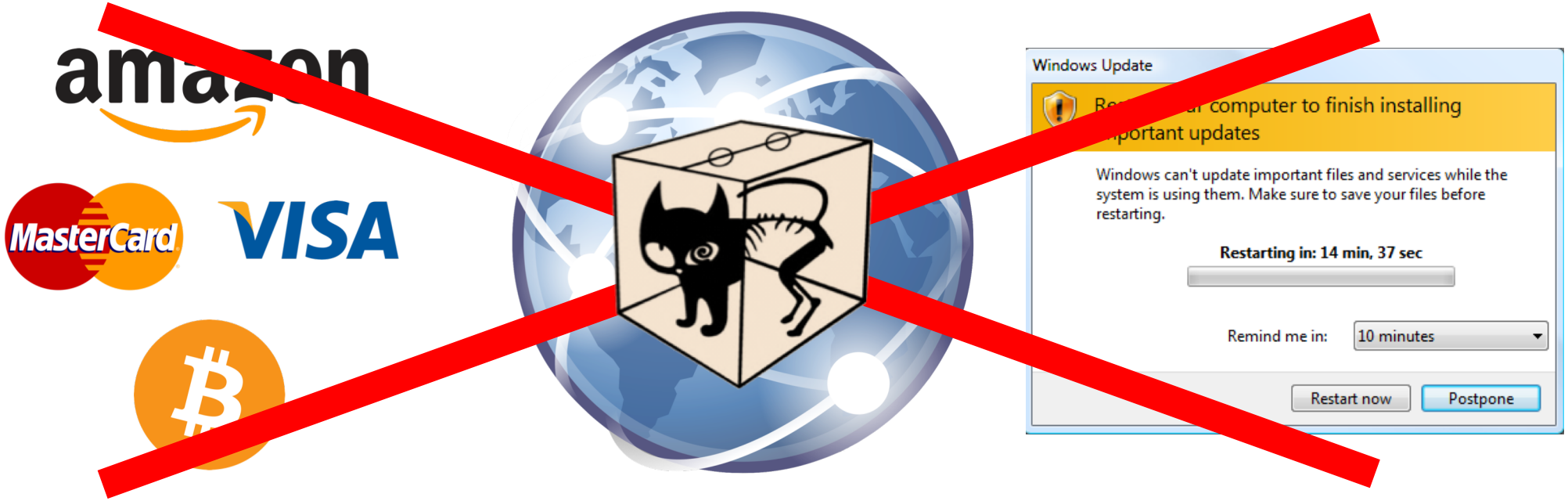
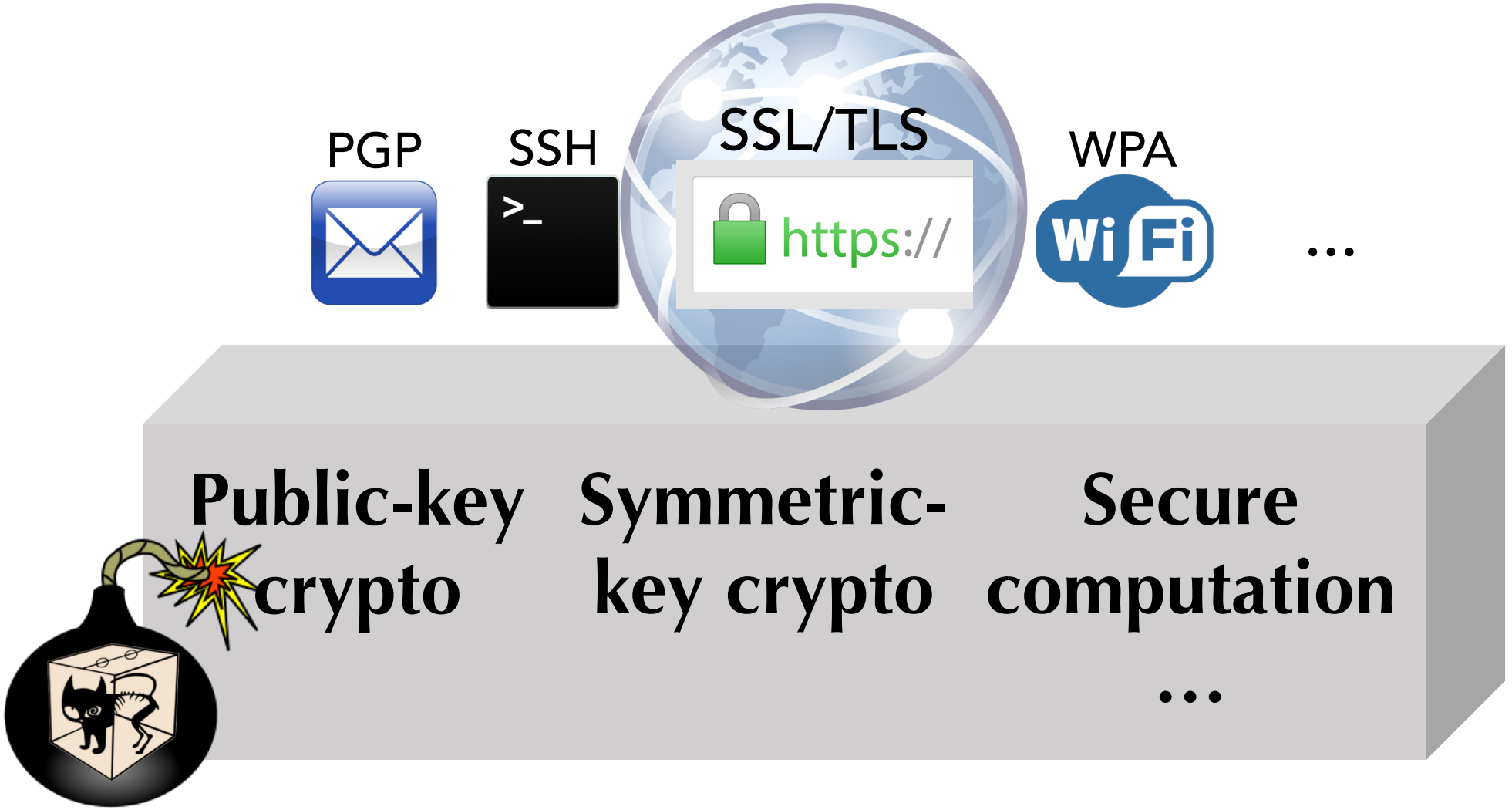
Quantum-safe cryptography

Secure Internet will be shattered by quantum computers in x years



Break at a foundation: Cryptography



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)

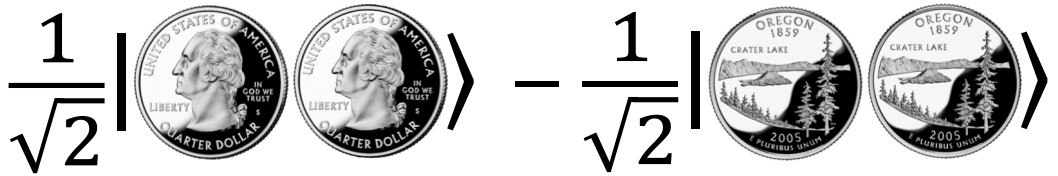
Physicists: Quantum weirdness

- Quantum Superposition
  - →No-cloning of unknown QState

Qubit

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

- Quantum Entanglement
  - (A non-classical correlation)



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

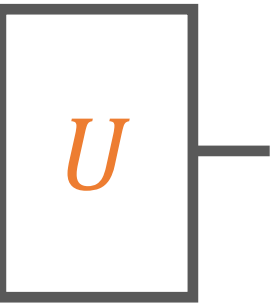
Computer scientists: a novel computer?

Build a quantum computer

Qubits

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

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

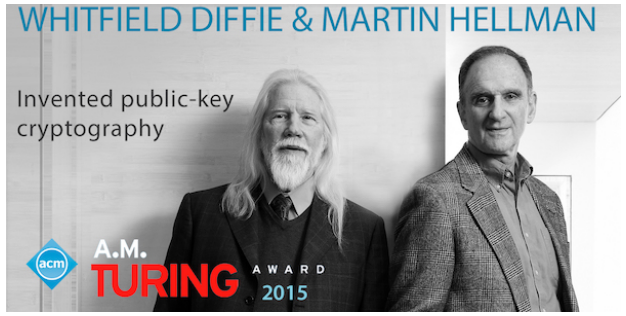


Quantum
gates & circuits

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

How do quantum attackers break cryptography?

1. Crack hard problems

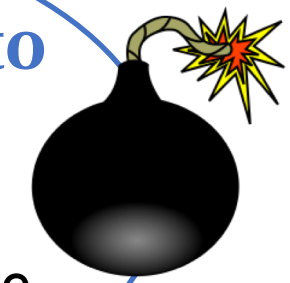


Assumption: (better be) hard to solve

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 → 1 Build on alternative problems

Security framework failed → 2 Quantum security framework

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)

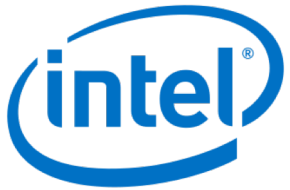
G. Kalai (Hebrew U)

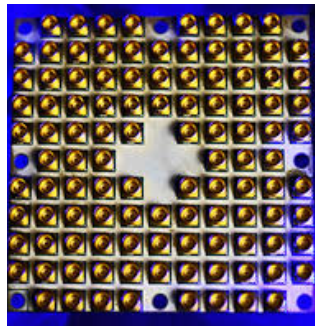
$X = -10$?

D-Wave
The Quantum Computing Company™

x — 2007 — 2018 — ∞

IBM





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

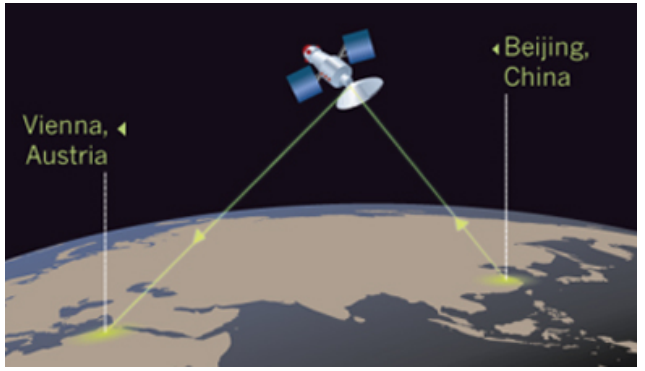
Let's play quantum too!

- 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

http://quantum-internet.team/

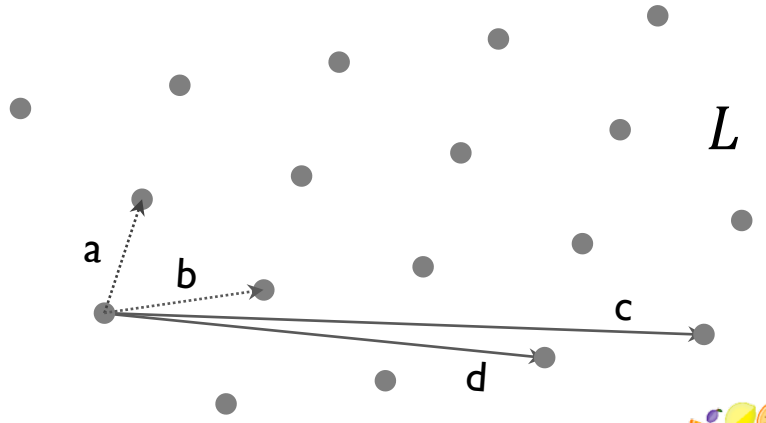


https://en.wikipedia.org/wiki/Quantum_Experiments_at_Space_Scale

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

Quantum alg's find a generator

[EHKS'STOC14]
[BS'SODA16]

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

The Hidden Subgroup Problem (HSP) framework

(captures most instances of quantum exponential speedup)

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)	$\mathbb{Z}_2^n$
Graph isomorphism	Symmetric group
Unique shortest vector problem	Dihedral group

Abelian groups

∃ efficient quantum algs

Non-abelian

Open question:

? efficient quantum algs

Recall: classical security framework fails

Crypto scheme ?

Quantum hard problem

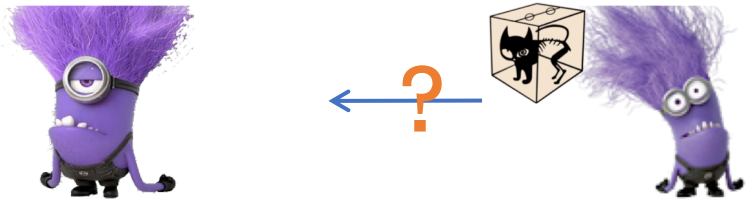
- Security models: inadequate for Q attacks

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

- Security analysis: can fail against Q attackers

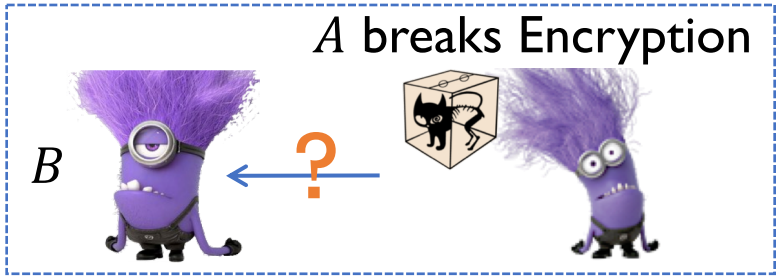
  ⟶ Quantum security analysis: subtle & challenging

B solves lattice problem A breaks Encryption

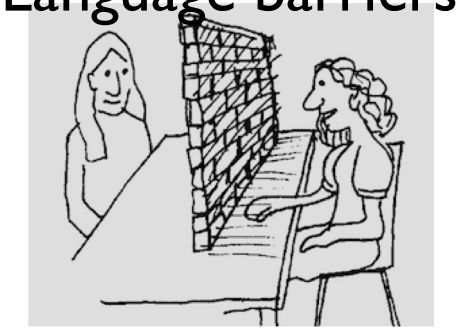


Reduction: Assume attacker A breaks scheme Σ,
→ Construct B solving hard problem Π.

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]

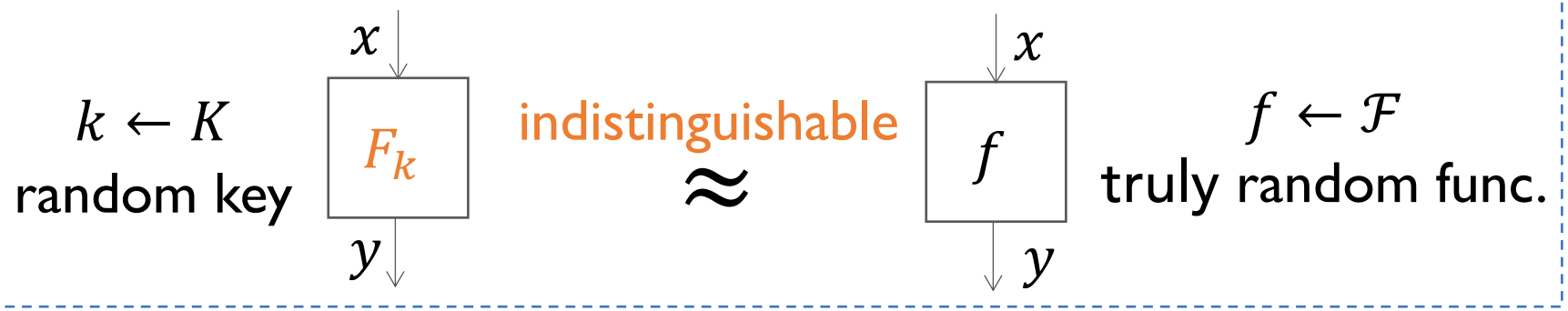
Easy on a quantum computer

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

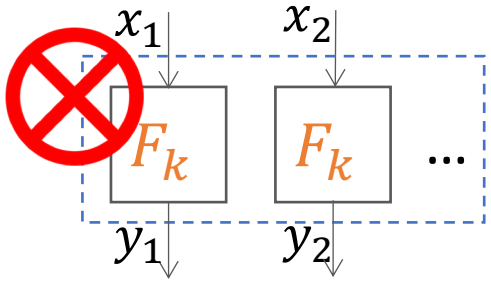
Block cipher and domain extension

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

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

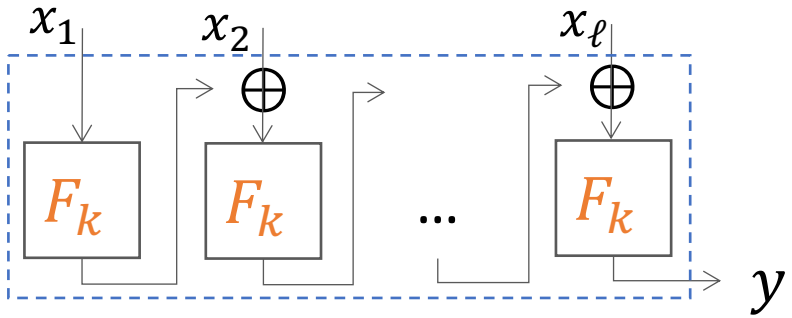


- How about long inputs: domain-extension
  - **Given** psodorandom $\{F_k\}$ on n-bit input
  - **Construct** pseudorandom $\{G_k\}$ on $\ell \cdot n$-bit input



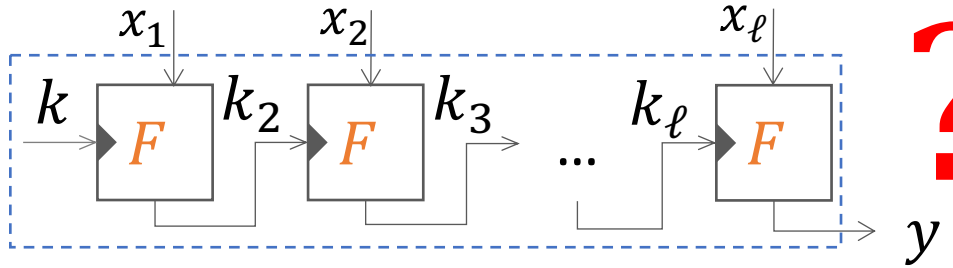
Classically secure domain-extension

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



Broken by quantum!

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



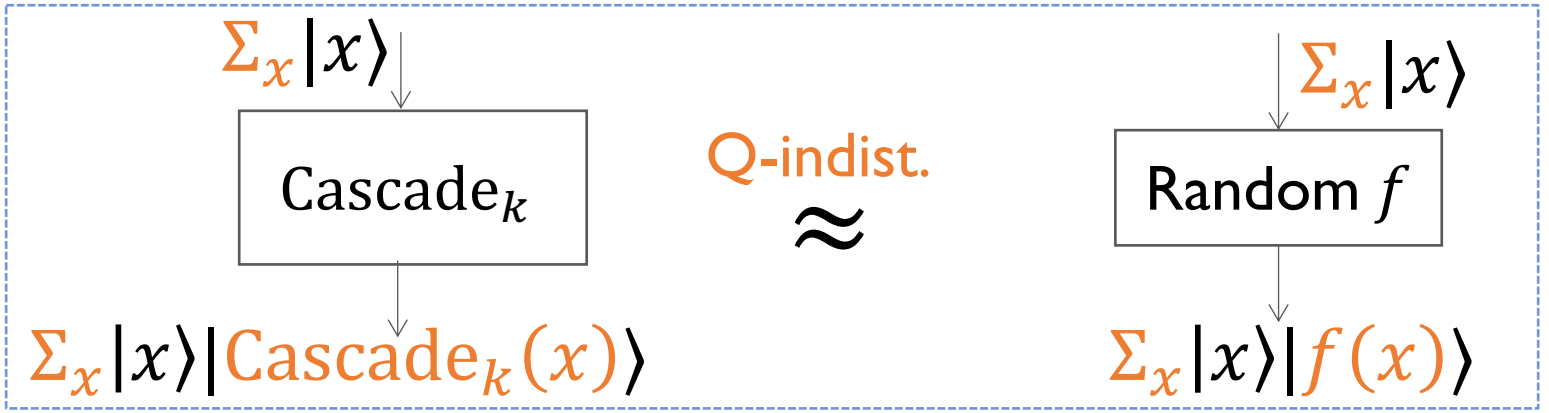
?

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

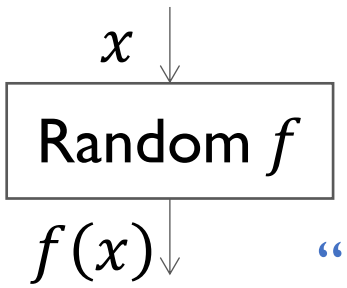
[SY'Crypto17]

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

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



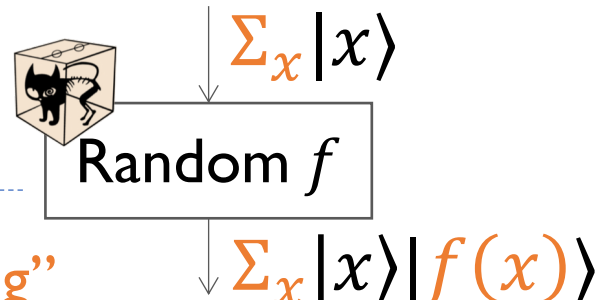
Power of quantum-superposition attack



Local view, one by one

← **Attacker** →

Global view, observe all?



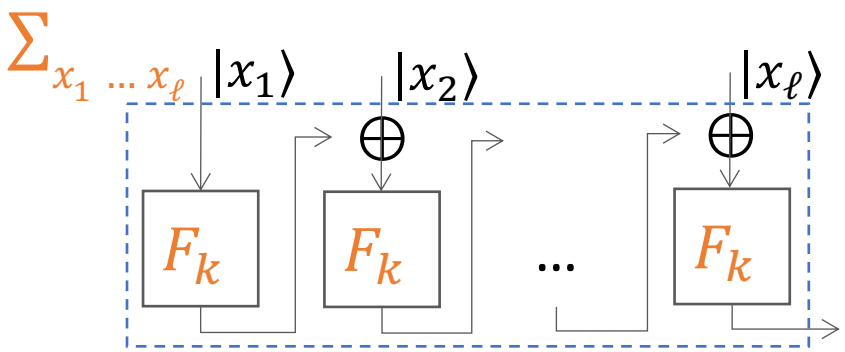
"Lazy" sampling
generate f *on-the-fly*

← **You** (designer) →

"Full committing"
sample entire f *ahead*

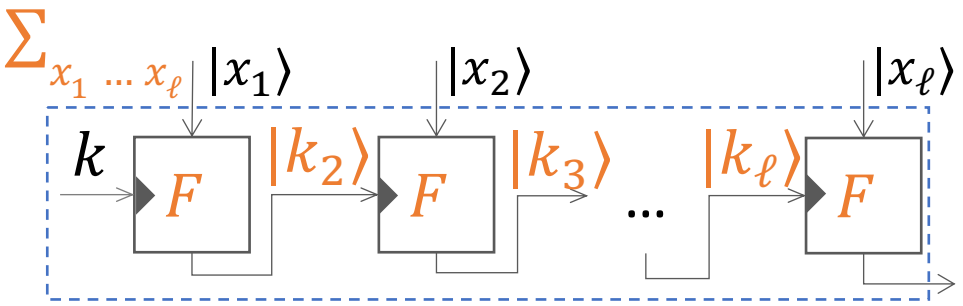
CBC-MAC **Broken!**

global view on F_k of a random k



Cascade

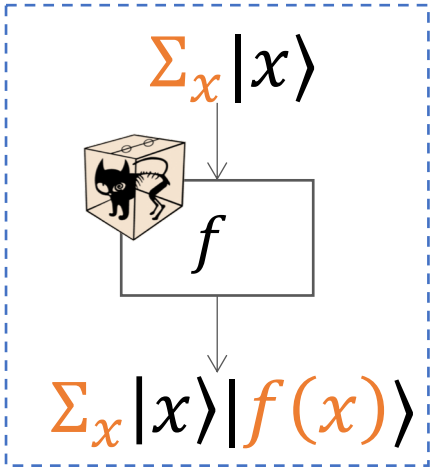
global view on F_k of all k!



we proved it's quantum secure

Is superposition attack realistic?

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



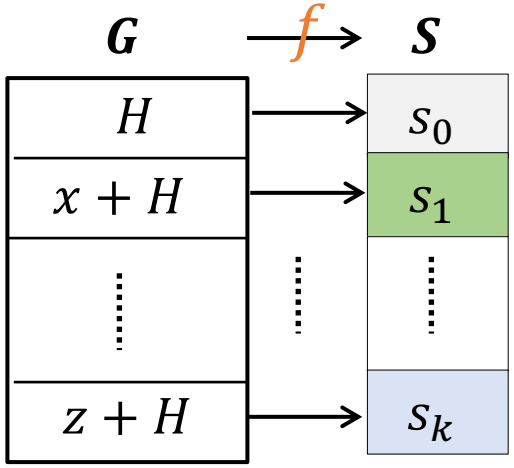
Attacker can implement f as a quantum circuit

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

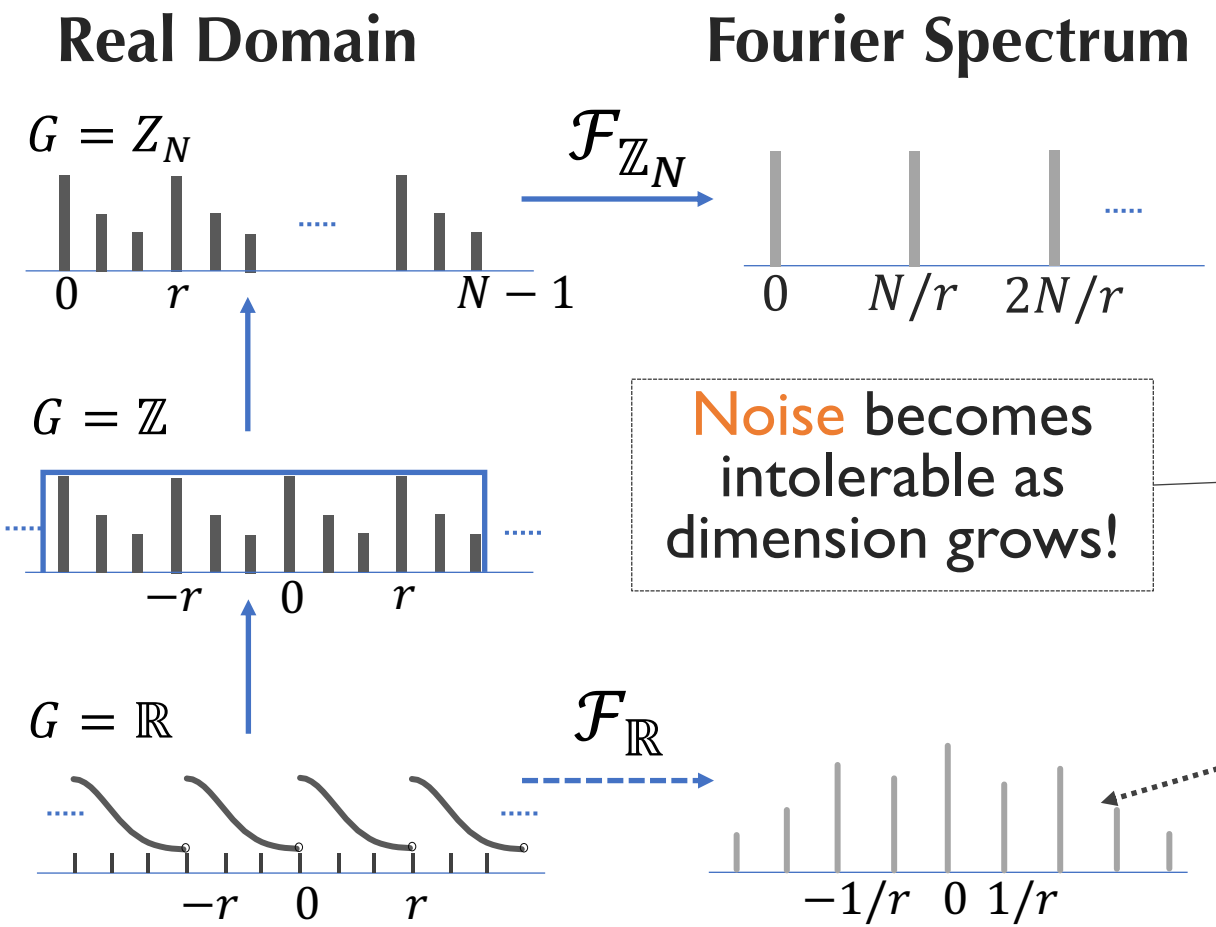
Goal: Find (hidden subgroup) H.

- 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!