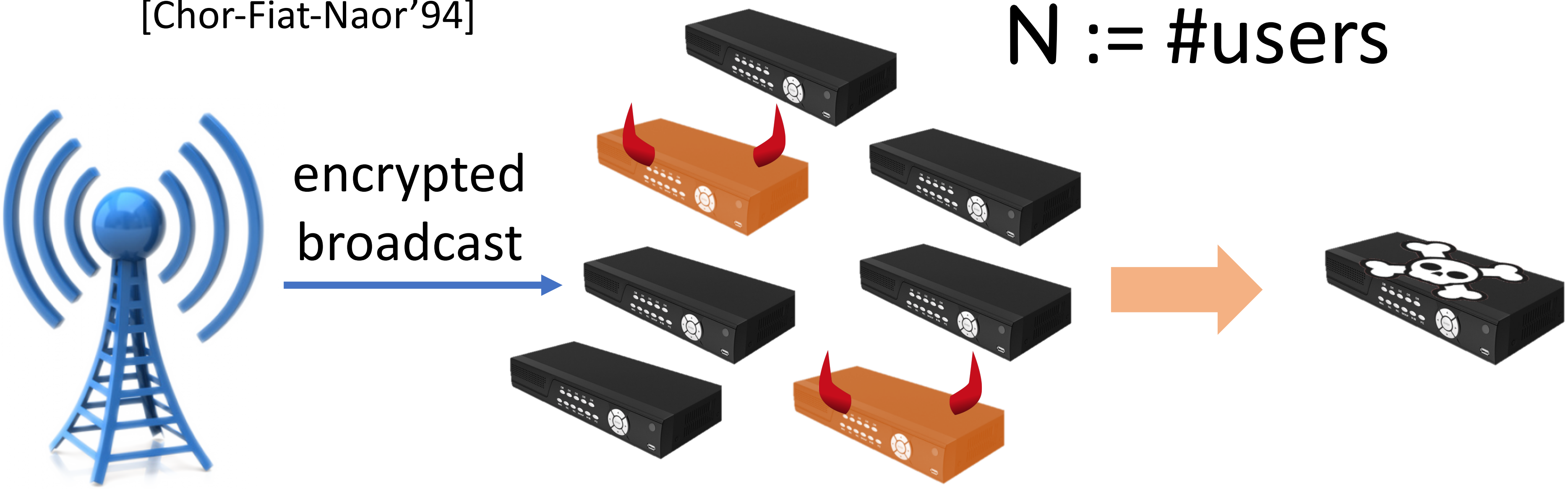
New Techniques for Traitor Tracing:

Size $N^{1/3}$ and More from Pairings

Mark Zhandry (Princeton & NTT Research)

Traitor Tracing

[Chor-Fiat-Naor'94]



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 ➡ |ctxt| = $O(1)$

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[decrypt] $\geq$ 0.9)

Problem 2:

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

➡ 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

$$(P,\ K,\ C) = \begin{array}{l} |PP| = P(N) \times \text{poly}(\lambda) \\ |sk| = K(N) \times \text{poly}(\lambda) \\ |ctxt| = C(N) \times \text{poly}(\lambda) \end{array}$$

Trivial:

PKE → (N,1,N)

IBE → (1,1,N)

Boneh-Naor'02:

PKE → $(N^2,N^2,1)$

IBE → $(1,N^2,1)$

Threshold

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

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

Goyal-Koppula-Waters'18: LWE → (1,1,1)

Some Previously Open Questions

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

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

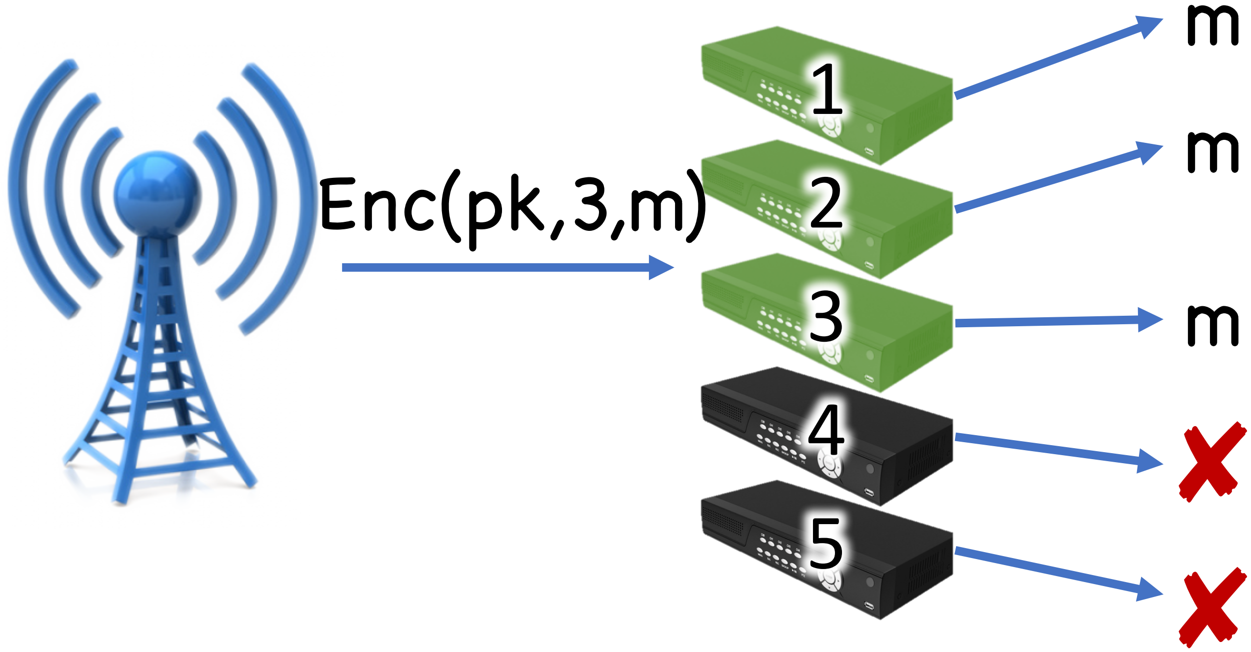
Anything but
LWE/iO → $(*,*,N^{0.49})$?
w/o threshold

Observation

(no threshold **or** fully sublinear)

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

Private Linear Broadcast Encryption (PLBE)

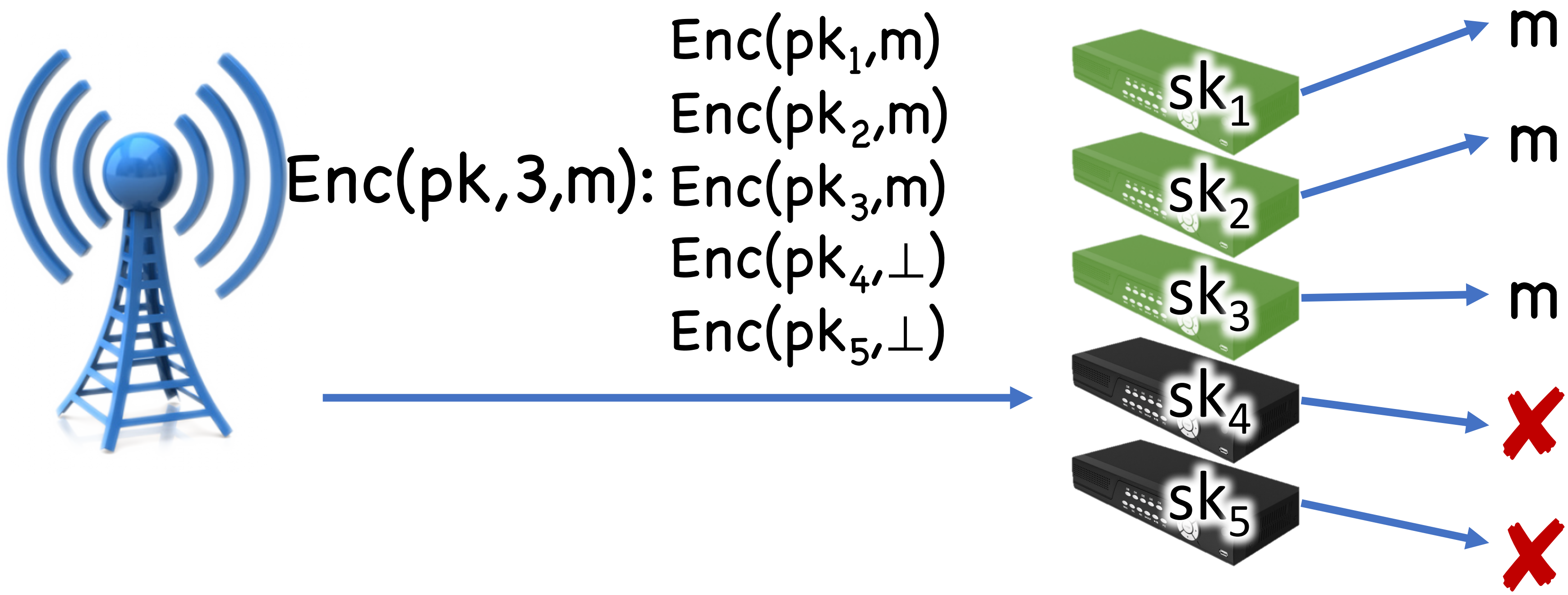


Can encrypt to users ≤ j, for any j

Plus: User i learns nothing about j, except whether i≤j

Thm ([Boneh-Sahai-Waters'06]): PLBE → Traitor Tracing

Trivial PLBE



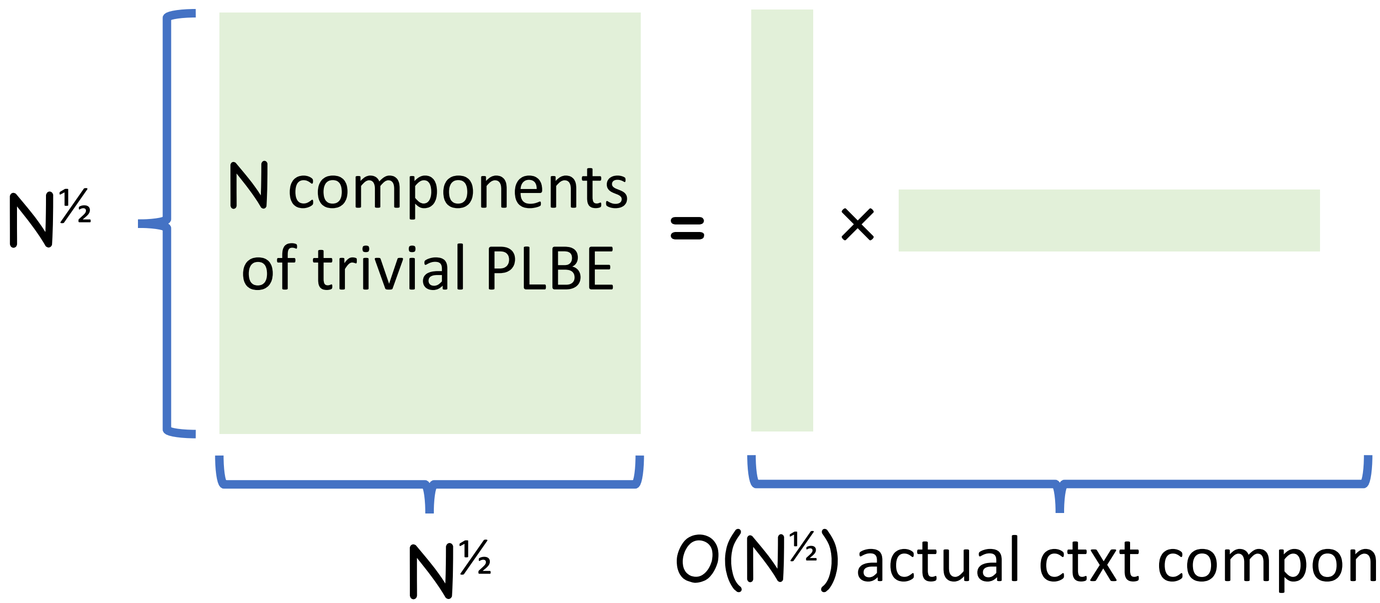
PLBE-Based Traitor Tracing

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

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

The $N^{½}$ Barrier for Pairings

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



$N^{½}$ = best known PLBE from pairings

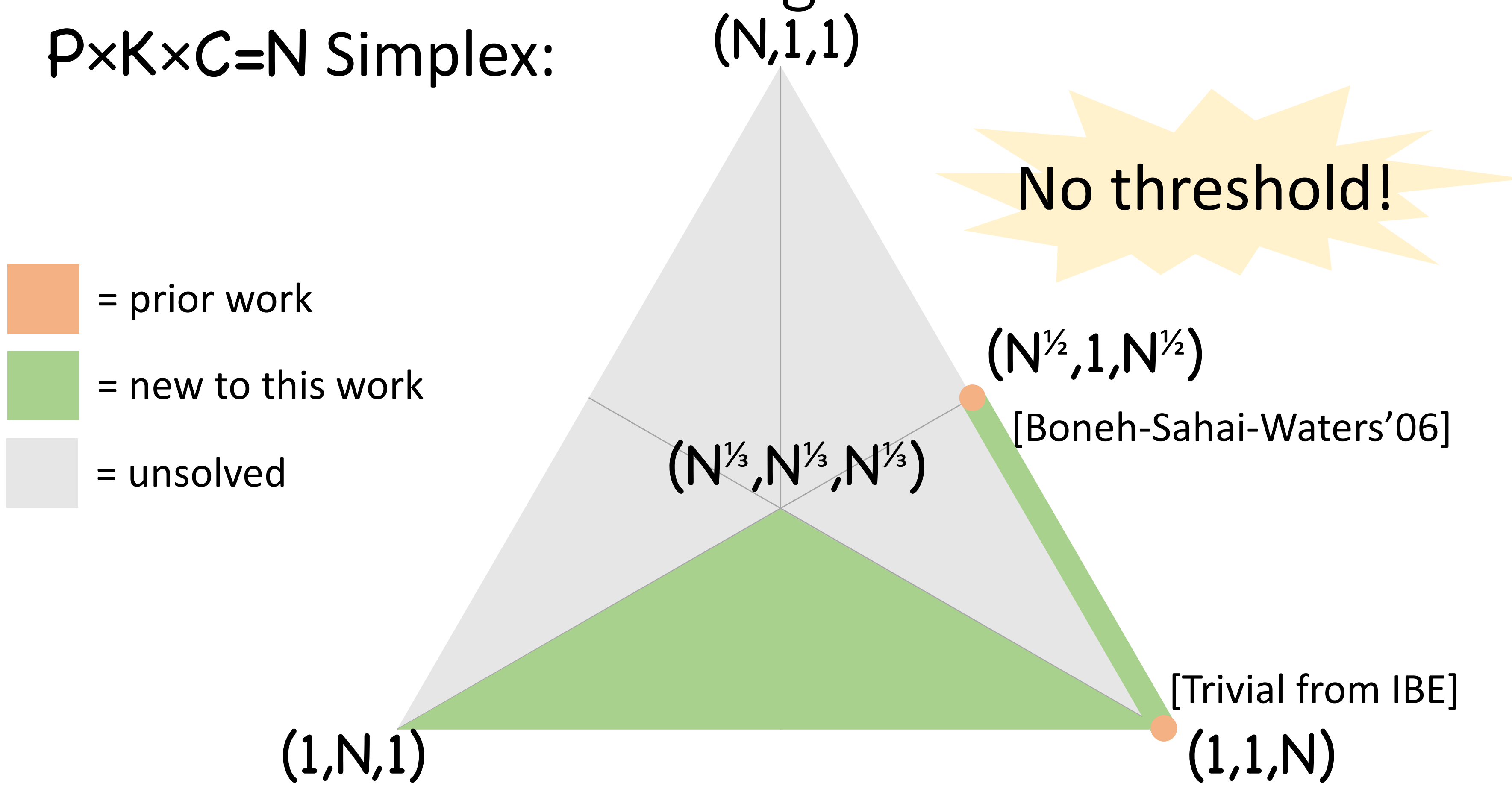
This Work: New techniques for (collusion-resistant) traitor tracing

⬇

New parameter trade-offs from pairings and other primitives

Parameters from Pairings

P×K×C=N Simplex:



Other Results

No threshold!

Pairings ➡ $(N^{1-a}, 1, N^{a})$ $\forall a \in [½, 1]$ w/ Broadcast

Compare w/ [Boneh-Water'06]: Pairings → $(N^{½}, N^{½}, N^{½})$

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

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

Other Results

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

No threshold!

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

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

$a=0 \rightarrow |ctxt| = O(1)$

$a=⅔ \rightarrow |sk|=|ctxt|=O(N^{⅔})$

Techniques

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

↓P,K ➡ ↑C

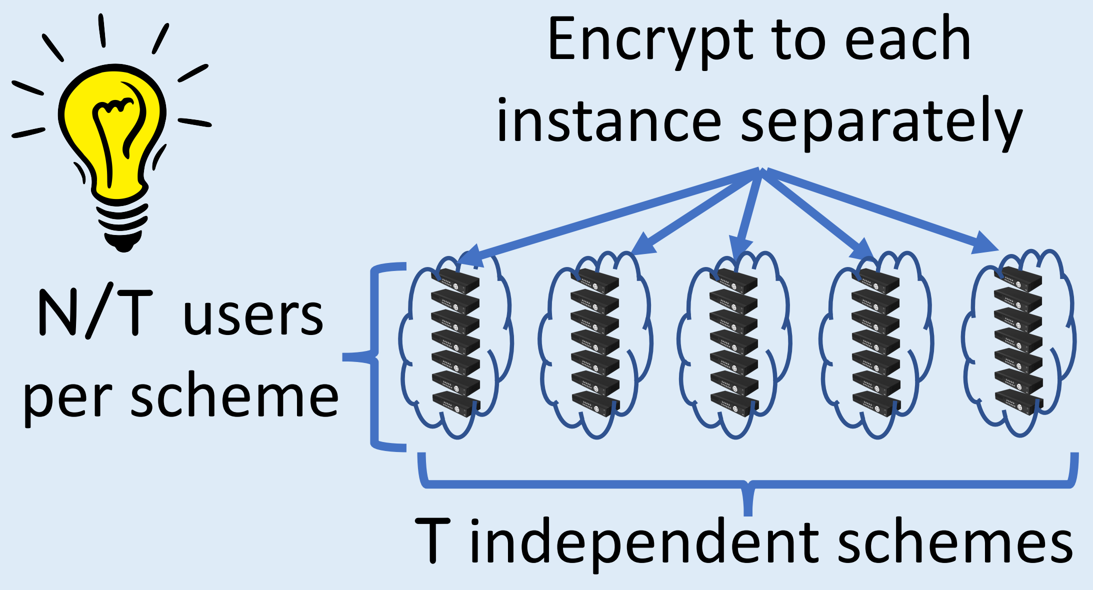
"risky" ➡ no risky (↑K)

Threshold* Broadcast ➡ traitor tracing

New algebraic instantiations from pairings

* Not to be confused w/ threshold tracing

Trading off C for P,K: Generalizing Trivial PLBE



Often, using IBE techniques

Parameters:

P(N) → ~~T~~×P(N/T)
K(N) → K(N/T)
C(N) → T×C(N/T)

Note: Factor T loss in tracing ➡ ~~Threshold tracing~~

Removing Thresholds

(Hardness amplification)

Key feature: #(shares) independent of N

Parameters:

P(N) → P(N)
K(N) → K(N)
C(N) → C(N)

Already enough for PKE/IBE results

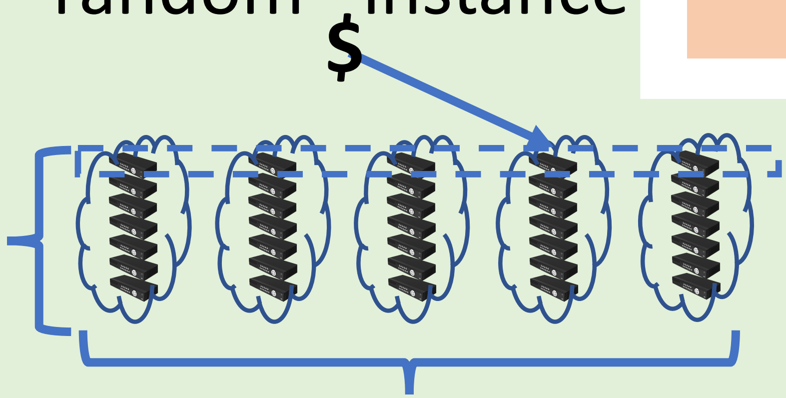
Mitigating Risk

α-Risky Tracing:
[Goyal-Koppula-Russel-Waters'17]

Pr[false positive] ≤ negl
Pr[false negative] ≤ 1−α

Pairings → (1/N)-risky, size (1,1,1)

Encrypt to *random* instance



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

N users per scheme

T independent schemes

Mitigating Risk

Tracing:

$Pr[\text{all traces fail}] = (1-\alpha)^T$

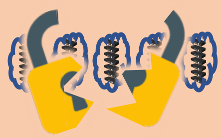
IBE techniques

Parameters:

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

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

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

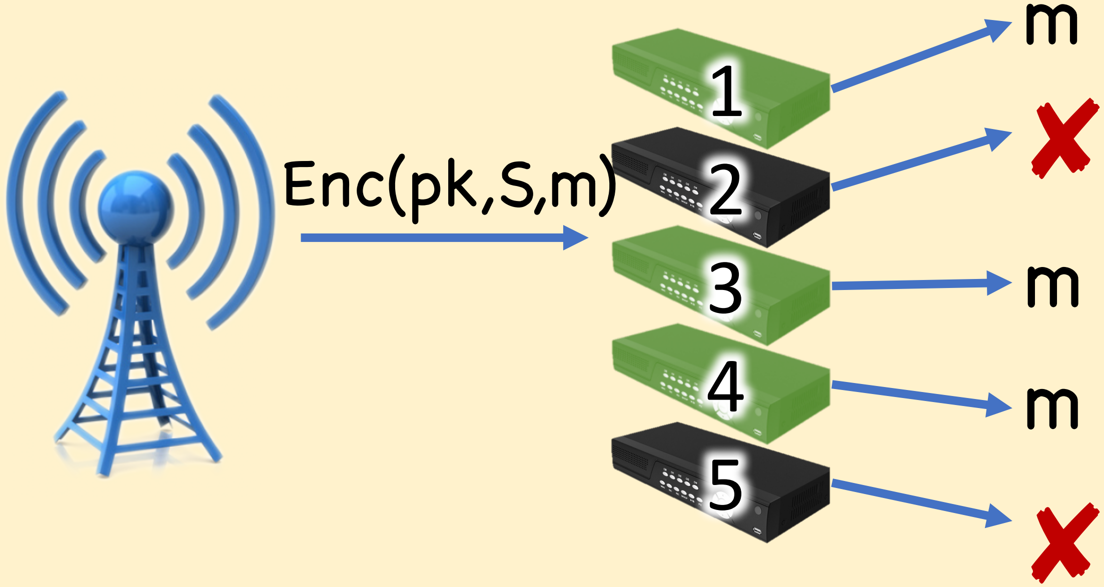
Note: Require Pr[] ≥ 0.9 → Only threshold scheme

Then apply threshold elimination

Enough for (1,N,1)

Threshold* Broadcast → 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 → 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

$(N^{1/3}, N^{1/3}, N^{1/3})$ Tracing

Lessons Learned

PLBE *not* inherent to traitor tracing

Thresholds no longer limitation

Risky and threshold tracing useful stepping stones