QIC891 Topics in Quantum Safe Cryptography

Module 1: Post-Quantum Cryptography
Lecture 4 Part II

Fang Song

Institute for Quantum Computing

University of Waterloo

We’ve seen many cryptographic constructions (new & old)…

… but, are they secure against classial & quantum attacks?

Recall: two necessary pieces of security

1. Are the underlying problems hard to solve?

i.e. are the computational assumptions really sound?

- EX. Is it ok to assume that SIS-function is ONE-WAY

- Complexity (lower bound): ex. solving A is no easier than some
- Algorithms (upper bound): ex. best algorithm needs sooooo long time

2. Are the schemes secure against quantum attacks?

- **Our focus: Provable** security (lower bound)
  - Formal proof (whenever possible): Breaking scheme is no easier than solving A

NOT TRUE!

Proving security against **classical** attacks ➔ Security against **quantum** attacks

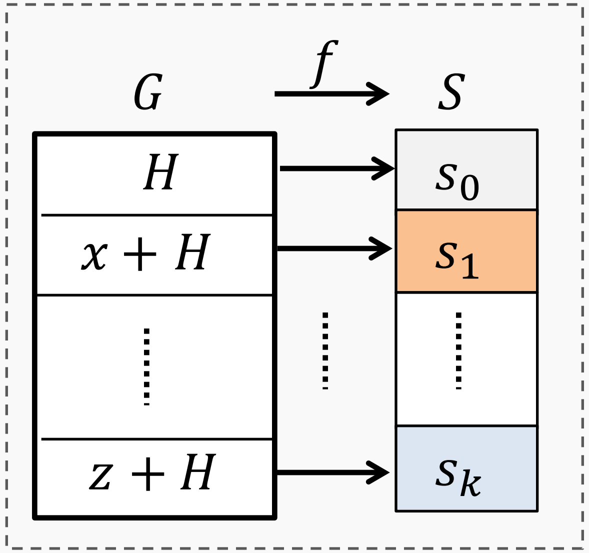
- Practical security (upper bound): ex. Best effort unable to break it

(Quantum) Hardness of candidate problems

Overview of general quantum algorithms

- Grover's quantum search: generic quadratic speedup
- Hidden Subgroup Problem (HSP): exponential speedup exists

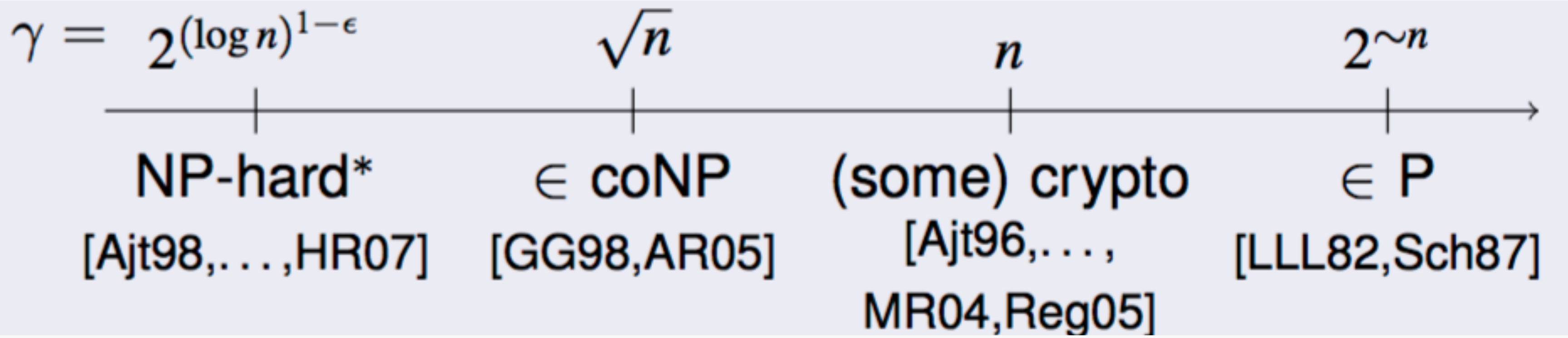
Computational Problems	HSP on G
[Shor97] Factoring	$\mathbb{Z}$
Discrete logarithm	$\mathbb{Z}_N \times \mathbb{Z}_N$
Principal Ideal Problem [EHKS14, BS16]	Continuous $\mathbb{R}^{O(n)}$



- G abelian: ∃ efficient quantum alg. (Fourier Sampling)
- G non-abelian: efficient quantum alg. often unknown

Lattice problems: lower bound

A coarse landscape for $GapSVP_\gamma$



n: lattice dimension

Curtesy of Peikert

- Worst-case: **NP**-hard
- Surprising & unique: Worst-case $\equiv$ average-case

$f_A(x) = Ax \bmod q$

Theorem: if $GapSVP_{n^c}$ hard in worst-case, then SIS-function is one-way.

NP-hard: SAT $\leq$ SVP (unlikely to have efficient algorithms)

Worst-case: for all lattices, do there exist one (or more) on which SVP is hard?

Average-case: sample a lattice at random (not necessarily uniform), is SVP hard?

Lattice problems: classical algorithms

- **Lattice basis reduction**
  - Find "short" & "orthogonal" basis
  - "efficient" but approx. solution

LLL (Lenstra–Lenstra–Lovász)

- $\leq 1.3^n \cdot$ shortest vector, poly(n) time

BKZ (block-Korkine-Zolotarev)

- k-block generalization of LLL

- **"Clever" Brute-Force**
  - "exact" solution, exponential time

* **Enumeration** [Kannan83, GNR10]

- $2^{O(n \log n)}$ time, poly(n) space

Sieving [AKS01,NV08,MV10a,MV10b]

- **Discrete Gauss-Sampling** [ADRS15]: $2^{n+o(n)}$ time & space

Often interplay

- **In practice: BKZ 2.0** [CN11]
  - BKZ + [GNR10] enumeration for k-block

Upshot: Best known classical algorithm for $GapSVP_{n^c}$ needs exponential time.

Lattice problems: quantum algorithms

- Grover's search algorithm
  - Better exponential enumeration & sieve alg's [MPT13]
- Connection to HSP on dihedral group [Regev04]
  - Unique-SVP & BDD $\leq$(standard approach to) dihedral-HSP [not solved so far]

- !!! Break lattice-based cryptosystems
  - [EHKS, BS16] quantum PIP algorithm + [CGS15,CDPR16] classical procedure

  ➔ Efficient quantum algorithm for a "non-standard" lattice problem
  - Several cryptosystems are actually based on this problem [SV10,GGH13,CGS15…]


QUANTA MAGAZINE illuminating science

CRYPTOGRAPHY

A Tricky Path to Quantum-Safe Encryption

Breaking some lattice crypto

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

Short-PIP	Ring-LWE	?	…

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

FHE[c], Multilinear mapping[d], …
broken

Find a short generator a principal ideal

Short-PIP

Our quantum alg's can find **a** generator

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

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

Coding problems: lower bound

- Worst-case: **NP**-hard
  - Decoding general linear code [BerlekampMT'78]
  - Reed-Solomon code (large error) [GuruswamiV05]
  - Binary code (as used in crypto)?

- Random instance in crypto: hopefully hard
  - "obfuscate" easy instances

Assumption 1	Assumption 2
Decoding random linear code hard	Random code ≈ "Obf" Goppa code

- Binary: Learning Parity with noise (LPN)

Coding problems: algorithms

1. Decoding random linear code

- "Clever" Brute-Force

Information Set Decoding
[LeeBrickell89,Leon88,Stern88,BJMM12]

Given: $s = He$, Find e w. $|e| = \beta$.

- $H = [Q_{(n-k)*k} | I_{n-k}]$, $e = (e_1|e_2)^T$.
- Assume $|e_1| = p$, $|e_2| = \beta - p$. (*)
- $He = Qe_1 + e_2$: search p columns in Q whose sum has distance $\beta - p$ to s.

Algorithm: $O(2^{\frac{n}{20}})$ Time

random permute $H \leftrightarrow$ permute e to format (*)

2. Random code ≈ "Obf" Goppa?

- Structural attacks

Distinguisher for **high-rate Goppa** code [Faugere et al. 2013]

Alg's for **Code Equivalence**

- **Support Splitting** [Sendrier00]: Exponential in $|C \cap C^{\perp}|$

!!! **Mind** your Code

- Many other codes unsafe: Reed-Muller, …
- Original proposal of McEliece still OK

Coding problems: quantum algorithms

- An "indicator" of quantum hardness [DinhMR11]

McEliece over Goppa code $\leq$ HSP on G

- G: some semi-direct product group

Quantum Fourier Sampling **NOT** enough for this HSP

How to interpret

- Interesting: same QFS technique solves factoring/DL
- Boundary: a natural attack seems difficult
  - (improper) analogue: reduce to 3-SAT

- Need more people from quantum computing!

Multivariate Quadratic Equations

Given: $p_i(x_1, \dots, x_n) = y_i, i = 1, \dots, m$. Find x_i.

- Hardness (lower bound)
  - Worst-case: NP-hard
  - Random instance in Crypto: hopefully hard
- Algorithms (upper bound)

Grobner basis [Buchberger65,EderFaugere14]

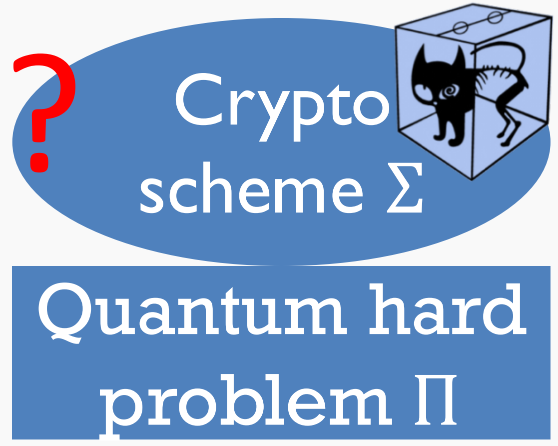
- Analogue: Gaussian elimination of linear systems
- Compute GB: exponential time when $m = O(n)$

Isomorphism of Polynomials [Patarin96,BFV12]

- Quantum Algorithms
  - Awaiting more effort & workforce

Provable quantum security

Provable security in PQC

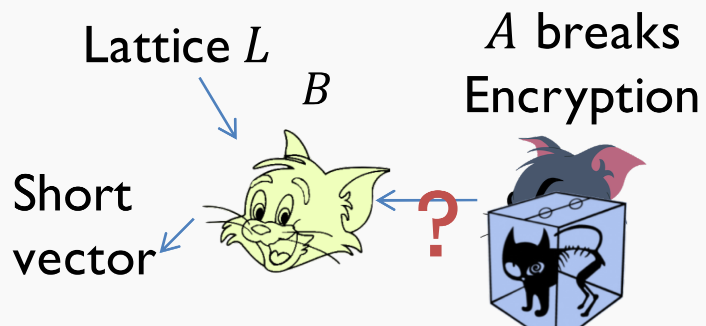


- Classical Security proofs
  - Lattice crypto: default
  - Code crypto: sometimes
  - MQ crypto: none?
- Rarely prove against quantum attack

✗ Security model inadequate for quantum attackers

- Quantum security models: Still at early stage [S14,HSS15]

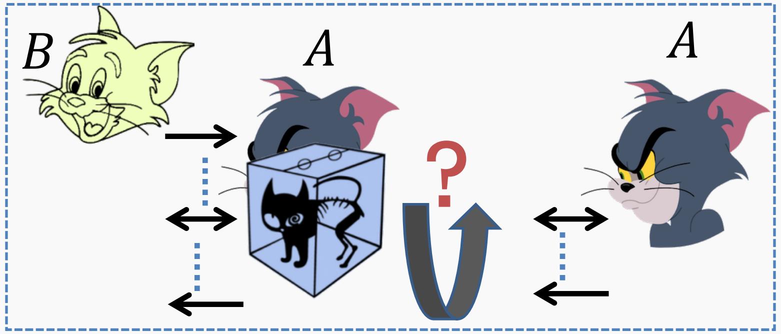
✗ Classical proofs can **fail** against quantum attackers



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 [Watrous09]

- Quantum security of many classical protocols unclear

Some solved [W09, HSS11,FKSZZ13]

- Zero-knowledge proof of knowledge
- Secure 2-party computation

Still a lot open:

- Constant-round Coin-flipping
- **Identification**

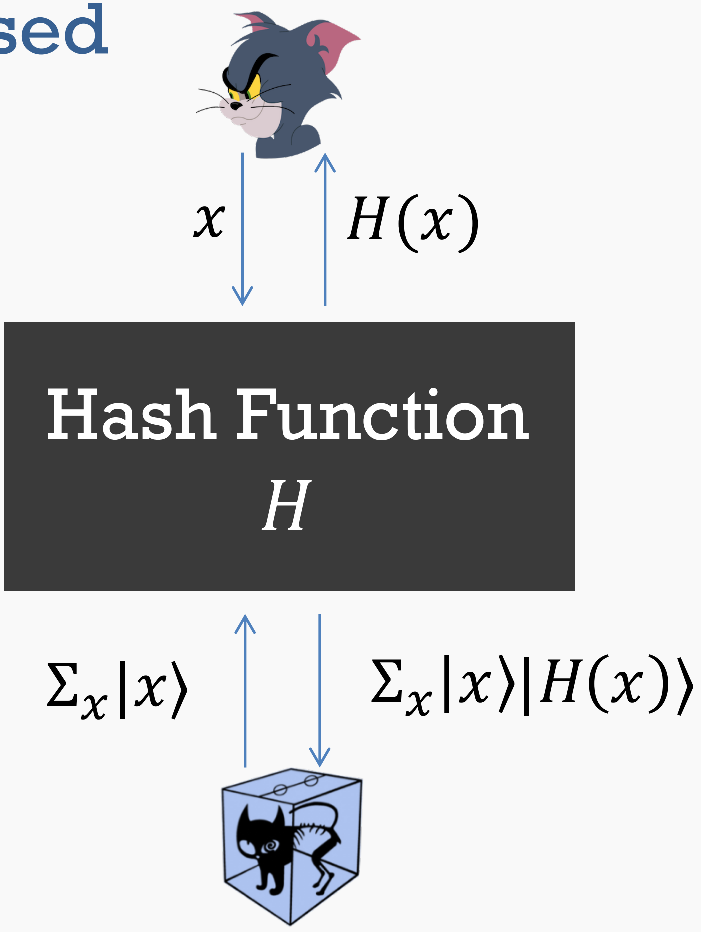
2

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**)

- A quantum-accessible Random Oracle

Nothing seems to work



Proofs with Programmable RO

Quantum Random-Oracle

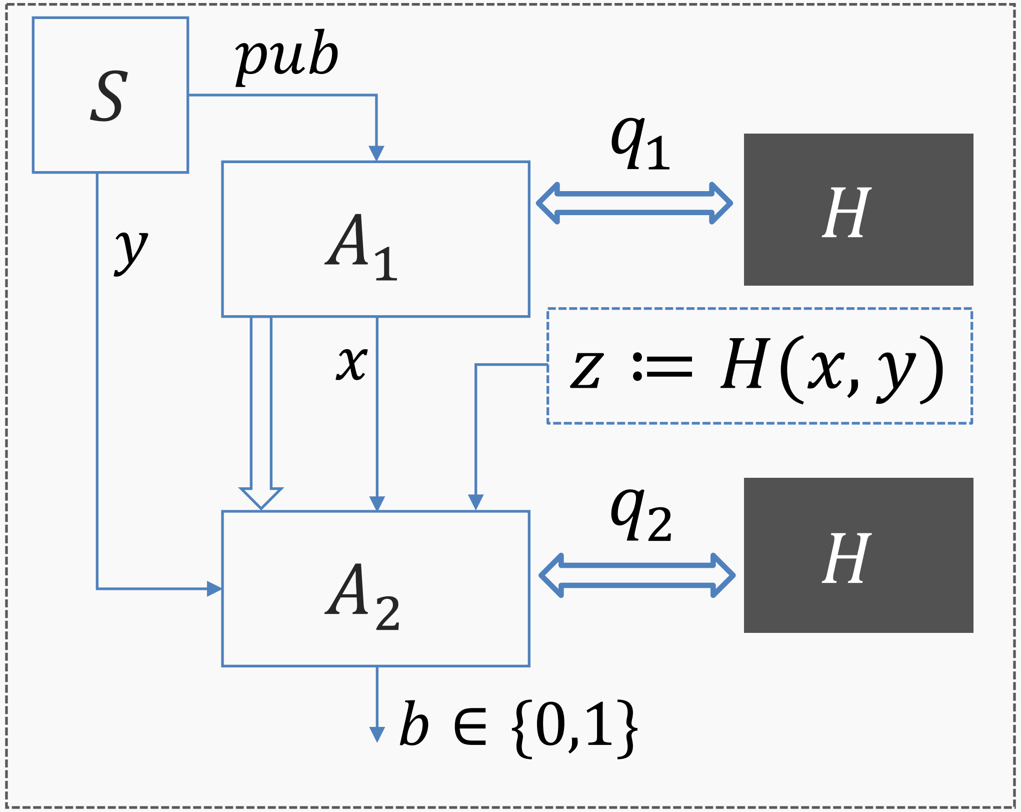
- Full domain Hash
  - OK [Zhandry12]
- OAEP, Fujisaki-Okamoto
  - Variant OK [TarghiU'15]
  - Original version & other conversions?
- Fiat-Shamir Transformation
  - In general fails [DFG13,ARU14]
  - Special cases?

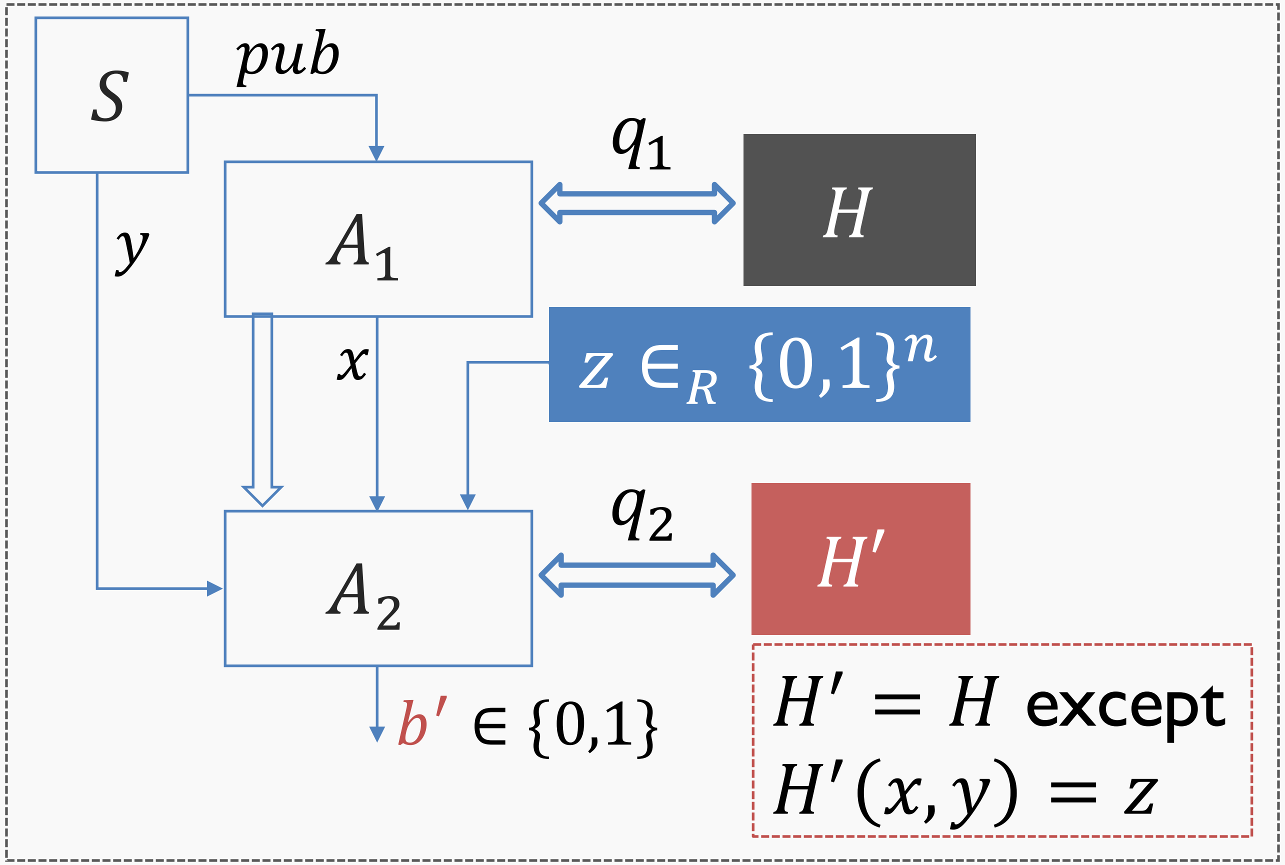
Programming a quantum RO

$H: \{0,1\}^* \rightarrow \{0,1\}^n$

Classical — Quantum

Lemma: $\Pr(b = 0) \approx \Pr(b' = 0)$, as long as y "unpredictable".





What’s ahead?

- An exciting & challenging field
  - Many problems unsolved
  - High risk with growing likelihood!
- Need a diverse workforce
  - Mathematicians & theoretical computer scientists
    - Classical & **Quantum** Algorithms, complexity
  - (Modern) cryptographers, physicists & engineers
  - Politicians?

Curtesy of cbcnews

"from the heart outwards"

Questions?