

---

# AACS

Advanced Access Content System

---

©2007 Chuck Liddell

---

# What is AACCS?

AACS is...

**“A specification for managing content stored on the next generation of prerecorded and recorded optical media for consumer use with PCs and CE devices. Advanced Access Content System will complement new innovations in the next-generation of optical discs, and enable consumers to enjoy next-generation content, including high-definition content.”** -Advanced Access Content System Licensing Administrator, LLC.

---

# Where Does AACCS Come From?

The companies listed here are the founders of the AACCS content distribution and digital rights management standard.

AACCS is the successor to CSS, the system used to encrypt and protect DVDs.

AACCS was developed to be stronger cryptographically than CSS, as well as providing a better system for dealing with hackers and attacks on the integrity of the system.



---

# How does AACCS work?

- AACCS encrypts the contents of the disc using AES (Advanced Encryption Standard, a block cipher) in Cipher Block Chaining (CBC) Mode. The 128-bit key used to encrypt the disc contents is called a “Title Key.” The same  $IV_0$  is always used for this step:
    - $0BA0F8DDFEA61FB3D8DF9F566A050F78_{16}$
  - The Title Key itself is then encrypted with AES in Electronic Code Book (ECB) Mode, using a new key. The encrypted result is stored in a special header on the disk.
  - This special header (called the Media Key Block) stores keys and also provides a way to blacklist certain players if they have been compromised.
-

---

# Device Keys

- Each player (either hardware or software) that intends to play AAC3-encrypted content must have a Device Key. Most players will have many Device Keys, though the exact number varies between individual players.
  - These keys must be kept secret.
  - A Device Key is 128-bits long.
-

# Calculation of Subsidiary Device Keys and Processing Keys

**k:**

128-bit input Device Key (may be a subsidiary DK)

**$s_0$ :**

secret 128-bit initialization value provided by the “licensing agency” (AACS LA)

**AES-128D:**

Decryption using the AES algorithm in ECB mode. A single 128-bit value is returned as output based on two 128-bit input values.

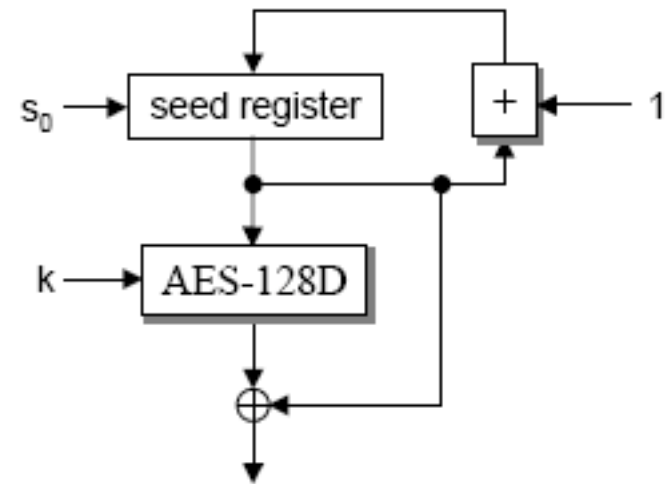
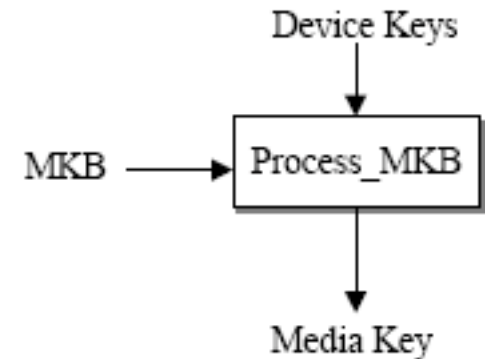


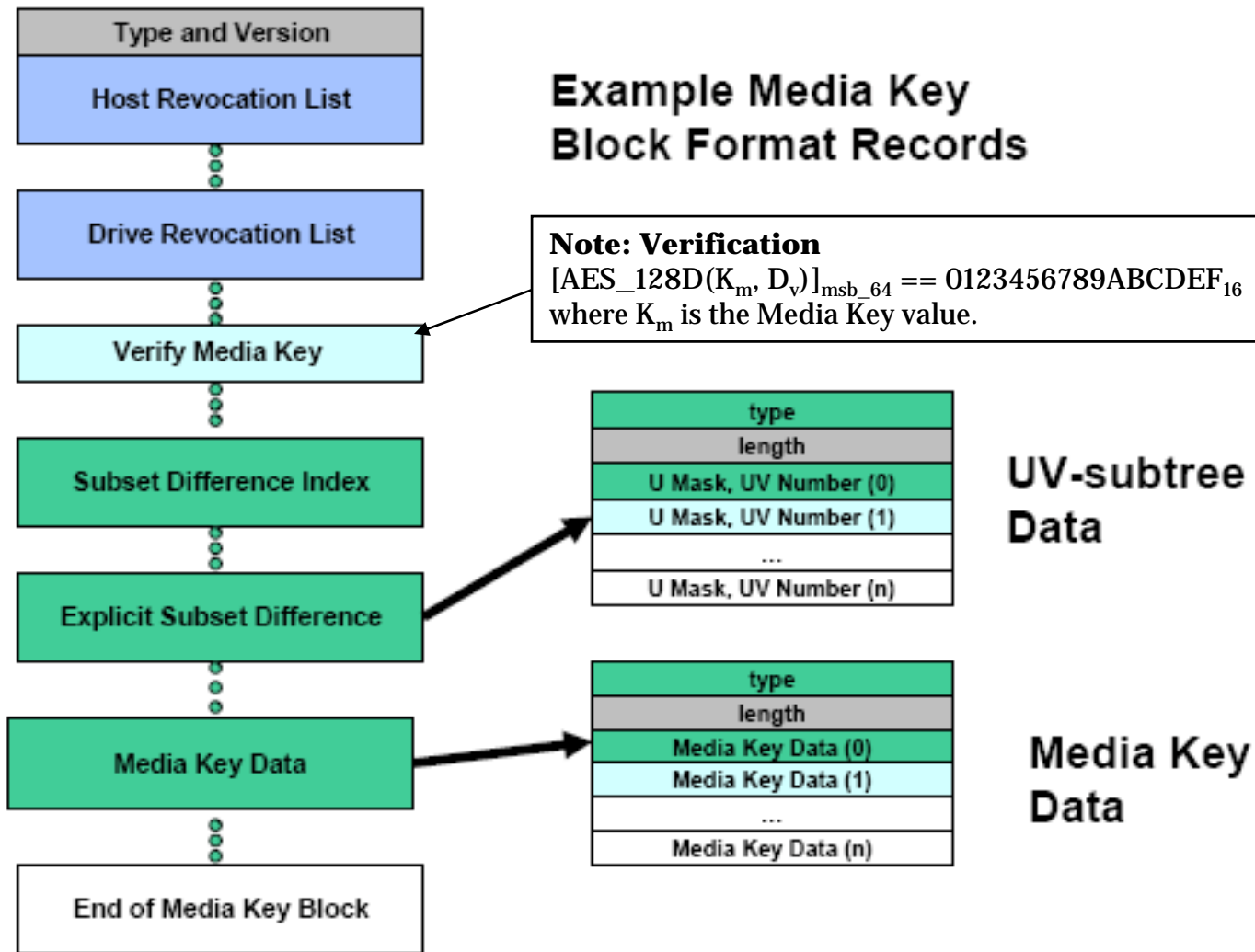
Figure 3-2 – Triple AES Generator (AES-G3)

# Media Key Block (MKB)

- The Media Key Block is a crucial component of the AACS system.
- It includes two major parts: the subset-difference identification part, and the key data part.
- It is of variable bit length, although always a multiple of 4 bytes.
- The MKB is generated by AACS LA and given to studios to include on their discs. A new one needs to be generated each time the revocation tables are updated.

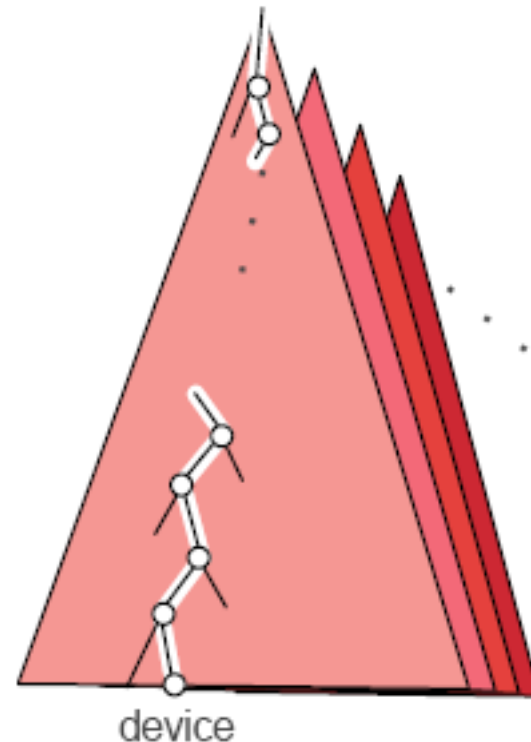


# Media Key Block (Continued)



# Subset-Difference Tree

- The Subset-Difference Tree is a series of binary trees used to revoke specific Device Keys once they have been compromised.
- Multiple sub-trees are used to deal with the problem of revoking non-contiguous Device Keys.
- Each device is uniquely associated with a leaf node of the tree.
- It is through this association that revocation of keys is possible.



# Retrieving Encrypted Media

MKB – Media Key Block

$K_m$  – Media Key

$K_{vu}$  – Volume Unique Key

$K_t$  – Title Key

AES-G – As shown below.

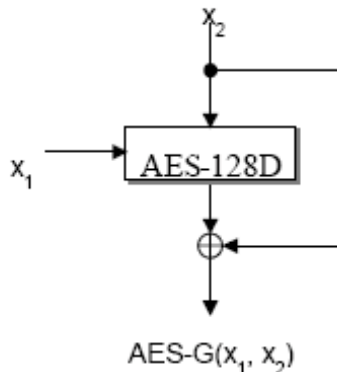
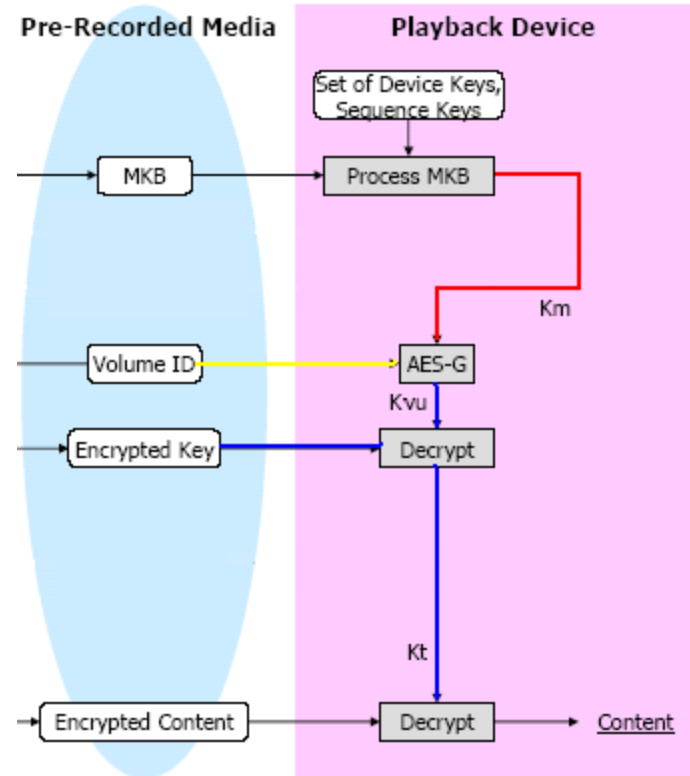


Figure 2-1 – AES-based One-way Function



---

# Other Anti-Piracy Measures

- **Audio Watermarks**
    - Sounds left in the audio tracks of movies that are inaudible to humans, but can be picked up by devices to ensure non-pirated media.
  - **“Traitor Tracing” (Sequence Keys)**
    - Using slightly tweaked movies that reveal whether a specific group of Device Keys was used to decode that movie.
-

---

# Timeline

- **19 November 2003** - the DVD Forum voted to support HD DVD as the high definition successor of the standard DVD.
  - **18 April 2006** - HD DVD released in the United States.
  - **20 June 2006** - BluRay released in the United States.
  - **26 December 2006** - "muslix64" publishes a utility named BackupHDDVD on doom9.net forums.
  - **12 January 2007** - doom9.net forum members release key info.
  - **13 January 2007** - the first pirated HD DVD, Serenity, was uploaded on a private torrent tracker.
  - **24 January 2007** - the Advanced Access Content System (AACs) Licensing Authority confirmed that the encryption on high-definition DVDs has been bypassed.
  - **4 March 2007** - "jx6bpm" revealed Cyberlink's PowerDVD's device key on doom9.net's forums, claiming this was the key in use by AnyDVD.
  - **6 April 2007** - Corel (owner of WinDVD) releases security update patching exploit.
  - **16 April 2007** - AACs LA announces security updates to both WinDVD and PowerDVD to patch security holes.
  - **23 April 2007** - The first HD DVDs are released that have non-empty device key revocation lists.
-

---

# Attacks on the System

- **Muslix64 – 26 December 2006**
    - **Published BackupHDDVD, which was a utility that allowed users to decrypt AACCS content provided they had the necessary Title Key.**
    - **He claimed to have retrieved Title Keys from main memory that were stored there un-encrypted by software players.**
-

---

# Response from AACCS LA

January 24, 2007

**“AACCS LA has confirmed that AACCS Title Keys have appeared on public web sites without authorization. Such unauthorized disclosures indicate an attack on one or more players sold by AACCS licensees. This development is limited to the compromise of specific implementations, and does not represent an attack on the AACCS system itself, nor is it exclusive to any particular format. Instead it illustrates the need for all AACCS licensees to follow the Compliance and Robustness Rules set forth in the AACCS license agreements to help ensure that product implementations are not compromised. AACCS LA employs both technical and legal measures to deal with attacks such as this one, and AACCS LA is using all appropriate remedies at its disposal to address the attack.”**

---

---

# Attacks on the System

- 13 January 2007
    - Doom9.net forums users discover a process key, which is then used to crack the HD DVD “Serenity”.
    - This attack is an extension of the one by muslix64, and the decryption is done using BackupHDDVD.
    - Serenity is the first HD DVD movie to be decrypted and shared on a public torrent site.
-

---

# Response from AACCS LA

February 15, 2007

**“Regarding the reported attacks on 2/13/2007, AACCS has confirmed that an additional key (called a “processing key”) has been published on public websites without authorization. This is a variation of the previously reported attack (a compromise of a specific implementation) on one or more players sold by AACCS licensees. Although a different key was extracted, this represents no adverse impact on the ability of the AACCS ecosystem to address the attack. All technical and legal measures applicable to the previously reported attack will be applicable against this attack as well.”**

---

---

# Attacks on the System

- **jx6bpm - 4 March 2007**
    - Publicly released the Device Key used by Cyberlink's PowerDVD to decrypt AACCS content:
      - 4737676058d7029452514f0ab186dc4cca8c578f
    - This device key enabled the decryption of all HD DVD and BluRay discs released to date.
    - Led to the start of development of third-party, open-source players capable of playing HD DVD and BluRay movies.
    - Claimed that SlySoft AnyDVD, the only commercial product that claims to decrypt AACCS, uses this Device Key.
-

---

# Attacks on the System

- SlySoft AnyDVD
    - Commercially available software that decrypts AACS-encrypted movies.
    - Their website describes the software as follows:
      - "AnyDVD HD comes with same functionality as AnyDVD, but with additional features for full HD-DVD (High Definition DVD) and Blu-Ray support, including decryption of HD-DVD & Blu-Ray movie discs.  
Allows you to watch movies over a digital display connection, without HDCP compliant graphics card and HDCP compliant display. No need to buy an expensive monitor."
    - SlySoft claims that "AACS has even more flaws in its implementation than CSS."
    - When questioned about AACS LA's revocation scheme, a SlySoft representative merely stated "AnyDVD HD will not be affected by this mechanism."
-

---

# Response from Corel

April 6, 2007

**“To our valued InterVideo WinDVD Customers,**

**Today Corel is releasing an important new security update for InterVideo WinDVD. We have taken this step to ensure that our customers continue to enjoy the latest HD DVD and BD content.**

**Our decision stems from recent reports that hackers have illegally obtained certain software licensing keys and have used them to duplicate copyrighted content without prior authorization. Corel takes this situation very seriously. We have been working closely with our partners and other industry organizations to ensure we take the steps necessary to prevent copyright infringement from happening in the future.**

**WinDVD customers who are currently using either HD DVD or BD playback will need to download the free security update from your PC or Drive manufacturer's websites.”**

---

---

# Response from AACCS LA

April 16, 2007 - AACCS LA Announces Security Updates

**“In response to attacks against certain PC-based applications for playing HD DVD and Blu-ray movie discs, Advanced Access Content System Licensing Administrator, LLC (“AACCS LA”) announces that it has taken action, in cooperation with relevant manufacturers, to expire the encryption keys associated with the specific implementations of AACCS-enabled software.**

**Consumers can continue to enjoy content that is protected by the AACCS technology by refreshing the encryption keys associated with their HD DVD and Blu-ray software players. This refresh process is accomplished via a straightforward online update.”**

---

---

# Conclusion

- AACS presents a dramatic improvement over its predecessor CSS.
  - The system itself is secure, and has not been broken.
  - However, AACS has been undermined by poor implementation in specific software players, and key information that should have remained secret has been made public.
  - The fight between AACS LA and software pirates will continue for some time; Neither side seems to be a clear winner based on current achievements.
-

---

# Sources / References

## **Websites:**

Wikipedia

[www.wikipedia.org](http://www.wikipedia.org)

AACS LA, LLC

[www.aacla.com](http://www.aacla.com)

Corel WinDVD

[www.intervideo.com](http://www.intervideo.com)

Doom9

[www.doom9.net](http://www.doom9.net)

SlySoft

[www.slysoft.com](http://www.slysoft.com)

## **Documents:** (released by AACS LA, LLC)

AACS Technical Overview

Introduction and Common Cryptographic Elements Rev 0.91

Pre-recorded Video Book Rev 0.91

HD DVD and DVD Pre-recorded Book Rev 0.912

## **News articles**

Freedom to Tinker: AACS blog

<http://www.freedom-to-tinker.com/?p=1104>

Yahoo! News: *HD DVD, Blu-ray protection in question after attacks*

[http://news.yahoo.com/s/infoworld/20070416/tc\\_infoworld/87720](http://news.yahoo.com/s/infoworld/20070416/tc_infoworld/87720)

DigitalTrend: *More Cracks Appear in AACS Hi-Def Armor*

[http://news.digitaltrends.com/news\\_printerfriendly12663.html](http://news.digitaltrends.com/news_printerfriendly12663.html)

---