High-bandwidth Digital Content Protection System

Amendment for HDCP on DLI

Revision 2.2

08 July, 2015

Digital Content Protection LLC

Notice

Acknowledgement

Owlink has 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

Email: info@digital-cp.com

Web: www.digital-cp.com

Revision History

July 08, 2015 - Revision 2.2: Initial Release

Table of Contents

List of Figures

HDCP Specification v2.2

Amendment for HDCP on DLI Interfaces

1. INTRODUCTION

1.1 SCOPE OF THIS DOCUMENT

This document is an amendment to the "High-bandwidth Digital Content Protection (HDCP) System: Mapping HDCP to HDMI, Rev 2.2 Specification" for implementation on a DLI interface. Herein, the term HDCP-DLI refers to this interface specification and devices employing it.

1.2 HDCP PROTECTION OF THE DLI VIDEO/AUDIO TRANSPORT SYSTEM

In a DLI system, an optical link is used to transport the uncompressed video/audio data from a DLI transmitter to a DLI receiver. The data transported over the DLI link needs to be protected. This amendment specifies the requirements and implementation of the HDCP protocol used to protect the video/audio content transported over the DLI link

1.3 DEFINITIONS

Digital Light Interface (DLI): An optical light interface that can transmit digital video, audio, and data simultaneously over a single optical light link.

HDCP-DLI Transmitter: An HDCP transmitter that uses the DLI interface to send protected data.

HDCP-DLI Receiver: An HDCP receiver that uses the DLI interface to receive protected data.

Downstream DLI Channel: The DLI communication channel that carries data from HDCP-DLI Transmitter to HDCP-DLI Receiver.

Upstream DLI Channel: The DLI communication channel that carries data from HDCP-DLI Receiver to HDCP-DLI Transmitter.

DLI Serializer: A Circuit in DLI Interface that converts 128 bit parallel data to serial data stream.

DLI Deserializer: A Circuit in DLI Interface that converts serial data stream to 128 bit parallel data.

2. AUTHENTICATION Protocols

The HDCP-DLI authentication mechanism works in the same way as that of HDCP on HDMI interface except for a few deviations. The following sections describe the differences of operation during the authentication phase.

2.1 DLI Data Packet

All data transmitted over the DLI link is in the format of packets. DLI packets are used to transmit all the protected video and audio data in the DLI downstream direction. DLI packets are also used to carry all the HDCP information exchange, key exchange and Control/Status exchange in both DLI downstream and upstream direction. In addition, DLI packets are used to carry other data that is not HDCP protected in both directions.

Each DLI packet contains a packet header and a payload of variable length. The payload could contain video data, audio data, HDCP exchange data, or other information.

Packet Header	Payload

The DLI packet header indicates packet type and payload length. The packet type can be one of the following:

- Video Packet
- Audio Packet
- I2C data packet for HDCP information, key exchange and control/Status information
- HDCP link integrity check packet
- Other packet that is not HDCP protected

2.2 Authentication and Key Exchange

The amendment does not make any change to the authentication protocol. The AKE process, pairing process, locality check, session key exchange, and all key values are kept the same as that in HDCP on HDMI interface.

2.3 Synchronization and Link Integrity Check

In the HDCP on HDMI system, HDCP Transmitter and HDCP Receiver use data island packets for link synchronization and integrity check.

In the DLI system, a special link synchronization packet shall be used for this Link Integrity check.

As in the HDCP on HDMI interface, both HDCP-DLI transmitter and HDCP-DLI receiver will keep a 64 bit *InputCtr*. HDCP-DLI transmitter and the HDCP-DLI receiver will use this *InputCtr* to synchronize the HDCP operation. This *InputCtr* is reset to 0 at session key exchange (SKE) and is incremented for every key produced.

The amendment does not make any change to the generation and operation of this *InputCtr*. However, in the DLI system, the inputCtr is passed from HDCP-DLI transmitter to HDCP-DLI receiver via the link synchronization packet at least once every video frame (VSYNC). The inputCtr value is first encrypted in the HDCP transmitter. The encrypted data is then transmitted to the HDCP receiver over DLI link. The HDCP Receiver will decrypt the received data and compare it against its locally generated inputCtr to determine if the link is in synchronization. A comparison mismatch will indicate a link synchronization error or encryption/decryption engine error.

The HDCP-DLI Receiver shall assert the REAUTH_REQ bit of the *RxStatus* register when there are 100 consecutive RX link synchronization or encryption/decryption failures. The HDCP-DLI Transmitter polls the *RxStatus* register and if it detects the REAUTH_REQ bit is set, it may initiate re-authentication.

Polling of the *RxStatus* register by the HDCP-DLI Transmitter is done at least once every second while the Transmitter is in the authenticated state.

2.4 HDCP-DLI STATE MACHINE

This amendment does not make any change to the operation and state diagram of the HDCP on HDMI transmitter and receiver.

2.5 HDCP-DLI PORT

In a HDCP on HDMI system, the HDCP related information that must be exchanged between the HDCP transmitter and HDCP receiver are communicated over the I2C serial bus of the HDCP-protected interface. The HDCP receiver must present a logical device on the I2C bus for the link that it supports. The eight bit I2C device address (including read/write bit, “x”) is 0111010x in binary, or 0x74 in the usual hexadecimal representation of I2C device address, where the read/write bit is set to zero.

In the HDCP on DLI system, I2C bus operation is transmitted over the DLI link with an I2C data packet between HDCP-DLI transmitter and HDCP-DLI receiver. It uses downstream and upstream communication channels to carry all the I2C read/write operation used for HDCP related data exchange.

In order to minimize changes from the HDCP on HDMI implementation, it keeps all the data content, offset address, and device address 0x74/0x75 unchanged. It puts all the information (address, data, and control) in the I2C data packet as payload. The packet is transmitted between HDCP-DLI transmitter and HDCP-DLI receiver.

For I2C write operations, the HDCP-DLI transmitter builds an I2C write command packet with a payload that contains device address, offset address, data length and associated data. It then sends the packet to HDCP-DLI receiver via the downstream DLI communication channel. The HDCP-DLI receiver will send back an acknowledge packet to the transmitter via the upstream DLI channel to indicate the write success.

After sending the write command packet, the HDCP-DLI transmitter expects to receive the acknowledge packet within 3 ms. If it fails to receive the acknowledgement packet after 4 ms, it declares a write failure and it will restart the same write operation.

For I2C read operations, the HDCP-DLI transmitter builds a packet with a payload that contains device address, offset address and data length to read. It then sends the packet to HDCP-DLI receiver via the downstream DLI communication channel. In response to the I2C read command packet, the HDCP-DLI receiver builds a packet with the offset address and the associated data. It then sends the packet back to the HDCP-DLI transmitter via the upstream DLI communication channel.

After sending the read command packet, the HDCP_DLI transmitter expects to receive the data packet from the HDCP_DLI receiver within 3 ms. If it fails to receive the expected data packet after 4 ms, it declares a read failure and it will start another read operation.

If the HDCP_DLI transmitter still fails to get the expected response after two retries of the same read or write operation (three times total), it will restart the authentication process from beginning. The details of the I2C write command packet, the I2C read command packet, and the I2C read acknowledge packet are in the HDCP-DLI specification.

3. DATA ENCRYPTION AND HDCP CIPHER

3.1 DLI Data Encryption

In a DLI based video/audio system, HDCP Encryption is applied on the 128 bit parallel data bus before the input of the DLI serializer at the HDCP-DLI transmitter. The decryption is applied on the 128 bit parallel data bus after the output of the DLI deserializer at the HDCP-DLI receiver. Using the same methods as that in a standard HDCP implementation, HDCP encryption consists of a bitwise exclusive-OR (XOR) of the parallel data with pseudo-random data stream provided by the HDCP Cipher module.

Figure 1 shows the circuit diagram of the HDCP-DLI encryption. It is the same as that in Figure 3-1 of HDCP Specification V2.2 except that the TMDS link is replaced by the DLI link. The parallel data bus width is a standard 128 bit which is used for DLI data transmission.

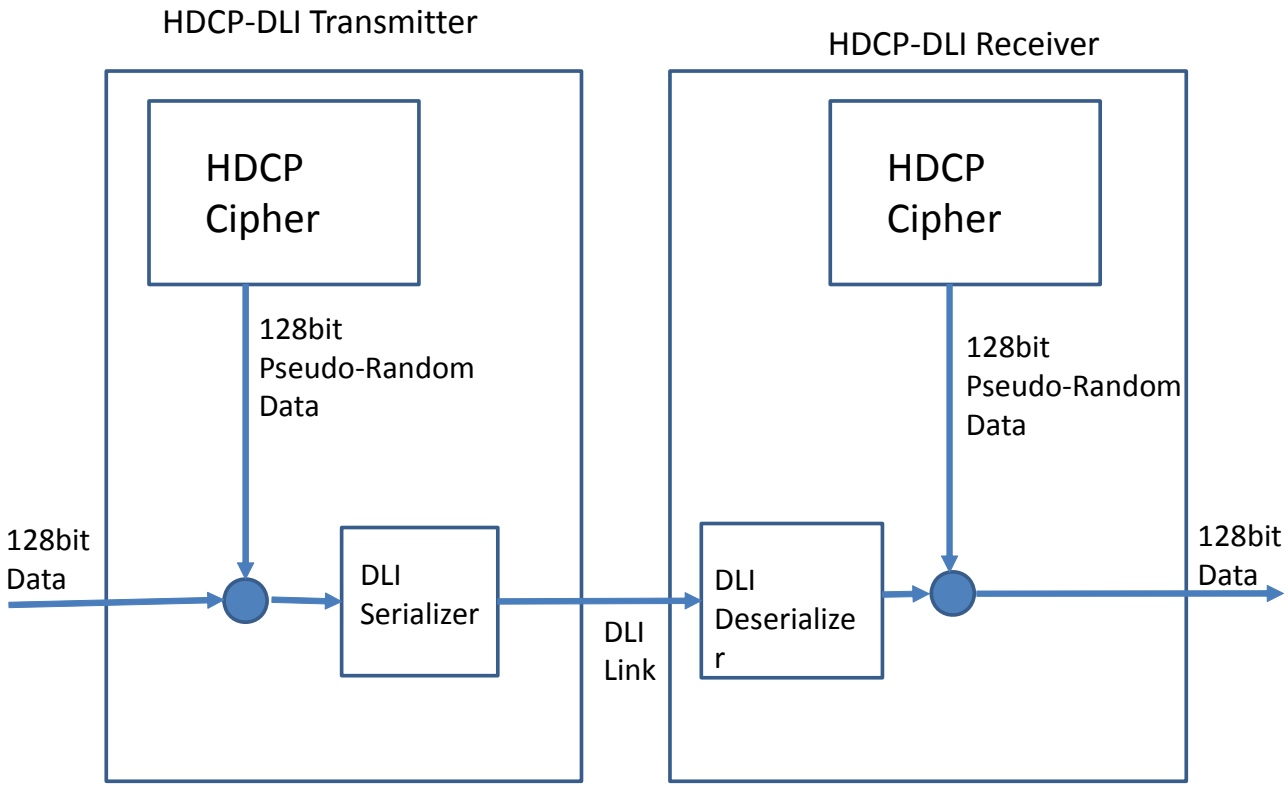

Figure 1: HDCP-DLI Encryption Diagram

The following are the specific rules for data encryption:

-The payload of video/audio data packet is HDCP encrypted if ENC_EN bit in the packet header is set.
-Payload of the HDCP link integrity check is encrypted.
-Packet header is not encrypted.
-Packets of other type are not encrypted.

The HDCP Cipher generates a new 128-bit word of the key stream for every DLI word which is also 128 bit.

DLI interface supports 24 bit video and other video formats with high color depth. All the video data are mapped to the 128 bit DLI data word pixel by pixel.

At the end of packet, if the last word does not contain the whole 128 bits of data, the remaining data will be filled with zero before encryption and ignored after decryption.

Similarly, the audio packet is also mapped to the 128 bit DLI interface word and encrypted with the 128 bit words of key stream.

3.2 HDCP Cipher

This amendment does not make any changes to this HDCP cipher scheme

3.3 Encryption Status Signaling

Instead of using CTL[3:0] signal to enable/disable HDCP encryption as in HDCP on HDMI systems, the HDCP on DLI protocol uses a different signaling scheme to enable/disable HDCP encryption.

In HDCP on DLI protocol, the ENC_EN signal is passed from HDCP-DLI Transmitter to HDCP-DLI Receiver via the ENC_EN bit in every video/audio data packet header. This "ENC_EN" is used to indicate whether the current packet is encrypted or not. The encryption and decryption functions are applied only to the packets that have ENC_EN bit set.

There is no change in the amendment for the generation of ENC_EN signal. After successful completion of the authentication phase, the HDCP-DLI Transmitter interface waits until the start of the first video frame (first VSYNC). From that time on, the HDCP-DLI Transmitter unit will set ENC_EN bit in all video/audio frames that need to be protected.

HDCP-DLI receiver shall decrypt all packets with ENC_EN bit set.

4. RENEWABILITY

This amendment does not make any change to the functions of the renewability of HDCP devices.