The ABC's of HDCP

Understanding the copy protection system that protects content transmitted over HDMI

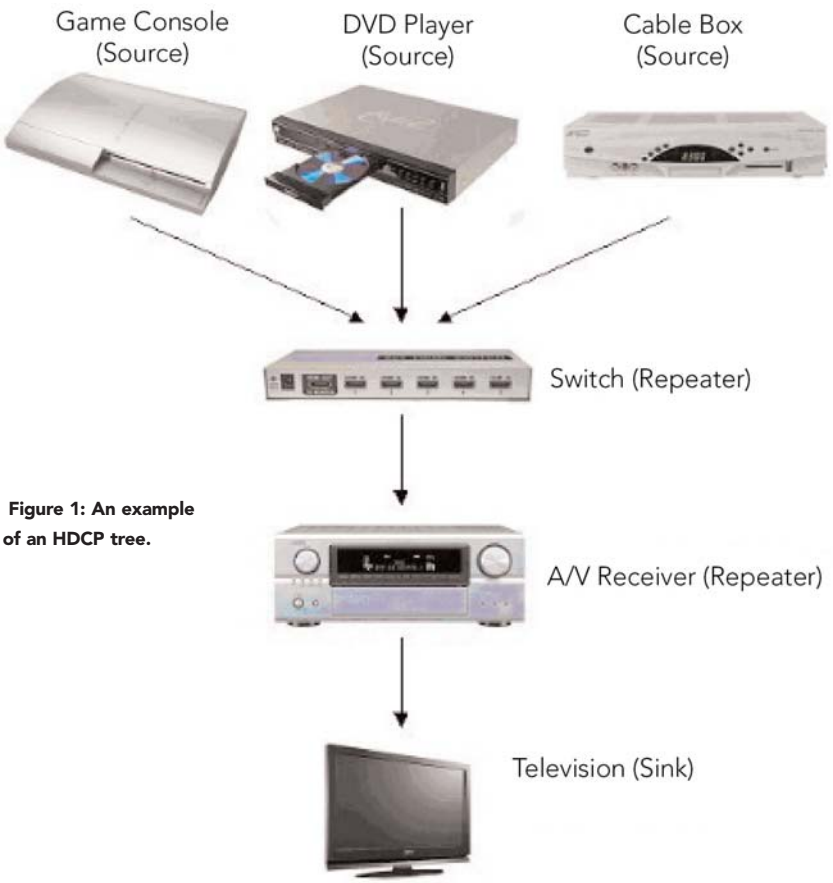

Figure 1: An example of an HDCP tree.

BY ROBERT CARTER

Digial content providers and institutions that distribute digital content are increasingly concerned about pirates copying and sharing copyrighted material. To protect digital content as it's transmitted over cables between devices, Intel developed a DRM scheme known as the High-bandwidth Digital Content Protection system (HDCP). HDCP has recently enjoyed rapid, widespread adoption in the consumer electronics space, but has been plagued by interoperability issues.

HDMI

HDCP was originally designed to protect AV content transmitted over the Digital Video Interface (DVI), then the High Definition Multimedia Interface (HDMI). The HDMI specification defines an interface for carrying digital audiovisual content from a source to a display device. Repeaters, such as switches or AV receivers, may accept and re-transmit HDMI content.

Repeaters have two separate HDMI connections: the upstream connection with the source and the downstream connection with the sink (or another repeater). Within each connection, the upstream device sends audiovisual data to the downstream device.

The physical HDMI cable carries many signals:

TMDS. The audiovisual data is encoded into three Transition Minimized Differential Signaling (TMDS) data channels. These channels and a TMDS clock are carried over four differential pairs from the source to the sink.

DDC. The Digital Display Channel (DDC) is a communications interface. This interface provides two-way communication in a master-slave relationship. The upstream device is the DDC master and the downstream device is the DDC slave.

Hot Plug Detect. The sink indicates its presence to the source with the Hot Plug Detect (HPD) signal. The sink can toggle the Hot Plug Detect signal to reset the HDMI connection (and thus the HDCP session).

RxSense. Though not specifically defined by HDMI, many devices support a feature known as RxSense. Similarly to HPD, this signal can be used to detect the presence of a sink.

HDCP Overview

To protect content, the HDCP system first authenticates HDCP devices and then encrypts the content. Authentication occurs over the DDC channel and assures that all devices receiving the content are licensed and authorized to receive the content. After successful authentication, the TMDS data streams are encrypted to prevent other devices from eavesdropping on the content during transmission.

HDCP devices are organized in a tree topology, as shown in the figure 1. The tree may have at most 127 devices and may be no more than 7 levels deep.

A single point-to-point HDCP link can involve only one HDCP transmitter and one HDCP receiver. As such, a repeater must decrypt the content at the HDCP receiver on each of its inputs. The repeater must then re-encrypt the data with an HDCP transmitter on each of its outputs. The repeater must inform the upstream device of its downstream connections, and it is the repeater's responsibility to maintain those connections. (See figure 2.)

HDCP Implementation Elements

The HDCP specification doesn't address implementation, but, in practice, device manufacturers typically buy HDCP chips from a DCP-licensed silicon vendor. These chips usually also provide TMDS encoders or decoders and other HDMI-specific features. Every transmitting device will have at least one HDCP transmitter chip and every receiving device will have at least one HDCP receiver chip. The HDCP transmitters and receivers frequently require a microprocessor to implement the authentication.

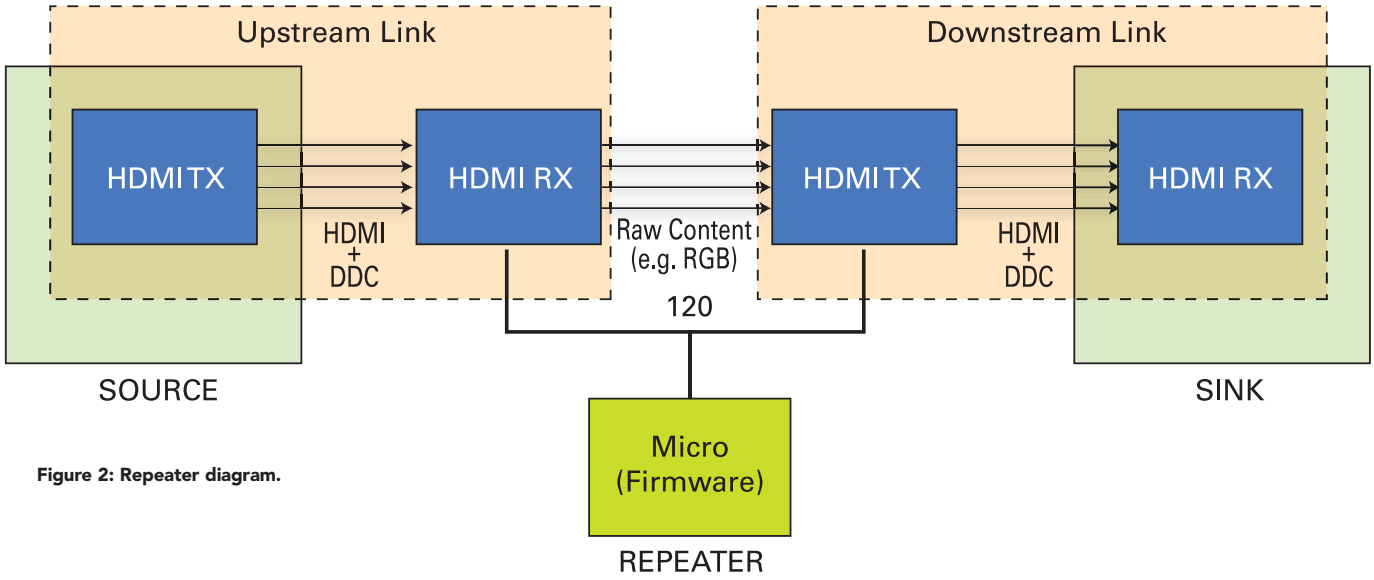

Figure 2: Repeater diagram.

To support HDCP, each transmitter and receiver must possess the following elements:

Keys. Each HDCP transmitter and receiver has 40 unique 56-bit private keys.

KSVs. Each HDCP chip also has a public 40-bit value known as the Key Selection Vector (KSV). The KSVs and keys of all licensed HDCP devices are mathematically related according to a cryptographic key exchange protocol similar to Blom's scheme. In this scheme, any two licensed devices can swap KSVs and use them, along with their private keys, to come up with a shared secret key. This shared key can be used to encrypt and decrypt the TMDS stream. The KSV can also be used to uniquely identify a transmitter or receiver.

HDCP Cipher. Each chip must implement the HDCP Cipher. The cipher accepts a seed value and uses it to generate a deterministic pseudo-random stream of data. This publicly defined cipher is used during both authentication and encryption.

Registers. Each HDCP receiver must provide a series of pre-defined DDC-accessible registers. All of the HDCP communications between the source and sink occurs by the source reading from and writing to these registers.

The Authentication and Encryption Protocols

HDCP authentication consists of three parts:

Part 1. The source authenticates with the device connected to its output. If successful, encryption is enabled and AV content transmission begins.

Part 2. This part is only used if the downstream device is a repeater. The repeater authenticates with the devices connected to its output(s) and passes the HDCP tree topology information up to the source.

Part 3. The source performs periodic checks with the downstream device to ensure that encryption is in sync.

HDCP also supports a key revocation mechanism that is designed to prevent content transmission to hacked devices. If any part of authentication fails or any revoked devices are found in the HDCP tree, the transmitter must stop sending protected content and authentication starts over at Part 1.

Interoperability Issues

Consumers have been plagued with flashing and snowy screens, long authentication times, disabled outputs, and complete failure. Many of the problems can be ascribed to the following causes:

Complexity. The HDCP protocol is managed by a microcontroller running complex state machines. Many manufacturers didn't initially appreciate this complexity when selecting components and establishing development schedules.

Implementation differences. Manufacturers implemented some seemingly minor details in different ways. HPD and RxSense behavior, for instance, isn't well standardized. Small differences can wreak havoc on the HDCP state machines of attached devices and cause video problems for the customer.

Requirement Confusion. There is confusion regarding legal requirements for HDCP. Some device manufacturers have encrypted everything regardless of whether or not the content required it. Some disable analog outputs while HDCP is active. Some restart their content from the beginning upon authentication failure. Others sources completely ignore authentication failures and transmit content anyway.

Repeaters. Adding an HDCP repeater to an installation greatly increases occurrence of problems. Repeaters are especially prone to problems because they have responsibilities of both a transmitter and a receiver. Add multiple inputs and outputs to the repeater, and the problem increase accordingly.

HDMI. HDMI has its own complexity issues. Resolution, color space, and audio problems can't be blamed on HDCP. Furthermore, HDMI problems can cause screen flashing just like HDCP.

Implementing HDMI and HDCP is a complex process that can cause serious problems for those unfamiliar with the layered and nuanced communication required among all devices in the system. Fortunately for our industry and our clients, more sophisticated HDMI solutions are in development and scheduled for release later this year.

This article is excerpted from the engineering white paper, "HDCPP Nuts and Bolts." For the full paper, go to www.crestron.com/hdcp.