

RSA[®]Conference2015

San Francisco | April 20-24 | Moscone Center

SESSION ID: CRYP-F03

Communication Optimal Tardos- based Asymmetric Fingerprinting

Qiang Tang

University of Connecticut & University of Athens
joint work with Aggelos Kiayias, Nikos Leonardos, Helger Lipmaa, and Kateryna Pavlyk

CHANGE

Challenge today's security thinking



A Motivational Example

A Movie Producer



Cinema 1



Cinema 2

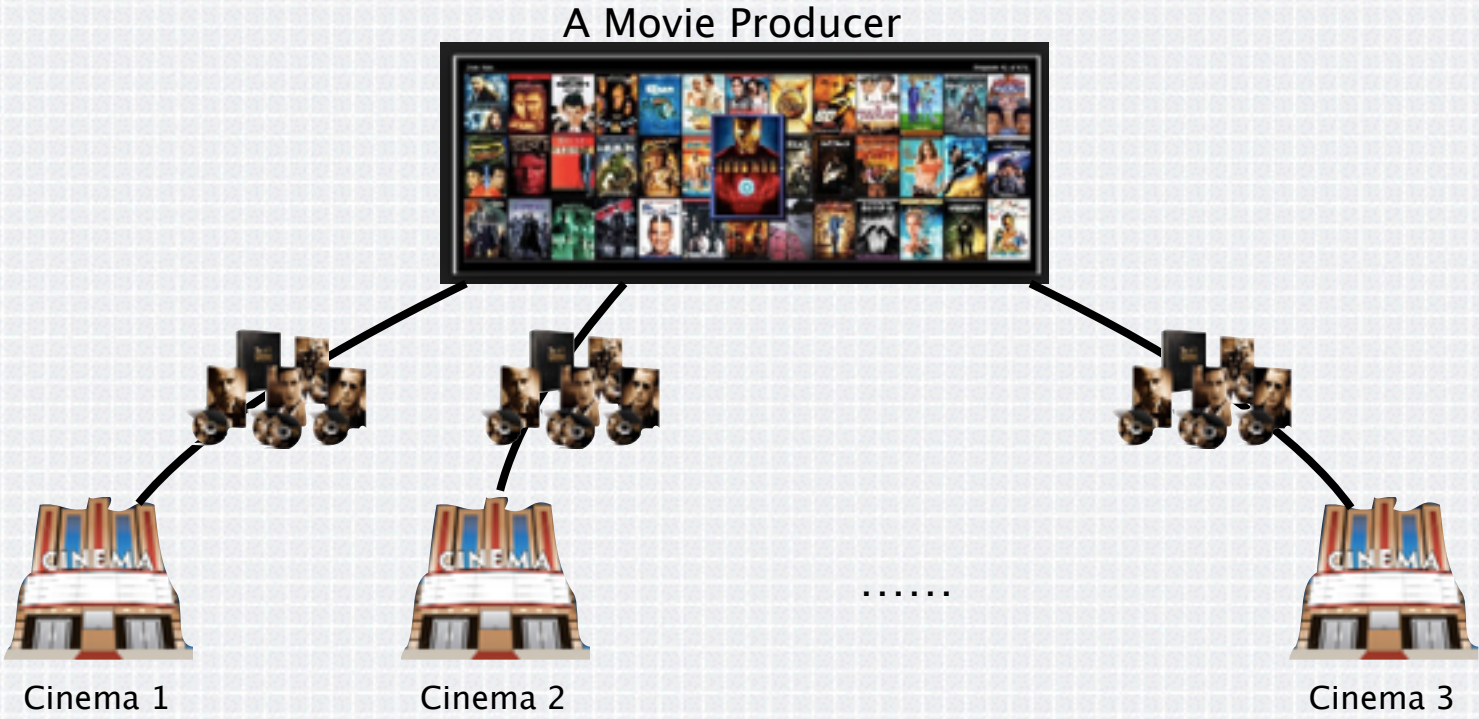
.....



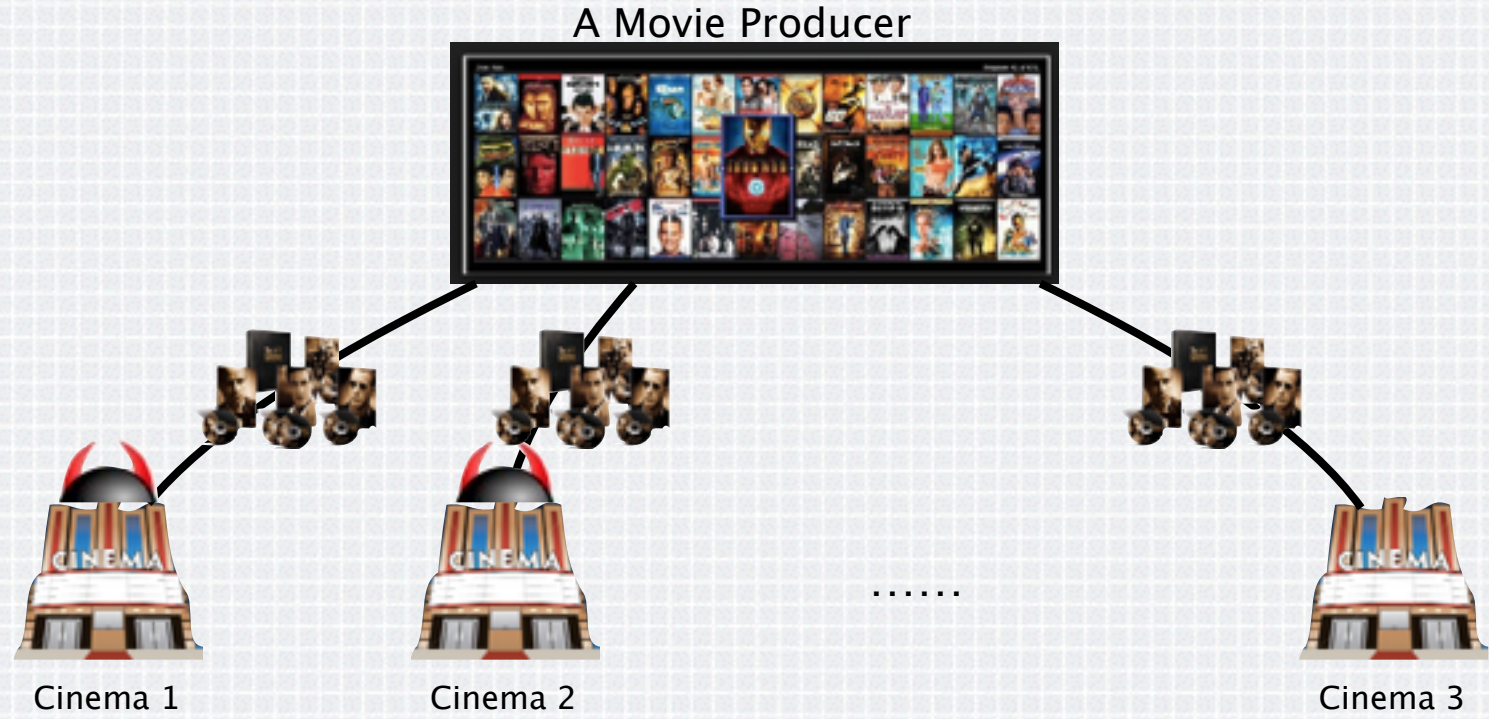
Cinema 3



A Motivational Example



A Motivational Example



A Motivational Example



The screenshot shows an eBay product listing for "Godfather-HD". The page layout includes the eBay logo, a search bar, and navigation tabs for various categories. The product title is "Godfather-HD" with a "FREE shipping" badge. The listing features a collage of images including the DVD box set and individual discs. The price is listed as \$5.99, and there are buttons for "Buy It Now" and "Add to cart". Additional options include a GeekSquad warranty for \$27.99. Shipping and delivery information is provided at the bottom of the listing.

ebay  HI, smeechiebutta! (Sign out)

CATEGORIES ELECTRONICS FASHION MOTORS TICKETS DEALS CLASSIFIEDS

Back to Daily Deals | Listed as Nexus 7 32GB, Wi-Fi, 7in - Black in category: Computers/Tablets & Networking > iPads, Tablets & ebook Readers

Godfather-HD 

Item condition: **New**

Quantity: Limited quantity available / 1,228 sold

Price \$5.99 [Buy It Now](#)

GeekSquad 2 yr warranty \$27.99
See other plans from \$19.99 [Add to cart](#)

[Add to Watch list](#)

Bill Me Later Get 6 months to pay
Subject to credit approval. See terms

Shipping: **FREE** Standard Shipping | See details
Item location: Elizabeth, New Jersey, United States
Ships to: United States See exclusions

Delivery: Estimated between Thu, Jan. 3 and Wed, Jan. 9
Use One-day Shipping to get it by Jan. 3

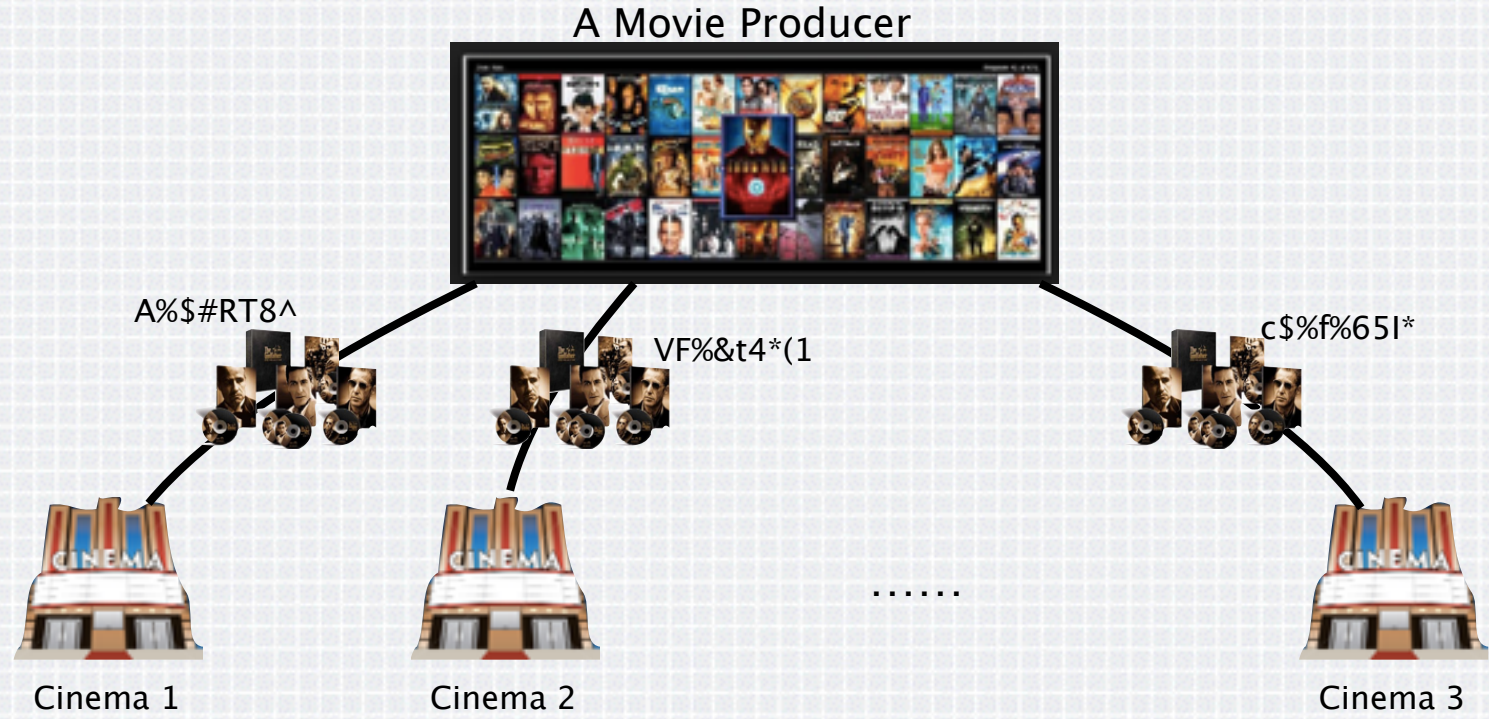
Payments: **PayPal**, Bill Me Later | See details

A Motivational Example

How to identify the source of the pirate?



Fingerprinting



A Motivational Example



The screenshot shows an eBay product listing for 'Godfather-HD'. The page layout includes the eBay logo, a search bar, and navigation tabs for 'ELECTRONICS', 'FASHION', 'MOTORS', 'TICKETS', 'DEALS', and 'CLASSIFIEDS'. The product title is 'Godfather-HD' with a 'FREE shipping' badge. The listing features a collage of images including the DVD box set and individual discs. The price is \$5.99, and there are buttons for 'Buy It Now' and 'Add to cart'. A 'GeekSquad 2 yr warranty' option is available for \$27.99. Shipping is free standard shipping, and delivery is estimated for January 3-9. Payment options include PayPal and 'Bill Me Later'.

ebay  HI, smeechiebutta! (Sign out)

CATEGORIES → ELECTRONICS FASHION MOTORS TICKETS DEALS CLASSIFIEDS

Back to Daily Deals | Listed as Nexus 7 32GB, Wi-Fi, 7in - Black in category: Computers/Tablets & Networking > iPads, Tablets & ebook Readers

Godfather-HD 

Like Want (4) Own (2) ★★★★★ 14 product reviews

Item condition: **New**

Quantity: Limited quantity available / 1,228 sold

Price \$5.99 **Buy It Now**

Add to cart

GeekSquad 2 yr warranty \$27.99
See other plans from \$19.99 **Add to watch list**

Bill Me Later Get 6 months to pay
Subject to credit approval. See terms

Shipping: **FREE** Standard Shipping | See details
Item location: Elizabeth, New Jersey, United States
Ships to: United States See exclusions

Delivery: Estimated between Thu, Jan. 3 and Wed, Jan. 9
Use One-day Shipping to get it by Jan. 3

Payments: **PayPal**, **Bill Me Later** | See details

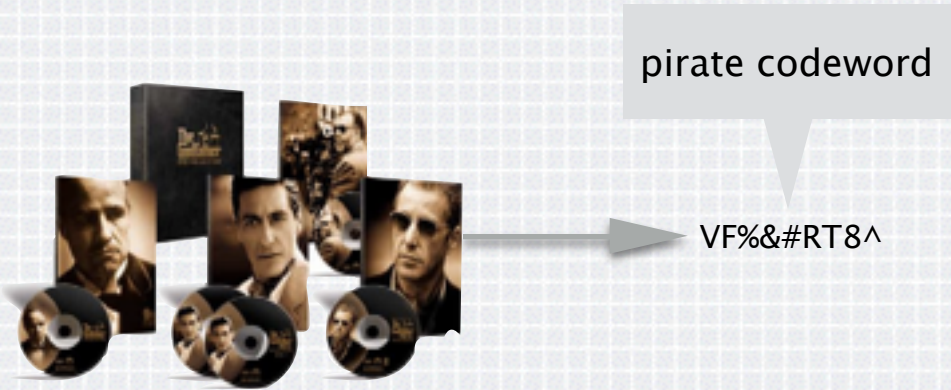
Fingerprinting



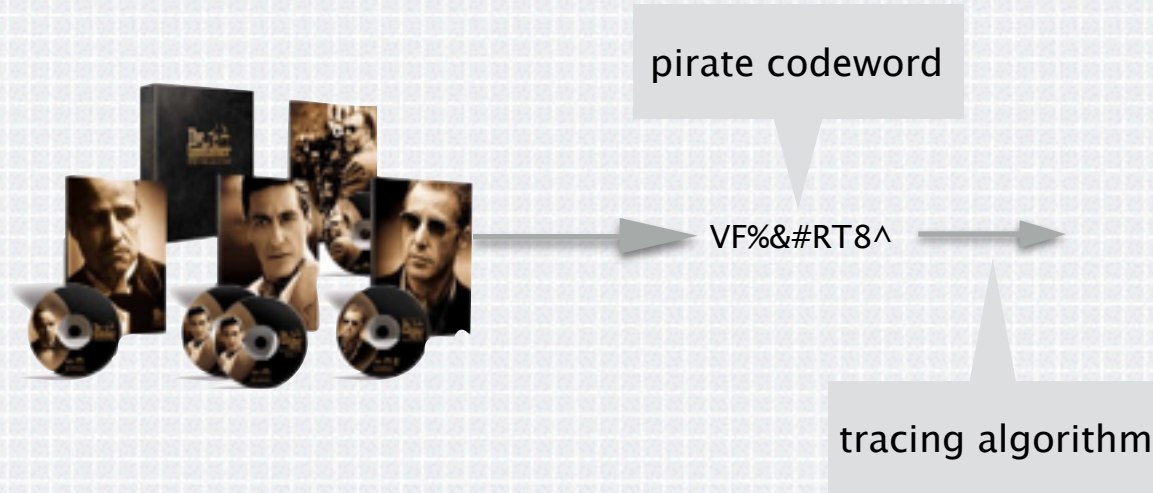
Fingerprinting



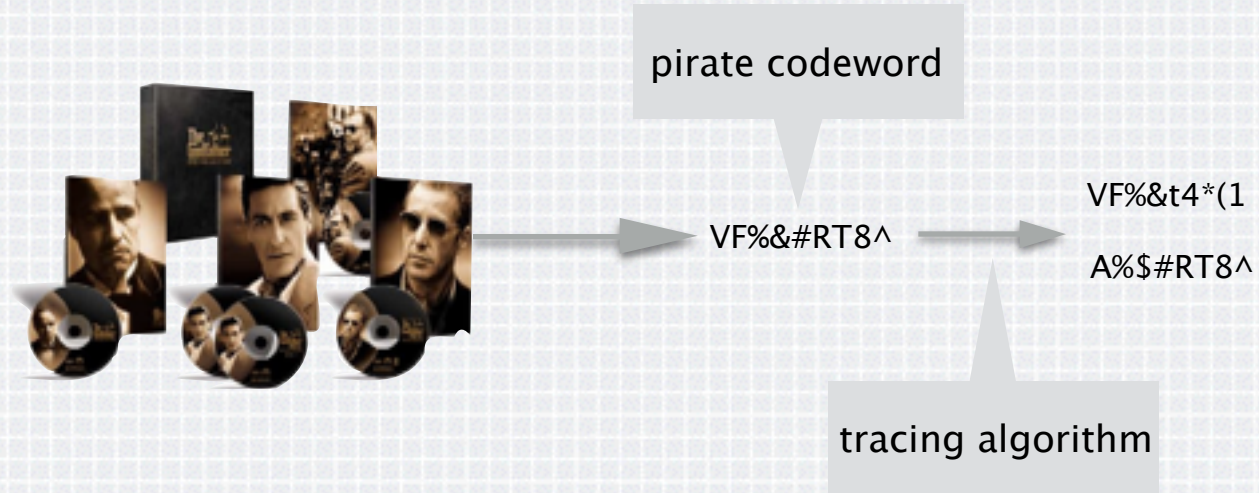
Fingerprinting



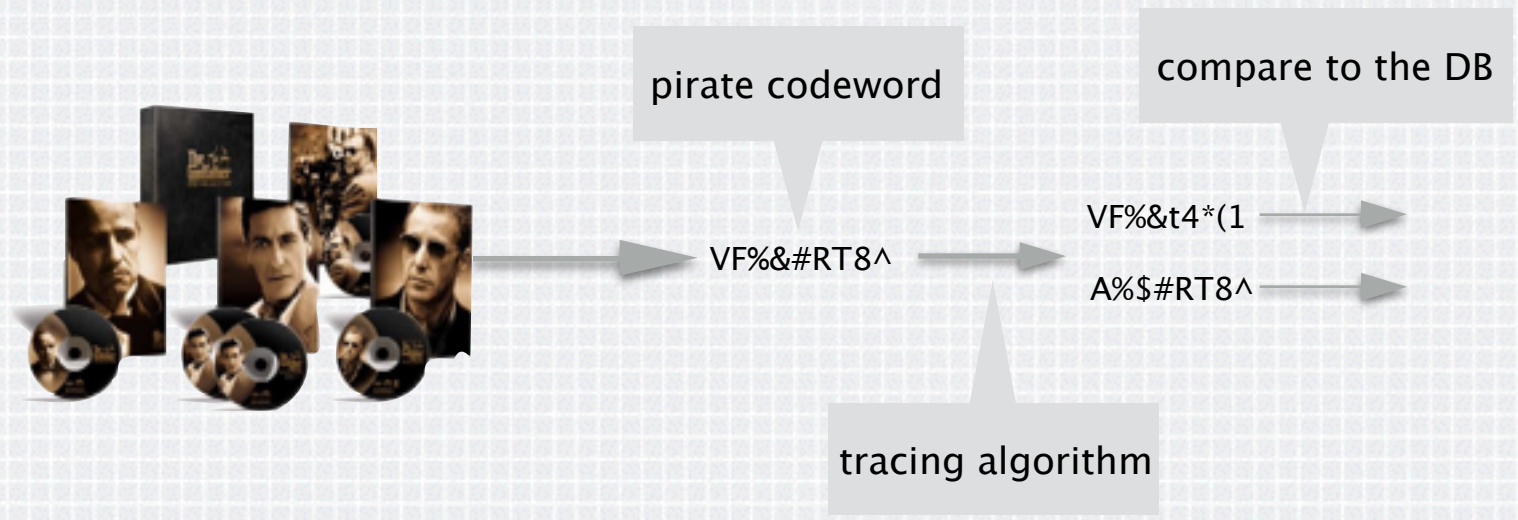
Fingerprinting



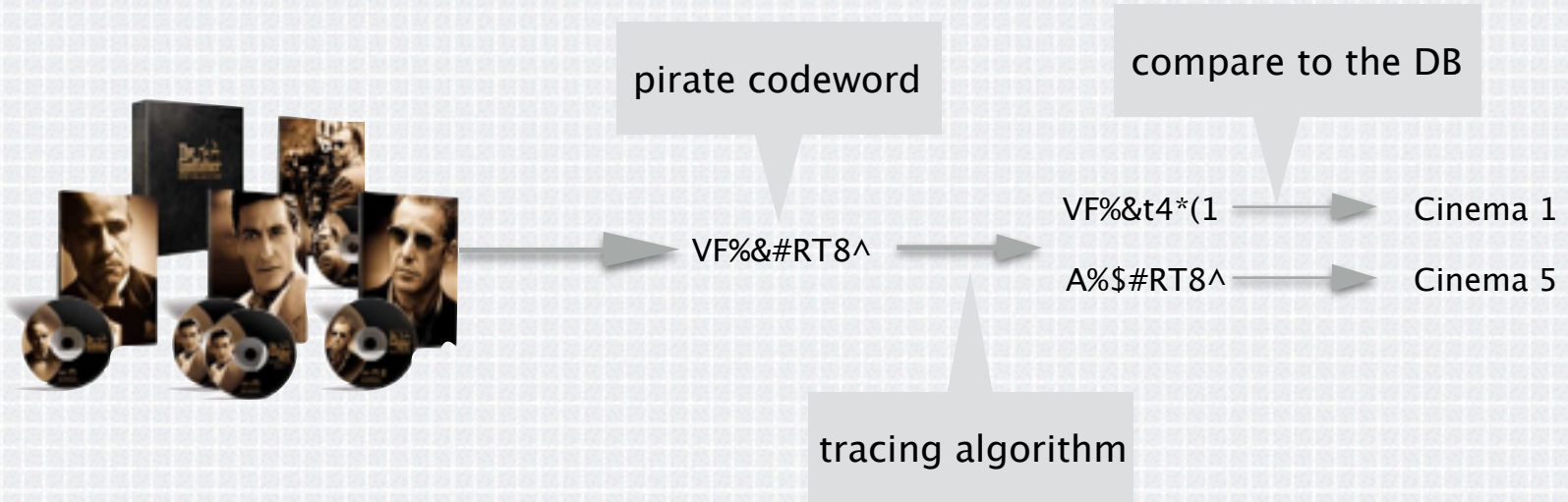
Fingerprinting



Fingerprinting



Fingerprinting



The Goals of Fingerprinting

- ◆ Individualize contents



The Goals of Fingerprinting

- ◆ Individualize contents
- ◆ Trace back to the sources



A Catch

Does fingerprinting really de-incentivize illegal content re-distribution?



A Catch

- ◆ **Both** the content provider and the content receiver can leak a copy



A Catch

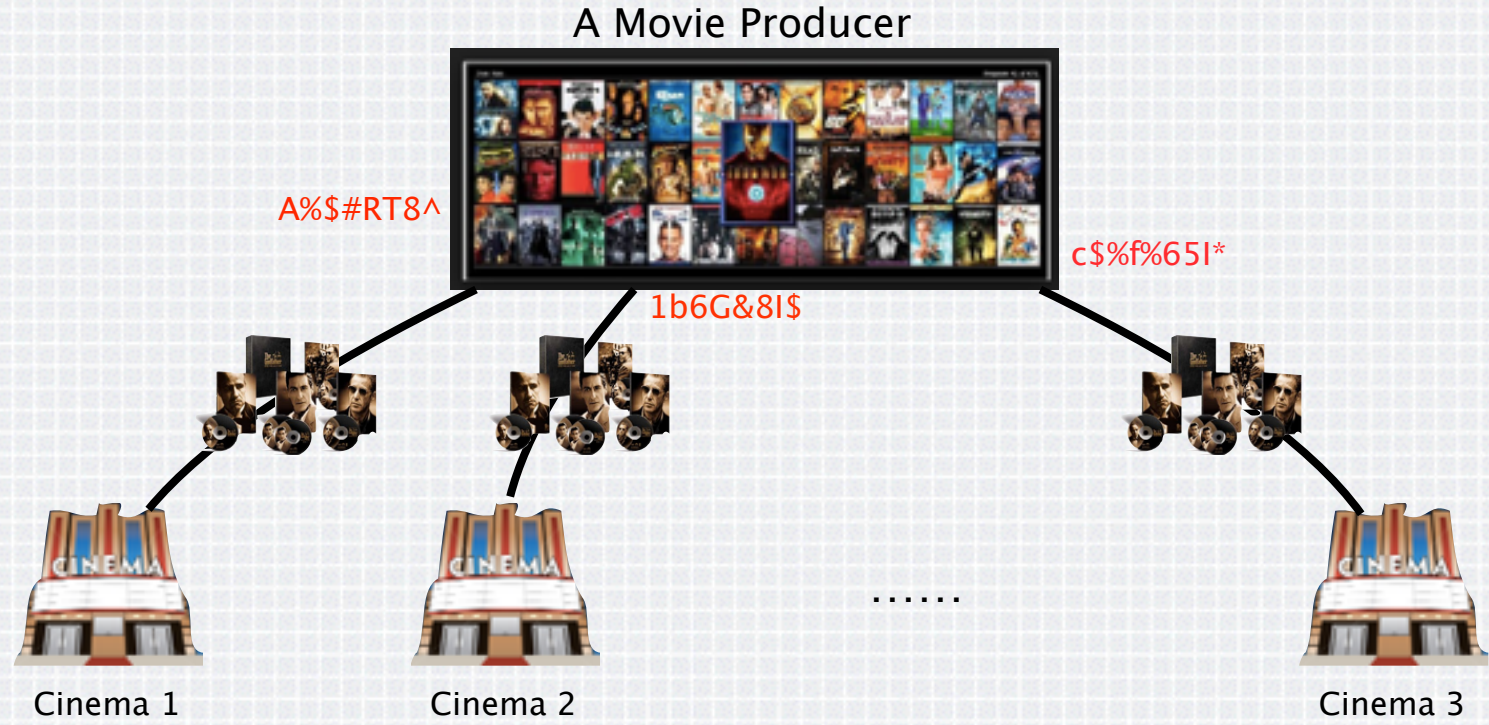
- ◆ **Both** the content provider and the content receiver can leak a copy
- ◆ The copy found in the public can not serve as a **undeniable** proof



Asymmetric Fingerprinting

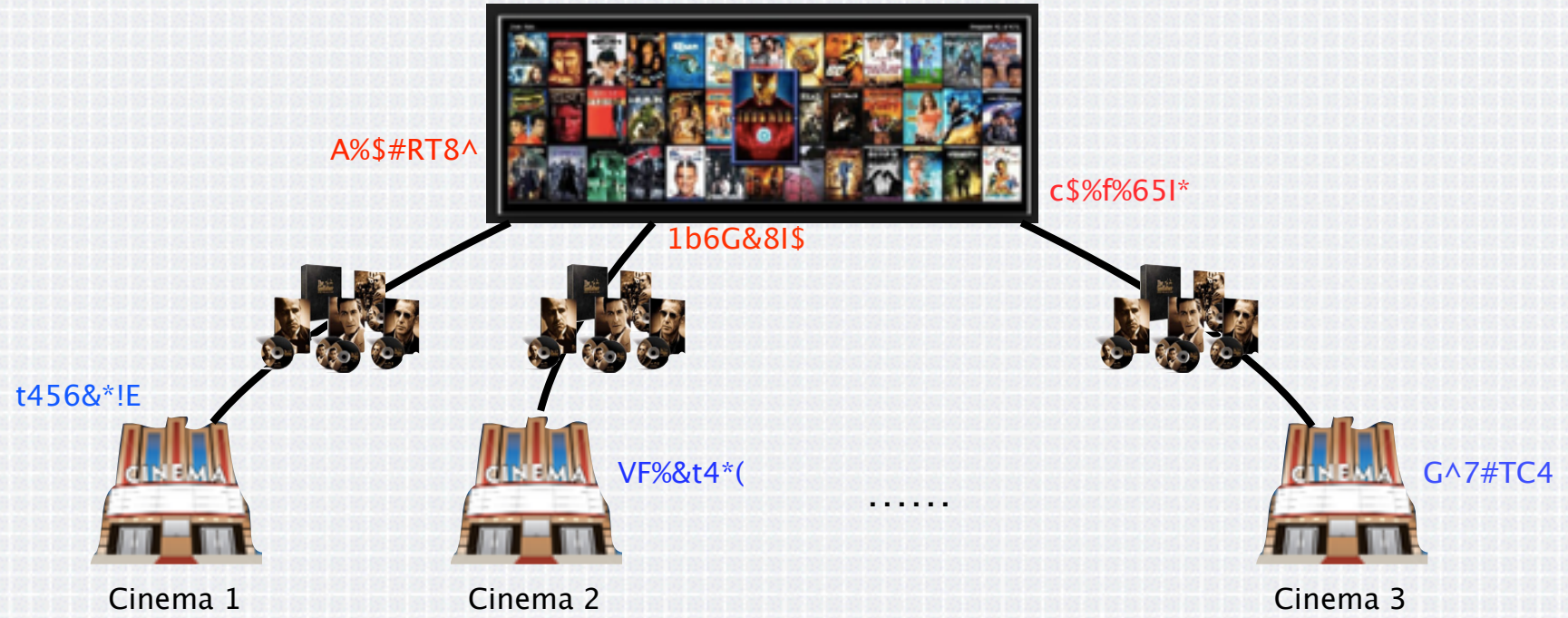


Asymmetric Fingerprinting

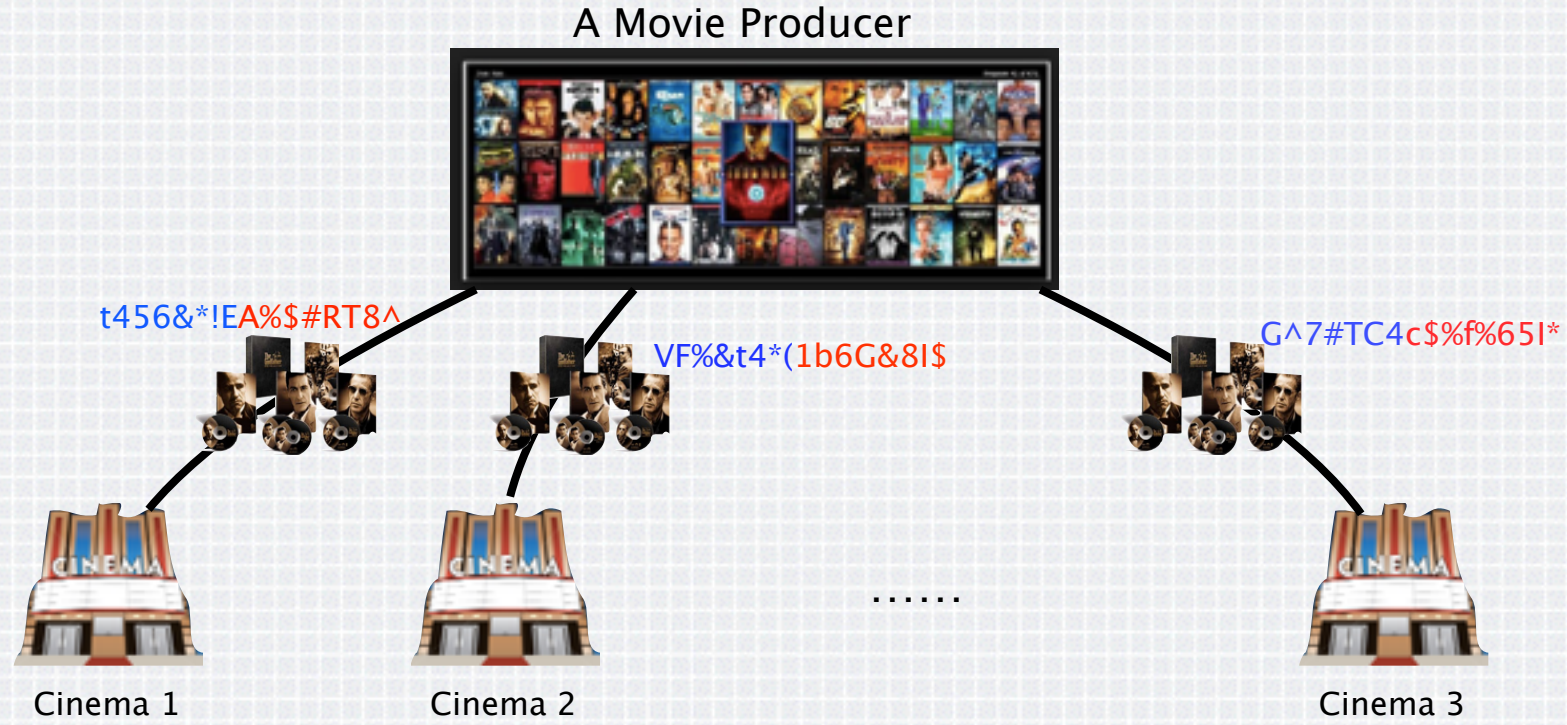


Asymmetric Fingerprinting

A Movie Producer



Asymmetric Fingerprinting



Asymmetric Fingerprinting

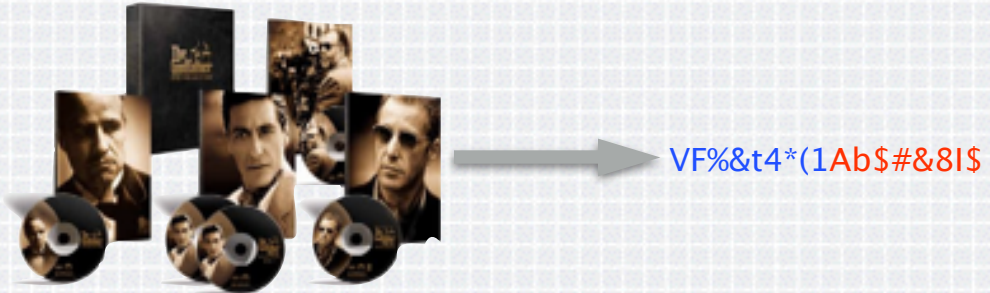
The screenshot shows an eBay product listing for 'Godfather-HD'. The listing includes a 'FREE shipping' badge, a 'Like' button, a 'Watch' button (with 4 items), and a 'Check out' button (with 2 items). The item condition is 'New' and the quantity is 1, with a note that 'Limited quantity available / 1,228 sold'. The price is \$5.99. There are 'Buy It Now' and 'Add to cart' buttons. A 'GeekSquad 2 yr warranty \$27.99' option is available, with other plans starting at \$19.99. There is also an 'Add to watch list' button. Below the main listing, there is a 'Bill Me Later' option for 6 months to pay, subject to credit approval. Shipping is free standard shipping from Elizabeth, New Jersey, United States, to the United States. Delivery is estimated between Thursday, Jan. 3 and Wednesday, Jan. 9. Payments are accepted via PayPal and Bill Me Later.



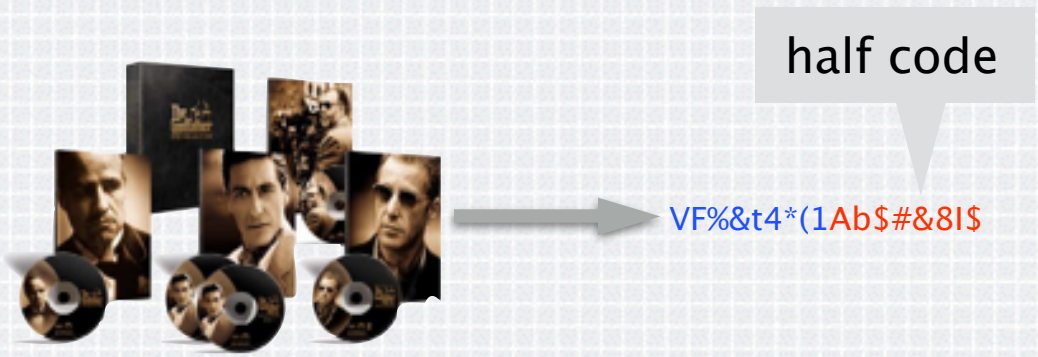
Asymmetric Fingerprinting



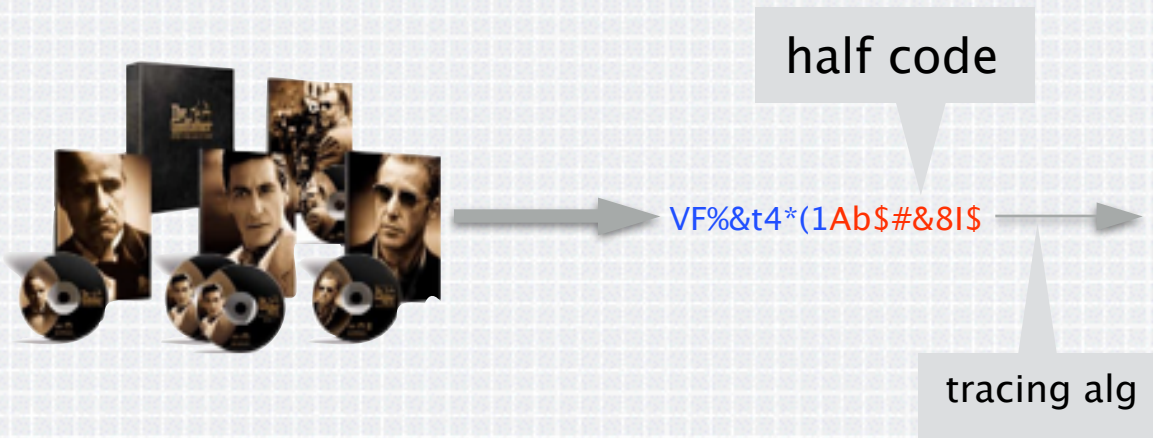
Asymmetric Fingerprinting



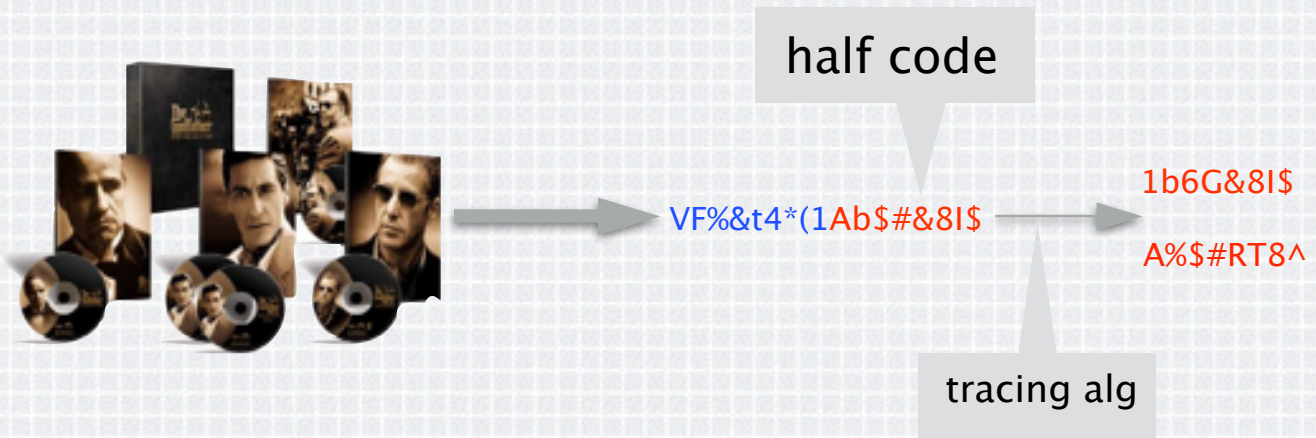
Asymmetric Fingerprinting



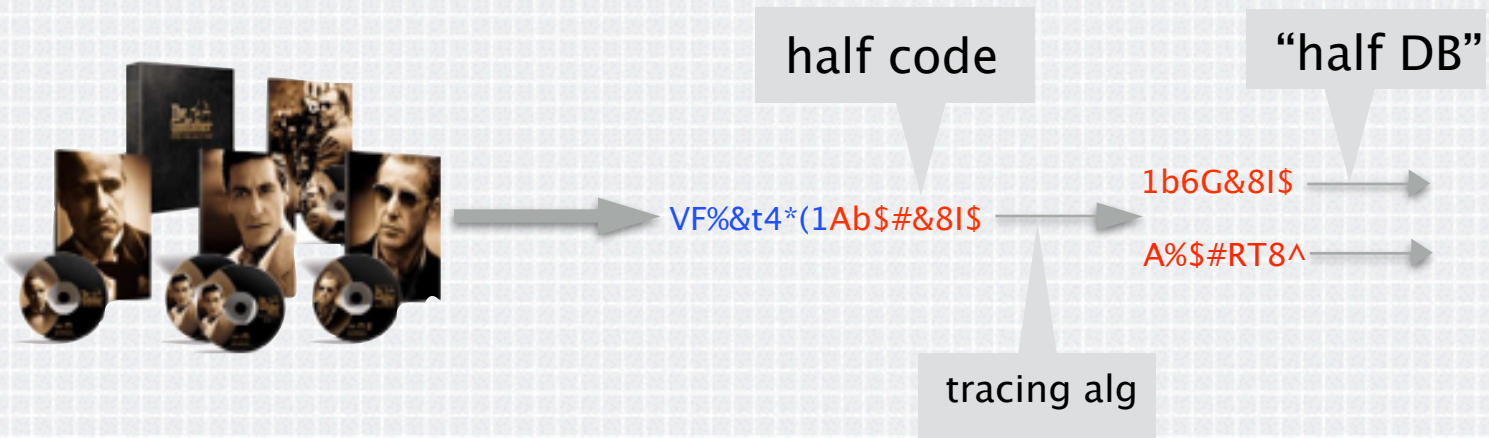
Asymmetric Fingerprinting



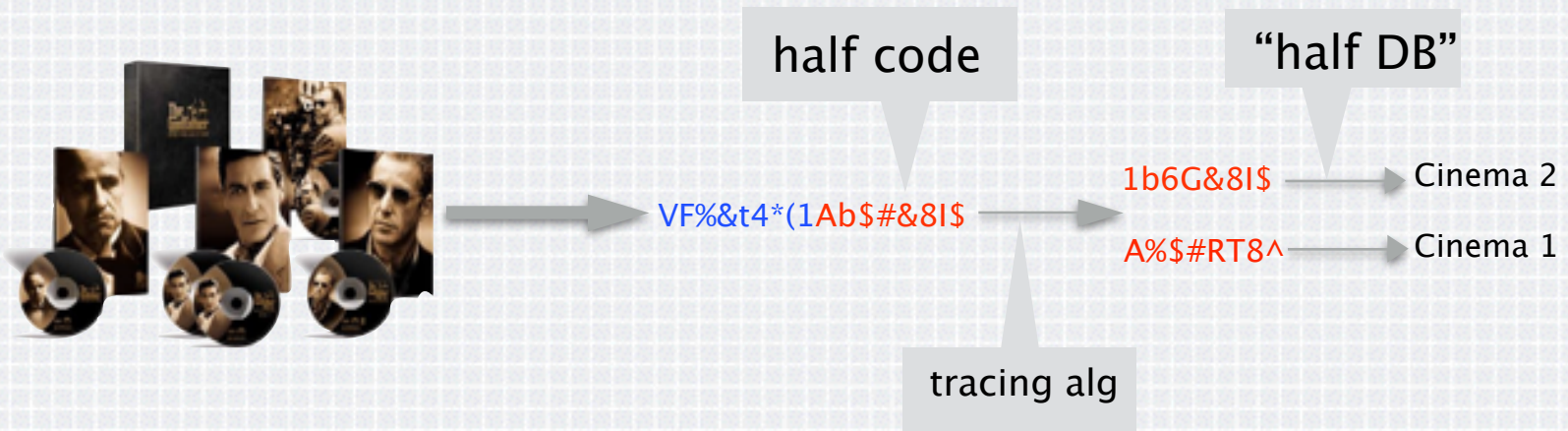
Asymmetric Fingerprinting



Asymmetric Fingerprinting



Asymmetric Fingerprinting



Asymmetric Fingerprinting

VF%&t4*(11b6G&8I\$ → Cinema 2

G^7#TC4A%\$#RT8^ → Cinema 1



Asymmetric Fingerprinting

VF%&t4*(11b6G&8I\$ → Cinema 2

G^7#TC4A%\$#RT8^ → Cinema 1



Cinema 1

t456&*!EA%\$#RT8^



Cinema 2

VF%&t4*(1b6G&8I\$



Asymmetric Fingerprinting

VF%&t4*(11b6G&8I\$ → Cinema 2

G^7#TC4A%\$#RT8^ → Cinema 1



Cinema 1

t456&*!EA%\$#RT8^

t456&*!E

VF%&t4*(



Cinema 2

VF%&t4*(1b6G&8I\$



Asymmetric Fingerprinting

VF%&t4*(11b6G&8I\$ → Cinema 2
 G^7#TC4A%\$#RT8^ → Cinema 1



Cinema 1

t456&*!EA%\$#RT8^

t456&*!E

VF%&t4*(



Cinema 2

VF%&t4*(1b6G&8I\$



Cinema 1 ✗

Cinema 2 ✓



Security Considerations

- ◆ The content provider can not frame a theater

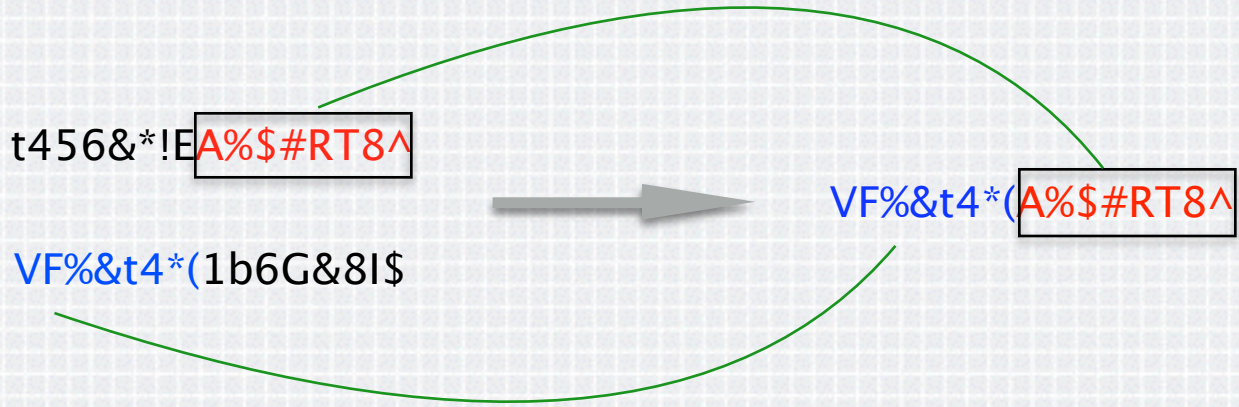


Security Considerations

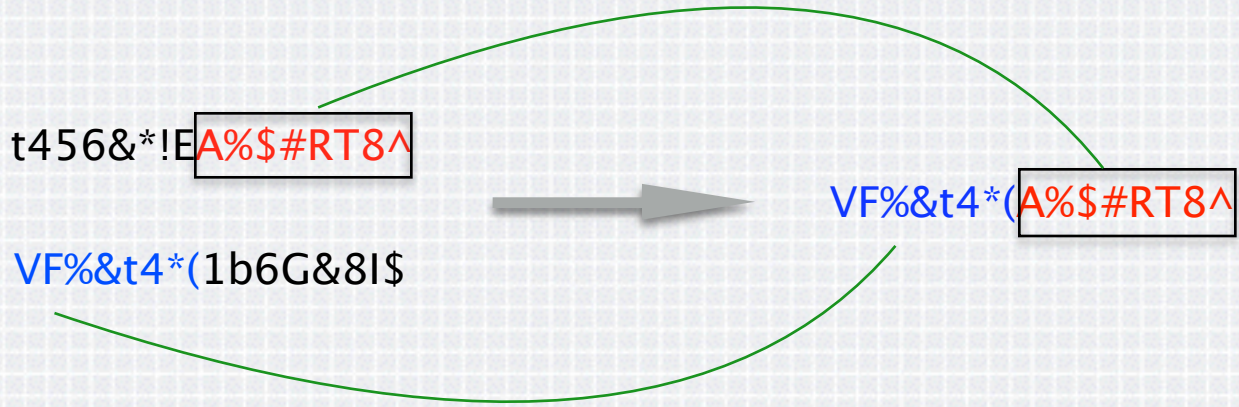
- ◆ The content provider can not frame a theater
- ◆ All suspects should be accused by the judge



A Subtle Security Consideration



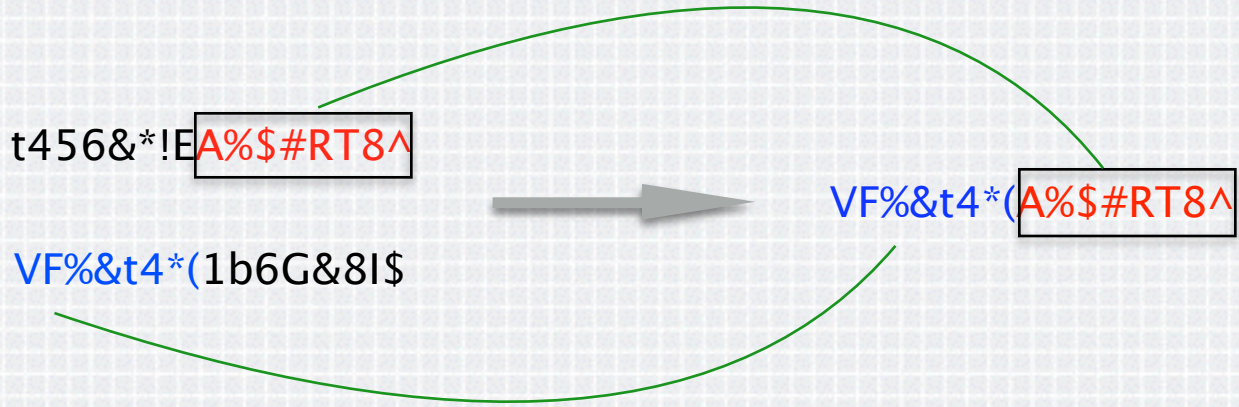
A Subtle Security Consideration



Cinema 1 will be the suspect, but the judge will not accuse him



A Subtle Security Consideration



Accusation Withdraw



A Subtle Security Consideration

1. Cinema should not know how the two halves are mixed



A Subtle Security Consideration

1. Cinema should not know how the two halves are mixed
2. Lower down the tracing parameter at the judge side



Important Efficiency Consideration

Building secure protocols brings some overhead



Important Efficiency Consideration

Even transmitting **2* movie size** kills the bandwidth



Important Efficiency Consideration

Even transmitting **2* movie size** kills the bandwidth

And will hinder the adoption of this technique



Important Efficiency Consideration

$$\text{Rate} = \frac{\text{Size of } \img alt="A cluster of movie covers and discs, including Star Wars characters." data-bbox="490 370 585 480"/>}{\text{Size of actual transmission}}$$

Important Efficiency Consideration

$$\text{Rate} = \frac{\text{Size of } \begin{array}{c} \text{CDs} \\ \text{DVDs} \end{array}}{\text{Size of actual transmission}} \longrightarrow 1$$



Important Efficiency Consideration

Fight Piracy without Extra Bandwidth Cost !



High-level Construction Idea



High-level Construction Idea

Careful protocol design to meet both **security** and **rate** efficiency



High-level Construction Idea

- ◆ Setup phase
- ◆ Fingerprint phase
- ◆ Identify phase
- ◆ Dispute phase



Fingerprint Phase



Cinema 1

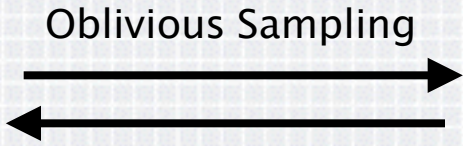
A Movie Producer



Fingerprint Phase



Cinema 1



A Movie Producer

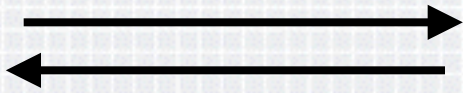


Fingerprint Phase



Cinema 1

Oblivious Sampling



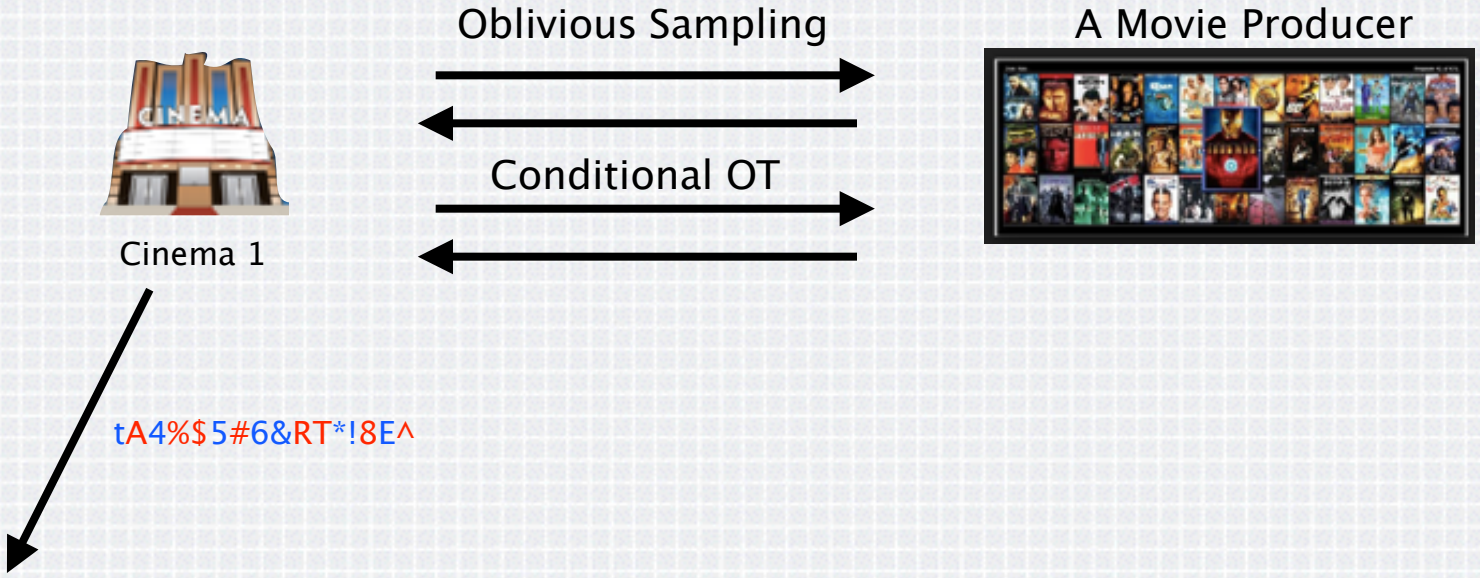
A Movie Producer



tA4%\$5#6&RT*!8E^



Fingerprint Phase



Cinema 1

Oblivious Sampling

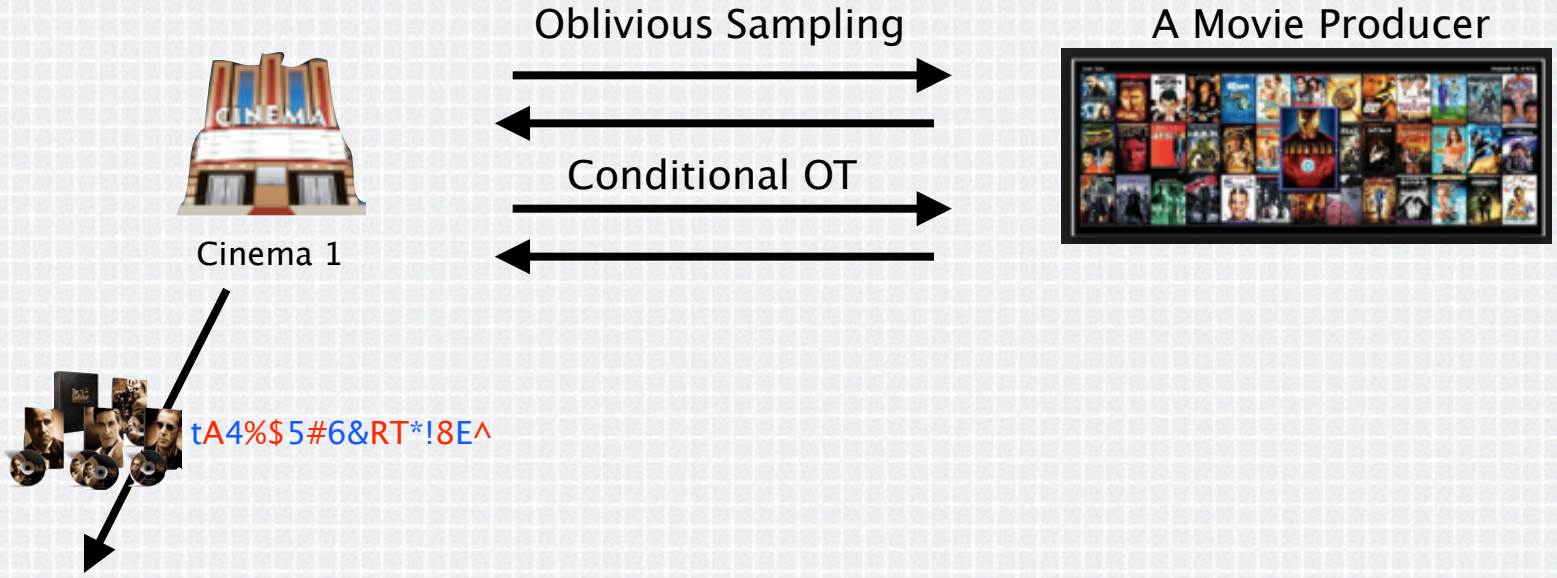
A Movie Producer

Conditional OT

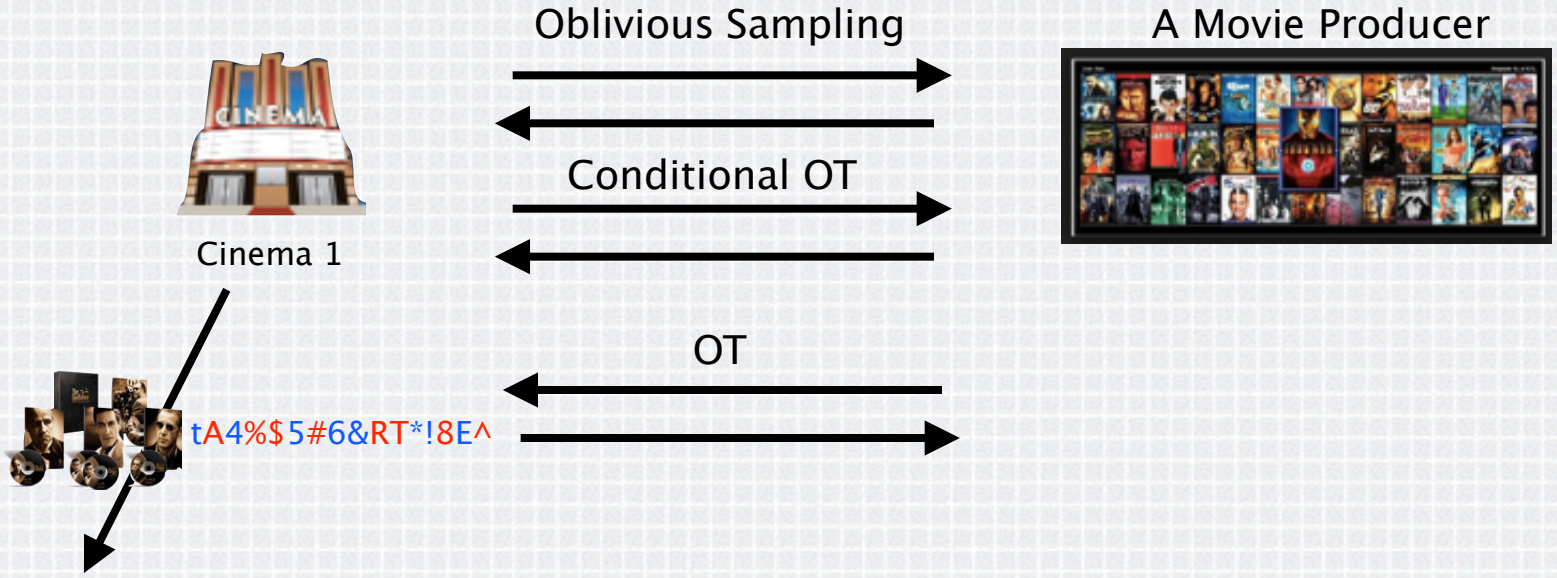
tA4%\$5#6&RT*!8E^



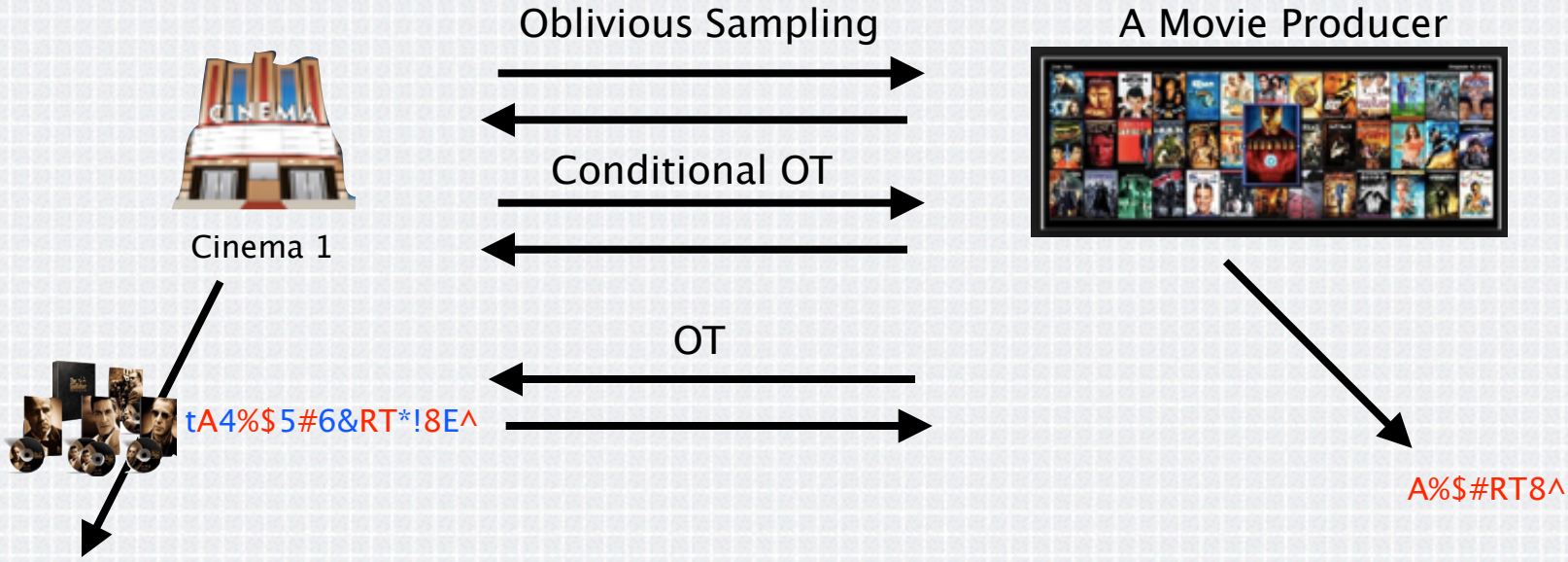
Fingerprint Phase



Fingerprint Phase



Fingerprint Phase



Fingerprint Phase

- ◆ Content provider only knows half of the codeword



Fingerprint Phase

- ◆ Content provider only knows half of the codeword
- ◆ Theaters don't know which part is known to the CP



Fingerprint Phase

- ◆ Content provider only knows half of the codeword
- ◆ Theaters don't know which part is known to the CP
- ◆ Rate optimal OT and COT are needed



Identify Phase

- ◆ Run the tracing algorithm of the underlying fingerprinting code on the half known to the content provider



Dispute Phase

- ◆ The accused theaters submit the other halves of the codewords (with proofs of validity)



Dispute Phase

- ◆ The accused theaters submit the other halves of the codewords (with proofs of validity)
- ◆ The judge also runs the tracing algorithm with a **less** restrict parameter on these halves



Dispute Phase

- ◆ The accused theaters submit the other halves of the codewords (with proofs of validity)
- ◆ The judge also runs the tracing algorithm with a **less** restrict parameter on these halves

Weaker judge side parameter is to avoid accusation withdraw



Communication Optimal Tardos-Based Asymmetric Fingerprinting



Linearly Homomorphic Encryption from DDH

Guilhem CASTAGNOS¹ Fabien LAGUILLAUMIE²

¹ Université de Bordeaux
INRIA Bordeaux - Sud-Ouest - LFANT
Institut de Mathématiques de Bordeaux UMR 5251,

² Université Claude Bernard Lyon 1
CNRS/ENSL/INRIA/UCBL LIP
Laboratoire de l'Informatique du Parallélisme

CT-RSA 2015



Outline

Linearly Homomorphic Encryption

Class Groups of Imaginary Quadratic Fields

New proposal

Outline

Linearly Homomorphic Encryption

Class Groups of Imaginary Quadratic Fields

New proposal

Linearly Homomorphic Encryption ?

- Public key encryption scheme with the following properties:
- Suppose that the set of plaintexts \mathcal{M} is a ring
- $c \leftarrow \text{Encrypt}(pk, m)$, $c' \leftarrow \text{Encrypt}(pk, m')$
- $c_1 \leftarrow \text{EvalSum}(pk, c, c')$ s.t.

$$\text{Decrypt}(sk, c_1) = m + m'$$

- For $\alpha \in \mathcal{M}$, $c_2 \leftarrow \text{EvalScal}(pk, c, \alpha)$ s.t.

$$\text{Decrypt}(sk, c_2) = \alpha m$$

- Applications: Electronic Voting, Private Information Retrieval, Mix-Net, Oblivious Transfer, Fingerprinting...

Examples from Factoring

- Goldwasser Micali (84)
 - Plaintext space $\mathcal{M} = \mathbb{Z}/2\mathbb{Z}$
 - Ciphertext space : $\mathbb{Z}/N\mathbb{Z}$ where $N = pq$ is an RSA integer
- Paillier (99)
 - Plaintext space $\mathcal{M} = \mathbb{Z}/N\mathbb{Z}$
 - Ciphertext space : $\mathbb{Z}/N^2\mathbb{Z}$ where $N = pq$ is an RSA integer
 - Plaintext encoding :

$$m \in \mathbb{Z}/N\mathbb{Z} \mapsto (1 + N)^m \equiv 1 + mN \pmod{N^2}$$

From DDH: ElGamal “in the exponent”

- Folklore message encoding: $m \in \mathbf{N} \mapsto g^m$
- $(c_1, c_2) = (g^r, h^r g^m) \leftarrow \text{Encrypt}(pk, m)$
- $\text{Decrypt}(pk, c) : c_2/c_1^x = g^m \rightsquigarrow m$
- m must be small. Can only do a bounded number of homomorphic operations:
 - $(c_1, c_2) = (g^r, h^r g^m) \leftarrow \text{Encrypt}(pk, m),$
 - $(c'_1, c'_2) = (g^{r'}, h^{r'} g^{m'}) \leftarrow \text{Encrypt}(pk, m'),$

$$(c_1 c'_1, c_2 c'_2) = (g^{r+r'}, h^{r+r'} g^{m+m'})$$

$$(c_1^\alpha, c_2^\alpha) = (g^{r\alpha}, h^{r\alpha} g^{m\alpha})$$

DDH group with an easy DL subgroup

- $(G, \times) = \langle g \rangle$ a cyclic group of order n
- $n = ps$, $\gcd(p, s) = 1$
- $\langle f \rangle = F \subset G$ subgroup of G of order p
- The DL problem is easy in F : There exists, Solve, a deterministic polynomial time algorithm s.t.

$$\text{Solve}(p, f, f^x) \rightsquigarrow x$$

- The DDH problem is hard in G even with access to the Solve algorithm

A Generic Linearly Homomorphic Encryption Scheme

- $\mathcal{M} = \mathbf{Z}/p\mathbf{Z}$
- $pk : h = g^x, sk : x$, where g has order $n = ps$ for an unknown s
- Encrypt : $c = (c_1, c_2) = (g^r, f^m h^r)$, where $f \in \langle g \rangle$ has order p
- Decrypt : $A \leftarrow c_2/c_1^x$, Solve(p, f, A) $\rightsquigarrow m$
- EvalSum :

$$(c_1 c'_1, c_2 c'_2) = (g^{r+r'}, h^{r+r'} f^{m+m'})$$

- EvalScal :

$$(c_1^\alpha, c_2^\alpha) = (g^{r\alpha}, h^{r\alpha} f^{m\alpha})$$

An Unsecure Instantiation

- p a prime and $G = \langle g \rangle = (\mathbf{Z}/p^2\mathbf{Z})^\times$ of order $n = p(p-1)$
- $f = 1 + p \in G$, $F = \langle f \rangle = \{1 + kp, k \in \mathbf{Z}/p\mathbf{Z}\}$
- $f^m = 1 + mp$.
- There exist a unique $(\alpha, r) \in (\mathbf{Z}/p\mathbf{Z}, (\mathbf{Z}/p\mathbf{Z})^\times)$ such that $g = f^\alpha r^p$

$$g^{p-1} = f^{\alpha(p-1)} = f^{-\alpha}$$

- Public key : $h = g^x$,

$$h^{p-1} = f^{-\alpha x} \rightsquigarrow x \pmod{p}$$

- $(c_1, c_2) = (g^r, h^r f^m)$

$$c_1^{p-1} = f^{-\alpha r} \rightsquigarrow r \pmod{p}$$

$$c_2^{p-1} = f^{-\alpha x r - m} \rightsquigarrow m \pmod{p}$$

Partial Discrete Logarithm Problem

- $(G, \times) = \langle g \rangle$ a cyclic group of order n
- $n = ps$, $\gcd(p, s) = 1$
- $\langle f \rangle = F \subset G$ subgroup of G of order p
- Partial Discrete Logarithm (PDL) Problem:

Given $X = g^x$ compute $x \pmod p$.

- The knowledge of s makes the PDL problem easy.

s must be hidden or unknown !

A Secure Instantiation

- Bresson, Catalano, Pointcheval (03)
- Let N be an RSA integer, $G = \langle g \rangle \subset (\mathbf{Z}/N^2\mathbf{Z})^\times$
- $n = \text{Card}(G) = Ns$ with $s \mid \varphi(N)$,
- $f = 1 + N \in G$, $F = \langle f \rangle = \{1 + kN, k \in \mathbf{Z}/N\mathbf{Z}\}$, of order N
- Public key : $h = g^x$, x secret key
- $(c_1, c_2) = (g^r, h^r f^m)$
- Based on DDH in $(\mathbf{Z}/N^2\mathbf{Z})^\times$ and the Factorisation problem.
- The factorisation of N acts as a second trapdoor.

Outline

Linearly Homomorphic Encryption

Class Groups of Imaginary Quadratic Fields

New proposal

Definitions

Imaginary Quadratic Fields

- $K = \mathbf{Q}(\sqrt{\Delta_K}), \Delta_K < 0$
- Fundamental Discriminant:
 - $\Delta_K \equiv 1 \pmod{4}$ square-free
 - $\Delta_K \equiv 0 \pmod{4}$ and $\Delta_K/4 \equiv 2, 3 \pmod{4}$ square-free
- Non Fundamental Discriminant:
 - $\Delta_\ell = \ell^2 \Delta_K$
 - ℓ is the conductor

Class Group of Discriminant Δ

- Finite Group denoted $C(\Delta)$
- Elements: Equivalence classes of Ideals
- Class Number: $h(\Delta) \approx \sqrt{|\Delta|}$

ElGamal in Class Group

- Buchmann and Williams (88): Diffie-Hellman key exchange and ElGamal
- Düllmann, Hamdy, Möller, Pohst, Schielzeth, Vollmer (90-07): Implementation
- Size of Δ_K ? Index calculus algorithm to compute $h(\Delta_K)$ and Discrete Logarithm in $C(\Delta_K)$
- Security Estimates from Biasse, Jacobson and Silvester (10):
 - Complexity conjectured $L_{|\Delta_K|}(1/2, o(1))$
 - Δ_k : 1348 bits as hard as factoring a 2048 bits RSA integer
 - Δ_k : 1828 bits as hard as factoring a 3072 bits RSA integer

Map between two Class Groups

- Let Δ_K be a fundamental negative discriminant, $\Delta_K \neq -3, -4$, ℓ a conductor, and $\Delta_\ell = \ell^2 \Delta_K$
- There exists a surjective morphism, denoted $\bar{\varphi}_\ell$, between $C(\Delta_\ell)$ and $C(\Delta_K)$
- $\bar{\varphi}_\ell$ is effective, can be computed if ℓ is known
- Used by the NICE cryptosystem by Paulus and Takagi (00), $\Delta_K = -q$, $\Delta_p = -qp^2$, p, q primes, p is the trapdoor
- C., Laguillaumie (09) :

In each non trivial class of $\ker \bar{\varphi}_p$, there exists an ideal of the

$$\text{form } \left[p^2 \mathbf{Z} + \frac{bp + \sqrt{\Delta_p}}{2} \mathbf{Z} \right]$$

Outline

Linearly Homomorphic Encryption

Class Groups of Imaginary Quadratic Fields

New proposal

A Subgroup with an Easy DL Problem

- $\Delta_K = -pq$, $\Delta_p = -qp^3$, p, q primes and $pq \equiv 3 \pmod{4}$

$$h(\Delta_p) = p \times h(\Delta_K)$$

- Let $f = \left[p^2 \mathbf{Z} + \frac{p + \sqrt{\Delta_p}}{2} \mathbf{Z} \right] \in \mathcal{C}(\Delta_p)$

- $F = \ker \bar{\varphi}_p = \langle f \rangle$ is of order p , and

$$f^m = \left[p^2 \mathbf{Z} + \frac{[m^{-1} \pmod{p}]p + \sqrt{\Delta_p}}{2} \mathbf{Z} \right]$$

A New Linearly Homomorphic Encryption Scheme

- $\Delta_K = -pq$, $\Delta_p = -qp^3$, p, q primes and $pq \equiv 3 \pmod{4}$ and $(p/q) = -1$, $q > 4p$
- Let g be an element of $C(\Delta_p)$, $h = g^x$ where x secret key
- g has order ps for an unknown $s|h(\Delta_K)$
- $(c_1, c_2) = (g^r, h^r f^m)$ where f has order p
- Based on DDH in $C(\Delta_p)$ (and the Class number problem).
- Linearly homomorphic over $\mathbf{Z}/p\mathbf{Z}$ where p can be chosen (almost) independently from the security parameter

Some Variants

- **Faster Variant:** most of the work in $C(\Delta_K)$ (based on a non standard problem)
- **More general message spaces:**
 - $\mathbf{Z}/N\mathbf{Z}$ with $N = \prod_{i=1}^n p_i$, with a discriminant of the form $\Delta_K = -Nq$
 - $\mathbf{Z}/p^t\mathbf{Z}$ for $t > 1$, with discriminants of the form $\Delta_{p^t} = p^{2t}\Delta_K$, and $\Delta_K = -pq$

Performance comparison

Cryptosystem	Parameter	Message Space	Encryption (ms)	Decryption (ms)
Paillier	2048 bits modulus	2048 bits	28	28
BCP03	2048 bits modulus	2048 bits	107	54
New Proposal	1348 bits Δ_K	80 bits	93	49
Fast Variant	1348 bits Δ_K	80 bits	82	45
Fast Variant	1348 bits Δ_K	256 bits	105	68
Paillier	3072 bits modulus	3072 bits	109	109
BCP03	3072 bits modulus	3072 bits	427	214
New Proposal	1828 bits Δ_K	80 bits	179	91
Fast Variant	1828 bits Δ_K	80 bits	145	78
Fast Variant	1828 bits Δ_K	512 bits	226	159
Fast Variant	1828 bits Δ_K	912 bits	340	271

Timings performed with Sage and PARI/GP.

Linearly Homomorphic Encryption from DDH

Guilhem CASTAGNOS¹ Fabien LAGUILLAUMIE²

¹ Université de Bordeaux
INRIA Bordeaux - Sud-Ouest - LFANT
Institut de Mathématiques de Bordeaux UMR 5251,

² Université Claude Bernard Lyon 1
CNRS/ENSL/INRIA/UCBL LIP
Laboratoire de l'Informatique du Parallélisme

CT-RSA 2015

