Cryptography in the Age of Quantum Computers

Mark Zhandry – MIT

Based on joint works with: Dan Boneh, Özgür Dagdelen, Marc Fischlin, Anja Lehmann, Christian Schaffner

Typical Crypto Application



Solution: (Private Key) Encryption



Major question: How is security defined?

Definition 1: 1-time security

For any **m₀,m₁**:

 $c_0 = Enc(> m_0) \approx c_1 = Enc(> m_1)$

Statistical security: statistical closeness

Computational security: computational indistinguishability

- Restrict adversaries running efficiently
- Now possible to have

Question: what if I encrypt a second message?

Definition 2: CPA Security

Indistinguishability under *chosen plaintext attack*



Definition 3: CCA Security

Indistinguishability under *chosen ciphertext attack*

Challenger Adversary Random bit **b**, Random key 📀 💭 Empty table **T** m_0, m_1 $c = Enc(m_h, m_h)$ С Add c to T С m = Dec(, c)m if c∉T b **Def:** CCA-Security $\Rightarrow \forall$ efficient **[57]**, **[Pr[b'=b]** - $\frac{1}{2}$ **]** < negl

Other Scenarios

Circular security:



Side-channel attacks:



Takeaway:

Models should give adversary as much power as possible

Quantum Computers

So far, assumed adversary obeys classical physics

What about quantum physics?

Quantum computing = using quantum physics to perform certain computations

- Active research area
- [Sho'94]: quantum computers can break lots of crypto

Post-Quantum CCA Security



Def: CCA-Security ⇒ ∀ efficient

Post-Quantum Security

Post-quantum = end-users are classical



Full Quantum Security

Full quantum = end-users are *quantum*



Quantum Background

Quantum states:

= superposition of **all** messages
= Σ
$$\alpha_{m}$$
 |m $(\Sigma | \alpha_{m} |^{2} = 1)$

Measurement:

$$m$$
 with probability $|\alpha_m|^2$

Simulate classical ops in superposition:

$$\xrightarrow{\mathbf{F}} \mathbf{F} \xrightarrow{\mathbf{F}} \mathbf{F} \xrightarrow{\mathbf{F}} \mathbf{\alpha}_{\mathsf{m}} | \mathbf{F}(\mathsf{m}) \rangle$$

Full Quantum CCA Security?



Def: CCA-Security ⇒ ∀ efficient

Are Full Quantum Attacks Plausible?

Objection: can always "classicalize" by sampling



 \Rightarrow Reduce attack to post-quantum attack!

Reasons to still use full quantum notions:

- Classicalization is burden on hardware designer
- What if adversary can bypass?
- Classicalization amounts to a hardware assumption

This Work

[BDFLSZ'11, Zha'12a, Zha'13]: Quantum random oracle model

[Zha'12b]: Pseudorandom functions

[BZ'13a]: Message Authentication Codes

[BZ'13b]: Digital signatures and encryption

Theorem: Full-quantum security > Post-quantum security

Theorem (Informal): Full-quantum security can be obtained with "minimal" overhead w.r.t. post-quantum security

Example: Pseudorandom Functions

Efficient keyed functions that "look like" random functions

Fundamental building block in symmetric crypto



Example: Pseudorandom Functions

Efficient keyed functions that "look like" random functions

Fundamental building block in symmetric crypto



Example: Pseudorandom Functions

Efficient keyed functions that "look like" random functions

Fundamental building block in symmetric crypto



How to build QPRFs?

Hope that existing PQ-secure PRFs are FQ secure

Examples: GGM, NR, BPR

Questions:

- Do classical security analyses carry over?
- If not, what new tools are needed?

Pseudorandom Generators



quantum adversaries

The GGM Construction



The GGM Construction





The GGM Construction







Quantum Security Proof?

Idea: follow classical steps

Turn PRF distinguisher into PRG distinguisher

Step 1: Hybridize over levels of tree







Hybrid 3:



Hybrid **n**:



Distinguish **PRF** from **Func(X,Y)** with adv. ε \downarrow Distinguish two adjacent hybrids with adv. ε/n **n** polynomial \Rightarrow acceptable loss



Distinguish **PRF** from **Func(X,Y)** with adv. ε \downarrow Distinguish two adjacent hybrids with adv. ε/n **n** polynomial \Rightarrow acceptable loss



Argument carries over to quantum setting unmodified

Quantum Security Proof?

Idea: follow classical steps

Turn PRF distinguisher into PRG distinguisher

Step 1: Hybridize over levels of tree

 \checkmark

Step 2: Simulate hybrids using PRG/Random samples

Simulating Hybrids



How It Was Done Classically

Active node: value used to answer query



Adversary only queries polynomial number of points

Quantum Simulation?



Adversary can query on all exponentially-many inputs

Quantum Simulation?



Adversary can query on all exponentially-many inputs

Need exponentially many samples to simulate!

Quantum Security Proof?

Idea: follow classical steps

Turn PRF distinguisher into PRG distinguisher

Step 1: Hybridize over levels of tree

Step 2: Simulate hybrids using PRG/Random samples ?

Step 3: Hybrid over samples

Hybrid Over Samples



Argument carries over to quantum setting unmodified

Quantum Security Proof?

Idea: follow classical steps

Turn PRF distinguisher into PRG distinguisher

Step 1: Hybridize over levels of tree

Step 2: Simulate hybrids using PRG/Random samples ?

Step 3: Hybrid over samples

- Exponential samples \Rightarrow exponential security loss
- Can only handle poly-many samples

Quantum Security Proof?

Idea: follow classical steps

Turn PRF distinguisher into PRG distinguisher

Step 1: Hybridize over levels of tree

Step 2: Simulate hybrids using PRG/Random samples X

Step 3: Hybrid over samples

- Exponential samples \Rightarrow exponential security loss
- Can only handle poly-many samples

A Distribution to Simulate

Distribution \mathbf{D} on $\mathbf{Y} \Rightarrow$ induces distribution on functions



Goal: simulate using poly-many samples

Solution: Small-Range Distributions



 $H \leftarrow SR_r^{X}(D)$

Small-Range Distributions

Theorem: $SR_r^{X}(D)$ is indistinguishable from D^{X} by any qquery quantum algorithm, except with advantage $O(q^3/r)$

Notes:

- Highly non-trivial
- Distinguishing prob not negligible, but good enough
 - We get to choose **r**
- Random function **R** not efficiently constructible

Theorem: Can simulate **R** using **k**-wise independence

Quantum GGM Proof



Quantum Security Proof

Idea: follow classical steps

Turn PRF distinguisher into PRG distinguisher

Step 1: Hybridize over levels of tree

Step 2: Approx. sim. hybrids using poly-many samples 🗸

Step 3: Hybrid over samples

Result: PRG distinguisher Impossible by assumption \Rightarrow PRF distinguisher impossible

Quantum Query Results

Quantum Collision Finding

Recall small-range distributions when \mathbf{D} is uniform:



 $H \leftarrow SR_r^{X}(Y)$

Quantum Collision Finding



Theorem: H is indistinguishable from random by any qquery quantum algorithm, except with advantage $O(q^3/r)$

Corollary: If $|Y| >> |X|^2$, impossible to find collision in H unless $q \ge \Omega(r^{1/3})$

Quantum Collision Finding

Corollary: If |Y|>>|X|², impossible to find collision in H unless q≥O(r^{1/3})

What about truly random functions with |Y| << |X|² ?

Theorem: $q \ge \Omega(r^{1/3})$ quantum queries are required to find collisions in a random function $R:X \rightarrow [r]$

Previous $r^{1/3}$ lower bounds known for different settings

- E.g. k-to-1 functions [AS'01]
- All prior settings required |Range| > |Domain|
- Our works for all domain/range sizes

```
Bound is tight: [BHT'97] q=O(r<sup>1/3</sup>)
```

Quantum Oracle Interrogation

Using q queries, determine function at k>q points



($x_1,\ F(x_1)$), ($x_2,\ F(x_2)$), ... ($x_k,\ F(x_k)$)

Important for MAC, signature security

Quantum Oracle Interrogation

Classically: hard $Adv = 1/|Y|^{k-q}$

- Large outputs: Adv = negl even for k=q+1
- Small outputs: Adv = negl for k = c q

Quantum: not so fast

Theorem [vD'98]: For $F:X \rightarrow \{0,1\}$, q quantum queries $\Rightarrow k = 1.9q$ points w.h.p

Also true for small ranges:

Theorem: For $F:X \rightarrow \{0,1\}^2$, **q** quantum queries $\Rightarrow k = 1.3q$ points w.h.p

Question: What about large range sizes?

Quantum Oracle Interrogation



New quantum impossibility tool: The Rank Method

Therefore:

- Small range: Pr[q+1 points] large
- Large range: Pr[q+1 points] small

Quantum Polynomial Interpolation

Using **q** queries to a polynomial, determine polynomial



Conclusion

Studying full quantum security notions important

- Quantum computers seem inevitable
- Unclear what attacks are possible
- Strive for strongest definitions
- Bonus: quantum query complexity results

Future work: more advanced primitives

- Identity-based encryption
- Functional encryption
- Fully homomorphic encryption
- Other quantum query questions

?