

Secure Content Management More than Encryption

Philips Research Natlab

Pim Tuyls

Jean-Paul Linnartz, Ton Kalker

PRANG-1

Let's make things better.



PHILIPS

Problem Setting

- Not just Alice and Bob (being trusted entities)
- No cryptographic solution for the problem

But through standardization:

Alice sells data to unreliable Bob, who can only process this data on a trusted device

Compliant world:

- CE devices using authenticated and encrypted links
- Manufacturer agreed to follow copy protection rules
 - Licensing agreement
 - Therefore he gets crypto keys
- Non-compliant devices never get anything in the clear

PRANG-2

Let's make things better.



PHILIPS

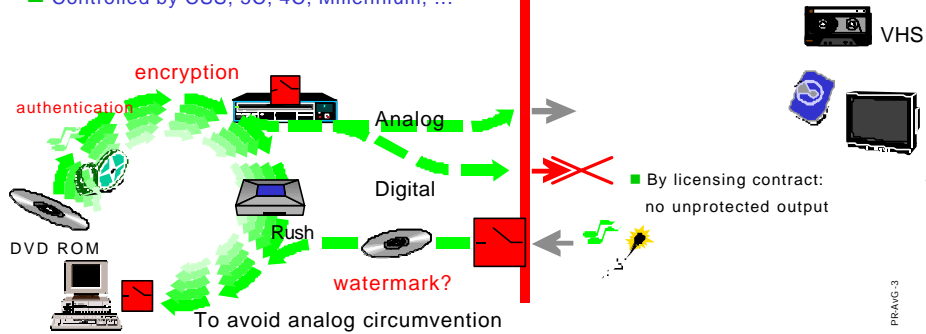
Copyrighted content in the digital world of the future will only flow over compliant devices

Compliant World

- All content is encrypted on all interfaces
- Controlled by CSS, 5C, 4C, Millennium, ...

Non-Compliant World

- All analog devices, some digital



Let's make things better.



PHILIPS

PRANG-3

Consequences of this approach

- Protected content is encrypted on any open interface
- Just encryption is not enough (bit-bit copying)
 - Authentication + session key for all interfaces
 - Physical Marks for Discs (Wobbles)
- End to end encryption is not suitable from a processing point of view
- Output is analog: additional protection is required:
watermarking

Let's make things better.

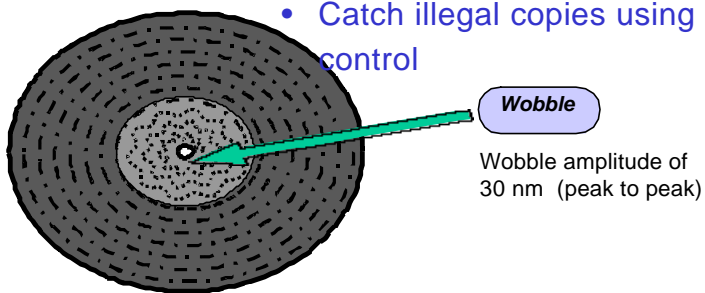


PHILIPS

PRANG-4

Anti-Cloning: use a physical mark for discs

- Encrypted content can be cloned.
- Store the keys as a physical id which is hard to duplicate, even in a disc press environment
- Catch illegal copies using play-back control



PRANG-5

Let's make things better.



PHILIPS

Watermarking

Requirements:

- Imperceptible
- Robust and/or fragile
- Difficult to remove
- Fast and Cheap
- Payload
- Prob of error should be small



Cryptography: bit exact

PRANG-6

Let's make things better.



PHILIPS

Applications of Watermarking

- Copyright control
 - playback, copy-generation control (DVD, SDMI)
- Meta data and referral service
- Broadcast monitoring
 - check on royalty payments
 - commercial verification
- Distribution tracing
 - fingerprinting
- Proof of ownership (with zero knowledge?)
- Proof of authenticity

PRANG-7

Let's make things better.



PHILIPS

Open Directions

- Theoretical model to quantify the security of Watermarks
 - formal definitions
 - tradeoffs between impercept-capacity-robustness-security
- Practical Methods for secure watermarking
 - coding schemes for a certain security level
 - benchmarking tools and methodologies
- Integration of Crypto and Watermarking
 - e.g. applications as DVD video
- Zero-Knowledge proof of ownership
 - committing to a watermark
 - showing presence in a permuted version (reveal either permuted watermark or permutation)

PRANG-8

Let's make things better.



PHILIPS

Other Directions

- Play/Copy Once.
- Traceability:
 - more efficient IPP/Frameproof codes
 - efficient (anonymous) embedding techniques
- Anonymity
- Key Management:
 - Revocation mechanisms
 - users leaving the system
 - compromised keys
- Robust Implementation
 - what can and what can not be achieved

PRAAG-9

Let's make things better.**PHILIPS**

Conclusions

- Content protection is critical in an economy that more and more relies on knowledge
- Content Providers do not want to stop the dissemination of content, they want to earn money with content
- How to build a good model that allows the validation of systems based on cryptographic and other tools as watermarking, wobbles....

PRAAG-10

Let's make things better.**PHILIPS**