МОСКОВСКИЙ ФИЗИКО-ТЕХНИЧЕСКИЙ ИНСТИТУТ
(ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ)

# Защита от копирования на перезаписываемых носителях (Copy Protection for Recordable Media)

**Эссе по курсу «Теория защиты информации» студента**
012 группы ФРТК Колмычевского И.А.
Долгопрудный 2004

# Введение

CPRM (Content Protection for Recordable Media) – это метод защиты от неавторизованного копирования и воспроизведения цифровых данных для различных типов физических носителей, таких как: портативных ATA устройств, CD, DVD-R, Audio DVD, Video DVD, flash и пр. В этом эссе делается краткий обзор CPRM, определяются криптографические процедуры, являющиеся общими для различного использования. Также более подробно излагаются особенности для DVD-R и DVD-RW носителей.

Данная технология защиты является результатом коллективного творчества «Организации 4 компаний» или «4C Entity»: Intel Corporation, International Business Machines Corporation, Matsushita Electric Industrial Co. и Ltd. Toshiba Corporation.

При проектировании технологии учитывались следующие критерии:

- удовлетворять требованиям безопасности при попытке воспроизведения копии.
- применимость для аудио и видео содержанию.
- простота реализации для ПК и прочих устройств.
- применимость для различных носителей.

Система основывается на следующих технических элементах:

- Управление ключами для взаимозаменяемых сред
- Кодирование содержания
- Воспроизведение зависящее от носителя

CPRM появился в 2000-м году, но пик популярности обрёл лишь в 2001. Данная методика в основном предназначалась для защиты различного рода трансляций. Например, слушая радио или просматривая фильм, вы можете беспрепятственно всё записывать и даже сделать копию, но вот воспроизвести копию вы уже не сможете. Также CPRM без труда стал применяться и к уже записанной информации, будь то фильм или музыкальный альбом. В том же 2001-м году были проведены попытки перенести CPRM на ATA интерфейс, т.е. на HDD. Но, встретив сильное сопротивление со стороны общественности, от этого отказались. Дело в том, что в новых условиях у пользователей будут возникать серьезные проблемы даже при выполнении самых обычных процедур типа профилактической дефрагментации диска или резервного копирования вполне законно приобретенных файлов и программ [2,3].

## Некоторые сокращения и аббревиатуры

$[x]_{msb\_z}$ = z старших разрядов числа x.

$[x]_{lsb\_z}$ = z младших разрядов числа x.

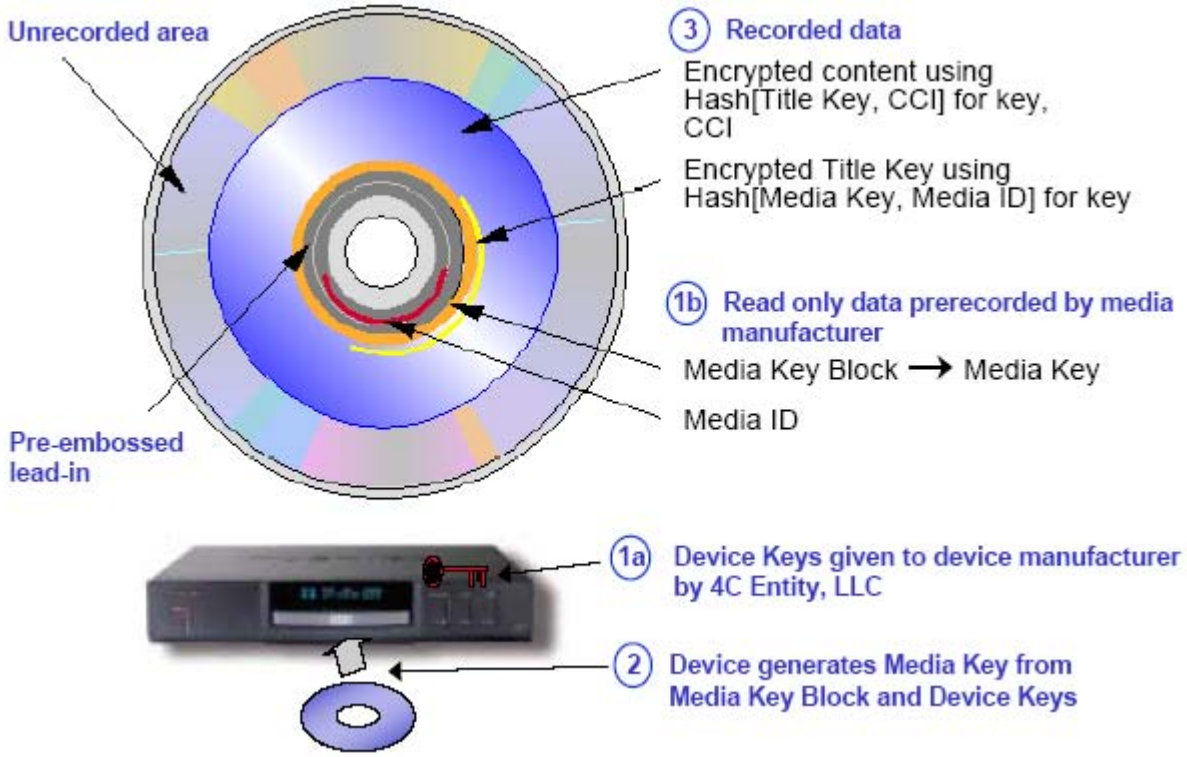
$[x]_{y:z}$ = биты между битом y и битом z в числе x.

4C = 4 компании (IBM, Intel, MEI, и Toshiba)

C-CBC = преобразованное сцепление блочного шифрования

C2 = Cryptomeria Cipher

## Общее описание




На рисунке продемонстрирован простой пример того, как система работает. Конкретные детали компонентов накопителя и криптографическое управление ключами сильно зависит от типа DVD и других поддерживаемых сред и приложений.

Шаг 1а. 4C обеспечивает секретным ключом производителей для встраивания оного в каждое производимое устройство.

Шаг 1б. Производители размещают Media Identifier и Media Key Block выданный 4C в каждый экземпляр накопителя.

Шаг 2. Когда носитель помещается в устройство чтения/записи, устройством генерируется секретный Media Key, используя собственные secret keys и Media Key Block, сохранённый на носителе.

Шаг 3. Данные сохранённые на носителе расшифровываются/шифруются посредством Content Key полученного из однонаправленной функции от secret Title Key и копии контрольной информации (CCI) связанной с содержанием. Title Key шифруется и сохраняется на носителе используя ключ полученный от однонаправленной функции от Media Key и Media ID. С другой стороны, действительные детали формирования ключей могут сильно зависеть от используемого приложения.

Зашифрованные данные с защищённого CPRM-носителя можно скопировать на другой CPRM-носитель. Также можно скопировать и заголовок, в котором хранится Content Key. Однако мы не сможем скопировать (записать на копию) Media Key и не сможем скопировать MKB (по крайней мере, это маловероятно). Соответственно, устройство будет не в состоянии получить с копии такого носителя Content Key и не сможет расшифровать записанные на таком носителе данные.

В CPRM также предусмотрен механизм отзыва секретных ключей устройств. Данная возможность была включена в стандарт, в связи с возможным взломом оных. Подробности механизма можно найти в документации и в [5].

Функции: Описание общих криптографических функций, используемых CPRM для различных приложений и типов носителей.

C2 Алгоритм блокового шифрования:

Общая криптографическая функция используемая для CPRM основывается на C2 блоковом шифре. Здесь приводится описание двух основных режимов работы C2 шифра: режим электронной кодовой книги (ECB) и C-CBC режим.

**1** C2 Block Cipher in Electronic Codebook (ECB) режим

ECB представлена функциями

C2_E(k, d)

Где k это 56-битный ключ, d это 64-битовое значение данных для шифрования, и C2_E возвращает 64-битный результат.

C2_D(k, d)

Где k это 56-битный ключ, d это 64-битовое значение данных для расшифрования, и C2_E возвращает 64-битный результат.

**2** C2 Block Cipher in Converted Cipher Block Chaining (C-CBC) режим

C2 шифр используется в C-CBC режиме для шифрования и расшифрования содержания защищаемого при помощи CPRM.

C2_ECBC(k, d)

Где k это 56-битный ключ, d фрейм данных, и C2_ECBC возвращает зашифрованный фрейм.

C2_DCBC(k, d)

Где k это 56-битный ключ, d фрейм данных, и C2_ECBC возвращает расшифрованный фрейм.

Размер фрейма зависит от конкретного формата приложения.

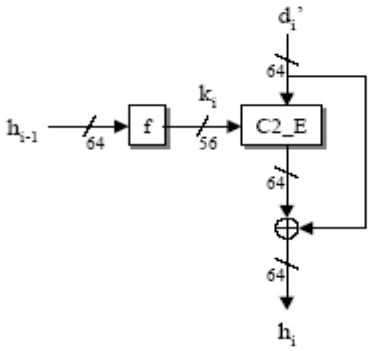
C2 Хэш-функция

C2_H(d)

Где d – входные данные произвольной длины, и C2_H возвращает 64-битный результат.

Для вычисления хэш данные подгоняются дописыванием нулей так, что новая длина становится кратной 64-м битам.

Подогнанные данные d’ делятся на n блоков длиной 64-бита: $d_1$’,$d_2$’,…$d_n$’, которые используются как показано на рисунке:




Функция преобразования f определяется как

$f(x) = [x]_{lsb\_56}$

где x это 64-бита входных данных.

4C Entity обеспечивают 64-бита начального значения $h_0$ для лицензирования CPRM для носителей и приложений в которых используется C2 хэш-функция.

Дальнейшие вычисления делаются рекурсивно для i от 1 до n:

$k_i = f(h_{i-1})$

$h_i = C2\_E(k_i, d_i') \oplus d_i'$.

Значение $h_n$ это конечный результат хэш, т.е. $C2\_H(d) = h_n$.

C2 односторонние функции

$C2\_G(d_1, d_2)$

Где $d_1$ это 56-бит входных данных, $d_2$ это 64-бит входных данных, и C2_G возвращает 64-битный результат.

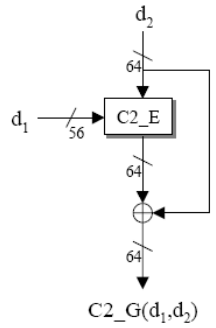
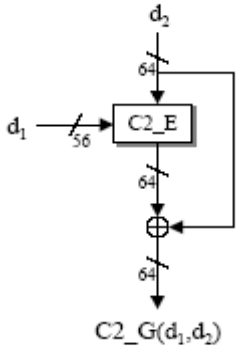



**Figure 2-2 – C2 One-way Function**

$C2\_G(d_1, d_2) = C2\_E(d_1, d_2) \oplus d_2$.

Криптографическое управление ключами

В этом разделе описывается общая процедура управления CPRM ключами, изображенная на рисунке, которая использует Media Key Block для обеспечения чтения копий, и Media Identifier - индивидуального идентификатора носителя.




• Device Keys ($K_{d\_0}$,$K_{d\_1}$,…,$K_{d\_n-1}$) используются для декодирования одного или более элементов Media Key Block (MKB), в порядке извлечения секретного Media Key ($K_m$).

• $K_m$ и Media Identifier ($ID_{media}$) комбинируются, при помощи C2 One-way Function, для получения Media Unique Key ($K_{mu}$).

Длины ключей и переменных представлены в таблице

| Ключ или переменная | Размер |
|---|---|
| Device Keys ($K_{d\_0}$,$K_{d\_1}$,…,$K_{d\_n-1}$) | 56 бита каждый |
| Media Key Block (MKB) | произвольный, кратный 4-м байтам |
| Media Key ($K_m$) | 56 бит |

| | |
|---|---|
| Media Identifier ($ID_{media}$) | 64 бит |
| Media Unique Key ($K_{mu}$) | 56 бит |

**1** Вычисление Media Key ($K_m$)

**1.1** Device Keys

Каждому CPRM устройству приписывается совокупность секретных Device Keys при производстве. Эти ключи выдаются 4C для использования с MKB, чтобы вычислить $K_m$. Ключ может быть уникальным или общим на группу устройств.

Каждое устройство получает n штук Device Keys: $K_{d\_i}$ (i=0,1,…,n-1). Все ключи хранятся в таблице n*n. Причём на каждую колонку приходится не более одного ключа, однако в строке может быть несколько ключей. Конкретное количество Device Keys зависит от типа устройства. Как сами Device Keys, так и их местоположения является не доступной для обычного пользователя информацией.

**1.2** Media Key Block (MKB)

Процедура управления ключами использует Media Key Block (MKB) чтобы было возможным делать копии. MKB выдаётся 4C и позволяет всем устройствам, использующим secret Device Keys, вычислить $K_m$. В случае, если на стадии вычисления $K_m$ произошла ошибка, то возвращается значение $00000000000000_{16}$.

MKB формируется как последовательность непрерывных записей. Каждая запись начинается с 1-го байта Record Type, затем 3 байта Record Length. Длина Record всегда кратна 4-м байтам. Поля Record Type и Record Length никогда не шифруются. Последующие поля могут быть зашифрованы C2 шифром в ECB режиме, в зависимости от Record Type.

Используя собственные Device Keys, устройство вычисляет $K_m$, обрабатывая MKB один за одним, по порядку, от первого до последнего. $K_m$ вычисляется рекурсивно, и результатом, показанным на рисунке, является последний $K_m$. Конкретная процедура вычисления данного ключа сложна и занимает 7 страниц оригинальной спецификации, поэтому здесь она приводится не будет.

**2** Вычисление Media Unique Key ($K_{mu}$)

**2.1** Media Identifier ($ID_{media}$)

Каждый экземпляр носителя должен содержать индивидуальный идентификатор. Этот идентификатор не является секретным, и располагается а области доступной только на чтение.

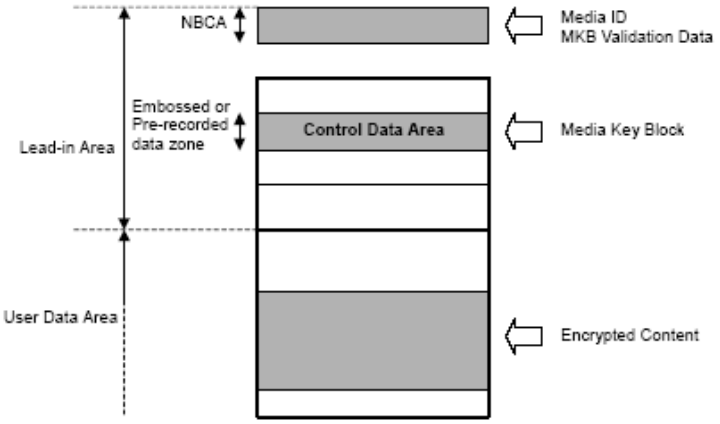
**2.2** Media Unique Key ($K_{mu}$)

CPRM криптографическое управление ключами использует Media Unique Key ($K_{mu}$), чтобы шифровать данные. $K_{mu}$ вычисляется с использованием $ID_{media}$ вычисленным ранее и $K_m$ следующим образом:

$K_{mu} = [C2\_G(K_m, ID_{media})]_{lsb\_56}$.

# CPRM компоненты для DVD-R и DVD-RW

Предполагается что читатель знаком с DVD-R и DVD-RW форматами и фокусируется внимание на те аспекты формата, которые непосредственно связаны с CPRM защитой. На рисунке приводится общее представление о положении CPRM элементов на DVD-R и DVD-RW носителях.




- Идентификатор носителя (IDmedia) записан в Narrow Burst Cutting Area (NBCA).
- Media Key Block (MKB) Validation Data записан там же.
- Media Key Block (MKB) записан а начале раздела.
- Зашифрованное содержание располагается в площади предназначенной для пользователя.

Кроме того, прочие специфические компоненты связанные с CPRM могут также храниться в User Data Area.

**1 Media Identifier и MKB Validation Data**

CPRM-совместимые DVD-R и DVD-RW носители должны содержать 64-бит Media Identifier (IDmedia) и 16-байт MKB Validation Data, расположенные в NBCA производителями. NBCA может содержать множество последовательных блоков данных, называемых BCA Records, причём каждый содержит информацию для различного использования. Каждый BCA Record начинается с 2-х байт BCA Record ID, затем 1 байт Version Number field, затем 1 байт Data Length (указывающий длину остальных данных в байтах). Устройство не должно использовать конкретное положение или размер данной BCA Record, и должно вместо того, чтобы использовать поля BCA Record ID и Data Length, идти от одной Record до другой, пока не найдёт желаемую Record. Для CPRM-совместимых DVD-R и DVD-RW носителей, NBCA должна содержать BCA Record и MKB Validation Data, чьи форматы показаны в таблице.

| Byte \ Bit | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 |
|---|---|---|---|---|---|---|---|---|
| 0 | (msb) | | | BCA Record ID: $0002_{16}$ | | | | |
| 1 | | | | | | | | (lsb) |
| 2 | Version Number: $01_{16}$ | | | | | | | |
| 3 | Data Length: $08_{16}$ | | | | | | | |
| 4 | (msb) | | | | | | | |
| : | | | | Record Data: Media Identifier | | | | |
| 11 | | | | | | | | (lsb) |
| 12 | (msb) | | | BCA Record ID: $0003_{16}$ | | | | |
| 13 | | | | | | | | (lsb) |
| 14 | Version Number: $01_{16}$ | | | | | | | |
| 15 | Data Length: $10_{16}$ | | | | | | | |
| 16 | (msb) | | | | | | | |
| : | | | | | | | | |
| : | | | | Record Data: MKB Validation Data | | | | |
| : | | | | | | | | |
| : | | | | | | | | |
| 31 | | | | | | | | (lsb) |

Поле BCA Record ID указывает на необходимость использовать BCA Record. Значение $0002_{16}$ указывает на Media Identifier Record, а значение $0003_{16}$ указывает на MKB Validation Data Record. Для Media Identifier Record поле Data Length field указывает длину в байтах последующего поля Record Data, что составляет $08_{16}$ для $01_{16}$–й версии. Media Identifier сам по себе содержит поле Record Data, чей формат указан в таблице для DVD-R и для DVD-RW.

| Byte \ Bit | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 |
|---|---|---|---|---|---|---|---|---|
| 0 | Reserved: $0000_2$ | | | | Type: $0001_2$ | | | |
| 1 | Manufacturer ID | | | | | | | |
| 2 | | | | | | | | |
| 3 | Serial Number | | | | | | | |
| 4 | | | | | | | | |
| 5 | | | | | | | | |
| 6 | | | | | | | | |
| 7 | | | | | | | | |

| Byte \ Bit | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 |
|---|---|---|---|---|---|---|---|---|
| 0 | Reserved: $0000_2$ | | | | Type: $0010_2$ | | | |
| 1 | Manufacturer ID | | | | | | | |
| 2 | | | | | | | | |
| 3 | Serial Number | | | | | | | |
| 4 | | | | | | | | |
| 5 | | | | | | | | |
| 6 | | | | | | | | |
| 7 | | | | | | | | |

Для MKB Validation Data Record поле Record Data имеет следующий вид

| Byte \ Bit | 7 | 6 | 5 | 4 | 3 | 2 | 1 | 0 |
|---|---|---|---|---|---|---|---|---|
| 0 | MKB_Hash | | | | | | | |
| : | | | | | | | | |
| 7 | | | | | | | | |
| 8 | MKB Verification Data ($D_v$) | | | | | | | |
| : | | | | | | | | |
| 15 | | | | | | | | |

.

Поле MKB_Hash содержит 8-ми байтный хэш сопровождающий MKB и замыкающийся нулями в случае необходимости. Вычисляется как

MKB_Hash = C2_H(MKB and trailing zeros).

MKB_Hash используется чтобы удостоверится в целостности MKB при копировании оного с носителя (drive) на устройство (host) используя аутентификацию. Стоит заметить, что MKB_Hash может быть вычислена при помощи иной формулы, приведённой выше. Протокол утверждения MKB учитывает этот факт.

Поле MKB Verification Data (Dv) содержит 8-байтное значение равное значению поля Verification Data Verify Media Key Record в MKB, т.е

$Dv = C2\_E(Km, DEADBEEF_{16} \,||\, XXXXXXXX_{16})$

где Km это правильный Media Key, и $XXXXXXXX_{16}$ это произвольное 4-х байтное число. Устройство которое не использует drive-host аутентификацию должно выполнять её для Media Key вычисленного из MKB, прочитав значение Dv из NBCA и использовав его для подтверждающего условия

$[C2\_D(Km, Dv)]_{msb\_32} == DEADBEEF_{16}$

где Km это Media Key вычисленный при помощи Process_MKB.

Устройство не должно использовать Km для проигрывания или записи зашифрованных CPRM данных пока это условие справедливо. Стоит заметить, что поле Verification_Data Verify_Media_ Key_Record в MKB само не должно использоваться для проверки аутентификации Media Key.

**2 Media Key Block (MKB)**

CPRM-совместимые DVD-R и DVD-RW носители должны содержать MKB и MKB Descriptor, объединённые вместе в MKB Frame. План размещения Control Data Area показан в таблице.

| ECC Blocks | Sectors | | |
|---|---|---|---|
| | 0-1 | 2-3 | 4-15 |
| 0-15 | Already Defined | Reserved | MKB Pack #0 |
| | | | ... |
| | | | MKB Pack #15 |
| 16-31 | | | MKB Pack #0 |
| | | | ... |
| | | | MKB Pack #15 |
| ... | | | ... |
| 160-175 | | | MKB Pack #0 |
| | | | ... |
| | | | MKB Pack #15 |

Control Data Area содержит 176 ECC блоков по 16 секторов каждый для сохранения MKB. 176 ECC блоков Control Data Area логически разделены на 11 групп по 16 ECC блоков каждый. Каждая группа из 16 ECC блоков содержит идентичные данные, т.е. данные повторяются 11 раз.

# Список литературы


1) Спецификация формата CPRM для различный носителей (pdf).
CPRM Specification, Introduction and Common Cryptographic Elements, Revision 1.0, January 17,2003
CPRM Specification, DVD Book, Revision 0.96, January 31, 2003
CPRM Specification, Portable ATA Storage Book, Revision 0.92, May 30, 2001
http://www.4centity.com/docs/doc_request_thanks.html

2) Издательство "Открытые системы". Лукас Мериан. 13.04.2001
IBM и Intel продвигают новый стандарт защиты информации на дисках
http://www.osp.ru/cw/2001/14/030_1_print.htm

3) ИнфоБизнес. Киви Берд. 10.01.2001
Голливуд готовится к новому крестовому походу против пиратов
http://www.ibusiness.ru/marcet/6587/

4) Газета "Компьютерные Вести" №9, Макс Курмаз. 2001 год
Защита от копирования - на жестких дисках?
http://www.kv.by/index2001093402.htm&print

5) АК-Центр Микросистемс. Энциклопедия flash-памяти.
SDMI-совместимые флеш-карты.
http://www.ak-cent.ru/?parent_id=14571&SID=4e60fd665d54e6ccb3ff4d9b4609f9d9