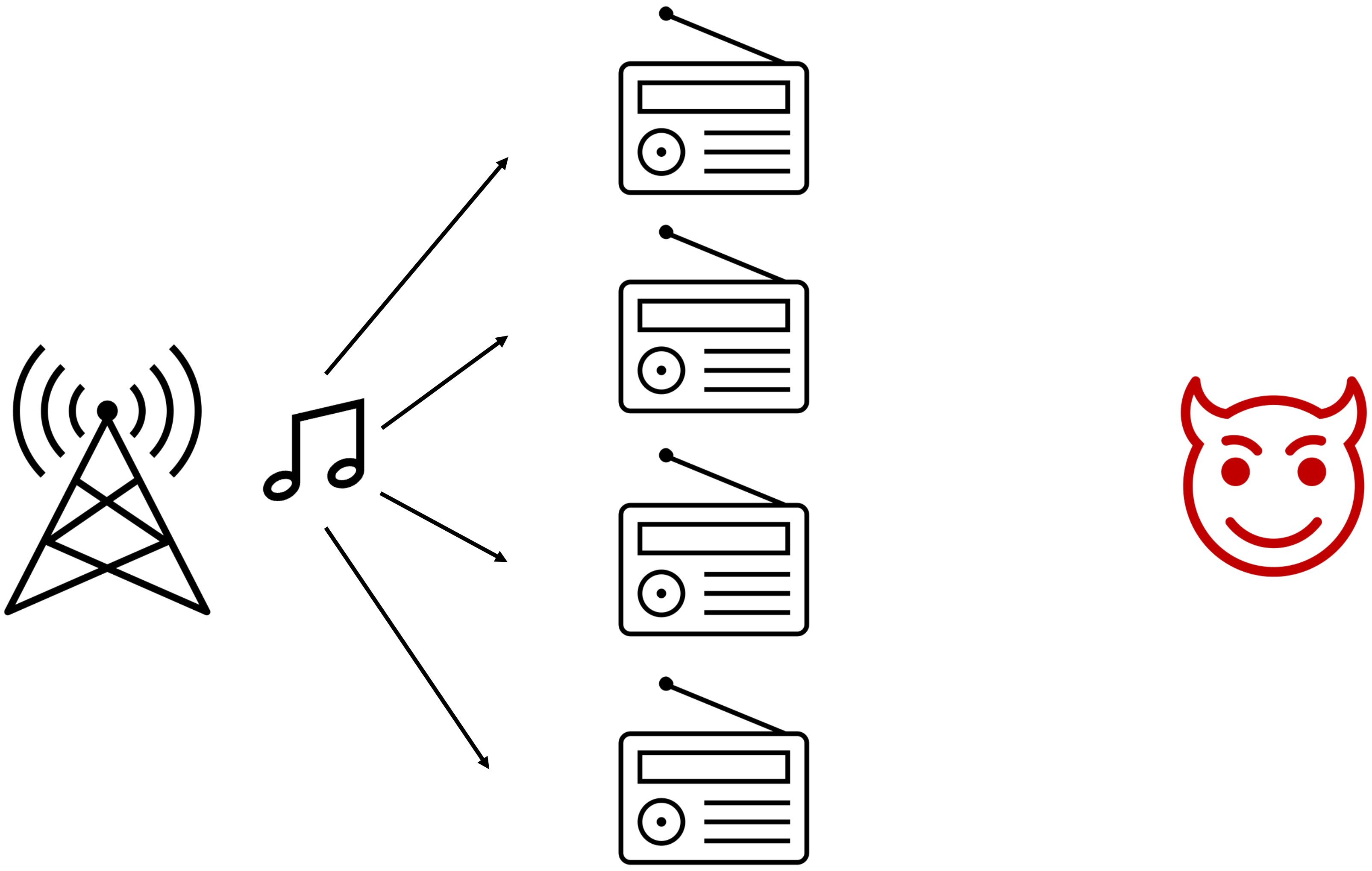
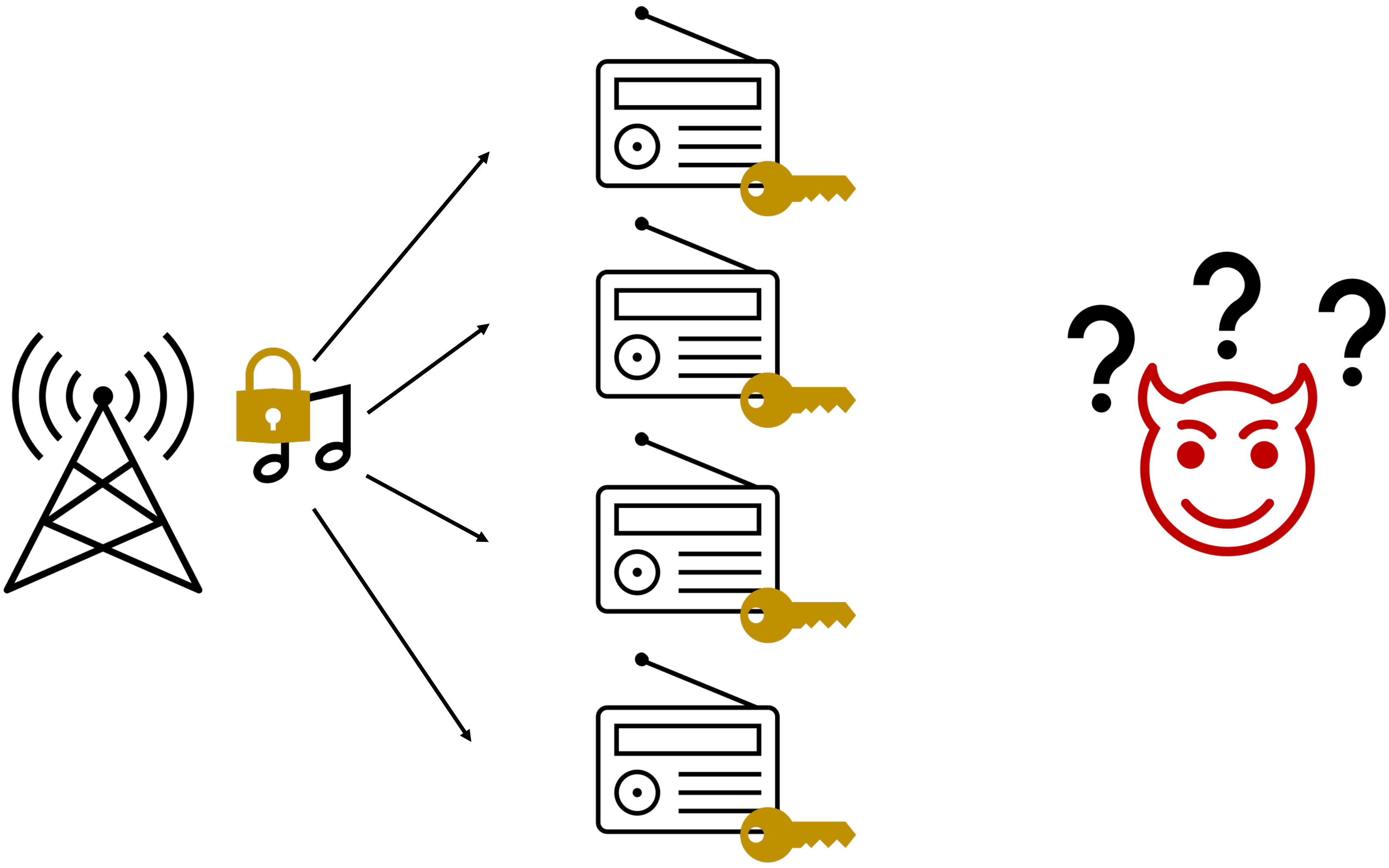
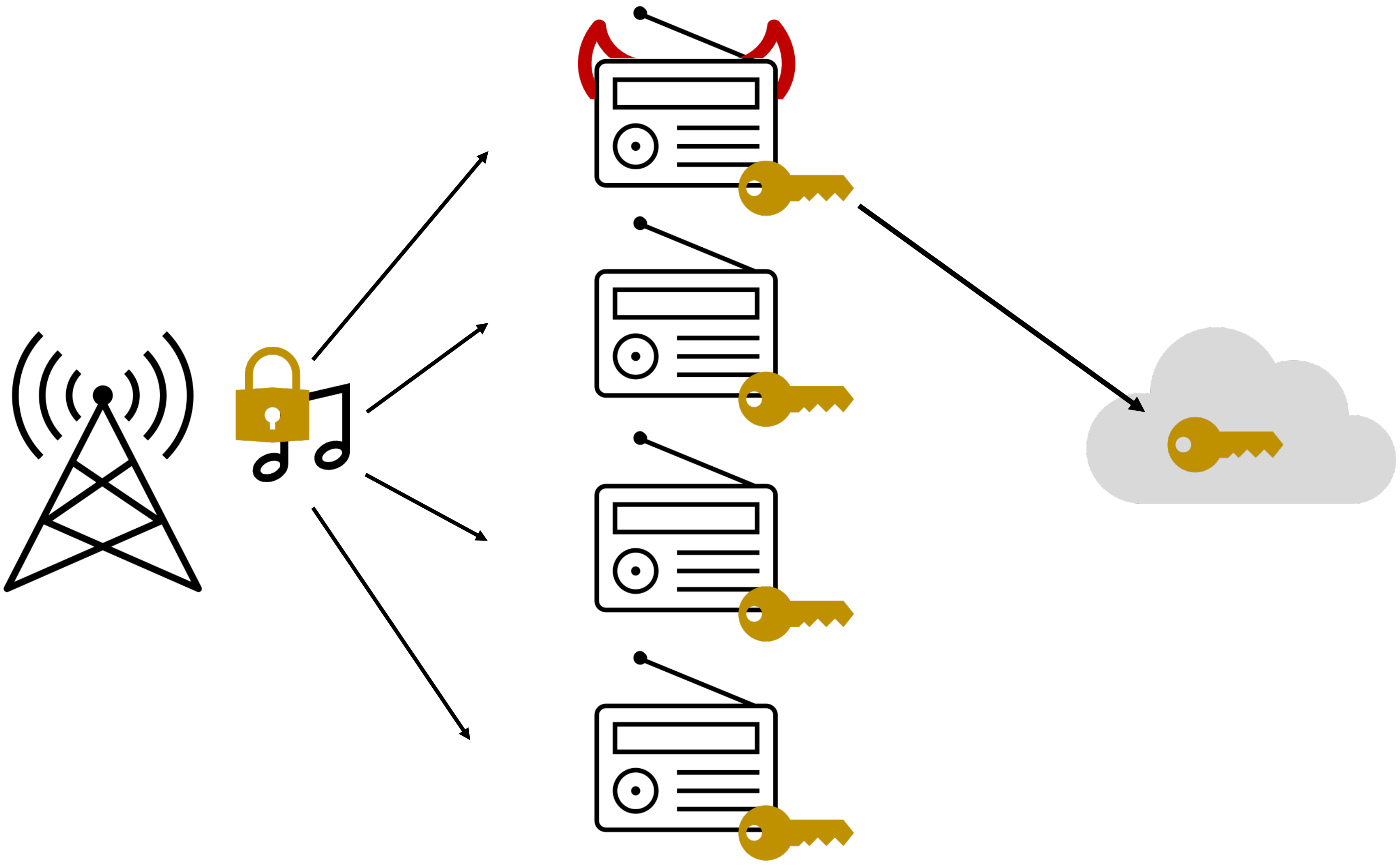
Optimal Traitor Tracing from Pairings

Mark Zhandry
NTT Research







Traitor Tracing [Chor-Fiat-Naor-Pinkas’94]:
Identify “traitor” who leaked key

Major Goal in Cryptography:

Traitor tracing with small ciphertexts, decryption keys

Want successful tracing even if:

- Multiple traitors collude
- Leaked key embedded in obfuscated decoder program

What is known?

	Max (|ctxt| , |decr key|)	Tool
[Chor-Fiat-Naor-Pinkas'94]	N	Generic Enc
[Boneh-Naor'02, Billet-Phan'08, Z'20]	$N^{2/3}$	Generic Enc

Notes:

- Only showing collusion-resistant schemes
- Can sometimes trade-off between parameter sizes
- Sizes ignore polynomial terms in security parameter
- \| encr key \| also important

What is known?

	Max (|ctxt| , |decr key|)	Tool
[Chor-Fiat-Naor-Pinkas’94]	N	Generic Enc
[Boneh-Naor’02, Billet-Phan’08, Z’20]	$N^{2/3}$	Generic Enc
[Boneh-Sahai-Waters’06]	$N^{1/2}$	Pairings
[Z’20, Gong-Luo-Wee’23]	$N^{1/3}$	Pairings

Notes:

- Only showing collusion-resistant schemes
- Can sometimes trade-off between parameter sizes
- Sizes ignore polynomial terms in security parameter
- | encr key | also important

What is known?

	Max (|ctxt| , |decr key|)	Tool
[Chor-Fiat-Naor-Pinkas'94]	N	Generic Enc
[Boneh-Naor'02, Billet-Phan'08, Z'20]	$N^{2/3}$	Generic Enc
[Boneh-Sahai-Waters'06]	$N^{1/2}$	Pairings
[Z'20, Gong-Luo-Wee'23]	$N^{1/3}$	Pairings
[Garg-Gentry-Halevi-Raykova-Sahao-Waters'13, Boneh-Z'14]	1	Obfuscation
[Goyal-Koppula-Waters'18]	1	Lattices

Notes:

- Only showing collusion-resistant schemes
- Can sometimes trade-off between parameter sizes
- Sizes ignore polynomial terms in security parameter
- | encr key | also important

What is known?

	Max (|ctxt| , |decr key|)	Tool
[Chor-Fiat-Naor-Pinkas'94]	N	Generic Enc
[Boneh-Naor'02, Billet-Phan'08, Z'20]	$N^{2/3}$	Generic Enc
[Boneh-Sahai-Waters'06]	$N^{1/2}$	Pairings
[Z'20, Gong-Luo-Wee'23]	$N^{1/3}$	Pairings
This work	1	**Pairings**
[Garg-Gentry-Halevi-Raykova-Sahao-Waters'13, Boneh-Z'14]	1	Obfuscation
[Goyal-Koppula-Waters'18]	1	Lattices

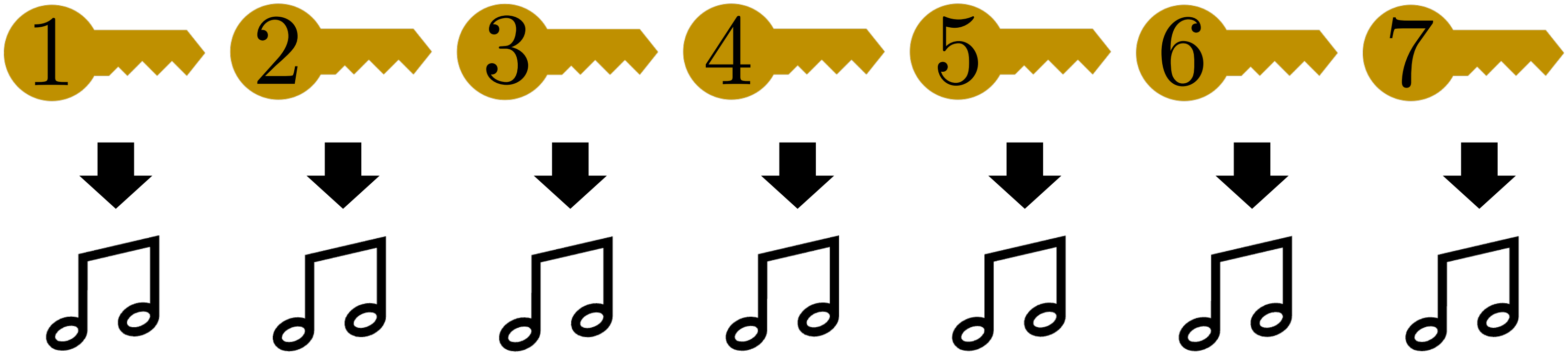
Traitor Tracing Background

The Private Linear Broadcast Approach

[Boneh-Sahai-Waters'06]

Publicly generated "normal" ciphertexts:

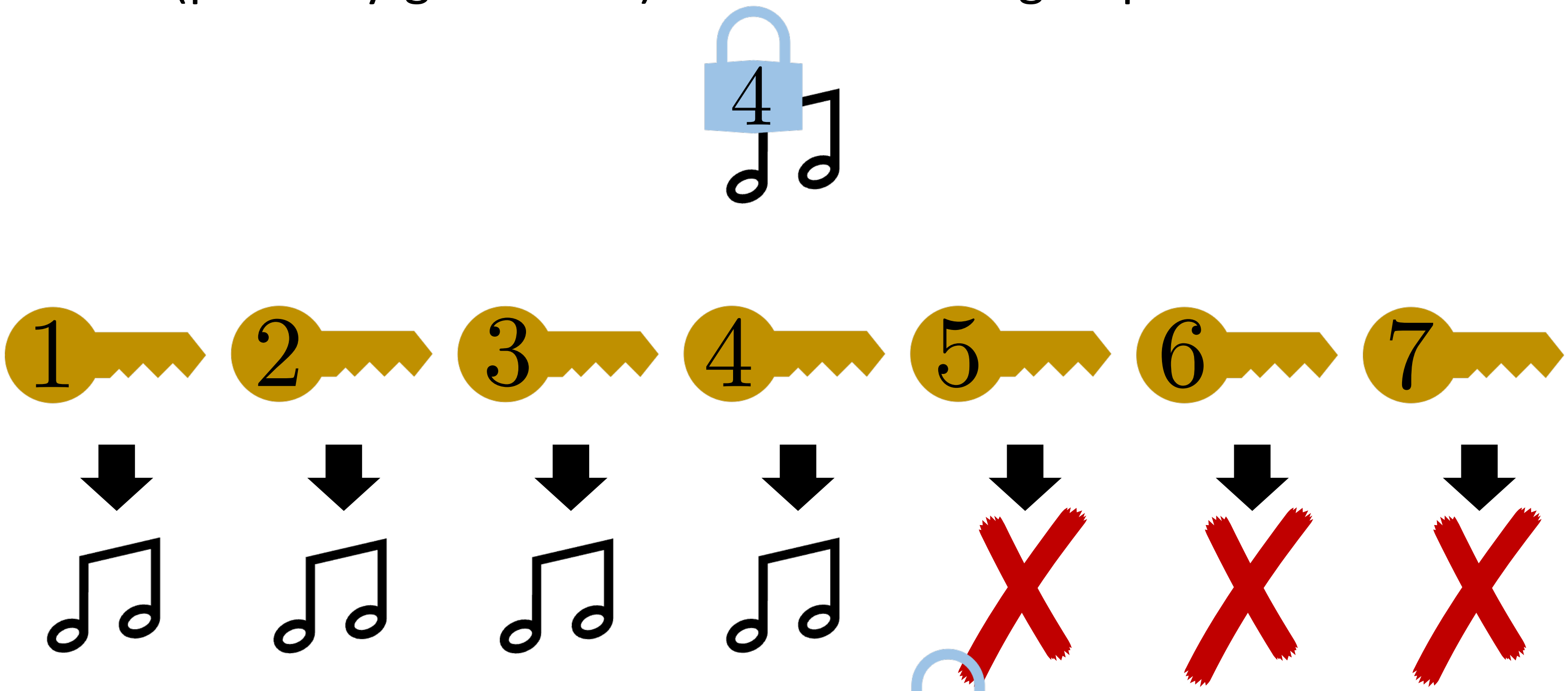
N secret keys, indexed by user #:



All secret keys decrypt normal ciphertexts

The Private Linear Broadcast Approach

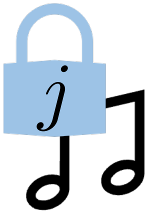
(privately-generated) indexed "tracing" ciphertexts:

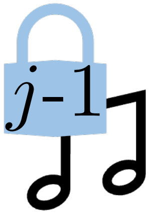


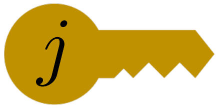
Message-hiding: i decrypts j if and only if $i \leq j$

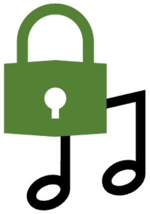
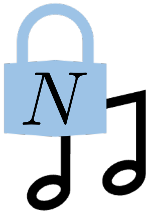
The Private Linear Broadcast Approach

Two additional requirements

Index-hiding: 

$\approx_C$ 

unless you possess 

Normal-hiding:  $\approx_C$ 

even with all the keys

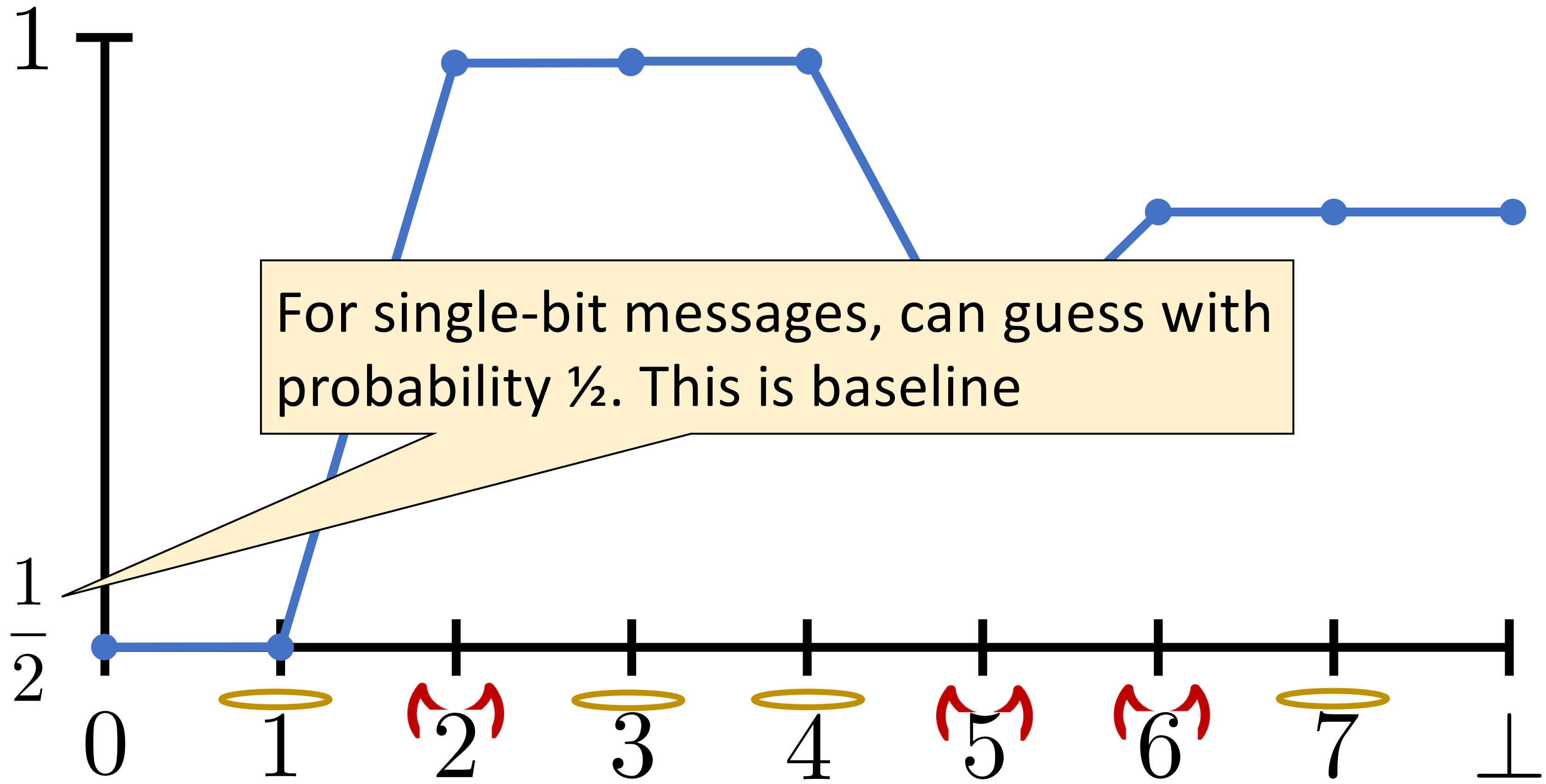
The Private Linear Broadcast Approach

Trace(📻) :

Define $p_j = \Pr[$ 📻 decrypts 🔒 j ♫ $]$

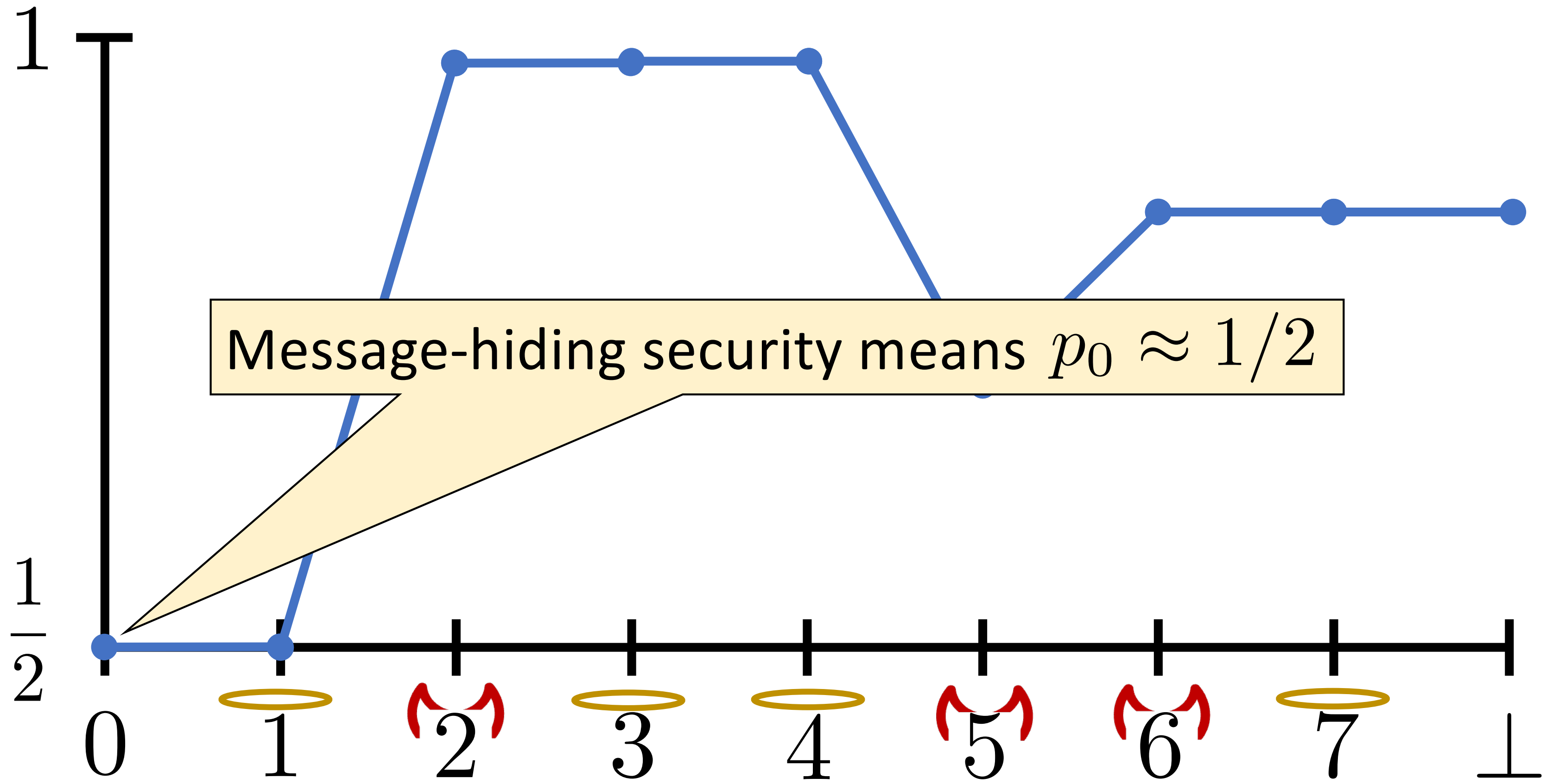
$p_\perp = \Pr[$ 📻 decrypts 🔒♫ $]$

The Private Linear Broadcast Approach



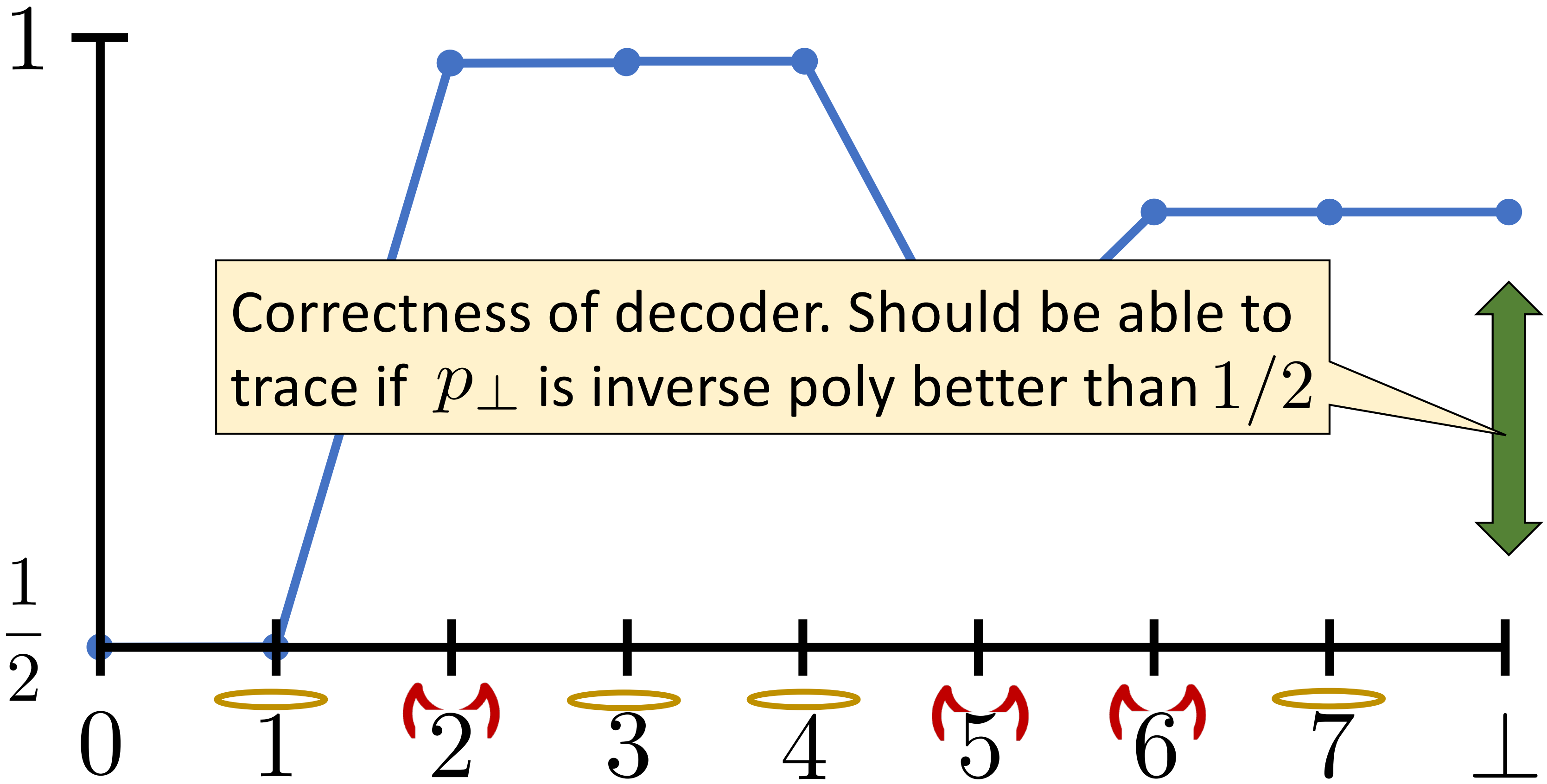
For single-bit messages, can guess with probability ½. This is baseline

The Private Linear Broadcast Approach



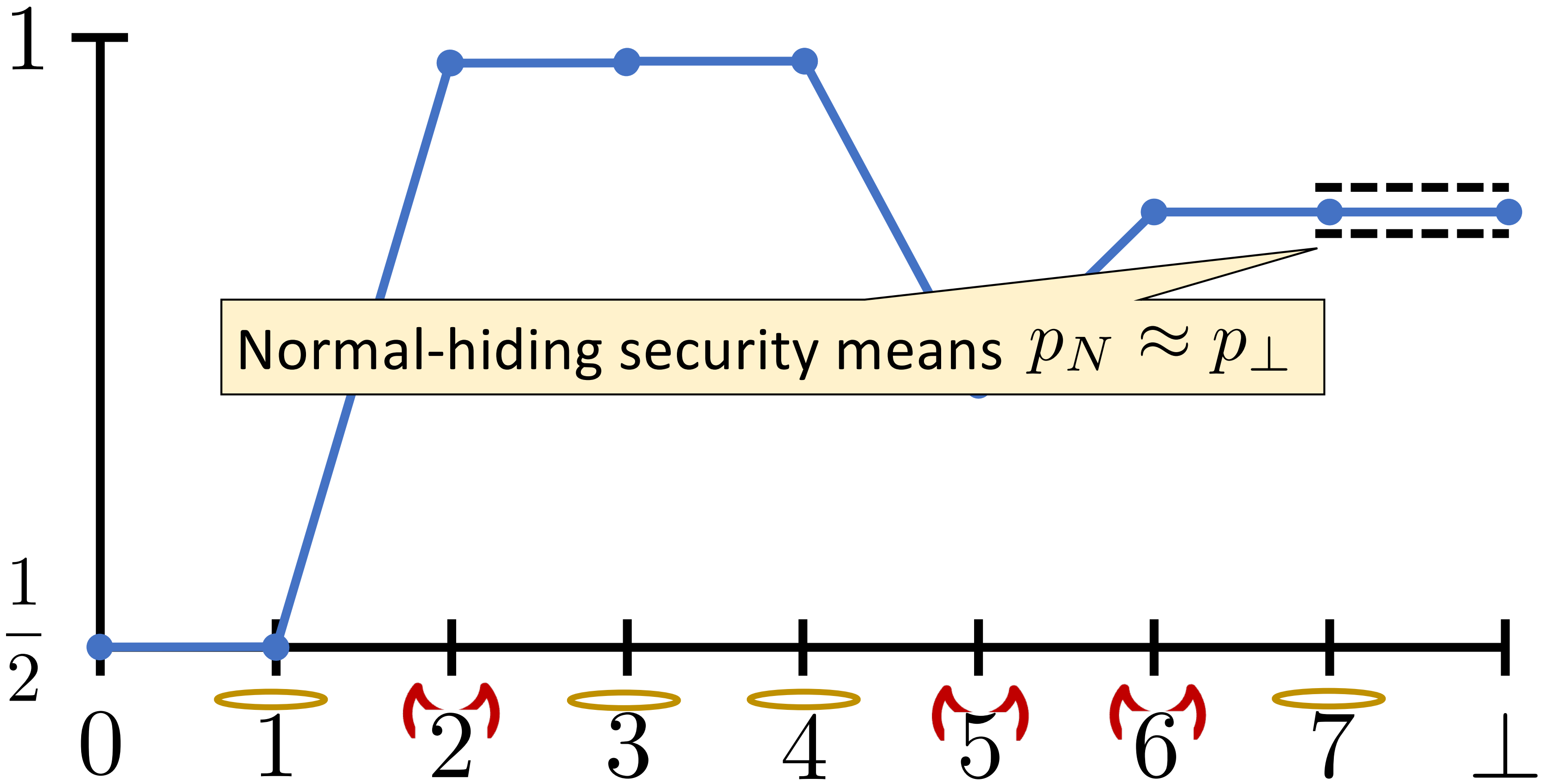
Message-hiding security means $p_0 \approx 1/2$

The Private Linear Broadcast Approach



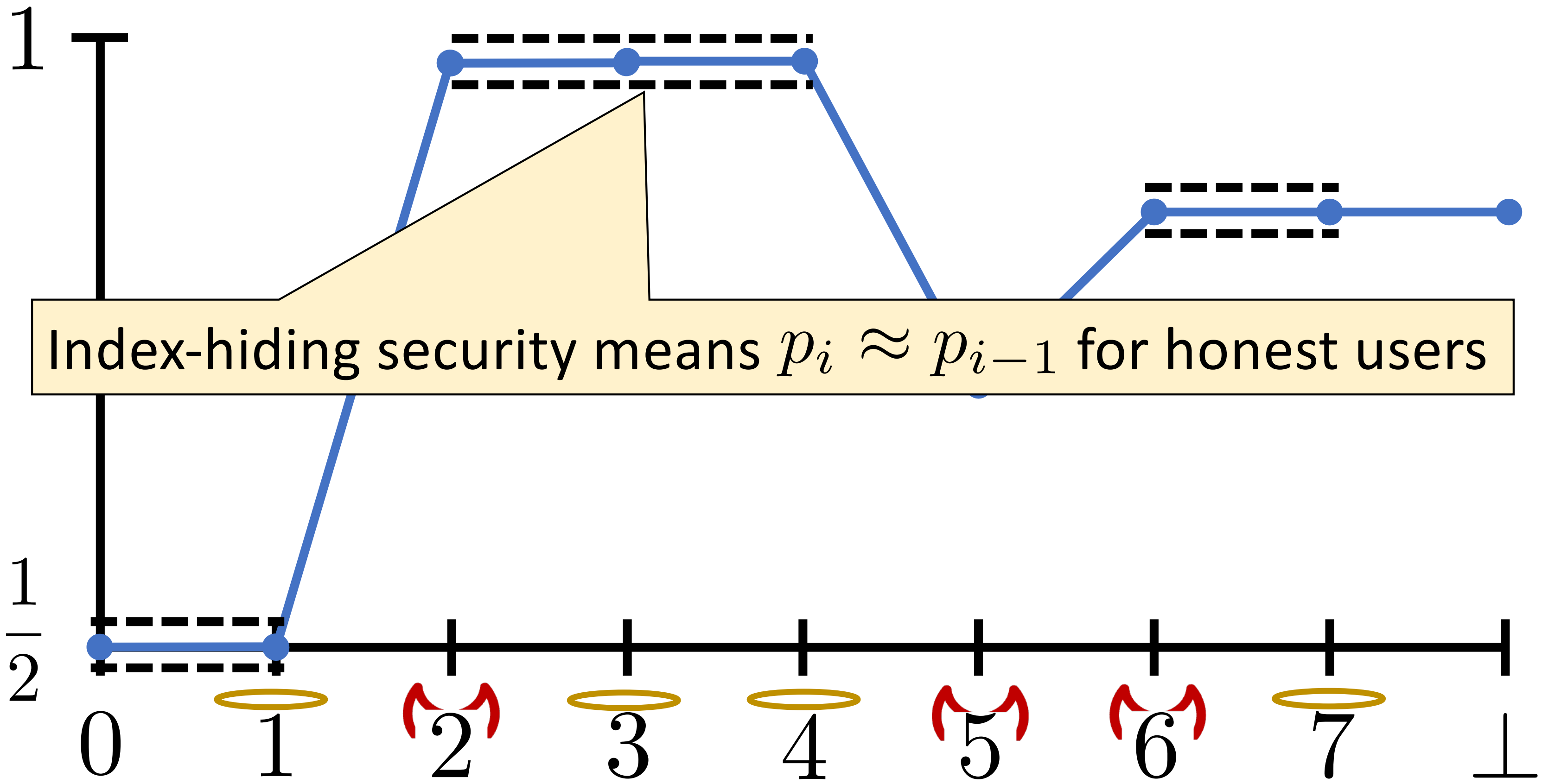
Correctness of decoder. Should be able to trace if $p_\perp$ is inverse poly better than $1/2$

The Private Linear Broadcast Approach



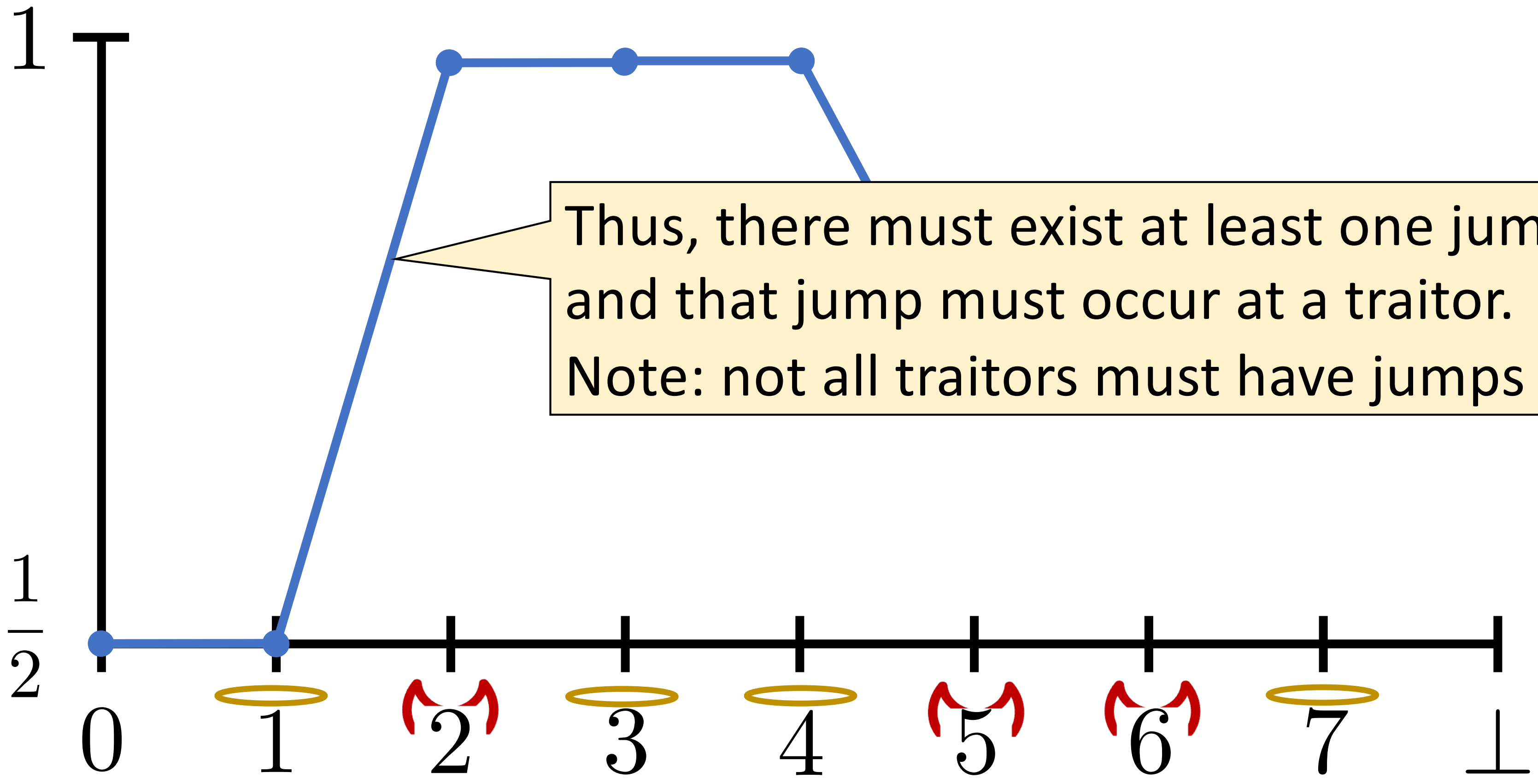
Normal-hiding security means $p_N \approx p_\perp$

The Private Linear Broadcast Approach



Index-hiding security means $p_i \approx p_{i-1}$ for honest users

The Private Linear Broadcast Approach



Thus, there must exist at least one jump, and that jump must occur at a traitor.
Note: not all traitors must have jumps

Theorem [Boneh-Sahai-Waters'06, Goyal-Koppula-Waters'18]:

♫ empty

Decryption just indicates ✓ or ✗

2-ctxt normal-hiding

Traitor tracing

Theorem [Goyal-Koppula-Waters'18]

Message-less PLBE w/

From lattices [Goyal-Koppula-Waters'18]

2-ctxt index-hiding
2-ctxt normal-hiding

Plain PLBE w/

2-ctxt message-hiding
2-ctxt index-hiding
2-ctxt normal-hiding

+ ABE for circuits

From lattices [Gorbunov-Vaikuntanathan-Wee'13]

Theorem [Boneh-Sahai-Waters'06, Goyal-Koppula-Waters'18]:

2-ctxt message-hiding
$+$ 2-ctxt index-hiding
$+$ 2-ctxt normal-hiding

$\Rightarrow$ Traitor tracing

Theorem [Goyal-Koppula-Waters'18]:

Message-less PLBE w/
q_1-ctxt index-hiding
q_2-ctxt normal-hiding

$+$ ABE which handles PLBE decryption

$\Rightarrow$ Plain PLBE w/
q_0-ctxt message-hiding
q_1-ctxt index-hiding
q_2-ctxt normal-hiding

ABE for log-depth from pairings [Goyal-Pandey-Sahai-Waters'06, Ishai-Wee'14, Chen-Gay-Wee'15, Lin-Luo'20]

Our Techniques

Theorem (This Work):

Plain PLBE w/
2-ctxt message-hiding
+ 2-ctxt index-hiding
+ **1**-ctxt normal-hiding

→ Traitor tracing

Theorem (This Work):

Weak PRFs → Message-less PLBE w/
2-ctxt index-hiding
+ **1**

In log-depth setting, both can be instantiated from pairings

Corollary (informal):

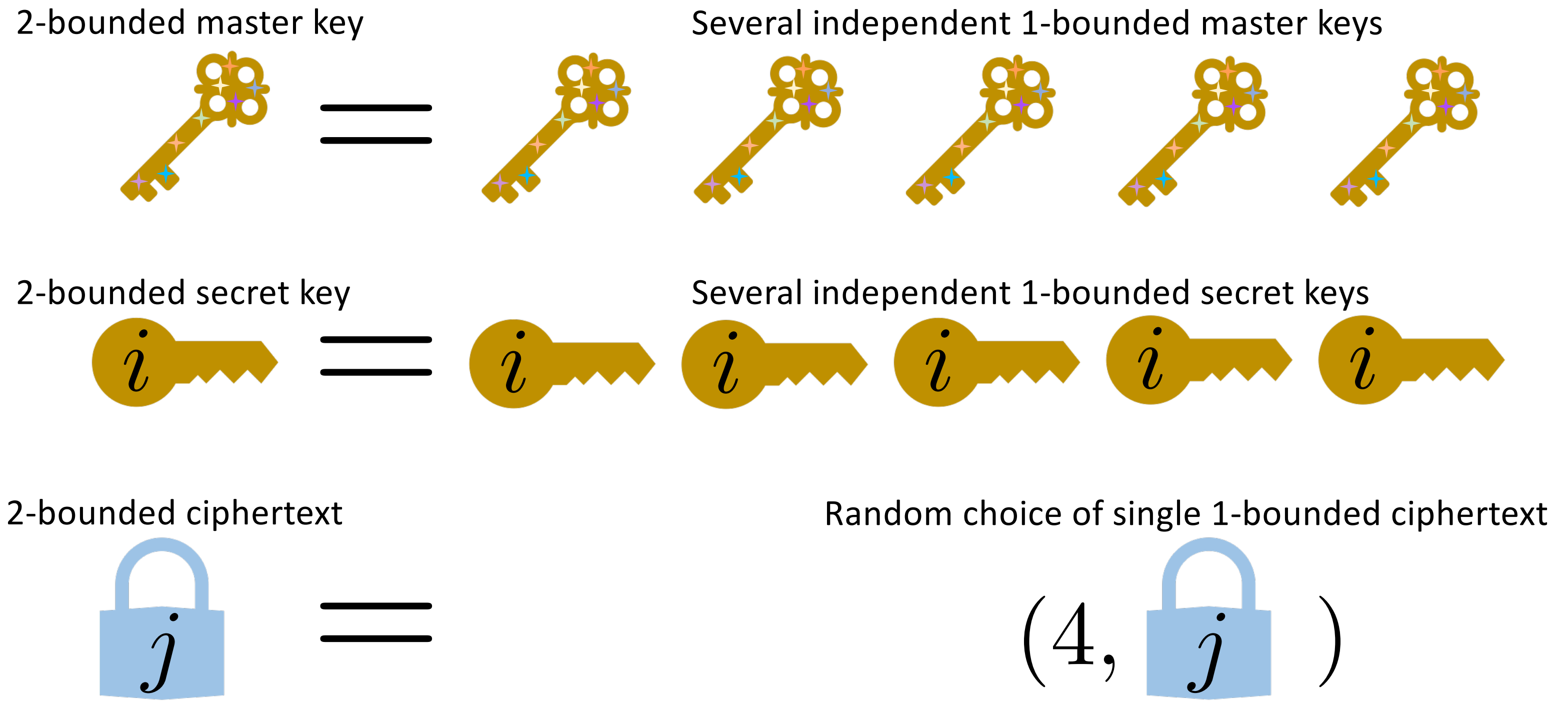
(log-depth) Weak PRFs
+ ABE (for log-depth comp.)

→ Traitor Tracing

Traitor Tracing from 1-ctxt Normal-Hiding

Can We Upgrade to 2-Bounded Security?

Simple black-box Idea: several parallel instances



2-bounded master key

Several independent 1-bounded master keys

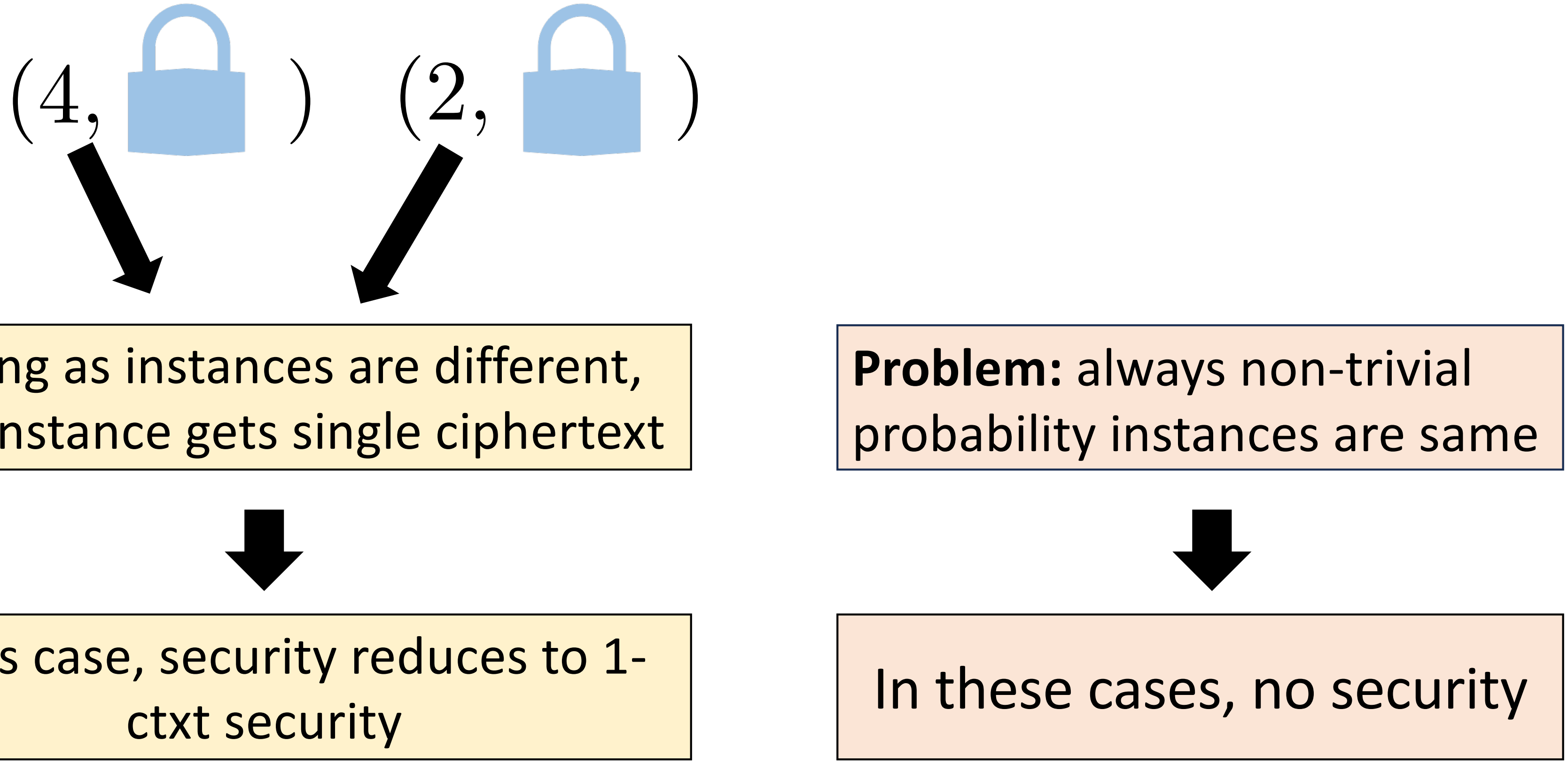
2-bounded secret key

Several independent 1-bounded secret keys

2-bounded ciphertext

Random choice of single 1-bounded ciphertext

Can We Upgrade to 2-Bounded Security?



$(4,$ 🔒 $)$ $(2,$ 🔒 $)$

As long as instances are different, each instance gets single ciphertext

In this case, security reduces to 1-ctxt security

Problem: always non-trivial probability instances are same

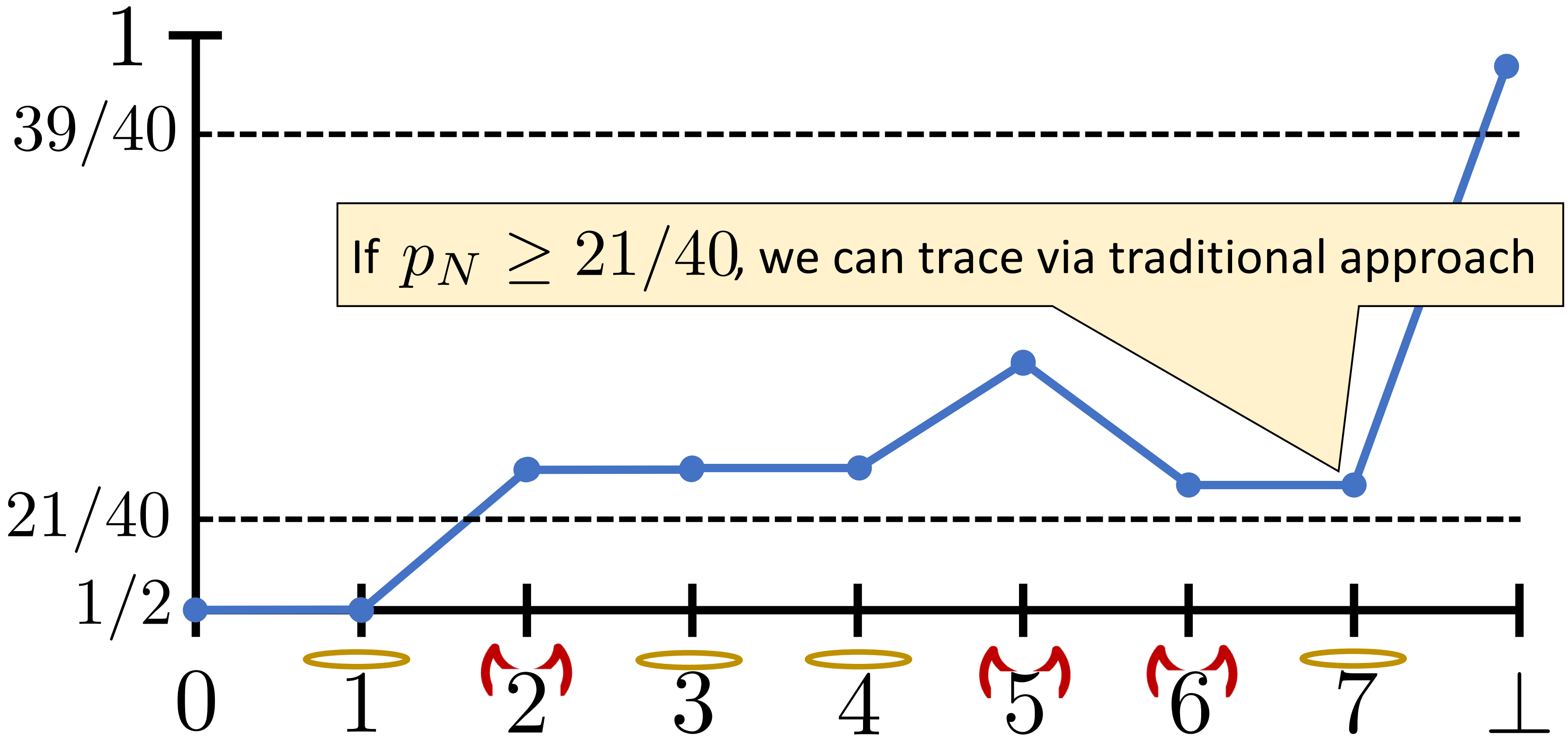
In these cases, no security

Weak Decoder-Based Normal-Hiding

Lemma (This Work, informal): Instantiate with 5 parallel instances. Then among decoders with $p_\perp \geq 39/40$, at least a fraction $1/82$ of them have $p_N \geq 21/40$

That is, ***very*** good decoders can't have tiny p_N too often

Our Tweaked Private Linear Broadcast Approach



If $p_N \geq 21/40$, we can trace via traditional approach

Our Tweaked Private Linear Broadcast Approach

Called “threshold” traitor tracing [Naor-Pinkas’98]

Problem: Our tracing algorithm

- Only has guarantees on decoders with high constant decryption probability
- Tracing of such decoders only successful with low constant probability

Called “risky” traitor tracing [Goyal-Koppula-Russell-Waters’17]

Theorem [Z’20]: Can generically remove both risky and threshold limitations. As long as probabilities are constant, no asymptotic change to parameters.

Thanks!