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

Part 1: Cryptographic Assumptions
Hidden Subgroup/Period Finding

\[ F(x) = F(x+h) \quad \forall h \in H \text{ (subgroup)} \]

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

**Easy Thm:** Classically, HSP is unconditionally black box hard
**Thm** [Simon’94, Shor’94, Kitaev’97]: Abelian HSP is easy, quantumly

**Quantum Fourier Sampling**

\[ x \xleftarrow{\$} H^\perp \]

\[ \mathcal{F} \]
**Thm [Shor’94]:** Factoring, Discrete Log reduce to Abelian HSP

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

\[ F(x, y) = g^x \times h^{-y} \quad \text{Abelian HSP} \quad H = < (a, 1) > \]
Now what?
Lattices

- Shortest vector
- Closest vector
- Basis
Group Actions

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

\[ F(u, v) = g^u \times h^{-v} \]

Abelian HSP

\[ H = \langle (a, 1) \rangle \]

Recall:

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

“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: \[ x + \text{noise} \]

Easy information-theoretically \cite{Ettinger-Høyer-Knill04}, 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

\[
x \in \mathbb{\{0,1\}}^n \\
G \\
y \in \mathbb{\{0,1\}}^m \\
(m > n)
\]

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

\[ | \Pr[A(y) = 1] - \Pr[A(G(x)) = 1] | < \epsilon \]
What about *post-quantum* pseudorandomness?

\[ x \in \{0,1\}^n \]

\[ y \in \{0,1\}^m \]

\[ (m>n) \]

**Def:** \( G \) is a post-quantum secure PRG if, \( \forall QPT A, \) negligible \( \varepsilon \) such that

\[ | \Pr[A(y)=1] - \Pr[A(G(x))=1] \ | < \varepsilon \]
Example: Computationally Binding Commitments

**Def:** Com is computationally binding if, ∀ PPT A, ∃ negligible ε such that
\[
\Pr[ \text{Com}(m_0;r_0) = \text{Com}(m_1;r_1) \land m_0 \neq m_1 : (m_0,m_1,r_0,r_1) \leftarrow A() ] < \varepsilon
\]
What about post-quantum binding?

**Def:** Com is post-quantum computationally binding if, \( \forall QPT_A, \exists \) negligible \( \epsilon \) such that

\[
\Pr[\text{Com}(m_0;r_0) = \text{Com}(m_1;r_1) \wedge m_0 \neq m_1 : (m_0,m_1,r_0,r_1) \xleftarrow{\text{A}} ] < \epsilon
\]
What is a commitment, really?

\[ c \leftarrow m \overset{r}{\rightarrow} c = \text{Com}(m;r) \]

**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 \(\Rightarrow\) Unequivocal Classically

Proof: Let A be supposed adversary

\[
\Pr[ \text{Com}(m_0, r_0) = \text{Com}(m_1, r_1) = c ] \geq \varepsilon^2
\]
**Quantum Unequivocal Proof??**

**Measurement principle:** extracting $r_0$ irreversibly altered $A$’s state
Now what?
Let $A$ be supposed (quantum) adversary

\[ V_d := \text{Com}(m_d; r_d) = c \quad \implies \quad \Pr[V_1] = \varepsilon \]
Let $A$ be supposed (quantum) adversary

**Step 1**

$A \xrightarrow{c} V_0 \xleftarrow{r_0} A$

**Step 2**

$A \xrightarrow{c} A \xleftarrow{\circ}$

**Step 3**

$A \xrightarrow{c} m_1 \neq m_0 \xleftarrow{r_1} A$

Lemma [Unruh’12]: $\Pr[V_0 \land V_1] \geq \varepsilon^3$

Still not done: $r_0$ no longer exists!
Solution: Better security for $\text{Com}$

**Def:** $\text{Com}$ is perfectly binding if there do not exist $m_0 \neq m_1, r_0, r_1$ such that $\text{Com}(m_0, r_0) = \text{Com}(m_1, r_1)$

$\Rightarrow m_0, r_0$ uniquely determined by $c$

$\Rightarrow$ measuring them has no effect

$\Rightarrow$ Obtain collision $\Rightarrow$ contradiction

**Limitation:** Perfect binding requires large commitments
Solution: Better security for Com

**Def [Unruh’16] (inf.):** Com is collapse binding if adversary cannot *detect* measuring $r_0$

$\implies$ measuring $r_0$ has no noticeable effect
$\implies$ Obtain collision $\implies$ contradiction

Collapse binding has become the standard post-quantum notion for commitments
Ambainis-Rosmanis-Unruh $\Rightarrow$ Not all $\text{Com}$ are collapse binding

**Thm [Unruh’16]:**
Random oracles are collapse binding

**Thms [Unruh’16b,Liu-Z’19]:**
Lossiness $\Rightarrow$ 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]: $\Pr[V_0 \land V_1] \geq \varepsilon^3$

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

Thm [Z’20]: Only constant rewinding using Unruh’s technique
Succinct Arguments

NP statement $\mathbf{\times}$

Witness $w$

Total communication $<< |w|$

**Thm** [Kilian’92]: Collision resistant hashing $\rightarrow$ Classical Succinct Argument
Proving Soundness

Problem:
\[ \#(\text{rewindings}) \geq \frac{|w|}{|\text{comm}|} \]
Our Solution

[Chiesa-Ma-Spooner-Z’21]

Success prob

\[ \varepsilon \]

Can now get arbitrarily many successes

\[ \lll \varepsilon \]

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

\[ \approx \varepsilon \]
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...

Failed quantum proofs $\rightarrow$ Novel applications (e.g. quantum money)

Intuition: breaking reduction implies adversary state is quantum + unclonable
Thanks!