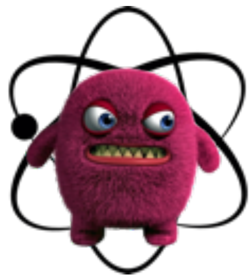
New Quantum Security Models

Mark Zhandry (Princeton & NTT Research)

Motivation

$\sum \alpha_{x,y} |x,y\rangle$

$\sum \alpha_{x,y} |x,y \oplus F(x)\rangle$



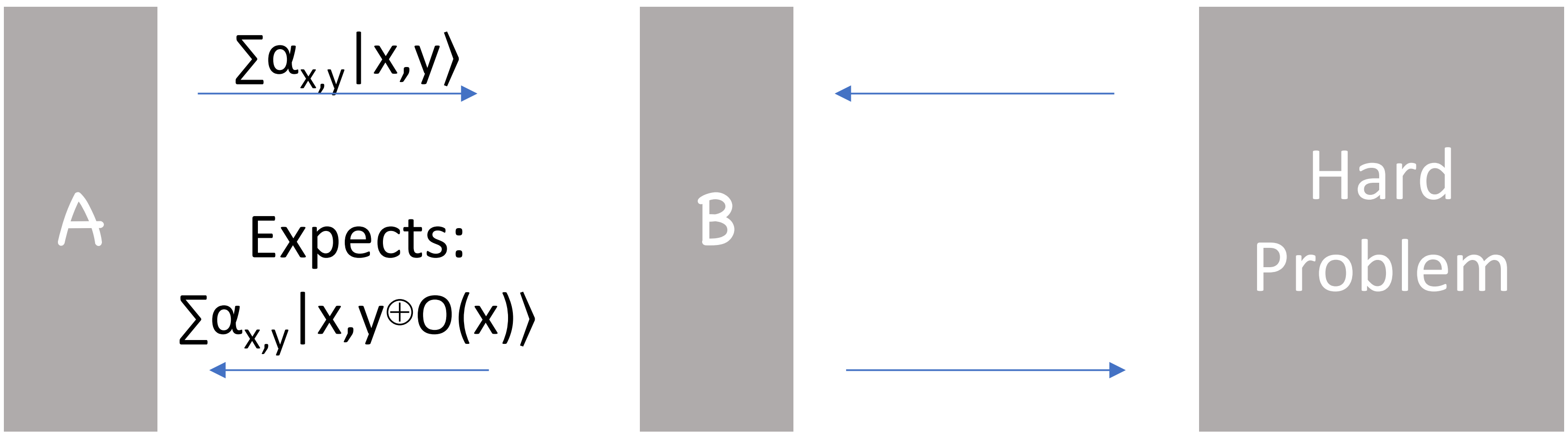
Higher level quantum protocol

F

Quantum random oracle model

(starting tomorrow)

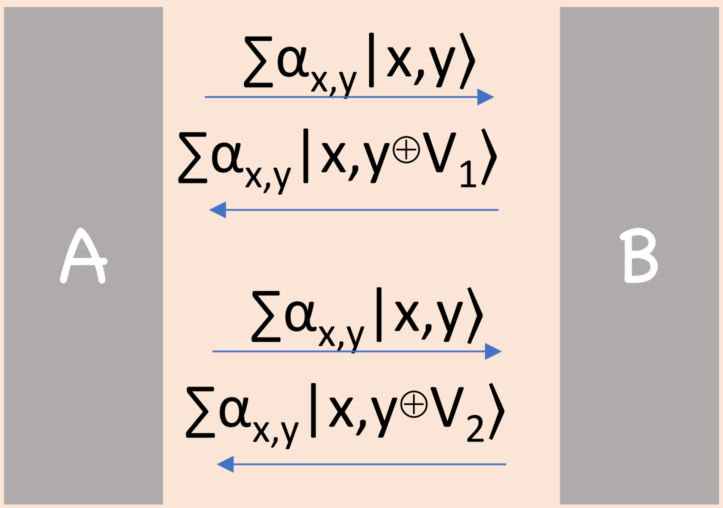
Security Proof Challenges



What does hybrid over queries look like?

Security Proof Challenges

Take 1: Per QUERY



Problem: repeated queries?

Problem: distinguishing attack

$\sum|x,0\rangle$ → , ← $\sum|x,V_1\rangle$ VS $\sum|x,0\rangle$ → , ← $\sum|x,O(x)\rangle$

Security Proof Challenges

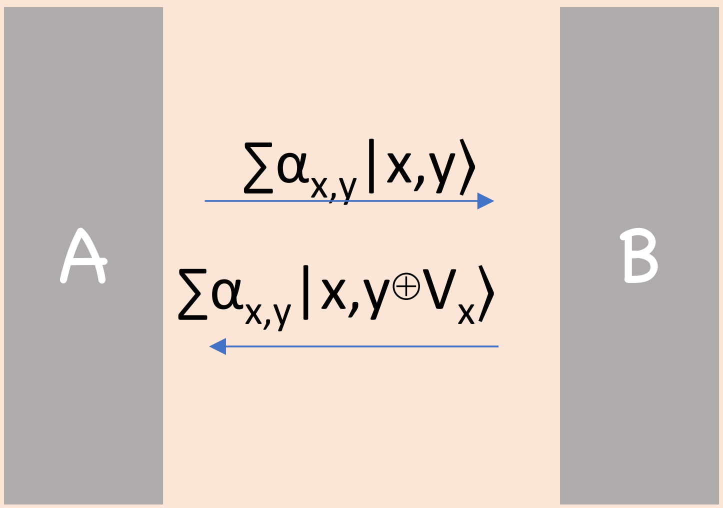
Typical reductions are commit to entire function O at beginning, remain consistent throughout

[Zhang-Yu-Feng-Fan-Zhang'19]: "Committed programming reductions"

Non-committing reductions: topic for later class

Security Proof Challenges

Take 2: Per VALUE



Problem: exp-many values

- Exponential loss in hybrid
- How to simulate efficiently?

PRF Recap

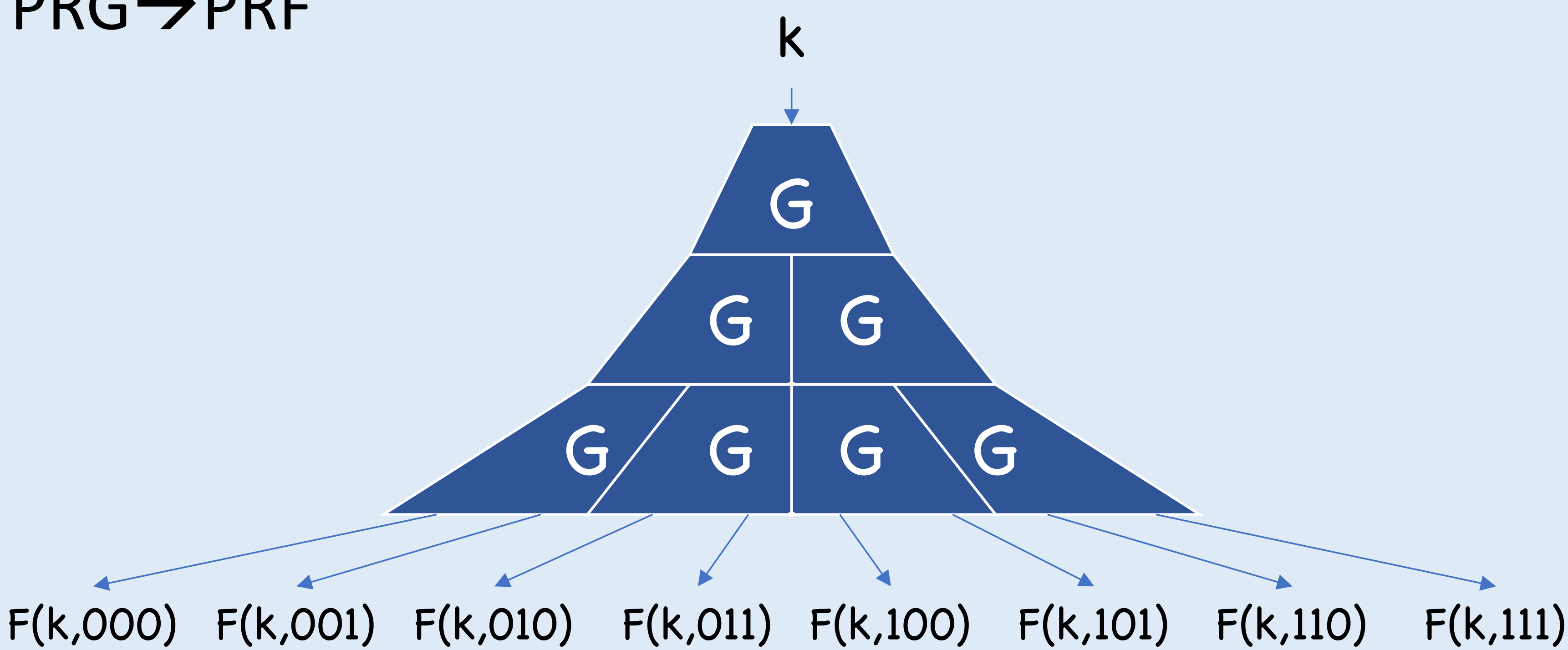
Def: F is a **Fully Quantum** secure PRF if,
$\forall$ **Q**PT A, $\exists$ negligible ε such that
$| \Pr[A^{|F(k,\cdot)\rangle}()=1] - \Pr[A^{|R(\cdot)\rangle}()=1] | < \varepsilon$

$A^{|O(\cdot)\rangle}$ means quantum queries:

$\sum \alpha_{x,y}|x,y\rangle \Rightarrow \sum \alpha_{x,y}|x,y \oplus O(x)\rangle$

PRF Recap

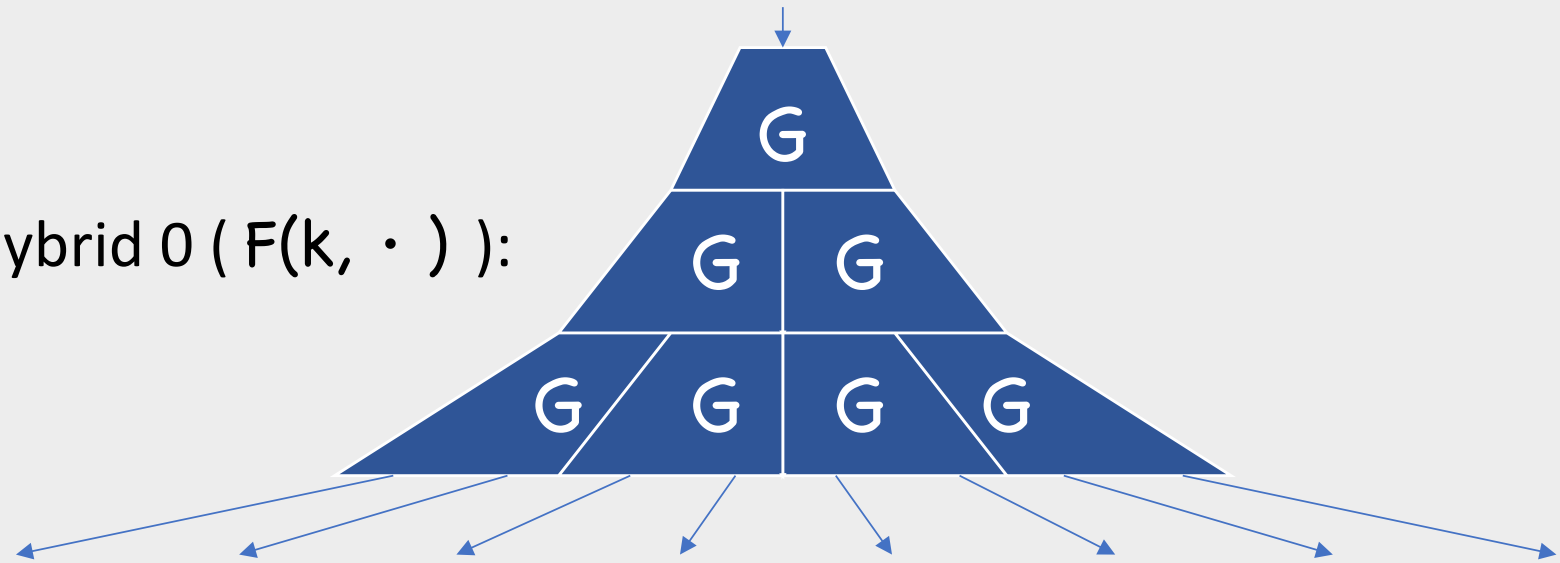
PRG→PRF



PRF Recap

Proof, step 1: Hybrid

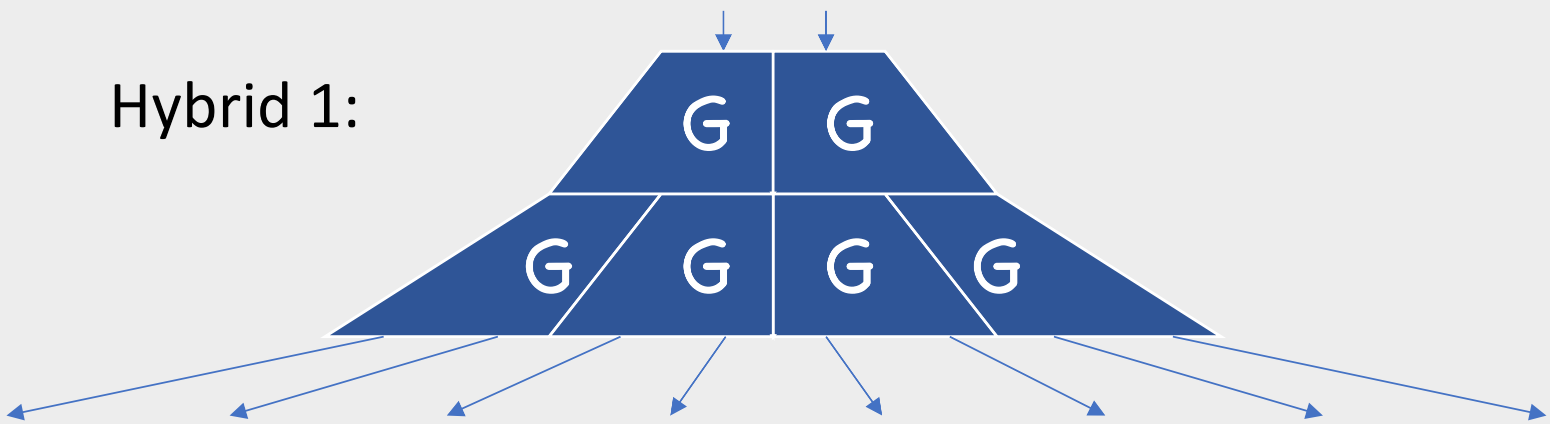
Hybrid 0 (F(k, ·)):



PRF Recap

Proof, step 1: Hybrid

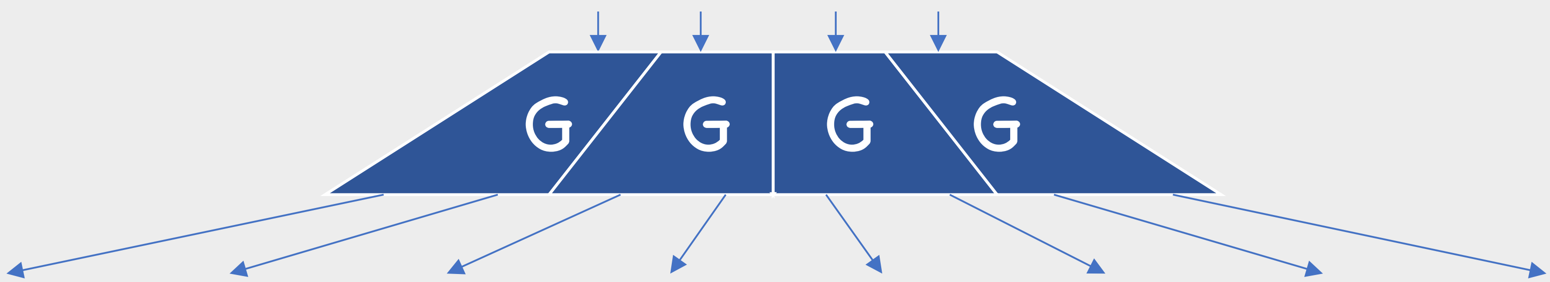
Hybrid 1:



PRF Recap

Proof, step 1: Hybrid

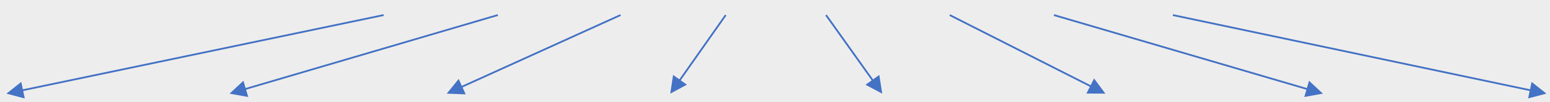
Hybrid 2:



PRF Recap

Proof, step 1: Hybrid

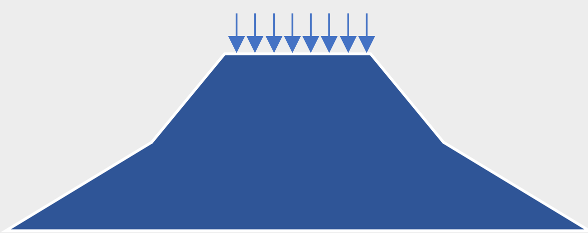
Hybrid n $(R(\cdot))$:



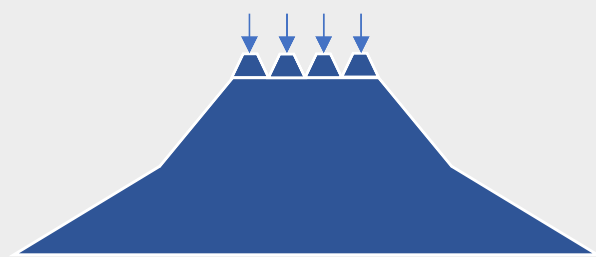
PRF Recap

Proof, step 1: Hybrid

$$\exists i \text{ s.t. } \left| \Pr[A^{\text{Hybrid } i+1}() = 1] - \Pr[A^{\text{Hybrid } i}() = 1] \right| \geq \varepsilon/n$$



VS



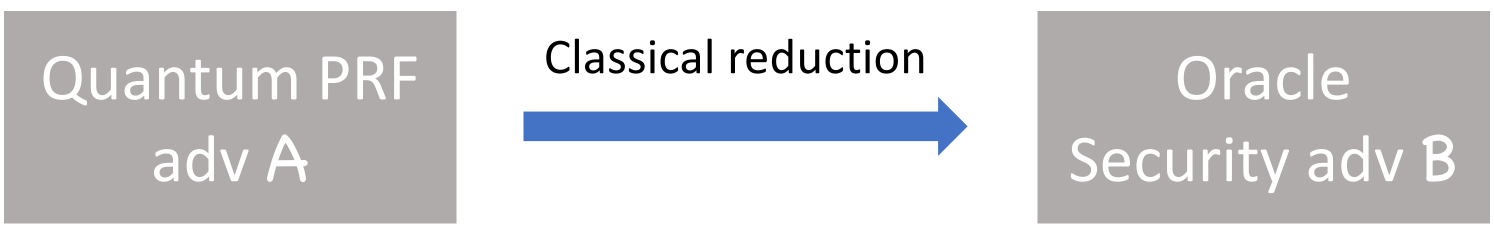
Step 1 makes sense if A classical, post-quantum, or fully quantum

Another View

Def: G is **Quantum Oracle Secure** if, $\forall$ QPT A, $\exists$ negligible ε such that

$$| \Pr[A^{|R\rangle} = 1] - \Pr[A^{|G \circ O\rangle} = 1] | < \varepsilon$$

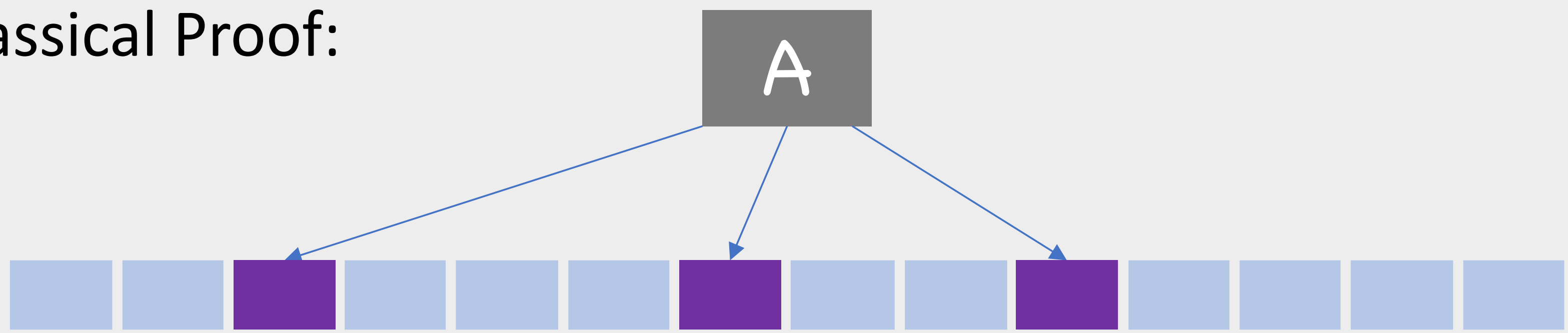
R,O random oracles



Another View

How to complete reduction from plain (post-quantum) PRGs?

Classical Proof:

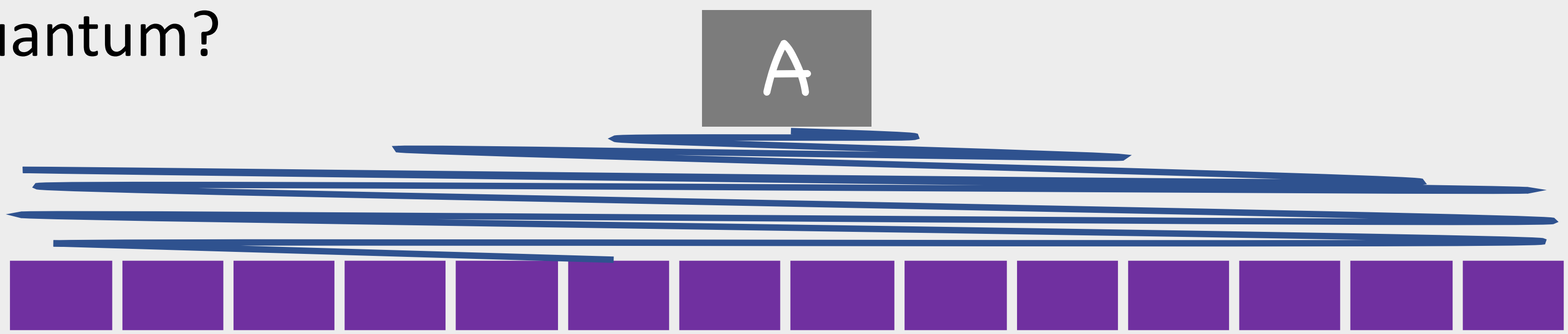


Only **q** queries → Can simulate with **q** samples; Hybrid over **q** values

Another View

How to complete reduction from plain (post-quantum) PRGs?

Quantum?



Need exponentially-many samples for perfect simulation

Reducing # of Hybrids

Goal: Simulate query responses using only poly-many samples

Simulating with Few Samples

Extreme 1: Same sample in all positions

V V V V V V V V V V V V V V

Distinguishable!

Middle ground: Several samples in random positions

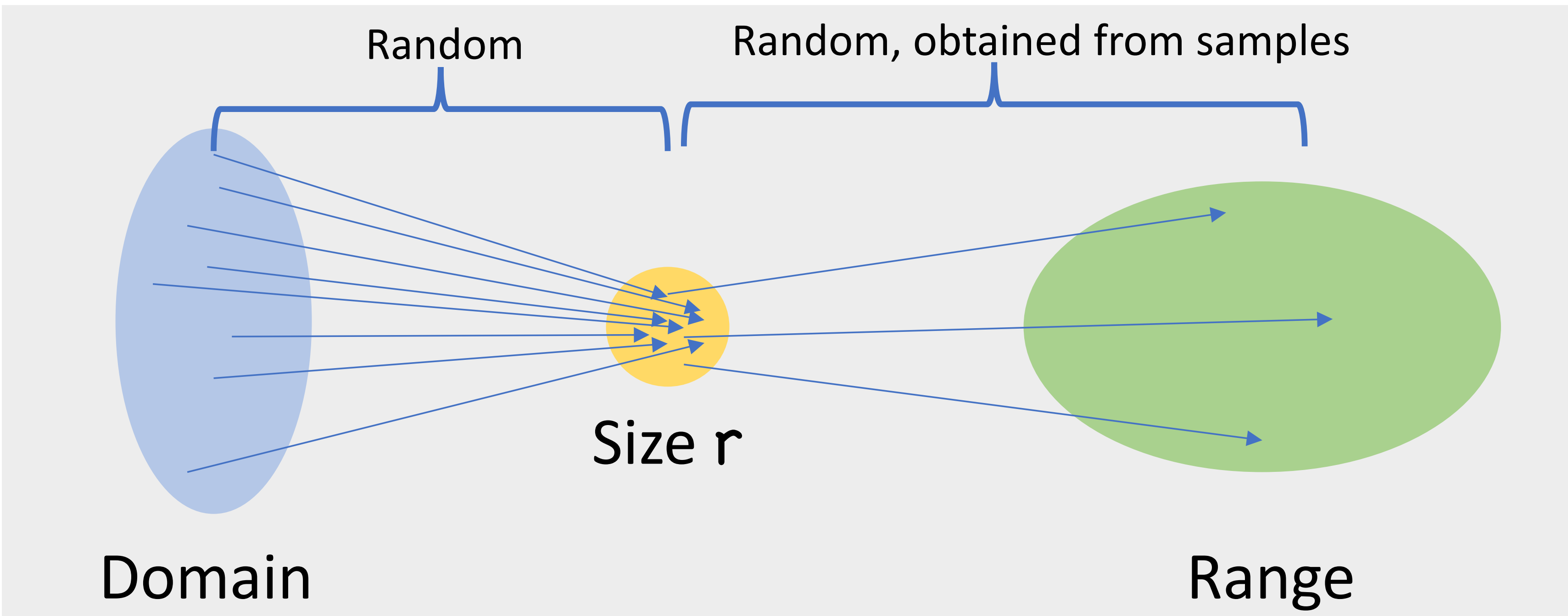
V_1 V_5 V_3 V_5 V_2 V_1 V_4 V_3 V_2 V_1 V_4 V_5 V_2 V_3

Extreme 2: Independent sample in each position

V_1 V_2 V_3 V_4 V_5 V_6 V_7 V_8 V_9 V_{10} V_{11} V_{12} V_{13} V_{14}

Exponential loss!

Small Range Distributions



How big of r to be indistinguishable from truly random?

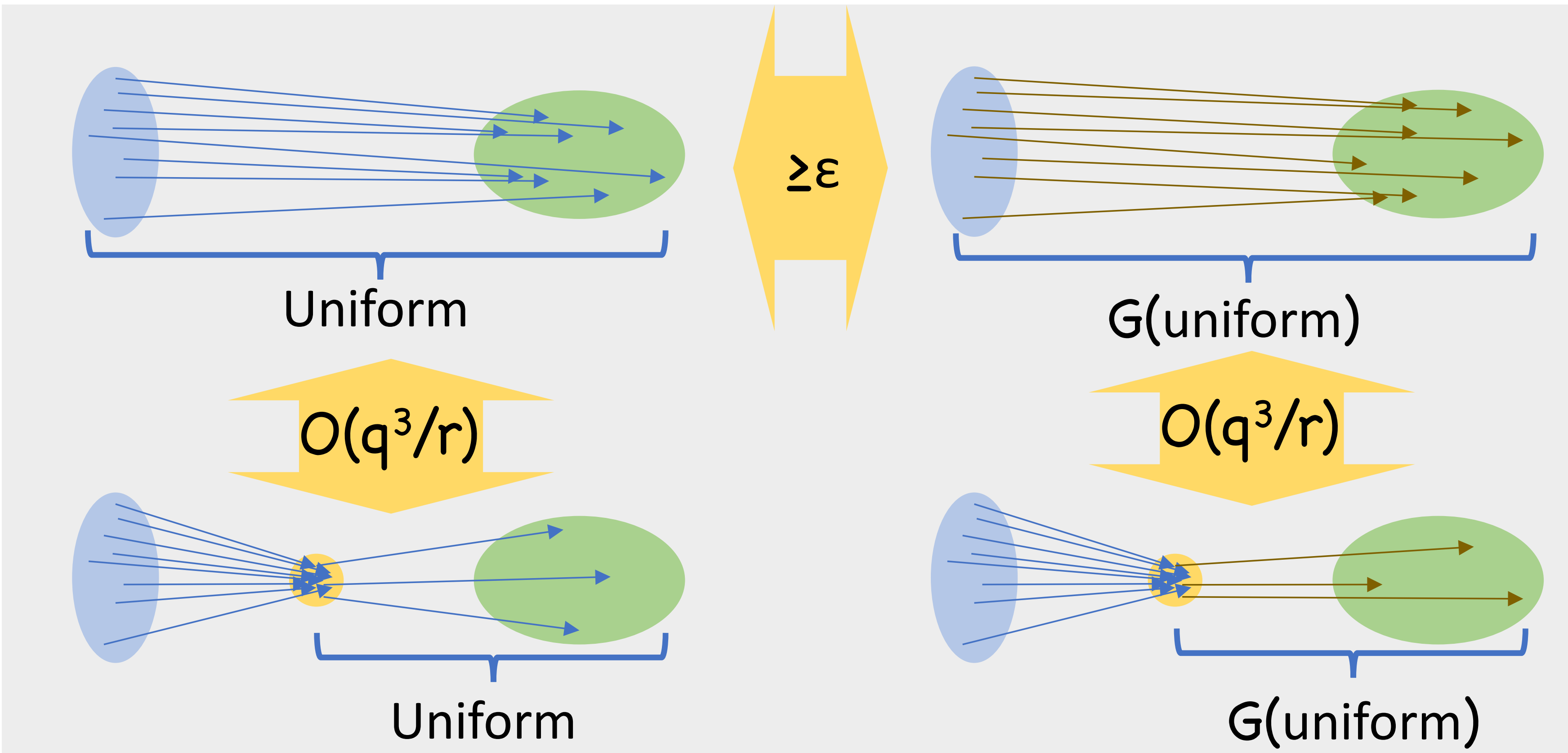
Small Range Distributions

Thm [Z'12b]: No **q** quantum query alg can distinguish SR_r from random, except with probability $O(q^3/r)$. Holds for any output distribution.

Quantum collision finding ➡ bound tight

$r=q^3$? $r=q^4$? $r=q^{20}$? $r=1.01^q$?

Quantum Proof



Quantum Proof

$$|\Pr[A^{|R\rangle}=1] - \Pr[A^{|G\circ O\rangle}=1]| \geq \varepsilon$$

⬇

$$|\Pr[B(y_1,\ldots,y_r)=1] - \Pr[B(G(x_1),\ldots,G(x_r))=1]| \geq \varepsilon - O(q^3/r)$$

⬇

$$|\Pr[C(y)=1] - \Pr[C(G(x))=1]| \geq \varepsilon/r - O(q^3/r^2)$$

Optimize by setting $r = O(q^3/\varepsilon)$ ➡ Final advantage $O(\varepsilon^2/q^3)$

Notes

Requires knowing ε

Can fix by guessing $\varepsilon=2^{-i}$ for random i

ε^2 means much bigger security loss

Proving SR Theorem

Thm [Z'12a]: If A makes q quantum queries to $O \leftarrow D$, then

$$\Pr[A^D()=1] = \sum_{\substack{x_1,\ldots,x_{2q} \\ y_1,\ldots,y_{2q}}} \Pr[D(x_i)=y_i \ \forall i \in [2q]]$$

(Restatement of polynomial method [Beals-Buhrman-Cleve-Mosca-de Wolf'01])

Thm [Z'12b]: For SR_r, the $\Pr[D(x_i)=y_i \ \forall i \in [k]]$ are degree k polynomials in $1/r$

➡ $\Pr[A^{SR_r}()=1]$ = degree 2q polynomial in $1/r$

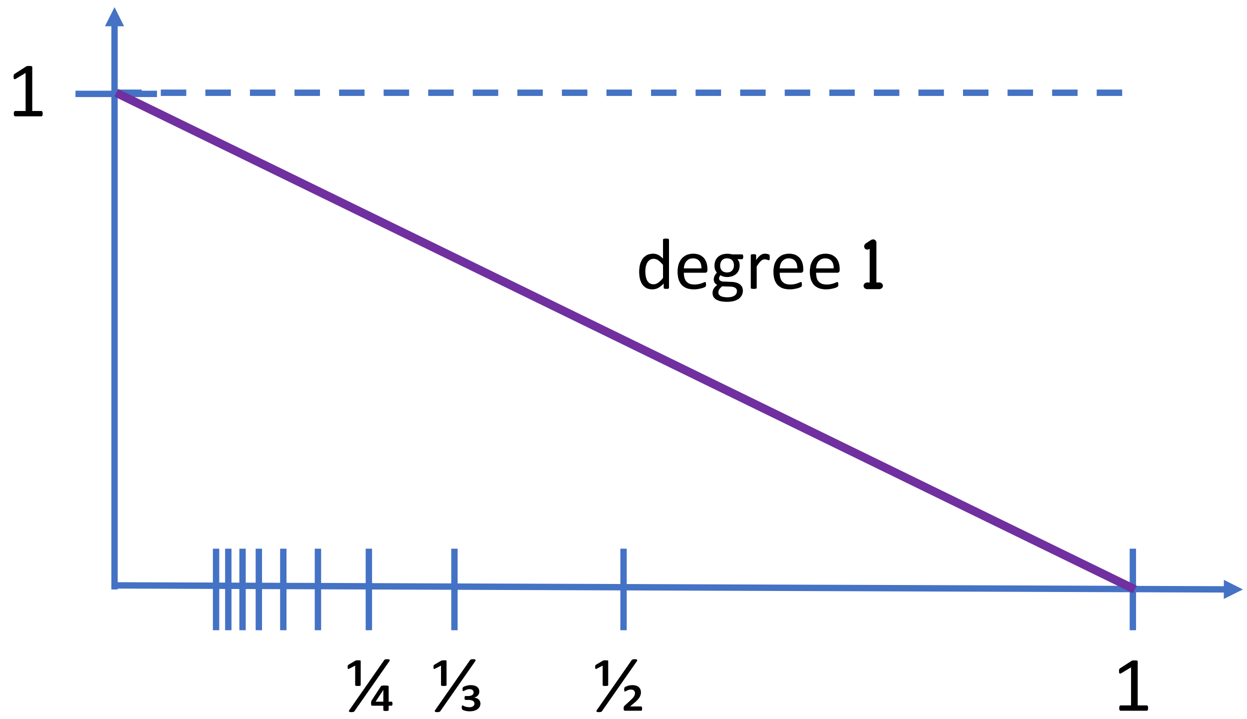
Proving SR Theorem

$\Pr[A^{SR_r}()=1] = P(1/r) =$ degree $2q$ polynomial

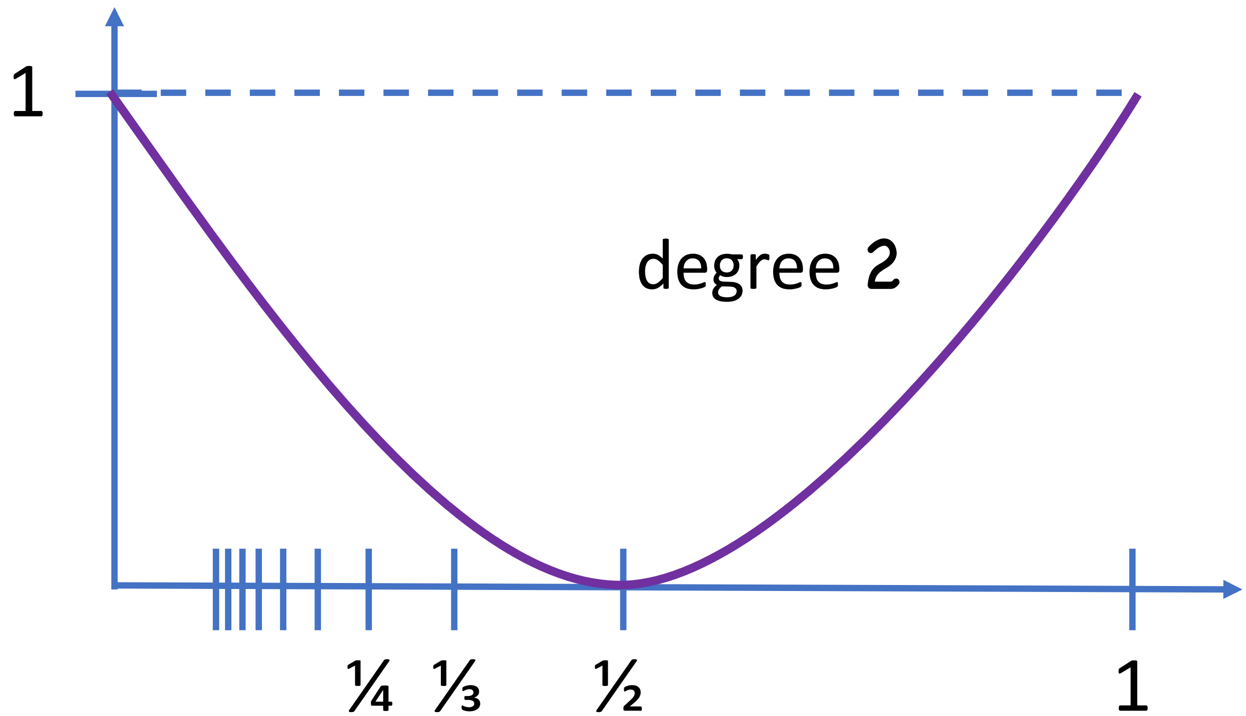
Additional observations:
- $SR_\infty =$ Truly random function
- $0 \leq P(1/r) \leq 1$ $\forall$ positive integers r

Goal: bound $| P(1/r) - P(0) |$

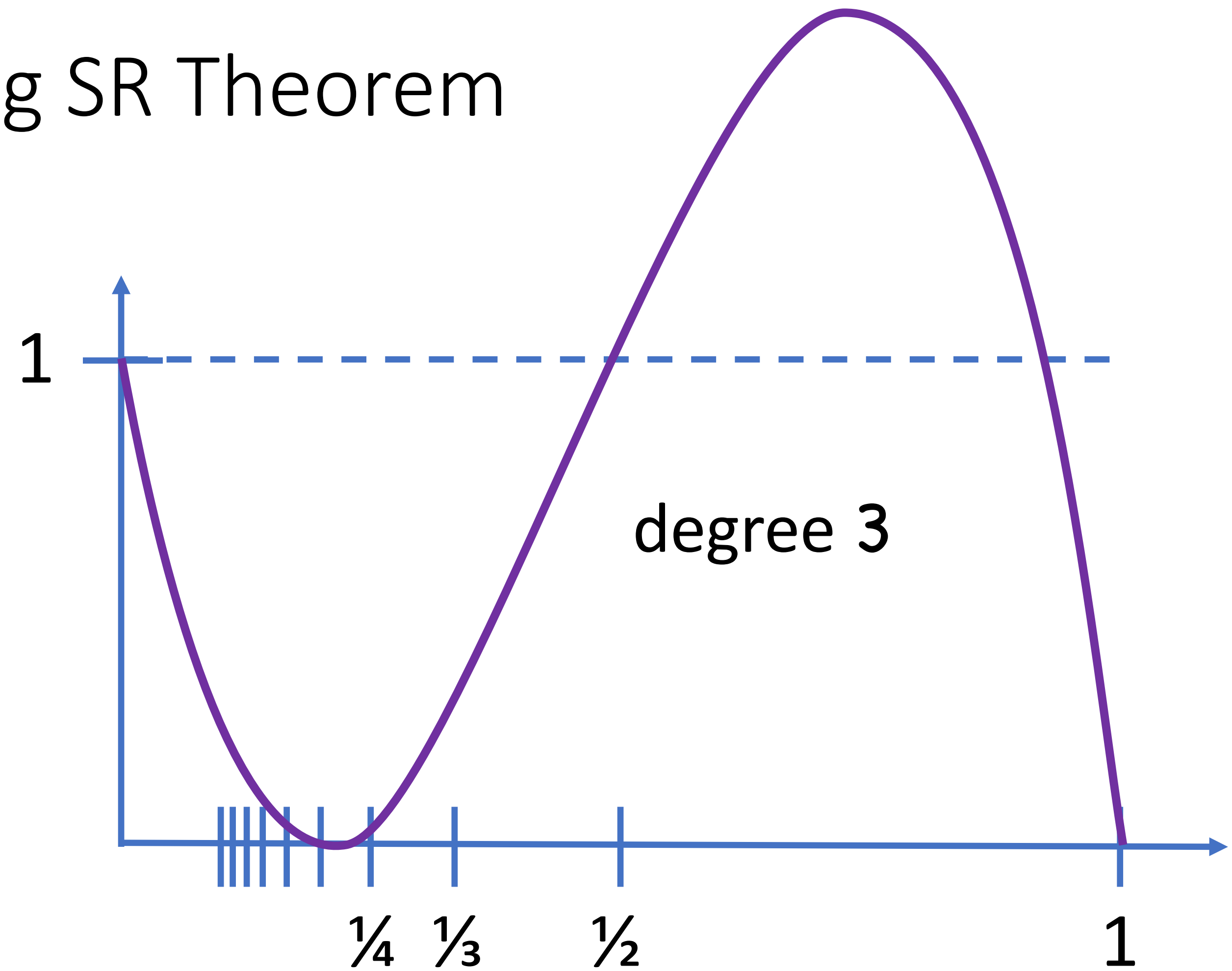
Proving SR Theorem



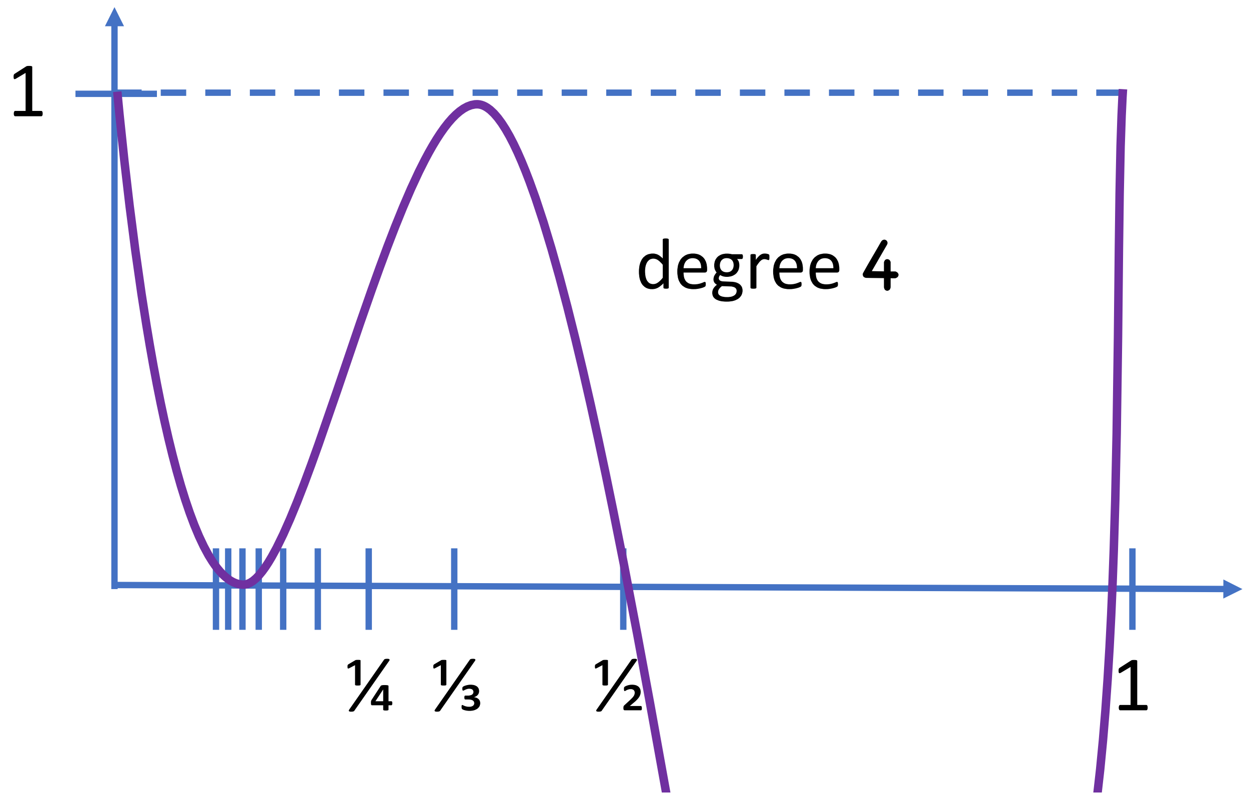
Proving SR Theorem



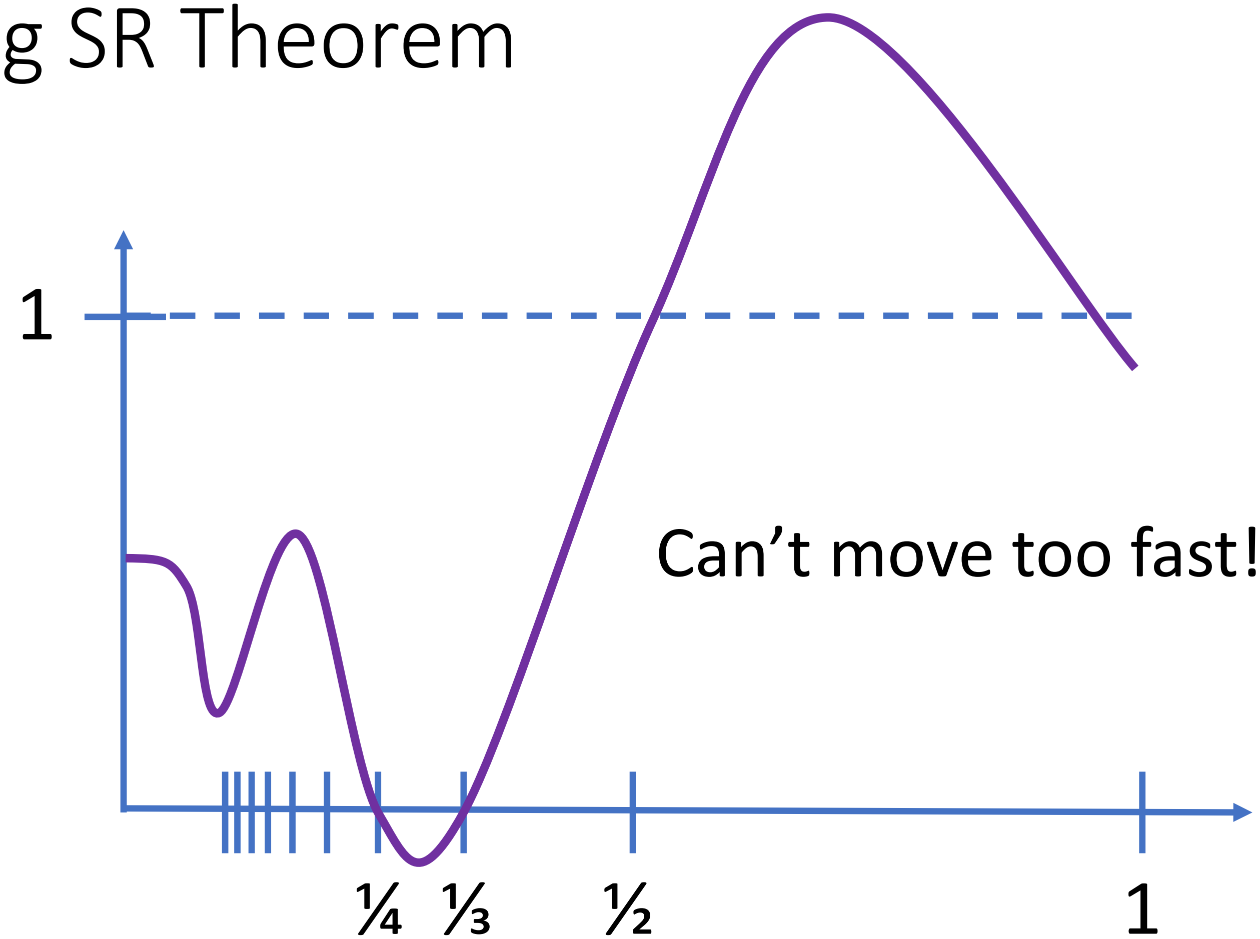
Proving SR Theorem



Proving SR Theorem



Proving SR Theorem



Proving SR Theorem

Thm [Z'12b]: If $P(1/r)$ satisfies:

- Degree $\leq k$
- $0 \leq p(1/r) \leq 1$ $\forall$ positive integers r

Then $|P(1/r) - P(0)| \leq 27k^3/r$

(Asymptotically tight)

Remaining Step

SR_r requires random functions; how to simulate?

Only **2q-wise** marginals matter

→ **2q**-wise independent functions "look" random

What else is out there?

Secret sharing

Encryption

Authentication

IBE

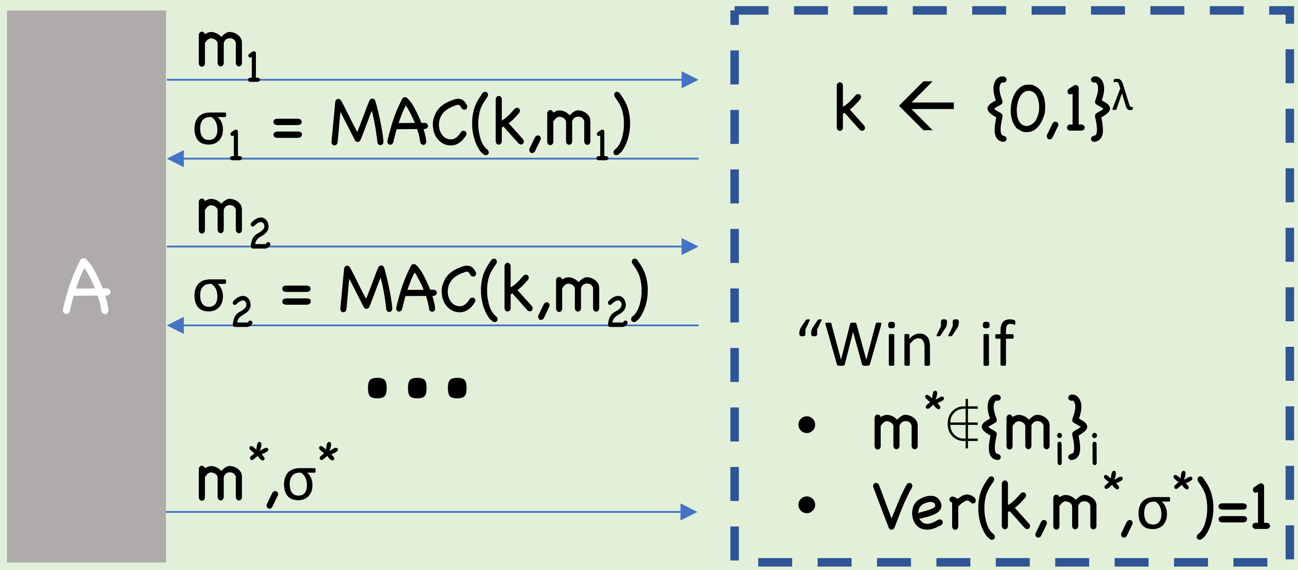
PRPs

MPC

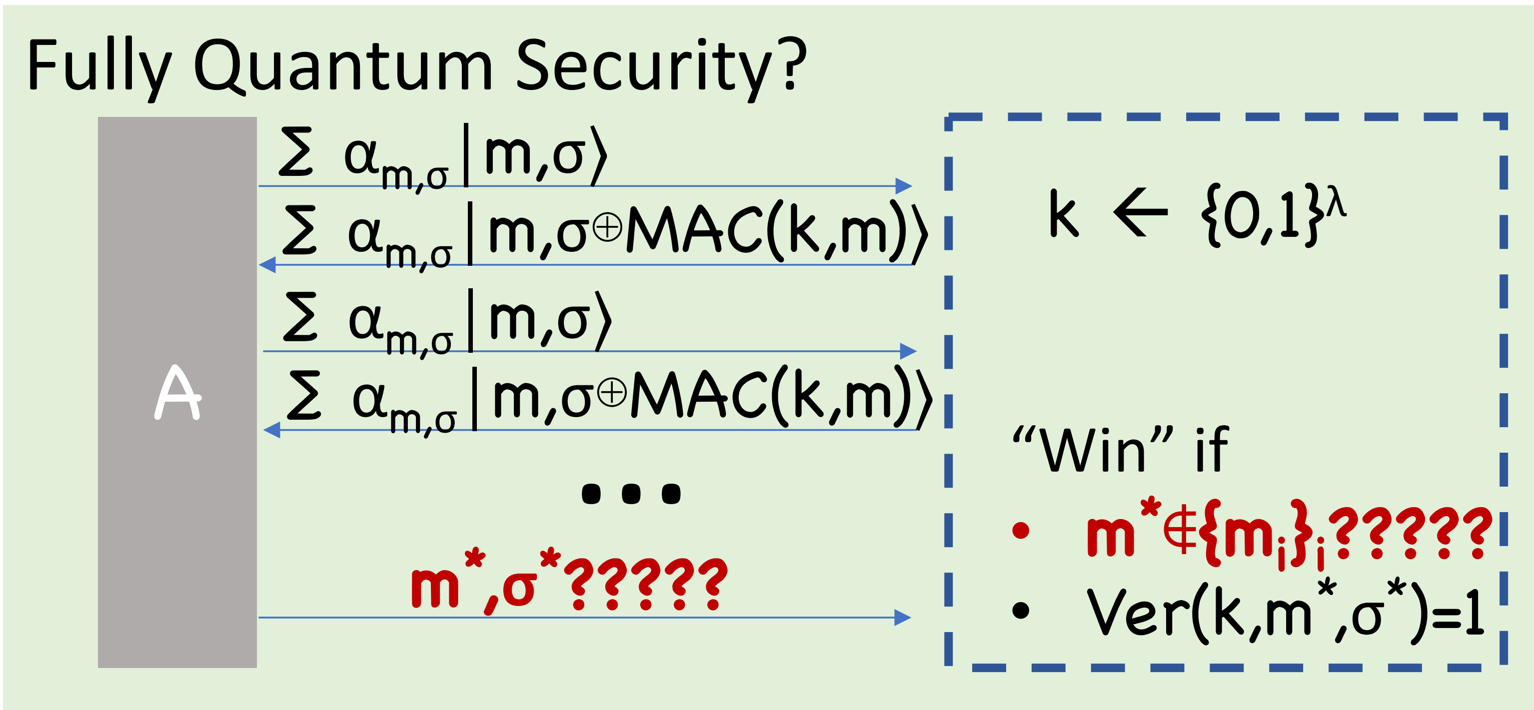
Remainder of lecture: definitional issues

Defining MACs/Signatures

Classical Security:



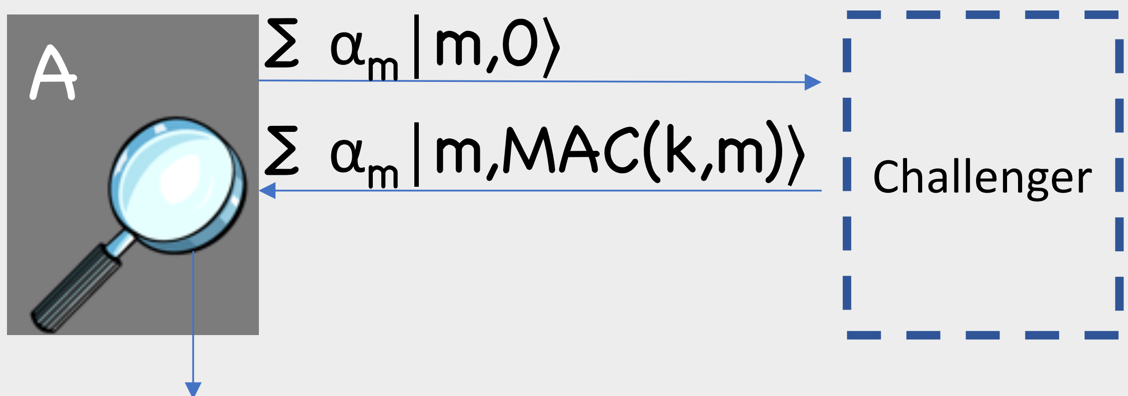
Defining MACs/Signatures



Defining MACs/Signatures

What does it mean to be "new"?

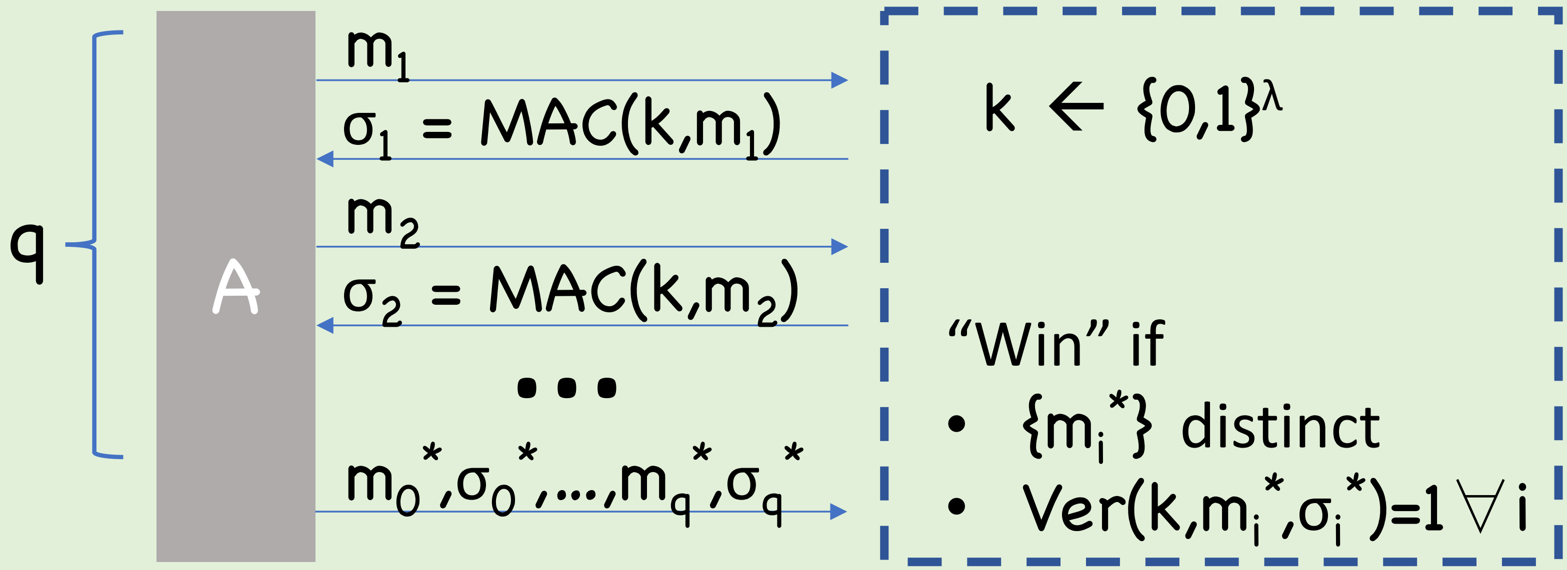
Example:



Random m, MAC(k,m)

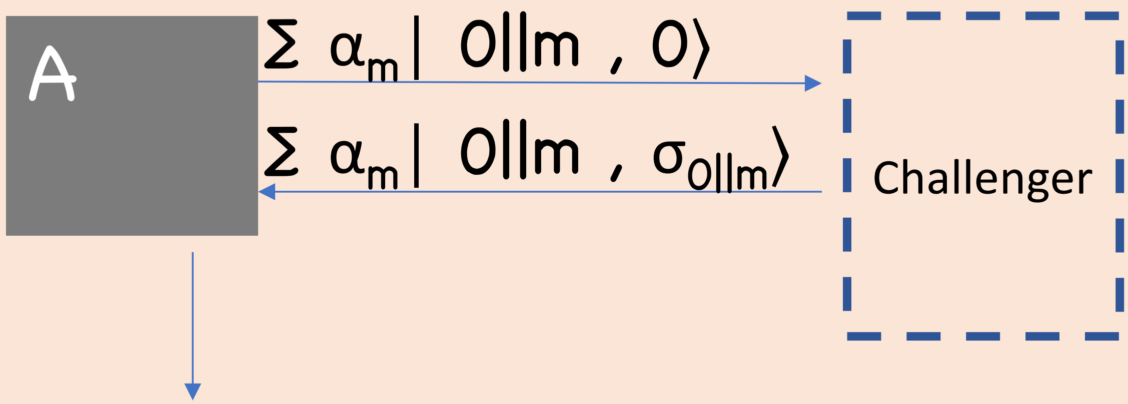
Defining MACs/Signatures

Partial Answer: One More Security [Boneh-Z'13a]



Defining MACs/Signatures

Limitation: Suppose:



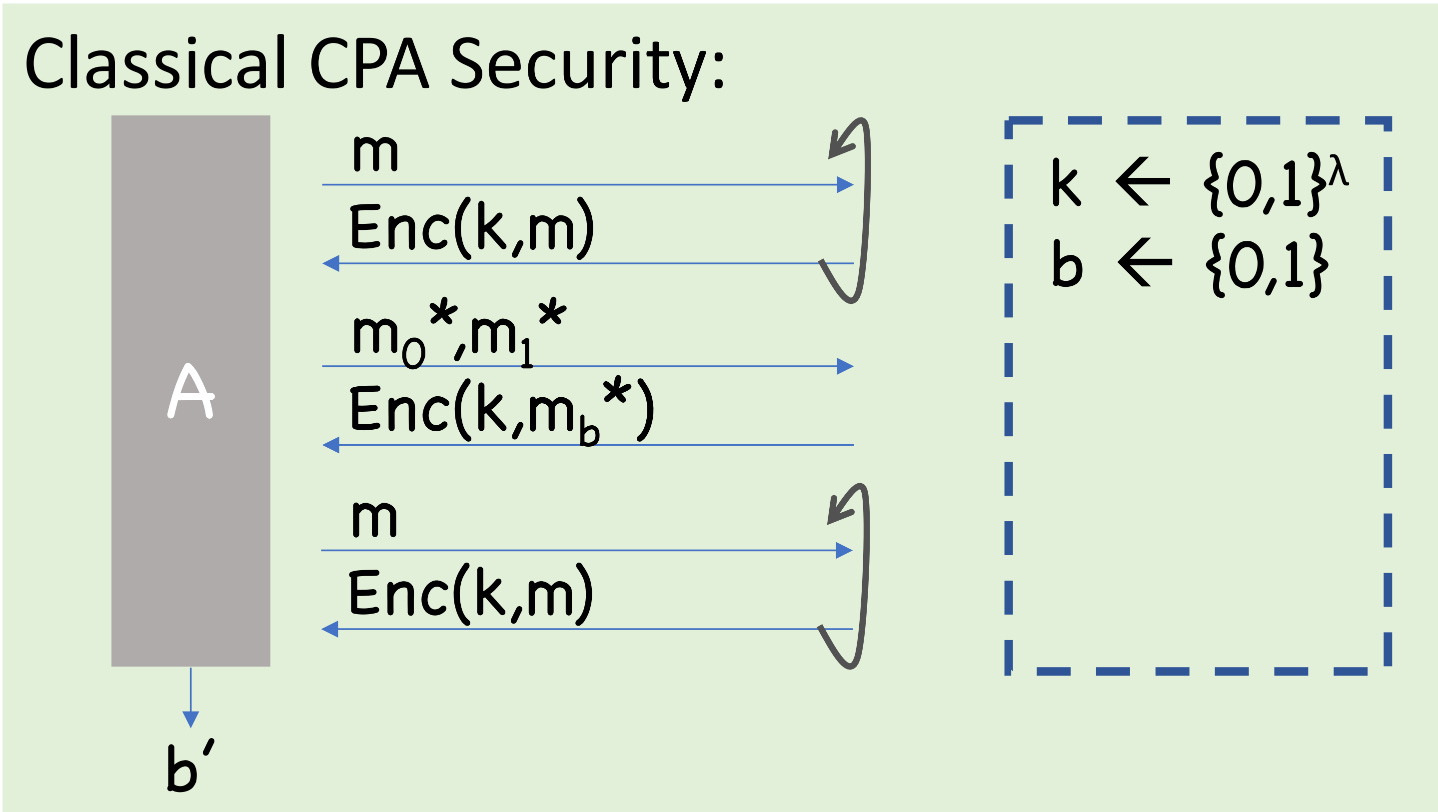
1||m, MAC(k, 1||m)

Doesn't violate one-more security!

Defining MACs/Signatures

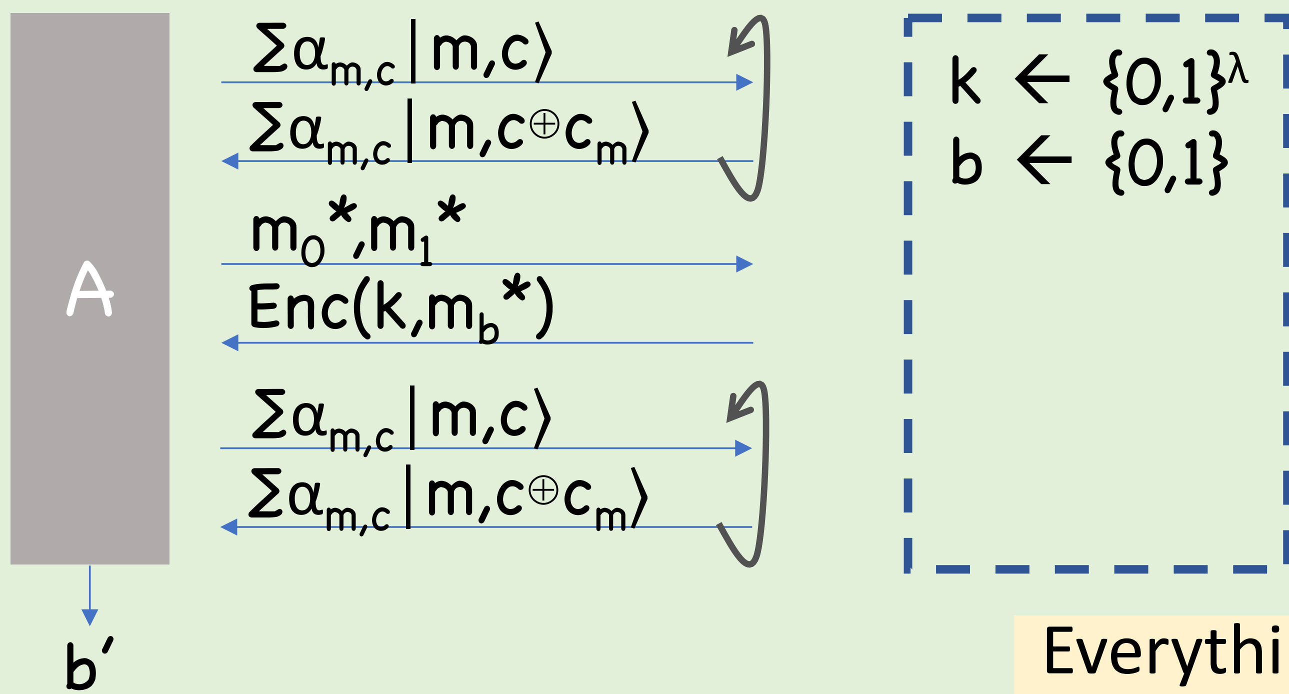
Other defs exist which fix this problem [Garg-Yuen-Z'17, Alagic-Majenz-Russell-Song'18], but IMO even satisfactory definition not yet solved

Defining Encryption



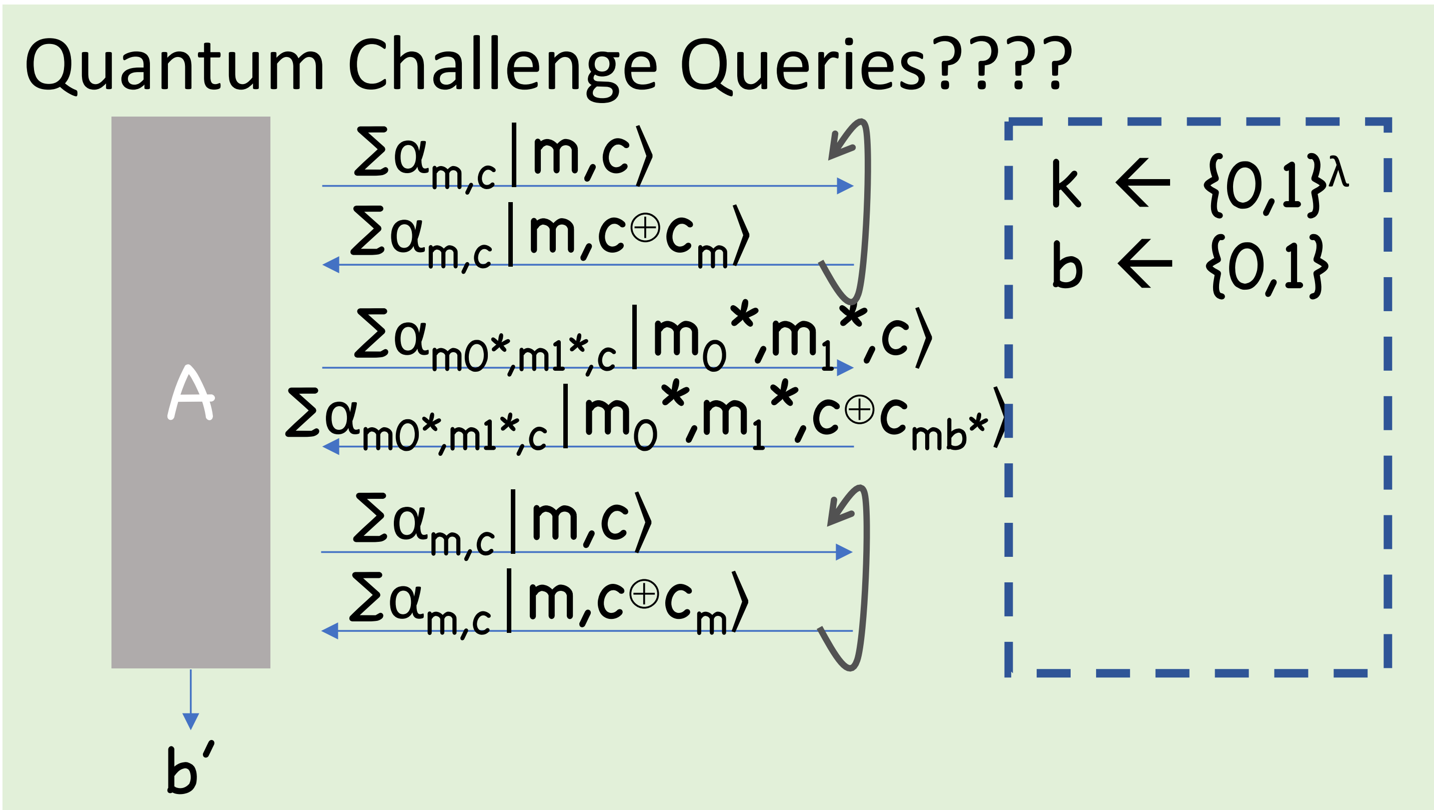
Defining Encryption

Quantum CPA Attacks?



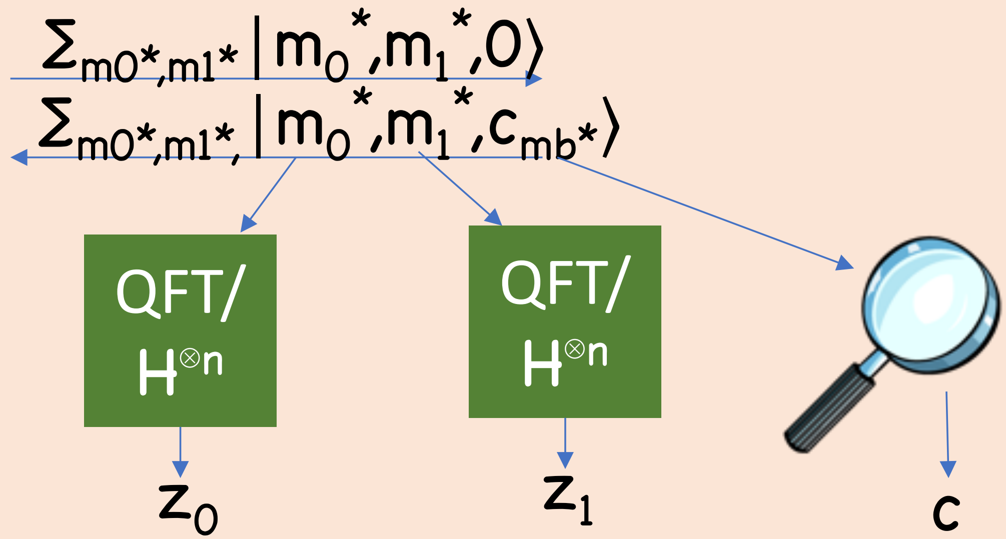
Everything is fine so far

Defining Encryption



Defining Encryption

Attack:



$z_{1-b}=0^n$ and whp $z_b \neq 0^n$

Defining Encryption

Classical encryption schemes are not secure for encrypting quantum messages, *if the attacker gets to see the original message registers*

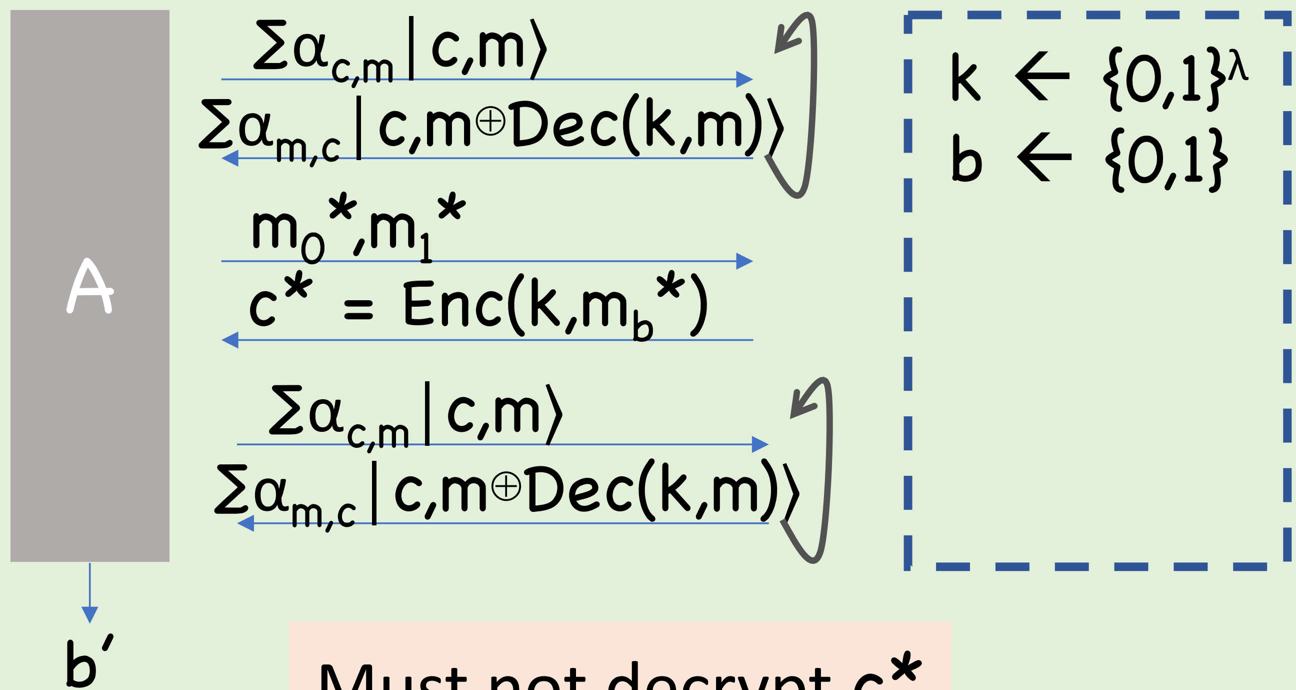
[Boneh-Z'13b]: don't allow quantum challenge queries

[Gagliardoni-Hülsing-Schaffner'16]: make sure quantum challenge query never returned

More subtle than it sounds

Defining Encryption

Quantum CCA Attacks?



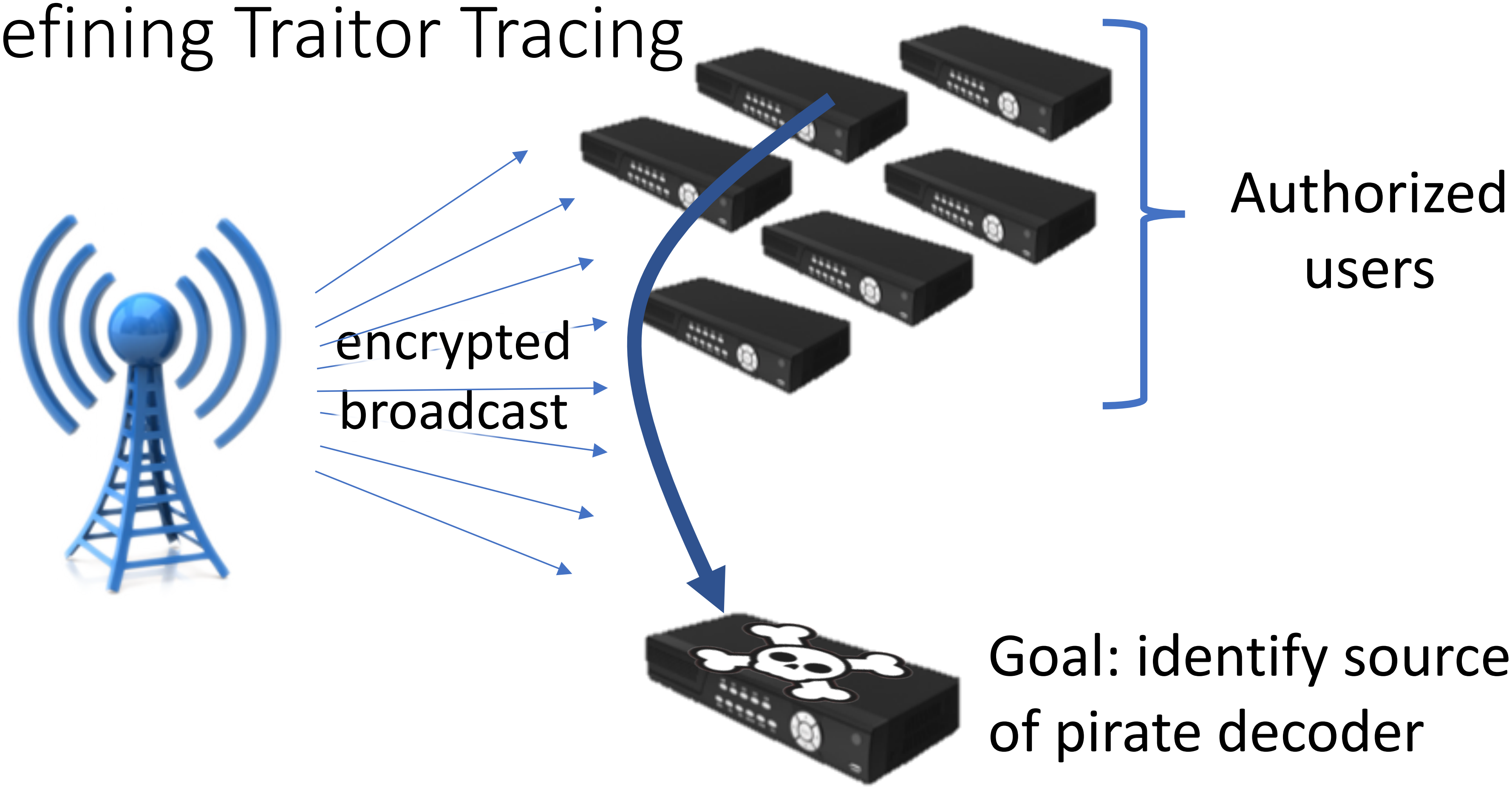
Must not decrypt c*

Defining Encryption

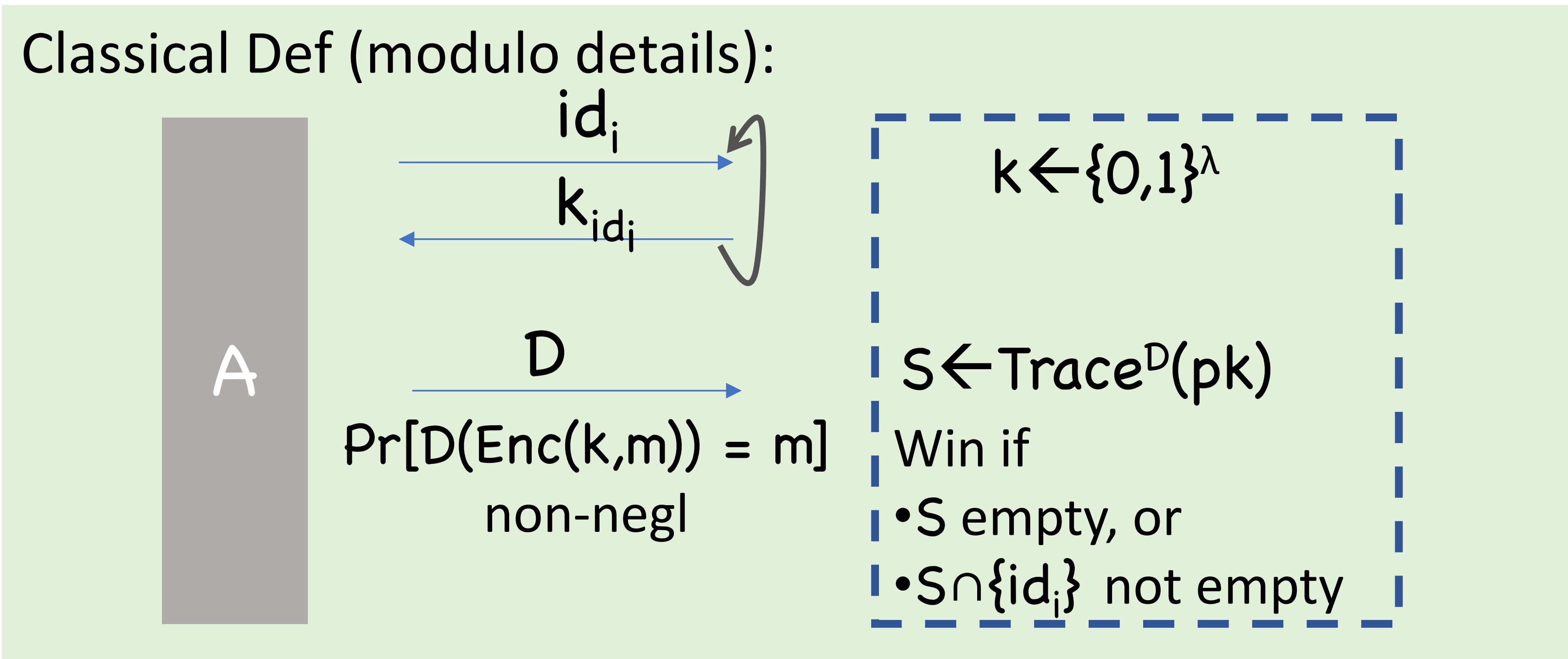
"Not decrypting **c***" problematic for quantum challenges

[Chevalier-Ebrahimi-Vu'20]: Formalize quantum CCA+Challenge

Defining Traitor Tracing



Defining Traitor Tracing



Defining Traitor Tracing

Problem: most prior work assumes
D is stateless/can be rewound

Somewhat inherent: single query
to D usually not enough to accuse

But if decoder has quantum state,
single query may alter decoder

[Z'20]: Formalize quantum analog of "stateless"

Tomorrow: Unavoidable Quantum Attacks

So far, issues concern new quantum attack models

My remaining lectures: attacks/issues even under existing attack model

- Rewinding
- Quantum Random Oracle Model