How CPRM & CPPM Work

Flexible Protection for Digital Content

January 2008

IBM, Intel, Panasonic and Toshiba formed the 4C Entity to develop technologies that will enable premium copyright-protected content to be shared on a wide range of electronic devices built by multiple manufacturers. 4C Entity is working to provide consumers with flexible access to all forms of digital content, while ensuring that the content is high quality, easy to store and maintain, transferable to similar digital devices and copyright-holder friendly.

4C Entity has developed a solution: Content Protection for Recordable Media (CPRM) and Content Protection for Pre-recorded Media (CPPM). The CPRM/CPPM specification defines a renewable cryptographic method for protecting entertainment content when recorded on removable and portable physical media including, but not limited to, DVD media and Flash memory.

The Complete Solution

The CPRM/CPPM specification was designed to meet the robustness and renewability requirements of content owners while balancing the implementation needs of both the consumer electronics and PC industries. Multimedia applications enabled by 4C technologies are creating vast new market opportunities for content providers, service providers, application developers and device manufacturers. By using 4C Entity standards, device manufacturers can offer consumers a wide range of choice for the authorized sharing of premium content among digital devices while reducing long development times and resources.

Content protection solutions combine technical and legal mechanisms to protect content. The technical mechanisms take the form of a cryptographic protocol through which content is distributed or stored in an encrypted form. Access to the cryptographic keys necessary to decrypt the protected content is subject to a license. Thus, cryptographic technology implementations provide the basis for content protection, while an effective licensing structure provides for enforcement.

There are two primary technical components of CPRM/CPPM: the C2 cipher and the Media Key Block.

The C2 Cipher

C2 is a 10-round Feistal network block cipher with a 64-bit block size and a 56-bit key. The C2 cipher is used to both encrypt and decrypt content and also as the basis of one-way and hash functions. The 4C companies designed and adopted C2, because no prevalent cipher was identified to provide the necessary balance between suitability of hardware and software implementation, minimal licensing fees, and the ability to be exclusively licensed for use in 4C content protection solutions. This last attribute is particularly important, as circumvention of the 4C technologies will likely require use of the C2 cipher algorithm, which must be licensed from the 4C Entity. This provides an added legal mechanism to protect content.

Media Key Blocks

Media Key Blocks (MKBs) are tables of cryptographic values that implement a form of broadcast key distribution, and provide for renewability in 4C content protection solutions. Each writable DVD disc that supports CPRM carries a Media Key Block (MKB) as read-only data stored in the lead-in area and a unique media identifier (Media ID) stored in the burst-cutting area, a region that is uniquely written on each disc in a manner that cannot be recorded or modified with consumer DVD equipment. MKBs are generated by the 4C Entity and enable compliant licensed products to calculate a common media key. Each licensed product (including both hardware and software) is given a set of Device Keys when manufactured (also provided by the 4C Entity), which are used to process the MKB to calculate the media key. Device Key sets may either be unique per device, or used commonly by multiple devices (the 4C licenses describe the details and requirements associated with these two alternatives).

If a set of device keys is compromised in a way that threatens the integrity of the system, updated MKBs can be released on the new generations of media that cause the compromised set of keys to calculate a different media key than is computed by the remaining compliant devices. In this way, the compromised device keys are “revoked” by new MKBs. In existing 4C solutions, MKBs are carried on compliant portable storage media, and devices use the corresponding medium’s key as the basis for encrypting and decrypting protected content stored on that medium.