Extron®

HDCP – A Technical Overview

Table of Contents

Abstract

HDCP - High-bandwidth Digital Content Protection is an encryption protocol for copy-protected video content such as Blu-ray Disc and HD movie downloads. This article describes HDCP in detail, introducing the components of an HDCP system – sources, repeaters, and sinks, as well as the three phases of the HDCP protocol – authentication, encryption, and renewability.

white paper

Background

Digital transmission of audio/video content enables perfect reproduction of source material. This is desirable when pursuing the highest possible quality, but is a concern for holders of intellectual property rights. High-bandwidth Digital Content Protection - HDCP is an encryption protocol incorporated into digital video connection interfaces to block unauthorized transmission and reproduction. As digital signal transmission proliferates in the marketplace, A/V professionals will encounter HDCP with increasing frequency.

HDCP is an encryption protocol applied at the digital interface between video sources and displays to prevent unauthorized access to protected content. HDCP version 1.0 applied initially to the DVI interface. HDMI was incorporated in HDCP version 1.1, and HDCP version 1.3 added support for DisplayPort. With the release of version 2.0 in October 2008, HDCP became interface-independent, and can be applied to any two-way digital transmission between sources and displays, wired or wireless, compressed or uncompressed.

Digital Content Protection, LLC, a subsidiary of Intel, administers HDCP licenses to equipment manufacturers, and manages the distribution of encryption keys to licensees. Every HDCP device must have a unique set of encryption keys, including one public key, also known as the KSV, and 40 private keys. Manufacturers under HDCP license pay for blocks of these encryption key sets to implement into their products.

Professional Digital A/V System with HDCP

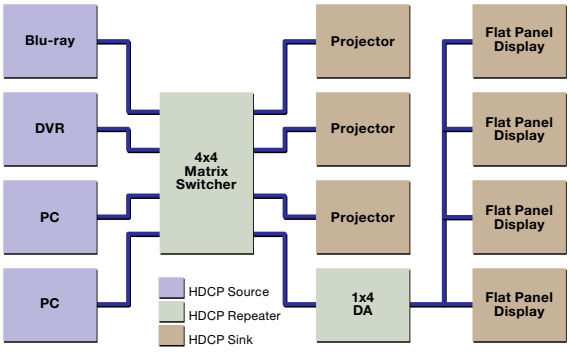

Figure 1: An HDCP 1.x system in a professional A/V application

HDCP 1.x Protocol and Operation

Until the introduction of HDCP 2.0, the basic protocol of HDCP had not changed substantially. The only major difference between HDCP versions 1.0 through 1.3 is in the type of physical connection between the various components of an A/V system. In an HDCP system, these components are defined as sources - e.g. PCs, Blu-ray Disc players - which originate the protected video signal, sinks - e.g. monitors, projectors - which display the content, and repeaters - e.g. switchers, distribution amplifiers - which may be placed between sources and sinks to distribute the A/V signal. HDCP repeaters include a receiver at the input - or upstream - connection and one or more transmitters at the output - or downstream - connection. Components in a HDCP 1.x system communicate over two-way ports, with each port driven by a transmitter and terminating at a receiver. Figure 1 shows a typical HDCP 1.x system in a professional A/V environment.

Operationally, the HDCP 1.x protocol comprises three phases: authentication, content encryption, and renewability. During the authentication phase, encrypted messages and public keys are exchanged between the HDCP transmitter and receiver to determine the receiver's identity, eligibility to accept protected content, and to identify whether the receiver is part of a repeater. If the receiver is part of a repeater, then the transmitters contained in the repeater will initiate the authentication protocol with downstream receivers to determine their eligibility. The repeater is also required to report the identities - public keys - and connection topology of all downstream devices back to the source transmitter. The success of the authentication phase is determined by the source transmitter based on the following:

- The receiver immediately downstream is able to demonstrate its eligibility in less than 100 ms.
- The identities and connection topology of all downstream devices are reported in less than 5 seconds.
- All downstream devices are eligible to receive HDCP content and have not been revoked.
- There are fewer than 128 total devices connected downstream.
- There are fewer than seven levels of repeaters downstream.

If the above conditions are met, then authentication is deemed successful, and the transmitter proceeds to the content encryption phase. It encrypts the protected A/V content using a 56-bit secret key which will also be used by the receiver to decrypt and ultimately display the protected A/V material. The secret key is independently calculated by each HDCP device and is never transmitted over the digital interface. Any downstream repeaters will decrypt the A/V content and re-encrypt using different secret keys for transmission further downstream. All of the secret keys are periodically refreshed during vertical sync for additional security.

The third phase, renewability, refers to the ability of the HDCP licensor to revoke HDCP devices that have been compromised or hacked, by listing their public keys in a file that is distributed with protected content. HDCP-protected content such as Blu-ray Disc contain system renewability messages (SRMs) with a revocation list of public keys for blacklisted devices. As new Blu-ray Discs are released, they will include a section of data that lists revoked keys. Blu-ray Disc players will read this data, store it in non-volatile memory, and compare the public keys of any downstream devices against the revocation list. If any downstream devices match, no video will be transmitted. HDCP devices are obligated to check for SRMs and to update their own internal memories as new revocation lists are distributed. The revocation list is used during HDCP authentication to check for blacklisted public keys.

Please see the appendix for further details on HDCP 1.x authentication and encryption.

HDCP 2.0

The latest version of HDCP was released in October 2008 with many important changes. With version 2.0, HDCP will no longer apply only to specific interfaces such as DVI, HDMI, DisplayPort, etc., but rather will be independent of the interface standard, so that any two-way digital communication scheme can be protected by HDCP, including wireless and compressed formats. For wireless connections, HDCP 2.0 adds a locality check to the authentication protocol, to ensure that only nearby devices will be able to receive protected content. Furthermore, HDCP 2.0 replaces the ad hoc 56-bit HDCP 1.x encryption scheme with two standard algorithms from the data security industry: for authentication, an RSA system with 1024 and 3072-bit keys, and for content encryption, a 128-bit AES system. In addition, the maximum number of connected devices is reduced to 32 and the maximum level of repeaters is reduced to four. All of these changes mean that HDCP 2.0 is not directly backward compatible with HDCP 1.x. However, the new specification provides for converters between HDCP 1.x and HDCP 2.0 devices to support mixed A/V systems with both versions of HDCP-compliant devices. These converters are important because the HDCP license agreement requires that licensees support any new specification within 18 months of release. This implies that soon, all HDCP devices available on the market will support version 2.0. An existing A/V system incorporating HDCP 1.3 will require converters if newly acquired HDCP 2.0 devices are to be added to the system. Table 1 lists the major changes for HDCP 2.0.

	HDCP 1.x	HDCP 2.0
Encryption Method	Specialized 56-bit symmetric system used for both authentication and video encryption	Authentication: Data security industry standard RSA 1024 and 3072-bit asymmetric system
		Video encryption: Data security industry standard AES 128-bit symmetric system
Applicable Interfaces	DVI, HDMI, DisplayPort	Any two-way digital interface
Maximum Downstream Receivers for Each Transmitter	< 128	< 32
Maximum Repeater Levels for Each Transmitter	< 7	< 4
Backward Compatibility	Yes, no electronic components required	Yes, using specialized electronic HDCP-1.x-to-2.0 and HDCP-2.0-to-1.x converters
Wireless Support	Ad hoc approval by Digital Content Protection, LLC	Explicitly specified with new locality check requirement

Table 1: Major changes in HDCP 2.0

Conclusion

HDCP support is required for all digital video equipment that transmits, processes, or displays commercial copy-protected high definition content such as Blu-ray Disc and Apple® iTunes® video downloads. HDCP encrypts the digital video and ensures that only authorized devices are able to decrypt and display the protected content. Furthermore, HDCP places limitations on the ability of an A/V system to distribute and simultaneously display content, based on the number of devices and levels of repeaters in the system. As HDCP specifications are revised, these restrictions also change. It is important for A/V professionals to understand HDCP operations and restrictions for proper system design and commissioning.

Implementation of the HDCP standard can vary by manufacturer. For example, even though the HDCP 1.x protocol specifies that the maximum number of receiver devices downstream from a video source be less than 128, this does not necessarily mean that all HDCP 1.x video sources will allow that many devices to be connected to it. In fact, the actual number of downstream receivers allowed by any particular HDCP source varies by model, and must be determined on a case-by-case basis.

Appendix – HDCP 1.x Authentication and Encryption Details

HDCP 1.x Authentication

Each HDCP 1.x device has a unique set of private keys along with a public key. To determine that a connected receiver is authorized and capable of receiving encrypted content, the HDCP transmitter sends a message containing its public key - Aksv to the receiver, and expects the receiver to return its public key - Bksv in exchange. If this occurs, then the transmitter examines the receiver's public key to determine that it is valid, and calculates a secret key - Km based on the receiver's public key and its own private key. At the same time, the receiver also calculates a secret key - Km' based on the transmitter's public key and its internal private key. The secret keys, Km and Km', calculated by the transmitter and the receiver are NOT sent over the communication port, but in the event that both parties are authorized HDCP devices, the secret keys will match. To show that it has a matching secret key, the receiver is expected to send an encrypted message RO' to the transmitter within 100 ms of the initial contact by the transmitter. If this does not occur, the authentication fails. Since RO' is generated using the secret key Km', the transmitter can match RO' against its own internal RO, generated using Km, so that if RO=RO', that would imply that Km=Km', and thus the receiver is initially authenticated. Note that secret keys or private keys are never sent over the HDCP port, so that any eavesdropper on the port would only see either public keys - Aksv or Bksv - or encrypted data traffic - RO'. Figure 2 illustrates a successful HDCP initial authentication.

The initial exchange of authentication messages between the HDCP transmitter and receiver also establish whether the receiver is a repeater, through the REPEATER status bit. In the event that the receiving device is a repeater, additional steps are required. The HDCP 1.x specifications restrict the total number of receivers connected to a source to be fewer than 128, and the total levels of repeaters between a source and a sink to be no more than seven. Therefore, if a HDCP source encounters a repeater, it must determine whether these maximum connection restrictions are being violated. Furthermore, the HDCP source must authenticate all connected devices before sending

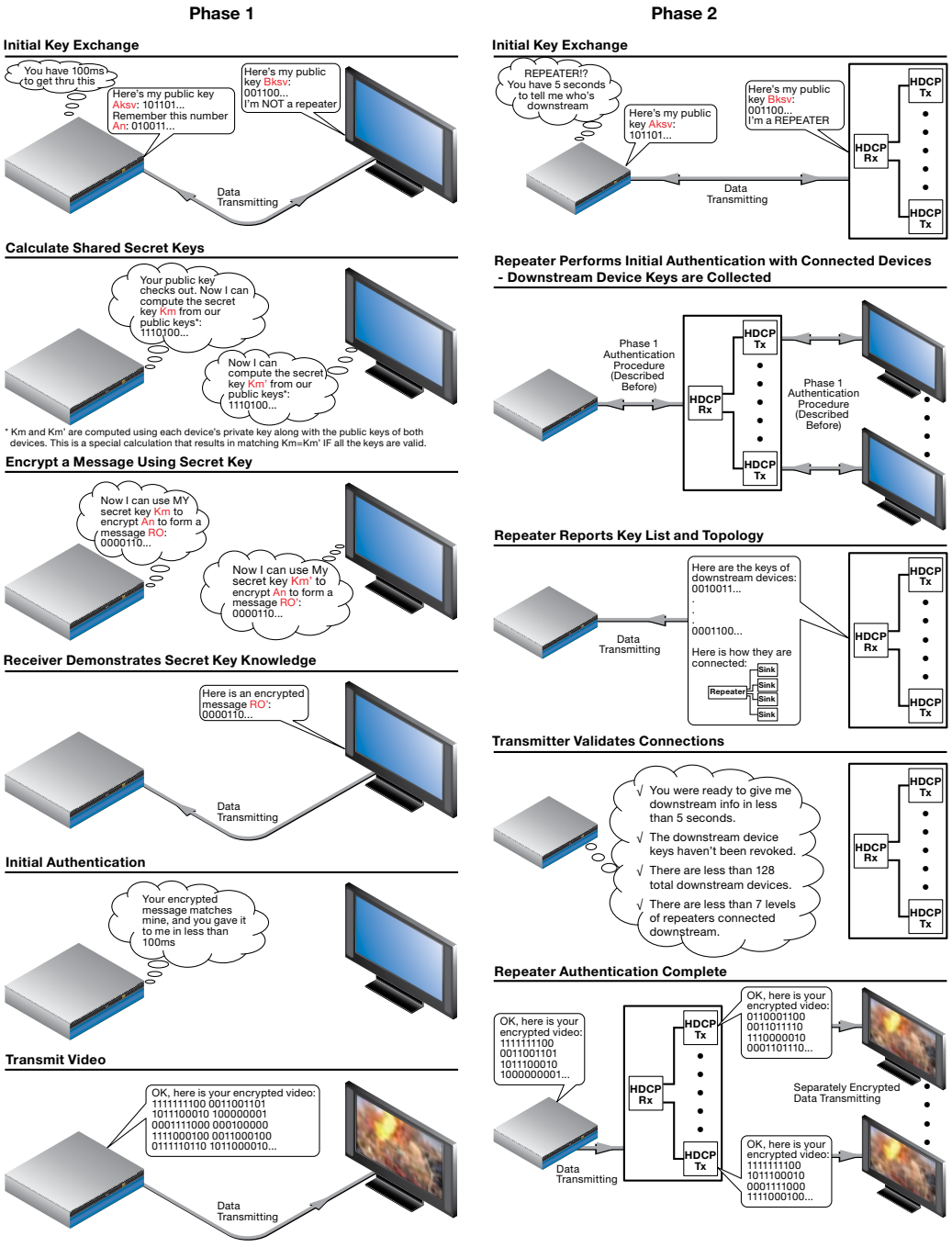

Figure 2: HDCP Authentication

protected content. To meet these requirements, the HDCP protocol specifies that a source will expect a repeater to send a list of public keys for downstream HDCP devices, along with how they are connected. This information must be sent to the source within five seconds following initial contact. HDCP repeaters behave as receivers to upstream devices, and also act as transmitters to downstream devices.

HDCP 1.x Encryption

After initial authentication is complete, the source begins to transmit digital A/V information whose encryption is based on the shared secret key - Km described earlier. Any authorized receiver would have a matching secret key Km', and would then use Km' to decrypt the A/V content. The actual encryption keys are changed periodically during vertical blanking intervals, so therefore the HDCP receiver must remain synchronized with the transmitter. Otherwise, it cannot continue to decrypt the A/V content. HDCP repeaters decrypt video received from upstream sources, and re-encrypt the video for transmission to downstream receivers. The HDCP 1.x encryption scheme is categorized as symmetric since each HDCP transmitter and its immediate downstream receiver uses the same shared secret key for both encryption and decryption.