

Cryptographic Aspects of DRM



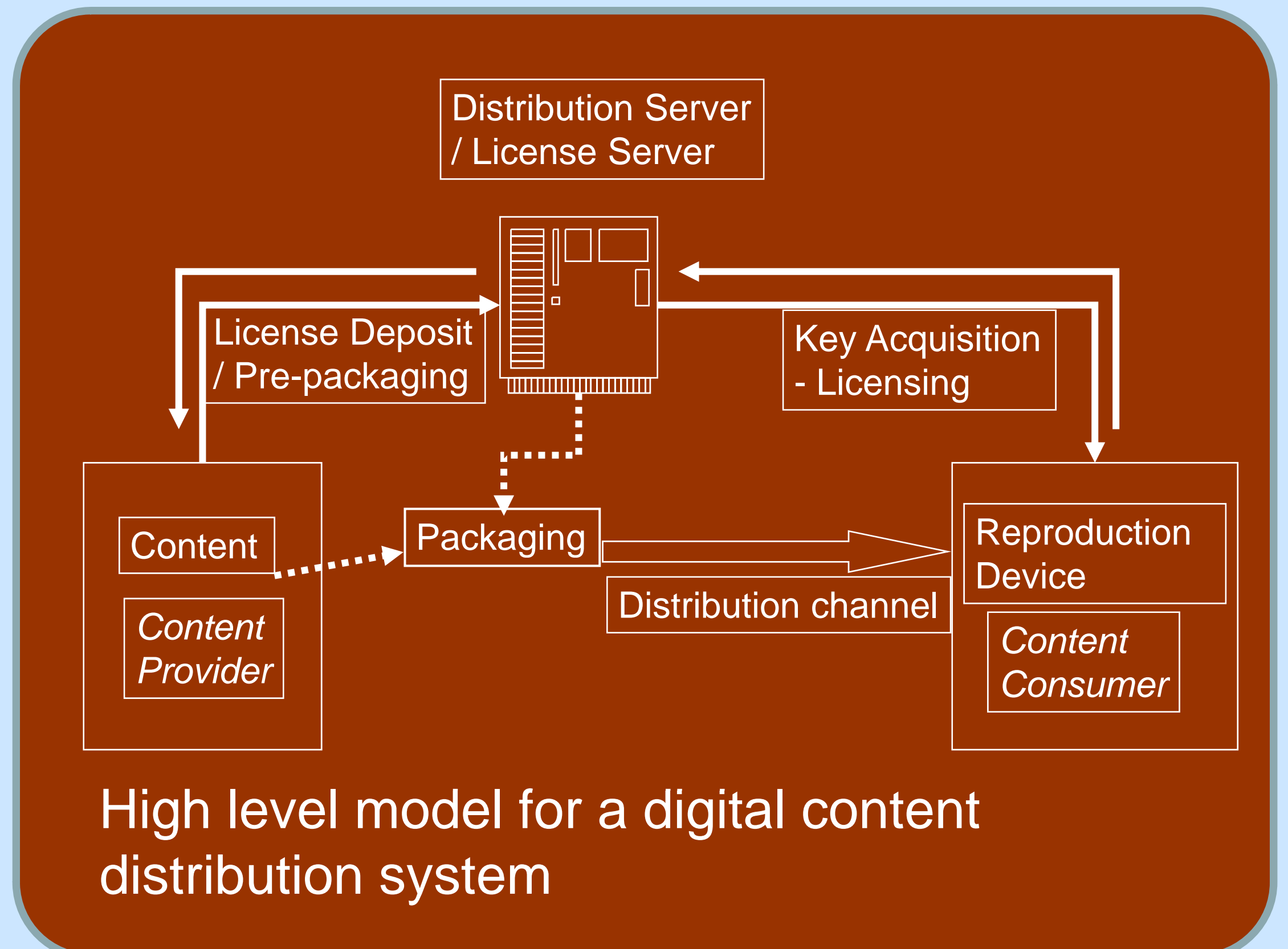
Aggelos Kiayias (PI)

www.cse.uconn.edu/~akiayias

Putting Cryptography to Work for DRM

How can intellectual products be distributed in the information highways so that the rights of **both** content producers and content consumers are upheld? **Digital rights management (DRM)** is a critical area that is at the heart of protecting human creativity in the digital world.

A Fundamental Question: At the heart of the DRM problem we have an issue of **trust**: by trusting that the underlying components of a DRM system operate ideally it is possible to obtain solutions. But building trustworthy components can be impossible or very costly. Can we use cryptographic methods to provide palatable guaranties for trustworthy operation in environments of mutually distrusting and possibly adversarial parties?



High level model for a digital content distribution system

Our current foci:

- Provable security of cryptographic primitives for DRM in realistic attack scenarios.
- Traitor tracing, tracing & revocation mechanisms, blind/group/hidden ID-based/traceable identification & signatures.
- Electronic Markets.
- Attacks against DRM encryption systems.

Approach and Impact

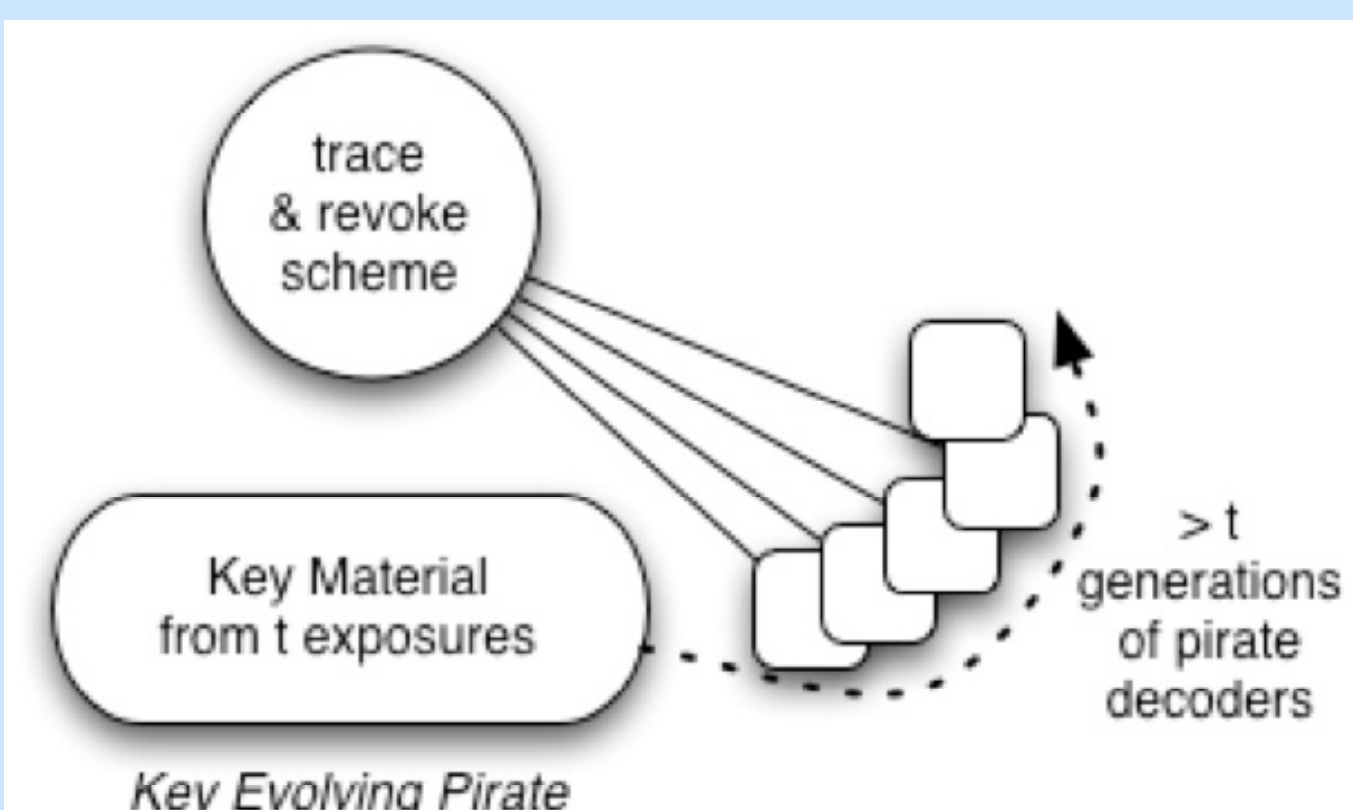
Research Impact:

- Design of composable DRM cryptographic primitives that can be used in a plug-and-play fashion.
- Evolve the new generation of DRM.
- Bring formal security arguments to the practice of DRM.
- Provide systems that facilitate basic human rights of expression and use.

some recent results

Pirate Evolution :

demonstrates how it is possible to prolong piracy by careful key scheduling. [Crypto 2007]



Blind Signatures :

First practical universally composable blind signature scheme. [TCC 2008]

Algebraic Structure of DRM related encryption :

