

# New Techniques for Traitor Tracing: Size $N^{1/3}$ and More from Pairings

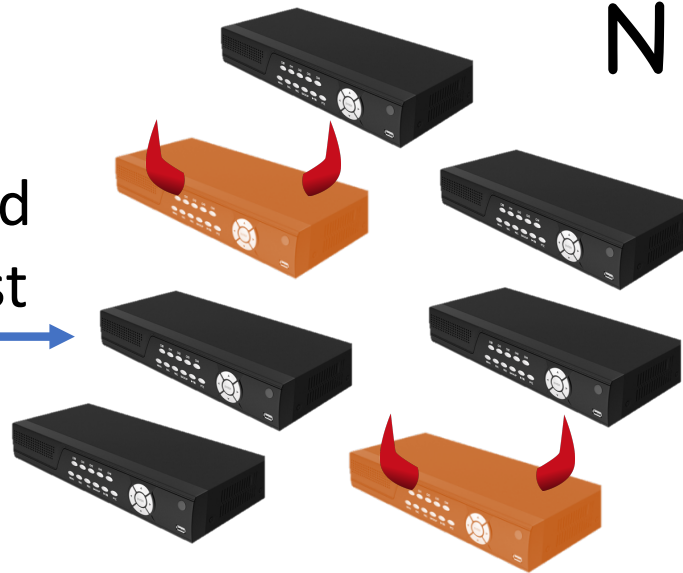
**Mark Zhandry** (Princeton & NTT Research)

# Traitor Tracing

[Chor-Fiat-Naor'94]



encrypted  
broadcast



$N := \#users$



## Requirement

Given pirate decoder, can identify the traitor(s)

- \* Even if arbitrarily many users collude
- \* Even if decoder fails most of the time

## Main Objective?

[me'13]

“The goal is to build collusion-resistant traitor tracing where ciphertext overhead in terms of  $N$  is minimized”

Sentiment common to  
much of the literature

Not the whole story...

Boneh-Naor'02:

PKE  $\rightarrow |ctx| = O(1)$

Combinatorial, uses  
“fingerprinting codes”  
[Boneh-Shaw'95]

Different views on  
why it doesn't “count”

**Problem 1:**

Only “threshold” secure  
(Can only trace decoder if  
 $\Pr[\text{decrypt}] \geq 0.9$ )

**Problem 2:**

$\Omega(N^2)$ -sized secret keys

$\rightarrow$  Considered  
too large

## Main Objective, Take 2

[me'20]

“The goal is to build collusion-resistant traitor tracing offering the best parameter-size *trade-offs* in terms of  $N$ ”

“And ideally, without the threshold limitation”

# What's Known

$$\begin{aligned} (P, K, C) = & \begin{aligned} |PP| &= P(N) \times \text{poly}(\lambda) \\ |sk| &= K(N) \times \text{poly}(\lambda) \\ |ctx| &= C(N) \times \text{poly}(\lambda) \end{aligned} \end{aligned}$$

Boneh-Sahai-Waters'06: Pairings  $\rightarrow (N^{1/2}, 1, N^{1/2})$

Garg-Gentry-Halevi-Raykova-Sahai-Waters'13, Boneh-Z'14: iO  $\rightarrow (1, 1, 1)$

Goyal-Koppula-Waters'18: LWE  $\rightarrow (1, 1, 1)$

Trivial:

PKE  $\rightarrow (N, 1, N)$

IBE  $\rightarrow (1, 1, N)$

Boneh-Naor'02:

PKE  $\rightarrow (N^2, N^2, 1)$

IBE  $\rightarrow (1, N^2, 1)$

Threshold

## Some Previously Open Questions


PKE, IBE,  
Pairing-free groups,  $\rightarrow (*, N^{1.99}, N^{0.99})?$   
or Factoring-like (even w/ threshold tracing)

Pairings  $\rightarrow (*, N^{1.99}, N^{0.49})?$   
(even w/ threshold tracing)

Anything but  
LWE/iO  $\rightarrow (*, *, N^{0.49})?$   
w/o threshold

# Observation

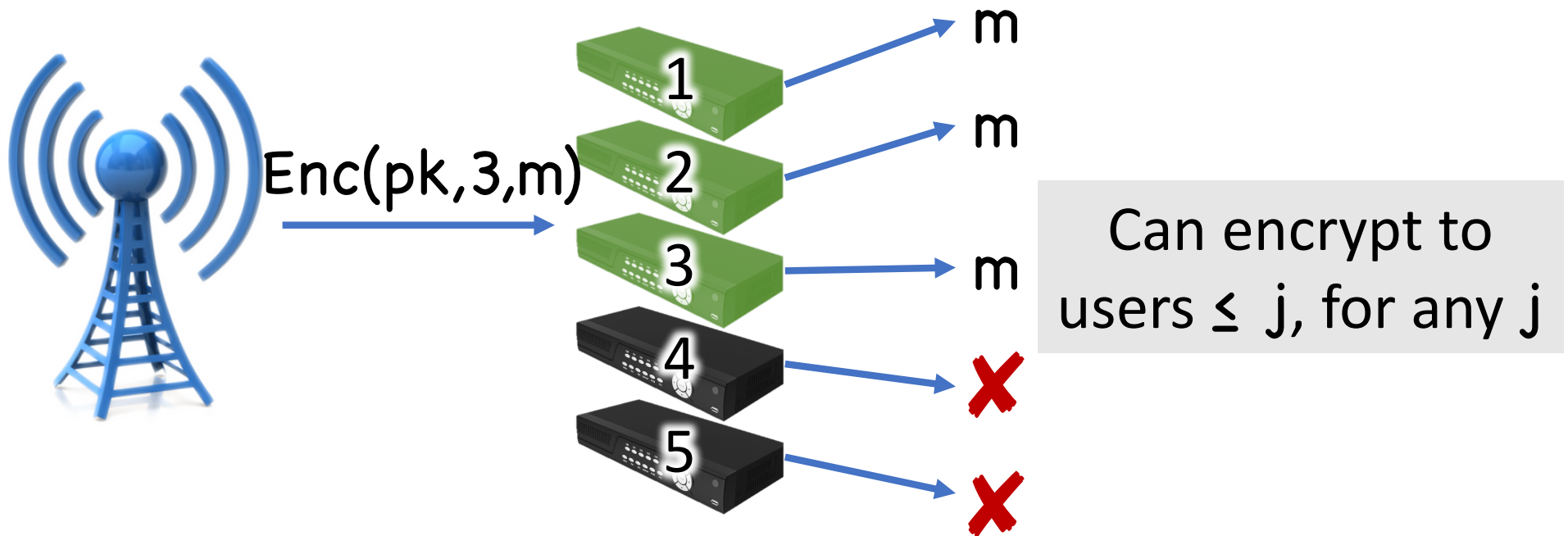
(no threshold **or** fully sublinear)



All the “best” collusion-resistant schemes in the literature follow “PLBE” framework



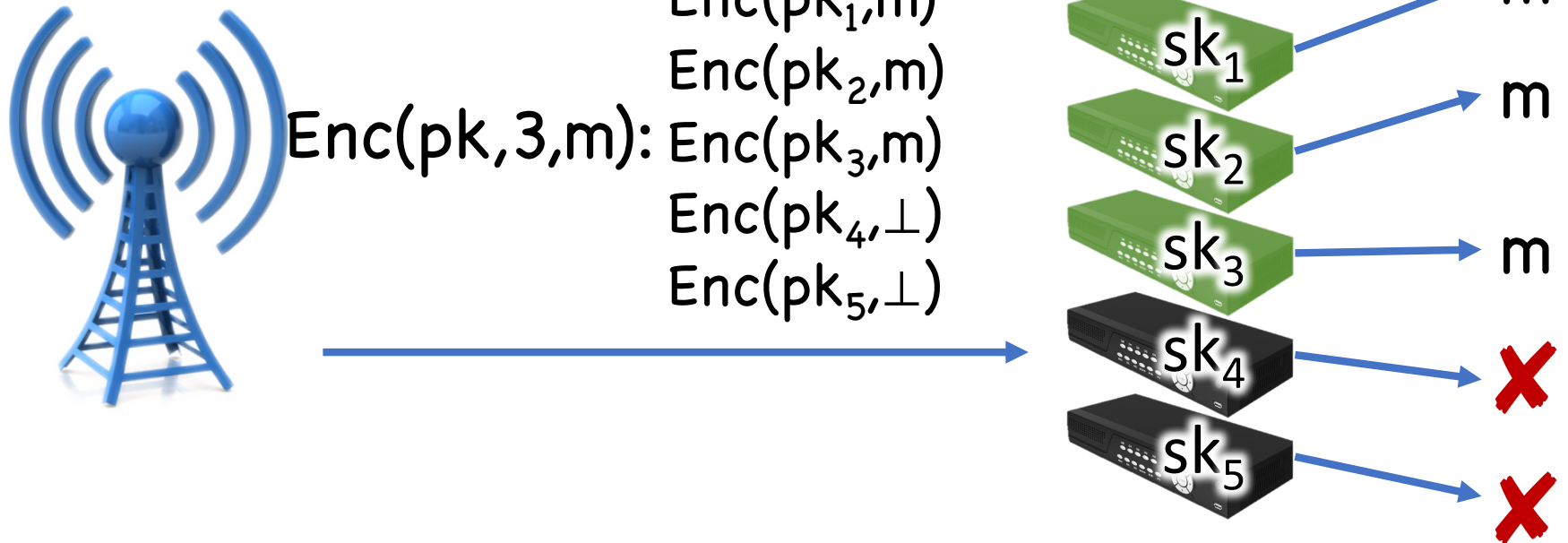
## Private Linear Broadcast Encryption (PLBE)



**Plus:** User  $i$  learns nothing about  $j$ , except whether  $i \leq j$

**Thm** ([Boneh-Sahai-Waters'06]): PLBE  $\rightarrow$  Traitor Tracing

## Trivial PLBE



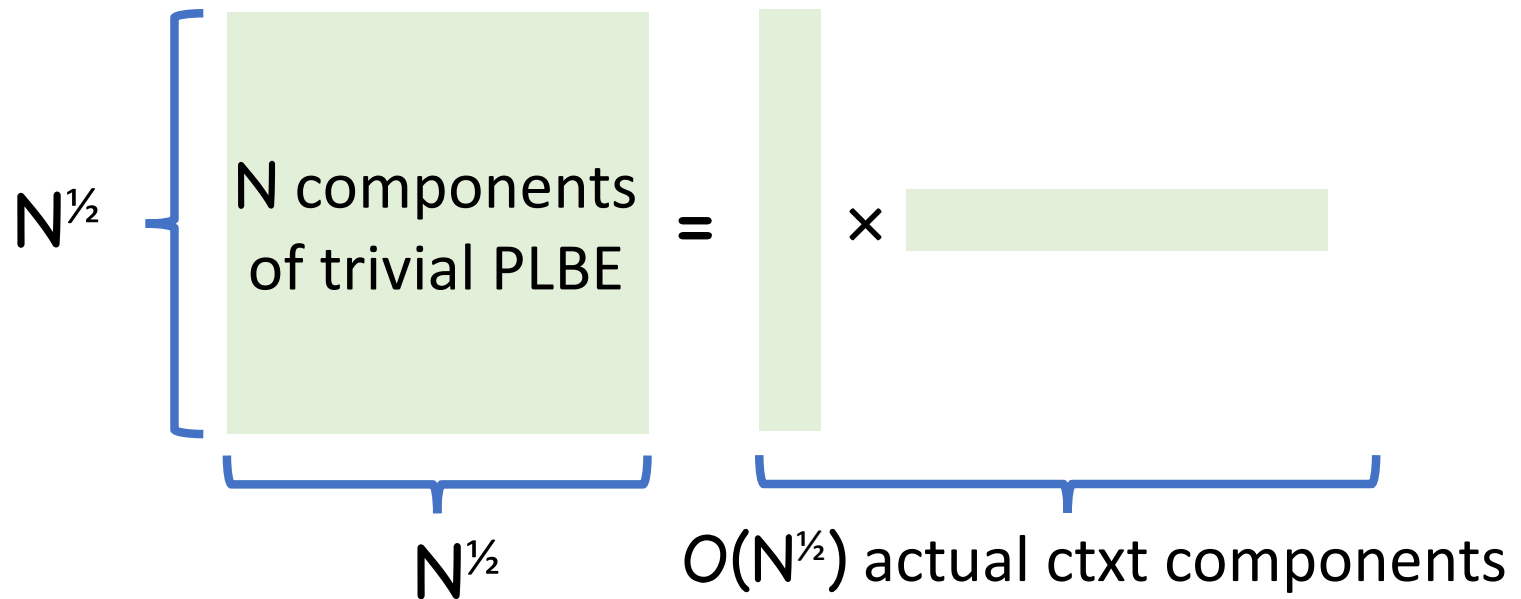
# PLBE-Based Traitor Tracing

Trivial PLBE:  $O(N)$ -sized ciphertexts

All the “best” traitor tracing schemes =  
improved algebraic constructions of PLBE

## The $N^{1/2}$ Barrier for Pairings

$e(g^a, g^b) = e(g, g)^{ab} \rightarrow$  Degree-2 functions in exponent



$N^{1/2}$  = best known PLBE from pairings




**This Work:** New techniques for  
(collusion-resistant) traitor tracing

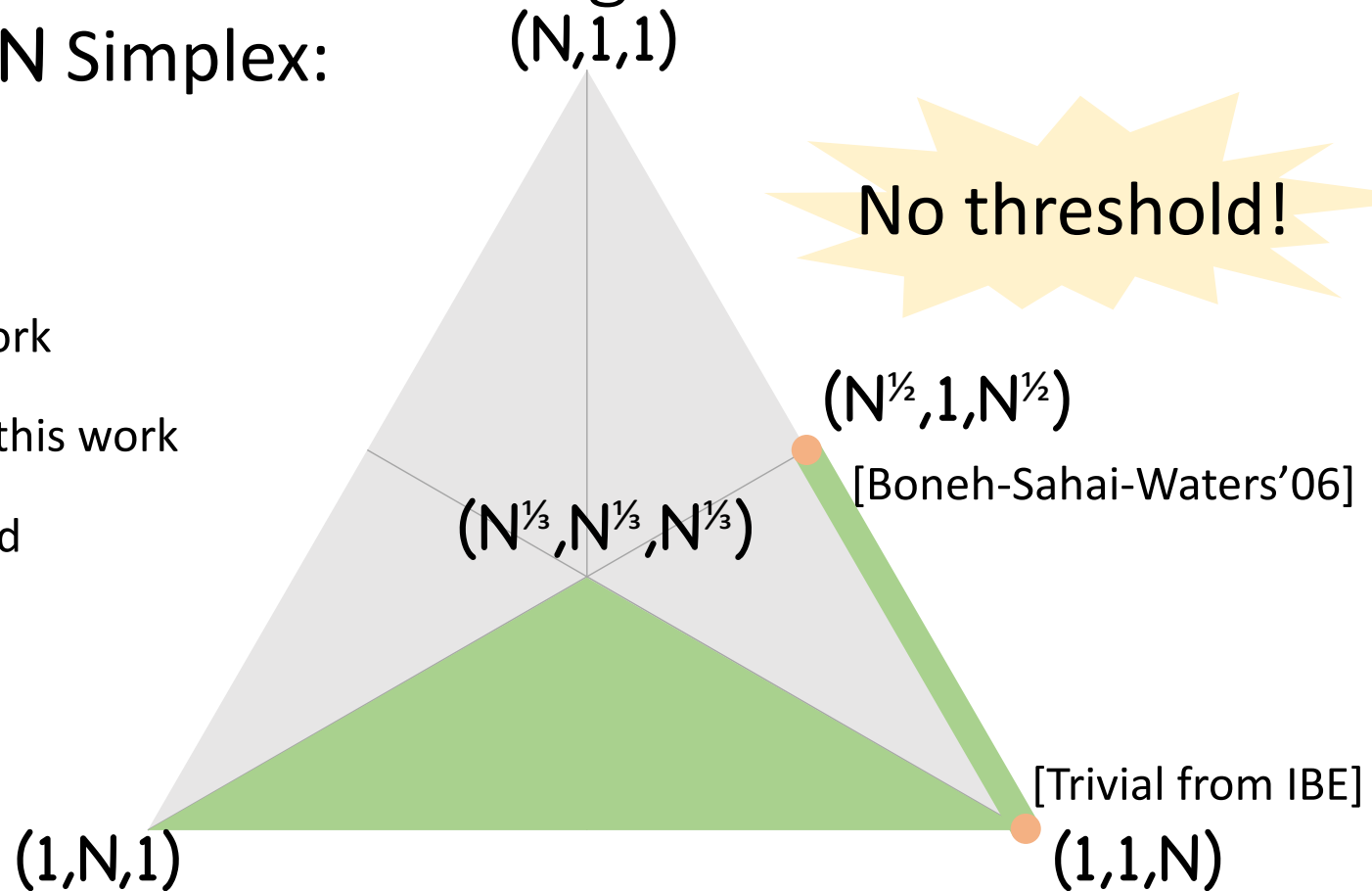


New parameter trade-offs from  
pairings and other primitives

# Parameters from Pairings

$P \times K \times C = N$  Simplex:

-  = prior work
-  = new to this work
-  = unsolved



## Other Results

No threshold!

Pairings  $\rightarrow (N^{1-a}, 1, N^a) \quad \forall a \in [\frac{1}{2}, 1]$  w/ Broadcast

Compare w/ [Boneh-Water'06]: Pairings  $\rightarrow (N^{\frac{1}{2}}, N^{\frac{1}{2}}, N^{\frac{1}{2}})$

Pairings  $\rightarrow (N^{1-a}, N^{1-a}, N^a) \quad \forall a \in [0, 1]$  w/ Broadcast

Compare w/ [Goyal-Quach-Waters-Wichs'19] : Pairings + LWE  $\rightarrow (N, N^2, N^\epsilon)$

## Other Results

$$\text{PKE} \rightarrow (N^{2-a}, N^{2-2a}, N^a) \quad \forall a \in [0,1]$$

$$\text{IBE} \rightarrow (1, N^{2-2a}, N^a) \quad \forall a \in [0,1]$$

No threshold!

$$a=0 \rightarrow |\text{ctx}| = O(1)$$

$$a=2/3 \rightarrow |\text{sk}| = |\text{ctx}| = O(N^{2/3})$$

First fully sub-linear schemes from pairing-free groups or factoring-like assumptions  
[Cocks'01, Döttling-Garg'17]



# Techniques

Generically remove thresholds w/o asymptotically changing  $(P,K,C)$

$\downarrow P, K \Rightarrow \uparrow C$

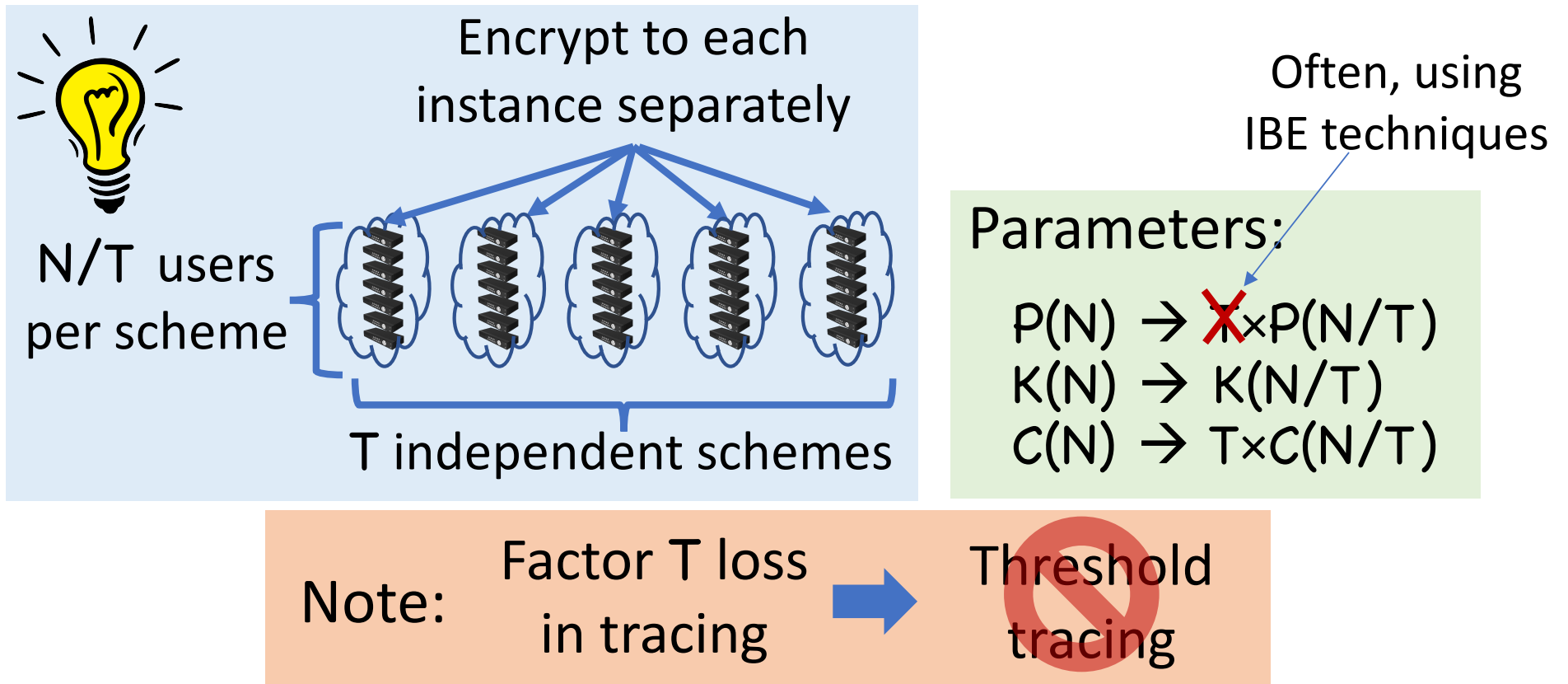
“risky”  $\Rightarrow$  no risky ( $\uparrow K$ )

Threshold\* Broadcast  $\Rightarrow$  traitor tracing

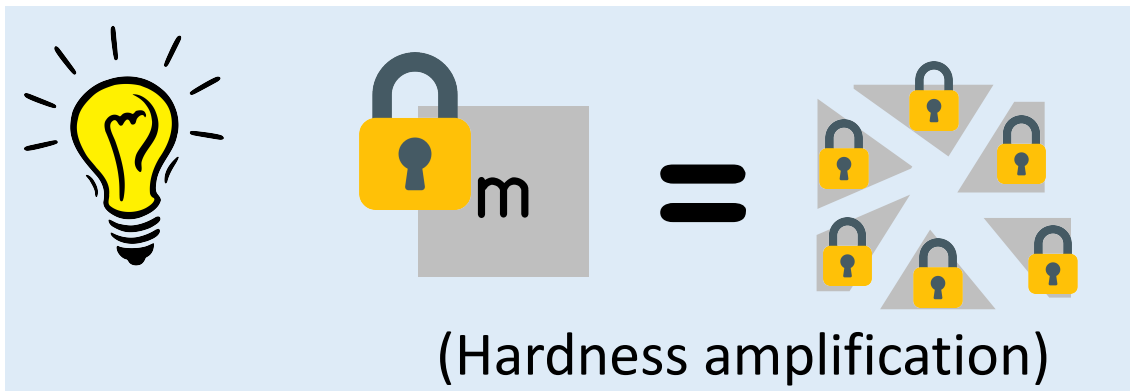
New algebraic instantiations from pairings

\* Not to be confused w/ threshold tracing

# Trading off $\mathcal{C}$ for $\mathcal{P}, \mathcal{K}$ : Generalizing Trivial PLBE



# Removing Thresholds



Key feature: #(shares)  
independent of  $N$

Parameters:

$P(N) \rightarrow P(N)$

$K(N) \rightarrow K(N)$

$C(N) \rightarrow C(N)$

Already enough for PKE/IBE results

# Mitigating Risk

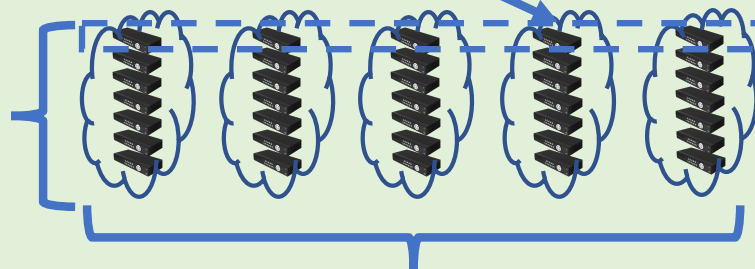
$\alpha$ -Risky Tracing:  $\Pr[\text{false positive}] \leq \text{negl}$   
[Goyal-Koppula-Russel-Waters'17]  $\Pr[\text{false negative}] \leq 1-\alpha$



Encrypt to  
\*random\* instance  
\$

Pairings  $\rightarrow$  (1/N)-risky,  
size (1,1,1)

N users  
per scheme

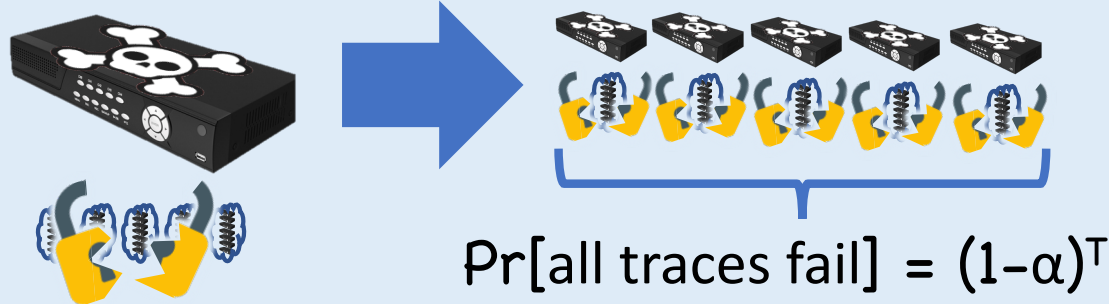


$sk_i = (sk_{j,i})_j$

T independent schemes

# Mitigating Risk

Tracing:



IBE techniques

Parameters:

$$P(N) \rightarrow \alpha^{-1} \times P(N)$$

$$K(N) \rightarrow \alpha^{-1} \times K(N)$$

$$C(N) \rightarrow C(N)$$

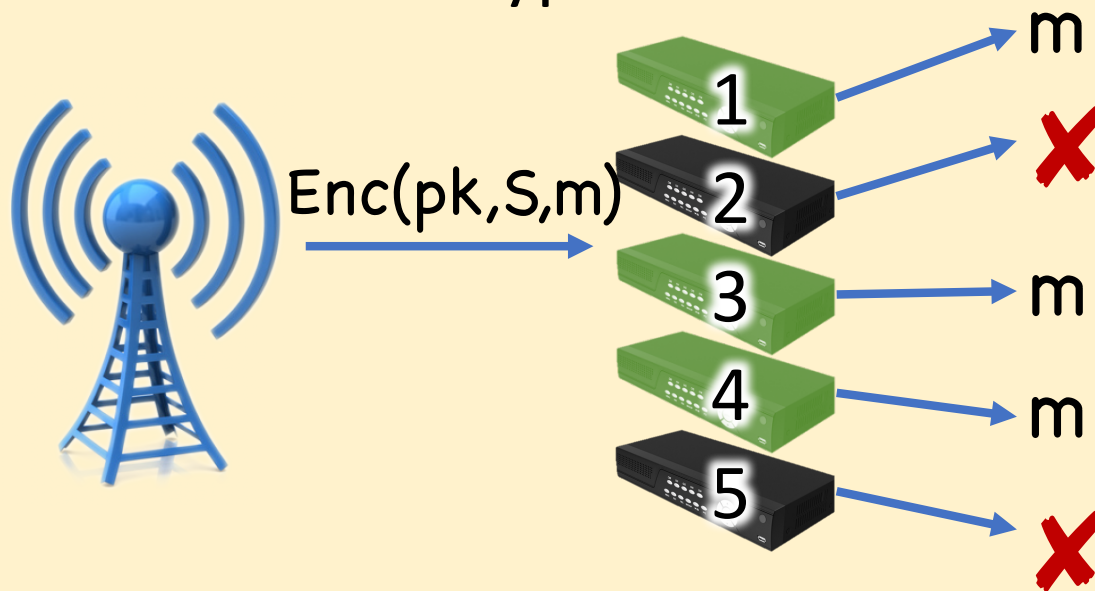
Note: Require  $\Pr[\text{hands}] \geq 0.9$  → Only threshold scheme

Then apply threshold elimination

Enough for  
(1,N,1)

# Threshold\* Broadcast $\rightarrow$ Traitor Tracing

Broadcast Encryption:



Can encrypt to any subset of users

Like PLBE, except:  
(1) Arbitrary  $S$   
(2)  $S$  public

\* Not to be confused w/ threshold tracing

# Threshold\* Broadcast $\rightarrow$ Traitor Tracing



How to encrypt to \*secret\* sets, when  $S$  is public?



Assign users (semi-)random identities  
(Only user/tracer knows their identity)

Problem: can “guess” user identity

Solution: generalize to threshold functionality

\* Not to be confused w/ threshold tracing

# Putting It All Together

[Attrapadung-Herranz-Laguillaumie-  
Libert-Panafieu-Ràfols'12]:

(N,N,1) Threshold Broadcast

Optimize for  
tracing app

Combine w/  
"risky" tracing

Apply  
compilers

$(N^{\frac{1}{3}}, N^{\frac{1}{3}}, N^{\frac{1}{3}})$   
Tracing



## Lessons Learned

PLBE \*not\* inherent  
to traitor tracing

Thresholds no  
longer limitation

Risky and threshold tracing  
useful stepping stones