

HDMI/DVI HDCP Handshake Problems & How to Avoid Them

By Mark Stockfisch, Quantum Data Inc.

With the advent of affordable 1080p displays, 8-channel 192 kHz sound systems and high-definition A/V sources, consumers are switching to HDMI & DVI uncompressed digital A/V interfaces en masse. Why? Because in many cases these interfaces are the only means to obtain protected content and to maintain pristine quality across long signal chains.

But there's a hitch. HDMI & DVI have a companion high-definition content protection (HDCP) system that sometimes leaves authorized consumers in mute, watching a blank screen, blinking video, or snow while being held hostage by a bug known as the “HDCP handshake problem.”

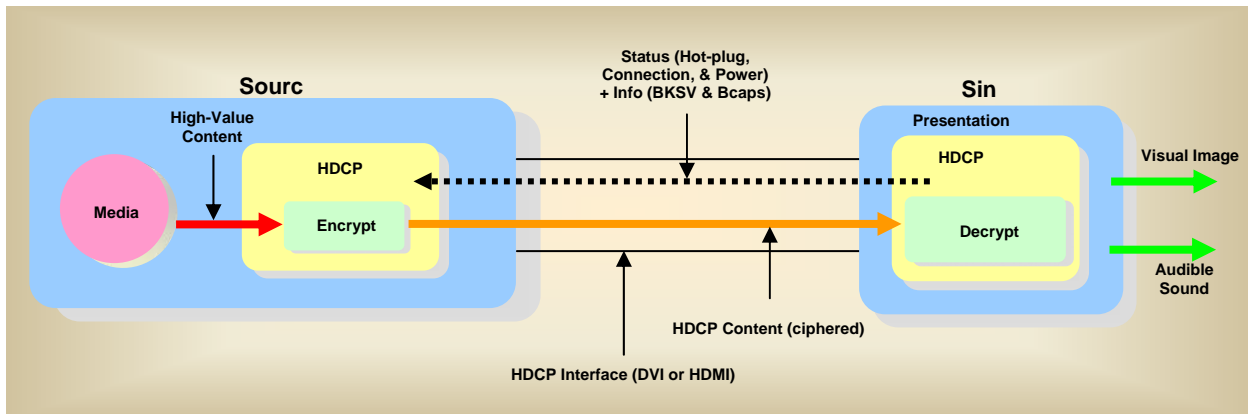
In this article, we'll review the key issues surrounding this problem and introduce you to some rules and tools that'll help you keep your HDMI and DVI design out of trouble.

The Basics

Both HDMI and DVI are HDCP interfaces. HDCP interfaces protect high-value content as it travels between HDCP transmitters and HDCP receivers on its way to presentation devices (see Figure 1). HDCP involves legal issues that are beyond the scope of this article – so you should consult your legal department before finalizing your design. For this discussion, we've boiled all the legal requirements down to three basic rules:

1. An HDCP interface must encrypt high-value content when told to do so. In the case of Blu-Ray and HD DVD players, content is encrypted whenever an Image Constraint Token (ICT flag) is true. Once encrypted, content is referred to as “HDCP content.”
2. HDCP content must stay encrypted until it reaches the presentation device. The only exceptions are outlined in Exhibit C of the HDCP License Agreement (<http://www.digital-cp.com/home/HDCPLicense01262006.pdf>). Exhibit C relaxes this rule slightly for audio, temporary buffering, repeater decrypt/re-encrypt (see Figure 2) and presentation device processing, such as scaling. The current HDCP license agreement assumes wired point-to-point routing, so for now networked A/V products that require LAN-based or wireless interfaces -- such as digital amplified speakers, video walls and the like - will have to wait for a new agreement from DCP LLC that allows transmission of HDCP content over “proprietary interfaces” incorporating encryption methods such as AES-128 and AES-256.

3. The HDCP interface must allow unprotected non-HDCP content to pass unencrypted.



Looking For Trouble

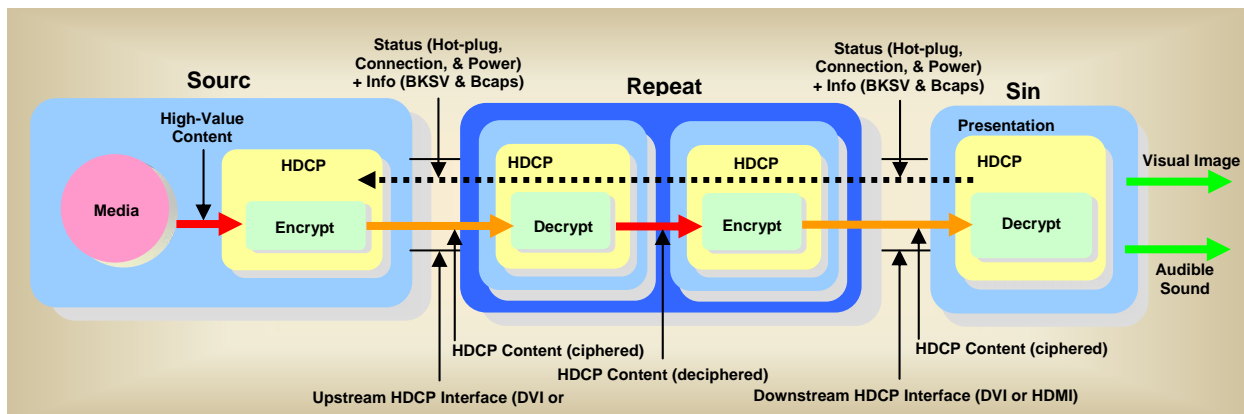
A recent survey of existing products indicates most HDCP problems have simple causes. This is not to say that troubleshooting such problems is always simple. HDCP handshake problems can be totally bewildering if you don't have the specialized tools necessary to detect root causes. Assuming you have the right tools, here are some problems to avoid and guidelines to follow:

HDCP Transmitter Issues

1. HDCP transmitters that don't distinguish between high-value HDCP content and unprotected content will encrypt everything. These source devices won't display anything on a non-HDCP receiver, even if the material being played is an unprotected homemade DVD.
2. There are source products that ignore sink power-cycles, hot-plugs, or reconnects. These sources typically require customers to disconnect and reconnect a cables or power-cycle equipment in order to trigger re-authentication. Sometimes, nothing works. When connecting a source to a repeater, hot-plugs become even more critical as up-stream sources must be informed of all down-stream sink changes. Make sure that your product detects all HDCP-critical sink device state and cabling changes. Make sure your product detects all hot-plugs – even the ones that only last for the minimum 100 milliseconds. Make sure that your source responds to hot-plugs in a timely manner. When you receive a hot-plug, immediately terminate existing display data channel (DDC) tasks and begin a new HDCP handshake.
3. **Doing things too fast can lead to blinking video.** When your HDMI transmitter drives an HDMI receiver, always mute before changing signal timing and un-mute afterwards. Allow the HDMI receiver some time to detect mute and process the timing change before you remove mute. DVI sources must cease transmission and re-authenticate only after signal timing stabilizes and the

receiver has had time to recover. The HDCP circuits in most sinks require stable timing in order to function properly.

4. **Ensure that your HDMI HDCP transmitter can detect and drive a DVI HDCP receiver.** Pay attention to the HDMI capability in the Bcaps register and switch to your HDMI transmitter to DVI-mode if necessary. Alternately, when you read the sink's EDID, look for an HDMI vendor specific data block (VSPD). If you can't find one, switch your HDMI transmitter to DVI mode.
5. **Support repeaters!** More consumers are inserting A/V receivers (AVRs) between their source and presentation products. Unfortunately, not all source products support repeaters. The ones that don't cause systems to stop working when the repeater is inserted. In this case, the innocent repeater manufacturer is often blamed.
6. **Do not transmit HDCP content to non-HDCP or revoked-HDCP receivers.** In the first case, your customers may end-up watching snow. In the latter case, you'll be defeating HDCP's renewability system.
7. **Do not transmit decrypted HDCP content.** This invites content theft and potential legal action.



HDCP Receiver Issues

1. If your sink has an HDMI HDCP receiver, ensure it can interoperate with a DVI HDCP transmitter.
2. Don't assume that all HDMI transmitters support HDCP. Make sure your sink functions with HDMI non-HDCP transmitters.

3. Ensure your HDCP Ri register supports both long and short reads. Most sources do long reads, but your sink may encounter a source that is tweaked for performance and therefore will want to read your HDCP Ri register using short reads.

HDCP Repeater Issues

Repeaters are probably the most difficult products to design. That contributes to the difficulty in finding a fully HDCP-compliant repeater today. Compliant repeaters exist, but what we typically find is varying degrees of non-compliance - ranging from “dangerous” to “almost perfect.”

The most dangerous repeaters forget to re-encrypt HDCP content. Other repeaters forget to forward hot-plugs to upstream devices, a behavior that can lead to loss of signal especially when switching between inputs.

Because source devices are not required to support repeaters, most repeaters on the market today purposely set their repeater bit false and masquerade as no-output presentation devices. Repeaters that properly announce themselves as such, sometimes forget to pass all downstream BKSVs to upstream devices – so they can be checked against the system renewability message (SRM). They also sometimes forget to indicate MAX_DEVS_EXCEEDED or MAX_CASCADE_EXCEEDED, when conditions warrant. The result is that HDCP’s renewability system is again compromised.

To design a compliant repeater with the repeater bit set to true, ensure that your design is compliant and robust. To do this, you must test rigorously. Here are some additional issues to pay attention to:

1. Make sure that your repeater behaves correctly in the presence of multiple format-switching sources and hot-plug-generating sinks.
2. Don't transmit HDCP content to "hidden" receivers; all downstream BKSVs should be made visible to upstream devices.
3. Don't transmit HDCP content to non-HDCP (or revoked-HDCP) receivers operating alone or to a splitter in parallel with a HDCP receiver.
4. Don't encrypt non-HDCP content from non-HDCP sources.
5. Cycle repeater power for each setup and make sure that your system recovers.

6. Make sure HDCP recovers after your repeater switches from one source to another (with a different timing) and back.
7. Make certain that your repeater detects and forwards all hot-plugs to up-stream devices, even if the hot-plug signals only last for 100 milliseconds.
8. When receiving, decrypting and re-transmitting HDCP content, make sure that re-transmitted HDCP content is re-encrypted. If HDCP content is re-transmitted over another interface, ensure the re-transmission is protected using an equally robust encryption method according to rule #2 previously discussed under “The Basics” above. For example, if you intend to decrypt, scale, compress and send protected content across a LAN to a display device, the content must be ciphered at every step along the way.
9. Make sure your list is big enough when building a timing list from data extracted from downstream EDIDs. Recent changes in the CEA-861 standard enable sink devices to declare support for all timings listed in the 861 standard.

General Testing Guidelines

When testing HDCP, test the highest pixel rate format first (e.g. 1080p60). Make sure HDCP recovers after format changes and hot-plugs. Always keep in mind that compliance does not equal interoperability. As we've seen in the case of repeaters, compliance can have a negative effect on interoperability.

Why are we here?

Historically speaking, most HDCP handshake problems can be traced back to missing infrastructure. Peer-reviewed test equipment and certification procedures are critical to any new technology. Unfortunately, in the case of HDCP, these came late. As a result, most products in the field today are non-compliant and interoperability problems abound.

Where are we going?

Quantum Data has joined forces with other industry leaders to solve this problem. The goal is compliance and compliant devices that interoperate.

Last year, DCP released a supplement and compliance test standard. HDCP compliance currently relies on self-policing. So there are no certificates - just information. DCP has established a test lab where HDCP licensees can come and test interoperability with a suite of real products.

Panasonic has developed a tool that it provides to HDMI authorized test centers for required HDCP compliance testing.

Quantum Data is following through with a two-pronged solution that includes grafting HDCP debug and compliance test features onto existing video test instruments - to help design engineers stem the flow of new non-compliant designs entering the market - and creating new tools to help installers isolate problems with legacy products already in the field.

Researchers have used the Quantum Data and Panasonic tools to survey a large cross-section of existing products. Their findings helped establish the list of design best practices discussed in this article. Researchers also have found and corrected weaknesses in the test equipment and the HDCP compliance test standard.

The industry working together is just the start. Designed-in compliance and interoperability is the future. Until then, understanding the issues and knowing how to address them is the next best thing.

About the author

A 30-year veteran of the video display industry, Mark Stockfisch is chief technology officer at Quantum Data, Inc., the inventor and manufacturer of test equipment used to identify and help solve interoperability problems between audio/visual products. All major consumer electronics manufacturers use quantum Data's test equipment. Mark started his career at Motorola Display Systems where he developed the video signal generators, video distribution systems, and systems for characterizing deflection yokes & CRTs needed by the fledgling high-definition computer display manufacturing business. Mark is a member of VESA, IEEE, SID, AES, CEA. He is co-chair of CEA's R4.8 WG7 workgroup, which is responsible for the CEA-861 uncompressed A/V interface standard. Mark also is a former chair of the DDWG DVI compliance & interoperability workgroup. He can be reached at mstockfisch@quantumdata.com