Practical Cryptographic Systems

Digital Rights Management I

Instructor: Matthew Green

A note on the legal situation

- 1990s:
  - Digital Millennium Copyright Act (DMCA)

-(Similar laws in the EU)

  - Makes "circumvention" illegal
  - Makes distribution of circumvention tools illegal
  - Makes reverse-engineering illegal except:

-For interoperability

-Exemptions for research (not v. useful)

A note on the legal situation

- Dmitri Sklyarov
  - PhD student
  - Worked for ElcomSoft (Russia)

-Wrote a tool for stripping protection off of eBooks

  - Arrested at DEFCON ’01
  - Went to jail
  - Charges ultimately dropped

GeoHot

Sony To Subpoena PayPal Account For PS3 Jailbreaker 'Geohot'

by Kris Graft

6 comments

March 17, 2011

Sony Computer Entertainment America this week made its next move in its case against PlayStation 3 "jailbreaker" George "Geohot" Hotz.

Court documents [PDF] show that a U.S. District Court on Tuesday authorized a proposal from plaintiff SCEA to serve a subpoena to online payment firm PayPal in order to collect records from Hotz' personal account for the period of January 1, 2009 through February 1, 2011.

SCEA said it is looking for "documents sufficient to identify the source of funds in California that went into any PayPal account" associated with Hotz' email address.

SCEA is adding the PayPal order to another group of subpoenas that seek to collect information from Hotz' web provider Bluehost, as well as records from YouTube, Google and Twitter.

The court also approved this week SCEA's proposal to require Hotz to sign a consent to allow SCEA to obtain his Twitter posts from January 1 2009 to present. New Jersey-based Hotz is also ordered to appear in California to be deposed relating specifically to the issue of personal jurisdiction.

In January, Sony alleged that Fail0verflow, a "hacking group," laid the groundwork for Hotz to "unlawfully ... [gain] access to a critical level of the PS3 System" protection measures in December.

The complaint alleges that Hotz distributed circumvention devices through the internet that were needed to access that critical level of PS3 security, and that he released software code used to run pirated software on the console in January. Hotz has denied the hack is meant to facilitate piracy.

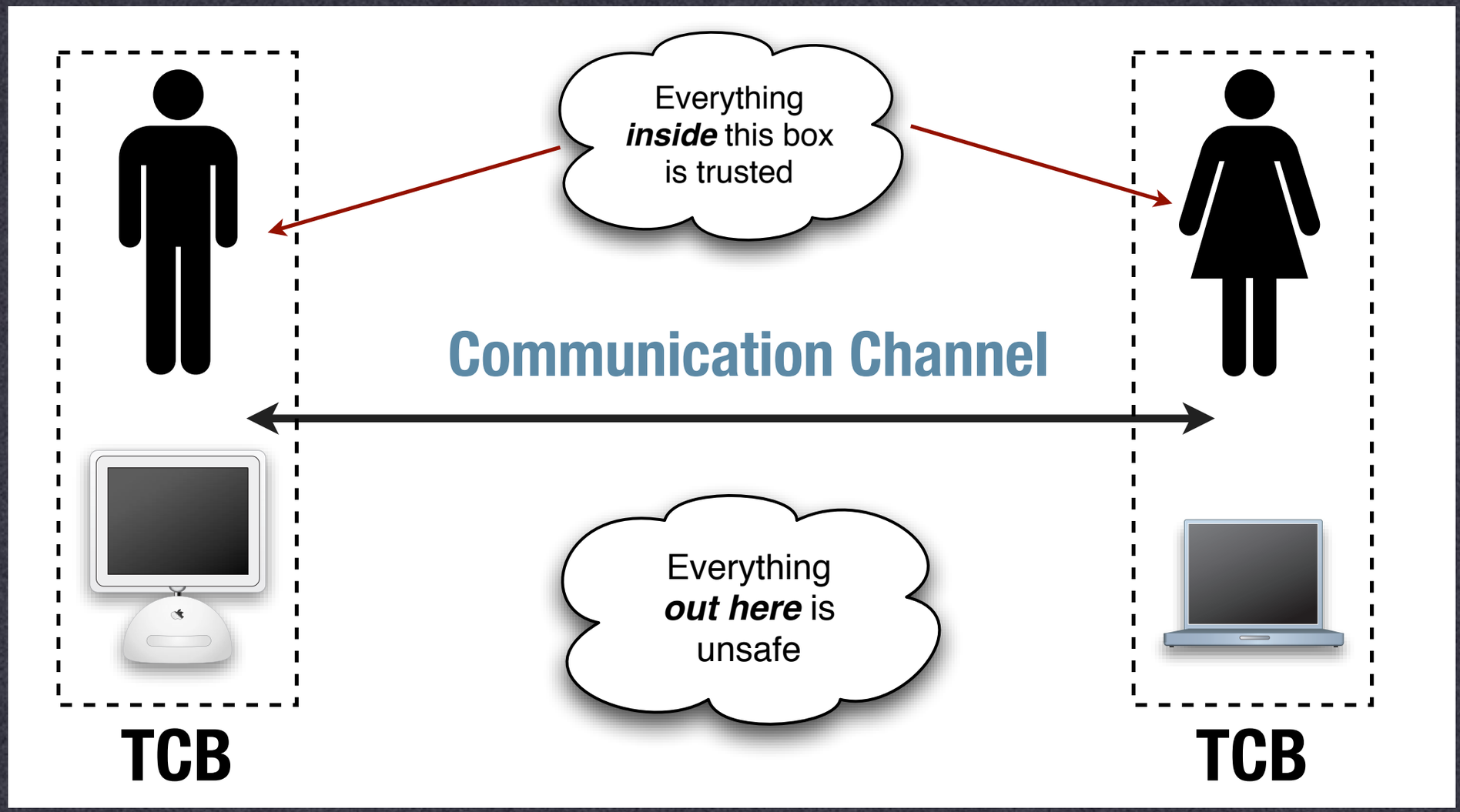
Motivation

- Intellectual property == $$
  - One can debate the ethical implications
  - Obvious problem: digital content easy to replicate

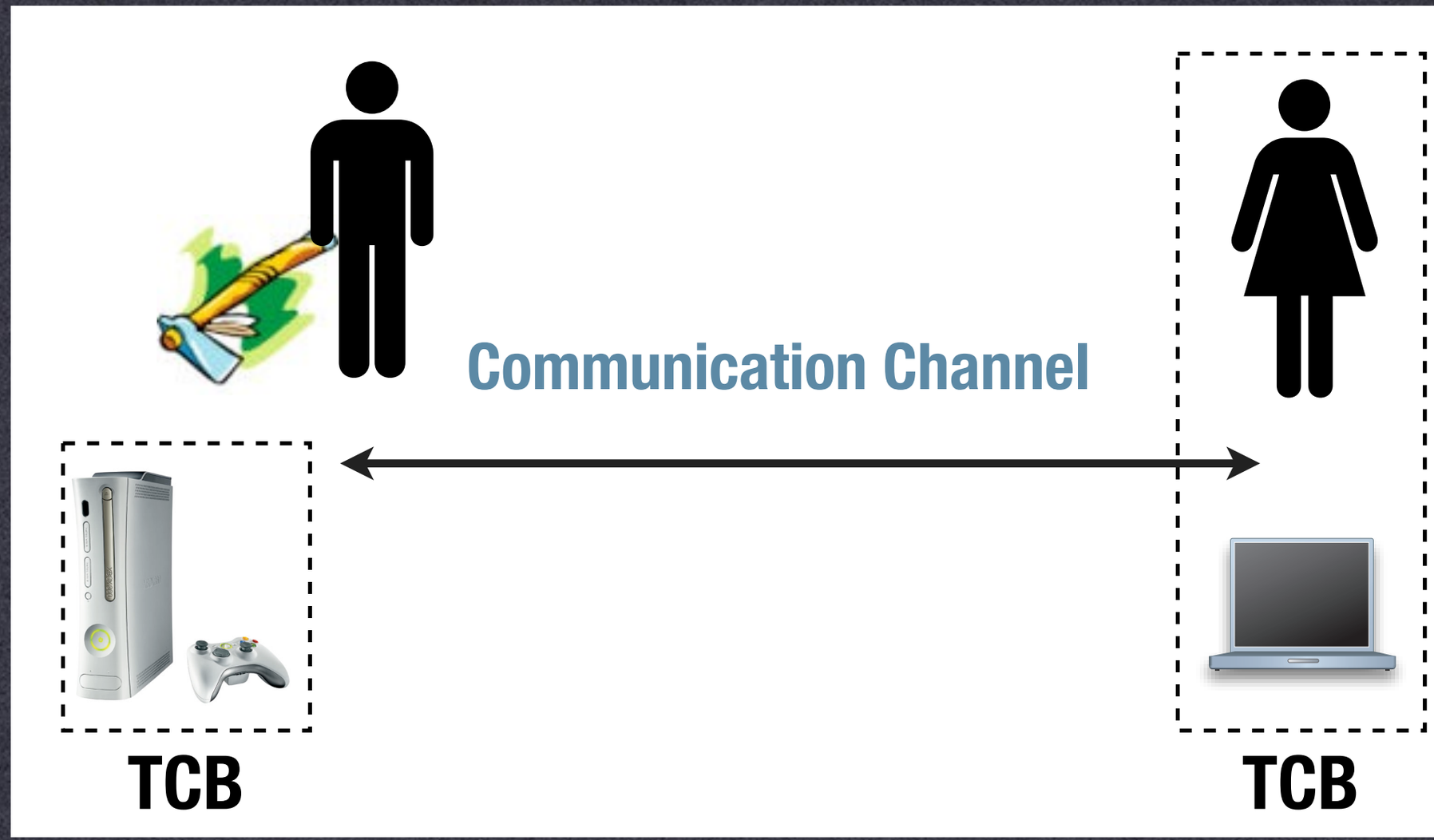
-Software/video/audio/e-books

-Legal documents/trade secrets/etc./etc.

Review

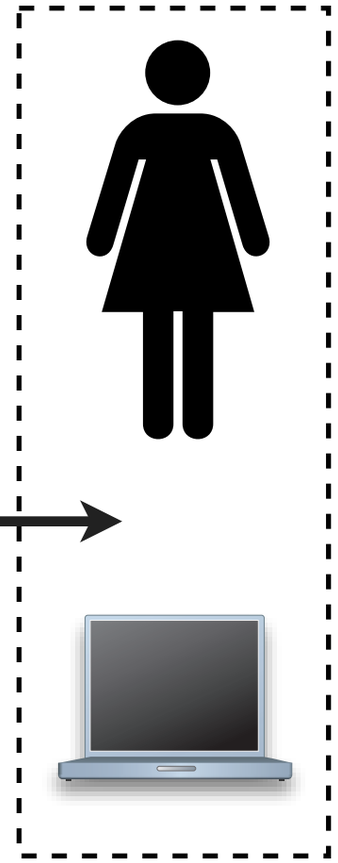

Everything
inside this box
is trusted
Communication Channel
Everything
out here is
unsafe
TCB
TCB

Today



Today

Communication Channel



TCB

Case Study: AACS

- Advanced Access Content System
  - Access control system for BluRay (and HD-DVD)
  - Public debut in 2006
  - Uses revokable broadcast encryption technology
    to provide renewable security

Background: DVD+CSS

- A little history
  - Late 90s, DVD video disks introduced
  - Hollywood demands DRM for content

-“Content Scramble System” (CSS)
40-bit proprietary stream cipher
disk encrypted under session key
session key encrypted under 408 player keys
hash check for each one

-Problems: unpublished cipher,
availability of software players,
limited renewability

Background: DVD+CSS

- A little history
  - 1999: “DeCSS” code & keys RE-ed from Xing software player (John Johansen + anonymous)
  - Later: key cracking in about 17 hrs
  - Later: player key recovery from hash check alone
  - After that: ciphertext-only attacks
  - Consortium response:

-Mostly litigation

Images courtesy Wikipedia.

Background: DVD+CSS

- CSS in brief:
  - 408 player keys
    (roughly 1-to-1 with manufacturers)

-If a player key leaks, can “renew” security,
but would require killing e.g., all Sony players

  - Software players == guaranteed key loss
  - Industry briefly considered revoking keys
  - Moot: cipher so bad it didn’t matter

Images courtesy Wikipedia.

DMCA again

- US Digital Millennium Copyright Act (DMCA)
  - Prohibition on circumventing access controls
  - Access control circumvention device ban
  - Copyright protection circumvention device ban
  - Prohibition on removal of Copyright Management Information
- Technically, covers “effective” measures
  - Legally this term covers almost anything

Source: http://www.chillingeffects.org/anticircumvention, Image: Wikipedia

AACS

- ~2004, new standard for HD video disks
  - Address CSS's problems and more:

-Separate keys per player (not manufacturer)

-Ability to efficiently revoke selected players

-Strong, standard encryption algorithms

-Content authentication

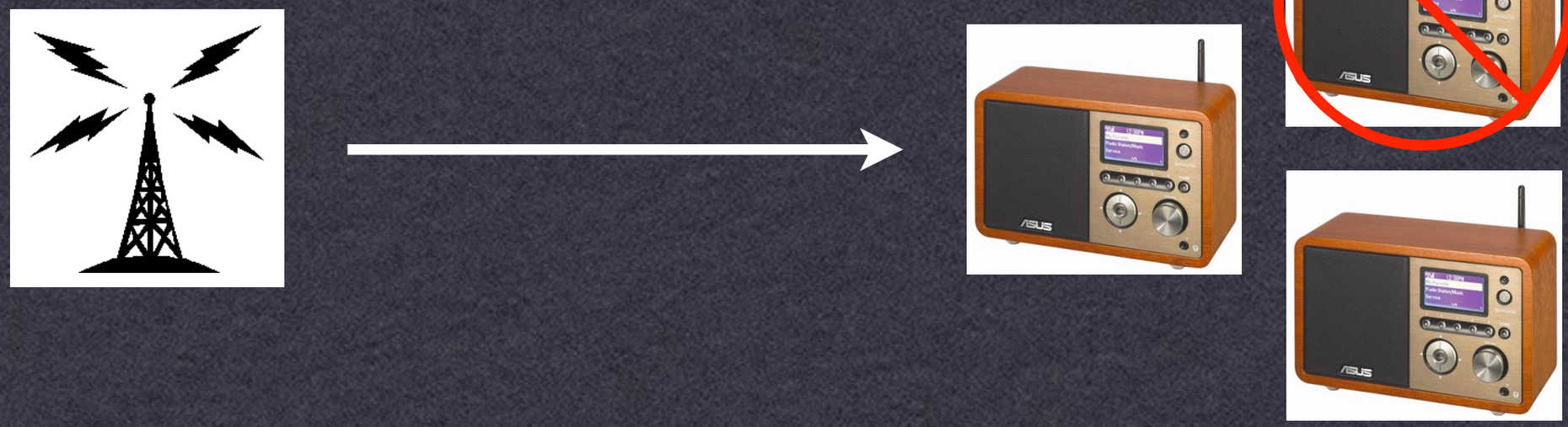
-Protocols for drive<->computer authentication

-Player watermarking capability

-(and more...)

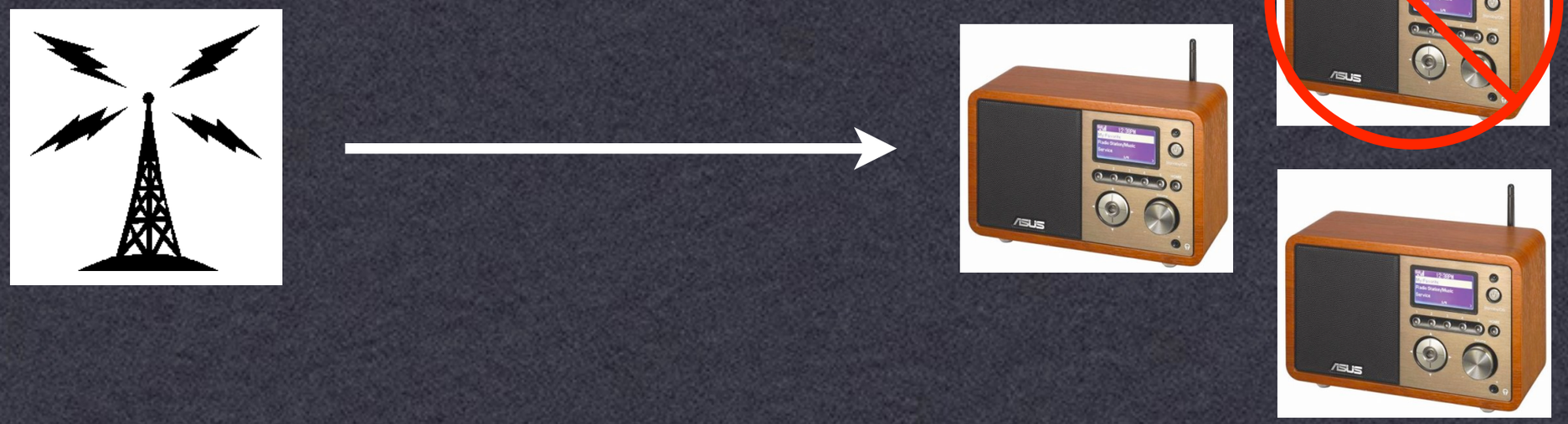
Per-player keys

- **Broadcast Encryption**
  - **Single sender, many receivers**
  - **Only authorized receivers can decrypt**
  - **The set of authorized receivers can change (receivers may be revoked)**
- **Stateful & Stateless / Efficient**



Per-player keys

- Notation
  - N: number of total receivers
  - r: number of revoked receivers
  - (N-r): total number of authorized receivers



Per-player keys

- How big is N?
  - The set of receivers is huge!
  - CEA: ~145M as of 2007

-And that's only US + Canada!

source: http://www.thedigitalbits.com/articles/cemadvdsales.html

-Naive BE size: 16 bytes * 145M = 2.2GB

-Not really feasible

  - HD players just starting out

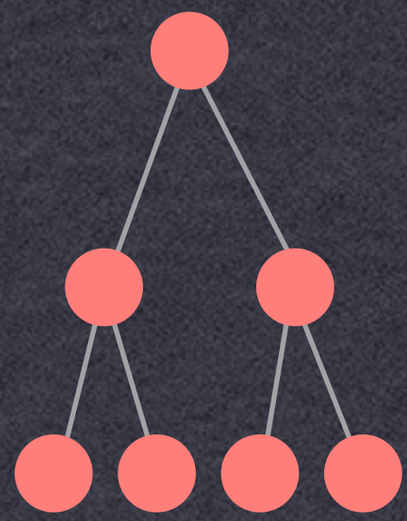
-But we need to estimate high

Per-player keys

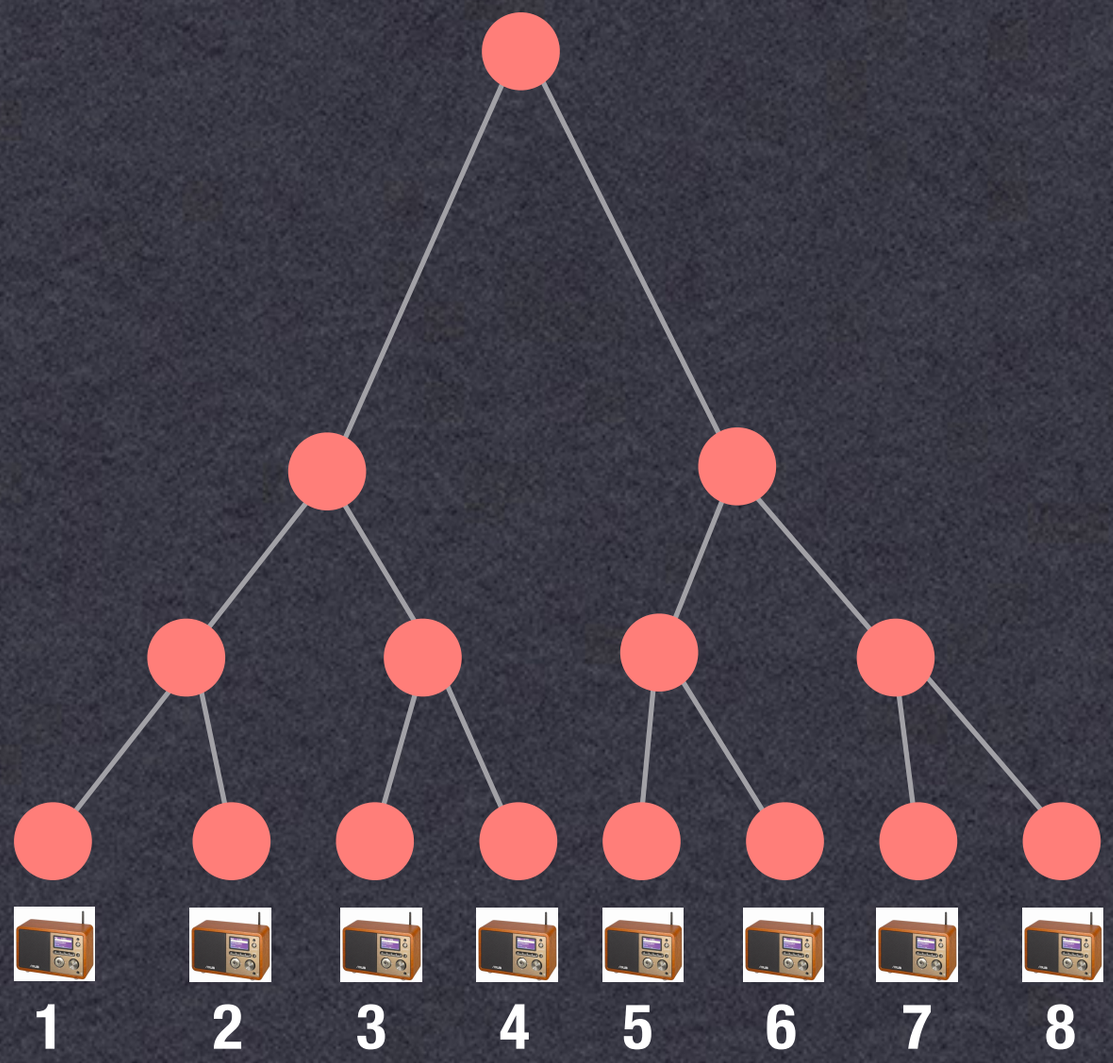
- Naor-Naor-Lotspeich BE
  - NNL trees give us an efficient way to do this with much less communication
  - Uses any standard block cipher (e.g., AES)
  - Two variants:

-Subset Cover $r \log(N/r)$

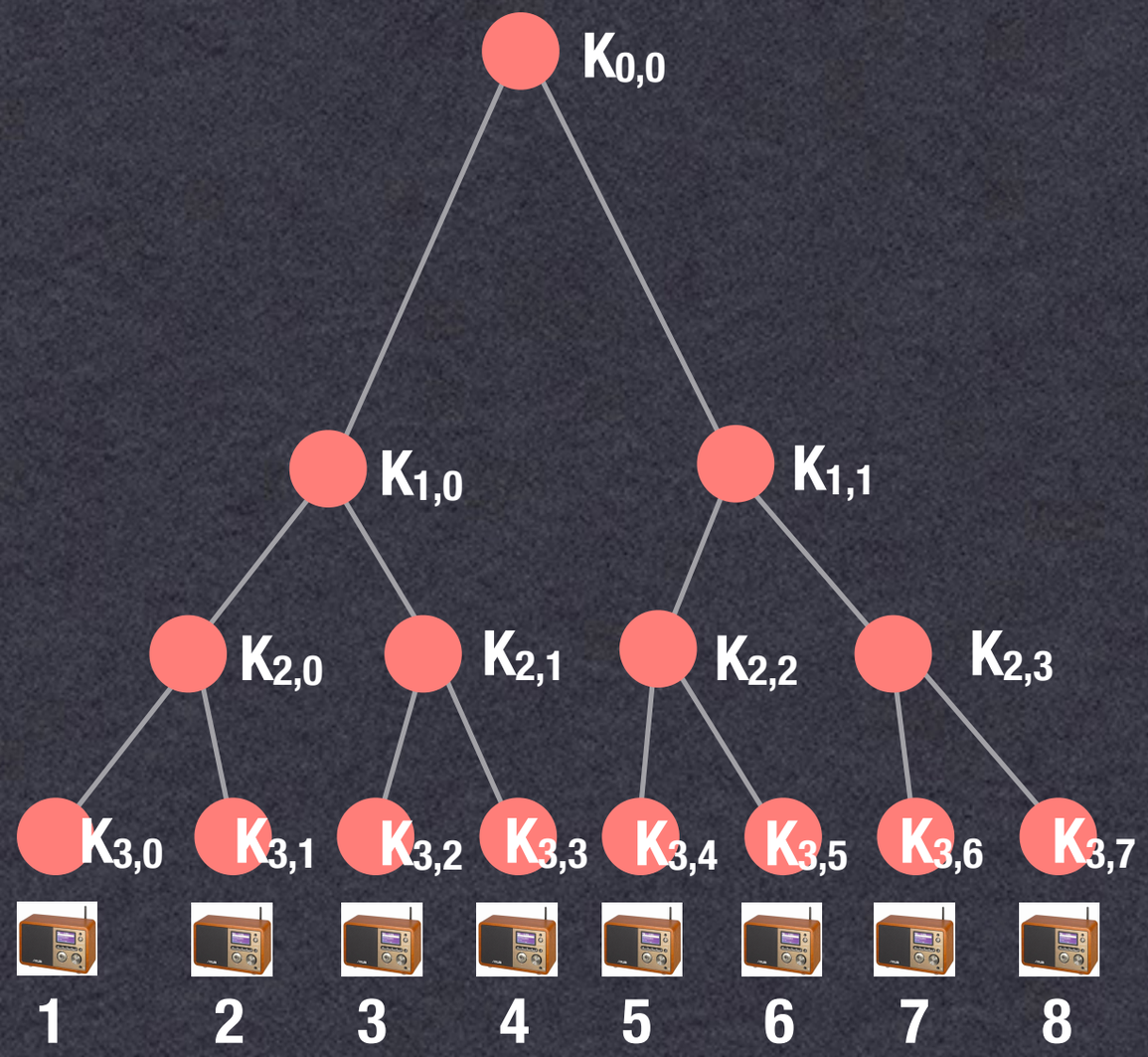
-Subset Difference $2r - 1$



NNL Subset Cover



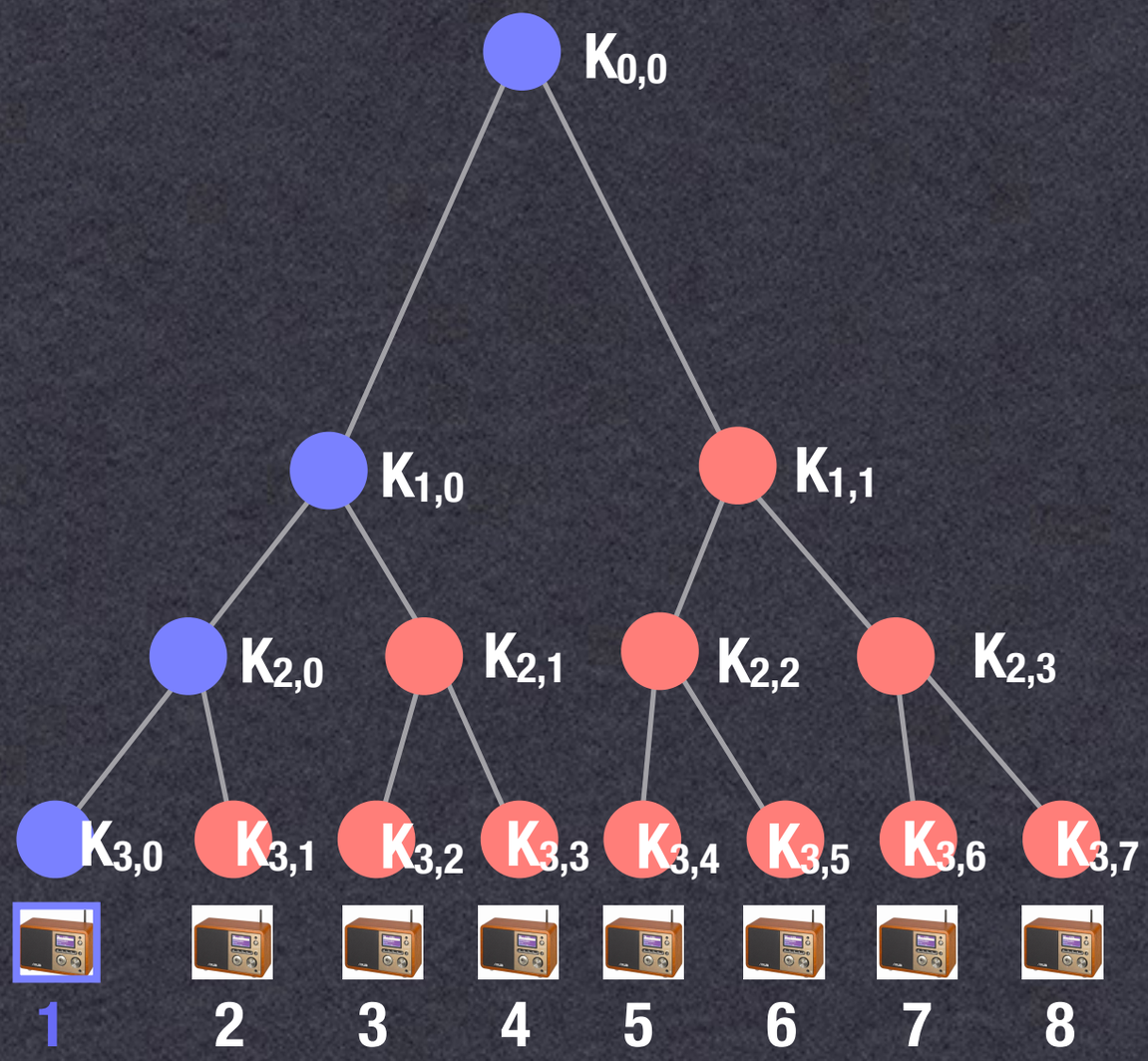
NNL Subset Cover



NNL Subset Cover

$K_{0,0}$ $K_{1,0}$ $K_{2,0}$ $K_{3,0}$

1



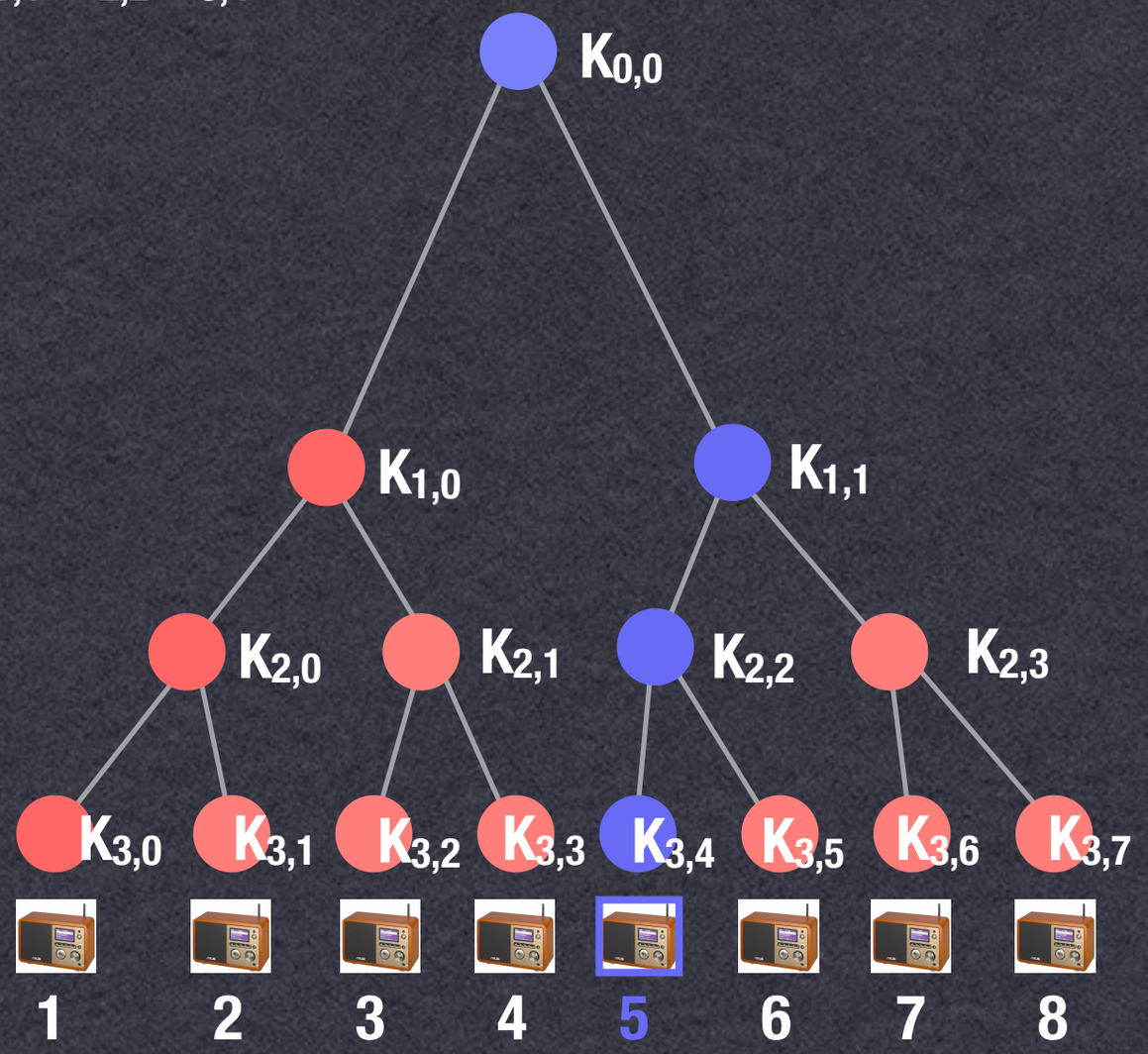
NNL Subset Cover

$K_{0,0}$ $K_{1,0}$ $K_{2,0}$ $K_{3,0}$

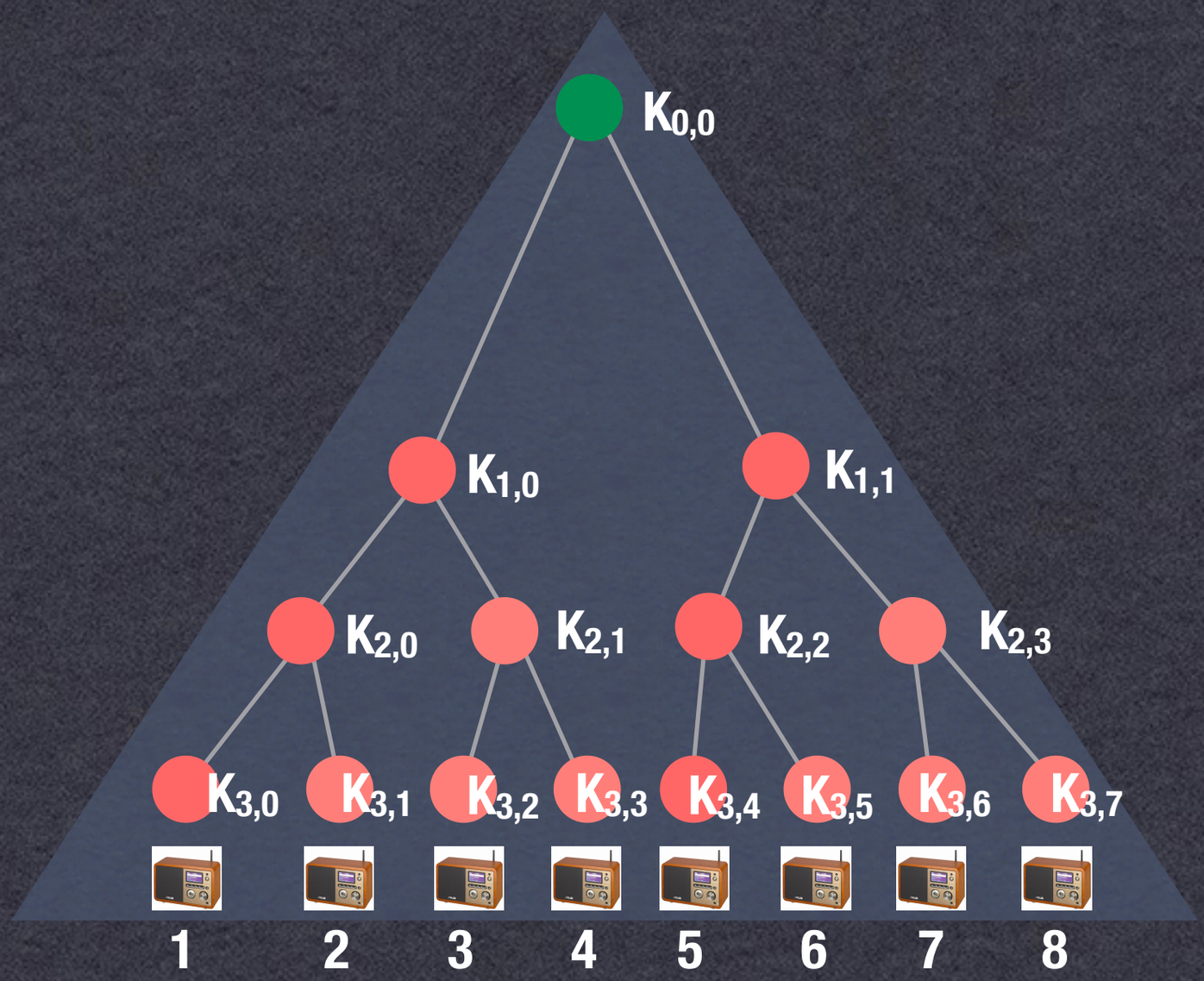
1

$K_{0,0}$ $K_{1,1}$ $K_{2,2}$ $K_{3,4}$

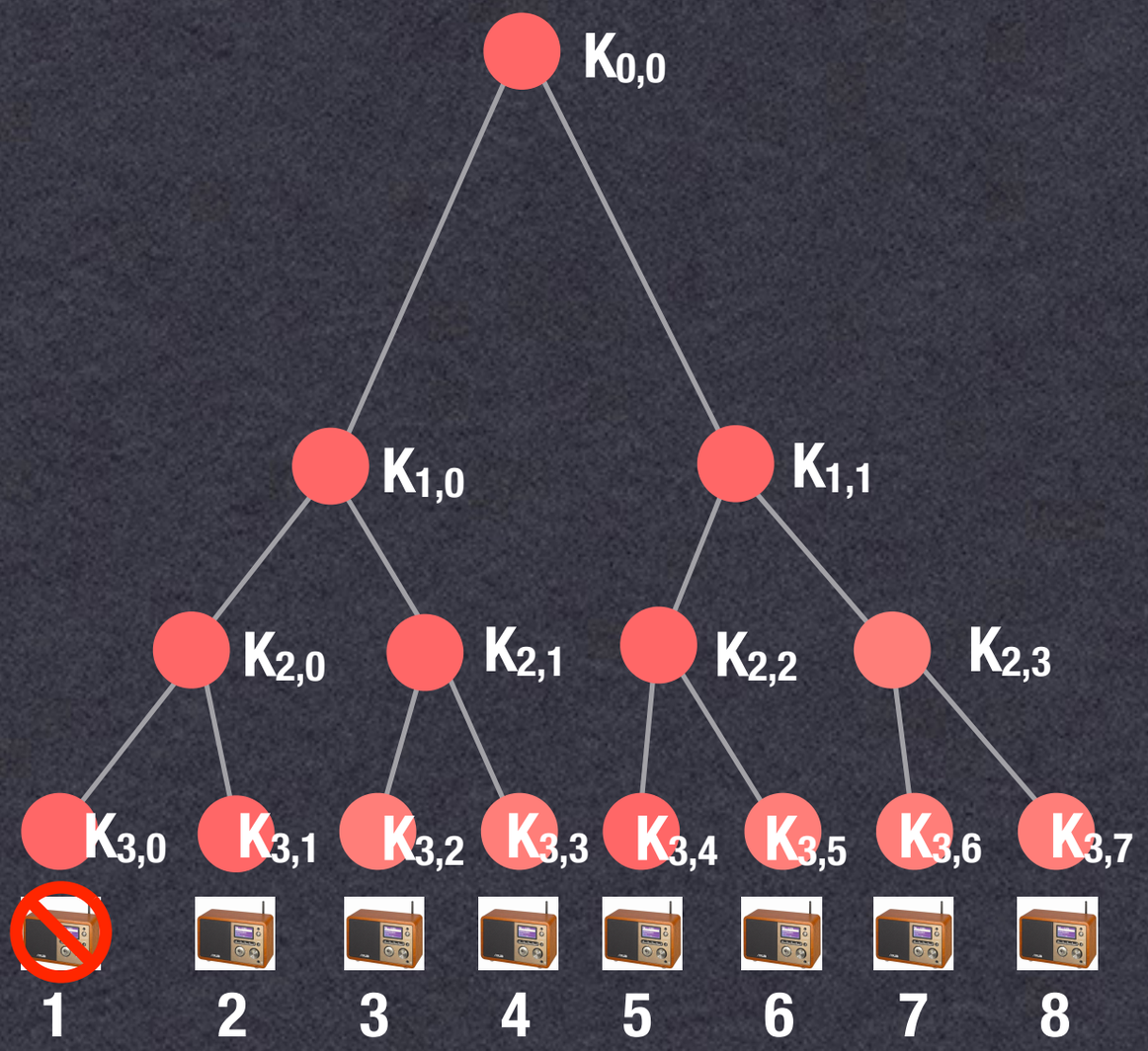
5



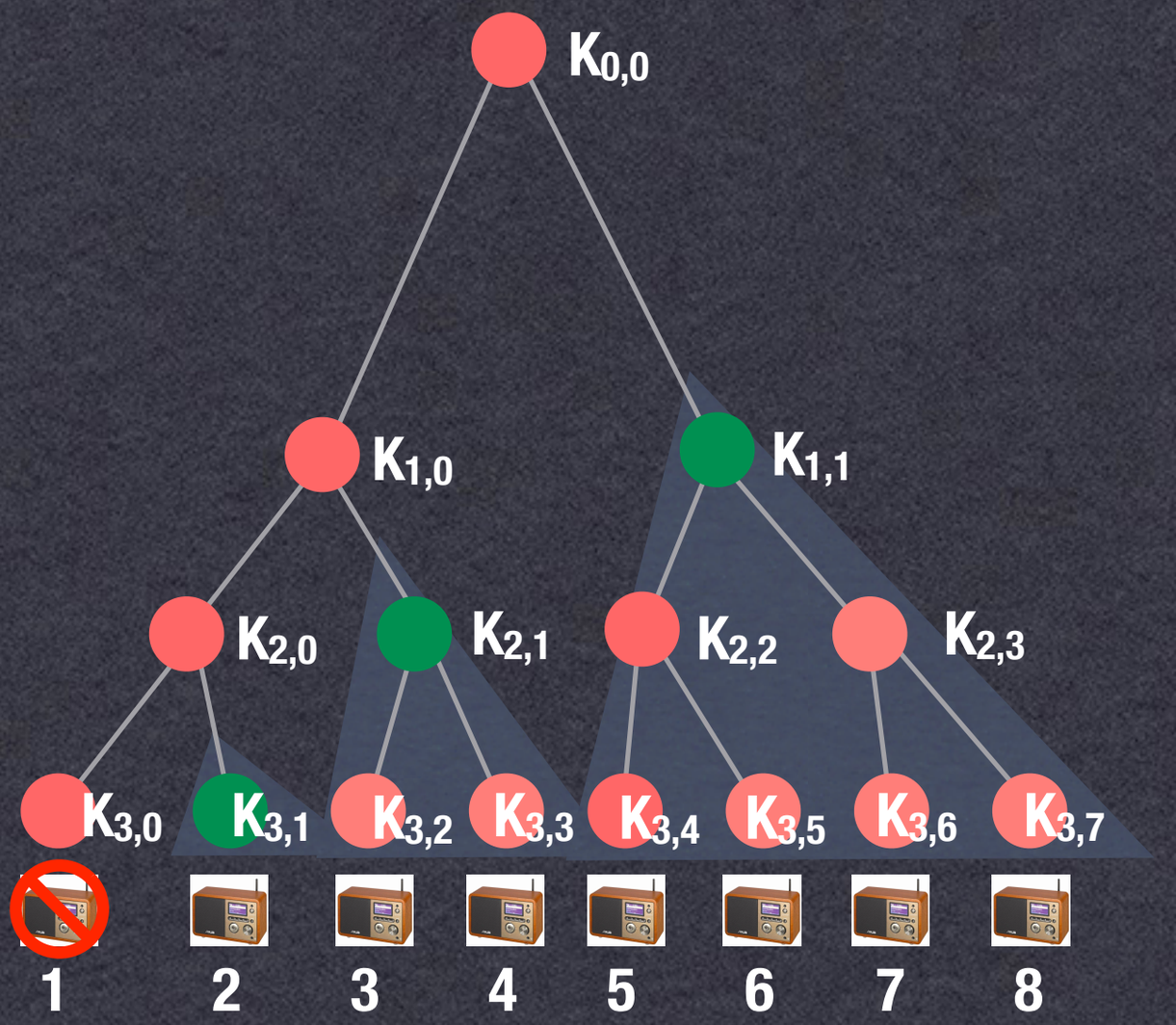
NNL Subset Cover



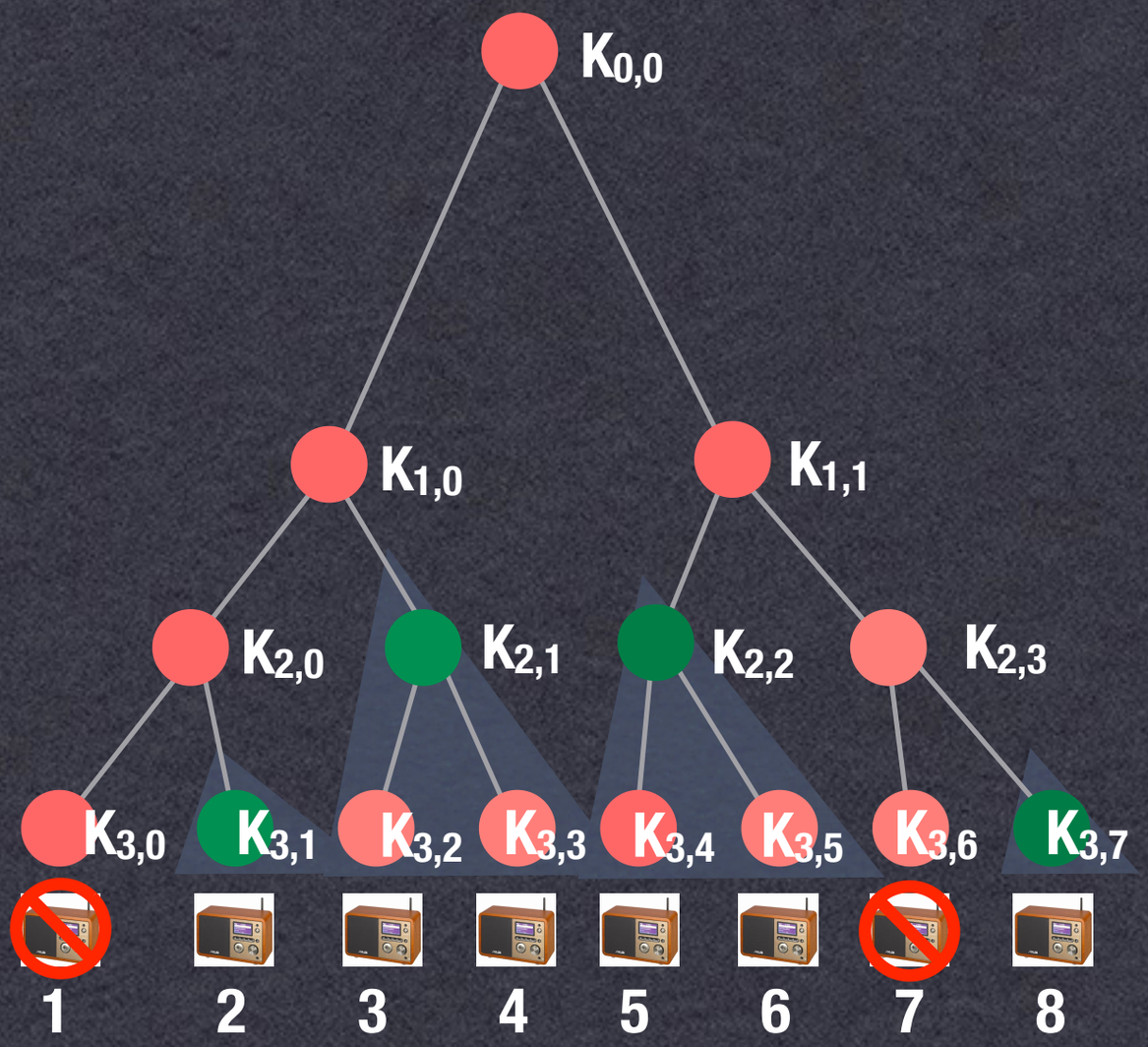
NNL Subset Cover



NNL Subset Cover



NNL Subset Cover



NNL Subset Difference

- AACS doesn't use Subset Cover
  - Uses an optimization called "Subset Difference"
  - Example, 1M players, 10k revoked:

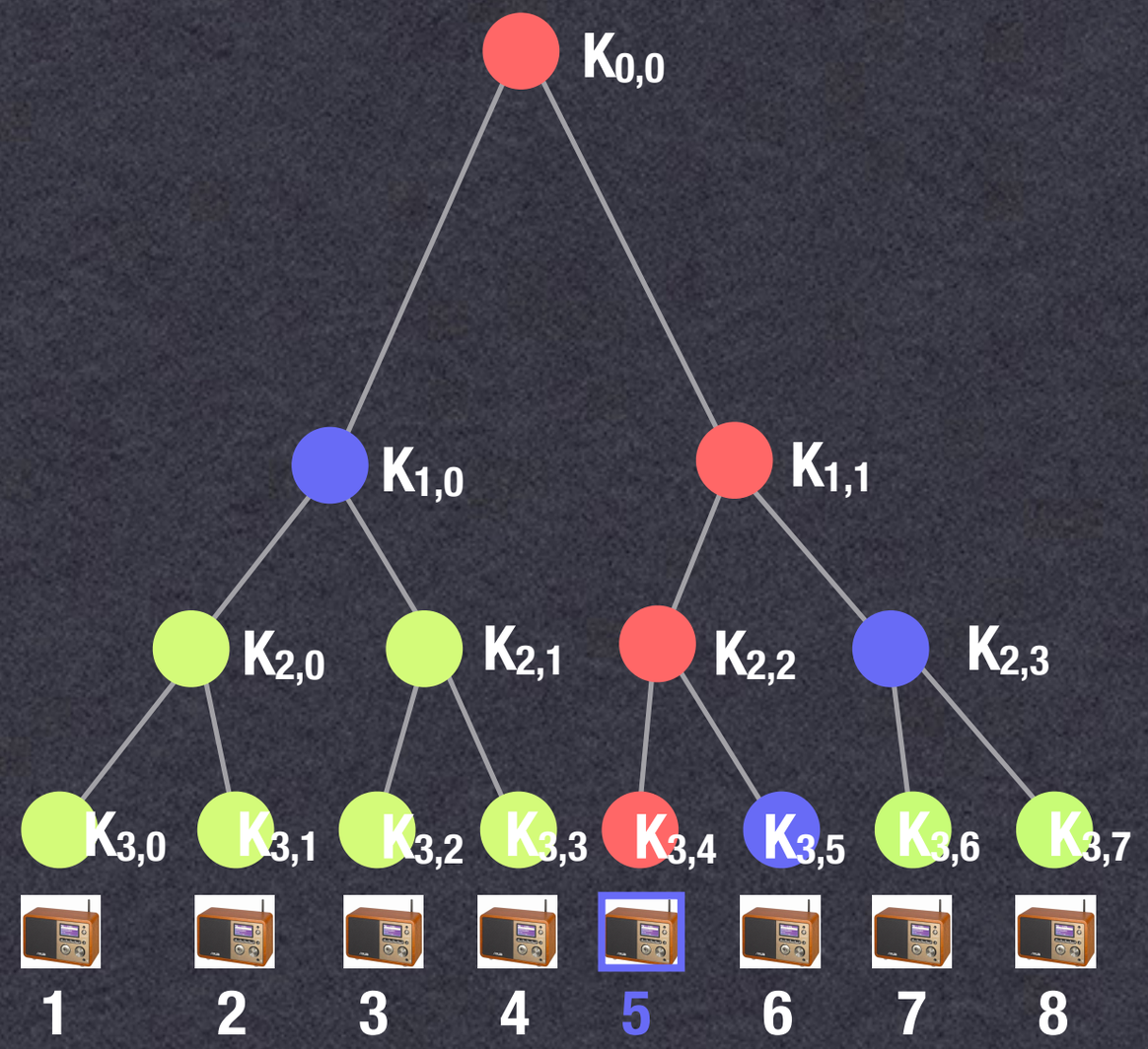
-<u>Subset Cover:</u>
~66,500 encryptions
about 1MB @ 16 bytes/per

-<u>Subset Difference:</u>
~20,000 encryptions
about 320KB

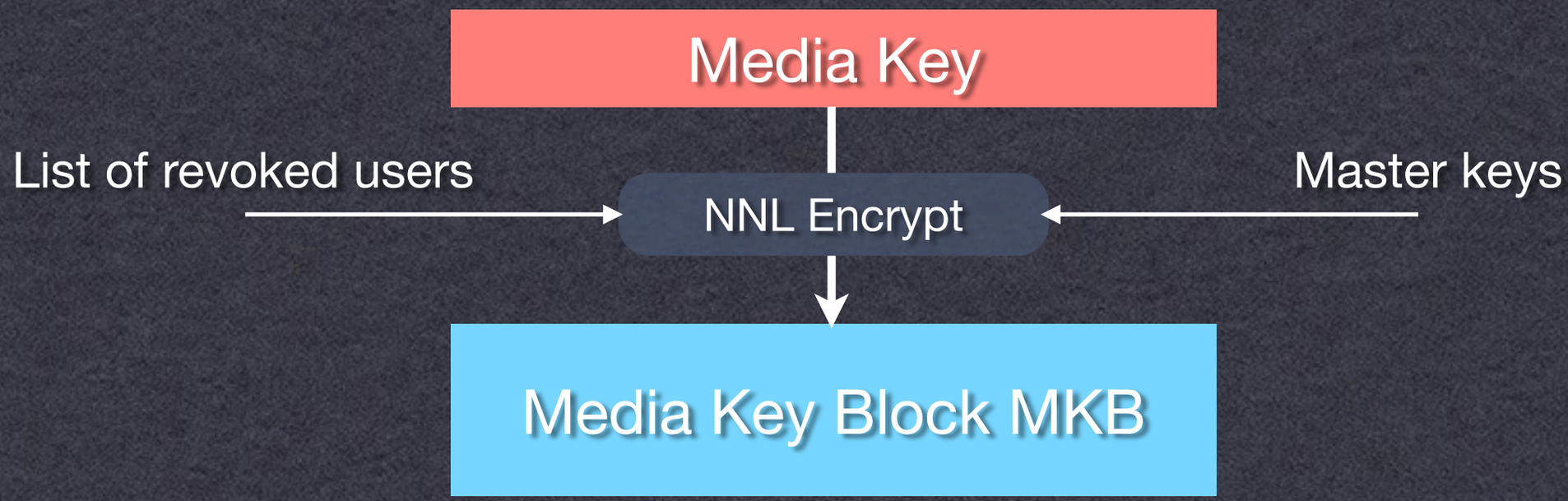
NNL Subset Difference

$K_{1,0}$ $K_{2,3}$ $K_{3,5}$

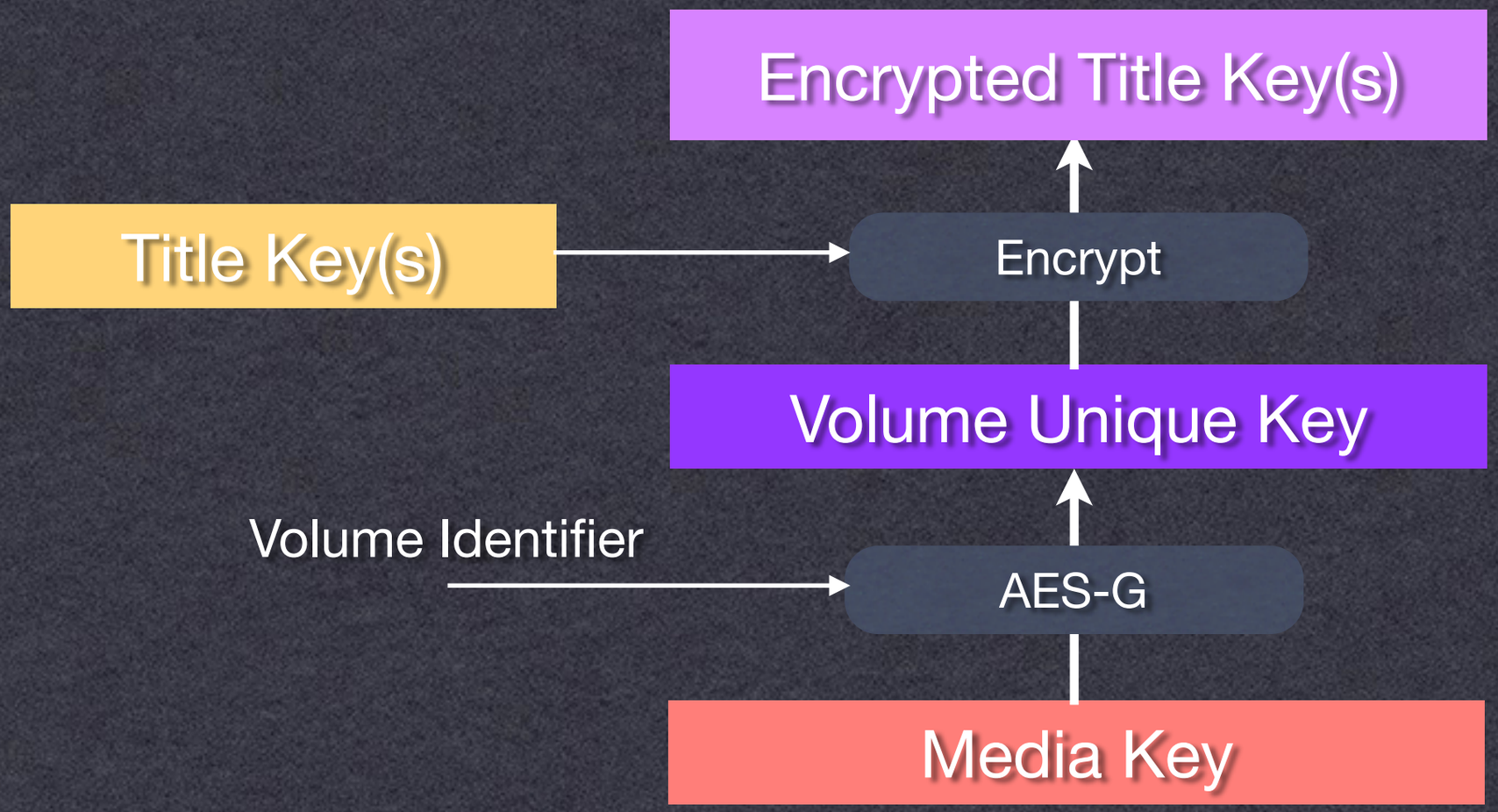
1



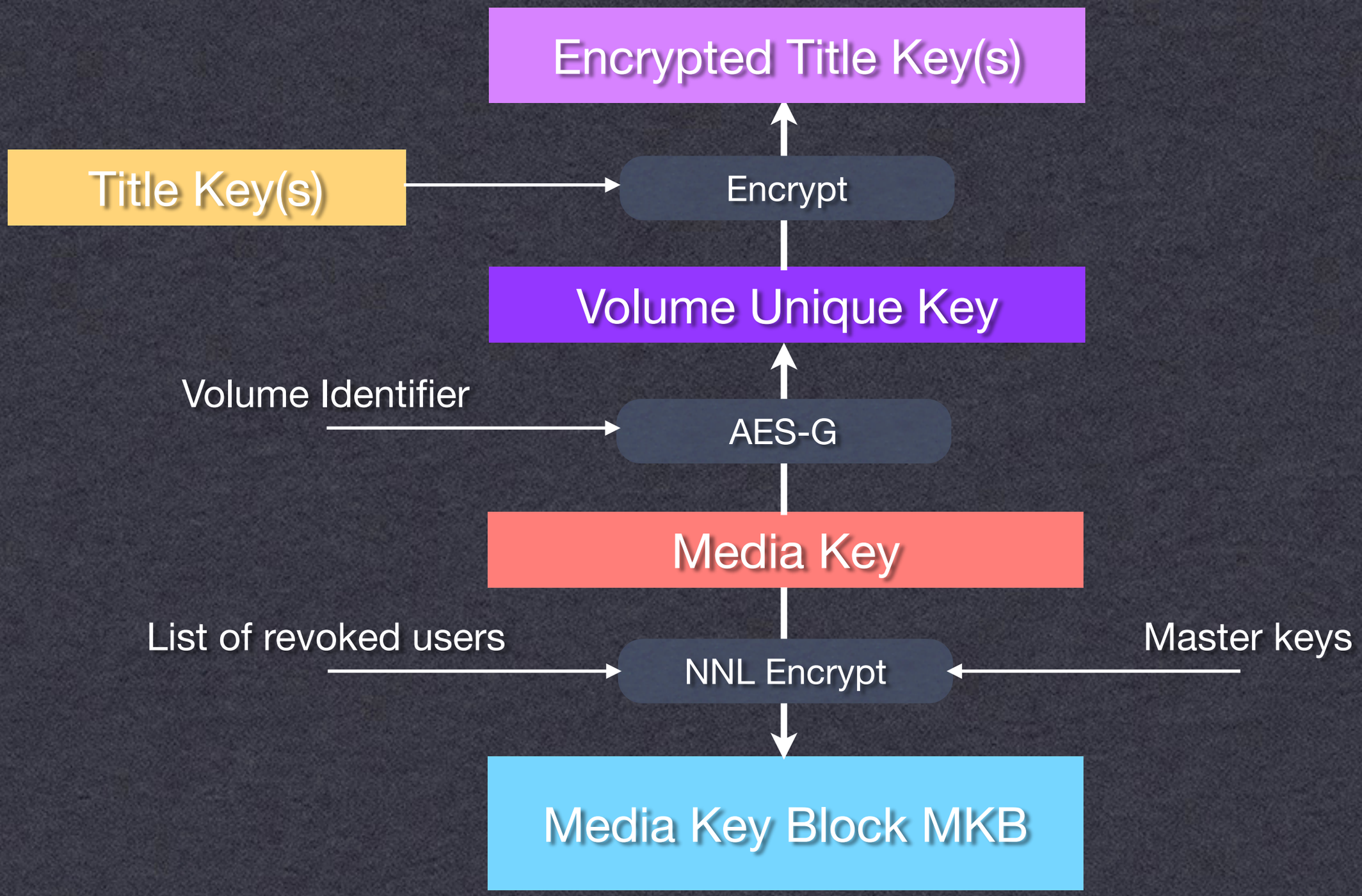
Key Flow (Encrypt)



Key Flow (Encrypt)



Key Flow (Encrypt)



Volume Identifier

- Another minor barrier
  - Each disk has a unique “Volume Identifier” (VID)

-Stored in a special area of the disk

-Can’t be accessed from filesystem

-Needed to derive VUKs

  - AACS designers: let’s make this hard to access

-Drive<->Computer cryptographic protocol

-uses Diffie-Hellman key agreement and MACs

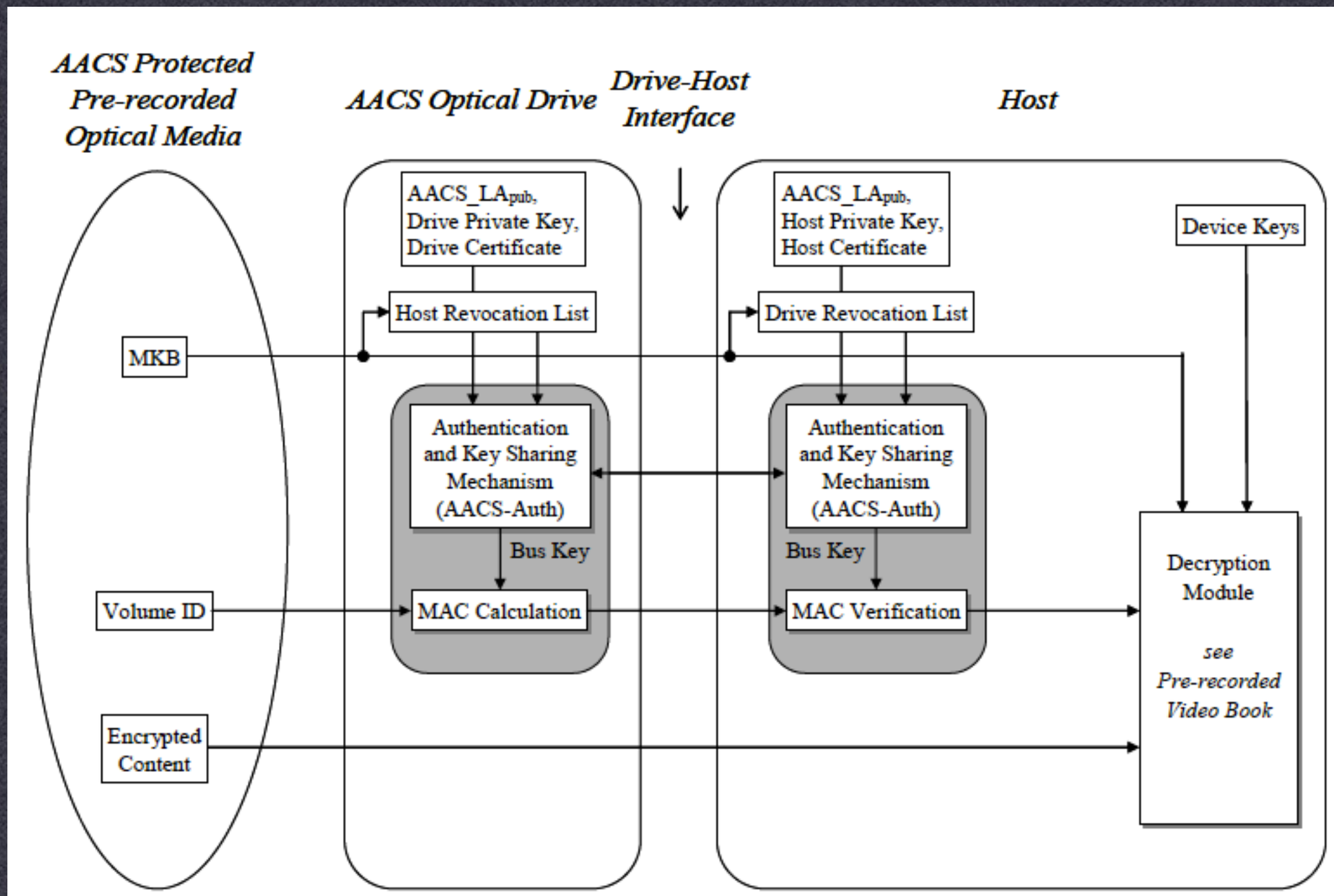


Figure 4-1 – Reading of Volume Identifier in a PC–based System

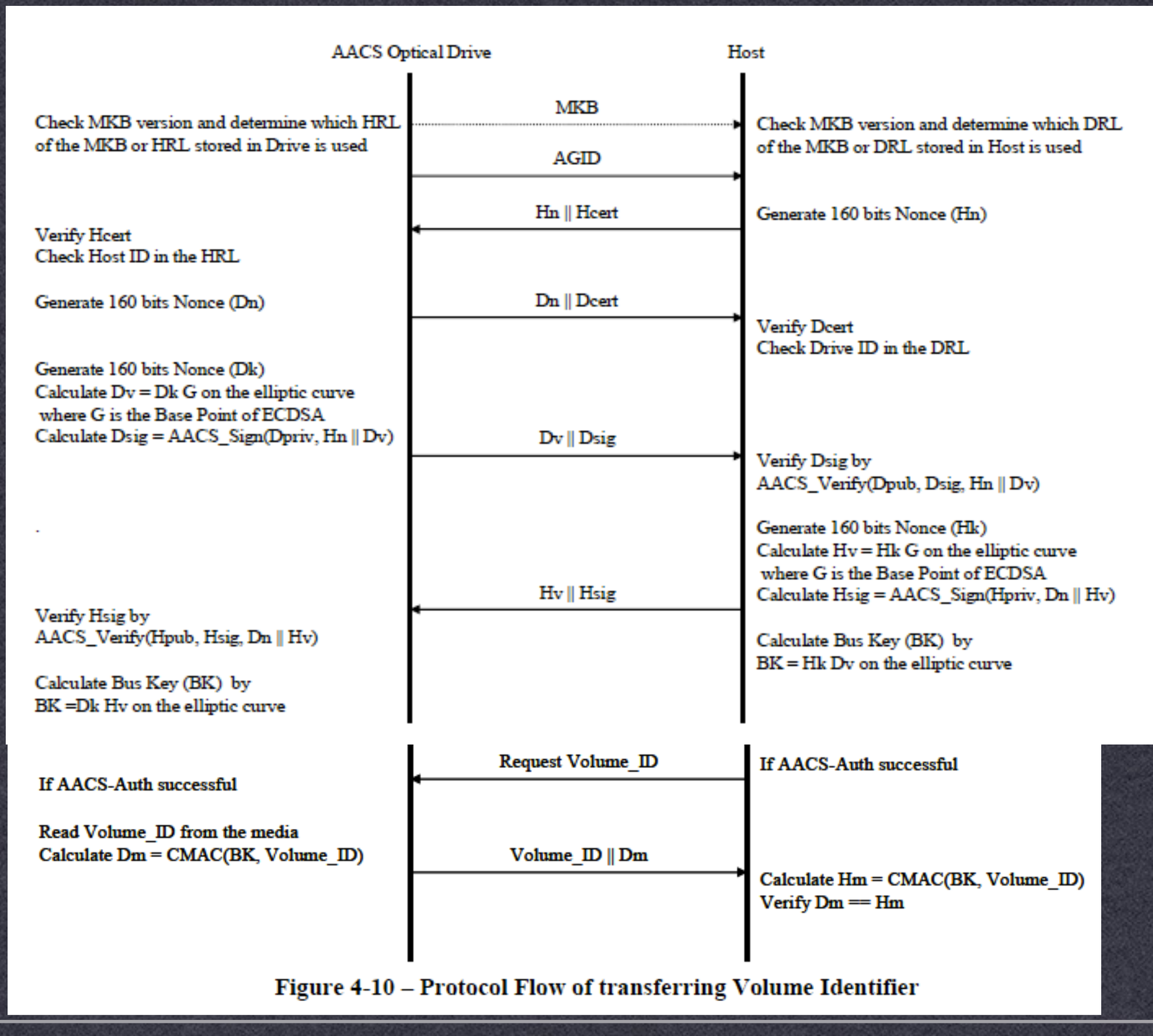


Figure 4-10 – Protocol Flow of transferring Volume Identifier

Content Signing