New Quantum Security Models

Mark Zhandry (Princeton & NTT Research)
Motivation

\[ \sum \alpha_{x,y} |x,y\rangle \]

\[ \sum \alpha_{x,y} |x,y \oplus F(x)\rangle \]

Higher level quantum protocol

Quantum random oracle model

(starting tomorrow)
Security Proof Challenges

What does hybrid over queries look like?

A \rightarrow \sum_{x,y} \alpha_{x,y} |x,y\rangle

B

\sum_{x,y} \alpha_{x,y} |x,y \oplus O(x)\rangle

Hard Problem
Security Proof Challenges

Take 1: Per QUERY

\[ \sum_{x,y} \alpha_{x,y} |x,y\rangle \]
\[ \sum_{x,y} \alpha_{x,y} |x,y \oplus V_1\rangle \]
\[ \sum_{x,y} \alpha_{x,y} |x,y\rangle \]
\[ \sum_{x,y} \alpha_{x,y} |x,y \oplus V_2\rangle \]

Problem: repeated queries?

Problem: distinguishing attack

\[ \sum |x,0\rangle \]
\[ \sum |x,V_1\rangle \]
\[ \sum |x,0\rangle \]
\[ \sum |x,O(x)\rangle \]

VS
Security Proof Challenges

Typical reductions are commit to entire function $O$ at beginning, remain consistent throughout

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

Non-committing reductions: topic for later class
Security Proof Challenges

Take 2: Per VALUE

\[ \sum_{x,y} \alpha_{x,y} |x,y\rangle \]
\[ \sum_{x,y} |x,y \oplus V_x\rangle \]

Problem: exp-many values
- Exponential loss in hybrid
- How to simulate efficiently?
PRF Recap

**Def:** $F$ is a **Fully Quantum** secure PRF if, 
\forall QPT $A$, \exists negligible $\epsilon$ such that 
$\left| \Pr[A \left| F(k, \cdot) \right. (\cdot) = 1] - \Pr[A \left| R(\cdot) \right. (\cdot) = 1] \right| < \epsilon$

$A^{O(\cdot)}$ means quantum queries:

$\Sigma \alpha_{x,y} |x, y\rangle \rightarrow \Sigma \alpha_{x,y} |x, y \oplus O(x)\rangle$
PRF Recap

PRG $\Rightarrow$ PRF

$F(k,000)$ $F(k,001)$ $F(k,010)$ $F(k,011)$ $F(k,100)$ $F(k,101)$ $F(k,110)$ $F(k,111)$
PRF Recap

Proof, step 1: Hybrid

Hybrid 0 (F(k, ·)):
PRF Recap

Proof, step 1: Hybrid

Hybrid 1:
PRF Recap

Proof, step 1: Hybrid

Hybrid 2:
PRF Recap

Proof, step 1: Hybrid

Hybrid n ( R( · ) ):
PRF Recap

Proof, step 1: Hybrid

\[ \exists i \text{ s.t. } | \Pr[A_{\text{Hybrid}}^{i+1}() = 1] - \Pr[A_{\text{Hybrid}}^i() = 1] | \geq \frac{\varepsilon}{n} \]

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

**Def:** $G$ is **Quantum Oracle Secure** if, \( \forall \) QPT \( A \), \( \exists \) negligible \( \varepsilon \) such that
\[
| \text{Pr}[A | R \rangle = 1] - \text{Pr}[A | G \circ O \rangle = 1] | < \varepsilon
\]

\( R,O \) random oracles

Quantum PRF adv \( A \) \hspace{5cm} \text{Classical reduction} \hspace{5cm} \text{Oracle Security adv} \( B \)
Another View

How to complete reduction from plain (post-quantum) PRGs?

Classical Proof:

Only $q$ queries → Can simulate with $q$ samples

Hybrid over $q$ values
Another View

How to complete reduction from plain (post-quantum) PRGs?

Quantum?

Need exponentially-many samples for perfect simulation
Reducing # of Hybrids

Goal: Simulate query responses using only poly-many samples
Simulating with Few Samples

<table>
<thead>
<tr>
<th>Extreme 1: Same sample in all positions</th>
</tr>
</thead>
<tbody>
<tr>
<td>V V V V V V V V V V V V V V V V V</td>
</tr>
<tr>
<td>Distinguishable!</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Middle ground: Several samples in random positions</th>
</tr>
</thead>
<tbody>
<tr>
<td>V₁ V₅ V₃ V₅ V₂ V₁ V₄ V₃ V₂ V₁ V₄ V₅ V₂ V₃</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Extreme 2: Independent sample in each position</th>
</tr>
</thead>
<tbody>
<tr>
<td>V₁ V₂ V₃ V₄ V₅ V₆ V₇ V₈ V₉ V₁₀ V₁₁ V₁₂ V₁₃ V₁₄</td>
</tr>
<tr>
<td>Exponential loss!</td>
</tr>
</tbody>
</table>
Small Range Distributions

How big of $r$ to be indistinguishable from truly random?
Small Range Distributions

**Thm [Z’12b]:** No $q$ quantum query alg can distinguish $SR_r$ from random, except with probability $O(q^3/r)$. Holds for any output distribution.

Quantum collision finding $\rightarrow$ bound tight

- $r=q^3$?
- $r=q^4$?
- $r=q^{20}$?
- $r=1.01q$?
Quantum Proof

\[ \text{Uniform} \quad O(q^3/r) \quad \geq \varepsilon \quad \text{Uniform} \]

\[ \text{G(uniform)} \quad O(q^3/r) \quad \text{G(uniform)} \]
Quantum Proof

\[ | \Pr[A^{\langle R \rangle} = 1] - \Pr[A^{\langle G \circ O \rangle} = 1] | \geq \varepsilon \]

\[ | \Pr[B(y_1, \ldots, y_r) = 1] - \Pr[B(G(x_1), \ldots, G(x_r)) = 1] | \geq \varepsilon - O(q^3/r) \]

\[ | \Pr[C(y) = 1] - \Pr[C(G(x)) = 1] | \geq \varepsilon/r - O(q^3/r^2) \]

Optimize by setting \( r = O(q^3/\varepsilon) \)  Final advantage \( O(\varepsilon^2/q^3) \)
Notes

Requires knowing $\varepsilon$

Can fix by guessing $\varepsilon=2^{-i}$ for random $i$

$\varepsilon^2$ means much bigger security loss
Proving SR Theorem

Thm [Z’12a]: If A makes q quantum queries to \( O \leftarrow D \), then
\[
\Pr[A^D()=1] = \sum_{x_1, \ldots, x_{2q}} \Pr[D(x_i)=y_i \ \forall \ i \in [2q]]
\]

(Restatement of polynomial method [Beals-Buhrman-Cleve-Mosca-de Wolf’01])

Thm [Z’12b]: For SR_r, the \( \Pr[D(x_i)=y_i \ \forall \ i \in [k]] \) are degree k polynomials in \( 1/r \)

\[
\Pr[A^{SR_r}()=1] = \text{degree } 2q \text{ polynomial in } 1/r
\]
Proving SR Theorem

Pr[A^{SR_r}()=1] = P(1/r) = degree 2q polynomial

Additional observations:
• SR_\infty = Truly random function
• 0 \leq P(1/r) \leq 1 \hspace{1em} \forall \text{ positive integers } r

Goal: bound \mid P(1/r) - P(0) \mid
Proving SR Theorem

degree 1
Proving SR Theorem

degree 2
Proving SR Theorem

degree 3
Proving SR Theorem

degree 4
Proving SR Theorem

Can’t move too fast!
Proving SR Theorem

Thm [Z’12b]: If $P(1/r)$ satisfies:
• Degree $\leq k$
• $0 \leq p(1/r) \leq 1$ $\forall$ positive integers $r$
Then $|P(1/r) - P(0)| \leq 27k^3/r$

(Asymptotically tight)
Remaining Step

$$\text{SR}_r$$ requires random functions; how to simulate?

Only 2q-wise marginals matter

$$\Rightarrow$$ 2q-wise independent functions “look” random
What else is out there?

Encryption

Authentication

PRPs

IBE

Secret sharing

MPC

Remainder of lecture: definitional issues
Defining MACs/Signatures

Classical Security:

\[ m_1 \]
\[ \sigma_1 = \text{MAC}(k,m_1) \]
\[ m_2 \]
\[ \sigma_2 = \text{MAC}(k,m_2) \]
\[ \cdots \]
\[ m^*,\sigma^* \]

A

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

“Win” if
- \( m^* \notin \{m_i\}_i \)
- \( \text{Ver}(k,m^*,\sigma^*) = 1 \)
Defining MACs/Signatures

Fully Quantum Security?

\[ \sum \alpha_{m,\sigma} |m,\sigma\rangle \]
\[ \sum \alpha_{m,\sigma} |m,\sigma^{\oplus}\text{MAC}(k,m)\rangle \]
\[ \sum \alpha_{m,\sigma} |m,\sigma\rangle \]
\[ \sum \alpha_{m,\sigma} |m,\sigma^{\oplus}\text{MAC}(k,m)\rangle \]

\[ \sum \alpha_{m,\sigma} |m,\sigma^{\oplus}\text{MAC}(k,m)\rangle \]
\[ \sum \alpha_{m,\sigma} |m,\sigma\rangle \]

A

\[ m^*,\sigma^* \]

k \leftarrow \{0,1\}^\lambda

“Win” if

- \[ m^* \notin \{m_i\}_i \]
- \[ \text{Ver}(k,m^*,\sigma^*) = 1 \]
Defining MACs/Signatures

What does it mean to be “new”? 

Example:

Random \( m, \text{MAC}(k,m) \)

A

\[ \sum \alpha_m |m,0\rangle \]

\[ \sum \alpha_m |m,\text{MAC}(k,m)\rangle \]

Challenger
Defining MACs/Signatures

Partial Answer: One More Security [Boneh-Z’13a]

\[
\begin{align*}
\text{q} & \quad \text{A} \\
\sigma_1 &= \text{MAC}(k,m_1) \\
\sigma_2 &= \text{MAC}(k,m_2) \\
\vdots & \\
\sigma_q &= \text{MAC}(k,m_q) \\
\end{align*}
\]

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

“Win” if

- \{m_i^*\} distinct
- \text{Ver}(k,m_i^*,\sigma_i^*) = 1 \quad \forall i
Defining MACs/Signatures

Limitation: Suppose:

\[ A \sum_{\alpha_m} |0||m, 0\rangle \]
\[ \sum_{\alpha_m} |0||m, \sigma_{0||m}\rangle \]

Challenger

1||m, MAC(k, 1||m )

Doesn’t violate one-more security!
Defining MACs/Signatures

Other defs exist which fix this problem [Garg-Yuen-Z’17, Alagic-Majenz-Russell-Song’18], but IMO even satisfactory definition not yet solved
Defining Encryption

Classical CPA Security:

\[
\begin{align*}
&k \leftarrow \{0,1\}^\lambda \\
&b \leftarrow \{0,1\}
\end{align*}
\]

\[
\begin{align*}
&m \\xrightarrow{} \text{Enc}(k,m) \\
&m_0^\ast, m_1^\ast \\xrightarrow{} \text{Enc}(k,m_b^\ast) \\
&m \\xrightarrow{} \text{Enc}(k,m)
\end{align*}
\]
Defining Encryption

Quantum CPA Attacks?

Everything is fine so far
Defining Encryption

Quantum Challenge Queries?

A

\[ \sum \alpha_{m,c} |m,c\rangle \]
\[ \sum \alpha_{m,c} |m,c^{\oplus}c_m\rangle \]
\[ \sum \alpha_{m_0^{*},m_1^{*},c} |m_{0}^{*},m_{1}^{*},c\rangle \]
\[ \sum \alpha_{m_0^{*},m_1^{*},c} |m_{0}^{*},m_{1}^{*},c^{\oplus}c_{mb}^{*}\rangle \]

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

Attack:

\[ \sum_{m_0^*, m_1^*} |m_0^*, m_1^*, 0\rangle \]
\[ \sum_{m_0^*, m_1^*, c_{mb^*}} |m_0^*, m_1^*, c_{mb^*}\rangle \]

\[ \text{QFT/} \quad H^\otimes n \quad \text{QFT/} \quad H^\otimes n \]

\[ z_0 \quad z_1 \quad c \]

\[ z_{1-b} = 0^n \text{ and whp } z_b \neq 0^n \]
Defining Encryption

Classical encryption schemes are not secure for encrypting quantum messages, if the attacker gets to see the original message registers.

[Boneh-Z’13b]: don’t allow quantum challenge queries

[Gagliardoni-Hülsing-Schaffner’16]: make sure quantum challenge query never returned

More subtle than it sounds
Defining Encryption

Quantum CCA Attacks?

\[ \sum_{\alpha_{c,m}} |c,m\rangle \]
\[ \sum_{\alpha_{m,c}} |c,m \oplus \text{Dec}(k,m)\rangle \]

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

\[ m_0^*, m_1^* \]
\[ c^* = \text{Enc}(k,m_b^*) \]

\[ \sum_{\alpha_{c,m}} |c,m\rangle \]
\[ \sum_{\alpha_{m,c}} |c,m \oplus \text{Dec}(k,m)\rangle \]

Must not decrypt \( c^* \)
Defining Encryption

“Not decrypting $c^*$” problematic for quantum challenges

[Chevalier-Ebrahimi-Vu’20]: Formalize quantum CCA+Challenge
Defining Traitor Tracing

encrypted broadcast

Authorized users

Goal: identify source of pirate decoder
Defining Traitor Tracing

Classical Def (modulo details):

A

\[ D \]

Pr\[D(Enc(k,m)) = m]\}
negl

Win if

\[ S \]

\[ \text{Trace}^D(pk) \]

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

• \( S \) empty, or
• \( S \cap \{id_i\} \) not empty
Defining Traitor Tracing

Problem: most prior work assumes $D$ is stateless/can be rewound

Somewhat inherent: single query to $D$ usually not enough to accuse

But if decoder has quantum state, single query may alter decoder

[Z’20]: Formalize quantum analog of “stateless”
Tomorrow: Unavoidable Quantum Attacks

So far, issues concern new quantum attack models

My remaining lectures: attacks/issues even under existing attack model

- Rewinding
- Quantum Random Oracle Model