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

Mark Zhandry (Princeton & NTT Research)
Traitor Tracing

[Chor-Fiat-Naor’94]

N := #users

encrypted broadcast

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?

“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:
\[ PKE \rightarrow |\text{ctxt}| = O(1) \]

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 \( \Pr[\text{decrypt}] \geq 0.9 \))

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

$$(P, K, C) =$$

\[
|PP| = P(N) \times \text{poly}(\lambda) \\
|sk| = K(N) \times \text{poly}(\lambda) \\
|ctxt| = C(N) \times \text{poly}(\lambda)
\]

Trivial:
- PKE $\rightarrow (N, 1, N)$
- IBE $\rightarrow (1, 1, N)$

Boneh-Naor’02:
- PKE $\rightarrow (N^2, N^2, 1)$
- IBE $\rightarrow (1, N^2, 1)$

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 $\rightarrow (1, 1, 1)$

Threshold
Some Previously Open Questions

PKE, IBE,
Pairing-free groups, \rightarrow (\ast, N^{1.99}, N^{0.99})? \hspace{1cm} (even w/ threshold tracing)
or Factoring-like

Pairings \rightarrow (\ast, N^{1.99}, N^{0.49})? \hspace{1cm} (even w/ threshold tracing)

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

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

(no threshold or fully sublinear)
Private Linear Broadcast Encryption (PLBE)

Enc(pk, 3, m)

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

Enc(pk, 3, m):

- Enc(pk_1, m)
- Enc(pk_2, m)
- Enc(pk_3, m)
- Enc(pk_4, ⊥)
- Enc(pk_5, ⊥)

m
m
m

✘
✘
PLBE-Based Traitor Tracing

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

All the “best” traitor tracing schemes = improved algebraic constructions of PLBE
The $N^{\frac{1}{2}}$ Barrier for Pairings

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

$$N^{\frac{1}{2}} \quad \text{N components of trivial PLBE}$$

$$\times$$

$$O(N^{\frac{1}{2}}) \quad \text{actual ctxt components}$$

$$N^{\frac{1}{2}} = \text{best known PLBE from pairings}$$
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:

- $(N,1,1)$
- $(N^{\frac{1}{3}},N^{\frac{1}{3}},N^{\frac{1}{3}})$
- $(N^{\frac{1}{2}},1,N^{\frac{1}{2}})$
- $(1,N,1)$
- $(1,1,N)$

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

- $\times \times \times$ = prior work
- $\times \times$ = new to this work
- $\times$ = unsolved

No threshold!
Other Results

Pairings $\Rightarrow (N^{1-a},1,N^a) \quad \forall a \in \left[\frac{1}{2},1\right]$ 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 $\Rightarrow (N,N^2,N^\epsilon)$

No threshold!
Other Results

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

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

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

\( a=\frac{2}{3} \rightarrow |\text{sk}| = |\text{ctxt}| = O(N^{\frac{2}{3}}) \)

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 $C$ for $P,K$: Generalizing Trivial PLBE

Parameters:
- $P(N) \rightarrow X \times P(N/T)$
- $K(N) \rightarrow K(N/T)$
- $C(N) \rightarrow T \times C(N/T)$

Note: Factor $T$ loss in tracing $\rightarrow$ Threshold tracing

Often, using IBE techniques

Encrypt to each instance separately

$N/T$ users per scheme

$T$ independent schemes
Removing Thresholds

Key feature: #(shares) independent of N

Parameters:
- $P(N) \rightarrow P(N)$
- $K(N) \rightarrow K(N)$
- $C(N) \rightarrow C(N)$

(Hardness amplification)

Already enough for PKE/IBE results
Mitigating Risk

\[ \Pr[\text{false positive}] \leq \negl \]
\[ \Pr[\text{false negative}] \leq 1 - \alpha \]

\( \alpha \)-Risky Tracing: \quad \text{[Goyal-Koppula-Russel-Waters’17]}

Encrypt to *random* instance

\[ \text{Pairings} \rightarrow (1/N) \text{-risky, size (1,1,1)} \]

\( N \) users per scheme

\( T \) independent schemes

\[ \text{sk}_i = (\text{sk}_{j,i})_j \]
Mitigating Risk

Tracing:

Pr[all traces fail] = (1-\alpha)^T

Parameters:

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

Note:

Pr[] \geq 0.9

Then apply threshold elimination

Only threshold scheme

Enough for (1,N,1)

IBE techniques
Threshold* Broadcast ➔ Traitor Tracing

Broadcast Encryption:

Can encrypt to any subset of users

- Enc(pk,S,m)

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

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

Optimize for tracing app

Combine w/ “risky” tracing

Apply compilers
Lessons Learned

PLBE *not* inherent to traitor tracing

Thresholds no longer limitation

Risky and threshold tracing useful stepping stones