Kopierschutz von SecureDigital und CompactFlash Karten

25.05.2009

Angewandte Informatik – TI2
Digitaltechnik 2
Thomas Lauritsch

Inhaltsverzeichnis

1 Welche Speicherkarten sind am Bekanntesten?

1.1 CompactFlash – Card (CF-Card)

Die CompactFlash–Karte wurde 1994 ursprünglich von SanDisk entwickelt und ist gewissermaßen die Mutter aller moderner Speicherkarten.
Sie bot erstmalig die Kombination von Flash–Technologie in Verbindung mit einem auf der Karte integrierten Controller. Dieser erlaubt es, ohne außen liegende Kontakte aus zukommen.
Aufgrund der vielen Vorteile, die CF-Karten bieten, z.B.:

- robust,
- kostengünstig und
- kapazitätsstark

setzen mittlerweile viele Hersteller auf die CompactFlash-Karte.

Dieses Medium war eine lange Zeit, vermehrt, in Digitalkameras, Camcordern, PDA's und MP3-Playern vertreten. Heute werden die Karten vom Typ I hauptsächlich von digitalen Spiegelreflexkameras verwendet.

Es sind zwei unterschiedliche Standards erhältlich, die sich auf den ersten Blick nur durch ihre Kartendicke unterscheiden.

- Typ I hat die Größe von 42,8mm x 36,4mm x 3,3mm (BxTxH).
- Typ II hat die Größe von 42,8mm x 36,4mm x 5,0mm (BxTxH).

Der am weitesten verbreitete Standard ist Typ I, da diese Karten auch mit Typ II vorgesehene Slots kompatibel sind, umgekehrt jedoch nicht.
Durch das im Vergleich zur SecureDigital oder MultiMediaCard großes Format ist bei CompactFlash, eine kostengünstige technische Realisierung wesentlich höherer Kapazitäten möglich.
Mit einem entsprechenden PC-Adapter, können CF–Karten zum Auslesen der gespeicherten Daten, sowie als externer Speicher für den Laptop oder den PC, nutzbar gemacht werden. Da der Controller in der Karte integriert ist, muss der Adapter nicht mit einem Controller versehen sein.

Secure CompactFlash (SCF) ermöglicht außerdem den Einsatz von CPRM.

1.2 SmartMedia-Card (SM-Card)

Die SmartMedia-Karte, SM-Card genannte Speicherkarte, ist ein wiederbeschreibbares Wechselspeichermedium ohne integrierten Controller und mit offenen Kontaktflächen, die sehr leicht beschädigt werden können.
Dadurch ist die SM-Card im Vergleich zu der CF-Card in der Handhabung wesentlich weniger robust und flexibel.
Die Karten haben die Größe von 45mm x 37mm x 0,76mm (BxTxH) und zählen somit zu den größten und auch zu den dünnsten Speicherkarten.
Ein großer Nachteil von SM-Cards ist der fehlende Controller, wodurch die gesamte

Steuerung vom Lesegerät übernommen werden muss, was in einigen Fällen zu Kompatibilitätsproblemen führen kann. Sie arbeiten im Vergleich zu anderen Karten extrem langsam und konnten nur bis zu einer maximalen Kapazität von 256 MB hergestellt werden. Außerdem können sie aufgrund ihrer geringen Dicke sehr leicht brechen.
Heute sind diese Karten nur noch in sehr geringen Mengen verfügbar, weil sie nicht mehr produziert werden.
Sie wurden hauptsächlich in Digitalkameras, MP3-Playern und Diktiergeräten verbaut.

1.3 MultiMedia-Cards (MMC)

Die MultiMedia-Card wurde 1997 auf den Markt gebracht und ist der Vorgänger der heutigen SecureDigital-Karte, allerdings werden MMC Karten noch bis heute weiterentwickelt.
Auf den Ersten Blick sehen Standard MMC Karten und SD Karten gleich aus. Mit einer Größe von 24mm x 32mm x 1,4 mm (BxTxH) ist die MMC Karte lediglich etwas dünner als die SD Karte.
Allerdings gibt es MMC Karten schon 4 Jahre länger als die SD Karte. Die Multimedia Card nach dem Standard 3.x ist kompatibel zur SD Karte.
In Geräten, die für SD Karten ausgelegt sind, kann man meistens auch problemlos MMC Karten verwenden. Umgekehrt passen, in Geräte die ausschließlich mit MMC Karten arbeiten, wegen der Dicke keine SD Karten hinein.

Die Multimedia Card besitzt einen eigenen Controller, allerdings noch keine Möglichkeit für ein „DRM (Digital Rights Management)" System.

2004 wurde ein neuer Standard für MMC Karten eingeführt, mit dem es möglich sein soll eine Übertragungsgeschwindigkeit von bis zu 52 MB/s zu erreichen.

Übersicht der verschiedenen MultiMedia-Cards:

MMC Karte	MMC Version	Größe in mm	Spannung	Kontakte
MMC	3.x seit 1997	24x32x1,4	3,3 Volt	7
RS-MMC	3.x seit 1997	24x18x1,4	3,3 Volt	7
RS-MMC DV	3.x seit 1997	24x18x1,4	1,8 Volt und 3,3 Volt	7
MMC-Plus	4.x seit 2004	24x32x1,4	3,3 Volt	13
MMC-mobile	4.x seit 2004	24x18x1,4	1,8 Volt und 3,3 Volt	13
MMC-micro	Seit 2005	12x14x1,1	1,8 Volt und 3,3 Volt	10

1.4 SecureDigital-Card (SD-Card)

Die SD-Karte wurde im Jahr 2001 von SanDisk auf Basis des älteren MMC-Standards entwickelt. Der Name Secure Digital leitet sich von zusätzlichen Hardware-Funktionen für das Digital Rights Management (DRM) ab.
Wie auch die MultiMedia-Card besitzt sie einen integrierten Controller und verfügt außerdem über eine manuell via Schalter – zu bedienende Schreibschutzfunktion, welche von manchen Lesegeräten jedoch ignoriert wird.

Bei SecureDigital-Karten gibt es 3 verschiedene Modelle:

- die normalen SD-Karten mit den Maßen 32mm × 24mm × 2,1mm (BxTxH),
- die miniSD-Karten mit den Maßen 20mm × 21,5mm × 1,4mm (BxTxH) und
- die microSD-Karten mit den Maßen 11mm × 15mm × 1mm (BxTxH).

Erweiterungen dieser Norm sind:

- SDHC (SD High Capacity)
- SDXC (SD eXtended Capacity)

Die genauen SDXC Spezifikationen wurden im Laufe des 1. Quartals 2009 veröffentlicht.
Unabhängig davon wurde die erste SDXC-Karte am 6. März 2009 von Pretec in den Handel gebracht, die eine Kapazität von 32GB aufweist.
Es gibt momentan keine Lesegeräte, die mit diesen Karten kompatibel sind.

1.5 MemoryStick (MS)

Sony hat den Memory Stick 1998 auf den Markt gebracht, da er mit 50mm x 21,5mm x 2,8mm (BxTxH) zu dieser Zeit sehr schmal war, konnte man diesen ideal in kompakten Geräten verwenden.
Memory Sticks werden bis heute nur von Sony Geräten verwendet. Dadurch, dass Sony eine sehr große Produktpalette im Angebot hat, gibt es auch ein weites Einsatzgebiet.
Die Produktpalette reicht von Digitalkameras, über PDA's und MP3-Player bis hin zu Spielekonsolen und Handys.

Da nur Sony die Memory Sticks nutzt hat diese Firma auch über lange Zeit als einzige diese Speicher hergestellt, dementsprechend teuer waren Memory Sticks.
Zwar dürfen heute auch andere Firmen Memory Sticks herstellen, da der Absatz gegenüber anderen Speicherkarten allerdings deutlich geringer ist, sind Memory Sticks auch heute noch relativ teuer.

Memory Sticks besitzen einen eingebauten Speicher-Controller, allerdings unterstützt der normale Memory Stick gerade mal eine Speicherkapazität von 128MB bei einer Schreibgeschwindigkeit von 1,8 MB/s, was heute nicht mehr zeitgemäß ist.
Deshalb hat Sony seinen Memory Stick in den letzten Jahren dementsprechend der Marktlage angepasst und diverse Neuentwicklungen auf den Markt gebracht.

Speicherkarte	Controller?	Kopierschutz	Größe (mm)	Spannung	Kontakte	Max. Speichergröße
Memory Stick (MS)	ja	ja	50 x 21,5 x 2,8	3,3V	10	128 MB
MS Select	ja	ja	50 x 21,5 x 2,8	3,3V	10	256 MB
MS Pro	ja	ja	50 x 21,5 x 2,8	3,3V	10	32 GB
MS Pro HG	ja	ja	50 x 21,5 x 2,8	3,3V	14	32 GB
MS Duo	ja	ja	31 x 20 x 1,6	3,3V	10	256 MB
MS Pro Duo	ja	ja	31 x 20 x 1,6	3,3V	10	32 GB
MS Pro-HG Duo	ja	ja	31 x 20 x 1,6	3,3V	14	32 GB
MS Micro (M2)	ja	ja	12,5 x 15 x 1,2	3,3V/1,8V	10	32 GB

Die Memory Sticks gibt es auch mit einem Kopierschutz, genannt „MagicGate". Dieser wird besonders beim Verkauf von Spielen, für die Spielkonsole PSP eingesetzt.

Memory Sticks besitzen, wie SD-Karten, einen kleinen Schiebeschalter, mit welchem man das versehentliche löschen der Speicherkarte verhindern kann.

1.6 XD-Picture Card

Die xD-Picture Card ist ein Ende Juli 2002 von Olympus und FujiFilm vorgestelltes Speichermedium für die Digitalfotografie und den Einsatz in einem PDA, das als Nachfolgetechnologie für SmartMedia-Speicherkarten konzipiert ist.
Allerdings verwenden nur die Kamerahersteller Fujifilm und Olympus selbst das Kartenformat xD.
Die xD Card verfügt, wie die SmartMedia-Card, über keinen eigenen Controller.

Im Vergleich zur SD-Card ist die xD-Picture Card auch teurer. Während SD-Karten einen Gigabyte-Preis von 2-5€ aufweisen, kosten 1-GB-xD-Karten mehr als 15 € (Stand: April 2009).

Die Karte misst 20mm x 25mm x 1,7mm und ist damit deutlich kleiner, aber nicht mehr so dünn wie die SmartMedia-Card.

Es gibt drei unterschiedliche Fertigungstechniken:

- die klassische Technik (keine Typen Bezeichnung; 16MB – 512MB)
- die platzsparende Technik (Typ M; 256MB – 2GB)
- und die HighSpeed Technik (Typ H; 512MB – 2GB)

2 Kopierschutz

2.1 Digital Rights Management (DRM)

2.1.1 Kurze Erläuterung

Digital Rights Management, oder kurz DRM, bezeichnet Verfahren, mit denen die Nutzung und Verbreitung digitaler Medien kontrolliert werden sollen.
Vor allem bei digital vorliegenden Film- und Tonaufnahmen, aber auch bei Software, elektronischen Dokumenten oder elektronischen Büchern findet die digitale Nutzungsverwaltung Verwendung.

Durch DRM-Systeme wird es den Anbietern ermöglicht, sich Nutzungsrechte mittels Lizenzen vergüten zu lassen, anstatt der Daten selbst.

2.1.2 Hintergrund

Einer der Hauptvorteile digitaler Daten ist die Möglichkeit sie ohne jeden Qualitätsverlust und ohne nennenswerten Aufwand kopieren zu können. Dieses Verhalten ist aber nicht immer erwünscht.

Ein DRM-System soll dabei helfen Urheberrechte zu schützen, indem es die Verwendung von Daten nur in dem von den jeweiligen Rechteinhabern definierten Rahmen ermöglicht.

Mechanismen der digitalen Rechteverwaltung sind allgemein jedoch stark umstritten. Befürworter sehen in Systemen der digitalen Rechteverwaltung hauptsächlich die Eröffnung neuer Geschäftsmodelle mit bedarfsgerechterer Abrechnung, wie z.B. Pay Per View.
Zudem können DRMS auch zum Schutz kritischer Daten wie z.B. Unternehmensinterna eingesetzt werden.

Zu einem ernsten Problem aus Sicht, der Musikindustrie wurde die beliebige Vervielfältigung von digitalen Inhalten erstmals Mitte der 90er Jahre, als CD-Brenner für Endverbraucher erschwinglich und Personal Computer leistungsfähig genug für den Umgang mit im MP3-Format komprimierter Musik wurden.
Ende der 90er Jahre erfuhren außerdem die so genannten „Internet-Tauschbörsen" immer stärkeren Zulauf, da Internet-Benutzer dort kostenlos Dateien von der Festplatte anderer Benutzer kopieren können. Oft handelt es sich dabei um urheberrechtlich geschützte Musik, Filme oder Software.

Erst im Jahr 2003 gewann schließlich mit der Eröffnung des iTunes Music Store ein Vertriebsweg mit integrierter digitaler Rechteverwaltung an kommerzieller Bedeutung.
Am 30. Mai 2007 wurde iTunes Plus eingeführt, in welchen man als Kunde die Möglichkeit hat, Musik ohne DRM Schutz zu erwerben und bis zum zweiten Quartal 2009, soll der komplette Katalog ohne DRM verfügbar sein.

2.1.3 Digital Rights Management Systeme (DRMS)

Es existiert derzeit keine einheitliche Definition zu Digital-Rights-Management-Systemen.
Im Allgemeinen bezeichnet man eine Bandbreite von Technologien mit dem Begriff „Digital Rights Management".
Die Vielzahl der Definitionen lassen sich in weit umfassende und engere Definitionen unterteilen.

2.1.3.1 Weit umfassende Definition

DRM-Systeme stellen eine technische Sicherheitsmaßnahme dar, um einem Rechteinhaber von Informationsgütern die Möglichkeit zu geben, die Art der Nutzung seines Eigentums durch Nutzer auf Basis einer zuvor getroffenen Nutzungsvereinbarung technisch zu erzwingen.
Zu DRMS gehören im Allgemeinen auch Watermarking-Technologien, diese bieten nur eingeschränkte Möglichkeiten zur Nutzungskontrolle.

2.1.3.2 Engere Definition

Elektronische Schutzmechanismen für digitale Informationen nennt man DRMS. Sie ermöglichen die Verwertung von digitalen Inhalten, über eine reine Pauschalvergütung hinaus und erlauben zusätzlich die individuelle Lizenzierung bzw. Abrechnung nach Häufigkeit, Dauer oder Umfang der Nutzung.
Einerseits wird damit die unbegrenzte Nutzung einschränkbar, andererseits werden On-Demand-Geschäftsmodelle ermöglicht, die vorher kaum zu realisieren waren.

2.1.3.3 Beispiele aus der Praxis

- Adobe Protected Streaming
- Digital Copy, d.h. das Recht eine legale Kopie auf einem PC und einem Portable Media Player anzufertigen (z.B. Filme)
- FairPlay (Apple iTunes)
- OMA DRM für mobile Endgeräte, implementiert in zahlreichen Handys
- WM DRM 10 (Microsoft Windows Media Digital Rights Management Version 10). Für Windows Media Audio (WMA) und Windows Media Video (WMV) Dateien.
- Nintendo Wii

2.1.4 Einsatzgebiete

DRM wird derzeit hauptsächlich bei digitalen Inhalten, wie Filmen oder Musik, eingesetzt. Am weitesten verbreitet sind die DRMS „FairPlay" von Apple, „Windows Media DRM" von Microsoft und das OMA DRM der Open Mobile Alliance.
Diese ermöglichen eine genaue Einstellung der Berechtigungen und können für verschiedene Audio- und Videodateien verwendet werden.

Apple nutzt FairPlay im iTunes Store, andere Onlineshops wie Napster und Musicload, aber auch „Video-on-Demand"-Dienste verwenden vornehmlich das DRM-System von Microsoft.

Das OMA DRM wird in fast jedem Mobiltelefon für Klingeltöne, Bilder, aber auch für mobile Musik- und Fernsehübertragungen, z. B. von Vodafone oder T-Mobile, eingesetzt.
Häufig werden die Systeme des OMA DRM und des Windows Media DRM kombiniert, um eine Interoperabilität zwischen Mobiltelefonen und PCs zu ermöglichen.
Beispiele für die Kombination von OMA DRM und Windows Media DRM sind Musicload und Vodafone.

In Zukunft könnten DRMS auch in vielen anderen Bereichen, wie im Automobilbereich , z.B. Softwareschutz, Online-Navigation, oder im Bereich eingebetteter Systeme, eine größere Rolle spielen.

2.1.5 Basistechniken

Zugangs- und Nutzungssteuerung benötigen die Basistechniken der Kryptografie und Rechtedefinitionssprachen.
Wasserzeichen sollen die Lizenz rechtlichen Bestimmungen auch außerhalb eines DRMS zumindest nachträglich erkennbar machen.

2.1.5.1 Verschlüsselung (Kryptografie)

Um die unberechtigte Nutzung, Veränderung oder Verfälschung geschützter Inhalte zu verhindern, können eine Vielzahl von kryptografischen Techniken verwendet werden. Kryptografische Verfahren kommen insbesondere im Rahmen der Zugriffs- und Nutzungskontrolle sowie der sicheren Abrechnung zum Einsatz (z.B. CPRM).

2.1.5.2 Digitale Wasserzeichen

Ziel der verschiedenen Wasserzeichenverfahren ist es, bestimmte Informationen unwiderruflich mit einem Medienprodukt zu verbinden.
Zu unterscheiden sind drei Varianten:

1. Bei **sichtbaren Wasserzeichen** wird eine klar erkennbare Urheberrechts-Markierung an das zu schützende Objekt angebracht, was die nicht autorisierte Nutzung unattraktiv machen soll und in jedem Fall zu einem, wenn auch manchmal marginalen, Qualitätsverlust führt. Nach dem legitimen Kauf eines Medienprodukts werden sichtbare Wasserzeichen in der Regel entfernt bzw. unsichtbare Wasserzeichen neu eingesetzt.

2. In **(unsichtbar-)robusten Wasserzeichen** werden Recht bezogene Informationen im Inhalt „versteckt", d.h. unsichtbar gespeichert und untrennbar mit dem Werk verbunden. Derartige Informationen werden häufig zur Überprüfung von Zugangs- und Nutzungsrechten und für Abrechnungszwecke genutzt. Gelegentlich umfassen robuste Wasserzeichen auch Informationen zum Lizenznehmer. Im letzten Fall spricht man von digitalen Fingerabdrücken, die sich zur Rechtsverfolgung einsetzen lassen.

3. **(Unsichtbar-)fragile Wasserzeichen** dienen dem Nachweis der Unversehrtheit, um Manipulationen zu erkennen. Hierbei wird überprüft ob eine Mediendatei manipuliert wurde. Dabei sollen fragile Wasserzeichen nur gegen Verarbeitungsoperationen, Komprimierung, Skalierung etc., robust sein, während bei inhaltlichen Änderungen, z.B. Bildmanipulationen, das Wasserzeichen zerstört werden soll. Daher lassen sich fragile Wasserzeichen für die Verfolgung von Rechtsverletzungen einsetzen.

Es ist immer noch nicht gelungen, intelligente Angriffe gegen Wasserzeichen wirklich auszuschließen.

Beispiele spezieller Anwendungen sind:

Anwendung	mögliche eingebettete Informationen
Erkennen eines Mediums	Eindeutige Identifikationsnummer des Inhaltes vergleichbar mit der ISBN
Nachweis der Urheberschaft	Identifikationsnummer des Urhebers
Nachweis des rechtmäßigen Eigentümers	Kundennummer, Kreditkartennummer
Kennzeichnung zum Verfolgen von Datenflüssen	Transaktionsnummer evtl. in Verbindung mit einer Nutzeridentifikationsnummer, z.B. durch die Markierung von Laser-Farbausdrucken
Kennzeichnung von Medien zur Werbemaßnahme	Nummer zur Identifikation der jeweiligen Werbemaßnahme

2.1.5.3 Rechtedefinitionssprachen

Rechtedefinitionssprachen erlauben die Beschreibung des Umfangs der eingeräumten Rechte und ggf. die gewählte Form der Abrechnung. Hierzu werden durch das DRMS je nach Anforderung die lizenzierten Nutzungsmöglichkeiten abgebildet und ggf. mit Preisen hinterlegt.

Beispiele für Rechtedefinitionssprachen sind z.B.:

- OASIS (Organization for the Advancement of Structured Information Standards)
- XrML (eXtensible rights Markup Language)
- ODRL (Open Digital Rights Language)

Je nachdem wie mächtig die Rechtedefinitionssprache ist, können Nutzungsrechte sehr differenziert abgebildet werden:

- Nutzungszeitraum
- Nutzungshäufigkeit
- Nutzungsqualität (Bild- und Tonqualität)
- Nutzungsoperationen (z.B. drucken, ändern, kopieren, etc.)
- geographische Einschränkungen
- sprachliche Einschränkungen

Rechteinformationen können entweder untrennbar an die Medienprodukte angefügt oder separat zu diesen geliefert werden.
Der Vorteil der ersteren Variante ist, dass es zu keiner unerwünschten Entkopplung zwischen Medienprodukt und Nutzungskontrollinformationen kommt.
Bei der zweiten Form können Rechtsinformationen flexibler geändert werden.

Ähnlich wie bei Verschlüsselungstechniken kommen Rechtedefinitionssprachen im Rahmen von DRMS umfassend zum Einsatz. Sie unterstützen mittels Einbringung von Kundeninformationen die Zugangssteuerung, indem das lokale Abgreifen der Medienprodukte nur vorab autorisierten Nutzern gestattet wird.
Primärziel ist jedoch die Realisierung einer flexiblen Nutzungssteuerung, sowie nutzungsabhängiger Abrechnung durch Rechts- und Abrechnungsinformationen.

2.2 Content Protection for Recordable Media (CPRM)

2.2.1 Kurze Erläuterung

CPRM steht für Content Protection for Recordable Media und wurde ursprünglich zum Schutz von MP3 Dateien entwickelt, um Raubkopien vorzubeugen.
Zu den treibenden Kräften gehörten Intel, IBM, Matsushita Electric und Toshiba. Diese Firmen gründeten die „4C Entity".

CPRM ist eine simple Hardware basierte Technologie (integriert in den Medien), mit welcher man, das Kopieren, Ändern und Verschieben, von digitalen Daten, kontrollieren bzw. einschränken kann.

2.2.2 Einsatzgebiete

Die Einsatzgebiete für CPRM, auf physikalischen Medien, sind keine Grenzen gesetzt, von DVDs über Flash Speicherkarten wie z.B. SecureDigital und Secure CompactFlash.
CPRM ist heute standardmäßig auf allen SD-Karten implementiert, allerdings bei den unbeschriebenen, im Handel erhältlichen Karten, deaktiviert.

Einsatzgebiete in der Praxis sind unter anderem:
- PC basierte DVD Brenn- und Player Software,
- DVD Player (stand-alone),
- portable DVD Player,
- im Automobilbereich (Entertainmentsysteme, Software für Navigationsgeräte),
- Handys mit Speicherkarten,
- MP3 Player (z.B. iPod),
- andere handheld Geräte mit SD Flash Unterstützung.

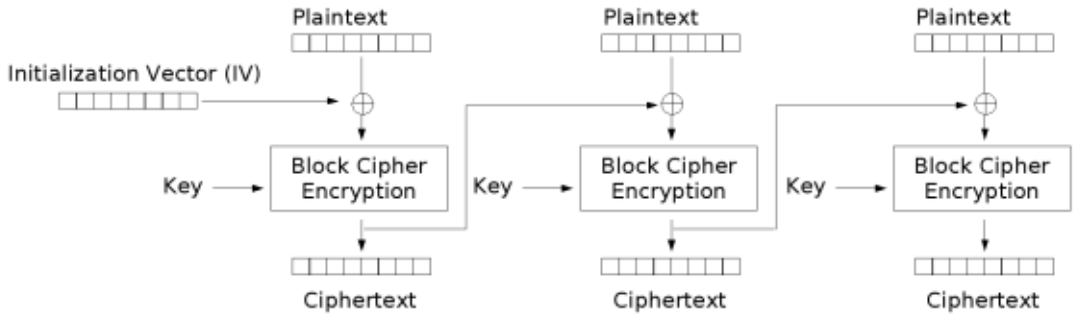
2.2.3 Funktion

2.2.3.1 Algorithmus

Aktuell benutzt CPRM den C2 Cipher Algorithmus. C2 ist ein symmetrischer Block Chiffre Algorithmus. Er wurde von der „4C Entity" für den Einsatz von CPRM lizenziert.

Was ist ein symmetrisches Kryptografie System?
Ein symmetrisches Kryptografie System, benutzt im Gegensatz zum asymmetrischen System, den gleichen Schlüssel zur Ver- und Entschlüsselung.
Der große Nachteil der symmetrischen Systeme ist, die sichere Übertragung des Schlüssels, welcher neben der Daten auch übertragen werden muss. Alles hängt von der Geheimhaltung des Schlüssels ab.

Was ist Blockverschlüsselung?
Blockverschlüsselung, auch Blockchiffre genannt, ist ein Algorithmus, der einen Datenblock mittels eines Schlüsselwertes verschlüsselt. Der daraus resultierende verschlüsselte Block hat dabei dieselbe Länge.
Moderne Verfahren haben typische Schlüssellängen, wie z.B. 64 Bit, 128 Bit, 168 Bit, 192 Bit oder 256 Bit.



Cipher Block Chaining (CBC) mode encryption

Wie in der Abbildung dargestellt, wird die Ausgabe des Blockchiffre mit dem Klartext bitweise, mittels XOR, verknüpft um daraus den Geheimtext zu bilden.

Als Initialisierungsvektor (IV) benutzt man
- Entweder einen Zeitstempel
- Oder eine zufällige Zahlenfolge.

Der CBC-Mode hat einige wichtige Vorteile:
- Klartextmuster werden zerstört.
- Identische Klartextblöcke ergeben unterschiedliche Geheimtexte.
- Verschiedene Angriffe, z.B. Klartextangriffe, werden erschwert.

Die bekanntesten Verfahren sind unter anderem:

- DES (Data Encrypted Standard)
- AES (Advanced Encrytion Standard)
- IDEA (International Data Encryption Algorithm)

2.2.3.2 Media Key Block (MKB)

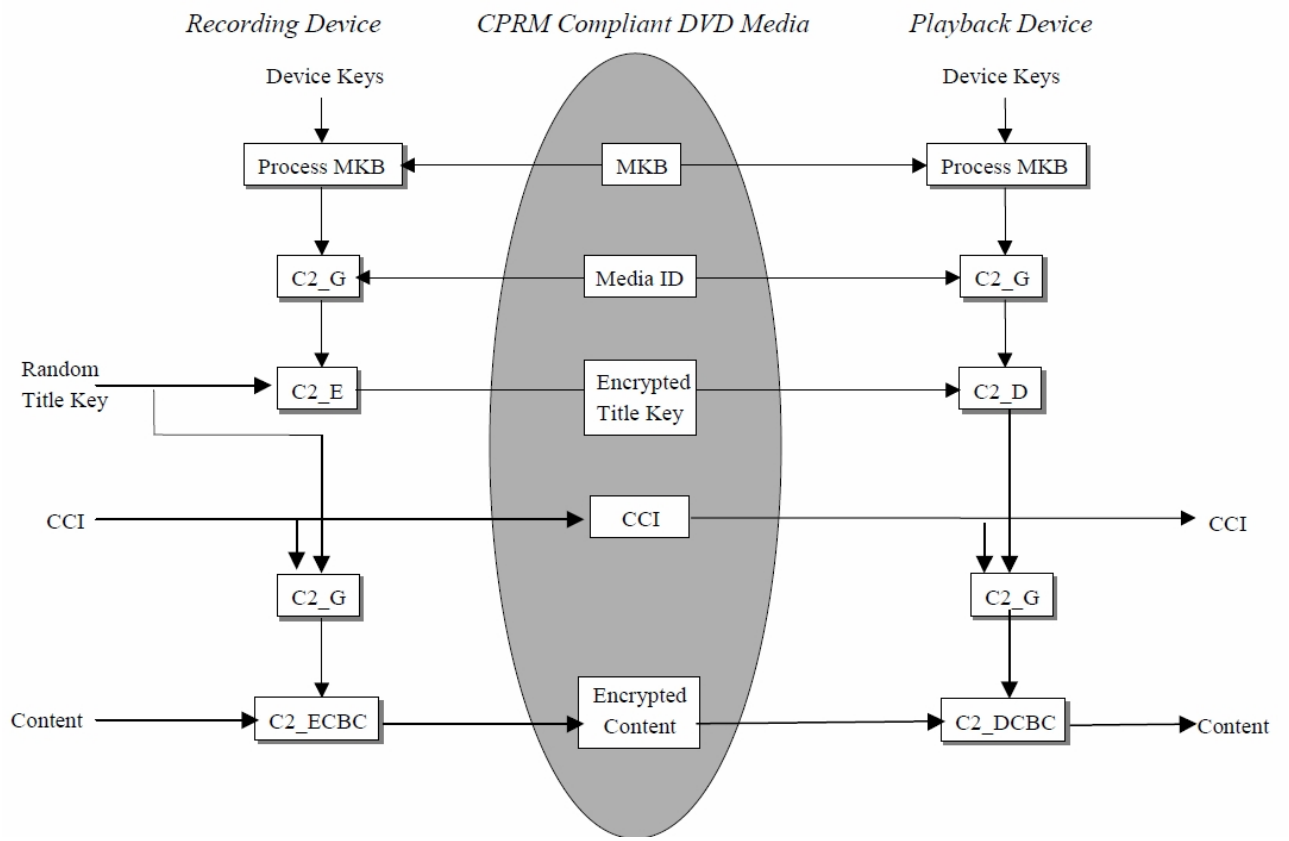
Die Media Key Block Technologie repräsentiert einen großen Durchbruch, weil es die Möglichkeit eröffnete, ein Gerät implizit zu authentifizieren, das versucht ein geschütztes Medium abzuspielen.
Ein solcher Block ist eine Tabelle, mit bis zu 65.636 Zeilen und 16 Spalten, deren Inhalt aus verschlüsselten Werten besteht.

Die geschützten Medien beinhalten diese Tabelle, die versteckt im Lead-in Bereich (z.B. CD, DVD) oder innerhalb eines versteckten Bereiches (z.B. SD-Karten) gespeichert wird.
Aufzeichnungs- und Abspielgeräte erhalten einen Satz an einzigartigen Schlüsseln (Device Key).
Bei Erkennung eines gestohlenen oder modifizierten Schlüssels, wird das Gerät veranlasst einen falschen Schlüssel zu generieren, welcher das Abspielen, des Mediums auf dem Gerät verhindert.

2.2.3.3 Digitale Wasserzeichen

Digitale Wasserzeichen wurden unter Punkt 2.1.5.2 beschrieben und sind hier nur, der Vollständigkeit halber aufgeführt.

2.2.4 Verschlüsselung einer CPRM geschützten DVD



Nun widmen wir uns der Ver- und Entschlüsselung der mit CPRM geschützten Daten.
Die generelle Funktionsweise, werde ich hier erstmal, Anhand einer DVD erklären.

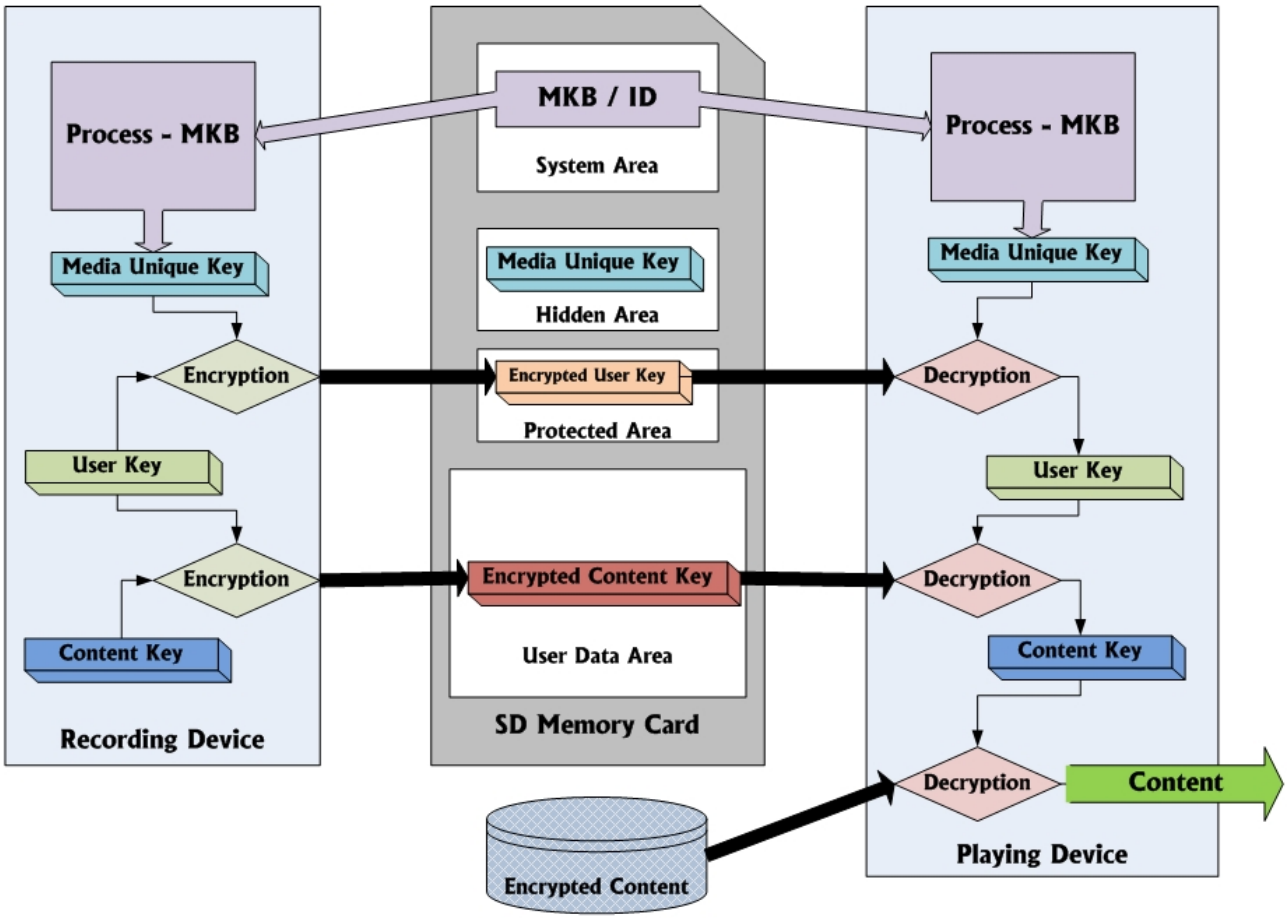
Wie unter Punkt 2.2.3.2 Media Key Block (MKB) bereits erwähnt, enthält jedes CPRM geschützte Medium einen Media Key Block, welcher sich im Lead-in Bereich befindet.
Im Lead-in Bereich kann es einen weiteren Bereich geben, nämlich den „Burst Cutting" Bereich, worin die Media ID gespeichert wird. Dieser Bereich kann nicht mit herkömmlichen Geräten modifiziert werden, dies bleibt professioneller Hardware vorbehalten.

Ein Rekorder (Hard- oder Software), der mit CPRM ausgestattet ist, erstellt eine erlaubte Kopie auf ein solches Medium wie folgt:

Der Rekorder liest den MKB vom Medium und benutzt den geheimen Device Key, um den Media Key zu generieren.
Der Media Key ist verbunden mit der Media ID und benutzt die C2 Algorithmus Funktion C2_G(enerate) um den Media Unique Key zu generieren.
Der Media Unique Key wird benutzt um den zufällig generierten Title Key mit der C2 Funktion C2_E(ncrypt) zu verschlüsseln, welcher im Daten Bereich des Mediums gespeichert wird.
Der Title Key wird außerdem mithilfe der Funktion C2_G(enerate), wiederum verbunden

mit der Copy Control Information (CCI).
Das daraus resultierende Ergebnis ist der Schlüssel, womit der Inhalt, mit der sogenannten C2_ECBC Funktion (Encryption in Converted Cipher Block Chaining) verschlüsselt wird.

2.2.5 CPRM für SD-SD (seperate Delivery)



Es gibt nun mit dem Zusatz SD (seperate Delivery), auch die Möglichkeit Inhalte zu ver- oder entschlüsseln, die sich nicht auf dem selben Medium befinden, wie hier Anhand einer SD-Karte gezeigt.

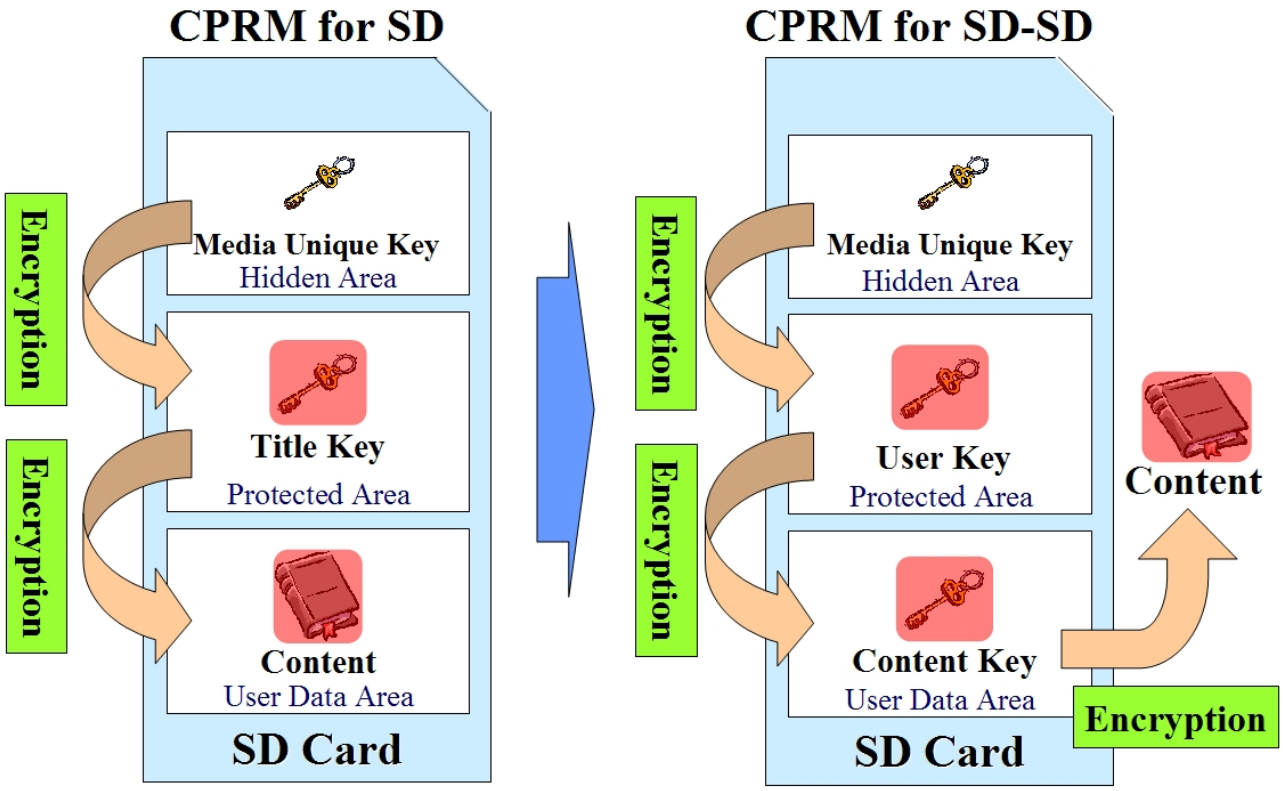
Bei der Ver- oder Entschlüsselung von einer SD-Karte verhält es sich ähnlich wie bei einer DVD.
Die SD Karte ist, wie oben im Bild dargestellt, in 4 Bereiche unterteilt, der

- System Area,
- der Hidden Area,
- der Protected Area und
- der User Data Area.

So wenn wir jetzt wieder die Verschlüsselung betrachten sehen wir, dass als erstes wieder der Media Key Block und die Media ID ausgelesen werden.
Daraus wird der Media Unique Key generiert und mithilfe des User Keys zum Encrypted User Key umgewandelt, welcher in der Protected Area der Karte gespeichert wird.

Aus dem User Key und dem Content Key wird schließlich der Encrypted Content Key generiert und in der User Data Area der Karte gespeichert.

2.2.6 CPRM für SD



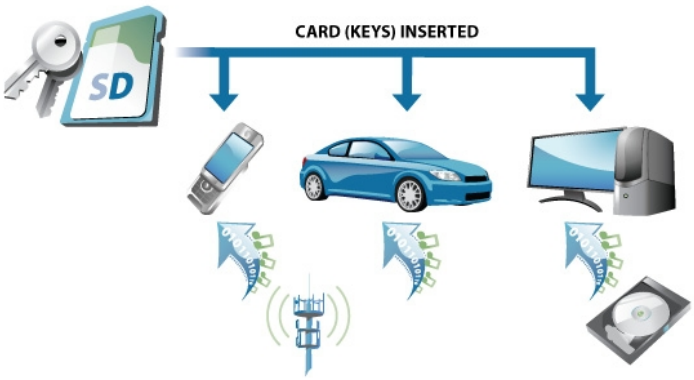
Der einzige Unterschied zum seperate Delivery, besteht darin, dass sich der Inhalt auf dem selben Medium, wie z.B. der SD-Karte, befindet.
Es gibt in diesem Falle nur den Title Key, welcher den Inhalt direkt verschlüsselt. Dieser befindet sich in der Protected Area der Karte.

2.2.7 Praktische Szenarien für CPRM SD-SD

2.2.7.1 Szenario 1

Schlüssel und verschlüsselter Inhalt befinden sich auf der SD-Karte. Die Karte wird in das Lesegerät, z.B. Handy, Navigationsgerät im Auto oder PC, eingeführt.
Der Inhalt kann aufgerufen werden.

2.2.7.2 Szenario 2



Die Schlüssel befinden sich auf der SD-Karte, welche wieder in das Lesegerät eingeführt wird. Diesmal befindet sich der Inhalt nicht auf derselben Karte, sondern wird gesondert empfangen (seperate Delivery).
Der verschlüsselte Inhalt kann sich z.B. im Netzwerk oder auf einer Festplatte befinden.

3 Quellen

Internet:

http://www.wikipedia.de
http://www.intel.com
http://www.sandisk.com
http://www.hardware-aktuell.com
http://www.netzwelt.de
http://www.heise.de
http://www.tomshardware.com
http://www.tecchannel.de
http://www.4centity.com
http://www.compactflash.com
http://www.comptech-info.de
http://www.sdcard.org