# Some Advances in

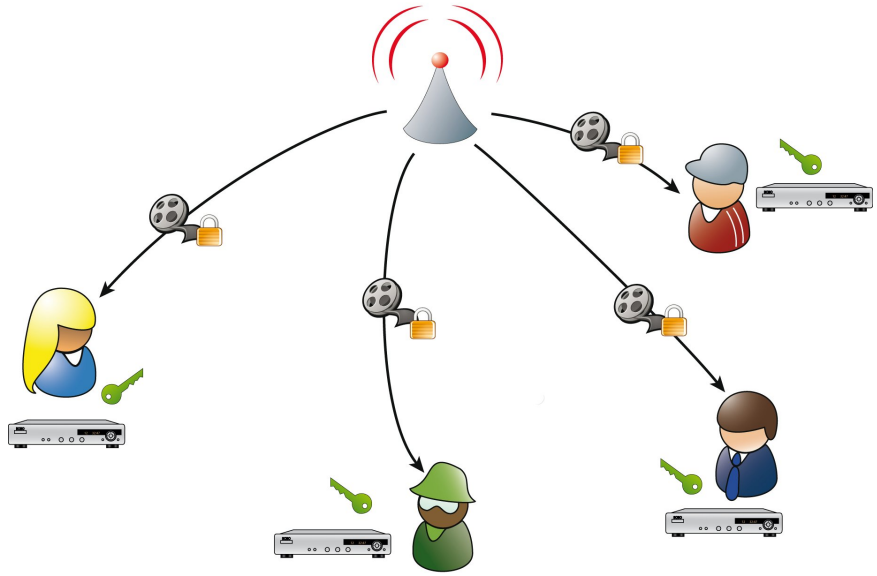
# Broadcast Encryption and Traitor Tracing

Duong Hieu Phan

(*Séminaire LIPN - 18 Novembre 2014 )*


# Multi-receiver Encryption

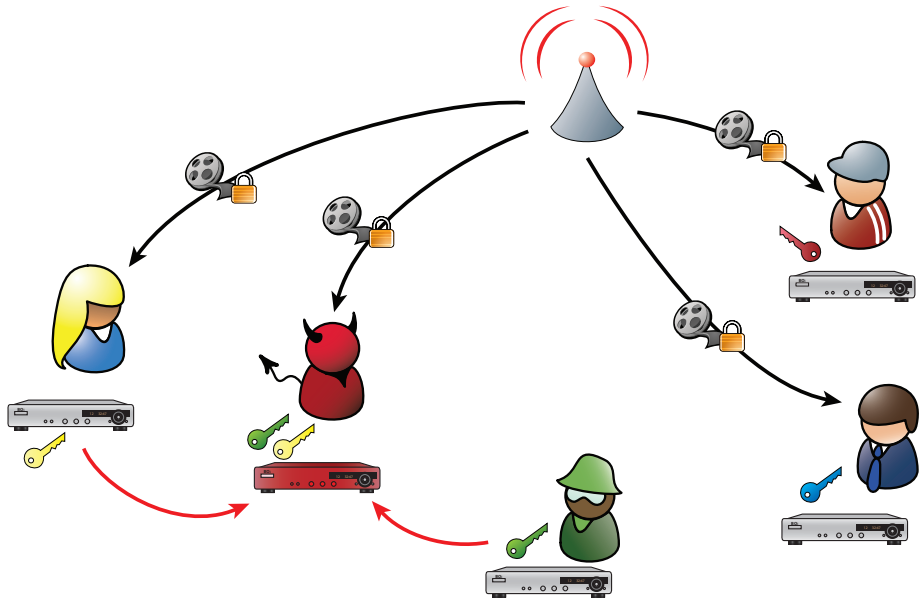
## From “One-to-one” to ‘one-to-many” communications



Provide all users with the same key $\rightarrow$ problems:

1. Impossibility to know the source of the key leakage (traitor)
2. Impossibility to revoke a user, except by resetting the parameters

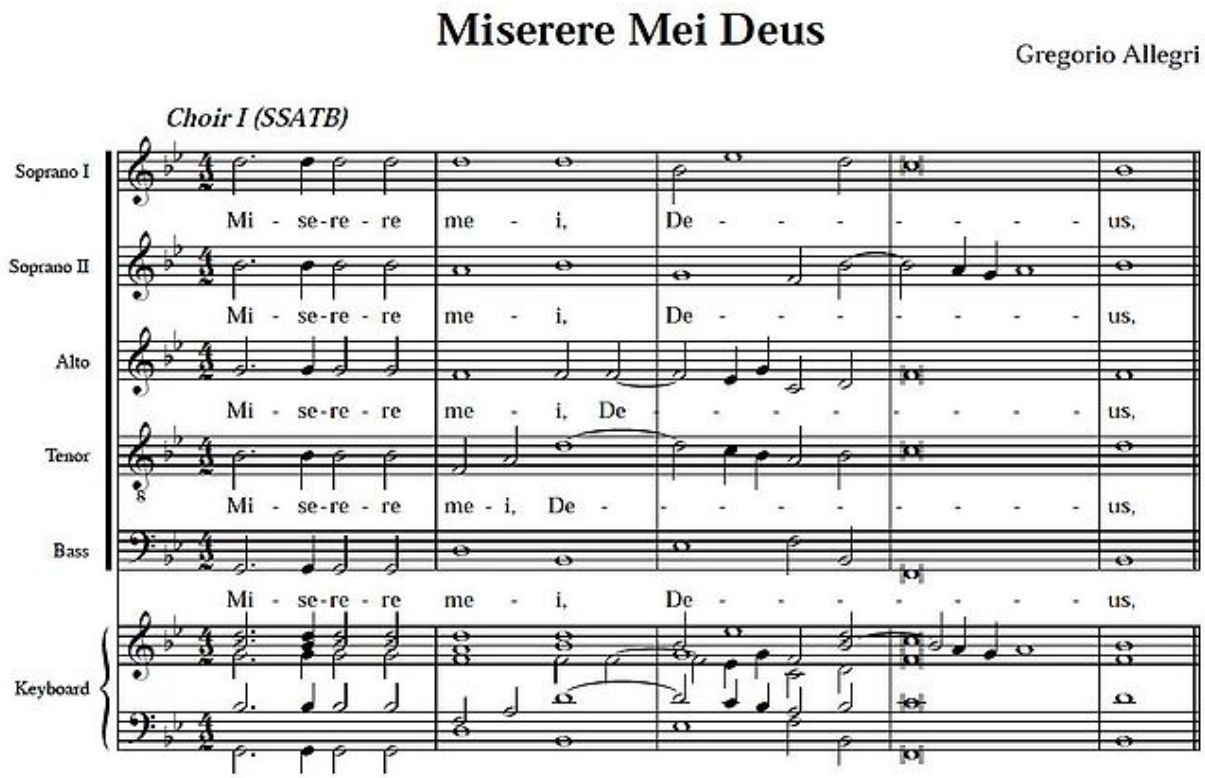
# Broadcast Encryption [B91,FN94] & Traitor Tracing [CFN94]



## Desired Properties

1. Tracing traitors from a pirate decoder
   - White-box tracing
   - Black-box confirmation, black-box tracing
2. Revoking non-legitimate users

# Broadcasting & Tracing




- Composed by G.Allegri (around 1630) for use in the Sistine Chapel on Wednesday and Friday
- Kept secret by the Vatican

# Broadcasting & Tracing

- The piece was revealed in 1771 $\rightarrow$ Mozart

# Broadcasting & Tracing

- The piece was revealed in 1771 $\rightarrow$ Mozart
- Only Mozart can do it!
- Same idea in traitor tracing: identify who is capable of producing the pirate decoder

# Outline

# Outline

# Exclusive Set System (ESS)

[ALO98]

$\mathcal{F}$ is an $(N, \ell, r, s)$-ESS if:

- $\mathcal{F}$: a family of $\ell$ subsets of $[N]$
- For any $R \subseteq [N]$ of size at most $r$, there exists $S_1, \ldots S_s \in \mathcal{F}$ s.t.

$$[N] - R = \bigcup_{i=1}^{s} S_i$$

# Exclusive Set System (ESS)

[ALO98]

$\mathcal{F}$ is an $(N, \ell, r, s)$-ESS if:

- $\mathcal{F}$: a family of $\ell$ subsets of $[N]$
- For any $R \subseteq [N]$ of size at most $r$, there exists $S_1, \ldots S_s \in \mathcal{F}$ s.t.

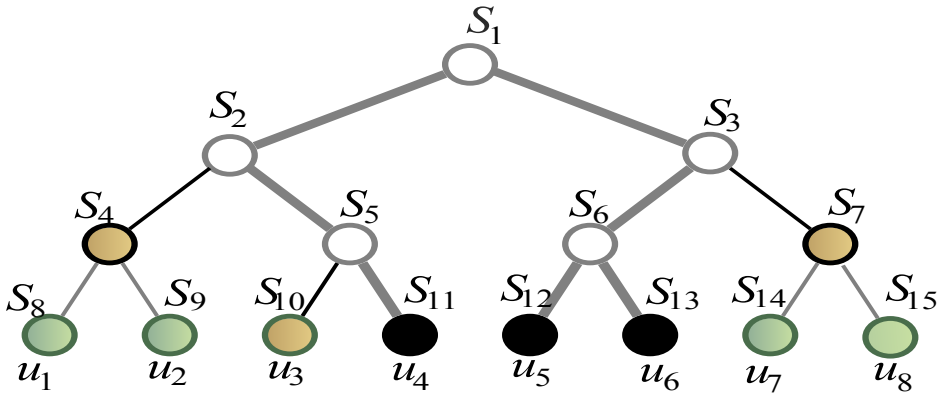
$$[N] - R = \bigcup_{i=1}^{s} S_i$$

## From ESS to Revoke System

- Each $S_i \in \mathcal{F}$ is associated to a key $K_i$
- User $u$ receives all keys $K_i$ that $u \in S_i$
- To revoke a set $R \subseteq [N]$ of size at most $r$:
  - Find $S_1, \ldots S_s \in \mathcal{F}$ s.t. $[N] - R = \bigcup_{i=1}^{s} S_i$
  - Encrypt the message with each key $K_i$

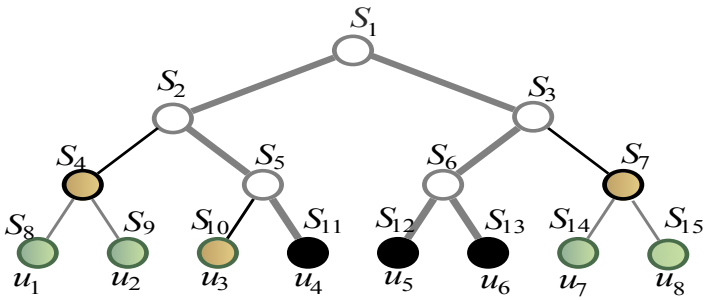
# NNL Schemes viewed as Exclusive Set Systems

[NNL01]



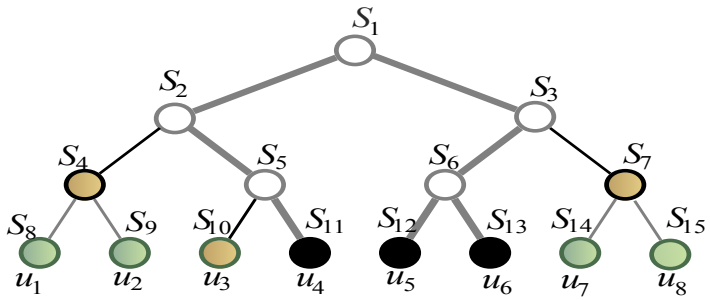

- $\mathcal{F} = \{S_1, S_2, \ldots, S_{15}\}$
- $S_i$ contains all users (*i.e.* leaves) in the subtree of node $i$ (e.g. $S_2 = \{u_1, u_2, u_3, u_4\}$)
- Revoked set $R = \{u_4, u_5, u_6\}$
- Encrypt with keys at $S_4, S_7, S_{10}$
- **Complete-subtree is a** $(N, 2N-1, r, r\log(N/r))$**-ESS**

# Exclusive Set System under Code's View




| | $u_1$ | $u_2$ | $u_3$ | $u_4$ | $u_5$ | $u_6$ | $u_7$ | $u_8$ |
|---|---|---|---|---|---|---|---|---|
| $S_1$ | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| $S_2$ | 1 | 1 | 1 | 1 | | | | |
| $S_3$ | | | | | 1 | 1 | 1 | 1 |
| $S_4$ | 1 | 1 | | | | | | |
| $S_5$ | | | 1 | 1 | | | | |
| $S_6$ | | | | | 1 | 1 | | |
| $S_7$ | | | | | | | 1 | 1 |
| $S_8$ | 1 | | | | | | 1 | |
| $S_9$ | | 1 | | | | | | |
| $S_{10}$ | | | 1 | | | | | |
| $S_{11}$ | | | | 1 | | | | |
| $S_{12}$ | | | | | 1 | | | |
| $S_{13}$ | | | | | | 1 | | |
| $S_{14}$ | | | | | | | 1 | |
| $S_{15}$ | | | | | | | | 1 |

# NNL Schemes

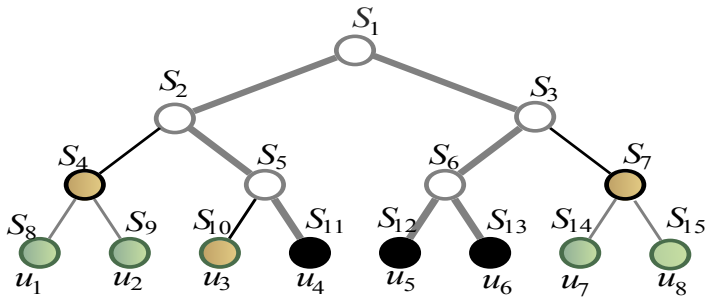



| | $u_1$ | $u_2$ | $u_3$ | $u_4$ | $u_5$ | $u_6$ | $u_7$ | $u_8$ |
|---|---|---|---|---|---|---|---|---|
| $S_1$ | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| $S_2$ | 1 | 1 | 1 | 1 | | | | |
| $S_3$ | | | | | 1 | 1 | 1 | 1 |
| $S_4$ | 1 | 1 | | | | | | |
| $S_5$ | | | 1 | 1 | | | | |
| $S_6$ | | | | | 1 | 1 | | |
| $S_7$ | | | | | | | 1 | 1 |
| $S_8$ | 1 | | | | | | 1 | |
| $S_9$ | | 1 | | | | | | |
| $S_{10}$ | | | 1 | | | | | |
| $S_{11}$ | | | | 1 | | | | |
| $S_{12}$ | | | | | 1 | | | |
| $S_{13}$ | | | | | | 1 | | |
| $S_{14}$ | | | | | | | 1 | |
| $S_{15}$ | | | | | | | | 1 |

## Tracing Levels for NNL schemes

- Relaxed level of black-box tracing
- Black-box tracing for “naive” decoders

# NNL Schemes

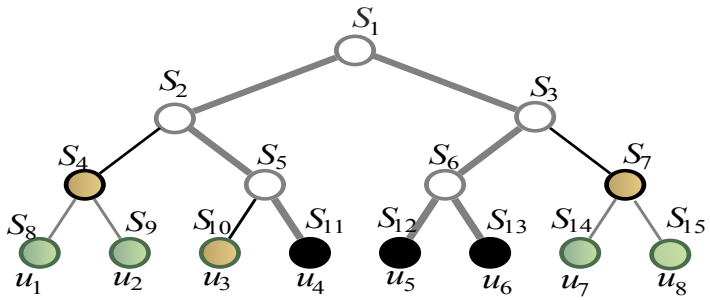



| | $u_1$ | $u_2$ | $u_3$ | $u_4$ | $u_5$ | $u_6$ | $u_7$ | $u_8$ |
|---|---|---|---|---|---|---|---|---|
| $S_1$ | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| $S_2$ | 1 | 1 | 1 | 1 | | | | |
| $S_3$ | | | | | 1 | 1 | 1 | 1 |
| $S_4$ | 1 | 1 | | | | | | |
| $S_5$ | | | 1 | 1 | | | | |
| $S_6$ | | | | | 1 | 1 | | |
| $S_7$ | | | | | | | 1 | 1 |
| $S_8$ | 1 | | | | | | 1 | |
| $S_9$ | | 1 | | | | | | |
| $S_{10}$ | | | 1 | | | | | |
| $S_{11}$ | | | | 1 | | | | |
| $S_{12}$ | | | | | 1 | | | |
| $S_{13}$ | | | | | | 1 | | |
| $S_{14}$ | | | | | | | 1 | |
| $S_{15}$ | | | | | | | | 1 |

## Weakness in Black-box Tracing

- Highly structured matrix
- Pirate could thus detect “dangerous” queries and refuse to decrypt

# NNL Schemes

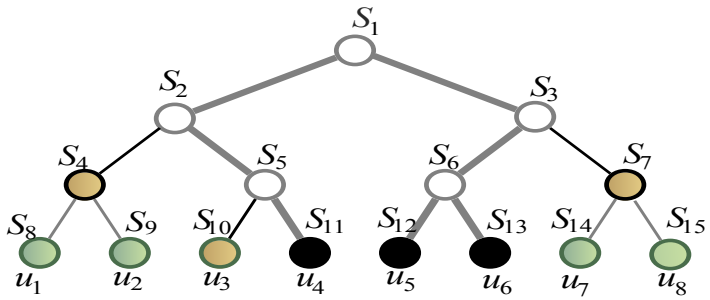



| | $u_1$ | $u_2$ | $u_3$ | $u_4$ | $u_5$ | $u_6$ | $u_7$ | $u_8$ |
|---|---|---|---|---|---|---|---|---|
| $S_1$ | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| $S_2$ | 1 | 1 | 1 | 1 | | | | |
| $S_3$ | | | | | 1 | 1 | 1 | 1 |
| $S_4$ | 1 | 1 | | | | | | |
| $S_5$ | | | 1 | 1 | | | | |
| $S_6$ | | | | | 1 | 1 | | |
| $S_7$ | | | | | | | 1 | 1 |
| $S_8$ | 1 | | | | | | 1 | |
| $S_9$ | | 1 | | | | | | |
| $S_{10}$ | | | 1 | | | | | |
| $S_{11}$ | | | | 1 | | | | |
| $S_{12}$ | | | | | 1 | | | |
| $S_{13}$ | | | | | | 1 | | |
| $S_{14}$ | | | | | | | 1 | |
| $S_{15}$ | | | | | | | | 1 |

## In General, Previous Results for ESS

- Black-box tracing for “naive” decoders (decrypt all ciphertexts without any strategy)
- *c*-traceability: a white-box tracing for “imperfect” decoders

# NNL Schemes

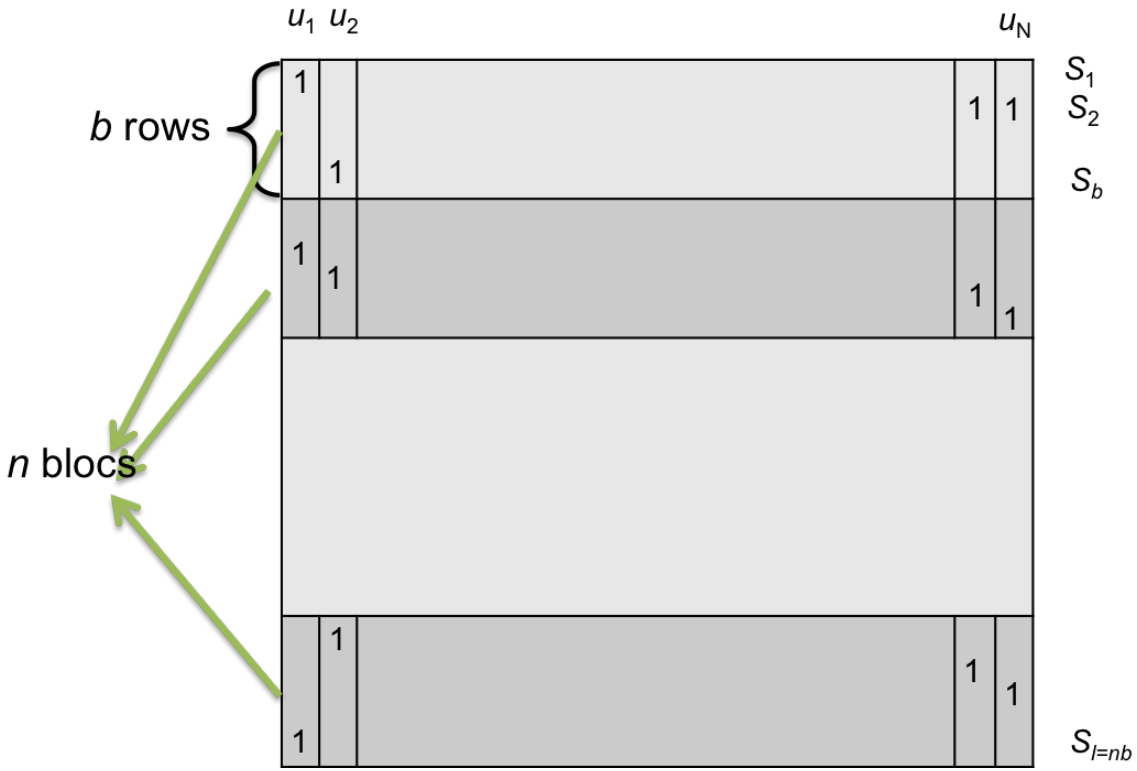



| | $u_1$ | $u_2$ | $u_3$ | $u_4$ | $u_5$ | $u_6$ | $u_7$ | $u_8$ |
|---|---|---|---|---|---|---|---|---|
| $S_1$ | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| $S_2$ | 1 | 1 | 1 | 1 | | | | |
| $S_3$ | | | | | 1 | 1 | 1 | 1 |
| $S_4$ | 1 | 1 | | | | | | |
| $S_5$ | | | 1 | 1 | | | | |
| $S_6$ | | | | | 1 | 1 | | |
| $S_7$ | | | | | | | 1 | 1 |
| $S_8$ | 1 | | | | | | 1 | |
| $S_9$ | | 1 | | | | | | |
| $S_{10}$ | | | 1 | | | | | |
| $S_{11}$ | | | | 1 | | | | |
| $S_{12}$ | | | | | 1 | | | |
| $S_{13}$ | | | | | | 1 | | |
| $S_{14}$ | | | | | | | 1 | |
| $S_{15}$ | | | | | | | | 1 |

## Our Objectives

Black-box tracing in ESS for “smart” decoders
(efficiency comparable to NNL schemes)

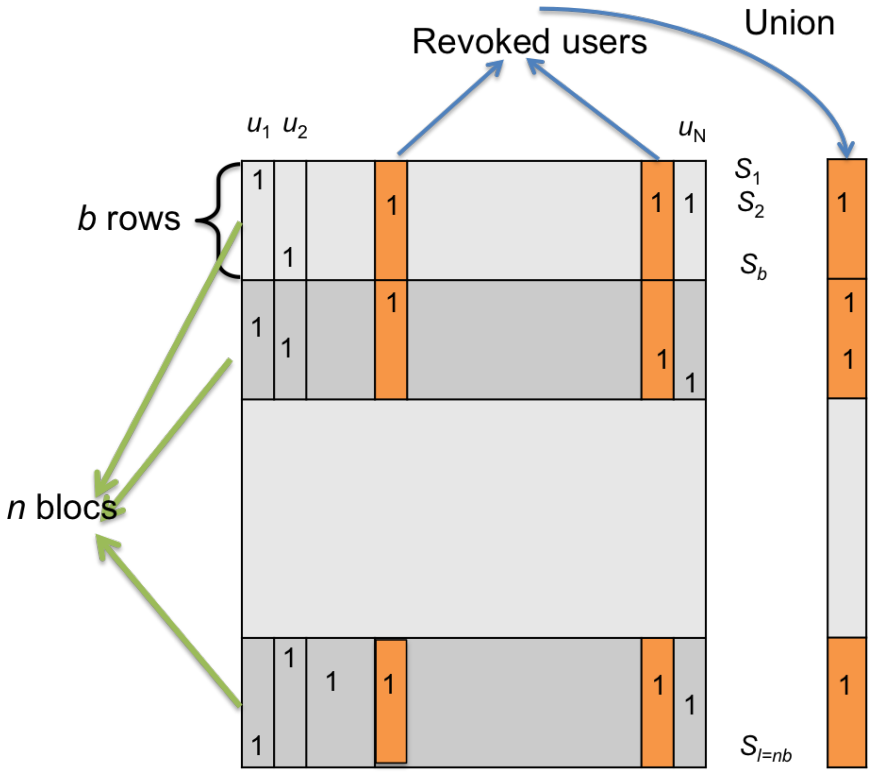
# Randomized ESS




## Recall

- 1 row $\rightarrow$ 1 subset $\rightarrow$ 1 key
- 1 column $\rightarrow$ 1 user $\rightarrow$ user $j$ has key $K_i$ iff $M_{ij} = 1$

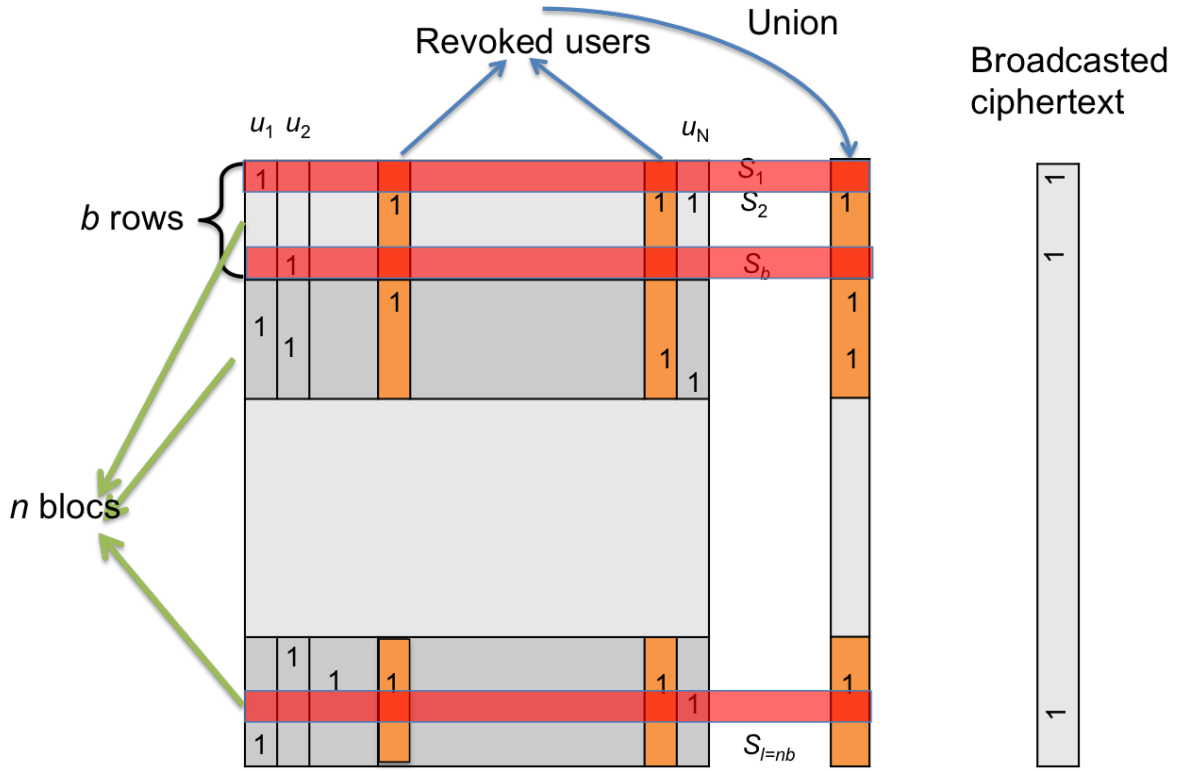
# Randomized ESS




## Recall

- 1 row $\rightarrow$ 1 subset $\rightarrow$ 1 key
- 1 column $\rightarrow$ 1 user $\rightarrow$ user $j$ has key $K_i$ iff $M_{ij} = 1$

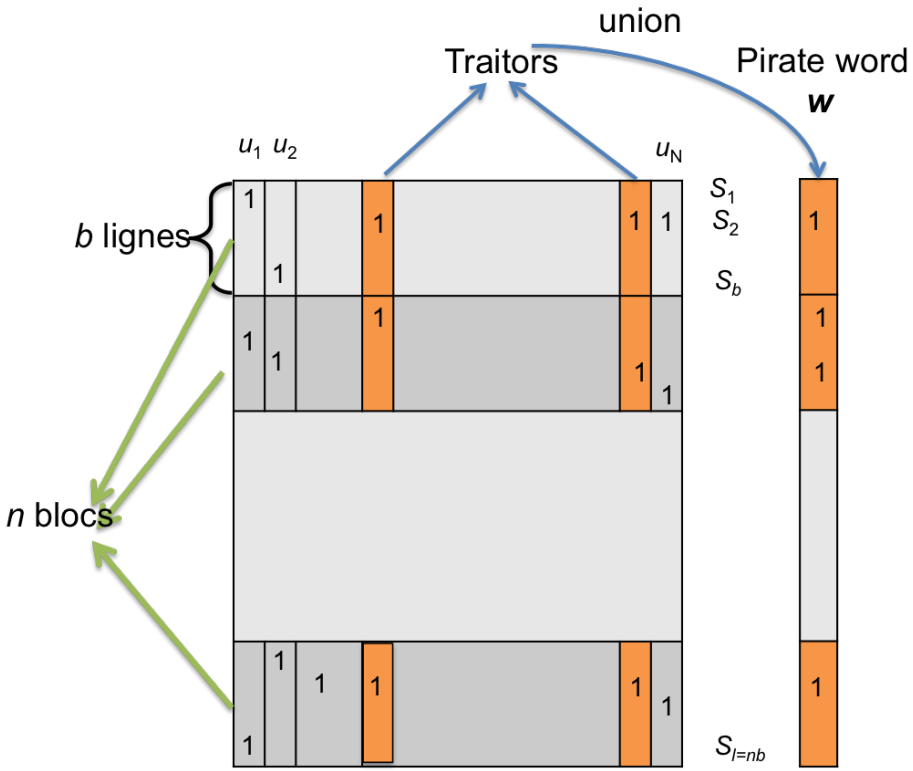
# Randomized ESS




## Property

- Set $n = r \log_2(N^2 e/r)$, $b = 4r$
- With overwhelming probability $\rightarrow (N, 8r^2 \log N, r, 8r \log N)$-ESS. (complete-subtree is $(N, 2N-1, r, r(\log(N/r))$-ESS)

# Tracing for ESS




## White-box

Tracer can open the box $\rightarrow$ get the pirate word $w$ which is the union of traitors' codewords

# White-box Tracing for ESS

## White-box Tracing

- $(r, s, N, l)$-ESS is also a $r$-disjunct matrix, *i.e.,* no column is contained in the union of any $r$ other columns
- $r$-disjunct matrix: from the union of at most $r$ columns, one can find back the $r$ columns (the *Group Testing technique*)

$\leftrightarrow$ Given the pirate word $w$, trace back the traitors

# White-box Tracing for ESS

## White-box Tracing

- $(r, s, N, l)$-ESS is also a $r$-disjunct matrix, *i.e.,* no column is contained in the union of any $r$ other columns
- $r$-disjunct matrix: from the union of at most $r$ columns, one can find back the $r$ columns (the *Group Testing technique*)

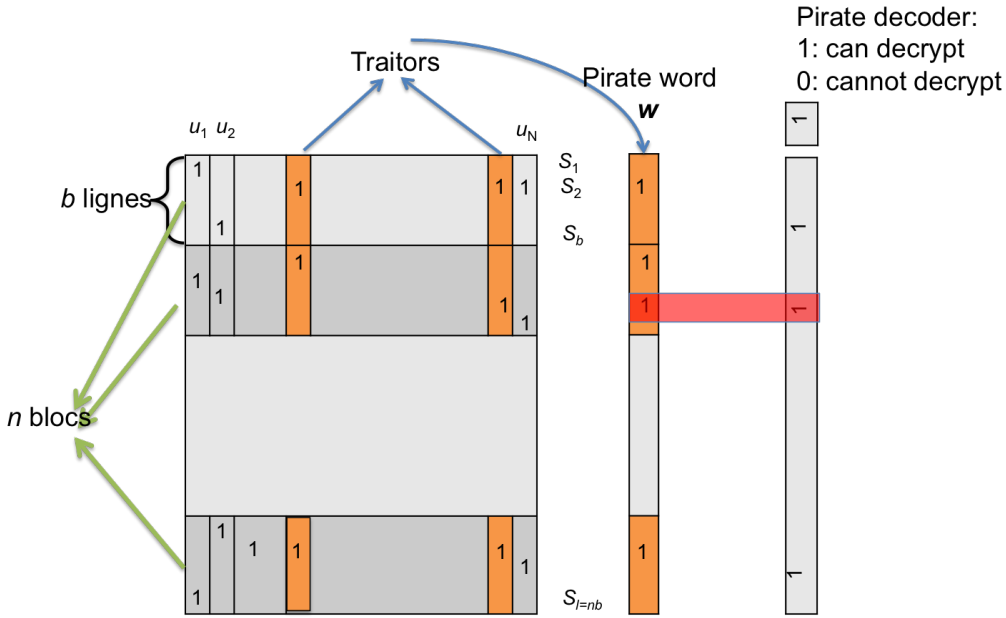
$\leftrightarrow$ Given the pirate word $w$, trace back the traitors

## Challenge for Black-box Tracing

How to find the pirate word $w$?

# Black-box Tracing for ESS

## Shadow Group Testing Technique[NPP, Algorithmica13]

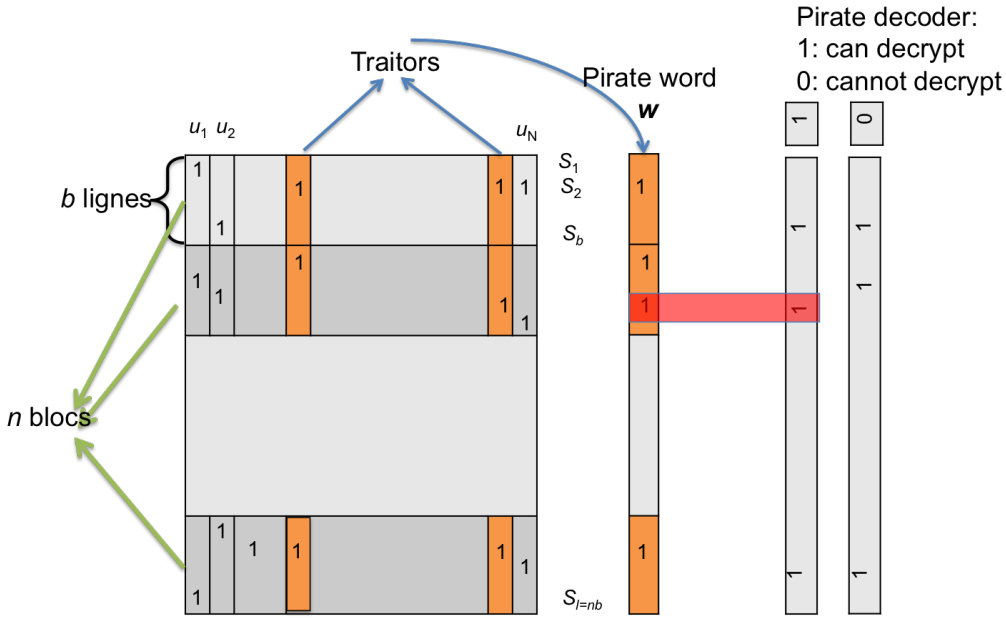



### Black-box access to pirate decoder

Asking random queries of the same form as broadcasted ciphertexts

# Black-box Tracing for ESS

## Shadow Group Testing Technique[NPP, Algorithmica13]

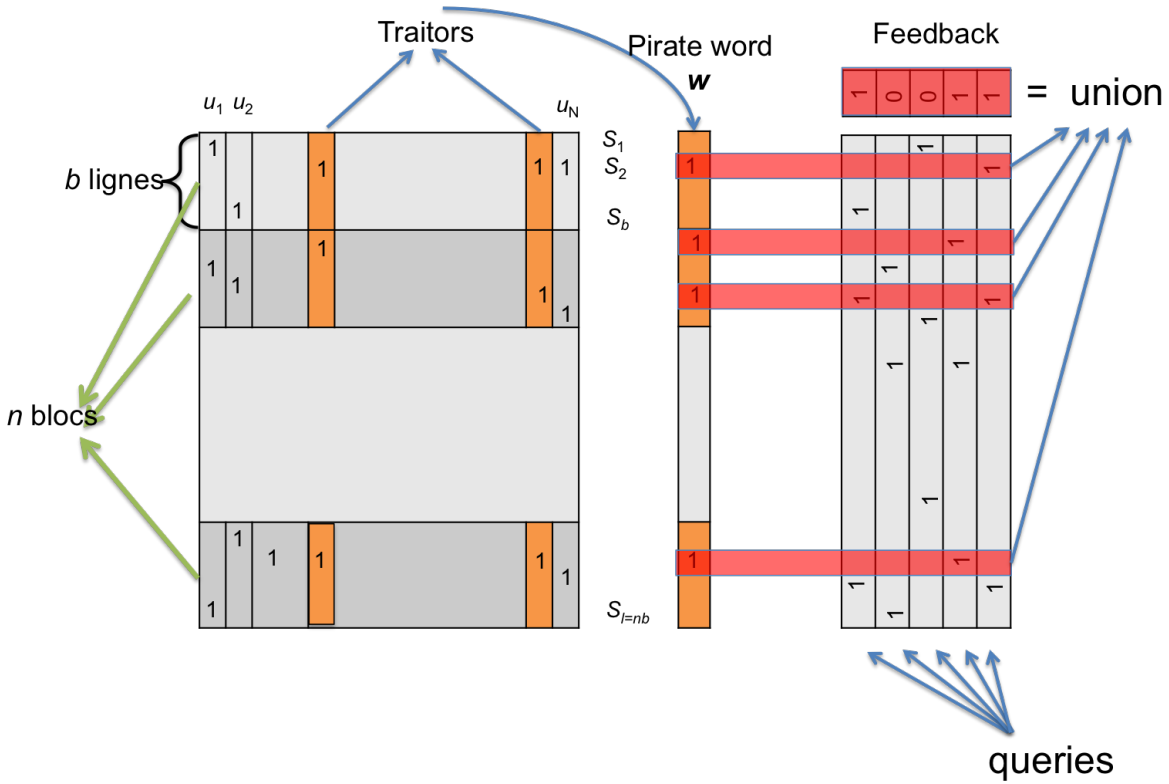



### Black-box Access to Pirate Decoder

Asking random queries of the same form as broadcasted ciphertexts

# Black-box Tracing for ESS

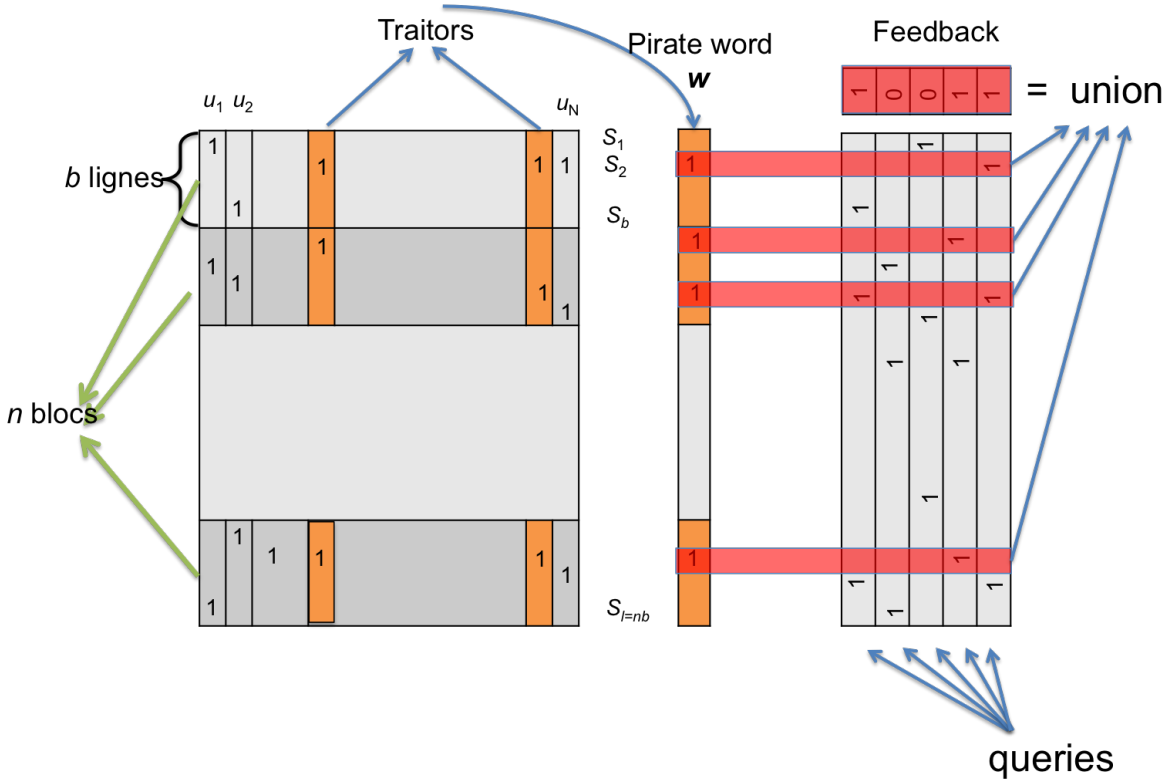
## Shadow Group Testing Technique[NPP, Algorithmica13]




- Test the decryptability of the piarte decoder on the queries
  $\rightarrow$ Get “Feedback” vector = union of the columns at position 1 in the pirate word $w$

# Black-box Tracing for ESS

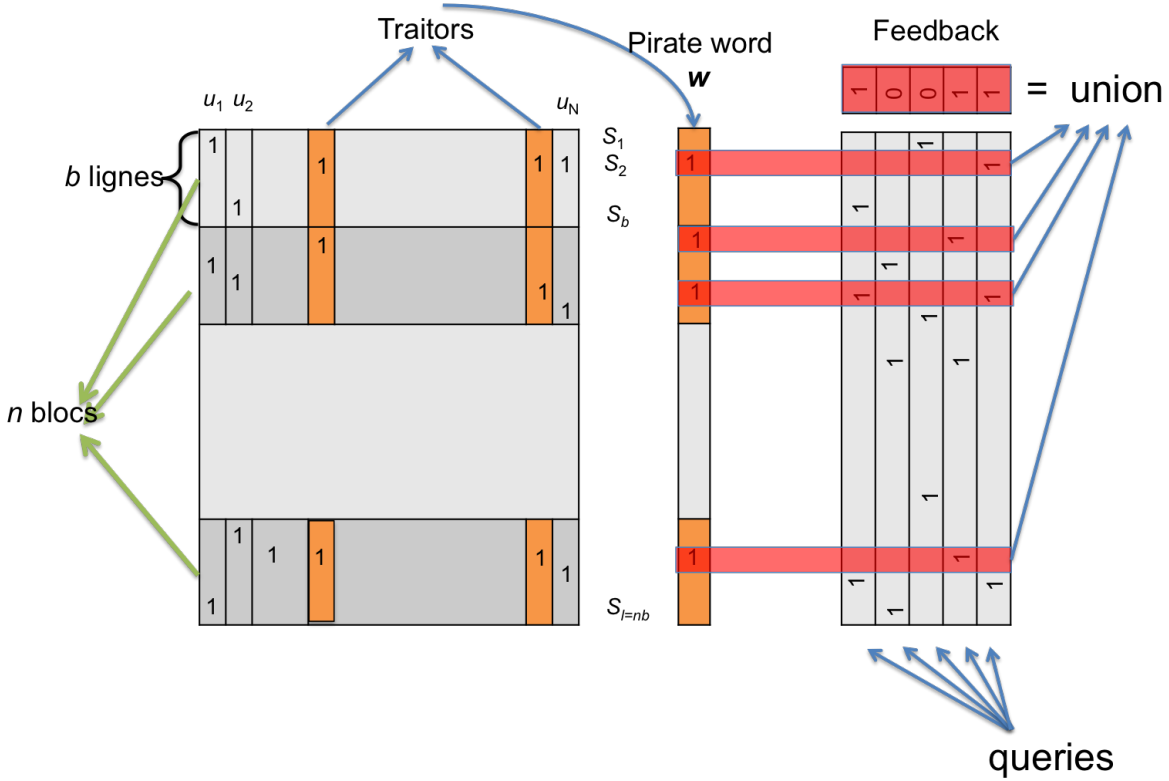
## Shadow Group Testing Technique[NPP, Algorithmica13]




- We show that the matrix of queries is also an ESS
  $\rightarrow$ From "Feedback" vector, get the pirate word $w$
- Large number of queries
  $\rightarrow$ the tracing is efficient when the number of traitors is $O(\log N)$

# Black-box Tracing for ESS

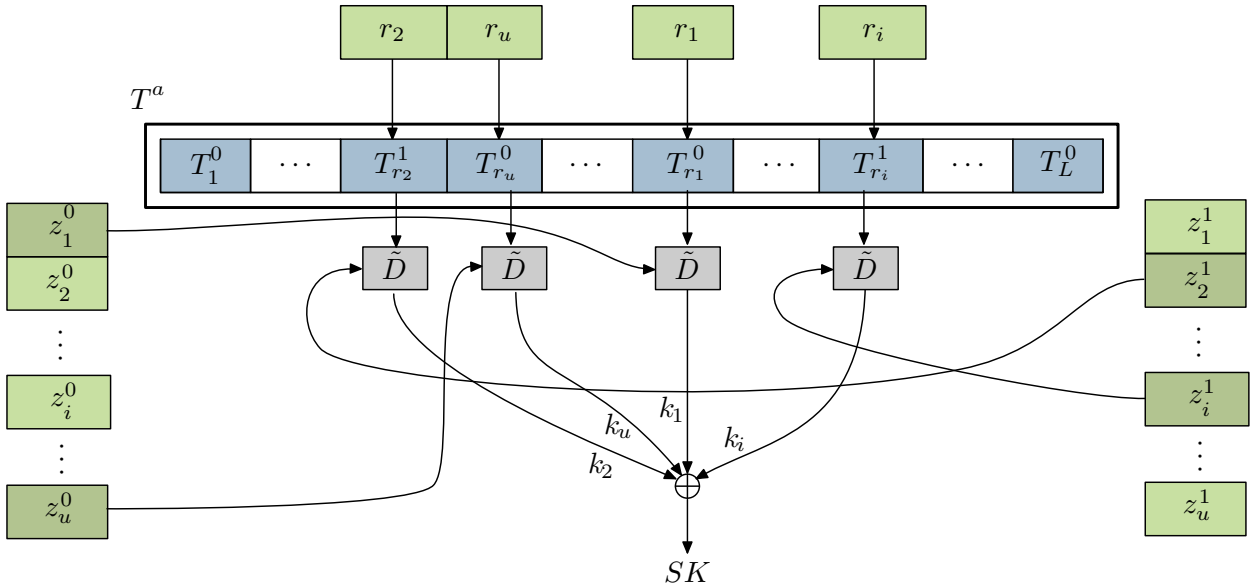
## Shadow Group Testing Technique[NPP, Algorithmica13]




In brief:

- We get $(N, 8r^2 \log N, r, 8r \log N)$-ESS
- Ciphertext: constant factor w.r.t the complete-subtree and a log $N$ factor w.r.t the subset-difference scheme
- The first black-box tracing ESS against non-naive pirates

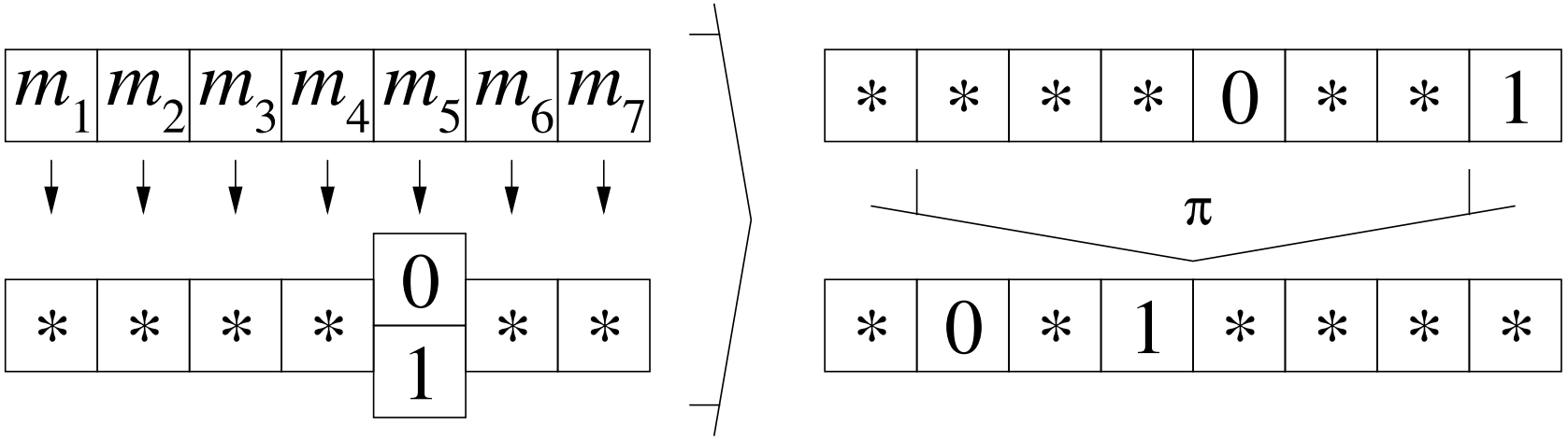
# Combinatorial Approach: Other Contributions




Constant-size Ciphertext [BP08]:

- Based on Robust Collusion Secure Code [S06,N09]
- Drawback: large secret key size ($O(t^2 \log^2(N/\epsilon))$)

# Combinatorial Approach: Other Contributions




Hiding a mark at position 5 in a sequence of 7 blocks.

Message Tracing with Optimal Transmission Rate [PPS12]

- The rate between ciphertext and plaintext is $\approx 1$ (constant size is achieved in [KY01)]
- It requires us to construct an efficient construction of 2-user Anonymous BE
- Large size plaintext $\rightarrow$ suitable for broadcasting messages

# Outline

# From Encryption to Multi-receiver Encryption

## ElGamal Encryption Scheme

- $G =< g >$ of order $q$
- Secret key: $\alpha \leftarrow \mathbb{Z}_q$
- Public key: $y = g^{\alpha}$
- Ciphertext: $(g^r, y^r m)$, where $r \leftarrow \mathbb{Z}_q$
- Decryption: from $\alpha$, compute $y^r = (g^r)^{\alpha}$ and recover $m$

# From Encryption to Multi-receiver Encryption

## ElGamal Encryption Scheme

- $G =< g >$ of order $q$
- Secret key: $\alpha \leftarrow \mathbb{Z}_q$
- Public key: $y = g^{\alpha}$
- Ciphertext: $(g^r, y^r m)$, where $r \leftarrow \mathbb{Z}_q$
- Decryption: from $\alpha$, compute $y^r = (g^r)^{\alpha}$ and recover $m$

## Boneh-Franklin Multi-receiver Encryption

- Main problem: How to extend the same $y$ to support many users?

# From Encryption to Multi-receiver Encryption

## ElGamal Encryption Scheme

- $G =< g >$ of order $q$
- Secret key: $\alpha \leftarrow \mathbb{Z}_q$
- Public key: $y = g^{\alpha}$
- Ciphertext: $(g^r, y^r m)$, where $r \leftarrow \mathbb{Z}_q$
- Decryption: from $\alpha$, compute $y^r = (g^r)^{\alpha}$ and recover $m$

## Boneh-Franklin Multi-receiver Encryption

- Main problem: How to extend the same $y$ to support many users?
- Each user receive a representation $(\alpha_1, \ldots, \alpha_k)$ of $y$ in a public basis $(h_1, \ldots, h_k)$: $(y = h_1^{\alpha_1} \ldots h_k^{\alpha_k})$
- Each user can compute $y^r$ from $(h_1^r, \ldots, h_k^r)$

# From Encryption to Multi-receiver Encryption

## ElGamal Encryption Scheme

- $G =< g >$ of order $q$
- Secret key: $\alpha \leftarrow \mathbb{Z}_q$
- Public key: $y = g^{\alpha}$
- Ciphertext: $(g^r, y^r m)$, where $r \leftarrow \mathbb{Z}_q$
- Decryption: from $\alpha$, compute $y^r = (g^r)^{\alpha}$ and recover $m$

## Boneh-Franklin Multi-receiver Encryption

- Main problem: How to extend the same $y$ to support many users?
- Each user receive a representation $(\alpha_1, \ldots, \alpha_k)$ of $y$ in a public basis $(h_1, \ldots, h_k)$: $(y = h_1^{\alpha_1} \ldots h_k^{\alpha_k})$
- Each user can compute $y^r$ from $(h_1^r, \ldots, h_k^r)$
- Public key: $(y, h_1, \ldots, h_k)$
- Ciphertext: $(h_1^r, \ldots, h_k^r, y^r m)$

# Boneh-Franklin Scheme

## Boneh-Franklin Traitor Tracing

- Transformation from Elgamal Encryption to Traitor Tracing: linear loss in the number of traitors
- Achieve white-box tracing and Black-box confirmation

# Boneh-Franklin Scheme

## Boneh-Franklin Traitor Tracing

- Transformation from Elgamal Encryption to Traitor Tracing: linear loss in the number of traitors
- Achieve white-box tracing and Black-box confirmation

## Our Work

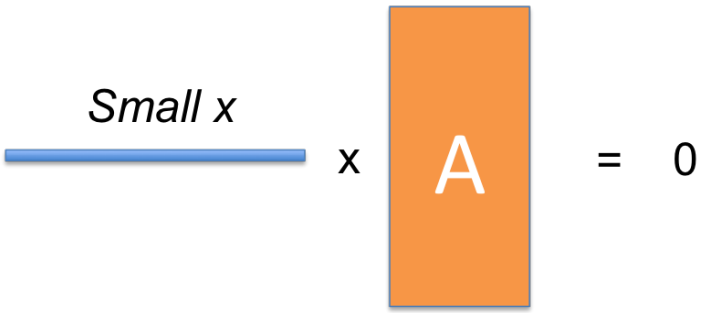
- Study the problem in lattice-based setting
- Get a more efficient transformation:

$$\text{LWE-based Encryption} \approx \text{LWE traitor tracing}$$

- Achieve Black-box confirmation as in Boneh-Franklin scheme

# The SIS and LWE problems

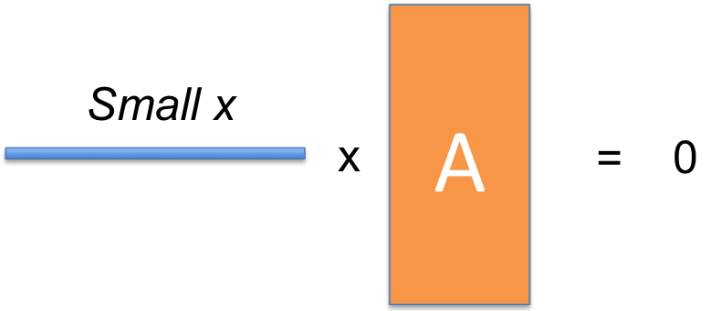
- Params: $m, n, q \geq 0$, $A \hookleftarrow U(\mathbb{Z}_q^{m \times n})$



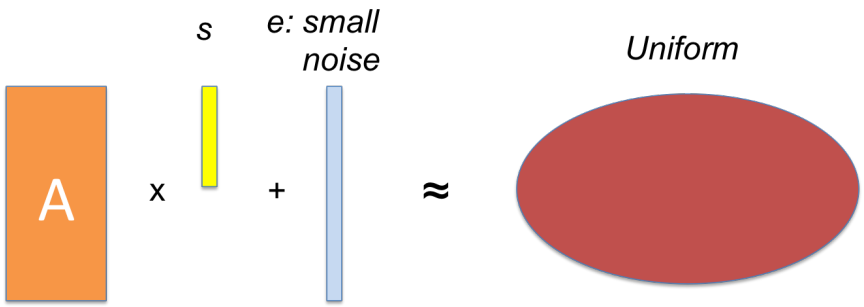

**SIS**
Find small $\mathbf{x} \in \mathbb{Z}^m \setminus \mathbf{0}$
s.t. $\mathbf{x}^t A = \mathbf{0}\ [q]$

# The SIS and LWE problems

- Params: $m, n, q \geq 0$, $A \hookleftarrow U(\mathbb{Z}_q^{m \times n})$



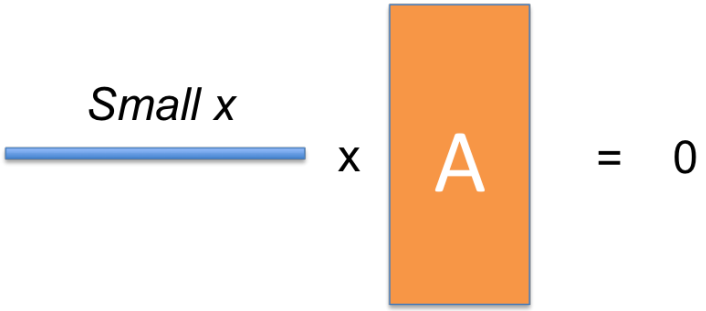

**SIS**
Find small $\mathbf{x} \in \mathbb{Z}^m \setminus \mathbf{0}$
s.t. $\mathbf{x}^t A = \mathbf{0}\ [q]$



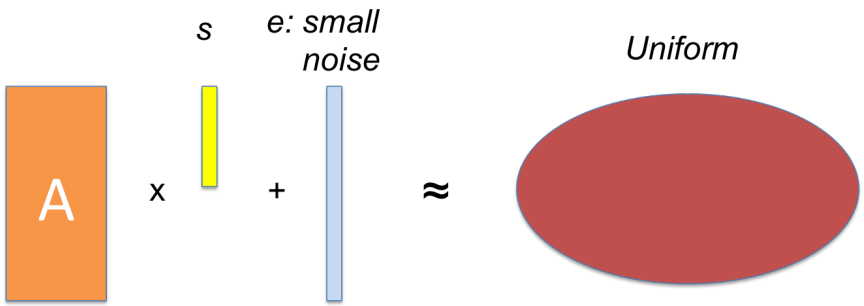

**LWE**
Dist. $A\mathbf{s} + \mathbf{e}$ and $U(\mathbb{Z}_q^m)$,
for $\mathbf{s} \hookleftarrow U(\mathbb{Z}_q^n)$, noise $\mathbf{e} \in \mathbb{Z}^m$

# The SIS and LWE problems

- Params: $m, n, q \geq 0$, $A \hookleftarrow U(\mathbb{Z}_q^{m \times n})$




**SIS**
Find small $\mathbf{x} \in \mathbb{Z}^m \setminus \mathbf{0}$
s.t. $\mathbf{x}^t A = \mathbf{0}\ [q]$



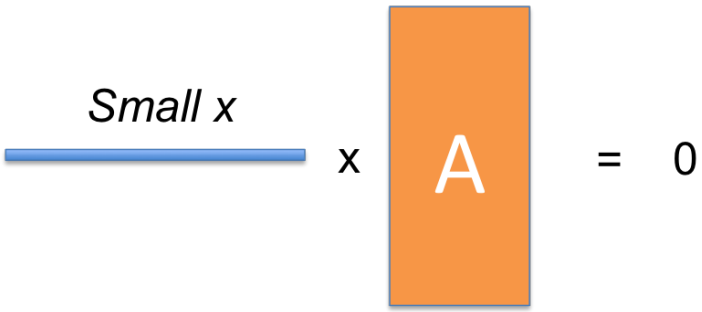

**LWE**
Dist. $A\mathbf{s} + \mathbf{e}$ and $U(\mathbb{Z}_q^m)$, for $\mathbf{s} \hookleftarrow U(\mathbb{Z}_q^n)$, noise $\mathbf{e} \in \mathbb{Z}^m$

## Applications

Hash function [Ajt'96], signature [GPV'08], encryption [Reg'05], ...

# SIS $\rightarrow$ $k$-SIS and LWE $\rightarrow$ $k$-LWE

- Params: $m, n, q \geq 0$, $A \hookleftarrow U(\mathbb{Z}_q^{m \times n})$
- $k$ small hints $(\mathbf{x}_i)_{i \leq k}$ s.t. $\mathbf{x}_i^t A = \mathbf{0}\ [q]$

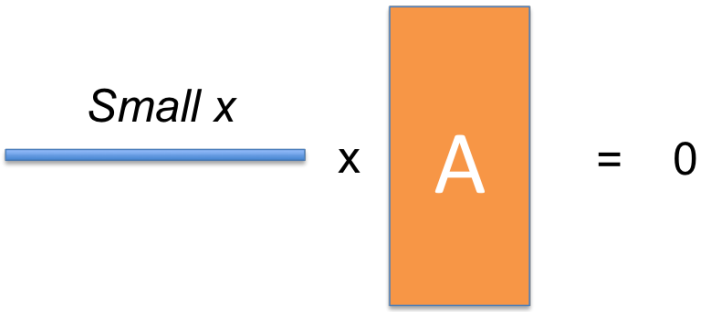



**$k$-SIS** [BoFr'11]
Find small $\mathbf{x} \in \mathbb{Z}^m$ s.t.

- $\mathbf{x}^t A = \mathbf{0}\ [q]$
- $\mathbf{x} \notin \mathrm{Span}(\mathbf{x}_i)$

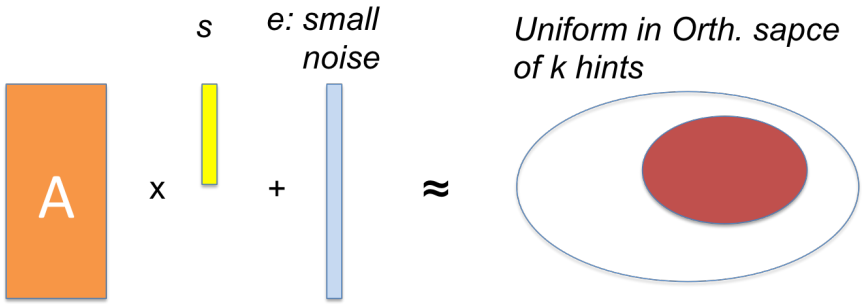
# SIS $\rightarrow$ $k$-SIS and LWE $\rightarrow$ $k$-LWE

- Params: $m, n, q \geq 0$, $A \hookleftarrow U(\mathbb{Z}_q^{m \times n})$
- $k$ small hints $(\mathbf{x}_i)_{i \leq k}$ s.t. $\mathbf{x}_i^t A = \mathbf{0}\ [q]$




**$k$-SIS** [BoFr'11]
Find small $\mathbf{x} \in \mathbb{Z}^m$ s.t.

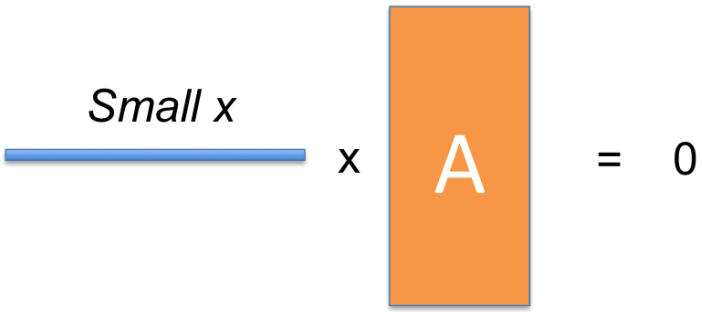
- $\mathbf{x}^t A = \mathbf{0}\ [q]$
- $\mathbf{x} \notin \mathrm{Span}(\mathbf{x}_i)$




**$k$-LWE**
Distinguish $A\mathbf{s} + \mathbf{e}$ and $U(\mathrm{Span}(\mathbf{x}_i)^{\perp}) + \mathbf{e}'$ for $\mathbf{s} \hookleftarrow U(\mathbb{Z}_q^n)$ and small noises $\mathbf{e}, \mathbf{e}' \in \mathbb{Z}^m$

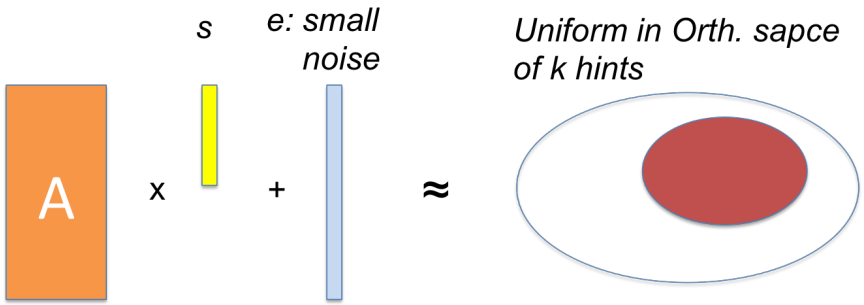
# SIS $\rightarrow$ $k$-SIS and LWE $\rightarrow$ $k$-LWE

- Params: $m, n, q \geq 0$, $A \hookleftarrow U(\mathbb{Z}_q^{m \times n})$
- $k$ small hints $(\mathbf{x}_i)_{i \leq k}$ s.t. $\mathbf{x}_i^t A = \mathbf{0}\ [q]$




**$k$-SIS** [BoFr'11]
Find small $\mathbf{x} \in \mathbb{Z}^m$ s.t.

- $\mathbf{x}^t A = \mathbf{0}\ [q]$
- $\mathbf{x} \notin \mathrm{Span}(\mathbf{x}_i)$




**$k$-LWE**
Distinguish $A\mathbf{s} + \mathbf{e}$ and $U(\mathrm{Span}(\mathbf{x}_i)^{\perp}) + \mathbf{e}'$ for $\mathbf{s} \hookleftarrow U(\mathbb{Z}_q^n)$ and small noises $\mathbf{e}, \mathbf{e}' \in \mathbb{Z}^m$

Original application of $k$-SIS: Homomorphic signatures [BoFr'11]

# Contributions [LPSS, Crypto14]

## New Variant of LWE

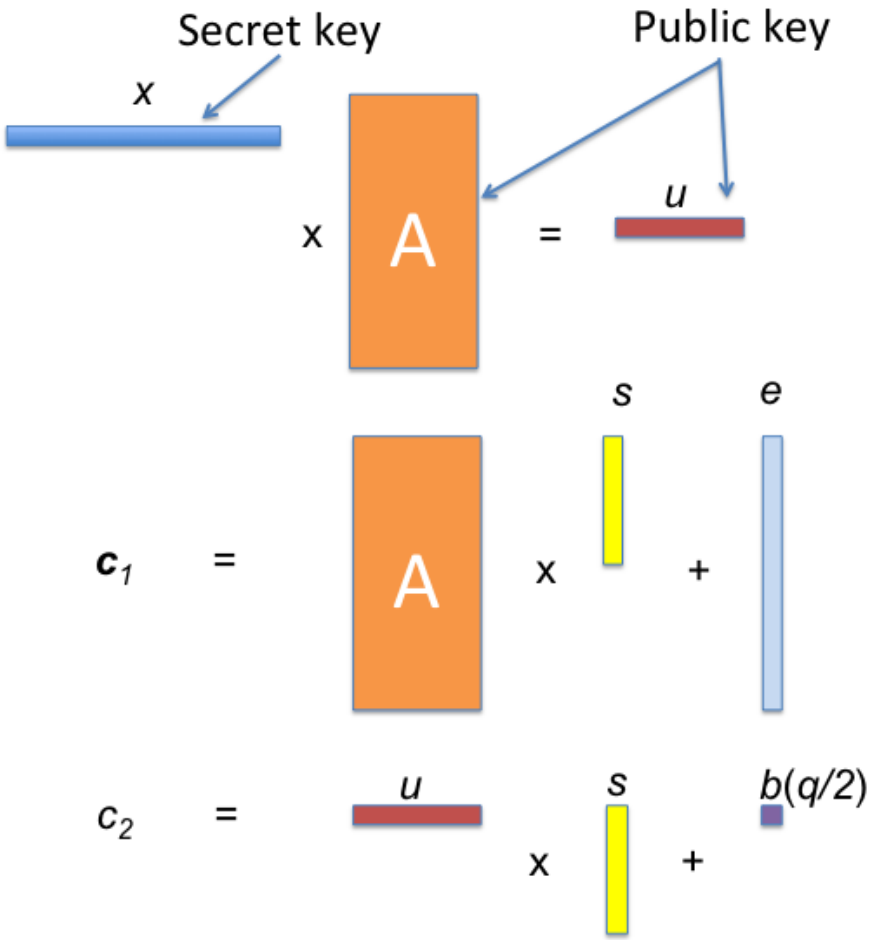
- Introduction of $k$-LWE
- A reduction from LWE to $k$-LWE (and from SIS to $k$-SIS) with polynomial loss in $k$

  (Boneh-Freeman11 from SIS to $k$-SIS: exponential loss in $k$. They left the open question to improve the reduction)

## Application

- Application to traitor tracing encryption, *à la* Boneh-Franklin
- A modification that enjoys public traceability

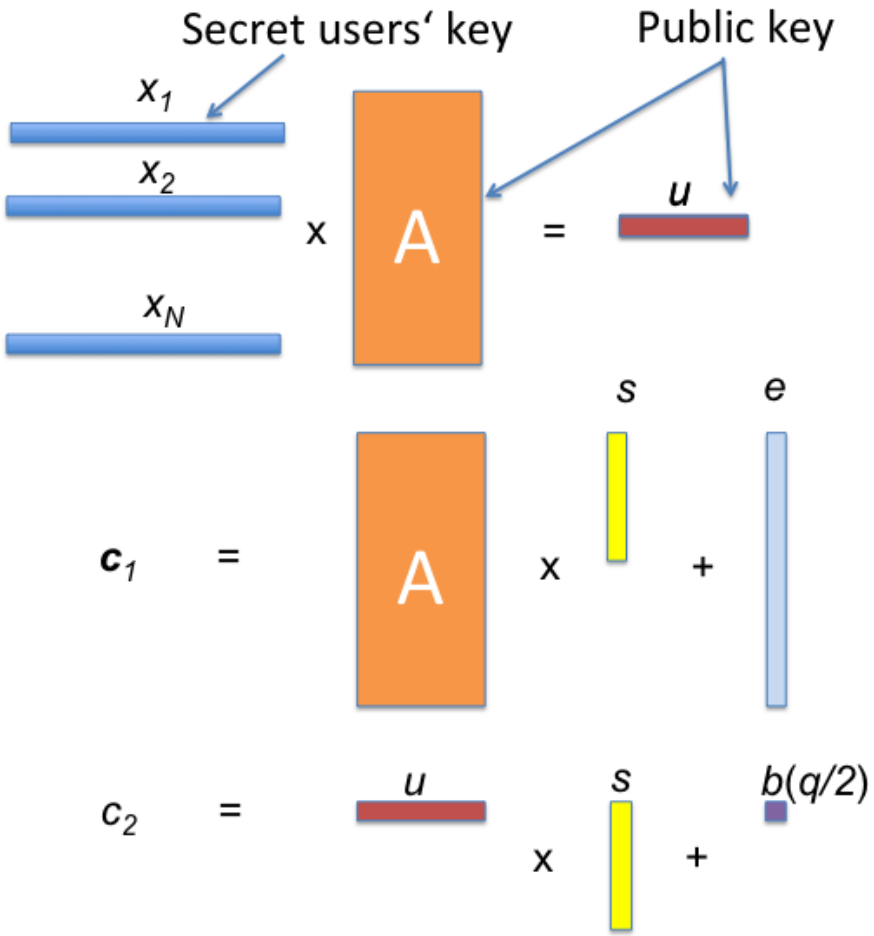
# A Multi-receiver Dual-Regev Encryption (based on [GPV'08])




## Dual-Regev Encryption

- Public key: $A \in \mathbb{Z}_q^{m \times n}$ and $\mathbf{u} \in \mathbb{Z}_q^n$
- Secret key: $\mathbf{x}$ gaussian s.t. $\mathbf{x}^t A = \mathbf{u}^t \ [q]$
- Ciphertext: $(\mathbf{c}_1, c_2)$
- Decryption: $c_2 - \mathbf{x}^t \mathbf{c}_1$

# A Multi-receiver Dual-Regev Encryption (based on [GPV'08])




## Multi-receiver Encryption

- Public key: $A \in \mathbb{Z}_q^{m \times n}$ and $\mathbf{u} \in \mathbb{Z}_q^n$
- Secret keys: $\mathbf{x}_i$ gaussian s.t. $\mathbf{x}_i^t A = \mathbf{u}^t \ [q]$
- Ciphertext: $(\mathbf{c}_1, c_2)$
- Decryption: $c_2 - \mathbf{x}^t \mathbf{c}_1$

Using trapdoor $T$ (full rank small $T \in \mathbb{Z}^{m \times m}$ s.t. $T \cdot A = 0 \ [q]$), one can sample many secret keys $\mathbf{x}_i$ [GPV08]

# $k$-LWE-based Traitor Tracing, *à la* Boneh-Frranklin

## Pirate

- Up to $k$ users may collude
  $\Rightarrow$ A coalition is given up to $k$ LWE hints to create a pirate decryption box

# $k$-LWE-based Traitor Tracing, *à la* Boneh-Frranklin

## Pirate

- Up to $k$ users may collude
  $\Rightarrow$ A coalition is given up to $k$ LWE hints to create a pirate decryption box

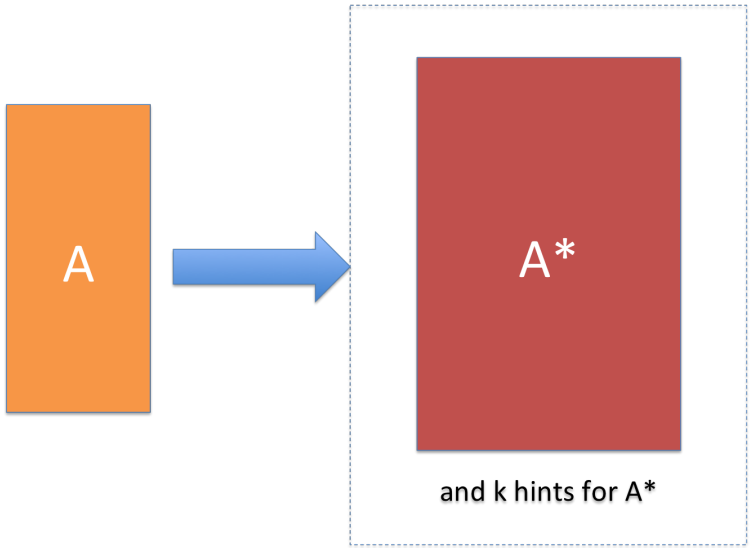
## Tracer

- Assume we suspect the coalition to be among users 1 to $k$.
- Test the behaviour of the box on the fake ciphertexts:

$$U\left((\mathrm{Span}_{i\leq k}(\mathbf{x}_i^t|1))^{\perp}\right).$$

- The coalition owns only those $\mathbf{x}_j$'s $\rightarrow$ the fake and normal ciphertexts are indistinguishable, under $k$-LWE

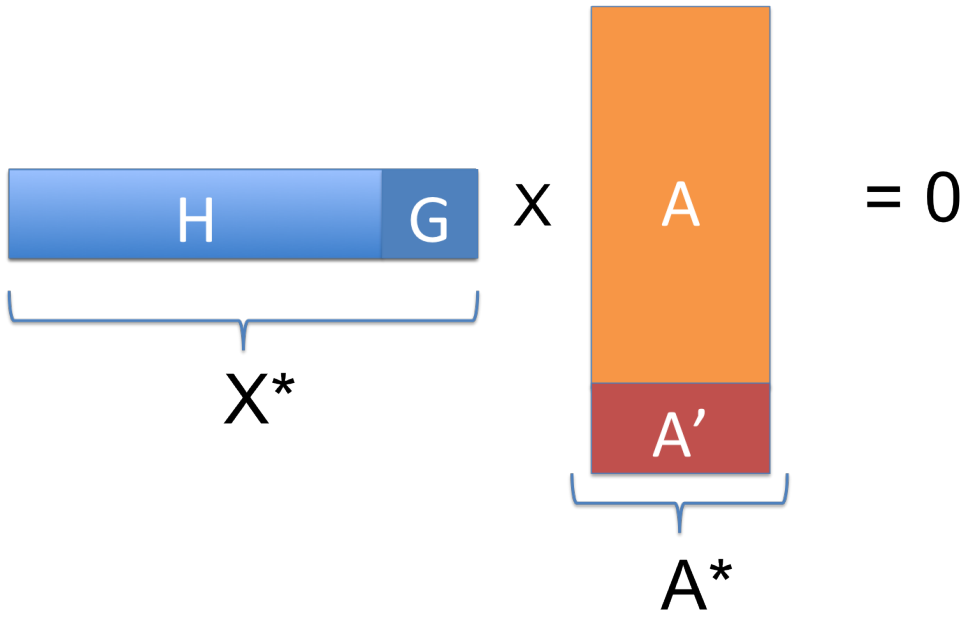
# How to Prove The Hardness of $k$-SIS and $k$-LWE




## Reducing LWE to $k$-LWE

- Input: a SIS / LWE instance corresponding to $A$
- From $A$, construct $A^*$ along with $k$ hints for $A^*$
- Give $A^*$ and the $k$ hints to a $k$-SIS / $k$-LWE solver
- Based on a $k$-SIS or $k$-LWE solution for $A^*$, derive a SIS / LWE solution for $A$

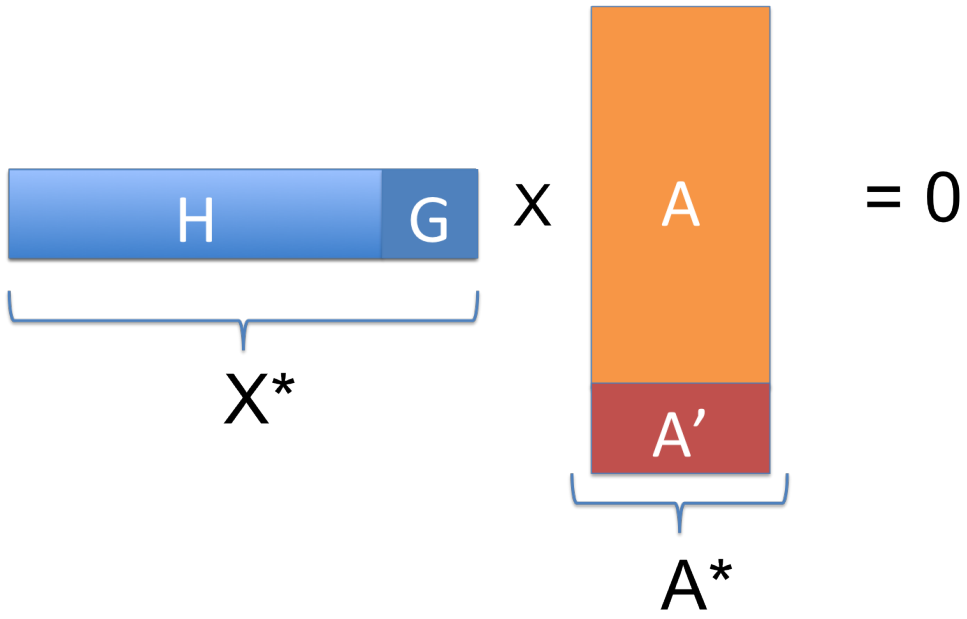
# Hardness of $k$-LWE: The [BF11] Approach




## Main Idea

1. Sample $k$ hints $\mathbf{x}_1, \ldots, \mathbf{x}_k$ that form a $k \times (m+k)$ matrix $X^* = (H|G)$ (using the $\mathbf{x}_i$'s as rows)
2. Append to $A$ an extra $k \times n$ matrix $A' = -G^{-1}H \cdot A \ [q]$
3. Append to $\mathbf{b} = A\mathbf{s} + \mathbf{e}$ an extra $\mathbf{b}' = -G^{-1}H \cdot \mathbf{b} \ [q]$

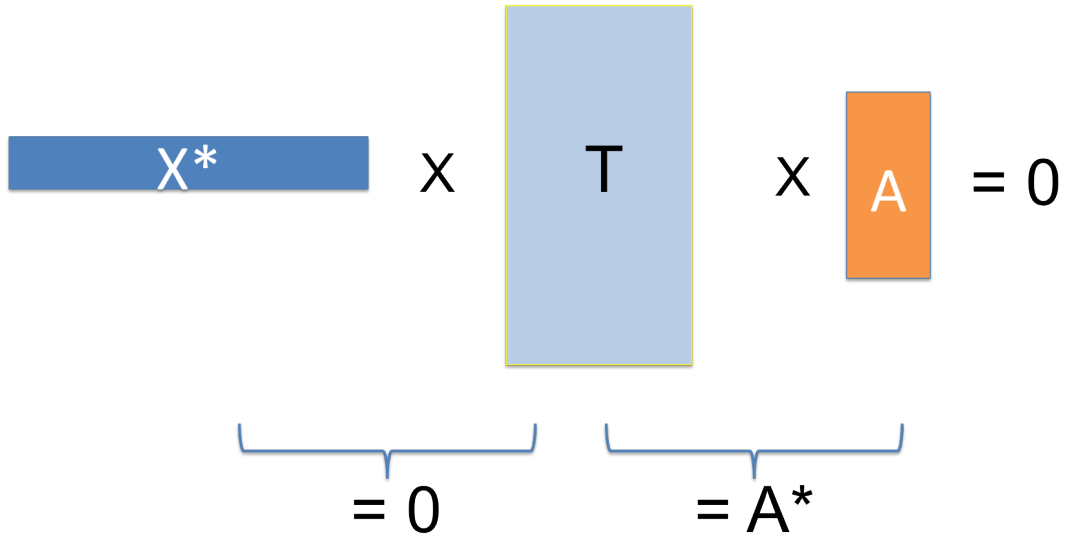
# Hardness of $k$-LWE: The [BF11] Approach




## Obstacle

- We have $\mathbf{b}' = A'\mathbf{s} + \mathbf{e}'$ with $\mathbf{e}' = -G^{-1}H \cdot \mathbf{e} \ \ [q]$
- $\mathbf{e}'$ is not small!
- To fix it, multiply everything by $\det(G)$
- Blow-up: $\|\mathbf{e}'\| \approx k!\|\mathbf{e}\|$, which is $\ll q$ for tiny $k$

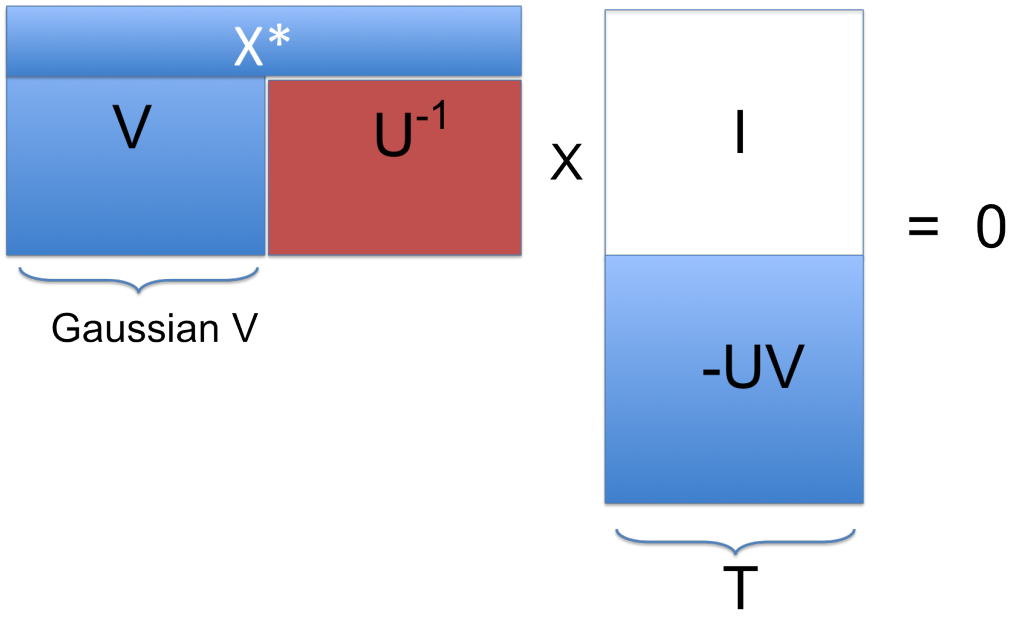
# Our Reduction: Polynomial Loss in $k$




## Main Steps

1. Generate a small transformation matrix $T$ such that it is easy to generate gaussian $X^*$ ($k$ hints matrix) : $X^* \times T = 0$
2. $T(A\mathbf{s} + \mathbf{e}) = (TA)\mathbf{s} + (T\mathbf{e}) = A^* + \mathbf{e}^*$
3. Avoid "exponential noise blowup", $T\mathbf{e}$ is of polynomial size in $\mathbf{e}$

# Transformation Matrix $T$ and Hints $X^*$




1. Main tool: A small $U$ such that the first $k$ rows of $U^{-1}$ are small Gaussian (relying on LHL)
2. Sampling a Gaussian matrix $V$
3. Define $X^*$ as the first $k$ rows of $V \,||\, U^{-1}$
4. $LWE(A, A\mathbf{s} + \mathbf{e}) \rightarrow k - LWE(TA, T(A\mathbf{s} + \mathbf{e}) + \mathbf{e}')$

# Public Traceability

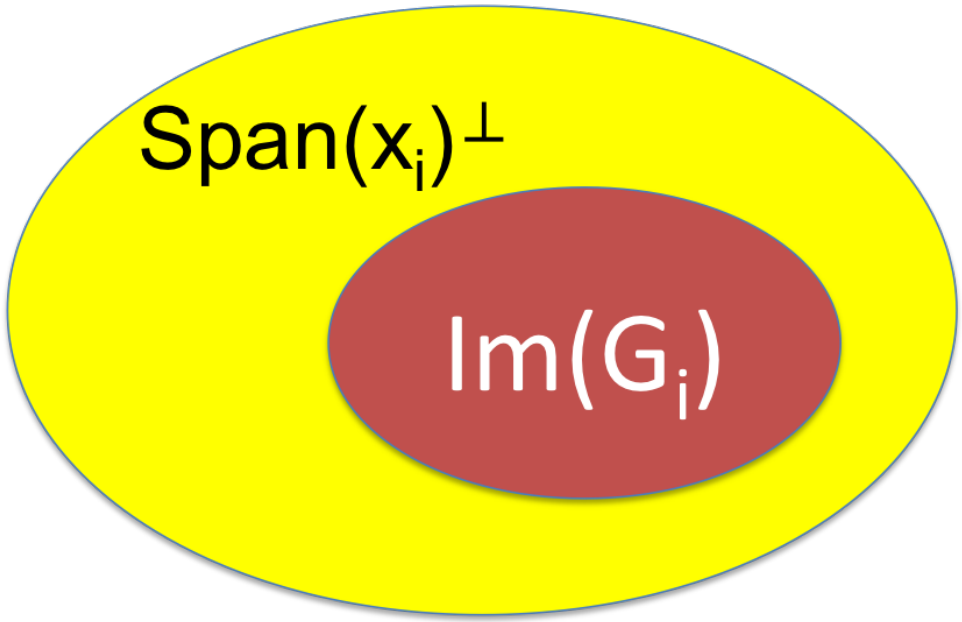
## Public Traceability [CPP05]

- Classical tracing: relies on the secret information.
  $\Rightarrow$ Complete trust in the tracing authority, huge tracing cost.
- Public tracing: anyone can trace using the public key $\Rightarrow$ Delegation of the tracing procedure

## Schemes with Public Traceability

- IPP code-based scheme [PST06]
- Pairings based scheme [BW06]: full collusion but with large ciphertext size $O(\sqrt{N})$

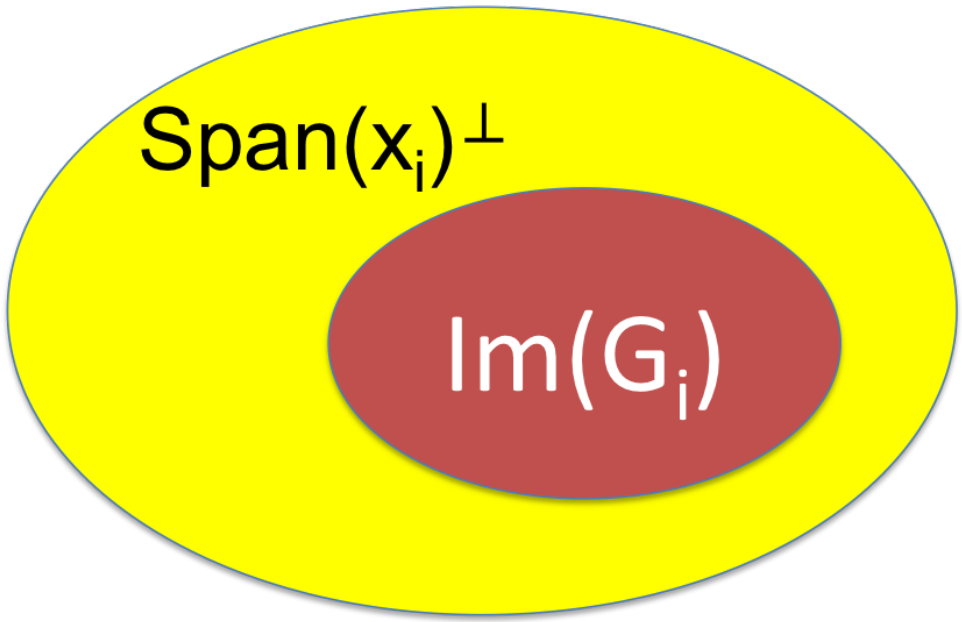
# Public Traceability




## Public Sampling

1. Each $\mathbf{x}_i$ is associated to a public matrix $G_i$
2. Hard to distinguish $U(\mathrm{Span}(\mathbf{x}_i^+)^\perp) + \textit{noise}$ and $\mathrm{Im}(G_k) + \textit{noise}$
3. Publicly sample a signal in $U(\mathrm{Span}(\mathbf{x}_i^+)^\perp) + \textit{noise}$ from $G_i$

# Public Traceability




## Public Tracing

1. Public matrix $G_i$
2. It is hard to distinguish $U(\mathrm{Span}_{i=1}^{j}(\mathbf{x}_i)^{\perp}) + \textit{noise}$ and $\mathrm{Im}(G_1) \cap \ldots \cap \mathrm{Im}(G_j) + \textit{noise}$, for any $1 \leq j \leq k$
3. We can thus sample tracing signals from $G_1, \ldots, G_k$

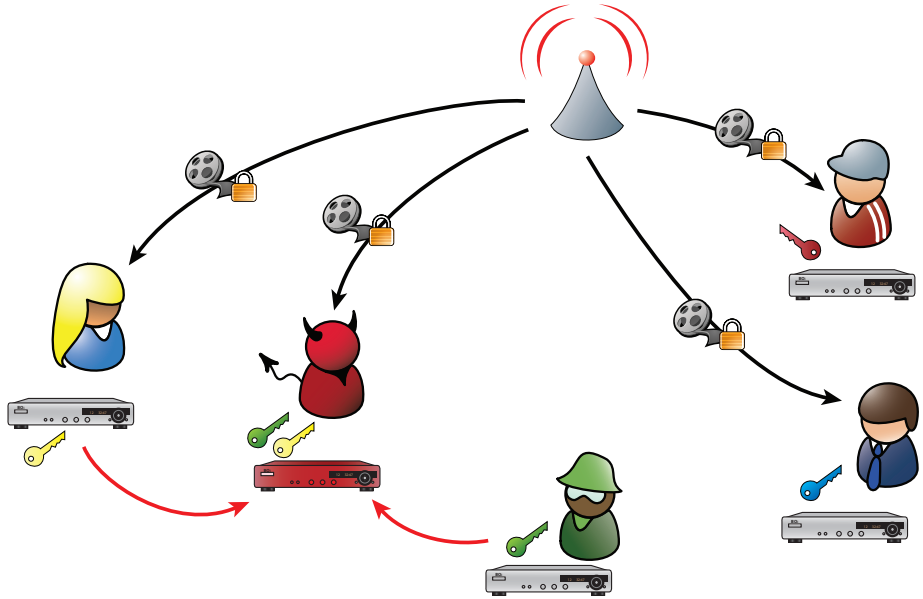
# Algebraic Approach: Other Contributions

## Pairings based Constructions

- BGW scheme: efficient pairing based broadcast encryption
  $\Rightarrow$ Extension: inclusive-exclusive mode and adaptive security [PPSS12]
- Combination of algebraic and combinatorial methods that relies on parings and collusion secure codes.
  - Identity-based Traitor Tracing [ADMNPS07]
  - Identity-based Trace & Revoke [PT11]

# Outline

# Classical Collusions

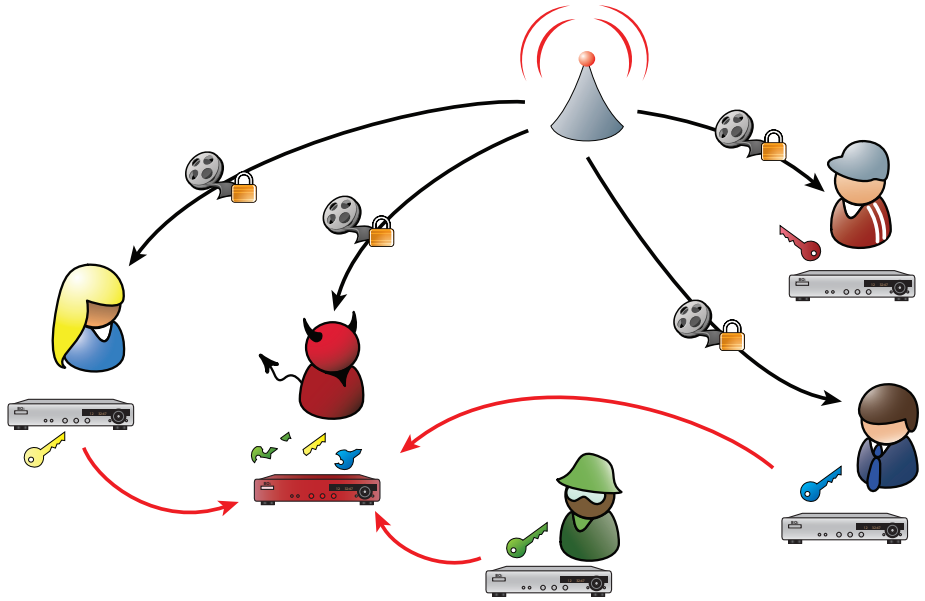


## Facts

- Each user contributes its whole key
- Traitors should trust each other

# Pirates 2.0: Traitors Collaborating in Public

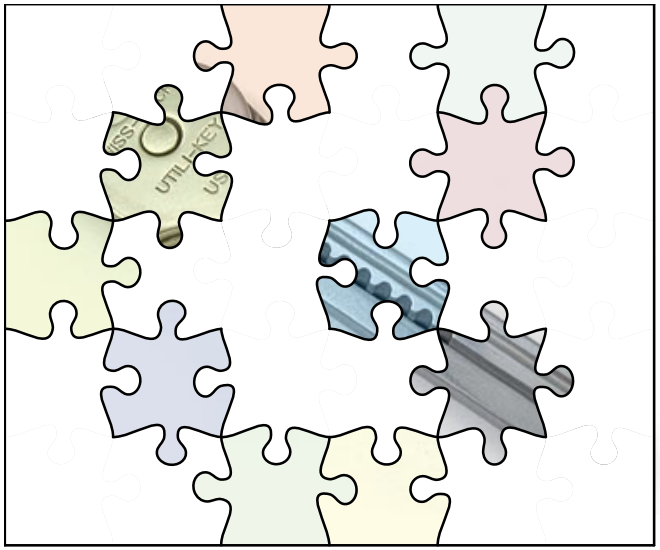
[BP, Eurocrypt09]



## Principle

- Each traitor contributes a partial or derived information
- “Imperfect” Pirate Decoder but still very efficient (inspired from Pirate Evolution Attack [KP07])
- High anonymity of traitors

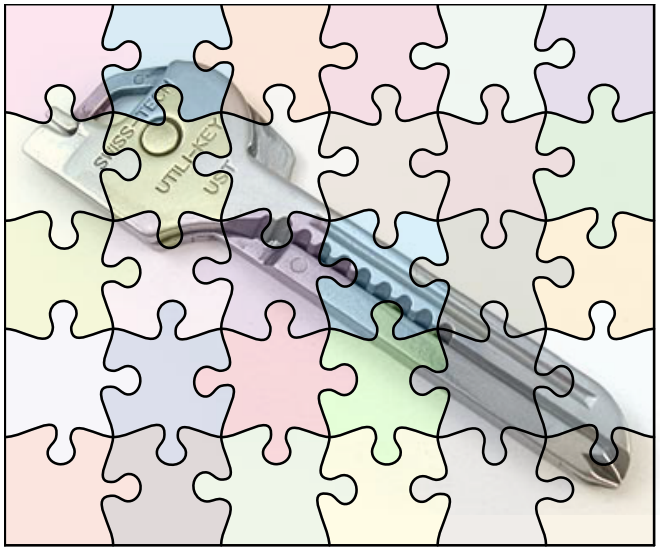
# Practical Impact of Pirates 2.0



## Collusion Size

- Traitors do not need to trust anyone
- Guaranteed anonymity is a big incentive to contribute secrets
- Even partial information extracted from tamper resistant or obfuscated decoders can be useful
- Traitors can contribute information adaptatively

# Practical Impact of Pirates 2.0



## Impact for Subset Difference Scheme

- Considering the classical setting which covers $2^{32}$ users
- Then, 10000 traitors (1000 in adaptative attacks) can decrypt all ciphertexts with headers of size less than 128 Mb
- High anonymity level: each traitor is covered by 4 millions users

# Extended Models: Other Contributions

## Multi-channel Broadcast Encryption [PPT13]

- Consider simultanous broadcast encryption
- New scheme with constant ciphertext size
- Compress session keys of all channels into one header $\rightarrow$ high-time complexity to decompress

# Extended Models: Other Contributions

## Multi-channel Broadcast Encryption [PPT13]

- Consider simultanous broadcast encryption
- New scheme with constant ciphertext size
- Compress session keys of all channels into one header $\rightarrow$ high-time complexity to decompress

## Decentralized Broadcast Encryption[PPS12]

- No need for a trusted authority
- Users agree on system parameters
- New tree-based scheme based on Diffie-Hellman perfect entropy extractor

# Discussion

## Summary

- Tools & constructions for combinatorial and algebraic schemes
- Extended models of attacks and generailizations for BE/TT

## Combinatorial Methods

- Better support for black-box tracing
- Larger key sizes
- Partial-leakage attacks

## Algebraic Method

- Generally more efficient
- Full collusion solutions still not satisfactory

# Open Questions

- Fully Collusion Resistance
  - Either the schemes are still quite inefficient
  - Or the security is still not clear (e.g., composite order multi-linear maps/iO)
- Additional Features
  - Efficient decentralised BE in a constant number of rounds
  - Efficient anonymous BE
- CCA lattice-based trace&revoke schemes
- Efficient construction from more general primitives?
  - Attribute-based encryption
  - Functional encryption
- Tracing in electronic voting