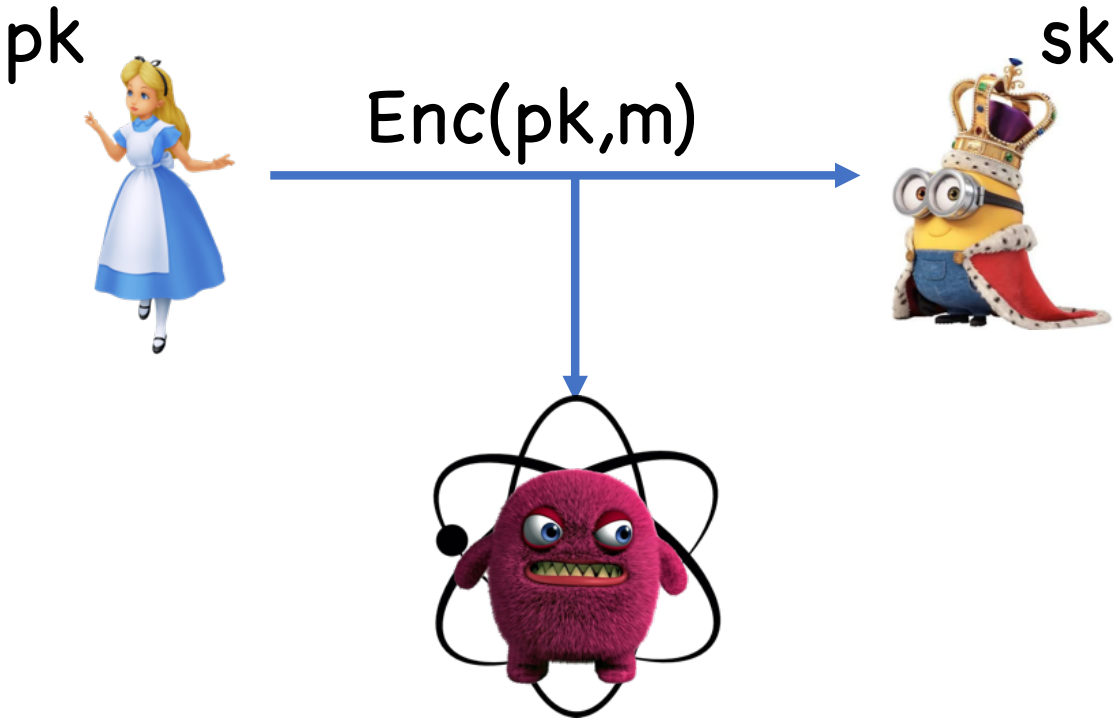
Schrödinger's Pirate: How To Trace a Quantum Decoder

Mark Zhandry (Princeton & NTT Research)

Typical Quantum Attacks on Classical Cryptosystems…

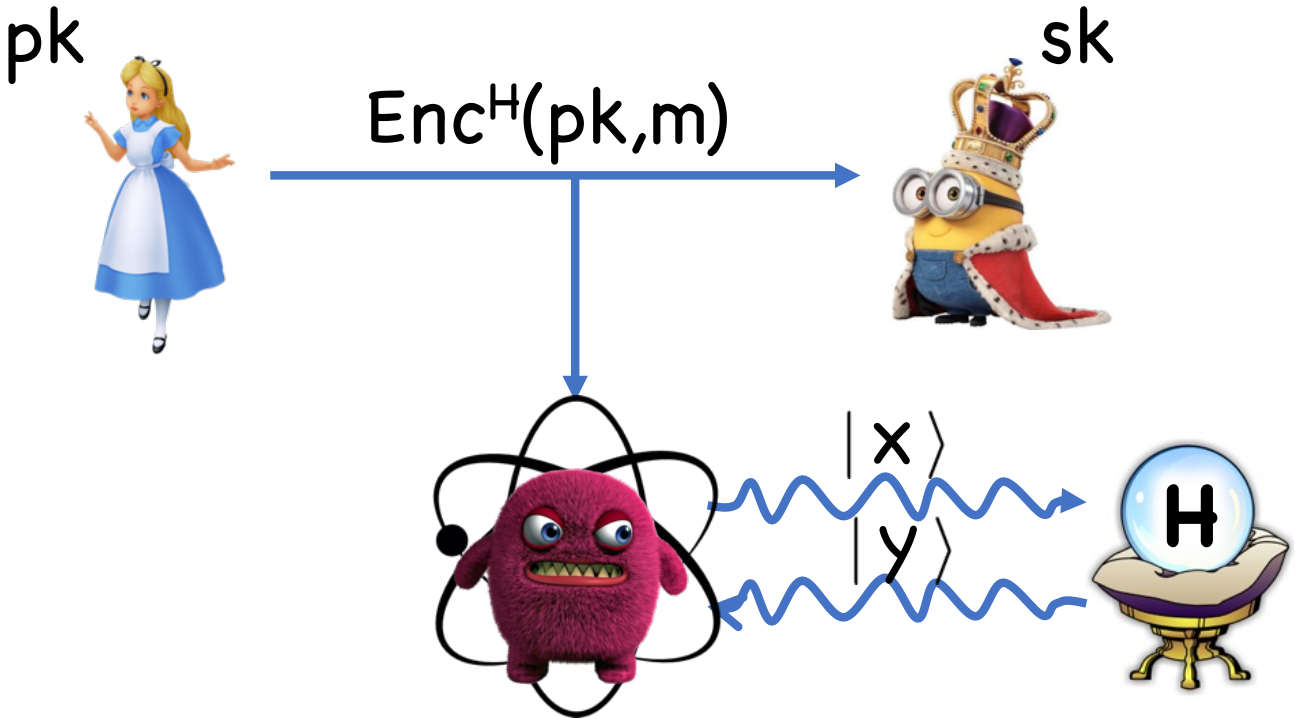
Quantum Computing Attacks

[Shor'94]



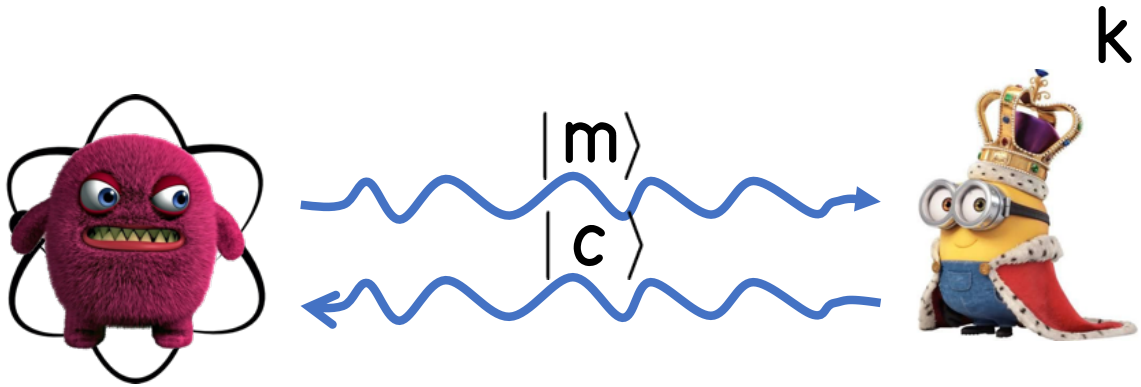
Quantum Random Oracles

[Bellare-Rogaway'93, Boneh-Dagdelen-Fischlin-Lehmann-Schaffner-Z'11,…]



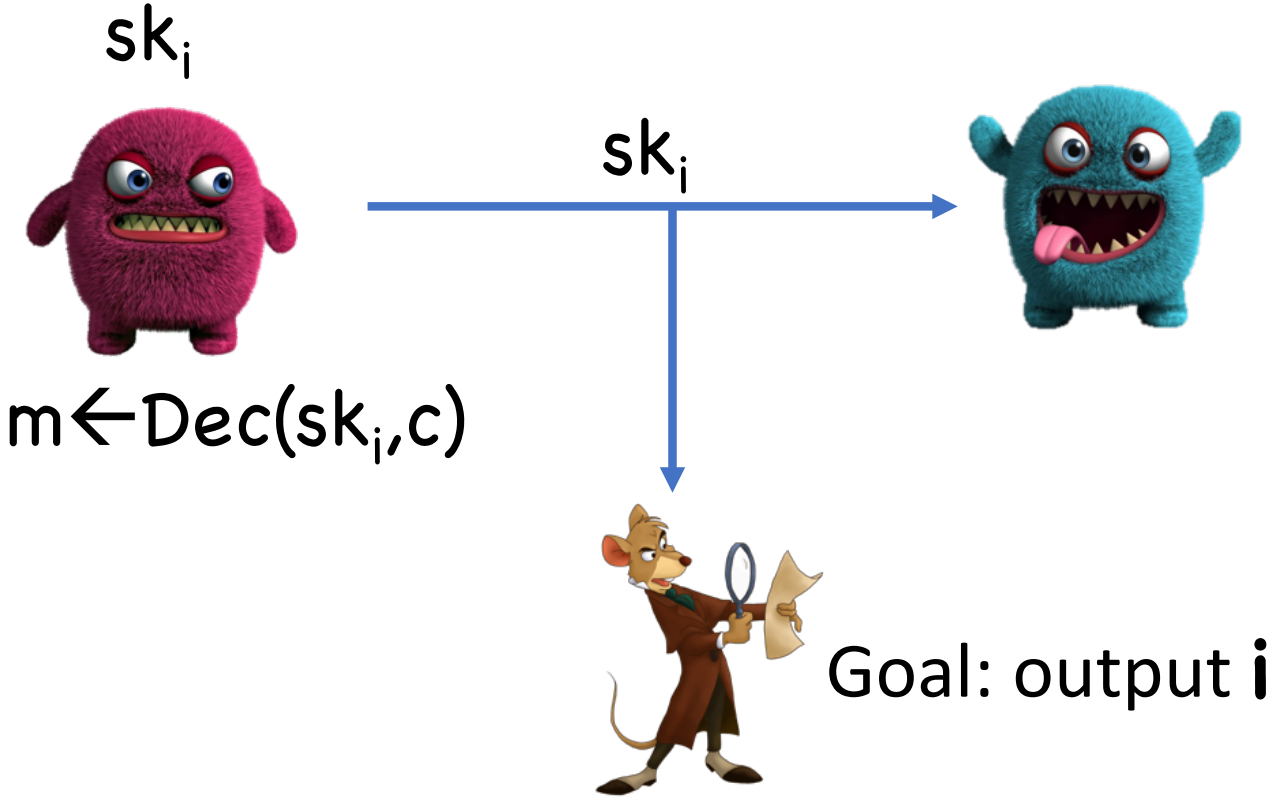
Superposition Attacks

[Aaronson'09,Kuwakado-Morii'10,Damgård-Funder-Nielsen-Salvail'11,Z'12,…]

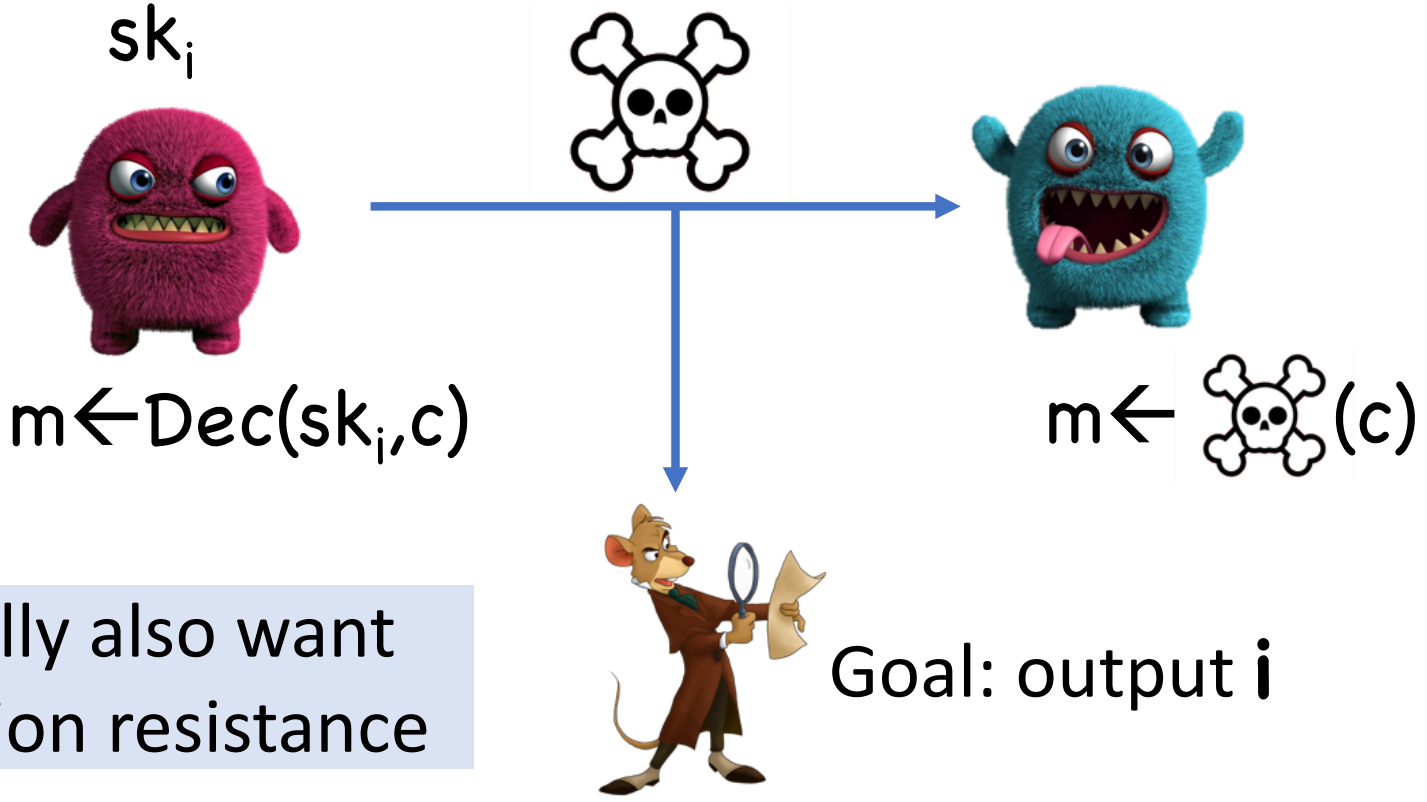


This work: Traitor Tracing Against Quantum Attacks

Traitor Tracing
[Chor-Fiat-Naor'94]

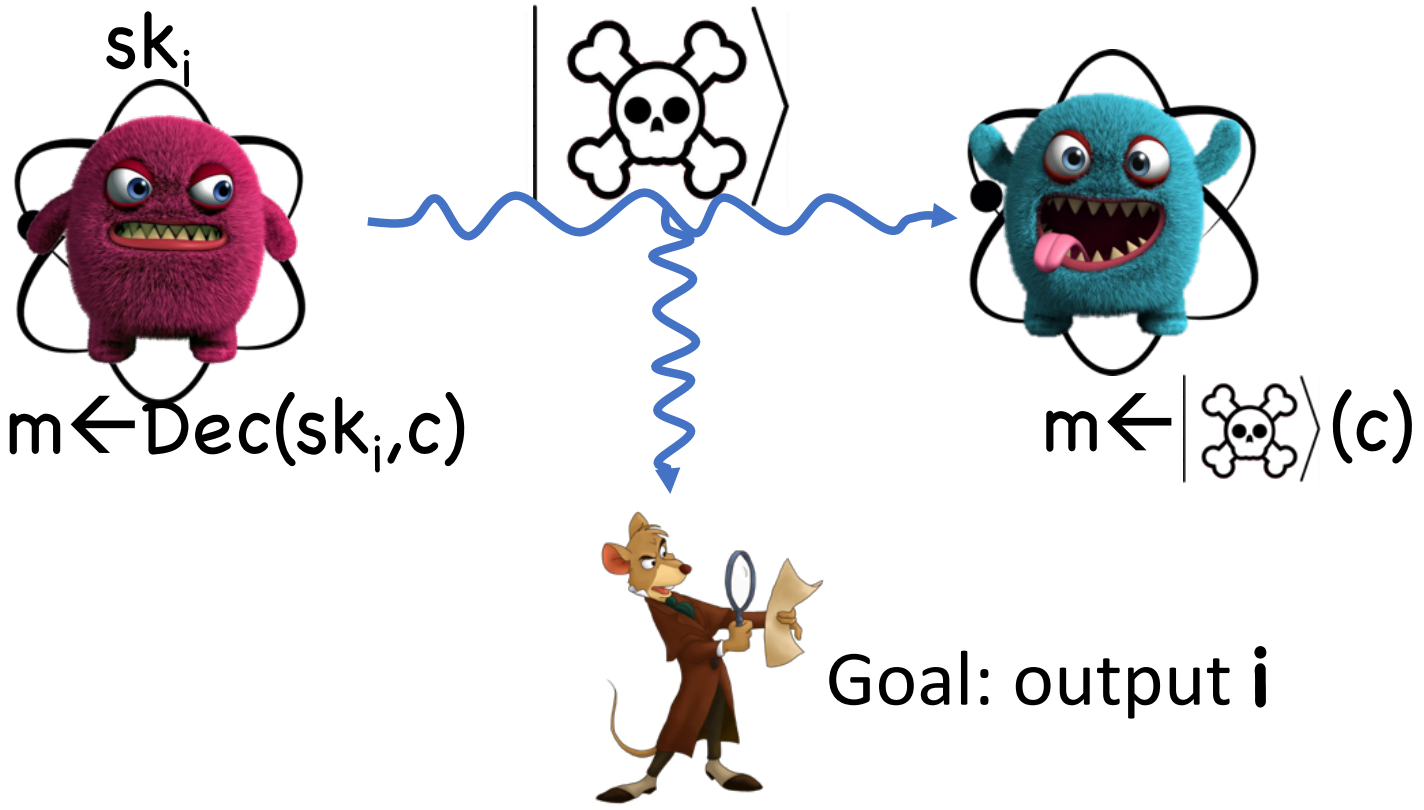


Traitor Tracing
[Chor-Fiat-Naor'94]



Usually also want collusion resistance

This Work: Quantum Traitor Tracing



Why Quantum Decoders?

Adversary channel "out of band"

➡ Can't prevent quantum messages

May help evade tracing?

➡ Use quantum crypto to hide i?

Other advantages for traitor?

➡ Unclonable or self-destructing $|$☠$\rangle$?

Results

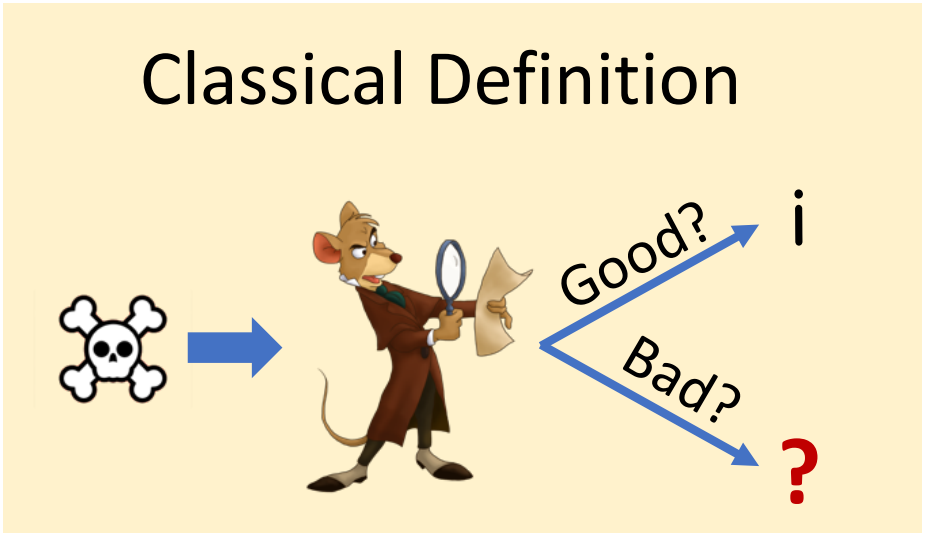
Definitions

Barrier/Impossibility for "classical" tracing strategies

Positive result for tracing certain kinds of PLBE

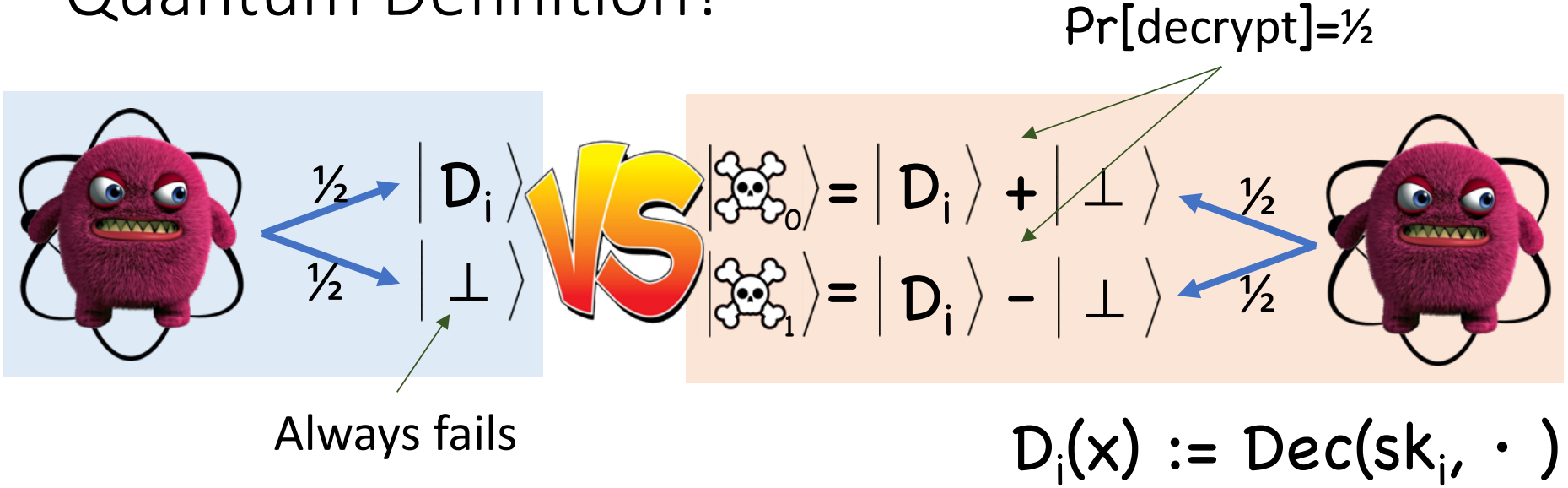
Includes
- generic construction from PKE,
- improved construction from iO,
- certain bounded collusion constructions

Defining Traitor Tracing



"Good"  := Pr[decrypt]>ε

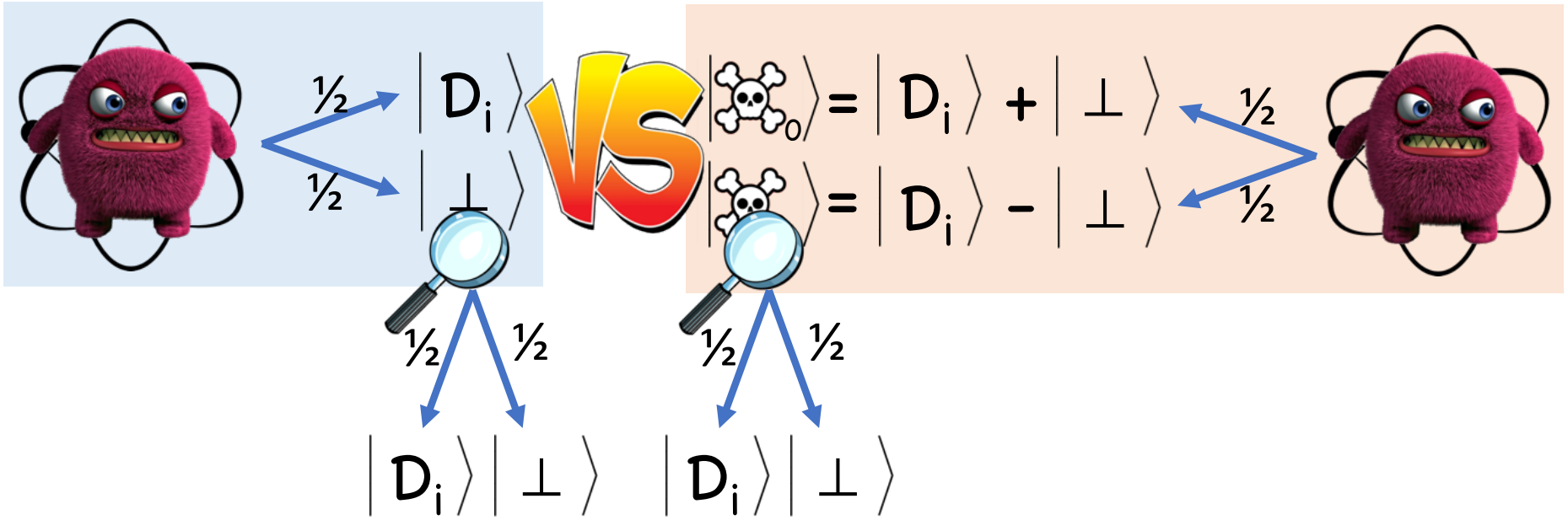
Quantum Definition?



Q: Which decoders are "good"?

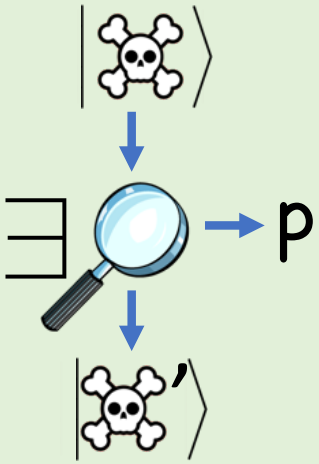
Problem: Attacks physically equivalent

Solution: Measure Decoder?



Problem: In general, will destroy decoder

Solution: Carefully Measure Decoder



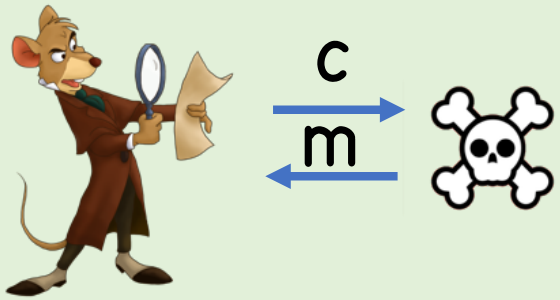
Projective Implementations

(1) Pr[$|\text{☠}'\rangle$ decrypts] = Pr[$|\text{☠}\rangle$ decrypts]

(2) Pr[$|\text{☠}'\rangle$ decrypts | p] = p

Classical Tracing vs Quantum Decoder

Classical Black Box Tracing



Classical [illegible] decoder

(needs [illegible] to run decoder, but otherwise classical)

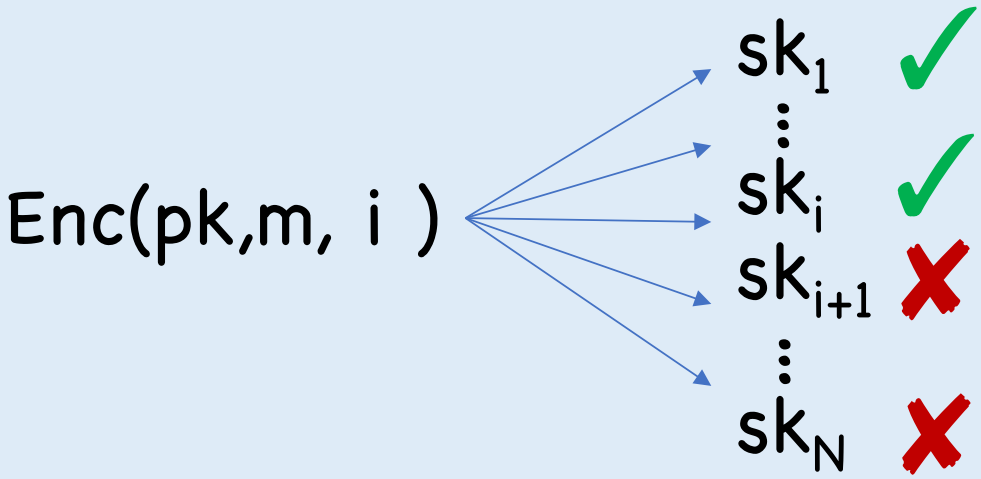
Proof idea: $|$  $\rangle$ degrades as queries made

Caveat: doesn't rule out weaker (but meaningful) tracing guarantees

Positive Result: PLBE

[Boneh-Sahai-Waters'06]

Private Linear Broadcast Encryption



Plus,

$Enc(pk,m, i) \approx_c Enc(pk,m, i-1)$, except to sk_i

PLBE → Classical Tracing [Boneh-Sahai-Waters'06]

$Enc_{TT}(pk,m) = Enc(pk,m, N)$

(1) Estimate p_i

(2) Output i s.t. $p_{i-1} \not\approx p_i$

$p_i := Pr[$  decrypts $Enc(pk,m,i)$ $]$

Proof:

PLBE security → $p_{i-1} \approx p_i$ for honest users, p_0 = "small"

Goodness of  → p_N = "big"

PLBE → Quantum Tracing?

By our impossibility

Problem: p_i non-physical

Problem: Can't estimate p_i by classical evaluations

Problem: $|☠\rangle$ may become useless at any point

PLBE → Quantum Tracing?

Solution: Quantum Alg for approx. measuring p_i

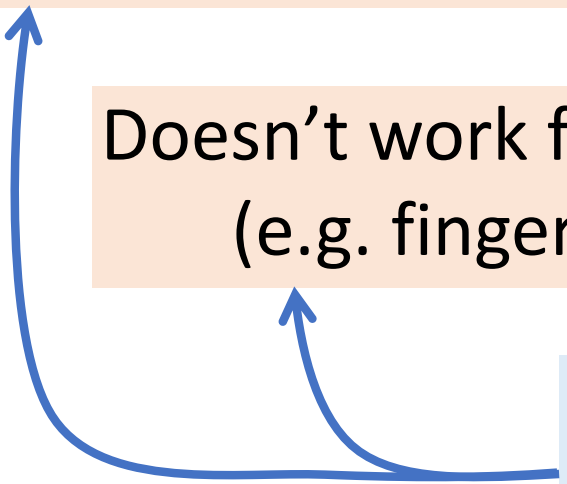
(Based on technique from [Watrous-Marriott'04])

Solution: Careful analysis → measuring (approximations of) p_i in *decreasing order* works

Limitations/Caveats

Doesn’t work for LWE-based TT [Goyal-Koppula-Waters’18]

Doesn’t work for many combinatorial constructions (e.g. fingerprinting codes [Boneh-Naor’02])



Directions for future work