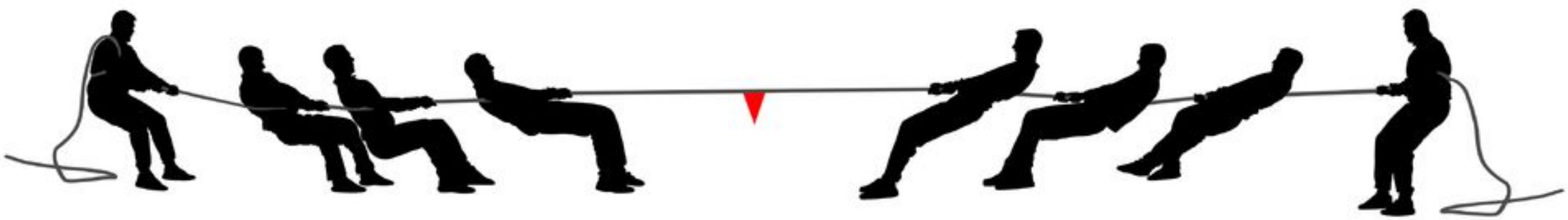
Post-Quantum Cryptography

Mark Zhandry (Princeton & NTT Research)

Pre-Modern Crypto (~2000 B.C. – 1900's A.D.)



Code makers

Code breakers

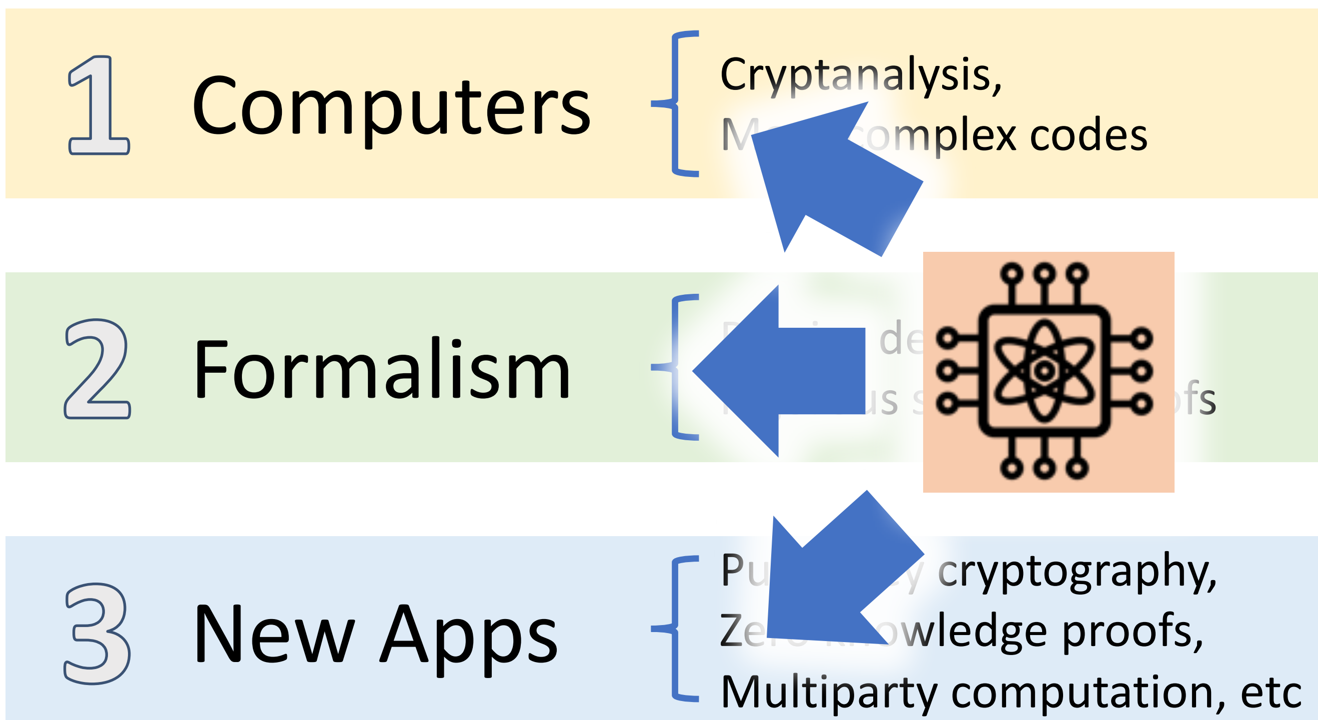
Modern Crypto (mid 1900's - Present)

1 Computers
- Cryptanalysis,
- More complex codes

2 Formalism
- Precise definitions
- Rigorous security proofs

3 New Apps
- Public key cryptography,
- Zero knowledge proofs,
- Multiparty computation, etc

Post-Quantum Crypto (2000’s - ???)



This talk: brief overview quantum computing threat to cryptography

Review of Modern Crypto

P=NP $\Longrightarrow$ Most crypto impossible

Most crypto relies on un-proven computational assumptions

Ex: Hardness of FACTORING, DLOG, lattice problems, inverting SHA3, etc.

Fundamental Formula of Modern Crypto

Crypto security "proof" = Computational Assumption P + Precise Security Def. D + Reduction from P to D

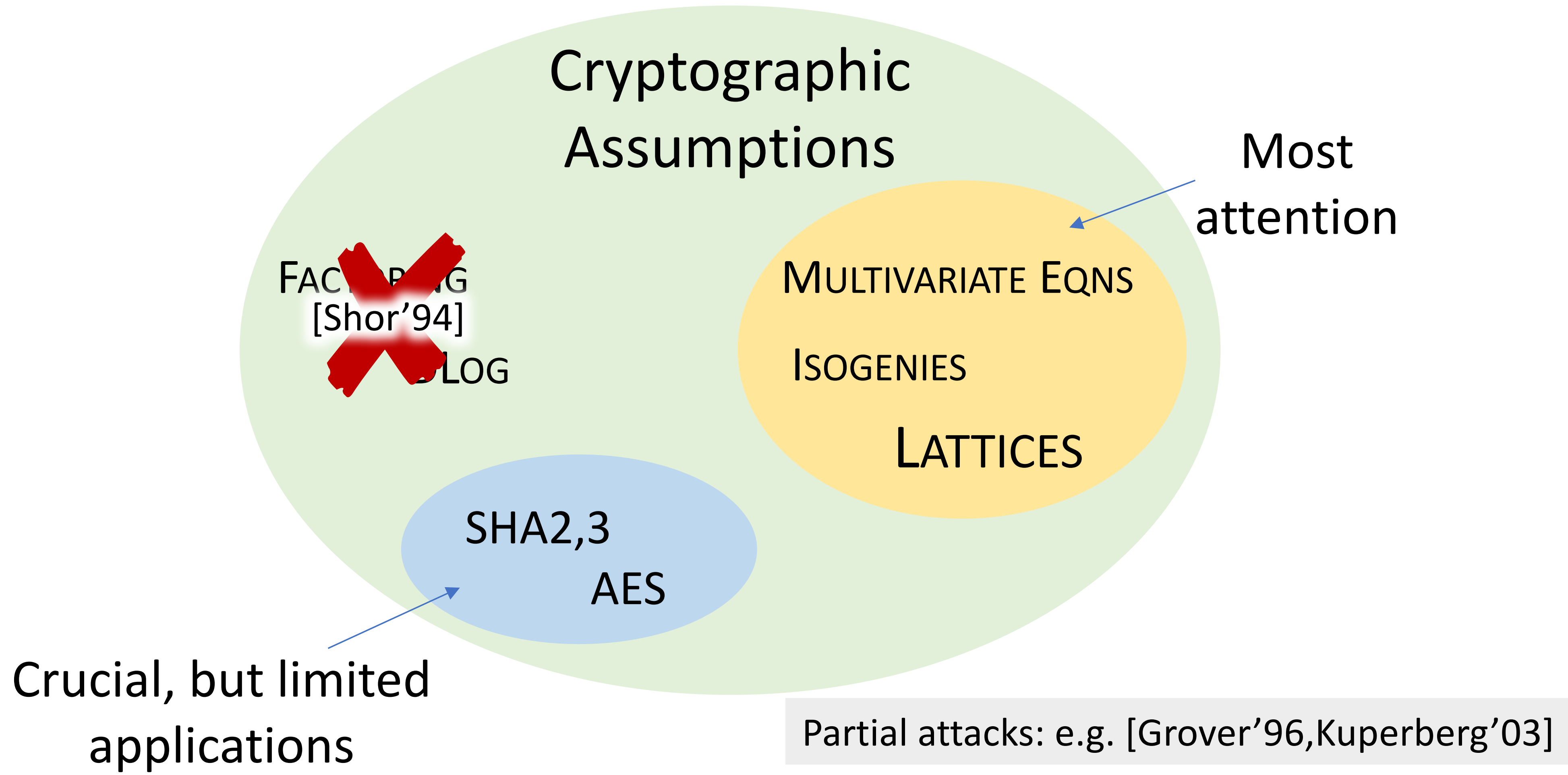
Problem: Typically only considers classical computers

Fundamental Formula of *PQ* Crypto

Post-quantum security proof = *Post-quantum* Assumption + Precise *PQ* Security Def. + *Quantum* Reduction

Must carefully revisit all three ingredients!

Cryptographic Assumptions


Cryptographic
Assumptions
Most
attention
[Shor’94]
MULTIVARIATE EQNS
ISOGENIES
LATTICES
SHA2,3
AES
Crucial, but limited
applications
Partial attacks: e.g. [Grover’96,Kuperberg’03]

Key Takeaway: Essentially all "total" quantum attacks view assumption as period finding/hidden subgroup over abelian groups

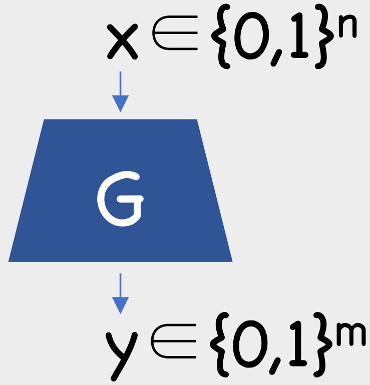
FACTORING: $f(a) = g^a \bmod N$ ➡ $g^{period/2}$ is root of 1

DLOG: $f(x,y) = g^x \times h^{-y}$ ➡ period $(a,1)$ where $h=g^a$

Rest of Talk:
Crypto Definitions
and Reductions

Example 1: PRGs

Example: Classical Pseudorandomness



$(m>n)$

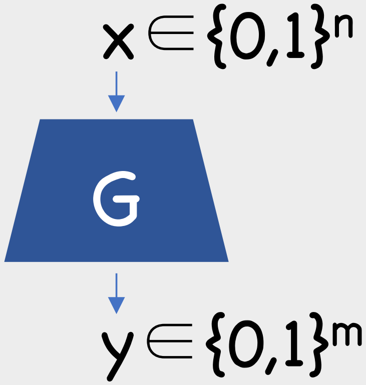
Def: G is a secure pseudorandom generator (PRG) if, $\forall$ PPT A, $\exists$ negligible ε such that

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

PPT = "Probabilistic Poly Time"
(aka, "efficient classical")

ε called "advantage" of A

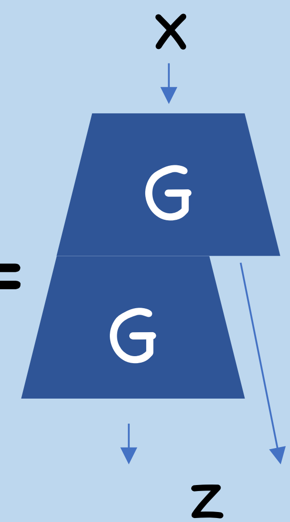
Example: Classical Pseudorandomness



(m>n)

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

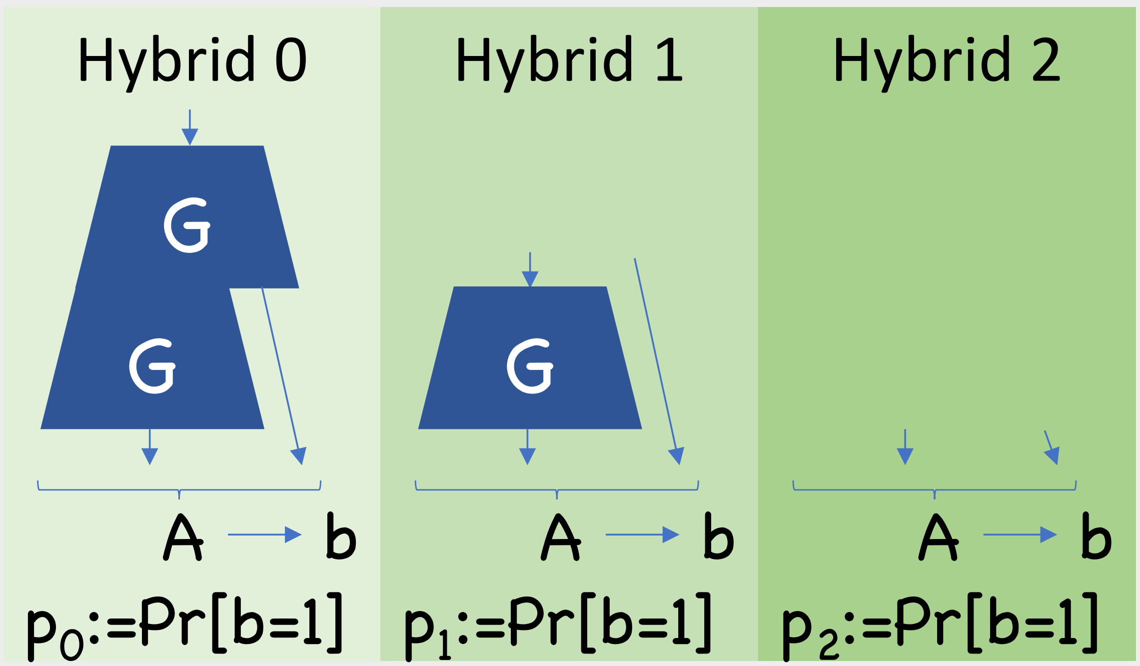
Solution: G_2 =



Thm: If G is secure, then so is G_2

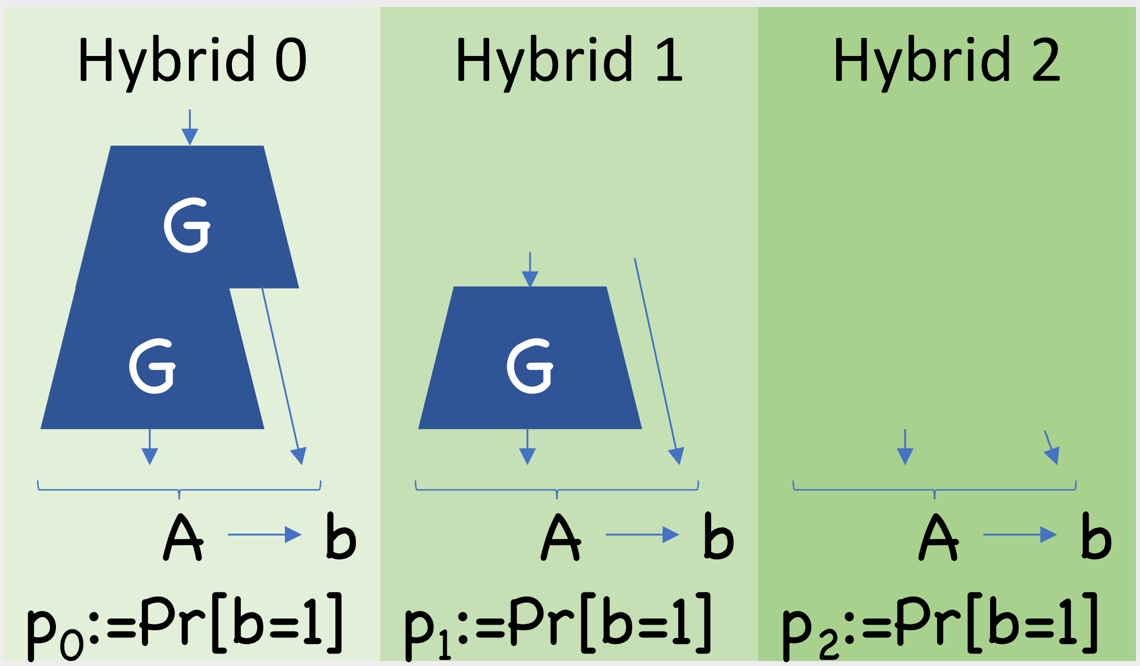
Proof: Suppose G_2 insecure. Then $\exists$ PPT A, non-negl ε s.t.

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



Proof: Suppose G_2 insecure. Then ∃ PPT A, non-negl ε s.t.

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



Either:
$|p_1-p_0| \geq \varepsilon/2$

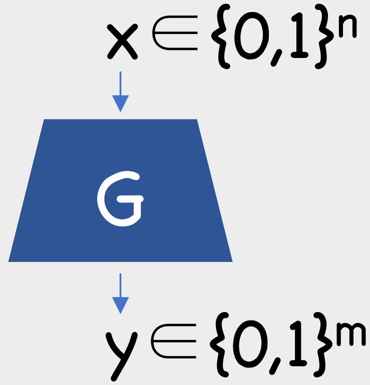
$B(y_0,y_1)=$
$A(G(y_0),y_1)$

Or:
$|p_2-p_1| \geq \varepsilon/2$

$B(y_0,y_1)=$
$A(y_0,y_1,\$)$

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

What about *post-quantum* pseudorandomness?



(m>n)

Def: G is a **post-quantum** secure PRG if,
$\forall$ **Q**PT A, $\exists$ negligible ε such that

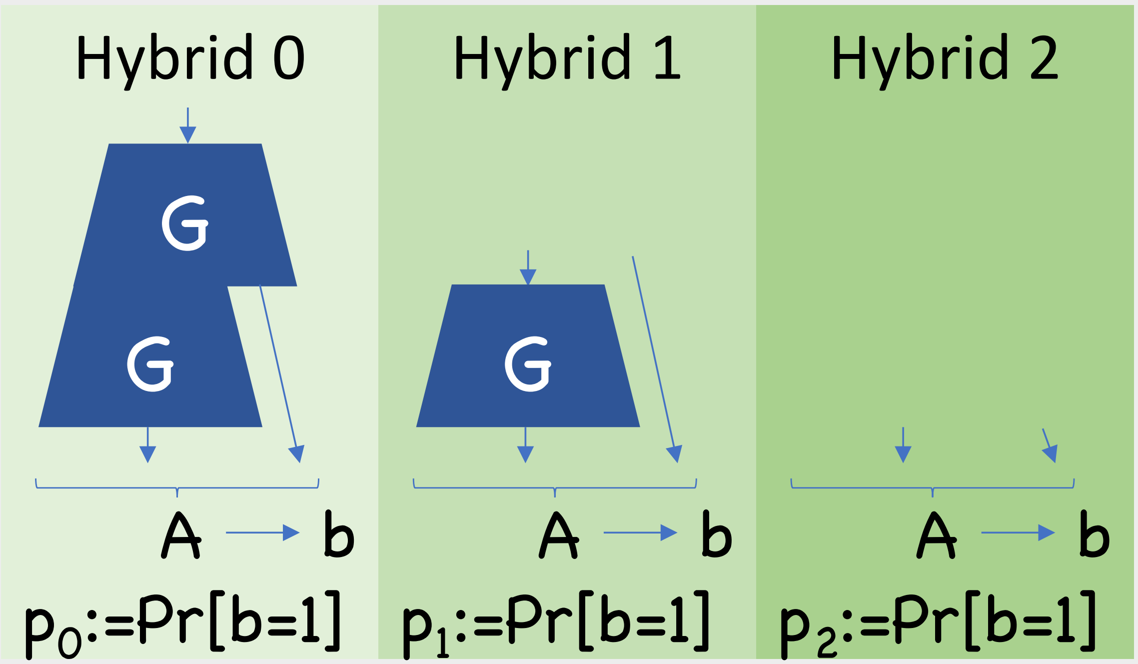
$$| \Pr[A(y)=1] - \Pr[A(G(x))=1] | < \varepsilon$$

QPT = "Quantum Poly Time"
(aka, "efficient quantum")

Thm: If G is post-quantum secure, then so is G_2

Proof: Suppose G_2 **PQ** insecure. Then $\exists$ **Q**PT A, non-negl ε s.t.

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



Either: $|p_1-p_0|\geq\varepsilon/2$

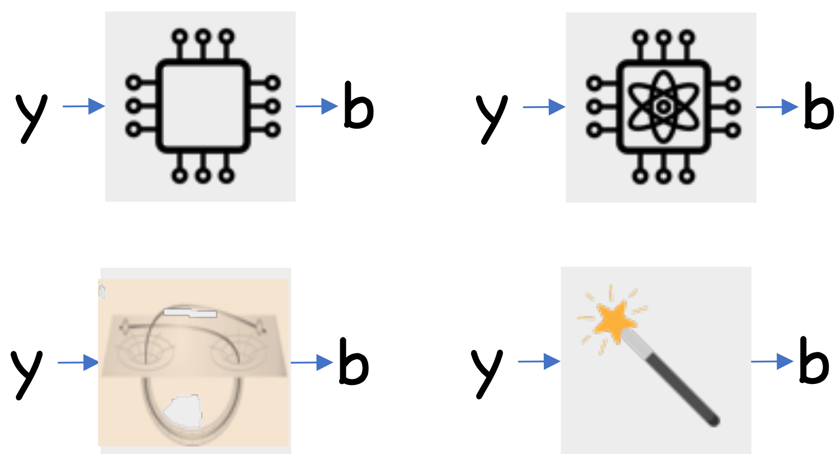
$B(y_0,y_1)= A(G(y_0),y_1)$

Or: $|p_2-p_1|\geq\varepsilon/2$

$B(y_0,y_1)= A(y_0,y_1,\$)$

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

Proof for G_2 doesn't care how A works internally, as long as it has non-negligible advantage



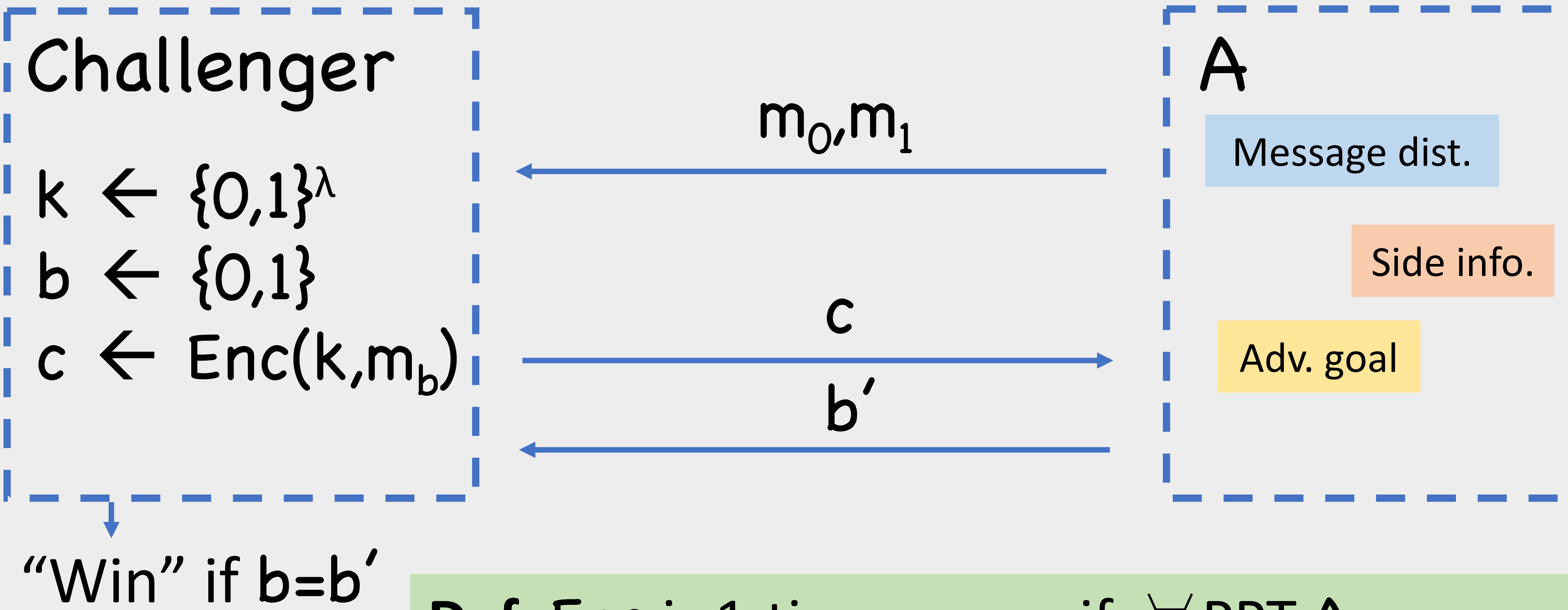
That is, proof treats A as "black box"

Key Takeaway: As long as reduction treats $\mathcal{A}$ as a *non-interactive single-run* black box, reduction likely works in quantum setting

Will continue updating throughout talk

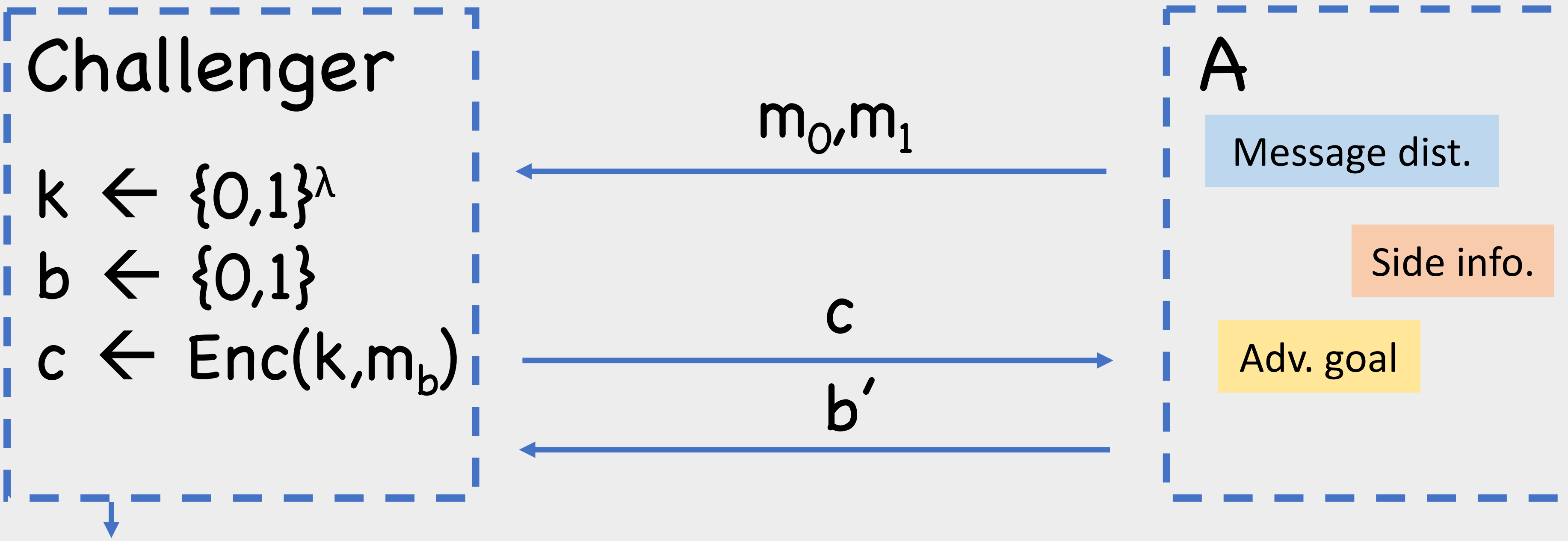
Example 2: Encryption

Example: Classical Encryption



Def: Enc is 1-time secure if, $\forall$ PPT A, $\exists$ negligible ε such that $|\Pr[\text{Win}] - \frac{1}{2}| < \varepsilon$

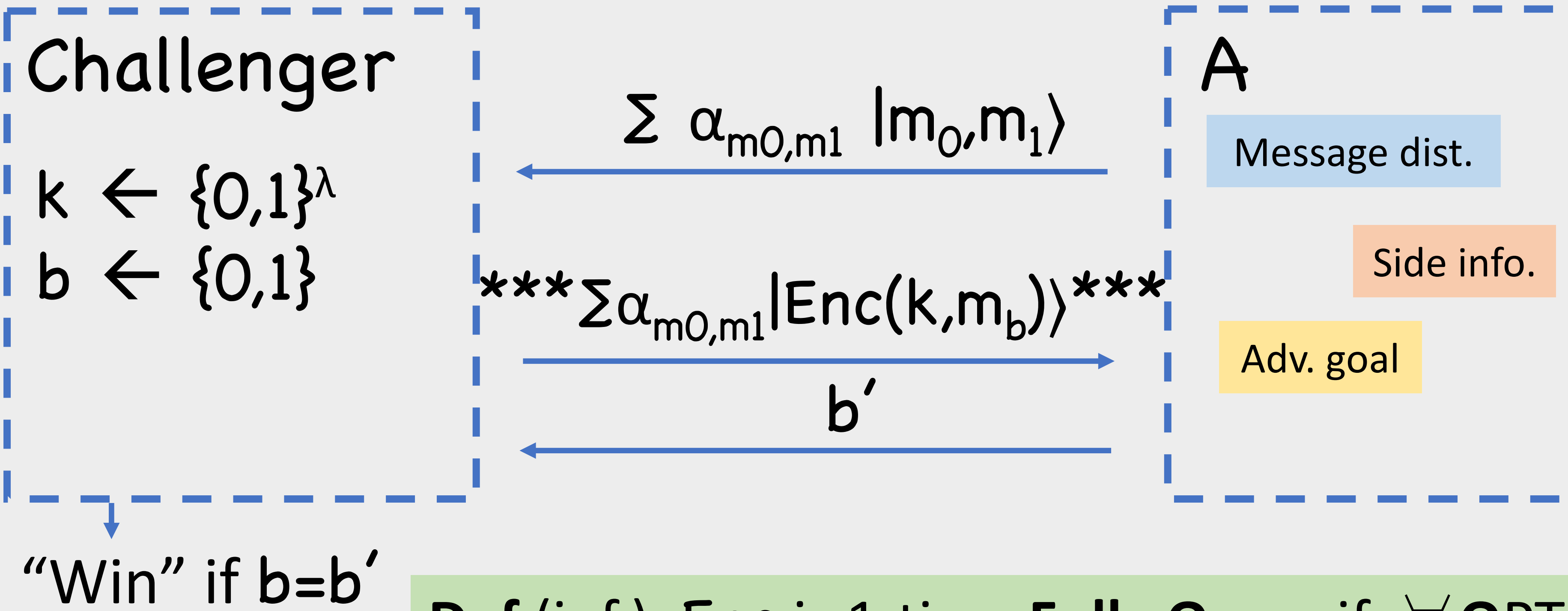
Example: PQ Encryption???



"Win" if $b=b'$

Def: Enc is 1-time **PQ** secure if, $\forall$ **Q**PT A, $\exists$ negligible ε such that | Pr[Win] − ½ | < ε

Example: PQ Encryption???



Def (inf.): **Enc** is 1-time **Fully Q** sec. if, $\forall$ **Q**PT A, $\exists$ negl ε such that $|\Pr[\text{Win}] - \frac{1}{2}| < \varepsilon$

Key Takeaway: Which definition to use depends on use-case, what kind of attacks may be possible

Classical honest users + remote adversary over classical network → PQ security likely sufficient

Quantum honest users and/or $\mathcal{A}$ has physical access → May need Full Quantum security

Example: PRGs → Encryption

$$\text{Enc}(k,m) = G(k) \oplus m$$

Thm: If G is secure, then so is Enc

Proof: Suppose Enc insecure. Then $\exists$ PPT A, non-negl ε …

Hybrid 0	$c = \text{Enc}(k,m_b)$ $= G(k) \oplus m_b$	$\Pr[b' = b] = ½+\varepsilon$
Hybrid 1	$c = \$ \oplus m_b$ $=$ random	$\Pr[b' = b] = ½$

Adversary B with advantage ε

Example: **PQ** PRGs → **PQ** Encryption

$$\mathrm{Enc}(k,m) = G(k) \oplus m$$

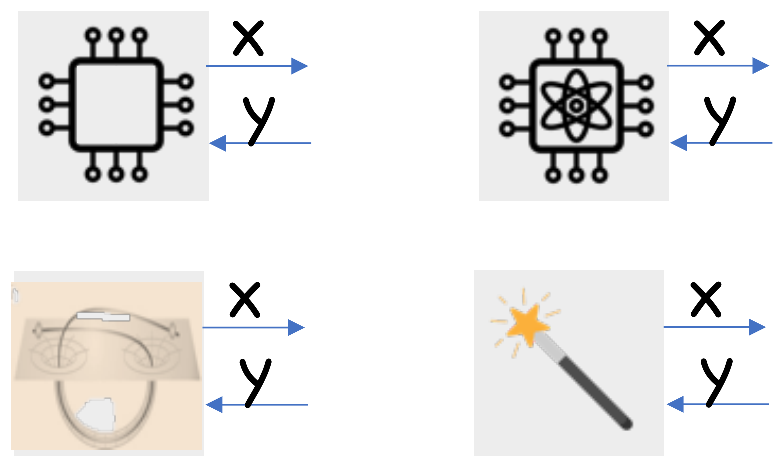
Thm: If G is **PQ** secure, then so is Enc

Proof: Suppose Enc **PQ** insecure. Then $\exists$ **Q**PT A, non-negl ε …

Hybrid 0	$c = \mathrm{Enc}(k,m_b)$ $= G(k) \oplus m_b$	$\Pr[b' = b] = ½+\varepsilon$
Hybrid 1	$c = \$ \oplus m_b$ $=$ random	$\Pr[b' = b] = ½$

→ **PQ** Adversary B with advantage ε

Proof doesn’t care how A works internally, as long as it has non-negligible advantage



➔ Also post-quantum reduction

Example: **PQ** PRGs vs **Fully Quantum** Encryption?

$$\text{Enc}(k,m) = G(k) \oplus m$$

Thm: Enc is **not** fully quantum secure

Proof:

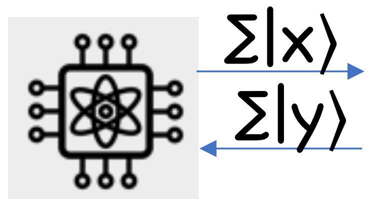
$$\sum_m |m,0\rangle \xrightarrow{b=0} \sum_m |G(k)\oplus m\rangle = \sum_m |m\rangle$$

$$\sum_m |m,0\rangle \xrightarrow{b=1} |G(k)\rangle$$

Easily distinguished by applying $H^{\otimes n}$

Q: Why does security proof fail for full quantum security?

A: Adversary no longer black box w/ classical interaction



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 interaction is quantum, all bets are off

Q: Construct fully quantum secure encryption?

A: Depends on exact definition:

- [Boneh-Z'13]: Some definitions unattainable
- [Gagliardoni-Hülsing-Schaffner'15, Alagic-Broadbent-Fefferman-Gagliardoni-Schaffner-Jules'16]: Some attainable definitions

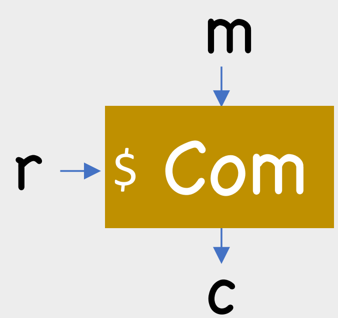
Example scheme (for *some* definition):

$$\mathrm{Enc}(k,m) = f_k(m)$$

f_k = sufficiently expanding pairwise-independent function

Example 3: Commitments and Coin Tossing

Example: Commitments

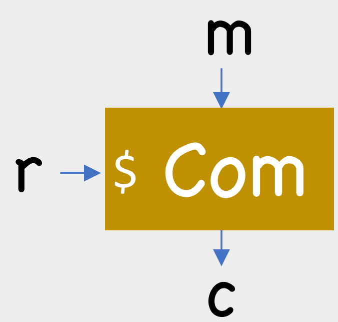


Def: *Com* is (computationally) binding if, $\forall$ PPT $\mathcal{A}$, $\exists$ negligible ε such that

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

Also want hiding, but we will ignore

Example: **PQ** Commitments???



Def: *Com* is **post-quantum** binding if, $\forall$ **Q**PT A,
$\exists$ negligible ε such that

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

Example: Commitments → Coin Tossing

$b_A \leftarrow \{0,1\}$
$r \leftarrow \$$

$c = com(b_A, r)$ →

← b_B

b_A, r →

$b_B \leftarrow \{0,1\}$

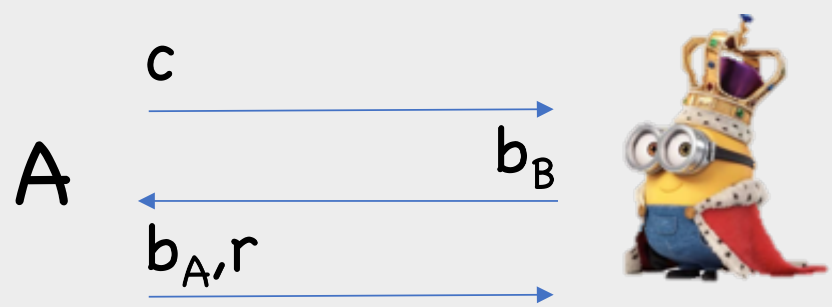
Verify $c = com(b_A, r)$

pass: $b = b_A \oplus b_B$

fail: $b = \perp$

Classical proof that Alice can't bias **b**:

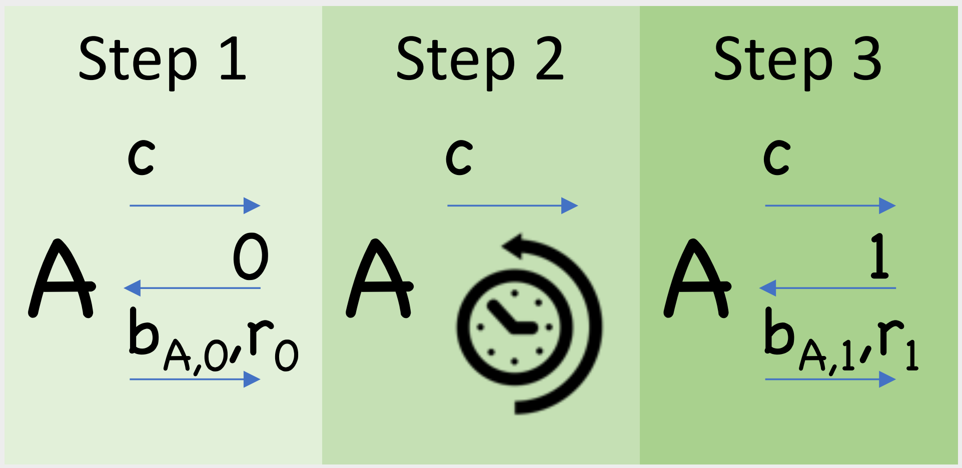
Let $\mathcal{A}$ be supposed adversary



$\Pr[b=0] > ½+\varepsilon$ ➡ For both $b_B=0$ and $b_B=1$, good chance $b_A=b_B$ and $\text{Com}(b_A,r)=c$

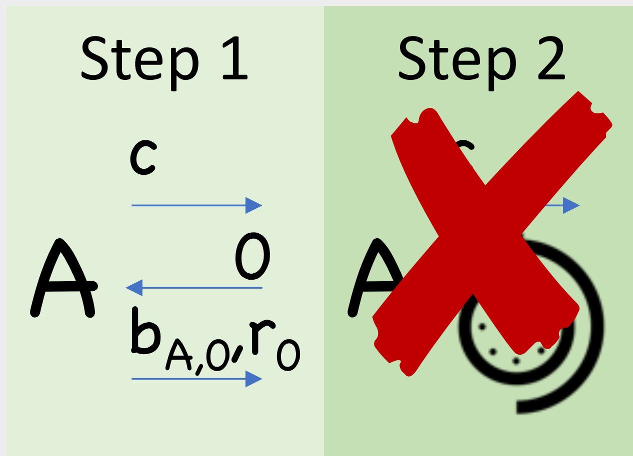
Classical proof that Alice can't bias b:

Let A be supposed adversary



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

Proof that **Quantum** Alice can’t bias **b**???



Measurement principle: extracting $b_{A,0}, r_0$ irreversibly altered A’s state

Thm (Ambainis-Rosmanis-Unruh'14,Unruh'16):
$\exists$ PQ binding *Com* s.t. Alice has a near-perfect strategy

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 $\mathcal{A}$ as a *single-run* black box (potentially w/ *classical* interaction), reduction likely works in quantum setting

! But if interaction is quantum, all bets are off

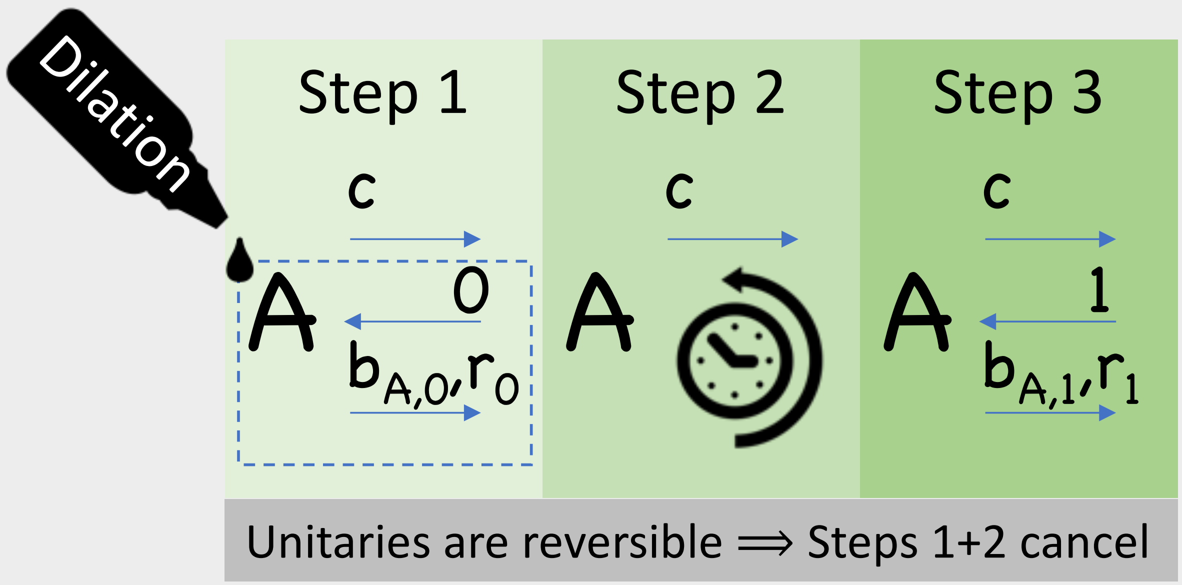
! But if rewinding $\mathcal{A}$, all bets are off

(even if interaction classical)

Q: Is there *some* commitment that gives coin tossing?

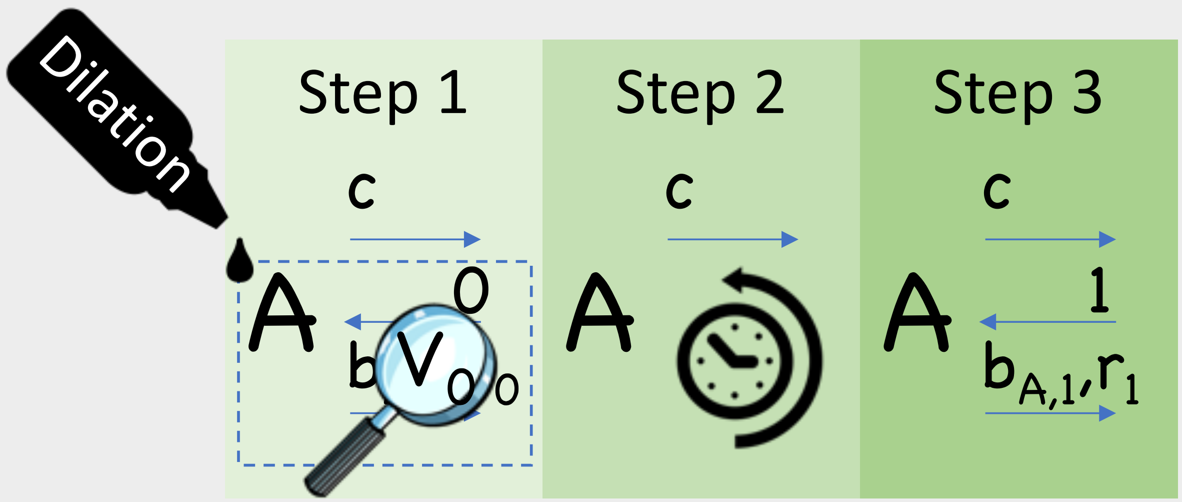
A: Yes!

Let A be supposed (quantum) adversary



$$V_d := b_{A,d} = d \wedge \mathrm{Com}(b_{A,d}, r_d) = c \quad \Longrightarrow \quad \Pr[\, V_1 \,] = \varepsilon$$

Let A be supposed (quantum) adversary



Lemma [Unruh'12]: $\Pr[\, V_0 \wedge V_1 \,] = \mathrm{poly}(\varepsilon)$

Still not done: $b_{A,0}, r_0$ no longer exist!

Solution: Better security for Com

Def: Com is perfectly binding if $\nexists\ m_0 \neq m_1, r_0, r_1$ s.t.

$$\mathsf{Com}(m_0,r_0)=\mathsf{Com}(m_1,r_1)$$

$\Longrightarrow$ $b_{A,0}, r_0$ uniquely determined by **c**

$\Longrightarrow$ measuring them has no effect

$\Longrightarrow$ Obtain collision $\Longrightarrow$ contradiction

Limitation: perfect binding requires large commitemnts

Solution: Better security for $\mathcal{C}om$

Def [Unruh'16] (inf.): $\mathcal{C}om$ is collapse binding if adversary cannot *detect* measuring $\mathsf{b}_{A,0},\mathsf{r}_0$

$\Longrightarrow$ $\mathsf{b}_{A,0},\mathsf{r}_0$ measuring them has no noticeable effect

$\Longrightarrow$ Obtain collision $\Longrightarrow$ contradiction

Collapse binding has become the standard post-quantum notion for commitments

Ambainis-Rosmanis-Unruh $\Longrightarrow$ Not all $\mathcal{Com}$ are collapse binding

Q: Do collapse binding $\mathcal{Com}$ exist? How to construct?

Thm [Unruh'16]: Random oracles are collapse binding

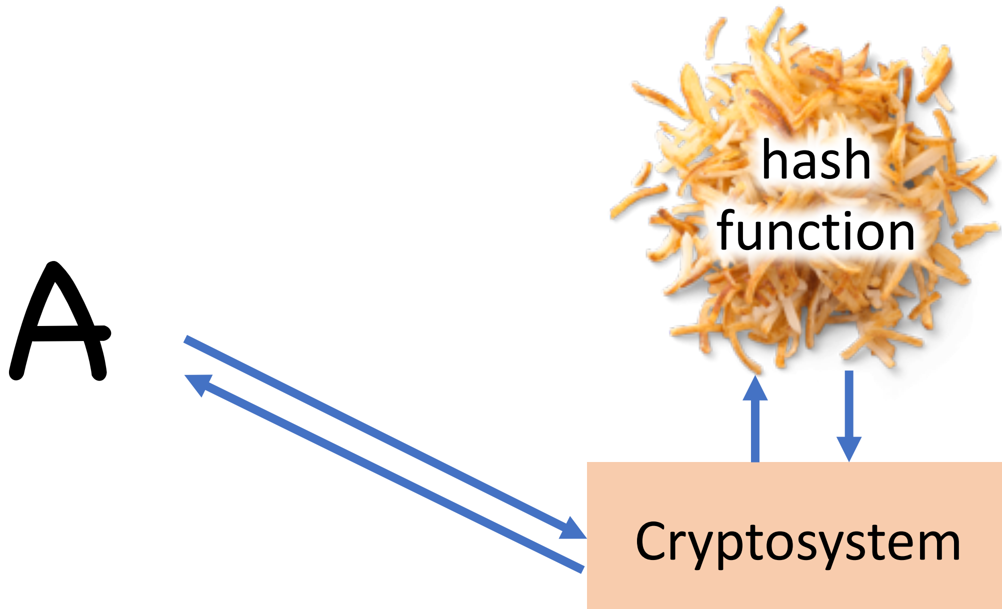
Thms [Unruh'16b,Liu-Zhandry'19]: LWE $\Longrightarrow$ Collapsing binding

Key Takeaway: Even if only worried about attacks over classical channel, sometimes need to consider security under quantum interaction.

Example 4: Random Oracle Model

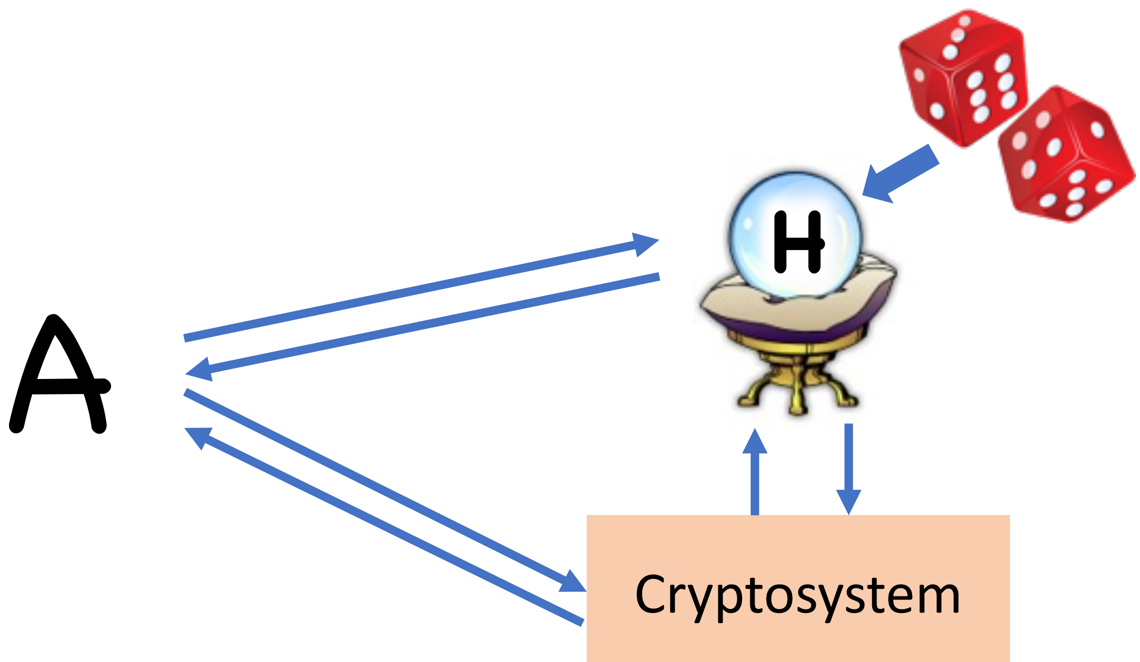
(Classical) Random Oracle Model (ROM)

[Bellare-Rogaway’93]



(Classical) Random Oracle Model (ROM)

[Bellare-Rogaway'93]



(Classical) Random Oracle Model (ROM)

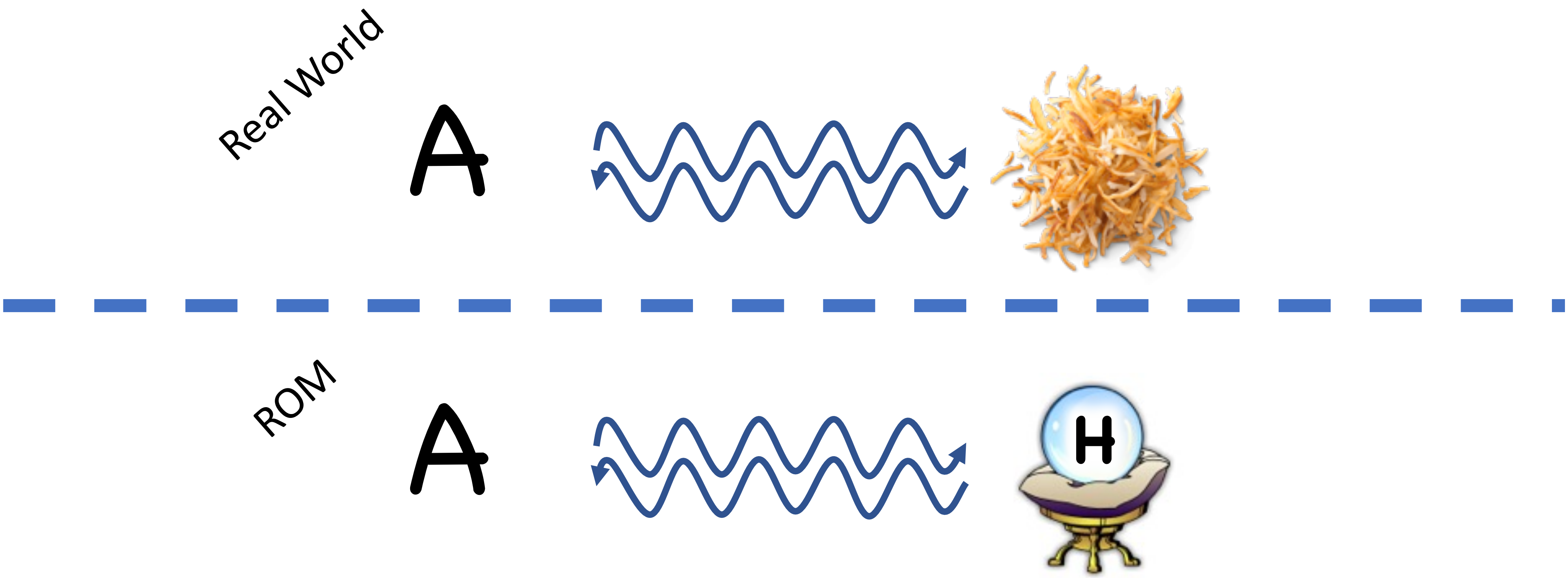
[Bellare-Rogaway'93]

Idea: If $\exists$ ROM security proof, any attack must exploit structure of hash function

Hopefully not possible for well-designed hash

The Quantum Random Oracle Model (QROM)

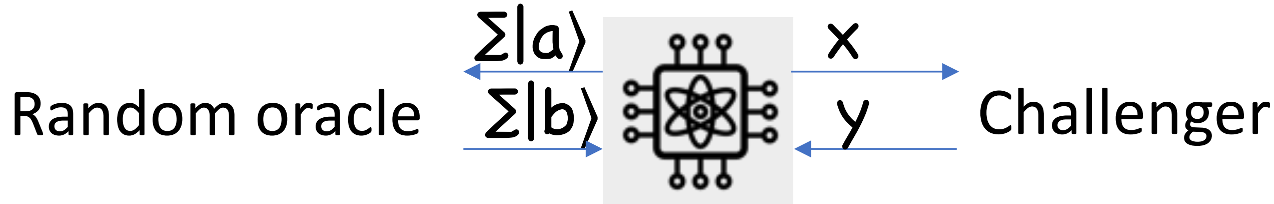
[Boneh-Dagdelen-Fischlin-Lehmann-Schaffner-Z'11]



Now standard in post-quantum crypto

Q: Do classical ROM Proofs carry over to QROM?

A: Usually not, since adversary has quantum interaction



As a consequence, essentially all ROM results need to be re-proved

Bad news: negative results [Yamakawa-Z'20]

Good news: most major results have been re-proved

The Silver Lining…

Thm [Z'19,Amos-Georgiou-Kiayias-Z'20] (inf.):

coin tossing counterexample → Novel applications (e.g. quantum money)

Intuition: winning coin tossing game implies adversary state is quantum + unclonable

Summary

PQ Crypto > Lattices