_ac189e9		0x3867f889
126	386	0x06e14ce69b85d41b	0xdbf3f9d_c8bb867_8ad1d10_5f5a2fa_1343528_92f0cc5	0x07	0x585a	0xdbf3f9d_c8bb867_8ad1d10_5f5a2fa_1343528_92f0cc5		0xc507585a
127	387	0x0dc291cd3f0ba837	0xbf85399_7c62d4d_4179484_c87396b_60e4ecd_9eac5d6	0x49	0x751f	0xbf85399_7c62d4d_4179484_c87396b_60e4ecd_9eac5d6		0xb849751f

128	388	0x0b85239a7617706f	0x3937c9b_d05a356_afb6a43_d273cff_4d8b097_b323273	0x2b	0xfc4d	0x3937c9b_d05a356_afb6a43_d273cff_4d8b097_b323273		0x5f2bfc4d
129	389	0x070a4734e42ee0df	0xbd531a0_360f2df_08ef7f0_00750de_32420b7_9d378ed	0x6e	0x9e21	0xbd531a0_360f2df_08ef7f0_00750de_32420b7_9d378ed		0x016e9e21
Frame key calc started								
clk	**Sym clk**	**LFSR[59:0]**	**BM0[167:0]**	**OF0[23:16]**	**OF0[15:0]**	**BM1[167:0]**		**OF1[31:0]**
-3	--	--	0xbf85399_7c62d4d_4179484_c87396b_60e4ecd_9eac5d6	--	--	0xbf85399_7c62d4d_4179484_c87396b_60e4ecd_9eac5d6		0xb849751f
-2	--	--	0x3937c9b_d05a356_afb6a43_d273cff_4d8b097_b323273	--	--	0x3937c9b_d05a356_afb6a43_d273cff_4d8b097_b323273		0x5f2bfc4d
-1	--	--	0xbd531a0_360f2df_08ef7f0_00750de_32420b7_9d378ed	--	--	0xbd531a0_360f2df_08ef7f0_00750de_32420b7_9d378ed		0x016e9e21
0	390	--	0x72473bf_324cce4_1d2560b_ac4198f_651748b_9eb7055	--	--	0x72473bf_324cce4_1d2560b_ac4198f_651748b_9eb7055		0xa5df2d60
1	391	--	0xc040e35_54294b7_0000000_7a3b0f9_42b1dbd_000006a	--	--	0x17503c8_29e61e0_67bf333_fb74227_bb68977_899974e		0x52bd3e31
2	392	--	0x6666a4e_47b5444_93d46aa_e4f374f_3cd0333_212d6ab	--	--	0xc73ae79_60221ba_a726ab3_73e9bda_d2e8ac7_b79689d		0xf3f00968
3	393	--	0x1232d67_ef6a7a5_6055678_d509b9f_427d387_e30af77	--	--	0x65b6ed7_bdc9a5e_b2a83ab_e7a2797_2b7f24f_676ccee		0x3d50cd7b
4	394	--	0x811566c_da14697_66f89db_84306fe_411d172_f9e3620	--	--	0x8927e15_093e591_c9d46f4_668739d_100edf2_782f7cb		0x6741e45f
5	395	--	0xf7027a4_dc24164_29716cf_f0cd06e_9fad21f_41cbe85	--	--	0x4b70562_37d2a78_2181422_e41f4f6_68921b1_6f026ea		0xeb20d359
…	…	…	…	…	…	...		…
45	435	--	0x8b0a742_b70da1c_2307640_c1ee9ee_710c4ce_f33ab64	--	--	0x7fe0102_09ec9bb_ce7b6aa_3f56579_c1ba5b0_9b5151d		0xdfd6149a
46	436	--	0x57dd199_d4f7e9b_b8	--	--	0x1c56325_e09d161_548802d		0xc61874

			5862b_d828b51_45921f8_f6be033			_ad80fbe_35d3929_f6c52d3		e5
47	437	--	0xc9472f7_c4371c6_667db05_a78da80_06664cc_375232b	--	--	0x2b49ba1_acafeaa_75b2c1e_3dd8850_0e03b41_816b993		0x0d87b6a5
48	438	--	0x2aeaf01_beef443_e0cd9a0_314db4f_985f085_e1aad05	--	--	0x0aff5b0_6cbc6c8_2c51392_5a4c178_2e2fc97_23ecb68		0xa799beaf
49	439	--	0x5cfb3bd_bb2e5ca_6f52793_70ae71a_2363694_1dad643	--	--	0xae7c618_dd136c4_6fc3f82_4a77f73_a35b75a_9eb2552		0xe94a7b50
50	440	0x091b19a51e15d71a	0x70ae71a_2363694_1dad643_7a3b0f9_42b1dbd_000006a	--	--	0xd3311c3_dc116ea_b92c13e_23af089_d963d43_1b25caf		0x72f0e07c
51	441	0x02363b4a3c2bae34	0xdbbdf28_dc37a1f_69aaca3_8d3b596_3cd0333_212d6ab	--	--	0x9e04483_9b47d49_35583ce_059fc36_c059e2f_d3f8296		0x0e9afbb8
…	…	…	…	…	…	...		…
105	495	0x060dc32a9f1ba948	0x45f1415_2da6811_2f9f883_8209d00_9abfc87_8c37ee0	0xec	0x7097	0x2ea28c3_fec180d_9139bcd_0d1a0c5_e63dd03_77f97e3		0xbce9ce6f
106	496	0x0c1b86553e377291	0x60802d3_082166d_6655d80_cb50245_8159b67_a5d1bde	0x83	0x2c89	0xa8a5563_e7ed957_50208d4_2fabfd0_48d5bdf_c829d70		0x3e33dd3f
107	497	0x0c1b86553e377291	0x60802d3_082166d_6655d80_cb50245_8159b67_a5d1bde	0x83	0x2c89	0x3b29cd7_d0e8d7c_c4c9d46_6859044_f28094d_d6fced8		0xb670eebd
108	498	0x0c1b86553e377291	0x60802d3_082166d_6655d80_cb50245_8159b67_a5d1bde	0x83	0x2c89	0xd5b76e5_4be2a76_89f31ba_e273edf_2f25fc9_eaafc72		0x952dd8aa
…	…	…	…	…	…	...		…
128	518	0x0c1b86553e377291	0x60802d3_082166d_6655d80_cb50245_8159b67_a5d1bde	0x83	0x2c89	0x1884068_7245b82_c46c5d5_750e16d_1f556cf_aab8509		0x58acda63
129	519	0x0c1b86553e377291	0x60802d3_082166d_6655d80_cb50245_8159b67_a5d1bde	0x83	0x2c89	0x60802d3_082166d_6655d80_cb50245_8159b67_a5d1bde		0x60832c89
Line Rekey Started								
clk	**Sym clk**	**LFSR[59:0]**	**BM0[167:0]**	**OF0[23:16]**	**OF0[15:0]**	**BM1[167:0]**		**OF1[31:0]**
-3	--	0x0c1b86553e377291	0x60802d3_082166d_6655d80	--	--	0xbeacd59_1a2511e_e26e9ff_fc2a039_4d7b9e0_96bf704		0x063a4d37

			_cb50245_8159b67_a5d1bde					
-2	--	0x0c1b86553e377291	0x60802d3_082166d_6655d80_cb50245_8159b67_a5d1bde	--	--	0x1884068_7245b82_c46c5d5_750e16d_1f556cf_aab8509		0x58acda63
-1	--	0x0c1b86553e377291	0x60802d3_082166d_6655d80_cb50245_8159b67_a5d1bde	--	--	0x60802d3_082166d_6655d80_cb50245_8159b67_a5d1bde		0x60832c89
0	520	0x083704aa746ee522	0x08c4020_30bc948_6b8a961_886718e_b4a6082_0074526	--	--	0x08c4020_30bc948_6b8a961_886718e_b4a6082_0074526		0x1a40be67
1	521	0x006e0154e0ddca44	0x5af75fe_5953161_a0038b7_c87ac01_cc9c416_9af5207	--	--	0x5af75fe_5953161_a0038b7_c87ac01_cc9c416_9af5207		0x3760f82a
2	522	0x00dc0aa9c9bbb488	0x1085a0e_5352770_6668fe6_e6ff8ab_9829251_b22863b	--	--	0x1085a0e_5350770_6668fe6_e6ff8ab_9829251_b22863b		0xe19de0a8
3	523	0x01b8155393776910	0x6fa6d38_71d9ac4_a0fab91_69d6700_99b4c1b_9e28386	--	--	0x6fa6d38_53f98e6_a0fab91_49d6700_99b4c1b_9e28386		0xe6c5c4b3
…	…	…	…	…	…	...		…
55	575	0x0a0644e20872e9ad	0xf99f5c2_06270a5_7ded43b_103d361_85052da_3ca9e17	--	--	0x78679c2_7b92110_188ac5f_95772f0_764392c_a1cef59		0x32a975a1
56	576	0x040c81c418e5f35b	0x7886306_1252fd3_da4da02_419a2fc_334d491_dc16b5b	--	--	0xead9731_4064062_364c15e_c48384b_2d20f54_de16319		0x4c15e552
57	577	0x040c81c418e5f35b	0x7886306_1252fd3_da4da02_419a2fc_334d491_dc16b5b	--	--	0x33e2803_a8be6fa_ff005bf_8c88d28_3e9f26f_e35ae7d		0xbb310e11
58	578	0x040c81c418e5f35b	0x7886306_1252fd3_da4da02_419a2fc_334d491_dc16b5b	--	--	0xa575b19_fd01fec_7a5a1dd_72cc751_302ce1d_af7d850		0xfd1aa71e
…	…	…	…	…	…	...		…
63	583	0x040c81c418e5f35b	0x7886306_1252fd3_da4da02_419a2fc_334d491_dc16b5b	--	--	0x2e017aa_94c93a9_b6a6fd3_9b64d35_89060ef_80cb85e		0x85d9c9b3
64	584	0x040c81c418e5f35b	0x7886306_1252fd3_da4da02_419a2fc_334d491_dc16b5b	--	--	0x44be25d_9fd286e_8e7fe89_b4470c4_fca81db_cf9fb85		0x68e0ea10
65	585	0x040c81c418e5f35b	0x7886306_1252fd3_da4da02	--	--	0x7886306_1252fd3_da4da02_419a2fc_334d491_dc16b5b		0x35572896

			_419a2fc_334d491_dc16b5b					
66	586	0x08190b8831cbc6b7	0xf3ffda5_59a8a35_55eadab_4b5c391_88699f4_c0c8eef	--	--	0xf3ffda5_59a8a35_55eadab_4b5c391_88699f4_c0c8eef		0x66737ce1
…	…	…	…	…	…	...		…
128	648	0x01a36ffb53321085	0x4068890_a51fbf1_414a524_280ec4e_a279d5c_e73e041	0x4c	0x3ac8	0x4068890_a51fbf1_414a524_280ec4e_a279d5c_e73e041		0xb84c3ac8
129	649	0x0346dff6a664010b	0x8380d0e_1f7cd07_dc77025_53d2eae_c16a800_6b31ba5	0x0c	0x1e28	0x8380d0e_1f7cd07_dc77025_53d2eae_c16a800_6b31ba5		0x850c1e28

Line Rekey Started

clk	Sym clk	LFSR[59:0]	BM0[167:0]	OF0[23:16]	OF0[15:0]	BM1[167:0]		OF1[31:0]
-3	--	0x00d1b3fdad991842	0x48e7c33_ef04d77_8a947c2_a40f5fc_51c2c8b_4d2ff08	--	--	0x48e7c33_ef04d77_8a947c2_a40f5fc_51c2c8b_4d2ff08		0x0a82caf4
-2	--	0x01a36ffb53321085	0x4068890_a51fbf1_414a524_280ec4e_a279d5c_e73e041	--	--	0x4068890_a51fbf1_414a524_280ec4e_a279d5c_e73e041		0xb84c3ac8
-1	--	0x0346dff6a664010b	0x8380d0e_1f7cd07_dc77025_53d2eae_c16a800_6b31ba5	--	--	0x8380d0e_1f7cd07_dc77025_53d2eae_c16a800_6b31ba5		0x850c1e28
0	650	0x068db7ed44c82217	0xf2bb890_3ea29ff_ed6af5f_5ef77c9_3b3308a_f7842b4	--	--	0xf2bb890_3ea29ff_ed6af5f_5ef77c9_3b3308a_f7842b4		0x623c1430
1	651	0x0d1b67da8190442f	0xe039b17_d2a806b_d6572dd_c1b67aa_0052141_5f600ae	--	--	0xe039b17_d2aa06b_d6572dd_c1b67aa_0052141_5f600ae		0xddaafc51
2	652	0x0a36cfb50b20a85f	0xf7a4696_ecfb5a3_9b7c296_5e80f87_2627aa3_4a96e73	--	--	0xf7a4696_cedb781_9b7c296_7e80f87_2627aa3_4a96e73		0x34c8387f
…	…	…	…	…	…	...		…
55	705	0x0bf3176d8e362cbe	0x2c2e73c_c07af5b_8b1d888_4ecdbdc_71de587_08cc449	--	--	0xc3c4e1e_92f3535_3ff5265_4d42754_54fbf8d_ee829c7		0xac1a6dc5
56	706	0x07e62edb1c6c597c	0xf9f65dd_b706dd2_75aa989_25cd567_d80c19f_c40ac69	--	--	0xad409c1_07a1bc8_c1fe768_67706de_7abc742_860407a		0xa8304199
57	707	0x07e62edb1c6c597c	0xf9f65dd_b706dd2_75aa989_25cd567_d80c19f_c40a	--	--	0x5e76131_95d7447_2740077_0227f05_9d059d9_234c6f4		0x57e84b6e

			c69					
58	708	0x07e62edb1c6c597c	0xf9f65dd_b706dd2_75aa989_25cd567_d80c19f_c40ac69	--	--	0xed349f1_23b7a22_3dc6aab_391ac55_2e45f61_3feffd9		0x01c6dd74
…	…	…	…	…	…	...		…
63	713	0x07e62edb1c6c597c	0xf9f65dd_b706dd2_75aa989_25cd567_d80c19f_c40ac69	--	--	0xc3526b0_349c3ff_cb1c4ec_97000f3_75697f8_88011ec		0x8dbb96a2
64	714	0x07e62edb1c6c597c	0xf9f65dd_b706dd2_75aa989_25cd567_d80c19f_c40ac69	--	--	0x0f0358a_8ff7cc3_33c4eab_54dcc1f_db33fcc_40fda8d		0x097fca8f
65	715	0x07e62edb1c6c597c	0xf9f65dd_b706dd2_75aa989_25cd567_d80c19f_c40ac69	--	--	0xf9f65dd_b706dd2_75aa989_25cd567_d80c19f_c40ac69		0x9a523c3c
66	716	0x0fcc55b630d892f9	0xc625801_b74ff0e_e0ac6b4_717f03f_d8ae9fb_2195879	--	--	0xc625801_b74ff0e_e0ac6b4_717f03f_d8ae9fb_2195879		0xf3f5be6c
…	…	…	…	…	…	...		…
128	778	0x0fc4084e4d5a4e04	0xa83ba29_272d608_d0f1db1_318f4b5_1c140ef_cd8317e	0xe3	0xb616	0xa83ba29_272d608_d0f1db1_318f4b5_1c140ef_cd8317e		0xf0e3b616
129	779	0x0f88109c9ab4bc09	0x90a9d7c_55dffee_8e07cdc_e758d7c_2175036_b19d4aa	0x68	0x2b8a	0x90a9d7c_55dffee_8e07cdc_e758d7c_2175036_b19d4aa		0xff682b8a

Frame key calc started

clk	Sym clk	LFSR[59:0]	BM0[167:0]	OF0[23:16]	OF0[15:0]	BM1[167:0]		OF1[31:0]
-3	--	--	0xc51f17e_201434d_a318c59_c85b7d1_a839945_13b6f66	--	--	0xc51f17e_201434d_a318c59_c85b7d1_a839945_13b6f66		0x29b5de9c
-2	--	--	0xa83ba29_272d608_d0f1db1_318f4b5_1c140ef_cd8317e	--	--	0xa83ba29_272d608_d0f1db1_318f4b5_1c140ef_cd8317e		0xf0e3b616
-1	--	--	0x90a9d7c_55dffee_8e07cdc_e758d7c_2175036_b19d4aa	--	--	0x90a9d7c_55dffee_8e07cdc_e758d7c_2175036_b19d4aa		0xff682b8a
0	780	--	0x8cdb786_0fde267_eea1746_c771efb_cffca87_2cf8884	--	--	0x8cdb786_0fde267_eea1746_c771efb_cffca87_2cf8884		0x574a71f3
1	781	--	0xc040e35_54294b7_0000000_3527097_5f70fcc_0000	--	--	0xb75dced_9a84a0b_b096d5d_ca15b00_6f3facf_081dea1		0x252a4f7c

			04b					

Table B-26. Cipher State in SST mode for 4-lane, Inter-BS Spacing = 130

Sym clk	stream	OF1[31:0]	encrypted stream
-3	0x1c1c1c1c	0x6559c03e	0x1c1c1c1c
-2	0x3c3c3c3c	0x6559c03e	0x3c3c3c3c
-1	0x3c3c3c3c	0x6559c03e	0x3c3c3c3c
0	0x1c1c1c1c	0x6559c03e	0x1c1c1c1c
1	0x39393939	0xb79ee5fe	0x8ea7dcc7
2	0x00000000	0x289af919	0x289af919
3	0x00000000	0xd25b5d6c	0xd25b5d6c
4	0x00000000	0xed55dcde	0xed55dcde
5	0x00000000	0xe4e58763	0xe4e58763
…	…	…	…
45	0x00000000	0x10f21d66	0x10f21d66
46	0x00000000	0x37affe86	0x37affe86
47	0x00000000	0x49152bc4	0x49152bc4
48	0x00000000	0x1f068148	0x1f068148
49	0x00000000	0xb79cb954	0xb79cb954
50	0x00000000	0xfe492f2a	0xfe492f2a
51	0x00000000	0x53331e18	0x53331e18
52	0x00000000	0x5c0e4039	0x5c0e4039
…	…	…	…
104	0x00000000	0x1d74baa3	0x1d74baa3
105	0x00000000	0xd8835587	0xd8835587
106	0x00000000	0xaf70715f	0xaf70715f
107	0x00000000	0xc861665f	0xc861665f
108	0x00000000	0x2bbcf09a	0x2bbcf09a
…	…	…	…
128	0x3c3c3c3c	0xedf08af9	0x3c3c3c3c
129	0x3c3c3c3c	0xb86284bb	0x3c3c3c3c
130	0xbcbcbcbc	0xb87439a6	0xbcbcbcbc
131	0x39393939	0xf701f1ed	0xce38c8d4
132	0x00000000	0x523d121c	0x523d121c
133	0x00000000	0xf96f47ae	0xf96f47ae
134	0x00000000	0xba695c5b	0xba695c5b
135	0x00000000	0x1163a5e9	0x1163a5e9

Table B-27. 4-lane Encrypted Output in SST mode for Inter-BS Spacing = 130

Test Vectors for 4-Lane Main Link Configuration in SST Mode (Inter-BS spacing = 131, CPSR Interval = 3)

Authentication

Table B-3 and Table B-4 provide the LFSR and Block module states during the first part of authentication.

Initial Bootstrapping

Table B-25 provides test vectors during the initial bootstrapping operation.

After start of encryption

Table B-28 provides test vectors generated after the start of encryption (beginning with the first CPSR symbol set that triggers encryption). Table B-29 provides encrypted cipher outputs.

clk	Sym clk	LFSR[59:0]	BM0[167:0]	OF0[23:16]	OF0[15:0]	BM1[167:0]	OF1[31:0]
Frame key calc started							
-3	--	--	0xd20317a_3725bc8_256af5e_6b9cc06_7d7aa18_87f9092	--	--	0xd20317a_3725bc8_256af5e_6b9cc06_7d7aa18_87f9092	0x6559c03e
-2	--	--	0xd20317a_3725bc8_256af5e_6b9cc06_7d7aa18_87f9092	--	--	0xd20317a_3725bc8_256af5e_6b9cc06_7d7aa18_87f9092	0x6559c03e
-1	--	--	0xd20317a_3725bc8_256af5e_6b9cc06_7d7aa18_87f9092	--	--	0xd20317a_3725bc8_256af5e_6b9cc06_7d7aa18_87f9092	0x6559c03e
0	0	--	0xd20317a_3725bc8_256af5e_6b9cc06_7d7aa18_87f9092	--	--	0xd20317a_3725bc8_256af5e_6b9cc06_7d7aa18_87f9092	0x6559c03e
1	1	--	0xc040e35_54294b7_0000000_f523e56_bf44e50_000001d	--	--	0x9b48c65_3f7de85_4cfb937_50d9c10_5d7fbdc_6a03908	0xb79ee5fe
2	2	--	0x6666a4e_47b5444_93d46aa_a1a9cb4_a206aaa_cacfa30	--	--	0x94ede66_8141634_5f900d1_5f7a0f0_f291dcb_5a0ce6e	0x289af919
3	3	--	0x1232d67_ef6a7a5_6055678_533e54c_e4b418a_91fbcbb	--	--	0x1f69314_9a31990_c4b92db_31a6525_6ab1304_928c3d8	0xd25b5d6c
4	4	--	0x811566c_da14697_66f89db_d9ce46b_c89e263_9e3097e	--	--	0x7f0a70c_d1bda54_34c9929_7df4b37_d8d588c_855d111	0xed55dcde
…	…	…	…	…	…	…	…
46	46	--	0x57dd199_d4f7e9b_b85862b_5cc55f4_2b5efea_85611ff	--	--	0x2789d57_f53ee8a_3cfeaf5_817480c_c30af76_2f49767	0x37affe86
47	47	--	0xc9472f7_c4371c6_667db05_9e19673_1fcfb80_9e1665f	--	--	0xfa07250_f725212_9bc279d_76fe61a_e1521fc_fb331b7	0x49152bc4
48	48	--	0x2aeaf01_beef443_e0cd9a0_d83548d_480c50a_5d4ed0e	--	--	0xcaf5121_1129806_3836e0a_9051c5e_34551ae_7f7b35a	0x1f068148
49	49	--	0x5cfb3bd_bb2e5ca_6f52793_8bb82fe_ea7c29	--	--	0x62e765a_09101ee_f92cab1_4cfd7ca_f8ad063	0xb79cb954

			8_d9a59fa			_1f97804	
50	50	0x0f53e0a6257702fe	0x8bb82fe_ea7c298_d9a59fa_f523e56_bf44e50_000001d	--	--	0x960d99e_e9b8b0f_782d158_645c7a9_312615f_ca46465	0xfe492f2a
51	51	0x0ea7c94c42ee05fd	0xb486149_cca6e3d_0355dff_2262329_a206aaa_cacfa30	--	--	0xb72431d_495f294_aba13a4_c1a5edc_d8ea59b_2cbcad0	0x53331e18
52	52	0x0d4f929885dc0bfb	0x120ec20_a1030d1_4c72806_a00fb45_e4b418a_75af954	--	--	0xe94a5e8_bad382a_b516ee3_2aea12a_04f35e9_6a44723	0x5c0e4039
…	…	…	…	…	…	…	…
101	101	0x08549a75241cec5b	0x283bb5d_356dc1d_5ef8302_740b636_1e2bbb1_77a9024	--	--	0x06af6be_8574776_6244dc1_1c04bf2_7da1a03_e962e82	0x96fc2396
102	102	0x00a934ea4839f8b6	0xd1bdb61_18b2c89_06d55fe_85d7861_4a2d2c4_3f0f76a	--	0x6a42	0x8000eaf_8f340fb_57fba9a_ece383b_5d4ccf2_e2ff34b	0xbc51d239
103	103	0x015269d49873d16c	0xabddb90_19d2b4a_7540b7a_458c215_014c756_aca7735	--	0xb1db	0x394e745_ec99143_e3f8f19_375ec6c_39c7cef_ba78801	0x8908e8ac
104	104	0x02a4d3a938e782d8	0x924eb87_b7a728b_8f829c6_35dd971_63da5b0_486ff01	0x97	0xd7a3	0x398cfb0_51408ef_9500162_a935d4f_835f420_da99144	0x1d74baa3
105	105	0x0549af5279cf05b1	0x711d28b_ffa6fca_923e67b_15707a7_42a4bb2_2deda6d	0xbb	0xb0f9	0xde9d7c1_83df898_1e55332_ddc9add_a82acb2_2885c03	0xd8835587
106	106	0x0a935ea4f39e2b63	0xeff1213_e232b20_0064b82_ae1968a_4a3cba4_40cb306	0x62	0x84bb	0xd887f8b_5d37e0d_fe4d145_6a55c77_9369bfb_5028d20	0xaf70715f
107	107	0x0a935ea4f39e2b63	0xeff1213_e232b20_0064b82_ae1968a_4a3cba4_40cb306	0x62	0x84bb	0xb77f694_6fed836_ec5fbda_befa034_2c5d690_ae478e9	0xc861665f
108	108	0x0a935ea4f39e2b63	0xeff1213_e232b20_0064b82_ae1968a_4a3cba4_40cb306	0x62	0x84bb	0xa67d45e_0b30f7d_2bb93be_e09b5f5_22ca847_b849198	0x2bbcf09a
…	…	…	…	…	…	…	…
127	127	0x0a935ea4f39e2b63	0xeff1213_e232b20_0064b82_ae1968a_4a3cba4_40cb306	0x62	0x84bb	0x6886c93_2065e45_773f684_82237f8_df3ef7a_cae90a7	0xc07ece76
128	128	0x0a935ea4f39e2b63	0xeff1213_e232b20_0064b82_ae1968a_4a3cba4_40cb306	0x62	0x84bb	0x9359a39_d450a12_51ce5bc_d3062b6_2c9cca3_c74edc4	0xedf08af9
129	129	0x0a935ea4f39e2b63	0xeff1213_e232b20_0064b82_ae1968a_4a3cba4_40cb306	0x62	0x84bb	0xeff1213_e232b20_0064b82_ae1968a_4a3cba4_40cb306	0xb86284bb
130	130	0x0526b549e73c76c7	0xddd552f_3d3bac2_fb230d5_83a2d78_5a1da41_8fed1d6	0x74	0x39a6	0xddd552f_3d3bac2_fb230d5_83a2d78_5a1da41_8fed1d6	0xb87439a6
Line rekey started							

clk	Sym clk	LFSR[59:0]	BM0[167:0]	OF0[23:16]	OF0[15:0]	BM1[167:0]	OF1[31:0]
-3	--	0x0a935ea4f39e2b63	0xeff1213_e232b20_0064b82_ae1968a_4a3cba4_40cb306	--	--	0x9359a39_d450a12_51ce5bc_d3062b6_2c9cca3_c74edc4	0xedf08af9
-2	--	0x0a935ea4f39e2b63	0xeff1213_e232b20_0064b82_ae1968a_4a3cba4_40cb306	--	--	0xeff1213_e232b20_0064b82_ae1968a_4a3cba4_40cb306	0xb86284bb
-1	--	0x0526b549e73c76c7	0xddd552f_3d3bac2_fb230d5_83a2d78_5a1da41_8fed1d6	--	--	0xddd552f_3d3bac2_fb230d5_83a2d78_5a1da41_8fed1d6	0xb87439a6
0	131	0x0a4d6293ce78ed8e	0xc258963_5d097d0_e50aa7c_fc50f00_a2a747b_a45b784	--	--	0xc258963_5d097d0_e50aa7c_fc50f00_a2a747b_a45b784	0xf701f1ed
1	132	0x049ac5279cf1fb1c	0xb06e6b7_c8209e8_82982f7_4bc1a13_8a3f797_9f0446e	--	--	0xb06e6b7_c8209e8_82982f7_4bc1a13_8a3f797_9f0446e	0x523d121c
2	133	0x09358a4f31e3d639	0xefd27df_0e46509_e0b63da_cb3dc05_af53ae8_4436e20	--	--	0xefd27df_0e46509_e0b63da_cb3dc05_af53ae8_4436e20	0xf96f47ae
…	…	…	…	…	…	…	…
54	185	0x034a5387aa6ead0c	0xda39225_0d2f8e6_487e46d_14adaff_c23321e_7e5a780	--	--	0x9fd4127_873eeab_d443857_d7bc533_04fa8ab_a4eee09	0xe8b7ea1e
55	186	0x0694af0f54dd7a18	0xb6bee9e_b0ef775_f7d10ad_5dce396_89b2597_acef7ea	--	--	0xd5858aa_e4354ca_b52fefd_c3e62de_3960ed5_cbc6aa5	0xac7e0ebc
56	187	0x0d29561ea1bad430	0x0beb3a9_cb636c5_ce7a6d6_3ab9bdb_c93d31b_c325019	--	--	0xed3734d_00d67e7_eb76874_e2d404c_09ed965_dc23211	0x233bf0c3
57	188	0x0d29561ea1bad430	0x0beb3a9_cb636c5_ce7a6d6_3ab9bdb_c93d31b_c325019	--	--	0xe17cdec_bc66357_8450c0e_5f72374_878db0c_6b13d1e	0x16208c84
58	189	0x0d29561ea1bad430	0x0beb3a9_cb636c5_ce7a6d6_3ab9bdb_c93d31b_c325019	--	--	0x55182ed_d8e05f7_37f417a_14ed44b_585f76b_94900de	0x2acbe06b
…	…	…	…	…	…	…	…
63	194	0x0d29561ea1bad430	0x0beb3a9_cb636c5_ce7a6d6_3ab9bdb_c93d31b_c325019	--	--	0x9f12b63_096eeec_28e9b90_a572681_09e03f4_85a8ee3	0x681b908d
64	195	0x0d29561ea1bad430	0x0beb3a9_cb636c5_ce7a6d6_3ab9bdb_c93d31b_c325019	--	--	0xfb4bddb_29ecd93_fee8c9d_9cef79d_167d4b2_7c33f78	0x3792bbc6
65	196	0x0d29561ea1bad430	0x0beb3a9_cb636c5_ce7a6d6_3ab9bdb_c93d31b_c325019	--	--	0x0beb3a9_cb636c5_ce7a6d6_3ab9bdb_c93d31b_c325019	0x0b653310
66	197	0x0a52a43d4b758861	0x6a3ad12_9854416_6c93fda_e14a23d_fbc4d3f_cceecdf	--	--	0x6a3ad12_9854416_6c93fda_e14a23d_fbc4d3f_cceecdf	0xc63474f4
	198			--	--		

67		0x04a5487a96eb30c2	0x6a9b47c_10a122e_494b633_ea430af_69d5a81_2aca65b			0x6a9b47c_10a122e_494b633_ea430af_69d5a81_2aca65b	0x9832c3f5
…	…	…	…	…	…	…	…
128	259	0x0804f2adef81483b	0x18f62ce_bba01f6_e05873b_02e1453_6d3fe03_73ffb2f	0x35	0x25c9	0x18f62ce_bba01f6_e05873b_02e1453_6d3fe03_73ffb2f	0x1a3525c9
129	260	0x0009e55bdf02b077	0x5cca5a8_2556f38_721cd54_ed0a7be_b322447_d4b665c	0xf6	0x02fc	0x5cca5a8_2556f38_721cd54_ed0a7be_b322447_d4b665c	0x94f602fc
130	261	0x0013cab7b60560ee	0xf76f879_1fbb56b_258f91d_e102fc0_cd59d02_20a20c1	0xdf	0xb4a0	0xf76f879_1fbb56b_258f91d_e102fc0_cd59d02_20a20c1	0xf4dfb4a0
Line rekey started							
clk	**Sym clk**	**LFSR[59:0]**	**BM0[167:0]**	**OF0[23:16]**	**OF0[15:0]**	**BM1[167:0]**	**OF1[31:0]**
-3	--	0x0804f2adef81483b	0x18f62ce_bba01f6_e05873b_02e1453_6d3fe03_73ffb2f	--	--	0x18f62ce_bba01f6_e05873b_02e1453_6d3fe03_73ffb2f	0x1a3525c9
-2	--	0x0009e55bdf02b077	0x5cca5a8_2556f38_721cd54_ed0a7be_b322447_d4b665c	--	--	0x5cca5a8_2556f38_721cd54_ed0a7be_b322447_d4b665c	0x94f602fc
-1	--	0x0013cab7b60560ee	0xf76f879_1fbb56b_258f91d_e102fc0_cd59d02_20a20c1	--	--	0xf76f879_1fbb56b_258f91d_e102fc0_cd59d02_20a20c1	0xf4dfb4a0
0	262	0x00279d6f640ae1dc	0x6491309_60f1012_d89dda7_994dc10_1d81194_a40a9ad	--	--	0x6491309_60f1012_d89dda7_994dc10_1d81194_a40a9ad	0x7df38818
1	263	0x004f32dec015c3b8	0x2f00991_88b8ef3_d667e82_a5b9bb7_0560435_9b9bc8b	--	--	0x2f00991_88b8ef3_d667e82_a5b9bb7_0560435_9b9bc8b	0xac45cfc9
2	264	0x009e65bd882b8770	0xd593def_28df9c5_04400b6_28ac3dd_309251c_91c3e34	--	--	0xd593def_28df9c5_04400b6_28ac3dd_309251c_91c3e34	0x12cdbee2
3	265	0x013cc37b18570ee1	0xabfc938_a7ed2ab_e658839_e80f130_05a2b26_b4a61e2	--	--	0xabfc938_a7ef2ab_e658839_e80f130_05a2b26_b4a61e2	0xafa34d79
…	…	…	…	…	…	…	…
54	316	0x0b9d2c7b67e8f6bc	0x6166a88_00c3a25_9f3dcbc_9f6f98d_c2465b1_3df1304	--	--	0x7128dc9_245f95c_e0190b2_4e296e5_d109dfe_2710abf	0x0e6838fb
55	317	0x073a50f6cfd1cd79	0xcb9ffcc_292b4c9_6a4747a_9a333fa_53b4ecd_2ebb6dc	--	--	0x5cc53c7_94bff90_cf33d37_3128cf9_5aa347c_902fdf9	0x05ff9298
56	318	0x0e74a1ed97a39af3	0xd048d69_884d2ce_e671d9e_dcdeb87_e721961_cb66cce	--	--	0x782d24c_2eca09c_752fcd8_7af4352_21844d5_51f9a5e	0x0ca02623
57	319	0x0e74a1ed97a39af3	0xd048d69_884d2ce_e671d9e_dcdeb87_e721961_cb66cce	--	--	0xf52893f_01626e7_1542cc1_1dd1b6d_32d6c9b_fa4305e	0xf6eee95b

…	…	…	…	…	…	…	…
63	325	0x0e74a1ed97a39af3	0xd048d69_884d2ce_e671d9e_dcdeb87_e721961_cb66cce	--	--	0xa5faffd_4eebb6d_a560f00_0c59adc_15aaee0_b8c79cc	0x90751aad
64	326	0x0e74a1ed97a39af3	0xd048d69_884d2ce_e671d9e_dcdeb87_e721961_cb66cce	--	--	0x8a4e6e8_b4b4209_9e39b2d_807d57e_82442fd_809bdcd	0x8dfb61d3
65	327	0x0e74a1ed97a39af3	0xd048d69_884d2ce_e671d9e_dcdeb87_e721961_cb66cce	--	--	0xd048d69_884d2ce_e671d9e_dcdeb87_e721961_cb66cce	0xadd3be2e
66	328	0x0ce943db2f4735e6	0x08dd310_dc83766_8e941fe_36e2c08_b5be35c_e03509c	--	--	0x08dd310_dc83766_8e941fe_36e2c08_b5be35c_e03509c	0x2a87a224
67	329	0x09d287b65e8e4bcd	0x275df3a_da41d84_acc2987_84a2d2d_052e2c9_15b23ec	--	--	0x275df3a_da41d84_acc2987_84a2d2d_052e2c9_15b23ec	0x8d12a9e0
…	…	…	…	…	…	…	…
127	389	0x070a4734e42ee0df	0x2aa1c09_89b38b3_80bbcc7_72afcf4_c21df7b_2b647e0	0xac	0xabe3	0x2aa1c09_89b38b3_80bbcc7_72afcf4_c21df7b_2b647e0	0x0bacabe3
128	390	0x0e148e69c05de1bf	0x002e137_c6bda63_92a289f_4a16efb_0ebf9d3_0158813	0x71	0x1f0e	0x002e137_c6bda63_92a289f_4a16efb_0ebf9d3_0158813	0x05711f0e
129	391	0x0c291cd380bbc37e	0xffc428c_4e594e1_59eaa16_c8677fb_7b02b5f_2fe0084	0xb5	0xc320	0xffc428c_4e594e1_59eaa16_c8677fb_7b02b5f_2fe0084	0x6ab5c320
130	392	0x085231a70177a6fc	0x5b61a07_13d4cb5_c7a21e0_6ad1270_2f1daa3_81176f2	0x51	0x2db0	0x5b61a07_13d4cb5_c7a21e0_6ad1270_2f1daa3_81176f2	0x1e512db0
Frame key calc started							
clk	**Sym clk**	**LFSR[59:0]**	**BM0[167:0]**	**OF0[23:16]**	**OF0[15:0]**	**BM1[167:0]**	**OF1[31:0]**
-3	--	--	0x002e137_c6bda63_92a289f_4a16efb_0ebf9d3_0158813	--	--	0x002e137_c6bda63_92a289f_4a16efb_0ebf9d3_0158813	0x05711f0e
-2	--	--	0xffc428c_4e594e1_59eaa16_c8677fb_7b02b5f_2fe0084	--	--	0xffc428c_4e594e1_59eaa16_c8677fb_7b02b5f_2fe0084	0x6ab5c320
-1	--	--	0x5b61a07_13d4cb5_c7a21e0_6ad1270_2f1daa3_81176f2	--	--	0x5b61a07_13d4cb5_c7a21e0_6ad1270_2f1daa3_81176f2	0x1e512db0
0	393	--	0xc7aee82_c72dc59_1208199_466e1d9_396a07c_a8625d6	--	--	0xc7aee82_c72dc59_1208199_466e1d9_396a07c_a8625d6	0xd3122373
1	394	--	0xc040e35_54294b7_0000000_7a3b0f9_42b1dbd_000006a	--	--	0x1108d74_c46b8dd_6fc8cb2_9ae7735_b89d32c_17382b4	0x66362f19
2	395	--	0x6666a4e_47b5444_93d46aa_e4f374f_3cd03	--	--	0x788f947_e7892cd_ff82306_64f6d94_434e1cd	0x8234137d

			33_212d6ab			_868d1b1	
3	396	--	0x1232d67_ef6a7a5_6055678_d509b9f_427d387_e30af77	--	--	0x0eeadd4_7638663_5839c5a_a886ef9_afedcfb_7f77c4f	0x8af77359
…	…	…	…	…	…	…	…
46	439	--	0x57dd199_d4f7e9b_b85862b_d828b51_45921f8_f6be033	--	--	0xe1dbcfb_6d85f70_53284f5_e137317_b1f7b44_42feef8	0xd89c9691
47	440	--	0xc9472f7_c4371c6_667db05_a78da80_06664cc_375232b	--	--	0xb0ad63e_2c8e6a1_c230f2f_12cdc4e_a7a6745_7087667	0x8d27edd6
48	441	--	0x2aeaf01_beef443_e0cd9a0_314db4f_985f085_e1aad05	--	--	0x909ec08_9b50823_e1b1f83_1f1bc01_72fa431_f292150	0xd6bc8f1a
49	442	--	0x5cfb3bd_bb2e5ca_6f52793_70ae71a_2363694_1dad643	--	--	0xc660e93_9388a22_e452add_c9da6f3_ec4fef2_b1cdf18	0x119ac175
50	443	0x091b19a51e15d71a	0x70ae71a_2363694_1dad643_7a3b0f9_42b1dbd_000006a	--	--	0xf724eb2_d7c54f0_c9414a0_297b236_c6303be_c88213c	0x0d9f2c6d
51	444	0x02363b4a3c2bae34	0xdbbdf28_dc37a1f_69aaca3_8d3b596_3cd0333_212d6ab	--	--	0xb4b15f7_46a0e47_8be20f8_b405b8a_f885feb_f354514	0x70bf24ff
…	…	…	…	…	…	…	…
104	497	0x0306e1954f8dd4a4	0x6e8a0b6_0a0bd64_b2c1dfb_4055af3_665407c_e11a757	0x82	0xc352	0x8b093a6_e687b3c_6132462_b94e38f_4f3116f_fccc9d1	0x38f1d556
105	498	0x060dc32a9f1ba948	0x45f1415_2da6811_2f9f883_8209d00_9abfc87_8c37ee0	0xec	0x7097	0x9213549_694c6e8_a34f0c3_d4328bc_adbd6db_742fcf2	0xe3798ffd
106	499	0x0c1b86553e377291	0x60802d3_082166d_6655d80_cb50245_8159b67_a5d1bde	0x83	0x2c89	0x31b79a6_31fdd76_22db2ad_367b896_22dd4c5_acf058d	0x5c4b25af
107	500	0x0c1b86553e377291	0x60802d3_082166d_6655d80_cb50245_8159b67_a5d1bde	0x83	0x2c89	0xcd6ff63_f04b0f2_569f95a_8ec0b6a_fe3a764_3fdf9ce	0xa194a243
108	501	0x0c1b86553e377291	0x60802d3_082166d_6655d80_cb50245_8159b67_a5d1bde	0x83	0x2c89	0xa2d3032_750310b_c891730_179f702_da513a0_211b79a	0x1808baa7
…	…	…	…	…	…	…	…
126	519	0x0c1b86553e377291	0x60802d3_082166d_6655d80_cb50245_8159b67_a5d1bde	0x83	0x2c89	0xf4e68b8_4672767_8eeeba1_8ab9750_dae6562_2443fa6	0xd2c408d1
127	520	0x0c1b86553e377291	0x60802d3_082166d_6655d80_cb50245_8159b67_a5d1bde	0x83	0x2c89	0x2742c41_61fbb93_9e97d44_4fffbb6_24b6915_5de2d8e	0xef354cda
128	521	0x0c1b86553e377291	0x60802d3_082166d_6655d80_cb50245_8159b67_a5d1bde	0x83	0x2c89	0x8cea32e_2e5b05c_bf505fd_53a40f2_c1ed47b_9110c05	0x2c12c578

129	522	0x0c1b86553e377291	0x60802d3_082166d_6655d80_cb50245_8159b67_a5d1bde	0x83	0x2c89	0x60802d3_082166d_6655d80_cb50245_8159b67_a5d1bde	0x60832c89
130	523	0x083704aa746ee522	0x08c4020_30bc948_6b8a961_886718e_b4a6082_0074526	0x40	0xbe67	0x08c4020_30bc948_6b8a961_886718e_b4a6082_0074526	0x1a40be67
Line rekey started							
clk	**Sym clk**	**LFSR[59:0]**	**BM0[167:0]**	**OF0[23:16]**	**OF0[15:0]**	**BM1[167:0]**	**OF1[31:0]**
-3	--	0x0c1b86553e377291	0x60802d3_082166d_6655d80_cb50245_8159b67_a5d1bde	--	--	0x8cea32e_2e5b05c_bf505fd_53a40f2_c1ed47b_9110c05	0x2c12c578
-2	--	0x0c1b86553e377291	0x60802d3_082166d_6655d80_cb50245_8159b67_a5d1bde	--	--	0x60802d3_082166d_6655d80_cb50245_8159b67_a5d1bde	0x60832c89
-1	--	0x083704aa746ee522	0x08c4020_30bc948_6b8a961_886718e_b4a6082_0074526	--	--	0x08c4020_30bc948_6b8a961_886718e_b4a6082_0074526	0x1a40be67
0	524	0x006e0154e0ddca44	0x5af75fe_5953161_a0038b7_c87ac01_cc9c416_9af5207	--	--	0x5af75fe_5953161_a0038b7_c87ac01_cc9c416_9af5207	0x3760f82a
1	525	0x00dc0aa9c9bbb488	0x1085a0e_5352770_6668fe6_e6ff8ab_9829251_b22863b	--	--	0x1085a0e_5350770_6668fe6_e6ff8ab_9829251_b22863b	0xe19de0a8
2	526	0x01b8155393776910	0x6fa6d38_71d9ac4_a0fab91_69d6700_99b4c1b_9e28386	--	--	0x6fa6d38_53f98e6_a0fab91_49d6700_99b4c1b_9e28386	0xe6c5c4b3
3	527	0x03702aa726eef220	0xcc7e643_3a7de8e_14e705e_966aab0_912ac08_ef0999d	--	--	0x229084d_83dc535_14e705e_97ee8a8_912ac08_cf4918d	0xfba3672c
…	…	…	…	…	…	…	…
52	576	0x02819338861caa6b	0xb7c1b19_1f01313_739a857_ca7b203_b589be1_69cf290	--	--	0xe32cf03_c423025_72e3fbc_86cb0af_fd5b2ee_14f9af4	0x25d25f81
53	577	0x05032671043974d6	0xf54baa2_516c179_8fa28c3_b35d1ca_0e4df45_d8c5524	--	--	0x2b9bf02_6567dd1_c90fcf3_cc1e869_fca1056_84dd5ab	0x8821df02
54	578	0x0a0644e20872e9ad	0xf99f5c2_06270a5_7ded43b_103d361_85052da_3ca9e17	--	--	0x78679c2_7b92110_188ac5f_95772f0_764392c_a1cef59	0x32a975a1
55	579	0x040c81c418e5f35b	0x7886306_1252fd3_da4da02_419a2fc_334d491_dc16b5b	--	--	0xead9731_4064062_364c15e_c48384b_2d20f54_de16319	0x4c15e552
56	580	0x08190b8831cbc6b7	0xf3ffda5_59a8a35_55eadab_4b5c391_88699f4_c0c8eef	--	--	0x33e2803_a8be6fa_ff005bf_8c88d28_3e9f26f_e35ae7d	0xbb310e11
57	581	0x08190b8831cbc6b7	0xf3ffda5_59a8a35_55eadab_4b5c391_88699f4_c0c8eef	--	--	0xa575b19_fd01fec_7a5a1dd_72cc751_302ce1d_af7d850	0xfd1aa71e
	582			--	--		

58		0x08190b8831cbc6b7	0xf3ffda5_59a8a35_55eadab_4b5c391_88699f4_c0c8eef			0x7beaafa_c3020d1_8583e6a_ff59928_c567224_f6475df	0xf2a9a6f9
…	…	…	…	…	…	…	…
63	587	0x08190b8831cbc6b7	0xf3ffda5_59a8a35_55eadab_4b5c391_88699f4_c0c8eef	--	--	0x44be25d_9fd286e_8e7fe89_b4470c4_fca81db_cf9fb85	0x68e0ea10
64	588	0x08190b8831cbc6b7	0xf3ffda5_59a8a35_55eadab_4b5c391_88699f4_c0c8eef	--	--	0x8cc7ec7_0b16fef_48d8f7e_d925213_156666c_a7b7959	0xfa00360b
65	589	0x08190b8831cbc6b7	0xf3ffda5_59a8a35_55eadab_4b5c391_88699f4_c0c8eef	--	--	0xf3ffda5_59a8a35_55eadab_4b5c391_88699f4_c0c8eef	0x66737ce1
66	590	0x00321f106b978d6e	0x83ef0b5_83a143f_677413b_aaff69e_87ec5ab_0e225b6	--	--	0x83ef0b5_83a143f_677413b_aaff69e_87ec5ab_0e225b6	0xf47748b2
67	591	0x00643e20d72f3adc	0xd606da8_74c4faf_7fe5a05_0e81aa1_ac79a3d_e0d0515	--	--	0xd606da8_74c4faf_7fe5a05_0e81aa1_ac79a3d_e0d0515	0x59b80f68
68	592	0x00c87c41ae5e55b8	0xa448523_8753368_aed28fe_9cced8d_83a3092_24f5ff1	--	--	0xa448523_8753368_aed28fe_9cced8d_83a3092_24f5ff1	0xecdb3b98
…	…	…	…	…	…	…	…
128	652	0x0346dff6a664010b	0x8380d0e_1f7cd07_dc77025_53d2eae_c16a800_6b31ba5	0x0c	0x1e28	0x8380d0e_1f7cd07_dc77025_53d2eae_c16a800_6b31ba5	0x850c1e28
129	653	0x068db7ed44c82217	0xf2bb890_3ea29ff_ed6af5f_5ef77c9_3b3308a_f7842b4	0x3c	0x1430	0xf2bb890_3ea29ff_ed6af5f_5ef77c9_3b3308a_f7842b4	0x623c1430
130	654	0x0d1b67da8190442f	0xe039b17_d2aa06b_d6572dd_c1b67aa_0052141_5f600ae	0xaa	0xfc51	0xe039b17_d2aa06b_d6572dd_c1b67aa_0052141_5f600ae	0xddaafc51
Line rekey started							

clk	**Sym clk**	**LFSR[59:0]**	**BM0[167:0]**	**OF0[23:16]**	**OF0[15:0]**	**BM1[167:0]**	**OF1[31:0]**
-3	--	0x0346dff6a664010b	0x8380d0e_1f7cd07_dc77025_53d2eae_c16a800_6b31ba5	--	--	0x8380d0e_1f7cd07_dc77025_53d2eae_c16a800_6b31ba5	0x850c1e28
-2	--	0x068db7ed44c82217	0xf2bb890_3ea29ff_ed6af5f_5ef77c9_3b3308a_f7842b4	--	--	0xf2bb890_3ea29ff_ed6af5f_5ef77c9_3b3308a_f7842b4	0x623c1430
-1	--	0x0d1b67da8190442f	0xe039b17_d2aa06b_d6572dd_c1b67aa_0052141_5f600ae	--	--	0xe039b17_d2aa06b_d6572dd_c1b67aa_0052141_5f600ae	0xddaafc51
0	655	0x0a36cfb50b20a85f	0xf7a4696_cedb781_9b7c296_7e80f87_2627aa3_4a96e73	--	--	0xf7a4696_cedb781_9b7c296_7e80f87_2627aa3_4a96e73	0x34c8387f
1	656	0x046d976a1e4150bf	0xf9e10ad_26ebfeb_e3b2ae8_d405d6d_82d19e6_700ddcb	--	--	0xf9e10ad_26ebfeb_e3b2ae8_d405d6d_82d19e6_700ddcb	0xf9f9c133

2	657	0x08db26d43482a17e	0x1ab27f1_1fce0bc_db12463_95c6a02_d289bae_3557833	--	--	0x1ab27f1_1fce0bc_db12463_95c6a02_d289bae_3557833	0x98e78102
3	658	0x01b64da8610542fc	0x878eed5_7415779_08698fc_22c75d3_96c33f5_22aa0fd	--	--	0x878eed5_7415779_08698fc_22c75d3_96c33f5_22aa0fd	0xb159bd1f
…	…	…	…	…	…	…	…
54	709	0x07e62edb1c6c597c	0xa6df5b7_9d237cb_9cf5ad7_0bd7ca7_424ce87_6f684eb	--	--	0xad409c1_07a1bc8_c1fe768_67706de_7abc742_860407a	0xa8304199
55	710	0x0fcc55b630d892f9	0x9de5ca4_9d46270_f297559_0231f1d_6fbfae5_af810b8	--	--	0x5e76131_95d7447_2740077_0227f05_9d059d9_234c6f4	0x57e84b6e
56	711	0x0f98a36c69b125f2	0xa217ca7_311f16d_cfb7158_e7be773_e5a3cef_24cd744	--	--	0xed349f1_23b7a22_3dc6aab_391ac55_2e45f61_3feffd9	0x01c6dd74
57	712	0x0f98a36c69b125f2	0xa217ca7_311f16d_cfb7158_e7be773_e5a3cef_24cd744	--	--	0x6185691_e4f678b_1de42f2_61510dd_971466e_da49c7b	0x9b7e6206
58	713	0x0f98a36c69b125f2	0xa217ca7_311f16d_cfb7158_e7be773_e5a3cef_24cd744	--	--	0x8ff263a_04db9c1_7805c8a_e59a6ac_ed700cc_69d157e	0x997d688e
…	…	…	…	…	…	…	…
63	718	0x0f98a36c69b125f2	0xa217ca7_311f16d_cfb7158_e7be773_e5a3cef_24cd744	--	--	0x65c9011_b36e2d8_26ef4ed_893c287_498abad_5c1d947	0x73cc1524
64	719	0x0f98a36c69b125f2	0xa217ca7_311f16d_cfb7158_e7be773_e5a3cef_24cd744	--	--	0x54bc6b8_335ddf4_6a1d196_9afdd3d_3c7854b_d117db4	0xca532e41
65	720	0x0f98a36c69b125f2	0xa217ca7_311f16d_cfb7158_e7be773_e5a3cef_24cd744	--	--	0xa217ca7_311f16d_cfb7158_e7be773_e5a3cef_24cd744	0x5041b60a
66	721	0x0f314ed8db624be5	0x5b245db_cbcbe10_921fd59_1505ea7_a17d5f8_fab66a9	--	--	0x5b245db_cbcbe10_921fd59_1505ea7_a17d5f8_fab66a9	0x4b326bfd
67	722	0x0e629db1b6c4b7cb	0xaab50ef_e646890_c76fd37_1c24710_17f70de_784ee98	--	--	0xaab50ef_e646890_c76fd37_1c24710_17f70de_784ee98	0x705cef4f
…	…	…	…	…	…	…	…
126	781	0x0fc4084e4d5a4e04	0x0b8bb58_d6d737d_b849287_60940bf_f4ffad9_a00f1ba	0x55	0xa17d	0x0b8bb58_d6d737d_b849287_60940bf_f4ffad9_a00f1ba	0xfe55a17d
127	782	0x0f88109c9ab4bc09	0xbf314e0_341cc32_bdb0743_fa86d53_80e7edd_6c944ec	0x6c	0xbae1	0xbf314e0_341cc32_bdb0743_fa86d53_80e7edd_6c944ec	0xcd6cbae1
128	783	0x0f10213935695812	0x35d37a8_f54fe65_0f65bc9_84d9f7c_09ef04b_db57cdb	0x7e	0x0828	0x35d37a8_f54fe65_0f65bc9_84d9f7c_09ef04b_db57cdb	0xbe7e0828
1	784	0x0e20427262d29	0x357adbe_4fc9fb5_44	0xac	0xc267	0x357adbe_4fc9fb5_448	0x76acc

29		024	8724b_c6ce2c3_aabd0c5_07afa24			724b_c6ce2c3_aabd0c5_07afa24	267
130	785	0x0c408ce4cda50049	0x6e01833_2dcb166_40b6d41_0858e4d_01457e4_c76b5c6	0x08	0x41ef	0x6e01833_2dcb166_40b6d41_0858e4d_01457e4_c76b5c6	0xbd0841ef

Table B-28. Cipher State in SST mode for 4-lane, Inter-BS Spacing = 131

clk	stream	cipher	enc stream
-3	0x1c1c1c1c	0x6559c03e	0x1c1c1c1c
-2	0x3c3c3c3c	0x6559c03e	0x3c3c3c3c
-1	0x3c3c3c3c	0x6559c03e	0x3c3c3c3c
0	0x1c1c1c1c	0x6559c03e	0x1c1c1c1c
1	0x39393939	0xb79ee5fe	0x8ea7dcc7
2	0x00000000	0x289af919	0x289af919
3	0x00000000	0xd25b5d6c	0xd25b5d6c
4	0x00000000	0xed55dcde	0xed55dcde
…	…	…	…
46	0x00000000	0x37affe86	0x37affe86
47	0x00000000	0x49152bc4	0x49152bc4
48	0x00000000	0x1f068148	0x1f068148
49	0x00000000	0xb79cb954	0xb79cb954
50	0x00000000	0xfe492f2a	0xfe492f2a
51	0x00000000	0x53331e18	0x53331e18
52	0x00000000	0x5c0e4039	0x5c0e4039
…	…	…	…
101	0x00000000	0x96fc2396	0x96fc2396
102	0x00000000	0xbc51d239	0xbc51d239
103	0x00000000	0x8908e8ac	0x8908e8ac
104	0x00000000	0x1d74baa3	0x1d74baa3
105	0x00000000	0xd8835587	0xd8835587
106	0x00000000	0xaf70715f	0xaf70715f
107	0x00000000	0xc861665f	0xc861665f
108	0x00000000	0x2bbcf09a	0x2bbcf09a
…	…	…	…
127	0x00000000	0xc07ece76	0xc07ece76
128	0xbcbcbcbc	0xedf08af9	0xbcbcbcbc
129	0x3c3c3c3c	0xb86284bb	0x3c3c3c3c
130	0x3c3c3c3c	0xb87439a6	0x3c3c3c3c
131	0xbcbcbcbc	0xf701f1ed	0xbcbcbcbc
132	0x39393939	0x523d121c	0x6b042b25
133	0x00000000	0xf96f47ae	0xf96f47ae
…	…	…	…
185	0x00000000	0xe8b7ea1e	0xe8b7ea1e
186	0x00000000	0xac7e0ebc	0xac7e0ebc
187	0x00000000	0x233bf0c3	0x233bf0c3
188	0x00000000	0x16208c84	0x16208c84
189	0x00000000	0x2acbe06b	0x2acbe06b
190	0x00000000	0xe856019a	0xe856019a
191	0x00000000	0xe2966145	0xe2966145
192	0x00000000	0x8151e92c	0x8151e92c

193	0x00000000	0xe228cfc1	0xe228cfc1
194	0x00000000	0x681b908d	0x681b908d
195	0x00000000	0x3792bbc6	0x3792bbc6
196	0x00000000	0x0b653310	0x0b653310
197	0x00000000	0xc63474f4	0xc63474f4
198	0x00000000	0x9832c3f5	0x9832c3f5
…	…	…	…
259	0xbcbcbcbc	0x1a3525c9	0xbcbcbcbc
260	0x3c3c3c3c	0x94f602fc	0x3c3c3c3c
261	0x3c3c3c3c	0xf4dfb4a0	0x3c3c3c3c

Table B-29. 4-lane Encrypted Output in SST mode for Inter-BS Spacing = 131

Test Vectors for 2-Lane Main Link Configuration in SST Mode (Inter-BS spacing = 130, CPSR Interval = 5)

Authentication

Table B-3 and Table B-4 provide the LFSR and Block module states during the first part of authentication.

Initial Bootstrapping

Table B-25 provides test vectors during the initial bootstrapping operation.

After start of encryption

Table B-30 provides test vectors generated after the start of encryption (beginning with the first CPSR symbol set that triggers encryption). Table B-31 provides encrypted cipher outputs.

clk	Sym clk	LFSR[59:0]	BM0[167:0]	OF0[23:16]	OF0[15:0]	BM1[167:0]	OF1[31:0]
Frame key calc started							
-3	--	--	0xd20317a_3725bc8_256af5e_6b9cc06_7d7aa18_87f9092	--	--	0xd20317a_3725bc8_256af5e_6b9cc06_7d7aa18_87f9092	0x6559c03e
-2	--	--	0xd20317a_3725bc8_256af5e_6b9cc06_7d7aa18_87f9092	--	--	0xd20317a_3725bc8_256af5e_6b9cc06_7d7aa18_87f9092	0x6559c03e
-1	--	--	0xd20317a_3725bc8_256af5e_6b9cc06_7d7aa18_87f9092	--	--	0xd20317a_3725bc8_256af5e_6b9cc06_7d7aa18_87f9092	0x6559c03e
0	0	--	0xd20317a_3725bc8_256af5e_6b9cc06_7d7aa18_87f9092	--	--	0xd20317a_3725bc8_256af5e_6b9cc06_7d7aa18_87f9092	0x6559c03e
1	1	--	0xc040e35_54294b7_0000000_f523e56_bf44e50_000001d	--	--	0x9b48c65_3f7de85_4cfb937_50d9c10_5d7fbdc_6a03908	0xb79ee5fe
2	3	--	0x6666a4e_47b5444_93d46aa_a1a9cb4_a206aaa_cacfa30	--	--	0x94ede66_8141634_5f900d1_5f7a0f0_f291dcb_5a0ce6e	0x289af919
3	5	--	0x1232d67_ef6a7a5_6055678_533e54c_e4b418a_91fbcbb	--	--	0x1f69314_9a31990_c4b92db_31a6525_6ab1304_928c3d8	0xd25b5d6c
4	7	--	0x811566c_da14697_66f89db_d9ce46b_c89e263_9e3097e	--	--	0x7f0a70c_d1bda54_34c9929_7df4b37_d8d588c_855d111	0xed55dcde
…	…	…	…	…	…	…	…
46	91	--	0x57dd199_d4f7e9b_b85862b_5cc55f4_2b5efea_85611ff	--	--	0x2789d57_f53ee8a_3cfeaf5_817480c_c30af76_2f49767	0x37affe86
47	93	--	0xc9472f7_c4371c6_667db05_9e19673_1fcfb80_9e1665f	--	--	0xfa07250_f725212_9bc279d_76fe61a_e1521fc_fb331b7	0x49152bc4
48	95	--	0x2aeaf01_beef443_e0cd9a0_d83548d_480c50a_5d4ed0e	--	--	0xcaf5121_1129806_3836e0a_9051c5e_34551ae_7f7b35a	0x1f068148
49	97	--	0x5cfb3bd_bb2e5ca_6f52793_8bb82fe_ea7c298_d9a59fa	--	--	0x62e765a_09101ee_f92cab1_4cfd7ca_f8ad063_1f97804	0xb79cb954

50	99	0x0f53e0a6257702fe	0x8bb82fe_ea7c298_d9a59fa_f523e56_bf44e50_000001d	--	--	0x960d99e_e9b8b0f_782d158_645c7a9_312615f_ca46465	0xfe492f2a
51	101	0x0ea7c94c42ee05fd	0xb486149_cca6e3d_0355dff_2262329_a206aaa_cacfa30	--	--	0xb72431d_495f294_aba13a4_c1a5edc_d8ea59b_2cbcad0	0x53331e18
52	103	0x0d4f929885dc0bfb	0x120ec20_a1030d1_4c72806_a00fb45_e4b418a_75af954	--	--	0xe94a5e8_bad382a_b516ee3_2aea12a_04f35e9_6a44723	0x5c0e4039
53	105	0x0a9f253103b837f6	0xc084d58_ee8b642_7dd6814_079525e_aef8c5e_ada7f43	--	--	0x8b46a53_283034d_84a452f_9958918_06c7952_3d3b8d2	0x4a040224
…	…	…	…	…	…	…	…
64	127	0x0914083b892b3051	0x5bfdd23_7ca0b5a_c12f127_495854a_19f3173_1c1ac03	--	--	0x8020fe9_f55f9f4_8fef65e_58f4d4b_bf0fe4e_d6f769b	0xc5f3500b
65	129	0x02281877125640a2	0xa1ac713_e2d283a_482c2bb_d437443_bd8ef95_076c262	--	--	0xbdc2425_78138b1_fae8859_7b0d9b3_9007256_f02725b	0xf254ffb6
Line rekey ignored (frame key calc in progress)							
66	131	0x045030ee2cac8144	0x3e289e0_1b214d0_e90ac42_1504b3f_58bc895_c98fa75	--	--	0x6ad3eed_82e9428_1f151a0_fefc1c7_231e1e6_0e7b8ba	0x14b8b17b
67	133	0x08a061dc59590289	0x0e8407c_bb5df9d_578e9dd_6e1b212_7e16013_78ef703	--	--	0xbcf19db_fd7dda6_60704fe_0a9e816_1645fbc_7b03898	0x36693806
…	…	…	…	…	…	…	…
103	205	0x015269d49873d16c	0xabddb90_19d2b4a_7540b7a_458c215_014c756_aca7735	--	0xb1db	0x394e745_ec99143_e3f8f19_375ec6c_39c7cef_ba78801	0x8908e8ac
104	207	0x02a4d3a938e782d8	0x924eb87_b7a728b_8f829c6_35dd971_63da5b0_486ff01	0x97	0xd7a3	0x398cfb0_51408ef_9500162_a935d4f_835f420_da99144	0x1d74baa3
105	209	0x0549af5279cf05b1	0x711d28b_ffa6fca_923e67b_15707a7_42a4bb2_2deda6d	0xbb	0xb0f9	0xde9d7c1_83df898_1e55332_ddc9add_a82acb2_2885c03	0xd8835587
106	211	0x0a935ea4f39e2b63	0xeff1213_e232b20_0064b82_ae1968a_4a3cba4_40cb306	0x62	0x84bb	0xd887f8b_5d37e0d_fe4d145_6a55c77_9369bfb_5028d20	0xaf70715f
107	213	0x0a935ea4f39e2b63	0xeff1213_e232b20_0064b82_ae1968a_4a3cba4_40cb306	0x62	0x84bb	0xb77f694_6fed836_ec5fbda_befa034_2c5d690_ae478e9	0xc861665f
108	215	0x0a935ea4f39e2b63	0xeff1213_e232b20_0064b82_ae1968a_4a3cba4_40cb306	0x62	0x84bb	0xa67d45e_0b30f7d_2bb93be_e09b5f5_22ca847_b849198	0x2bbcf09a
…	…	…	…	…	…	…	…
127	253	0x0a935ea4f39e2b63	0xeff1213_e232b20_0064b82_ae1968a_4a3cba4_40cb306	0x62	0x84bb	0x6886c93_2065e45_773f684_82237f8_df3ef7a_cae90a7	0xc07ece76
128	255	0x0a935ea4f39	0xeff1213_e232b20_00	0x62	0x84bb	0x9359a39_d450a12_51c	0xedf08af

		e2b63	64b82_ae1968a_4a3cba4_40cb306			e5bc_d3062b6_2c9cca3_c74edc4	9
129	257	0x0a935ea4f39e2b63	0xeff1213_e232b20_0064b82_ae1968a_4a3cba4_40cb306	0x62	0x84bb	0xeff1213_e232b20_0064b82_ae1968a_4a3cba4_40cb306	0xb86284bb
130	259	0x0526b549e73c76c7	0xddd552f_3d3bac2_fb230d5_83a2d78_5a1da41_8fed1d6	0x74	0x39a6	0xddd552f_3d3bac2_fb230d5_83a2d78_5a1da41_8fed1d6	0xb87439a6
Line rekey started							
clk	**Sym clk**	**LFSR[59:0]**	**BM0[167:0]**	**OF0[23:16]**	**OF0[15:0]**	**BM1[167:0]**	**OF1[31:0]**
-3	--	0x0a935ea4f39e2b63	0xeff1213_e232b20_0064b82_ae1968a_4a3cba4_40cb306	--	--	0x9359a39_d450a12_51ce5bc_d3062b6_2c9cca3_c74edc4	0xedf08af9
-2	--	0x0a935ea4f39e2b63	0xeff1213_e232b20_0064b82_ae1968a_4a3cba4_40cb306	--	--	0xeff1213_e232b20_0064b82_ae1968a_4a3cba4_40cb306	0xb86284bb
-1	--	0x0526b549e73c76c7	0xddd552f_3d3bac2_fb230d5_83a2d78_5a1da41_8fed1d6	--	--	0xddd552f_3d3bac2_fb230d5_83a2d78_5a1da41_8fed1d6	0xb87439a6
0	260	0x0526b549e73c76c7	0xddd552f_3d3bac2_fb230d5_83a2d78_5a1da41_8fed1d6	--	--	0xddd552f_3d3bac2_fb230d5_83a2d78_5a1da41_8fed1d6	0xb87439a6
1	261	0x0a4d6293ce78ed8e	0xc258963_5d097d0_e50aa7c_fc50f00_a2a747b_a45b784	--	--	0xc258963_5d097d0_e50aa7c_fc50f00_a2a747b_a45b784	0xf701f1ed
2	263	0x049ac5279cf1fb1c	0xb06e6b7_c8209e8_82982f7_4bc1a13_8a3f797_9f0446e	--	--	0xb06e6b7_c8209e8_82982f7_4bc1a13_8a3f797_9f0446e	0x523d121c
3	265	0x09358a4f31e3d639	0xefd27df_0e46509_e0b63da_cb3dc05_af53ae8_4436e20	--	--	0xefd27df_0e46509_e0b63da_cb3dc05_af53ae8_4436e20	0xf96f47ae
…	…	…	…	…	…	…	…
52	363	0x02694c70f74ddda1	0x014c513_1161f8b_41c9b49_a64a8b3_0ad9135_6c6337b	--	--	0x88eca24_fa0719b_0e475ea_fd01238_77fac9c_2a2fe35	0x241e4836
53	365	0x04d290e1ee9bbb43	0x5f74778_7bae847_3858c2e_6d9a242_bc9a02f_e4fdf87	--	--	0x276fafa_fb8c5a8_95210b1_8d295f2_09e27e6_b737720	0x673be722
54	367	0x09a529c3d5375686	0x41c3db8_7e60b5d_ade6c26_0335bb1_0313ffb_ce6d556	--	--	0xde83510_f93dd7e_8f09cca_fd7e979_439879a_5870c89	0x0e661a04
55	369	0x034a5387aa6ead0c	0xda39225_0d2f8e6_487e46d_14adaff_c23321e_7e5a780	--	--	0x9fd4127_873eeab_d443857_d7bc533_04fa8ab_a4eee09	0xe8b7ea1e
56	371	0x0694af0f54dd7a18	0xb6bee9e_b0ef775_f7d10ad_5dce396_89b2597_acef7ea	--	--	0xd5858aa_e4354ca_b52fefd_c3e62de_3960ed5_cbc6aa5	0xac7e0ebc
57	373	0x0694af0f54dd7a18	0xb6bee9e_b0ef775_f7d10ad_5dce396_89b2597_acef7ea	--	--	0xed3734d_00d67e7_eb76874_e2d404c_09ed965_dc23211	0x233bf0c3

58	375	0x0694af0f54dd7a18	0xb6bee9e_b0ef775_f7d10ad_5dce396_89b2597_acef7ea	--	--	0xe17cdec_bc66357_8450c0e_5f72374_878db0c_6b13d1e	0x16208c84
…	…	…	…	…	…	…	…
63	385	0x0694af0f54dd7a18	0xb6bee9e_b0ef775_f7d10ad_5dce396_89b2597_acef7ea	--	--	0x5b908ab_b2fdadc_ab7f84a_88d8992_bb6fc94_30a7b52	0xe228cfc1
64	387	0x0694af0f54dd7a18	0xb6bee9e_b0ef775_f7d10ad_5dce396_89b2597_acef7ea	--	--	0x9f12b63_096eeec_28e9b90_a572681_09e03f4_85a8ee3	0x681b908d
65	389	0x0694af0f54dd7a18	0xb6bee9e_b0ef775_f7d10ad_5dce396_89b2597_acef7ea	--	--	0xb6bee9e_b0ef775_f7d10ad_5dce396_89b2597_acef7ea	0xabaaaf5a

Line rekey started

clk	Sym clk	LFSR[59:0]	BM0[167:0]	OF0[23:16]	OF0[15:0]	BM1[167:0]	OF1[31:0]
-3	--	0x0694af0f54dd7a18	0xb6bee9e_b0ef775_f7d10ad_5dce396_89b2597_acef7ea	--	--	0x5b908ab_b2fdadc_ab7f84a_88d8992_bb6fc94_30a7b52	0xe228cfc1
-2	--	0x0694af0f54dd7a18	0xb6bee9e_b0ef775_f7d10ad_5dce396_89b2597_acef7ea	--	--	0x9f12b63_096eeec_28e9b90_a572681_09e03f4_85a8ee3	0x681b908d
-1	--	0x0694af0f54dd7a18	0xb6bee9e_b0ef775_f7d10ad_5dce396_89b2597_acef7ea	--	--	0xb6bee9e_b0ef775_f7d10ad_5dce396_89b2597_acef7ea	0xabaaaf5a
0	390	0x0694af0f54dd7a18	0xb6bee9e_b0ef775_f7d10ad_5dce396_89b2597_acef7ea	--	--	0xb6bee9e_b0ef775_f7d10ad_5dce396_89b2597_acef7ea	0xabaaaf5a
1	391	0x0d29561ea1bad430	0x0beb3a9_cb636c5_ce7a6d6_3ab9bdb_c93d31b_c325019	--	--	0x0beb3a9_cb616c5_ce7a6d6_3ab9bdb_c93d31b_c325019	0x0b6d3310
2	393	0x0a52a43d4b758861	0x6a3ad12_9856416_6c93fda_e14a23d_fbc4d3f_cceecdf	--	--	0x6a3ad12_ba76634_6c93fda_c14a23d_fbc4d3f_cceecdf	0xcd7c74f2
3	395	0x04a5487a96eb30c2	0x6a9b47c_328300c_494b633_ca430af_69d5a81_2aca65b	--	--	0x8475a72_8b20bb7_494b633_cbc72b7_69d5a81_0a8a65b	0xb840f90b
…	…	…	…	…	…	…	…
52	493	0x09d88114a91d6c86	0x158c91b_e318b99_beb3950_3261d4d_11ed2fc_cddbf33	--	--	0xdd4cbea_e2291a5_0790d34_cd78b17_b2ba07c_472207a	0x0b11e356
53	495	0x03b10229523af90d	0xea16628_c0a7e70_6830104_292dab8_472ab7a_94bf148	--	--	0x9ae1079_2563218_0bb4370_b3ec2a2_1237195_9312c25	0x335ce895
54	497	0x07620452ac75f21a	0x59dfc75_a004a32_88e6c6e_fb13a24_e0d0832_527ea13	--	--	0xf8cf95b_ffd5e27_f2c1cc7_70c42fa_9cf89b7_b10391d	0xe6b9cdca
55	499	0x0ec400a550ebc434	0xfad6e6f_5f6fdb3_d540264_dcffdd2_6c56b8a_20339ee	--	--	0xe640131_5eccf76_402b806_ab13ed0_4b35670_f6e6475	0xc8fdaa38

56	501	0x0d88014aa9d78868	0x3877c5f_6897f66_20df19d_f362ef4_1d4b3ac_c306a61	--	--	0xc4ca394_c370a68_af900b7_41db7ce_319fbf5_8ac799e	0x758db7f6
57	503	0x0d88014aa9d78868	0x3877c5f_6897f66_20df19d_f362ef4_1d4b3ac_c306a61	--	--	0x16e9a66_d7d3dd4_e4deb61_55def1e_3c5e946_c4682e7	0x8bd0f8ac
58	505	0x0d88014aa9d78868	0x3877c5f_6897f66_20df19d_f362ef4_1d4b3ac_c306a61	--	--	0x18fbf5e_2fc6f5e_559b25b_a26b764_2f36fa3_d301a85	0xcbf58ee5
…	…	…	…	…	…	…	…
63	515	0x0d88014aa9d78868	0x3877c5f_6897f66_20df19d_f362ef4_1d4b3ac_c306a61	--	--	0x7e0ae16_884db5b_0bb4b68_0a1e5f8_6c38195_ff4c09b	0xb1056ff8
64	517	0x0d88014aa9d78868	0x3877c5f_6897f66_20df19d_f362ef4_1d4b3ac_c306a61	--	--	0x9eb4b99_b784a43_554b033_5068a0a_3652f72_45e1b03	0xe29bb233
65	519	0x0d88014aa9d78868	0x3877c5f_6897f66_20df19d_f362ef4_1d4b3ac_c306a61	--	--	0x3877c5f_6897f66_20df19d_f362ef4_1d4b3ac_c306a61	0xed8f9447
Line rekey started							
clk	**Sym clk**	**LFSR[59:0]**	**BM0[167:0]**	**OF0[23:16]**	**OF0[15:0]**	**BM1[167:0]**	**OF1[31:0]**
-3	--	0x0d88014aa9d78868	0x3877c5f_6897f66_20df19d_f362ef4_1d4b3ac_c306a61	--	--	0x7e0ae16_884db5b_0bb4b68_0a1e5f8_6c38195_ff4c09b	0xb1056ff8
-2	--	0x0d88014aa9d78868	0x3877c5f_6897f66_20df19d_f362ef4_1d4b3ac_c306a61	--	--	0x9eb4b99_b784a43_554b033_5068a0a_3652f72_45e1b03	0xe29bb233
-1	--	0x0d88014aa9d78868	0x3877c5f_6897f66_20df19d_f362ef4_1d4b3ac_c306a61	--	--	0x3877c5f_6897f66_20df19d_f362ef4_1d4b3ac_c306a61	0xed8f9447
0	520	0x0d88014aa9d78868	0x3877c5f_6897f66_20df19d_f362ef4_1d4b3ac_c306a61	--	--	0x3877c5f_6897f66_20df19d_f362ef4_1d4b3ac_c306a61	0xed8f9447
1	521	0x0b100a955baf10d0	0xee5976d_b4255e6_00a9f64_cb596c6_165b075_aac6b82	--	--	0xee5976d_b4275e6_00a9f64_cb596c6_165b075_aac6b82	0xac6ca86f
2	523	0x0620152ab75e01a0	0xdcf5875_52832e7_c6b95ed_4af3a31_4761d31_42d51ac	--	--	0xdcf5875_70a30c5_c6b95ed_6af3a31_4761d31_42d51ac	0x097cba38
3	525	0x0c4022556ebc0341	0x3a50a7a_cf93a57_d44036c_637c92a_2c8387b_1906d46	--	--	0xd4be474_76321ec_d44036c_62f8b32_2c8387b_3946d46	0x38e5e68b
4	527	0x08804caadd780683	0x094fd46_c5f35dc_49aa945_61af390_c6fbcba_1eaa206	--	--	0x81c9562_f8b96ef_00fb99b_2e1a12b_4e73c32_7cd8ee2	0x81aca347
…	…	…	…	…	…	…	…
52	623	0x06825f6d671e2e00	0x7a6ae83_d368595_b07ea04_7e7838e_b1cd85a_bfdcec5	--	--	0x34fff33_8d55bc0_8e80626_247612b_0df8888_554e3a9	0xb38a778d

53	625	0x0d04bedac63c7c01	0xdd556b1_d83e031_69733ba_750f95d_0836d6b_2234cfc	--	--	0x5039243_2e6e320_41a3b08_26d877e_b3f96ee_79afb57	0xee178f0a
54	627	0x0a0975b58c78f802	0xa537290_0223b9d_fdc79e4_5776298_3da43d8_d4fdc71	--	--	0x5f703b5_cac4f78_33463ca_b6e708a_568b2a1_a0632d4	0x6547c164
55	629	0x0412e36b18f1f005	0xb45badb_b6d21ce_37a5b20_4d251e0_264ccc8_8d30739	--	--	0xdf5278d_79d9e22_34d08ae_aed2457_206b9a7_e0b8e1d	0xcfbe3198
56	631	0x0825ced639e3e00b	0x12fb7db_8ddeb78_06aba23_b39837b_c40ad56_1f15c73	--	--	0x01e7b9e_1b89938_65118be_6579fd3_5a040ff_a9ce078	0xc5a3707e
57	633	0x0825ced639e3e00b	0x12fb7db_8ddeb78_06aba23_b39837b_c40ad56_1f15c73	--	--	0x924e8c5_e0cccc7_06de74a_04c8464_b8cc7ff_79f1e68	0xd376a249
58	635	0x0825ced639e3e00b	0x12fb7db_8ddeb78_06aba23_b39837b_c40ad56_1f15c73	--	--	0xddb674d_b26e6e5_1e2663d_4e90e02_07ffbaa_825f148	0x02f0d7a9
…	…	…	…	…	…	…	…
63	645	0x0825ced639e3e00b	0x12fb7db_8ddeb78_06aba23_b39837b_c40ad56_1f15c73	--	--	0x0ec9923_487a5ad_0247aa0_6b80eb2_146d209_edd1e23	0x3608f5f0
64	647	0x0825ced639e3e00b	0x12fb7db_8ddeb78_06aba23_b39837b_c40ad56_1f15c73	--	--	0xdcd97ff_ad691cf_c283195_73f2e0f_555ee7f_46d6ab8	0x259c6071
65	649	0x0825ced639e3e00b	0x12fb7db_8ddeb78_06aba23_b39837b_c40ad56_1f15c73	--	--	0x12fb7db_8ddeb78_06aba23_b39837b_c40ad56_1f15c73	0xe14db495

Frame key calc started

clk	Sym clk	LFSR[59:0]	BM0[167:0]	OF0[23:16]	OF0[15:0]	BM1[167:0]	OF1[31:0]
-3	--	--	0x12fb7db_8ddeb78_06aba23_b39837b_c40ad56_1f15c73	--	--	0x0ec9923_487a5ad_0247aa0_6b80eb2_146d209_edd1e23	0x3608f5f0
-2	--	--	0x12fb7db_8ddeb78_06aba23_b39837b_c40ad56_1f15c73	--	--	0xdcd97ff_ad691cf_c283195_73f2e0f_555ee7f_46d6ab8	0x259c6071
-1	--	--	0x12fb7db_8ddeb78_06aba23_b39837b_c40ad56_1f15c73	--	--	0x12fb7db_8ddeb78_06aba23_b39837b_c40ad56_1f15c73	0xe14db495
0	650	--	0x12fb7db_8ddeb78_06aba23_b39837b_c40ad56_1f15c73	--	--	0x12fb7db_8ddeb78_06aba23_b39837b_c40ad56_1f15c73	0xe14db495
1	651	--	0xc040e35_54294b7_0000000_7a3b0f9_42b1dbd_000006a	--	--	0xbad5dac_5b7b2f1_20e8ec2_e3383e4_6bd240c_3c3d602	0x9d86303c
2	653	--	0x6666a4e_47b5444_93d46aa_e4f374f_3cd0333_212d6ab	--	--	0xcc686b2_640bbc5_e3c929c_c421f26_890af42_16c4796	0x0bedc07d
3	655	--	0x1232d67_ef6a7a5_60	--	--	0xf54e27f_1c5ce10_addc	0xc3b619

			55678_d509b9f_427d387_e30af77			e23_a345b6e_c05059f_bb6df7a	33

Table B-30. Cipher State in SST mode for 2-lane, Inter-BS Spacing = 130

Sym clk	stream	cipher	encrypted stream
-3	0x1c1c	0x6559c03e	0x1c1c
-2	0x3c3c	0x6559c03e	0x3c3c
-1	0x3c3c	0x6559c03e	0x3c3c
0	0x1c1c	0x6559c03e	0x1c1c
1	0x3939	0xb79ee5fe	0xdcc7
2	0x0000	0xb79ee5fe	0xb79e
3	0x0000	0x289af919	0xf919
4	0x3939	0x289af919	0x11a3
5	0x0000	0xd25b5d6c	0x5d6c
6	0x0000	0xd25b5d6c	0xd25b
7	0x0000	0xed55dcde	0xdcde
…	…	…	…
91	0x0000	0x37affe86	0xfe86
92	0x0000	0x37affe86	0x37af
93	0x0000	0x49152bc4	0x2bc4
94	0x0000	0x49152bc4	0x4915
95	0x0000	0x1f068148	0x8148
96	0x0000	0x1f068148	0x1f06
97	0x0000	0xb79cb954	0xb954
98	0x0000	0xb79cb954	0xb79c
99	0x0000	0xfe492f2a	0x2f2a
100	0x0000	0xfe492f2a	0xfe49
101	0x0000	0x53331e18	0x1e18
102	0x0000	0x53331e18	0x5333
103	0x0000	0x5c0e4039	0x4039
104	0x0000	0x5c0e4039	0x5c0e
105	0x0000	0x4a040224	0x0224
…	…	…	…
127	0xbcbc	0xc5f3500b	0xbcbc
128	0x3c3c	0xc5f3500b	0x3c3c
129	0x3c3c	0xf254ffb6	0x3c3c
130	0xbcbc	0xf254ffb6	0xbcbc
131	0x3939	0x14b8b17b	0x8842
132	0x0000	0x14b8b17b	0x14b8
133	0x0000	0x36693806	0x3806
…	…	…	…
205	0x0000	0x8908e8ac	0xe8ac
206	0x0000	0x8908e8ac	0x8908
207	0x0000	0x1d74baa3	0xbaa3
208	0x0000	0x1d74baa3	0x1d74
209	0x0000	0xd8835587	0x5587

210	0x0000	0xd8835587	0xd883
211	0x0000	0xaf70715f	0x715f
212	0x0000	0xaf70715f	0xaf70
213	0x0000	0xc861665f	0x665f
214	0x0000	0xc861665f	0xc861
215	0x0000	0x2bbcf09a	0xf09a
…	…	…	…
253	0x0000	0xc07ece76	0xce76
254	0x0000	0xc07ece76	0xc07e
255	0x0000	0xedf08af9	0x8af9
256	0x0000	0xedf08af9	0xedf0
257	0xbcbc	0xb86284bb	0xbcbc
258	0x3c3c	0xb86284bb	0x3c3c
259	0x3c3c	0xb87439a6	0x3c3c
260	0xbcbc	0xb87439a6	0xbcbc
261	0x3939	0xf701f1ed	0xc8d4
262	0x0000	0xf701f1ed	0xf701
263	0x0000	0x523d121c	0x121c
264	0x3939	0x523d121c	0x6b04
265	0x0000	0xf96f47ae	0x47ae
266	0x0000	0xf96f47ae	0xf96f

Table B-31. 2-lane Encrypted Output in SST mode for Inter-BS Spacing = 130

Test Vectors for 2-Lane Main Link Configuration in SST Mode (Inter-BS spacing = 131, CPSR Interval = 5)

Authentication

Table B-3 and Table B-4 provide the LFSR and Block module states during the first part of authentication.

Initial Bootstrapping

Table B-25 provides test vectors during the initial bootstrapping operation.

After start of encryption

Table B-32 provides test vectors generated after the start of encryption (beginning with the first CPSR symbol set that triggers encryption). Table B-33 provides encrypted cipher outputs.

Frame key calc started

clk	Sym clk	LFSR[59:0]	BM0[167:0]	OF0[23:16]	OF0[15:0]	BM1[167:0]	OF1[31:0]
-3	--	--	0xd20317a_3725bc8_256af5e_6b9cc06_7d7aa18_87f9092	--	--	0xd20317a_3725bc8_256af5e_6b9cc06_7d7aa18_87f9092	0x6559c03e
-2	--	--	0xd20317a_3725bc8_256af5e_6b9cc06_7d7aa18_87f9092	--	--	0xd20317a_3725bc8_256af5e_6b9cc06_7d7aa18_87f9092	0x6559c03e
-1	--	--	0xd20317a_3725bc8_256af5e_6b9cc06_7d7aa18_87f9092	--	--	0xd20317a_3725bc8_256af5e_6b9cc06_7d7aa18_87f9092	0x6559c03e
0	0	--	0xd20317a_3725bc8_256af5e_6b9cc06_7d7aa18_87f9092	--	--	0xd20317a_3725bc8_256af5e_6b9cc06_7d7aa18_87f9092	0x6559c03e
1	1	--	0xc040e35_54294b7_0000000_f523e56_bf44e50_000001d	--	--	0x9b48c65_3f7de85_4cfb937_50d9c10_5d7fbdc_6a03908	0xb79ee5fe
2	3	--	0x6666a4e_47b5444_93d46aa_a1a9cb4_a206aaa_cacfa30	--	--	0x94ede66_8141634_5f900d1_5f7a0f0_f291dcb_5a0ce6e	0x289af919
3	5	--	0x1232d67_ef6a7a5_6055678_533e54c_e4b418a_91fbcbb	--	--	0x1f69314_9a31990_c4b92db_31a6525_6ab1304_928c3d8	0xd25b5d6c
4	7	--	0x811566c_da14697_66f89db_d9ce46b_c89e263_9e3097e	--	--	0x7f0a70c_d1bda54_34c9929_7df4b37_d8d588c_855d111	0xed55dcde
…	…	…	…	…	…	…	…
46	91	--	0x57dd199_d4f7e9b_b85862b_5cc55f4_2b5efea_85611ff	--	--	0x2789d57_f53ee8a_3cfeaf5_817480c_c30af76_2f49767	0x37affe86
47	93	--	0xc9472f7_c4371c6_667db05_9e19673_1fcfb80_9e1665f	--	--	0xfa07250_f725212_9bc279d_76fe61a_e1521fc_fb331b7	0x49152bc4
48	95	--	0x2aeaf01_beef443_e0cd9a0_d83548d_480c50a_5d4ed0e	--	--	0xcaf5121_1129806_3836e0a_9051c5e_34551ae_7f7b35a	0x1f068148
49	97	--	0x5cfb3bd_bb2e5ca_6f52793_8bb82fe_ea7c298_d9a59fa	--	--	0x62e765a_09101ee_f92cab1_4cfd7ca_f8ad063_1f97804	0xb79cb954
50	99	0x0f53e0a6257702fe	0x8bb82fe_ea7c298_d9a59fa_f523e56_bf44e50_000001d	--	--	0x960d99e_e9b8b0f_782d158_645c7a9_312615f_ca46465	0xfe492f2a
51	101	0x0ea7c94c42ee05fd	0xb486149_cca6e3d_0355dff_2262329_a206aaa_cacfa30	--	--	0xb72431d_495f294_aba13a4_c1a5edc_d8ea59b_2cbcad0	0x53331e18
52	103	0x0d4f929885dc0bfb	0x120ec20_a1030d1_4c72806_a00fb45_e4b418a_75af954	--	--	0xe94a5e8_bad382a_b516ee3_2aea12a_04f35e9_6a44723	0x5c0e4039

53	105	0x0a9f253103b837f6	0xc084d58_ee8b642_7dd6814_079525e_aef8c5e_ada7f43	--	--	0x8b46a53_283034d_84a452f_9958918_06c7952_3d3b8d2	0x4a040224
54	107	0x053e42620f704fec	0xa45476a_cc524a0_e8b84ed_ed3997e_6fd0590_43c8e4c	--	--	0x3256280_505a587_885c3a1_e9a868e_d1e9b70_d727f22	0xd49657b0
…	…	…	…	…	…	…	…
65	129	0x02281877125640a2	0xa1ac713_e2d283a_482c2bb_d437443_bd8ef95_076c262	--	--	0xbdc2425_78138b1_fae8859_7b0d9b3_9007256_f02725b	0xf254ffb6
66	131	0x045030ee2cac8144	0x3e289e0_1b214d0_e90ac42_1504b3f_58bc895_c98fa75	--	--	0x6ad3eed_82e9428_1f151a0_fefc1c7_231e1e6_0e7b8ba	0x14b8b17b
Line rekey ignored (frame key calc in progress)							
67	133	0x08a061dc59590289	0x0e8407c_bb5df9d_578e9dd_6e1b212_7e16013_78ef703	--	--	0xbcf19db_fd7dda6_60704fe_0a9e816_1645fbc_7b03898	0x36693806
68	135	0x0140c3b8b2b22512	0x7d0a4b8_3eda746_1d77d70_0293f78_0031fd6_6dab5e6	--	--	0x6ffb9d8_4b94ccf_9e88e41_6fd5114_b45199e_2be2560	0x377c62a2
69	137	0x02818f7165646a25	0x16477db_148dbef_208e96f_3b2aeca_7a8b1e0_2df93a0	--	--	0x0466847_2bf5700_cf0dfc9_79a99b7_e39c678_6e62432	0x1dae33a6
…	…	…	…	…	…	…	…
101	201	0x08549a75241cec5b	0x283bb5d_356dc1d_5ef8302_740b636_1e2bbb1_77a9024	--	--	0x06af6be_8574776_6244dc1_1c04bf2_7da1a03_e962e82	0x96fc2396
102	203	0x00a934ea4839f8b6	0xd1bdb61_18b2c89_06d55fe_85d7861_4a2d2c4_3f0f76a	--	0x6a42	0x8000eaf_8f340fb_57fba9a_ece383b_5d4ccf2_e2ff34b	0xbc51d239
103	205	0x015269d49873d16c	0xabddb90_19d2b4a_7540b7a_458c215_014c756_aca7735	--	0xb1db	0x394e745_ec99143_e3f8f19_375ec6c_39c7cef_ba78801	0x8908e8ac
104	207	0x02a4d3a938e782d8	0x924eb87_b7a728b_8f829c6_35dd971_63da5b0_486ff01	0x97	0xd7a3	0x398cfb0_51408ef_9500162_a935d4f_835f420_da99144	0x1d74baa3
105	209	0x0549af5279cf05b1	0x711d28b_ffa6fca_923e67b_15707a7_42a4bb2_2deda6d	0xbb	0xb0f9	0xde9d7c1_83df898_1e55332_ddc9add_a82acb2_2885c03	0xd8835587
106	211	0x0a935ea4f39e2b63	0xeff1213_e232b20_0064b82_ae1968a_4a3cba4_40cb306	0x62	0x84bb	0xd887f8b_5d37e0d_fe4d145_6a55c77_9369bfb_5028d20	0xaf70715f
107	213	0x0a935ea4f39e2b63	0xeff1213_e232b20_0064b82_ae1968a_4a3cba4_40cb306	0x62	0x84bb	0xb77f694_6fed836_ec5fbda_befa034_2c5d690_ae478e9	0xc861665f
…	…	…	…	…	…	…	…
127	253	0x0a935ea4f39e2b63	0xeff1213_e232b20_0064b82_ae1968a_4a3cba4_40cb306	0x62	0x84bb	0x6886c93_2065e45_773f684_82237f8_df3ef7a_cae90a7	0xc07ece76
128	255	0x0a935ea4f39e2b63	0xeff1213_e232b20_0064b82_ae1968a_4a3cba4_40cb306	0x62	0x84bb	0x9359a39_d450a12_51ce5bc_d3062b6_2c9cca3_c74edc4	0xedf08af9
129	257	0x0a935ea4f39e2b63	0xeff1213_e232b20_0064b82_ae1968a_4a3cba4_40cb306	0x62	0x84bb	0xeff1213_e232b20_0064b82_ae1968a_4a3cba4_40cb306	0xb86284bb
130	259	0x0526b549e73c76c7	0xddd552f_3d3bac2_fb230d5_83a2d78_5a1da41_8fed1d6	0x74	0x39a6	0xddd552f_3d3bac2_fb230d5_83a2d78_5a1da41_8fed1d6	0xb87439a6
131	261	0x0a4d6293ce78ed8e	0xc258963_5d097d0_e50aa7c_fc50f00_a2a747b_a45b784	0x01	0xf1ed	0xc258963_5d097d0_e50aa7c_fc50f00_a2a747b_a45b784	0xf701f1ed

Line rekey started

clk	Sym clk	LFSR[59:0]	BM0[167:0]	OF0[23:16]	OF0[15:0]	BM1[167:0]	OF1[31:0]
-3	--	0x0a935ea4f39e2b63	0xeff1213_e232b20_0064b82_ae1968a_4a3cba4_40cb306	--	--	0xeff1213_e232b20_0064b82_ae1968a_4a3cba4_40cb306	0xb86284bb
-2	--	0x0526b549e73c76c7	0xddd552f_3d3bac2_fb230d5_83a2d78_5a1da41_8fed1d6	--	--	0xddd552f_3d3bac2_fb230d5_83a2d78_5a1da41_8fed1d6	0xb87439a6
-1	--	0x0a4d6293ce78ed8e	0xc258963_5d097d0_e50aa7c_fc50f00_a2a747b_a45b784	--	--	0xc258963_5d097d0_e50aa7c_fc50f00_a2a747b_a45b784	0xf701f1ed
0	262	0x0a4d6293ce78ed8e	0xc258963_5d097d0_e50aa7c_fc50f00_a2a747b_a45b784	--	--	0xc258963_5d097d0_e50aa7c_fc50f00_a2a747b_a45b784	0xf701f1ed
1	263	0x049ac5279cf1fb1c	0xb06e6b7_c8209e8_82982f7_4bc1a13_8a3f797_9f0446e	--	--	0xb06e6b7_c8209e8_82982f7_4bc1a13_8a3f797_9f0446e	0x523d121c
2	265	0x09358a4f31e3d639	0xefd27df_0e46509_e0b63da_cb3dc05_af53ae8_4436e20	--	--	0xefd27df_0e46509_e0b63da_cb3dc05_af53ae8_4436e20	0xf96f47ae
3	267	0x026b1c9e63c7ac73	0xc479a9c_8c09955_e4b84bc_f4d23b6_286c3cc_fbefcbb	--	--	0xc479a9c_8c0b955_e4b84bc_f4d23b6_286c3cc_fbefcbb	0xba695c5b
…	…	…	…	…	…	…	…
52	365	0x04d290e1ee9bbb43	0x5f74778_7bae847_3858c2e_6d9a242_bc9a02f_e4fdf87	--	--	0x276fafa_fb8c5a8_95210b1_8d295f2_09e27e6_b737720	0x673be722
53	367	0x09a529c3d5375686	0x41c3db8_7e60b5d_ade6c26_0335bb1_0313ffb_ce6d556	--	--	0xde83510_f93dd7e_8f09cca_fd7e979_439879a_5870c89	0x0e661a04
54	369	0x034a5387aa6ead0c	0xda39225_0d2f8e6_487e46d_14adaff_c23321e_7e5a780	--	--	0x9fd4127_873eeab_d443857_d7bc533_04fa8ab_a4eee09	0xe8b7ea1e
55	371	0x0694af0f54dd7a18	0xb6bee9e_b0ef775_f7d10ad_5dce396_89b2597_acef7ea	--	--	0xd5858aa_e4354ca_b52fefd_c3e62de_3960ed5_cbc6aa5	0xac7e0ebc
56	373	0x0d29561ea1bad430	0x0beb3a9_cb636c5_ce7a6d6_3ab9bdb_c93d31b_c325019	--	--	0xed3734d_00d67e7_eb76874_e2d404c_09ed965_dc23211	0x233bf0c3
57	375	0x0d29561ea1bad430	0x0beb3a9_cb636c5_ce7a6d6_3ab9bdb_c93d31b_c325019	--	--	0xe17cdec_bc66357_8450c0e_5f72374_878db0c_6b13d1e	0x16208c84
58	377	0x0d29561ea1bad430	0x0beb3a9_cb636c5_ce7a6d6_3ab9bdb_c93d31b_c325019	--	--	0x55182ed_d8e05f7_37f417a_14ed44b_585f76b_94900de	0x2acbe06b
…	…	…	…	…	…	…	…
63	387	0x0d29561ea1bad430	0x0beb3a9_cb636c5_ce7a6d6_3ab9bdb_c93d31b_c325019	--	--	0x9f12b63_096eeec_28e9b90_a572681_09e03f4_85a8ee3	0x681b908d
64	389	0x0d29561ea1bad430	0x0beb3a9_cb636c5_ce7a6d6_3ab9bdb_c93d31b_c325019	--	--	0xfb4bddb_29ecd93_fee8c9d_9cef79d_167d4b2_7c33f78	0x3792bbc6
65	391	0x0d29561ea1bad430	0x0beb3a9_cb636c5_ce7a6d6_3ab9bdb_c93d31b_c325019	--	--	0x0beb3a9_cb636c5_ce7a6d6_3ab9bdb_c93d31b_c325019	0x0b653310
66	393	0x0a52a43d4b758861	0x6a3ad12_9854416_6c93fda_e14a23d_fbc4d3f_cceecdf	--	--	0x6a3ad12_9854416_6c93fda_e14a23d_fbc4d3f_cceecdf	0xc63474f4

Line rekey started

clk	Sym clk	LFSR[59:0]	BM0[167:0]	OF0[23:16]	OF0[15:0]	BM1[167:0]	OF1[31:0]
-3	--	0x0d29561ea1bad430	0x0beb3a9_cb636c5_ce7a6d6_3ab9bdb_c93d31b_c325019	--	--	0xfb4bddb_29ecd93_fee8c9d_9cef79d_167d4b2_7c33f78	0x3792bbc6
-2	--	0x0d29561ea1bad430	0x0beb3a9_cb636c5_ce7a6d6_3ab9bdb_c93d31b_c325019	--	--	0x0beb3a9_cb636c5_ce7a6d6_3ab9bdb_c93d31b_c325019	0x0b653310
-1	--	0x0a52a43d4b758861	0x6a3ad12_9854416_6c93fda_e14a23d_fbc4d3f_cceecdf	--	--	0x6a3ad12_9854416_6c93fda_e14a23d_fbc4d3f_cceecdf	0xc63474f4
0	393	0x0a52a43d4b758861	0x6a3ad12_9854416_6c93fda_e14a23d_fbc4d3f_cceecdf	--	--	0x6a3ad12_9854416_6c93fda_e14a23d_fbc4d3f_cceecdf	0xc63474f4
1	395	0x04a5487a96eb30c2	0x6a9b47c_10a322e_494b633_ea430af_69d5a81_2aca65b	--	--	0x6a9b47c_10a122e_494b633_ea430af_69d5a81_2aca65b	0x9832c3f5
2	397	0x094a98f52dd66185	0x697465f_2138d24_6420e6d_dc45678_b3f26bd_ac15ebd	--	--	0x697465f_031af06_6420e6d_fc45678_b3f26bd_ac15ebd	0xedac5ec3
3	399	0x029531ea53acc30b	0x905883e_69e67c4_f13b13c_dde4f16_a9419c1_17133b1	--	--	0x7eb6630_f267e5d_f13b13c_fc60d0e_a9419c1_37533b1	0xccfe6554
…	…	…	…	…	…	…	…
52	497	0x07620452ac75f21a	0x951a1c5_af748e5_6762204_2739c1a_d7ca7fb_7ffebb2	--	--	0xbb0821e_652203c_c692f7a_be966cc_c0d3aeb_e5fb8c3	0x256d3a25
53	499	0x0ec400a550ebc434	0x7dbb091_b0fe23f_b678529_65a5868_35ccece_0ccbf96	--	--	0x7e06bc3_deffce3_a122963_9c8046c_a0f5407_95d2175	0x40160ab9
54	501	0x0d88014aa9d78868	0xba70910_a993630_7a0bb4b_929c3fa_d4032ea_3730bc5	--	--	0xed60095_28f7296_5e3de79_258d6e5_9808185_1f17b14	0xe58099af
55	503	0x0b100a955baf10d0	0x2ead2b5_3199407_9908a29_b00f65c_9bc7820_1d7be03	--	--	0x3e64190_abd2d40_ff33171_2088e1e_054137c_09cd3f8	0x9e1df619
56	505	0x0620152ab75e01a0	0xf8fcf70_76e6257_f2af903_62e652e_6c669c8_bb8b2c3	--	--	0xa57486d_59d17c9_b6020be_95b5c4a_163fe40_0ae4b70	0x5c23cbee
57	507	0x0620152ab75e01a0	0xf8fcf70_76e6257_f2af903_62e652e_6c669c8_bb8b2c3	--	--	0x10c6a0f_37fc336_65d0558_86a6794_5dd9ca5_7ae8a9d	0x68207f9b
58	509	0x0620152ab75e01a0	0xf8fcf70_76e6257_f2af903_62e652e_6c669c8_bb8b2c3	--	--	0x1be27ff_340bb29_413a310_2f0de95_9258438_9ce0e2b	0x06e1abf6
…	…	…	…	…	…	…	…
63	519	0x0620152ab75e01a0	0xf8fcf70_76e6257_f2af903_62e652e_6c669c8_bb8b2c3	--	--	0x5cca5a8_2556f38_721cd54_ed0a7be_b322447_d4b665c	0x94f602fc
64	521	0x0620152ab75e01a0	0xf8fcf70_76e6257_f2af903_62e652e_6c669c8_bb8b2c3	--	--	0xf76f879_1fbb56b_258f91d_e102fc0_cd59d02_20a20c1	0xf4dfb4a0
65	523	0x0620152ab75e01a0	0xf8fcf70_76e6257_f2af903_62e652e_6c669c8_bb8b2c3	--	--	0xf8fcf70_76e6257_f2af903_62e652e_6c669c8_bb8b2c3	0x29ed1fbe

Line rekey started

clk	Sym clk	LFSR[59:0]	BM0[167:0]	OF0[23:16]	OF0[15:0]	BM1[167:0]	OF1[31:0]
-3	--	0x0620152ab75e01a0	0xf8fcf70_76e6257_f2af903_62e652e_6c669c8_bb8b2c3	--	--	0x5cca5a8_2556f38_721cd54_ed0a7be_b322447_d4b665c	0x94f602fc

-2	--	0x0620152ab75e01a0	0xf8fcf70_76e6257_f2af903_62e652e_6c669c8_bb8b2c3	--	--	0xf76f879_1fbb56b_258f91d_e102fc0_cd59d02_20a20c1	0xf4dfb4a0
-1	--	0x0620152ab75e01a0	0xf8fcf70_76e6257_f2af903_62e652e_6c669c8_bb8b2c3	--	--	0xf8fcf70_76e6257_f2af903_62e652e_6c669c8_bb8b2c3	0x29ed1fbe
0	524	0x0620152ab75e01a0	0xf8fcf70_76e6257_f2af903_62e652e_6c669c8_bb8b2c3	--	--	0xf8fcf70_76e6257_f2af903_62e652e_6c669c8_bb8b2c3	0x29ed1fbe
1	525	0x0c4022556ebc0341	0x6ec489f_457b2b0_8ca19cf_094be1f_a6ecdaf_6392c72	--	--	0x6ec489f_45792b0_8ca19cf_094be1f_a6ecdaf_6392c72	0xdb0dcbb4
2	527	0x08804caadd780683	0x1570e26_fd97d4e_dab6c21_60ee032_1ec213f_83a1901	--	--	0x1570e26_dfb5f6c_dab6c21_40ee032_1ec213f_83a1901	0xe292f2e8
3	529	0x01009955baf02d07	0x496a8cb_58c35bb_4ab021c_8bfac8a_cbffe7c_73d27f5	--	--	0xa7846c5_c342c22_4ab021c_aa7ee92_cbffe7c_53927f5	0x224652cf
…	…	…	…	…	…	…	…
51	625	0x0d04bedac63c7c01	0xa28dadd_d6ab782_5e86738_2cae385_514c1d0_48c6561	--	--	0xf2d12de_afa231d_3f0a99d_ac1f00f_b59645c_0dd4f54	0x4c447dea
52	627	0x0a0975b58c78f802	0x582e93d_8c529de_96f4651_3ab716e_1575947_15ce4f0	--	--	0xca13929_c9e78f9_ea3d3d5_7b767be_fe59685_8ccd51b	0xad273750
53	629	0x0412e36b18f1f005	0x116d712_1c678db_3d92522_08ba027_3e26f74_0be143a	--	--	0xc0527e9_f598826_faebef1_15e6832_458da16_b1f001f	0xd1b3765a
54	631	0x0825ced639e3e00b	0x43a027c_087701e_28e98ab_3548c6f_f05357d_1b03d51	--	--	0x8532407_0b10fa7_22aae39_30e473a_7e4ffff_9319a8d	0x6fcb7c49
55	633	0x004b9dac7bc7e016	0x8d2dabb_2310c83_81d3e1b_355c68e_e949cd8_5799143	--	--	0xef5bea9_2dfb784_23544a0_70143c1_c333be5_32610df	0xcdb013bf
56	635	0x00973b58f78fc02d	0x20132f5_3be281d_ad1f6ca_5bdff9f_6e8007e_760fb37	--	--	0x56d33f3_d815596_69e95be_88b187b_692bce7_8c7e3f8	0x30d7d101
57	637	0x00973b58f78fc02d	0x20132f5_3be281d_ad1f6ca_5bdff9f_6e8007e_760fb37	--	--	0xb4062a1_be4b528_7468ee8_25e5f38_5e80888_37e3221	0x5da46729
…	…	…	…	…	…	…	…
63	649	0x00973b58f78fc02d	0x20132f5_3be281d_ad1f6ca_5bdff9f_6e8007e_760fb37	--	--	0x7c3f37b_5e68111_ffee55d_858d359_d604f53_40b70fd	0x2077f4ea
64	651	0x00973b58f78fc02d	0x20132f5_3be281d_ad1f6ca_5bdff9f_6e8007e_760fb37	--	--	0xb54e4d2_8ca945e_7881d64_2347782_d160f10_44ccc0d	0x0835d911
65	653	0x00973b58f78fc02d	0x20132f5_3be281d_ad1f6ca_5bdff9f_6e8007e_760fb37	--	--	0x20132f5_3be281d_ad1f6ca_5bdff9f_6e8007e_760fb37	0x7f81abbc
Frame key calc started							
clk	**Sym clk**	**LFSR[59:0]**	**BM0[167:0]**	**OF0[23:16]**	**OF0[15:0]**	**BM1[167:0]**	**OF1[31:0]**
-3	--	--	0x20132f5_3be281d_ad1f6ca_5bdff9f_6e8007e_760fb37	--	--	0x7c3f37b_5e68111_ffee55d_858d359_d604f53_40b70fd	0x2077f4ea
-2	--	--	0x20132f5_3be281d_ad1f6ca_5bdff9f_6e8007e_760fb37	--	--	0xb54e4d2_8ca945e_7881d64_2347782_d160f10_44ccc0d	0x0835d911
-1	--	--	0x20132f5_3be281d_ad1f6ca	--	--	0x20132f5_3be281d_ad1f6ca_5bdff9f_	0x7f81abbc

			_5bdff9f_6e8007e_760fb37			6e8007e_760fb37	
0	655	--	0x53927a9_6f45129_2a11a47_387e18d_2114556_d7188a6	--	--	0x53927a9_6f45129_2a11a47_387e18d_2114556_d7188a6	0x23d38fdf
1	656	--	0xc040e35_54294b7_0000000_7a3b0f9_42b1dbd_000006a	--	--	0xc848319_9f9aab1_20cb2c8_bf7e6c4_14a5538_6d27dfa	0x9486041b
2	658	--	0x6666a4e_47b5444_93d46aa_e4f374f_3cd0333_212d6ab	--	--	0xaa05ee4_5f3ca50_ff75fa2_151450c_17b33e6_e01b935	0x13e73875
3	660	--	0x1232d67_ef6a7a5_6055678_d509b9f_427d387_e30af77	--	--	0xc3080b2_5d79eae_9201cda_37c8dc5_4318278_5e138b7	0x790f10b8
4	662	--	0x811566c_da14697_66f89db_84306fe_411d172_f9e3620	--	--	0x889d6b6_6dbc445_8bd69f7_136a3d0_b995996_159c4e9	0x5ac4a8c4
5	664	--	0xf7027a4_dc24164_29716cf_f0cd06e_9fad21f_41cbe85	--	--	0x8fbe53f_23a7a5f_d3d5d1e_d7615c2_493400f_d6051fe	0xea9be05f

Table B-32. Cipher State in SST mode for 2-lane, Inter-BS Spacing = 131

clk	stream	cipher	enc stream
-3	0x1c1c	0x6559c03e	0x1c1c
-2	0x3c3c	0x6559c03e	0x3c3c
-1	0x3c3c	0x6559c03e	0x3c3c
0	0x1c1c	0x6559c03e	0x1c1c
1	0x3939	0xb79ee5fe	0xdcc7
2	0x0000	0xb79ee5fe	0xb79e
3	0x0000	0x289af919	0xf919
4	0x3939	0x289af919	0x11a3
5	0x0000	0xd25b5d6c	0x5d6c
6	0x0000	0xd25b5d6c	0xd25b
7	0x0000	0xed55dcde	0xdcde
…	…	…	…
91	0x0000	0x37affe86	0xfe86
92	0x0000	0x37affe86	0x37af
93	0x0000	0x49152bc4	0x2bc4
94	0x0000	0x49152bc4	0x4915
95	0x0000	0x1f068148	0x8148
96	0x0000	0x1f068148	0x1f06
97	0x0000	0xb79cb954	0xb954
98	0x0000	0xb79cb954	0xb79c
99	0x0000	0xfe492f2a	0x2f2a
100	0x0000	0xfe492f2a	0xfe49
101	0x0000	0x53331e18	0x1e18
102	0x0000	0x53331e18	0x5333
103	0x0000	0x5c0e4039	0x4039
104	0x0000	0x5c0e4039	0x5c0e
105	0x0000	0x4a040224	0x0224
106	0x0000	0x4a040224	0x4a04
107	0x0000	0xd49657b0	0x57b0
…	…	…	…
129	0x3c3c	0xf254ffb6	0x3c3c
130	0x3c3c	0xf254ffb6	0x3c3c
131	0xbcbc	0x14b8b17b	0xbcbc
132	0x3939	0x14b8b17b	0x2d81
133	0x0000	0x36693806	0x3806
134	0x0000	0x36693806	0x3669
135	0x3939	0x377c62a2	0x5b9b
136	0x0000	0x377c62a2	0x377c
137	0x0000	0x1dae33a6	0x33a6
…	…	…	…
201	0x0000	0x96fc2396	0x2396
202	0x0000	0x96fc2396	0x96fc

203	0x0000	0xbc51d239	0xd239
204	0x0000	0xbc51d239	0xbc51
205	0x0000	0x8908e8ac	0xe8ac
206	0x0000	0x8908e8ac	0x8908
207	0x0000	0x1d74baa3	0xbaa3
208	0x0000	0x1d74baa3	0x1d74
209	0x0000	0xd8835587	0x5587
210	0x0000	0xd8835587	0xd883
211	0x0000	0xaf70715f	0x715f
212	0x0000	0xaf70715f	0xaf70
213	0x0000	0xc861665f	0x665f
…	…	…	…
253	0x0000	0xc07ece76	0xce76
254	0x0000	0xc07ece76	0xc07e
255	0x0000	0xedf08af9	0x8af9
256	0x0000	0xedf08af9	0xedf0
257	0x0000	0xb86284bb	0x84bb
258	0x0000	0xb86284bb	0xb862
259	0xbcbc	0xb87439a6	0xbcbc
260	0x3c3c	0xb87439a6	0x3c3c
261	0x3c3c	0xf701f1ed	0x3c3c
262	0xbcbc	0xf701f1ed	0xbcbc
263	0x3939	0x523d121c	0x2b25
264	0x0000	0x523d121c	0x523d
265	0x0000	0xf96f47ae	0x47ae
266	0x3939	0xf96f47ae	0xc056
267	0x0000	0xba695c5b	0x5c5b

Table B-33. 2-lane Encrypted Output in SST mode for Inter-BS Spacing = 131

Test Vectors for 1-Lane Main Link Configuration in SST Mode (Inter-BS spacing = 130, CPSR Interval = 9)

Authentication

Table B-3 and Table B-4 provide the LFSR and Block module states during the first part of authentication.

Initial Bootstrapping

Table B-25 provides test vectors during the initial bootstrapping operation.

After start of encryption

Table B-34 provides test vectors generated after the start of encryption (beginning with the first CPSR symbol set that triggers encryption). Table B-35 provides encrypted cipher outputs.

Frame key calc started

clk	Sym clk	LFSR[59:0]	BM0[167:0]	OF0[23:16]	OF0[15:0]	BM1[167:0]	OF1[31:0]
-3	--	--	0xd20317a_3725bc8_256af5e_6b9cc06_7d7aa18_87f9092	--	--	0xd20317a_3725bc8_256af5e_6b9cc06_7d7aa18_87f9092	0x6559c03e
-2	--	--	0xd20317a_3725bc8_256af5e_6b9cc06_7d7aa18_87f9092	--	--	0xd20317a_3725bc8_256af5e_6b9cc06_7d7aa18_87f9092	0x6559c03e
-1	--	--	0xd20317a_3725bc8_256af5e_6b9cc06_7d7aa18_87f9092	--	--	0xd20317a_3725bc8_256af5e_6b9cc06_7d7aa18_87f9092	0x6559c03e
0	0	--	0xd20317a_3725bc8_256af5e_6b9cc06_7d7aa18_87f9092	--	--	0xd20317a_3725bc8_256af5e_6b9cc06_7d7aa18_87f9092	0x6559c03e
1	1	--	0xc040e35_54294b7_0000000_f523e56_bf44e50_000001d	--	--	0x9b48c65_3f7de85_4cfb937_50d9c10_5d7fbdc_6a03908	0xb79ee5fe
2	5	--	0x6666a4e_47b5444_93d46aa_a1a9cb4_a206aaa_cacfa30	--	--	0x94ede66_8141634_5f900d1_5f7a0f0_f291dcb_5a0ce6e	0x289af919
3	9	--	0x1232d67_ef6a7a5_6055678_533e54c_e4b418a_91fbcbb	--	--	0x1f69314_9a31990_c4b92db_31a6525_6ab1304_928c3d8	0xd25b5d6c
4	13	--	0x811566c_da14697_66f89db_d9ce46b_c89e263_9e3097e	--	--	0x7f0a70c_d1bda54_34c9929_7df4b37_d8d588c_855d111	0xed55dcde
…	…	…	…	…	…	…	…
32	125	--	0x58f7c56_8ff3888_97eb44c_25c4a1a_310ffae_84d8e08	--	--	0x2221028_0c49069_b9a604c_d5025c1_052df5f_59112d6	0x2f4436cb
33	129	--	0x315c455_d59f35b_40693cd_5dbf7bd_2df8f08_22cacad	--	--	0x3596433_4643480_8853c0f_95d957d_e351de7_9412e3e	0x7847ef0d
Line rekey ignored (frame key calc in progress)							
34	133	--	0x080bd0f_043ff91_b512030_bbfa516_f3753d8_957c88c	--	--	0x6267937_99593b7_3013a64_3a0aa4d_b46ea95_1e99035	0xf96f47cd
35	137	--	0x65b6244_8461884_2bffcba_a8f7581_264cecb_2cca0f2	--	--	0xdc51ed3_daa4ef1_5dafba7_4ea8052_6f0f06e_712dc22	0x30f12a24
36	141	--	0x259b412_3a73ddc_ddf0be5_8794752_f7203fa_f4acf98	--	--	0x4b2ad3d_0aed7f5_9a40045_f0dc0bd_12077f3_dc5bdc2	0xd47a2546
…	…	…	…	…	…	…	…
45	177	--	0x8b0a742_b70da1c_2307640_f0093a0_6c69ad6_2dfc26d	--	--	0x4736b27_c7ebca1_aa86bef_4539c7b_6c6bdec_c4b1f11	0x10f21d66
46	181	--	0x57dd199_d4f7e9b_b85862b_5cc55f4_2b5efea_85611ff	--	--	0x2789d57_f53ee8a_3cfeaf5_817480c_c30af76_2f49767	0x37affe86

47	185	--	0xc9472f7_c4371c6_667db05_9e19673_1fcfb80_9e1665f	--	--	0xfa07250_f725212_9bc279d_76fe61a_e1521fc_fb331b7	0x49152bc4
48	189	--	0x2aeaf01_beef443_e0cd9a0_d83548d_480c50a_5d4ed0e	--	--	0xcaf5121_1129806_3836e0a_9051c5e_34551ae_7f7b35a	0x1f068148
49	193	--	0x5cfb3bd_bb2e5ca_6f52793_8bb82fe_ea7c298_d9a59fa	--	--	0x62e765a_09101ee_f92cab1_4cfd7ca_f8ad063_1f97804	0xb79cb954
50	197	0x0f53e0a6257702fe	0x8bb82fe_ea7c298_d9a59fa_f523e56_bf44e50_000001d	--	--	0x960d99e_e9b8b0f_782d158_645c7a9_312615f_ca46465	0xfe492f2a
51	201	0x0ea7c94c42ee05fd	0xb486149_cca6e3d_0355dff_2262329_a206aaa_cacfa30	--	--	0xb72431d_495f294_aba13a4_c1a5edc_d8ea59b_2cbcad0	0x53331e18
52	205	0x0d4f929885dc0bfb	0x120ec20_a1030d1_4c72806_a00fb45_e4b418a_75af954	--	--	0xe94a5e8_bad382a_b516ee3_2aea12a_04f35e9_6a44723	0x5c0e4039
53	209	0x0a9f253103b837f6	0xc084d58_ee8b642_7dd6814_079525e_aef8c5e_ada7f43	--	--	0x8b46a53_283034d_84a452f_9958918_06c7952_3d3b8d2	0x4a040224
54	213	0x053e42620f704fec	0xa45476a_cc524a0_e8b84ed_ed3997e_6fd0590_43c8e4c	--	--	0x3256280_505a587_885c3a1_e9a868e_d1e9b70_d727f22	0xd49657b0
…	…	…	…	…	…	…	…
64	253	0x0914083b892b3051	0x5bfdd23_7ca0b5a_c12f127_495854a_19f3173_1c1ac03	--	--	0x8020fe9_f55f9f4_8fef65e_58f4d4b_bf0fe4e_d6f769b	0xc5f3500b
65	257	0x02281877125640a2	0xa1ac713_e2d283a_482c2bb_d437443_bd8ef95_076c262	--	--	0xbdc2425_78138b1_fae8859_7b0d9b3_9007256_f02725b	0xf254ffb6
Line rekey ignored (frame key calc in progress)							
66	261	0x045030ee2cac8144	0x3e289e0_1b214d0_e90ac42_1504b3f_58bc895_c98fa75	--	--	0x6ad3eed_82e9428_1f151a0_fefc1c7_231e1e6_0e7b8ba	0x14b8b17b
67	265	0x08a061dc59590289	0x0e8407c_bb5df9d_578e9dd_6e1b212_7e16013_78ef703	--	--	0xbcf19db_fd7dda6_60704fe_0a9e816_1645fbc_7b03898	0x36693806
68	269	0x0140c3b8b2b22512	0x7d0a4b8_3eda746_1d77d70_0293f78_0031fd6_6dab5e6	--	--	0x6ffb9d8_4b94ccf_9e88e41_6fd5114_b45199e_2be2560	0x377c62a2
…	…	…	…	…	…	…	…
96	381	0x0a42a093abe0e662	0xa484b59_ef409db_2099d43_fa392a8_d652e3b_858f2fc	--	--	0x8f75a0a_cd4dd88_4f85d46_9e81bd1_339d041_abfc845	0x158ec50e
97	385	0x0485492757c1ccc5	0x11bdfc4_3f44509_dc60452_8edd2a4_e4559ab_8b6d4fe	--	--	0xd3b12c9_844aafa_898747c_bbb6e5e_2227eca_65f628b	0x64408b2c
98	389	0x090a924ea783998b	0x7b231ab_9d1a11b_aff6b1e_47d273f_c29f20f_81f9565	--	--	0x340a433_93e7bdf_71416c2_002b998_4c9ad89_96f283c	0x03b468b1
Line rekey ignored (frame key calc in progress)							
99	393	0x0215249d4f073316	0x42b915a_4075db8_54cbde6_2fff97e_9882703_c1ac336	--	--	0x4ece638_a7d51a9_7f9e886_f70ae3d_7bb4fdb_35f33c7	0x9328a53d
100	397	0x042a493a960e662d	0x0960b32_d33d3ea_415be5f_662f358_ea77b3e_bae1860	--	--	0x0eea7d6_bdf8fd6_29fff0a_a341b36_7b88cea_18ceb50	0xb5e38b64
101	401	0x08549a75241cec5b	0x283bb5d_356dc1d_5ef8302_740b636_1e2bbb1_77a9024	--	--	0x06af6be_8574776_6244dc1_1c04bf2_7da1a03_e962e82	0x96fc2396
102	405	0x00a934ea4839f8b6	0xd1bdb61_18b2c89_06d55fe_85d7861_4a2d2c4_3f0f76a	--	0x6a42	0x8000eaf_8f340fb_57fba9a_ece383b_5d4ccf2_e2ff34b	0xbc51d239
103	409	0x015269d49873d16c		--	0xb1db		0x8908e8ac

			0xabddb90_19d2b4a_7540b7a_458c215_014c756_aca7735			0x394e745_ec99143_e3f8f19_375ec6c_39c7cef_ba78801	
104	413	0x02a4d3a938e782d8	0x924eb87_b7a728b_8f829c6_35dd971_63da5b0_486ff01	0x97	0xd7a3	0x398cfb0_51408ef_9500162_a935d4f_835f420_da99144	0x1d74baa3
105	417	0x0549af5279cf05b1	0x711d28b_ffa6fca_923e67b_15707a7_42a4bb2_2deda6d	0xbb	0xb0f9	0xde9d7c1_83df898_1e55332_ddc9add_a82acb2_2885c03	0xd8835587
106	421	0x0a935ea4f39e2b63	0xeff1213_e232b20_0064b82_ae1968a_4a3cba4_40cb306	0x62	0x84bb	0xd887f8b_5d37e0d_fe4d145_6a55c77_9369bfb_5028d20	0xaf70715f
107	425	0x0a935ea4f39e2b63	0xeff1213_e232b20_0064b82_ae1968a_4a3cba4_40cb306	0x62	0x84bb	0xb77f694_6fed836_ec5fbda_befa034_2c5d690_ae478e9	0xc861665f
108	429	0x0a935ea4f39e2b63	0xeff1213_e232b20_0064b82_ae1968a_4a3cba4_40cb306	0x62	0x84bb	0xa67d45e_0b30f7d_2bb93be_e09b5f5_22ca847_b849198	0x2bbcf09a
109	433	0x0a935ea4f39e2b63	0xeff1213_e232b20_0064b82_ae1968a_4a3cba4_40cb306	0x62	0x84bb	0xbc0eacd_d272a44_b4bd07a_9968125_908c788_ad1214e	0xd4bd6f59
…	…	…	…	…	…	…	…
127	505	0x0a935ea4f39e2b63	0xeff1213_e232b20_0064b82_ae1968a_4a3cba4_40cb306	0x62	0x84bb	0x6886c93_2065e45_773f684_82237f8_df3ef7a_cae90a7	0xc07ece76
128	509	0x0a935ea4f39e2b63	0xeff1213_e232b20_0064b82_ae1968a_4a3cba4_40cb306	0x62	0x84bb	0x9359a39_d450a12_51ce5bc_d3062b6_2c9cca3_c74edc4	0xedf08af9
129	513	0x0a935ea4f39e2b63	0xeff1213_e232b20_0064b82_ae1968a_4a3cba4_40cb306	0x62	0x84bb	0xeff1213_e232b20_0064b82_ae1968a_4a3cba4_40cb306	0xb86284bb
130	517	0x0526b549e73c76c7	0xddd552f_3d3bac2_fb230d5_83a2d78_5a1da41_8fed1d6	0x74	0x39a6	0xddd552f_3d3bac2_fb230d5_83a2d78_5a1da41_8fed1d6	0xb87439a6
Line rekey started							
clk	**Sym clk**	**LFSR[59:0]**	**BM0[167:0]**	**OF0[23:16]**	**OF0[15:0]**	**BM1[167:0]**	**OF1[31:0]**
-3	--	0x0a935ea4f39e2b63	0xeff1213_e232b20_0064b82_ae1968a_4a3cba4_40cb306	--	--	0x9359a39_d450a12_51ce5bc_d3062b6_2c9cca3_c74edc4	0xedf08af9
-2	--	0x0a935ea4f39e2b63	0xeff1213_e232b20_0064b82_ae1968a_4a3cba4_40cb306	--	--	0xeff1213_e232b20_0064b82_ae1968a_4a3cba4_40cb306	0xb86284bb
-1	--	0x0526b549e73c76c7	0xddd552f_3d3bac2_fb230d5_83a2d78_5a1da41_8fed1d6	--	--	0xddd552f_3d3bac2_fb230d5_83a2d78_5a1da41_8fed1d6	0xb87439a6
0	520	0x0526b549e73c76c7	0xddd552f_3d3bac2_fb230d5_83a2d78_5a1da41_8fed1d6	--	--	0xddd552f_3d3bac2_fb230d5_83a2d78_5a1da41_8fed1d6	0xb87439a6
1	521	0x0a4d6293ce78ed8e	0xc258963_5d097d0_e50aa7c_fc50f00_a2a747b_a45b784	--	--	0xc258963_5d097d0_e50aa7c_fc50f00_a2a747b_a45b784	0xf701f1ed
2	525	0x049ac5279cf1fb1c	0xb06e6b7_c8209e8_82982f7_4bc1a13_8a3f797_9f0446e	--	--	0xb06e6b7_c8209e8_82982f7_4bc1a13_8a3f797_9f0446e	0x523d121c
3	529	0x09358a4f31e3d639	0xefd27df_0e46509_e0b63da_cb3dc05_af53ae8_4436e20	--	--	0xefd27df_0e46509_e0b63da_cb3dc05_af53ae8_4436e20	0xf96f47ae
…	…	…	…	…	…	…	…
32	645	0x0a1ff9b72023b8b0	0x1eddec2_367c831_dfa58d0_bde33d6_c404795_6d6649c	--	--	0xf05af93_ac6c798_15d7af6_0645bf3_fb3db41_8ac0307	0x7acceb15
33	649	0x043ffb6e40477160	0x4a342ae_82a9a69_1f8a0d6_7852eba_50bcd92_f0ca19b	--	--	0x126d6a1_c8267a1_d20ba63_1d62a80_4849d54_c22adc6	0xcafb3096
Line rekey ignored (line rekey in progress)							

34	653	0x087ff6dc808ee2c0	0xacd0bda_d7d29d8_a2da5ac_535a6be_7b87b62_3dc28c5	--	--	0x090c831_428d360_ae27819_7cdfcea_2f86695_f5113b9	0xc50ff5c5
35	657	0x00ffedb9091de580	0xfe540b1_c0aa0d3_dc2cc45_c9ace54_b5a739e_9384394	--	--	0xd90e59c_f9f3d1b_6480004_14d76a9_ba528a2_170c303	0xce6d0db0
…	…	…	…	…	…	…	…
51	721	0x0934a6387ba6fed0	0xb39166a_8c1b092_9679527_b34e394_86a9ea3_8c02b91	--	--	0x01eab39_3961796_96cf800_65550a2_286c641_1cf5ec3	0xcdd5ddb2
52	725	0x02694c70f74ddda1	0x014c513_1161f8b_41c9b49_a64a8b3_0ad9135_6c6337b	--	--	0x88eca24_fa0719b_0e475ea_fd01238_77fac9c_2a2fe35	0x241e4836
53	729	0x04d290e1ee9bbb43	0x5f74778_7bae847_3858c2e_6d9a242_bc9a02f_e4fdf87	--	--	0x276fafa_fb8c5a8_95210b1_8d295f2_09e27e6_b737720	0x673be722
54	733	0x09a529c3d5375686	0x41c3db8_7e60b5d_ade6c26_0335bb1_0313ffb_ce6d556	--	--	0xde83510_f93dd7e_8f09cca_fd7e979_439879a_5870c89	0x0e661a04
55	737	0x034a5387aa6ead0c	0xda39225_0d2f8e6_487e46d_14adaff_c23321e_7e5a780	--	--	0x9fd4127_873eeab_d443857_d7bc533_04fa8ab_a4eee09	0xe8b7ea1e
56	741	0x0694af0f54dd7a18	0xb6bee9e_b0ef775_f7d10ad_5dce396_89b2597_acef7ea	--	--	0xd5858aa_e4354ca_b52fefd_c3e62de_3960ed5_cbc6aa5	0xac7e0ebc
57	745	0x0694af0f54dd7a18	0xb6bee9e_b0ef775_f7d10ad_5dce396_89b2597_acef7ea	--	--	0xed3734d_00d67e7_eb76874_e2d404c_09ed965_dc23211	0x233bf0c3
58	749	0x0694af0f54dd7a18	0xb6bee9e_b0ef775_f7d10ad_5dce396_89b2597_acef7ea	--	--	0xe17cdec_bc66357_8450c0e_5f72374_878db0c_6b13d1e	0x16208c84
…	…	…	…	…	…	…	…
63	769	0x0694af0f54dd7a18	0xb6bee9e_b0ef775_f7d10ad_5dce396_89b2597_acef7ea	--	--	0x5b908ab_b2fdadc_ab7f84a_88d8992_bb6fc94_30a7b52	0xe228cfc1
64	773	0x0694af0f54dd7a18	0xb6bee9e_b0ef775_f7d10ad_5dce396_89b2597_acef7ea	--	--	0x9f12b63_096eeec_28e9b90_a572681_09e03f4_85a8ee3	0x681b908d
65	777	0x0694af0f54dd7a18	0xb6bee9e_b0ef775_f7d10ad_5dce396_89b2597_acef7ea	--	--	0xb6bee9e_b0ef775_f7d10ad_5dce396_89b2597_acef7ea	0xabaaaf5a
Line rekey started							
clk	**Sym clk**	**LFSR[59:0]**	**BM0[167:0]**	**OF0[23:16]**	**OF0[15:0]**	**BM1[167:0]**	**OF1[31:0]**
-3	--	0x0694af0f54dd7a18	0xb6bee9e_b0ef775_f7d10ad_5dce396_89b2597_acef7ea	--	--	0x5b908ab_b2fdadc_ab7f84a_88d8992_bb6fc94_30a7b52	0xe228cfc1
-2	--	0x0694af0f54dd7a18	0xb6bee9e_b0ef775_f7d10ad_5dce396_89b2597_acef7ea	--	--	0x9f12b63_096eeec_28e9b90_a572681_09e03f4_85a8ee3	0x681b908d
-1	--	0x0694af0f54dd7a18	0xb6bee9e_b0ef775_f7d10ad_5dce396_89b2597_acef7ea	--	--	0xb6bee9e_b0ef775_f7d10ad_5dce396_89b2597_acef7ea	0xabaaaf5a
0	780	0x0694af0f54dd7a18	0xb6bee9e_b0ef775_f7d10ad_5dce396_89b2597_acef7ea	--	--	0xb6bee9e_b0ef775_f7d10ad_5dce396_89b2597_acef7ea	0xabaaaf5a
1	781	0x0d29561ea1bad430	0x0beb3a9_cb636c5_ce7a6d6_3ab9bdb_c93d31b_c325019	--	--	0x0beb3a9_cb616c5_ce7a6d6_3ab9bdb_c93d31b_c325019	0x0b6d3310
2	785	0x0a52a43d4b758861	0x6a3ad12_9856416_6c93fda_e14a23d_fbc4d3f_cceecdf	--	--	0x6a3ad12_ba76634_6c93fda_c14a23d_fbc4d3f_cceecdf	0xcd7c74f2
3	789	0x04a5487a96eb30c2	0x6a9b47c_328300c_494b633_ca430af_69d5a81_2aca65b	--	--	0x8475a72_8b20bb7_494b633_cbc72b7_69d5a81_0a8a65b	0xb840f90b

…	…	…	…	…	…	…	…
32	905	0x0faa8d210bbc53cc	0x9e20232_1b8852c_da7850c_69a0ccf_09711f8_1bff46c	--	--	0x6346d78_498b996_2df1893_143ee9a_48ea3a7_698c386	0x28dfb66d
33	909	0x0f5512421f78a798	0xc0cbd80_ad28630_d9d0a19_422ea4e_bddd575_6d11e44	--	--	0x35c5b26_85f8221_89bcc6c_ca3c8e8_0759551_7f7f36b	0xd332bbd6
Line rekey ignored (line rekey in progress)							
34	913	0x0eaa24843ef16f31	0x794a3d2_b913293_dc1755f_0394182_e94bdc4_3b60b30	--	--	0x436f362_313a7d9_74f9699_db94187_c869310_31eaa13	0x14ad3c71
35	917	0x0d54490875e2de63	0xe2b3f71_443f61a_f93d67b_c7266b5_c10857c_08a2e37	--	--	0x7f867d8_37dccb8_f9ad872_ebba5cb_406c9e0_cb2389a	0xa1eeb626
…	…	…	…	…	…	…	…
52	985	0x09d88114a91d6c86	0x158c91b_e318b99_beb3950_3261d4d_11ed2fc_cddbf33	--	--	0xdd4cbea_e2291a5_0790d34_cd78b17_b2ba07c_472207a	0x0b11e356
53	989	0x03b10229523af90d	0xea16628_c0a7e70_6830104_292dab8_472ab7a_94bf148	--	--	0x9ae1079_2563218_0bb4370_b3ec2a2_1237195_9312c25	0x335ce895
54	993	0x07620452ac75f21a	0x59dfc75_a004a32_88e6c6e_fb13a24_e0d0832_527ea13	--	--	0xf8cf95b_ffd5e27_f2c1cc7_70c42fa_9cf89b7_b10391d	0xe6b9cdca
55	997	0x0ec400a550ebc434	0xfad6e6f_5f6fdb3_d540264_dcffdd2_6c56b8a_20339ee	--	--	0xe640131_5eccf76_402b806_ab13ed0_4b35670_f6e6475	0xc8fdaa38
56	1001	0x0d88014aa9d78868	0x3877c5f_6897f66_20df19d_f362ef4_1d4b3ac_c306a61	--	--	0xc4ca394_c370a68_af900b7_41db7ce_319fbf5_8ac799e	0x758db7f6
57	1005	0x0d88014aa9d78868	0x3877c5f_6897f66_20df19d_f362ef4_1d4b3ac_c306a61	--	--	0x16e9a66_d7d3dd4_e4deb61_55def1e_3c5e946_c4682e7	0x8bd0f8ac
58	1009	0x0d88014aa9d78868	0x3877c5f_6897f66_20df19d_f362ef4_1d4b3ac_c306a61	--	--	0x18fbf5e_2fc6f5e_559b25b_a26b764_2f36fa3_d301a85	0xcbf58ee5
…	…	…	…	…	…	…	…
63	1029	0x0d88014aa9d78868	0x3877c5f_6897f66_20df19d_f362ef4_1d4b3ac_c306a61	--	--	0x7e0ae16_884db5b_0bb4b68_0a1e5f8_6c38195_ff4c09b	0xb1056ff8
64	1033	0x0d88014aa9d78868	0x3877c5f_6897f66_20df19d_f362ef4_1d4b3ac_c306a61	--	--	0x9eb4b99_b784a43_554b033_5068a0a_3652f72_45e1b03	0xe29bb233
65	1037	0x0d88014aa9d78868	0x3877c5f_6897f66_20df19d_f362ef4_1d4b3ac_c306a61	--	--	0x3877c5f_6897f66_20df19d_f362ef4_1d4b3ac_c306a61	0xed8f9447
Line rekey started							
clk	**Sym clk**	**LFSR[59:0]**	**BM0[167:0]**	**OF0[23:16]**	**OF0[15:0]**	**BM1[167:0]**	**OF1[31:0]**
-3	--	0x0d88014aa9d78868	0x3877c5f_6897f66_20df19d_f362ef4_1d4b3ac_c306a61	--	--	0x7e0ae16_884db5b_0bb4b68_0a1e5f8_6c38195_ff4c09b	0xb1056ff8
-2	--	0x0d88014aa9d78868	0x3877c5f_6897f66_20df19d_f362ef4_1d4b3ac_c306a61	--	--	0x9eb4b99_b784a43_554b033_5068a0a_3652f72_45e1b03	0xe29bb233
-1	--	0x0d88014aa9d78868	0x3877c5f_6897f66_20df19d_f362ef4_1d4b3ac_c306a61	--	--	0x3877c5f_6897f66_20df19d_f362ef4_1d4b3ac_c306a61	0xed8f9447
0	1040	0x0d88014aa9d78868	0x3877c5f_6897f66_20df19d_f362ef4_1d4b3ac_c306a61	--	--	0x3877c5f_6897f66_20df19d_f362ef4_1d4b3ac_c306a61	0xed8f9447
1	1041	0x0b100a955baf10d0	0xee5976d_b4255e6_00a9f64_cb596c6_165b075_aac6b82	--	--	0xee5976d_b4275e6_00a9f64_cb596c6_165b075_aac6b82	0xac6ca86f

2	1045	0x0620152ab75e01a0	0xdcf5875_52832e7_c6b95ed_4af3a31_4761d31_42d51ac	--	--	0xdcf5875_70a30c5_c6b95ed_6af3a31_4761d31_42d51ac	0x097cba38
3	1049	0x0c4022556ebc0341	0x3a50a7a_cf93a57_d44036c_637c92a_2c8387b_1906d46	--	--	0xd4be474_76321ec_d44036c_62f8b32_2c8387b_3946d46	0x38e5e68b
…	…	…	…	…	…	…	…
31	1161	0x06c95fc7cbd4caea	0xfdc5cc7_b507124_bc32f03_7b3d7e2_ed85fe6_e096f6f	--	--	0x89b5021_93d5992_50ac7b1_adf6ad1_303116d_a26b698	0x0c32ffa3
32	1165	0x0d92bf8f97a9b5d4	0xc804851_43465fa_79550d0_ae63875_3cef24d_0d49077	--	--	0xd4e7f92_5925086_f9e3242_e4cb6b6_1616e96_bcc6da4	0x3d5ca893
33	1169	0x0b25771f2f534ba8	0x86182cc_e81a4a7_e001066_7e05787_fef01ff_fd56f44	--	--	0xa40e296_6736de2_ce6f048_8320090_09f8877_ac4839b	0xb2d49ebf
Line rekey discarded, frame key calc started							
clk	**Sym clk**	**LFSR[59:0]**	**BM0[167:0]**	**OF0[23:16]**	**OF0[15:0]**	**BM1[167:0]**	**OF1[31:0]**
-3	--	--	0xfdc5cc7_b507124_bc32f03_7b3d7e2_ed85fe6_e096f6f	--	--	0x89b5021_93d5992_50ac7b1_adf6ad1_303116d_a26b698	0x0c32ffa3
-2	--	--	0xc804851_43465fa_79550d0_ae63875_3cef24d_0d49077	--	--	0xd4e7f92_5925086_f9e3242_e4cb6b6_1616e96_bcc6da4	0x3d5ca893
-1	--	--	0x86182cc_e81a4a7_e001066_7e05787_fef01ff_fd56f44	--	--	0xa40e296_6736de2_ce6f048_8320090_09f8877_ac4839b	0xb2d49ebf
0	1170	--	0x86182cc_e81a4a7_e001066_7e05787_fef01ff_fd56f44	--	--	0xa40e296_6736de2_ce6f048_8320090_09f8877_ac4839b	0xb2d49ebf
1	1171	--	0xc040e35_54294b7_0000000_7a3b0f9_42b1dbd_000006a	--	--	0x6a27a80_79a39b3_a61ea62_7d71689_83bd599_d357fa6	0x8a74734e
2	1175	--	0x6666a4e_47b5444_93d46aa_e4f374f_3cd0333_212d6ab	--	--	0xfe39743_4a35128_1b32a92_9b496ba_7394c08_7ca393c	0x027787b2
3	1179	--	0x1232d67_ef6a7a5_6055678_d509b9f_427d387_e30af77	--	--	0x8e9c0fa_71756da_8a609cd_e818b0c_b33990f_d316390	0xa8067c60
4	1183	--	0x811566c_da14697_66f89db_84306fe_411d172_f9e3620	--	--	0x0401baf_6698ed7_9e69ef2_8d1ab25_f2ecea2_a714d6e	0xc0a584a5
5	1187	--	0xf7027a4_dc24164_29716cf_f0cd06e_9fad21f_41cbe85	--	--	0xebbc23c_5ca8af6_b67be11_2c4af10_e436e94_66fbc55	0xebf55c01

Table B-34. Cipher State in SST Mode for 1-lane, Inter-BS Spacing = 130

Sym clk	stream	cipher	encrypted stream
-3	0x1c	0x6559c03e	0x1c
-2	0x3c	0x6559c03e	0x3c
-1	0x3c	0x6559c03e	0x3c
0	0x1c	0x6559c03e	0x1c
1	0x39	0xb79ee5fe	0xc7
2	0x00	0xb79ee5fe	0xe5
3	0x00	0xb79ee5fe	0x9e
4	0x39	0xb79ee5fe	0x8e
5	0x00	0x289af919	0x19
6	0x00	0x289af919	0xf9
7	0x39	0x289af919	0xa3
8	0x00	0x289af919	0x28
9	0x00	0xd25b5d6c	0x6c
10	0x39	0xd25b5d6c	0x64
11	0x00	0xd25b5d6c	0x5b
12	0x00	0xd25b5d6c	0xd2
13	0x00	0xed55dcde	0xde
…	…	…	…
125	0x00	0x2f4436cb	0xcb
126	0x00	0x2f4436cb	0x36
127	0xbc	0x2f4436cb	0xbc
128	0x3c	0x2f4436cb	0x3c
129	0x3c	0x7847ef0d	0x3c
130	0xbc	0x7847ef0d	0xbc
131	0x39	0x7847ef0d	0x7e
132	0x00	0x7847ef0d	0x78
133	0x00	0xf96f47cd	0xcd
134	0x39	0xf96f47cd	0x7e
135	0x00	0xf96f47cd	0x6f
136	0x00	0xf96f47cd	0xf9
137	0x39	0x30f12a24	0x1d
138	0x00	0x30f12a24	0x2a
139	0x00	0x30f12a24	0xf1
140	0x39	0x30f12a24	0x09
141	0x00	0xd47a2546	0x46
…	…	…	…
177	0x00	0x10f21d66	0x66
178	0x00	0x10f21d66	0x1d
179	0x00	0x10f21d66	0xf2
180	0x00	0x10f21d66	0x10
181	0x00	0x37affe86	0x86

182	0x00	0x37affe86	0xfe
183	0x00	0x37affe86	0xaf
184	0x00	0x37affe86	0x37
185	0x00	0x49152bc4	0xc4
186	0x00	0x49152bc4	0x2b
187	0x00	0x49152bc4	0x15
188	0x00	0x49152bc4	0x49
189	0x00	0x1f068148	0x48
190	0x00	0x1f068148	0x81
191	0x00	0x1f068148	0x06
192	0x00	0x1f068148	0x1f
193	0x00	0xb79cb954	0x54
194	0x00	0xb79cb954	0xb9
195	0x00	0xb79cb954	0x9c
196	0x00	0xb79cb954	0xb7
197	0x00	0xfe492f2a	0x2a
198	0x00	0xfe492f2a	0x2f
199	0x00	0xfe492f2a	0x49
200	0x00	0xfe492f2a	0xfe
201	0x00	0x53331e18	0x18
202	0x00	0x53331e18	0x1e
203	0x00	0x53331e18	0x33
204	0x00	0x53331e18	0x53
205	0x00	0x5c0e4039	0x39
206	0x00	0x5c0e4039	0x40
207	0x00	0x5c0e4039	0x0e
208	0x00	0x5c0e4039	0x5c
209	0x00	0x4a040224	0x24
210	0x00	0x4a040224	0x02
211	0x00	0x4a040224	0x04
212	0x00	0x4a040224	0x4a
213	0x00	0xd49657b0	0xb0
…	…	…	…
253	0x00	0xc5f3500b	0x0b
254	0x00	0xc5f3500b	0x50
255	0x00	0xc5f3500b	0xf3
256	0x00	0xc5f3500b	0xc5
257	0xbc	0xf254ffb6	0xbc
258	0x3c	0xf254ffb6	0x3c
259	0x3c	0xf254ffb6	0x3c
260	0xbc	0xf254ffb6	0xbc
261	0x39	0x14b8b17b	0x42
262	0x00	0x14b8b17b	0xb1
263	0x00	0x14b8b17b	0xb8

264	0x39	0x14b8b17b	0x2d
265	0x00	0x36693806	0x06
266	0x00	0x36693806	0x38
267	0x39	0x36693806	0x50
268	0x00	0x36693806	0x36
269	0x00	0x377c62a2	0xa2
…	…	…	…
381	0x00	0x158ec50e	0x0e
382	0x00	0x158ec50e	0xc5
383	0x00	0x158ec50e	0x8e
384	0x00	0x158ec50e	0x15
385	0x00	0x64408b2c	0x2c
386	0x00	0x64408b2c	0x8b
387	0xbc	0x64408b2c	0xbc
388	0x3c	0x64408b2c	0x3c
389	0x3c	0x03b468b1	0x3c
390	0xbc	0x03b468b1	0xbc
391	0x39	0x03b468b1	0x8d
392	0x00	0x03b468b1	0x03
393	0x00	0x9328a53d	0x3d
394	0x39	0x9328a53d	0x9c
395	0x00	0x9328a53d	0x28
396	0x00	0x9328a53d	0x93
397	0x39	0xb5e38b64	0x5d
398	0x00	0xb5e38b64	0x8b
399	0x00	0xb5e38b64	0xe3
400	0x39	0xb5e38b64	0x8c
401	0x00	0x96fc2396	0x96
402	0x00	0x96fc2396	0x23
403	0x00	0x96fc2396	0xfc
404	0x00	0x96fc2396	0x96
405	0x00	0xbc51d239	0x39
406	0x00	0xbc51d239	0xd2
407	0x00	0xbc51d239	0x51
408	0x00	0xbc51d239	0xbc
409	0x00	0x8908e8ac	0xac
410	0x00	0x8908e8ac	0xe8
411	0x00	0x8908e8ac	0x08
412	0x00	0x8908e8ac	0x89
413	0x00	0x1d74baa3	0xa3
414	0x00	0x1d74baa3	0xba
415	0x00	0x1d74baa3	0x74
416	0x00	0x1d74baa3	0x1d
417	0x00	0xd8835587	0x87

418	0x00	0xd8835587	0x55
419	0x00	0xd8835587	0x83
420	0x00	0xd8835587	0xd8
421	0x00	0xaf70715f	0x5f
422	0x00	0xaf70715f	0x71
423	0x00	0xaf70715f	0x70
424	0x00	0xaf70715f	0xaf
425	0x00	0xc861665f	0x5f
426	0x00	0xc861665f	0x66
427	0x00	0xc861665f	0x61
428	0x00	0xc861665f	0xc8
429	0x00	0x2bbcf09a	0x9a
430	0x00	0x2bbcf09a	0xf0
431	0x00	0x2bbcf09a	0xbc
432	0x00	0x2bbcf09a	0x2b
433	0x00	0xd4bd6f59	0x59
…	…	…	…
505	0x00	0xc07ece76	0x76
506	0x00	0xc07ece76	0xce
507	0x00	0xc07ece76	0x7e
508	0x00	0xc07ece76	0xc0
509	0x00	0xedf08af9	0xf9
510	0x00	0xedf08af9	0x8a
511	0x00	0xedf08af9	0xf0
512	0x00	0xedf08af9	0xed
513	0x00	0xb86284bb	0xbb
514	0x00	0xb86284bb	0x84
515	0x00	0xb86284bb	0x62
516	0x00	0xb86284bb	0xb8
517	0xbc	0xb87439a6	0xbc
518	0x3c	0xb87439a6	0x3c
519	0x3c	0xb87439a6	0x3c
520	0xbc	0xb87439a6	0xbc
521	0x39	0xf701f1ed	0xd4
522	0x00	0xf701f1ed	0xf1
523	0x00	0xf701f1ed	0x01
524	0x39	0xf701f1ed	0xce
525	0x00	0x523d121c	0x1c

Table B-35. 1-lane Encrypted Output in SST mode for Inter-BS Spacing = 130

Test Vectors for 1-Lane Main Link Configuration in SST Mode (Inter-BS spacing = 131, CPSR Interval = 9)

Authentication

Table B-3 and Table B-4 provide the LFSR and Block module states during the first part of authentication.

Initial Bootstrapping

Table B-25 provides test vectors during the initial bootstrapping operation.

After start of encryption

Table B-36 provides test vectors generated after the start of encryption (beginning with the first CPSR symbol set that triggers encryption). Table B-37 provides encrypted cipher outputs.

Frame key calc started							
clk	**Sym clk**	**LFSR[59:0]**	**BM0[167:0]**	**OF0[23:16]**	**OF0[15:0]**	**BM1[167:0]**	**OF1[31:0]**
-3	--	--	0xd20317a_3725bc8_256af5e_6b9cc06_7d7aa18_87f9092	--	--	0xd20317a_3725bc8_256af5e_6b9cc06_7d7aa18_87f9092	0x6559c03e
-2	--	--	0xd20317a_3725bc8_256af5e_6b9cc06_7d7aa18_87f9092	--	--	0xd20317a_3725bc8_256af5e_6b9cc06_7d7aa18_87f9092	0x6559c03e
-1	--	--	0xd20317a_3725bc8_256af5e_6b9cc06_7d7aa18_87f9092	--	--	0xd20317a_3725bc8_256af5e_6b9cc06_7d7aa18_87f9092	0x6559c03e
0	0	--	0xd20317a_3725bc8_256af5e_6b9cc06_7d7aa18_87f9092	--	--	0xd20317a_3725bc8_256af5e_6b9cc06_7d7aa18_87f9092	0x6559c03e
1	1	--	0xc040e35_54294b7_0000000_f523e56_bf44e50_000001d	--	--	0x9b48c65_3f7de85_4cfb937_50d9c10_5d7fbdc_6a03908	0xb79ee5fe
2	5	--	0x6666a4e_47b5444_93d46aa_a1a9cb4_a206aaa_cacfa30	--	--	0x94ede66_8141634_5f900d1_5f7a0f0_f291dcb_5a0ce6e	0x289af919
3	9	--	0x1232d67_ef6a7a5_6055678_533e54c_e4b418a_91fbcbb	--	--	0x1f69314_9a31990_c4b92db_31a6525_6ab1304_928c3d8	0xd25b5d6c
4	13	--	0x811566c_da14697_66f89db_d9ce46b_c89e263_9e3097e	--	--	0x7f0a70c_d1bda54_34c9929_7df4b37_d8d588c_855d111	0xed55dcde
…	…	…	…	…	…	…	…
32	125	--	0x58f7c56_8ff3888_97eb44c_25c4a1a_310ffae_84d8e08	--	--	0x2221028_0c49069_b9a604c_d5025c1_052df5f_59112d6	0x2f4436cb
33	129	--	0x315c455_d59f35b_40693cd_5dbf7bd_2df8f08_22cacad	--	--	0x3596433_4643480_8853c0f_95d957d_e351de7_9412e3e	0x7847ef0d
Line rekey ignored (frame key calc in progress)							
34	133	--	0x080bd0f_043ff91_b512030_bbfa516_f3753d8_957c88c	--	--	0x6267937_99593b7_3013a64_3a0aa4d_b46ea95_1e99035	0xf96f47cd
35	137	--	0x65b6244_8461884_2bffcba_a8f7581_264cecb_2cca0f2	--	--	0xdc51ed3_daa4ef1_5dafba7_4ea8052_6f0f06e_712dc22	0x30f12a24

36	141	--	0x259b412_3a73ddc_ddf0be5_8794752_f7203fa_f4acf98	--	--	0x4b2ad3d_0aed7f5_9a40045_f0dc0bd_12077f3_dc5bdc2	0xd47a2546
…	…	…	…	…	…	…	…
46	181	--	0x57dd199_d4f7e9b_b85862b_5cc55f4_2b5efea_85611ff	--	--	0x2789d57_f53ee8a_3cfeaf5_817480c_c30af76_2f49767	0x37affe86
47	185	--	0xc9472f7_c4371c6_667db05_9e19673_1fcfb80_9e1665f	--	--	0xfa07250_f725212_9bc279d_76fe61a_e1521fc_fb331b7	0x49152bc4
48	189	--	0x2aeaf01_beef443_e0cd9a0_d83548d_480c50a_5d4ed0e	--	--	0xcaf5121_1129806_3836e0a_9051c5e_34551ae_7f7b35a	0x1f068148
49	193	--	0x5cfb3bd_bb2e5ca_6f52793_8bb82fe_ea7c298_d9a59fa	--	--	0x62e765a_09101ee_f92cab1_4cfd7ca_f8ad063_1f97804	0xb79cb954
…	…	…	…	…	…	…	…
50	197	0x0f53e0a6257702fe	0x8bb82fe_ea7c298_d9a59fa_f523e56_bf44e50_000001d	--	--	0x960d99e_e9b8b0f_782d158_645c7a9_312615f_ca46465	0xfe492f2a
51	201	0x0ea7c94c42ee05fd	0xb486149_cca6e3d_0355dff_2262329_a206aaa_cacfa30	--	--	0xb72431d_495f294_aba13a4_c1a5edc_d8ea59b_2cbcad0	0x53331e18
52	205	0x0d4f929885dc0bfb	0x120ec20_a1030d1_4c72806_a00fb45_e4b418a_75af954	--	--	0xe94a5e8_bad382a_b516ee3_2aea12a_04f35e9_6a44723	0x5c0e4039
…	…	…	…	…	…	…	…
65	257	0x02281877125640a2	0xa1ac713_e2d283a_482c2bb_d437443_bd8ef95_076c262	--	--	0xbdc2425_78138b1_fae8859_7b0d9b3_9007256_f02725b	0xf254ffb6
66	261	0x045030ee2cac8144	0x3e289e0_1b214d0_e90ac42_1504b3f_58bc895_c98fa75	--	--	0x6ad3eed_82e9428_1f151a0_fefc1c7_231e1e6_0e7b8ba	0x14b8b17b
Line rekey ignored (frame key calc in progress)							
67	265	0x08a061dc59590289	0x0e8407c_bb5df9d_578e9dd_6e1b212_7e16013_78ef703	--	--	0xbcf19db_fd7dda6_60704fe_0a9e816_1645fbc_7b03898	0x36693806
68	269	0x0140c3b8b2b22512	0x7d0a4b8_3eda746_1d77d70_0293f78_0031fd6_6dab5e6	--	--	0x6ffb9d8_4b94ccf_9e88e41_6fd5114_b45199e_2be2560	0x377c62a2
69	273	0x02818f7165646a25	0x16477db_148dbef_208e96f_3b2aeca_7a8b1e0_2df93a0	--	--	0x0466847_2bf5700_cf0dfc9_79a99b7_e39c678_6e62432	0x1dae33a6
…	…	…	…	…	…	…	…
97	385	0x0485492757c1ccc5	0x11bdfc4_3f44509_dc60452_8edd2a4_e4559ab_8b6d4fe	--	--	0xd3b12c9_844aafa_898747c_bbb6e5e_2227eca_65f628b	0x64408b2c
98	389	0x090a924ea783998b	0x7b231ab_9d1a11b_aff6b1e_47d273f_c29f20f_81f9565	--	--	0x340a433_93e7bdf_71416c2_002b998_4c9ad89_96f283c	0x03b468b1
99	393	0x0215249d4f073316	0x42b915a_4075db8_54cbde6_2fff97e_9882703_c1ac336	--	--	0x4ece638_a7d51a9_7f9e886_f70ae3d_7bb4fdb_35f33c7	0x9328a53d
Line rekey ignored (frame key calc in progress)							
100	397	0x042a493a960e662d	0x0960b32_d33d3ea_415be5f_662f358_ea77b3e_bae1860	--	--	0x0eea7d6_bdf8fd6_29fff0a_a341b36_7b88cea_18ceb50	0xb5e38b64
101	401	0x08549a75241cec5b	0x283bb5d_356dc1d_5ef8302_740b636_1e2bbb1_77a9024	--	--	0x06af6be_8574776_6244dc1_1c04bf2_7da1a03_e962e82	0x96fc2396
102	405	0x00a934ea4839f8b6	0xd1bdb61_18b2c89_06d55fe_85d7861_4a2d2c4_3f0f76a	--	0x6a42	0x8000eaf_8f340fb_57fba9a_ece383b_5d4ccf2_e2ff34b	0xbc51d239
103	409	0x015269d49873d16c		--	0xb1db		0x8908e8ac

			0xabddb90_19d2b4a_7540b7a _458c215_014c756_aca7735			0x394e745_ec99143_e3f8f19_ 375ec6c_39c7cef_ba78801	
104	413	0x02a4d3a938e782d8	0x924eb87_b7a728b_8f829c6_ 35dd971_63da5b0_486ff01	0x97	0xd7a3	0x398cfb0_51408ef_9500162_ a935d4f_835f420_da99144	0x1d74baa3
105	417	0x0549af5279cf05b1	0x711d28b_ffa6fca_923e67b_1 5707a7_42a4bb2_2deda6d	0xbb	0xb0f9	0xde9d7c1_83df898_1e55332_ ddc9add_a82acb2_2885c03	0xd8835587
106	421	0x0a935ea4f39e2b63	0xeff1213_e232b20_0064b82_ ae1968a_4a3cba4_40cb306	0x62	0x84bb	0xd887f8b_5d37e0d_fe4d145_ 6a55c77_9369bfb_5028d20	0xaf70715f
107	425	0x0a935ea4f39e2b63	0xeff1213_e232b20_0064b82_ ae1968a_4a3cba4_40cb306	0x62	0x84bb	0xb77f694_6fed836_ec5fbda_b efa034_2c5d690_ae478e9	0xc861665f
108	429	0x0a935ea4f39e2b63	0xeff1213_e232b20_0064b82_ ae1968a_4a3cba4_40cb306	0x62	0x84bb	0xa67d45e_0b30f7d_2bb93be_ e09b5f5_22ca847_b849198	0x2bbcf09a
…	…	…	…	…	…	…	…
127	505	0x0a935ea4f39e2b63	0xeff1213_e232b20_0064b82_ ae1968a_4a3cba4_40cb306	0x62	0x84bb	0x6886c93_2065e45_773f684_ 82237f8_df3ef7a_cae90a7	0xc07ece76
128	509	0x0a935ea4f39e2b63	0xeff1213_e232b20_0064b82_ ae1968a_4a3cba4_40cb306	0x62	0x84bb	0x9359a39_d450a12_51ce5bc_ d3062b6_2c9cca3_c74edc4	0xedf08af9
129	513	0x0a935ea4f39e2b63	0xeff1213_e232b20_0064b82_ ae1968a_4a3cba4_40cb306	0x62	0x84bb	0xeff1213_e232b20_0064b82_ ae1968a_4a3cba4_40cb306	0xb86284bb
130	517	0x0526b549e73c76c7	0xddd552f_3d3bac2_fb230d5_ 83a2d78_5a1da41_8fed1d6	0x74	0x39a6	0xddd552f_3d3bac2_fb230d5_ 83a2d78_5a1da41_8fed1d6	0xb87439a6
131	521	0x0a4d6293ce78ed8e	0xc258963_5d097d0_e50aa7c_ fc50f00_a2a747b_a45b784	0x01	0xf1ed	0xc258963_5d097d0_e50aa7c_ fc50f00_a2a747b_a45b784	0xf701f1ed
Line rekey started							
clk	**Sym clk**	**LFSR[59:0]**	**BM0[167:0]**	**OF0[23:16]**	**OF0[15:0]**	**BM1[167:0]**	**OF1[31:0]**
-3	--	0x0a935ea4f39e2b63	0xeff1213_e232b20_0064b82_ ae1968a_4a3cba4_40cb306	--	--	0xeff1213_e232b20_0064b82_ ae1968a_4a3cba4_40cb306	0xb86284bb
-2	--	0x0526b549e73c76c7	0xddd552f_3d3bac2_fb230d5_ 83a2d78_5a1da41_8fed1d6	--	--	0xddd552f_3d3bac2_fb230d5_ 83a2d78_5a1da41_8fed1d6	0xb87439a6
-1	--	0x0a4d6293ce78ed8e	0xc258963_5d097d0_e50aa7c_ fc50f00_a2a747b_a45b784	--	--	0xc258963_5d097d0_e50aa7c_ fc50f00_a2a747b_a45b784	0xf701f1ed
0	524	0x0a4d6293ce78ed8e	0xc258963_5d097d0_e50aa7c_ fc50f00_a2a747b_a45b784	--	--	0xc258963_5d097d0_e50aa7c_ fc50f00_a2a747b_a45b784	0xf701f1ed
1	525	0x049ac5279cf1fb1c	0xb06e6b7_c8209e8_82982f7_ 4bc1a13_8a3f797_9f0446e	--	--	0xb06e6b7_c8209e8_82982f7_ 4bc1a13_8a3f797_9f0446e	0x523d121c
2	529	0x09358a4f31e3d639	0xefd27df_0e46509_e0b63da_ cb3dc05_af53ae8_4436e20	--	--	0xefd27df_0e46509_e0b63da_ cb3dc05_af53ae8_4436e20	0xf96f47ae
3	533	0x026b1c9e63c7ac73	0xc479a9c_8c09955_e4b84bc_ f4d23b6_286c3cc_fbefcbb	--	--	0xc479a9c_8c0b955_e4b84bc_ f4d23b6_286c3cc_fbefcbb	0xba695c5b
…	…	…	…	…	…	…	…
32	649	0x043ffb6e40477160	0x4a342ae_82a9a69_1f8a0d6_ 7852eba_50bcd92_f0ca19b	--	--	0x126d6a1_c8267a1_d20ba63_ 1d62a80_4849d54_c22adc6	0xcafb3096
33	653	0x087ff6dc808ee2c0	0xacd0bda_d7d29d8_a2da5ac_ 535a6be_7b87b62_3dc28c5	--	--	0x090c831_428d360_ae27819 _7cdfcea_2f86695_f5113b9	0xc50ff5c5
Line rekey ignored (line rekey in progress)							

34	657	0x00ffedb9091de580	0xfe540b1_c0aa0d3_dc2cc45_c9ace54_b5a739e_9384394	--	--	0xd90e59c_f9f3d1b_6480004_14d76a9_ba528a2_170c303	0xce6d0db0
35	661	0x01ffd3721a3beb00	0x591fc74_00754e2_bfa4739_d848399_afd0bfb_726948b	--	--	0x7f99cd9_7bc4777_4f5593a_643b662_d78d88d_1dd73e0	0x704bd830
36	665	0x03ffa6e43c77d601	0x43b5667_02d61d2_f5812e5_4e9c794_3d4cdb0_9530772	--	--	0x4b13e98_07bda78_c94b39a_f01addb_0943b5d_1f7d73a	0x81f96994
…	…	…	…	…	…	…	…
51	725	0x02694c70f74ddda1	0x014c513_1161f8b_41c9b49_a64a8b3_0ad9135_6c6337b	--	--	0x88eca24_fa0719b_0e475ea_fd01238_77fac9c_2a2fe35	0x241e4836
52	729	0x04d290e1ee9bbb43	0x5f74778_7bae847_3858c2e_6d9a242_bc9a02f_e4fdf87	--	--	0x276fafa_fb8c5a8_95210b1_8d295f2_09e27e6_b737720	0x673be722
53	733	0x09a529c3d5375686	0x41c3db8_7e60b5d_ade6c26_0335bb1_0313ffb_ce6d556	--	--	0xde83510_f93dd7e_8f09cca_fd7e979_439879a_5870c89	0x0e661a04
54	737	0x034a5387aa6ead0c	0xda39225_0d2f8e6_487e46d_14adaff_c23321e_7e5a780	--	--	0x9fd4127_873eeab_d443857_d7bc533_04fa8ab_a4eee09	0xe8b7ea1e
55	741	0x0694af0f54dd7a18	0xb6bee9e_b0ef775_f7d10ad_5dce396_89b2597_acef7ea	--	--	0xd5858aa_e4354ca_b52fefd_c3e62de_3960ed5_cbc6aa5	0xac7e0ebc
56	745	0x0d29561ea1bad430	0x0beb3a9_cb636c5_ce7a6d6_3ab9bdb_c93d31b_c325019	--	--	0xed3734d_00d67e7_eb76874_e2d404c_09ed965_dc23211	0x233bf0c3
57	749	0x0d29561ea1bad430	0x0beb3a9_cb636c5_ce7a6d6_3ab9bdb_c93d31b_c325019	--	--	0xe17cdec_bc66357_8450c0e_5f72374_878db0c_6b13d1e	0x16208c84
58	753	0x0d29561ea1bad430	0x0beb3a9_cb636c5_ce7a6d6_3ab9bdb_c93d31b_c325019	--	--	0x55182ed_d8e05f7_37f417a_14ed44b_585f76b_94900de	0x2acbe06b
…	…	…	…	…	…	…	…
63	773	0x0d29561ea1bad430	0x0beb3a9_cb636c5_ce7a6d6_3ab9bdb_c93d31b_c325019	--	--	0x9f12b63_096eeec_28e9b90_a572681_09e03f4_85a8ee3	0x681b908d
64	777	0x0d29561ea1bad430	0x0beb3a9_cb636c5_ce7a6d6_3ab9bdb_c93d31b_c325019	--	--	0xfb4bddb_29ecd93_fee8c9d_9cef79d_167d4b2_7c33f78	0x3792bbc6
65	781	0x0d29561ea1bad430	0x0beb3a9_cb636c5_ce7a6d6_3ab9bdb_c93d31b_c325019	--	--	0x0beb3a9_cb636c5_ce7a6d6_3ab9bdb_c93d31b_c325019	0x0b653310
66	785	0x0a52a43d4b758861	0x6a3ad12_9854416_6c93fda_e14a23d_fbc4d3f_cceecdf	--	--	0x6a3ad12_9854416_6c93fda_e14a23d_fbc4d3f_cceecdf	0xc63474f4
Line rekey started							
clk	**Sym clk**	**LFSR[59:0]**	**BM0[167:0]**	**OF0[23:16]**	**OF0[15:0]**	**BM1[167:0]**	**OF1[31:0]**
-3	--	0x0d29561ea1bad430	0x0beb3a9_cb636c5_ce7a6d6_3ab9bdb_c93d31b_c325019	--	--	0xfb4bddb_29ecd93_fee8c9d_9cef79d_167d4b2_7c33f78	0x3792bbc6
-2	--	0x0d29561ea1bad430	0x0beb3a9_cb636c5_ce7a6d6_3ab9bdb_c93d31b_c325019	--	--	0x0beb3a9_cb636c5_ce7a6d6_3ab9bdb_c93d31b_c325019	0x0b653310
-1	--	0x0a52a43d4b758861	0x6a3ad12_9854416_6c93fda_e14a23d_fbc4d3f_cceecdf	--	--	0x6a3ad12_9854416_6c93fda_e14a23d_fbc4d3f_cceecdf	0xc63474f4
0	786	0x0a52a43d4b758861	0x6a3ad12_9854416_6c93fda_e14a23d_fbc4d3f_cceecdf	--	--	0x6a3ad12_9854416_6c93fda_e14a23d_fbc4d3f_cceecdf	0xc63474f4
1	789	0x04a5487a96eb30c2	0x6a9b47c_10a322e_494b633_ea430af_69d5a81_2aca65b	--	--	0x6a9b47c_10a122e_494b633_ea430af_69d5a81_2aca65b	0x9832c3f5

2	793	0x094a98f52dd66185	0x697465f_2138d24_6420e6d_dc45678_b3f26bd_ac15ebd	--	--	0x697465f_031af06_6420e6d_fc45678_b3f26bd_ac15ebd	0xedac5ec3
…	…	…	…	…	…	…	…
32	913	0x0eaa24843ef16f31	0xa7aa4f2_ab024a6_1526de4_bd54215_b7616e3_f6b9ac6	--	--	0xe302e64_32b8ce1_c3235d5_d7e3d88_62b6ba0_596e2e7	0x7fc7073d
33	917	0x0d54490875e2de63	0x743b6b3_47964b3_ae1dca7_bc3fbb3_75aa0de_e57713d	--	--	0x6c7478d_7db25e0_9090e3b_c771065_0e48dc5_76362fe	0xb0623f59
Line rekey ignored (line rekey in progress)							
34	921	0x0aa89a10e3c5bcc6	0xeb2c3b9_13e277a_67aba2b_11b6e45_1067bcd_d84489c	--	--	0x1026dae_539147f_d4370ae_301ffb6_c109d01_1c55524	0x9979fe29
35	925	0x05513421c78b598c	0xc72feb1_8e34f2c_af96f6b_e0d7889_e3a168f_a0c4b77	--	--	0x094395e_de6af10_6feef16_5a53c1d_95183c3_574ee5f	0x19764485
36	929	0x0aa2604387169318	0xf812b8c_1e9b06f_6b8d523_2a37cf3_89531f8_c8047ae	--	--	0xf103087_0ca8df6_9ff9562_088d55d_9dc44ff_5987962	0x240ebacf
…	…	…	…	…	…	…	…
52	993	0x07620452ac75f21a	0x951a1c5_af748e5_6762204_2739c1a_d7ca7fb_7ffebb2	--	--	0xbb0821e_652203c_c692f7a_be966cc_c0d3aeb_e5fb8c3	0x256d3a25
53	997	0x0ec400a550ebc434	0x7dbb091_b0fe23f_b678529_65a5868_35ccece_0ccbf96	--	--	0x7e06bc3_deffce3_a122963_9c8046c_a0f5407_95d2175	0x40160ab9
54	1001	0x0d88014aa9d78868	0xba70910_a993630_7a0bb4b_929c3fa_d4032ea_3730bc5	--	--	0xed60095_28f7296_5e3de79_258d6e5_9808185_1f17b14	0xe58099af
55	1005	0x0b100a955baf10d0	0x2ead2b5_3199407_9908a29_b00f65c_9bc7820_1d7be03	--	--	0x3e64190_abd2d40_ff33171_2088e1e_054137c_09cd3f8	0x9e1df619
56	1009	0x0620152ab75e01a0	0xf8fcf70_76e6257_f2af903_62e652e_6c669c8_bb8b2c3	--	--	0xa57486d_59d17c9_b6020be_95b5c4a_163fe40_0ae4b70	0x5c23cbee
57	1013	0x0620152ab75e01a0	0xf8fcf70_76e6257_f2af903_62e652e_6c669c8_bb8b2c3	--	--	0x10c6a0f_37fc336_65d0558_86a6794_5dd9ca5_7ae8a9d	0x68207f9b
58	1017	0x0620152ab75e01a0	0xf8fcf70_76e6257_f2af903_62e652e_6c669c8_bb8b2c3	--	--	0x1be27ff_340bb29_413a310_2f0de95_9258438_9ce0e2b	0x06e1abf6
…	…	…	…	…	…	…	…
63	1037	0x0620152ab75e01a0	0xf8fcf70_76e6257_f2af903_62e652e_6c669c8_bb8b2c3	--	--	0x5cca5a8_2556f38_721cd54_ed0a7be_b322447_d4b665c	0x94f602fc
64	1041	0x0620152ab75e01a0	0xf8fcf70_76e6257_f2af903_62e652e_6c669c8_bb8b2c3	--	--	0xf76f879_1fbb56b_258f91d_e102fc0_cd59d02_20a20c1	0xf4dfb4a0
65	1045	0x0620152ab75e01a0	0xf8fcf70_76e6257_f2af903_62e652e_6c669c8_bb8b2c3	--	--	0xf8fcf70_76e6257_f2af903_62e652e_6c669c8_bb8b2c3	0x29ed1fbe
Line rekey started							
clk	**Sym clk**	**LFSR[59:0]**	**BM0[167:0]**	**OF0[23:16]**	**OF0[15:0]**	**BM1[167:0]**	**OF1[31:0]**
-3	--	0x0620152ab75e01a0	0xf8fcf70_76e6257_f2af903_62e652e_6c669c8_bb8b2c3	--	--	0x5cca5a8_2556f38_721cd54_ed0a7be_b322447_d4b665c	0x94f602fc
-2	--	0x0620152ab75e01a0	0xf8fcf70_76e6257_f2af903_62e652e_6c669c8_bb8b2c3	--	--	0xf76f879_1fbb56b_258f91d_e102fc0_cd59d02_20a20c1	0xf4dfb4a0
-1	--	0x0620152ab75e01a0	0xf8fcf70_76e6257_f2af903_62e652e_6c669c8_bb8b2c3	--	--	0xf8fcf70_76e6257_f2af903_62e652e_6c669c8_bb8b2c3	0x29ed1fbe

0	1048	0x0620152ab75e01a0	0xf8fcf70_76e6257_f2af903_62e652e_6c669c8_bb8b2c3	--	--	0xf8fcf70_76e6257_f2af903_62e652e_6c669c8_bb8b2c3	0x29ed1fbe
1	1049	0x0c4022556ebc0341	0x6ec489f_457b2b0_8ca19cf_094be1f_a6ecdaf_6392c72	--	--	0x6ec489f_45792b0_8ca19cf_094be1f_a6ecdaf_6392c72	0xdb0dcbb4
2	1053	0x08804caadd780683	0x1570e26_fd97d4e_dab6c21_60ee032_1ec213f_83a1901	--	--	0x1570e26_dfb5f6c_dab6c21_40ee032_1ec213f_83a1901	0xe292f2e8
3	1057	0x01009955baf02d07	0x496a8cb_58c35bb_4ab021c_8bfac8a_cbffe7c_73d27f5	--	--	0xa7846c5_c342c22_4ab021c_aa7ee92_cbffe7c_53927f5	0x224652cf
…	…	…	…	…	…	…	…
32	1173	0x064aee3e56a6b751	0xa52286b_3054187_31a82e6_e0e7c66_2d487f1_2660968	--	--	0x811db73_a2b5101_0d9534e_976eb27_d6359b0_17b2ab9	0xd6cbf92e
33	1177	0x0c95d47ca54d6ea2	0xcf6cf56_9ccac18_ca94c9c_101c2a2_e80365e_97324c9	--	--	0x600d794_eaefdb6_2109242_2f572ec_b5dba16_7a872d9	0xf34f7270
Line rekey discarded, frame key calc started							
clk	**Sym clk**	**LFSR[59:0]**	**BM0[167:0]**	**OF0[23:16]**	**OF0[15:0]**	**BM1[167:0]**	**OF1[31:0]**
-3	--	--	0xcb389f7_a24e0f5_eb23921_7e44a14_53aabbc_1eac782	--	--	0xf3dc76c_3a76a4b_e271ebf_98a464a_e44feb4_ca9e8ae	0xb554bcc8
-2	--	--	0xa52286b_3054187_31a82e6_e0e7c66_2d487f1_2660968	--	--	0x811db73_a2b5101_0d9534e_976eb27_d6359b0_17b2ab9	0xd6cbf92e
-1	--	--	0xcf6cf56_9ccac18_ca94c9c_101c2a2_e80365e_97324c9	--	--	0x600d794_eaefdb6_2109242_2f572ec_b5dba16_7a872d9	0xf34f7270
0	1179	--	0xcf6cf56_9ccac18_ca94c9c_101c2a2_e80365e_97324c9	--	--	0x600d794_eaefdb6_2109242_2f572ec_b5dba16_7a872d9	0xf34f7270
1	1180	--	0xc040e35_54294b7_0000000_7a3b0f9_42b1dbd_000006a	--	--	0x028eaf0_8778f88_b616f0a_09e755b_b2838fe_e410d5d	0x404f661b
2	1184	--	0x6666a4e_47b5444_93d46aa_e4f374f_3cd0333_212d6ab	--	--	0xcc05aba_a660bd4_2e010e0_fb8f410_0b7603a_c894453	0xf8b70a3c
3	1188	--	0x1232d67_ef6a7a5_6055678_d509b9f_427d387_e30af77	--	--	0xaf62c4a_4928645_fbb5620_9cc01dd_b989bf1_7a1a46a	0x51de8dfe
4	1192	--	0x811566c_da14697_66f89db_84306fe_411d172_f9e3620	--	--	0x1eb5935_9814a53_b06003d_dd01355_680b268_1db2636	0xe679bb16
5	1196	--	0xf7027a4_dc24164_29716cf_f0cd06e_9fad21f_41cbe85	--	--	0x32ae238_2a1faa2_f48728f_974c785_020e18e_46e182b	0xbdbd6c65

Table B-36. Cipher State in SST mode for 1-lane, Inter-BS Spacing = 131

clk	stream	cipher	enc stream
-3	0x1c	0x6559c03e	0x1c
-2	0x3c	0x6559c03e	0x3c
-1	0x3c	0x6559c03e	0x3c
0	0x1c	0x6559c03e	0x1c
1	0x39	0xb79ee5fe	0xc7
2	0x00	0xb79ee5fe	0xe5
3	0x00	0xb79ee5fe	0x9e
4	0x39	0xb79ee5fe	0x8e
5	0x00	0x289af919	0x19
6	0x00	0x289af919	0xf9
7	0x39	0x289af919	0xa3
8	0x00	0x289af919	0x28
9	0x00	0xd25b5d6c	0x6c
10	0x39	0xd25b5d6c	0x64
11	0x00	0xd25b5d6c	0x5b
12	0x00	0xd25b5d6c	0xd2
13	0x00	0xed55dcde	0xde
…	…	…	…
125	0x00	0x2f4436cb	0xcb
126	0x00	0x2f4436cb	0x36
127	0x00	0x2f4436cb	0x44
128	0xbc	0x2f4436cb	0xbc
129	0x3c	0x7847ef0d	0x3c
130	0x3c	0x7847ef0d	0x3c
131	0xbc	0x7847ef0d	0xbc
132	0x39	0x7847ef0d	0x41
133	0x00	0xf96f47cd	0xcd
134	0x00	0xf96f47cd	0x47
135	0x39	0xf96f47cd	0x56
136	0x00	0xf96f47cd	0xf9
137	0x00	0x30f12a24	0x24
138	0x39	0x30f12a24	0x13
139	0x00	0x30f12a24	0xf1
140	0x00	0x30f12a24	0x30
141	0x39	0xd47a2546	0x7f
…	…	…	…
181	0x00	0x37affe86	0x86
182	0x00	0x37affe86	0xfe
183	0x00	0x37affe86	0xaf
184	0x00	0x37affe86	0x37
185	0x00	0x49152bc4	0xc4
186	0x00	0x49152bc4	0x2b

187	0x00	0x49152bc4	0x15
188	0x00	0x49152bc4	0x49
189	0x00	0x1f068148	0x48
190	0x00	0x1f068148	0x81
191	0x00	0x1f068148	0x06
192	0x00	0x1f068148	0x1f
193	0x00	0xb79cb954	0x54
…	…	…	…
197	0x00	0xfe492f2a	0x2a
198	0x00	0xfe492f2a	0x2f
199	0x00	0xfe492f2a	0x49
200	0x00	0xfe492f2a	0xfe
201	0x00	0x53331e18	0x18
202	0x00	0x53331e18	0x1e
203	0x00	0x53331e18	0x33
204	0x00	0x53331e18	0x53
205	0x00	0x5c0e4039	0x39
…	…	…	…
257	0x00	0xf254ffb6	0xb6
258	0x00	0xf254ffb6	0xff
259	0xbc	0xf254ffb6	0xbc
260	0x3c	0xf254ffb6	0x3c
261	0x3c	0x14b8b17b	0x3c
262	0xbc	0x14b8b17b	0xbc
263	0x39	0x14b8b17b	0x81
264	0x00	0x14b8b17b	0x14
265	0x00	0x36693806	0x06
266	0x39	0x36693806	0x01
267	0x00	0x36693806	0x69
268	0x00	0x36693806	0x36
269	0x39	0x377c62a2	0x9b
270	0x00	0x377c62a2	0x62
271	0x00	0x377c62a2	0x7c
272	0x39	0x377c62a2	0x0e
273	0x00	0x1dae33a6	0xa6
…	…	…	…
385	0x00	0x64408b2c	0x2c
386	0x00	0x64408b2c	0x8b
387	0x00	0x64408b2c	0x40
388	0x00	0x64408b2c	0x64
389	0x00	0x03b468b1	0xb1
390	0xbc	0x03b468b1	0xbc
391	0x3c	0x03b468b1	0x3c
392	0x3c	0x03b468b1	0x3c

393	0xbc	0x9328a53d	0xbc
394	0x39	0x9328a53d	0x9c
395	0x00	0x9328a53d	0x28
396	0x00	0x9328a53d	0x93
397	0x39	0xb5e38b64	0x5d
398	0x00	0xb5e38b64	0x8b
399	0x00	0xb5e38b64	0xe3
400	0x39	0xb5e38b64	0x8c
401	0x00	0x96fc2396	0x96
402	0x00	0x96fc2396	0x23
403	0x39	0x96fc2396	0xc5
404	0x00	0x96fc2396	0x96
405	0x00	0xbc51d239	0x39
406	0x00	0xbc51d239	0xd2
407	0x00	0xbc51d239	0x51
408	0x00	0xbc51d239	0xbc
409	0x00	0x8908e8ac	0xac
410	0x00	0x8908e8ac	0xe8
411	0x00	0x8908e8ac	0x08
412	0x00	0x8908e8ac	0x89
413	0x00	0x1d74baa3	0xa3
414	0x00	0x1d74baa3	0xba
415	0x00	0x1d74baa3	0x74
416	0x00	0x1d74baa3	0x1d
417	0x00	0xd8835587	0x87
418	0x00	0xd8835587	0x55
419	0x00	0xd8835587	0x83
420	0x00	0xd8835587	0xd8
421	0x00	0xaf70715f	0x5f
422	0x00	0xaf70715f	0x71
423	0x00	0xaf70715f	0x70
424	0x00	0xaf70715f	0xaf
425	0x00	0xc861665f	0x5f
426	0x00	0xc861665f	0x66
427	0x00	0xc861665f	0x61
428	0x00	0xc861665f	0xc8
429	0x00	0x2bbcf09a	0x9a
…	…	…	…
505	0x00	0xc07ece76	0x76
506	0x00	0xc07ece76	0xce
507	0x00	0xc07ece76	0x7e
508	0x00	0xc07ece76	0xc0
509	0x00	0xedf08af9	0xf9
510	0x00	0xedf08af9	0x8a

511	0x00	0xedf08af9	0xf0
512	0x00	0xedf08af9	0xed
513	0x00	0xb86284bb	0xbb
514	0x00	0xb86284bb	0x84
515	0x00	0xb86284bb	0x62
516	0x00	0xb86284bb	0xb8
517	0x00	0xb87439a6	0xa6
518	0x00	0xb87439a6	0x39
519	0x00	0xb87439a6	0x74
520	0x00	0xb87439a6	0xb8
521	0xbc	0xf701f1ed	0xbc
522	0x3c	0xf701f1ed	0x3c
523	0x3c	0xf701f1ed	0x3c
524	0xbc	0xf701f1ed	0xbc
525	0x39	0x523d121c	0x25
526	0x00	0x523d121c	0x12
527	0x00	0x523d121c	0x3d
528	0x39	0x523d121c	0x6b
529	0x00	0xf96f47ae	0xae

Table B-37. 1-lane Encrypted Output in SST mode for Inter-BS Spacing = 131

Test Vectors for 1-Lane Main Link Configuration in SST Mode (Inter-BS spacing = 132, CPSR Interval = 9)

Authentication

Table B-3 and Table B-4 provide the LFSR and Block module states during the first part of authentication.

Initial Bootstrapping

Table B-25 provides test vectors during the initial bootstrapping operation.

After start of encryption

Table B-38 provides test vectors generated after the start of encryption (beginning with the first CPSR symbol set that triggers encryption). Table B-39 provides encrypted cipher outputs.

Frame key calc started							
clk	**Sym clk**	**LFSR[59:0]**	**BM0[167:0]**	**OF0[23:16]**	**OF0[15:0]**	**BM1[167:0]**	**OF1[31:0]**
-3	--	--	0xd20317a_3725bc8_256af5e_6b9cc06_7d7aa18_87f9092	--	--	0xd20317a_3725bc8_256af5e_6b9cc06_7d7aa18_87f9092	0x6559c03e
-2	--	--	0xd20317a_3725bc8_256af5e_6b9cc06_7d7aa18_87f9092	--	--	0xd20317a_3725bc8_256af5e_6b9cc06_7d7aa18_87f9092	0x6559c03e
-1	--	--	0xd20317a_3725bc8_256af5e_6b9cc06_7d7aa18_87f9092	--	--	0xd20317a_3725bc8_256af5e_6b9cc06_7d7aa18_87f9092	0x6559c03e
0	0	--	0xd20317a_3725bc8_256af5e_6b9cc06_7d7aa18_87f9092	--	--	0xd20317a_3725bc8_256af5e_6b9cc06_7d7aa18_87f9092	0x6559c03e
1	1	--	0xc040e35_54294b7_0000000_f523e56_bf44e50_000001d	--	--	0x9b48c65_3f7de85_4cfb937_50d9c10_5d7fbdc_6a03908	0xb79ee5fe
2	5	--	0x6666a4e_47b5444_93d46aa_a1a9cb4_a206aaa_cacfa30	--	--	0x94ede66_8141634_5f900d1_5f7a0f0_f291dcb_5a0ce6e	0x289af919
3	9	--	0x1232d67_ef6a7a5_6055678_533e54c_e4b418a_91fbcbb	--	--	0x1f69314_9a31990_c4b92db_31a6525_6ab1304_928c3d8	0xd25b5d6c
4	13	--	0x811566c_da14697_66f89db_d9ce46b_c89e263_9e3097e	--	--	0x7f0a70c_d1bda54_34c9929_7df4b37_d8d588c_855d111	0xed55dcde
…	…	…	…	…	…	…	…
32	125	--	0x58f7c56_8ff3888_97eb44c_25c4a1a_310ffae_84d8e08	--	--	0x2221028_0c49069_b9a604c_d5025c1_052df5f_59112d6	0x2f4436cb
33	129	--	0x315c455_d59f35b_40693cd_5dbf7bd_2df8f08_22cacad	--	--	0x3596433_4643480_8853c0f_95d957d_e351de7_9412e3e	0x7847ef0d
Line rekey ignored (frame key calc in progress)							
34	133	--	0x080bd0f_043ff91_b512030_bbfa516_f3753d8_957c88c	--	--	0x6267937_99593b7_3013a64_3a0aa4d_b46ea95_1e99035	0xf96f47cd
35	137	--	0x65b6244_8461884_2bffcba_a8f7581_264cecb_2cca0f2	--	--	0xdc51ed3_daa4ef1_5dafba7_4ea8052_6f0f06e_712dc22	0x30f12a24
36	141	--	0x259b412_3a73ddc_ddf0be5_8794752_f7203fa_f4acf98	--	--	0x4b2ad3d_0aed7f5_9a40045_f0dc0bd_12077f3_dc5bdc2	0xd47a2546
…	…	…	…	…	…	…	…
47	185	--	0xc9472f7_c4371c6_667db05_9e19673_1fcfb80_9e1665f	--	--	0xfa07250_f725212_9bc279d_76fe61a_e1521fc_fb331b7	0x49152bc4
48	189	--	0x2aeaf01_beef443_e0cd9a0_d83548d_480c50a_5d4ed0e	--	--	0xcaf5121_1129806_3836e0a_9051c5e_34551ae_7f7b35a	0x1f068148

49	193	--	0x5cfb3bd_bb2e5ca_6f52793_8bb82fe_ea7c298_d9a59fa	--	--	0x62e765a_09101ee_f92cab1_4cfd7ca_f8ad063_1f97804	0xb79cb954
50	197	0x0f53e0a6257702fe	0x8bb82fe_ea7c298_d9a59fa_f523e56_bf44e50_000001d	--	--	0x960d99e_e9b8b0f_782d158_645c7a9_312615f_ca46465	0xfe492f2a
51	201	0x0ea7c94c42ee05fd	0xb486149_cca6e3d_0355dff_2262329_a206aaa_cacfa30	--	--	0xb72431d_495f294_aba13a4_c1a5edc_d8ea59b_2cbcad0	0x53331e18
52	205	0x0d4f929885dc0bfb	0x120ec20_a1030d1_4c72806_a00fb45_e4b418a_75af954	--	--	0xe94a5e8_bad382a_b516ee3_2aea12a_04f35e9_6a44723	0x5c0e4039
53	209	0x0a9f253103b837f6	0xc084d58_ee8b642_7dd6814_079525e_aef8c5e_ada7f43	--	--	0x8b46a53_283034d_84a452f_9958918_06c7952_3d3b8d2	0x4a040224
…	…	…	…	…	…	…	…
65	257	0x02281877125640a2	0xa1ac713_e2d283a_482c2bb_d437443_bd8ef95_076c262	--	--	0xbdc2425_78138b1_fae8859_7b0d9b3_9007256_f02725b	0xf254ffb6
66	261	0x045030ee2cac8144	0x3e289e0_1b214d0_e90ac42_1504b3f_58bc895_c98fa75	--	--	0x6ad3eed_82e9428_1f151a0_fefc1c7_231e1e6_0e7b8ba	0x14b8b17b
Line rekey ignored (frame key calc in progress)							
67	265	0x08a061dc59590289	0x0e8407c_bb5df9d_578e9dd_6e1b212_7e16013_78ef703	--	--	0xbcf19db_fd7dda6_60704fe_0a9e816_1645fbc_7b03898	0x36693806
68	269	0x0140c3b8b2b22512	0x7d0a4b8_3eda746_1d77d70_0293f78_0031fd6_6dab5e6	--	--	0x6ffb9d8_4b94ccf_9e88e41_6fd5114_b45199e_2be2560	0x377c62a2
…	…	…	…	…	…	…	…
98	389	0x090a924ea783998b	0x7b231ab_9d1a11b_aff6b1e_47d273f_c29f20f_81f9565	--	--	0x340a433_93e7bdf_71416c2_002b998_4c9ad89_96f283c	0x03b468b1
99	393	0x0215249d4f073316	0x42b915a_4075db8_54cbde6_2fff97e_9882703_c1ac336	--	--	0x4ece638_a7d51a9_7f9e886_f70ae3d_7bb4fdb_35f33c7	0x9328a53d
Line rekey ignored (frame key calc in progress)							
100	397	0x042a493a960e662d	0x0960b32_d33d3ea_415be5f_662f358_ea77b3e_bae1860	--	--	0x0eea7d6_bdf8fd6_29fff0a_a341b36_7b88cea_18ceb50	0xb5e38b64
101	401	0x08549a75241cec5b	0x283bb5d_356dc1d_5ef8302_740b636_1e2bbb1_77a9024	--	--	0x06af6be_8574776_6244dc1_1c04bf2_7da1a03_e962e82	0x96fc2396
102	405	0x00a934ea4839f8b6	0xd1bdb61_18b2c89_06d55fe_85d7861_4a2d2c4_3f0f76a	--	0x6a42	0x8000eaf_8f340fb_57fba9a_ece383b_5d4ccf2_e2ff34b	0xbc51d239
103	409	0x015269d49873d16c	0xabddb90_19d2b4a_7540b7a_458c215_014c756_aca7735	--	0xb1db	0x394e745_ec99143_e3f8f19_375ec6c_39c7cef_ba78801	0x8908e8ac
104	413	0x02a4d3a938e782d8	0x924eb87_b7a728b_8f829c6_35dd971_63da5b0_486ff01	0x97	0xd7a3	0x398cfb0_51408ef_9500162_a935d4f_835f420_da99144	0x1d74baa3
105	417	0x0549af5279cf05b1	0x711d28b_ffa6fca_923e67b_15707a7_42a4bb2_2deda6d	0xbb	0xb0f9	0xde9d7c1_83df898_1e55332_ddc9add_a82acb2_2885c03	0xd8835587
106	421	0x0a935ea4f39e2b63	0xeff1213_e232b20_0064b82_ae1968a_4a3cba4_40cb306	0x62	0x84bb	0xd887f8b_5d37e0d_fe4d145_6a55c77_9369bfb_5028d20	0xaf70715f
107	425	0x0a935ea4f39e2b63	0xeff1213_e232b20_0064b82_ae1968a_4a3cba4_40cb306	0x62	0x84bb	0xb77f694_6fed836_ec5fbda_befa034_2c5d690_ae478e9	0xc861665f
…	…	…	…	…	…	…	…
127	505	0x0a935ea4f39e2b63	0xeff1213_e232b20_0064b82_ae1968a_4a3cba4_40cb306	0x62	0x84bb	0x6886c93_2065e45_773f684_82237f8_df3ef7a_cae90a7	0xc07ece76

128	509	0x0a935ea4f39e2b63	0xeff1213_e232b20_0064b82_ae1968a_4a3cba4_40cb306	0x62	0x84bb	0x9359a39_d450a12_51ce5bc_d3062b6_2c9cca3_c74edc4	0xedf08af9
129	513	0x0a935ea4f39e2b63	0xeff1213_e232b20_0064b82_ae1968a_4a3cba4_40cb306	0x62	0x84bb	0xeff1213_e232b20_0064b82_ae1968a_4a3cba4_40cb306	0xb86284bb
130	517	0x0526b549e73c76c7	0xddd552f_3d3bac2_fb230d5_83a2d78_5a1da41_8fed1d6	0x74	0x39a6	0xddd552f_3d3bac2_fb230d5_83a2d78_5a1da41_8fed1d6	0xb87439a6
131	521	0x0a4d6293ce78ed8e	0xc258963_5d097d0_e50aa7c_fc50f00_a2a747b_a45b784	0x01	0xf1ed	0xc258963_5d097d0_e50aa7c_fc50f00_a2a747b_a45b784	0xf701f1ed
132	525	0x049ac5279cf1fb1c	0xb06e6b7_c8209e8_82982f7_4bc1a13_8a3f797_9f0446e	0x3d	0x121c	0xb06e6b7_c8209e8_82982f7_4bc1a13_8a3f797_9f0446e	0x523d121c
Line rekey started							
clk	**Sym clk**	**LFSR[59:0]**	**BM0[167:0]**	**OF0[23:16]**	**OF0[15:0]**	**BM1[167:0]**	**OF1[31:0]**
-3	--	0x0526b549e73c76c7	0xddd552f_3d3bac2_fb230d5_83a2d78_5a1da41_8fed1d6	--	--	0xddd552f_3d3bac2_fb230d5_83a2d78_5a1da41_8fed1d6	0xb87439a6
-2	--	0x0a4d6293ce78ed8e	0xc258963_5d097d0_e50aa7c_fc50f00_a2a747b_a45b784	--	--	0xc258963_5d097d0_e50aa7c_fc50f00_a2a747b_a45b784	0xf701f1ed
-1	--	0x049ac5279cf1fb1c	0xb06e6b7_c8209e8_82982f7_4bc1a13_8a3f797_9f0446e	--	--	0xb06e6b7_c8209e8_82982f7_4bc1a13_8a3f797_9f0446e	0x523d121c
0	528	0x049ac5279cf1fb1c	0xb06e6b7_c8209e8_82982f7_4bc1a13_8a3f797_9f0446e	--	--	0xb06e6b7_c8209e8_82982f7_4bc1a13_8a3f797_9f0446e	0x523d121c
1	529	0x09358a4f31e3d639	0xefd27df_0e46509_e0b63da_cb3dc05_af53ae8_4436e20	--	--	0xefd27df_0e46509_e0b63da_cb3dc05_af53ae8_4436e20	0xf96f47ae
2	533	0x026b1c9e63c7ac73	0xc479a9c_8c09955_e4b84bc_f4d23b6_286c3cc_fbefcbb	--	--	0xc479a9c_8c0b955_e4b84bc_f4d23b6_286c3cc_fbefcbb	0xba695c5b
3	537	0x04d6313ccf8f58e6	0x6f9b366_49610cf_895c70f_eaf2c27_410aaa3_e0e83bf	--	--	0x6f9b366_6b432ed_895c70f_caf2c27_410aaa3_e0e83bf	0x1163a5e9
…	…	…	…	…	…	…	…
32	653	0x087ff6dc808ee2c0	0xacd0bda_d7d29d8_a2da5ac_535a6be_7b87b62_3dc28c5	--	--	0x090c831_428d360_ae27819_7cdfcea_2f86695_f5113b9	0xc50ff5c5
33	657	0x00ffedb9091de580	0xfe540b1_c0aa0d3_dc2cc45_c9ace54_b5a739e_9384394	--	--	0xd90e59c_f9f3d1b_6480004_14d76a9_ba528a2_170c303	0xce6d0db0
Line rekey ignored (line rekey in progress)							
34	661	0x01ffd3721a3beb00	0x591fc74_00754e2_bfa4739_d848399_afd0bfb_726948b	--	--	0x7f99cd9_7bc4777_4f5593a_643b662_d78d88d_1dd73e0	0x704bd830
35	665	0x03ffa6e43c77d601	0x43b5667_02d61d2_f5812e5_4e9c794_3d4cdb0_9530772	--	--	0x4b13e98_07bda78_c94b39a_f01addb_0943b5d_1f7d73a	0x81f96994
…	…	…	…	…	…	…	…
51	729	0x04d290e1ee9bbb43	0x5f74778_7bae847_3858c2e_6d9a242_bc9a02f_e4fdf87	--	--	0x276fafa_fb8c5a8_95210b1_8d295f2_09e27e6_b737720	0x673be722
52	733	0x09a529c3d5375686	0x41c3db8_7e60b5d_ade6c26_0335bb1_0313ffb_ce6d556	--	--	0xde83510_f93dd7e_8f09cca_fd7e979_439879a_5870c89	0x0e661a04
53	737	0x034a5387aa6ead0c	0xda39225_0d2f8e6_487e46d_14adaff_c23321e_7e5a780	--	--	0x9fd4127_873eeab_d443857_d7bc533_04fa8ab_a4eee09	0xe8b7ea1e
54	741	0x0694af0f54dd7a18	0xb6bee9e_b0ef775_f7d10ad_	--	--	0xd5858aa_e4354ca_b52fefd_c3e	0xac7e0ebc

			5dce396_89b2597_acef7ea			62de_3960ed5_cbc6aa5	
55	745	0x0d29561ea1bad430	0x0beb3a9_cb636c5_ce7a6d6_3ab9bdb_c93d31b_c325019	--	--	0xed3734d_00d67e7_eb76874_e2d404c_09ed965_dc23211	0x233bf0c3
56	749	0x0a52a43d4b758861	0x6a3ad12_9856416_6c93fda_e14a23d_fbc4d3f_cceecdf	--	--	0xe17cdec_bc66357_8450c0e_5f72374_878db0c_6b13d1e	0x16208c84
57	753	0x0a52a43d4b758861	0x6a3ad12_9856416_6c93fda_e14a23d_fbc4d3f_cceecdf	--	--	0x55182ed_d8e05f7_37f417a_14ed44b_585f76b_94900de	0x2acbe06b
58	757	0x0a52a43d4b758861	0x6a3ad12_9856416_6c93fda_e14a23d_fbc4d3f_cceecdf	--	--	0x56aaf6d_07f58d8_abfa327_62d4dd6_60f966f_d4fe34f	0xe856019a
…	…	…	…	…	…	…	…
63	777	0x0a52a43d4b758861	0x6a3ad12_9856416_6c93fda_e14a23d_fbc4d3f_cceecdf	--	--	0xfb4bddb_29ecd93_fee8c9d_9cef79d_167d4b2_7c33f78	0x3792bbc6
64	781	0x0a52a43d4b758861	0x6a3ad12_9856416_6c93fda_e14a23d_fbc4d3f_cceecdf	--	--	0x6a915c3_b74a718_800888e_a7c90f3_64965d8_d4ac098	0x5807ee8e
65	785	0x0a52a43d4b758861	0x6a3ad12_9856416_6c93fda_e14a23d_fbc4d3f_cceecdf	--	--	0x6a3ad12_9856416_6c93fda_e14a23d_fbc4d3f_cceecdf	0xc63c74f4
66	789	0x04a5487a96eb30c2	0x6a9b47c_328300c_494b633_ca430af_69d5a81_2aca65b	--	--	0x6a9b47c_328300c_494b633_ca430af_69d5a81_2aca65b	0x937ac3f3
Line rekey started							
clk	**Sym clk**	**LFSR[59:0]**	**BM0[167:0]**	**OF0[23:16]**	**OF0[15:0]**	**BM1[167:0]**	**OF1[31:0]**
-3	--	0x0a52a43d4b758861	0x6a3ad12_9856416_6c93fda_e14a23d_fbc4d3f_cceecdf	--	--	0x6a915c3_b74a718_800888e_a7c90f3_64965d8_d4ac098	0x5807ee8e
-2	--	0x0a52a43d4b758861	0x6a3ad12_9856416_6c93fda_e14a23d_fbc4d3f_cceecdf	--	--	0x6a3ad12_9856416_6c93fda_e14a23d_fbc4d3f_cceecdf	0xc63c74f4
-1	--	0x04a5487a96eb30c2	0x6a9b47c_328300c_494b633_ca430af_69d5a81_2aca65b	--	--	0x6a9b47c_328300c_494b633_ca430af_69d5a81_2aca65b	0x937ac3f3
0	792	0x04a5487a96eb30c2	0x6a9b47c_328300c_494b633_ca430af_69d5a81_2aca65b	--	--	0x6a9b47c_328300c_494b633_ca430af_69d5a81_2aca65b	0x937ac3f3
1	793	0x094a98f52dd66185	0x879a851_989969f_6420e6d_ddc1460_b3f26bd_8c556ad	--	--	0x879a851_989b69f_6420e6d_ddc1460_b3f26bd_8c556ad	0x79da1e88
2	797	0x029531ea53acc30b	0x18de01a_54ae4f7_e218387_8350cbc_03ebb4b_1e54508	--	--	0x18de01a_768c6d5_e218387_a350cbc_03ebb4b_1e54508	0x67f2a9c2
3	801	0x052a6bd4a759a617	0xf77d2c6_a95dfb3_6962b83_6c086e6_e2f16b4_cbb7986	--	--	0x1993cc8_32de62a_6962b83_4d8c4fe_e2f16b4_ebf7986	0x083a8ba3
…	…	…	…	…	…	…	…
32	917	0x0d54490875e2de63	0xe2b3f71_443f61a_f93d67b_c7266b5_c10857c_08a2e37	--	--	0x0fd7f64_5d9e1c4_ae918db_f5e9bbe_d1a8c02_9ed8cf5	0xcd4bea37
33	921	0x0aa89a10e3c5bcc6	0x69f7a55_ff47835_424a6b1_1c1ccf2_e948f48_1ee2fc8	--	--	0x51a294a_276600b_d59545e_68635da_c45c0e7_a962e89	0x8b73649f
Line rekey ignored (line rekey in progress)							
34	925	0x05513421c78b598c	0x9085754_5e74852_d131846_017bde7_7bf9ec0_f6cf74b	--	--	0xd7aca29_889bac2_ffd8d76_446ecbc_b8ee21c_69d14b3	0x02ba87f6
35	929	0x0aa2604387169318	0x1b15e6b_b38f913_90d8ad1_54df227_d51128b_fc3845e	--	--	0x3ccd221_f7a33c5_b9cfdd3_1334641_674cc6d_039ed41	0x41a13092

…	…	…	…	…	…	…	…
51	993	0x07620452ac75f21a	0x59dfc75_a004a32_88e6c6e_fb13a24_e0d0832_527ea13	--	--	0x69424dd_aa8bca0_76430e1_ebd8622_e7a1ec3_5a39904	0x4bde1221
52	997	0x0ec400a550ebc434	0xfad6e6f_5f6fdb3_d540264_dcffdd2_6c56b8a_20339ee	--	--	0x18df1d0_28e2827_eb3147b_dcdf2d9_c411a74_e9829bc	0xc6999ae5
53	1001	0x0d88014aa9d78868	0x3877c5f_6897f66_20df19d_f362ef4_1d4b3ac_c306a61	--	--	0x2db5093_9288b13_3ee4f4a_80f7eb9_290e217_d92e5f4	0xcbf473a9
54	1005	0x0b100a955baf10d0	0xee5976d_b4255e6_00a9f64_cb596c6_165b075_aac6b82	--	--	0xbf50be3_a693358_38a4a80_2186957_ba82f6c_8895fa2	0x673542a6
55	1009	0x0620152ab75e01a0	0xdcf5875_52832e7_c6b95ed_4af3a31_4761d31_42d51ac	--	--	0xae00e68_517b4b4_7de84dc_f7fb234_4bca73f_80f4c73	0x3173e010
56	1013	0x0c4022556ebc0341	0x3a50a7a_cf93a57_d44036c_637c92a_2c8387b_1906d46	--	--	0x2cd390c_12f1d92_ccb0f59_1d1f860_16aa9fb_304a3dc	0x459d0f2f
57	1017	0x0c4022556ebc0341	0x3a50a7a_cf93a57_d44036c_637c92a_2c8387b_1906d46	--	--	0xe29dc85_2ed2398_37e2616_42a9516_d3aa0c8_e268bd9	0x96e30b57
58	1021	0x0c4022556ebc0341	0x3a50a7a_cf93a57_d44036c_637c92a_2c8387b_1906d46	--	--	0x57a3287_d9b745b_d715c19_0e684e5_ffb924e_5478cea	0x9624dba8
…	…	…	…	…	…	…	…
63	1041	0x0c4022556ebc0341	0x3a50a7a_cf93a57_d44036c_637c92a_2c8387b_1906d46	--	--	0xa49f8d6_e3d322b_634677c_9f212a1_05db67f_e4bf49b	0x693505a8
64	1045	0x0c4022556ebc0341	0x3a50a7a_cf93a57_d44036c_637c92a_2c8387b_1906d46	--	--	0xb02007d_130a847_06de012_2bfecc2_9a26f56_d516b99	0xbccbcea6
65	1049	0x0c4022556ebc0341	0x3a50a7a_cf93a57_d44036c_637c92a_2c8387b_1906d46	--	--	0x3a50a7a_cf93a57_d44036c_637c92a_2c8387b_1906d46	0x0252ac66
66	1053	0x08804caadd780683	0x094fd46_c5f15dc_49aa945_61af390_c6fbcba_1eaa206	--	--	0x094fd46_c5f15dc_49aa945_61af390_c6fbcba_1eaa206	0x84ab700f

Line rekey started

clk	Sym clk	LFSR[59:0]	BM0[167:0]	OF0[23:16]	OF0[15:0]	BM1[167:0]	OF1[31:0]
-3	--	0x0c4022556ebc0341	0x3a50a7a_cf93a57_d44036c_637c92a_2c8387b_1906d46	--	--	0xb02007d_130a847_06de012_2bfecc2_9a26f56_d516b99	0xbccbcea6
-2	--	0x0c4022556ebc0341	0x3a50a7a_cf93a57_d44036c_637c92a_2c8387b_1906d46	--	--	0x3a50a7a_cf93a57_d44036c_637c92a_2c8387b_1906d46	0x0252ac66
-1	--	0x08804caadd780683	0x094fd46_c5f15dc_49aa945_61af390_c6fbcba_1eaa206	--	--	0x094fd46_c5f15dc_49aa945_61af390_c6fbcba_1eaa206	0x84ab700f
0	1056	0x08804caadd780683	0x094fd46_c5f15dc_49aa945_61af390_c6fbcba_1eaa206	--	--	0x094fd46_c5f15dc_49aa945_61af390_c6fbcba_1eaa206	0x84ab700f
1	1057	0x01009955baf02d07	0xd3f72fa_72933c3_99994fb_9e79e94_5fa70d1_f704527	--	--	0xd3f72fa_72913c3_99994fb_9e79e94_5fa70d1_f704527	0x692cc554
2	1061	0x02013aab7de05a0e	0x4377c9f_267d429_f248fa0_bdc63ce_3356361_839d9c4	--	--	0x4377c9f_045d60b_f248fa0_9dc63ce_3356361_839d9c4	0x5250cb8c
3	1065	0x04027d56f3c0b41d	0x5cd53b7_9b184aa_127e149_ab4dda9_535832c_b2aed33	--	--	0xb23bdb9_22b9f11_127e149_aac9fb1_535832c_92ee523	0xb79a0877
…	…	…	…	…	…	…	…
32	1181	0x092ba0f9429afd45	0x7fd3b56_20a21e9_9676568_	--	--	0xc1d738e_2f7cda6_b19ca19_64	0x2f0f90a4

			7da63eb_cbb2c41_3f5ae3f			a4da5_5f013a9_56978d4	
33	1185	0x025749f28d35da8b	0x3270393_ca8b412_d539c4d_98f03fe_6ee3b48_c0fc7fa	--	--	0xfd4a918_5a8503d_7f3df16_d00b92b_175a37c_74b4cea	0x16b4575f
Line rekey discarded, frame key calc started							
clk	**Sym clk**	**LFSR[59:0]**	**BM0[167:0]**	**OF0[23:16]**	**OF0[15:0]**	**BM1[167:0]**	**OF1[31:0]**
-3	--	--	0x9456894_4c2e428_f2b5681_d808d47_5e773fe_b4b20b2	--	--	0x90e1384_c6d7bce_4a6b23c_9b126ae_a75b8e2_9b3f934	0x8fd0fabd
-2	--	--	0x7fd3b56_20a21e9_9676568_7da63eb_cbb2c41_3f5ae3f	--	--	0xc1d738e_2f7cda6_b19ca19_64a4da5_5f013a9_56978d4	0x2f0f90a4
-1	--	--	0x3270393_ca8b412_d539c4d_98f03fe_6ee3b48_c0fc7fa	--	--	0xfd4a918_5a8503d_7f3df16_d00b92b_175a37c_74b4cea	0x16b4575f
0	1188	--	0x3270393_ca8b412_d539c4d_98f03fe_6ee3b48_c0fc7fa	--	--	0xfd4a918_5a8503d_7f3df16_d00b92b_175a37c_74b4cea	0x16b4575f
1	1189	--	0xc040e35_54294b7_0000000_7a3b0f9_42b1dbd_000006a	--	--	0x79a1e2f_56762af_4729924_e8161bd_436a4af_b679e37	0x69f0745b
2	1193	--	0x6666a4e_47b5444_93d46aa_e4f374f_3cd0333_212d6ab	--	--	0xe5ae184_653d0d6_422cdb0_9326751_8b5b722_ac8c588	0xe5251ab5
3	1197	--	0x1232d67_ef6a7a5_6055678_d509b9f_427d387_e30af77	--	--	0xa3ba60c_7603384_5fecb24_a18686f_e876abd_c64f9a5	0xc3d0c8b0
4	1201	--	0x811566c_da14697_66f89db_84306fe_411d172_f9e3620	--	--	0x6906bae_8dc0578_5d70a0d_ba5d190_c7a72b9_a417c09	0xac19348a
5	1205	--	0xf7027a4_dc24164_29716cf_f0cd06e_9fad21f_41cbe85	--	--	0x3d7c436_17b78b9_16aed72_d5984c5_204904c_a5e135b	0xb7a8f9fb

Table B-38. Cipher State in SST mode for 1-lane, Inter-BS Spacing = 132

clk	stream	cipher	enc stream
-3	0x1c	0x6559c03e	0x1c
-2	0x3c	0x6559c03e	0x3c
-1	0x3c	0x6559c03e	0x3c
0	0x1c	0x6559c03e	0x1c
1	0x39	0xb79ee5fe	0xc7
2	0x00	0xb79ee5fe	0xe5
3	0x00	0xb79ee5fe	0x9e
4	0x39	0xb79ee5fe	0x8e
5	0x00	0x289af919	0x19
6	0x00	0x289af919	0xf9
7	0x39	0x289af919	0xa3
8	0x00	0x289af919	0x28
9	0x00	0xd25b5d6c	0x6c
10	0x39	0xd25b5d6c	0x64
11	0x00	0xd25b5d6c	0x5b
12	0x00	0xd25b5d6c	0xd2
13	0x00	0xed55dcde	0xde
…	…	…	…
125	0x00	0x2f4436cb	0xcb
126	0x00	0x2f4436cb	0x36
127	0x00	0x2f4436cb	0x44
128	0x00	0x2f4436cb	0x2f
129	0xbc	0x7847ef0d	0xbc
130	0x3c	0x7847ef0d	0x3c
131	0x3c	0x7847ef0d	0x3c
132	0xbc	0x7847ef0d	0xbc
133	0x39	0xf96f47cd	0xf4
134	0x00	0xf96f47cd	0x47
135	0x00	0xf96f47cd	0x6f
136	0x39	0xf96f47cd	0xc0
137	0x00	0x30f12a24	0x24
138	0x00	0x30f12a24	0x2a
139	0x39	0x30f12a24	0xc8
140	0x00	0x30f12a24	0x30
141	0x00	0xd47a2546	0x46
…	…	…	…
185	0x00	0x49152bc4	0xc4
186	0x00	0x49152bc4	0x2b
187	0x00	0x49152bc4	0x15
188	0x00	0x49152bc4	0x49
189	0x00	0x1f068148	0x48
190	0x00	0x1f068148	0x81

191	0x00	0x1f068148	0x06
192	0x00	0x1f068148	0x1f
193	0x00	0xb79cb954	0x54
194	0x00	0xb79cb954	0xb9
195	0x00	0xb79cb954	0x9c
196	0x00	0xb79cb954	0xb7
197	0x00	0xfe492f2a	0x2a
198	0x00	0xfe492f2a	0x2f
199	0x00	0xfe492f2a	0x49
200	0x00	0xfe492f2a	0xfe
201	0x00	0x53331e18	0x18
202	0x00	0x53331e18	0x1e
203	0x00	0x53331e18	0x33
204	0x00	0x53331e18	0x53
205	0x00	0x5c0e4039	0x39
206	0x00	0x5c0e4039	0x40
207	0x00	0x5c0e4039	0x0e
208	0x00	0x5c0e4039	0x5c
209	0x00	0x4a040224	0x24
…	…	…	…
257	0x00	0xf254ffb6	0xb6
258	0x00	0xf254ffb6	0xff
259	0x00	0xf254ffb6	0x54
260	0x00	0xf254ffb6	0xf2
261	0xbc	0x14b8b17b	0xbc
262	0x3c	0x14b8b17b	0x3c
263	0x3c	0x14b8b17b	0x3c
264	0xbc	0x14b8b17b	0xbc
265	0x39	0x36693806	0x3f
266	0x00	0x36693806	0x38
267	0x00	0x36693806	0x69
268	0x39	0x36693806	0x0f
269	0x00	0x377c62a2	0xa2
…	…	…	…
389	0x00	0x03b468b1	0xb1
390	0x00	0x03b468b1	0x68
391	0x00	0x03b468b1	0xb4
392	0x00	0x03b468b1	0x03
393	0xbc	0x9328a53d	0xbc
394	0x3c	0x9328a53d	0x3c
395	0x3c	0x9328a53d	0x3c
396	0xbc	0x9328a53d	0xbc
397	0x39	0xb5e38b64	0x5d
398	0x00	0xb5e38b64	0x8b

399	0x00	0xb5e38b64	0xe3
400	0x39	0xb5e38b64	0x8c
401	0x00	0x96fc2396	0x96
402	0x00	0x96fc2396	0x23
403	0x39	0x96fc2396	0xc5
404	0x00	0x96fc2396	0x96
405	0x00	0xbc51d239	0x39
406	0x39	0xbc51d239	0xeb
407	0x00	0xbc51d239	0x51
408	0x00	0xbc51d239	0xbc
409	0x00	0x8908e8ac	0xac
410	0x00	0x8908e8ac	0xe8
411	0x00	0x8908e8ac	0x08
412	0x00	0x8908e8ac	0x89
413	0x00	0x1d74baa3	0xa3
414	0x00	0x1d74baa3	0xba
415	0x00	0x1d74baa3	0x74
416	0x00	0x1d74baa3	0x1d
417	0x00	0xd8835587	0x87
418	0x00	0xd8835587	0x55
419	0x00	0xd8835587	0x83
420	0x00	0xd8835587	0xd8
421	0x00	0xaf70715f	0x5f
422	0x00	0xaf70715f	0x71
423	0x00	0xaf70715f	0x70
424	0x00	0xaf70715f	0xaf
425	0x00	0xc861665f	0x5f
…	…	…	…
505	0x00	0xc07ece76	0x76
506	0x00	0xc07ece76	0xce
507	0x00	0xc07ece76	0x7e
508	0x00	0xc07ece76	0xc0
509	0x00	0xedf08af9	0xf9
510	0x00	0xedf08af9	0x8a
511	0x00	0xedf08af9	0xf0
512	0x00	0xedf08af9	0xed
513	0x00	0xb86284bb	0xbb
514	0x00	0xb86284bb	0x84
515	0x00	0xb86284bb	0x62
516	0x00	0xb86284bb	0xb8
517	0x00	0xb87439a6	0xa6
518	0x00	0xb87439a6	0x39
519	0x00	0xb87439a6	0x74
520	0x00	0xb87439a6	0xb8

521	0x00	0xf701f1ed	0xed
522	0x00	0xf701f1ed	0xf1
523	0x00	0xf701f1ed	0x01
524	0x00	0xf701f1ed	0xf7
525	0xbc	0x523d121c	0xbc
526	0x3c	0x523d121c	0x3c
527	0x3c	0x523d121c	0x3c
528	0xbc	0x523d121c	0xbc
529	0x39	0xf96f47ae	0x97

Table B-39. 1-lane Encrypted Output in SST mode for Inter-BS Spacing = 132

Test Vectors for 1-Lane Main Link Configuration in SST Mode (Inter-BS spacing = 133, CPSR Interval = 9)

Authentication

Table B-3 and Table B-4 provide the LFSR and Block module states during the first part of authentication.

Initial Bootstrapping

Table B-25 provides test vectors during the initial bootstrapping operation.

After start of encryption

Table B-40 provides test vectors generated after the start of encryption (beginning with the first CPSR symbol set that triggers encryption). Table B-41 provides encrypted cipher outputs.

Frame key calc started							
clk	**Sym clk**	**LFSR[59:0]**	**BM0[167:0]**	**OF0[23:16]**	**OF0[15:0]**	**BM1[167:0]**	**OF1[31:0]**
-3	--	--	0xd20317a_3725bc8_256af5e_6b9cc06_7d7aa18_87f9092	--	--	0xd20317a_3725bc8_256af5e_6b9cc06_7d7aa18_87f9092	0x6559c03e
-2	--	--	0xd20317a_3725bc8_256af5e_6b9cc06_7d7aa18_87f9092	--	--	0xd20317a_3725bc8_256af5e_6b9cc06_7d7aa18_87f9092	0x6559c03e
-1	--	--	0xd20317a_3725bc8_256af5e_6b9cc06_7d7aa18_87f9092	--	--	0xd20317a_3725bc8_256af5e_6b9cc06_7d7aa18_87f9092	0x6559c03e
0	0	--	0xd20317a_3725bc8_256af5e_6b9cc06_7d7aa18_87f9092	--	--	0xd20317a_3725bc8_256af5e_6b9cc06_7d7aa18_87f9092	0x6559c03e
1	1	--	0xc040e35_54294b7_0000000_f523e56_bf44e50_000001d	--	--	0x9b48c65_3f7de85_4cfb937_50d9c10_5d7fbdc_6a03908	0xb79ee5fe
2	5	--	0x6666a4e_47b5444_93d46aa_a1a9cb4_a206aaa_cacfa30	--	--	0x94ede66_8141634_5f900d1_5f7a0f0_f291dcb_5a0ce6e	0x289af919
3	9	--	0x1232d67_ef6a7a5_6055678_533e54c_e4b418a_91fbcbb	--	--	0x1f69314_9a31990_c4b92db_31a6525_6ab1304_928c3d8	0xd25b5d6c
4	13	--	0x811566c_da14697_66f89db_d9ce46b_c89e263_9e3097e	--	--	0x7f0a70c_d1bda54_34c9929_7df4b37_d8d588c_855d111	0xed55dcde
…	…	…	…	…	…	…	…
33	129	--	0x315c455_d59f35b_40693cd_5dbf7bd_2df8f08_22cacad	--	--	0x3596433_4643480_8853c0f_95d957d_e351de7_9412e3e	0x7847ef0d
34	133	--	0x080bd0f_043ff91_b512030_bbfa516_f3753d8_957c88c	--	--	0x6267937_99593b7_3013a64_3a0aa4d_b46ea95_1e99035	0xf96f47cd
Line rekey ignored (frame key calc in progress)							
35	137	--	0x65b6244_8461884_2bffcba_a8f7581_264cecb_2cca0f2	--	--	0xdc51ed3_daa4ef1_5dafba7_4ea8052_6f0f06e_712dc22	0x30f12a24
36	141	--	0x259b412_3a73ddc_ddf0be5_8794752_f7203fa_f4acf98	--	--	0x4b2ad3d_0aed7f5_9a40045_f0dc0bd_12077f3_dc5bdc2	0xd47a2546
37	145	--	0x690258d_d03b464_369ae4e_f6cad0a_6018395_0ad8b2a	--	--	0x9d9faf8_16fc911_3eb21eb_939e3bf_17ecf2e_f9fc4f6	0x2e79fa0f
…	…	…	…	…	…	…	…
47	185	--	0xc9472f7_c4371c6_667db05_9e19673_1fcfb80_9e1665f	--	--	0xfa07250_f725212_9bc279d_76fe61a_e1521fc_fb331b7	0x49152bc4
48	189	--	0x2aeaf01_beef443_e0cd9a0_d83548d_480c50a_5d4ed0e	--	--	0xcaf5121_1129806_3836e0a_9051c5e_34551ae_7f7b35a	0x1f068148

49	193	--	0x5cfb3bd_bb2e5ca_6f52793_8bb82fe_ea7c298_d9a59fa	--	--	0x62e765a_09101ee_f92cab1_4cfd7ca_f8ad063_1f97804	0xb79cb954
50	197	0x0f53e0a6257702fe	0x8bb82fe_ea7c298_d9a59fa_f523e56_bf44e50_000001d	--	--	0x960d99e_e9b8b0f_782d158_645c7a9_312615f_ca46465	0xfe492f2a
51	201	0x0ea7c94c42ee05fd	0xb486149_cca6e3d_0355dff_2262329_a206aaa_cacfa30	--	--	0xb72431d_495f294_aba13a4_c1a5edc_d8ea59b_2cbcad0	0x53331e18
52	205	0x0d4f929885dc0bfb	0x120ec20_a1030d1_4c72806_a00fb45_e4b418a_75af954	--	--	0xe94a5e8_bad382a_b516ee3_2aea12a_04f35e9_6a44723	0x5c0e4039
53	209	0x0a9f253103b837f6	0xc084d58_ee8b642_7dd6814_079525e_aef8c5e_ada7f43	--	--	0x8b46a53_283034d_84a452f_9958918_06c7952_3d3b8d2	0x4a040224
…	…	…	…	…	…	…	…
66	261	0x045030ee2cac8144	0x3e289e0_1b214d0_e90ac42_1504b3f_58bc895_c98fa75	--	--	0x6ad3eed_82e9428_1f151a0_fefc1c7_231e1e6_0e7b8ba	0x14b8b17b
67	265	0x08a061dc59590289	0x0e8407c_bb5df9d_578e9dd_6e1b212_7e16013_78ef703	--	--	0xbcf19db_fd7dda6_60704fe_0a9e816_1645fbc_7b03898	0x36693806
Line rekey ignored (frame key calc in progress)							
68	269	0x0140c3b8b2b22512	0x7d0a4b8_3eda746_1d77d70_0293f78_0031fd6_6dab5e6	--	--	0x6ffb9d8_4b94ccf_9e88e41_6fd5114_b45199e_2be2560	0x377c62a2
69	273	0x02818f7165646a25	0x16477db_148dbef_208e96f_3b2aeca_7a8b1e0_2df93a0	--	--	0x0466847_2bf5700_cf0dfc9_79a99b7_e39c678_6e62432	0x1dae33a6
70	277	0x050316e2cac8f44a	0x45e715d_f0a0b8b_2ecd869_23fc80c_2466dbb_f235be8	--	--	0xd39af3a_26aa551_1820274_f0a7d41_ce6244a_1c5aa1e	0xbcde2a64
…	…	…	…	…	…	…	…
98	389	0x090a924ea783998b	0x7b231ab_9d1a11b_aff6b1e_47d273f_c29f20f_81f9565	--	--	0x340a433_93e7bdf_71416c2_002b998_4c9ad89_96f283c	0x03b468b1
99	393	0x0215249d4f073316	0x42b915a_4075db8_54cbde6_2fff97e_9882703_c1ac336	--	--	0x4ece638_a7d51a9_7f9e886_f70ae3d_7bb4fdb_35f33c7	0x9328a53d
100	397	0x042a493a960e662d	0x0960b32_d33d3ea_415be5f_662f358_ea77b3e_bae1860	--	--	0x0eea7d6_bdf8fd6_29fff0a_a341b36_7b88cea_18ceb50	0xb5e38b64
Line rekey ignored (frame key calc in progress)							
101	401	0x08549a75241cec5b	0x283bb5d_356dc1d_5ef8302_740b636_1e2bbb1_77a9024	--	--	0x06af6be_8574776_6244dc1_1c04bf2_7da1a03_e962e82	0x96fc2396
102	405	0x00a934ea4839f8b6	0xd1bdb61_18b2c89_06d55fe_85d7861_4a2d2c4_3f0f76a	--	0x6a42	0x8000eaf_8f340fb_57fba9a_ece383b_5d4ccf2_e2ff34b	0xbc51d239
103	409	0x015269d49873d16c	0xabddb90_19d2b4a_7540b7a_458c215_014c756_aca7735	--	0xb1db	0x394e745_ec99143_e3f8f19_375ec6c_39c7cef_ba78801	0x8908e8ac
104	413	0x02a4d3a938e782d8	0x924eb87_b7a728b_8f829c6_35dd971_63da5b0_486ff01	0x97	0xd7a3	0x398cfb0_51408ef_9500162_a935d4f_835f420_da99144	0x1d74baa3
105	417	0x0549af5279cf05b1	0x711d28b_ffa6fca_923e67b_15707a7_42a4bb2_2deda6d	0xbb	0xb0f9	0xde9d7c1_83df898_1e55332_ddc9add_a82acb2_2885c03	0xd8835587
106	421	0x0a935ea4f39e2b63	0xeff1213_e232b20_0064b82_ae1968a_4a3cba4_40cb306	0x62	0x84bb	0xd887f8b_5d37e0d_fe4d145_6a55c77_9369bfb_5028d20	0xaf70715f
107	425	0x0a935ea4f39e2b63	0xeff1213_e232b20_0064b82_ae1968a_4a3cba4_40cb306	0x62	0x84bb	0xb77f694_6fed836_ec5fbda_befa034_2c5d690_ae478e9	0xc861665f
108	429	0x0a935ea4f39e2b63		0x62	0x84bb		0x2bbcf09a

			0xeff1213_e232b20_0064b82_ae1968a_4a3cba4_40cb306			0xa67d45e_0b30f7d_2bb93be_e09b5f5_22ca847_b849198	
…	…	…	…	…	…	…	…
127	505	0x0a935ea4f39e2b63	0xeff1213_e232b20_0064b82_ae1968a_4a3cba4_40cb306	0x62	0x84bb	0x6886c93_2065e45_773f684_82237f8_df3ef7a_cae90a7	0xc07ece76
128	509	0x0a935ea4f39e2b63	0xeff1213_e232b20_0064b82_ae1968a_4a3cba4_40cb306	0x62	0x84bb	0x9359a39_d450a12_51ce5bc_d3062b6_2c9cca3_c74edc4	0xedf08af9
129	513	0x0a935ea4f39e2b63	0xeff1213_e232b20_0064b82_ae1968a_4a3cba4_40cb306	0x62	0x84bb	0xeff1213_e232b20_0064b82_ae1968a_4a3cba4_40cb306	0xb86284bb
130	517	0x0526b549e73c76c7	0xddd552f_3d3bac2_fb230d5_83a2d78_5a1da41_8fed1d6	0x74	0x39a6	0xddd552f_3d3bac2_fb230d5_83a2d78_5a1da41_8fed1d6	0xb87439a6
131	521	0x0a4d6293ce78ed8e	0xc258963_5d097d0_e50aa7c_fc50f00_a2a747b_a45b784	0x01	0xf1ed	0xc258963_5d097d0_e50aa7c_fc50f00_a2a747b_a45b784	0xf701f1ed
132	525	0x049ac5279cf1fb1c	0xb06e6b7_c8209e8_82982f7_4bc1a13_8a3f797_9f0446e	0x3d	0x121c	0xb06e6b7_c8209e8_82982f7_4bc1a13_8a3f797_9f0446e	0x523d121c
133	529	0x09358a4f31e3d639	0xefd27df_0e46509_e0b63da_cb3dc05_af53ae8_4436e20	0x6f	0x47ae	0xefd27df_0e46509_e0b63da_cb3dc05_af53ae8_4436e20	0xf96f47ae
Line rekey started							
clk	**Sym clk**	**LFSR[59:0]**	**BM0[167:0]**	**OF0[23:16]**	**OF0[15:0]**	**BM1[167:0]**	**OF1[31:0]**
-3	--	0x0a4d6293ce78ed8e	0xc258963_5d097d0_e50aa7c_fc50f00_a2a747b_a45b784	--	--	0xc258963_5d097d0_e50aa7c_fc50f00_a2a747b_a45b784	0xf701f1ed
-2	--	0x049ac5279cf1fb1c	0xb06e6b7_c8209e8_82982f7_4bc1a13_8a3f797_9f0446e	--	--	0xb06e6b7_c8209e8_82982f7_4bc1a13_8a3f797_9f0446e	0x523d121c
-1	--	0x09358a4f31e3d639	0xefd27df_0e46509_e0b63da_cb3dc05_af53ae8_4436e20	--	--	0xefd27df_0e46509_e0b63da_cb3dc05_af53ae8_4436e20	0xf96f47ae
0	532	0x09358a4f31e3d639	0xefd27df_0e46509_e0b63da_cb3dc05_af53ae8_4436e20	--	--	0xefd27df_0e46509_e0b63da_cb3dc05_af53ae8_4436e20	0xf96f47ae
1	533	0x026b1c9e63c7ac73	0xc479a9c_8c09955_e4b84bc_f4d23b6_286c3cc_fbefcbb	--	--	0xc479a9c_8c0b955_e4b84bc_f4d23b6_286c3cc_fbefcbb	0xba695c5b
2	537	0x04d6313ccf8f58e6	0x6f9b366_49610cf_895c70f_eaf2c27_410aaa3_e0e83bf	--	--	0x6f9b366_6b432ed_895c70f_caf2c27_410aaa3_e0e83bf	0x1163a5e9
…	…	…	…	…	…	…	…
32	657	0x00ffedb9091de580	0xfe540b1_c0aa0d3_dc2cc45_c9ace54_b5a739e_9384394	--	--	0xd90e59c_f9f3d1b_6480004_14d76a9_ba528a2_170c303	0xce6d0db0
33	661	0x01ffd3721a3beb00	0x591fc74_00754e2_bfa4739_d848399_afd0bfb_726948b	--	--	0x7f99cd9_7bc4777_4f5593a_643b662_d78d88d_1dd73e0	0x704bd830
34	665	0x03ffa6e43c77d601	0x43b5667_02d61d2_f5812e5_4e9c794_3d4cdb0_9530772	--	--	0x4b13e98_07bda78_c94b39a_f01addb_0943b5d_1f7d73a	0x81f96994
Line rekey ignored (line rekey in progress)							
35	669	0x07ff4dc870ef8c02	0xe50cdad_3747032_e95e7a5_fbc8e6e_e00ef74_445984d	--	--	0x1f02567_0a2ef15_2a264cf_36062be_b694461_9d4aa76	0xf8ddfa97
36	673	0x0ffe9390e1df3805	0x9619e54_1321c4e_8daeffc_2fd5d59_3c9fd1b_50801a0	--	--	0xd958cac_b612b7c_ffd80c1_501b9c0_0285d24_79ab641	0x141411f4
37	677	0x0ffd2721c3be700b	0x344225f_a33ef5d_b899367_a4f6a6d_b708baa_67e4ac3	--	--	0x4aac08f_4b6a84d_858627d_d97d18f_b43bc3d_6de1bbf	0xaf5a5b30

…	…	…	…	…	…	…	…
51	733	0x09a529c3d5375686	0x41c3db8_7e60b5d_ade6c26_0335bb1_0313ffb_ce6d556	--	--	0xde83510_f93dd7e_8f09cca_fd7e979_439879a_5870c89	0x0e661a04
52	737	0x034a5387aa6ead0c	0xda39225_0d2f8e6_487e46d_14adaff_c23321e_7e5a780	--	--	0x9fd4127_873eeab_d443857_d7bc533_04fa8ab_a4eee09	0xe8b7ea1e
53	741	0x0694af0f54dd7a18	0xb6bee9e_b0ef775_f7d10ad_5dce396_89b2597_acef7ea	--	--	0xd5858aa_e4354ca_b52fefd_c3e62de_3960ed5_cbc6aa5	0xac7e0ebc
54	745	0x0d29561ea1bad430	0x0beb3a9_cb636c5_ce7a6d6_3ab9bdb_c93d31b_c325019	--	--	0xed3734d_00d67e7_eb76874_e2d404c_09ed965_dc23211	0x233bf0c3
55	749	0x0a52a43d4b758861	0x6a3ad12_9856416_6c93fda_e14a23d_fbc4d3f_cceecdf	--	--	0xe17cdec_bc66357_8450c0e_5f72374_878db0c_6b13d1e	0x16208c84
56	753	0x04a5487a96eb30c2	0x6a9b47c_328300c_494b633_ca430af_69d5a81_2aca65b	--	--	0x55182ed_d8e05f7_37f417a_14ed44b_585f76b_94900de	0x2acbe06b
57	757	0x04a5487a96eb30c2	0x6a9b47c_328300c_494b633_ca430af_69d5a81_2aca65b	--	--	0x56aaf6d_07f58d8_abfa327_62d4dd6_60f966f_d4fe34f	0xe856019a
58	761	0x04a5487a96eb30c2	0x6a9b47c_328300c_494b633_ca430af_69d5a81_2aca65b	--	--	0x2580555_5d338c9_26f9fd1_6d25c0e_039fddc_e85384f	0xe2966145
63	781	0x04a5487a96eb30c2	0x6a9b47c_328300c_494b633_ca430af_69d5a81_2aca65b	--	--	0x6a915c3_b74a718_800888e_a7c90f3_64965d8_d4ac098	0x5807ee8e
64	785	0x04a5487a96eb30c2	0x6a9b47c_328300c_494b633_ca430af_69d5a81_2aca65b	--	--	0x777e0ab_9d33db8_5d4bfca_8ece80c_37d57f2_24fd7b7	0x62b4c1ae
65	789	0x04a5487a96eb30c2	0x6a9b47c_328300c_494b633_ca430af_69d5a81_2aca65b	--	--	0x6a9b47c_328300c_494b633_ca430af_69d5a81_2aca65b	0x937ac3f3
66	793	0x094a98f52dd66185	0x879a851_989b69f_6420e6d_ddc1460_b3f26bd_8c556ad	--	--	0x879a851_989b69f_6420e6d_ddc1460_b3f26bd_8c556ad	0x79da1e88
67	797	0x029531ea53acc30b	0x18de01a_768c6d5_e218387_a350cbc_03ebb4b_1e54508	--	--	0x18de01a_768c6d5_e218387_a350cbc_03ebb4b_1e54508	0x67f2a9c2
Line rekey started							
clk	**Sym clk**	**LFSR[59:0]**	**BM0[167:0]**	**OF0[23:16]**	**OF0[15:0]**	**BM1[167:0]**	**OF1[31:0]**
-3	--	0x04a5487a96eb30c2	0x6a9b47c_328300c_494b633_ca430af_69d5a81_2aca65b	--	--	0x6a9b47c_328300c_494b633_ca430af_69d5a81_2aca65b	0x937ac3f3
-2	--	0x094a98f52dd66185	0x879a851_989b69f_6420e6d_ddc1460_b3f26bd_8c556ad	--	--	0x879a851_989b69f_6420e6d_ddc1460_b3f26bd_8c556ad	0x79da1e88
-1	--	0x029531ea53acc30b	0x18de01a_768c6d5_e218387_a350cbc_03ebb4b_1e54508	--	--	0x18de01a_768c6d5_e218387_a350cbc_03ebb4b_1e54508	0x67f2a9c2
0	798	0x029531ea53acc30b	0x18de01a_768c6d5_e218387_a350cbc_03ebb4b_1e54508	--	--	0x18de01a_768c6d5_e218387_a350cbc_03ebb4b_1e54508	0x67f2a9c2
1	801	0x052a6bd4a759a617	0x1993cc8_32dc62a_6962b83_4d8c4fe_e2f16b4_ebf7986	--	--	0x1993cc8_32de62a_6962b83_4d8c4fe_e2f16b4_ebf7986	0x083a8ba3
2	805	0x0a54dfa946b34c2e	0x0e822db_a83031f_a9c4a5b_2943f8c_cf24631_4ffcb67	--	--	0x0e822db_8a1213d_a9c4a5b_0943f8c_cf24631_4ffcb67	0xf9b2505f
…	…	…	…	…	…	…	…
32	925	0x05513421c78b598c	0x6a80987_0e95bf5_ff13137_2f7f90f_559cb7c_8763f11	--	--	0xd7aca29_889bac2_ffd8d76_446ecbc_b8ee21c_69d14b3	0x02ba87f6
33	929	0x0aa2604387169318		--	--		0x41a13092

			0x964fcca_e183cf2_cc9a9b2_d9aef6c_96b722f_9ba5081			0x3ccd221_f7a33c5_b9cfdd3_1334641_674cc6d_039ed41	
Line rekey ignored (line rekey in progress)							
34	933	0x0544c8870e2d0631	0xd0a7549_827ecb5_0e9b0be_6001de0_120a3d0_f6e29bb	--	--	0x42fe8b9_145cf66_d8bb70a_b8e892a_5ed212b_4b15bf3	0x099981e4
35	937	0x0a89990e145a0c62	0xfa86c8d_1af071c_687b404_fdd2043_264ea97_a41bbed	--	--	0xe2cf8f4_69fa1f8_07d760d_a5c7214_bda88c2_8f3d44a	0xb9f0f349
…	…	…	…	…	…	…	…
53	1009	0x0620152ab75e01a0	0xc34595a_3b6bd29_a9ace02_421d3d2_98cf20a_12441ff	--	--	0xae00e68_517b4b4_7de84dc_f7fb234_4bca73f_80f4c73	0x3173e010
54	1013	0x0c4022556ebc0341	0x17b53ed_79f6295_1d7c546_51c3843_88920d9_ccfbe63	--	--	0x2cd390c_12f1d92_ccb0f59_1d1f860_16aa9fb_304a3dc	0x459d0f2f
55	1017	0x08804caadd780683	0xf9b9441_325afe9_ffd7607_8f5c1fa_88ef726_e63027d	--	--	0xe29dc85_2ed2398_37e2616_42a9516_d3aa0c8_e268bd9	0x96e30b57
56	1021	0x01009955baf02d07	0xb55b860_68abd28_4f65ac8_383454a_8f10900_4081619	--	--	0x57a3287_d9b745b_d715c19_0e684e5_ffb924e_5478cea	0x9624dba8
57	1025	0x01009955baf02d07	0xb55b860_68abd28_4f65ac8_383454a_8f10900_4081619	--	--	0xb1e4394_55e273f_70532c8_5dfaa41_abb4601_d8ff7cd	0x8dec989a
58	1029	0x01009955baf02d07	0xb55b860_68abd28_4f65ac8_383454a_8f10900_4081619	--	--	0x6ee584a_348883e_f31e258_2534612_8801757_fa0915d	0xff3d0703
…	…	…	…	…	…	…	…
63	1049	0x01009955baf02d07	0xb55b860_68abd28_4f65ac8_383454a_8f10900_4081619	--	--	0xccbcc90_3a26f7f_fa84ec6_6b64021_7acb60a_90a0769	0x14b2c4f0
64	1053	0x01009955baf02d07	0xb55b860_68abd28_4f65ac8_383454a_8f10900_4081619	--	--	0xb71fa43_96268fa_eb8c722_56fe792_22b83b0_3a96d93	0x2564b543
65	1057	0x01009955baf02d07	0xb55b860_68abd28_4f65ac8_383454a_8f10900_4081619	--	--	0xb55b860_68abd28_4f65ac8_383454a_8f10900_4081619	0x71144aa6
66	1061	0x02013aab7de05a0e	0xc28b46c_b53905a_b27971e_368bd36_d1ddedf_d2632fb	--	--	0xc28b46c_b53905a_b27971e_368bd36_d1ddedf_d2632fb	0xae82b903
Line rekey started							
clk	**Sym clk**	**LFSR[59:0]**	**BM0[167:0]**	**OF0[23:16]**	**OF0[15:0]**	**BM1[167:0]**	**OF1[31:0]**
-3	--	0x01009955baf02d07	0xb55b860_68abd28_4f65ac8_383454a_8f10900_4081619	--	--	0xb71fa43_96268fa_eb8c722_56fe792_22b83b0_3a96d93	0x2564b543
-2	--	0x01009955baf02d07	0xb55b860_68abd28_4f65ac8_383454a_8f10900_4081619	--	--	0xb55b860_68abd28_4f65ac8_383454a_8f10900_4081619	0x71144aa6
-1	--	0x02013aab7de05a0e	0xc28b46c_b53905a_b27971e_368bd36_d1ddedf_d2632fb	--	--	0xc28b46c_b53905a_b27971e_368bd36_d1ddedf_d2632fb	0xae82b903
0	1064	0x02013aab7de05a0e	0xc28b46c_b53905a_b27971e_368bd36_d1ddedf_d2632fb	--	--	0xc28b46c_b53905a_b27971e_368bd36_d1ddedf_d2632fb	0xae82b903
1	1065	0x04027d56f3c0b41d	0xee77b50_0034f9a_6c6262d_530e647_2bdd9a7_11d3cf8	--	--	0xee77b50_0036f9a_6c6262d_530e647_2bdd9a7_11d3cf8	0x345dcf27
2	1069	0x0804f2adef81483b	0x0dc1123_a65032c_1c26806_a9aae5a_1e40b3e_9a04ff9	--	--	0x0dc1123_847210e_1c26806_89aae5a_1e40b3e_9a04ff9	0x15f96dbb
3	1073	0x0009e55bdf02b077	0x400c396_707f793_668d894_d1814b4_3c09240_82d6f30	--	--	0xaee2d98_ebfce0a_668d894_f0056ac_3c09240_a2d6720	0xea8546eb

…	…	…	…	…	…	…	…
32	1189	0x04ae9be51a6bb517	0x5c0ad37_b7ca0ba_f946b32_8322662_1a5f634_2e91771	--	--	0x7ee4fe7_bb32144_9dbba9e_fd70a6d_72e9c54_25a03d6	0x1f19ab19
33	1193	0x095d37ca3cd76a2e	0x78ed1ab_7507e03_3b961a0_e02d291_65ce57c_d4a3c9c	--	--	0x067d1fe_363749e_27ef059_d05c4f2_7ed36e6_06b050d	0xe2ceec41
Line rekey discarded, frame key calc started							
clk	**Sym clk**	**LFSR[59:0]**	**BM0[167:0]**	**OF0[23:16]**	**OF0[15:0]**	**BM1[167:0]**	**OF1[31:0]**
-3	--	--	0x5b9dc62_cabb993_c6412b8_04f1e29_5830aec_cb8bab3	--	--	0x67b8eef_6080601_7077dfa_4358f6c_ac5f74e_4941ecf	0x6fe03b2d
-2	--	--	0x5c0ad37_b7ca0ba_f946b32_8322662_1a5f634_2e91771	--	--	0x7ee4fe7_bb32144_9dbba9e_fd70a6d_72e9c54_25a03d6	0x1f19ab19
-1	--	--	0x78ed1ab_7507e03_3b961a0_e02d291_65ce57c_d4a3c9c	--	--	0x067d1fe_363749e_27ef059_d05c4f2_7ed36e6_06b050d	0xe2ceec41
0	1197	--	0x3493fbf_7fec72a_d00e4a6_51eae22_ad0c80d_f18d4e6	--	--	0xec1fa05_dc2f319_2353dc8_99431ee_21fe2b8_1b8671d	0xe55bdb57
1	1198	--	0xc040e35_54294b7_0000000_7a3b0f9_42b1dbd_000006a	--	--	0x20afe0a_406fe7b_801a956_42c07ac_2048374_d872687	0x37a7ad67
2	1202	--	0x6666a4e_47b5444_93d46aa_e4f374f_3cd0333_212d6ab	--	--	0x0010b30_a015e96_19a299b_8ccca7f_f8d3670_4eec3e0	0x4dcc0b1d
3	1206	--	0x1232d67_ef6a7a5_6055678_d509b9f_427d387_e30af77	--	--	0x241b2b1_5cad5e0_e28a200_6132372_64cabb7_050fd0b	0x0a0a9458
4	1210	--	0x811566c_da14697_66f89db_84306fe_411d172_f9e3620	--	--	0x802e4a0_24e6726_230bb03_2e7e544_c3b5aba_ba94642	0x3f6037e5
5	1214	--	0xf7027a4_dc24164_29716cf_f0cd06e_9fad21f_41cbe85	--	--	0x64e40d7_0798734_eed6444_034e9e0_d7a7c97_7f29c38	0x3df2daf4

Table B-40. Cipher State in SST mode for 1-lane, Inter-BS Spacing = 133

clk	stream	cipher	enc stream
-3	0x1c	0x6559c03e	0x1c
-2	0x3c	0x6559c03e	0x3c
-1	0x3c	0x6559c03e	0x3c
0	0x1c	0x6559c03e	0x1c
1	0x39	0xb79ee5fe	0xc7
2	0x00	0xb79ee5fe	0xe5
3	0x00	0xb79ee5fe	0x9e
4	0x39	0xb79ee5fe	0x8e
5	0x00	0x289af919	0x19
6	0x00	0x289af919	0xf9
7	0x39	0x289af919	0xa3
8	0x00	0x289af919	0x28
9	0x00	0xd25b5d6c	0x6c
10	0x39	0xd25b5d6c	0x64
11	0x00	0xd25b5d6c	0x5b
12	0x00	0xd25b5d6c	0xd2
13	0x00	0xed55dcde	0xde
…	…	…	…
129	0x00	0x7847ef0d	0x0d
130	0xbc	0x7847ef0d	0xbc
131	0x3c	0x7847ef0d	0x3c
132	0x3c	0x7847ef0d	0x3c
133	0xbc	0xf96f47cd	0xbc
134	0x39	0xf96f47cd	0x7e
135	0x00	0xf96f47cd	0x6f
136	0x00	0xf96f47cd	0xf9
137	0x39	0x30f12a24	0x1d
138	0x00	0x30f12a24	0x2a
139	0x00	0x30f12a24	0xf1
140	0x39	0x30f12a24	0x09
141	0x00	0xd47a2546	0x46
142	0x00	0xd47a2546	0x25
143	0x39	0xd47a2546	0x43
144	0x00	0xd47a2546	0xd4
145	0x00	0x2e79fa0f	0x0f
…	…	…	…
185	0x00	0x49152bc4	0xc4
186	0x00	0x49152bc4	0x2b
187	0x00	0x49152bc4	0x15
188	0x00	0x49152bc4	0x49
189	0x00	0x1f068148	0x48
190	0x00	0x1f068148	0x81

191	0x00	0x1f068148	0x06
192	0x00	0x1f068148	0x1f
193	0x00	0xb79cb954	0x54
194	0x00	0xb79cb954	0xb9
195	0x00	0xb79cb954	0x9c
196	0x00	0xb79cb954	0xb7
197	0x00	0xfe492f2a	0x2a
198	0x00	0xfe492f2a	0x2f
199	0x00	0xfe492f2a	0x49
200	0x00	0xfe492f2a	0xfe
201	0x00	0x53331e18	0x18
202	0x00	0x53331e18	0x1e
203	0x00	0x53331e18	0x33
204	0x00	0x53331e18	0x53
205	0x00	0x5c0e4039	0x39
206	0x00	0x5c0e4039	0x40
207	0x00	0x5c0e4039	0x0e
208	0x00	0x5c0e4039	0x5c
209	0x00	0x4a040224	0x24
…	…	…	…
261	0x00	0x14b8b17b	0x7b
262	0x00	0x14b8b17b	0xb1
263	0xbc	0x14b8b17b	0xbc
264	0x3c	0x14b8b17b	0x3c
265	0x3c	0x36693806	0x3c
266	0xbc	0x36693806	0xbc
267	0x39	0x36693806	0x50
268	0x00	0x36693806	0x36
269	0x00	0x377c62a2	0xa2
270	0x39	0x377c62a2	0x5b
271	0x00	0x377c62a2	0x7c
272	0x00	0x377c62a2	0x37
273	0x39	0x1dae33a6	0x9f
274	0x00	0x1dae33a6	0x33
275	0x00	0x1dae33a6	0xae
276	0x39	0x1dae33a6	0x24
277	0x00	0xbcde2a64	0x64
…	…	…	…
389	0x00	0x03b468b1	0xb1
390	0x00	0x03b468b1	0x68
391	0x00	0x03b468b1	0xb4
392	0x00	0x03b468b1	0x03
393	0x00	0x9328a53d	0x3d
394	0x00	0x9328a53d	0xa5

395	0x00	0x9328a53d	0x28
396	0xbc	0x9328a53d	0xbc
397	0x3c	0xb5e38b64	0x3c
398	0x3c	0xb5e38b64	0x3c
399	0xbc	0xb5e38b64	0xbc
400	0x39	0xb5e38b64	0x8c
401	0x00	0x96fc2396	0x96
402	0x00	0x96fc2396	0x23
403	0x39	0x96fc2396	0xc5
404	0x00	0x96fc2396	0x96
405	0x00	0xbc51d239	0x39
406	0x39	0xbc51d239	0xeb
407	0x00	0xbc51d239	0x51
408	0x00	0xbc51d239	0xbc
409	0x39	0x8908e8ac	0x95
410	0x00	0x8908e8ac	0xe8
411	0x00	0x8908e8ac	0x08
412	0x00	0x8908e8ac	0x89
413	0x00	0x1d74baa3	0xa3
414	0x00	0x1d74baa3	0xba
415	0x00	0x1d74baa3	0x74
416	0x00	0x1d74baa3	0x1d
417	0x00	0xd8835587	0x87
418	0x00	0xd8835587	0x55
419	0x00	0xd8835587	0x83
420	0x00	0xd8835587	0xd8
421	0x00	0xaf70715f	0x5f
422	0x00	0xaf70715f	0x71
423	0x00	0xaf70715f	0x70
424	0x00	0xaf70715f	0xaf
425	0x00	0xc861665f	0x5f
426	0x00	0xc861665f	0x66
427	0x00	0xc861665f	0x61
428	0x00	0xc861665f	0xc8
429	0x00	0x2bbcf09a	0x9a
…	…	…	…
505	0x00	0xc07ece76	0x76
506	0x00	0xc07ece76	0xce
507	0x00	0xc07ece76	0x7e
508	0x00	0xc07ece76	0xc0
509	0x00	0xedf08af9	0xf9
510	0x00	0xedf08af9	0x8a
511	0x00	0xedf08af9	0xf0
512	0x00	0xedf08af9	0xed

513	0x00	0xb86284bb	0xbb
514	0x00	0xb86284bb	0x84
515	0x00	0xb86284bb	0x62
516	0x00	0xb86284bb	0xb8
517	0x00	0xb87439a6	0xa6
518	0x00	0xb87439a6	0x39
519	0x00	0xb87439a6	0x74
520	0x00	0xb87439a6	0xb8
521	0x00	0xf701f1ed	0xed
522	0x00	0xf701f1ed	0xf1
523	0x00	0xf701f1ed	0x01
524	0x00	0xf701f1ed	0xf7
525	0x00	0x523d121c	0x1c
526	0x00	0x523d121c	0x12
527	0x00	0x523d121c	0x3d
528	0x00	0x523d121c	0x52
529	0xbc	0xf96f47ae	0xbc
530	0x3c	0xf96f47ae	0x3c
531	0x3c	0xf96f47ae	0x3c
532	0xbc	0xf96f47ae	0xbc
533	0x39	0xba695c5b	0x62

Table B-41. 1-lane Encrypted Output in SST mode for Inter-BS Spacing = 133

Test Vectors for 1-Lane Main Link Configuration in SST Mode (Inter-BS spacing = 607, CPSR Interval = 5)

Authentication

Table B-3 and Table B-4 provide the LFSR and Block module states during the first part of authentication.

Initial Bootstrapping

Table B-25 provides test vectors during the initial bootstrapping operation.

After start of encryption

Table B-42 provides test vectors generated after the start of encryption (beginning with the first CPSR symbol set that triggers encryption). Table B-43 provides encrypted cipher outputs.

Frame key calc started

clk	Sym clk	LFSR[59:0]	BM0[167:0]	OF0[23:16]	OF0[15:0]	BM1[167:0]	OF1[31:0]
-3	--	--	0xd20317a_3725bc8_256af5e_6b9cc06_7d7aa18_87f9092	--	--	0xd20317a_3725bc8_256af5e_6b9cc06_7d7aa18_87f9092	0x6559c03e
-2	--	--	0xd20317a_3725bc8_256af5e_6b9cc06_7d7aa18_87f9092	--	--	0xd20317a_3725bc8_256af5e_6b9cc06_7d7aa18_87f9092	0x6559c03e
-1	--	--	0xd20317a_3725bc8_256af5e_6b9cc06_7d7aa18_87f9092	--	--	0xd20317a_3725bc8_256af5e_6b9cc06_7d7aa18_87f9092	0x6559c03e
0	0	--	0xd20317a_3725bc8_256af5e_6b9cc06_7d7aa18_87f9092	--	--	0xd20317a_3725bc8_256af5e_6b9cc06_7d7aa18_87f9092	0x6559c03e
1	1	--	0xc040e35_54294b7_0000000_f523e56_bf44e50_000001d	--	--	0x9b48c65_3f7de85_4cfb937_50d9c10_5d7fbdc_6a03908	0xb79ee5fe
2	5	--	0x6666a4e_47b5444_93d46aa_a1a9cb4_a206aaa_cacfa30	--	--	0x94ede66_8141634_5f900d1_5f7a0f0_f291dcb_5a0ce6e	0x289af919
3	9	--	0x1232d67_ef6a7a5_6055678_533e54c_e4b418a_91fbcbb	--	--	0x1f69314_9a31990_c4b92db_31a6525_6ab1304_928c3d8	0xd25b5d6c
4	13	--	0x811566c_da14697_66f89db_d9ce46b_c89e263_9e3097e	--	--	0x7f0a70c_d1bda54_34c9929_7df4b37_d8d588c_855d111	0xed55dcde
…	…	…	…	…	…	…	…
45	177	--	0x8b0a742_b70da1c_2307640_f0093a0_6c69ad6_2dfc26d	--	--	0x4736b27_c7ebca1_aa86bef_4539c7b_6c6bdec_c4b1f11	0x10f21d66
46	181	--	0x57dd199_d4f7e9b_b85862b_5cc55f4_2b5efea_85611ff	--	--	0x2789d57_f53ee8a_3cfeaf5_817480c_c30af76_2f49767	0x37affe86
47	185	--	0xc9472f7_c4371c6_667db05_9e19673_1fcfb80_9e1665f	--	--	0xfa07250_f725212_9bc279d_76fe61a_e1521fc_fb331b7	0x49152bc4
48	189	--	0x2aeaf01_beef443_e0cd9a0_d83548d_480c50a_5d4ed0e	--	--	0xcaf5121_1129806_3836e0a_9051c5e_34551ae_7f7b35a	0x1f068148
49	193	--	0x5cfb3bd_bb2e5ca_6f52793_8bb82fe_ea7c298_d9a59fa	--	--	0x62e765a_09101ee_f92cab1_4cfd7ca_f8ad063_1f97804	0xb79cb954
50	197	0x0f53e0a6257702fe	0x8bb82fe_ea7c298_d9a59fa_f523e56_bf44e50_000001d	--	--	0x960d99e_e9b8b0f_782d158_645c7a9_312615f_ca46465	0xfe492f2a
51	201	0x0ea7c94c42ee05fd	0xb486149_cca6e3d_0355dff_2262329_a206aaa_cacfa30	--	--	0xb72431d_495f294_aba13a4_c1a5edc_d8ea59b_2cbcad0	0x53331e18
52	205	0x0d4f929885dc0bfb	0x120ec20_a1030d1_4c72806_a00fb45_e4b418a_75af954	--	--	0xe94a5e8_bad382a_b516ee3_2aea12a_04f35e9_6a44723	0x5c0e4039

53	209	0x0a9f253103b837f6	0xc084d58_ee8b642_7dd6814_079525e_aef8c5e_ada7f43	--	--	0x8b46a53_283034d_84a452f_9958918_06c7952_3d3b8d2	0x4a040224
…	…	…	…	…	…	…	…
101	401	0x08549a75241cec5b	0x283bb5d_356dc1d_5ef8302_740b636_1e2bbb1_77a9024	--	--	0x06af6be_8574776_6244dc1_1c04bf2_7da1a03_e962e82	0x96fc2396
102	405	0x00a934ea4839f8b6	0xd1bdb61_18b2c89_06d55fe_85d7861_4a2d2c4_3f0f76a	--	0x6a42	0x8000eaf_8f340fb_57fba9a_ece383b_5d4ccf2_e2ff34b	0xbc51d239
103	409	0x015269d49873d16c	0xabddb90_19d2b4a_7540b7a_458c215_014c756_aca7735	--	0xb1db	0x394e745_ec99143_e3f8f19_375ec6c_39c7cef_ba78801	0x8908e8ac
104	413	0x02a4d3a938e782d8	0x924eb87_b7a728b_8f829c6_35dd971_63da5b0_486ff01	0x97	0xd7a3	0x398cfb0_51408ef_9500162_a935d4f_835f420_da99144	0x1d74baa3
105	417	0x0549af5279cf05b1	0x711d28b_ffa6fca_923e67b_15707a7_42a4bb2_2deda6d	0xbb	0xb0f9	0xde9d7c1_83df898_1e55332_ddc9add_a82acb2_2885c03	0xd8835587
106	421	0x0a935ea4f39e2b63	0xeff1213_e232b20_0064b82_ae1968a_4a3cba4_40cb306	0x62	0x84bb	0xd887f8b_5d37e0d_fe4d145_6a55c77_9369bfb_5028d20	0xaf70715f
107	425	0x0a935ea4f39e2b63	0xeff1213_e232b20_0064b82_ae1968a_4a3cba4_40cb306	0x62	0x84bb	0xb77f694_6fed836_ec5fbda_befa034_2c5d690_ae478e9	0xc861665f
108	429	0x0a935ea4f39e2b63	0xeff1213_e232b20_0064b82_ae1968a_4a3cba4_40cb306	0x62	0x84bb	0xa67d45e_0b30f7d_2bb93be_e09b5f5_22ca847_b849198	0x2bbcf09a
…	…	…	…	…	…	…	…
125	497	0x0a935ea4f39e2b63	0xeff1213_e232b20_0064b82_ae1968a_4a3cba4_40cb306	0x62	0x84bb	0x166a2ba_5f9a304_a43b4df_8fbe5a7_9a54da6_efc6a5c	0xee629a59
126	501	0x0a935ea4f39e2b63	0xeff1213_e232b20_0064b82_ae1968a_4a3cba4_40cb306	0x62	0x84bb	0x449391b_636e0e9_7fcec83_c85f608_d20d4b9_1a23cd8	0x0d25408d
127	505	0x0a935ea4f39e2b63	0xeff1213_e232b20_0064b82_ae1968a_4a3cba4_40cb306	0x62	0x84bb	0x6886c93_2065e45_773f684_82237f8_df3ef7a_cae90a7	0xc07ece76
128	509	0x0a935ea4f39e2b63	0xeff1213_e232b20_0064b82_ae1968a_4a3cba4_40cb306	0x62	0x84bb	0x9359a39_d450a12_51ce5bc_d3062b6_2c9cca3_c74edc4	0xedf08af9
129	513	0x0a935ea4f39e2b63	0xeff1213_e232b20_0064b82_ae1968a_4a3cba4_40cb306	0x62	0x84bb	0xeff1213_e232b20_0064b82_ae1968a_4a3cba4_40cb306	0xb86284bb
130	517	0x0526b549e73c76c7	0xddd552f_3d3bac2_fb230d5_83a2d78_5a1da41_8fed1d6	0x74	0x39a6	0xddd552f_3d3bac2_fb230d5_83a2d78_5a1da41_8fed1d6	0xb87439a6
131	521	0x0a4d6293ce78ed8e	0xc258963_5d097d0_e50aa7c_fc50f00_a2a747b_a45b784	0x01	0xf1ed	0xc258963_5d097d0_e50aa7c_fc50f00_a2a747b_a45b784	0xf701f1ed
…	…	…	…	…	…	…	…
151	601	0x00854389327a1c4b	0x3ee198a_04b39f8_f01ee89_e392916_3d7c268_0807828	0x6e	0x587b	0x3ee198a_04b39f8_f01ee89_e392916_3d7c268_0807828	0x7a6e587b
152	605	0x010a87126cf41896	0xa229e89_1f7747e_b6ce495_101202e_020e264_4873cd6	0xc7	0xb3a7	0xa229e89_1f7747e_b6ce495_101202e_020e264_4873cd6	0x09c7b3a7
Line rekey started							
clk	**Sym clk**	**LFSR[59:0]**	**BM0[167:0]**	**OF0[23:16]**	**OF0[15:0]**	**BM1[167:0]**	**OF1[31:0]**
-3	--	0x0842a5c49d3d0e25	0x2284715_70e251b_ec74b73_4f59d37_3639be9_33147ad	--	--	0x2284715_70e251b_ec74b73_4f59d37_3639be9_33147ad	0x07b605a2
-2	--	0x00854389327a1c4b	0x3ee198a_04b39f8_f01ee89_e392916_3d7c268_0807828	--	--	0x3ee198a_04b39f8_f01ee89_e392916_3d7c268_0807828	0x7a6e587b

-1	--	0x010a87126cf41896	0xa229e89_1f7747e_b6ce495_101202e_020e264_4873cd6	--	--	0xa229e89_1f7747e_b6ce495_101202e_020e264_4873cd6	0x09c7b3a7
0	607	0x010a87126cf41896	0xa229e89_1f7747e_b6ce495_101202e_020e264_4873cd6	--	--	0xa229e89_1f7747e_b6ce495_101202e_020e264_4873cd6	0x09c7b3a7
1	609	0x02150e24d9e8112c	0xbb4fcd4_65d2a21_9da18b8_f7c7444_ede2441_5fb7c54	--	--	0xbb4fcd4_65d0a21_9da18b8_f7c7444_ede2441_5fb7c54	0xe99f1ab9
2	613	0x042a1c49b3d02258	0xf88c179_8283a29_9e918a0_728f834_dd58f33_f612d38	--	--	0xf88c179_a0a380b_9e918a0_528f834_dd58f33_f612d38	0xe0c2bae1
…	…	…	…	…	…	…	…
53	817	0x0ddf7c3b6de5087d	0x7aa576c_d6954c2_025f54b_0597c54_4e0e339_50de5de	--	--	0x93032a8_7eff58c_cc0b9fd_767a3d9_1c24c82_240b8d8	0x7934d11a
54	821	0x0bbef876d3ca30fb	0xaaa16f1_994f7c7_416ec60_a50cafd_715cb28_eed01cd	--	--	0xc19b327_4186271_2b65083_596deb1_08d0625_2d7c6b9	0xacec5614
55	825	0x077df0eda79461f6	0x8384a84_eb31208_e891ec2_baef4bc_8682091_48cdf98	--	--	0x24a0a37_cee160d_6b5c2a6_b60bcca_8b01543_001faa2	0x4245f339
56	829	0x0efbe9db4f28e3ec	0x2e8ead4_111923a_e352ad2_82fae0c_ee8f19d_b8f923f	--	--	0x3cbdc43_32b8e7a_92772b0_4387711_51c0238_b79fbc6	0xca1df67d
57	833	0x0efbe9db4f28e3ec	0x2e8ead4_111923a_e352ad2_82fae0c_ee8f19d_b8f923f	--	--	0x899a862_d763610_0daaa5a_602aa33_755d00a_c74c9ad	0xe841bd65
58	837	0x0efbe9db4f28e3ec	0x2e8ead4_111923a_e352ad2_82fae0c_ee8f19d_b8f923f	--	--	0xcab52b0_aa02f0e_aa41b32_2dd31cb_4456835_13c2d55	0x4ce9f128
…	…	…	…	…	…	…	…
63	857	0x0efbe9db4f28e3ec	0x2e8ead4_111923a_e352ad2_82fae0c_ee8f19d_b8f923f	--	--	0x700fcce_a6ebaaf_bc73fae_3737c9c_fa39ed7_13cea02	0x4438a053
64	861	0x0efbe9db4f28e3ec	0x2e8ead4_111923a_e352ad2_82fae0c_ee8f19d_b8f923f	--	--	0x63ad196_1a4aaae_0a04b5e_d2bec56_d4200b9_9df191d	0x05f192f1
65	865	0x0efbe9db4f28e3ec	0x2e8ead4_111923a_e352ad2_82fae0c_ee8f19d_b8f923f	--	--	0x2e8ead4_111923a_e352ad2_82fae0c_ee8f19d_b8f923f	0x38f334b5
66	869	0x0df7d3b69651c7d9	0x7de7769_467ed69_42481d2_8a6a74d_0563f88_a0886b6	--	--	0x7de7769_467ed69_42481d2_8a6a74d_0563f88_a0886b6	0x4d15ca49
67	873	0x0befaf6d24a3afb3	0x1901f63_3db4f22_cd30662_1af51fb_f335afc_c547562	--	--	0x1901f63_3db4f22_cd30662_1af51fb_f335afc_c547562	0xa72b6f8f
…	…	…	…	…	…	…	…
146	1189	0x0d34123b6f78ee70	0x19d38b1_1ae4799_8d65e75_d9ccc48_b6413b9_0238e37	0x7f	0x7236	0x19d38b1_1ae4799_8d65e75_d9ccc48_b6413b9_0238e37	0x827f7236
147	1193	0x0a682476d6f1fce0	0x1647278_26c99c0_5ae364b_9cde46f_f994a55_7a19093	0xb4	0x229d	0x1647278_26c99c0_5ae364b_9cde46f_f994a55_7a19093	0x67b4229d
148	1197	0x04d048edade3d9c0	0x0c236d1_0c44b86_2c65940_294db46_d4f0bd4_9d4f143	0x22	0xd36f	0x0c236d1_0c44b86_2c65940_294db46_d4f0bd4_9d4f143	0x4922d36f
149	1201	0x09a091db5bc79380	0xbf7fdbb_1c49be1_0ed1f71_35196be_85e46dc_07a94c3	0xe8	0x026e	0xbf7fdbb_1c49be1_0ed1f71_35196be_85e46dc_07a94c3	0x03e8026e
150	1205	0x03412bb6b78f0700	0xafdeca3_c2817f6_0b25f01_ccdf10b_8966e0b_740a387	0xa5	0xd0b2	0xafdeca3_c2817f6_0b25f01_ccdf10b_8966e0b_740a387	0x37a5d0b2
151	1209	0x06825f6d671e2e00	0x3539b72_bc47849_3f4d63b_0e47996_d5468c8_c044629	0xcb	0x37de	0x3539b72_bc47849_3f4d63b_0e47996_d5468c8_c044629	0xa2cb37de

152	1213	0x0d04bedac63c7c01	0x70aa1ee_1916e53_9343318_005bd33_3b75a71_09bbf47	0xae	0xbe27	0x70aa1ee_1916e53_9343318_005bd33_3b75a71_09bbf47	0x2faebe27

Line rekey started

clk	Sym clk	LFSR[59:0]	BM0[167:0]	OF0[23:16]	OF0[15:0]	BM1[167:0]	OF1[31:0]
-3	--	0x03412bb6b78f0700	0xafdeca3_c2817f6_0b25f01_ccdf10b_8966e0b_740a387	--	--	0xafdeca3_c2817f6_0b25f01_ccdf10b_8966e0b_740a387	0x37a5d0b2
-2	--	0x06825f6d671e2e00	0x3539b72_bc47849_3f4d63b_0e47996_d5468c8_c044629	--	--	0x3539b72_bc47849_3f4d63b_0e47996_d5468c8_c044629	0xa2cb37de
-1	--	0x0d04bedac63c7c01	0x70aa1ee_1916e53_9343318_005bd33_3b75a71_09bbf47	--	--	0x70aa1ee_1916e53_9343318_005bd33_3b75a71_09bbf47	0x2faebe27
0	1214	0x0d04bedac63c7c01	0x70aa1ee_1916e53_9343318_005bd33_3b75a71_09bbf47	--	--	0x70aa1ee_1916e53_9343318_005bd33_3b75a71_09bbf47	0x2faebe27
1	1217	0x0a0975b58c78f802	0x6473668_6edbd72_18cde47_543cfc8_280f59c_4f0aa4f	--	--	0x6473668_6edbd72_18cde47_543cfc8_280f59c_4f0aa4f	0xec826407
2	1221	0x0412e36b18f1f005	0x4062b97_1fa7e73_56a1368_64e283c_50b7071_be7ea79	--	--	0x4062b97_1fa5e73_56a1368_64e283c_50b7071_be7ea79	0x08d9520f
3	1225	0x0825ced639e3e00b	0x187657d_1bae281_577b323_27b87e3_dff8031_77f6960	--	--	0x187657d_398e0a3_577b323_07b87e3_dff8031_77f6960	0x9229ca33
…	…	…	…	…	…	…	…
54	1429	0x02dd72ef0ad2ab2a	0x015e056_3d174cb_61f12f7_ceaec6b_ea36d88_4f78f49	--	--	0x427e9c7_f5e2cf2_b4bb979_2abdc06_af382c9_df34c0b	0x9358df33
55	1433	0x05baedde15a55655	0x6dd23f9_77a2cfe_a1509e3_6dd7565_844a532_efdedf3	--	--	0x10eafbc_28d649e_523d073_a6e6130_773879d_7aa0d48	0x59933d4f
56	1437	0x0b75d3bc234a8cab	0xed6c213_29d6a1b_bfa1457_27122de_3583f4c_ac0485b	--	--	0x1807382_897ae40_0577723_e4bed34_14fa1a3_b651616	0x60f868f0
57	1441	0x0b75d3bc234a8cab	0xed6c213_29d6a1b_bfa1457_27122de_3583f4c_ac0485b	--	--	0xde91fea_e662530_3fff72a_0f4b685_9fc8293_def8cbd	0x5ea82a7f
58	1445	0x0b75d3bc234a8cab	0xed6c213_29d6a1b_bfa1457_27122de_3583f4c_ac0485b	--	--	0x709e987_2482dfc_ee4c8fd_f1fc2b0_bbc2710_81cd189	0x648c61e4
…	…	…	…	…	…	…	…
63	1465	0x0b75d3bc234a8cab	0xed6c213_29d6a1b_bfa1457_27122de_3583f4c_ac0485b	--	--	0x65ae8b7_960a7cc_e0b3217_819f988_147cfcb_c90de71	0x4d425756
64	1469	0x0b75d3bc234a8cab	0xed6c213_29d6a1b_bfa1457_27122de_3583f4c_ac0485b	--	--	0xa212ff3_af64926_1cef2d6_3793d49_1dce673_6ec6f5f	0x78b3b2b0
65	1473	0x0b75d3bc234a8cab	0xed6c213_29d6a1b_bfa1457_27122de_3583f4c_ac0485b	--	--	0xed6c213_29d6a1b_bfa1457_27122de_3583f4c_ac0485b	0x1a9f10bf
66	1477	0x06eba77846951957	0xdb2be4a_e6d5c6c_fd3b272_53119bb_e360e8e_e20d6ec	--	--	0xdb2be4a_e6d5c6c_fd3b272_53119bb_e360e8e_e20d6ec	0x10450485
…	…	…	…	…	…	…	…
149	1809	0x03d7a5bff04e9cb4	0x8edb847_8675f37_836ad25_46cbd6f_071cd46_2d7238d	0xc5	0x8401	0x8edb847_8675f37_836ad25_46cbd6f_071cd46_2d7238d	0x2dc58401
150	1813	0x07af437fe09d3969	0x303b450_962052f_068a297_586af27_1c8588c_2134010	0x1a	0x5769	0x303b450_962052f_068a297_586af27_1c8588c_2134010	0x471a5769
151	1817	0x0f5e86ffc93a52d2	0x661e31f_da4e8d8_26b1a6c_92884a0_e7ace26_278a053	0xfc	0xf86d	0x661e31f_da4e8d8_26b1a6c_92884a0_e7ace26_278a053	0x3ffcf86d

152	1821	0x0ebd0dff9274a5a4	0x678bd2e_7f114df_7937fa5_98a1699_6dfe262_931dede	0xb2	0x77e8	0x678bd2e_7f114df_7937fa5_98a1699_6dfe262_931dede	0xa1b277e8
Line rekey started							
clk	**Sym clk**	**LFSR[59:0]**	**BM0[167:0]**	**OF0[23:16]**	**OF0[15:0]**	**BM1[167:0]**	**OF1[31:0]**
-3	--	0x07af437fe09d3969	0x303b450_962052f_068a297_586af27_1c8588c_2134010	--	--	0x303b450_962052f_068a297_586af27_1c8588c_2134010	0x471a5769
-2	--	0x0f5e86ffc93a52d2	0x661e31f_da4e8d8_26b1a6c_92884a0_e7ace26_278a053	--	--	0x661e31f_da4e8d8_26b1a6c_92884a0_e7ace26_278a053	0x3ffcf86d
-1	--	0x0ebd0dff9274a5a4	0x678bd2e_7f114df_7937fa5_98a1699_6dfe262_931dede	--	--	0x678bd2e_7f114df_7937fa5_98a1699_6dfe262_931dede	0xa1b277e8
0	1821	0x0ebd0dff9274a5a4	0x678bd2e_7f114df_7937fa5_98a1699_6dfe262_931dede	--	--	0x678bd2e_7f114df_7937fa5_98a1699_6dfe262_931dede	0xa1b277e8
1	1825	0x0d7a1bff2ce94b48	0x961d456_ba4e844_4822f7d_c115bb4_b9a7cd0_d1f0b4a	--	--	0x961d456_ba4c844_4822f7d_c115bb4_b9a7cd0_d1f0b4a	0x20ad5acd
2	1829	0x0af437fe51d2b691	0x6b7b5af_f6f9e49_94dd872_671a42d_f71b647_a76f725	--	--	0x6b7b5af_d4d9c6b_94dd872_471a42d_f71b647_a76f725	0x5ac6af2c
3	1833	0x05e86ffcaba54d23	0xabd0450_6ee980e_50ab2ee_ae14835_ab3757c_89fc114	--	--	0x453ea5e_d74a3b5_50ab2ee_af90a2d_ab3757c_89bc914	0x89e574b6
…	…	…	…	…	…	…	…
52	2029	0x014d6a7fe218fcab	0x2f8ccdb_bf14967_c12b253_7ef7195_137e17f_7cef7ab	--	--	0x95aa32d_c583b9f_7a25930_74ad1ce_6ba43aa_7a1fb46	0xe2393209
53	2033	0x029ad4ffcc31f956	0x8294c57_4b513c0_c76e41f_108530e_8fbf75f_7f420fa	--	--	0x0d9ac04_f284d0f_375d7a0_95c0d30_174b66d_c276479	0xa51654b0
54	2037	0x0535a1ff9863d2ad	0x93cc2ce_bff777d_f01c5c9_aa605a3_368cb36_5aa0ed3	--	--	0xfc35737_2fb1d79_724af5e_5867aad_56dad9b_9717e0e	0x73b00e9d
55	2041	0x0a6b43ff30c7855b	0x5dda3ba_f850ba4_6330bd2_51471de_0f381a3_f9b5cdb	--	--	0xd54a82b_a40d79c_e5b982c_ee4f848_1de227f_21275fa	0xd7b89c7f
56	2045	0x04d68ffe618f0ab7	0x5fc9fcf_0f481b9_28e7945_1ec42cc_db8cf36_d2b5473	--	--	0x9270c19_8d62e20_0fbc0b6_d45108f_566a782_cb9b568	0x8b6eb18c
57	2049	0x04d68ffe618f0ab7	0x5fc9fcf_0f481b9_28e7945_1ec42cc_db8cf36_d2b5473	--	--	0xe9929da_9311d50_83706a7_993039f_26fa43c_d9f9464	0x6ae57838
58	2053	0x04d68ffe618f0ab7	0x5fc9fcf_0f481b9_28e7945_1ec42cc_db8cf36_d2b5473	--	--	0xa9a2bf5_953d012_dcec733_4481a53_de7f357_c173c2e	0x2a2993ef
…	…	…	…	…	…	…	…
63	2073	0x04d68ffe618f0ab7	0x5fc9fcf_0f481b9_28e7945_1ec42cc_db8cf36_d2b5473	--	--	0xd7cf516_da7fd8d_5922a88_ee95b88_e3a21ef_b68f62d	0xf69dce11
64	2077	0x04d68ffe618f0ab7	0x5fc9fcf_0f481b9_28e7945_1ec42cc_db8cf36_d2b5473	--	--	0x1f1cb7b_3ef0296_7945b04_230cc02_2575564_ed00c6f	0x73e6b534
65	2081	0x04d68ffe618f0ab7	0x5fc9fcf_0f481b9_28e7945_1ec42cc_db8cf36_d2b5473	--	--	0x5fc9fcf_0f481b9_28e7945_1ec42cc_db8cf36_d2b5473	0x67d0529a
66	2085	0x09ad1ffccb1e156f	0xd979a98_acc905e_c103198_f3d4b0d_4bfc68e_94e2561	--	--	0xd979a98_acc905e_c103198_f3d4b0d_4bfc68e_94e2561	0xbdf01ae1
…	…	…	…	…	…	…	…
149	2417	0x0f2e686921141790	0x75e2cc2_263ef54_12f4007_a8c7ce0_0862671_45f2381	0x96	0x9bbd	0x75e2cc2_263ef54_12f4007_a8c7ce0_0862671_45f2381	0x4b969bbd

150	2421	0x0e5cd8d24a282f20	0xddfd82e_9435151_e9f407d_a34bc54_a807337_8b9716b	0x22	0xe8c2	0xddfd82e_9435151_e9f407d_a34bc54_a807337_8b9716b	0x3422e8c2
151	2425	0x0cb9b9a494507e40	0x8731da3_ae8f262_d50a6f7_2e8af8f_162834d_a0db88a	0x2c	0xc686	0x8731da3_ae8f262_d50a6f7_2e8af8f_162834d_a0db88a	0x492cc686

Line rekey started

clk	Sym clk	LFSR[59:0]	BM0[167:0]	OF0[23:16]	OF0[15:0]	BM1[167:0]	OF1[31:0]
-3	--	0x0f2e686921141790	0x75e2cc2_263ef54_12f4007_a8c7ce0_0862671_45f2381	--	--	0x75e2cc2_263ef54_12f4007_a8c7ce0_0862671_45f2381	0x4b969bbd
-2	--	0x0e5cd8d24a282f20	0xddfd82e_9435151_e9f407d_a34bc54_a807337_8b9716b	--	--	0xddfd82e_9435151_e9f407d_a34bc54_a807337_8b9716b	0x3422e8c2
-1	--	0x0cb9b9a494507e40	0x8731da3_ae8f262_d50a6f7_2e8af8f_162834d_a0db88a	--	--	0x8731da3_ae8f262_d50a6f7_2e8af8f_162834d_a0db88a	0x492cc686
0	2428	0x0cb9b9a494507e40	0x8731da3_ae8f262_d50a6f7_2e8af8f_162834d_a0db88a	--	--	0x8731da3_ae8f262_d50a6f7_2e8af8f_162834d_a0db88a	0x492cc686
1	2429	0x09737b4920a0dc80	0x4f1a195_203e725_a55bed4_3fa962c_363cd1e_21a68e1	--	--	0x4f1a195_203e725_a55bed4_3fa962c_363cd1e_21a68e1	0xc1c3f9a5
2	2433	0x02e6f6924141b900	0xfd2fe5d_ad23585_444bbf4_bbbfa17_3e813d6_10eb1b8	--	--	0xfd2fe5d_ad23585_444bbf4_bbbfa17_3e813d6_10eb1b8	0xac7bf9bc
3	2437	0x05cded248a835200	0xa3f6f0e_27e1d17_8068512_f2a0c7a_d8a1348_52d69dd	--	--	0xa3f6f0e_27e3d17_8068512_f2a0c7a_d8a1348_52d69dd	0xf9b28698
…	…	…	…	…	…	…	…
53	2637	0x009902720f55c8a2	0xcb3d921_b529c95_93a9b97_1e329a3_f572434_8f4a029	--	--	0xaad31bb_bee9df1_bc82fbb_4895fd7_12e81d5_52becda	0xd7727bff
54	2641	0x013204e41eab9144	0x467c1f9_2bc3593_fde7bf3_7e4c4d7_3093f37_71cfbdb	--	--	0x9c66f60_977c8ae_fcab7d2_bdef8b1_bedef54_e0560ee	0x5d776d85
55	2645	0x026409c83d570288	0x1ee73c4_8c7937d_27def6d_3934df5_3c8ac46_be5a7fe	--	--	0x9561fe7_92cbe0e_4cb229b_bf95573_49e8c09_38df9e8	0xbd905de0
56	2649	0x04c813907aae0510	0x56b8276_705aa09_36808da_d2c6e3d_d4490c2_4dcd9d0	--	--	0xe295cb7_5ccf4d8_0739259_b2dd86d_f77c182_328d7ab	0xe7f4a0ae
57	2653	0x04c813907aae0510	0x56b8276_705aa09_36808da_d2c6e3d_d4490c2_4dcd9d0	--	--	0x4613a4d_00e6788_d35c539_9558c93_c89cb9f_1bbf4a7	0x760add56
58	2657	0x04c813907aae0510	0x56b8276_705aa09_36808da_d2c6e3d_d4490c2_4dcd9d0	--	--	0x6d75447_73bdb2d_3e70fd5_450fd53_85f3e47_dd0bf2e	0xf87efda7
59	2661	0x04c813907aae0510	0x56b8276_705aa09_36808da_d2c6e3d_d4490c2_4dcd9d0	--	--	0x4096dab_0f0b9bb_8102604_ae08eb5_c551bfa_e0d526d	0x4a1e9198
…	…	…	…	…	…	…	…
150	3025	0x0a16bf62cd31bc9a	0x0e7bcb2_eb234f9_3d1d6cf_29b1c26_5f074c7_8ed335c	0x6b	0x5134	0x0e7bcb2_eb234f9_3d1d6cf_29b1c26_5f074c7_8ed335c	0xbd6b5134
151	3029	0x042d7ec59a635935	0x17dc8e4_02e774b_0f4f683_776adcf_895d394_3ea7c28	0xe5	0xb11e	0x17dc8e4_02e774b_0f4f683_776adcf_895d394_3ea7c28	0x24e5b11e
152	3033	0x085afd8b3cc6926b	0x6024417_9d066de_933b5ba_77ee47f_c9a4e2a_90340e9	0xd8	0xefcd	0x6024417_9d066de_933b5ba_77ee47f_c9a4e2a_90340e9	0xc1d8efcd

Frame key calc started

clk	Sym clk	LFSR[59:0]	BM0[167:0]	OF0[23:16]	OF0[15:0]	BM1[167:0]	OF1[31:0]
-3	--	--		--	--		0xbd6b5134

			0x0e7bcb2_eb234f9_3d1d6cf_29b1c26_5f074c7_8ed335c			0x0e7bcb2_eb234f9_3d1d6cf_29b1c26_5f074c7_8ed335c	
-2	--	--	0x17dc8e4_02e774b_0f4f683_776adcf_895d394_3ea7c28	--	--	0x17dc8e4_02e774b_0f4f683_776adcf_895d394_3ea7c28	0x24e5b11e
-1	--	--	0x6024417_9d066de_933b5ba_77ee47f_c9a4e2a_90340e9	--	--	0x6024417_9d066de_933b5ba_77ee47f_c9a4e2a_90340e9	0xc1d8efcd
0	3035	--	0x6024417_9d066de_933b5ba_77ee47f_c9a4e2a_90340e9	--	--	0x6024417_9d066de_933b5ba_77ee47f_c9a4e2a_90340e9	0xc1d8efcd
1	3036	--	0xc040e35_54294b7_0000000_7a3b0f9_42b1dbd_000006a	--	--	0x8b95c94_67980f9_e80bf24_3dd8f7f_8212841_f6fc1fb	0xfbce91d1
2	3040	--	0x6666a4e_47b5444_93d46aa_e4f374f_3cd0333_212d6ab	--	--	0x850a54e_9bfeeaf_b3826ce_320e2fe_7f72bae_3351845	0xeeede7a0
3	3044	--	0x1232d67_ef6a7a5_6055678_d509b9f_427d387_e30af77	--	--	0x208d15c_5e8e452_aa6072c_909c7c7_2d7880a_79a1701	0xd38ba7b2
4	3048	--	0x811566c_da14697_66f89db_84306fe_411d172_f9e3620	--	--	0x1496c59_3387aa1_3da2fc7_cd41184_b3a9829_158eebe	0x26090ed0
5	3052	--	0xf7027a4_dc24164_29716cf_f0cd06e_9fad21f_41cbe85	--	--	0xe80cf33_d794c6a_641034c_fd4aa6a_4e47123_cdf36a7	0x9118f55e

Table B-42. Cipher State in SST mode for 1-lane, Inter-BS Spacing = 607

clk	stream	cipher	enc stream
-3	0x1c	0x6559c03e	0x1c
-2	0x3c	0x6559c03e	0x3c
-1	0x3c	0x6559c03e	0x3c
0	0x1c	0x6559c03e	0x1c
1	0x39	0xb79ee5fe	0xc7
2	0x00	0xb79ee5fe	0xe5
3	0x00	0xb79ee5fe	0x9e
4	0x39	0xb79ee5fe	0x8e
5	0x00	0x289af919	0x19
6	0x00	0x289af919	0xf9
7	0x39	0x289af919	0xa3
8	0x00	0x289af919	0x28
9	0x00	0xd25b5d6c	0x6c
10	0x39	0xd25b5d6c	0x64
11	0x00	0xd25b5d6c	0x5b
12	0x00	0xd25b5d6c	0xd2
13	0x00	0xed55dcde	0xde
…	…	…	…
177	0x00	0x10f21d66	0x66
178	0x00	0x10f21d66	0x1d
179	0x00	0x10f21d66	0xf2
180	0x00	0x10f21d66	0x10
181	0x00	0x37affe86	0x86
182	0x00	0x37affe86	0xfe
183	0x00	0x37affe86	0xaf
184	0x00	0x37affe86	0x37
185	0x00	0x49152bc4	0xc4
186	0x00	0x49152bc4	0x2b
187	0x00	0x49152bc4	0x15
188	0x00	0x49152bc4	0x49
189	0x00	0x1f068148	0x48
190	0x00	0x1f068148	0x81
191	0x00	0x1f068148	0x06
192	0x00	0x1f068148	0x1f
193	0x00	0xb79cb954	0x54
194	0x00	0xb79cb954	0xb9
195	0x00	0xb79cb954	0x9c
196	0x00	0xb79cb954	0xb7
197	0x00	0xfe492f2a	0x2a
198	0x00	0xfe492f2a	0x2f
199	0x00	0xfe492f2a	0x49
200	0x00	0xfe492f2a	0xfe

201	0x00	0x53331e18	0x18
202	0x00	0x53331e18	0x1e
203	0x00	0x53331e18	0x33
204	0x00	0x53331e18	0x53
205	0x00	0x5c0e4039	0x39
206	0x00	0x5c0e4039	0x40
207	0x00	0x5c0e4039	0x0e
208	0x00	0x5c0e4039	0x5c
209	0x00	0x4a040224	0x24
…	…	…	…
401	0x00	0x96fc2396	0x96
402	0x00	0x96fc2396	0x23
403	0x00	0x96fc2396	0xfc
404	0x00	0x96fc2396	0x96
405	0x00	0xbc51d239	0x39
406	0x00	0xbc51d239	0xd2
407	0x00	0xbc51d239	0x51
408	0x00	0xbc51d239	0xbc
409	0x00	0x8908e8ac	0xac
410	0x00	0x8908e8ac	0xe8
411	0x00	0x8908e8ac	0x08
412	0x00	0x8908e8ac	0x89
413	0x00	0x1d74baa3	0xa3
414	0x00	0x1d74baa3	0xba
415	0x00	0x1d74baa3	0x74
416	0x00	0x1d74baa3	0x1d
417	0x00	0xd8835587	0x87
418	0x00	0xd8835587	0x55
419	0x00	0xd8835587	0x83
420	0x00	0xd8835587	0xd8
421	0x00	0xaf70715f	0x5f
422	0x00	0xaf70715f	0x71
423	0x00	0xaf70715f	0x70
424	0x00	0xaf70715f	0xaf
425	0x00	0xc861665f	0x5f
426	0x00	0xc861665f	0x66
427	0x00	0xc861665f	0x61
428	0x00	0xc861665f	0xc8
429	0x00	0x2bbcf09a	0x9a
…	…	…	…
497	0x00	0xee629a59	0x59
498	0x00	0xee629a59	0x9a
499	0x00	0xee629a59	0x62
500	0x00	0xee629a59	0xee

501	0x00	0x0d25408d	0x8d
502	0x00	0x0d25408d	0x40
503	0x00	0x0d25408d	0x25
504	0x00	0x0d25408d	0x0d
505	0x00	0xc07ece76	0x76
506	0x00	0xc07ece76	0xce
507	0x00	0xc07ece76	0x7e
508	0x00	0xc07ece76	0xc0
509	0x00	0xedf08af9	0xf9
510	0x00	0xedf08af9	0x8a
511	0x00	0xedf08af9	0xf0
512	0x00	0xedf08af9	0xed
513	0x00	0xb86284bb	0xbb
514	0x00	0xb86284bb	0x84
515	0x00	0xb86284bb	0x62
516	0x00	0xb86284bb	0xb8
517	0x00	0xb87439a6	0xa6
518	0x00	0xb87439a6	0x39
519	0x00	0xb87439a6	0x74
520	0x00	0xb87439a6	0xb8
521	0x00	0xf701f1ed	0xed
…	…	…	…
601	0x00	0x7a6e587b	0x7b
602	0x00	0x7a6e587b	0x58
603	0x00	0x7a6e587b	0x6e
604	0xbc	0x7a6e587b	0xbc
605	0x3c	0x09c7b3a7	0x3c
606	0x3c	0x09c7b3a7	0x3c
607	0xbc	0x09c7b3a7	0xbc
608	0x39	0x09c7b3a7	0x30
609	0x00	0xe99f1ab9	0xb9

Table B-43. 1-lane Encrypted Output in SST mode for Inter-BS Spacing = 607

Appendix C. Confidentiality and Integrity of Values

Table C-1 identifies the requirements of confidentiality and integrity for values within the protocol. A *confidential* value must never be revealed. The *integrity* of many values in the system is protected by fail-safe mechanisms of the protocol. Values that are not protected in this manner require active measures beyond the protocol to ensure integrity. Such values are noted in Table C-1 as requiring integrity.

Value	Size (Bytes)	Confidentiality Required[†]?	Integrity Required[†]?	Function
Aksv	5	No	No	HDCP Transmitter's Key Selection Vector
An	8	No	Yes[*]	Pseudo-random value sent to HDCP Receiver/Repeater by transmitter
Bksv	5	No	Yes[*]	HDCP Receiver/repeater's Key Selection Vector
Bx,By,Bz	84 bits	Yes	Yes	Cipher state
Km,Km'	7	Yes	Yes	Secret value generated by HDCP Transmitter and receiver/repeater during authentication
Ks,Ks'	84 bits	Yes	Yes	Secret session key
K_i, K_i'	84 bits	Yes	Yes	Secret frame key
Akeys[**]	280	Yes	Yes	HDCP Transmitter's device keys
Bkeys[**]	280	Yes	Yes	HDCP Receiver/repeater's device keys
LFSR0,1,2,3	13,14,16, 17 bits	Yes	Yes	Cipher state
M_i, M_i'	8	Yes	Yes	Integrity verification key and HDCP cipher initialization value
R_0, R_0'	2	No	No	Value generated at the transmitter and receiver that indicates the success of the authentication exchange
SH-0,1,2,3	2,2,2,2 bits	Yes	Yes	Cipher state
REPEATER	1 bit	No	Yes	Repeater capability status bit
MAX_CASCADE_EXCEEDED	1 bit	No	Yes	Repeater topology error status bit
MAX_DEVS_EXCEEDED	1 bit	No	Yes	Repeater topology error status bit
DEVICE_COUNT	7 bits	No	Yes	Repeater topology status bit
DEPTH	3 bits	No	Yes	Repeater topology status bit
V'	20	No	No	KSV list integrity value generated by repeater

[†] According to the robustness rules in the HDCP Adopter's License.
[*] Only within the transmitter
[**] KSV position excluded (see *Aksv*, *Bksv*)

V	20	Yes	Yes	KSV list integrity verification value generated by transmitter
KSV List	Varies	No	Yes	List of downstream KSV gathered by repeater devices
Kx, Ky, Kz	84 bits	Yes	Yes	Internal HDCP cipher values
L[1]	128	No	Yes	Digital Content Protection LLC DSS Public Key

Table C-1. Confidentiality and Integrity of Values

Appendix D. Transmission of IDLE Pattern in SST Mode

In the SST mode, the HDCP Devices must keep encryption enabled during the transmission of IDLE pattern. Figure D-1 depicts the transmission of the LINK_VERIFICATION_PATTERN during transition from active video streams to IDLE pattern. The same approach applies to transition from IDLE pattern to active video streams.

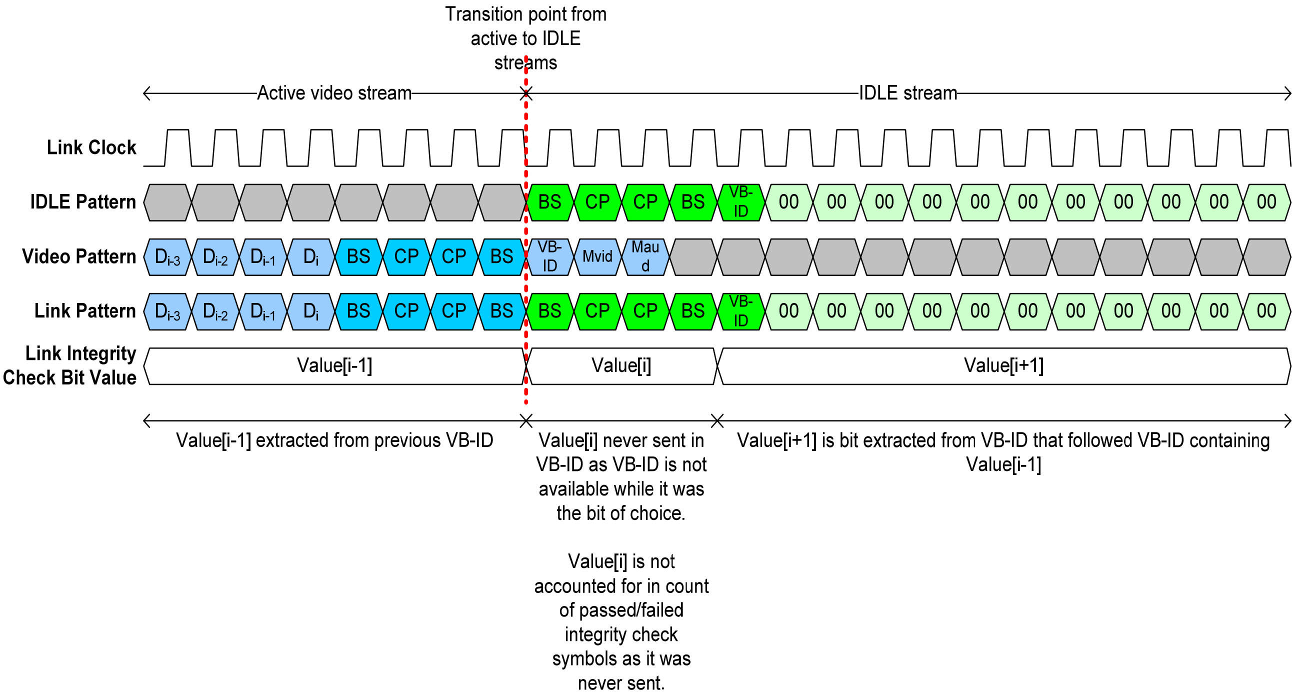
Transition point from active to IDLE streams
Active video stream
IDLE stream
Link Clock
IDLE Pattern
BS
CP
CP
BS
VB-ID
00
Video Pattern
D_{i-3}
D_{i-2}
D_{i-1}
D_i
Mvid
Maud
Link Pattern
Link Integrity Check Bit Value
Value[i-1]
Value[i]
Value[i+1]
Value[i-1] extracted from previous VB-ID
Value[i] never sent in VB-ID as VB-ID is not available while it was the bit of choice.
Value[i] is not accounted for in count of passed/failed integrity check symbols as it was never sent.
Value[i+1] is bit extracted from VB-ID that followed VB-ID containing Value[i-1]

Figure D-1. Transmission of LINK_VERIFICATION_PATTERN during transition from active to IDLE streams

As illustrated in Figure D-1, during transition from active streams to IDLE pattern, VB-ID, Mvid and Maud may not be transmitted following CPBS/CPSR. In such cases, the bit position of the LINK_VERIFICATION_PATTERN is advanced but the corresponding bit is not transmitted as there is no VB-ID available.

Appendix E. Timing Diagrams in SST Mode

Figure E-1 and Figure E-2 depict the frame key calculation timing for a 2-lane configuration in which the HDCP cipher clock is running at LS_CLK/2, which results in two possible relative phases between the end of the enhanced CPSR symbol and the HDCP cipher clock. Figure E-3, Figure E-4, Figure E-5 and Figure E-6 depict the frame key calculation timing for a 1-lane configuration in which the HDCP cipher clock is running at LS_CLK/4, which results in four possible relative phases between the end of the enhanced CPSR symbol and the HDCP cipher clock.

Figure E-7 and Figure E-8 depict the 2-Lane line re-key timing diagrams for the two possible relative phases. Figure E-9, Figure E-10, Figure E-11 and Figure E-12 depict 1-Lane line re-key timing diagrams for the four possible relative phases.

Figure E-13, Figure E-14 and Figure E-15 depict the initial frame key calculation timing for 1-lane, 2-lane and 4-lane configurations respectively. In this situation both BM0 and BM1 are initially stalled after completing the initial authentication bootstrap operation.

Figure E-16, Figure E-17, Figure E-18, Figure E-19, Figure E-20 and Figure E-21 depict various collisions that occur, i.e. a CPBS arrives during frame key calculation, a CPSR arrives during line re-key etc, in a 4-Lane Main-Link Configuration and how they are handled.

Note: The states X_i, X_{i+1} etc in the timing diagrams indicate the BM0 and BM1 register states at the beginning of a particular cycle and are directly used to generate the corresponding encrypted output at each cycle.

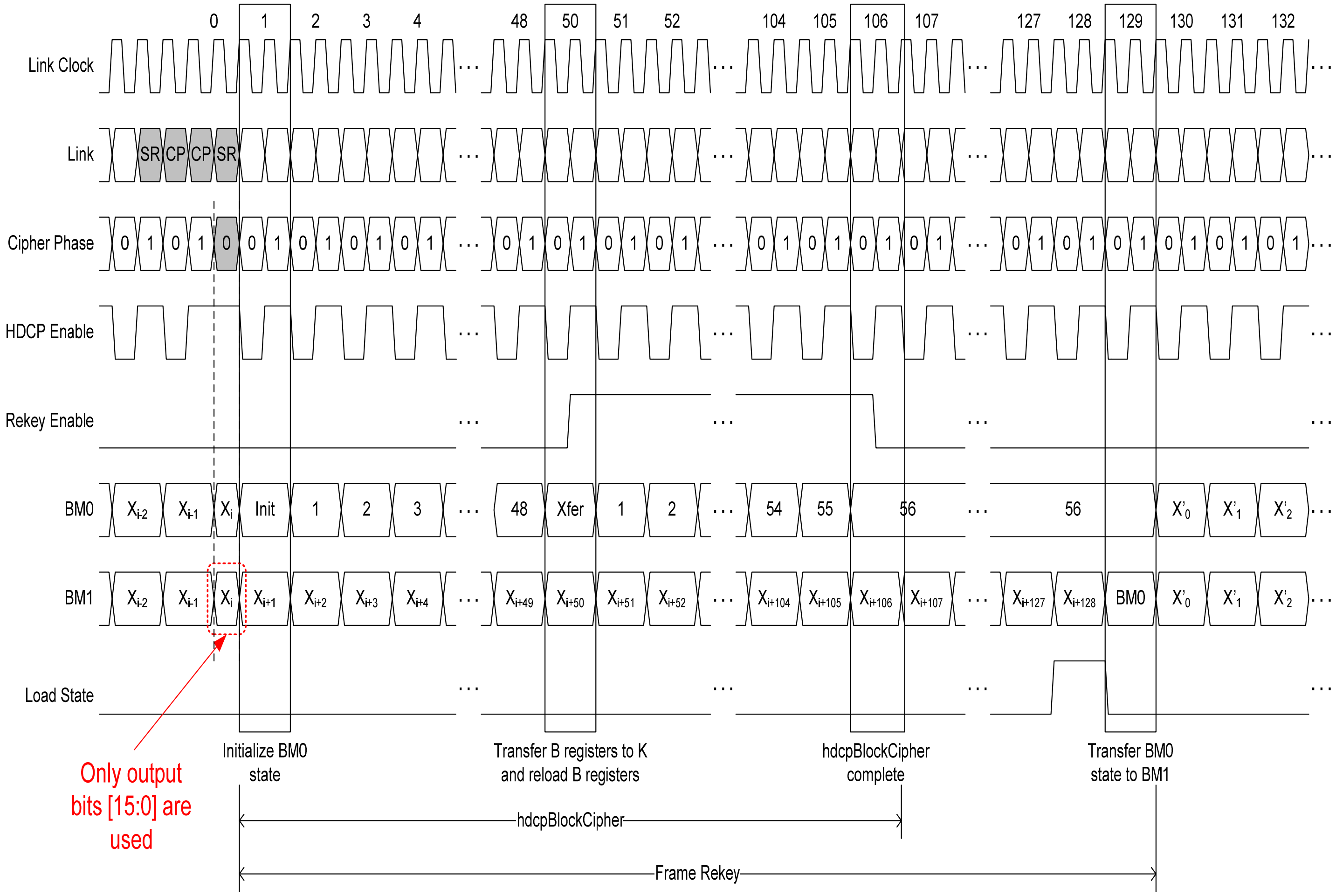

Figure E-1. 2-Lane Frame Key Calculation Timing Diagram (Phase 0)

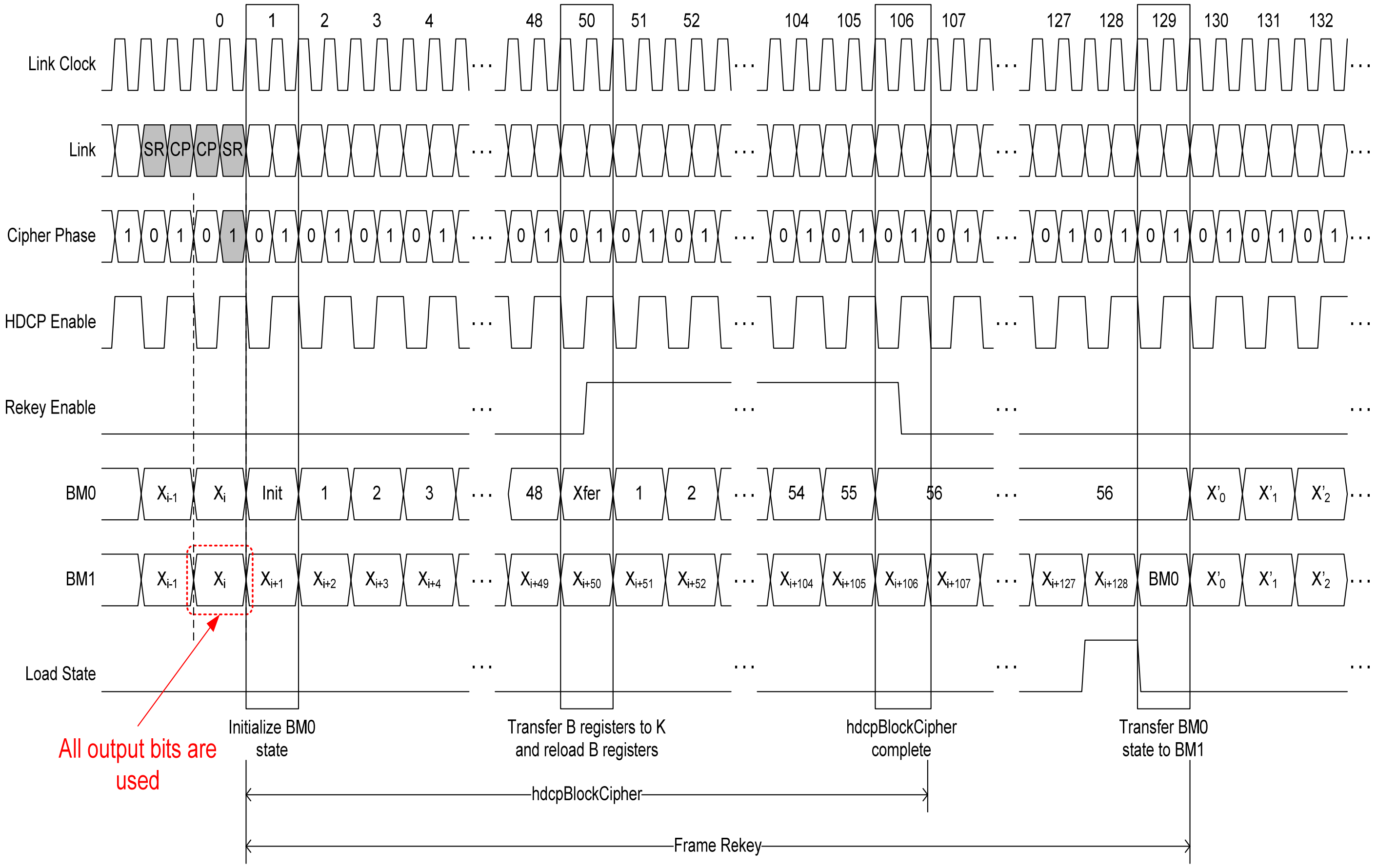

Figure E-2. 2-Lane Frame Key Calculation Timing Diagram (Phase 1)

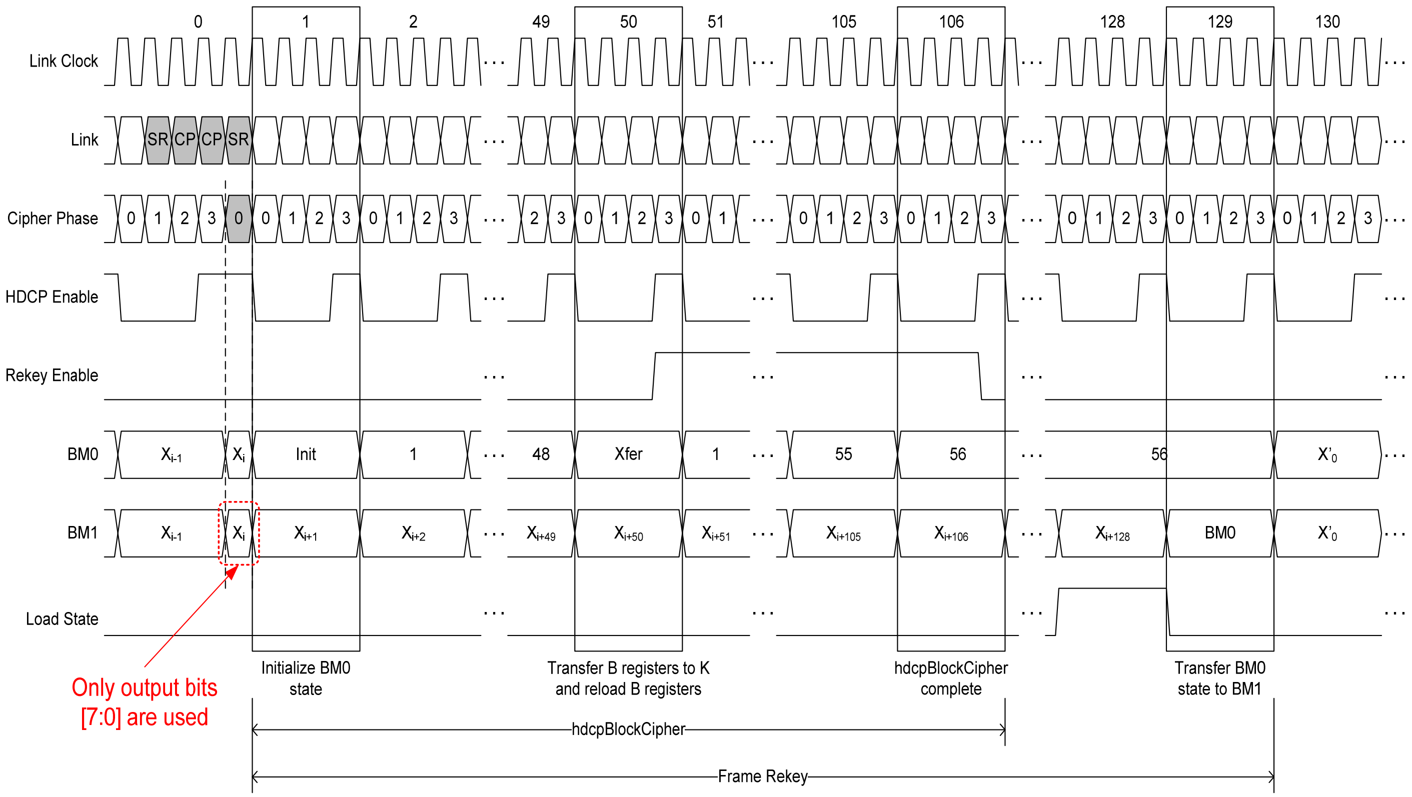

Figure E-3. 1-Lane Frame Key Calculation Timing Diagram (Phase 0)

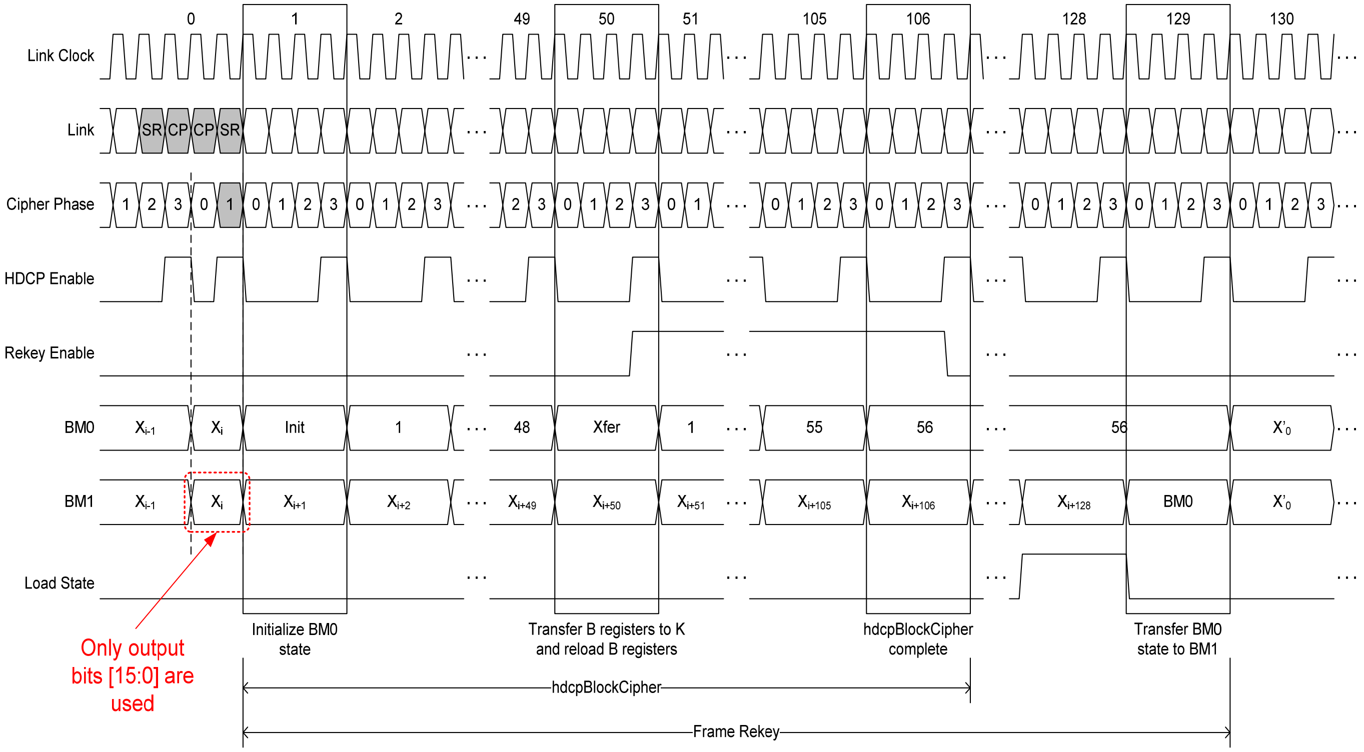

Figure E-4. 1-Lane Frame Key Calculation Timing Diagram (Phase 1)

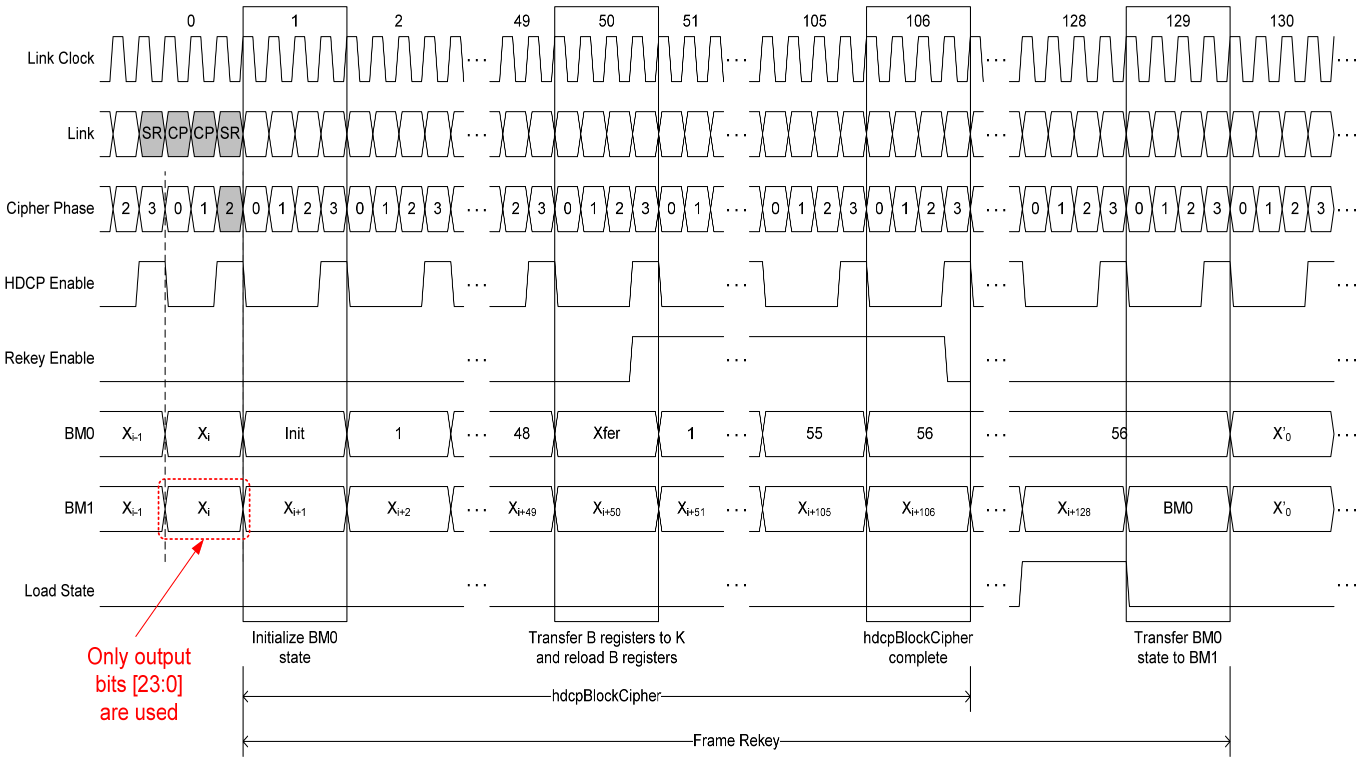

Figure E-5. 1-Lane Frame Key Calculation Timing Diagram (Phase 2)

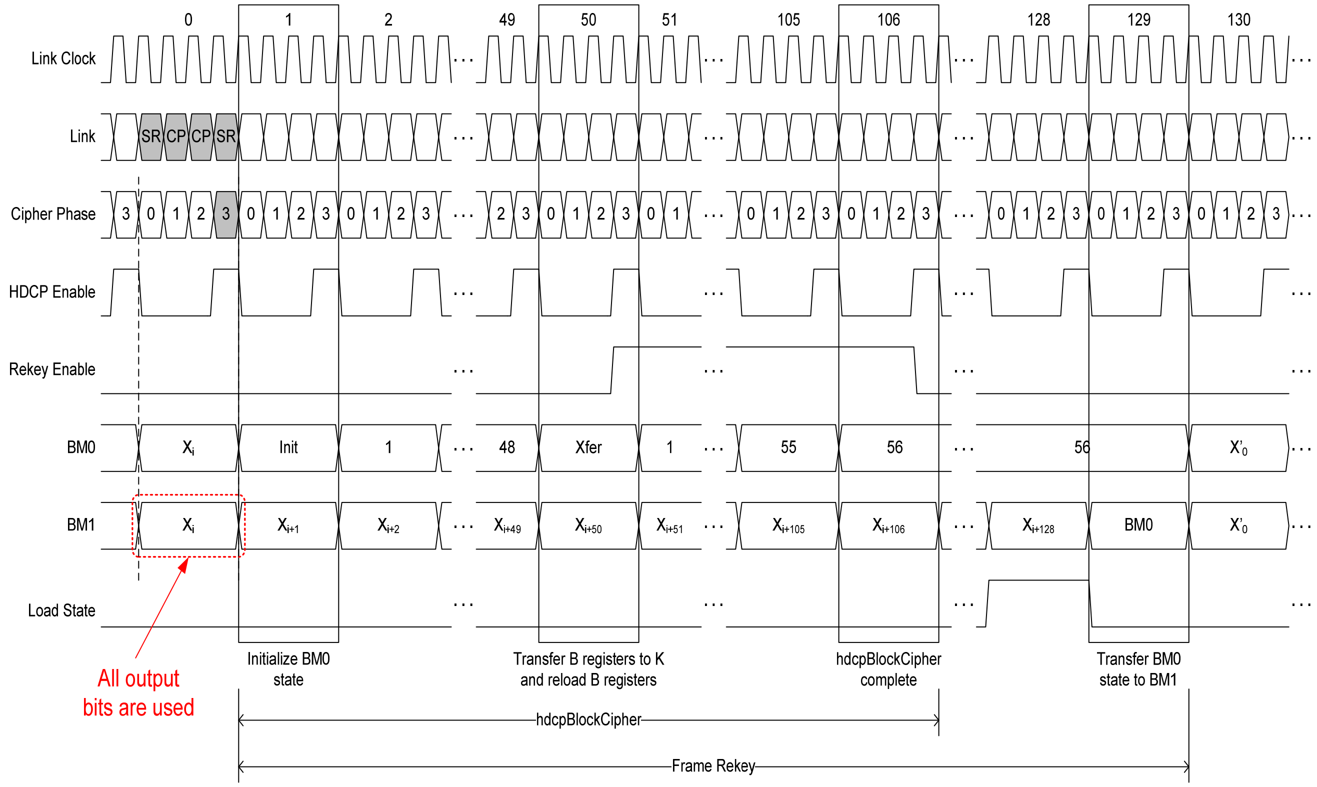

Figure E-6. 1-Lane Frame Key Calculation Timing Diagram (Phase 3)

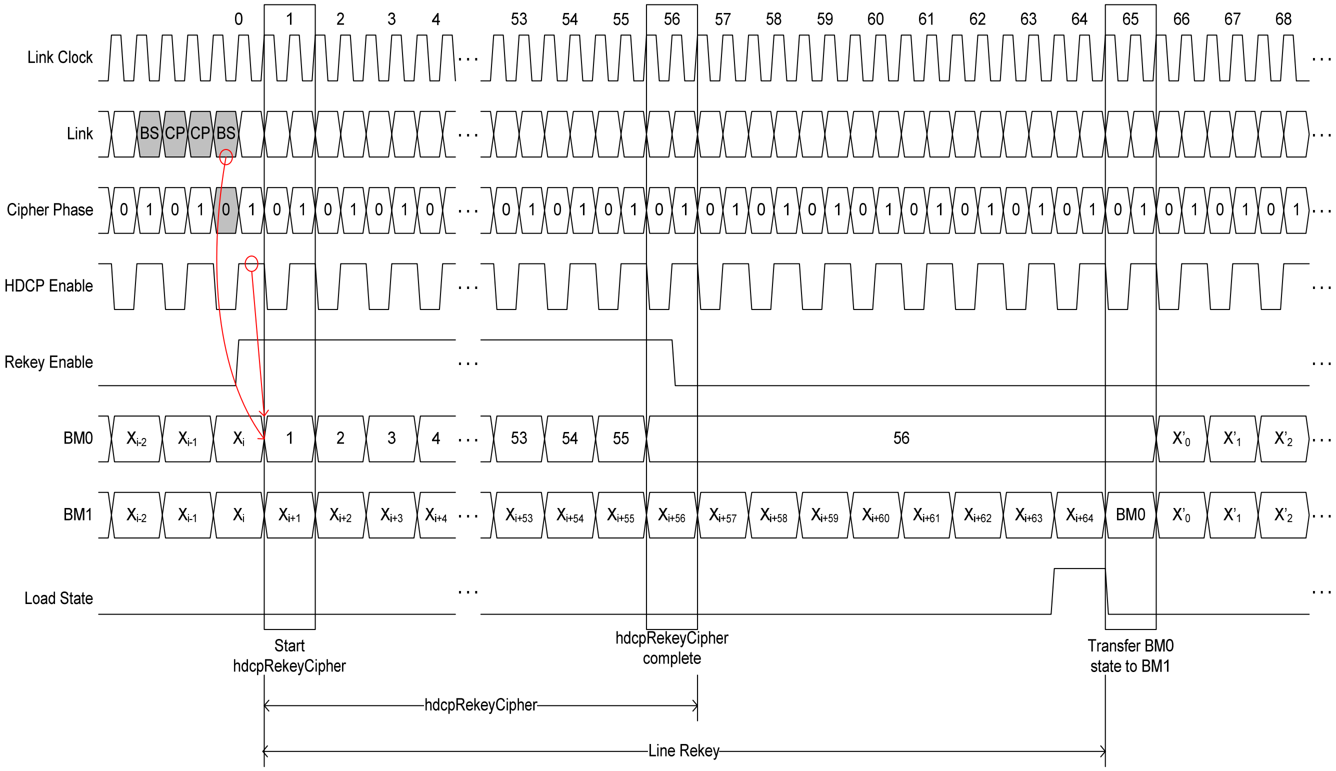

Figure E-7. 2-Lane Line Re-Key Calculation Timing Diagram (Phase 0)

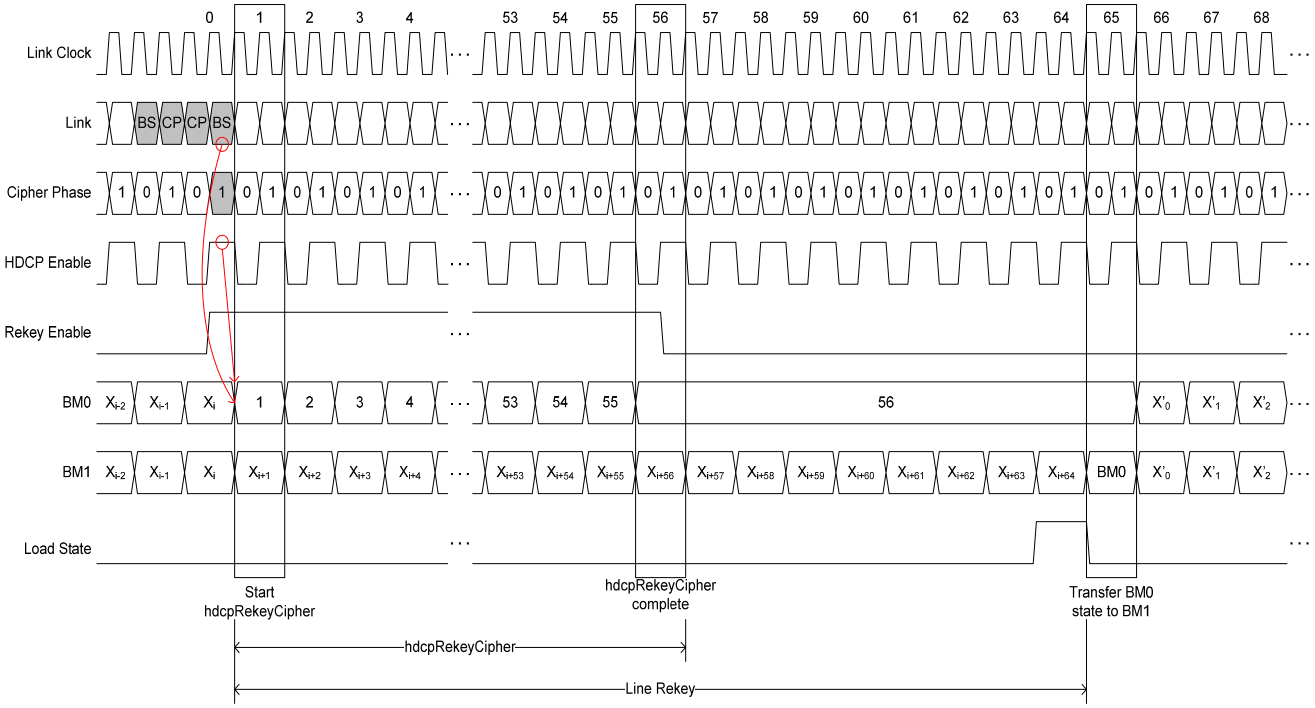

Figure E-8. 2-Lane Line Re-Key Calculation Timing Diagram (Phase 1)

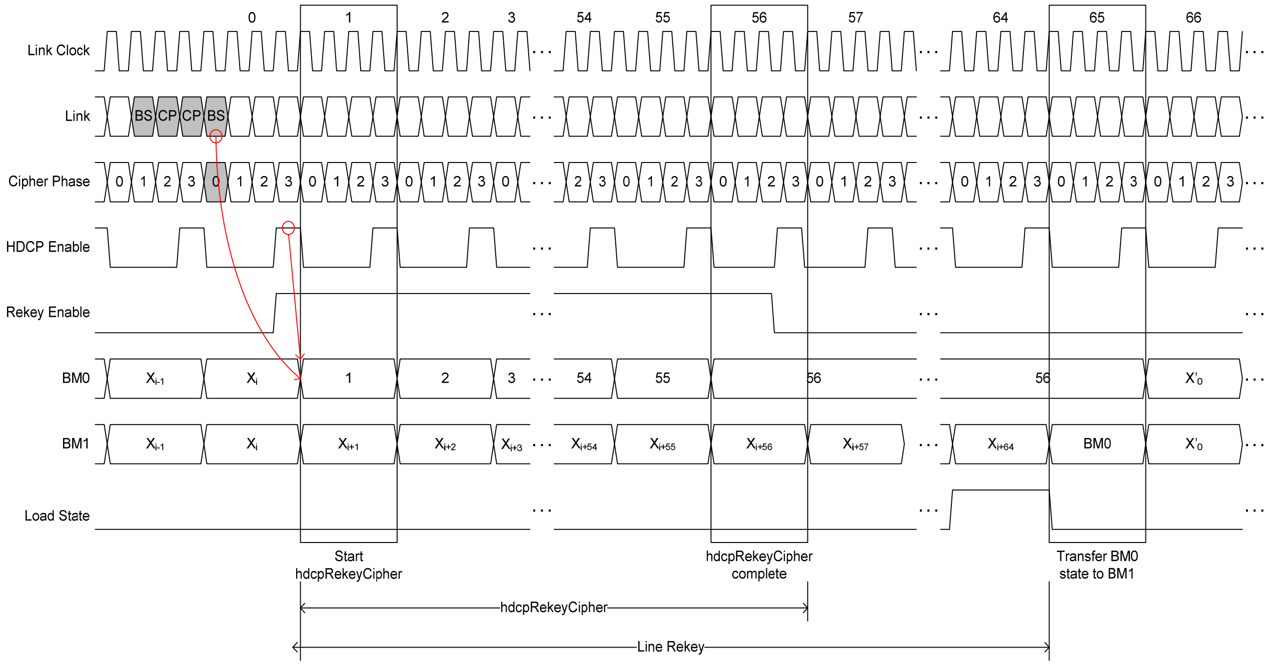

Figure E-9. 1-Lane Line Re-Key Timing Diagram (Phase 0)

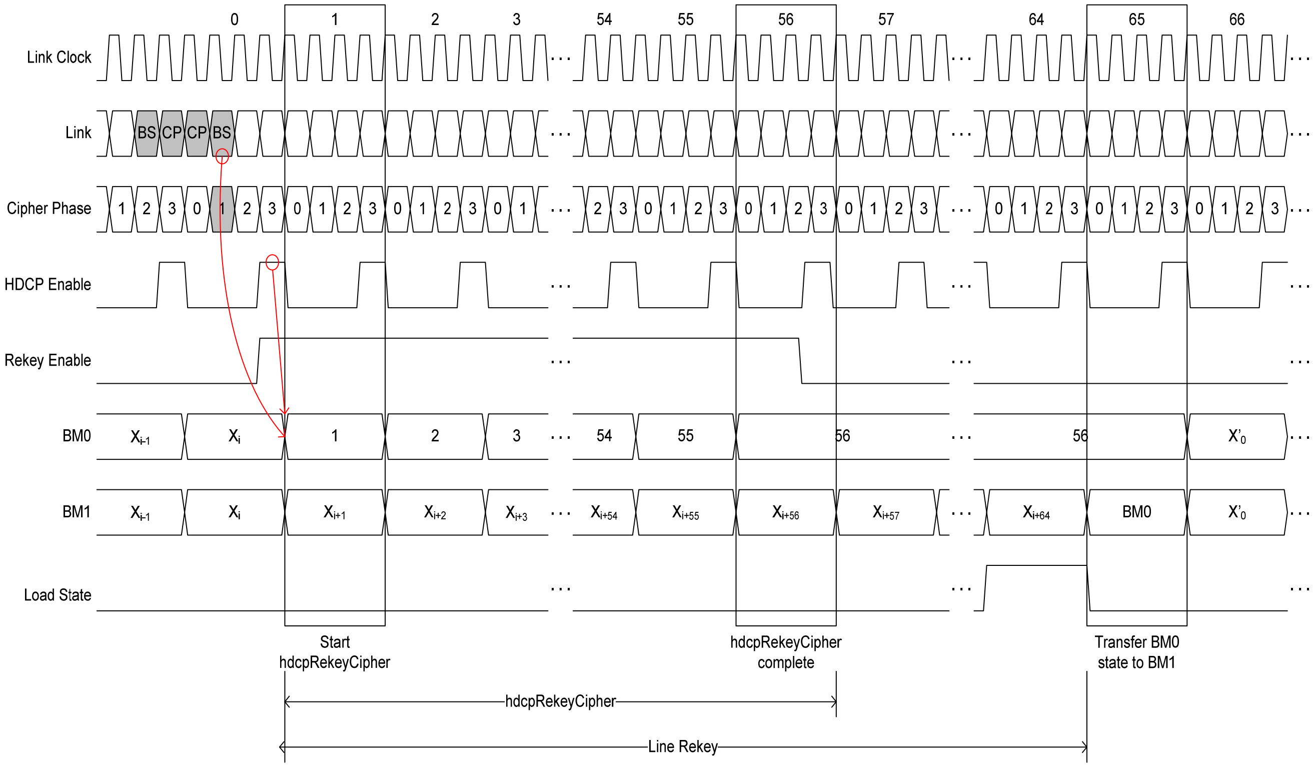

Figure E-10. 1-Lane Line Re-Key Timing Diagram (Phase 1)

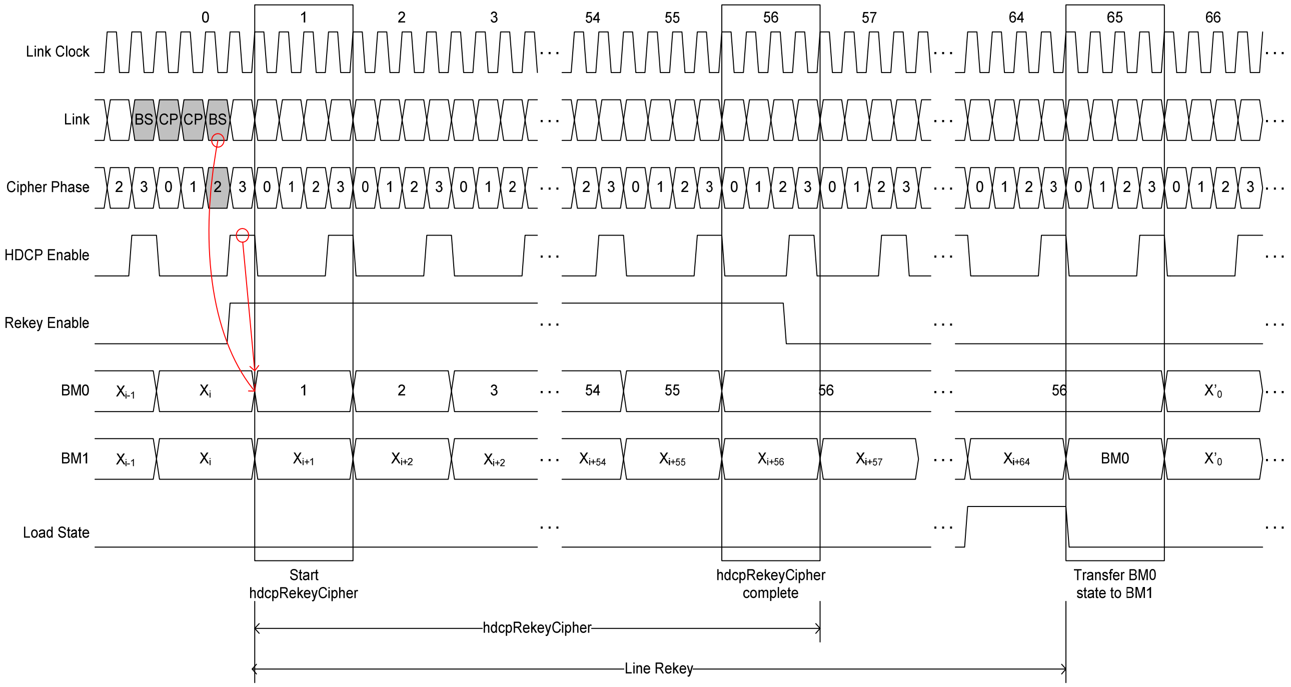

Figure E-11. 1-Lane Line Re-Key Timing Diagram (Phase 2)

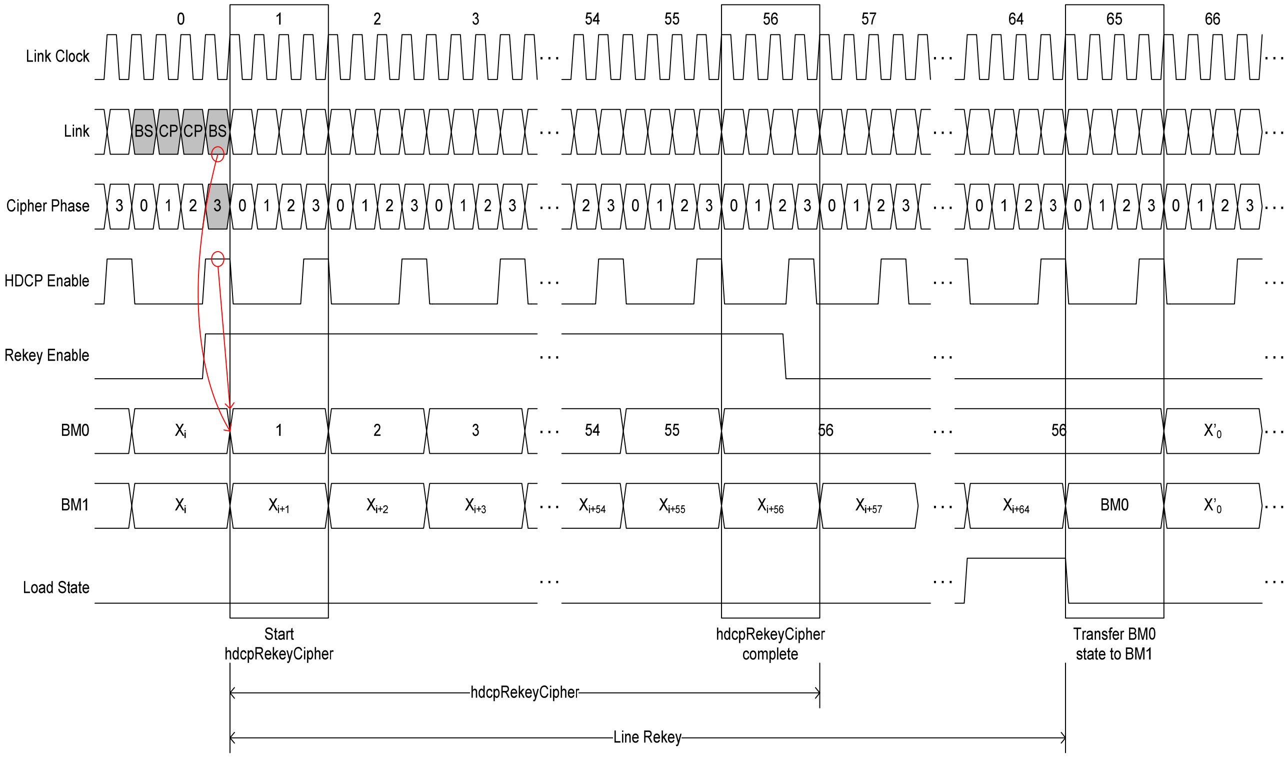

Figure E-12. 1-Lane Line Re-Key Timing Diagram (Phase 3)

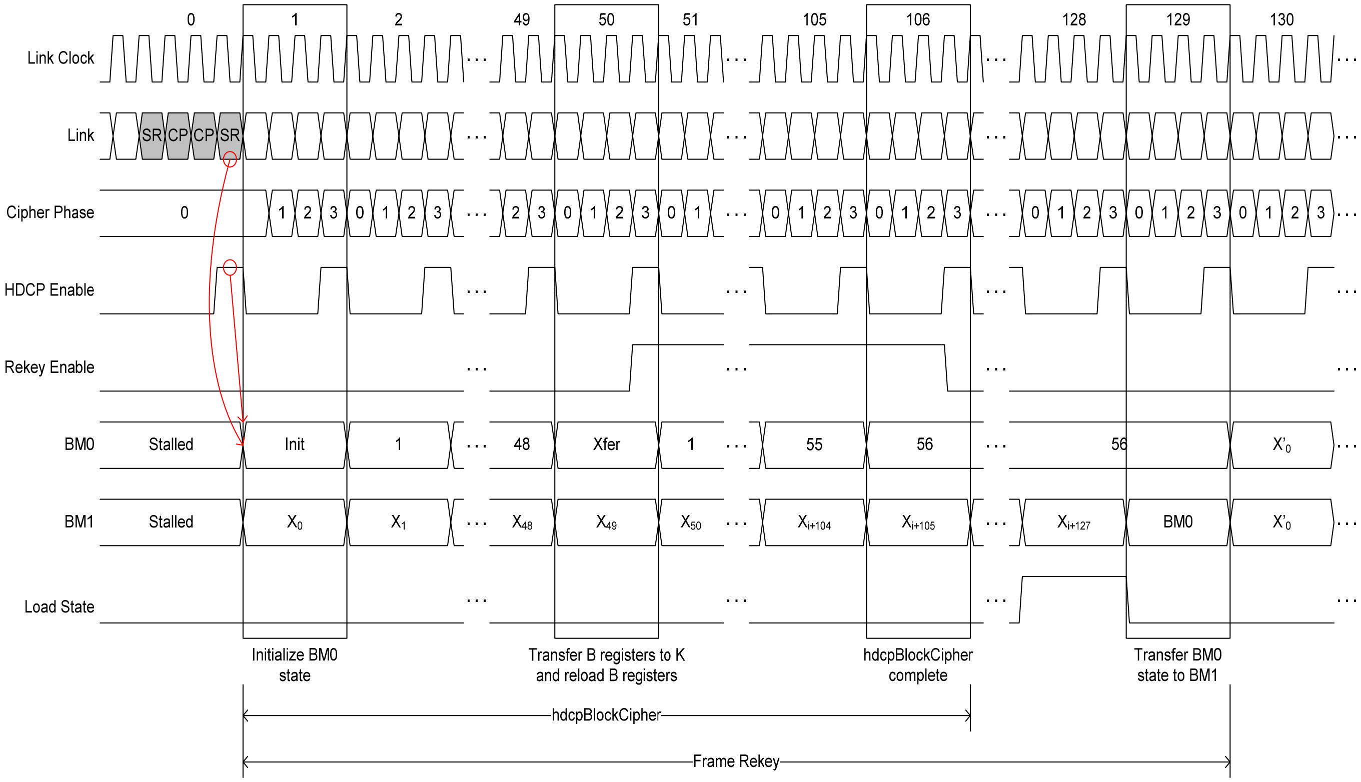

Figure E-13. 1-Lane Initial Frame Key Calculation Timing Diagram

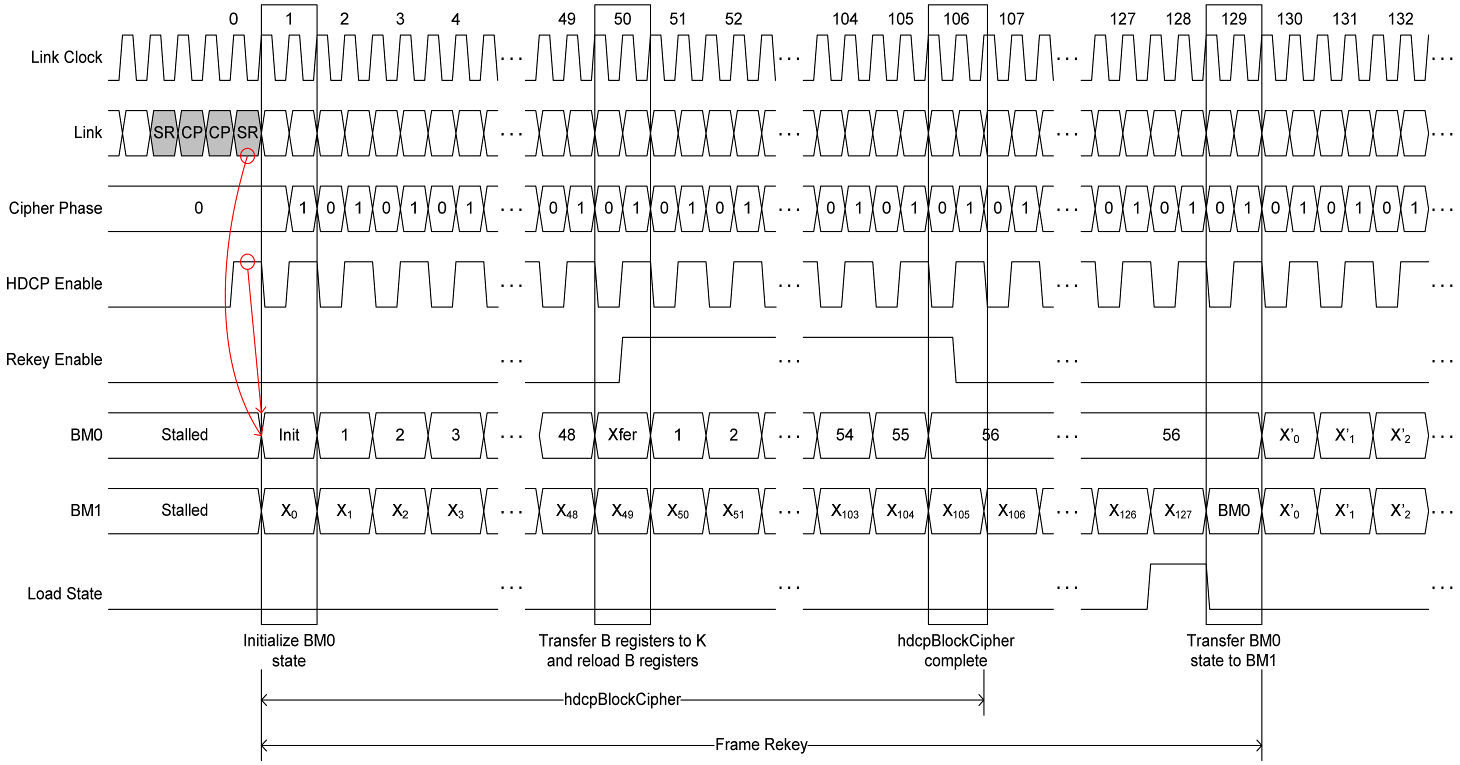

Figure E-14. 2-Lane Initial Frame Key Calculation Timing Diagram

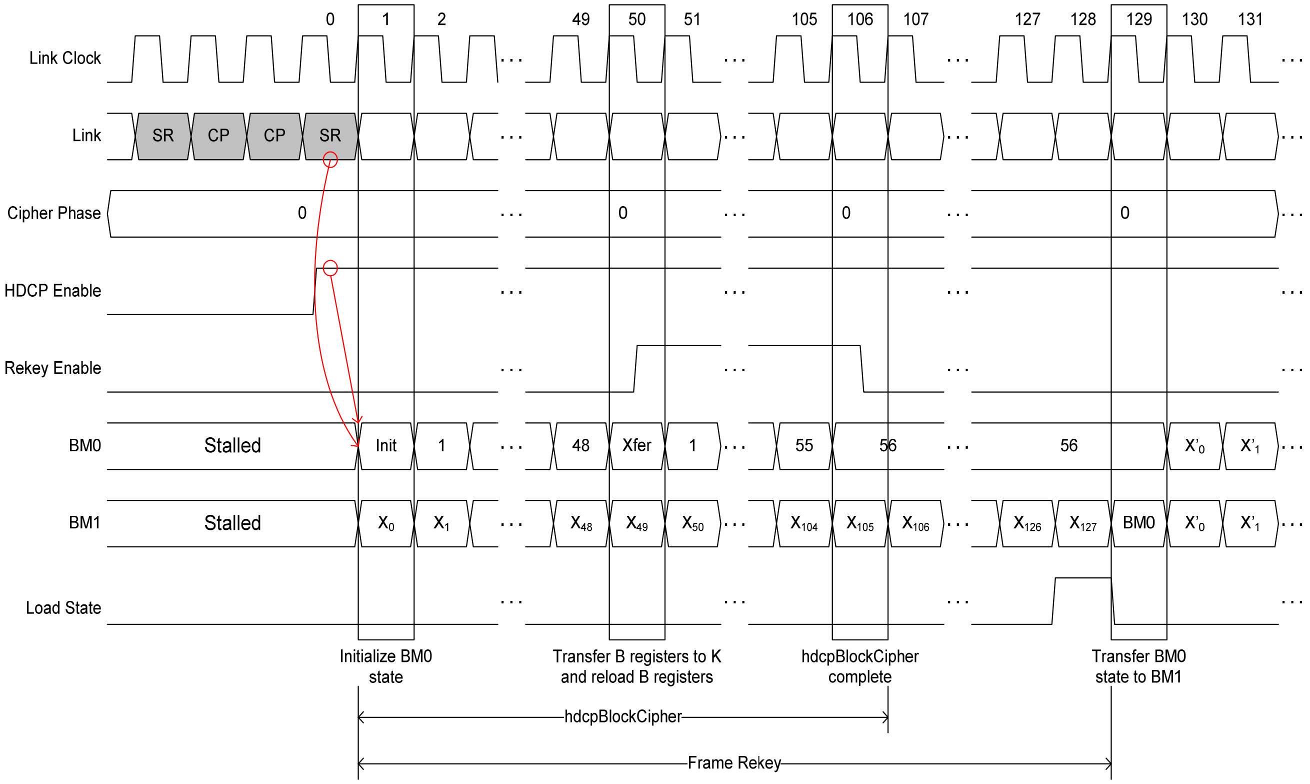

Figure E-15. 4-Lane Initial Frame Key Calculation Timing Diagram

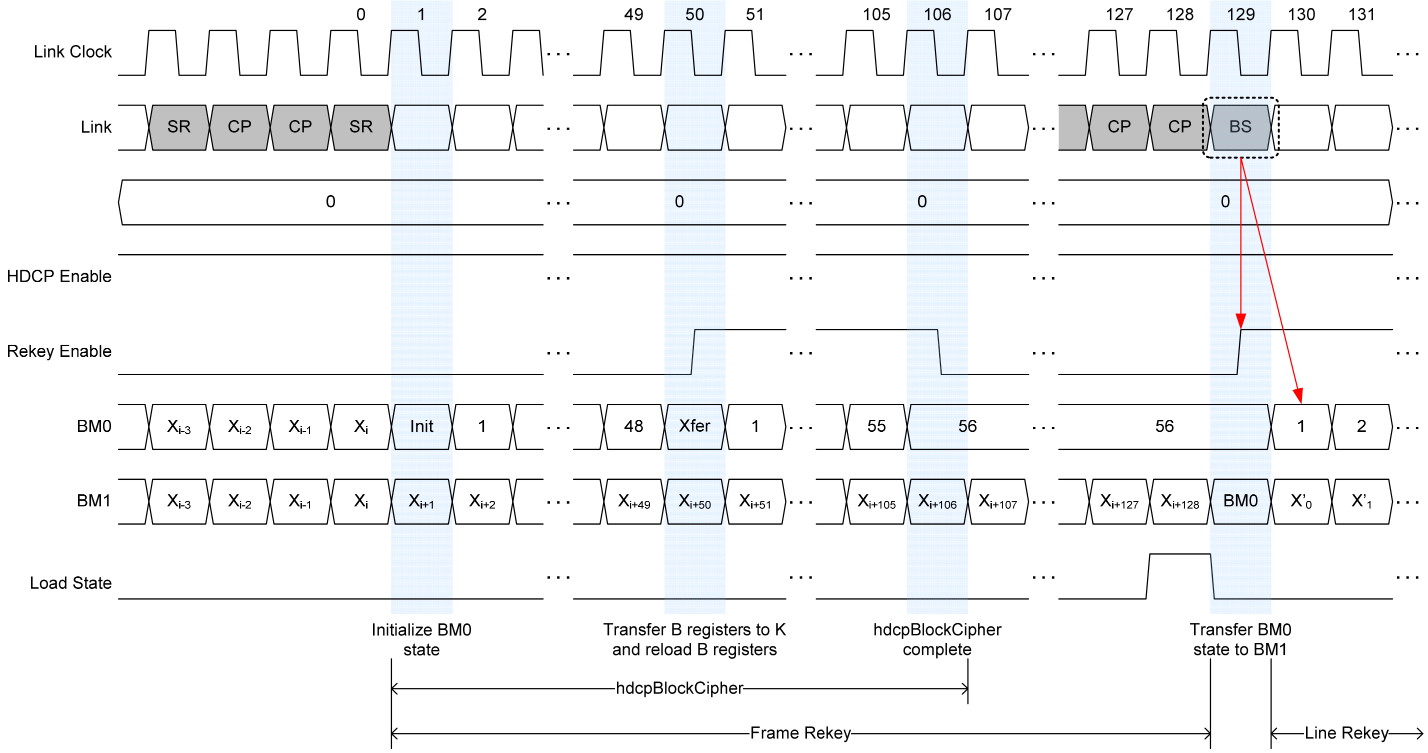
0 1 2 49 50 51 105 106 107 127 128 129 130 131
Link Clock
Link
SR CP CP SR
CP CP BS
0
HDCP Enable
Rekey Enable
BM0
Xi-3 Xi-2 Xi-1 Xi Init 1 48 Xfer 1 55 56 56 1 2
BM1
Xi-3 Xi-2 Xi-1 Xi Xi+1 Xi+2 Xi+49 Xi+50 Xi+51 Xi+105 Xi+106 Xi+107 Xi+127 Xi+128 BM0 X'0 X'1
Load State
Initialize BM0 state
Transfer B registers to K and reload B registers
hdcpBlockCipher complete
Transfer BM0 state to BM1
hdcpBlockCipher
Frame Rekey
Line Rekey

Figure E-16. CPBS Detected Immediately After Completion of Frame Key Calculation in 4-Lane Configuration

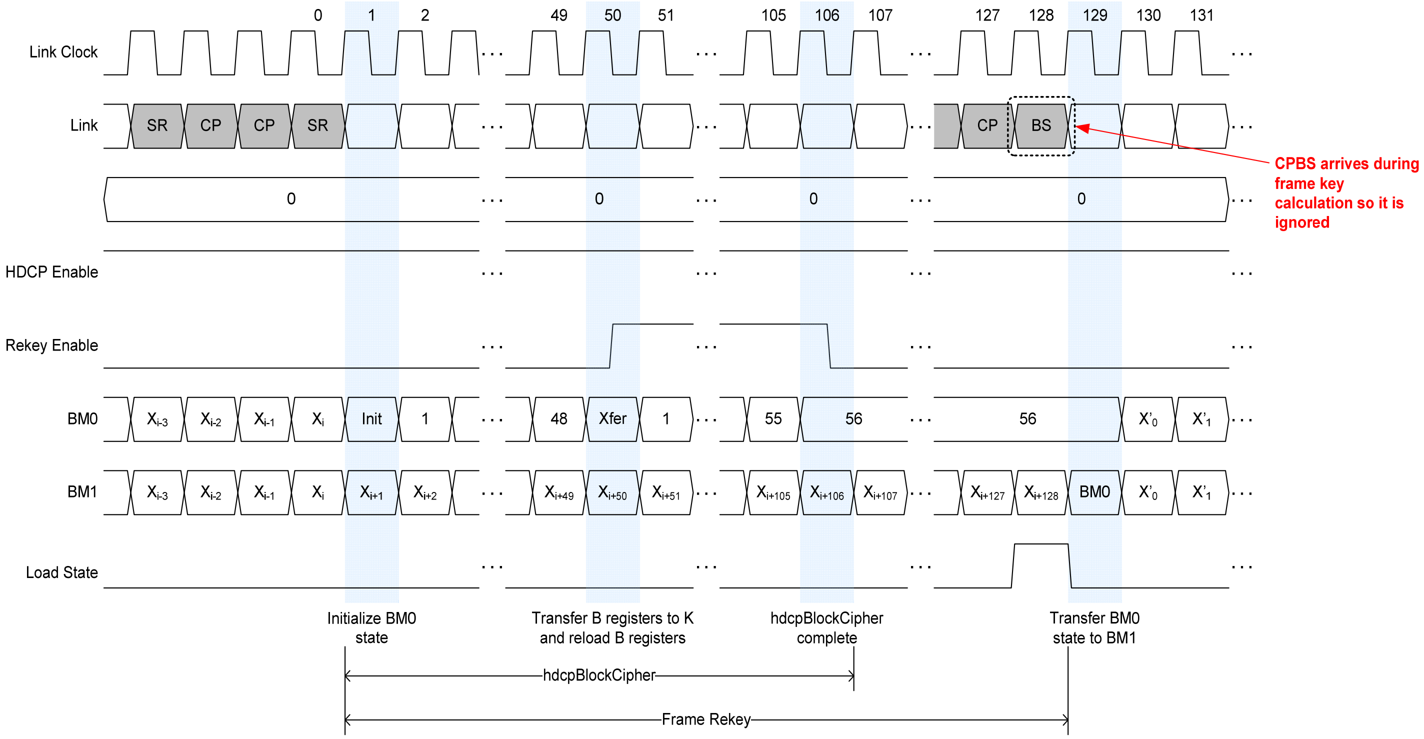

Figure E-17. CPBS Detected During Frame Key Calculation in 4-Lane Configuration

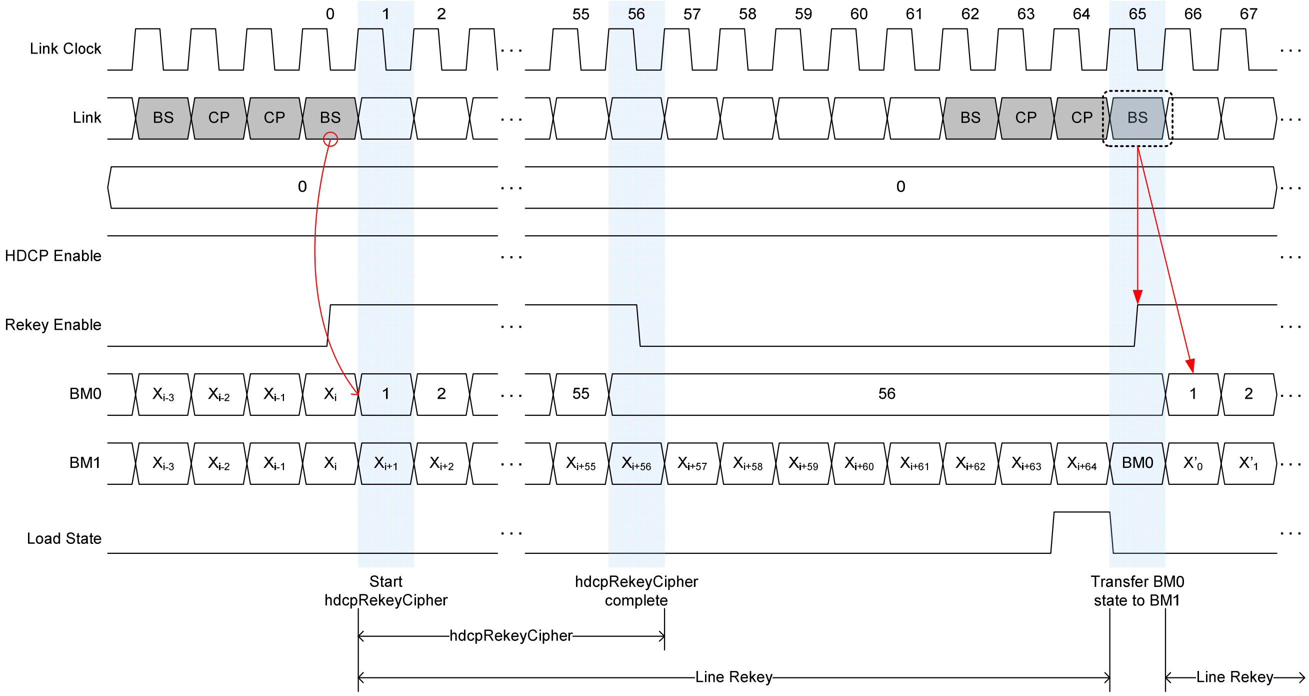

Figure E-18. CPBS Detected Immediately After Completion of Line Re-Key in 4-Lane Configuration

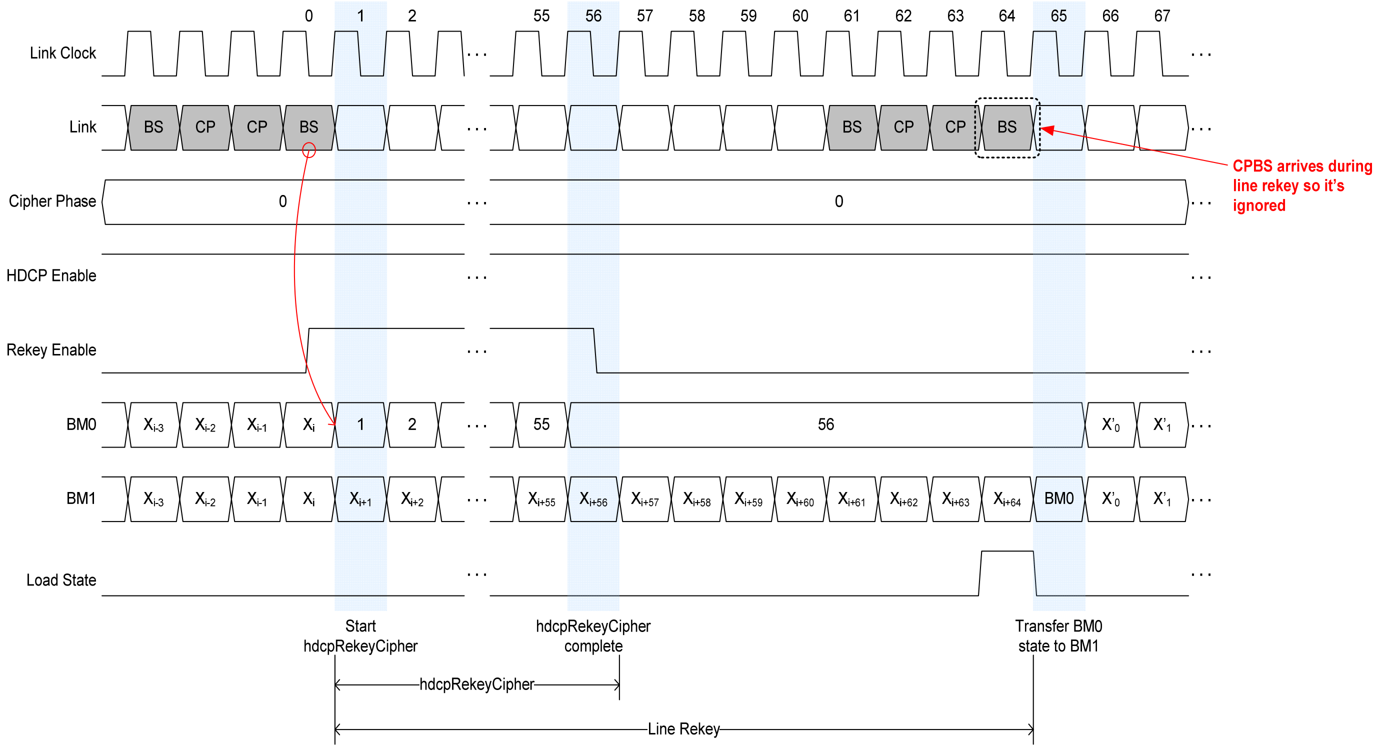

Figure E-19. CPBS Detected During Line Re-Key in 4-Lane Configuration

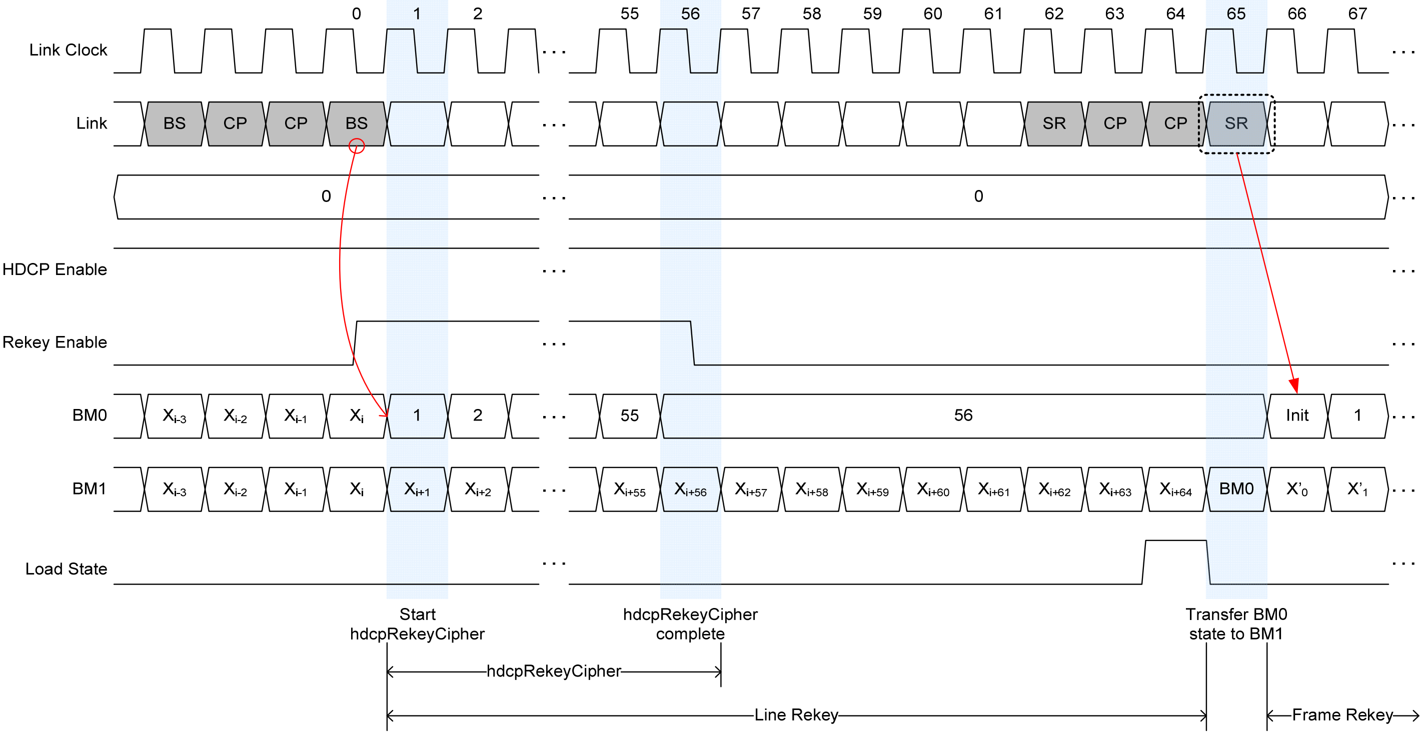

Figure E-20. CPSR Detected Immediately After Completion of Line Re-Key in 4-Lane Configuration

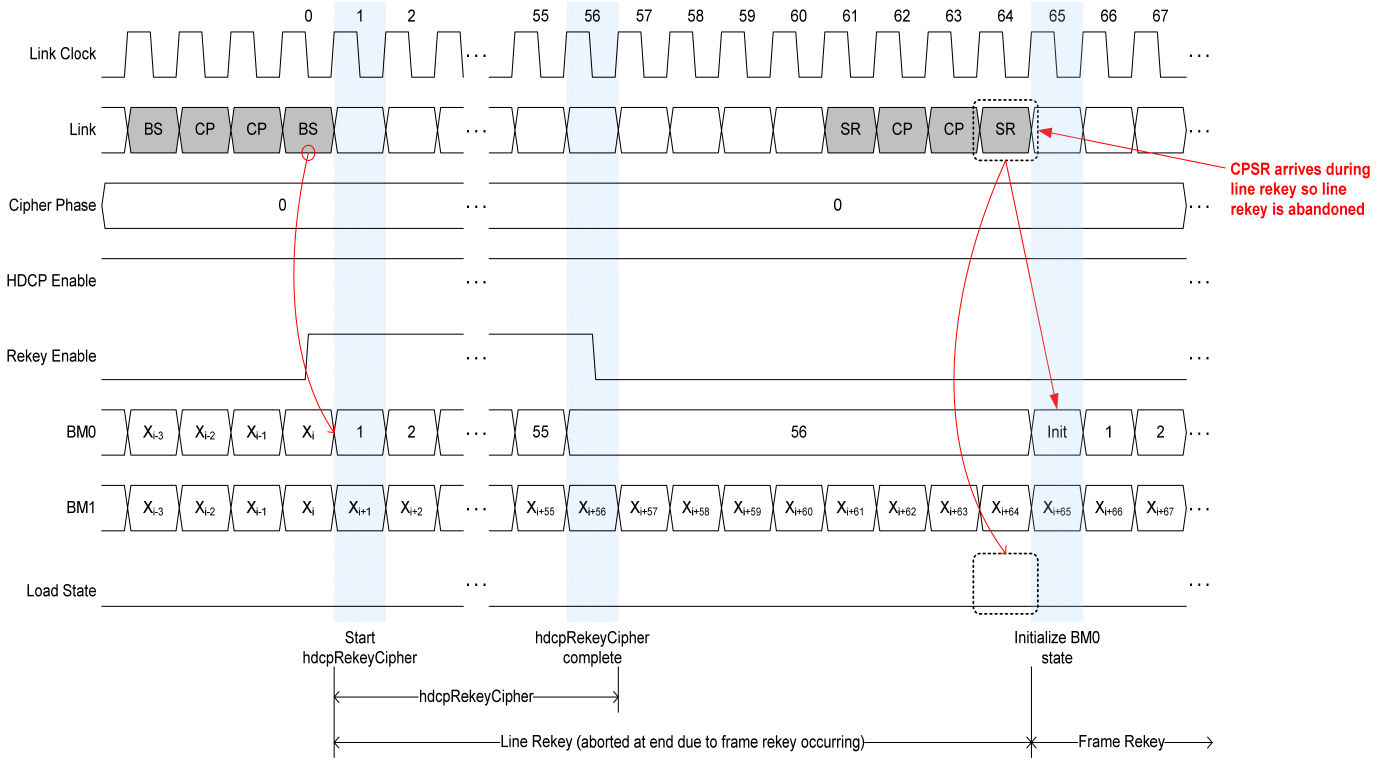

Figure E-21. CPSR Detected During Line Re-Key in 4-Lane Configuration