Post-Quantum Cryptography

Mark Zhandry (NTT Research & Stanford University)

Outline for this morning

1. Crash course in quantum computing

2. Impacts on existing cryptosystems

3. An overview of post-quantum cryptography
   - New cryptographic assumptions
   - New security proofs
   - New definitions

1. A crash course in quantum computing

Classical Probabilistic Systems: Modeling Uncertainty

State of system
= probability vector

$$\mathbf{v} = \begin{bmatrix} 0.1 \\ 0.3 \\ 0.2 \\ 0.1 \\ 0.2 \\ 0.1 \end{bmatrix}$$

"state is **x** with prob $\mathbf{v}_x$"

$\mathbf{v} \geq \mathbf{0}$

$|\mathbf{v}|_1 = \sum_x \mathbf{v}_x = \mathbf{1}$

Act on system by
stochastic process

$$\mathbf{v} \rightarrow \mathbf{A.v}$$

$$\mathbf{A} = \begin{bmatrix} 0.3 & 0.3 & 0.1 & 1.0 & 0.2 & 0.1 \\ 0.3 & 0.4 & 0.1 & 0.0 & 0.2 & 0.2 \\ 0.2 & 0.0 & 0.1 & 0.0 & 0.2 & 0.3 \\ 0.1 & 0.2 & 0.1 & 0.0 & 0.2 & 0.4 \\ 0.1 & 0.1 & 0.6 & 0.0 & 0.2 & 0.0 \end{bmatrix}$$

"**x** moves to **y** with probability $\mathbf{A}_{yx}$"

$\mathbf{A} \geq \mathbf{0}$

$|\mathbf{A}_x|_1 = \mathbf{1}\ \forall \mathbf{x}$

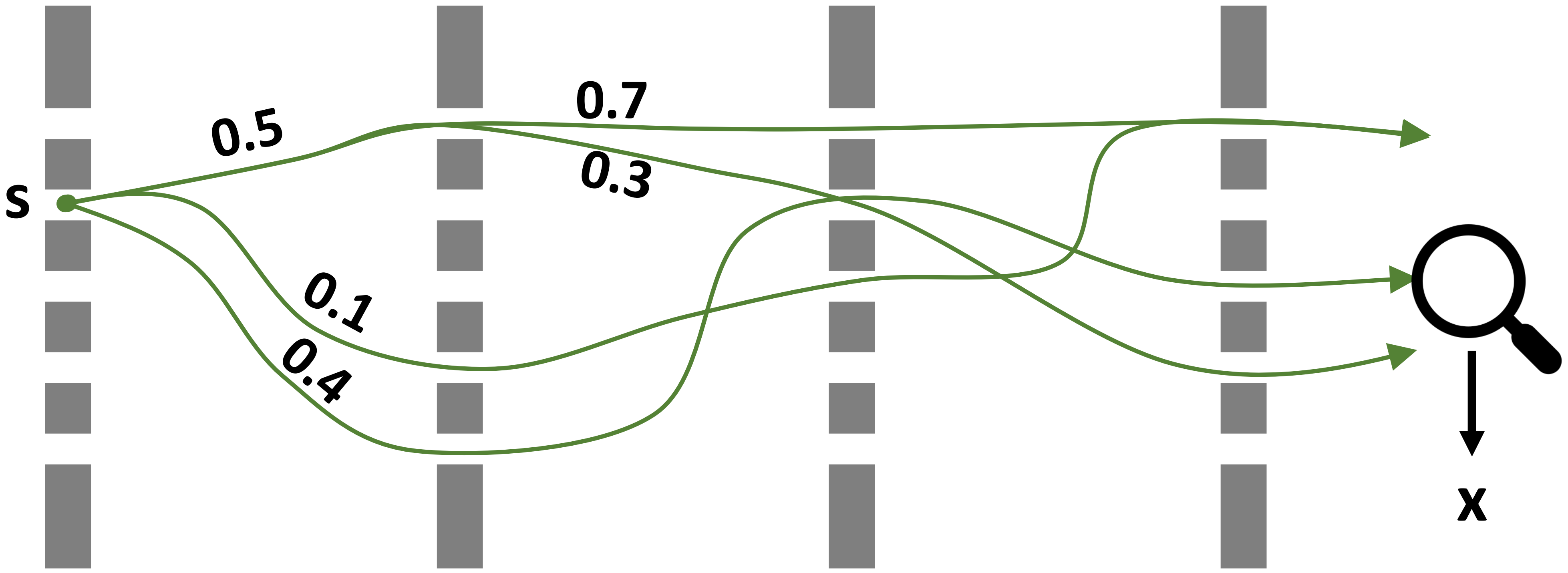
Preserves norm of state vector

Get info out by
observations

x with prob $\mathbf{v}_x$

State "collapses" to
have all amplitude on **x**

Classical Probabilistic Systems



W(path **p) :=** $\prod$**(**probabilities along path**) = Pr[p]**

$$\mathbf{Pr[x] = \sum_{p:s \to x} W(p)}$$

Quantum Systems

State of system
= **amplitude** vector

$$\mathbf{v} = \begin{bmatrix} -0.1 \\ 0.3 \\ 0.2+0.4i \\ 0.6 \\ -0.3 \\ 0.4-0.3i \end{bmatrix}$$

$$|\mathbf{v}|_2^2 = \sum_x |\mathbf{v}_x|^2 = 1$$

$$(\ |a+bi|^2 = a^2+b^2 \ )$$

Act on system by
unitary matrices

$$\mathbf{v} \rightarrow \mathbf{U.v}$$

To preserve norm,
U is *unitary:*

$$\mathbf{U^\dagger U = UU^\dagger = I}$$

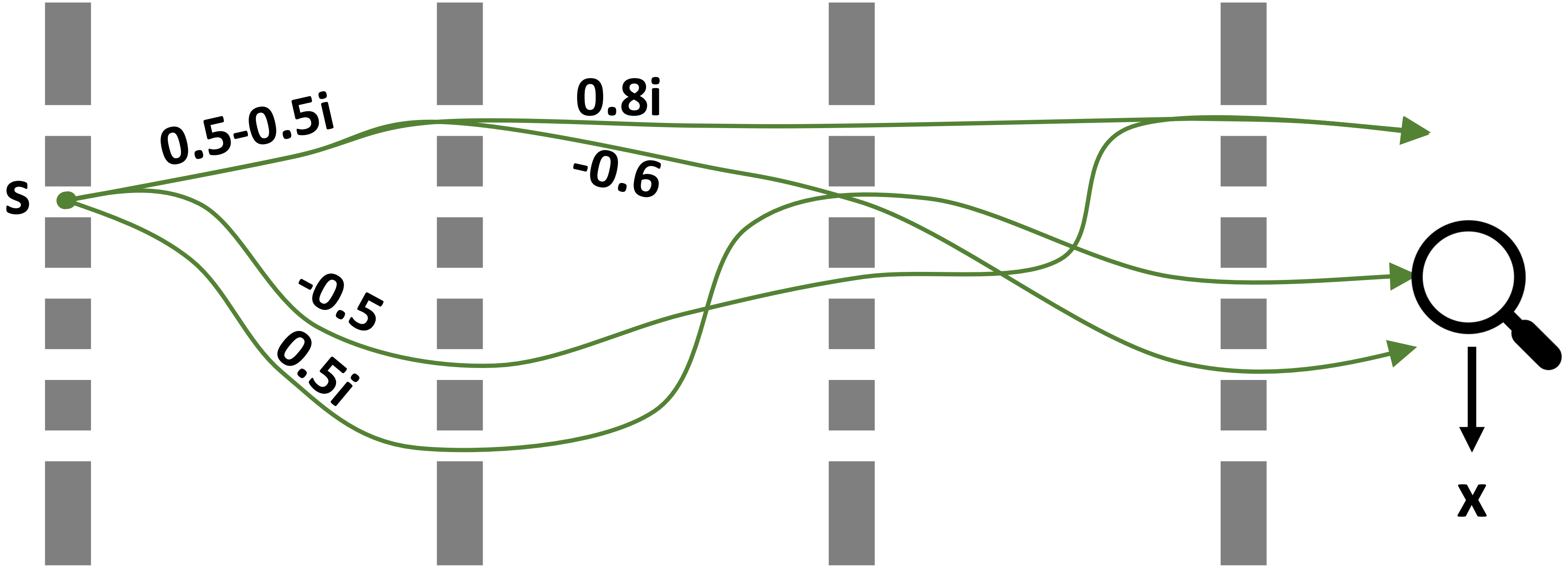
Replace **i** with
–i, transpose

Get info out by
measurements

x with prob $|\mathbf{v}_x|^2$

State "collapses" to
have all amplitude on **x**

Quantum Systems



W(path **p) :=** $\prod$**(**weights along path**)**

$$\Pr[y] = \left| \sum_{p:s \to y} W(p) \right|^2$$

Conceptual Diffs Between Quantum and Classical

Quantum states are physical (do **not** model uncertainty)

(density matrix formalism for uncertain quantum states)

Paths can "interact", or interfere:

Constructive interference: $\left| \sum W(p) \right|^2 \gg \sum \left| W(p) \right|^2$

Destructive interference: $\left| \sum W(p) \right|^2 \ll \sum \left| W(p) \right|^2$

Verifying Quantum States

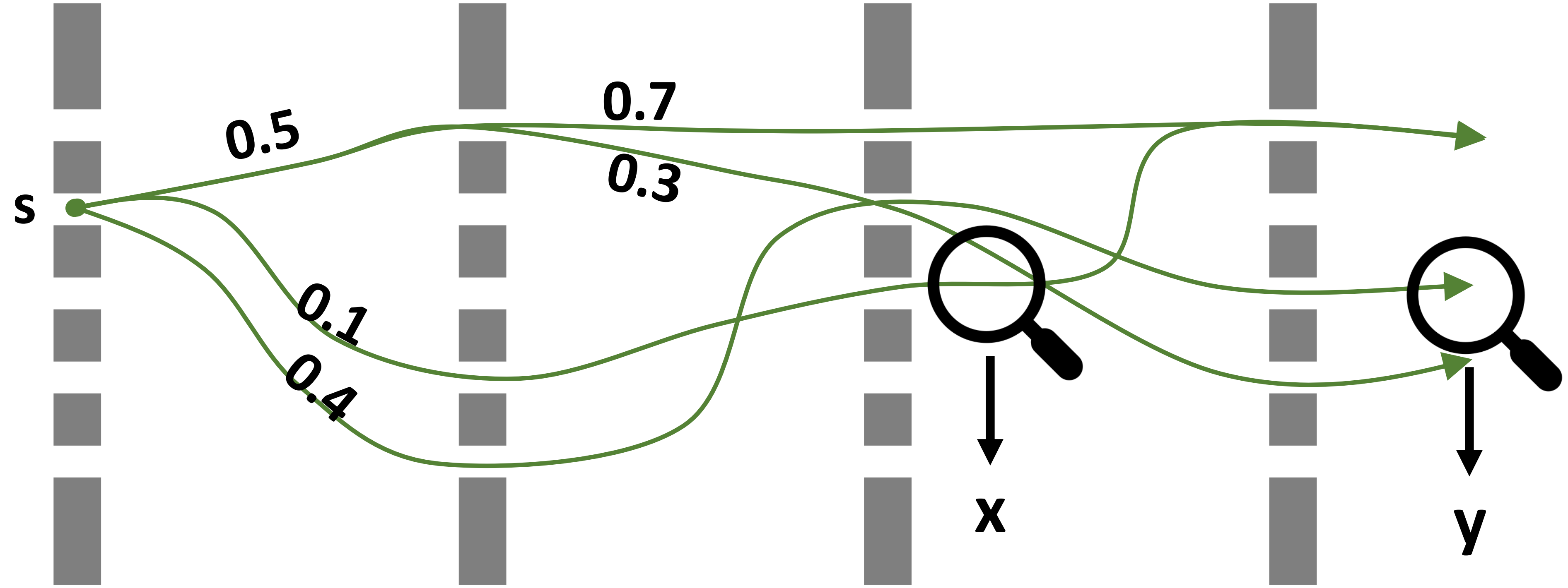
For any state $\mathbf{v}$, ∃ unitary $\mathbf{U_v}$ such that

$$\mathbf{U_v} \, . \, \mathbf{v} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} \Rightarrow$$

Can verify if a state is $\mathbf{v}$ by applying $\mathbf{U_v}$ and then measuring

Equivalent statement for stochastic processes: given sample from distribution, decide if that distribution is $\mathbf{v}$. Impossible!

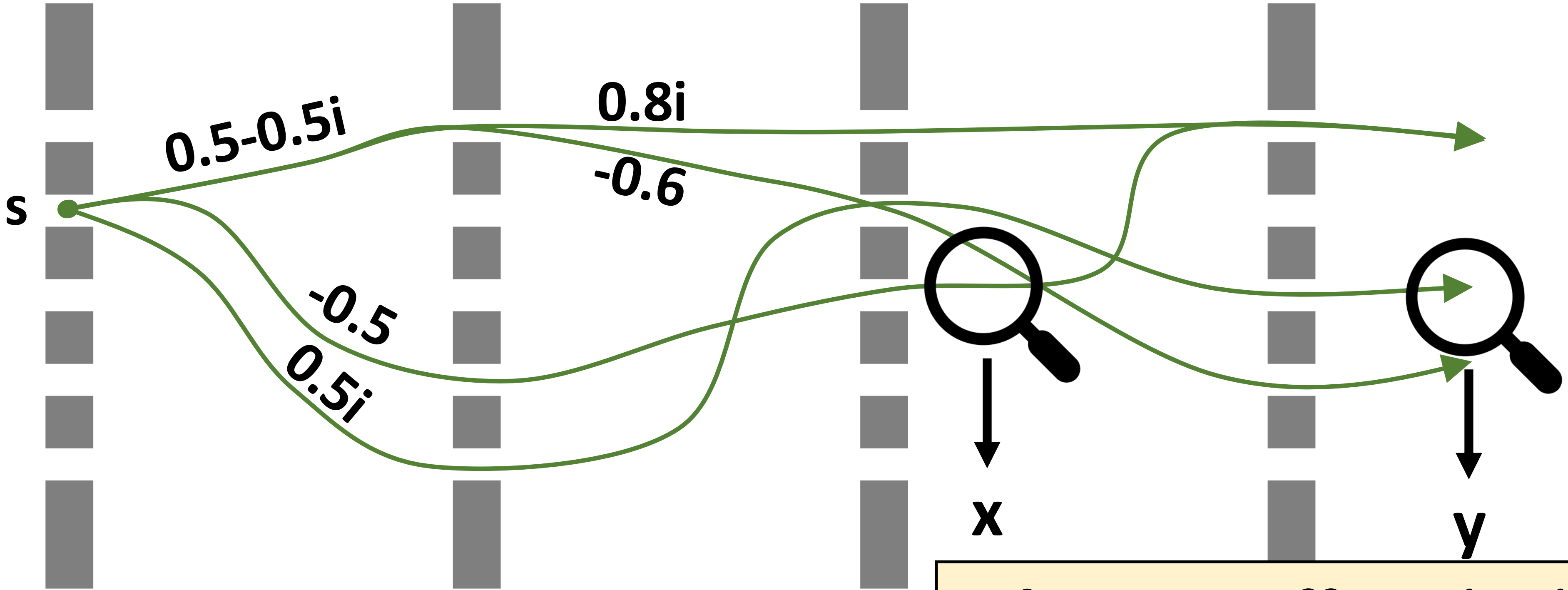
Intermediate Observation in Classical Process



$$\Pr[x \wedge y] = \sum_{p:s \rightarrow x \rightarrow y} W(p)$$

$$\sum_{x} \Pr[x \wedge y] = \sum_{x,p:s \rightarrow x \rightarrow y} W(p) = \sum_{p:s \rightarrow y} W(p) = \Pr[y]$$

Intermediate Observation in Quantum Process



$$\Pr[x \wedge y] = \Big| \sum_{p: s \to x \to y} W(p) \Big|^2$$

Observer effect: looking at a quantum system changes it

$$\sum_x \Pr[x \wedge y] = \sum_x \Big| \sum_{p: s \to x \to y} W(p) \Big|^2 \neq \Pr[y]$$

Quantum No Cloning

Sample from unknown distribution

Classical "no cloning": given unknown stochastic state, impossible to produce two copies of that state

Two iid samples from same distribution

Actual physical state

Quantum "no cloning": given unknown quantum state, impossible to produce two copies of that state

Quantum computing =

Using constructive interference to get answer with higher probability

⬍

Get answer *faster*

Ket Notation

Typically denote quantum state vectors with “ket” notation

$$|\psi\rangle = \sum_x \alpha_x |x\rangle$$

$|0\rangle$ $|1\rangle$

All amplitude on 0 All amplitude on 1

Quantum ≥ Classical

$$f : \{0,1\}^n \to \{0,1\}^m$$

⬇

$$O_f \sum_{x,y} \alpha_{x,y} |x, y\rangle = \sum_{x,y} \alpha_{x,y} |x, y \oplus f(x)\rangle$$

If **f** is efficiently computable by classical circuit, $\mathbf{O_f}$ is efficiently computable by quantum circuit

Needed to ensure unitarity, regardless of **f**

Quantum Fourier Transform (QFT)

$$|\psi\rangle = \sum_{x=0}^{N-1} \alpha_x |x\rangle \mapsto |\hat{\psi}\rangle = \sum_{y=0}^{N-1} \hat{\alpha}_y |y\rangle$$

$$\hat{\alpha}_y = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} \alpha_x e^{i2\pi xy/N}$$

$$\alpha_x = \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} \hat{\alpha}_y e^{-i2\pi xy/N}$$

Quantum Fourier Transform (QFT)

Uniform superposition: $\text{QFT}_N|0\rangle = \frac{1}{\sqrt{N}}\sum_{y=0}^{N-1}|y\rangle$

Subspaces: $|S\rangle = \frac{1}{\sqrt{|S|}}\sum_{x\in S}|x\rangle \mapsto |S^\perp\rangle = \frac{1}{\sqrt{|S^\perp|}}\sum_{y\in S^\perp}|y\rangle$

Shift→Phase: $\sum_x \alpha_x|x+\Delta \bmod N\rangle \mapsto \sum_y \hat{\alpha}_y e^{i2\pi y\Delta}|y\rangle$

Convolve→Product: $\sum_x \alpha_x\beta_z|x+z \bmod N\rangle \mapsto \sqrt{N}\sum_y \hat{\alpha}_y\hat{\beta}_y|y\rangle$

Quantum Period-Finding

(aka Abelian Hidden Subgroup Problem)

Suppose given function **f** with promise that there exists (hidden) subspace **S** s.t.:

$$f(x+y) = f(x) \forall y \in S$$

$$f(x+y) \neq f(x) \forall y \notin S$$

Goal: find **S**

Easy Thm: Any classical algorithm that treats **f** as black box requires exponential time

Quantum Period-Finding

(aka Abelian Hidden Subgroup Problem)

An efficient quantum algorithm [Simon'94,Shor'94]

(1) Prepare $$\sum_x |x, 0\rangle$$

(2) Apply $\mathbf{O_f}$: $$\sum_x |x, f(x)\rangle$$

(3) Measure **f(x)**: obtain **y**, state collapses to

$$\sum_{x:f(x)=y} |x, y\rangle$$

Quantum Period-Finding

(aka Abelian Hidden Subgroup Problem)

An efficient quantum algorithm [Simon'94,Shor'94]

(4) Discard **y**: $\sum_{x:f(x)=y} |x\rangle = \sum_{x \in S} |x + x_0\rangle$

$\mathbf{x_0}$ arbitrary s.t. $\mathbf{f(x_0)=y}$

(5) Apply **QFT**: $\sum_{z \in S^\perp} e^{i2\pi x_0 z/N} |z\rangle$

(6) Measure **z** to obtain random vector in $\mathbf{S}^\perp$

Repeat **O(dimension)** times to learn $\mathbf{S}^\perp$, and hence **S**

2. Impacts on existing cryptosystems

For this morning, will only consider **classical** cryptosystems, but allow adversary **quantum** attacks

Discrete Log as Period Finding [Shor'94]

Discrete log: given $\mathbf{g},\mathbf{h}=\mathbf{g}^{\mathbf{a}}$ (over some group **G**), find **a**

Define $\mathbf{f(x,y) = g^x h^y}$

Observe $\mathbf{f(\ (x,y) + (-a,1)\ ) = f(x,y)}$

Period finding → find **(-a,1)** → **a**

Factoring as Period Finding [Shor'94]

Factoring: given **N=pq,** find **p,q**

Define $\mathbf{f(x) = g^x \bmod N}$

Observe $\mathbf{f(\ x + (p-1)(q-1)\ ) = f(x)}$

Period finding → find **(p-1)(q-1)** → **p,q**

(Not actually how it works. Some annoying details to get it totally right)

Consequences

Public Key Cryptography:

- All widely-used schemes rely on Factoring or Dlog
- → quantumly insecure

Private-key Cryptography:

- Typical schemes (SHA, AES) don’t have the needed periodic structure → seem immune to Shor’s algorithm
- Quadratic speedups due to [Grover’96] → must double key sizes

3. An overview of post-quantum cryptography

Fundamental Formula of Modern Cryptography

Crypto security "proof" =

Formal Security Model **M**

Captures "realizable" attacks
E.g. EUF-CMA, IND-CCA

\+

Computational Assumption **P**

Must be realistic assumptions
Concrete: Factoring, Dlog, LWE
Generic: ∃OWF, ∃PKE

\+

Reduction from **P** to **M**

Breaking **M** at least as hard as **P**

Fundamental Formula of PQ Cryptography

Post-quantum “proof” = *Post-quantum* Model **M** + *Post-quantum* Assumption **P** + *Post-quantum* Reduction

Post-quantum Model **M**: Model should capture actual quantum attack scenarios

Post-quantum Assumption **P**:
Concrete: (quantum) LWE
Generic: ∃ (quantum-immune) OWF, ∃PKE

Post-quantum Reduction: *Quantumly* breaking **M** at least as hard as *quantumly* solving **P**

An Incorrect Formula!

Post-quantum "proof"

$\neq$

Classical Model **M**

+

Post-quantum Assumption **P**

+

Classical Reduction

Must revisit all three ingredients!

3a. Post-Quantum Assumptions

Group Actions

Recall Classical Diffie-Hellman:

Only need exponentiation, not group multiplication

g^a $\rightarrow$ $\leftarrow$ g^b

$a \leftarrow Z_p^*$ $b \leftarrow Z_p^*$

$$k = g^{ab} = (g^a)^b = (g^b)^a$$

Group Actions

[Brassard-Yung'90]

Group **G** acting on a set **X** via $\mathbf{*} : \mathbf{G \times X \rightarrow X}$

Key identity: $\mathbf{(ab)*x = a*(b*x)}$

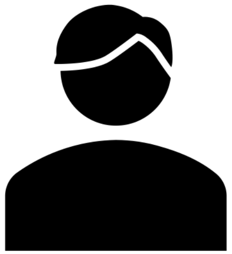
Exponentiation is a group action with group $\mathbf{G' = Z_p^*}$ acting on set $\mathbf{X = G}$

Group Actions

(Abelian) Group action Diffie-Hellman:

a*x →

← **b*x**



a ← G

b ← G

$$\mathbf{k = (ab)*x = a*(b*x) = b*(a*x)}$$

Group Actions

Analogs of traditional assumptions:

- Dlog: **(x, g*x) → g**
- CDH: **(x, a*x, b*x) → (ab)*x**
- DDH: **(x, a*x, b*x, (ab)*x) vs (x, a*x, b*x, c*x)**

Group Actions

[Couveignes'06, Rostovtsev-Stolbunov'06]: Shor's algorithm doesn't seem to apply to group actions that are not also groups

Recall that Dlog attack finds period of $\mathbf{f(x,y) = g^x \times h^y}$

↑

No analog on group actions!

Therefore, group actions may be plausible post-quantum candidates

Group Actions

Candidate post-quantum group actions:

- Isogenies over elliptic curves (abelian)
- Some non-abelian ones (e.g. McEliece)

General quantum hardness:

- [Ettinger-Hoyer-Knill'04]: Attack making **polylog(|G|)** queries to group action, but runs exponential time
- [Kuperberg'03]: For abelian case, attack with running time and query complexity $\mathbf{2^{O(\sqrt{|G|})}}$

Group Actions

Problem: lack of structure breaks many applications

Schnorr signatures from groups:

Sign(sk, m) = ($a=g^s$, c = H(a||m), r = s + sk c)

Ver($pk=g^{sk}$, m, (a,c,r)): Check **c == H(a||m)**
g^r==a×pk^c

No analog on group actions!

Group Actions

Problem: lack of structure breaks many applications

Group action Schnorr:

in **{0,1}**

Sign(sk, m) = (a = s*x, b = H(a||m), r = sk^b/s)

Ver(pk=sk*x, m, (a,b,r)): Check
b == H(a||m)
r*a == x if **b==0**
r*a == pk if **b==1**

Can think of as testing **r*a == $pk^b x^{1-b}$**

Group Actions

Problem: lack of structure breaks many applications

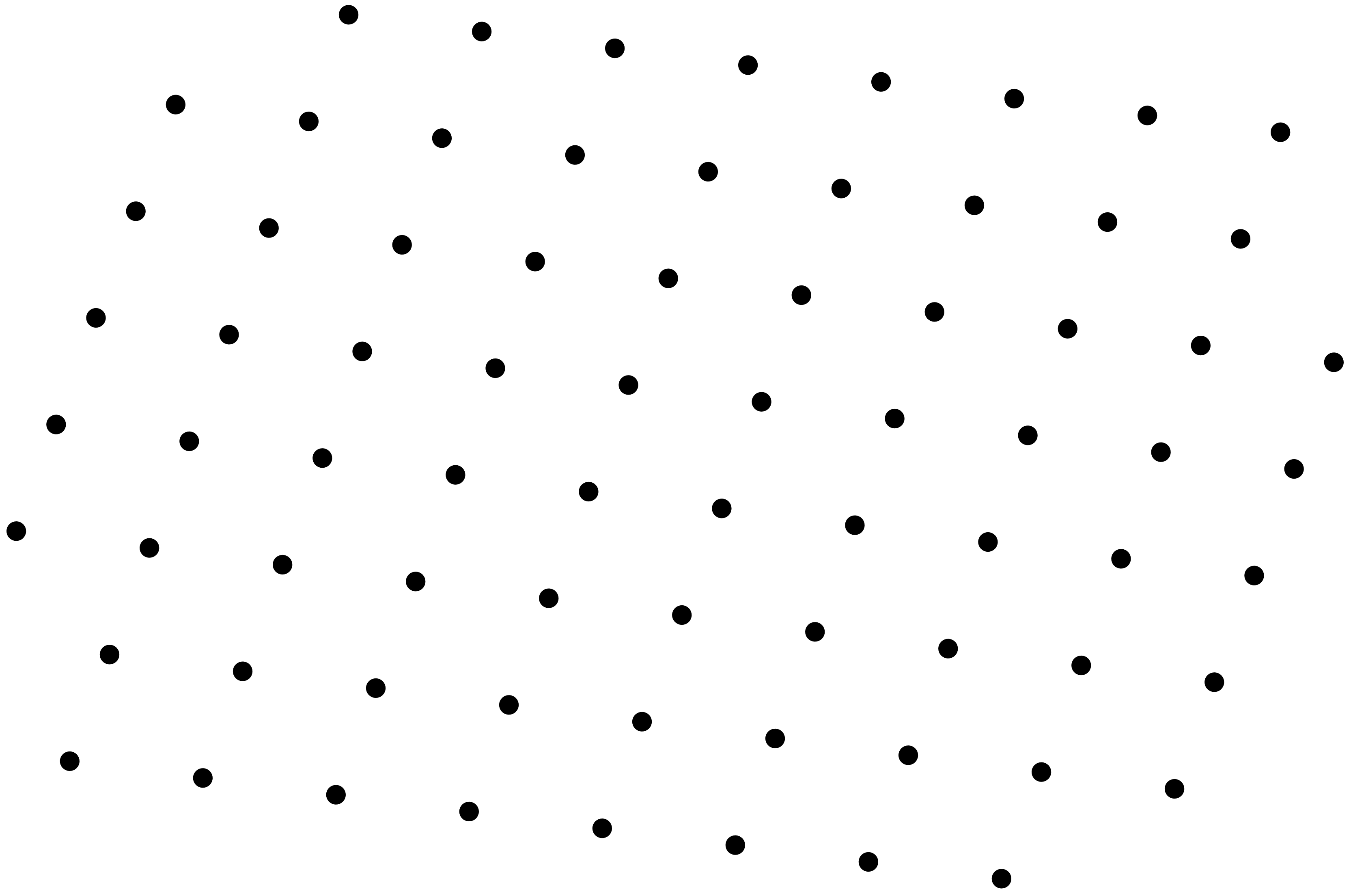
In order to get $\mathbf{2}^{-\lambda}$ soundness, must repeat $\boldsymbol{\lambda}$ times

Can optimize to $\boldsymbol{\lambda}$ **/ log(**$\boldsymbol{\lambda}$**)** [De Feo-Galbraith'19], which is optimal amongst large class of schemes [Boneh-Guan-**Z**'23]

Results in much larger signatures than classical

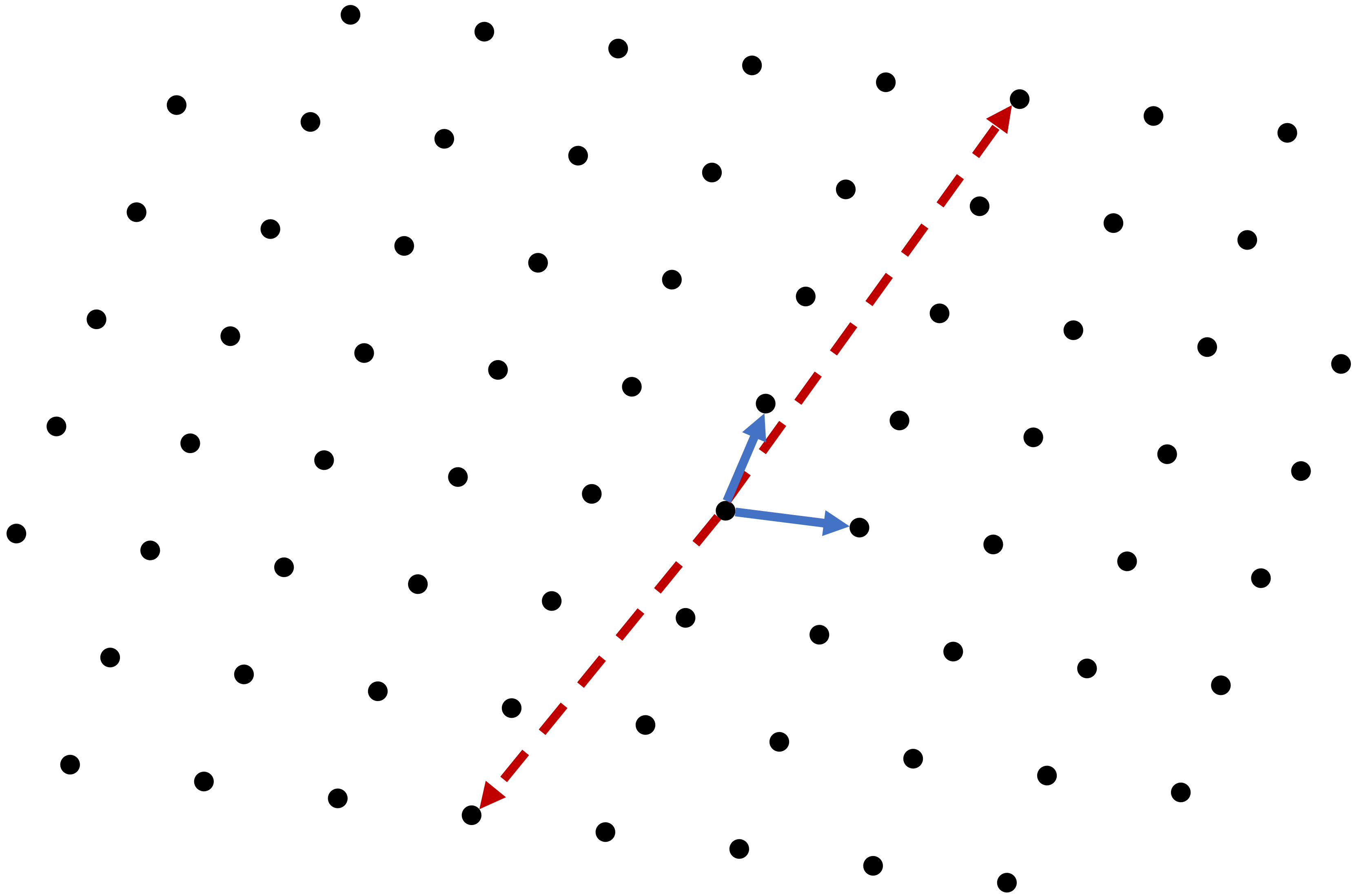
(Note: SQISign [De Feo-Kohel-Leroux-Petit-Wesolowski'22] is based on isogenies and achieves much better signature length. But departs from group action abstraction)

Lattices



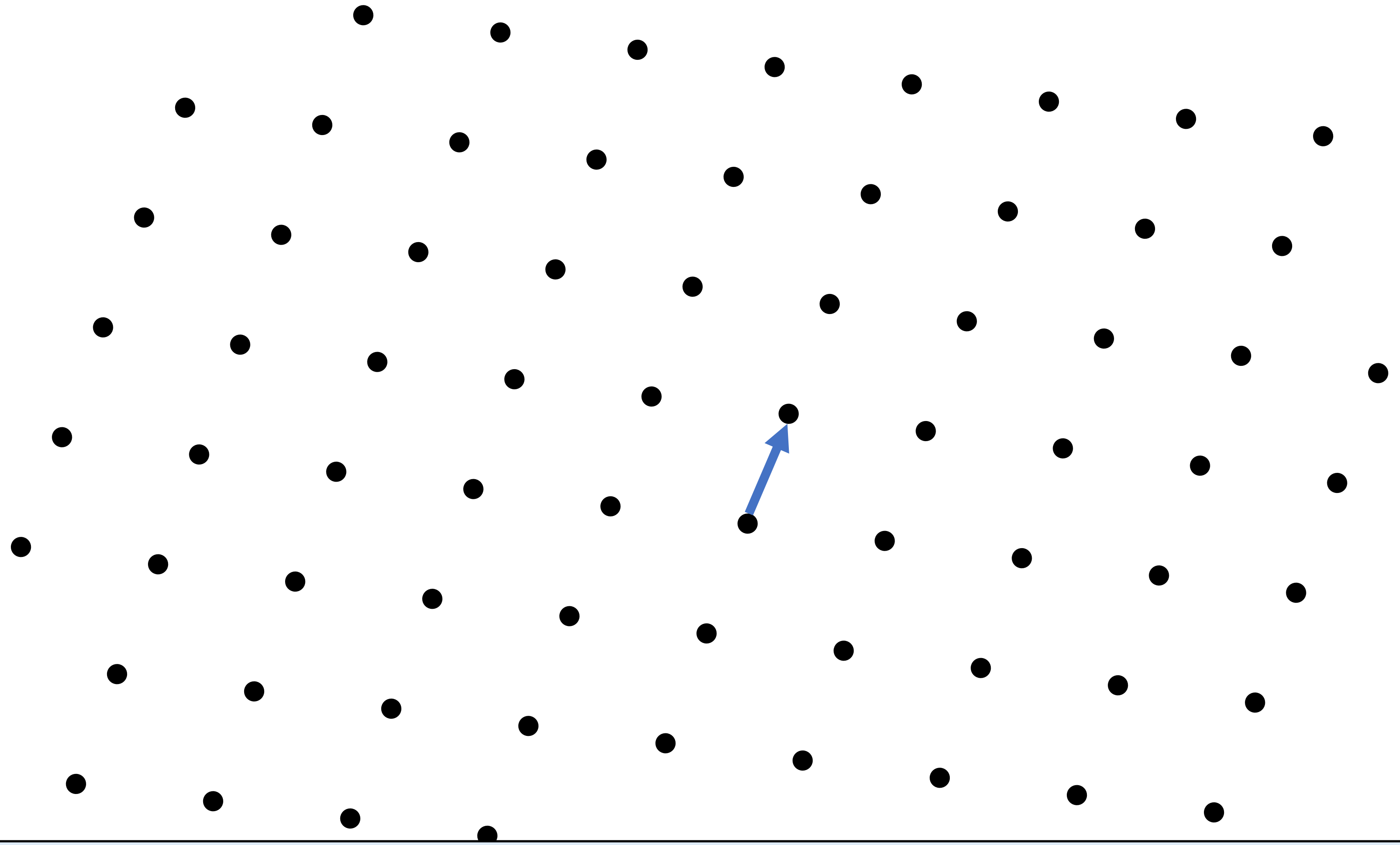
Imagine dimension in the 100s

Lattices



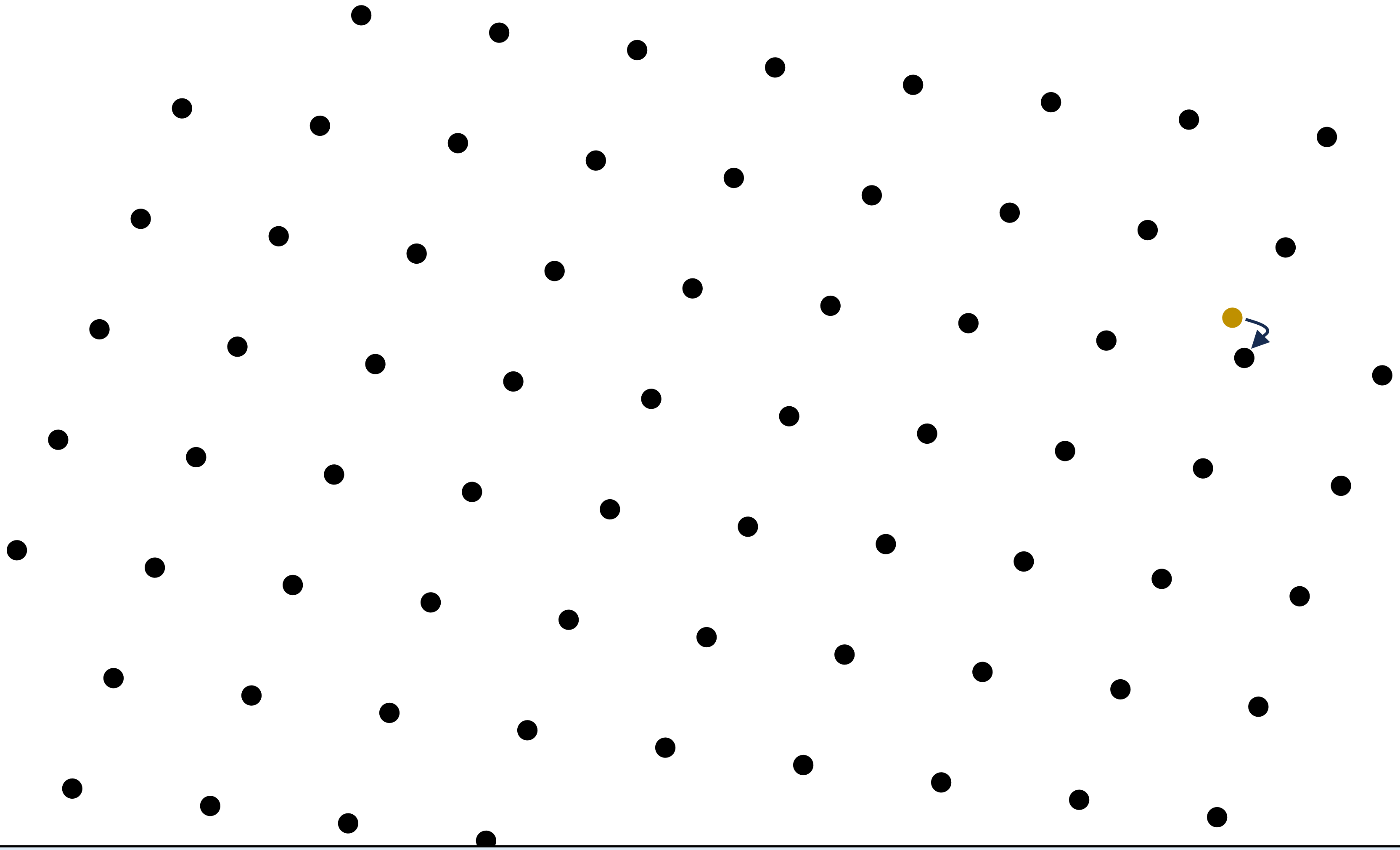
Basis: minimal set of vectors that generate lattice

Lattices



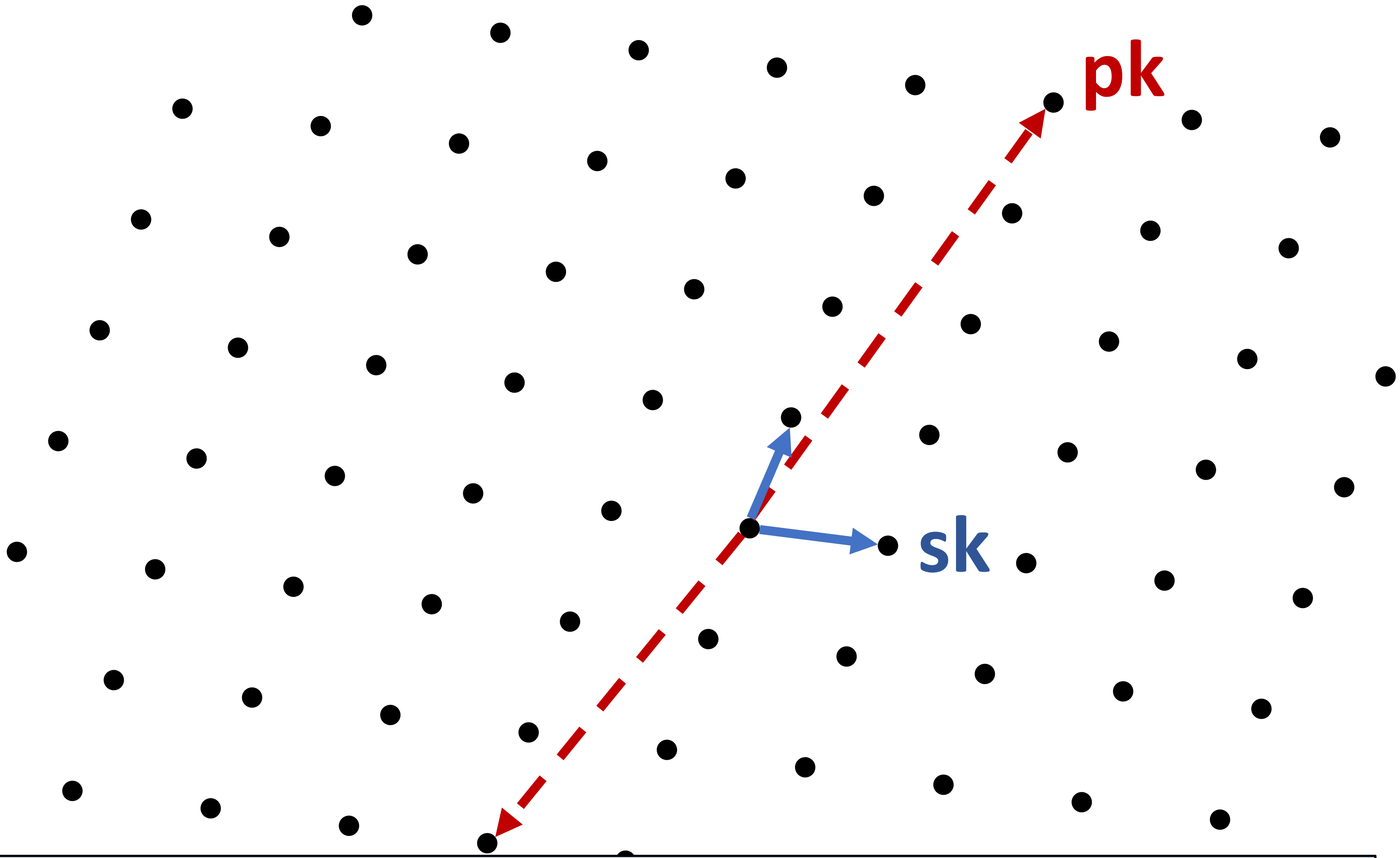
(Approx.) shortest vector problem (SVP): given lattice (described by some basis), find (approx.) shortest vector

Lattices



(Approx.) closest vector problem (CVP): given lattice and point off lattice, find (approx.) closest lattice point

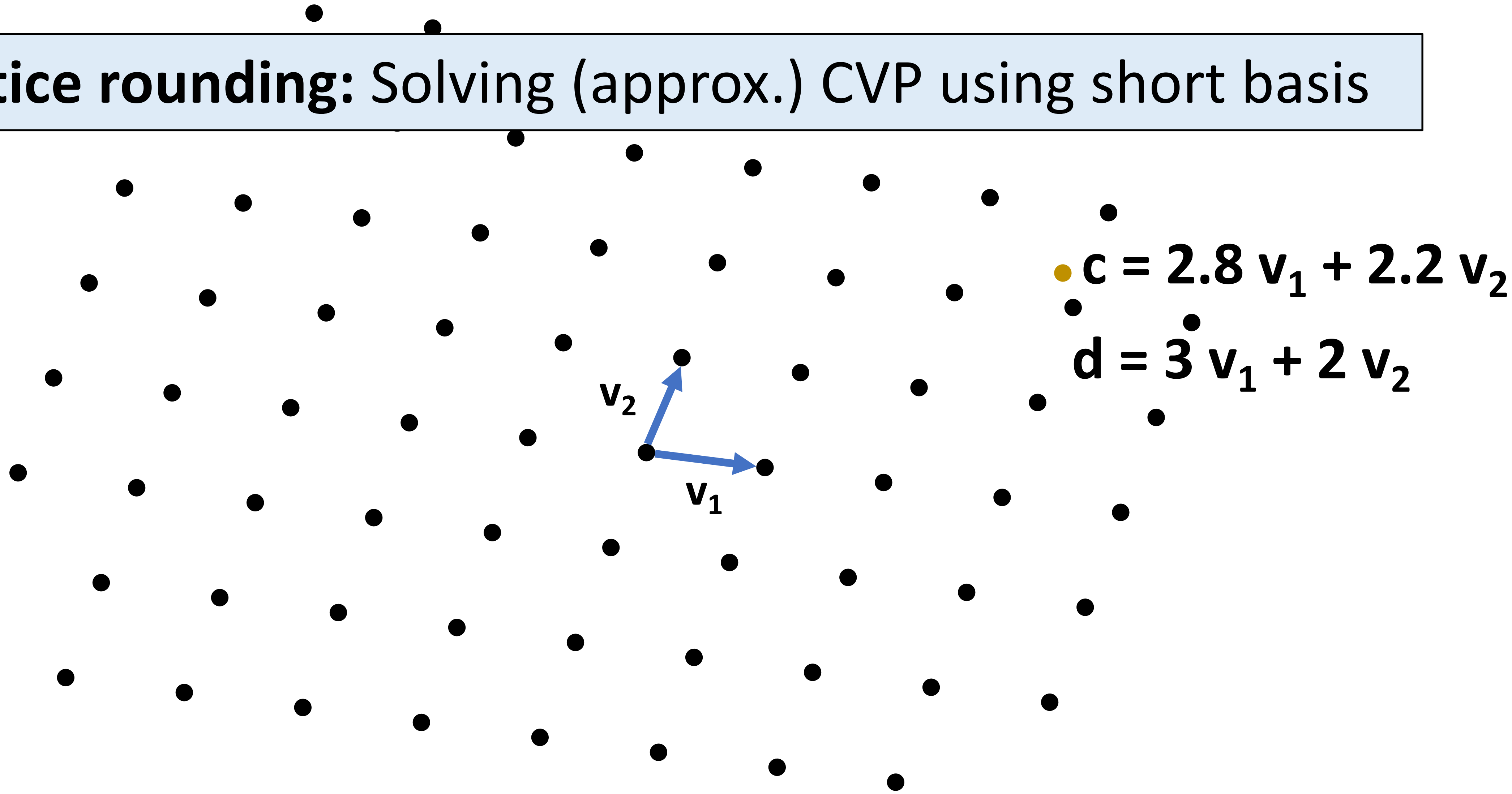
Lattices



Trapdoor: Give out large basis as public key, keep short basis as secret key / trapdoor

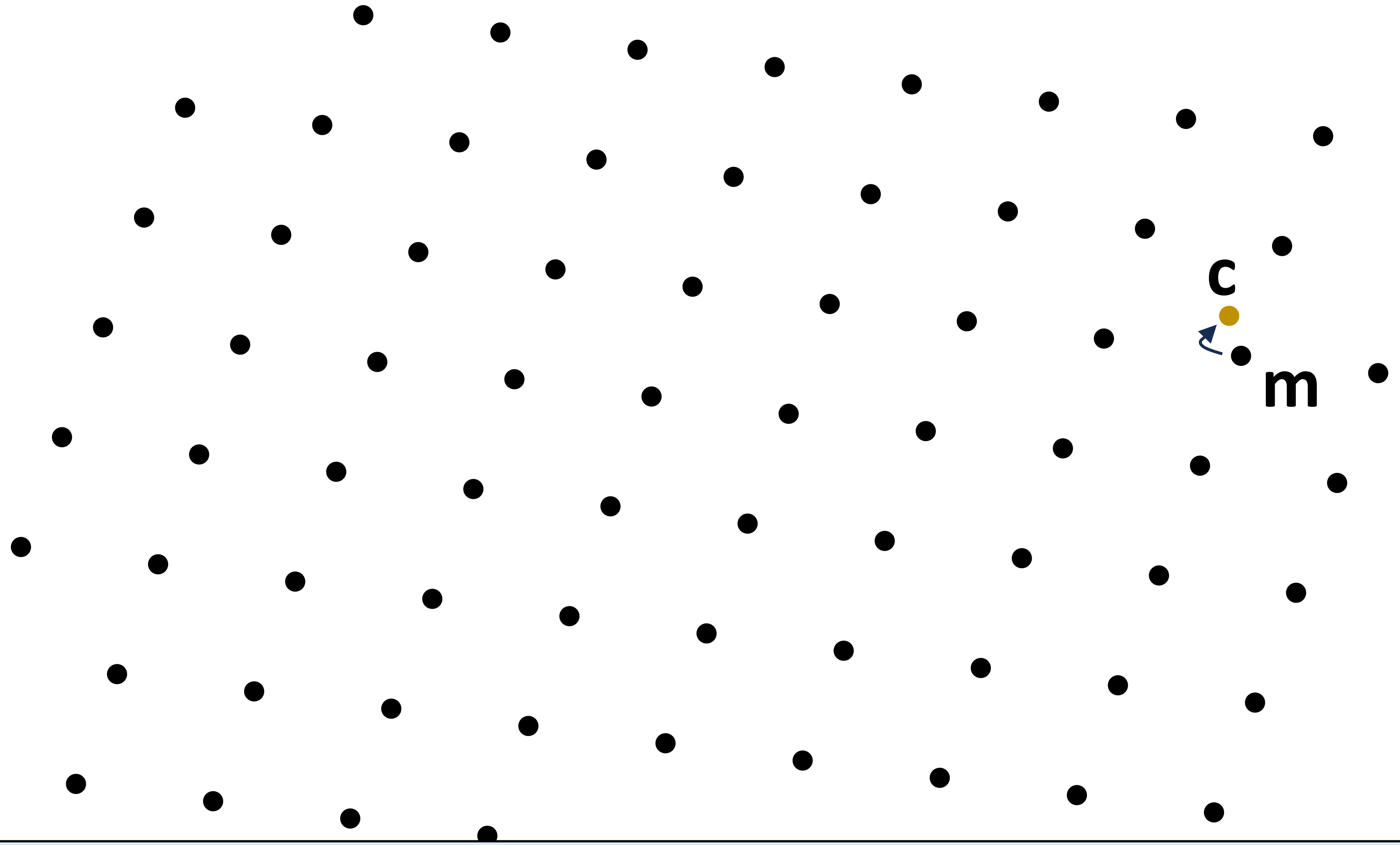
Lattices

Lattice rounding: Solving (approx.) CVP using short basis



Shorter bases give closer rounding

Lattices



Encrypt **m**: (1) Map **m** to lattice point

(2) Output close non-lattice point

Lattices

SIS [Ajtai'96]: Distribution over hard approx. SVP instances
LWE [Regev'05]: Distribution over hard approx. CVP instances

Lattices are periodic, but lattice/period typically known (bad basis); SVP/SIS asks to find *short* description (good basis) of period

⬇

Period-finding doesn't seem relevant; presumed quantum hardness

Note: many applications of lattices (e.g. FHE) beyond presumed quantum resistance

Other types of post-quantum assumptions

Concrete assumptions:

- From coding theory (e.g. McEliece)
- LPN
- Non-abelian groups
- Most symmetric crypto

Can also make generic assumptions

- ∃PQ-PKE, PQ-PRG, etc

Open Questions

Better understanding of quantum hardness of group actions, lattices, etc.

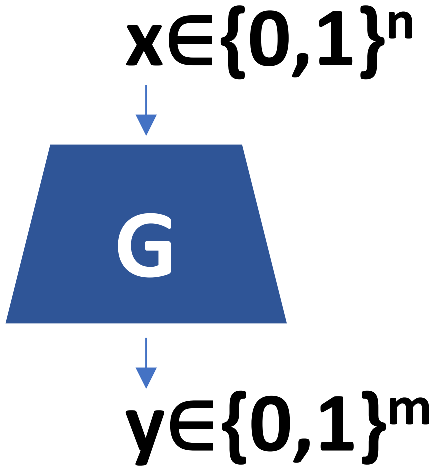
More techniques for using group actions / impossibilities
- Especially using non-abelian group actions

Exact security of symmetric cryptography
- Non-trivial quantum algorithms for SHA, AES?
- Know time-hardness of inversion ($\mathbf{\Theta(2^{n/2})}$) and collision-finding ($\mathbf{\Theta(2^{n/3})}$), but space-time-hardness of collision still open

[Brassard-Høyer-Tapp'98]: $\mathbf{O(2^{n/3})}$ time and space, but unknown if space is necessary

3b. Post-quantum Security Proofs

Example: PRG Length Extension

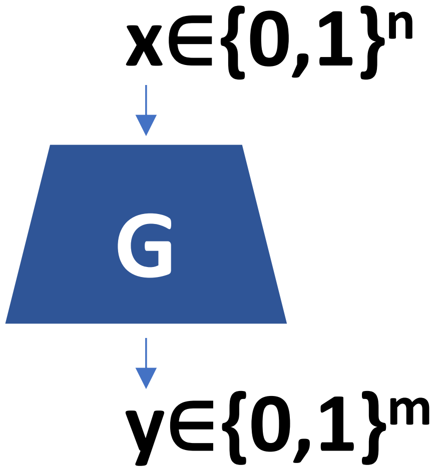


Def: G is a secure pseudorandom generator (PRG) if, ∀PPT **A**, ∃negligible **ε** such that

$$| \Pr[A(y)=1] - \Pr[A(G(x))=1] | < \varepsilon$$

Non-triviality: **(m>n)**

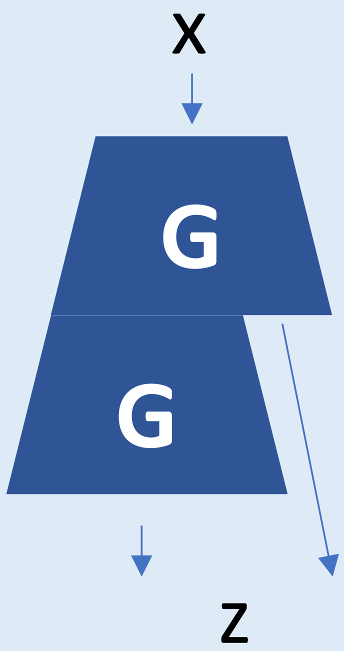
Example: PRG Length Extension



Non-triviality: **(m>n)**

Suppose **m=n+1**. How to get larger stretch?

Solution: $\mathbf{G_2}$ =

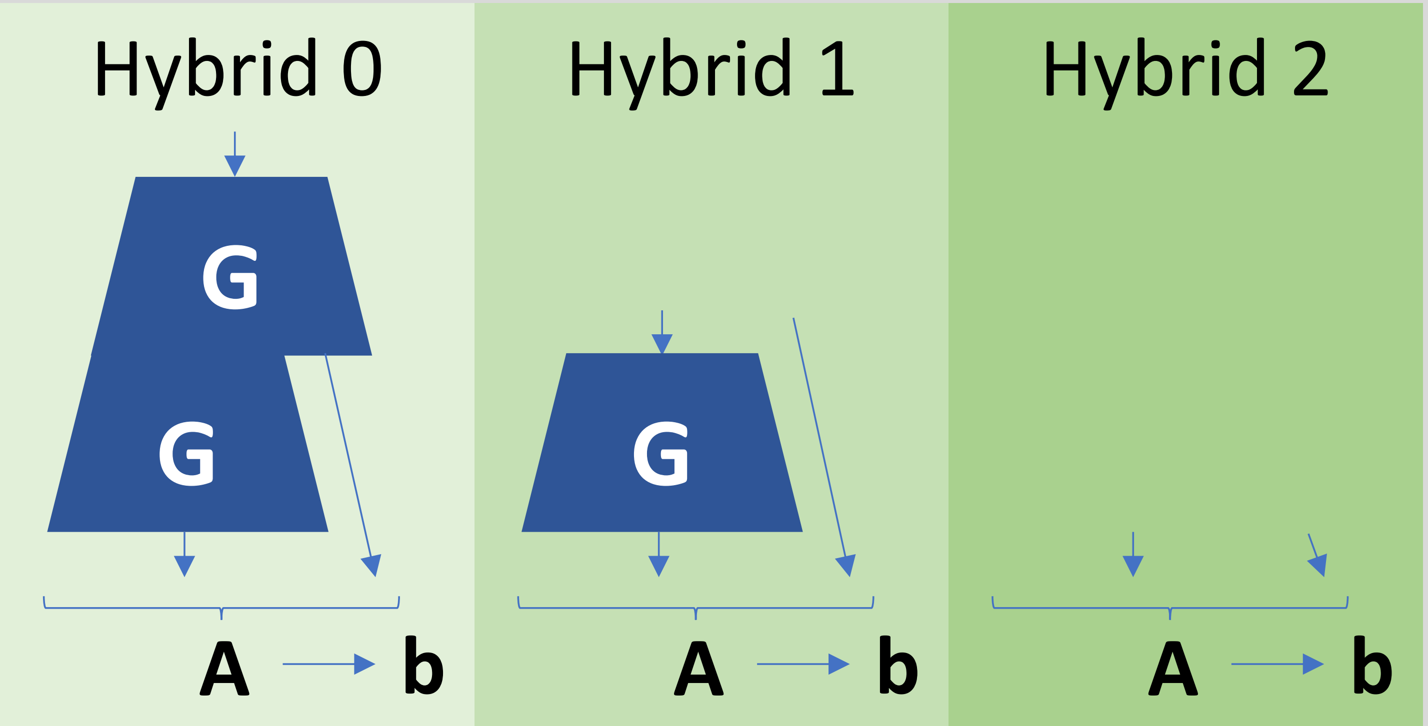


Thm: If **G** is secure, then so is $\mathbf{G_2}$

Example: PRG Length Extension

Proof: Suppose $\mathbf{G_2}$ insecure. Then ∃PPT **A**, non-negl **ε** such that

$$\mathbf{| \Pr[A(y)=1] - \Pr[A(G_2(x))=1] | \geq \varepsilon}$$

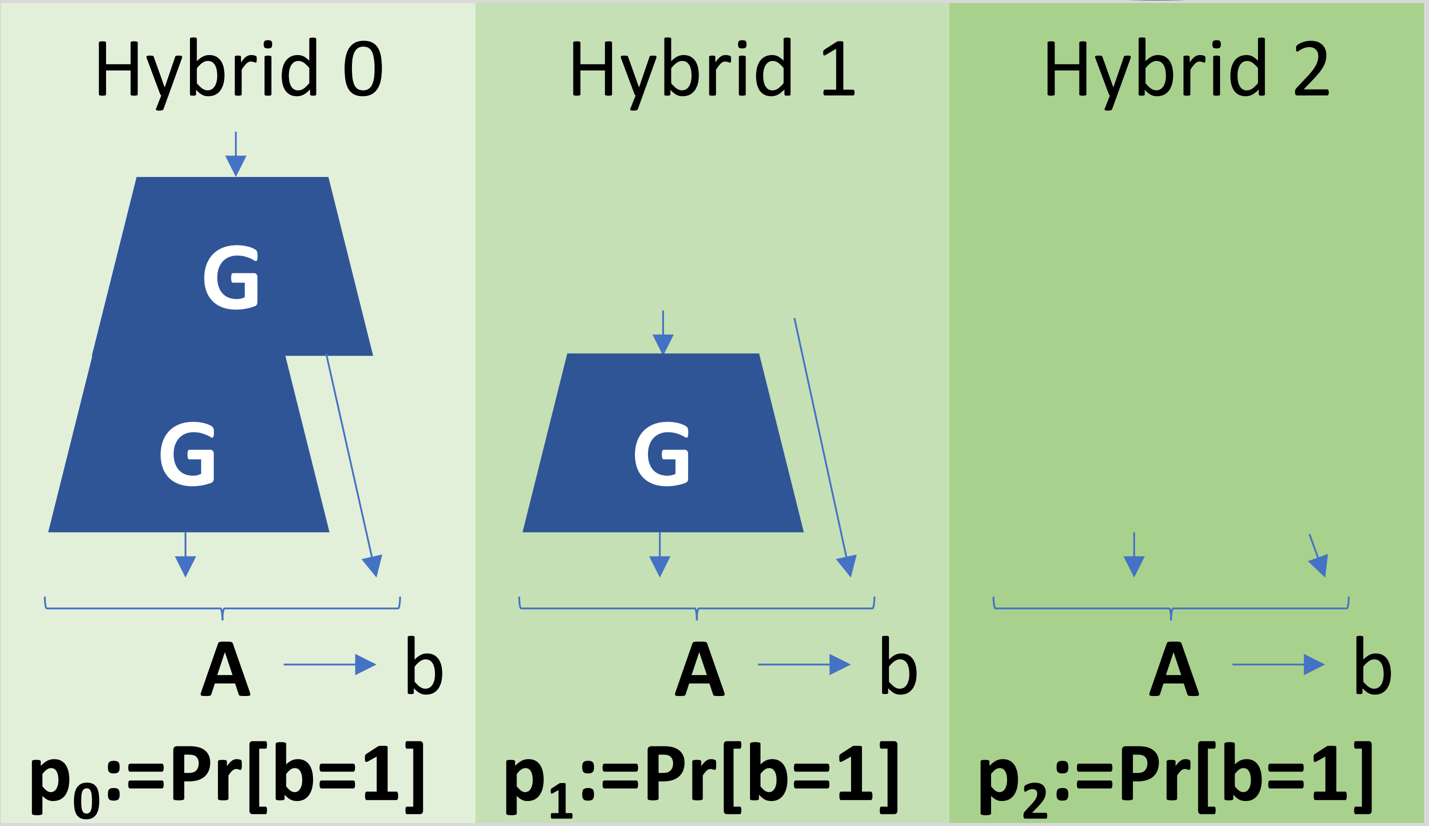


$\mathbf{p_0 := \Pr[b=1]}$ $\mathbf{p_1 := \Pr[b=1]}$ $\mathbf{p_2 := \Pr[b=1]}$

Example: PRG Length Extension

Proof: Suppose $\mathbf{G_2}$ insecure. Then ∃PPT **A**, non-negl **ε** such that

$$|p_2 - p_0| \geq \varepsilon$$



Either: $|p_1-p_0| \geq \varepsilon/2$ ⇒ $\mathbf{B(y_0,y_1)= A(G(y_0),y_1)}$

Or: $|p_2-p_1| \geq \varepsilon/2$ ⇒ $\mathbf{B(y_0,y_1)= A(y_0,y_1,\$)}$

In either case, **B** has advantage **ε/2** against security of **G**

Example: PRG Length Extension

What about quantum?

Def: G is a **post-quantum** secure PRG if,
∀**Q**PT **A**, ∃negligible **ε** such that

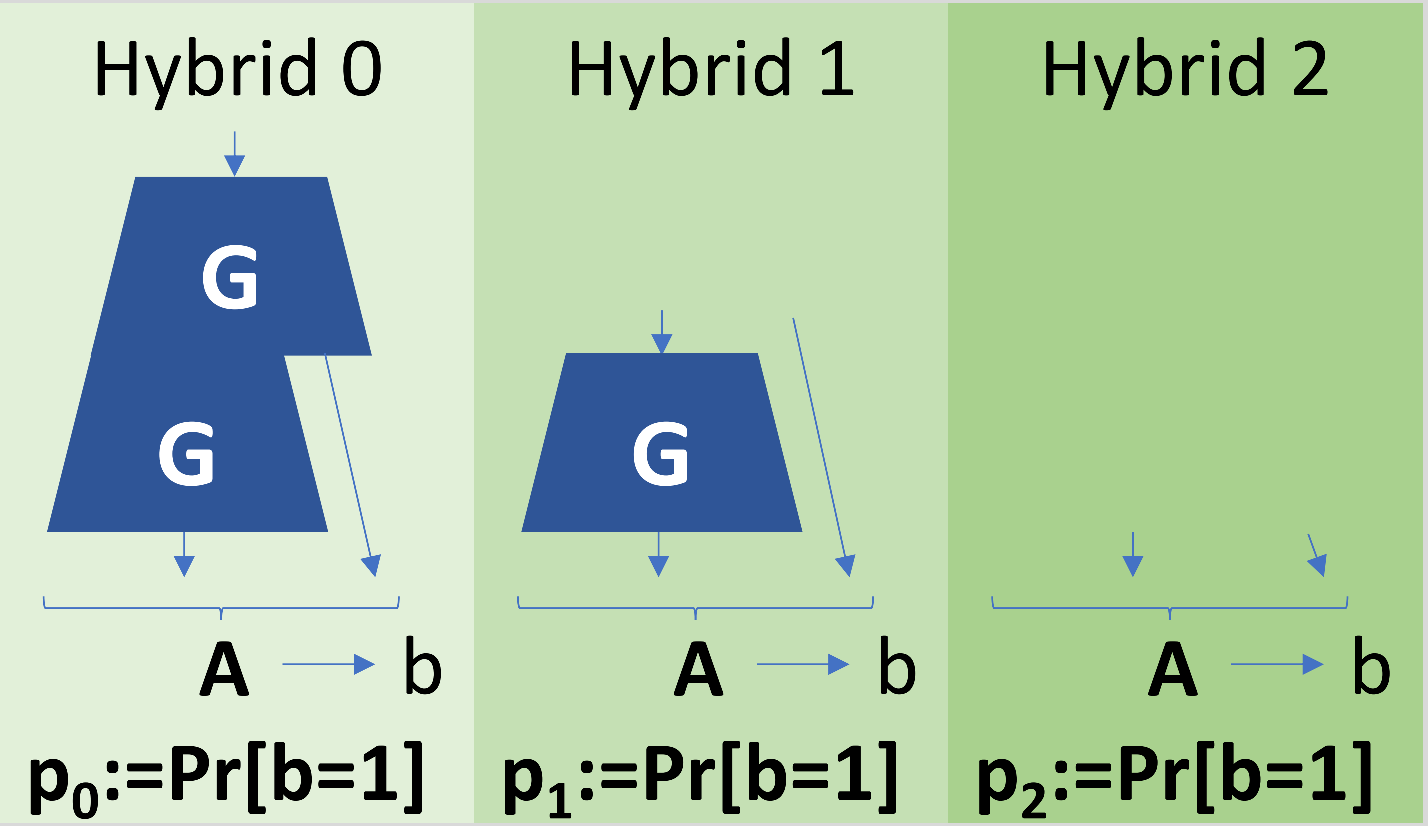
$$\mathbf{| \Pr[A(y)=1] - \Pr[A(G(x))=1] | < \varepsilon}$$

Thm: If **G** is post-quantum secure, then so is $\mathbf{G_2}$

Example: PRG Length Extension

Proof: Suppose $\mathbf{G_2}$ is **PQ** insecure. Then ∃**Q**PT A, non-negl **ε** s.t.

$$|p_2 - p_0| \geq \varepsilon$$



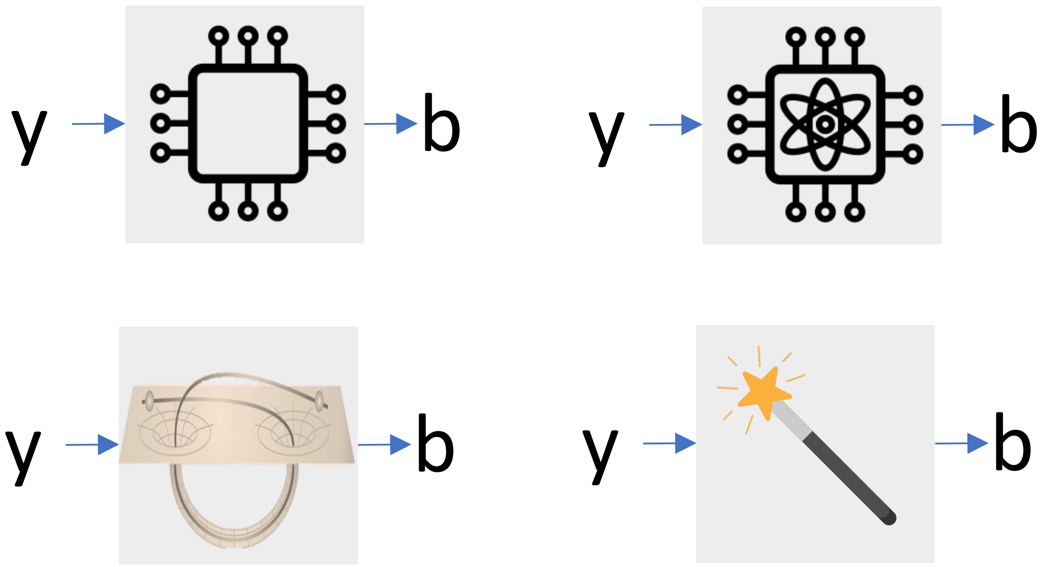
Either: $|p_1 - p_0| \geq \varepsilon/2$ ⇓ $\mathbf{B(y_0,y_1)= A(G(y_0),y_1)}$

Or: $|p_2 - p_1| \geq \varepsilon/2$ ⇓ $\mathbf{B(y_0,y_1)= A(y_0,y_1,\$)}$

In either case, **B** has advantage **ε/2** against **PQ** security of **G**

Example: PRG Length Extension

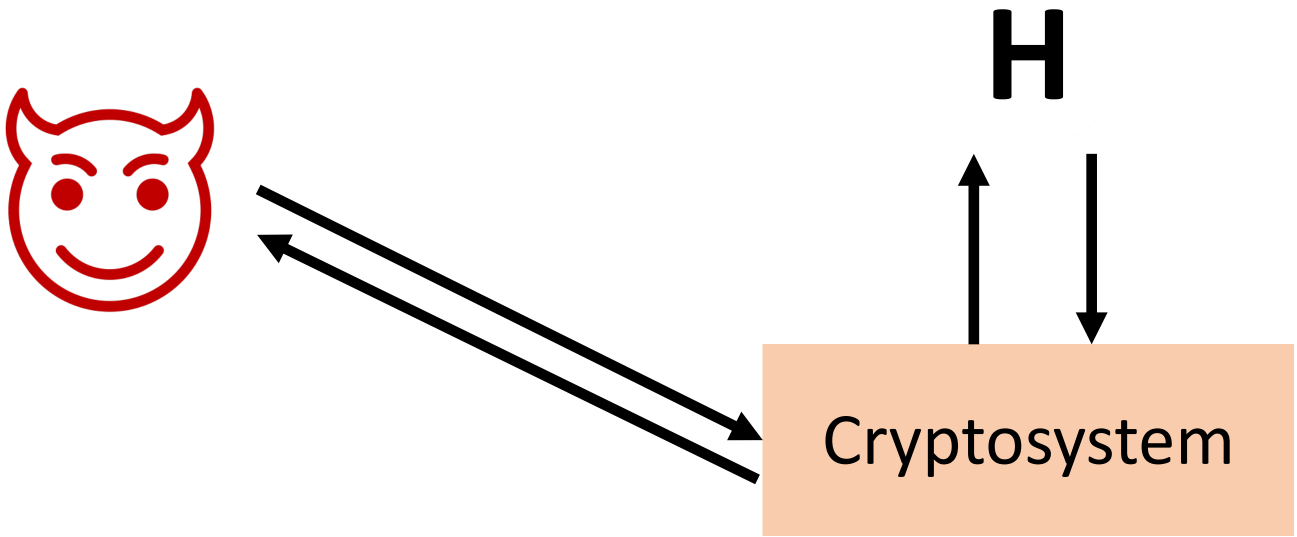
Proof for $\mathbf{G_2}$ doesn't care how **A** works internally, as long as it has non-negligible advantage



That is, proof treats **A** as "black box"

Example: Random Oracle Model

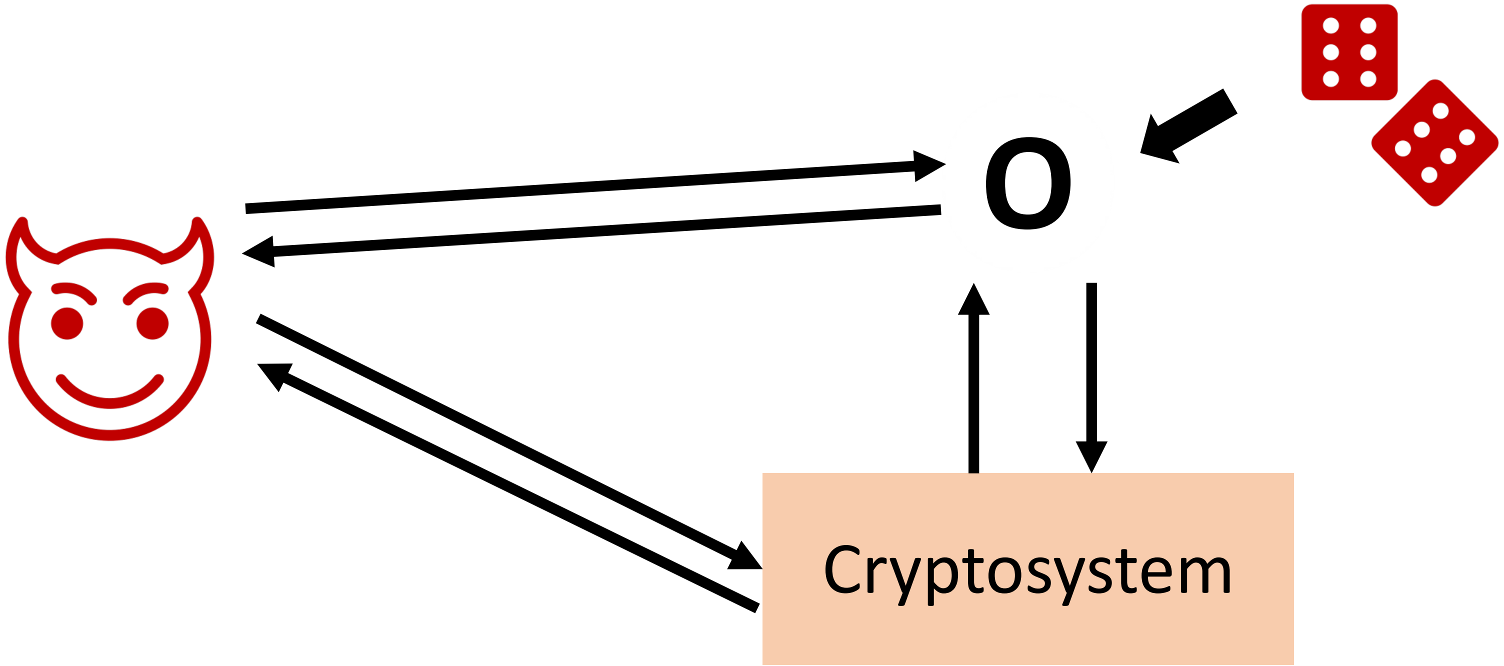
Consider cryptosystem using hash function **H**



Examples: OAEP, Fujisaki-Okamoto, Full-Domain Hash, …

Example: Random Oracle Model

[Bellare-Rogaway'93]: model **H** as random function



Example: Random Oracle Model

Hope: If ∃ROM security proof, no "real world" attacks on sufficiently well-designed hash function

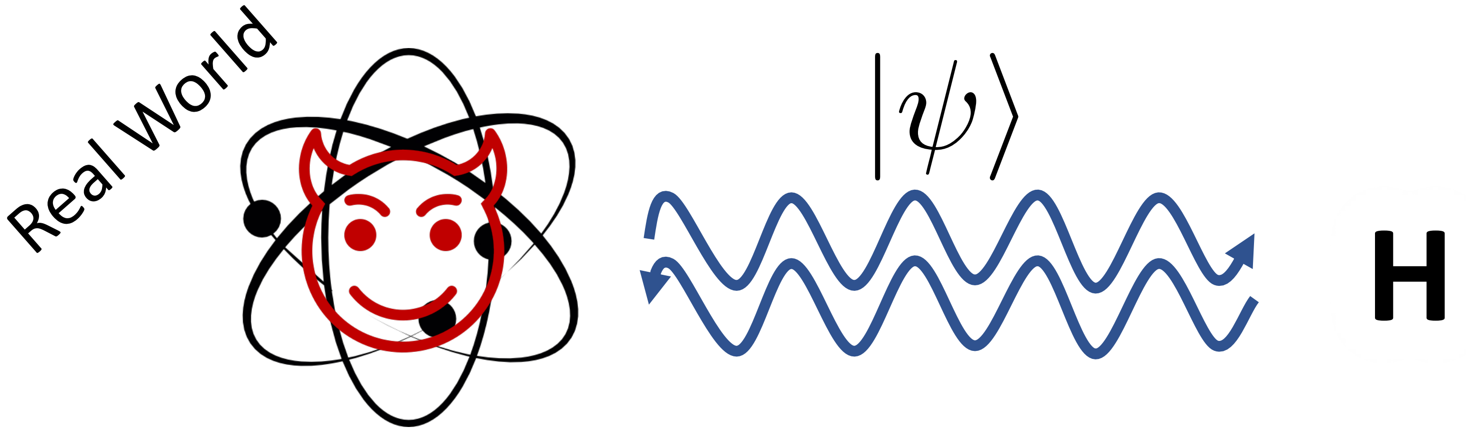
Theoretical attacks known [Canetti-Goldreich-Halevi'98], but heuristic has held up in practice. Basis for essentially all of the most efficient cryptosystems.

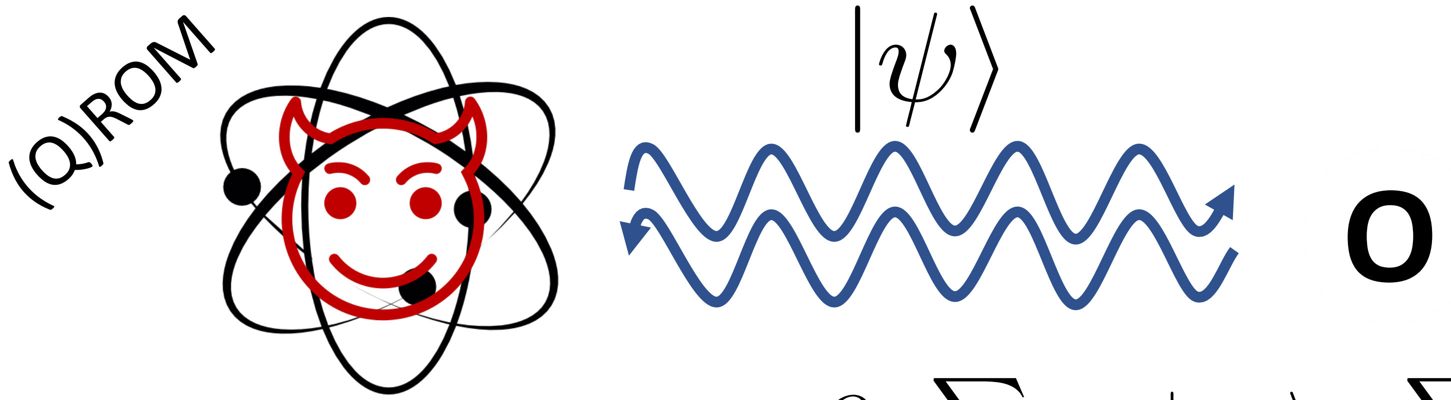
Example: Random Oracle Model

Enter quantum…

Example: Random Oracle Model

[Boneh-Dagdelen-Fischlin-Lehmann-Schaffner-Z'11]:



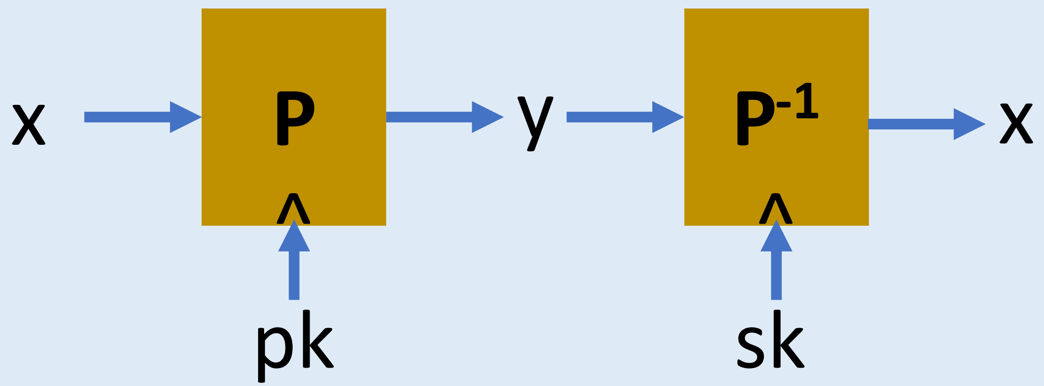


Concretely, can apply $O_O \sum_{x,y} \alpha_{x,y} |x, y\rangle = \sum_{x,y} \alpha_{x,y} |x, y \oplus O(x)\rangle$

Example: Random Oracle Model

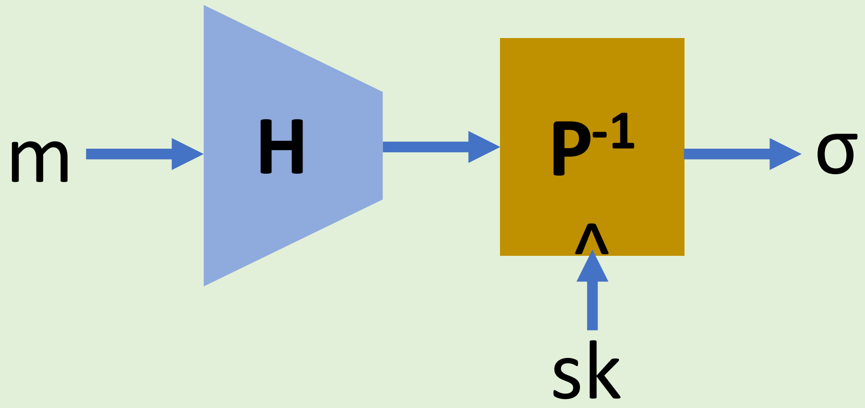
Consider Full Domain Hash Signatures

Building Block: Trapdoor Permutations



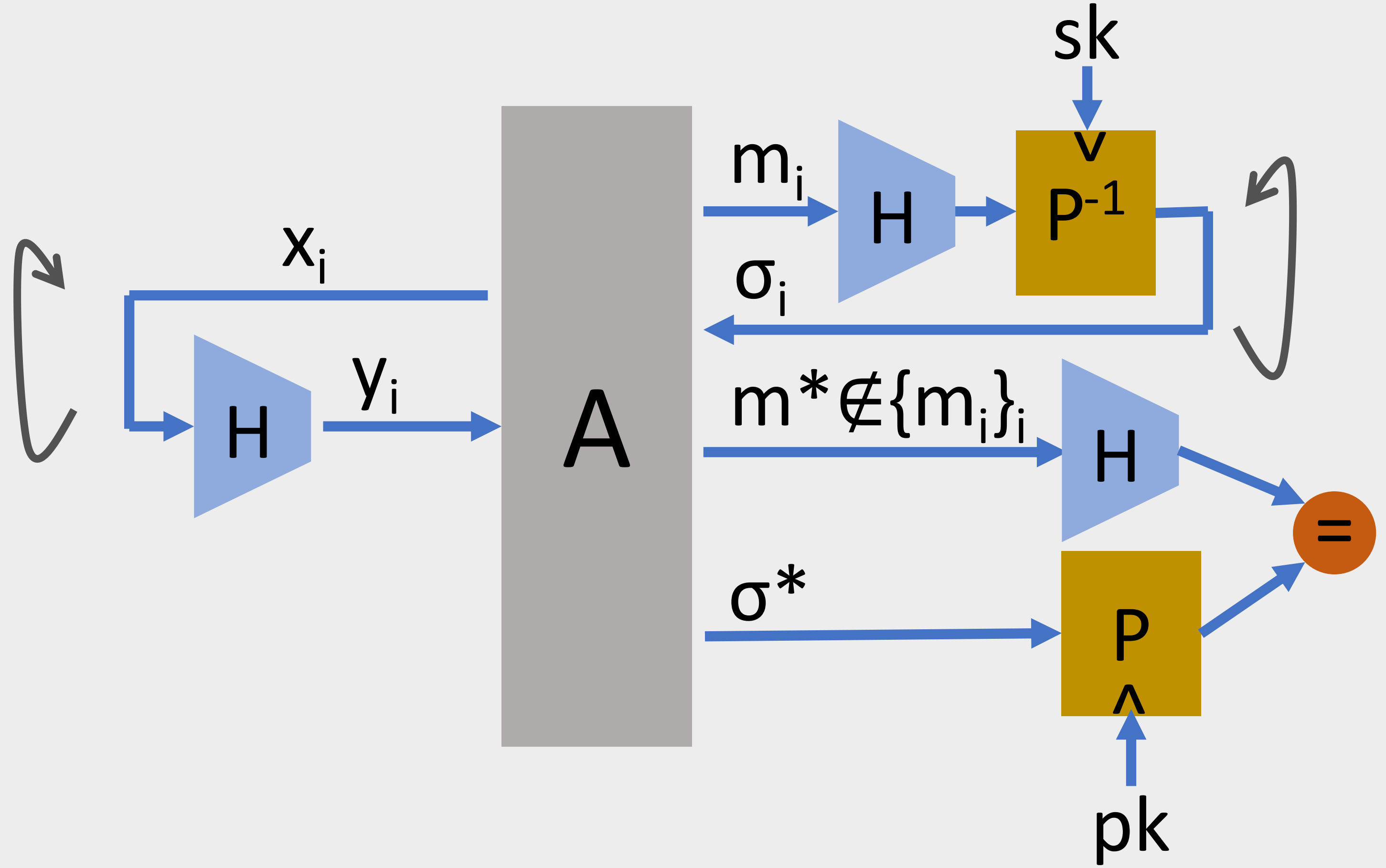
Security: ∀PPT **A**, **Pr[A(pk,y)=x] < negl**

Sigs from TDPs



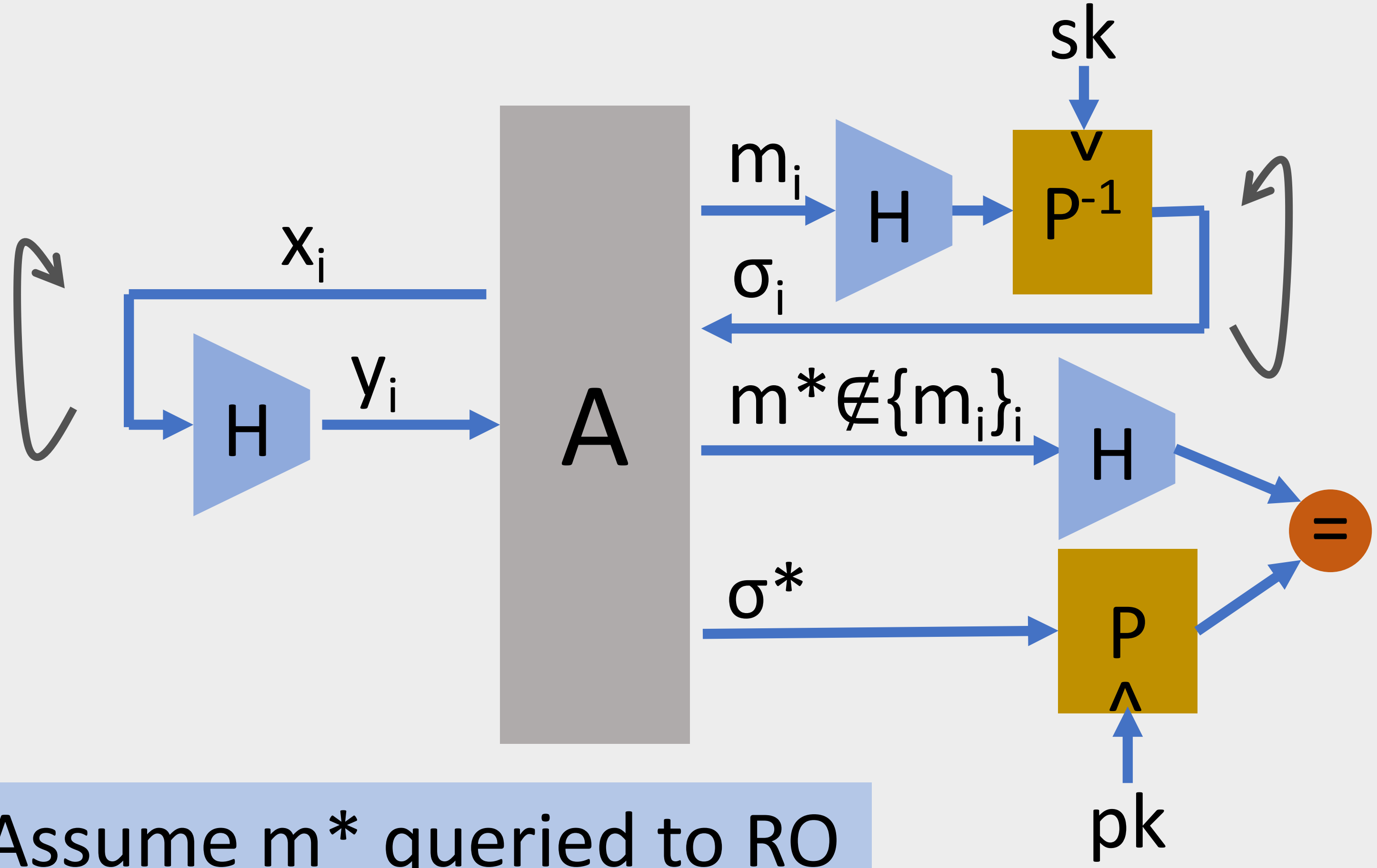
Example: Random Oracle Model

ROM security proof: Assume toward contradiction



Example: Random Oracle Model

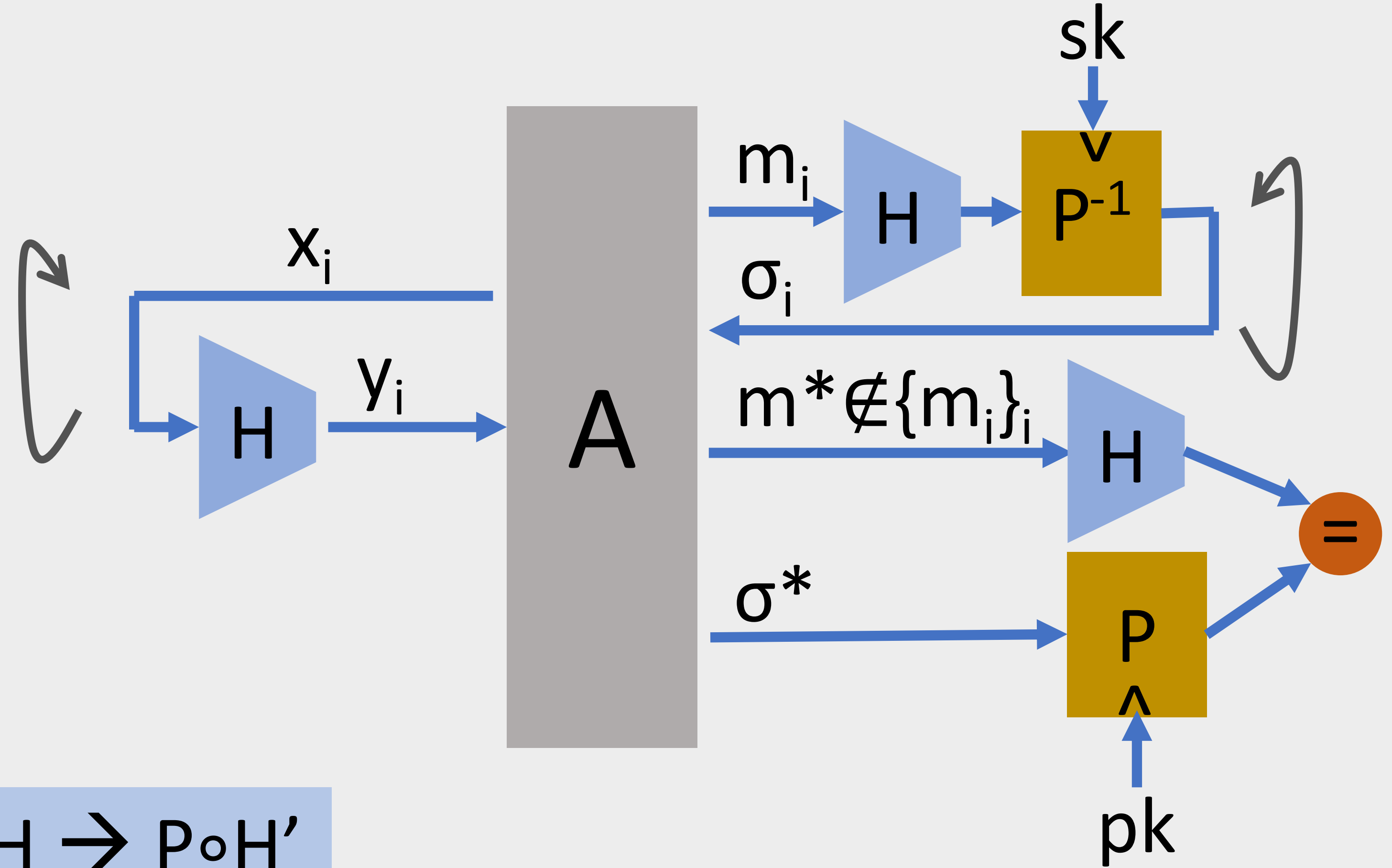
ROM security proof:



Step 0: Assume m* queried to RO

Example: Random Oracle Model

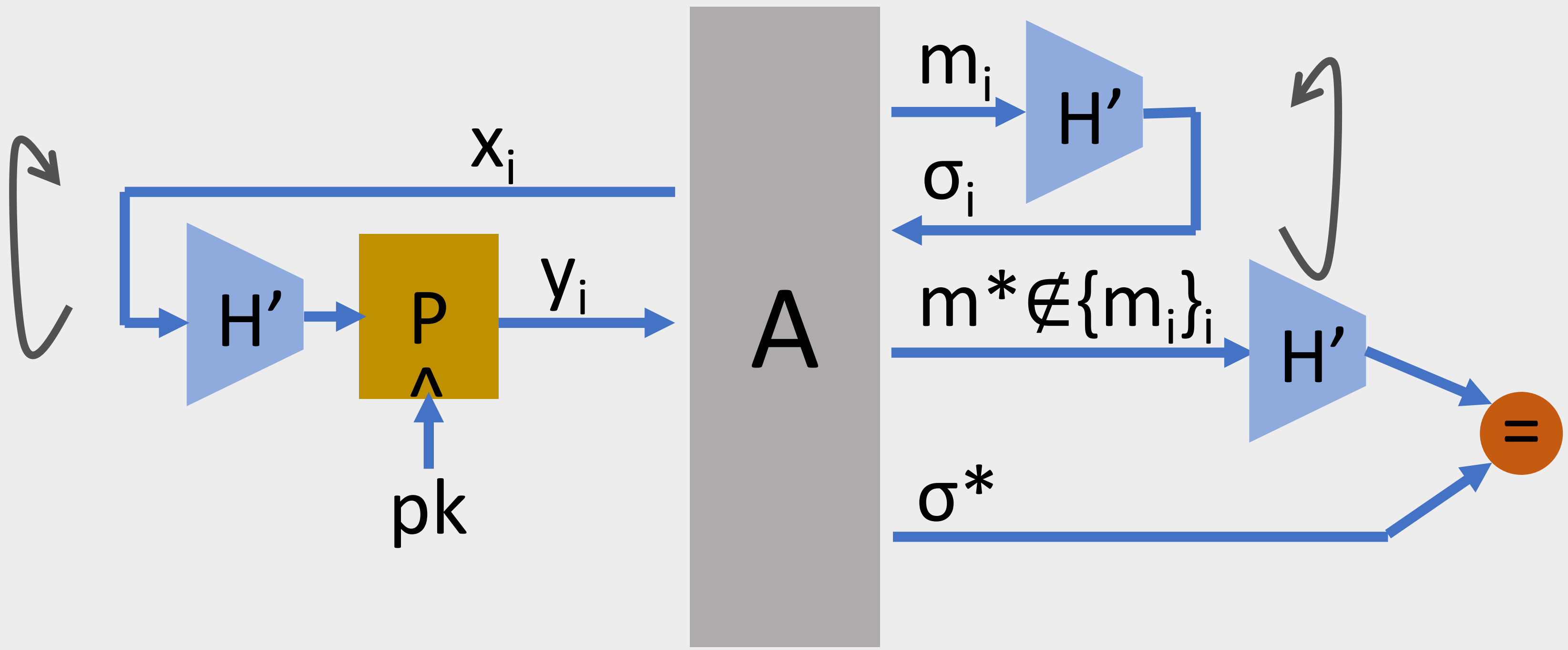
ROM security proof:



Step 1: H → P∘H’

Example: Random Oracle Model

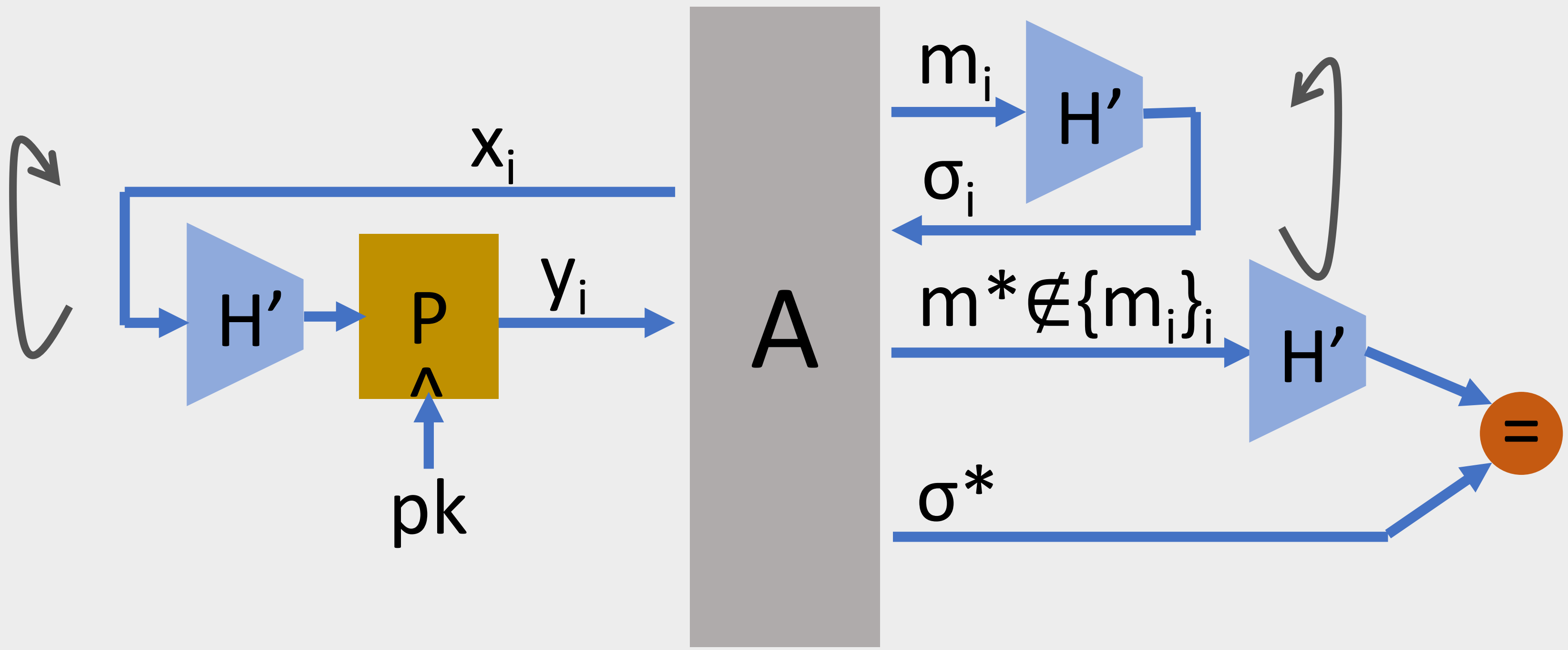
ROM security proof:



Step 1: H → P∘H’

Example: Random Oracle Model

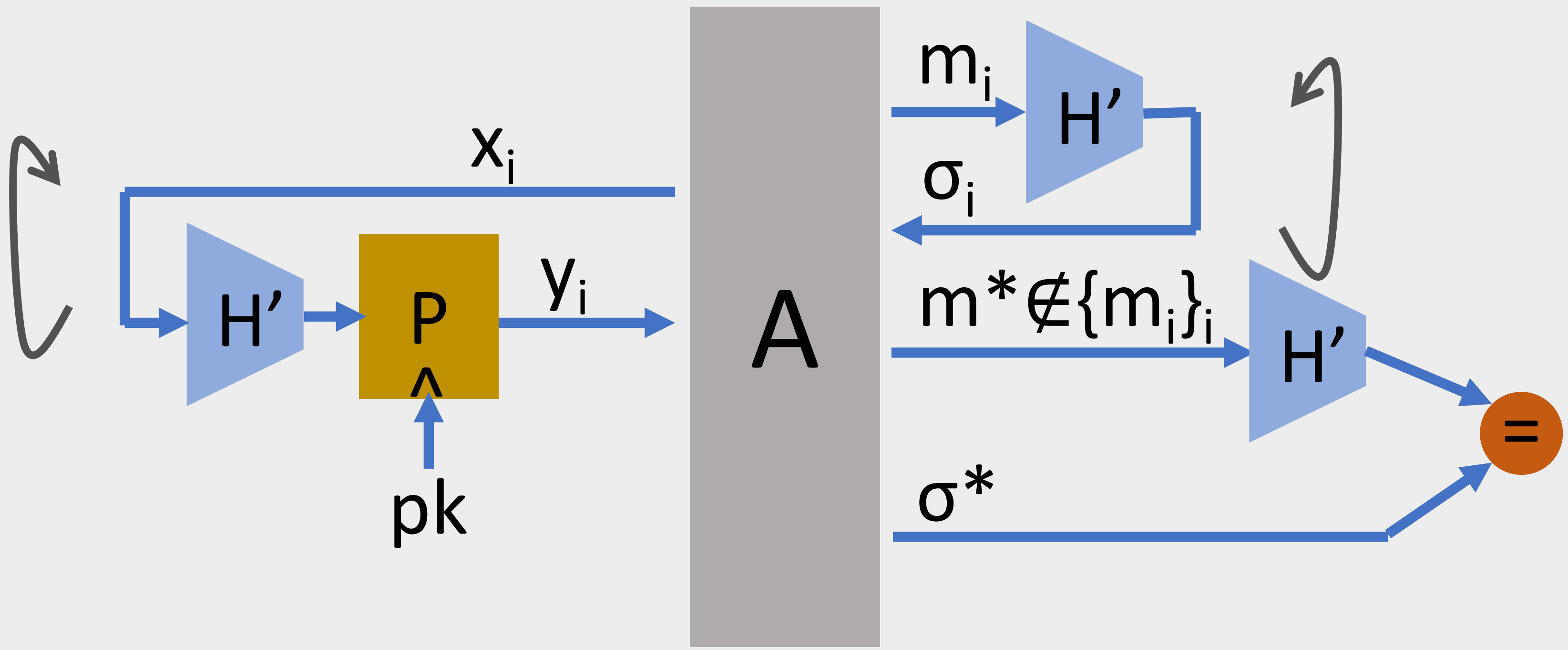
ROM security proof:



A computes **H'(m*)**, given only **H(m*)=P(pk,H'(m*))**

Example: Random Oracle Model

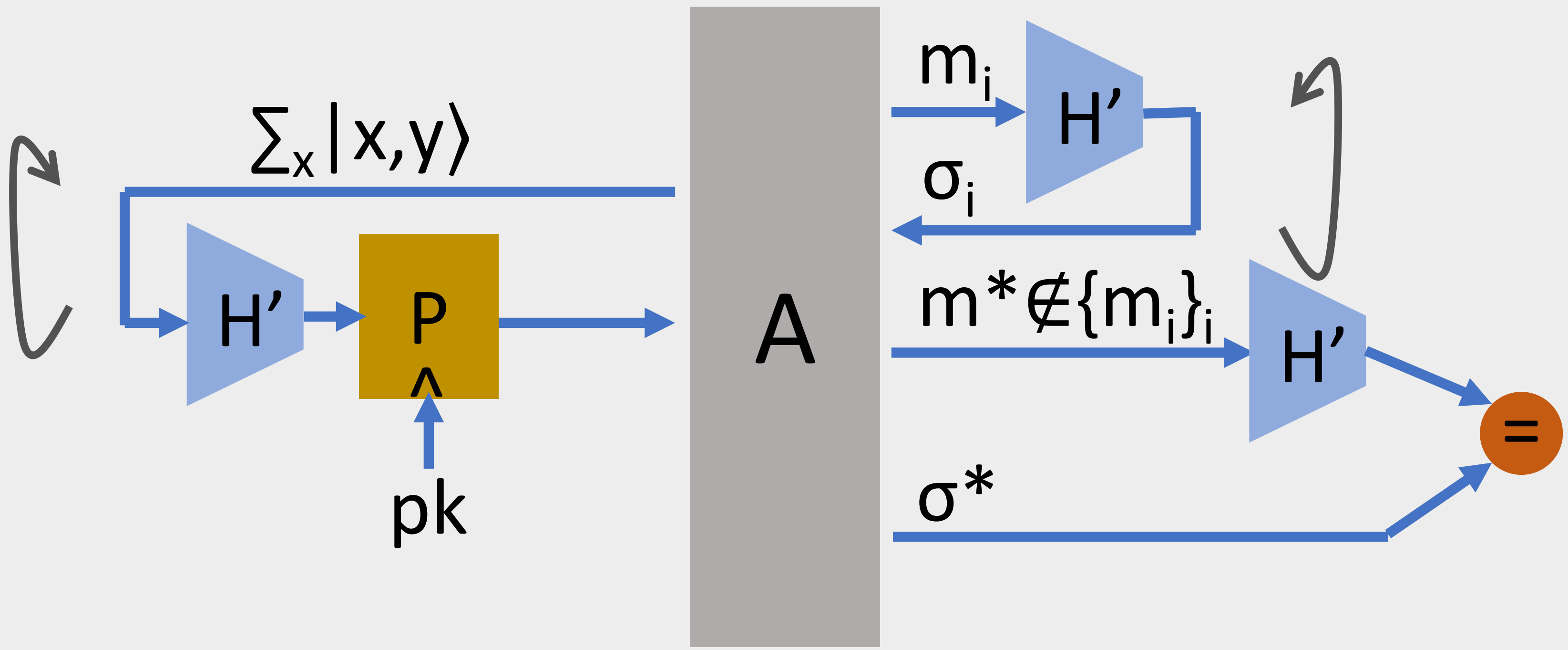
ROM security proof:



B(y*): set **$H(x_i)=y^*$** for random query → advantage **ε/q**

Example: Random Oracle Model

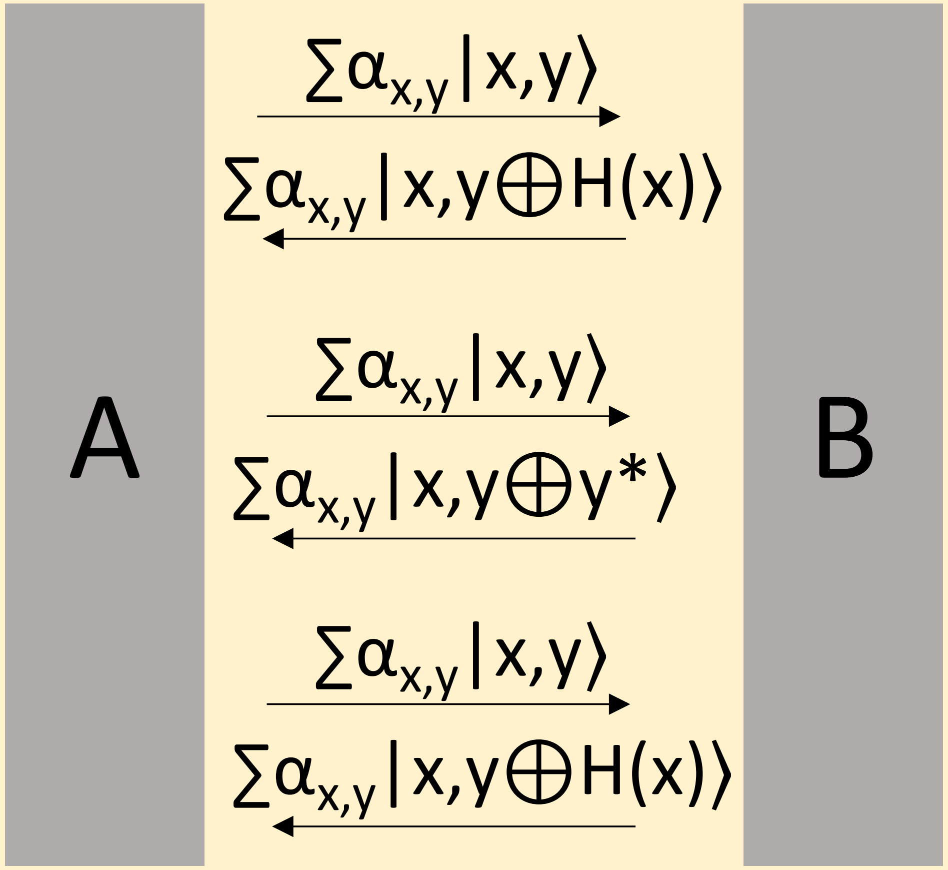
QROM Proof?



How does **B(y*)** insert challenge into **H**?

Example: Random Oracle Model

Attempt 1: Insert at random QUERY



Problem: repeated queries?

Problem: distinguishing attack

$\sum|x,0\rangle \rightarrow$, $\leftarrow \sum|x,y^*\rangle$ VS $\sum|x,0\rangle \rightarrow$, $\leftarrow \sum|x,O(x)\rangle$

Example: Random Oracle Model

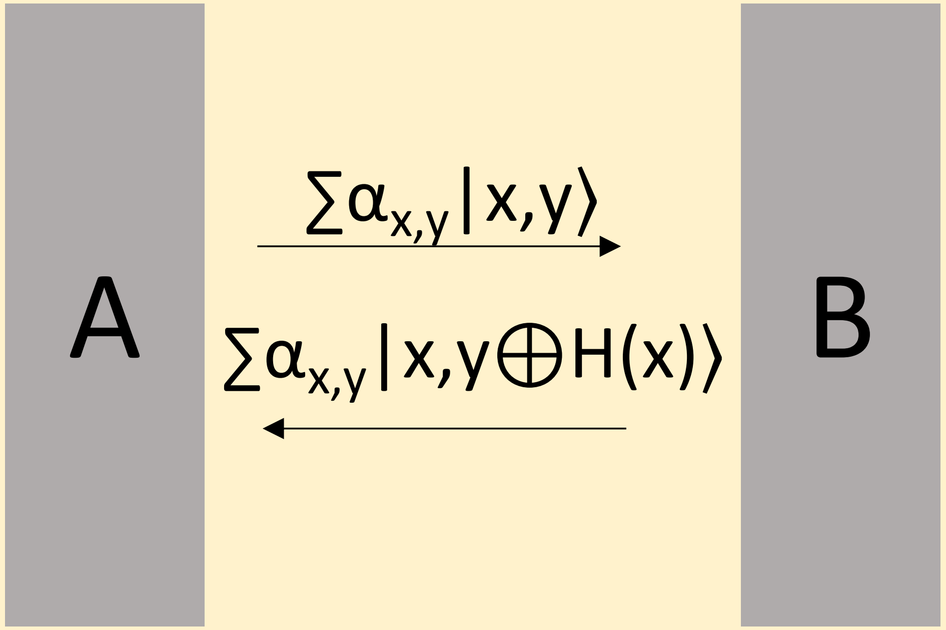
Typical QROM reductions commit to entire function H at beginning, remain consistent throughout

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

Note: growing number of techniques exmploying non-committing reductions [Unruh'15, **Z**'19, Kuchta-Sakzad-Stehle-Steinfeld-Sun'20, Alagic-Carolan-Majenz-Tokat'25,...]

Example: Random Oracle Model

Take 2: Insert at random VALUE



$H(m^*) = y^*$

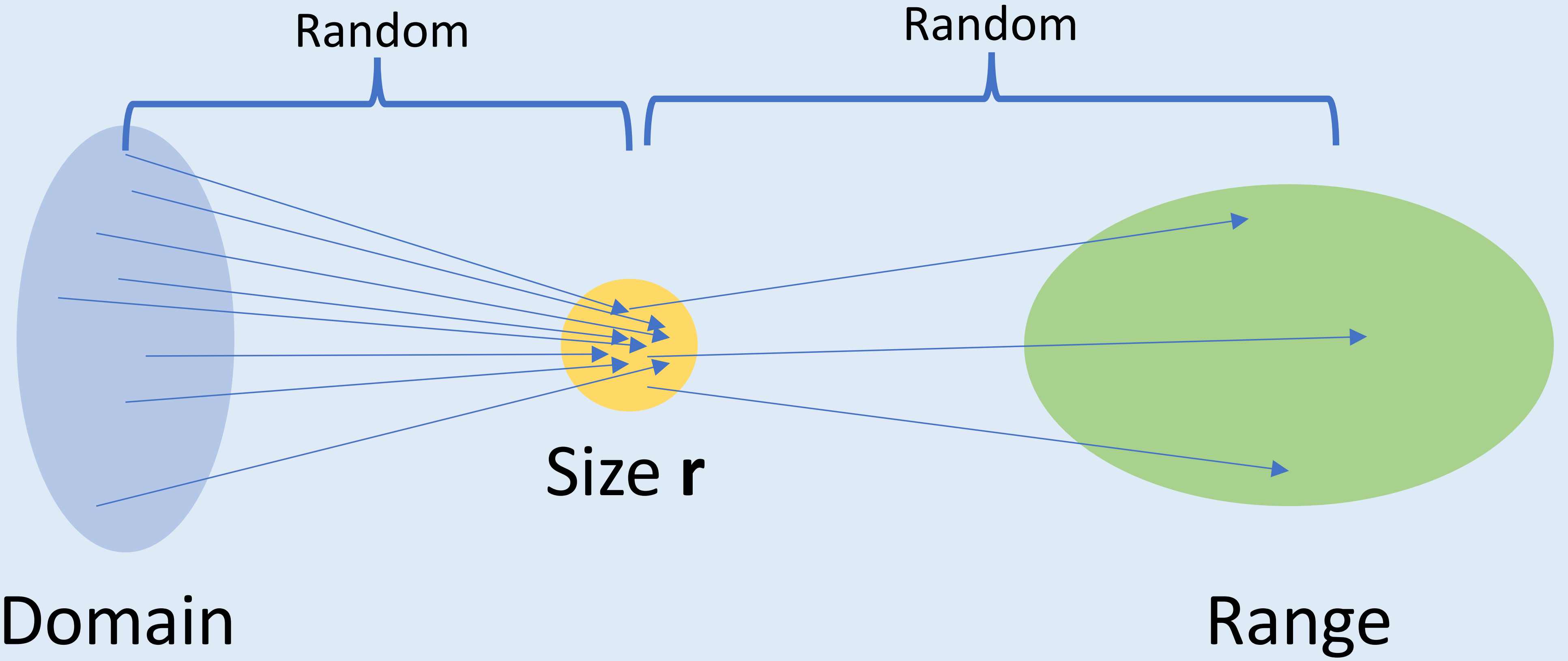
$H(x) = \$$** if **$x \neq m^*$

Problem: exp-many values

→ **Pr[**correctly guess **m*] =negl**

Example: Random Oracle Model

Solution: Small-Range Distributions [Z'12]



Example: Random Oracle Model

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

Quantum collision finding ➡ bound tight
[Brassard-Høyer-Tapp'98]

Example: Random Oracle Model

Finishing the proof:

Pr[A wins | **H'** random **]** $\geq$ **ε**

⬇

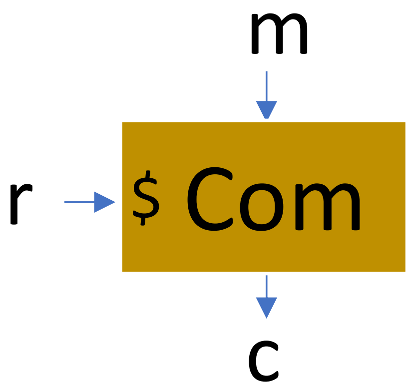
Pr[A wins | **H' = SR_r]** $\geq$ **ε – $O(q^3/r)$**

B(y*) inserts **y*** into random output

➡ **Pr[B** inverts **y]** $\geq$ **$\varepsilon/r - O(q^3/r^2) = O(\varepsilon^2/q^3)$**

$r=O(q^3/\varepsilon)$

Example: Coin Tossing

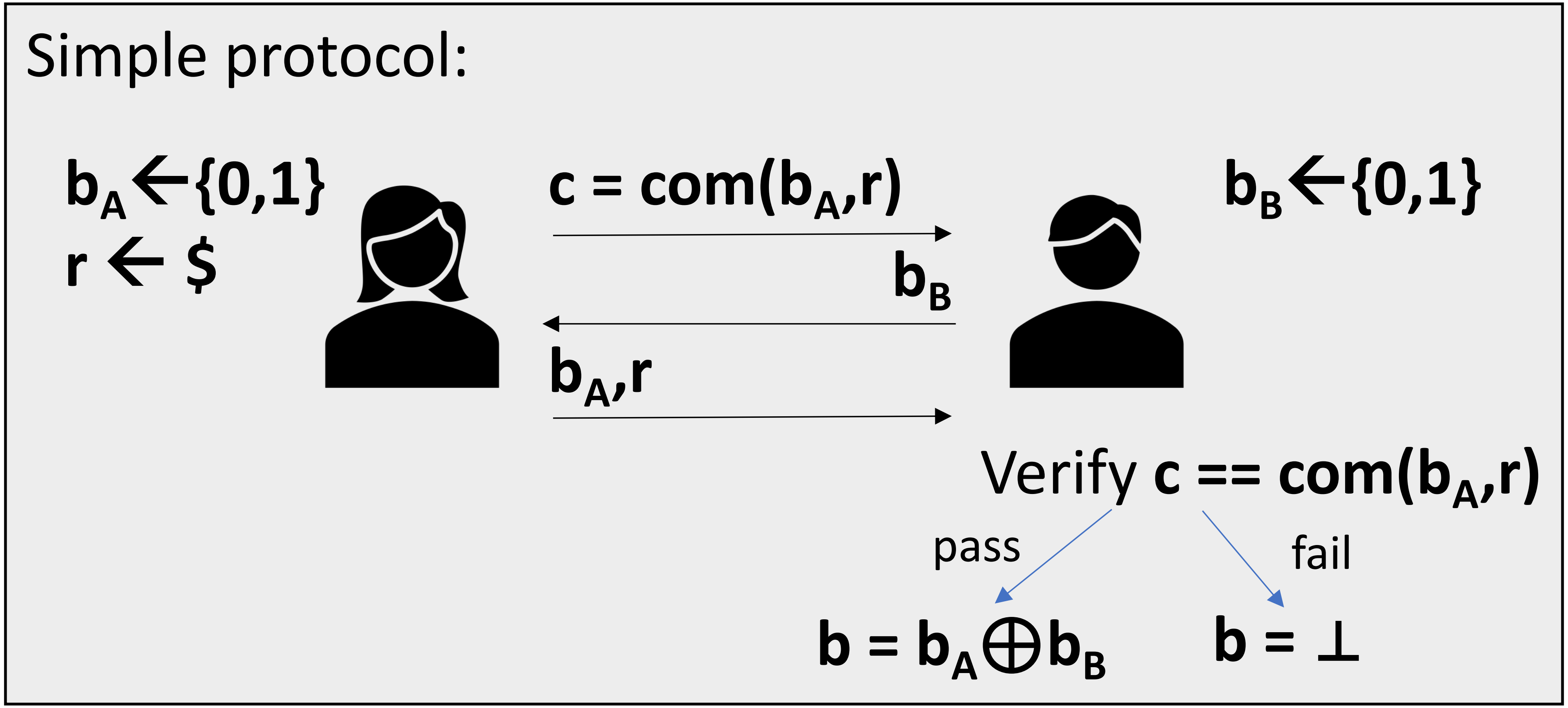


Def: Com is (computationally) binding if, ∀PPT **A**, ∃negligible **ε** such that

$$\mathbf{Pr}\left[\ \begin{array}{c} m_0 \neq m_1 \wedge \\ \mathrm{Com}(m_0,r_0)=\mathrm{Com}(m_1,r_1) \end{array} : (m_0,r_0,m_1,r_1) \leftarrow A()\ \right] < \varepsilon$$

Also want hiding, but we will ignore

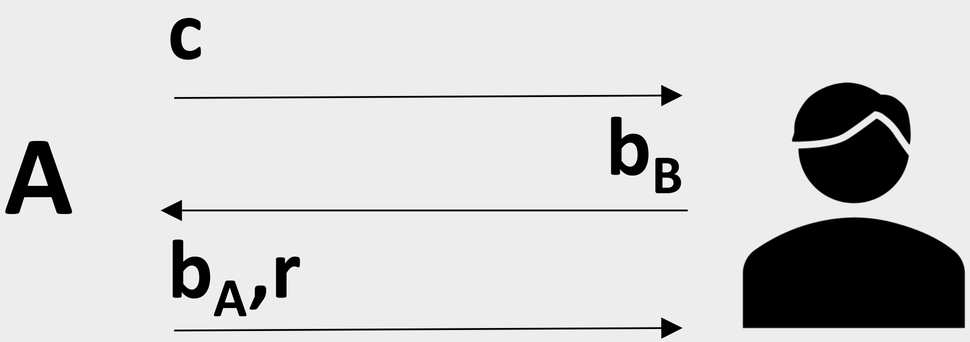
Example: Coin Tossing



Example: Coin Tossing

Proof that Alice can't bias **b**:

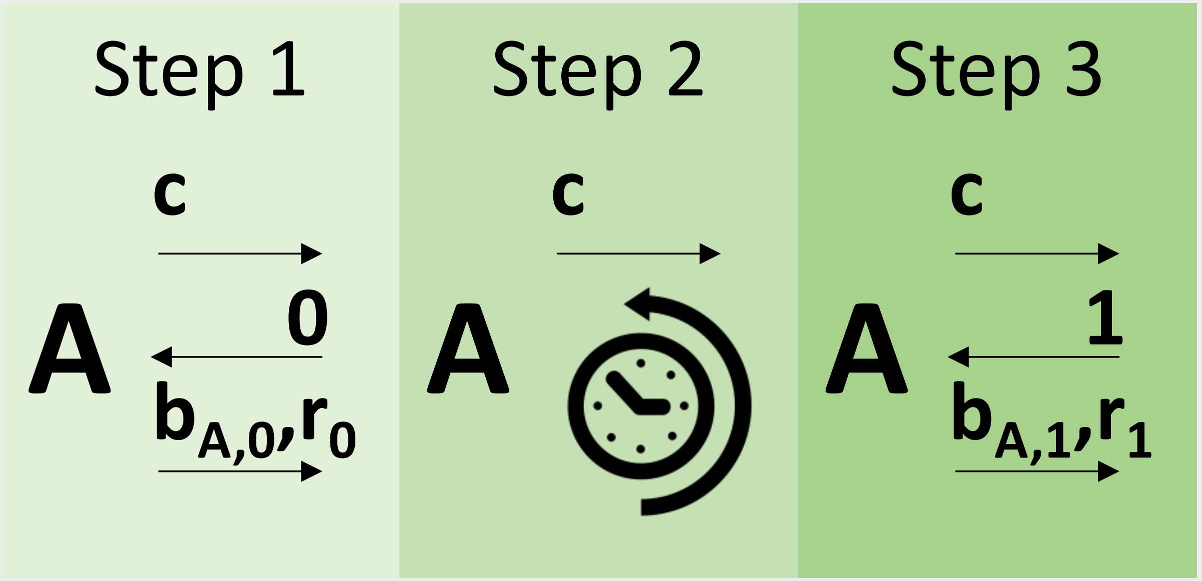
Let **A** be supposed adversary



$\Pr[b=0] > \frac{1}{2}+\varepsilon$ ⇒ For both $b_B=0$ and $b_B=1$, good chance $b_A=b_B$ and $\mathrm{Com}(b_A,r)=c$

Example: Coin Tossing

Proof that Alice can't bias **b**:



$$\Pr\left[\begin{array}{l} b_{A,0} = 0 \wedge b_{A,1} = 1 \wedge \\ \mathrm{Com}(b_{A,0}, r_0) = \mathrm{Com}(b_{A,1}, r_1) = c \end{array} \right] \geq \mathrm{poly}(\varepsilon)$$

Example: Coin Tossing

What about quantum?

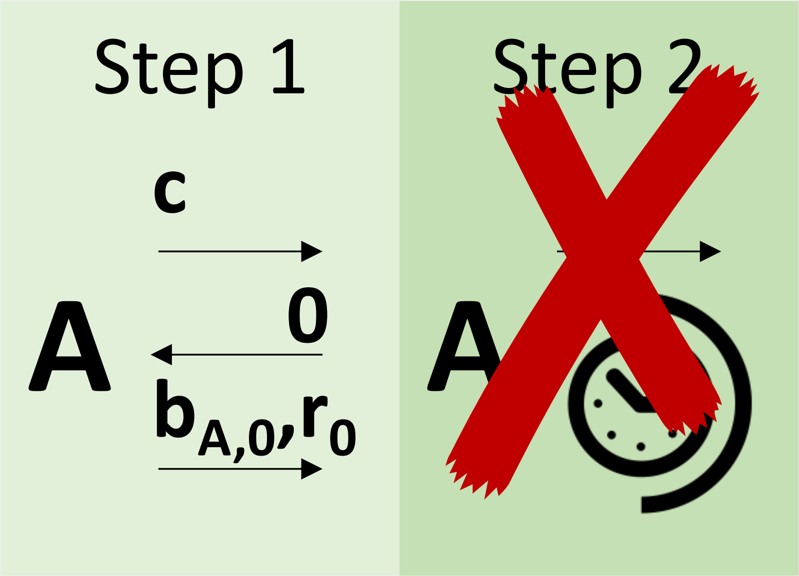
Def: Com is **post-quantum** (computationally) binding if, ∀**Q**PT **A**, ∃negligible **ε** such that

$$\mathbf{Pr}\left[\begin{array}{c} m_0 \neq m_1 \wedge \\ Com(m_0,r_0)=Com(m_1,r_1) \end{array} : (m_0,r_0,m_1,r_1) \leftarrow A() \right] < \varepsilon$$

Define coin-tossing goal similarly

Example: Coin Tossing

Proof that **quantum** Alice can't bias **b**?



Observer effect: extracting $\mathbf{b_{A,0}, r_0}$ irreversibly altered **A**'s state

Example: Coin Tossing

Thm (Ambainis-Rosmanis-Unruh'14,Unruh'16, Shmueli-Z'25):
∃PQ binding **Com** s.t. Alice has a near-perfect strategy (either relative to an oracle, or under appropriate computational assumptions)

I.e., quantumly, ability to produce either of two values isn't the same as ability to produce both simultaneously

Key Takeaway: As long as reduction treats **A** as a *single-run* black box (potentially w/ *classical* interaction), reduction likely works in quantum setting

! But if idealized model (e.g. RO), must be careful

! But if rewinding **A**, must be careful

Open Questions

Find other proof techniques that fail quantumly / show that they don't exist

Some positive progress: [Chan-Freitag-Pass'22, Bitansky-Brakerski-Kalai'22]

Which RO results can be lifted to quantum world?

Numerous works lifting specific techniques;
No fully-general lifting theorem [Yamakawa-**Z**'21, '22]
Lifting for specific classes [Yamakawa-**Z**'21, Katz-Sela'24,
Cojocaru-Hhan-Liu-Yamakawa-Yun'25]

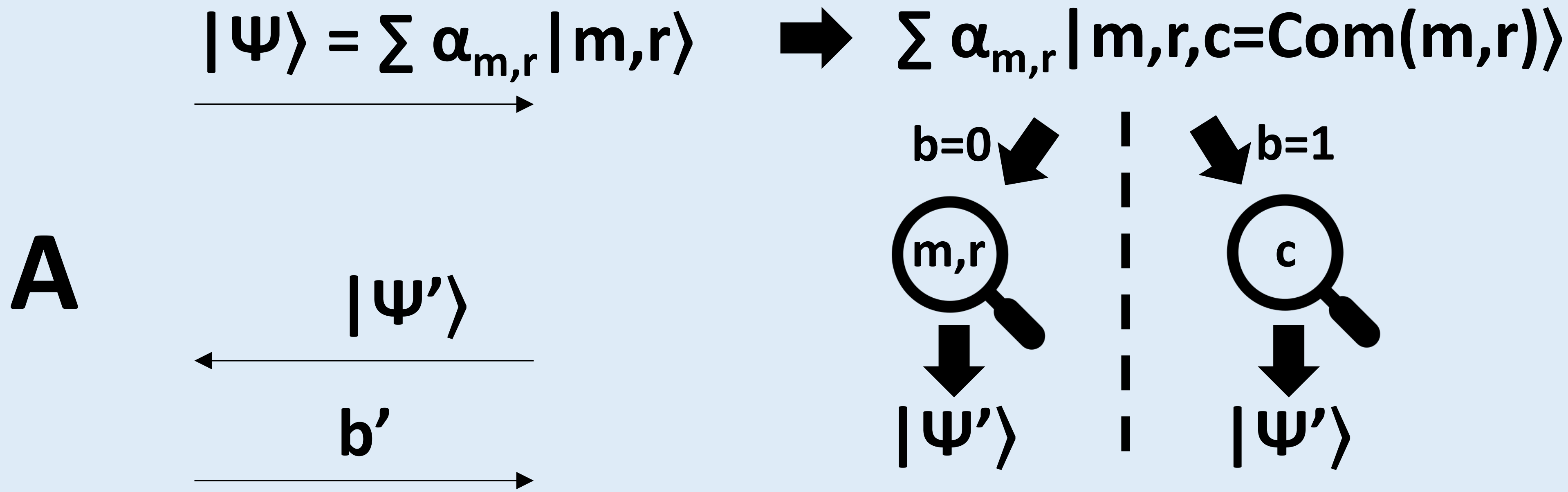
General conditions for lifting rewinding results?

Specific techniques [Watrous'06, Unruh'12,'16, Chiesa-Ma-Spooner-**Z**'21,…]

3c. Post-quantum Definitions

Collapsing Commitments [Unruh'16]

Def: Com is **collapsing** if, ∀QPT **A**, ∃negligible **ε** such that $|\mathbf{p_0} - \mathbf{p_1}| < \boldsymbol{\varepsilon}$ where:



$$\mathbf{p_b = Pr[b'=1|b]}$$

Also analogous notion of collapsing hash functions

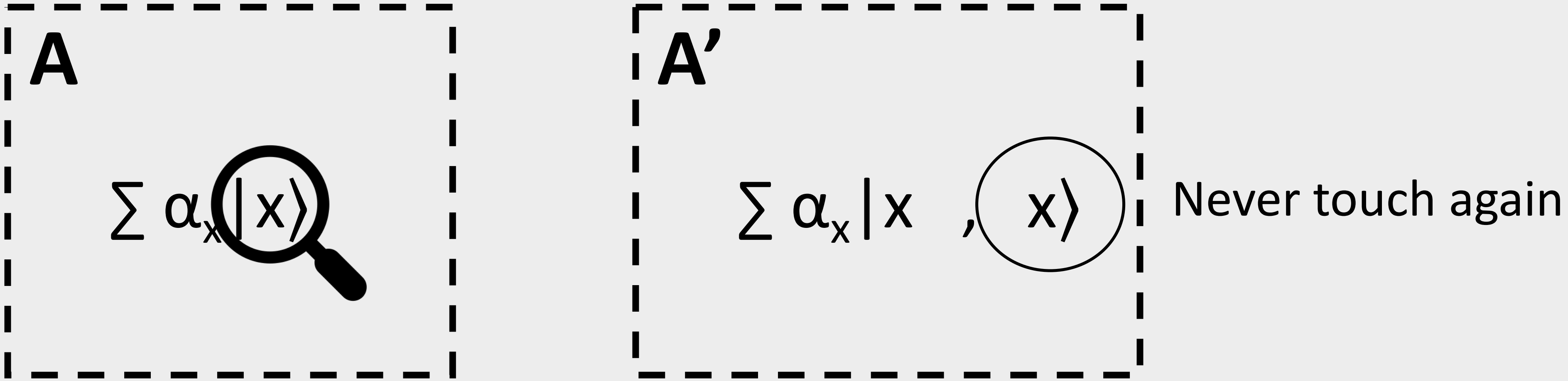
Collapsing Commitments

Intuition: if **Com** is injective, then measuring input and output result in same post-measurement state
→ Perfectly collapse-binding

Computational collapse binding makes sense even if **Com** is not injective (say, succinct commitments)

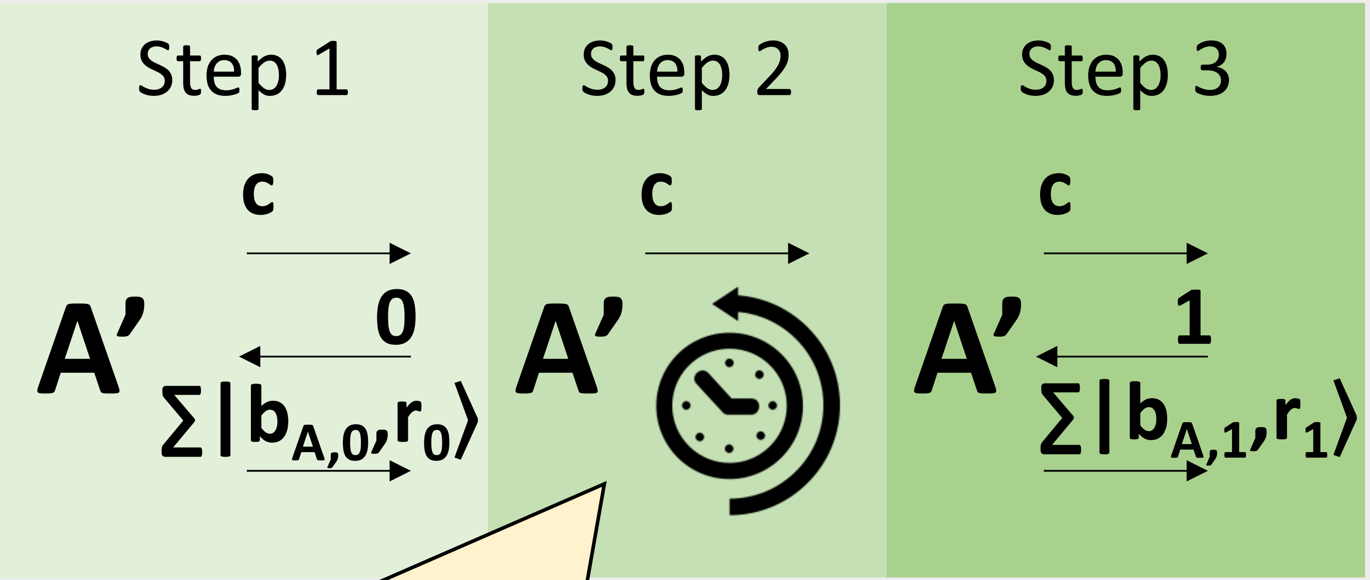
Proof that **quantum** Alice can't bias **b**

First, let's remove all *post-commitment* measurements from **A**



Exercise: A and **A'** behave identically

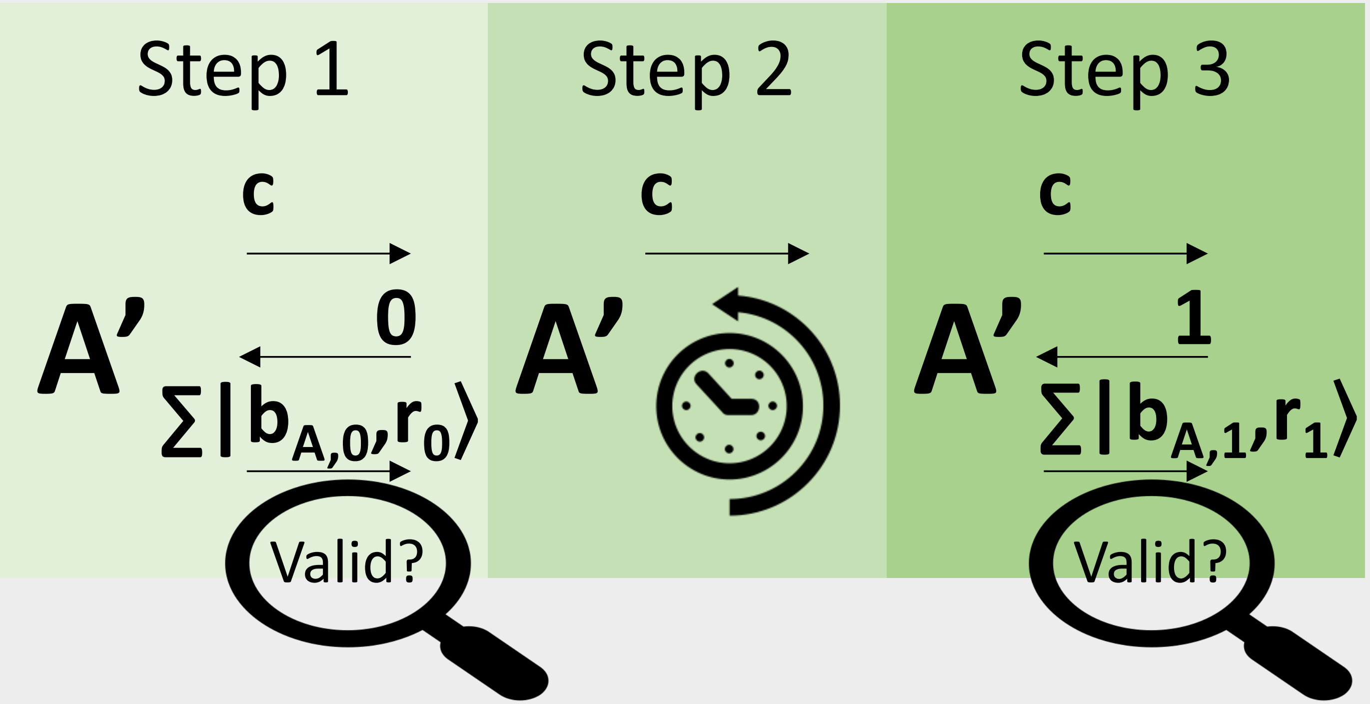
Proof that **quantum** Alice can't bias **b**



Can now rewind since post-commitment **A'** is unitary

But, rewinding also erased $\mathbf{b_{A,0}}$**!!!**

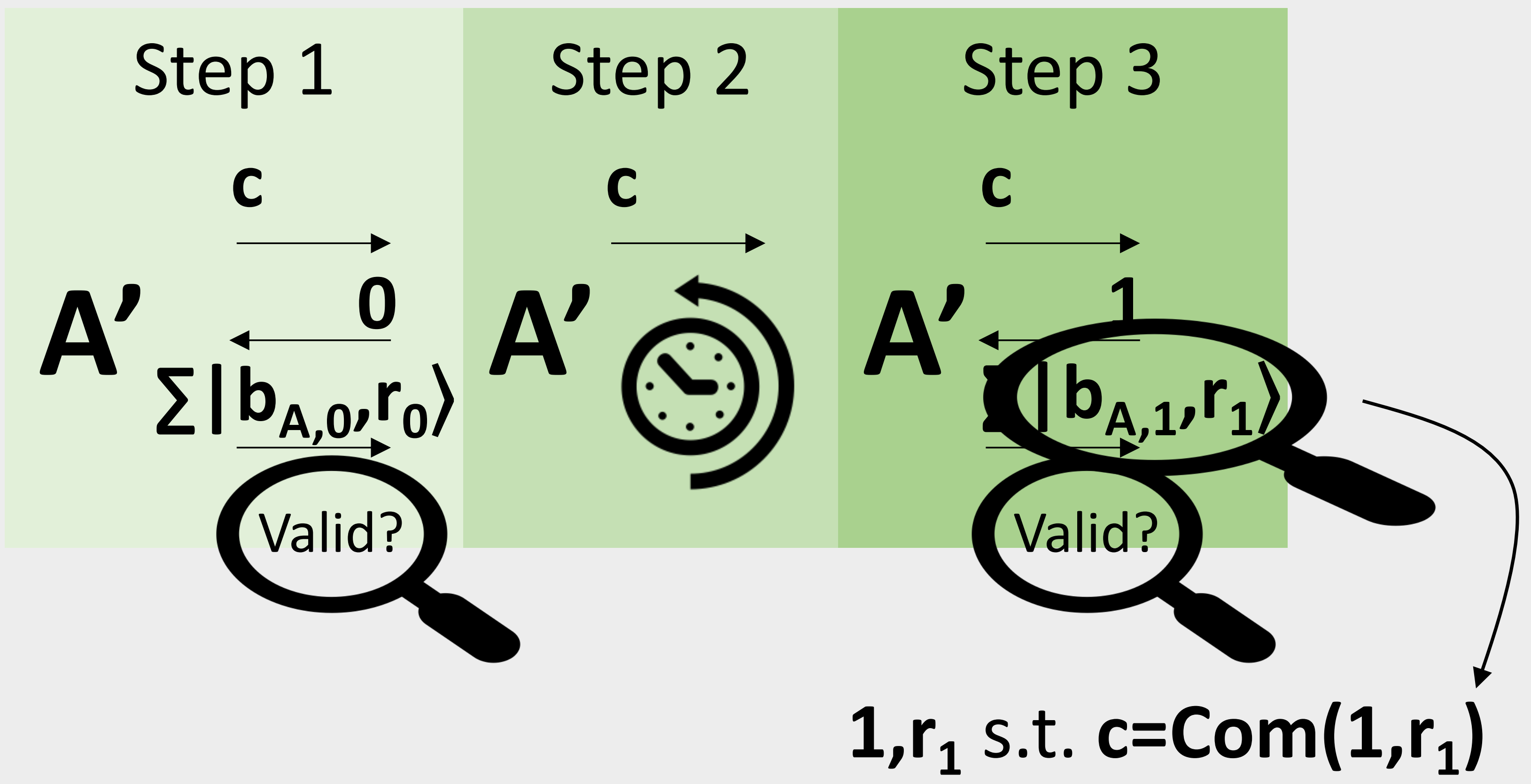
Proof that **quantum** Alice can't bias **b**



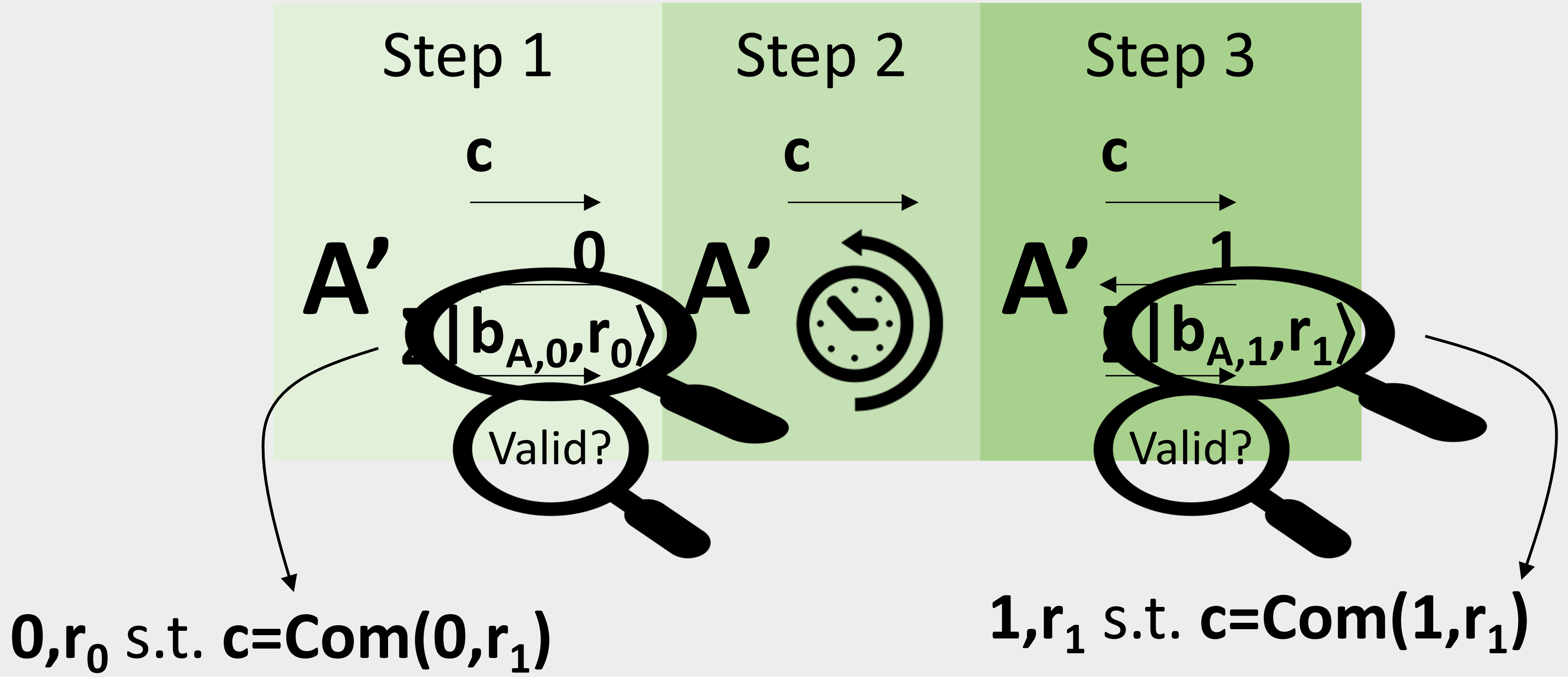
Lemma [Unruh'12]: both will be valid with probability ≥ ε^3

Still don't get a collision…

Proof that **quantum** Alice can't bias **b**



Proof that **quantum** Alice can't bias **b**



If measuring step 1 causes step 3 to fail, contradicts collapsing

Collapsing Commitments

Constructions:
- Any injective commitment
- Random oracle [Unruh'16a]
- From lossy functions (LWE) [Unruh'16b]
- The SIS hash function [Liu-**Z**'19, Liu-Montgomery-**Z**'23]
- [**Z**'22] from many other assumptions, basically matching known feasibility of plain PQ binding (constructions different)

Better rewinding techniques: [Chiesa-Ma-Spooner-**Z**'21, Lombardi-Ma-Spooner'22]

Collapsing not always necessary

Example: Hashing before signing

Sign’(sk, m) = Sign(sk, H(m))

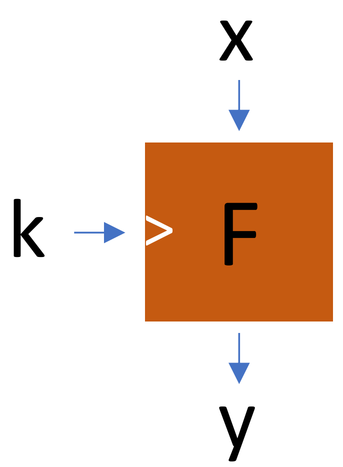
Security proof works quantumly (no rewinding), produces classical collision for **H**

Fully-Quantum Notions

So far, end goal (e.g. coin tossing) is still a classical game, but we want security against local quantum computation

But in a quantum world, there may be attacks that exploit quantum *interaction*

Example: PRFs



Def: F is a secure pseudorandom function (PRF) if, ∀PPT **A**, ∃ negligible **ε** such that

$$\left| \Pr[A^{F(k,\cdot)}()=1] - \Pr[A^{R(\cdot)}()=1] \right| < \varepsilon$$

Notes:

- **k** random
- **R** uniformly random function
- $\mathbf{A}^{O(\cdot)}$ means **A** makes queries on **x**, receives **O(x)**

Example: PRFs

What is a post-quantum PRF?

$\mathbf{A}^{|f(\cdot)\rangle}$ means can query unitary $\mathbf{O}_f$

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

↓

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

Def: F is a **PQ** secure PRF if, ∀**Q**PT **A**, ∃ negligible **ε** such that

$$| \Pr[A^{F(k,\cdot)}()=1] - \Pr[A^{R(\cdot)}()=1] | < \varepsilon$$

Def: F is a **Fully Quantum** secure PRF if, ∀**Q**PT **A**, ∃ negligible **ε** such that

$$| \Pr[A^{|F(k,\cdot)\rangle}()=1] - \Pr[A^{|R(\cdot)\rangle}()=1] | < \varepsilon$$

Example: PRFs

Is there a difference? YES!

Proof: make periodic

$$\mathbf{PRF'((k,z),\ x) = PRF(k,\ \{x, x \oplus z\})}$$

Example: PRFs

Ok. Which definition do we want? It depends…

PRFs → CPA-secure encryption

Enc(k,m) = **r ← $**
c = (r, F(k,r)⊕m)

Encrypter (honest) chooses **r** → always classical

PQ security suffices

Example: PRFs

Ok. Which definition do we want? It depends…

PRFs → MAC

MAC(k,m) = F(k,m)

Security model lets attacker choose **m**, but signer (honest) actually computes MAC

Can attacker force signer to MAC superpositions? Consider smartcard applications where adv has physical access to signer

Example: PRFs

Ok. Which definition do we want? It depends…

PRFs → Pseudorandom quantum states

[Ji-Liu-Song'18,Brakerski-Shmueli'19]

$$\sum_x (-1)^{F(k,x)} |x\rangle$$

Generation of state makes superposition query to **F**

Need full quantum security

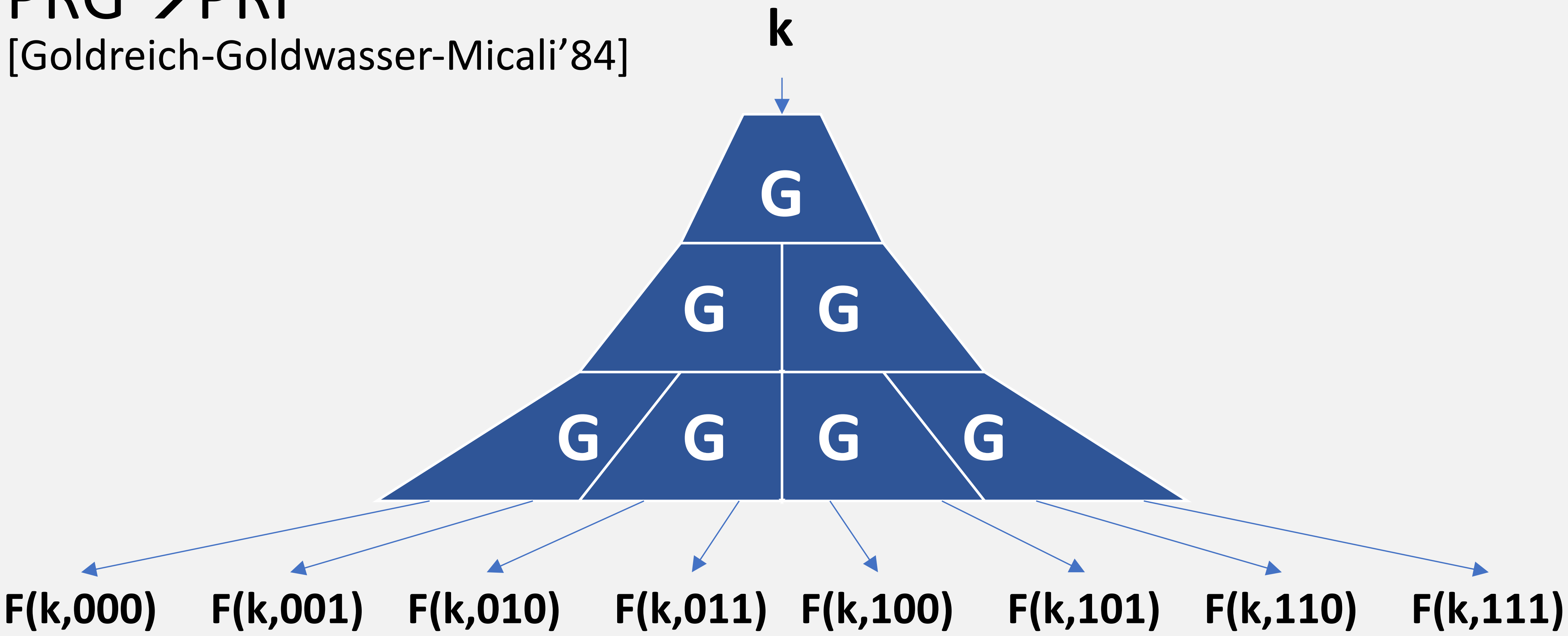
Example: PRFs

So what do classical PRF proofs give us?

Example: PRFs

PRG→PRF

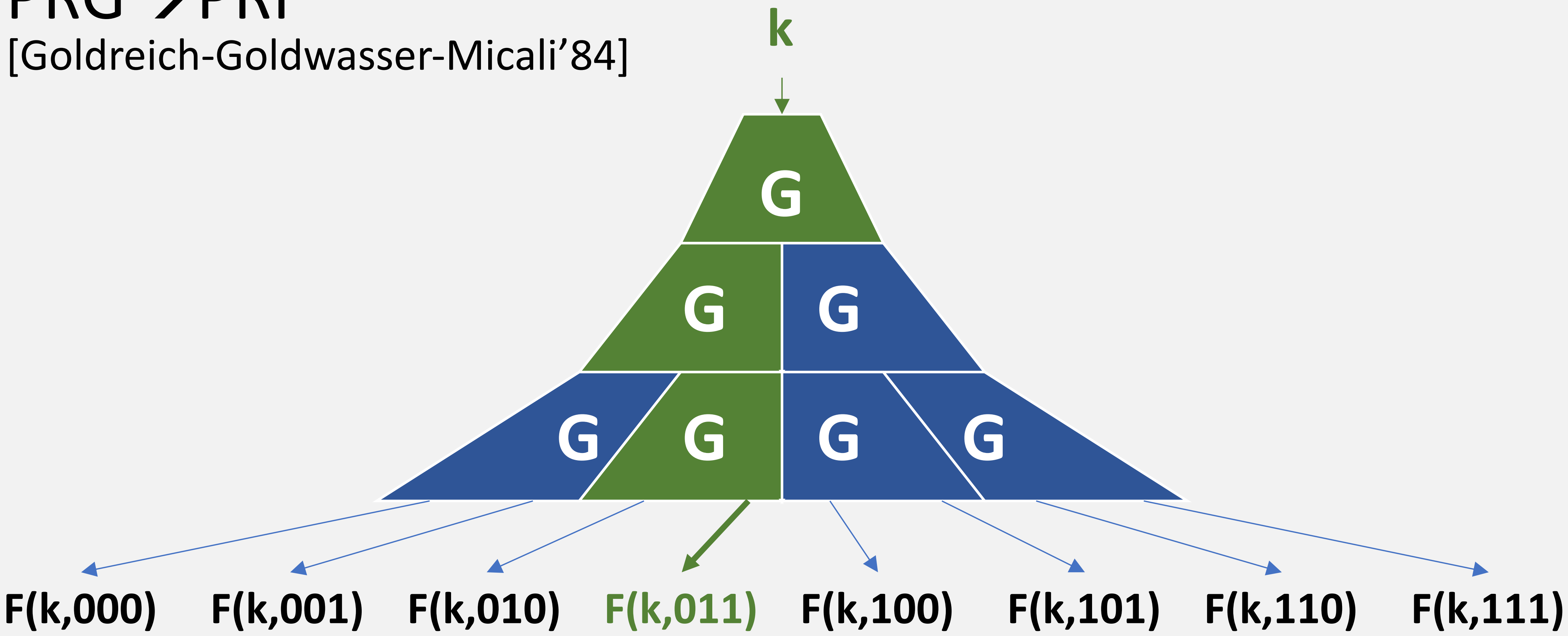
[Goldreich-Goldwasser-Micali'84]



Example: PRFs

PRG→PRF

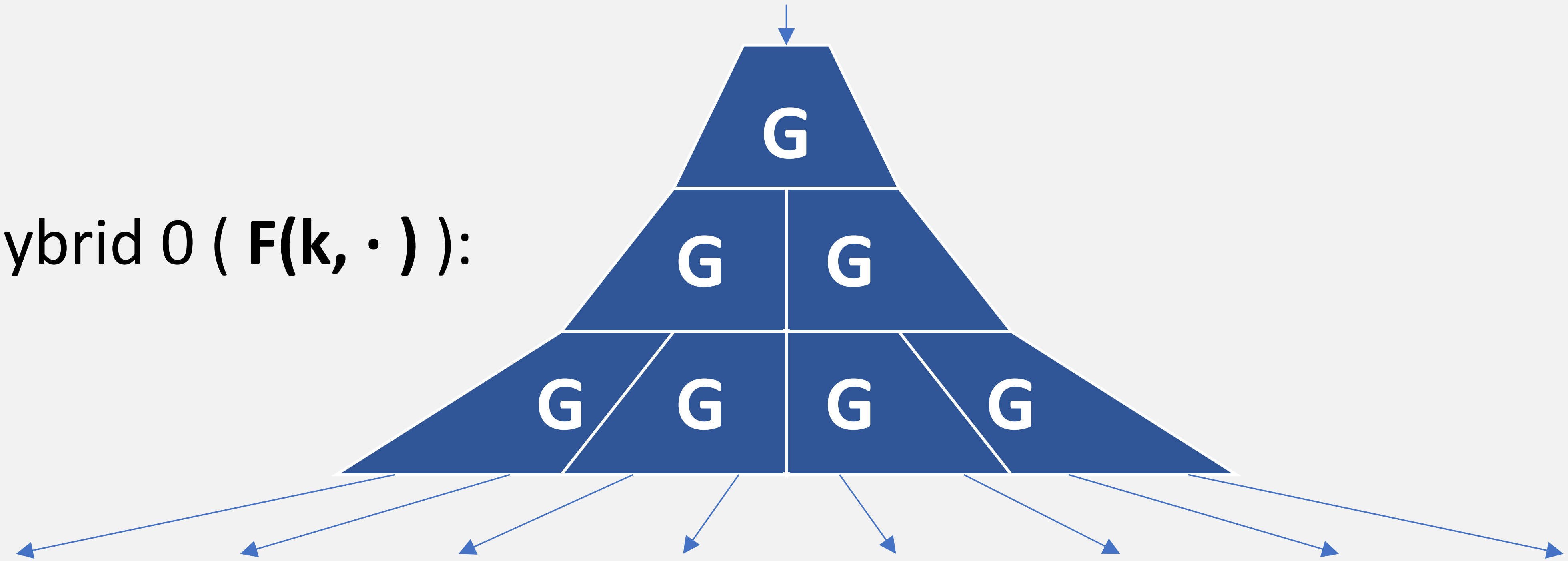
[Goldreich-Goldwasser-Micali'84]



Example: PRFs

Classical proof, step 1: Hybrid

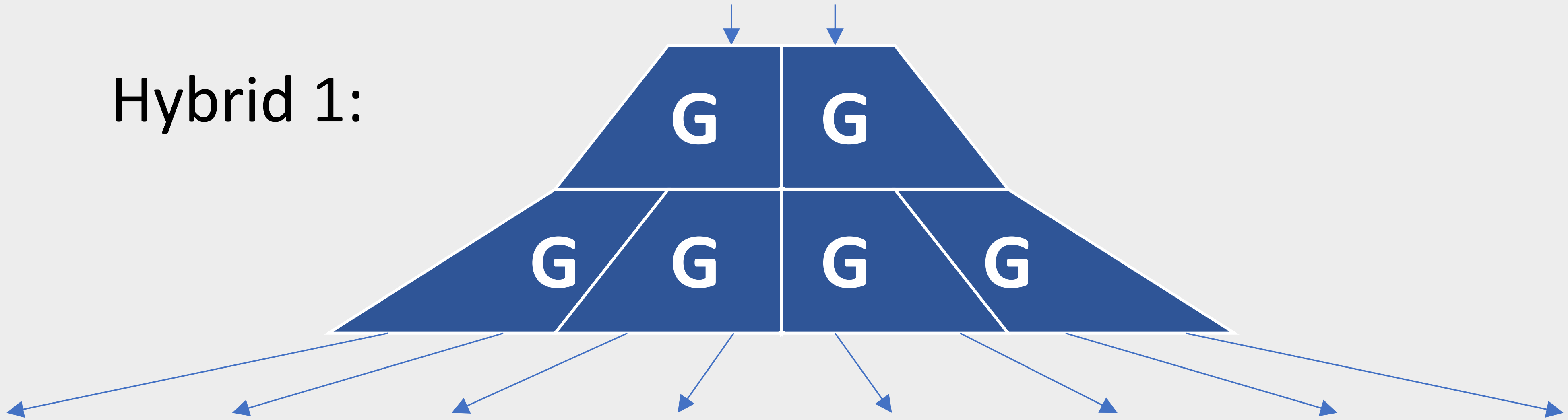
Hybrid 0 (**F(k, ·)**):



Example: PRFs

Classical proof, step 1: Hybrid

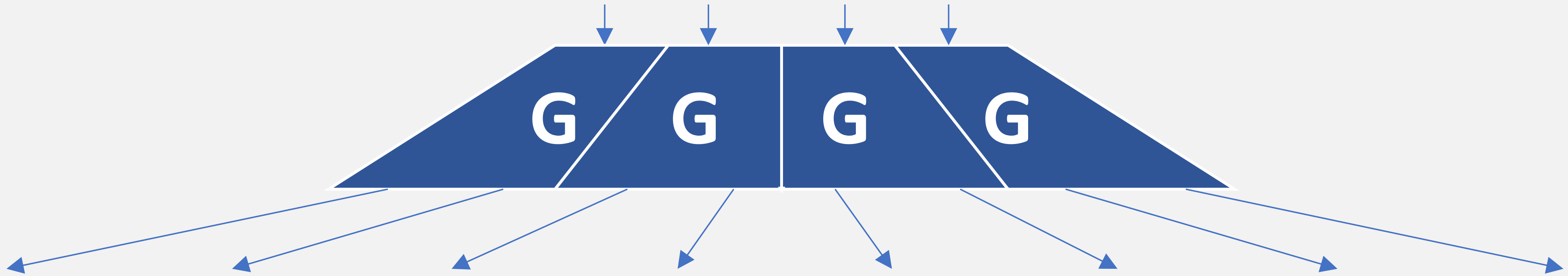
Hybrid 1:



Example: PRFs

Classical proof, step 1: Hybrid

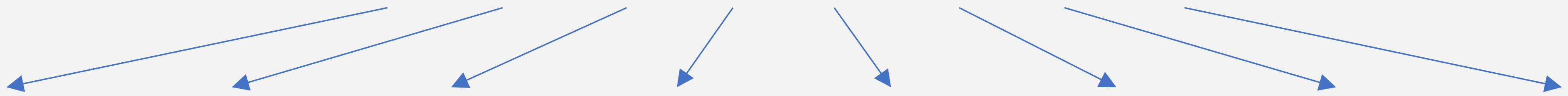
Hybrid 2:



Example: PRFs

Classical proof, step 1: Hybrid

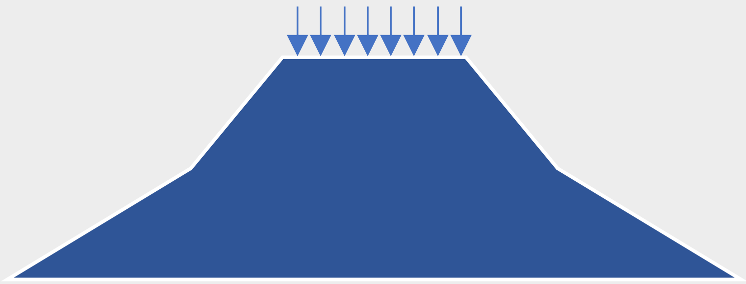
Hybrid **n** (**R(·)**):



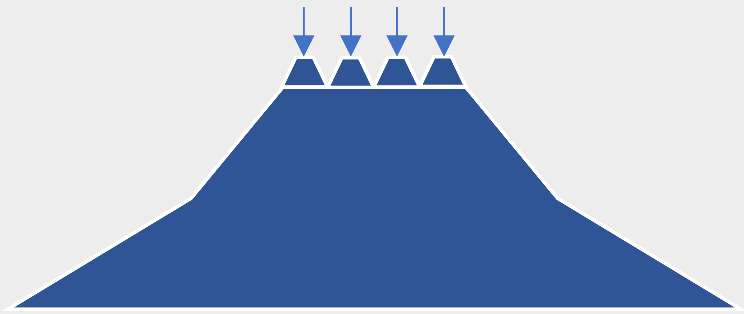
Example: PRFs

Classical proof, step 1: Hybrid

$\exists$**i** s.t. **| Pr[A$^{\text{Hybrid } i+1}$() = 1] - Pr[A$^{\text{Hybrid } i}$() = 1] | ≥ ε/n**



VS

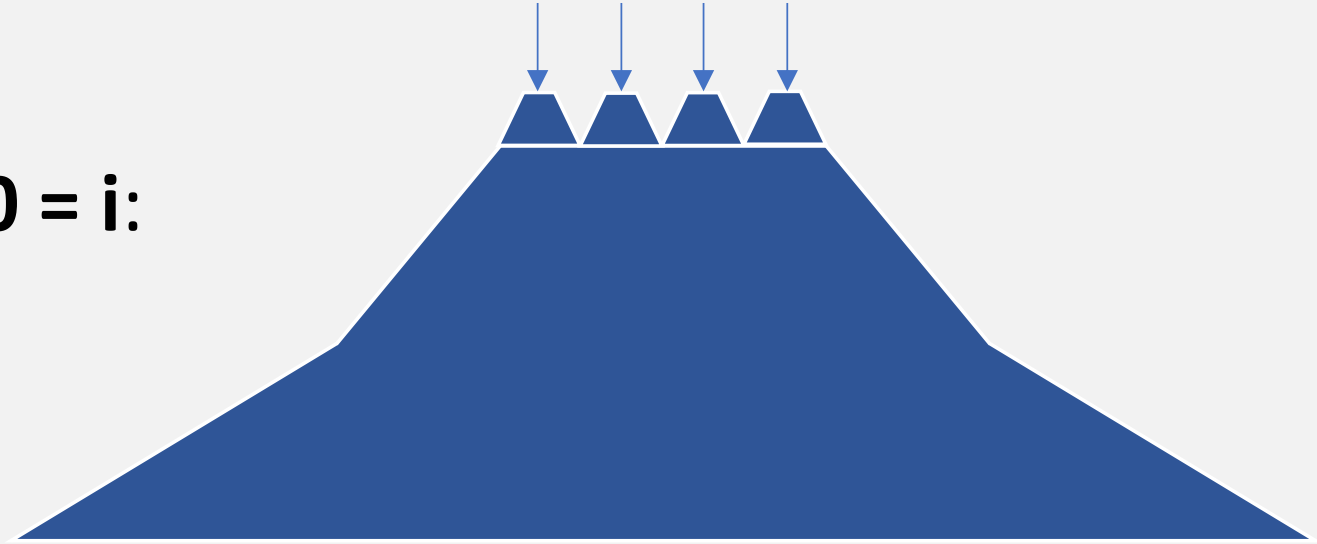


Step 1 makes sense if **A** classical, post-quantum, or fully quantum

Example: PRFs

Classical proof, step 2: Another hybrid

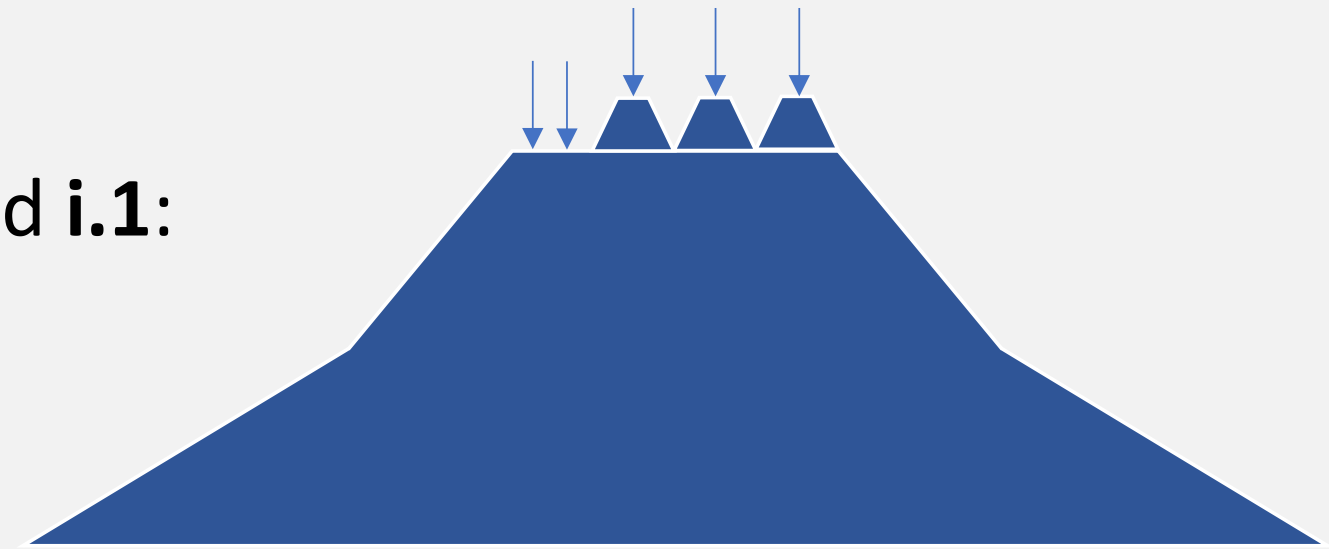
Hybrid **i.0 = i**:



Example: PRFs

Classical proof, step 2: Another hybrid

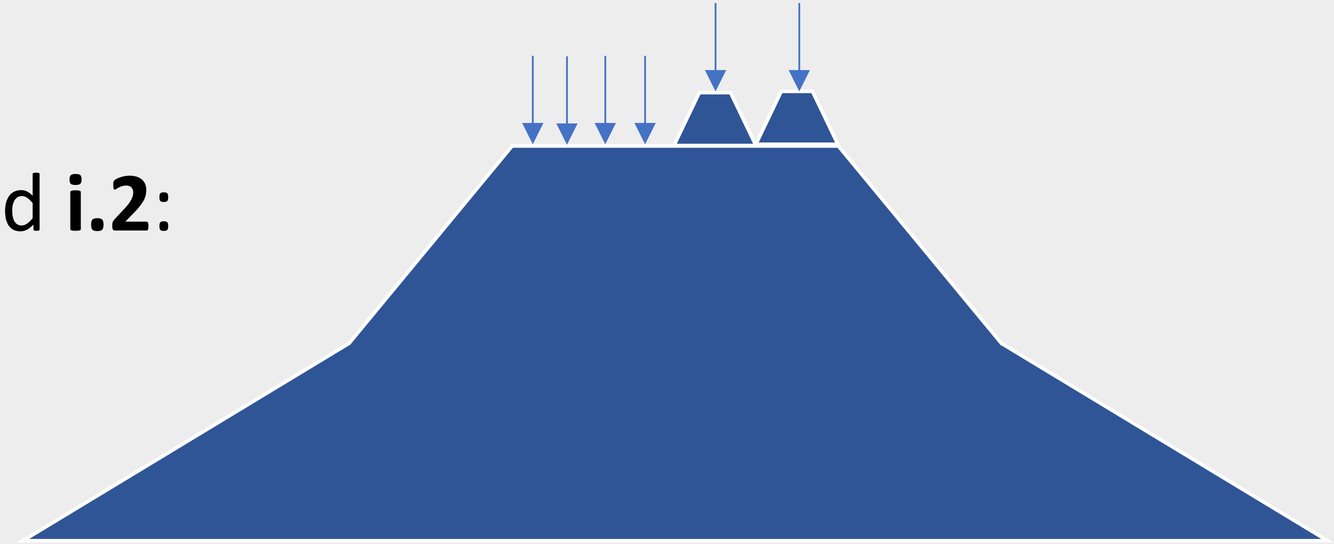
Hybrid **i.1**:



Example: PRFs

Classical proof, step 2: Another hybrid

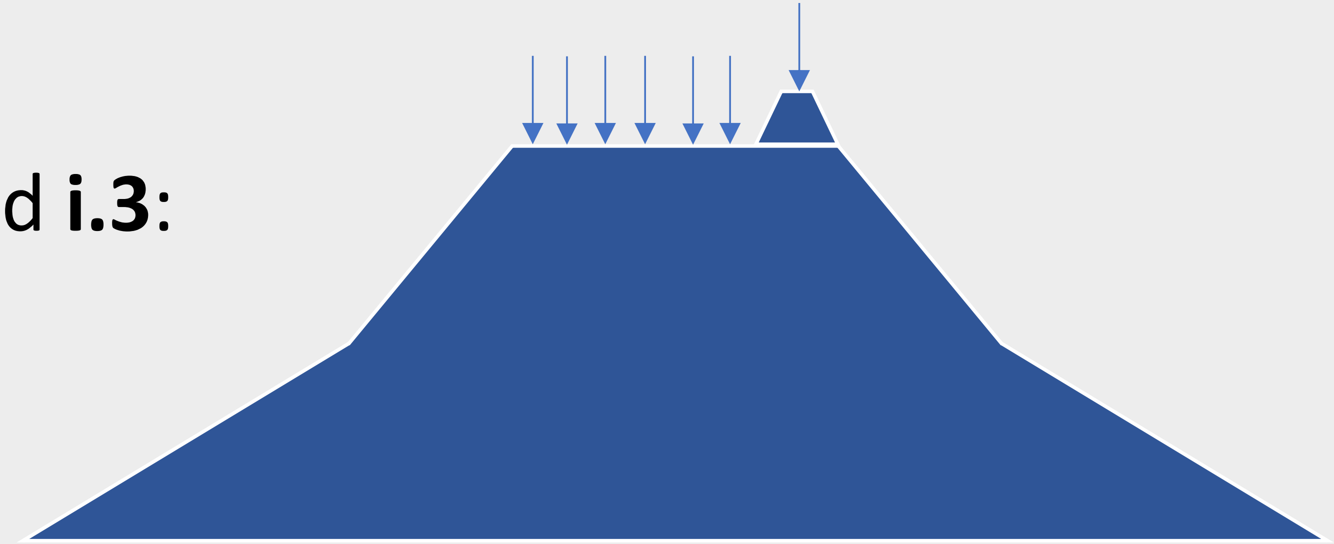
Hybrid **i.2**:



Example: PRFs

Classical proof, step 2: Another hybrid

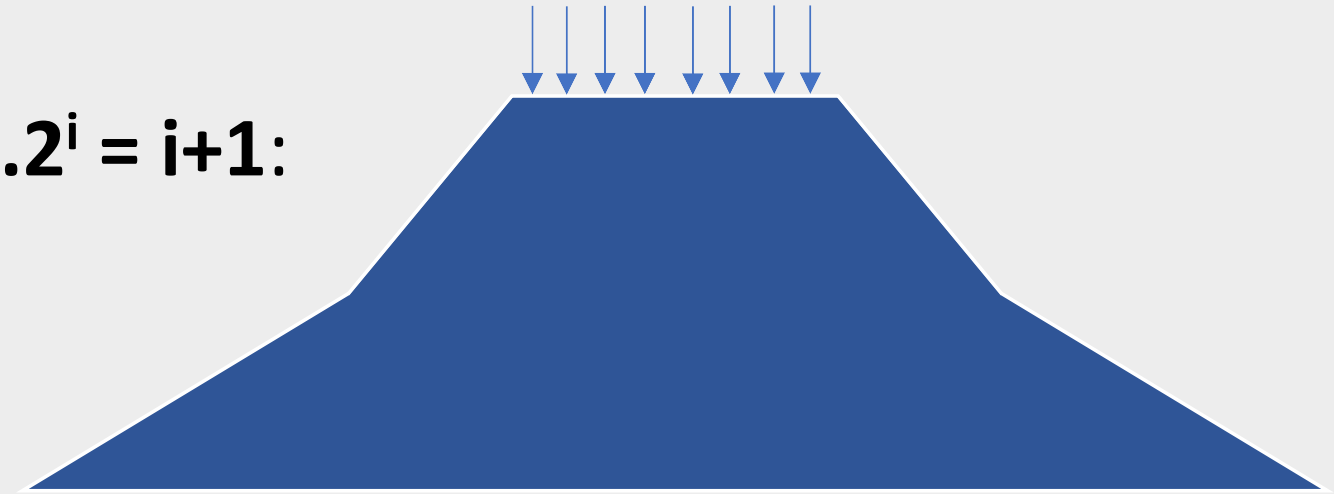
Hybrid **i.3**:



Example: PRFs

Classical proof, step 2: Another hybrid

Hybrid **i.2^{i} = i+1**:

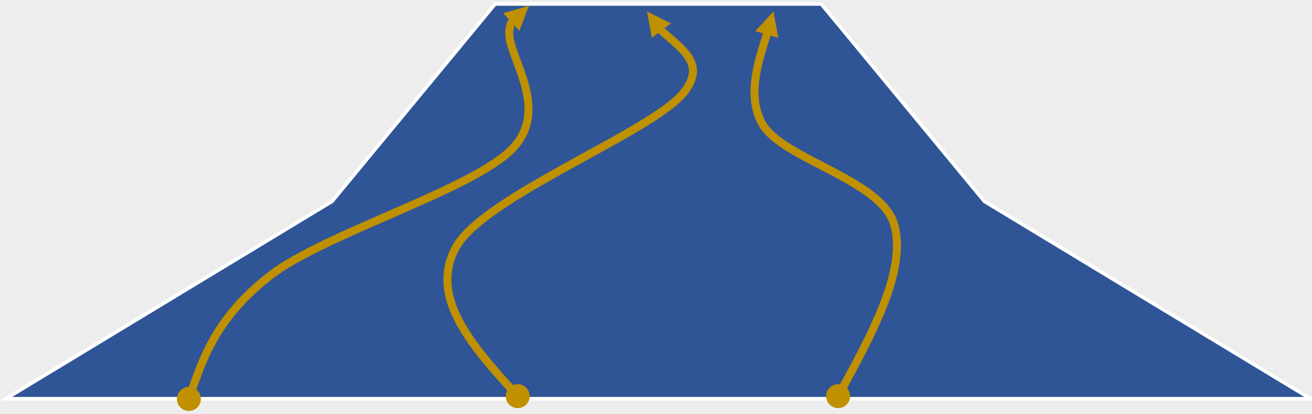


Problem: 2^{i} loss potentially exponential

Example: PRFs

Classical proof, step 2: Another hybrid

Solution: lazy/on-the-fly sampling

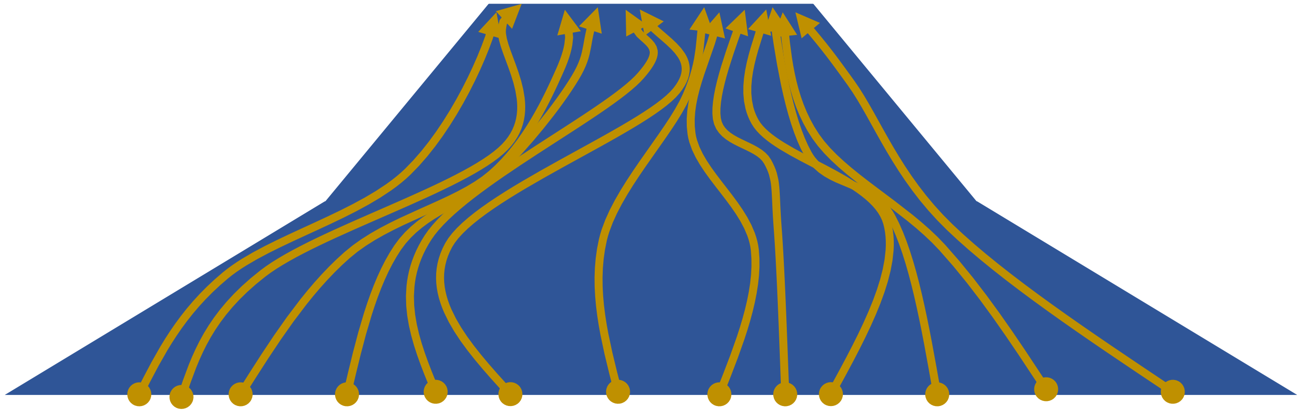


q queries → Only hybrid over **q** “active” positions

Example: PRFs

What about full quantum security?

Even single query touches **everything**



Solution: Small-range distributions! [Z'12]

Open Questions

Efficient fully-quantum *PRP*s (e.g. Luby-Rackoff)

- [**Z**'16] is rather inefficient

Build quantum ideal cipher from RO

- Need "indifferentiable" PRP

The "right" definition for superposition attacks on signatures

- [Boneh-**Z**'13, Garg-Yuen-**Z**'17] have major limitations
- Unclear if [Alagic-Majenz-Russell-Song'18] captures everything

?