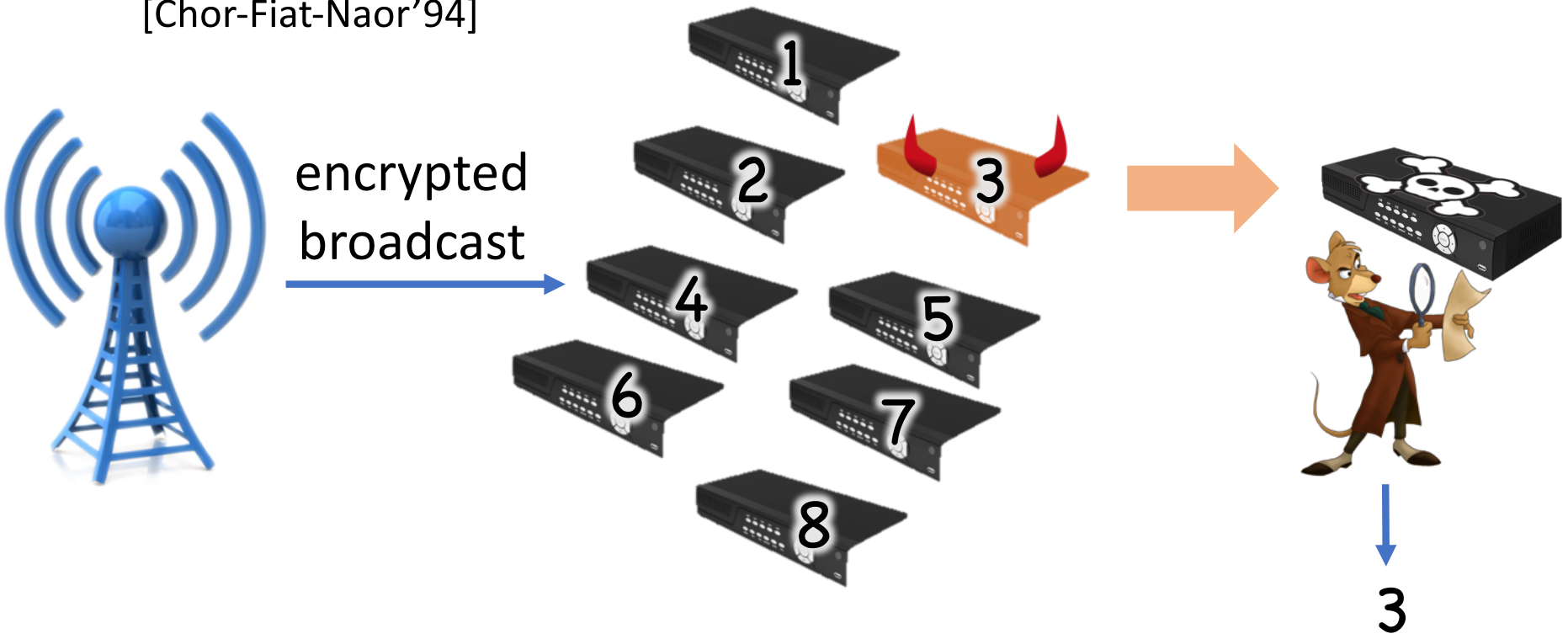
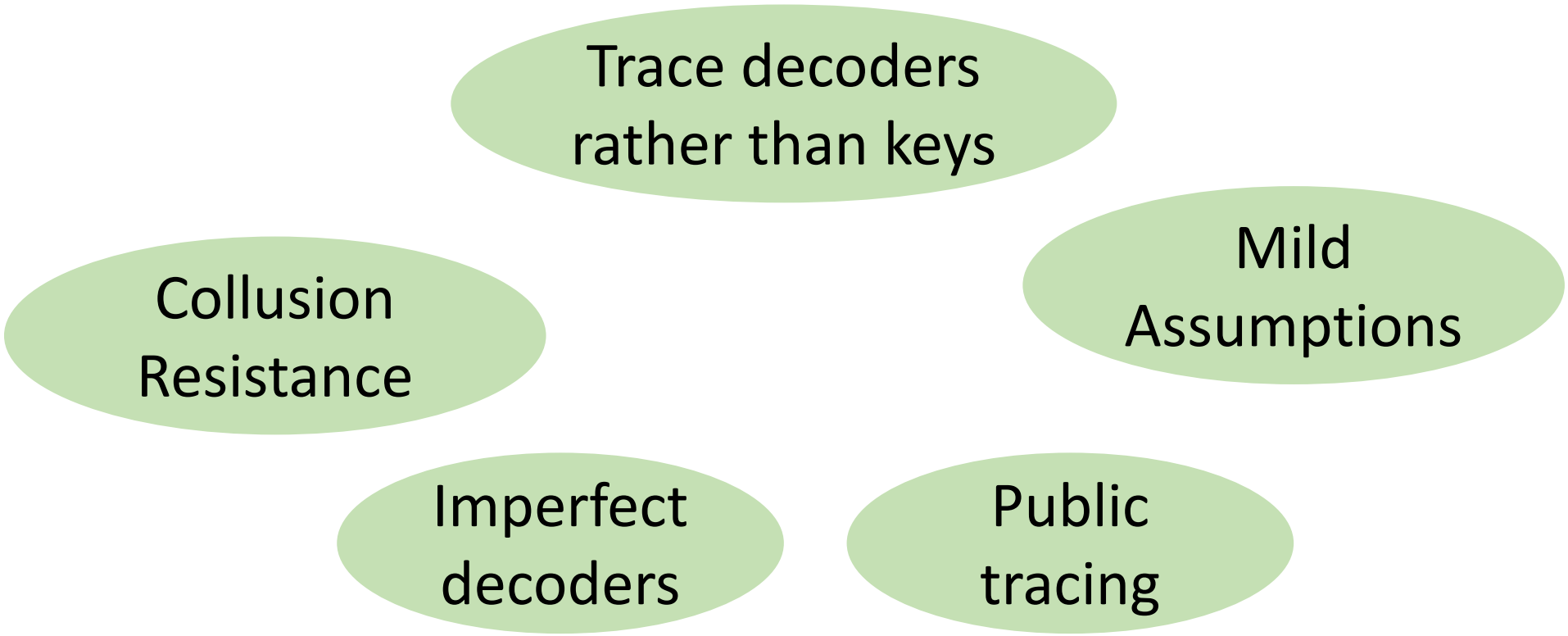
White Box Traitor Tracing

Mark Zhandry (Princeton & NTT Research)

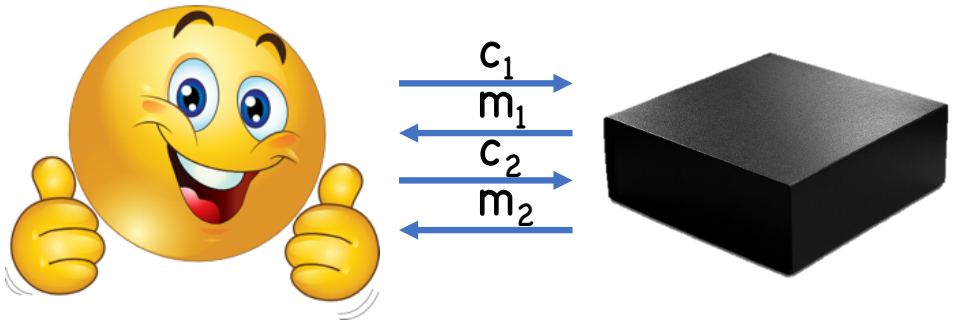
Traitor Tracing
[Chor-Fiat-Naor'94]



Some Desirable features



Black Box Tracing



Focus of all “modern” traitor tracing literature

“Trivial Solution”

$c_1 = Enc(pk_1, m)$
$c_2 = Enc(pk_2, m)$
…
$c_N = Enc(pk_N, m)$

Advantages:
- Collusion resistant
- Minimal assumptions
- Traces imperfect decoders
- Public tracing
- Black box tracing

Problem: large ciphertexts/public keys

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

Trivial:
PKE $\Longrightarrow (N, 1, N)$

[Boneh-Naor'02, Sirvent'06, Billet-Phan'08]:
PKE $\Longrightarrow (N^2, N^2, 1)$

Consequence:
Most tracing literature = shorter parameters

[Garg-Gentry-Halevi-Sahai-Waters'13,Boneh-Z'13]:
iO $\Longrightarrow (1,1,1)$

[Goyal-Koppula-Waters'18]:
LWE $\Longrightarrow (1,1,1)$

[Z'20]:
Pairings $\Longrightarrow (N^{1/3}, N^{1/3}, N^{1/3})$
IBE $\Longrightarrow (1, N^{2/3}, N^{2/3})$

Notation: (|pk|, |msk|, |ctxt|)

Desirable Feature: Embedded Identities

[Nishimaki-Wichs-Z'16]

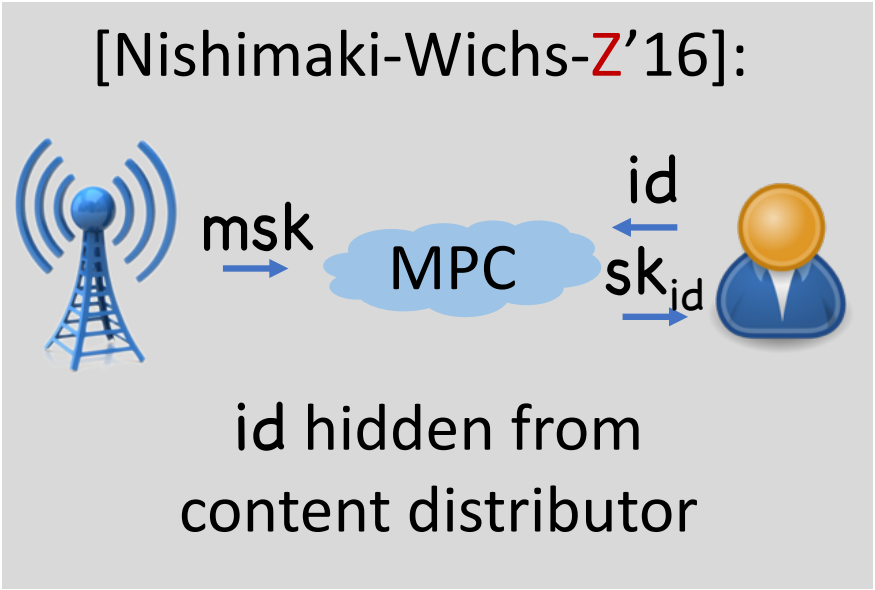
Most schemes:
(including trivial scheme)
user id = index $\in [N]$

Embedded identities:
user id $\in \{0,1\}^n$

Advantages of embedded identities:
- Increased deterrence (esp. w/ public tracing)
- "Anonymity"

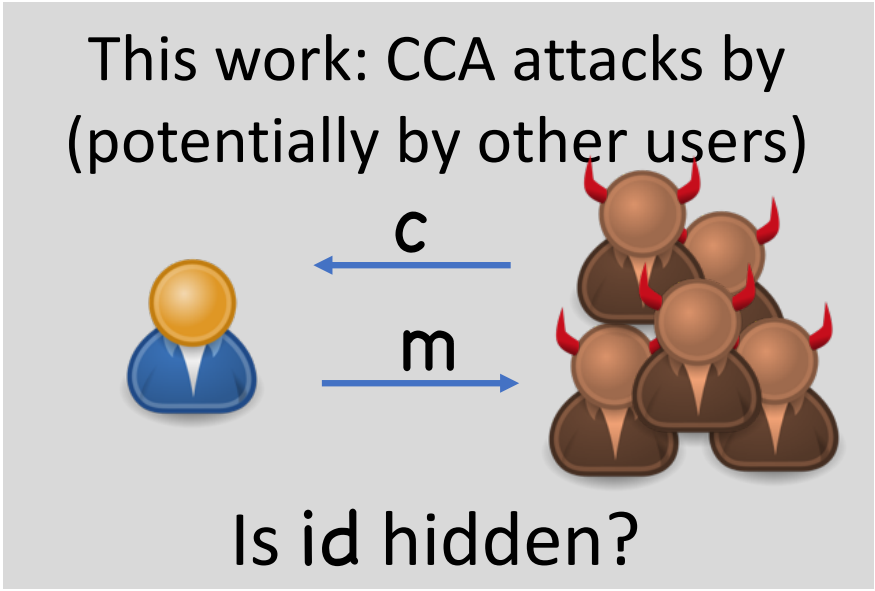
Desirable Feature: Anonymity/User Privacy

Suppose id contains sensitive info. Can it be kept secret?



Desirable Feature: Anonymity/User Privacy

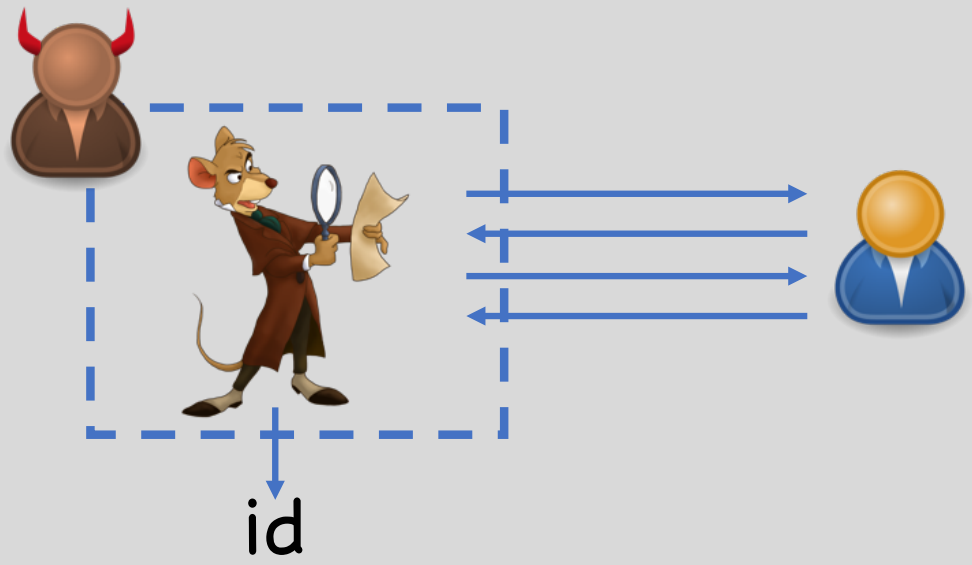
Suppose id contains sensitive info. Can it be kept secret?



Impossibility

Thm: Black Box $\Longrightarrow$ No user privacy under CCA attacks, against anyone who can trace

Proof:

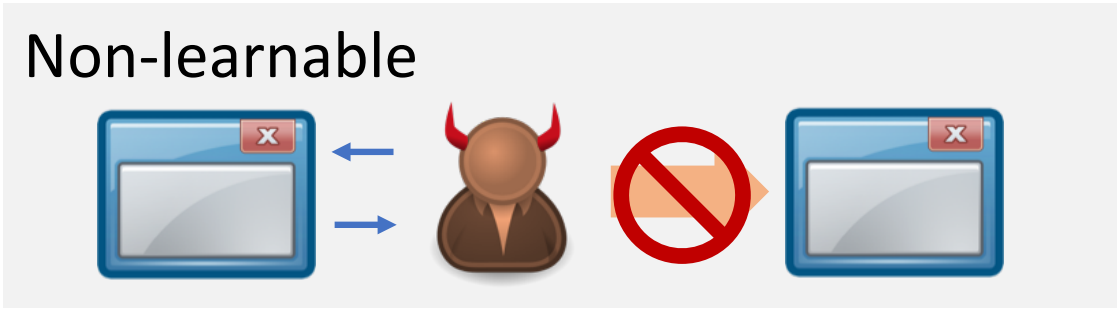


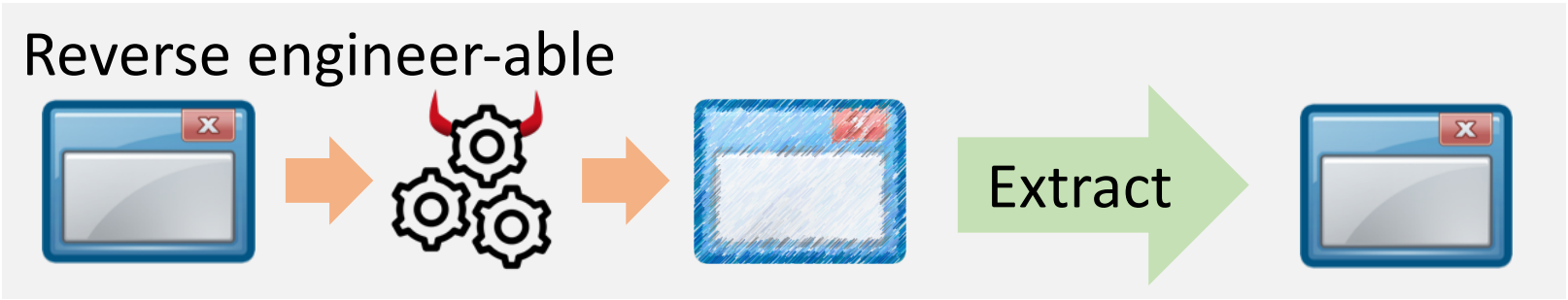
Positive Result

Thm: Functional Encryption (+ NIZKs) $\Longrightarrow$ public tracing + user privacy

Note: Necessarily use *white box* tracing (inspect actual code)

Proof Idea: Unobfuscatable Programs





[Barak-Goldreich-Impagliazzo-Rudich-Sahai-Vadhan-Yang'01]

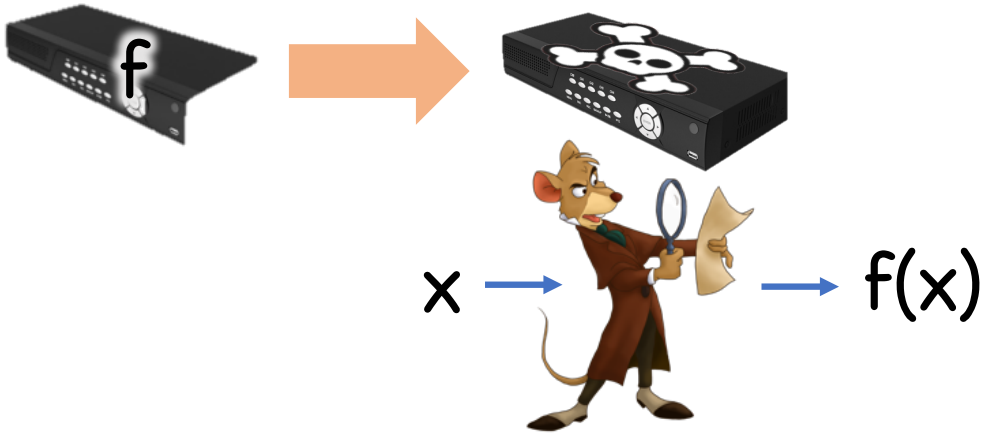
Failed Attempt

Assume embedded identity system (with black box tracing)

id =  ?

Problem: remote user recovers  using black box tracing

Our Solution: Function-Embedded TT



But can't learn code for f!

Thm: FE (+ NIZKs) $\Longrightarrow$ Function-Embedded TT

Extension of [Nishimaki-Wichs-Z'16]

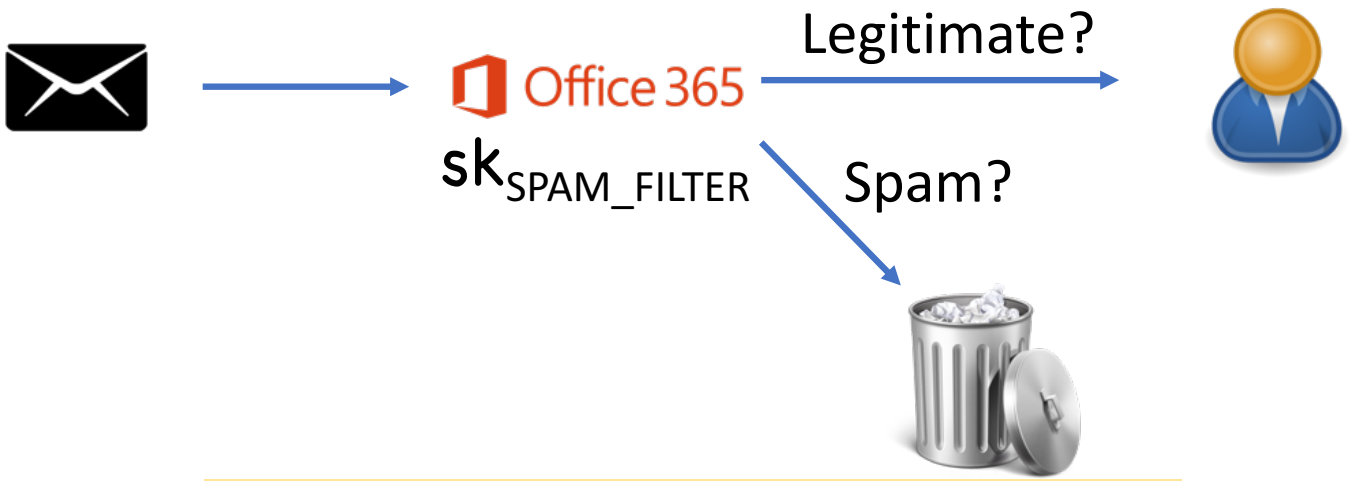
Our Solution: Function-Embedded TT

Thm: Function-Embedded TT (even w/ black box tracing)
+ Un-obfuscatable Programs
$\Longrightarrow$ public tracing + user privacy

Proof:

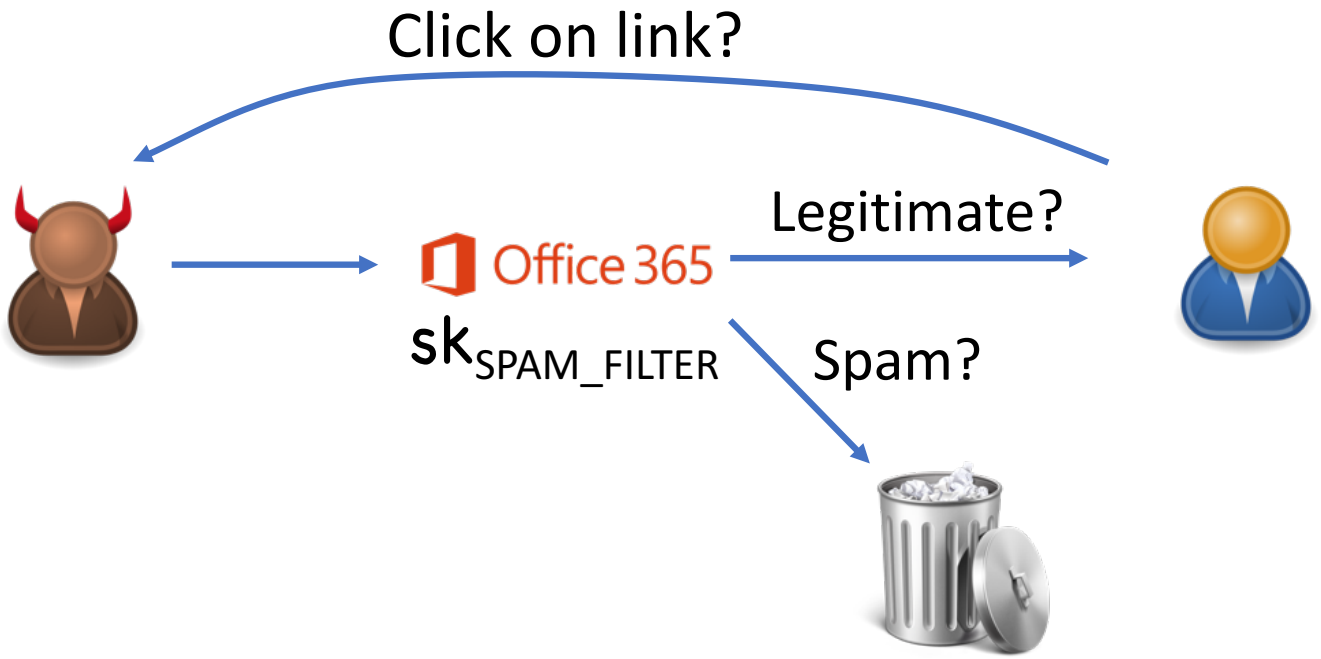
$f =$ 

Aside: CCA Attacks on Functional Encryption



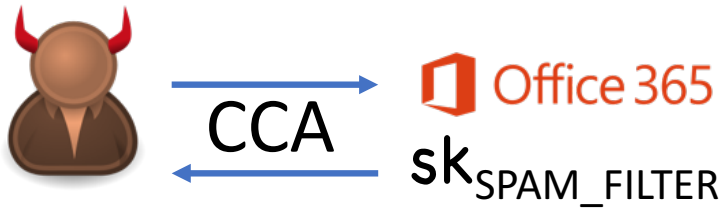
FE motivation: hide message content from email provider

Aside: CCA Attacks on Functional Encryption

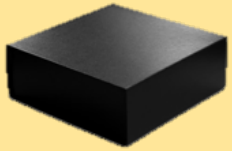


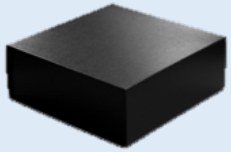
Q: what about security against spammer?

Aside: CCA Attacks on Functional Encryption



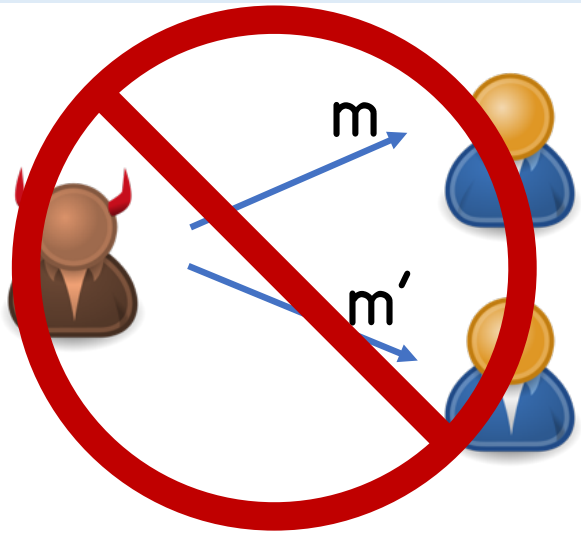
Q: What can adv learn about SPAM_FILTER?

$\geq$  , maybe:

Black box function privacy: $\leq$ 

Desirable Feature: Consistency

Typical malicious MPC assumption:
reliable broadcast channel

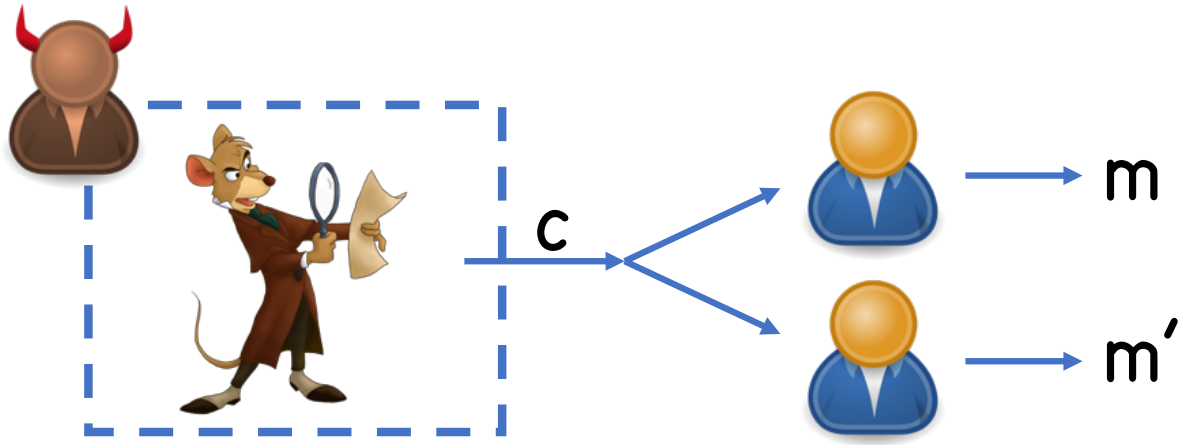


Q: What if channel encrypted under TT scheme?

Impossibility

Thm: Black Box + Public Tracing $\Longrightarrow$ Inconsistent decryptions

Proof:



Thm: FHE + Lockable Obfuscation $\Longrightarrow$ Consistency, tracing under $O(1)$ collusions

Note: again, necessarily *white box* tracing

Proof idea:

- Tracing requires secrets
- Secrets encrypted under FHE
- Tracing performed homomorphically
- Use lockable obfuscation to get result

Future Direction: Software Watermarking

Traitor tracing ≈ watermarking for decryption programs

All prior watermarking results use black box tracing

Q: Privacy, consistency for other watermarking settings?

Q: Watermark more programs with white box tracing?