The Fundamental Formula of Post-Quantum Cryptography

Mark Zhandry (Princeton & NTT Research)

Two Revolutionary Ideas

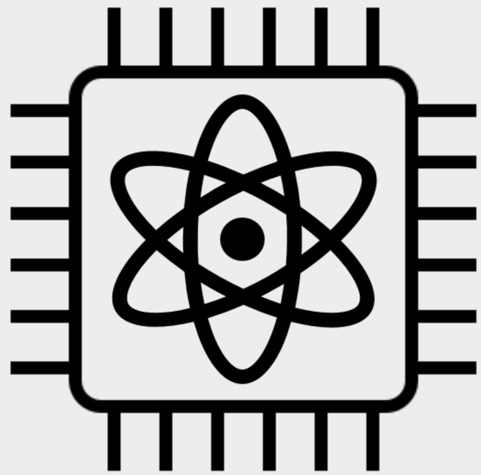
Fundamental Formula of Modern Crypto

[Goldwasser-Micali'82]

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

Quantum Computation

[Benioff’80, Manin’80, Feynman’82]



Fundamental Formula of PQ Crypto

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

Part 1: Cryptographic Assumptions

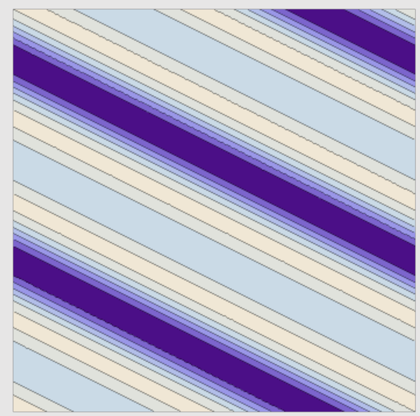
Hidden Subgroup/Period Finding

(description of) H

F

$F(x) = F(x+h) \quad \forall h \in H$ (subgroup)

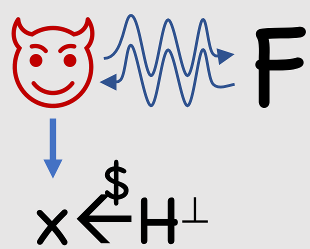
$F(x) \neq F(x+h) \quad \forall h \notin H$

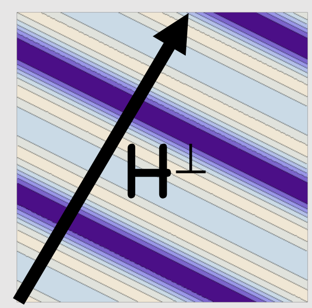


Easy Thm: Classically, HSP is unconditionally black box hard

Thm [Simon'94, Shor'94, Kitaev'97]**:**
Abelian HSP is easy, quantumly

Quantum Fourier Sampling





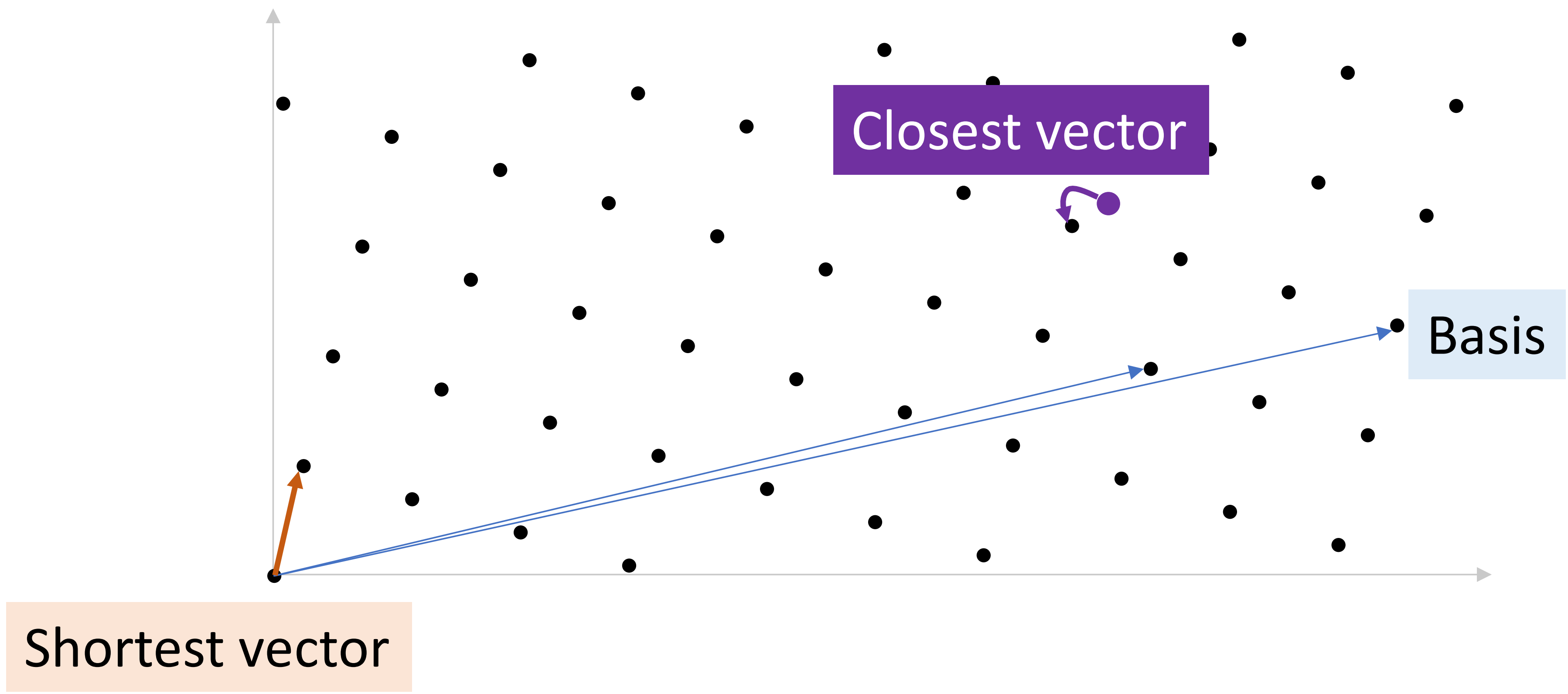
Thm [Shor'94]**:** Factoring, Discrete Log reduce to Abelian HSP

Discrete log: $(g, h=g^a)$

$F(x,y)=g^x \times h^{-y} \xrightarrow{\text{Abelian HSP}} H = \langle (a,1) \rangle$

Now what?

Lattices



Group Actions

Recall:

Discrete log: $(g, h=g^a)$

$$F(u,v)=g^u \times h^{-v} \xrightarrow{\text{Abelian HSP}} H = \langle (a,1) \rangle$$

Idea [Couveignes'97, Rostovtsev-Stolbunov'06]:

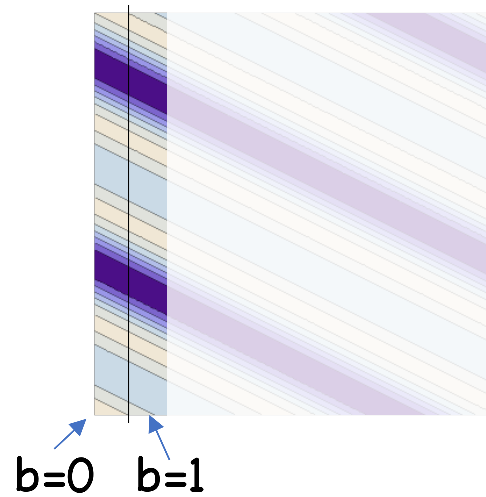
$$\cancel{\times} \longrightarrow \text{"Group Action"}$$

+ show good enough for Diffie-Hellman
+ candidate based on isogenies over elliptic curves

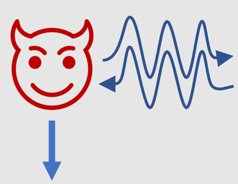
Are Group Actions Post-Quantum Hard?

$$F(u,b)= \begin{cases} g^u \text{ if } b=0 \\ h^u \text{ if } b=1 \end{cases}$$

Dihedral HSP



Quantum Fourier Sampling:



F

x+noise

Easy information-theoretically [Ettinger-Høyer-Knill'04], but seems hard computationally

Open Questions

1. What are the limits of group actions? How does their utility compare to plain groups?

2. Is there a algebraic model which

(a) Is useful for crypto,

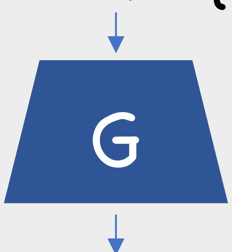
(b) Has a plausible instantiation, and

(c) Has *unconditional black box quantum* hardness?

Part 2: Definitions

Example: Classical Pseudorandomness

$x \in \{0,1\}^n$



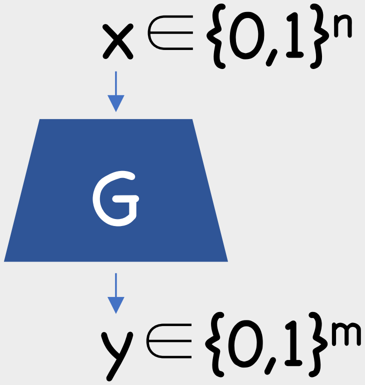
$y \in \{0,1\}^m$

$(m>n)$

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

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

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

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

Example: Computationally Binding Commitments

Def: *Com* is computationally binding if, $\forall$ PPT A, $\exists$ negligible ε such that

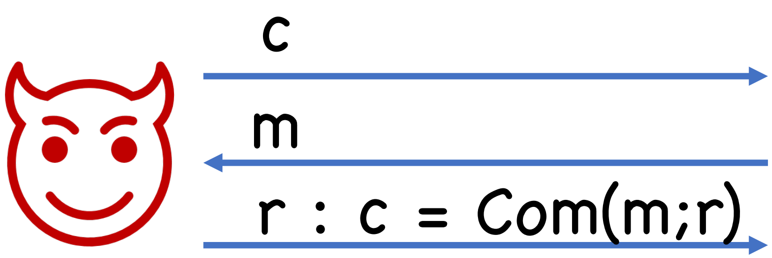
$$\Pr[\ Com(m_0;r_0)=Com(m_1;r_1) \wedge m_0 \neq m_1\ :\ (m_0,m_1,r_0,r_1) \leftarrow A()\ ] < \varepsilon$$

What about *post-quantum* binding?

Def: Com is **p[illegible]qu[illegible]m** computationally binding if, $\forall$ **Q**[illegible] negligible ε such that

$$\Pr[\ \mathsf{Com}([illegible]) = \mathsf{Com}(m_1;r_1) \wedge m_0 \neq m_1\ :\ [illegible]) \leftarrow A()\ ] < \varepsilon$$

What is a commitment, really?



Unequivocal: Adv shouldn't be able to do better than guessing challenger's m and committing to it

Thm [Ambainis-Rosmanis-Unruh'14,Unruh'16]:
Relative to an oracle, $\exists$ PQ binding *Com* s.t. quantum can win equivocation game with near-perfect probability

Takeaway

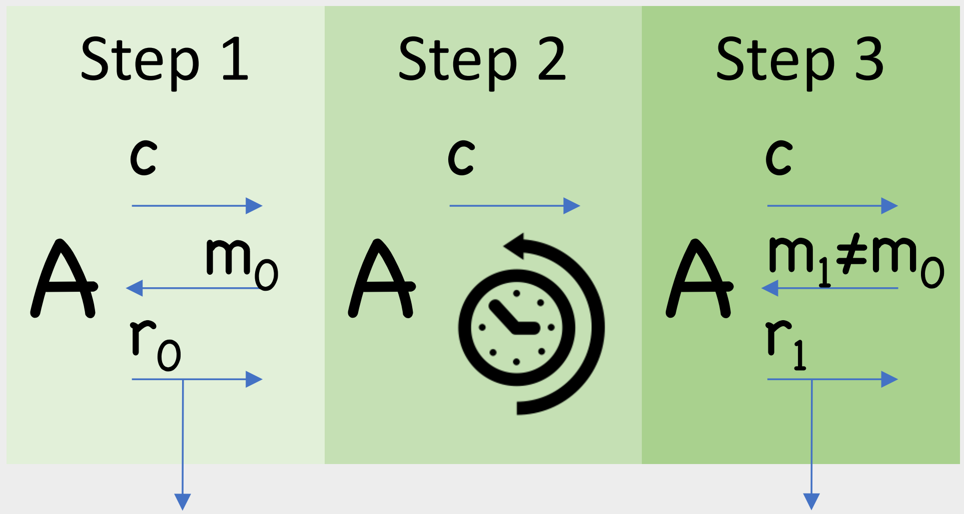
The “right” classical definition was probably not binding, since it doesn’t capture unequivocality. Certainly binding is wrong quantumly

So why is computational binding OK classically?

Part 3: Security Proofs

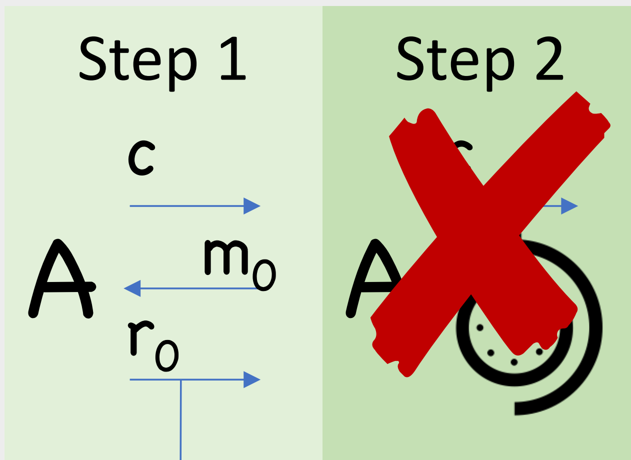
Binding ➔ Unequivocal Classically

Proof: Let $\mathcal{A}$ be supposed adversary



$$\Pr[\ \mathrm{Com}(m_0,r_0) = \mathrm{Com}(m_1,r_1) = c\ ] \geq \varepsilon^2$$

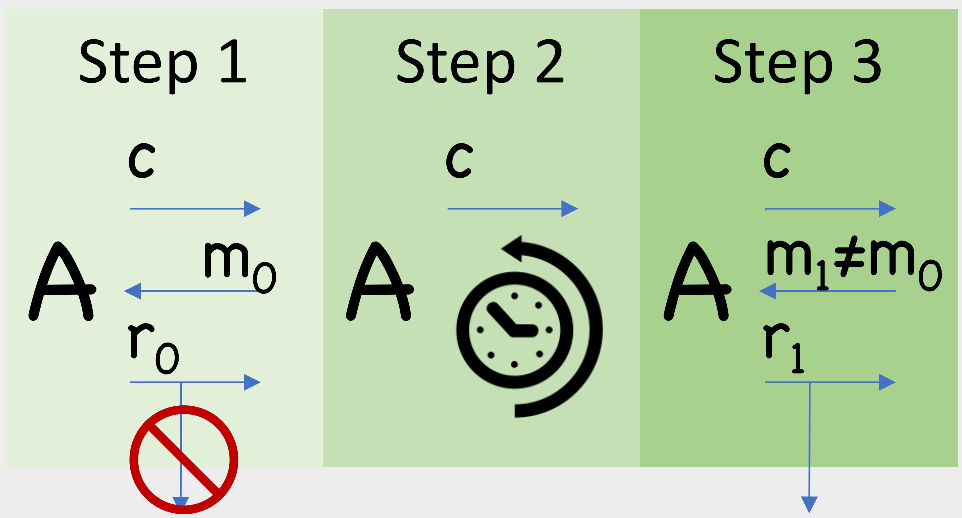
Quantum Unequivocal Proof???



Measurement principle: extracting r_0 irreversibly altered A's state

Now what?

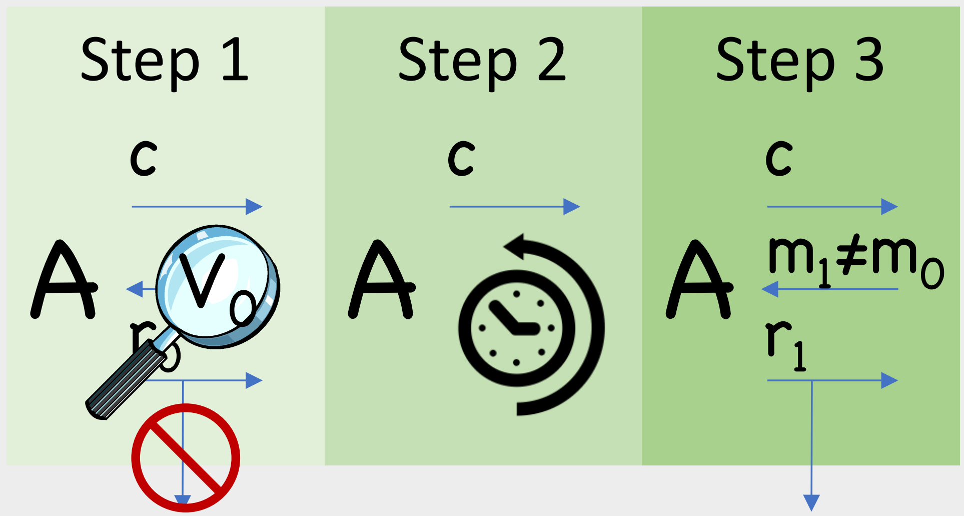
Let A be supposed (quantum) adversary



Without measurements, quantum *is reversible* $\Longrightarrow$ Steps 1+2 cancel

$V_d := Com(m_d;r_d) == c$ $\Longrightarrow$ $Pr[\ V_1\ ] = \varepsilon$

Let A be supposed (quantum) adversary



Lemma [Unruh'12]: $\Pr[\, V_0 \wedge V_1 \,] \geq \varepsilon^3$

Still not done: r_0 no longer exists!

Solution: Better security for Com

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

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

$\Longrightarrow$ m_0, r_0 uniquely determined by **c**

$\Longrightarrow$ measuring them has no effect

$\Longrightarrow$ Obtain collision $\Longrightarrow$ contradiction

Limitation: perfect binding requires large commitments

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

Def [Unruh'16] (inf.): $\mathcal{C}om$ is collapse binding if adversary cannot *detect* measuring r_0

$\Longrightarrow$ measuring r_0 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

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

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

Open Questions

3. Construct collapse-binding commitments from more general tools

4. Revisit existing classical defs, make sure they are "right" quantumly

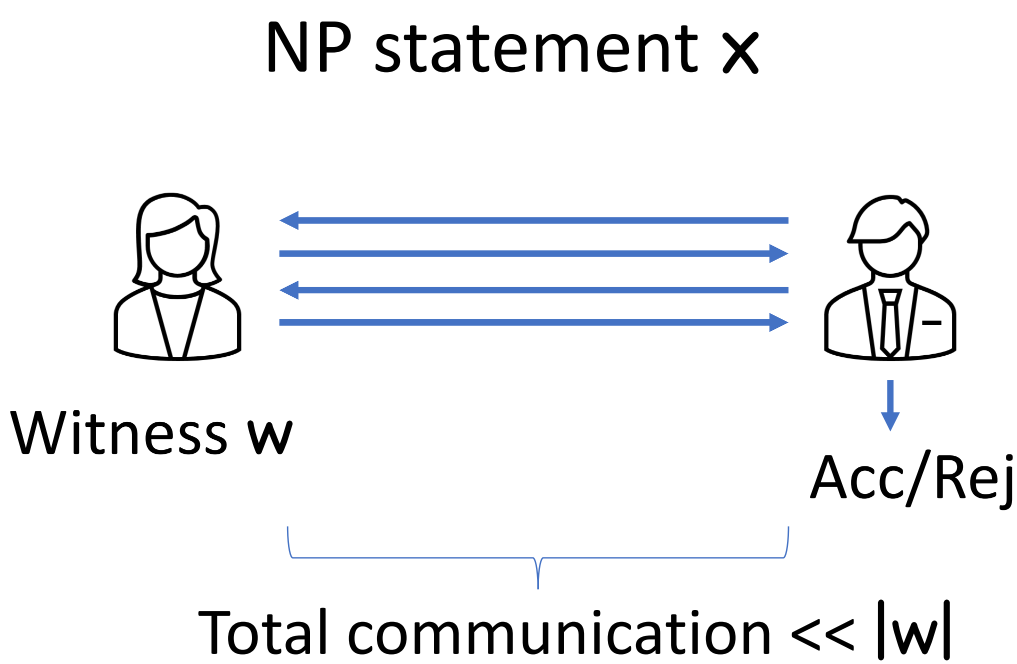
Limitations of [Unruh'12] Rewinding

Lemma [Unruh'12]: $\Pr[\ V_0 \ \wedge \ V_1\ ] \geq \varepsilon^3$

Lemma [Don-Fehr-Majenz-Schaffner'19]:
$\Pr[\ V_0 \ \wedge \ V_1 \ \wedge \ \ldots \ \wedge \ V_{k-1}\ ] \geq \varepsilon^{2k-1}$

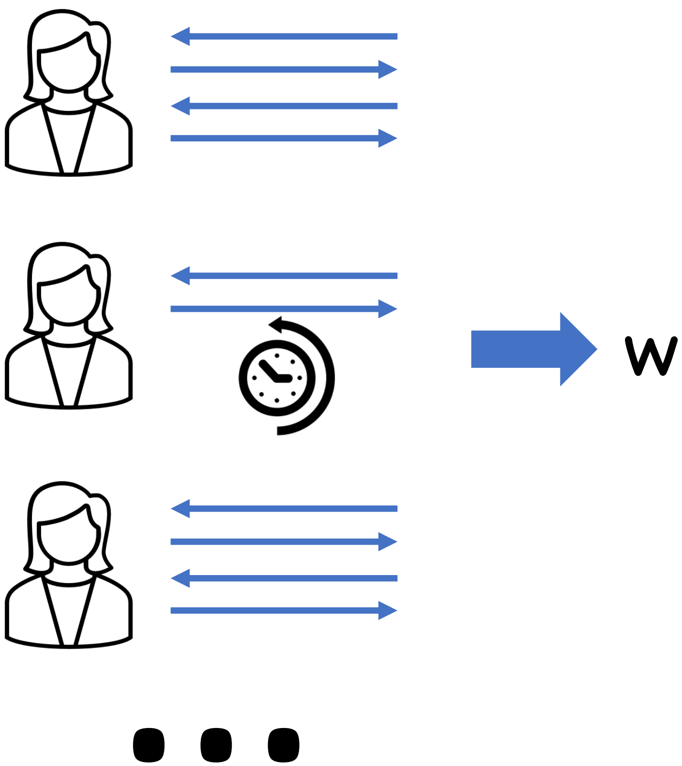
Thm [Z'20]: Only constant rewindings using Unruh's technique

Succinct Arguments



Thm [Kilian'92]: Collision resistant hashing → Classical Succinct Argument

Proving Soundness

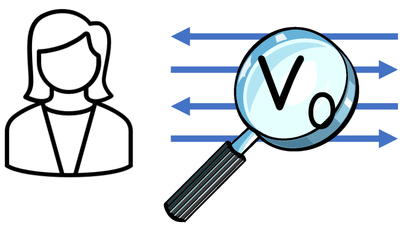


Problem:
#(rewindings) $\geq$ |w| / |comm|

Our Solution

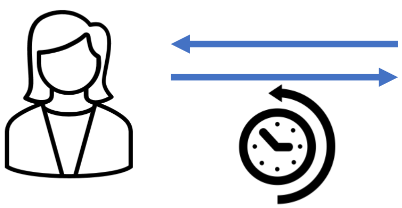
[Chiesa-Ma-Spooner-Z’21]

Success prob

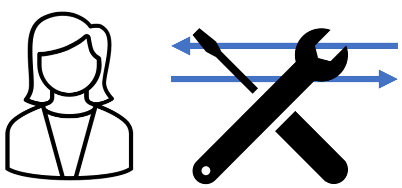


ε

Can now get arbitrarily many successes



<<ε



State repair

≈ε

Some caveats on applicability. In particular, works provided only extracting bit indicating success

Our Solution
[Chiesa-Ma-Spooner-Z’21]

Lingering issue: Need to actually extract transcript, not just success bit.

Use “collapsing” protocol

Lingering issue: Trials not independent → how to guarantee extraction?

Careful argument

Our Solution

[Chiesa-Ma-Spooner-Z’21]

Thm: “Collapsing hash function” → Post-Quantum Succinct Arguments

Open Questions

5. Explore limits of quantum rewinding. Any protocols where independence is crucial?

6. Gain better intuition for what goes on in various quantum rewinding protocols

The Silver Lining…

Thesis [Brakerski-Christiano-Mahadev-Vazirani-Vidick'18,Z'19,Amos-Georgiou-Kiayias-Z'20] (inf.):

Failed quantum proofs → Novel applications (e.g. quantum money)

Intuition: breaking reduction implies adversary state is quantum + unclonable

Thanks!