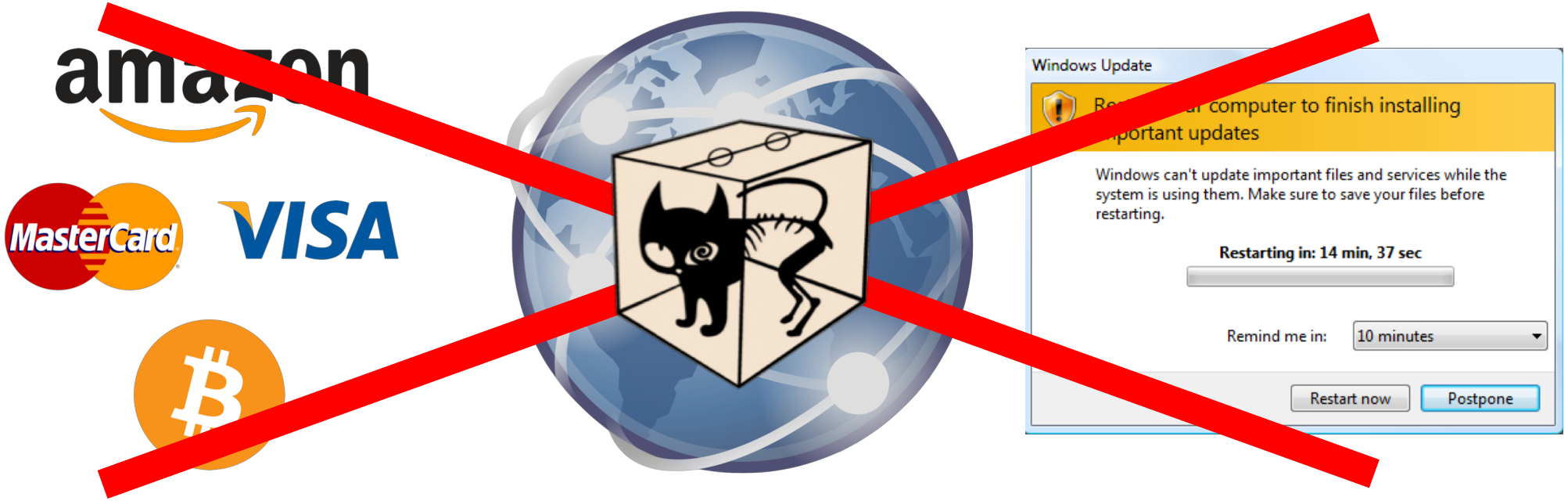
Quantum-safe cryptography & more

Fang Song

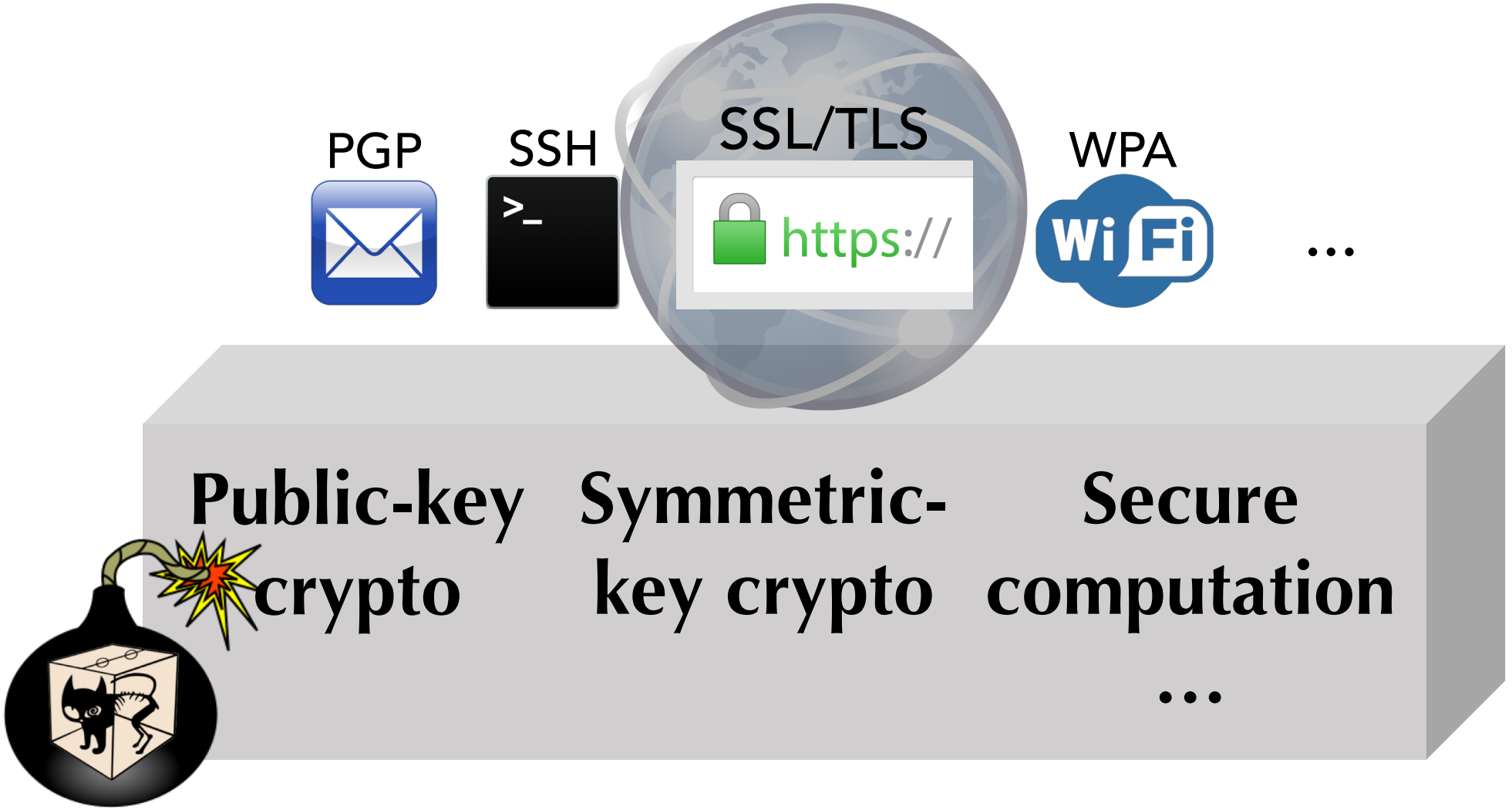
~~Portland State U~~

Texas A&M U fang.song@tamu.edu

Secure Internet will be shattered by quantum computers in x years

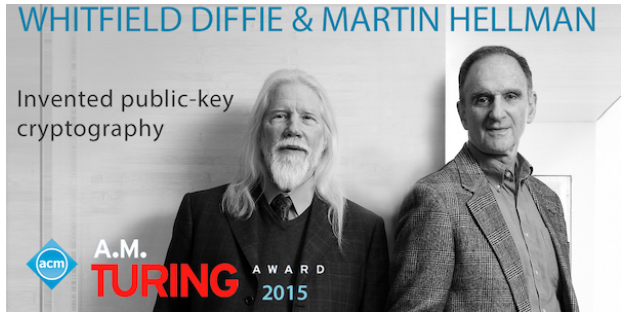


Break at a foundation: Cryptography



How do quantum attackers break cryptography?

1. Crack hard problems

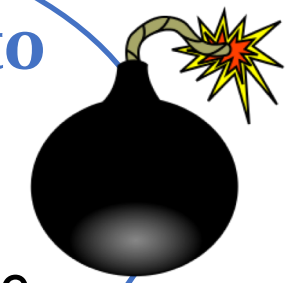


Assumption: (better be) hard to solve

Public-key crypto

- RSA encryption
- Digital signature
- DH key-exchange

• • •



Factoring
Discrete Logarithm

[a][Shor94]

Quantum computer solves them[a], **fast!**

2. Transform security methodology

- Alert: unique quantum attacks
  - A classical protocol proved "unconditionally" secure,
  - Broken by quantum entanglement (vs. shared randomness) [b]

[b][CSST11]

"… created mathematical structures that turned cryptography from an art into a science"

- Formal framework of modern crypto

Crypto scheme Σ

- ~~Security model~~
- ~~Security Analysis (Proof)~~
  - Breaking Σ is as hard as solving Π

Hard problem Π

- Computational assumption

Post-Quantum Cryptography

How to secure cryptography against quantum attackers?

Hard problems cracked

Security framework failed

1 Build on alternative problems

2 Quantum security framework

My work on Post-Quantum Crypto

1. Design efficient quantum algorithms [5,8]

- Solve algebraic problems exponentially faster
- Break candidate quantum-safe problem & cryptosystems
- Develop new quantum algorithmic tools

5.SODA16
8. STOC14, QIP15

2. Acquire quantum-safe crypto

i. Develop formal methodology for quantum security [4,7,10]

- Model quantum security: composable protocols, …
- Develop general techniques: "quantum-friendly" reductions, fined-grained quantum complexity …

ii. Construct and analyze quantum-secure schemes [1,2,6,9,10]

- Two-party computation protocols
- Hash functions and random-oracle heuristic
- Block ciphers and message-authentication

1.PQCrypto18
2.Crypto17
4.PKC16
6.TQC15
7.PQCrypto14
9.TCC13
10.Crypto11,QIP11

What is x, after all?

universal, fault-tolerant (e.g., run Shor's factoring alg.)

x=?: born of a quantum computer

S. Aaronson (UT Austin)

G. Kalai (Hebrew U)

$X = -10$?

D-Wave
The Quantum Computing Company™

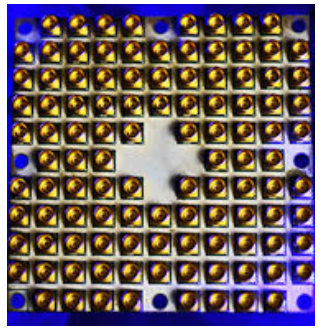
x — 2007 — 2018 — ∞

Google

IBM

intel

rigetti



CES 2018: Intel's 49-Qubit Chip Shoots for Quantum Supremacy

Quantum threat is pressing

- x=?: universal quantum computer (breaking public-key crypto)

A: time to transit to new cryptosystems
B: how long your data needs to be safe

⟵ >>>> your expected time!

Theorem. If $A + B > X$, then act now!

- $x \leq 0$: quantum attack on cryptography ⟵ Available now!

"… we announce preliminary plans for transitioning to quantum resistant algorithms."

Aug 19, 2015

www.nsa.gov/ia/programs/suiteb_cryptography/

NIST National Institute of Standards and Technology U.S. Department of Commerce

Post-Quantum Cryptography Standardization

Feb 24-26, 2016	NIST Presentation at PQCrypto 2016: *Announcement* *Dustin Moody*
April 28, 2016	NIST releases NISTIR 8105, Report on Post-Quantum
Dec 20, 2016	Formal Call for Proposals
Nov 30, 2017	Deadline for submissions
Dec 4, 2017	NIST Presentation at AsiaCrypt 2017: *The Ship Has Sa* *Dustin Moody*
Early 2018	Workshop - Submitter's Presentations
3-5 years	Analysis Phase - NIST will report findings *1-2 workshops during this phase*
2 years later	Draft Standards ready

Quantum cryptography: another approach

Let's play quantum too!

- Supplement (and **outperform**) classical cryptography
  - Quantum key distribution: secure against **unbounded** eavesdroppers
- Protect **quantum** information
  - Encrypt & authenticate quantum data …

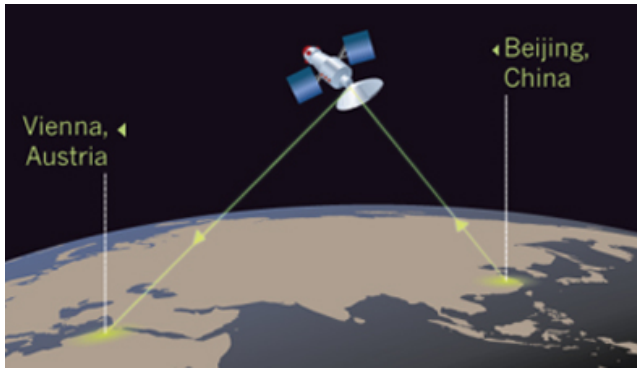
Impossible by classical crypto

Technology closer: commercial QKD products on the market

QIA

QUANTUM INTERNET ALLIANCE

http://quantum-internet.team/



https://en.wikipedia.org/wiki/Quantum_Experiments_at_Space_Scale

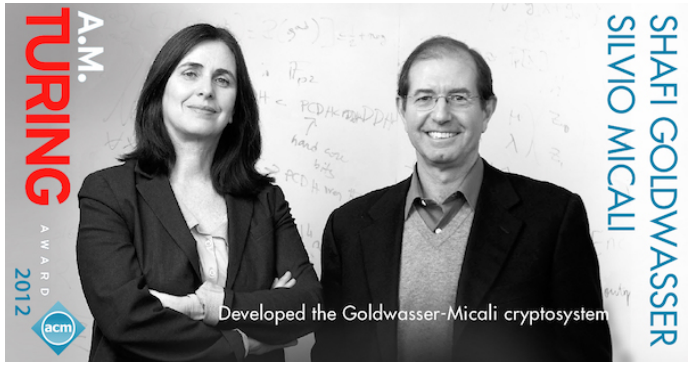
My work on quantum cryptography

- Construct quantum protocols bypassing classical impossibility [9]

[9]TCC13

- Construct zero-knowledge proof systems for Quantum NP [3]

[3]FOCS16



Triumph of zero-knowledge proof, classically

"… pioneered new methods for efficient verification of mathematical proofs"

- Construct pseudorandom quantum states and quantum money *

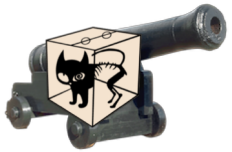
Analogous to pseudorandom number generator

* JL**S**'Preprint17

Summary of my main work

Post-Quantum Cryptography

1. Design efficient quantum algorithms
   - Solve algebraic problems exponentially faster
   - **Break** candidate quantum-safe problem & cryptosystems



5.SODA16
8. STOC14, QIP15

2. Acquire quantum-safe crypto

   i. Establish a formal methodology for quantum security

   ii. Construct and analyze quantum-secure schemes

   - Two-party computation, hash functions …
   - Block ciphers & message-authentication

1.PQCrypto18
2.Crypto17
4.PKC16
6.TQC15
7.PQCrypto14
9.TCC13
10.Crypto11,QIP11

Quantum Cryptography

- Quantum protocols bypassing classical impossibility
- Zero-knowledge for Quantum NP, quantum money …

3.FOCS16
7.TCC13

This Talk

1 Design efficient quantum algorithms

- Solve algebraic problems exponentially faster
- **Break** candidate quantum-safe problem & cryptosystems
- Develop new quantum algorithmic tools

2 Acquire quantum-safe crypto-systems

- Challenges of analyzing quantum security
- Block cipher domain-extension & message-authentication

Become a quantum expert in 3 minutes

- **Quantum = ++ Prob. theory**
  - $p_0, p_1 \in \mathbb{C}$ (negative OK)
  - $|p_0|^2 + |p_1|^2 = 1$ (ℓ_2-normalized)

- **Probability theory**
  - $0 \le p_0, p_1 \le 1$
  - $p_0 + p_1 = 1$ (ℓ_1-normalized)

Physicists: Quantum weirdness

- Quantum Superposition
  - → No-cloning of unknown QState

Qubit

$$= \frac{1}{\sqrt{2}}|\rangle - \frac{1}{\sqrt{2}}|\rangle$$

- Quantum Entanglement
  - (A non-classical correlation)

$$\frac{1}{\sqrt{2}}|\rangle - \frac{1}{\sqrt{2}}|\rangle$$

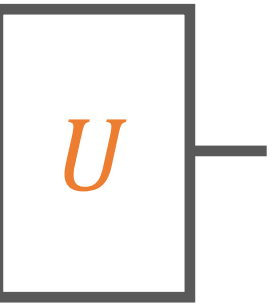
Computer scientists: a novel computer?

Build a quantum computer

Qubits

$\sum_{x\in\{0,1\}^n} p_x|x\rangle$

with $\sum_x |p_x|^2 = 1$



Quantum

gates & circuits

- Is it any good?
  - Classical computer cannot simulate
    (300 qubits ~ 2^{300} bits to describe)
  - Solve hard problems faster
    by constructive interference (≠ mass parallelism)

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	[EHKS'STOC14]	[BS'SODA16]	

Best known classical algorithms need (at least) sub-exponential time

Our contributions

Unit group	S-units
Principal ideal problem	Norm equations
Class group	…

- Efficient quantum algorithms for basic problems in number fields of **arbitrary**-degree

- More examples of quantum **exponential** speedup

- New **quantum** algorithmic tools

- **Break** several lattice cryptosystems **believed quantum-safe before**

QUANTA MAGAZINE illuminating science

CRYPTOGRAPHY

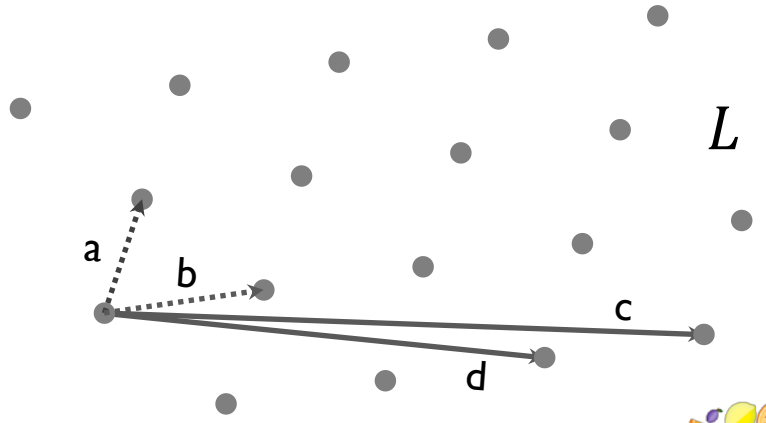
A Tricky Path to Quantum-Safe Encryption

https://www.quantamagazine.org/quantum-secure-cryptography-crosses-red-line-20150908/

Lattice-based cryptography

- Lattice problems
  - Shortest vector problem, …

Conjecture: hard even for quantum computers



- A neo-tree of crypto grows

Hash function, signature

Public-key encryption, ID-based encryption

Fully homomorphic encryption, program obfuscation …

Breaking some lattice crypto

- For efficiency, often use lattices with more structures

Short-PIP ✗ | Ring-LWE ? | …

[CramerDW'Eurocrypt17]: extension to break more

- Short-PIP based cryptosystems broken!

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

broken

Our quantum alg's find a generator

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

Our algorithms: a generalized framework

- **The Hidden Subgroup Problem (HSP) framework**
  (captures most instances of quantum exponential speedup)

- **Our contribution**
  - **a** A **continuous** HSP framework
    - subsumes standard HSP
    - conceptually a lot simpler
  - **b** Employ quantum power in reduction already

Interesting HSP instances

Computational Problems	HSP on G
Factoring	$\mathbb{Z}$
Discrete logarithm	$\mathbb{Z}_N \times \mathbb{Z}_N$
Number fields (PIP etc.)	Continuous $\mathbb{R}^{O(n)}$
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

This Talk

1 Design efficient quantum algorithms

- Solve algebraic problems exponentially faster
- **Break** candidate quantum-safe problem & cryptosystems
- Develop new quantum algorithmic tools

2 Acquire quantum-safe crypto-systems

- Challenges of analyzing quantum security
- Block cipher domain-extension & message-authentication

Recall: classical security framework fails

Crypto scheme ?

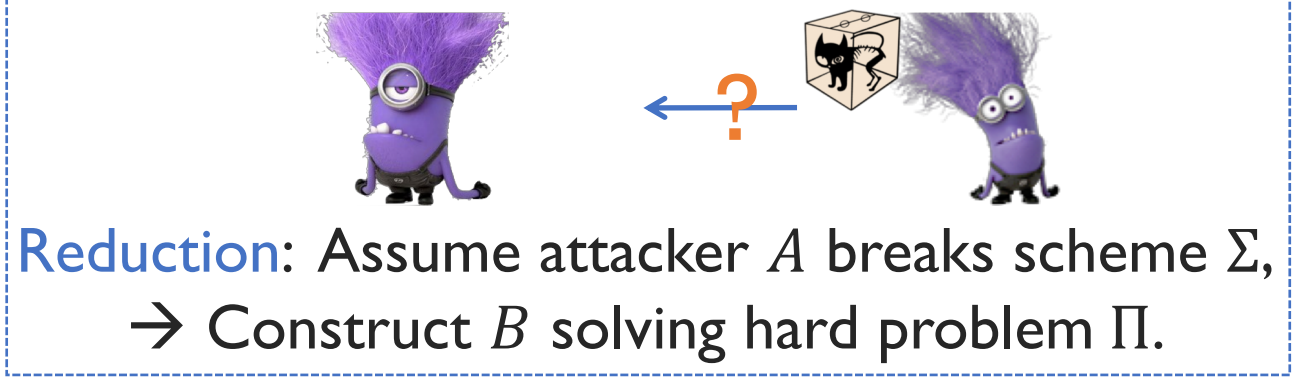
Quantum hard problem

- Security models: inadequate for Q attacks

  ➡ Quantum security models: catching up and a lot to do

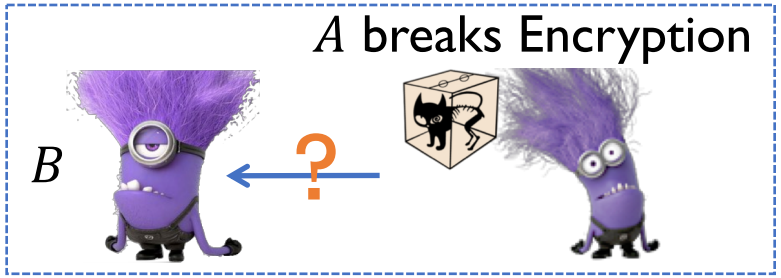
- Security analysis: can fail against Q attackers

  ➡ Quantum security analysis: subtle & challenging

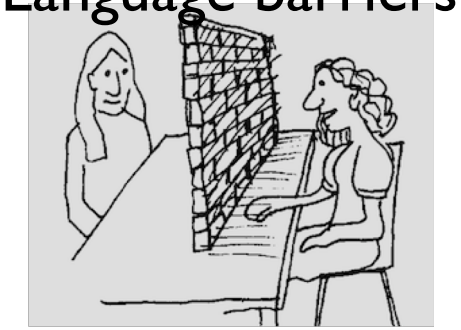


Reduction: Assume attacker A breaks scheme Σ,
→ Construct B solving hard problem Π.

Difficulties of analyzing quantum security



"Language barriers"



(Classical) probability	Quantum
Fix randomness of A	Quantum A no explicit random coins (inherently randomized)
If "A does Z", B works	Event "A does Z" ill-defined
Rewinding: B take snapshots of A at various points, run it back and forth	Quantum rewinding, really? • Quantum no-cloning • Observations destructive
…	

We are not totally clueless…

ge barriers”

Quantum (difficulties)

Quantum A no explicit random coins (inherently randomized)

Event “A does Z” ill-defined

Quantum rewinding, really?

Some progress (in my work [1,4,6,9,10])

- Hardness of search ➔ security
- Restore random-oracle heuristic & hash function security in the quantum world

- Special Q-rewinding [Watrous09]
- Quantum-secure zero-knowledge proofs of knowledge & 2-party computation

??? Constant round Zero-Knowledge, …

Quantum attackers,
is that the best you can do?

Fine, I know you can

- Solve factor, DL, some lattice problem, and break most public-key crypto
- Make my life miserable to struggle with new security models & analysis methodology

Apparently, you haven't broken symmetric-key crypto yet

I've still got AES, try it…

Break symmetric-key crypto (block-cipher related)

- Block Cipher
  - Apps: hash functions (SHA-2), authentication, encryption, …
  - Examples: DES, AES (Advanced Encryption Standard)

Broken!

Core of DES	**3-round Feistel Cipher**
Simplified AES	**Even-Mansour Cipher**
Message authentication	**CBC-MAC**
Authenticated encryption	**Galois/Counter mode**
	…

[KM10'12]
[KLL+16]

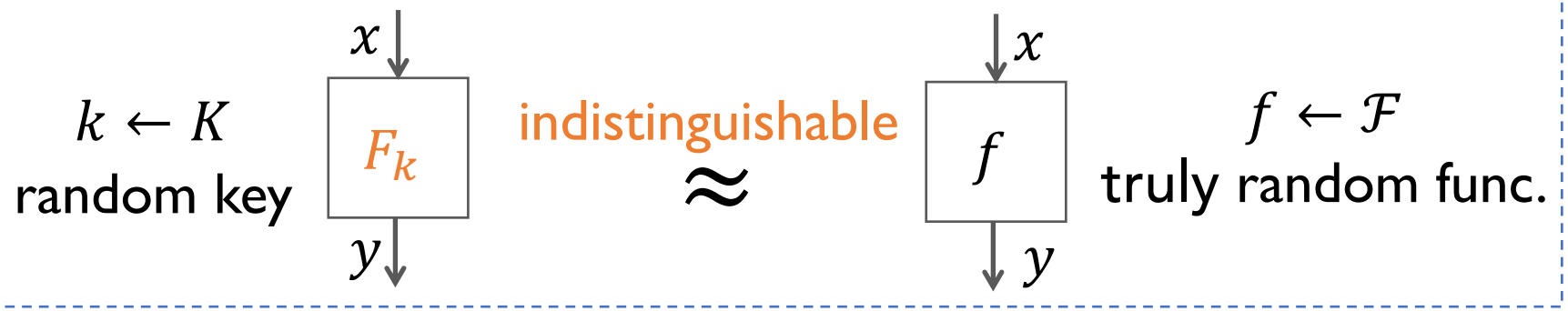
Easy on a quantum computer

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

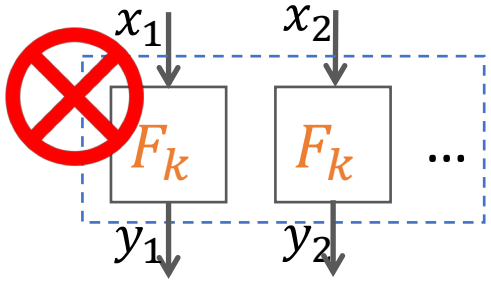
Block cipher and domain extension

- Block Cipher $\{F_k\}$
  - "Efficiently computable permutation that looks random (with random key k)"

$$\{F_k\} \subseteq \mathcal{F} := \{f : \{0,1\}^n \to \{0,1\}^n\} \text{ (e.g., } n = 128)$$

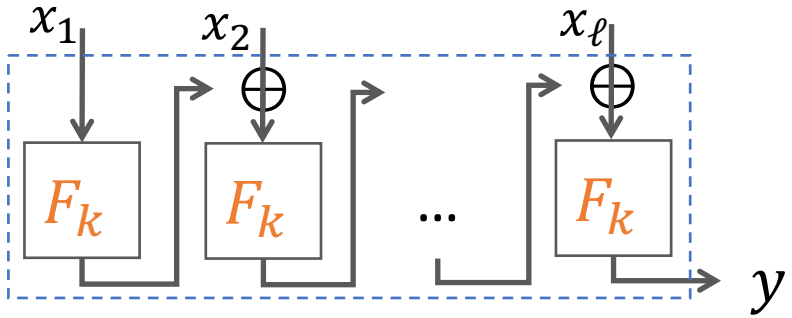


- How about long inputs: domain-extension
  - **Given** psodorandom $\{F_k\}$ on n-bit input
  - **Construct** pseudorandom $\{G_k\}$ on $\ell \cdot n$-bit input



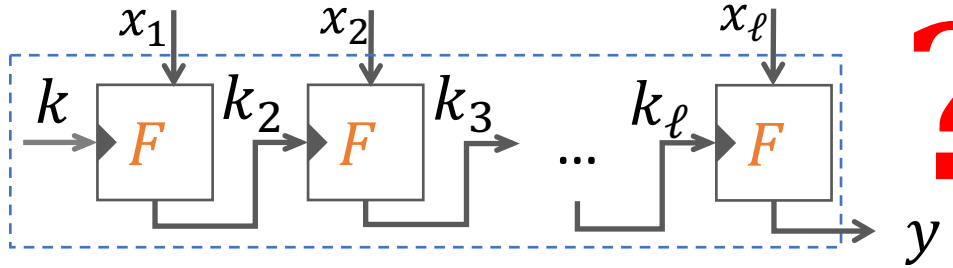
Classically secure domain-extension

- **CBC-MAC** ANSI X9.19, ISO/IEC 9797



Broken by quantum!

- **Cascade (NMAC, HMAC)** NIST.FIPS.198, IPSec, TLS



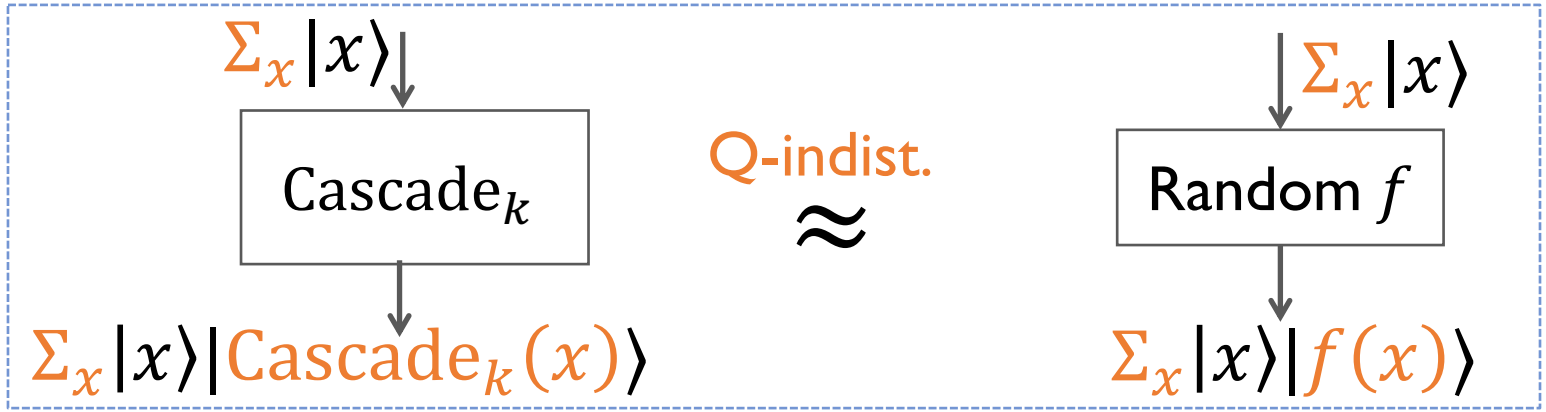
?

- Cascade (NMAC & HMAC) quantum-secure?
- Is quantum-secure domain-extension even possible?

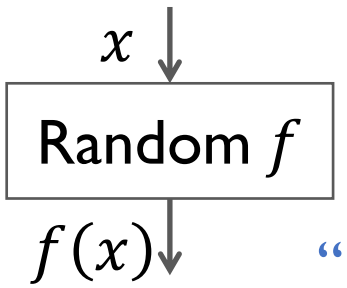
Our main result

Cascade, NMAC, HMAC (and more) are quantum-secure

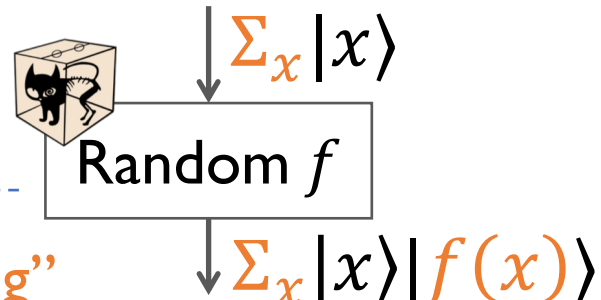
i.e., quantum-indistinguishable from a truly random function



Power of quantum-superposition attack



Local view, one by one ⟵ **Attacker** ⟶ Global view, observe all?



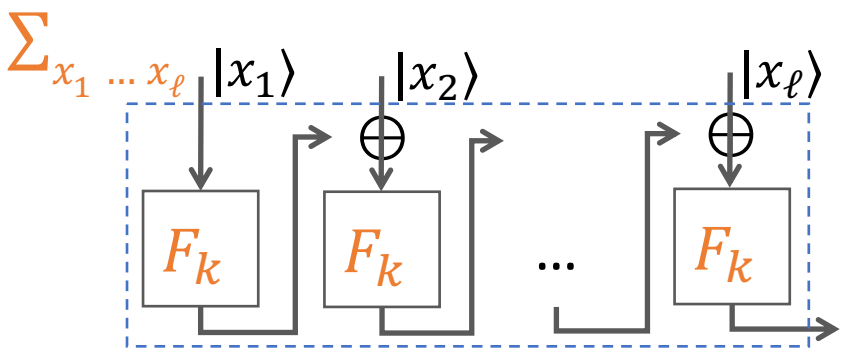
"Lazy" sampling
generate f *on-the-fly*

⟵ **You** (designer) ⟶

"Full committing"
sample entire f *ahead*

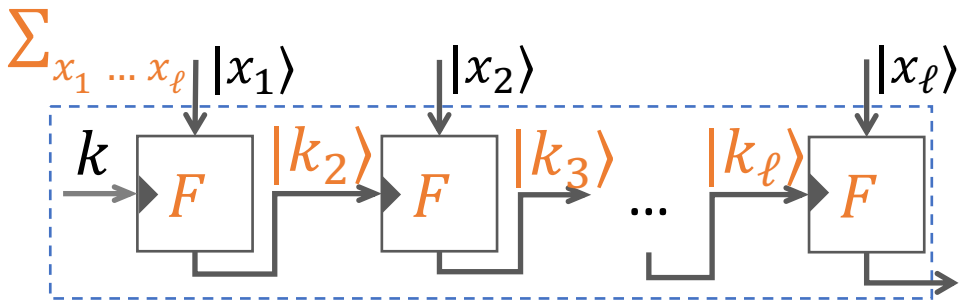
CBC-MAC **Broken!**

global view on F_k of a random k



Cascade

global view on F_k of all k!



we proved it's quantum secure

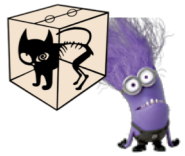
Future directions

Quantum-safe Crypto

Emerging security issues

Power of quantum computing

Future work: quantum-safe crypto

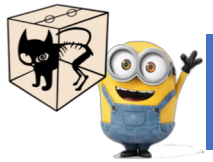


Post-quantum crypto

- Are new candidates indeed hard?
  - Break other lattice problems? Multivariate-equations? …
- How to get quantum-secure cryptosystems?
  - Fine-grained analysis of hash functions & block ciphers
  - Quantum-safe Bitcoin & blockchain

NSF:Medium:Collaborative

- New complexity foundation
- Q-secure auth., signature …



Quantum crypto

- What else are possible? & a formal framework?
  - Quantum money, quantum tokenized crypto…

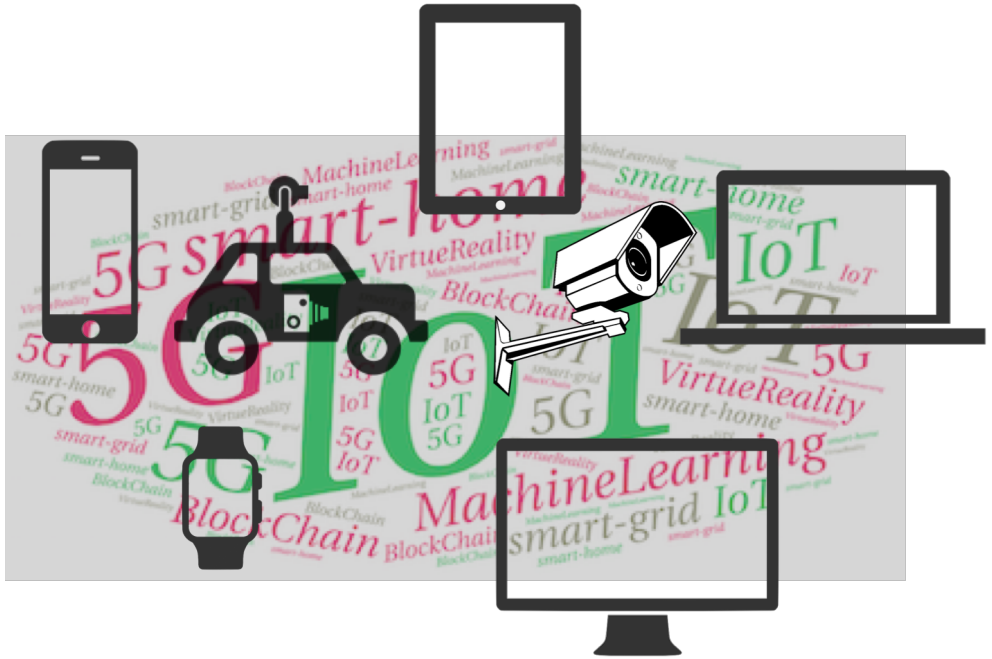
Future work: securing advancing technology

What do they bring?

IoT, 5G, Cloud, Big Data, ML …

- Diverse players of imbalanced resource

- Lightweight Cryptography
  - ☺ Memory-friendly, energy-friendly …
  - ☹ **Attack**-friendly too?
- Update security model
  - Always poly-time adversary too coarse
- Design protocols that better fit
  - Workload respects capacity



Future work: embracing quantum power

Quantum algorithms

- Machine learning
- Chemistry /Biology
- Big Data
- . . .

- Quantum sensing
- Q Software foundations
- Limitations of QC

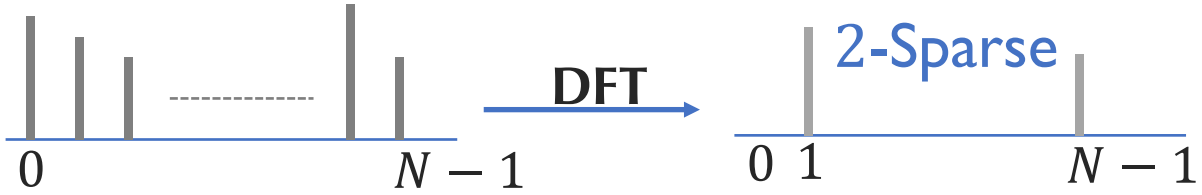
Quantum Fourier Transform

- Exponentially faster than classical FFT algorithm
- Using one quantum sample of input data

Expensive!

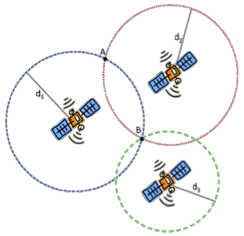
Sparse Quantum FT?

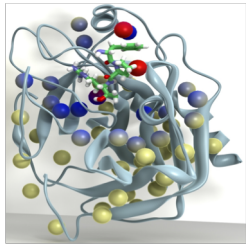
- Using a few classical samples? and even faster?
- Useful in **near-term** (noisy 100-qubit processor)?



Many apps in data analysis

MIT sFFT group





Quantum-safe Crypto

Emerging security issues

Power of quantum computing

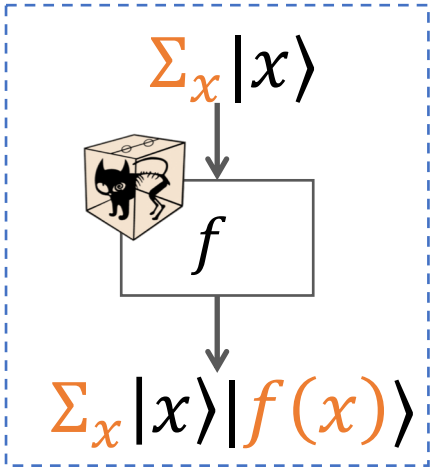
Thank you!

References (my own)

1. Quantum Collision-Finding in Non-Uniform Random Functions. Marko Balogh and Edward Eaton and Fang Song. PQCrypto 2018.
2. Quantum Security of NMAC and Related Constructions. Fang Song and Aaram Yun. Crypto 2017.
3. Zero-knowledge proof systems for QMA. Anne Broadbent, Zhengfeng Ji, Fang Song and John Watrous. FOCS 2016.
4. Mitigating multi-target attacks in hash-based signatures. Andreas Hülsing, Joost Rijneveld and Fang Song. PKC 2016.
5. Efficient quantum algorithms for computing class groups and solving the principal ideal problem in arbitrary degree number fields. Jean-François Biasse and Fang Song. SODA 2016.
6. Making existentially unforgeable signatures strongly unforgeable in the quantum-random oracle model Authors: Edward Eaton and Fang Song. TQC 2015.
7. A note on quantum security for post-quantum cryptography. Fang Song. PQCrypto 2014.
8. A quantum algorithm for computing the unit group of an arbitrary degree number field. Kirsten Eisenträger, Sean Hallgren, Alexei Kitaev and Fang Song. STOC 2014.
9. Feasibility and completeness of cryptographic tasks in the quantum world. Serge Fehr, Jonathan Katz, Fang Song, Hong-Sheng Zhou and Vassilis Zikas TCC 2013.
10. Classical cryptographic protocols in a quantum world. Sean Hallgren, Adam Smith and Fang Song. Crypto 2011.
11. Pseudorandom states and unitaries, and applications to quantum money. Zhengfeng Ji, Yi-Kai Liu, Fang Song. arXiv:1711.00385, 2017
12. Basing cryptography on NP-hardness using quantum reductions. Nai-Hui Chia, Sean Hallgren, Fang Song. October 2017

Is superposition attack realistic?

f: crypto-algorithm (Enc, Sign, etc..) with secret key



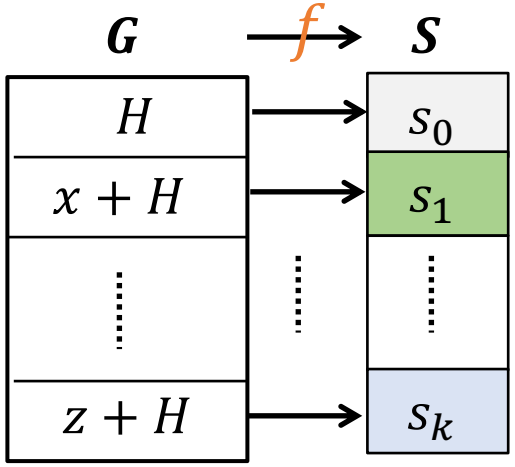
Attacker can implement f as a quantum circuit

- Could occur in public-key setting
  - Ex. Block cipher to Pub-key Enc via obfuscation
- Building block in big system
  - Be conservative (quantum & classical hybrid Internet)
- Makes our POSITIVE result stronger!

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) $\quad x - y \notin H \Rightarrow f(x) \neq f(y)$

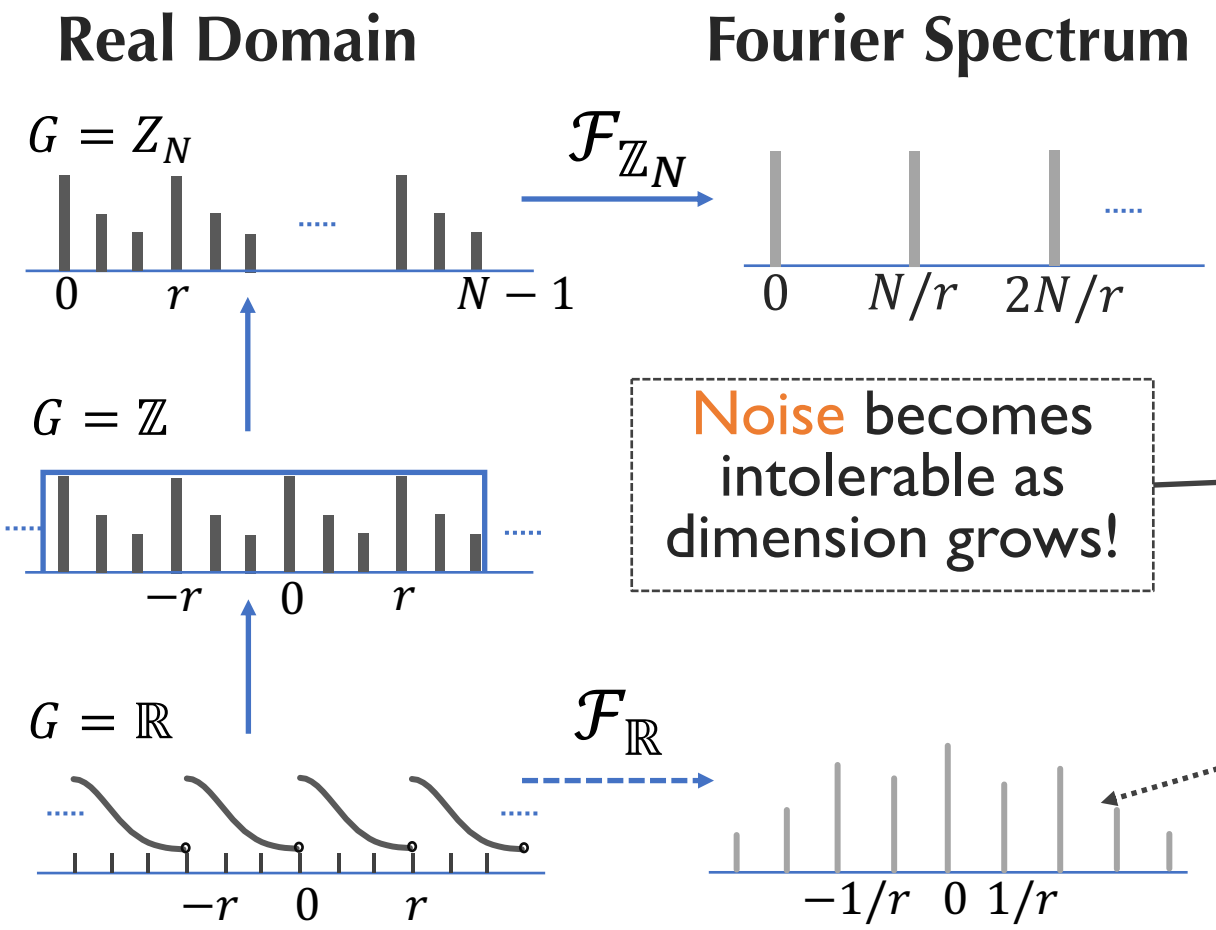
Goal: Find (hidden subgroup) H.

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

Solving HSP: quantum Fourier sampling

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

Goal: find H



Noise becomes intolerable as dimension grows!

Standard method for finite G

- Quantum Fourier Sampling: quantum Fourier transform & measure
- 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!