Post-Quantum Cryptography

Mark Zhandry (Princeton & NTT Research)
Pre-Modern Crypto (~2000 B.C. – 1900’s A.D.)

Code makers  vs  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 - ???)

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.
This talk: brief overview quantum computing threat to cryptography
Review of Modern Crypto

\[ P = \text{NP} \implies \text{Most crypto impossible} \]

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

Crucial, but limited applications:

- SHA2,3
- AES

Partial attacks: e.g. [Grover’96, Kuperberg’03]

Most attention

- LATTICES
- ISOGENIES
- MULTIVARIATE EQNS

CRYPTOGRAPHIC

[Shor’94]

- FACTORING
- LOG

- [Shor’94]

Crucial, but limited applications
**Key Takeaway:** Essentially all “total” quantum attacks view assumption as period finding/hidden subgroup over abelian groups

**Factoring:** \( f(a) = g^a \mod N \implies g^{\text{period}/2} \text{ is root of 1} \)

**DLog:** \( f(x,y) = g^{x \times h^{-y}} \implies \text{period } (a,1) \text{ where } h=g^a \)
Rest of Talk:
Crypto Definitions
and Reductions
Example 1: PRGs
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 \( \epsilon \) such that

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

PPT = “Probabilistic Poly Time”
(aka, “efficient classical”)

\( \epsilon \) called “advantage” of \( A \)
Example: Classical Pseudorandomness

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

Solution: $G_2 = \begin{array}{c}
\text{Thm: If } G \text{ is secure, then so is } G_2
\end{array}$
Proof: Suppose $G_2$ insecure. Then $\exists$ PPT $A$, non-negl $\varepsilon$ s.t.

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

Hybrid 0

```
A \rightarrow b
p_0 := \Pr[b=1]
```

Hybrid 1

```
A \rightarrow b
p_1 := \Pr[b=1]
```

Hybrid 2

```
A \rightarrow b
p_2 := \Pr[b=1]
```
**Proof:** Suppose $G_2$ insecure. Then $\exists$ PPT $A$, non-negl $\epsilon$ s.t.

$$|p_2 - p_0| \geq \epsilon$$

Hybrid 0

$A \rightarrow b$

$p_0 := \Pr[b=1]$

Hybrid 1

$A \rightarrow b$

$p_1 := \Pr[b=1]$

Hybrid 2

$A \rightarrow b$

$p_2 := \Pr[b=1]$

Either:

$$|p_1 - p_0| \geq \epsilon/2$$

Or:

$$|p_2 - p_1| \geq \epsilon/2$$

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

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

In either case, $B$ has advantage $\epsilon/2$ against security of $G$
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,
\[ \forall\text{ QPT } A, \exists\text{ negligible } \varepsilon \text{ such that} \]
\[ | \Pr[A(y)=1] - \Pr[A(G(x))=1] | < \varepsilon \]

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 $\exists$ QPT $A$, non-negl $\varepsilon$ s.t.

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

Hybrid 0

<table>
<thead>
<tr>
<th>$G$</th>
<th>$G$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$A \rightarrow b$</td>
<td>$A \rightarrow b$</td>
</tr>
</tbody>
</table>

$p_0 := \Pr[b=1]$

Hybrid 1

<table>
<thead>
<tr>
<th>$G$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$A \rightarrow b$</td>
</tr>
</tbody>
</table>

$p_1 := \Pr[b=1]$

Hybrid 2

| $A \rightarrow b$ |

$p_2 := \Pr[b=1]$

Either:

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

Or:

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

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

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

In either case, $B$ has advantage $\varepsilon/2$ 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 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

Challenger

\[ k \leftarrow \{0,1\}^\lambda \]
\[ b \leftarrow \{0,1\} \]
\[ c \leftarrow \text{Enc}(k,m_b) \]

“Win” if \( b = b' \)

A

Message dist.

Side info.

Adv. goal

Def: \text{Enc} is 1-time secure if, \( \forall \) PPT A,
\[ \exists \text{negligible } \varepsilon \text{ such that } | Pr[\text{Win}] - \frac{1}{2} | < \varepsilon \]
Example: PQ Encryption???

**Challenger**

- \( k \leftarrow \{0,1\}^\lambda \)
- \( b \leftarrow \{0,1\} \)
- \( c \leftarrow \text{Enc}(k,m_b) \)

“Win” if \( b = b' \)

**Def:** \( \text{Enc} \) is 1-time \( \text{PQ} \) secure if, \( \forall \) QPT \( A \), \( \exists \) negligible \( \varepsilon \) such that \( | \Pr[\text{Win}] - \frac{1}{2} | < \varepsilon \)

**A**

- Message dist.
- Side info.
- Adv. goal
Example: PQ Encryption???

Challenger:

\[ k \leftarrow \{0,1\}^\lambda \]
\[ b \leftarrow \{0,1\} \]

“A”

Message dist.

Side info.

Adv. goal

“Win” if \( b = b' \)

**Def (inf.):** \( \text{Enc} \) is 1-time **Fully Q sec.** if, \( \forall \ QPT A, \ \exists \ \text{negl} \ \varepsilon \ \text{such that} \ | \Pr[\text{Win}] - \frac{1}{2} | < \varepsilon \)
**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 A has physical access → May need Full Quantum security
Example: PRGs $\rightarrow$ Encryption

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

**Thm:** If $G$ is secure, then so is $\text{Enc}$

**Proof:** Suppose $\text{Enc}$ insecure. Then $\exists$ PPT $A$, non-negl $\epsilon$ ...

<table>
<thead>
<tr>
<th>Hybrid 0</th>
<th>$c = \text{Enc}(k,m_b)$</th>
<th>$\Pr[b' = b] = \frac{1}{2} + \epsilon$</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>$= G(k) \oplus m_b$</td>
<td></td>
</tr>
<tr>
<td>Hybrid 1</td>
<td>$c = $ \oplus m_b$</td>
<td>$\Pr[b' = b] = \frac{1}{2}$</td>
</tr>
<tr>
<td></td>
<td>$= \text{random}$</td>
<td></td>
</tr>
</tbody>
</table>

Adversary $B$ with advantage $\epsilon$
Example: PQ PRGs $\rightarrow$ PQ Encryption

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

**Thm:** If $G$ is PQ secure, then so is $\text{Enc}

**Proof:** Suppose $\text{Enc}$ PQ insecure. Then $\exists$ QPT $A$, non-negl $\epsilon$ ...

<table>
<thead>
<tr>
<th>Hybrid 0</th>
<th>$c = \text{Enc}(k,m_b)$</th>
<th>$\Pr[b' = b] = \frac{1}{2} + \epsilon$</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>$= G(k) \oplus m_b$</td>
<td></td>
</tr>
<tr>
<td>Hybrid 1</td>
<td>$c = $ \oplus m_b$</td>
<td>$\Pr[b' = b] = \frac{1}{2}$</td>
</tr>
<tr>
<td></td>
<td>$= \text{random}$</td>
<td>PQ Adversary $B$ with advantage $\epsilon$</td>
</tr>
</tbody>
</table>
Proof doesn’t care how $A$ works internally, as long as it has non-negligible advantage.

$\Rightarrow$ Also post-quantum reduction
Example: **PQ PRGs vs Fully Quantum Encryption?**

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

**Thm:** \( \text{Enc} \) is not fully quantum secure

**Proof:**

\[ \sum_m |m, 0\rangle \]

\[ b=0 \quad \sum_m |G(k) \oplus m\rangle = \sum_m |m\rangle \]

\[ b=1 \quad |G(k)\rangle \]

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):

\[ \text{Enc}(k,m) = f_k(m) \]

\[ f_k = \text{sufficiently expanding pairwise-independent function} \]
Example 3: Commitments and Coin Tossing
Example: Commitments

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

$$\Pr[ m_0 \neq m_1 \land \text{Com}(m_0, r_0) = \text{Com}(m_1, r_1) : (m_0, r_0, m_1, r_1) \leftarrow A()] < \varepsilon$$

Also want hiding, but we will ignore
Example: **PQ Commitments**

Def: $\text{Com}$ is **post-quantum** binding if, $\forall \text{QPT } A$, $\exists$ negligible $\epsilon$ such that

$$\Pr[ m_0\neq m_1 \land \text{Com}(m_0,r_0) = \text{Com}(m_1,r_1) : (m_0,r_0,m_1,r_1) \leftarrow A()] < \epsilon$$
Example: Commitments $\rightarrow$ Coin Tossing

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

$c = \text{com}(b_A, r)$

$b_A, r \rightarrow b_B$

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

Verify $c = \text{com}(b_A, r)$

$b = b_A \oplus b_B$

$b = \perp$

pass

fail
Classical proof that Alice can’t bias $b$:
Let $A$ be supposed adversary

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 $\text{Com}(b_A,r)=c$
Classical proof that Alice can’t bias $b$:
Let $A$ be supposed adversary

$$\Pr\left[ b_{A,0} = 0 \land b_{A,1} = 1 \land \text{Com}(b_{A,0}, r_0) = \text{Com}(b_{A,1}, r_1) = c \right] \geq \text{poly}(\varepsilon)$$
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):
\[ \exists \text{PQ binding Com s.t. Alice has a near-perfect strategy} \]

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 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 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

Unitaries are reversible $\implies$ Steps 1+2 cancel

$V_d := b_{A,d} = d \land \text{Com}(b_{A,d},r_d) = c \implies \Pr[V_1] = \epsilon$
Let $A$ be supposed (quantum) adversary

Lemma [Unruh’12]: $\Pr[V_0 \land V_1] = \text{poly}(\varepsilon)$

Still not done: $b_{A,0}, r_0$ no longer exist!
Solution: Better security for Com

**Def**: Com is perfectly binding if \( \forall m_0 \neq m_1, r_0, r_1 \) s.t.
\[
\text{Com}(m_0, r_0) = \text{Com}(m_1, r_1)
\]

\[\Rightarrow b_{A,0,r_0} \text{ uniquely determined by } c\]
\[\Rightarrow \text{measuring them has no effect}\]
\[\Rightarrow \text{Obtain collision} \Rightarrow \text{contradiction}\]

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

Def [Unruh’16] (inf.): Com is collapse binding if adversary cannot detect measuring $b_{A,0}, r_0$

$\Rightarrow b_{A,0}, r_0$ measuring them has no noticeable effect

$\Rightarrow$ Obtain collision $\Rightarrow$ contradiction

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

Q: Do collapse binding Com exist? How to construct?

\textbf{Thm [Unruh’16]:} Random oracles are collapse binding

\textbf{Thms [Unruh’16b,Liu-Zhandry’19]:} LWE \implies 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]

Real World

A

ROM

A

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

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

coin tossing counterexample  \rightarrow  Novel applications (e.g. quantum money)
Summary

PQ Crypto > Lattices