Summary of Errata and Clarifications to the HDCP on DisplayPort Specification Rev 2.2

Page 7, insert the following definition under Section 1.2

> **Permitted Type 1 Audio Portion**. *Permitted Type 1 Audio Portion* consists of the audio portion of Audiovisual Type 1 Content Stream which is sampled at no more than 24 bits, with a sampling frequency of no more than 192 kHz and no more than 8 channels. Such audio portions may be transmitted by the HDCP Repeater to all HDCP Devices. The HDCP Repeater must support the transmission of Permitted Type 1 Audio Portions to HDCP-protected Interface Ports connected to HDCP Devices compliant with HDCP 2.2 or higher, if such ports are available at the HDCP Repeater.

Replace all references to HDCP2_0_REPEATER_DOWNSTREAM with HDCP2_LEGACY_DEVICE_DOWNSTREAM.

Page 3, replace the third paragraph with the following

> Locality Check – The HDCP Transmitter enforces locality on the content by requiring that the Round Trip Time (RTT) between a pair of messages is not more than 16ms.

Page 12, delete the last three sentences in the second paragraph and replace with the following

> The AKE_Send_Cert message must be available for the transmitter to start the read within 100ms from the time the transmitter finishes writing the AKE_Init message parameters to the HDCP Receiver. The transmitter may attempt to read AKE_Send_Cert message sooner than 100ms and the receiver may respond with AUX_DEFERs until the message is ready to be read. The transmitter aborts the authentication protocol if (a) the AKE_Send_Cert message is not available for the transmitter to start the read after 100 ms or (b) the transmitter has not received the entire AKE_Send_Cert message within 110ms since the initiation of the AKE_Send_Cert message read.

Page 13, delete the last two sentences in the first paragraph and replace with the following

> The CP_IRQ interrupt must be generated and the AKE_Send_H_prime message must be available for the transmitter to start the read within one second from the time the transmitter finishes writing the AKE_No_Stored_km message parameters to the HDCP Receiver. The transmitter may attempt to read AKE_Send_H_prime message sooner than one second and the receiver may respond with AUX_DEFERs until the message is ready to be read. The transmitter aborts the authentication protocol if (a) the AKE_Send_H_prime message is not available for the transmitter to start the read after one second or (b) the transmitter has not received the entire AKE_Send_H_prime message within 7ms since the initiation of the AKE_Send_H_prime message read or (c) there is a mismatch between H and H’.

Page 13, delete the last two sentences in the eighth paragraph and replace with the following

> The CP_IRQ interrupt must be generated and the AKE_Send_H_prime message must be available for the transmitter to start the read within 200ms from the time the transmitter finishes writing the AKE_Stored_km message parameters to the HDCP Receiver. The transmitter may attempt to read AKE_Send_H_prime message sooner than 200ms and the receiver may respond with AUX_DEFERs until the message is ready to be read. The transmitter aborts the authentication protocol if (a) the AKE_Send_H_prime message is not available for the transmitter to start the read after 200ms or (b) the transmitter has not received the entire AKE_Send_H_prime message within 7ms since the initiation of the AKE_Send_H_prime message read or (c) there is a mismatch between H and H’.

Page 13, delete the last sentence in the tenth paragraph and replace with the following

> The AKE_Send_Cert message must be available for the transmitter to start the read within 100ms from the time the transmitter finishes writing the AKE_Init message parameters to the HDCP Receiver.

Page 14, delete the last sentence in the second paragraph and replace with the following

> The AKE_Send_H_prime message must be available for the transmitter to start the read within one second from the time the transmitter finishes writing the AKE_No_Stored_km message parameters to the HDCP Receiver.

Page 14, delete the last sentence in the seventh paragraph and replace with the following

> The AKE_Send_H_prime message must be available for the transmitter to start the read within 200ms from the time the transmitter finishes writing the AKE_Stored_km message parameters to the HDCP Receiver.

Page 14, delete the last sentence in the fourth paragraph under Section 2.2.1 and replace with the following

> This message must be available for the transmitter to start the read within 200ms from the time the transmitter finishes writing the AKE_Send_H_prime message parameters to the HDCP Receiver.

Page 14, delete the third sentence in the fifth paragraph under Section 2.2.1 and replace with the following

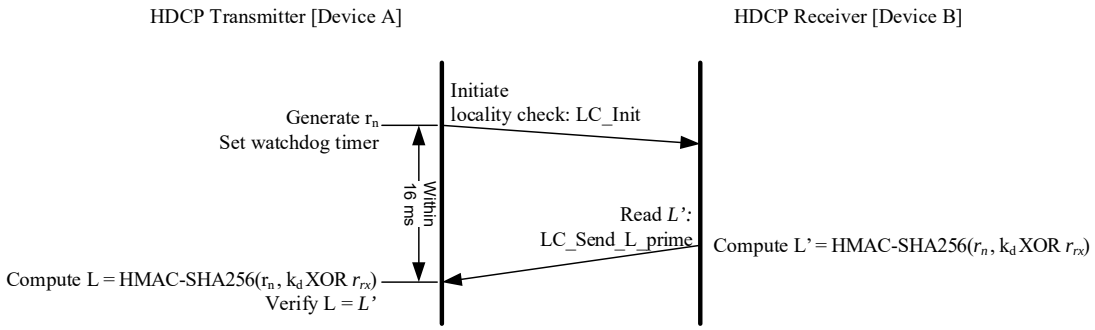
> The transmitter may attempt to read AKE_Send_Pairing_Info message sooner than 200ms and the receiver may respond with AUX_DEFERs until the message is ready to be read. Authentication fails and the transmitter aborts the authentication protocol if (a) the AKE_Send_Pairing_Info message is not available for the transmitter to start the read after 200ms or (b) the transmitter has not received the entire

AKE_Send_Pairing_Info message within 5ms since the initiation of the AKE_Send_Pairing_Info message read.

Page 15, replace the fourth paragraph under Section 2.3 with the following

Sets its watchdog timer to 16ms. The LC_Send_L_prime message must be received by the transmitter within 16ms from the time the transmitter finishes writing the LC_Init message parameters to the HDCP Receiver i.e. 16ms from the time the last byte of r_n has been written to the time the last byte of LC_Send_L_prime message has been received. If the LC_Send_L_prime message is not received by the transmitter within 16ms, locality check fails and the transmitter aborts the authentication protocol.

Page 16, replace Figure 2.4 with the following



Page 16, replace the last sentence in the sixth paragraph with the following

The LC_Send_L_prime message must be received by the transmitter within 16ms from the time the transmitter finishes writing the LC_Init message parameters to the HDCP Receiver.

Page 16, Section 2.4, replace 1st paragraph under Section 2.4 with the following

Successful completion of AKE and locality check stages affirms to HDCP Transmitter that the HDCP Receiver is authorized to receive HDCP Content. Session Key Exchange (SKE) is initiated by the HDCP Transmitter after a successful locality check. The HDCP Transmitter sends encrypted Session Key to the HDCP Receiver at least 200 ms before enabling HDCP Encryption and beginning the transmission of HDCP Content. If the attached HDCP Receiver is not an HDCP Repeater, the HDCP Transmitter also writes the Type value corresponding to the Content Stream to be transmitted to the HDCP Receiver at least 200 ms before enabling HDCP Encryption.

HDCP Encryption may be enabled 200 ms after the transmission of the encrypted Session Key and Type value to the HDCP Receiver and at no time prior. Type value is written only to HDCP Receivers that are not HDCP Repeaters. Content encrypted with the Session Key k_s starts to flow between the HDCP

Transmitter and HDCP Receiver. HDCP Encryption must be enabled only after successful completion of AKE, locality check and SKE stages.

Page 21, replace Table 2.2 with the following

From	To	Max Delay	Conditions and Comments
SKE_Send_Eks1 Session Key received from Upstream HDCP Transmitter	SKE_Send_Eks2 k_s generated by HDCP Repeater transmitted downstream	110ms	Downstream propagation time.
SKE_Send_Eks3 k_s transmitted to all downstream HDCP-protected Interface Ports	RDY1 Upstream READY asserted	220ms	Upstream propagation time when no downstream HDCP Repeaters are attached (no downstream Receiver ID lists to process)
RDY1 Downstream *Receiver ID*s and topology information received	RDY2 Upstream READY asserted	220ms	Upstream propagation time when one or more HDCP Repeaters are attached. From latest downstream READY (downstream Receiver ID lists must be processed)
SKE_Send_Eks1 Upstream HDCP Transmitter transmits k_s	RDY2 Upstream transmitter receives CP_IRQ with READY asserted	1.32 seconds	For the Maximum of four repeater levels, 4 * (110ms + 220ms)

Table 2.2. HDCP Repeater Protocol Timing Requirements

Page 22, replace third sentence in 3rd paragraph under Section 2.5.2 with the following

Type 0 Content Streams (see Section 4.2.12) and Permitted Type 1 Audio Portions may be transmitted by the HDCP Repeater to all HDCP Devices.

Page 22, replace last sentence in 3rd paragraph under Section 2.5.2 with the following

Type 1 Content Streams (see Section 4.2.12), except Permitted Type 1 Audio Portions, must not be transmitted by the HDCP Repeater through its HDCP-protected Interface Ports connected to HDCP 1.x-compliant Devices, HDCP 2.0-compliant Devices and HDCP 2.1-compliant Devices.

Page 22, replace first sentence in the fourth paragraph under Section 2.5.2 with the following

The HDCP Transmitter must write the RepeaterAuth_Stream_Manage message specifying Type values assigned to Content Streams, to the attached HDCP Repeater at least 110ms before the transmission of the corresponding Content Streams after HDCP Encryption.

Page 23, replace the first two sentences in the third paragraph with the following

The RepeaterAuth_Stream_Ready message must be available for the transmitter to start the read within 100ms from the time the transmitter finishes writing the RepeaterAuth_Stream_Manage message parameters to the HDCP Receiver.

Page 23, replace the last sentence in the fourth paragraph with the following

The transmitter may attempt to read RepeaterAuth_Stream_Ready message sooner than 100ms and the receiver may respond with AUX_DEFERs until the message is ready to be read. The HDCP Transmitter must not transmit the Content Streams identified in the corresponding RepeaterAuth_Stream_Manage message if (a) the RepeaterAuth_Stream_Ready message is not available for the transmitter to start the read after 100ms or (b) the transmitter has not received the entire RepeaterAuth_Stream_Ready message within 7ms since the initiation of the RepeaterAuth_Stream_Ready message read or (c) if M is not equal to M'.

Page 28, replace the last sentence in the fifth paragraph with the following

It reads AKE_Send_Cert from the receiver within the time period specified in Section 2.2.

Page 28, replace the last sentence in the sixth paragraph with the following

It computes H, receives AKE_Send_H_prime message from the receiver containing H' within the time period specified in Section 2.2 and compares H' against H.

Page 28, replace the last sentence in the seventh paragraph with the following

It computes H, reads AKE_Send_H_prime message from the receiver containing H' within the time period specified in Section 2.2 and compares H' against H.

Page 28, replace the last sentence in the ninth paragraph with the following

> This transition also occurs if AKE_Send_H_prime message is not received within the time period specified in Section 2.2.

Page 28, replace the last sentence in the twelfth paragraph with the following

> Locality check fails when the watchdog timer at the HDCP Transmitter expires or on a mismatch between L and *L′*.

Page 30, replace the last three sentences in the second paragraph with the following

> The HDCP Transmitter sends the RepeaterAuth_Stream_Manage message specifying Type values assigned to Content Streams, to the attached HDCP Repeater at least 110ms before the transmission of the corresponding Content Streams after HDCP Encryption. It must receive the RepeaterAuth_Stream_Ready message from the HDCP Repeater within the time period specified in Section 2.5.2, and verifies *M′*. This step fails if the RepeaterAuth_Stream_Ready message is not available to read within the time period specified in Section 2.5.2, or if *M* is not equal to *M′*.

Page 23, Section 2.6.1, replace the 4th sentence in the 1st paragraph under Section 2.6.1 with the following

> The transmitter sets the two MTPH timeslots following a given SR symbol to the corresponding byte of the pattern, encrypts the MTPHs with the Type input to the HDCP Cipher set to 0x00 (Refer to Section 3.2) and sends the MTPHs to the receiver.

Page 24, Section 2.6.2, replace the 8th sentence in the 1st paragraph under Section 2.6.2 with the following

> 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 with the Type input to the HDCP Cipher set to the Type value corresponding to the Content Stream to be encrypted (Refer to Section 3.2)and sends the VB-ID to the receiver.

Page 31, replace the last sentence in the fourth paragraph with the following

> It makes AKE_Send_H_prime message available for reading immediately after computation of *H′* to ensure that the message is received by the transmitter within the time period specified in Section 2.2.

Page 31, replace the last sentence in the fifth paragraph with the following

> It makes AKE_Send_H_prime message available for reading immediately after computation of *H′* to ensure that the message is received by the transmitter within the time period specified in Section 2.2.

Page 36, replace the last sentence in the fifth paragraph with the following

> It reads AKE_Send_Cert from the receiver within the time period specified in Section 2.2.

Page 36, replace the last sentence in the sixth paragraph with the following

> It computes H, receives AKE_Send_H_prime message from the receiver containing *H′* within the time period specified in Section 2.2 and compares *H′* against H.

Page 36, replace the last sentence in the seventh paragraph with the following

> It computes H, receives AKE_Send_H_prime message from the receiver containing *H′* within the time period specified in Section 2.2 and compares *H′* against H.

Page 36, replace the last sentence in the ninth paragraph with the following

> This transition also occurs if AKE_Send_H_prime message is not received within the time period specified in Section 2.2.

Page 36, replace the last sentence in the twelfth paragraph with the following

> Locality check fails when the watchdog timer at the downstream side expires or on a mismatch between L and *L′*.

Page 38, replace the second sentence in the second paragraph with the following

> The downstream side propagates the Content Stream management information, received from the upstream transmitter, using the RepeaterAuth_Stream_Manage message to the attached HDCP Repeater at least 110ms before the transmission of the corresponding Content Streams after HDCP Encryption.

Page 38, replace the third paragraph with the following

> The downstream side must receive the RepeaterAuth_Stream_Ready message from the HDCP Repeater within the time period specified in Section 2.5.2, and verifies *M′*. This step fails if the RepeaterAuth_Stream_Ready message is not available to read within the time period specified in Section 2.5.2, or if *M* is not equal to *M′*.

Page 39, replace the last sentence in the sixth paragraph with the following

> It makes available the AKE_Send_H_prime message within the time period specified in Section 2.2.

Page 39, replace the last sentence in the seventh paragraph with the following

> It makes available the AKE_Send_H_prime message within the time period specified in Section 2.2.

Page 40, replace the last sentence in the tenth paragraph (under Transition C5:C0) with the following

> This transition may also occur if all downstream HDCP-protected Interface Ports have reached the state of unconnected or unauthenticated.

Page 42, replace the first sentence in the first paragraph with the following

> This transition may also occur when a downstream port that was previously in an authenticated state transitions in to an unauthenticated or unconnected state.

Page 42, add the following sentence under the first paragraph

> Note that the upstream side need not transition from State C8 to State C5 when a previously authenticated downstream port transitions in to an unauthenticated or unconnected state.

Page 43, replace Table 2.3 with the following

From	To	Max Delay	Conditions and Comments
SKE_Send_Eks1 Session Key received from Upstream HDCP Transmitter	AKSV1 HDCP Repeater's *Aksv* transmitted downstream	110 ms	Downstream propagation time.
AKSV1 HDCP Repeater's *Aksv* transmitted downstream	RDY1 Upstream READY asserted	220 ms	Upstream propagation time when no downstream HDCP Repeaters are attached (no downstream KSV lists to process)

Table 2.3. HDCP 2 – HDCP 1.x Repeater Protocol Timing with Receiver Attached

Page 43, replace Table 2.4 with the following

From	To	Max Delay	Conditions and Comments
SKE_Send_Eks1 Session Key received from Upstream HDCP Transmitter	AKSV1 HDCP Repeater's *Aksv* transmitted downstream	110 ms	Downstream propagation time.

RDY1 Downstream Receiver IDs and topology information received	RDY2 Upstream READY asserted	220 ms	Upstream propagation time when one or more HDCP 1.x-compliant Repeaters are attached. From latest downstream READY. (downstream KSV lists must be processed)

Table 2.4. HDCP 2 – HDCP 1.x Repeater Protocol Timing with Repeater Attached

Page 44, replace Table 2.5 with the following

From	To	Max Delay	Conditions and Comments
AKSV1 Upstream HDCP Transmitter *Aksv* received	SKE_Send_Eks1 k_s generated by HDCP Repeater transmitted downstream	410 ms	Downstream propagation time.
SKE_Send_Eks1 k_s generated by HDCP Repeater transmitted downstream	RDY1 Upstream READY asserted	520 ms	Upstream propagation time when no downstream HDCP Repeaters are attached (no downstream Receiver ID lists to process)

Table 2.5. HDCP 1.x – HDCP 2 Repeater Protocol Timing with Repeater Attached

Page 45, replace Table 2.6 with the following

From	To	Max Delay	Conditions and Comments
AKSV1 Upstream HDCP Transmitter *Aksv* received	SKE_Send_Eks1 k_s generated by HDCP Repeater transmitted downstream	410 ms	Downstream propagation time.
RDY1 READY asserted by downstream repeater	RDY2 Upstream READY asserted	520 ms	Upstream propagation time when one or more HDCP Repeaters are attached. From latest downstream READY (downstream Receiver ID lists must be processed)

Table 2.6. HDCP 1.x – HDCP 2 Repeater Protocol Timing with Repeater Attached

Page 47, replace rows corresponding to $cert_{rx}$, r_{rx}, *RxCaps*, *H'*, $E_{kh}\_k_m$, *L'*, *seq_num_M*, *k*, *StreamID_Type* and *M'* in Table 2.7 with the following

Offset (hex)	Name	Size in Bytes	Rd/Wr	Function
0x6900B	$cert_{rx}$	522	Rd	HDCP Receiver Public Key Certificate read by the HDCP Transmitter as part of AKE_Send_Cert message.
0x69215	r_{rx}	8	Rd	Pseudo-random value read as part of AKE_Send_Cert message.
0x6921D	*RxCaps*	3	Rd	This multi-byte value is read as part of AKE_Send_Cert message. Refer to **Error! Reference source not found.** for definitions.
0x692C0	*H´*	32	Rd	HMAC computed during AKE and read as part of AKE_Send_H_prime message.
0x692E0	$E_{kh}\_k_m$	16	Rd	Encrypted k_m read as part of AKE_Send_Pairing_Info message.
0x692F8	*L´*	32	Rd	HMAC computed during Locality Check and read as part of LC_Send_L_prime message.
0x693F0	*seq_num_M*	3	Wr	Sequence number used for the computation of *M/M'* and written as part of RepeaterAuth_Stream_Manage message. This multi-byte value is written before *k* is written.
0x693F3	*k*	2	Wr	This value indicates the number of Content Streams that are being transmitted by the HDCP Transmitter to the attached HDCP Repeater during the HDCP Session and is written as part of RepeaterAuth_Stream_Manage message. This multi-byte value is written before *StreamID_Type* is written.
0x693F5	*StreamID_Type*	126	Wr	Concatenation of Stream Identifiers and Type values of Content Streams that are being transmitted by the HDCP Transmitter to the attached HDCP Repeater during the HDCP Session and is written as part of RepeaterAuth_Stream_Manage message.

0x69473	*M′*	32	Rd	HMAC computed during downstream propagation of Content Stream management information and read as part of RepeaterAuth_Stream_Ready message.

Page 48, Section 2.15, delete the last two rows in Table 2.7 and insert the following rows at the end of the table

0x69494	Type	1	Wr	Type value assigned to the Content Stream to be transmitted to the HDCP Receiver. This value is written by the HDCP Transmitter only to HDCP Receivers and not to HDCP Repeaters.
0x69495	Rsvd	131	Rd	All bytes read as 0x00
0x69518	dbg	64	Rd/ Wr	Implementation-specific debug registers. Confidential values must not be exposed through these registers.

Page 50, replace the row corresponding to HDCP2_0_REPEATER_DOWNSTREAM in Table 2.9 with the following

HDCP2_LEGACY_DEVICE_DOWNSTREAM	1	Rd	When set to one, indicates presence of an HDCP2.0-compliant Device or HDCP2.1-compliant Device in the topology

Page 55, Section 3.2, replace the 2nd sentence in the 4th paragraph under Section 3.2 with the following

> Type value is associated with the VC PayloadID corresponding to a Content Stream as explained in Section 4.2.12.

Page 57, Section 3.3, add the following sentence at the end of the 10th paragraph under Section 3.3

> The XOR Enable/Disable status for timeslots specified by the HDCP_Encryption_Control must also apply at the link frame boundary.

Page 57, Section 3.3, add the following sentence at the end of the 11th paragraph under Section 3.3

> The XOR Enable/Disable status for timeslots specified by the HDCP_Encryption_Control preceding a standalone ACT must apply starting after the MTP carrying the end of the ACT sequence.

Page 57, Section 3.3, add the following figure after the 11th paragraph under Section 3.3

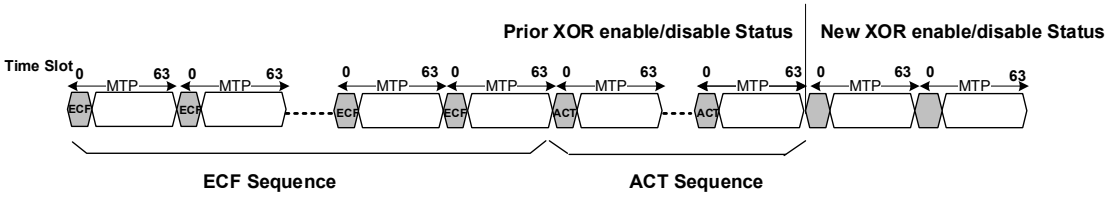


Figure Error! No text of specified style in document.**-1: HDCP_Encryption_Control preceding a standalone ACT**

Page 62, delete the last sentence in the paragraph under Section 4.2.2.

Page 62, replace the paragraph under Section 4.2.5 with the following

AKE_Send_H_prime must be available for the transmitter to start the read within one second after writing the AKE_No_Stored_km message i.e. after the last byte of $E_{kpub}\_k_m$ has been written, or within 200 ms after writing the AKE_Stored_km message i.e. after the last byte of m has been written.

Page 63, replace the paragraph under Section 4.2.6 with the following

AKE_Send_Pairing_Info must be available for the transmitter to start the read within 200 ms from the time the transmitter finishes writing the AKE_Send_H_prime message parameters to the HDCP Receiver i.e. after the last byte of H' has been written.

Page 63, replace the paragraph under Section 4.2.8 with the following

The LC_Send_L_prime message must be received by the transmitter within 16ms from the time the transmitter finishes writing the LC_Init message parameters to the HDCP Receiver i.e. 16ms from the time the last byte of r_n has been written to the time the last byte of LC_Send_L_prime message has been received

Page 65, replace the paragraph under Section 4.2.13 with the following

The RepeaterAuth_Stream_Ready message must be available for the transmitter to start the read within 100ms from the time the transmitter finishes writing the RepeaterAuth_Stream_Manage message parameters to the HDCP Receiver i.e. after the last byte of *StreamID_Type* has been written.

Page 64, replace 4th paragraph under Section 4.2.10 with the following

The HDCP Repeater sets *RxInfo*.HDCP2_LEGACY_DEVICE_DOWNSTREAM bit to one if an HDCP 2.0-compliant Device or HDCP 2.1-compliant Device is attached to any one of its downstream

ports, else it sets *RxInfo*.HDCP2_LEGACY_DEVICE_DOWNSTREAM to zero.

Page 64, Section 4.2.12, replace 2nd paragraph under Section 4.2.12 with the following

The VC Payload ID, assigned to a Content Stream as specified in the DisplayPort specification, is followed by its assigned Type value in the RepeaterAuth_Stream_Manage message. All Content Streams transmitted by the HDCP Transmitter to the HDCP Repeater, after HDCP Encryption, are assigned Type values.

Page 65, Section 4.2.12, replace 3rd paragraph under Section 4.2.12 with the following

StreamID_Type = VC Payload ID_1 || Type || VC Payload ID_2 || Type ||… || VC Payload ID_k || Type

VC Payload ID assigned to a Content Stream is concatenated with its assigned Type value. All values are in big-endian order.

In SST mode, the VC Payload ID is set to 0 (zero).

Page 65, replace Table 4.13 with the following

Parameter	No. of Bytes	Description
VC Payload ID	1	VC Payload ID, corresponding to the Content Stream, as defined in the DisplayPort specification. VC Payload ID is set to 0 (zero) in SST mode
Type	1	0x00: Type 0 Content Stream. May be transmitted by the HDCP Repeater to all HDCP Devices. 0x01: Type 1 Content Stream. Except for Permitted Type 1 Audio Portion, must not be transmitted by the HDCP Repeater to HDCP 1.x-compliant Devices, HDCP 2.0-compliant Devices and HDCP 2.1-compliant Devices. 0x02 – 0xFF : Reserved for future use only. Content Streams with reserved Type values must be treated similar to Type 1 Content Streams

Page 65, rename Table 4.13 to “VC Payload ID, Type Decryption”

Appendix D. Test Vectors

D.1 Facsimile Keys

Note: The facsimile keys provided must be used ONLY for test purposes.

All values are provided in big-endian order.

Table D.1 provides facsimile key information for transmitter T1.

	Value in Hex
Global Constant lc_{128}	93 ce 5a 56 a0 a1 f4 f7 3c 65 8a 1b d2 ae f0 f7

Table D.1

Table D.2 provides the facsimile public parameters associated with the DCP LLC key $kpub_{dcp}$. These parameters are used only for test purposes. They are not used in production devices or SRMs.

	Value in Hex
Modulus n	A2 C7 55 57 54 CB AA A7 7A 27 92 C3 1A 6D C2 31 CF 12 C2 24 BF 89 72 46 A4 8D 20 83 B2 DD 04 DA 7E 01 A9 19 EF 7E 8C 47 54 C8 59 72 5C 89 60 62 9F 39 D0 E4 80 CA A8 D4 1E 91 E3 0E 2C 77 55 6D 58 A8 9E 3E F2 DA 78 3E BA D1 05 37 07 F2 88 74 0C BC FB 68 A4 7A 27 AD 63 A5 1F 67 F1 45 85 16 49 8A E6 34 1C 6E 80 F5 FF 13 72 85 5D C1 DE 5F 01 86 55 86 71 E8 10 33 14 70 2A 5F 15 7B 5C 65 3C 46 3A 17 79 ED 54 6A A6 C9 DF EB 2A 81 2A 80 2A 46 A2 06 DB FD D5 F3 CF 74 BB 66 56 48 D7 7C 6A 03 14 1E 55 56 E4 B6 FA 38 2B 5D FB 87 9F 9E 78 21 87 C0 0C 63 3E 8D 0F E2 A7 19 10 9B 15 E1 11 87 49 33 49 B8 66 32 28 7C 87 F5 D2 2E C5 F3 66 2F 79 EF 40 5A D4 14 85 74 5F 06 43 50 CD DE 84 E7 3C 7D 8E 8A 49 CC 5A CF 73 A1 8A 13 FF 37 13 3D AD 57 D8 51 22 D6 32 1F C0 68 4C A0 5B DD 5F 78 C8 9F 2D 3A A2 B8 1E 4A E4 08 55 64 05 E6 94 FB EB 03 6A 0A BE 83 18 94 D4 B6 C3 F2 58 9C 7A 24 DD D1 3A B7 3A B0 BB

	E5 D1 28 AB AD 24 54 72 0E 76 D2 89 32 EA 46 D3 78 D0 A9 67 78 C1 2D 18 B0 33 DE DB 27 CC B0 7C C9 A4 BD DF 2B 64 10 32 44 06 81 21 B3 BA CF 33 85 49 1E 86 4C BD F2 3D 34 EF D6 23 7A 9F 2C DA 84 F0 83 83 71 7D DA 6E 44 96 CD 1D 05 DE 30 F6 1E 2F 9C 99 9C 60 07
Public Exponent e	03

Table D.2

Table D.3 and Table D.4 provide the facsimile certificates ($cert_{rx}$) for receivers R1 and R2.

As provided in Table 2.1 of High-bandwidth Digital Content Protection System, Revision 2.2, Mapping HDCP to DisplayPort specification, the certificate format consists of 40-bit Receiver ID, followed by 1048-bit Receiver Public Key, 4-bit Reserved2, 12-bit Reserved1 and 3072-bit Signature fields. All values are stored in big-endian format.

For example, in Table D.3, 0x745bb8bd04 is the Receiver ID which is followed by Receiver Public Key, Reserved2, Reserved1 and Signature fields.

	Value (Sequence of Hexadecimal bytes) for R1
Certificate ($cert_{rx}$)	74 5b b8 bd 04 af b5 c5 c6 7b c5 3a 34 90 a9 54 c0 8f b7 eb a1 54 d2 4f 22 de 83 f5 03 a6 c6 68 46 9b c0 b8 c8 6c db 26 f9 3c 49 2f 02 e1 71 df 4e f3 0e c8 bf 22 9d 04 cf bf a9 0d ff 68 ab 05 6f 1f 12 8a 68 62 eb fe c9 ea 9f a7 fb 8c ba b1 bd 65 ac 35 9c a0 33 b1 dd a6 05 36 af 00 a2 7f bc 07 b2 dd b5 cc 57 5c dc c0 95 50 e5 ff 1f 20 db 59 46 fa 47 c4 ed 12 2e 9e 22 bd 95 a9 85 59 a1 59 3c c7 83 01 00 01 10 00 0b a3 73 77 dd 03 18 03 8a 91 63 29 1e a2 95 74 42 90 78 d0 67 25 b6 32 2f cc 23 2b ad 21 39 3d 14 ba 37 a3 65 14 6b 9c cf 61 20 44 a1 07 bb cf c3 4e 95 5b 10 cf c7 6f f1 c3 53 7c 63 a1 8c b2 e8 ab 2e 96 97 c3 83 99 70 d3 dc 21 41 f6 0a d1 1a ee f4 cc eb fb a6 aa b6 9a af 1d 16 5e e2 83 a0 4a 41 f6 7b 07 bf 47 85 28 6c a0 77 a6 a3 d7 85 a5 c4 a7 e7 6e b5 1f 40 72 97 fe c4 81 23 a0 c2 90 b3 49 24 f5 b7 90 2c bf fe 04 2e 00 a9 5f 86 04 ca c5 3a cc 26 d9 39 7e a9 2d 28 6d c0 cc 6e 81 9f b9 b7 11 33 32 23 47 98 43 0d a5 1c 59 f3 cd d2 4a b7 3e 69 d9

	21 53 9a f2 6e 77 62 ae 50 da 85 c6 aa c4 b5 1c cd a8 a5 dd 6e 62 73 ff 5f 7b d7 3c 17 ba 47 0c 89 0e 62 79 43 94 aa a8 47 f4 4c 38 89 a8 81 ad 23 13 27 0c 17 cf 3d 83 84 57 36 e7 22 26 2e 76 fd 56 80 83 f6 70 d4 5c 91 48 84 7b 18 db 0e 15 3b 49 26 23 e6 a3 e2 c6 3a 23 57 66 b0 72 b8 12 17 4f 86 fe 48 0d 53 ea fe 31 48 7d 86 de eb 82 86 1e 62 03 98 59 00 37 eb 61 e9 f9 7a 40 78 1c ba bc 0b 88 fb fd 9d d5 01 11 94 e0 35 be 33 e8 e5 36 fb 9c 45 cb 75 af d6 35 ff 78 92 7f a1 7c a8 fc b7 f7 a8 52 a9 c6 84 72 3d 1c c9 df 35 c6 e6 00 e1 48 72 ce 83 1b cc f8 33 2d 4f 98 75 00 3c 41 df 7a ed 38 53 b1

Table D.3

	Value (Sequence of Hexadecimal bytes) for R2
Certificate ($cert_{rx}$)	8b a4 47 42 fb e4 68 63 8a da 97 2d de 9a 8d 1c b1 65 4b 85 8d e5 46 d6 db 95 a5 f6 66 74 ea 81 0b 9a 58 58 66 26 86 a6 b4 56 2b 29 43 e5 bb 81 74 86 a7 b7 16 2f 07 ec d1 b5 f9 ae 4f 98 89 a9 91 7d 58 5b 8d 20 d5 c5 08 40 3b 86 af f4 d6 b9 20 95 e8 90 3b 8f 9f 36 5b 46 b6 d4 1e f5 05 88 80 14 e7 2c 77 5d 6e 54 e9 65 81 5a 68 92 a5 d6 40 78 11 97 65 d7 64 36 5e 8d 2a 87 a8 eb 7d 06 2c 10 f8 0a 7d 01 00 01 10 00 06 40 99 8f 5a 54 71 23 a7 6a 64 3f bd dd 52 b2 79 6f 88 26 94 9e af a4 de 7d 8d 88 10 c8 f6 56 f0 8f 46 28 48 55 51 c5 af a1 a9 9d ac 9f b1 26 4b eb 39 ad 88 46 af bc 61 a8 7b f9 7b 3e e4 95 d9 a8 79 48 51 00 be a4 b6 96 7f 3d fd 76 a6 b7 bb b9 77 dc 54 fb 52 9c 79 8f ed d4 b1 bc 0f 7e b1 7e 70 6d fc b9 7e 66 9a 86 23 3a 98 5e 32 8d 75 18 54 64 36 dd 92 01 39 90 b9 e3 af 6f 98 a5 c0 80 c6 2f a1 02 ad 8d f4 d6 66 7b 45 e5 74 18 b1 27 24 01 1e ea d8 f3 79 92 e9 03 f5 57 8d 65 2a 8d 1b f0 da 58 3f 58 a0 f4 b4 be cb 21 66 e9 21 7c 76 f3 c1 7e 2e 7c 3d 61 20 1d c5 c0 71 28 2e b7 0f 1f 7a c1 d3 6a 1e a3 54 34 8e 0d d7 96 93 78 50 c1 ee 27 72 3a bd 57 22 f0 d7 6d 9d 65 c4 07 9c 82 a6 d4 f7 6b 9a e9 c0 6c 4a 4f 6f be 8e 01 37 50 3a 66 d9 e9 d9 f9 06 9e 00 a9 84 a0 18 b3 44 21 24 a3 6c cd b7 0f 31 2a e8 15 b6 93 6f b9 86 e5 28 01 1a 5e 10 3f 1f 4d 35 a2 8d b8 54 26 68 3a cd cb 5f fa 37 4a 60 10 b1 0a fe ba 9b 96 5d 7e 99 cf 01 98 65 87 ad 40 d5 82 1d 61 54 a2 d3 16 3e f7 e3 05 89 8d 8a 50 87 47 be 29 18 01 b7 c3 dd 43 23 7a cd 85 1d 4e a9 c0 1a a4 77 ab e7 31 9a 33 1b 7a 86 e1 e5 ca 0c 43 1a fa ec 4c 05 c6

	d1 43 12 f9 4d 3e f7 d6 05 9c 1c dd

Table D.4

Table D.5 and Table D.6 provide the private keys for receivers R1 and R2.

	Value in Hex for R1
P	ec be e5 5b 9e 7a 50 8a 96 80 c8 db b0 ed 44 f2 ba 1d 5d 80 c1 c8 b3 c2 74 de ee 28 ec dc 78 c8 67 53 07 f2 f8 75 9c 4c a5 6c 48 94 c8 eb ad d7 7d d2 ea df 74 20 62 c9 81 a8 3c 36 b9 ea 40 fd
Q	be 00 19 76 c6 b4 ba 19 d4 69 fa 4d e2 f8 30 27 36 2b 4c c4 34 ab d3 d9 8c d6 b8 0d 37 5e 59 4b 76 70 68 2b 1f 4c 3d 47 5f a5 b1 cd 74 56 88 fe 7c f8 3b 30 6f fd c3 ed 87 3c a1 53 84 c3 d2 7f
d mod (p-1)	60 71 9b e9 e8 f3 97 1f fe 13 d4 bf 7a a2 0d f6 7b cf 3e aa 17 47 75 c3 7f ec d9 44 9e c9 6a 02 e9 e4 af 56 51 d5 47 a9 09 b2 c5 16 a7 8b 2b 34 a0 33 6e 2f 3d 95 7b e8 ef 02 e4 14 bf 44 28 d9
d mod (q-1)	10 0e 2e 18 ad 5d e4 43 fe 81 1e 17 aa d0 52 31 5e 10 76 a2 35 d9 37 43 b0 f5 0c 04 81 e3 45 24 6d 53 be 59 b6 81 58 c4 49 3e d5 31 89 5d 2e a2 62 a9 0f 47 5e 8f 51 19 27 4e 66 4b 8a 72 89 bd
q^-1 mod p	3e 53 0a f4 8e 75 e1 52 c6 24 e9 f7 bb ac 3f 22 5f e8 e0 79 35 ff 91 ee 22 56 d2 00 68 32 c4 e1 5f ff f8 b1 1d ee dc 57 81 d1 ab 8b 37 22 e3 9f d0 a1 c1 ce 1d d0 24 23 a0 0e f7 a6 db a3 ea d3

Table D.5

	Value in Hex for R2
P	f5 f6 fa 44 a2 16 2f a7 1f 7f 16 05 99 26 c4 1b 80 7f fa 52 4e 3e aa 3d 1e b0 f1 9a c6 3d 8f 57 2b 9e cd e8 03 d6 f3 91 75 e2 19 44 9e 11 58 5f d6 88 7c c4 c1 5b 45 9b 84 cf 72 1d 35 bf 24 d5
q	ed ba 08 bf 42 2c 0e fa 3a c4 d2 c7 01 51 25 ae b0 a1 cc db 67 9b aa 50 f0 80 ac 4b 9f 5c ba 1e f4 7f a9 b3 21 8b 62 2c 36 da cd a7 4d a4 d6 44 ed b1 34 e7 69 10 77 5a 6a ff f5 63 8a 2c 43 09
d mod (p-1)	61 5a c4 6c 6e 0b 82 09 10 3a 69 29 06 19 85 fd ac ba fb 05 a0 da c4 df 34 4a ad 16 a9 e8 ab d7 c0 f8 36 5f e3 45 2d 5b 21 e1 c0 46 9c 9a 18 f4 b6 21 87 e1 08 f7 6b 71 c6 fb a5 1b 52 ae b9 91
d mod (q-1)	5a 83 7f bb 1a bd dd c2 06 c8 54 1c b3 72 ab 2f 55 4f 75 c9 80 2c 73 ef b7 72 b6 a7 60 79 14 e0 9e 65 51 3e c4 21 e6 f2 40 bc 94 9b 03 e4 24 35 40 6f 3d 5e 72 d1 73 30 39 17 55 de 5d 88 b6 c9
q^-1 mod p	bc 91 2a 93 6a 8d 24 3c d5 7d 12 3b a3 71 c7 3a f0 64 72 50 7e 18 71 e1 b4 3b 1e fc 38 ca e6 8c 16 51 97 d6 3f 04 ee 23 8b 45 0c 4b 98 36 18 27 29 1b 4d 73 7e e8 b0 1a c7 fb 5c ea 78 d0 6e 97

Table D.6

Table D.7 provides the global constant (lc_{128}) used for receivers R1 and R2. Note that the same global constant is used in T1, R1 and R2.

	Value in Hex for R1	Value in Hex for R2
Global Constant lc_{128}	93 ce 5a 56 a0 a1 f4 f7 3c 65 8a 1b d2 ae f0 f7	93 ce 5a 56 a0 a1 f4 f7 3c 65 8a 1b d2 ae f0 f7

Table D.7

D.2 Authentication Protocol

Table D.8 provides test vectors generated during the authentication protocol between T1-R1 and T1-R2. The values provided in the table are as generated or received on the transmitter (T1) side.

	Value in Hex for R1	Value in Hex for R2
Authentication and Key Exchange (Without stored k_m)		
r_{tx}	18 fa e4 20 6a fb 51 49	f9 f1 30 a8 2d 5b e5 c3
Receiver ID(Extracted from certificate $cert_{rx}$)	74 5b b8 bd 04	8b a4 47 42 fb
RxCaps	02 00 03 (Device is an HDCP Repeater, *RxCaps*.REPEATER is set to one)	02 00 02 (Device is not an HDCP Repeater, *RxCaps*.REPEATER is zero)
TxCaps	02 00 00	02 00 00
Certificate signature verification	Hash: 4d d6 ef 0f 5a dd d4 82 a8 ce bc 62 1d c3 b5 f0 50 f6 39 f1 d3 8b a6 a4 4f ca 58 4b 45 a9 e9 39 Encoded Message EM: 00 01 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff f f ff ff ff ff ff ff ff ff ff ff ff	Hash: 08 fe 9c 34 64 c3 ca 9a 76 38 43 b0 61 4f 55 b4 db 7b 9b 3e c2 8f 72 09 04 0e 81 4e 5c 2e 75 bd Encoded Message EM: 00 01 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff

	ff ff ff ff ff ff	ff ff ff ff ff ff
	ff ff ff ff ff ff	ff ff ff ff ff ff
	ff ff ff ff ff ff	ff ff ff ff ff ff
	ff ff ff ff ff ff	ff ff ff ff ff ff
	ff ff ff ff ff ff	ff ff ff ff ff ff
	ff ff ff ff ff ff	ff ff ff ff ff ff
	ff ff ff ff ff ff	ff ff ff ff ff ff
	ff ff ff ff ff ff	ff ff ff ff ff ff
	ff ff ff ff ff ff	ff ff ff ff ff ff
	ff ff ff ff ff ff	ff ff ff ff ff ff
	ff ff ff ff ff ff	ff ff ff ff ff ff
	ff ff ff ff ff ff	ff ff ff ff ff ff
	ff ff ff ff ff ff	ff ff ff ff ff ff
	ff ff ff ff ff ff	ff ff ff ff ff ff
	ff ff ff ff ff ff	ff ff ff ff ff ff
	ff ff ff ff ff ff	ff ff ff ff ff ff
	ff ff ff ff ff ff	ff ff ff ff ff ff
	ff ff ff ff ff ff	ff ff ff ff ff ff
	ff ff ff ff ff ff	ff ff ff ff ff ff
	ff ff ff ff ff ff	ff ff ff ff ff ff
	ff ff ff ff ff ff	ff ff ff ff ff ff
	ff ff ff ff ff ff	ff ff ff ff ff ff
	ff ff ff ff ff ff	ff ff ff ff ff ff
	ff ff ff ff ff ff	ff ff ff ff ff ff
	ff ff ff ff ff ff	ff ff ff ff ff ff
	ff ff ff ff ff ff	ff ff ff ff ff ff
	ff ff ff ff ff ff	ff ff ff ff ff ff
	ff ff ff ff ff ff	ff ff ff ff ff ff
	ff ff ff ff ff ff	ff ff ff ff ff ff
	ff ff ff ff ff ff	ff ff ff ff ff ff
	ff ff ff ff ff ff	ff ff ff ff ff ff
	ff ff ff ff ff ff	ff ff ff ff ff ff
	ff ff ff ff ff ff	ff ff ff ff ff ff
	ff ff ff ff ff ff	ff ff ff ff ff ff
	ff ff ff ff ff ff	ff ff ff ff ff ff
	ff ff ff ff ff ff	ff ff ff ff ff ff
	ff ff ff ff ff ff	ff ff ff ff ff ff
	ff ff ff ff ff ff	ff ff ff ff ff ff
	ff ff ff ff ff ff	ff ff ff ff ff ff
	ff ff ff ff ff ff	ff ff ff ff ff ff
	ff ff ff ff ff ff	ff ff ff ff ff ff
	ff ff ff ff ff ff	ff ff ff ff ff ff
	ff ff ff ff ff ff	ff ff ff ff ff ff
	ff ff ff ff ff ff	ff ff 00 30 31 30
	ff ff ff 00 30 31	0d 06 09 60 86 48
	30 0d 06 09 60 86	01 65 03 04 02 01
	48 01 65 03 04 02	05 00 04 20 08 fe
	01 05 00 04 20 4d	9c 34 64 c3 ca 9a
	d6 ef 0f 5a dd d4	76 38 43 b0 61 4f
	82 a8 ce bc 62 1d	55 b4 db 7b 9b 3e
	c3 b5 f0 50 f6 39	c2 8f 72 09 04 0e

	f1 d3 8b a6 a4 4f ca 58 4b 45 a9 e9 39	81 4e 5c 2e 75 bd
$kpub_{rx}$ (Extracted from certificate $cert_{rx}$)	n: af b5 c5 c6 7b c5 3a 34 90 a9 54 c0 8f b7 eb a1 54 d2 4f 22 de 83 f5 03 a6 c6 68 46 9b c0 b8 c8 6c db 26 f9 3c 49 2f 02 e1 71 df 4e f3 0e c8 bf 22 9d 04 cf bf a9 0d ff 68 ab 05 6f 1f 12 8a 68 62 eb fe c9 ea 9f a7 fb 8c ba b1 bd 65 ac 35 9c a0 33 b1 dd a6 05 36 af 00 a2 7f bc 07 b2 dd b5 cc 57 5c dc c0 95 50 e5 ff 1f 20 db 59 46 fa 47 c4 ed 12 2e 9e 22 bd 95 a9 85 59 a1 59 3c c7 83 e: 01 00 01	n: e4 68 63 8a da 97 2d de 9a 8d 1c b1 65 4b 85 8d e5 46 d6 db 95 a5 f6 66 74 ea 81 0b 9a 58 58 66 26 86 a6 b4 56 2b 29 43 e5 bb 81 74 86 a7 b7 16 2f 07 ec d1 b5 f9 ae 4f 98 89 a9 91 7d 58 5b 8d 20 d5 c5 08 40 3b 86 af f4 d6 b9 20 95 e8 90 3b 8f 9f 36 5b 46 b6 d4 1e f5 05 88 80 14 e7 2c 77 5d 6e 54 e9 65 81 5a 68 92 a5 d6 40 78 11 97 65 d7 64 36 5e 8d 2a 87 a8 eb 7d 06 2c 10 f8 0a 7d e: 01 00 01
k_m	68 bc c5 1b a9 db 1b d0 fa f1 5e 9a d8 a5 af b9	ca 9f 83 95 70 d0 d0 f9 cf e4 eb 54 7e 09 fa 3b
$E_{kpub}(km)$	Seed: 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F lhash: e3 b0 c4 42 98 fc 1c 14 9a fb f4 c8 99 6f b9 24 27 ae 41 e4 64 9b 93 4c a4 95 99 1b 78 52 b8 55 $E_{kpub}(km)$: 9b 9f 80 19 ad 0e a2 f0 dd a0 29 33 d9 6d 1c 77 31 37	Seed: 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F lhash: e3 b0 c4 42 98 fc 1c 14 9a fb f4 c8 99 6f b9 24 27 ae 41 e4 64 9b 93 4c a4 95 99 1b 78 52 b8 55 $E_{kpub}(km)$: a8 55 c2 c4 c6 be ef cd cb 9f e3 9f 2a b7 29 76 fe d8 da c9 38 fa 39 f0

	57 e0 e5 b2 bd dd 36 3e 38 4e 7d 40 78 66 97 7a 4c ce c5 c7 5d 01 57 26 cc a2 f6 de 34 dd 29 be 5e 31 e8 f 1 34 e8 1a 63 a3 6d 46 dc 0a 06 08 99 9d db 3c a2 9c 04 dd 4e d9 02 7d 20 54 ec ca 86 42 1b 18 da 30 9c c4 cb ac b4 54 de 84 68 71 53 6d 92 17 ca 08 8a 7a f9 98 9a b6 7b 22 92 ac 7d 0d 6b d6 7f 31 ab f0 10 c5 2a 0f 6d 27 a0	ab ca 8a ed 95 7b 93 b2 df d0 7d 09 9d 05 96 66 03 6e ba e0 63 0f 30 77 c2 bb e2 11 39 e5 27 78 ee 64 f2 85 36 57 c3 39 d2 7b 79 03 b7 cc 82 cb f0 62 82 43 38 09 9b 71 aa 38 a6 3f 48 12 6d 8c 5e 07 90 76 ac 90 99 51 5b 06 a5 fa 50 e4 f9 25 c3 07 12 37 64 92 d7 db d3 34 1c e4 fa dd 09 e6 28 3d 0c ad a9 d8 e1 b5
r_{rx}	3b a0 be de 0c 46 a9 91	e1 7a b0 fd 0f 54 40 52
$dkey_0$	4f 14 8d 11 dd 49 18 10 6f ab 16 6f f6 fd a6 ed	2a 04 d7 eb 0a 0b 4e 20 26 45 84 01 1e ab 0a 4a
$dkey_1$	b5 02 0c 0d f2 81 ba df e4 19 77 fa d0 ac 61 17	f9 dc 18 97 e8 ee d8 f9 ec 6a 5d 34 a9 62 02 c9
k_d	4f 14 8d 11 dd 49 18 10 6f ab 16 6f f6 fd a6 ed b5 02 0c 0d f2 81 ba df e4 19 77 fa d0 ac 61 17	2a 04 d7 eb 0a 0b 4e 20 26 45 84 01 1e ab 0a 4a f9 dc 18 97 e8 ee d8 f9 ec 6a 5d 34 a9 62 02 c9
H	2e f5 ed f8 7f d8 a3 d0 f4 a9 d8 ac 3a d0 b4 56 2e 32 19 11 41 16 f1 ef 0f 02 3d 3a 78 e2 2a c6	82 b8 1a ca ed fc 87 72 7d 17 23 53 cb 81 83 bf db ba fb 90 b2 4e 96 fe ba 6d ad 67 aa 2b 2a 56
H'	2e f5 ed f8 7f d8 a3 d0 f4 a9 d8 ac 3a d0 b4 56 2e 32 19 11 41 16 f1 ef 0f 02 3d 3a 78 e2 2a c6	82 b8 1a ca ed fc 87 72 7d 17 23 53 cb 81 83 bf db ba fb 90 b2 4e 96 fe ba 6d ad 67 aa 2b 2a 56
Pairing		
$E_{kh}(k_m)$	Hash of private = SHA256 hash on concatenation of p, q, d mod (p-1), d mod (q-1),	Hash of private = SHA256 hash on concatenation of p, q, d mod (p-1), d mod (q-1), q^-1 mod

	q^-1 mod p i.e. SHA-256(p ||q||d mod (p-1)||d mod (q-1)||q^-1 mod p): db e7 c0 f2 32 e8 dd 33 43 00 c3 9b 20 57 7a da 85 86 c7 b6 6d 9f b3 66 a0 76 0c fb c2 ab 4d 34 k_h: 85 86 c7 b6 6d 9f b3 66 a0 76 0c fb c2 ab 4d 34 $E_{kh}(k_m)$: b8 9f f9 72 6a 6f 2c 1e 29 b6 44 8d dc a3 10 bd	p i.e. SHA-256(p ||q||d mod (p-1)||d mod (q-1)||q^-1 mod p): 8a da 77 4a e0 1b 26 f8 c8 9d e1 f3 23 fd e2 15 c6 aa 14 eb b0 35 4d 50 83 f5 de 74 2a 8c 1b a2 k_h: c6 aa 14 eb b0 35 4d 50 83 f5 de 74 2a 8c 1b a2 $E_{kh}(k_m)$: e6 57 8e bc c7 68 44 87 88 8a 9b d7 d6 ae 38 be
m	18 fa e4 20 6a fb 51 49 3b a0 be de 0c 46 a9 91	f9 f1 30 a8 2d 5b e5 c3 e1 7a b0 fd 0f 54 40 52
Locality Check		
r_n	32 75 3e a8 78 a6 38 1c	a0 fe 9b b8 20 60 58 ca
L	bc 20 92 33 54 91 c1 9e a4 de 8b 30 49 c2 06 6a d8 11 a2 2a b1 46 df 74 58 47 05 a8 b7 67 fb dd	f2 0f 13 6e 85 53 c1 0c d3 dd b2 f9 6d 33 31 f9 cb 6e 97 8c cd 5e da 13 dd ea 41 44 10 9b 51 b0
L'	bc 20 92 33 54 91 c1 9e a4 de 8b 30 49 c2 06 6a d8 11 a2 2a b1 46 df 74 58 47 05 a8 b7 67 fb dd	f2 0f 13 6e 85 53 c1 0c d3 dd b2 f9 6d 33 31 f9 cb 6e 97 8c cd 5e da 13 dd ea 41 44 10 9b 51 b0
Session Key Exchange		
k_s	f3 df 1d d9 57 96 12 3f 98 97 89 b4 21 e1 2d e1	f3 df 1d d9 57 96 12 3f 98 97 89 b4 21 e1 2d e1
r_{iv}	40 2b 6b 43 c5 e8 86 d8	9a 6d 11 00 a9 b7 6f 64
$dkey_2$	bf ed 5a cb 93 28 d4 56 a9 f5 2e 0e f3 36 75 f3	45 54 97 7d 85 5d a8 c0 2a de f8 90 95 02 7d 1a
$E_{dkey}(k_s)$	4c 32 47 12 c4 be c6 69 0a c2 19 64	b6 8b 8a a4 d2 cb ba ff 53 33 c1 d9

	de 91 f1 83	bb b7 10 a9
Authentication with Repeaters		
Upstream Propagation of Topology Information		
Receiver ID$_0$	47 8e 71 e2 0f	N/A as R2 is not an HDCP Repeater
Receiver ID$_1$	35 79 6a 17 0e	
Receiver ID$_2$	74 e8 53 97 a2	
Receiver ID list	47 8e 71 e2 0f 35 79 6a 17 0e 74 e8 53 97 a2	
RxInfo *RxInfo* fields Rsvd DEPTH DEVICE_COUNT MAX_DEVS_EXCEEDED MAX_CASCADE_EXCEEDED HDCP2_LEGACY_DEVICE_DOWNSTREAM HDCP1_DEVICE_DOWNSTREAM	02 31 Values in binary 0000_b 001_b 00011_b 0_b 0_b 0_b 1_b	
seq_num_V	00 00 00	
V	63 6d c5 08 4d 6c b1 0e 93 a5 28 67 0f 34 1f 88	
V'	bc cc 7d 16 e6 bc b9 02 60 08 1d f7 4a b4 5c 8a	
Downstream Propagation of Content Stream Management Information		
STREAM_ID	00	
Type	01	
seq_num_M	00 00 00	
StreamID_Type||*seq_num_M*	00 01 00 00 00	
SHA256(k_d)	1e 6c 5c a4 40 9a 66 a6 20 96 fe cd fc f3 f6 b0 45 e4 44 6b f5 45 c8 45 2b 4a ee 48 0c 53 c4 dd	
M'	dd 26 e9 52 6e 0e 1d 69 c8 84 e4 cc c8 09 aa c7 71 e9 97 b5 61 89 09 6e 4d 94 24 c2 1b 64 58 c6	

Table D.8

Table D.9 provides an HDCP 2 facsimile SRM signed with the facsimile DCP LLC key in Table D.2. The SRM revokes Receiver IDs of receivers R1 and R2

Receiver IDs revoked	74 5b b8 bd 04, 8b a4 47 42 fb

SRM Version	00 01
SRM Value	91 00 00 01 01 00 01 91 00 80 00 00 74 5b b8 bd 04 8b a4 47 42 fb 17 07 e9 ea 61 ad b4 2e 9a 44 a9 1e 44 ba ab 6f 6b 37 27 50 bb 17 8e ad c5 7f e8 f5 21 b4 60 1e 54 80 da 2a 1a 59 f3 9d e3 98 54 43 24 70 ca 83 47 64 2d c6 26 6d 30 05 b4 ee 9b b6 69 a2 f3 7c 7d 13 cf f3 a7 c7 89 ef 50 0d 32 e1 d2 2c d1 b5 46 d6 36 44 25 52 65 06 b6 31 e7 26 d2 5c 1c 17 b7 26 6f 73 e5 8a 6e e9 db 00 27 70 11 bb 75 a0 49 30 ff 38 b3 d8 2d 03 c1 78 50 74 ca 60 aa 32 03 28 8d e4 a1 8c 62 2d f3 61 6c bf a1 9c ab b3 d7 e7 d6 dc 31 f6 74 1a ab c0 9c 6a 0a c2 65 e4 29 bd 4e 22 73 5a 2c c7 75 96 e9 7a 16 a6 70 6b 3c ba 50 60 5a 33 d5 d7 f2 76 5b 5e 2d 45 e2 0e f1 4c 6d 8d cf af 39 23 79 a5 fb ae cb 8f d8 de df db 24 20 52 10 74 ba 42 6f ad bb 3e 3a a5 ce 99 0d ff 41 a6 0f 60 7f ae 05 00 3c 2c f3 ba 5a 86 1b 04 7f 53 e5 e3 68 dc 6b 36 25 73 69 95 5d 15 37 d6 98 d6 6b a8 d0 35 37 2d 2f f1 53 90 aa 32 87 99 3b b7 33 48 0e ce e4 f1 d8 93 51 eb 98 92 e7 2d ac a2 32 fb e1 f9 f1 7d 92 26 37 5d 4c 0c f8 a2 11 4c 2a 49 b6 48 bc cc 44 01 06 cb 74 da 0d 70 fa 06 64 a6 54 e6 7c 65 34 ff 97 ed db 8a 8d 40 be fe 60 e5 0c bf 50 60 7b 16 71 bd ff c3 1b fb 15 a5 10 07 6a 5d 1a 6c fa 67 dc b3 cd a3 85 6e eb 77 5f 92 8f ee fb d5 34 58 72 b1 55
SRM Signature Verification	Hash: 3b 11 c9 ee f0 b6 ec 5b 68 34 b2 67 95 7c 2d 03 1d 83 0a d7 38 78 07 24 c9 14 c6 74 4e f6 70 b0 Encoded Message: 00 01 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff

	ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff 00 30 31 30 0d 06 09 60 86 48 01 65 03 04 02 01 05 00 04 20 3b 11 c9 ee f0 b6 ec 5b 68 34 b2 67 95 7c 2d 03 1d 83 0a d7 38 78 07 24 c9 14 c6 74 4e f6 70 b0

Table D.9

D.3 Encryption

Table D.10, D.11 and D.12 provides encryption test vectors generated by transmitter T1 for Receiver R2. The test vectors are generated for 4-lane, 2-lane and 1-lane main link configurations, respectively, in SST mode with the Type input to the HDCP Cipher set to 0x00 (Refer to Section 3.2).

4 Lane, Inter-BS spacing = 15, Inter-SR spacing = 3

	Link Clock	Stream	Stream Type	Cipher Key [127:0]	Cipher Key Name [127:0]	Encrypted Stream			
						Lane3	Lane2	Lane1	Lane0
	-3	1c1c1c1c	SR	--	--	1c	1c	1c	1c
	-2	3c3c3c3c	CP	--	--	3c	3c	3c	3c
	-1	3c3c3c3c	CP	--	--	3c	3c	3c	3c
	0	1c1c1c1c	SR	--	--	1c	1c	1c	1c
Line 1 encrypted	1	39393939	VB-ID	69cfe2f4	key0_w0	50	f6	db	cd
	2	00000000	Mvid	af464ed8	key0_w1	af	46	4e	d8
	3	00000000	Maud	29d2b86d	key0_w2	29	d2	b8	6d
	4	00000000	null stream	218b93a3	key0_w3	21	8b	93	a3
	5	00000000	null stream	3b643a4f	key1_w0	3b	64	3a	4f
	6	00000000	null stream	61d2ec7b	key1_w1	61	d2	ec	7b
	7	00000000	null stream	245b7198	key1_w2	24	5b	71	98
	8	00000000	null stream	d0fe7230	key1_w3	d0	fe	72	30
	9	00000000	null stream	c5caaccd	key2_w0	c5	ca	ac	cd
	10	00000000	null stream	a339cf1b	key2_w1	a3	39	cf	1b
	11	00000000	null stream	16cc1d5c	key2_w2	16	cc	1d	5c
	12	bcbcbcbc	BS	4bf3f06c	key2_w3	bc	bc	bc	bc
	13	3c3c3c3c	CP	83fffdd6	key3_w0	3c	3c	3c	3c
	14	3c3c3c3c	CP	a9fbd4c0	key3_w1	3c	3c	3c	3c

	15	bcbcbcbc	BS	b8b6ab60	key3_w2	bc	bc	bc	bc
Line 2 encrypted	16	39393939	VB-ID	85046ba5	key3_w3	bc	3d	52	9c
	17	00000000	Mvid	a93d210c	key4_w0	a9	3d	21	0c
	18	00000000	Maud	18081647	key4_w1	18	08	16	47
	19	00000000	null stream	c3aed66b	key4_w2	c3	ae	d6	6b
	20	00000000	null stream	7150f614	key4_w3	71	50	f6	14
	21	00000000	null stream	5493ec02	key5_w0	54	93	ec	02
	22	00000000	null stream	75a45c61	key5_w1	75	a4	5c	61
	23	00000000	null stream	4d0a6492	key5_w2	4d	0a	64	92
	24	00000000	null stream	70875305	key5_w3	70	87	53	05
	25	00000000	null stream	bc0ae724	key6_w0	bc	0a	e7	24
	26	00000000	null stream	19e1c0de	key6_w1	19	e1	c0	de
	27	bcbcbcbc	BS	4eacadd7	key6_w2	bc	bc	bc	bc
	28	3c3c3c3c	CP	576649cf	key6_w3	3c	3c	3c	3c
	29	3c3c3c3c	CP	f4493ca1	key7_w0	3c	3c	3c	3c
	30	bcbcbcbc	BS	a1b39698	key7_w1	bc	bc	bc	bc
Line 3 encrypted	31	39393939	VB-ID	8139ccb8	key7_w2	b8	0	f5	81
	32	00000000	Mvid	1cf0557a	key7_w3	1c	f0	55	7a
	33	00000000	Maud	f7fb2377	key8_w0	f7	fb	23	77
	34	00000000	null stream	3a2584a6	key8_w1	3a	25	84	a6
	35	00000000	null stream	2e2e8d7a	key8_w2	2e	2e	8d	7a
	36	00000000	null stream	807c95ce	key8_w3	80	7c	95	ce
	37	00000000	null stream	8bfe8444	key9_w0	8b	fe	84	44
	38	00000000	null stream	e9113fdb	key9_w1	e9	11	3f	db
	39	00000000	null stream	bcd89d52	key9_w2	bc	d8	9d	52
	40	00000000	null stream	4d18cf3b	key9_w3	4d	18	cf	3b
	41	00000000	null stream	aad0da4b	key10_w0	aa	d0	da	4b
	42	1c1c1c1c	SR	f1732414	key10_w1	1c	1c	1c	1c
	43	7c7c7c7c	BF	8dcca69a	key10_w2	7c	7c	7c	7c
	44	7c7c7c7c	BF	a9ebf689	key10_w3	7c	7c	7c	7c
	45	1c1c1c1c	SR	9dfdad56	key11_w0	1c	1c	1c	1c
Line 4	46	19191919	VB-ID	--	--	19	19	19	19

unencrypted									
	47	00000000	Mvid	--	--	00	00	00	00
	48	00000000	Maud	--	--	00	00	00	00
	49	00000000	null stream	--	--	00	00	00	00
	50	00000000	null stream	--	--	00	00	00	00
	51	00000000	null stream	--	--	00	00	00	00
	52	00000000	null stream	--	--	00	00	00	00
	53	00000000	null stream	--	--	00	00	00	00
	54	00000000	null stream	--	--	00	00	00	00
	55	00000000	null stream	--	--	00	00	00	00
	56	00000000	null stream	--	--	00	00	00	00
	57	bcbcbcbc	BS	--	--	bc	bc	bc	bc
	58	7c7c7c7c	BF	--	--	7c	7c	7c	7c
	59	7c7c7c7c	BF	--	--	7c	7c	7c	7c
	60	bcbcbcbc	BS	--	--	bc	bc	bc	bc
Line 5 unencrypted	61	19191919	VB-ID	--	--	19	19	19	19
	62	00000000	Mvid	--	--	00	00	00	00
	63	00000000	Maud	--	--	00	00	00	00
	64	00000000	null stream	--	--	00	00	00	00
	65	00000000	null stream	--	--	00	00	00	00
	66	00000000	null stream	--	--	00	00	00	00
	67	00000000	null stream	--	--	00	00	00	00
	68	00000000	null stream	--	--	00	00	00	00
	69	00000000	null stream	--	--	00	00	00	00
	70	00000000	null stream	--	--	00	00	00	00
	71	00000000	null stream	--	--	00	00	00	00
	72	bcbcbcbc	BS	--	--	bc	bc	bc	bc
	73	7c7c7c7c	BF	--	--	7c	7c	7c	7c
	74	7c7c7c7c	BF	--	--	7c	7c	7c	7c
	75	bcbcbcbc	BS	--	--	bc	bc	bc	bc
Line 6 unencrypted	76	19191919	VB-ID	--	--	19	19	19	19
	77	00000000	Mvid	--	--	00	00	00	00

	78	00000000	Maud	--	--	00	00	00	00
	79	00000000	null stream	--	--	00	00	00	00
	80	00000000	null stream	--	--	00	00	00	00
	81	00000000	null stream	--	--	00	00	00	00
	82	00000000	null stream	--	--	00	00	00	00
	83	00000000	null stream	--	--	00	00	00	00
	84	00000000	null stream	--	--	00	00	00	00
	85	00000000	null stream	--	--	00	00	00	00
	86	00000000	null stream	--	--	00	00	00	00
	87	1c1c1c1c	SR	--	--	1c	1c	1c	1c
	88	3c3c3c3c	CP	--	--	3c	3c	3c	3c
	89	3c3c3c3c	CP	--	--	3c	3c	3c	3c
	90	1c1c1c1c	SR	--	--	1c	1c	1c	1c
Line 7 encrypted	91	39393939	VB-ID	a848e938	key11_w1	91	71	d0	01
	92	00000000	Mvid	7dac8830	key11_w2	7d	ac	88	30
	93	00000000	Maud	ed4fbedb	key11_w3	ed	4f	be	db
	94	00000000	null stream	b6c43464	key12_w0	b6	c4	34	64
	95	00000000	null stream	85efb23a	key12_w1	85	ef	b2	3a
	96	00000000	null stream	e921d3a8	key12_w2	e9	21	d3	a8
	97	00000000	null stream	aa67e16b	key12_w3	aa	67	e1	6b
	98	00000000	null stream	0d49ff31	key13_w0	0d	49	ff	31

Table D.10

	2 Lane, Inter-BS spacing = 18						
	Link Clock	**Stream**	**Stream Type**	**Cipher Key [127:0]**	**Cipher Key Name [127:0]**	**Encrypted Stream**	
						Lane1	**Lane0**
	-3	1c1c	SR	--	--	1c	1c
	-2	3c3c	CP	--	--	3c	3c
	-2	3c3c	CP	--	--	3c	3c
	0	1c1c	SR	--	--	1c	1c
Line 1 encrypted	1	3939	VB-ID	e2f4	key0_w0_0	db	cd
	2	0000	Mvid	69cf	key0_w0_1	69	cf
	3	0000	Maud	4ed8	key0_w1_0	4e	d8

	4	3939	VB-ID	af46	key0_w1_1	96	7f
	5	0000	Mvid	b86d	key0_w2_0	b8	6d
	6	0000	Maud	29d2	key0_w2_1	29	d2
	7	0000	null stream	93a3	key0_w3_0	93	a3
	8	0000	null stream	218b	key0_w3_1	21	8b
	9	0000	null stream	3a4f	key1_w0_0	3a	4f
	10	0000	null stream	3b64	key1_w0_1	3b	64
	11	0000	null stream	ec7b	key1_w1_0	ec	7b
	12	0000	null stream	61d2	key1_w1_1	61	d2
	13	0000	null stream	7198	key1_w2_0	71	98
	14	0000	null stream	245b	key1_w2_1	24	5b
	15	bcbc	BS	7230	key1_w3_0	bc	bc
	16	3c3c	CP	d0fe	key1_w3_1	3c	3c
	17	3c3c	CP	accd	key2_w0_0	3c	3c
	18	bcbc	BS	c5ca	key2_w0_1	bc	bc
Line 2 encrypted	19	3939	VB-ID	cf1b	key2_w1_0	f6	22
	20	0000	Mvid	a339	key2_w1_1	a3	39
	21	0000	Maud	1d5c	key2_w2_0	1d	5c
	22	3939	VB-ID	16cc	key2_w2_1	2f	f5
	23	0000	Mvid	f06c	key2_w3_0	f0	6c
	24	0000	Maud	4bf3	key2_w3_1	4b	f3
	25	0000	null stream	fdd6	key3_w0_0	fd	d6
	26	0000	null stream	83ff	key3_w0_1	83	ff
	27	0000	null stream	d4c0	key3_w1_0	d4	c0
	28	0000	null stream	a9fb	key3_w1_1	a9	fb
	29	0000	null stream	ab60	key3_w2_0	ab	60
	30	0000	null stream	b8b6	key3_w2_1	b8	b6
	31	0000	null stream	6ba5	key3_w3_0	6b	a5
	32	0000	null stream	8504	key3_w3_1	85	04
	33	bcbc	BS	210c	key4_w0_0	bc	bc
	34	3c3c	CP	a93d	key4_w0_1	3c	3c
	35	3c3c	CP	1647	key4_w1_0	3c	3c
	36	bcbc	BS	1808	key4_w1_1	bc	bc
Line 3 encrypted	37	3939	VB-ID	d66b	key4_w2_0	ef	52

	38	0000	Mvid	c3ae	key4_w2_1	c3	ae
	39	0000	Maud	f614	key4_w3_0	f6	14
	40	3939	VB-ID	7150	key4_w3_1	48	69
	41	0000	Mvid	ec02	key5_w0_0	ec	02
	42	0000	Maud	5493	key5_w0_1	54	93
	43	0000	null stream	5c61	key5_w1_0	5c	61
	44	0000	null stream	75a4	key5_w1_1	75	a4
	45	0000	null stream	6492	key5_w2_0	64	92
	46	0000	null stream	4d0a	key5_w2_1	4d	0a
	47	0000	null stream	5305	key5_w3_0	53	05
	48	0000	null stream	7087	key5_w3_1	70	87
	49	0000	null stream	e724	key6_w0_0	e7	24
	50	0000	null stream	bc0a	key6_w0_1	bc	0a
	51	1c1c	SR	c0de	key6_w1_0	1c	1c
	52	7c7c	BF	19e1	key6_w1_1	7c	7c
	53	7c7c	BF	add7	key6_w2_0	7c	7c
	54	1c1c	SR	4eac	key6_w2_1	1c	1c
Line 4 unencrypted	55	1919	VB-ID	--	--	19	19
	56	0000	Mvid	--	--	00	00
	57	0000	Maud	--	--	00	00
	58	1919	VB-ID	--	--	19	19
	59	0000	Mvid	--	--	00	00
	60	0000	Maud	--	--	00	00
	61	0000	null stream	--	--	00	00
	62	0000	null stream	--	--	00	00
	63	0000	null stream	--	--	00	00
	64	0000	null stream	--	--	00	00
	65	0000	null stream	--	--	00	00
	66	0000	null stream	--	--	00	00
	67	0000	null stream	--	--	00	00
	68	0000	null stream	--	--	00	00
	69	bcbc	BS	--	--	bc	bc
	70	7c7c	BF	--	--	7c	7c
	71	7c7c	BF	--	--	7c	7c

	72	bcbc	BS	--	--	bc	bc
Line 5 unencrypted	73	1919	VB-ID	--	--	19	19
	74	0000	Mvid	--	--	00	00
	75	0000	Maud	--	--	00	00
	76	1919	VB-ID	--	--	19	19
	77	0000	Mvid	--	--	00	00
	78	0000	Maud	--	--	00	00
	79	0000	null stream	--	--	00	00
	80	0000	null stream	--	--	00	00
	81	0000	null stream	--	--	00	00
	82	0000	null stream	--	--	00	00
	83	0000	null stream	--	--	00	00
	84	0000	null stream	--	--	00	00
	85	0000	null stream	--	--	00	00
	86	0000	null stream	--	--	00	00
	87	bcbc	BS	--	--	bc	bc
	88	7c7c	BF	--	--	7c	7c
	89	7c7c	BF	--	--	7c	7c
	90	bcbc	BS	--	--	bc	bc
Line 6 unencrypted	91	1919	VB-ID	--	--	19	19
	92	0000	Mvid	--	--	00	00
	93	0000	Maud	--	--	00	00
	94	1919	VB-ID	--	--	19	19
	95	0000	Mvid	--	--	00	00
	96	0000	Maud	--	--	00	00
	97	0000	null stream	--	--	00	00
	98	0000	null stream	--	--	00	00
	99	0000	null stream	--	--	00	00
	100	0000	null stream	--	--	00	00
	101	0000	null stream	--	--	00	00
	102	0000	null stream	--	--	00	00
	103	0000	null stream	--	--	00	00
	104	0000	null stream	--	--	00	00
	105	1c1c	SR	--	--	1c	1c

	106	3c3c	CP	--	--	3c	3c
	107	3c3c	CP	--	--	3c	3c
	108	1c1c	SR	--	--	1c	1c
Line 7 encrypted	109	3939	VB-ID	49cf	key6_w3_0	70	f6
	110	0000	Mvid	5766	key6_w3_1	57	66
	111	0000	Maud	3ca1	key7_w0_0	3c	a1
	112	3939	VB-ID	f449	key7_w0_1	cd	70
	113	0000	Mvid	9698	key7_w1_0	96	98
	114	0000	Maud	a1b3	key7_w1_1	a1	b3
	115	0000	null stream	ccb8	key7_w2_0	cc	b8
	116	0000	null stream	8139	key7_w2_1	81	39
	117	0000	null stream	557a	key7_w3_0	55	7a
	118	0000	null stream	1cf0	key7_w3_1	1c	f0
	119	0000	null stream	2377	key8_w0_0	23	77

Table D.11

	1 Lane, Inter-BS spacing = 24					
	Link Clock	**Stream**	**Stream Type**	**Cipher Key [127:0]**	**Cipher Key Name [127:0]**	**Encrypted Stream**
						Lane0
	-3	1c	SR	--	--	1c
	-2	3c	CP	--	--	3c
	-2	3c	CP	--	--	3c
	0	1c	SR	--	--	1c
Line 1 encrypted	1	39	VB-ID	f4	key0_b0	cd
	2	00	Mvid	e2	key0_b1	e2
	3	00	Maud	cf	key0_b2	cf
	4	39	VB-ID	69	key0_b3	50
	5	00	Mvid	d8	key0_b4	d8
	6	00	Maud	4e	key0_b5	4e
	7	39	VB-ID	46	key0_b6	7f
	8	00	Mvid	af	key0_b7	af
	9	00	Maud	6d	key0_b8	6d
	10	39	VB-ID	b8	key0_b9	81
	11	00	Mvid	d2	key0_b10	d2
	12	00	Maud	29	key0_b11	29
	13	00	null stream	a3	key0_b12	a3
	14	00	null stream	93	key0_b13	93
	15	00	null stream	8b	key0_b14	8b

	16	00	null stream	21	key0_b15	21
	17	00	null stream	4f	key1_b0	4f
	18	00	null stream	3a	key1_b1	3a
	19	00	null stream	64	key1_b2	64
	20	00	null stream	3b	key1_b3	3b
	21	bc	BS	7b	key1_b4	bc
	22	3c	CP	ec	key1_b5	3c
	23	3c	CP	d2	key1_b6	3c
	24	bc	BS	61	key1_b7	bc
Line 2 encrypted	25	39	VB-ID	98	key1_b8	a1
	26	00	Mvid	71	key1_b9	71
	27	00	Maud	5b	key1_b10	5b
	28	39	VB-ID	24	key1_b11	1d
	29	00	Mvid	30	key1_b12	30
	30	00	Maud	72	key1_b13	72
	31	39	VB-ID	fe	key1_b14	c7
	32	00	Mvid	d0	key1_b15	d0
	33	00	Maud	cd	key2_b0	cd
	34	39	VB-ID	ac	key2_b1	95
	35	00	Mvid	ca	key2_b2	ca
	36	00	Maud	c5	key2_b3	c5
	37	00	null stream	1b	key2_b4	1b
	38	00	null stream	cf	key2_b5	cf
	39	00	null stream	39	key2_b6	39
	40	00	null stream	a3	key2_b7	a3
	41	00	null stream	5c	key2_b8	5c
	42	00	null stream	1d	key2_b9	1d
	43	00	null stream	cc	key2_b10	cc
	44	00	null stream	16	key2_b11	16
	45	bc	BS	6c	key2_b12	bc
	46	3c	CP	f0	key2_b13	3c
	47	3c	CP	f3	key2_b14	3c
	48	bc	BS	4b	key2_b15	bc
Line 3 encrypted	49	39	VB-ID	d6	key3_b0	ef
	50	00	Mvid	fd	key3_b1	fd
	51	00	Maud	ff	key3_b2	ff

	52	39	VB-ID	83	key3_b3	ba
	53	00	Mvid	c0	key3_b4	c0
	54	00	Maud	d4	key3_b5	d4
	55	39	VB-ID	fb	key3_b6	c2
	56	00	Mvid	a9	key3_b7	a9
	57	00	Maud	60	key3_b8	60
	58	39	VB-ID	ab	key3_b9	92
	59	00	Mvid	b6	key3_b10	b6
	60	00	Maud	b8	key3_b11	b8
	61	00	null stream	a5	key3_b12	a5
	62	00	null stream	6b	key3_b13	6b
	63	00	null stream	04	key3_b14	04
	64	00	null stream	85	key3_b15	85
	65	00	null stream	0c	key4_b0	0c
	66	00	null stream	21	key4_b1	21
	67	00	null stream	3d	key4_b2	3d
	68	00	null stream	a9	key4_b3	a9
	69	1c	SR	47	key4_b4	47
	70	7c	BF	16	key4_b5	16
	71	7c	BF	08	key4_b6	08
	72	1c	SR	18	key4_b7	18
Line 4 unencrypted	73	19	VB-ID	--	--	19
	74	00	Mvid	--	--	00
	75	00	Maud	--	--	00
	76	19	VB-ID	--	--	19
	77	00	Mvid	--	--	00
	78	00	Maud	--	--	00
	79	19	VB-ID	--	--	19
	80	00	Mvid	--	--	00
	81	00	Maud	--	--	00
	82	19	VB-ID	--	--	19
	83	00	Mvid	--	--	00
	84	00	Maud	--	--	00
	85	00	null stream	--	--	00
	86	00	null stream	--	--	00
	87	00	null stream	--	--	00
	88	00	null stream	--	--	00

	89	00	null stream	--	--	00
	90	00	null stream	--	--	00
	91	00	null stream	--	--	00
	92	00	null stream	--	--	00
	93	bc	BS	--	--	bc
	94	7c	BF	--	--	7c
	95	7c	BF	--	--	7c
	96	bc	BS	--	--	bc
Line 5 unencrypted	97	19	VB-ID	--	--	19
	98	00	Mvid	--	--	00
	99	00	Maud	--	--	00
	100	19	VB-ID	--	--	19
	101	00	Mvid	--	--	00
	102	00	Maud	--	--	00
	103	19	VB-ID	--	--	19
	104	00	Mvid	--	--	00
	105	00	Maud	--	--	00
	106	19	VB-ID	--	--	19
	107	00	Mvid	--	--	00
	108	00	Maud	--	--	00
	109	00	null stream	--	--	00
	110	00	null stream	--	--	00
	111	00	null stream	--	--	00
	112	00	null stream	--	--	00
	113	00	null stream	--	--	00
	114	00	null stream	--	--	00
	115	00	null stream	--	--	00
	116	00	null stream	--	--	00
	117	bc	BS	--	--	bc
	118	7c	BF	--	--	7c
	119	7c	BF	--	--	7c
	120	bc	BS	--	--	bc
Line 6 unencrypted	121	19	VB-ID	--	--	19
	122	00	Mvid	--	--	00
	123	00	Maud	--	--	00
	124	19	VB-ID	--	--	19
	125	00	Mvid	--	--	00

	126	00	Maud	--	--	00
	127	19	VB-ID	--	--	19
	128	00	Mvid	--	--	00
	129	00	Maud	--	--	00
	130	19	VB-ID	--	--	19
	131	00	Mvid	--	--	00
	132	00	Maud	--	--	00
	133	00	null stream	--	--	00
	134	00	null stream	--	--	00
	135	00	null stream	--	--	00
	136	00	null stream	--	--	00
	137	00	null stream	--	--	00
	138	00	null stream	--	--	00
	139	00	null stream	--	--	00
	140	00	null stream	--	--	00
	141	1c	SR	--	--	1c
	142	3c	CP	--	--	3c
	143	3c	CP	--	--	3c
	144	1c	SR	--	--	1c
Line 7 encrypted	145	39	VB-ID	6b	key4_b8	52
	146	00	Mvid	d6	key4_b9	d6
	147	00	Maud	ae	key4_b10	ae
	148	39	VB-ID	c3	key4_b11	fa
	149	00	Mvid	14	key4_b12	14
	150	00	Maud	f6	key4_b13	f6
	151	39	VB-ID	50	key4_b14	69
	152	00	Mvid	71	key4_b15	71
	153	00	Maud	02	key5_b0	02
	154	39	VB-ID	ec	key5_b1	d5
	155	00	Mvid	93	key5_b2	93
	156	00	Maud	54	key5_b3	54
	157	00	null stream	61	key5_b4	61
	158	00	null stream	5c	key5_b5	5c
	159	00	null stream	a4	key5_b6	a4
	160	00	null stream	75	key5_b7	75
	161	00	null stream	92	key5_b8	92

Table D.12

Table D.13, D.14 and D.15 provides encryption test vectors generated by transmitter T1 for Receiver R2. The test vectors are generated for 4-lane, 2-lane and 1-lane main link configurations, respectively, in SST mode with the Type input to the HDCP Cipher set to 0x01 (Refer to Section 3.2).

4 Lane, Inter-BS spacing = 15, Inter-SR spacing = 3									
	Link Clock	Stream	Stream Type	Cipher Key [127:0]	Cipher Key Name [127:0]	Encrypted Stream			
						Lane3	Lane2	Lane1	Lane0
	-3	1c1c1c1c	SR	--	--	1c	1c	1c	1c
	-2	3c3c3c3c	CP	--	--	3c	3c	3c	3c
	-1	3c3c3c3c	CP	--	--	3c	3c	3c	3c
	0	1c1c1c1c	SR	--	--	1c	1c	1c	1c
Line 1 encrypted	1	39393939	VB-ID	f2d19ee4	key0_w0	cb	e8	a7	dd
	2	00000000	Mvid	8d97b2da	key0_w1	8d	97	b2	da
	3	00000000	Maud	b1705349	key0_w2	b1	70	53	49
	4	00000000	null stream	214c1eb0	key0_w3	21	4c	1e	b0
	5	00000000	null stream	f2d3c2c0	key1_w0	f2	d3	c2	c0
	6	00000000	null stream	87f39b60	key1_w1	87	f3	9b	60
	7	00000000	null stream	fe935293	key1_w2	fe	93	52	93
	8	00000000	null stream	6dda674c	key1_w3	6d	da	67	4c
	9	00000000	null stream	fab7598d	key2_w0	fa	b7	59	8d
	10	00000000	null stream	b7083eb3	key2_w1	b7	08	3e	b3
	11	00000000	null stream	f729a5ee	key2_w2	f7	29	a5	ee
	12	bcbcbcbc	BS	1e436134	key2_w3	bc	bc	bc	bc
	13	3c3c3c3c	CP	643aee5e	key3_w0	3c	3c	3c	3c
	14	3c3c3c3c	CP	2fca1d7c	key3_w1	3c	3c	3c	3c
	15	bcbcbcbc	BS	bdd265f4	key3_w2	bc	bc	bc	bc
Line 2 encrypted	16	39393939	VB-ID	9877cbf9	key3_w3	a1	4e	f2	c0
	17	00000000	Mvid	cf16b1aa	key4_w0	cf	16	b1	aa
	18	00000000	Maud	cd18ba83	key4_w1	cd	18	ba	83
	19	00000000	null stream	461f352b	key4_w2	46	1f	35	2b

	20	00000000	null stream	ee18d5ad	key4_w3	ee	18	d5	ad
	21	00000000	null stream	a0585757	key5_w0	a0	58	57	57
	22	00000000	null stream	c55ffc47	key5_w1	c5	5f	fc	47
	23	00000000	null stream	b9d95384	key5_w2	b9	d9	53	84
	24	00000000	null stream	02ebaf35	key5_w3	02	eb	af	35
	25	00000000	null stream	e85d8e5d	key6_w0	e8	5d	8e	5d
	26	00000000	null stream	417aacb3	key6_w1	41	7a	ac	b3
	27	bcbcbcbc	BS	6820b5f7	key6_w2	bc	bc	bc	bc
	28	3c3c3c3c	CP	7933aef5	key6_w3	3c	3c	3c	3c
	29	3c3c3c3c	CP	989e0649	key7_w0	3c	3c	3c	3c
	30	bcbcbcbc	BS	9b1aee75	key7_w1	bc	bc	bc	bc
Line 3 encrypted	31	39393939	VB-ID	cd09c7fa	key7_w2	f4	30	fe	c3
	32	00000000	Mvid	d1994b82	key7_w3	d1	99	4b	82
	33	00000000	Maud	080eeadc	key8_w0	08	0e	ea	dc
	34	00000000	null stream	7c6eb859	key8_w1	7c	6e	b8	59
	35	00000000	null stream	8b223dcf	key8_w2	8b	22	3d	cf
	36	00000000	null stream	9567f928	key8_w3	95	67	f9	28
	37	00000000	null stream	c6eed14d	key9_w0	c6	ee	d1	4d
	38	00000000	null stream	237450000	key9_w1	02	37	45	e4
	39	00000000	null stream	b33d3067	key9_w2	b3	3d	30	67
	40	00000000	null stream	5b9749ef	key9_w3	5b	97	49	ef
	41	00000000	null stream	eb1789c3	key10_w0	eb	17	89	c3
	42	1c1c1c1c	SR	3460077d	key10_w1	1c	1c	1c	1c
	43	7c7c7c7c	BF	ce5be2c6	key10_w2	7c	7c	7c	7c
	44	7c7c7c7c	BF	da8f478a	key10_w3	7c	7c	7c	7c
	45	1c1c1c1c	SR	33f82ab2	key11_w0	1c	1c	1c	1c
Line 4 unencrypted	46	19191919	VB-ID	--	--	19	19	19	19
	47	00000000	Mvid	--	--	00	00	00	00
	48	00000000	Maud	--	--	00	00	00	00
	49	00000000	null stream	--	--	00	00	00	00
	50	00000000	null stream	--	--	00	00	00	00

	51	00000000	null stream	--	--	00	00	00	00
	52	00000000	null stream	--	--	00	00	00	00
	53	00000000	null stream	--	--	00	00	00	00
	54	00000000	null stream	--	--	00	00	00	00
	55	00000000	null stream	--	--	00	00	00	00
	56	00000000	null stream	--	--	00	00	00	00
	57	bcbcbcbc	BS	--	--	bc	bc	bc	bc
	58	7c7c7c7c	BF	--	--	7c	7c	7c	7c
	59	7c7c7c7c	BF	--	--	7c	7c	7c	7c
	60	bcbcbcbc	BS	--	--	bc	bc	bc	bc
Line 5 unencrypted	61	19191919	VB-ID	--	--	19	19	19	19
	62	00000000	Mvid	--	--	00	00	00	00
	63	00000000	Maud	--	--	00	00	00	00
	64	00000000	null stream	--	--	00	00	00	00
	65	00000000	null stream	--	--	00	00	00	00
	66	00000000	null stream	--	--	00	00	00	00
	67	00000000	null stream	--	--	00	00	00	00
	68	00000000	null stream	--	--	00	00	00	00
	69	00000000	null stream	--	--	00	00	00	00
	70	00000000	null stream	--	--	00	00	00	00
	71	00000000	null stream	--	--	00	00	00	00
	72	bcbcbcbc	BS	--	--	bc	bc	bc	bc
	73	7c7c7c7c	BF	--	--	7c	7c	7c	7c
	74	7c7c7c7c	BF	--	--	7c	7c	7c	7c
	75	bcbcbcbc	BS	--	--	bc	bc	bc	bc
Line 6 unencrypted	76	19191919	VB-ID	--	--	19	19	19	19
	77	00000000	Mvid	--	--	00	00	00	00
	78	00000000	Maud	--	--	00	00	00	00
	79	00000000	null stream	--	--	00	00	00	00
	80	00000000	null stream	--	--	00	00	00	00
	81	00000000	null stream	--	--	00	00	00	00

	82	00000000	null stream	--	--	00	00	00	00
	83	00000000	null stream	--	--	00	00	00	00
	84	00000000	null stream	--	--	00	00	00	00
	85	00000000	null stream	--	--	00	00	00	00
	86	00000000	null stream	--	--	00	00	00	00
	87	1c1c1c1c	SR	--	--	1c	1c	1c	1c
	88	3c3c3c3c	CP	--	--	3c	3c	3c	3c
	89	3c3c3c3c	CP	--	--	3c	3c	3c	3c
	90	1c1c1c1c	SR	--	--	1c	1c	1c	1c
Line 7 encrypted	91	39393939	VB-ID	4b6aed30	key11_w1	72	53	d4	09
	92	00000000	Mvid	371d00a2	key11_w2	37	1d	00	a2
	93	00000000	Maud	ac4f116c	key11_w3	ac	4f	11	6c
	94	00000000	null stream	67175daa	key12_w0	67	17	5d	aa
	95	00000000	null stream	4b430585	key12_w1	4b	43	05	85
	96	00000000	null stream	839c59f6	key12_w2	83	9c	59	f6
	97	00000000	null stream	4b562ac6	key12_w3	4b	56	2a	c6
	98	00000000	null stream	965ef150	key13_w0	96	5e	f1	50

Table D.13

2 Lane, Inter-BS spacing = 18							
	Link Clock	**Stream**	**Stream Type**	**Cipher Key [127:0]**	**Cipher Key Name [127:0]**	**Encrypted Stream**	
						Lane1	**Lane0**
	-3	1c1c	SR	--	--	1c	1c
	-2	3c3c	CP	--	--	3c	3c
	-2	3c3c	CP	--	--	3c	3c
	0	1c1c	SR	--	--	1c	1c
Line 1 encrypted	1	3939	VB-ID	9ee4	key0_w0_0	a7	dd
	2	0000	Mvid	f2d1	key0_w0_1	f2	d1
	3	0000	Maud	b2da	key0_w1_0	b2	da
	4	3939	VB-ID	8d97	key0_w1_1	b4	ae
	5	0000	Mvid	5349	key0_w2_0	53	49
	6	0000	Maud	b170	key0_w2_1	b1	70
	7	0000	null stream	1eb0	key0_w3_0	1e	b0
	8	0000	null	214c	key0_w3_1	21	4c

			stream				
	9	0000	null stream	c2c0	key1_w0_0	c2	c0
	10	0000	null stream	f2d3	key1_w0_1	f2	d3
	11	0000	null stream	9b60	key1_w1_0	9b	60
	12	0000	null stream	87f3	key1_w1_1	87	f3
	13	0000	null stream	5293	key1_w2_0	52	93
	14	0000	null stream	fe93	key1_w2_1	fe	93
	15	bcbc	BS	674c	key1_w3_0	bc	bc
	16	3c3c	CP	6dda	key1_w3_1	3c	3c
	17	3c3c	CP	598d	key2_w0_0	3c	3c
	18	bcbc	BS	fab7	key2_w0_1	bc	bc
Line 2 encrypted	19	3939	VB-ID	3eb3	key2_w1_0	07	8a
	20	0000	Mvid	b708	key2_w1_1	b7	08
	21	0000	Maud	a5ee	key2_w2_0	a5	ee
	22	3939	VB-ID	f729	key2_w2_1	ce	10
	23	0000	Mvid	6134	key2_w3_0	61	34
	24	0000	Maud	1e43	key2_w3_1	1e	43
	25	0000	null stream	ee5e	key3_w0_0	ee	5e
	26	0000	null stream	643a	key3_w0_1	64	3a
	27	0000	null stream	1d7c	key3_w1_0	1d	7c
	28	0000	null stream	2fca	key3_w1_1	2f	ca
	29	0000	null stream	65f4	key3_w2_0	65	f4
	30	0000	null stream	bdd2	key3_w2_1	bd	d2
	31	0000	null stream	cbf9	key3_w3_0	cb	f9
	32	0000	null stream	9877	key3_w3_1	98	77
	33	bcbc	BS	b1aa	key4_w0_0	bc	bc
	34	3c3c	CP	cf16	key4_w0_1	3c	3c
	35	3c3c	CP	ba83	key4_w1_0	3c	3c
	36	bcbc	BS	cd18	key4_w1_1	bc	bc
Line 3 encrypted	37	3939	VB-ID	352b	key4_w2_0	0c	12
	38	0000	Mvid	461f	key4_w2_1	46	1f
	39	0000	Maud	d5ad	key4_w3_0	d5	ad
	40	3939	VB-ID	ee18	key4_w3_1	d7	21
	41	0000	Mvid	5757	key5_w0_0	57	57
	42	0000	Maud	a058	key5_w0_1	a0	58

	43	0000	null stream	fc47	key5_w1_0	fc	47
	44	0000	null stream	c55f	key5_w1_1	c5	5f
	45	0000	null stream	5384	key5_w2_0	53	84
	46	0000	null stream	b9d9	key5_w2_1	b9	d9
	47	0000	null stream	af35	key5_w3_0	af	35
	48	0000	null stream	02eb	key5_w3_1	02	eb
	49	0000	null stream	8e5d	key6_w0_0	8e	5d
	50	0000	null stream	e85d	key6_w0_1	e8	5d
	51	1c1c	SR	acb3	key6_w1_0	1c	1c
	52	7c7c	BF	417a	key6_w1_1	7c	7c
	53	7c7c	BF	b5f7	key6_w2_0	7c	7c
	54	1c1c	SR	6820	key6_w2_1	1c	1c
Line 4 unencrypted	55	1919	VB-ID	--	--	19	19
	56	0000	Mvid	--	--	00	00
	57	0000	Maud	--	--	00	00
	58	1919	VB-ID	--	--	19	19
	59	0000	Mvid	--	--	00	00
	60	0000	Maud	--	--	00	00
	61	0000	null stream	--	--	00	00
	62	0000	null stream	--	--	00	00
	63	0000	null stream	--	--	00	00
	64	0000	null stream	--	--	00	00
	65	0000	null stream	--	--	00	00
	66	0000	null stream	--	--	00	00
	67	0000	null stream	--	--	00	00
	68	0000	null stream	--	--	00	00
	69	bcbc	BS	--	--	bc	bc
	70	7c7c	BF	--	--	7c	7c
	71	7c7c	BF	--	--	7c	7c
	72	bcbc	BS	--	--	bc	bc
Line 5 unencrypted	73	1919	VB-ID	--	--	19	19
	74	0000	Mvid	--	--	00	00
	75	0000	Maud	--	--	00	00
	76	1919	VB-ID	--	--	19	19

	77	0000	Mvid	--	--	00	00
	78	0000	Maud	--	--	00	00
	79	0000	null stream	--	--	00	00
	80	0000	null stream	--	--	00	00
	81	0000	null stream	--	--	00	00
	82	0000	null stream	--	--	00	00
	83	0000	null stream	--	--	00	00
	84	0000	null stream	--	--	00	00
	85	0000	null stream	--	--	00	00
	86	0000	null stream	--	--	00	00
	87	bcbc	BS	--	--	bc	bc
	88	7c7c	BF	--	--	7c	7c
	89	7c7c	BF	--	--	7c	7c
	90	bcbc	BS	--	--	bc	bc
Line 6 unencrypted	91	1919	VB-ID	--	--	19	19
	92	0000	Mvid	--	--	00	00
	93	0000	Maud	--	--	00	00
	94	1919	VB-ID	--	--	19	19
	95	0000	Mvid	--	--	00	00
	96	0000	Maud	--	--	00	00
	97	0000	null stream	--	--	00	00
	98	0000	null stream	--	--	00	00
	99	0000	null stream	--	--	00	00
	100	0000	null stream	--	--	00	00
	101	0000	null stream	--	--	00	00
	102	0000	null stream	--	--	00	00
	103	0000	null stream	--	--	00	00
	104	0000	null stream	--	--	00	00
	105	1c1c	SR	--	--	1c	1c
	106	3c3c	CP	--	--	3c	3c
	107	3c3c	CP	--	--	3c	3c
	108	1c1c	SR	--	--	1c	1c
Line 7 encrypted	109	3939	VB-ID	aef5	key6_w3_0	97	cc
	110	0000	Mvid	7933	key6_w3_1	79	33

	111	0000	Maud	0649	key7_w0_0	06	49
	112	3939	VB-ID	989e	key7_w0_1	a1	a7
	113	0000	Mvid	ee75	key7_w1_0	ee	75
	114	0000	Maud	9b1a	key7_w1_1	9b	1a
	115	0000	null stream	c7fa	key7_w2_0	c7	fa
	116	0000	null stream	cd09	key7_w2_1	cd	09
	117	0000	null stream	4b82	key7_w3_0	4b	82
	118	0000	null stream	d199	key7_w3_1	d1	99
	119	0000	null stream	eadc	key8_w0_0	ea	dc

Table D.14

1 Lane, Inter-BS spacing = 24						
	Link Clock	**Stream**	**Stream Type**	**Cipher Key [127:0]**	**Cipher Key Name [127:0]**	**Encrypted Stream**
						Lane0
	-3	1c	SR	--	--	1c
	-2	3c	CP	--	--	3c
	-2	3c	CP	--	--	3c
	0	1c	SR	--	--	1c
Line 1 encrypted	1	39	VB-ID	e4	key0_b0	dd
	2	00	Mvid	9e	key0_b1	9e
	3	00	Maud	d1	key0_b2	d1
	4	39	VB-ID	f2	key0_b3	cb
	5	00	Mvid	da	key0_b4	da
	6	00	Maud	b2	key0_b5	b2
	7	39	VB-ID	97	key0_b6	ae
	8	00	Mvid	8d	key0_b7	8d
	9	00	Maud	49	key0_b8	49
	10	39	VB-ID	53	key0_b9	6a
	11	00	Mvid	70	key0_b10	70
	12	00	Maud	b1	key0_b11	b1
	13	00	null stream	b0	key0_b12	b0
	14	00	null stream	1e	key0_b13	1e
	15	00	null stream	4c	key0_b14	4c
	16	00	null stream	21	key0_b15	21
	17	00	null stream	c0	key1_b0	c0
	18	00	null stream	c2	key1_b1	c2
	19	00	null stream	d3	key1_b2	d3
	20	00	null stream	f2	key1_b3	f2
	21	bc	BS	60	key1_b4	bc
	22	3c	CP	9b	key1_b5	3c
	23	3c	CP	f3	key1_b6	3c
	24	bc	BS	87	key1_b7	bc
Line 2 encrypted	25	39	VB-ID	93	key1_b8	aa
	26	00	Mvid	52	key1_b9	52
	27	00	Maud	93	key1_b10	93
	28	39	VB-ID	fe	key1_b11	c7
	29	00	Mvid	4c	key1_b12	4c
	30	00	Maud	67	key1_b13	67
	31	39	VB-ID	da	key1_b14	e3

	32	00	Mvid	6d	key1_b15	6d
	33	00	Maud	8d	key2_b0	8d
	34	39	VB-ID	59	key2_b1	60
	35	00	Mvid	b7	key2_b2	b7
	36	00	Maud	fa	key2_b3	fa
	37	00	null stream	b3	key2_b4	b3
	38	00	null stream	3e	key2_b5	3e
	39	00	null stream	08	key2_b6	08
	40	00	null stream	b7	key2_b7	b7
	41	00	null stream	ee	key2_b8	ee
	42	00	null stream	a5	key2_b9	a5
	43	00	null stream	29	key2_b10	29
	44	00	null stream	f7	key2_b11	f7
	45	bc	BS	34	key2_b12	bc
	46	3c	CP	61	key2_b13	3c
	47	3c	CP	43	key2_b14	3c
	48	bc	BS	1e	key2_b15	bc
Line 3 encrypted	49	39	VB-ID	5e	key3_b0	67
	50	00	Mvid	ee	key3_b1	ee
	51	00	Maud	3a	key3_b2	3a
	52	39	VB-ID	64	key3_b3	5d
	53	00	Mvid	7c	key3_b4	7c
	54	00	Maud	1d	key3_b5	1d
	55	39	VB-ID	ca	key3_b6	f3
	56	00	Mvid	2f	key3_b7	2f
	57	00	Maud	f4	key3_b8	f4
	58	39	VB-ID	65	key3_b9	5c
	59	00	Mvid	d2	key3_b10	d2
	60	00	Maud	bd	key3_b11	bd
	61	00	null stream	f9	key3_b12	f9
	62	00	null stream	cb	key3_b13	cb
	63	00	null stream	77	key3_b14	77
	64	00	null stream	98	key3_b15	98
	65	00	null stream	aa	key4_b0	aa
	66	00	null stream	b1	key4_b1	b1

	67	00	null stream	16	key4_b2	16
	68	00	null stream	cf	key4_b3	cf
	69	1c	SR	83	key4_b4	83
	70	7c	BF	ba	key4_b5	ba
	71	7c	BF	18	key4_b6	18
	72	1c	SR	cd	key4_b7	cd
Line 4 unencrypted	73	19	VB-ID	--	--	19
	74	00	Mvid	--	--	00
	75	00	Maud	--	--	00
	76	19	VB-ID	--	--	19
	77	00	Mvid	--	--	00
	78	00	Maud	--	--	00
	79	19	VB-ID	--	--	19
	80	00	Mvid	--	--	00
	81	00	Maud	--	--	00
	82	19	VB-ID	--	--	19
	83	00	Mvid	--	--	00
	84	00	Maud	--	--	00
	85	00	null stream	--	--	00
	86	00	null stream	--	--	00
	87	00	null stream	--	--	00
	88	00	null stream	--	--	00
	89	00	null stream	--	--	00
	90	00	null stream	--	--	00
	91	00	null stream	--	--	00
	92	00	null stream	--	--	00
	93	bc	BS	--	--	bc
	94	7c	BF	--	--	7c
	95	7c	BF	--	--	7c
	96	bc	BS	--	--	bc
Line 5 unencrypted	97	19	VB-ID	--	--	19
	98	00	Mvid	--	--	00
	99	00	Maud	--	--	00
	100	19	VB-ID	--	--	19
	101	00	Mvid	--	--	00
	102	00	Maud	--	--	00
	103	19	VB-ID	--	--	19
	104	00	Mvid	--	--	00
	105	00	Maud	--	--	00

	106	19	VB-ID	--	--	19
	107	00	Mvid	--	--	00
	108	00	Maud	--	--	00
	109	00	null stream	--	--	00
	110	00	null stream	--	--	00
	111	00	null stream	--	--	00
	112	00	null stream	--	--	00
	113	00	null stream	--	--	00
	114	00	null stream	--	--	00
	115	00	null stream	--	--	00
	116	00	null stream	--	--	00
	117	bc	BS	--	--	bc
	118	7c	BF	--	--	7c
	119	7c	BF	--	--	7c
	120	bc	BS	--	--	bc
Line 6 unencrypted	121	19	VB-ID	--	--	19
	122	00	Mvid	--	--	00
	123	00	Maud	--	--	00
	124	19	VB-ID	--	--	19
	125	00	Mvid	--	--	00
	126	00	Maud	--	--	00
	127	19	VB-ID	--	--	19
	128	00	Mvid	--	--	00
	129	00	Maud	--	--	00
	130	19	VB-ID	--	--	19
	131	00	Mvid	--	--	00
	132	00	Maud	--	--	00
	133	00	null stream	--	--	00
	134	00	null stream	--	--	00
	135	00	null stream	--	--	00
	136	00	null stream	--	--	00
	137	00	null stream	--	--	00
	138	00	null stream	--	--	00
	139	00	null stream	--	--	00

	140	00	null stream	--	--	00
	141	1c	SR	--	--	1c
	142	3c	CP	--	--	3c
	143	3c	CP	--	--	3c
	144	1c	SR	--	--	1c
Line 7 encrypted	145	39	VB-ID	2b	key4_b8	12
	146	00	Mvid	35	key4_b9	35
	147	00	Maud	1f	key4_b10	1f
	148	39	VB-ID	46	key4_b11	7f
	149	00	Mvid	ad	key4_b12	ad
	150	00	Maud	d5	key4_b13	d5
	151	39	VB-ID	18	key4_b14	21
	152	00	Mvid	ee	key4_b15	ee
	153	00	Maud	57	key5_b0	57
	154	39	VB-ID	57	key5_b1	6e
	155	00	Mvid	58	key5_b2	58
	156	00	Maud	a0	key5_b3	a0
	157	00	null stream	47	key5_b4	47
	158	00	null stream	fc	key5_b5	fc
	159	00	null stream	5f	key5_b6	5f
	160	00	null stream	c5	key5_b7	c5
	161	00	null stream	84	key5_b8	84

Table D.15