PQC Asia Forum Seoul, 2016

What are we talking about when we talk about **post-quantum** cryptography?

Portland State
Computer Science

Fang Song
Portland State University

PQC Asia Forum Seoul, 2016

A personal view on post-quantum cryptography & a bite on quantum algorithms

Portland State
Computer Science

Fang Song
Portland State University

How does cryptography **change** in a quantum world?

Triumph of modern cryptography

2015 A.M. Turing Award

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**."

Crypto scheme Σ

Hard problem Π

- Security Model
- Security Analysis (Proof)
  - Breaking Σ is as hard as solving Π
- Computational assumption
  - EX. Factoring & Discrete Log hard to solve

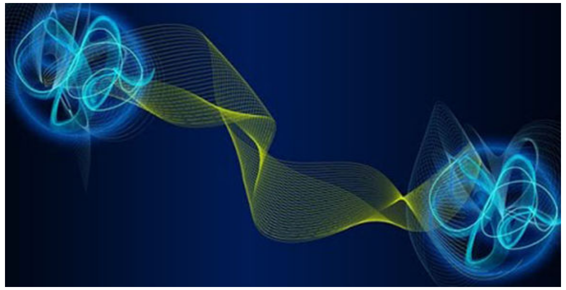
Into a quantum world: the dark cat rises

Physicists: quantum weirdness

Quantum **superposition**

$$\frac{1}{\sqrt{2}}(|\text{ALIVE}\rangle + |\text{DEAD}\rangle)$$

Quantum Entanglement



- Non-classical correlation

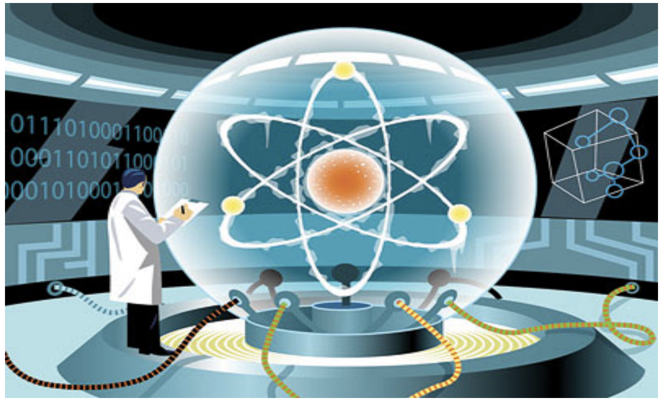
"Spooky action at a distance"

– 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,…) ✗ Broken!

Factoring/DL ✗

- 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

Crypto schemes ?

Lattices, …

- Security Model ✗
- Security Analysis
- Computational assumption:

hard for **quantum** computer

Alert: unique quantum attacks

> ∃ information-theoretically secure protocol
> Broken[b] by quantum entanglement! (vs. shared randomness)

This can happen now!

(Technology available)

[b][CSST11]

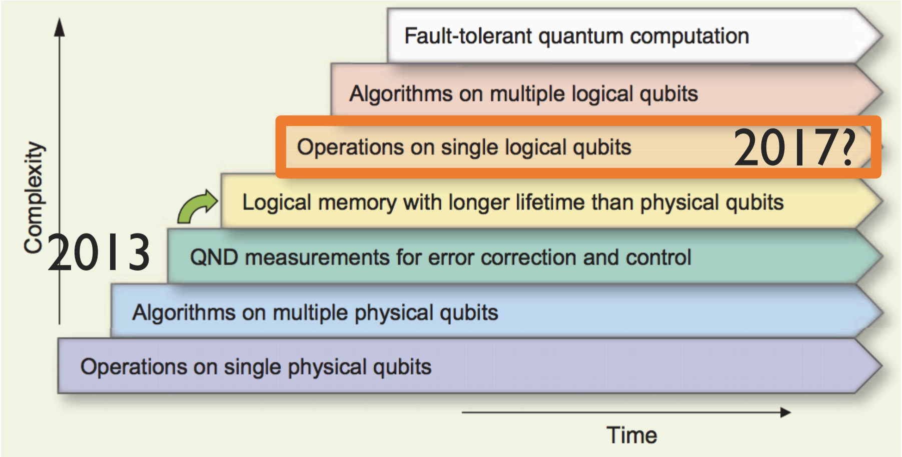
Need: quantum provable-security framework

Re-examine EVERY link against quantum attackers

☹ Largely missing in PQC research…

Any quantum ingredient could be a threat

	Task	Need	Availability
I	Run quantum factoring algorithm (to break public key crypto)	Full-scale fault-tolerant QC	



	Task	Need	Availability
II	**Quantum attack classical crypto**	Ex. Quantum entanglement	**Available now**

How to Build Your Own Quantum Entanglement Experiment, Part 1 (of 2)

How does cryptography **change** in a quantum world?

Post-Quantum Cryptography

Hard problems broken → Construct on new problems

Security framework fail → 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

exponentially

Which problems admit faster |quantum⟩ algorithms than classical algorithms?

∃ Poly-time quantum algorithms for:

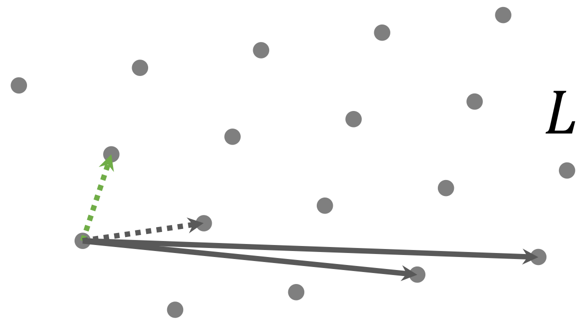
- Factoring and discrete logarithm [Shor'94]
- Basic problems in algebraic number theory

	Unit group	Principal ideal problem	Class group
Constant degree number fields	[Hallgren'02'05,SV05]		
Arbitrary degree	[EHK**S**'STOC14]	[B**S**'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



QUANTA MAGAZINE illuminating science

CRYPTOGRAPHY

A Tricky Path to Quantum-Safe Encryption

Breaking some lattice crypto

- For efficiency, often use problems in lattices w/ more **structures**

Short-PIP | Ring-LWE ? | …

Bad news: Short-PIP based cryptosystems are broken!

FHE[c], Multilinear mapping[d], PKE by GCHQ[e]… **broken**

Our quantum alg's find A generator

Find a short generator of a principal ideal lattice

Short-PIP → PIP

Find A generator of a principal ideal lattice

Classical procedure: reduce size of generator in cyclotomic fields[e,f]

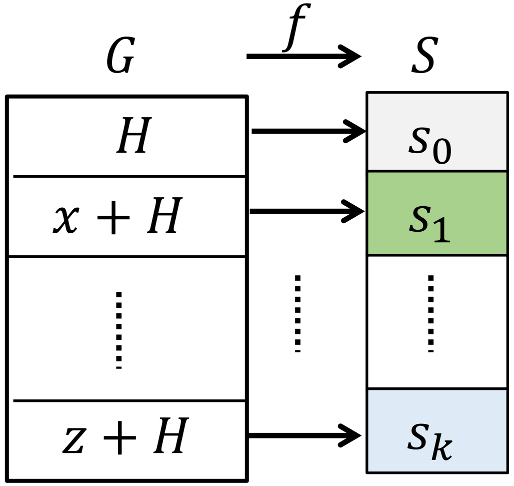
[c]SmartV10
[d]GargGH13
[e]CampellGS15
[f]CramerDPR15

How do quantum computers solve these problems?

The Hidden Subgroup Problem (HSP) framework

Captures most quantum exponential speedup

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



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

1. (Periodic on H) $\quad x - y \in H \Rightarrow f(x) = f(y)$
2. (Injective on G/H) $\quad x - y \notin H \Rightarrow f(x) \neq f(y)$

Goal: Find (hidden subgroup) H.

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

Interesting HSP instances

Computational Problems	HSP on G
Factoring	$\mathbb{Z}$
Discrete logarithm	$\mathbb{Z}_N \times \mathbb{Z}_N$
Number fields (PIP etc.)	$\mathbb{R}^{O(n)}$
Simon's problem (Crypto app later)	$\mathbb{Z}_2^n$

Abelian groups

∃ efficient quantum algs

Graph isomorphism	Symmetric group
Unique shortest vector problem	Dihedral group

Non-abelian

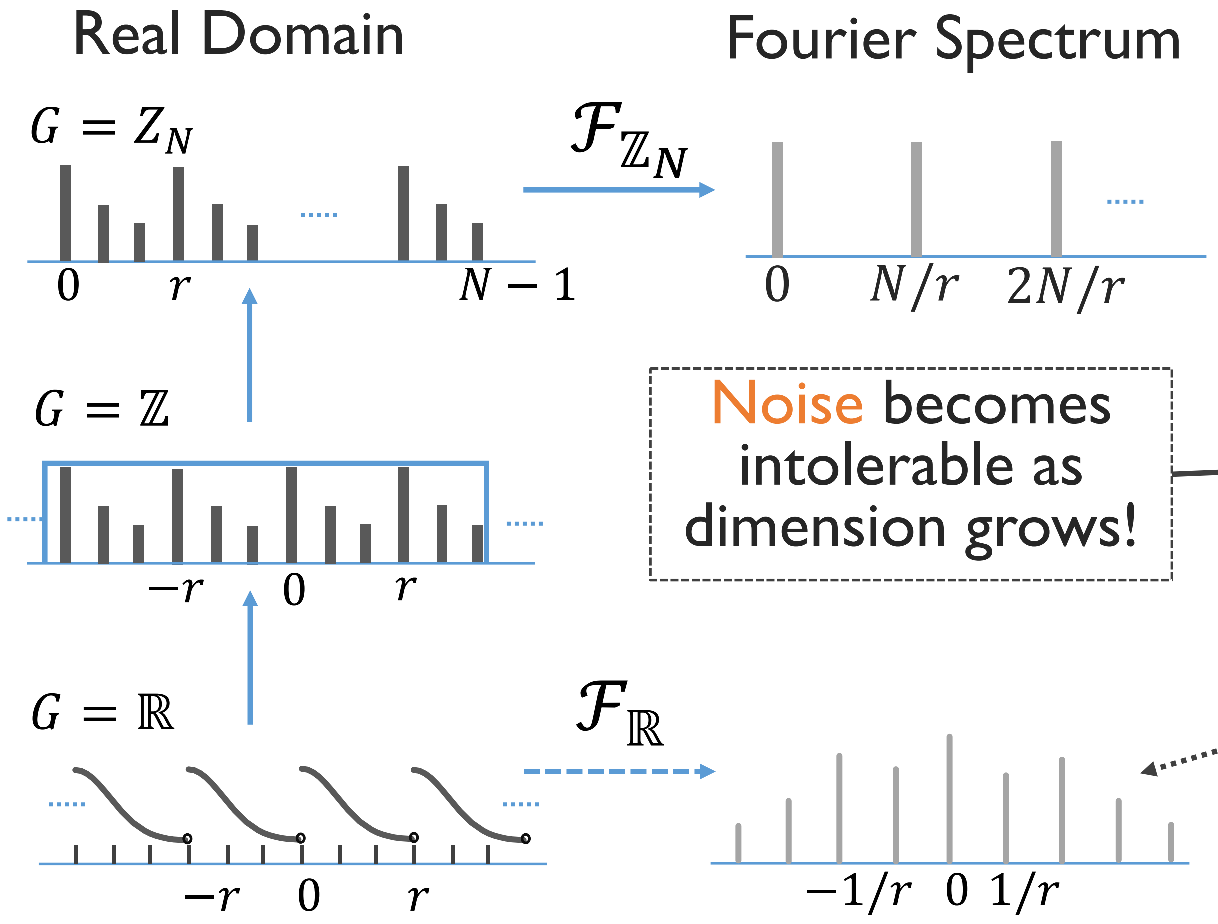
Open question:

? efficient quantum algs

Solving HSP: quantum Fourier sampling

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

Goal: find H



Standard method for finite G

1. Quantum Fourier Sampling:
   - Quantum Fourier transform & measure
2. Recover H from samples

Old method for $\mathbb{R}^{constant}$

- Discretize & Truncate
- Reduce to finite G

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

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

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

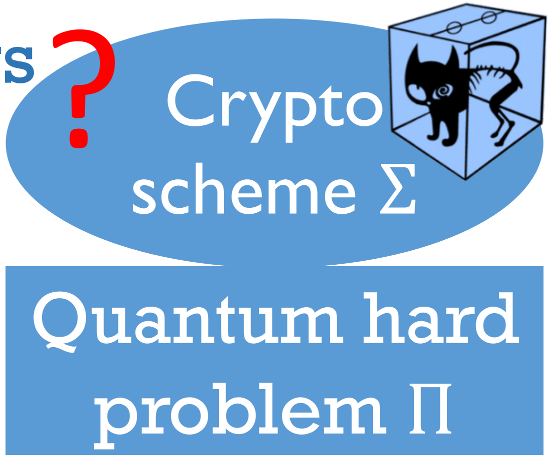
2 Examples: classical security framework inadequate

- Quantum Rewinding
- Quantum random oracle model
- Quantum attack on symmetric crypto

Recall: classical security framework fails

Security model inadequate for quantum attackers

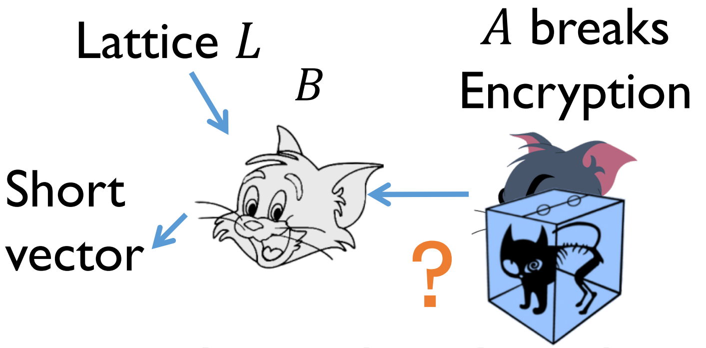
➡ Quantum security models: Still at early stage



Classical proofs can **fail** against quantum attackers

Many PostQuantumC only consider classical attackers in proofs

See more in [Song'PQC14]

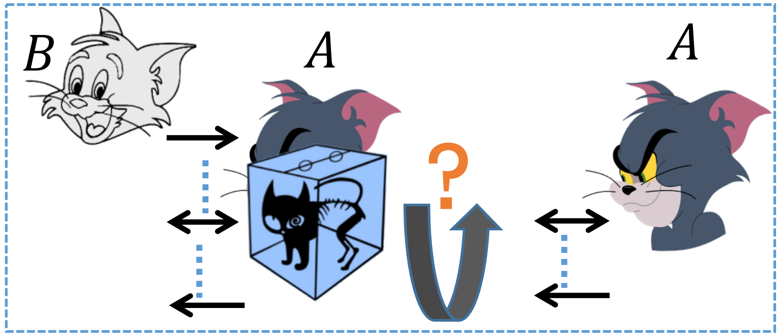


Assume attacker A breaks scheme Σ,

→ Construct B from A solving hard problem Π.

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

Only special cases possible[g]

[g][Watrous09]

→ **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)

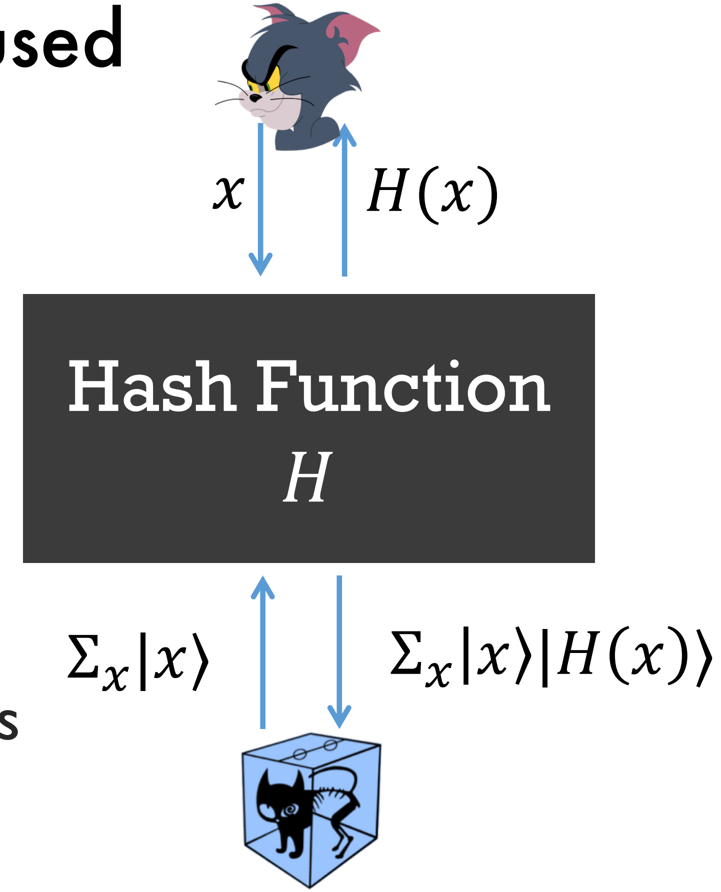
II. Hash function: common heuristic fails?

- Hash functions are everywhere:

  Signature, message authentication, key derivation, bitcoin,…

- The **R**andom **O**racle (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 developement restoring classical proofs



III. Quantum attacking symmetric crypto

3-round Feistel Cipher

CBC-MAC

…

Broken!?

[KM10]
[KLL+16]
[SS'16]
→

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

Easy on a quantum computer

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

* In my opinion unrealistic but still possible

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

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!