Greetings from Schrödinger's cat:

How are you doing in a quantum world, **cryptography**?

Fang Song

Institute for Quantum Computing

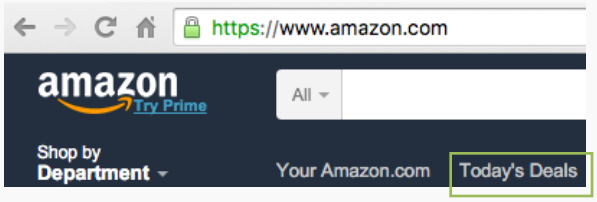
University of Waterloo

Ph.D. **PSU**

Internet citizens: are we safe?

Cybersecurity: integral part of safety for individuals, organizations and society!

Cryptography: a pillar of cybersecurity



- ✓ Is this really Amazon?
- ✓ Is my password secure?
- ✓ How about credit card info.?

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, …

Other things to worry: implementation, design, hardware, users…

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

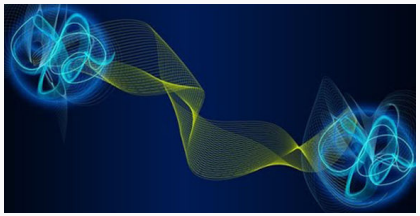
Physicists: quantum weirdness

Quantum **superposition**

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

Quantum Entanglement

- Non-classical correlation



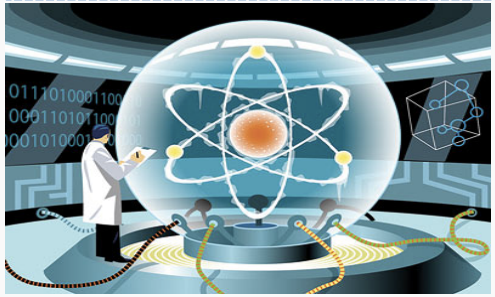
"Spooky action at a distance"

– A. Einstein

Computer scientists

Qubit

$\alpha|0\rangle + \beta|1\rangle$



Quantum

gates & circuits

? What does it mean for Cryptography?

1 Quantum attacks: 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

- Lattice-based, code-based, …

Question: are new candidates quantum-safe?

2 Quantum attacks: invalidate classical framework

Alert: unique quantum attacks

∃ information-theoretically secure protocol
Broken[b] by quantum entanglement!
(vs. shared randomness) [b][CSST11]

This can happen now!
(Technology available)

Crypto schemes ?

Lattices, …

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

Need: Re-examine every link against quantum attackers

Question: How to obtain quantum-safe cryptosystems?

My work on quantum-safe classical crypto

a.k.a. Post-Quantum Cryptography

Classical crypto against quantum attacks

1 Design efficient quantum algorithms[2,3,5]

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

2 Acquire quantum-safe crypto-systems

Security model[6,8]

Construction & analysis[1,4,6,7,8]

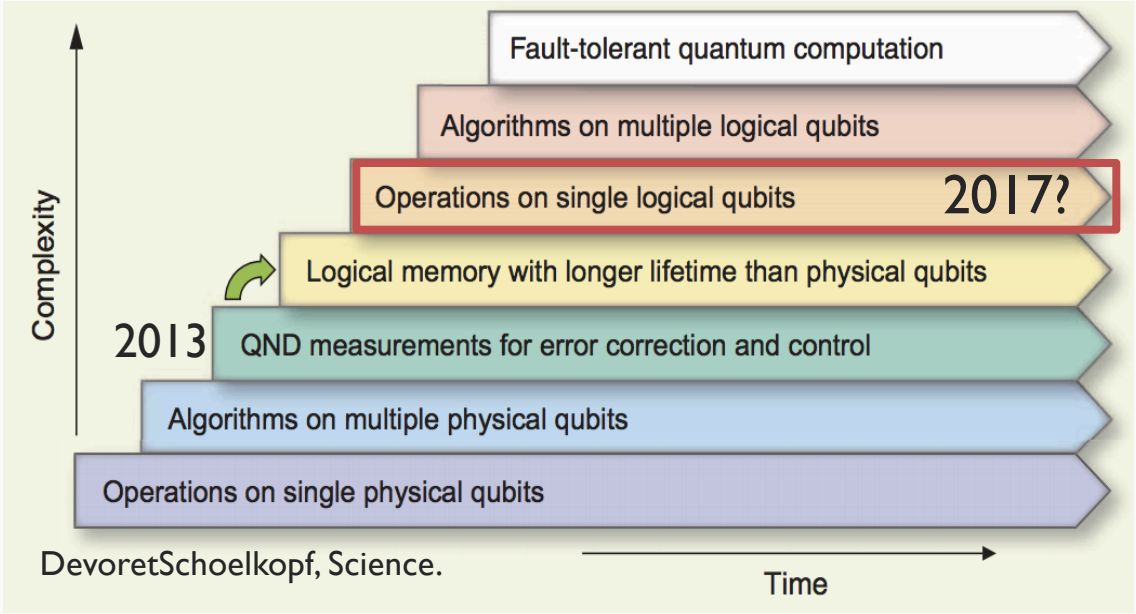
- Characterize "quantum-friendly" analyses[6,8]
- Construct quantum-secure 2-party computation protocols[7,8]
- Establish quantum security of hash functions[1,4,6]
  - Generic proof techniques for hash-based schemes

[2]SODA16
[3]CACR15
[5]STOC14, QIP15

[1]PKC16
[4]TQC15
[6]PQCrypto14
[7]TCC13
[8]Crypto11,QIP11

How far is a quantum computer away?

- Hardware



UCSB + Google

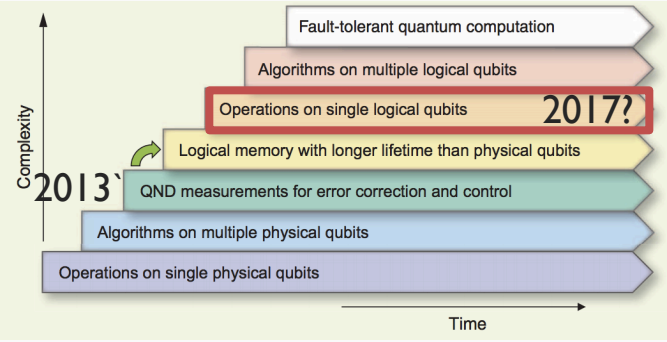
IBM

…

- Optimize quantum circuits

Microsoft QuArc | Intel | Niels Bohr Institute …

Any quantum ingredient could be a threat

	Task	Need	Availability
1	Run quantum factoring algorithm (to break public key crypto)	Full-scale fault-tolerant QC 	
2	**Quantum attack classical crypto**	Ex. Quantum entanglement 	**Available now** How to Build Your Own Quantum Entanglement Experiment, Part 1 (of 2)

Concerned voices

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

Post-Quantum Cryptography:
NIST's Plan for the Future

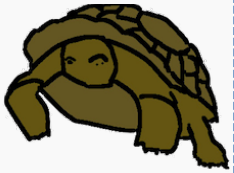
ETSI

3rd ETSI/IQC Workshop on Quantum-Safe Cryptography

5-7 OCTOBER 2015

European Telecommunications Standards Institute

PQCRYPTO
ICT-645622



CISCO

Next Generation Encryption updates regarding quantum computers

PQChat

Your Post-Quantum Secure Messenger

NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA

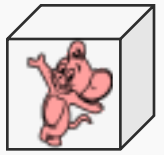
Aug 19, 2015, www.nsa.gov/ia/programs/suiteb_cryptography/

"… Currently, Suite B cryptographic algorithms are specified by the National Institute of Standards and Technology (NIST) and are used by NSA's Information Assurance Directorate in solutions approved for protecting classified and unclassified National Security Systems (NSS). Below, we announce preliminary plans for transitioning to **quantum resistant algorithms**."

Quantum cryptography: another strategy

Wiesner's mouse

Let's play quantum too!



- Make **classically impossible** possible
  - Ex. Quantum Key Distribution against **unbounded** eavesdropper
- Protect **quantum** information
  - Ex. Encrypt quantum secrets

Technology ready: commercial QKD products available

My work on quantum cryptography

- Construct quantum protocols, classically **impossible**[7]

[7]TCC13

- Construct zero-knowledge proof systems for Quantum NP*

*Preprint'BJ**S**W16

The triumph of zero-knowledge proof, classically


The Knowledge Complexity of Interactive Proof-Systems

(Extended Abstract)

Shafi Goldwasser MIT
Silvio Micali MIT
Charles Rackoff University of Toronto

2012 ACM A.M. Turing Award

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

Summary of my main work

a.k.a. Post-Quantum Cryptography

Classical crypto against quantum attacks

1 Design efficient quantum algorithms[2,3,5]

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

2 Acquire quantum-safe crypto-systems

Security model[6,8] | **Construction & analysis**[1,4,6,7,8]

- Characterize "quantum-friendly" analyses[6,8]
- Construct quantum-secure 2-party computation[7,8]
- Establish quantum security of hash functions[1,4,6]
  - Generic proof techniques for hash-based schemes

[2]SODA16
[3]CACR15
[5]STOC14, QIP15

[1]PKC16
[4]TQC15
[6]PQCrypto14
[7]TCC13
[8]Crypto11, QIP11

Quantum crypto

3 Design quantum cryptographic schemes

- Show more quantum protocols, classically impossible[7]
- Construct zero-knowledge proof systems for Quantum NP*

*Preprint'BJSW16

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**

- Establish quantum security of hash functions[1,4,6]
  - Generic proof techniques for hash-based schemes

A little later

1

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-based cryptosystems believed quantum safe before

QUANTA MAGAZINE

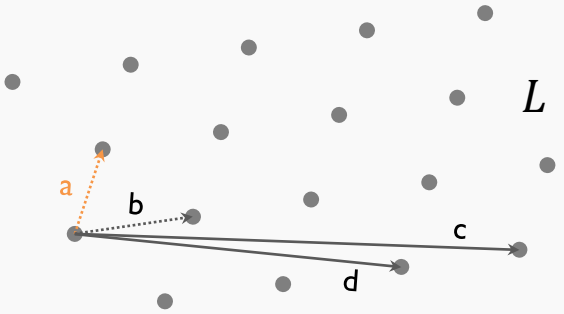
CRYPTOGRAPHY

A Tricky Path to Quantum-Safe Encryption

Lattice-based Cryptography

- Lattice problems
  - Shortest vector problem, …

Believed hard even for quantum computers



- A neo-tree of crypto grows

One-way function, signature

Public-key encryption, ID-based encryption

Fully homomorphic encryption,
program obfuscation …

Breaking some lattice crypto

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

- Short-PIP based cryptosystems are **broken!**

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

Our quantum alg's find A generator

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

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]

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

- Establish quantum security of hash functions[1,4,6]
  - Generic proof techniques for hash-based schemes

A little later

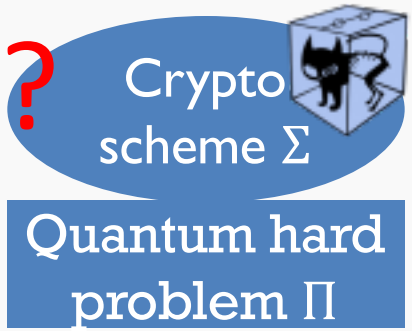
2

Recall: classical security framework fails

✗ Security model inadequate for quantum attackers

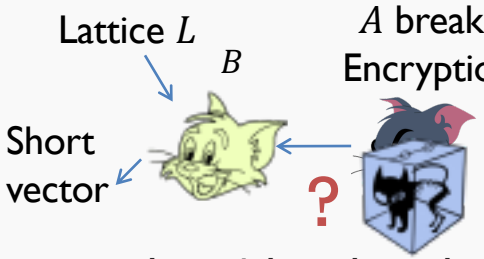
➡ Quantum security models: Still at early stage[6,8]

[6] S'14
[8] HSS'11'15



✗ Classical proofs can **fail** against quantum attackers

- Many PostQuantumCrypto only consider classical attackers in proofs

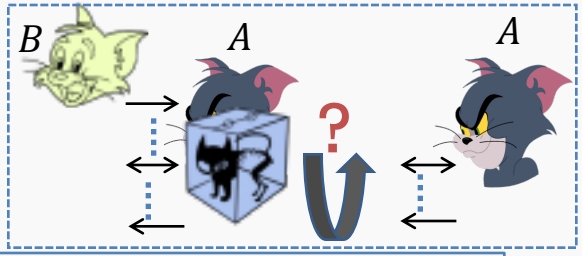


Assume attacker A breaks scheme Σ,
→ Construct B from A solving hard problem Π.

2

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



Only special cases possible[g]

[g][Watrous09]

[7]TCC13

[8]Crypto11,QIP11

Quantum secure protocols?	Our work[7,8]
Zero-knowledge proof of knowledge	✓ New constructions
Secure 2-party computation	
Constant-round zero-knowledge	?
…	

2

II. Hash function: common heuristic fails?

- Hash functions are everywhere:

Signature, message authentication, key derivation, bitcoin,…

- The Random Oracle (RO) heuristic widely used
  1. Proving security properties of hash functions
     - "Lazy" sampling: decide $H(\cdot)$ on-the-fly
     - **Trivial**: H is one-way, target-resistant, …
  2. Program RO: change $H(\cdot)$ adaptively
     - Ease security proof of hash-based schemes (otherwise **impossible**)

x $H(x)$

Hash Function H

$\Sigma_x|x\rangle$ $\Sigma_x|x\rangle|H(x)\rangle$

- A quantum-accessible Random Oracle

Nothing seems to work

2

Our contributions

1. Prove security properties against superposition attacks[1]

- 2nd-preimage resistance, target-resistance, multi-target, multi-function variants, …
- Extend quantum query complexity to cryptographic setting

[1][HRS'PKC16]

worst-case	average-case
Goal: big (constant) success prob. impossible	Goal: **any** small (noticeable) success prob. impossible

- **Application**: improve efficiency of post-quantum hash-based signature

2. Program a **quantum** Random Oracle, adaptively[1,4]

- General proof techniques, useful in many hash-based schemes
- Ex. making signature schemes strongly unforgeable

[4][ES'TQC15]

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**

- Establish quantum security of hash functions[1,4,6]
  - Generic proof techniques for hash-based schemes

Now it's time! ← A little later

Where our algorithms start

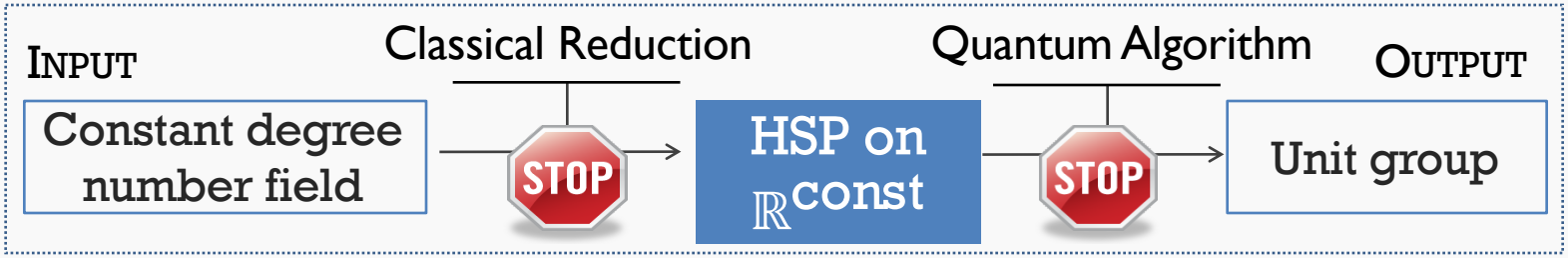
Goal: compute the unit group of an arbitrary degree number field

The Hidden Subgroup Problem (HSP) framework

- Captures most quantum exponential speedup

Challenges from constant to high degree

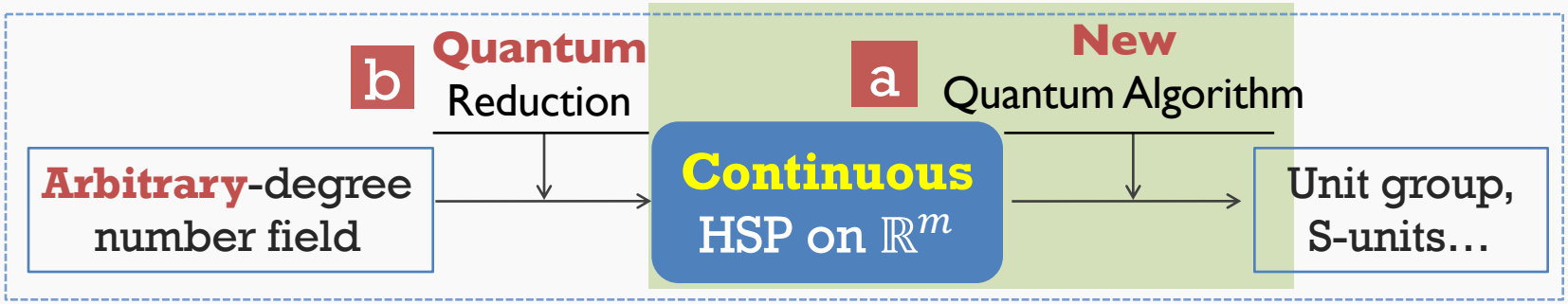
- Previous **Constant**-degree unit-group algorithms* *[Hallgren'02'05,SV05]



- Fail in **high**-degree:
  - Reduction running time exponential in degree
  - Resulting HSP instance difficult to solve

1

Our algorithms for **arbitrary** degree



b Use quantum power in reduction already

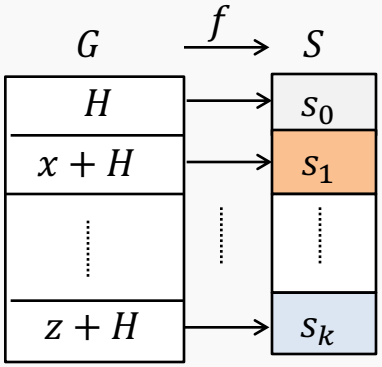
Bonus: a canonical quantum representation for real-valued lattices

- Unknown classically

a A new algorithmic framework

Hidden Subgroup Problem (HSP)

- 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.

- Our Continuous HSP[3] on $\mathbb{R}^m$ (Earlier defs. only suitable for constant m)

Given: $f: \mathbb{R}^m \to S$

1. Periodic on H
2. Injective on $\mathbb{R}^m/H$ (approximately)
3. Lipschitz continuous*

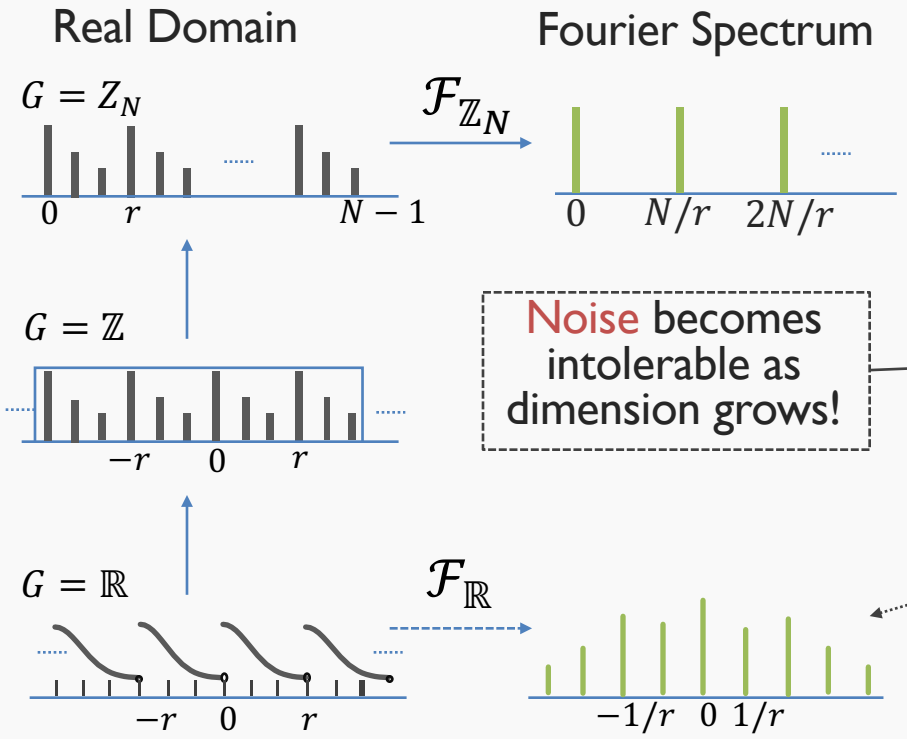
[3] [EHKS'STOC14]

* $\left|\left|f(x) - f(y)\right|\right| \leq a \cdot \left|\left|x - y\right|\right|$

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

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

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

- Discretize & Truncate
- Reduce to finite G

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

- Informal: try to approx. sample the ideal Fourier spectrum directly!
- **Continuity** condition crucial

Interesting HSP instances

Computational Problems	HSP on G
Factoring	$\mathbb{Z}$
Discrete logarithm	$\mathbb{Z}_N \times \mathbb{Z}_N$
Problems in constant-degree fields	$\mathbb{R}^{const}$
Our work: **arbitrary**-degree n	Continuous $\mathbb{R}^{O(n)}$

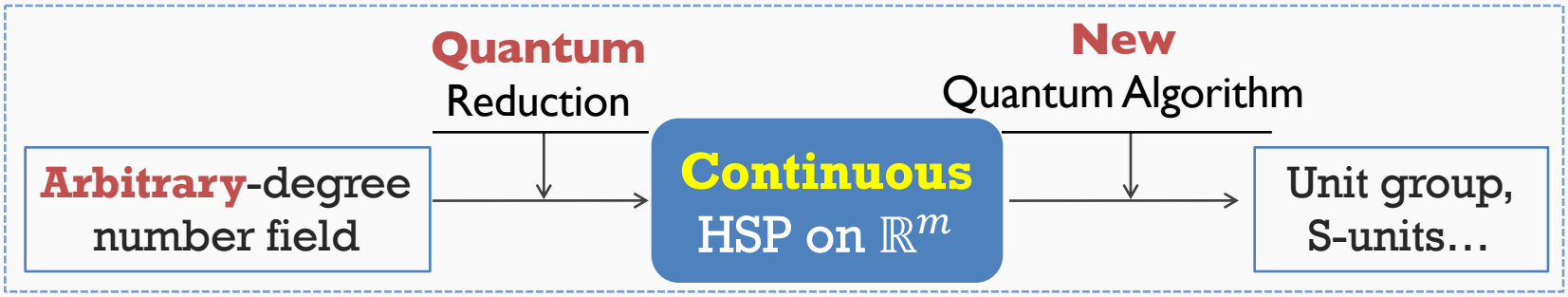
Abelian groups
∃ efficient quantum algs

Graph isomorphism	Symmetric group
Unique shortest vector problem	Dihedral group

Non-abelian
Open question:
? efficient quantum algs

1

Our Algorithms



- New quantum algorithmic tools
- Break several lattice-based cryptosystems believed quantum safe

Future work

Post-quantum crypto

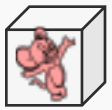
Quantum crypto

Keep up crypto with evolving technology

Power of quantum computing

Future work

Post-quantum crypto



Quantum crypto

i. Are quantum-safe candidates indeed hard?

ii. What crypto-systems are quantum safe?

iii. What are possible? A formal foundation?

i

- Breaking other lattice problems: Ring-LWE, NTRU, …

ii

- "White-box" analysis of hash functions
- Efficient secure computation protocols
- Quantum-safe Bitcoin
  - Both block chain & trans. signature **insecure** against quantum

iii

- Quantum money, quantum FHE…

Future work

Keep up crypto with evolving technology

i. Crypto for BIG DATA
ii. Cope with diverse players
iii. Crypto against mass surveillance

- Update security model with network architecture
  - Poly-time adversary is too coarse!
- Design protocols that better fit
  - Workload respects capability

Security in Cloud/Fog computing & Internet of Things

Future work

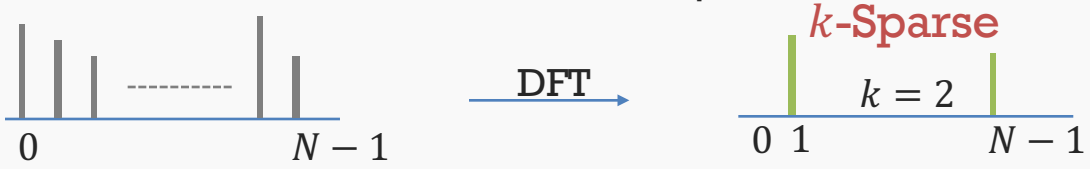
Power of quantum computing

i. Quantum algorithms for BIG DATA
ii. Limits of quantum computing
iii. Nature of computation & quantum theory

- Standard Quantum Fourier Transform
  - Exponentially faster than classical FFT algorithm
  - using one quantum sample of input data

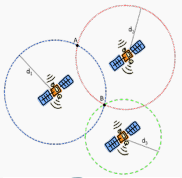
? Sparse QuantumFT

- Even faster with few classical samples?

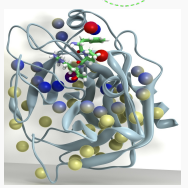


- Sparse FT: many apps in data analysis

Magnetic Resonance Imaging



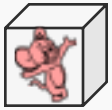
GPS



Nuclear Magnetic Resonance

Courtesy: MIT sFFT group

Post-quantum crypto



Quantum crypto

Keep up crypto with evolving technology

Power of quantum computing

Thank you!