Intel and CPRM/CPPM
Advancing content protection to parallel innovation in the digital home

The technology vision

Intel has played a leading role in both the CPRM and CPPM specifications. These specifications enable both innovative protection for premium entertainment content and flexibility in protected copying for consumers. The first specification, Content Protection for Prerecorded Media (CPPM), protects DVD-Audio, an emerging physical audio format. The second specification, Content Protection for Recordable Media (CPRM), provides a robust mechanism for recording high value content on recordable DVDs, SD Cards, and other forms of recordable media.

Like the Digital Transmission Content Protection specification (see Intel® and DTCP*), Intel helped develop the actual CPPM and CPRM specifications. Intel also promotes their use among content providers (such as movie studios and record labels) and information technology (IT) and consumer electronics (CE) manufacturers.

The CPRM/CPPM specifications define a renewable cryptographic method for protecting entertainment content when recorded on physical media. As part of the group creating these specifications, Intel had three goals:

1. Enable consumer choice, content portability and flexibility in the digital media experience.
2. Protect the rights of content providers and content owners, recognizing their right to be compensated for their intellectual property.
3. Make content protection simple and inexpensive to deploy for PC and consumer electronics (CE) manufacturers.

Intel sees the CPRM/CPPM specifications as another key piece in the overall effort to maximize the experience of digital content throughout the home. The objective is to provide a robust environment without noticeable performance or quality impact for the delivery and consumption of premium entertainment content. This case study discusses the origins of the group that created the CPRM/CPPM specifications, the development and technology behind these specifications, key learnings for Intel along the way, and what lies ahead for the specifications.

Content protection chain example showing where CPRM fits in. The "permitted" outputs shown (for example, 1394* with DTCP* and DVI with HDCP) are examples only—not the only outputs allowed.
The origins of the 4C Entity, LLC. and CPRM/CPPM

In the late 1990s, a new physical audio format was on the way: DVD-Audio. It represented a major advance in audio performance, providing a sampling frequency 4.3 times greater than the traditional RedBook audio CD (the original audio CD format), plus 256 times finer resolution. Its extraordinary dynamic range (up to 144dB versus 96dB for audio CDs) gives outstanding clarity and realism to recordings. But the very quality of this new format amplified the need for even better content management. Such high-quality recordings could lead to equally high-quality copies and the loss of fair compensation for music labels and artists.

Seeing the success of the DTCP specification, Warner Music approached Intel and some of the companies responsible for this specification to see if a new kind of content protection could be created for this next generation audio. An adhoc group of companies consisting of IBM, Intel, MEI, Toshiba and Warner Music began to investigate adapting the Content Scrambling System (CSS) used to protect DVD Video discs for DVD-Audio. The new technology was to be called CSS 2 for DVD-Audio.

At approximately the same time, Intel was in discussions with IBM about an IBM technology called Broadcast Encryption based on Key Blocks. It had been developed originally as a content protection solution to be applied during transmission between devices across a network. The problem was that Key Blocks were large data structures requiring too much overhead while moving content between devices. This disadvantage though didn't apply to recordable media, such as recordable DVDs, where storage space isn't an issue. Thus Intel approached IBM about brainstorming ways their Key Block technology could be applied to protecting content on various forms of physical media.

At this point, an unexpected event created the need for a completely new content protection solution other than CSS 2 for DVD-Audio. CSS for DVD Video was hacked. As a consequence, the music industry wanted nothing to do with any solution based on CSS. They wanted a new approach. IBM and Intel saw great potential for providing this solution through the Media Key Block they were working on and decided to bring in some interested CE companies as well. A group called the 4C Entity was formed that included IBM, Intel, MEI and Toshiba.

"After CSS was hacked, the technical group within the 4C did a fantastic job of coming up in two or three months with an entirely new encryption algorithm with a new approach that was much more robust than the CSS approach had been and is very well regarded today."

- Bruce Turnbull, Partner, Weil, Gotshal & Manges LLP and Chair of the 4C Policy Group

A climate of fear, uncertainty and doubt

The music industry had made its move to digital media with the audio CD nearly 15 years prior to DVD-Audio. Audio CDs from the beginning were unprotected. Long accustomed to making copies of audio tapes and vinyl records with audio tape recorders, people used these same audio tape recorders to copy their audio CDs. When CD recording devices were introduced, people immediately began using them as well to copy audio CDs. As other digital media (such as portable music players) came on the scene, they became additional ways to copy and store music. The digital nature of audio CDs and these recording devices enabled anyone to make perfect copies for personal use, as well as to swap music with friends or over the Internet through peer-to-peer networks. Fearing revenue loss from piracy, the music industry began to see DVD-Audio as both a way to deliver an enhanced listening experience and as a way to introduce copy protection.

From its 5C experience, Intel and other members of the 4C believed the most effective copy protection effort would come from a small number of very focused companies willing to work together, make a significant investment, and develop the necessary technologies. The fundamental goal for all these companies was to enable the ecosystem rather than profit directly from the adoption of the technology itself through intellectual property royalties. Initial attempts to include music labels in early discussions slowed progress because of the sheer number of participants and the differences in technological expertise. The 4C decided to forge ahead alone. The intention was to develop a technological solution and then engage the music labels in discussions on its use and adoption.

Since content protection was such an important issue for the music industry, the labels started a standards effort of their own, the Secure Digital Music Initiative (SDMI). Their goal was to develop specifications for a
content protection system to be enforced by future music players/recorders. They sought to hinder unauthorized copying by various technologies such as audio watermarking. Because of the high membership in this group (over 100 companies), their progress was significantly slower. Recognizing the importance of having the SDMI understand the 4C efforts and use the 4C technology, the 4C participated in SDMI and ended up working with them on several important issues.

**Media key block technology (making dumb plastic smart)**

The problem faced by the 4C with DVD-Audio (and later recordable DVDs) was fundamentally much different than earlier content protection solutions addressing transmission of media. In the case of Internet delivery for instance, the two devices on either end of the transmission are active and intelligent enough to be able to establish their mutual compliance with the content protection specification governing the particular content they're exchanging. The necessary key is then provided to decrypt it. In the case of DVD-Audio, content comes in encrypted form on a passive piece of plastic that can't communicate with a device to verify its compliance. Early solutions to this communications problem involved trying to make the plastic smart by embedding a chip in it or other methods. These solutions didn't work, were too expensive, or proved otherwise impractical.

Media Key Block technology represented a major breakthrough because it enabled a plastic disc to implicitly authenticate the device that is trying to play it. The Media Key Block is a table (an array of up to 65,636 rows and 16 columns) of encrypted values that is provided to licensed media manufacturers. Protected prerecorded DVD-Audio discs each have this table stored on them. Compliant devices (players, player/recorders) are given a unique set of keys. If a device has a valid set of keys, it is able to process the Media Key Block and derive the cryptographic key that is used to decrypt the content that is on the disc. Processing requires a device to perform a complex sequence of mathematical operations to extract a Media Key from the Media Key Block. The device then combines that key with the Album Identifier to create a base decryption key.

What if a device doesn't have a valid set of keys? Then it's not a compliant device and won't be able to play protected DVDs. If it's discovered that a set of keys has been stolen from a compliant player through reverse engineering or some other approach, the thieves can be thwarted in a short amount of time. The 4C can modify specific locations in the Media Key Block and issue this modified Media Key Block for use on all subsequent protected prerecorded DVD-Audio discs. If a device with the stolen key attempts to play one of the newer discs, the modifications in the Media Key Block's data structure trigger this device to calculate an incorrect key. The player is then unable to decrypt the content and is useless for playing the disc.

Media Key Blocks are unique for every DVD-Audio title and reissued every three months to enable quick invalidation of any noncompliant devices. Naturally, these changes are imperceptible to normal users. Their devices continue to play DVD-Audio titles no matter what the Media Key Block. The technology is designed to stop piracy, not normal usage and recording.

**Five additional 4C innovations to content protection**

The 4C brought five more innovations to content protection, each of which we briefly describe here.

**New set of cryptographic techniques**

The 4C studied CSS technology and concluded that two limitations led to it being cracked. At the time CSS was created, export rules limited it to 40-bit encryption. That was one weakness. The other was that the technology hadn't been subjected to a high enough level of scrutiny. Once CSS was broken, many flaws were found in its cryptography that made it more susceptible than originally thought.

Fortunately for the 4C, export rules changed as the group began work on its solution. Consequently, CPPM employs a more robust 56-bit encryption based on a different algorithm. To ensure a more airtight cryptographic solution, the 4C did a thorough review of current cryptographic techniques, employing outside cryptographic consulting firms and doing more thorough reviews themselves. The result is a solution replacing the CSS single Player Key with a set of 16 secret Device Keys issued to every licensed
manufacturer of hardware or software players. Of course, the centerpiece of CPPM’s cryptographic innovation is the Media Key Block.

**Making a content protection specification a public process**

Though public review of encryption-based technologies in other applications was widely accepted, content protection specifications and encryption technologies had always been treated as highly confidential information. The 4C turned that thinking on its head and did something almost unheard of. It initiated public review of cryptographic algorithms for content protection technologies. Departing from the usual secrecy, the group invited public review of and comment on the algorithms. CPPM and CPRM thus achieved a higher level of scrutiny and gained the confidence of all parties before being implemented as a solution.

"Everyone had previously thought that we should keep all this stuff secret. Security through obscurity was going to make things more robust. The 4C dramatically departed from that approach by making its specifications public."

- Brendan Traw, Intel Fellow, Director, Content Protection Architecture

**Audio watermarking**

Music labels wanted an embedded signaling technology called an audio watermark to protect DVD-Audio content that gets out through an analog output. Encryption, key exchange and authentication were all great in the digital world, but the labels felt that when content was transferred to the analog domain, technologies like audio watermarks were required to keep content protection rights intact and protect against any further recording back to a digital form. The 4C launched a thorough technology evaluation and selected an audio watermark technology from an outside vendor. Fortunately, the SDMI selected the same technology as 4C, preventing the possibility and unnecessary complication of two watermarks. Today, through CPPM, a watermark enables digital media players/recorders to recognize that analog content derived from DVD-Audio is protected and can only be used according to the rights granted the user.

"Watermarking is basically a way to embed content protection information into content in a way that isn’t perceivable to the viewer or listener, but can be detected by equipment that knows how to look for this mark."

- Mike Ripley, Intel Content Protection Architect

**Content Protection System Architecture—seeing the big picture**

CPPM and CPRM are just two of the many content protection solutions being used and under development today. This ever-growing number of content protection solutions created a unique challenge for the content, CE and IT industries. It was becoming difficult for companies to keep all of the technologies straight and fit all the pieces together for a comprehensive solution. Nobody had ever written and published a systematic and comprehensive overview of how all of these technologies are supposed to work together with digital and analog devices and all the various forms of transmission. This omission was sure to slow adoption and proper usage of the technologies.

The 4C decided an overall architecture incorporating current solutions and guiding future solutions was needed. In response, the 4C produced Content Protection System Architecture (CPSA). This was a seminal thought piece clearly laying out how content protection solutions work together and the role of each current technology. CPSA also includes a set of examples showing from a conceptual point of view where cryptography, watermarking, and all the other elements fit, not just from a 4C perspective, but as an overall content protection system. Probably the most important part of CPSA are 11 axioms (self-evident truths or maxims) that describe how CPSA-compliant devices handle three major areas—content management information, access and recording—critical to ensuring a comprehensive, consistent content protection scheme. These axioms and the CPSA white paper still guide how the content protection ecosystem thinks about content protection and continuing work in the field.

"Content protection requires certain actions on the part of the content owners, on the part of the playback devices, on the part of recording devices, and it all needs to be addressed by a consistent and coherent mechanism. This drove our focus on an overall system architecture, CPSA."

- Mike Ripley
Managed copies

The 4C believed that maintaining reasonable and customary use was an important concept in introducing next-generation technologies. People long accustomed to making personal copies of audio CDs on tape or other media would expect the same with DVD-Audio. If DVD-Audio were introduced and no copying was permitted, Intel and others felt it would be rejected by consumers. Consequently, Intel championed the idea of "managed copies." This involved finding a way to permit people to make at least one digital copy of CPPM-protected DVD-Audio content while at the same time preventing indiscriminate redistribution. This means being able to include copy-control information as part of the content-management information on the disc.

Content Protection for Recordable Media (CPRM)

While the 4C was working on CPPM (content protection specific to DVD-Audio), the group foresaw the need for a companion solution to handle the digital copies that could be made from music and video downloads as writable DVDs and SD Flash Memory cards became widespread. The solution, CPRM, employs a similar methodology as CPPM, only instead of protecting recorded media, it binds copyrighted recordings to unrecorded media. It allows protected content to be recorded on a blank disc (or other media), but doesn't allow that content to then be indiscriminately copied from this disc to other blank media.

CPRM uses a CPPM-style Media Key Block. Every writable DVD blank (or other protected recorded media) has an indelible 64-bit Media ID embossed in a hidden area of the disc. This ID specifies the type of media and its manufacturer. It also includes a 40-bit serial number unique to the disc. When someone copies copy-protected content to a disc, CPRM encrypts it with a multistage process that uses the Media ID to generate encryption and decryption keys. If a person then tries to copy the protected content on this disc, the new blank disc is recognized as having a different Media ID and the content isn't properly decrypted. By not allowing one formerly blank disk to copy to a new blank disk, CPRM prevents a chain of copies. On the other hand, it does permit DVD blanks to be used to make a single copy.

The 4C today

While DVD-Audio as a market category has only had limited success so far, 4C content protection has been widely implemented in PC and CE devices. The SD card, which uses the 4C's CPRM technology, has been phenomenally successful—a testament to both the inherent attributes of the SD card in size and form factor, as well as the fact that it's a protected format. Sales of DVD recorders are on the rise and CPRM technology is the dominant form of content protection. CPRM is used in the DVD-R, -RW and -RAM formats.

The 4C is now investigating getting into content protection for eBooks, interactive games, and potentially personal media such as consumer medical records. The 4C is also investigating using its technology with other systems, such as Microsoft Windows Media digital rights management (DRM). The 4C's CPSA continues to provide the framework for content protection technology efforts aimed at the digital home.

A major role of the 4C continues to be license agreements. When a manufacturer gets a 4C key for production of a recorder or player, the company has to sign a license agreement that it will make a product that follows specific rules in handling content. The 4C has developed the specifics of this license through extensive negotiations with record labels and movie studios.

Key learnings

Through the formation of the 4C, the development of CPPM and CPRM, and co-authoring CPSA came many key learnings—both about content protection and working with companies in different industries toward a similar objective. Many of these learnings are summarized here.

Know your customer

In the case of the 4C, the customer for the technology was the content industry. Nonetheless, the 4C quickly discovered there were major differences between the movie industry and the music industry—even when
they’re part of the same family, such as Warner Music and Warner Brothers. The business concerns of the two industries are quite different. To meet each industry’s needs, it was important to understand their unique issues and concerns. (Note: Warner Music and Warner Brothers are no longer affiliated, but were when the 4C was working on CPPM/CPRM.)

**Respect your customer (particularly their expectations)**

For content protection of DVD-Audio, one of the 4C’s first assumptions was that consumers would expect to be able to make at least one copy. After all, consumers have been able to copy their audio CDs, why not DVD-Audio as well? The 4C felt the ability to back up a DVD-Audio purchase was essential to the success of this new media. The music industry disagreed and it took a long time to resolve this difference. In fact, it basically stalled the format for several years and this delay may be partly responsible for the slow acceptance of DVD-Audio in the marketplace.

**Watch out for unintended consequences**

The idea for a watermark was essentially a request from the music industry. Fortunately, both the 4C and music industry were able to voluntarily agree on one watermark technology. Unfortunately, an unintended consequence was an attempt by the movie industry to make watermarking a legislative mandate. The danger here was they wanted watermark detection technology in nearly every product that might touch digital media (such as routers), including many places where it was intrusive in product design and unnecessary. There was also the issue that such a law would set a bad precedent with respect to using legislation to dictate content protection and product design. In response, the IT industry vigorously lobbied Congress to avoid a watermark mandate, consuming huge amounts of time and effort, and setting back discussions between the industries.

**If you build it, market it**

The 4C was set up as an organization to develop technologies and then license them to companies. No marketing arm was really created. It was felt that “if you build it, they’ll use it.” As a consequence, promoting the 4C and its solutions has fallen on the shoulders of the founders. The lack of a strong marketing group within the organization has slowed the acceptance and use of the 4C technologies. The 4C didn’t do as good a job as it should have of explaining its technology to the individual music labels and film studios.

**To develop better encryption, give everybody a look**

It may seem counterintuitive, but to build a more robust solution that would be easily accepted by the industry, the 4C decided to make its specifications available for public review and commentary. This enabled world-class cryptographers, universities and others to validate the algorithms and other technological innovations of the solution. The result was a pair of specifications that were already endorsed before being implemented in any device or media.

**Don't forget the big picture**

Initially, content protection began as individual solutions targeted to specific applications. The 4C was no different. It first developed only a solution for DVD-Audio. But the 4C quickly realized that the plethora of content protection solutions, digital devices and transmission options required an overall system architecture that could guide product manufacturers in selecting content protection technologies and assure content providers their content was protected within the overall framework. In reaction, the group produced CPSA, a conceptual explanation of how content protection technologies can and do work together. Today, CPSA continues to provide the framework for most content protection efforts, reducing confusion, and helping foster the growth of the digital entertainment industry.

**What lies ahead**

CPPM and CPRM made great technological strides over the earliest widely adopted content protection technologies. Today, 4C technology is in a position to be a connective technology for many of the digital-
rights-management systems coming out from Microsoft and other companies. It’s a complimentary technology, perfect for SD Cards and other media that could be used to make copies of music or video content.

Today the 4C's role is to port the solution to different media formats and get it approved in other usages so that it's interoperable. For example, the 4C is working with Cable Labs to approve CPRM for the recording of conditional access content. CPRM has also been approved by the Federal Communications Commission (FCC) for recording digital TV broadcasts that have the broadcast flag inserted in them.

As the transmission of video becomes increasingly digital via cable, satellite, broadband and broadcast, new issues in content protection will surface. Consumers may soon become more aware of new limitations to things they are used to doing. What may bring this to a head is a burgeoning increase in video content protection that goes beyond the rudimentary protection of DVD video. The 4C and other content protection organizations would be well advised to start educating consumers on the nature of the freedoms and restrictions they will see as homes and the content coming to and from them grows increasingly digital.

"I think that a big challenge for all content protection or digital rights management systems is to explain to consumers what they can do and what they can't do. It's hard because explaining what you can't do isn't great marketing. But we are on the cusp of there being sufficient confusion in the consumer marketplace that this is going to be a big issue''

- Bruce Turnbull

Learn more

Discover more about Intel's work in content protection by visiting the following areas of the Intel Web site:

- The digital home: content protection
- Protecting content in the digital age: balancing creative use with creator rights
- Content protection in the digital home Intel Technology Journal, volume 6, issue 4.
- Intel® and DTCP*: protecting premium content and its use in the digital home

"You can use encryption, key exchange and authentication in the digital world, but when you transfer over to the analog domain, you have to use other technologies, like watermarks. By creating CPSA, the 4C developed a foundation for how to move in and out of the digital and analog domains that is very much in use today."

- Stephen Balogh, Business Development Manager