HDCP specification v2.2 Amendment for GVIF

Rev1.0

29 September, 2016
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.

© Intel Corporation. Third-party brands and names are the property of their respective owners.

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


1.3 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.

Digital Content Protection LLC
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 Figure 3.1, Data Encryption for HDCP-GVIF system is same as that for HDMI. Only difference is TMDS Encoder/Decoder is replaced by GVIF Encoder/decoder.

![Figure 3.1 HDCP Encryption and Decryption](image)

Out of 128-bit word of Cipher output, 120-bit word data is applied to GVIF Encoder. Remaining 8-bit data is discarded.
Table 3.1 Encryption Stream Mapping

<table>
<thead>
<tr>
<th>Cipher Output</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>127:120</td>
<td>discard</td>
</tr>
<tr>
<td>119:96</td>
<td>data4</td>
</tr>
<tr>
<td>95:72</td>
<td>data3</td>
</tr>
<tr>
<td>71:48</td>
<td>data2</td>
</tr>
<tr>
<td>47:24</td>
<td>data1</td>
</tr>
<tr>
<td>23:0</td>
<td>data0</td>
</tr>
</tbody>
</table>

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.

Figure 3.2 HDCP Cipher Structure

\[ k_s \text{ XOR } Ic_{128} \rightarrow \text{AES-CTR} \]

\[ p = (r_{iv}) \parallel inputCtr, \text{ All values are in big-endian order.} \]

\text{InputCtr} \text{ 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   | 0   | 0   | 0   | x   | 1   | 0   | 0   | 1   | 1   | 1   | 0   | 0   | x    |
| HDCP_Enable5 | 1   | 1   | 1   | 1   | 0   | 0   | 0   | x   | 1   | 0   | 0   | 1   | 1   | 1   | 0    |
| HDCP_Enable4 | 1   | 1   | 1   | 1   | 0   | 0   | 0   | x   | 1   | 0   | 0   | 1   | 1   | 1   | 0    |
| HDCP_Enable3 | 1   | 1   | 1   | 1   | 0   | 0   | 0   | x   | 1   | 0   | 0   | 1   | 1   | 1   | 0    |
| HDCP_Enable2 | 1   | 1   | 1   | 1   | 0   | 0   | 0   | x   | 1   | 0   | 0   | 1   | 1   | 1   | 0    |
| HDCP_Enable1 | 1   | 1   | 1   | 1   | 0   | 0   | 0   | x   | 1   | 0   | 0   | 1   | 1   | 1   | 0    |
| HDCP_Enable0 | 1   | 1   | 1   | 1   | 0   | 0   | 0   | x   | 1   | 0   | 0   | 1   | 1   | 1   | 0    |
| HDCP_Disable | 1   | 1   | 1   | 0   | 0   | 0   | x   | 1   | 0   | 0   | 1   | 1   | 1   | 1   | 0    | 1    |

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