HDCP specification v2.2 Amendment for GVIF2

Rev1.0

29 September, 2016

Digital Content Protection LLC

Notice

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

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

Acknowledgement

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 GVIF2 (Giga-bit Video Interface2). 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.

In most cases, terminology 'HDMI' in the HDCP Specification rev 2.2 can be replaced by 'GVIF2' unless otherwise noted.

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-GVIF2 devices. Adopters must also ensure that implementations satisfy the robustness and compliance rules described in the technology license.

1.2 References

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

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

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

1.3 Overview

HDCP-GVIF2 Transmitter and Receiver are capable of handling multiple data streams. HDCP-GVIF2 Transmitter encrypts incoming HDCP content on a stream-by-stream basis. Since each video stream operates on an independent clock, HDCP-GVIF2Transmitter executes padding so as to handle the video streams on the same common clock domain. Then HDCP-GVIF2 Transmitter multiplexes them into single serial bit stream and transmits them to the HDCP-GVIF2 Receiver. The HDCP-GVIF2 Receiver does the opposite of the transmitter.

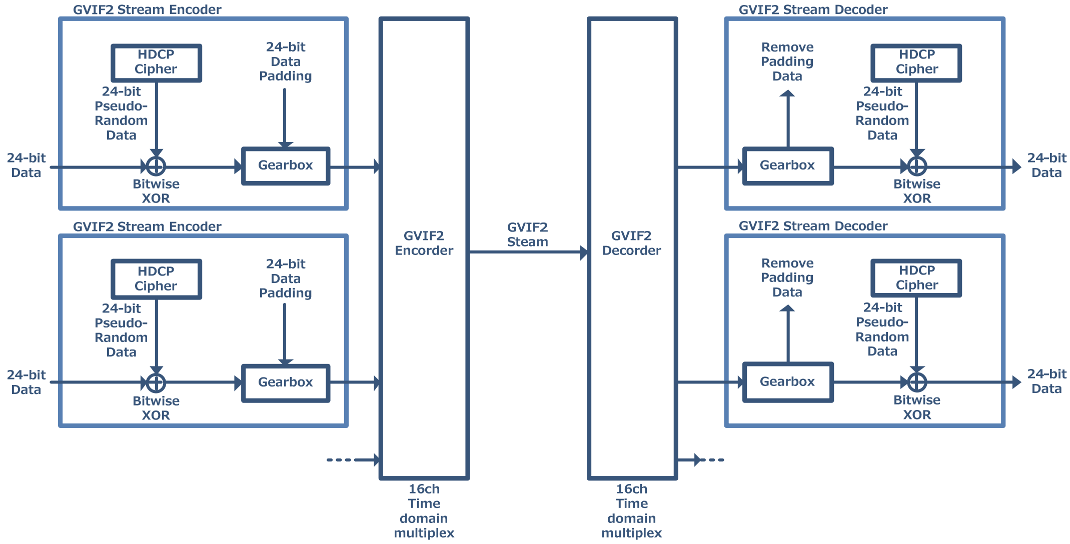

Figure1.1 Data Encryption

1.4 Definitions

HDCP-GVIF2 Transmitter. An HDCP transmitter which uses GVIF2 as physical layer. HDCP-GVIF2 Transmitter encrypts and emits HDCP Content.

HDCP-GVIF2 Receiver. An HDCP receiver which uses GVIF2 as physical layer. HDCP-GVIF2 Receiver receives and decrypts HDCP Content.

HDCP-GVIF2 Repeater. An HDCP repeater which uses GVIF2 as physical layer. HDCP-GVIF2 Repeater receives, decrypts, re-encrypts and emits HDCP Content to downstream HDCP-GVIF2 Devices.

2. Authentication Protocol

2.1 Overview

Authentication protocol is an exchange between an HDCP-GVIF2 Transmitter and an HDCP-GVIF2 Receiver to ensure the HDCP-GVIF2 Receiver is authorized to receive HDCP content. The HDCP-GVIF2 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-GVIF2, GVIF2 channel embedded communication is used for the exchanges instead of I2C bus.

2.2 Downstream Propagation of Content Stream Management Information

Since GVIF2 is multi-stream capable, HDCP-GVIF2 Transmitter must propagate Content Stream management information. Handling of Content Stream Management Information is compliant to HDCP Interface Independent Adaptation specification, Rev2.2.

2.3 RepeaterAuth Stream Manage (Transmitter to Receiver)

Content Streams are assigned a Type value by the most upstream HDCP Transmitter based on instructions received from the Upstream Content Control Function.

The Stream ID, assigned to a content stream, is followed by its assigned Type value in the RepeaterAuth Stream message, All content streams transmitted by the HDCP Transmitter to the HDCP Repeater, after HDCP Encryption, are assigned Type values.

Syntax	No. of Bytes	Identifier
RepeaterAuth_Stream_Manage{		
msg_id	1	unit
seq_num_M	3	unit
k	2	unit
for(j=0;j<*k*;j++) {		
streamIDj	4	unit
ContentStreamIDj	2	unit
Type	1	unit
}		
}		

Table 2.1 RepeaterAuth Stream Manage Payload

STREAMID_TYPE = streamID1 || ContentStreamID1 || Type || streamID2 || ContentStreamID2 || Type || … || streamID*k* || ConentStreamID*k* || Type

2.4 Link Synchronization

Once encrypted content starts to flow, a periodic Link Synchronization is performed to maintain cipher synchronization between the HDCP-GVIF2 Transmitter and the HDCP-GVIF2 Receiver.

Link Synchronization is achieved every time a Packet Header is transmitted, by the inclusion of *inputCtr* and streamID in the header. (See Section 3.2 for details about *inputCtr* and streamID). The header is transmitted during every vertical blanking interval.

In case only audio signal is available, the header is transmitted at least every 1/60 second. The HDCP-GVIF2 Receiver updates its *inputCtr* corresponding to the stream (as indicated by the streamID value) with the *inputCtr* value received from the transmitter.

3. HDCP Encryption

3.1 Data Encryption

As shown in Figure3.1, Data Encryption for HDCP-GVIF2 system is same as that for HDMI. Only difference is TMDS Encoder/Decoder is replaced by GVIF2 Encoder/decoder.

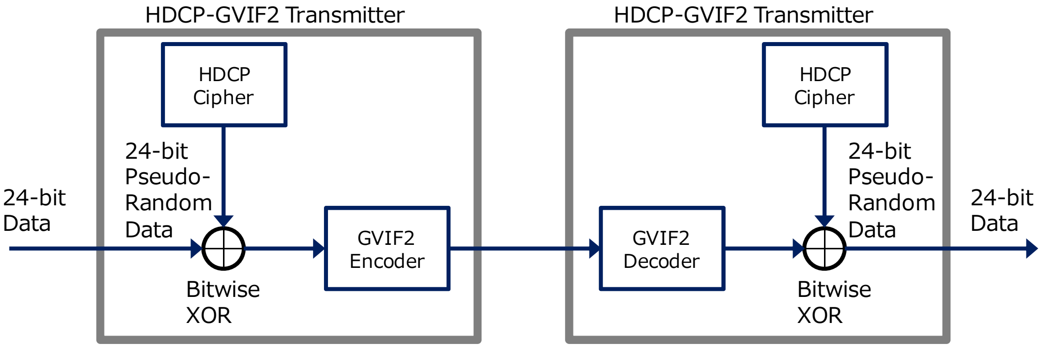

Figure3.1 HDCP Encryption and Decryption

Out of 128-bit word of Cipher output, 120-bit word data is applied to GVIF2 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-GVIF2 system also consists of a 128-bit AES module that is operated in a counter mode. HDCP Cipher for HDCP-GVIF2 system is based on HDCP Cipher for HDMI system, except adding Stream ID due to its multi-stream capable feature.

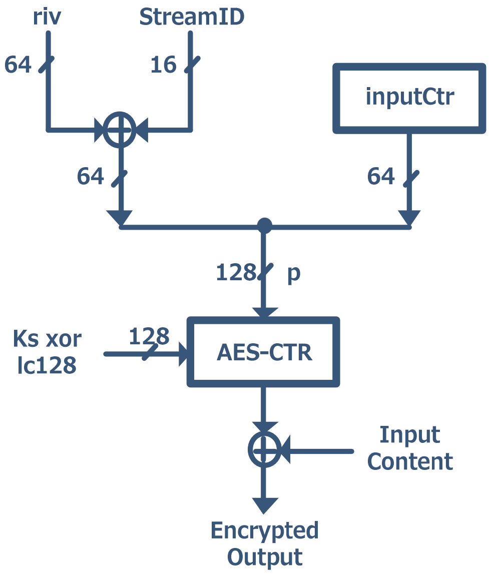

Figure3.2 HDCP Cipher Structure

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

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

The StreamID is a 16-bit ID number and associated with Content Stream to be encrypted. The StreamID must be distinct for each Content Stream transmitted by the HDCP Transmitter, if those Content Streams share the same k_s and r_{iv}. *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. Each Content Stream is associated with its own *inputCtr*. The *inputCtr* is incremented by one after every 5-word x 24-bit data is transmitted.

3.3 Encryption Status Signaling

HDCP-GVIF2 Transmitter signals the status of HDCP Encryption to HDCP-GVIF2 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-GVIF2 Receiver receives the HDCP Enable[6:0] symbols including 64-bit *inputCtr* successfully, it deems following audio/video content stream is HDCP encrypted. This HDCP Encryption status signaling is updated during every vertical blanking interval. In case only audio signal is available, it is updated at least every 1/60 second.

When HDCP-GVIF2 Transmitter is required to stop HDCP Encryption, it sends the HDCP Disable symbol. HDCP-GVIF2 Receiver stops to decrypt content stream right after the reception of the HDCP Disable symbol.

For the case of multi-stream system, encryption status can be set independently by Content Stream. In the same manner as a single stream case, HDCP Encryption is active after sending the HDCP Enable symbols including *inputCtr* and inactive after sending the HDCP Disable symbol.

END OF DOCUMENT