What are we talking about when we talk about \textbf{post-quantum} cryptography?
A personal view on post-quantum cryptography & a bite on quantum algorithms
How does cryptography change in a quantum world?
Triumph of modern cryptography

Public-key cryptography
- Digital signature: DSA, …
- Public-key encryption: RSA, …
- Diffie-Hellmann key exchange

Symmetric-key cryptography
- Block ciphers: AES
- Cryptographic hash function: SHA-2, …

Cryptographic protocols
- Secure two/multi-party computation
  - e-voting, …

Cryptography: a pillar of security for individuals, organizations and society!
Modern cryptography as a science

A formal framework: **provable security**

2012 ACM A.M. Turing Award
“… created mathematical structures that turned cryptography from an **art** into a **science**.”

- Security Model
- Security Analysis (Proof)
  - Breaking $\Sigma$ is as hard as solving $\Pi$
- Computational assumption
  - EX. Factoring & Discrete Log hard to solve

Crypto scheme $\Sigma$

Hard problem $\Pi$
Into a quantum world: the dark cat rises

Physicists: quantum weirdness

- Quantum superposition
  \[ \frac{1}{\sqrt{2}} (|\text{ALIVE}\rangle + |\text{DEAD}\rangle) \]

- Quantum Entanglement

  - Non-classical correlation
    “Spooky action at a distance”
    \[ \text{– A. Einstein} \]

Computer scientists

- Qubit
  \( \alpha |0\rangle + \beta |1\rangle \)

- Quantum gates & circuits
How does cryptography change in a quantum world?
Quantum attacks 1: break classical foundation

Public-key crypto (DSA, RSA, DH, …) \(\times\) Broken!

- Computational assumption
  - Factoring & Discrete Log hard to solve

Quantum computer can solve them\(^a\), fast! \(^a[Shor94]\)

Need: alternative problems to build crypto on
  - Exciting progress: lattice-based, code-based, …

Question: are the new problems hard for classical & quantum computers? Is this all we need to worry about?
Quantum attacks 2: invalidate classical framework

- Security Model
- Security Analysis
- Computational assumption: hard for quantum computer

Alert: unique quantum attacks
∃ information-theoretically secure protocol
Broken\(^b\) by quantum entanglement!
(vers. shared randomness)\(^b [\text{CSST11}]\)

Need: quantum provable-security framework
Re-examine EVERY link against quantum attackers

⚠️ Largely missing in PQC research…
Any quantum ingredient could be a threat

**Task**
- Run quantum factoring algorithm (to break public key crypto)

**Need**
- Full-scale fault-tolerant QC

**Availability**

<table>
<thead>
<tr>
<th>Complexity</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fault-tolerant quantum computation</td>
<td>2017?</td>
</tr>
<tr>
<td>Algorithms on multiple logical qubits</td>
<td></td>
</tr>
<tr>
<td>Operations on single logical qubits</td>
<td></td>
</tr>
<tr>
<td>Logical memory with longer lifetime than physical qubits</td>
<td>2013</td>
</tr>
<tr>
<td>QND measurements for error correction and control</td>
<td></td>
</tr>
<tr>
<td>Algorithms on multiple physical qubits</td>
<td></td>
</tr>
<tr>
<td>Operations on single physical qubits</td>
<td></td>
</tr>
</tbody>
</table>

**Available now**
- How to Build Your Own Quantum Entanglement Experiment, Part 1 (of 2)

**II**
- Quantum attack classical crypto
- Ex. Quantum entanglement

---
Post-Quantum Cryptography

- Hard problems broken
- Security framework fail
- Construct on new problems
- Analyze Security against quantum adv

Quantum Cryptography

- Outperform classical protocols
  - Ex. Quantum key distribution
- Crypto tools for quantum tasks
  - Ex. Encrypt quantum data

NB. Many already available (even as commercial products)
This Talk

1 Quantum algorithms
   • A recent breakthrough: quantum algorithm for high-degree number fields
     Application: break some lattice crypto!
   • The Hidden Subgroup Problem & Quantum Fourier Sampling

2 Examples: classical security framework inadequate
   • Quantum Rewinding
   • Quantum random oracle model
   • Quantum attack on symmetric crypto
Which problems admit faster quantum algorithms than classical algorithms?

∃ Poly-time quantum algorithms for:

- Factoring and discrete logarithm [Shor’94]
- Basic problems in algebraic number theory
  - Unit group
  - Principal ideal problem
  - Class group
    - Constant degree number fields [Hallgren’02’05,SV05]
    - Arbitrary degree
      - [EHKS’STOC14]
      - [BS’SODA16]

Best known classical algorithms need (at least) sub-exponential time
Our quantum algorithms for Unit group, Principal ideal problem

Break several lattice-based cryptosystems believed quantum safe before
Breaking some lattice crypto

- For efficiency, often use problems in lattices with more structures

- Short-PIP
- Ring-LWE
- ...

Bad news: Short-PIP based cryptosystems are broken!

Find a short generator of a principal ideal lattice

FHE\textsuperscript{c}, Multilinear mapping\textsuperscript{d}, PKE by GCHQ\textsuperscript{e}...

\textbf{broken}

\textbf{Our quantum alg's find A generator}

\textbf{Find A generator of a principal ideal lattice}

Classical procedure: reduce size of generator in cyclotomic fields\textsuperscript{e,f}

\textsuperscript{c}SmartV10
\textsuperscript{d}GargGH13
\textsuperscript{e}CampellGS15
\textsuperscript{f}CramerDPR15
How do quantum computers solve these problems?
The Hidden Subgroup Problem (HSP) framework

INPUT
Problem Π

Reduction

HSP on a group G

Quantum Algorithm

OUTPUT
Solution to Π

Captures most quantum exponential speedup

- **Standard Def.: HSP on finite group** $G$

  **Given:** oracle function $f: G \rightarrow S$, s.t. $\exists H \leq G$,

  1. **(Periodic on $H$)** $x - y \in H \Rightarrow f(x) = f(y)$

  2. **(Injective on $G/H$)** $x - y \notin H \Rightarrow f(x) \neq f(y)$

**Goal:** Find (hidden subgroup) $H$.

- Continuous $G$ (e.g. $\mathbb{R}^n$) tricky, but we can handle [EHKS14]
### Interesting HSP instances

<table>
<thead>
<tr>
<th>Computational Problems</th>
<th>HSP on G</th>
</tr>
</thead>
<tbody>
<tr>
<td>Factoring</td>
<td>$\mathbb{Z}$</td>
</tr>
<tr>
<td>Discrete logarithm</td>
<td>$\mathbb{Z}_N \times \mathbb{Z}_N$</td>
</tr>
<tr>
<td>Number fields (PIP etc.)</td>
<td>$\mathbb{R}^{O(n)}$</td>
</tr>
<tr>
<td>Simon’s problem (Crypto app later)</td>
<td>$\mathbb{Z}_2^n$</td>
</tr>
</tbody>
</table>

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Graph isomorphism</td>
<td>Symmetric group</td>
</tr>
<tr>
<td>Unique shortest vector</td>
<td>Dihedral group</td>
</tr>
</tbody>
</table>

#### Abelian groups

∃ efficient quantum algs

#### Non-abelian

Open question:

? efficient quantum algs
Solving HSP: quantum Fourier sampling

**Given:** oracle $f: G \to S$ periodic on $H$ & …

**Goal:** find $H$

**Real Domain**

- $G = \mathbb{Z}_N$
  - $G = \{0, r, 2r, \ldots, N-1\}$

- $G = \mathbb{Z}$
  - $G = \{\ldots, -r, 0, r, \ldots\}$

- $G = \mathbb{R}$
  - $G = (-r, 0, r, \ldots)$

**Fourier Spectrum**

- $\mathcal{F}_{\mathbb{Z}_N}$
  - $\mathcal{F}_{\mathbb{Z}_N} = \{0, N/r, 2N/r, \ldots\}$

- $\mathcal{F}_{\mathbb{Z}}$
  - $\mathcal{F}_{\mathbb{Z}} = \{\ldots, -1/r, 0, 1/r, \ldots\}$

**Standard method for finite $G$**

1. Quantum Fourier Sampling:
   - Quantum Fourier transform & measure

2. Recover $H$ from samples

**Old method for $\mathbb{R}_{\text{constant}}$**

- Discretize & Truncate
- Reduce to finite $G$

**Our method for continuous $\mathbb{R}^m$**

- Informal: try to approx. sample the ideal Fourier spectrum directly!

---

Noise becomes intolerable as dimension grows!
This Talk

1 Quantum algorithms
   • A recent breakthrough: quantum algorithm for high-degree number fields
   Application: break some lattice crypto!
   • The Hidden Subgroup Problem & Quantum Fourier Sampling

2 Examples: classical security framework inadequate
   • Quantum Rewinding
   • Quantum random oracle model
   • Quantum attack on symmetric crypto
Recall: classical security framework fails

Security model inadequate for quantum attackers

- Quantum security models: Still at early stage

Classical proofs can fail against quantum attackers

- Many PostQuantumC only consider classical attackers in proofs

See more in [Song’PQC14]
I. Difficulty of quantum rewinding

- **Rewinding argument**
  - Take snapshot of an adversary & continue
  - Later “rewind” & restart from snapshot

- **Rewinding quantum adversary difficult**
  - Cannot *copy* unknown quantum state
  - Information gain → disturbance on state

⇒ **Quantum security of many classical protocols unclear**

- **Not often seen in PQC literature?**
  - Usually does not affect analysis of encryption, signature, …
  - But does *matter*: e.g. Quantum-secure Identification scheme (to get signature by Fiat-Shamir)
II. Hash function: common heuristic fails?

- **Hash functions are everywhere:**
  - Signature, message authentication, key derivation, bitcoin,…

- **The Random Oracle (RO) heuristic widely used**
  - “Lazy” sampling: decide \( H(\cdot) \) on-the-fly
  - Program RO: change \( H(\cdot) \) adaptively
    - Ease security proof of hash-based schemes (otherwise **impossible**)

- **Quantum-accessible Random Oracle**
  - Nothing appears to work…
  - A lot exciting development restoring classical proofs
III. Quantum attacking symmetric crypto

- These attacks need specific* quantum model
  - Assume attackers have QUANTUM access to the SECRET enc/auth algorithm

- Quantum random oracle is more justified
  - Hash functions are public, any (quantum) user can implement it quantumly

Broken!?

3-round Feistel Cipher
CBC-MAC

...  

Simon’s Problem ≡ HSP on $\mathbb{Z}_2^n$

Easy on a quantum computer

* In my opinion unrealistic but still possible

[KM10] [KLL+16] [SS'16]
Concluding Remarks

How does cryptography change in a quantum world?

Post-Quantum Cryptography

- Hard problems broken
- Construct on new problems
- Need more study on (quantum) hardness
- Security framework fail
- Analyze Security against quantum adv
- Be aware and cautious!
  Many issues unclear

Quantum Cryptography
Possible complement
I’m hiring

- **2-3 PhD students to work on**
  - Quantum algorithms
  - Analyzing quantum security of classical crypto
  - Quantum crypto

- **Maybe 1 Post-doc too**

- **Get in touch if interested**
  - Check my webpage for more: fangsong.info
  - Email: fang.song@pdx.edu

**Portland State Computer Science**

**Young but strong in**

- Programming language, machine learning, vision, …
- Portland is absolutely nice in many ways~

Thank you!