HDCP specification v2.2 Amendment for GVIF

Rev1.0

29 September, 2016

Digital Content Protection LLC

Notice

Acknowledgement

Sony Corporation 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

Email: info@digital-cp.com

Web: www.digital-cp.com

Revision History

29 September 2016 1.0 initial release

1. Introduction

1.1 Scope

This document describes amendment of the High-bandwidth Digital Content Protection (HDCP) system, mapping HDCP rev2.2 to HDMI specification, limiting to implementation onto GVIF (Giga-bit Video Interface). It is based on HDCP 2.2, which is a revision update to HDCP Revision 2.00 and its errata, referred to collectively as HDCP 2.2.

Implementations must include all elements of the content protection system described herein and in the High-bandwidth Digital Content Protection System, Mapping to HDMI, Revision 2.2 ("HDCP2.2 over HDMI"), unless the element is specifically identified as informative or optional. Where the mandatory or optional requirements specified in the HDCP2.2 over HDMI specification and this specification are different, the mandatory or optional requirements specified in this specification take precedence for the implementation of HDCP-GVIF devices. Adopters must also ensure that implementations satisfy the robustness and compliance rules described in the technology license.

1.2 References

[1] International Electrotechnical Commission IEC 62889:2015 Digital video interface –Gigabit video interface for multimedia systems

[2] Standard of Japan Electronics and Information Technology Industries Association JEITA CP-6101 Digital monitor interface GVIF, January, 2012

[3] Digital Content Protection (DCP) LLC, High-bandwidth Digital Content Protection System, Revision 1.4, July 8, 2009

[4] Digital Content Protection (DCP) LLC, High-bandwidth Digital Content Protection System, Revision 2.2, October 16, 2012

[5] HDCP 2.2 on HDMI Specification, February 13, 2013

1.3 Definitions

HDCP-GVIF Transmitter. An HDCP transmitter which uses GVIF as physical layer. HDCP-GVIF Transmitter encrypts and emits HDCP Content.

HDCP-GVIF Receiver. An HDCP receiver which uses GVIF as physical layer. HDCP-GVIF Receiver receives and decrypts HDCP Content.

HDCP-GVIF Repeater. An HDCP repeater which uses GVIF as physical layer. HDCP-GVIF Repeater receives, decrypts, re-encrypts and emits HDCP Content to downstream HDCP-GVIF Devices.

2. Authentication Protocol

2.1 Overview

Authentication protocol is an exchange between an HDCP-GVIF Transmitter and an HDCP-GVIF Receiver to ensure the HDCP-GVIF Receiver is authorized to receive HDCP content. The HDCP-GVIF authentication protocol works in the same manner as the authentication protocol described in HDCP2.2 on HDMI, except for the following change. In case of HDCP-GVIF, GVIF channel embedded communication is used for the exchanges instead of I2C bus.

2.2 Link Synchronization

Once encrypted content starts to flow, a periodic Link Synchronization is performed to maintain cipher synchronization between the HDCP-GVIF Transmitter and the HDCP-GVIF Receiver.

Link Synchronization is achieved every time a header is transmitted, by the inclusion of *inputCtr* in the header. (See Section 3.2 for details about *inputCtr*). The header is transmitted during every vertical blanking interval. The HDCP-GVIF Receiver updates its *inputCtr* with the *inputCtr* value received from the HDCP-GVIF Transmitter.

3. HDCP Encryption

3.1 Data Encryption

As shown in Figure3.1, Data Encryption for HDCP-GVIF system is same as that for HDMI. Only difference is TMDS Encoder/Decoder is replaced by GVIF Encoder/decoder.

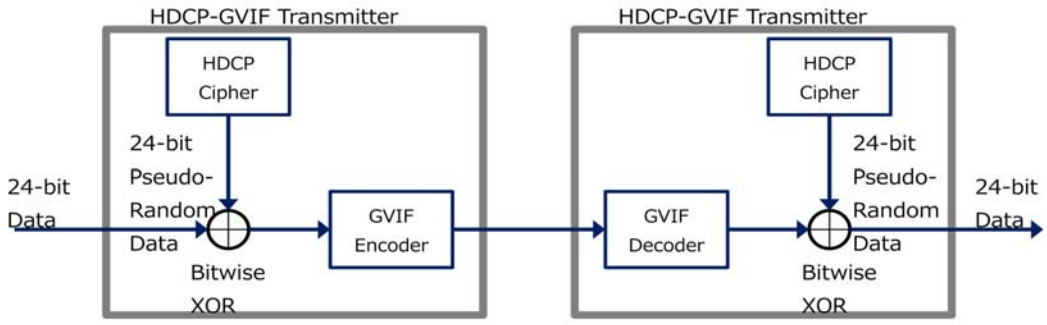

Figure3.1 HDCP Encryption and Decryption

Out of 128-bit word of Cipher output, 120-bit word data is applied to GVIF Encoder. Remaining 8-bit data is discarded.

Cipher Output	Data
127:120	discard
119:96	data4
95:72	data3
71:48	data2
47:24	data1
23:0	data0

Table3.1 Encryption Stream Mapping

3.2 HDCP Cipher

As specified in the HDCP specification Rev2_2, HDCP Cipher for HDCP-GVIF system also consists of a 128-bit AES module that is operated in a counter mode. HDCP Cipher for HDCP-GVIF system does not make any change to HDCP Cipher for HDMI interface.

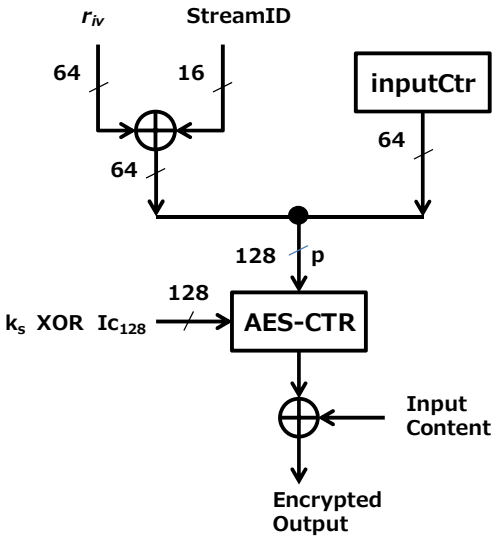

Figure3.2 HDCP Cipher Structure

k_s is the 128-bit Session Key which is XORed with Ic_{128}.

p = (r_{iv}) || *inputCtr*, All values are in big-endian order.

InputCtr is a 64-bit counter. It is initialized to zero when HDCP Encryption is enabled for the first time during the HDCP session i.e. immediately after AKE and must not be reset at any other time. It is incremented by one after every 5-word x 24-bit data is transmitted.

3.3 Encryption Status Signaling

HDCP-GVIF Transmitter signals the status of HDCP Encryption to HDCP-GVIF Receiver by sending the HDCP Enable and Disable symbols including *inputCtr*. Table 3.2 shows the details of the HDCP Enable and Disable symbols.

Bit number	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
HDCP_Enable6	1	1	1	1	0	0	0	x	1	0	0	1	1	1	0	0	x	*inputCtr* [63:56]							
HDCP_Enable5	1	1	1	1	0	0	0	x	1	0	0	1	1	1	0	*inputCtr* [55:46]									
HDCP_Enable4	1	1	1	1	0	0	0	x	1	0	0	1	1	1	0	*inputCtr* [45:36]									
HDCP_Enable3	1	1	1	1	0	0	0	x	1	0	0	1	1	1	0	*inputCtr* [35:26]									
HDCP_Enable2	1	1	1	1	0	0	0	x	1	0	0	1	1	1	0	*inputCtr* [25:16]									
HDCP_Enable1	1	1	1	1	0	0	0	x	1	0	0	1	1	1	0	*inputCtr* [15:6]									
HDCP_Enable0	1	1	1	1	0	0	0	x	1	0	0	1	1	1	0	*inputCtr* [5:0]						Reserved [12:9]			
HDCP_Disable	1	1	1	1	0	0	0	x	1	0	0	1	1	1	0	1	Reserved [8:0]								

Table 3.2 HDCP Enable and Disable symbols

When HDCP-GVIF Receiver receives the HDCP Enable[6:0] symbols including 64-bit *inputCtr* successfully, it deems following audio/video content stream is HDCP encrypted. The HDCP Encryption status signaling is updated during every vertical blanking interval.

When HDCP-GVIF Transmitter is required to stop HDCP Encryption, it sends the HDCP Disable symbol. HDCP-GVIF Receiver stops to decrypt content stream right after the reception of the HDCP Disable symbol.

END OF DOCUMENT