04/22/2021
@ISQA 486/585

“Better watch out, Crypto”, says quantum computing

Fang Song
Computer Science
Portland State University

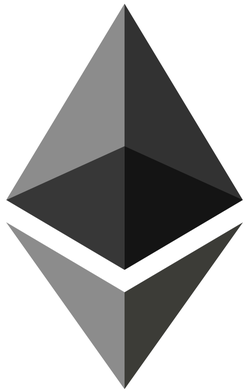
04/22/2021
@ISQA 486/585

a.k.a.

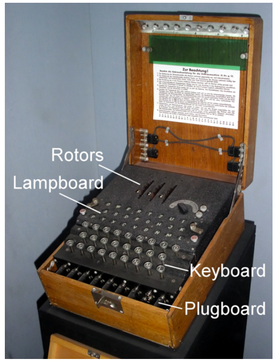
Quantum computing, its impact on cybersecurity, and more

Fang Song
Computer Science
Portland State University

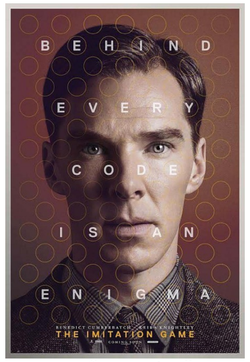
Everyone loves crypto



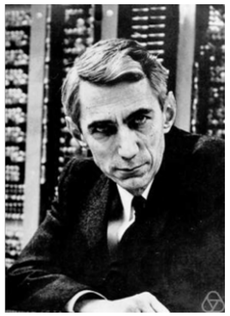
… but, not my crypto

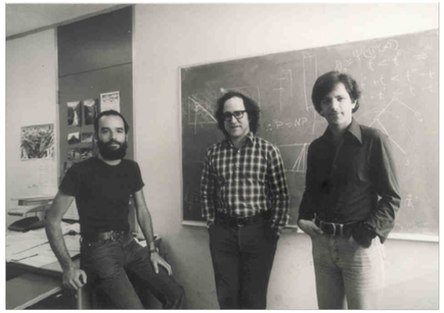


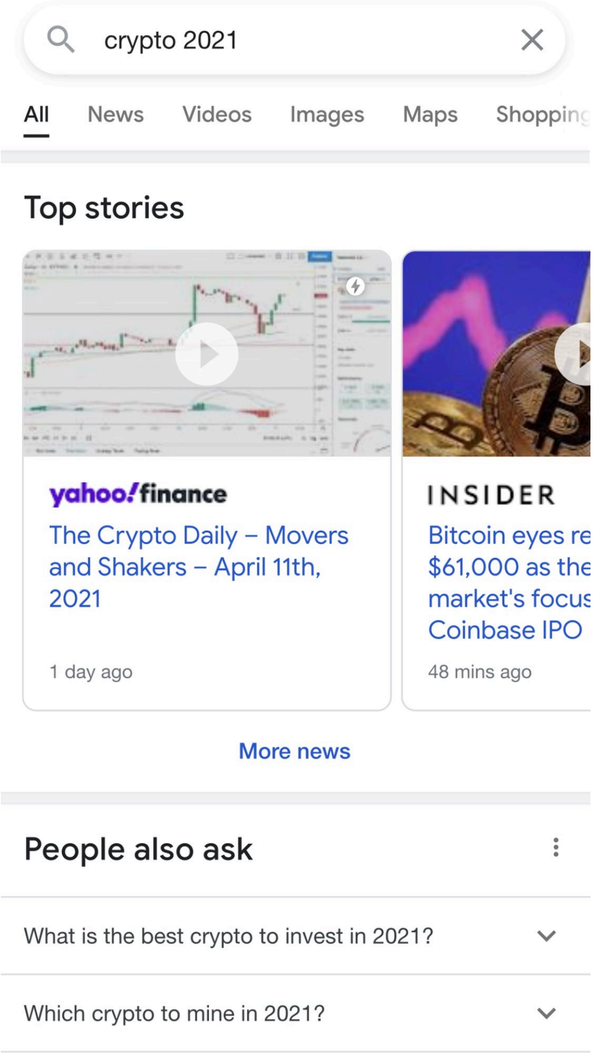
Alan Turing



Source: imdb

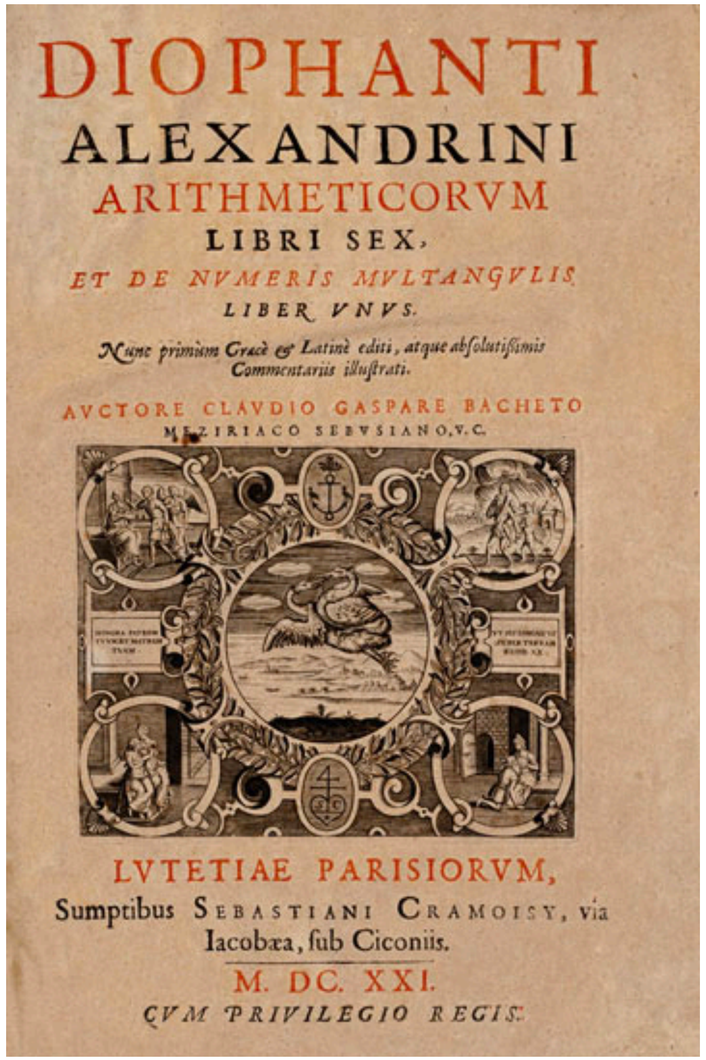






Modern Cryptography involves the study of mathematical techniques for securing {digital information, systems and computations} against adversarial attacks

An ancient problem, but still matters …


DIOPHANTI
ALEXANDRINI
ARITHMETICORVM
LIBRI SEX.
ET DE NVMERIS MVLTANGVLIS
LIBER VNVS.
Nunc primùm Græcè & Latinè editi, atque absolutissimis Commentariis illustrati.
AVCTORE CLAVDIO GASPARE BACHETO
MEZIRIACO SEBVSIANO, V.C.
LVTETIAE PARISIORVM,
Sumptibus SEBASTIANI CRAMOISY, via Iacobæa, sub Ciconiis.
M. DC. XXI.
CVM PRIVILEGIO REGIS.

Diophantine equation

$$ax^2 + by^2 = k$$

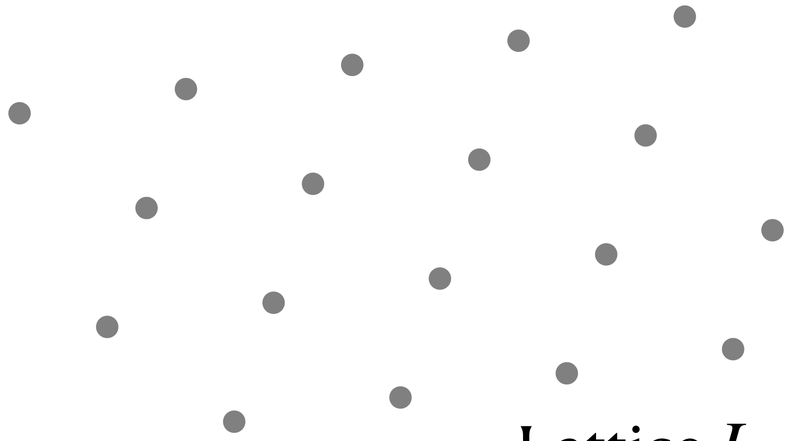
$$a, b, k, x, y \in \mathbb{Z}$$

Pell's equation

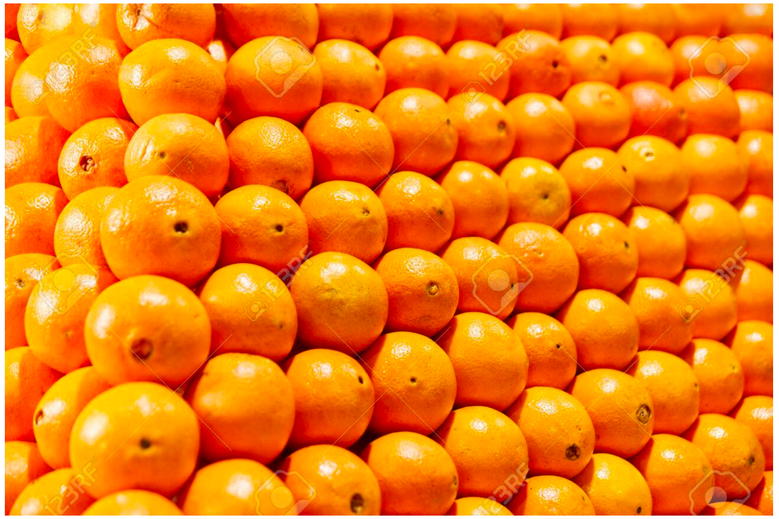
$$x^2 - dy^2 = 1$$

Lattices

- Solutions to Pell's equation form a lattice



Lattice L



Factorization

- **Multiplication** $3 \times 5 = 15$ $244176193 \times 176944583 = 43205654648912519$
- **Prime factorization** $N = p \times q$

$$15 = 3 \times 5 \qquad 5551468579728803 = 247252597 \times 224526199$$

$$\begin{aligned} &843002475649511842193612279762997050616506062956573779745859755522680385970 07 \\ &\times 776952340341598436718639700818347835362497022407857843873019621452481583262 89 \end{aligned}$$

- Best known algorithm (Number field sieve): ~ $2^{c(\log N)^{\frac{1}{3}}(\log\log N)^{\frac{2}{3}}}$ exponential time.
- Feb 28, 2020: RSA-250 (250 decimal digits = 829 bits) factored!

  Total computation time ~ 2700 core-years (Intel Xeon Gold 6130)

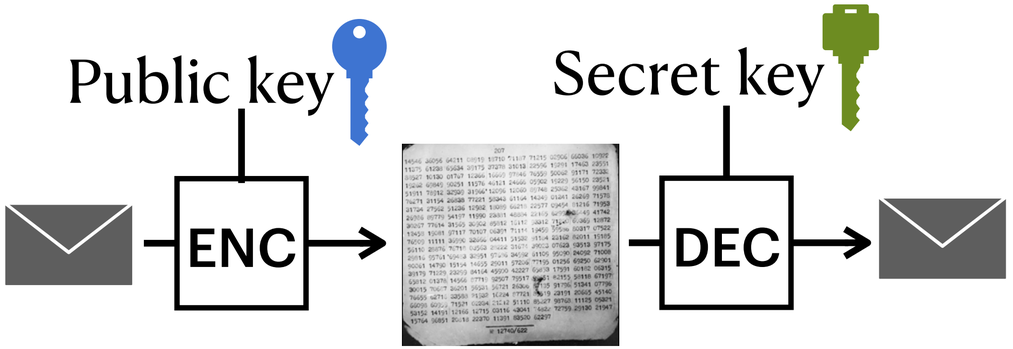
Fact. Solving Pell's eqn. helps with factorization. (Factoring* $\leq$ Pell's equation)

* almost all

Public-key cryptography based on factoring

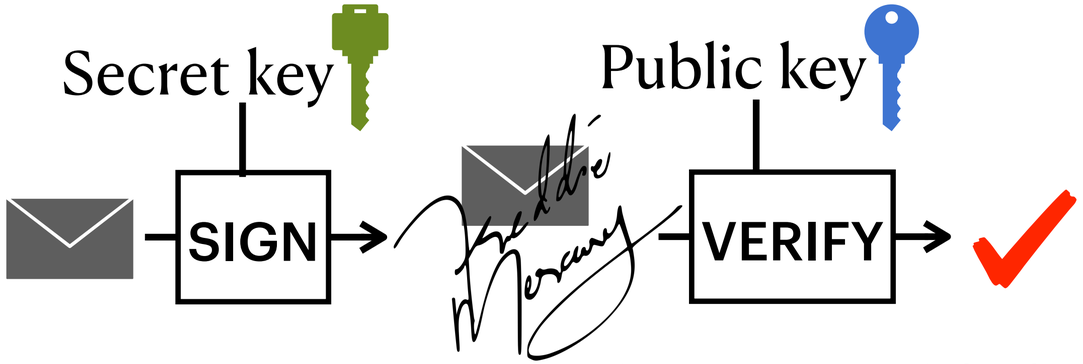
RSA

Public-key encryption



Secrecy: no one else can read

Digital signature



Authentication: no one else can modify/forge

Foundation of a secure cyberspace

[Cryptographic algorithms]

RSA, ECDSA, ...

Broken in a quantum world

Quantum computer can solve factoring etc. efficiently! ’1994

Peter Shor

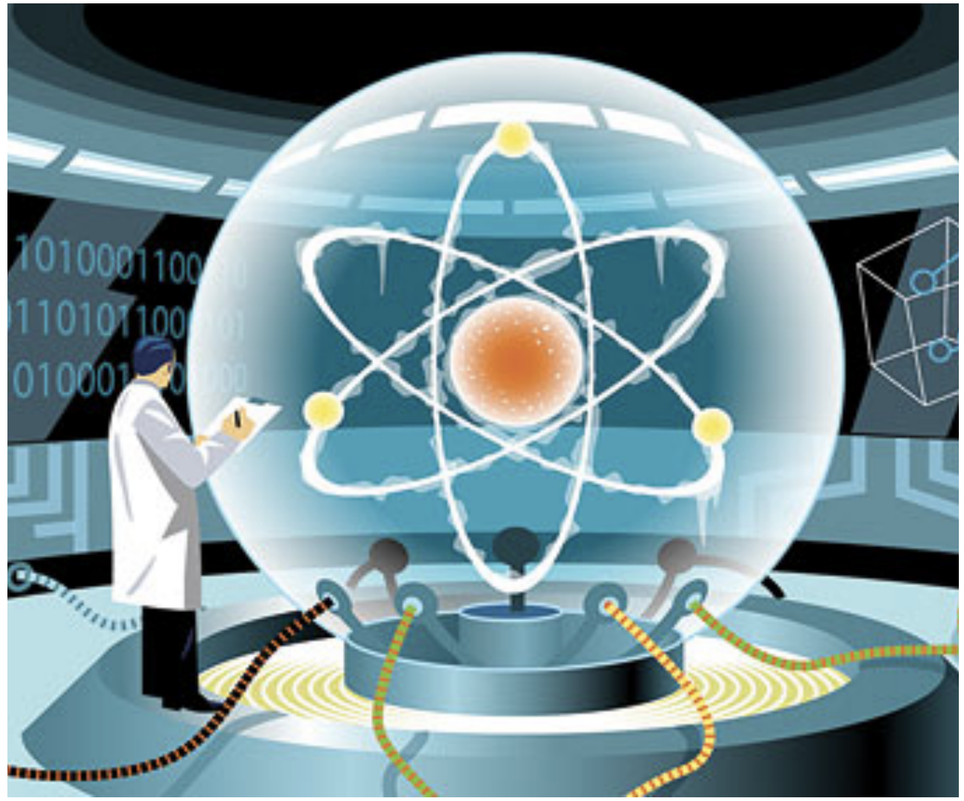
Alexei Kitaev

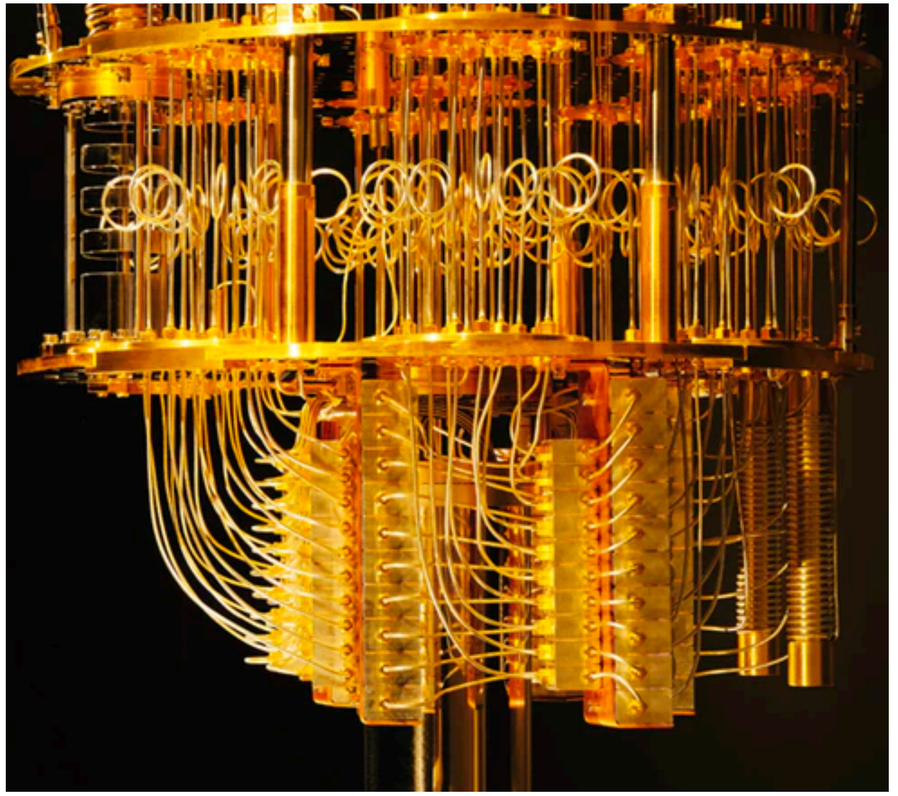
[Cryptographic algorithms]
RSA, ECDSA, …

This talk

1. Quantum threat to cryptography
2. Quantum computing 101
3. Migrating to post-quantum cryptography

What is a quantum computer





Quantum bits

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

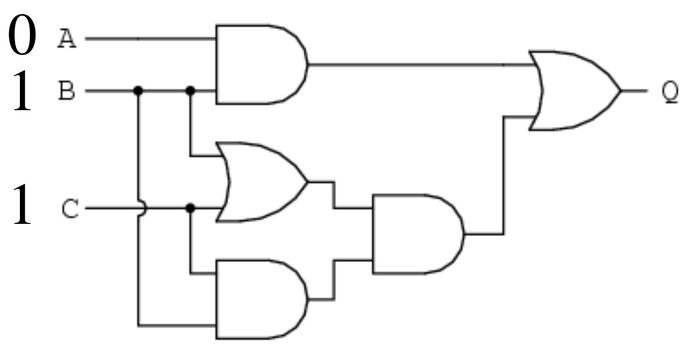
- **Quantum = Prob. theory ++**
  - Amplitudes $p_0, p_1 \in \mathbb{C}$ (negative OK)
  - $|p_0|^2 + |p_1|^2 = 1$ (ℓ_2- normalized)

Qubit

(Quantum superposition)

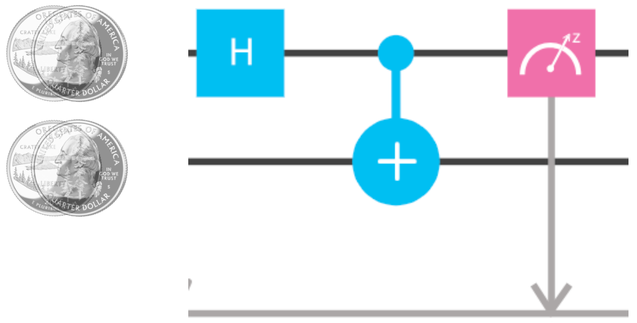
Quantum circuits

- **Classical computer**



Boolean gates and circuits

- **Quantum computer**



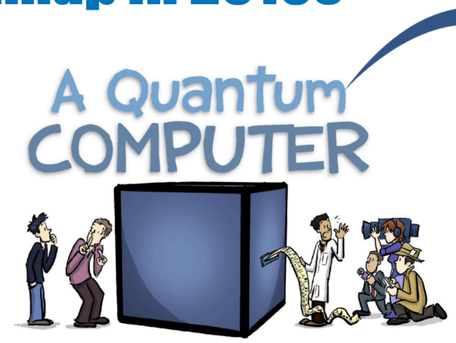
Quantum gates and circuits

What do we gain?

- Infeasible to simulate by a classical computer (300 qubits ~ 2^{300} bits to describe)
- Solve hard problems faster by constructive inference (≠ mass parallelism)

What's in the news?

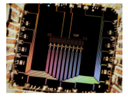
Roadmap in 2010s



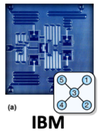
(2012)

Ion-Trap (UMD)

Super-conducting



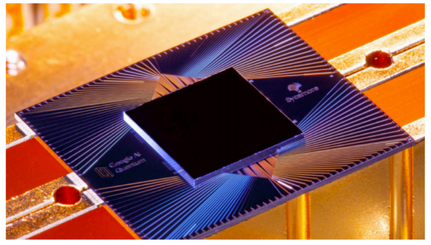
Google



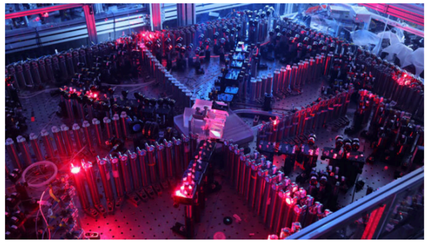
IBM

(2017)

(2019)



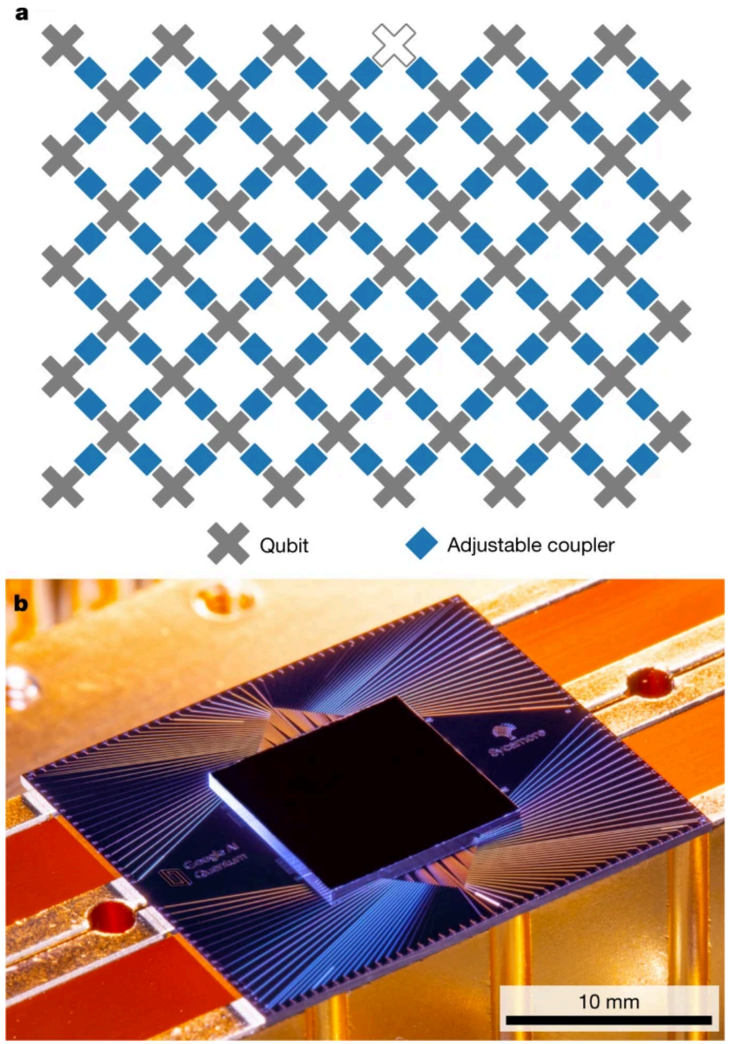
Google Supremacy: RCS (2019)



USTC: Boson Sampling (2020)

Curtesy of X. Wu

Quantum computational supremacy



Google's Sycamore chip, 2019

- **Goal**: use a quantum computer to solve some well-defined problems that would take orders of magnitude longer to solve with any currently known algorithms running on existing classical computers.
- Google's experiment: Random circuit sampling
  - 53-qubit super conducting chip
  - 200 seconds to sample a million times
  - 10,000 years on state-of-the-art classical supercomputer (IBM claims a few days suffice)

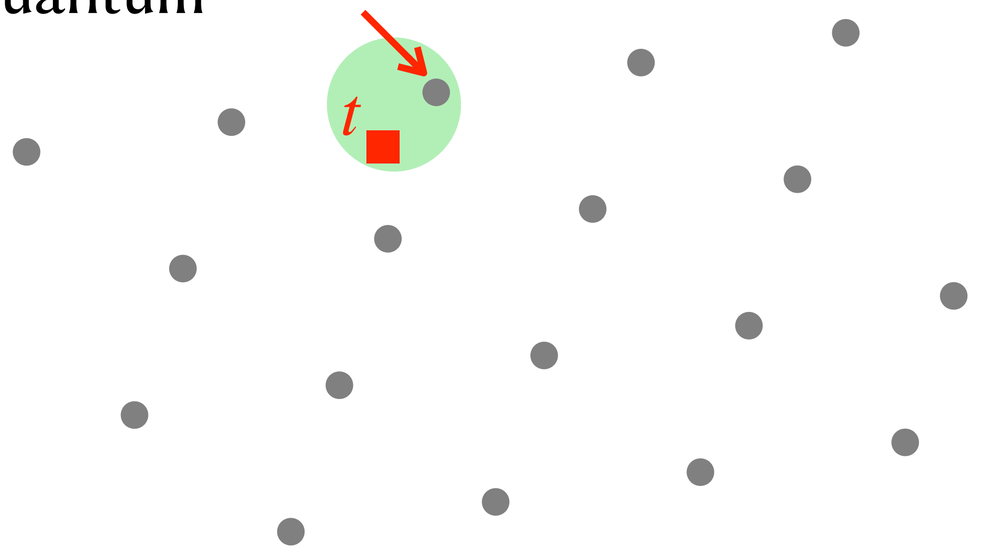
Scott Aaronson's FAQ: https://www.scottaaronson.com/blog/?p=4317

This talk

1. Quantum threat to cryptography
2. Quantum computing 101 &
3. Migrating to post-quantum cryptography

We've got lattices!

- Intractable problems (as dimension grows)
  - **CVP** (closest vector problem)
  - **SVP** (shortest vector problem) = closest lattice point to origin
  - Best algorithms take time 2^{cn}, classical or quantum



Lattice-based cryptography

Hash functions, digital signatures

Public-key encryption, ID-based encryption

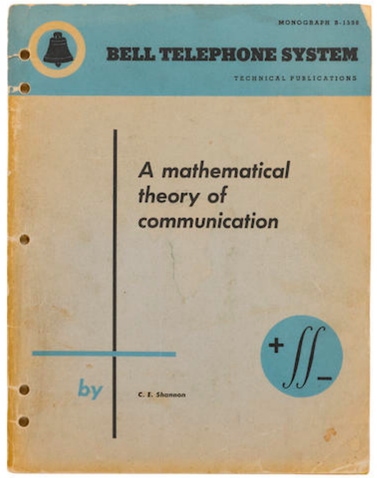
Fully homomorphic encryption, functional encryption,

Program obfuscation …

Lattice problems

More post-quantum candidates

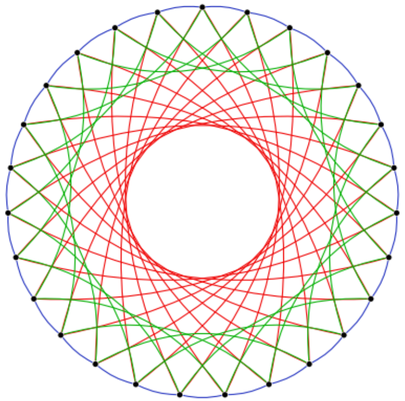
- **Coding theory**
  - McEliece PKE



- **Multivariate equations**
  - Rainbow signature

$$\begin{cases} y_1 = x_1x_2 + x_1x_3 + x_1x_5 + x_2x_5 + x_2x_6 + x_3x_5 + x_5x_6 \pmod p \\ y_2 = x_1x_3 + x_2x_4 + x_3x_5 \pmod p \\ y_3 = x_1x_3 + x_1x_5 + x_2x_3 + x_3x_4 + x_3x_6 + x_5x_6 \pmod p \\ y_4 = x_1x_2 + x_3x_5 \pmod p \\ y_5 = x_1x_3 + x_1x_4 + x_1x_5 + x_2x_4 + x_3x_4 + x_3x_6 \pmod p \\ y_6 = x_1x_3 + x_1x_4 + x_2x_3 + x_2x_5 + x_3x_4 + x_4x_5 + x_4x_6 \pmod p \end{cases}$$

- **(Elliptic-curve) Isogeny**
  - Supersingular-Isogeny-Key-Exchange (SIKE)



- **Hash-based signature.**
  - XMSS (RFC8391), LMS (RFC8554)

Yes, this is serious business

"... we announce preliminary plans for transitioning to quantum resistant algorithms." **Aug 19, 2015**

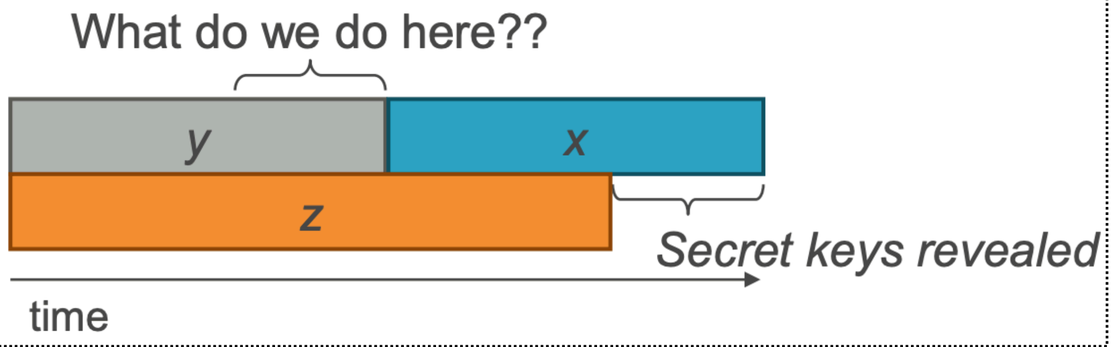
www.nsa.gov/ia/programs/suiteb_cryptography/

- **How soon do we need to worry?**
  - x: time your data needs to be safe
  - y: time to transit to quantum-safe infrastructure

  - z: time to build a full-scale quantum computer

Mosca's theorem

Theorem 1: If $x + y > z$, then worry.



NIST post-quantum crypto standardization

https://csrc.nist.gov/projects/post-quantum-cryptography

- **Scope**
  - Digital signatures
  - Public-key encryption / Key-encapsulation Mechanism
- **Expected outcome**
  - A few algorithms rather than a single winner (unlike AES, SHA-3)
- **Evaluation criteria**
  - Security, performance, other features (e.g., drop-in replacement)

NIST PQC standardization - Timeline

- It takes time, for sure
  - 2006 – 1st PQCrypto conference in Leuven, Belgium
  - 2009 – NIST PQC survey Quantum Resistant Public Key Cryptography: A Survey [Perlner, Cooper]
  - 2012 – NIST begins PQC project
  - Apr 2015 – NIST Workshop on Cybersecurity in a Post-Quantum World
  - Aug 2015 – NSA announcement
  - Feb 2016 – NIST Report on PQC (NISTIR 8105)
  - Feb 2016 – NIST announcement of "competition-like process" at PQCrypto in Japan
  - Dec 2016 – Final requirements and evaluation criteria published
  - Nov 2017 – Deadline for Submissions
  - Dec 2017 – Round 1 begins – 69 candidates accepted as "complete and proper"
  - Apr 2018 – 1st NIST PQC Standardization Workshop
  - Jan 2019 – Round 2 candidates announced
  - Aug 2019 – 2nd NIST PQC Standardization Workshop

July 22, 2020	Third Round Candidates announced (7 Finalists and 8 Alternates)
October 1, 2020	Deadline for updated submission packages for the Third Round
2022/2024	Draft Standards Available

https://csrc.nist.gov/Projects/post-quantum-cryptography/round-3-submissions

NIST PQC standardization - 3rd round contenders

- **Public-key Encryption and Key-establishment Algorithms**
  - Classic McEliece (Code-based)
  - CRYSTALS-KYBER (Lattice-based)
  - NTRU (Lattice-based)
  - SABER (Lattice-based)
- **Digital Signature Algorithms**
  - CRYSTALS-DILITHIUM (Lattice-based)
  - FALCON (Lattice-based)
  - Rainbow (Multivariate-equation-based)

July 22, 2020

NIST PQC standardization, stay tuned

- Mailing list: pqc-forum@list.nist.gov

Email List

NIST has set up a **pqc-forum@list.nist.gov** mailing list. The mailing list will be used to discuss the standardization and adoption of secure, interoperable and efficient post-quantum algorithms.

You must be subscribed to send email to the mailing list. Please use the instructions below to subscribe.

To join:

mailto:pqc-forum+subscribe@list.nist.gov

You will receive a response message from jupyter+subconfirm@list.nist.gov. Please click the "Join" link inside that email to confirm your subscription request.

To unsubscribe:

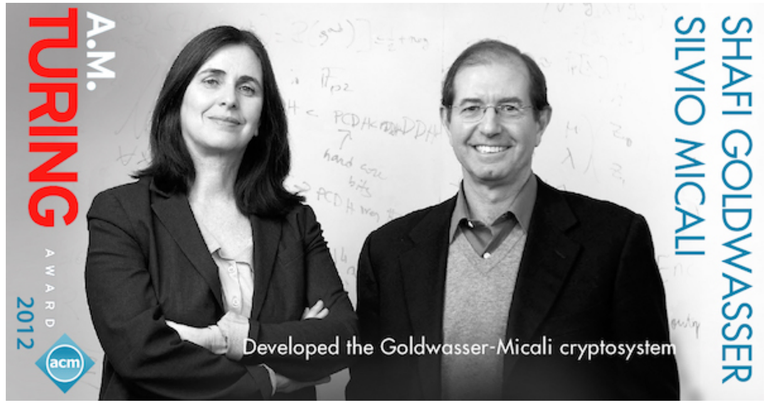
mailto:pqc-forum+unsubscribe@list.nist.gov

A cautionary tale

- **An unexpected quantum break of some lattice crypto**
  - These systems assume a high-dimension generalization of Pell's equation is hard to solve.
  - My work gives an efficient quantum algorithm for this generalized problem. [EHKS14,BS16]
- **Hardness of the PQC candidates needs more scrutiny by more people**

Another “invisible” issue

The formal framework of modern cryptography needs “retrofitting”



“... created mathematical structures that turned cryptography from an art into a science”

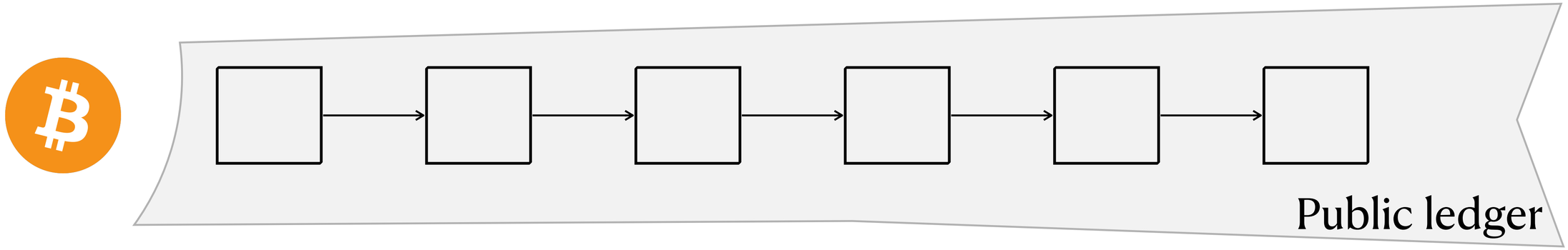
Crypto schemes

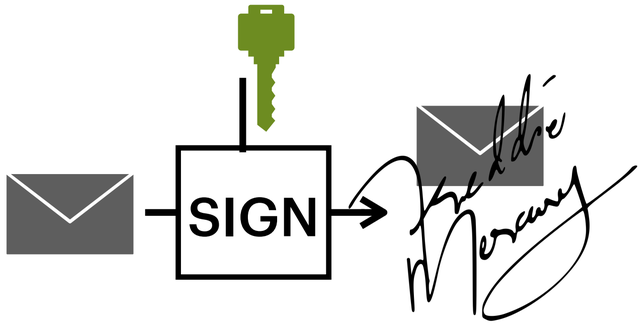
Hard problems

Can’t claim quantum security of a crypto scheme, solely because it builds on a quantum hard problem

Find out more in my talk at PQCAsia forum 2016 YouTube

Enough, should I sell my crypto(currency)?



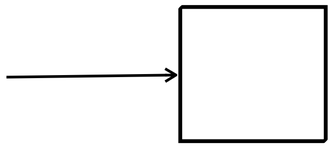


Elliptic-Curve Digital Signature Algorithm (ECDSA), Schnnor signature

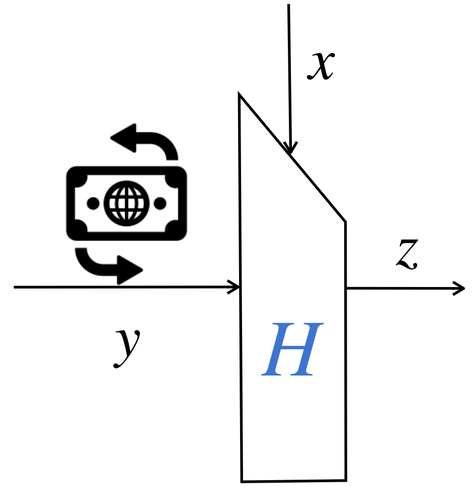
Broken by quantum computers

Recommendation:

Upgrade to post-quantum signatures (hash-based, ...)

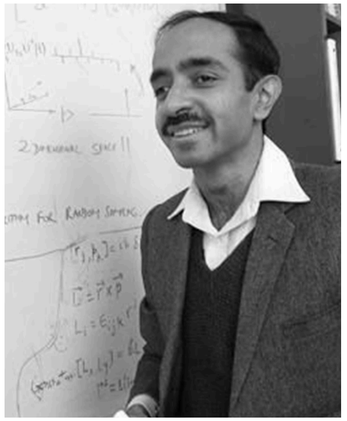


How about the blockchain?



- How to generate a block: Proof-of-Work (PoW)
  - H: cryptographic hash function (SHA-256)

    Compress a long input to a random short digest ($\leq$ N).
  - PoW: find x, such that $H(x; y) = z \leq T$ (hardness threshold)
  - Cost: ~ N/T evaluations of H.
- A good chain: need honest majority hashing power
- Malicious miners with quantum computers?
  - Grover's quantum search algorithm solves PoW faster ~ $\sqrt{N/T}$
  - Further investigation is challenging and undergoing arXiv:2012.15254



QC: prospects & broader impacts?

Quantum cryptography

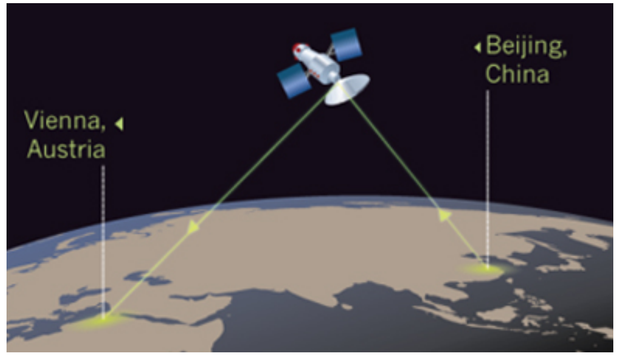
Honest users can harness quantum capability too

- **Quantum-Key-Distribution (QKD)** [BB84,E91]
  - Secure against computationally unbounded eavesdroppers
  - Impossible by classical communication alone
- **Protect quantum information**
  - Encrypt and authenticate quantum data …
- **Technology is maturer than full QC**

idquantique.com

Quantum Internet

… a pan-European Quantum Internet by ground-breaking technological advances. **1b€, 10 years.**



Micius quantum satellite. **QUESS** project (**Qu**antum**E**xperiments at **S**pace**S**cale)

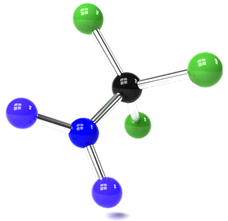
The President's Budget includes $25 million for the Department of Energy Office of Science to support early stage research for a quantum internet. … improving the security of our communications … **FY21.**

(noisy intermediate-scale quantum)
NISQ era and beyond

Quantum simulation

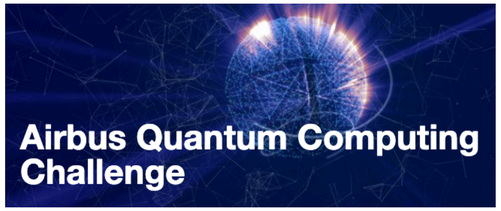
Origin of a “quantum computer”, proposed by Richard Feynman in 80’s

- Energy efficient fertilizer: 1.2% of the world’s total energy
- Drug discovery
- …



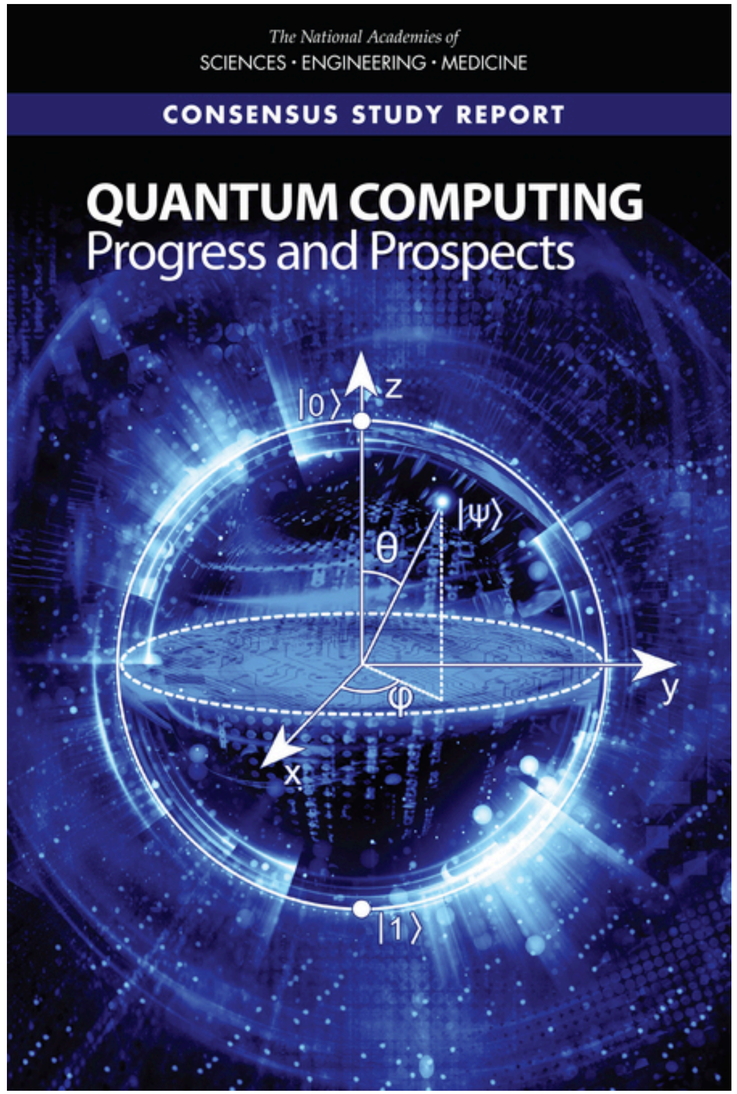
Quantum optimization

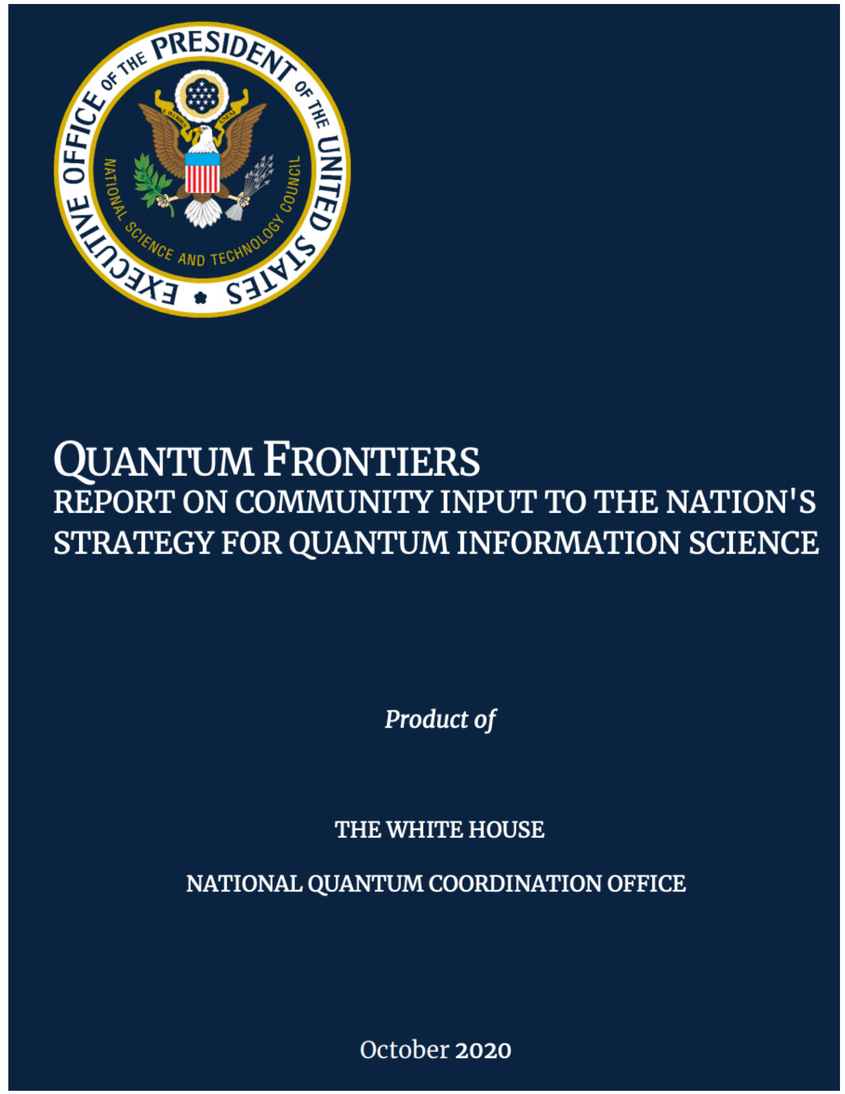
e.g., variational quantum methods



Quantum sensing

Read more …





Thanks!

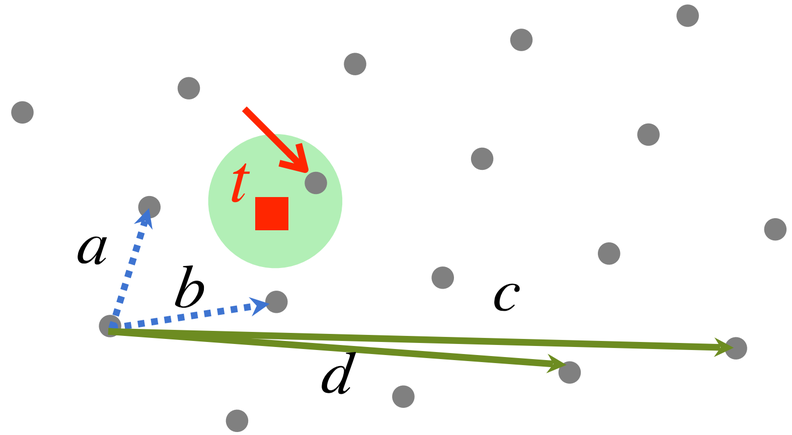
Scratch

Supplement

A toy (insecure) signature scheme [GGH97]

Public key: a bad basis B

Secret key: a good basis A



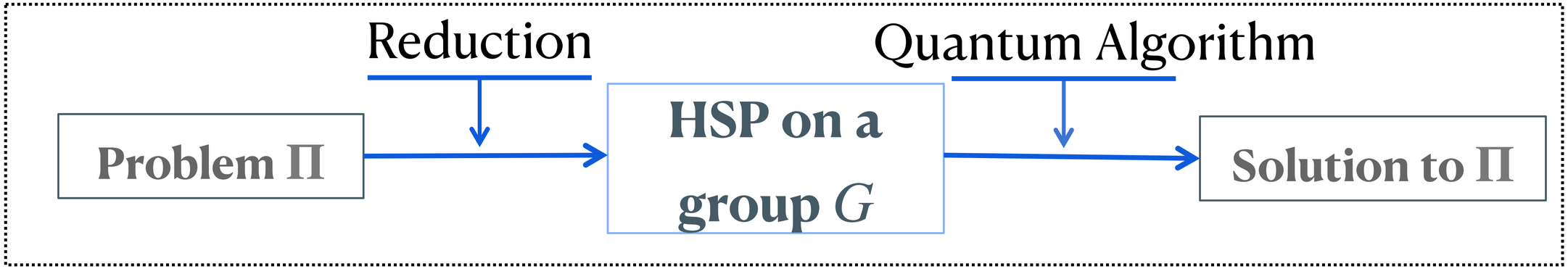
Signing: on msg $t \in \mathbb{R}^n$, use good basis to find closest $v \in L$.

Verification: on (t, v), verify $v \in L(B)$ and $\|v - t\|$ small.

Forging a signature is difficult ($\approx$ CVP) without a good basis

- Unfortunately, the signatures reveal information about the good basis
- Nonetheless, lattices appear well suited to construct cryptography

Hidden subgroup problem (HSP)

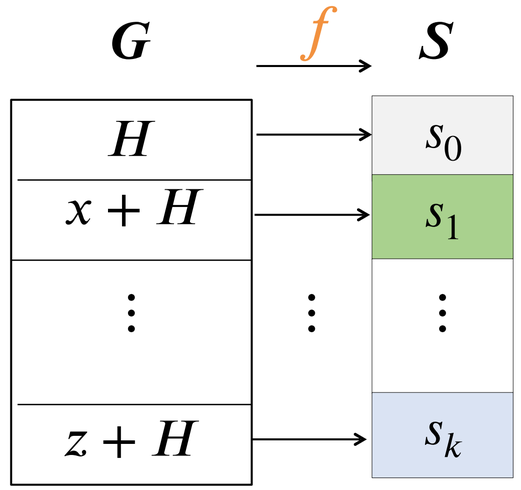


- **Standard HSP on finite group G**

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

$$f(x) = f(y) \text{ iff. } x - y \in H$$

Goal: Find H with few evaluations of f.



- **Continuous $\mathbb{R}^n$ is tricky. We've found a solution [EHKS14]**

Interesting HSP instances

Computational Problems	HSP on G
Factoring	$\mathbb{Z}$
Discrete logarithm	$\mathbb{Z}_N \times \mathbb{Z}_N$
Pell's equation	$\mathbb{R}$
PIP etc.	Continuous $\mathbb{R}^n$
Graph isomorphism	Symmetric group
Unique shortest vector	Dihedral group

Abelian groups
∃ efficient quantum algs

Non-abelian
efficient quantum algs unknown