QIC891 Topics in Quantum Safe Cryptography (Spring 2016)

Module 1: Post-Quantum Cryptography

Fang Song

Institute for Quantum Computing

University of Waterloo

Administration

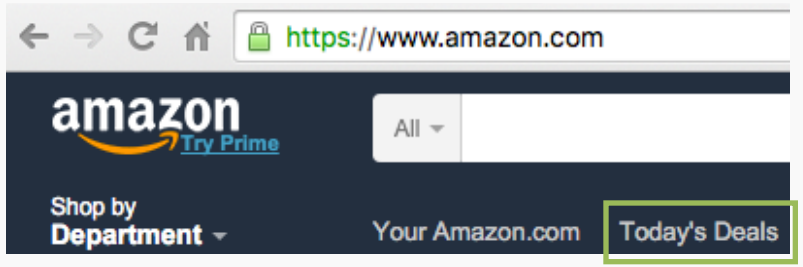
- Lectures
  - 10:30-12:00 on May 10, 12, 17, 19.
  - All at **QNC 1201** (attention: differs from initial announcement).
- Course webpage
  - http://fangsong.info/s16_uw_pqc/
  - Tentative schedule, references, lecture notes …
- For academic credit (QIC891):
  - one homework assignment for this module, due 2 weeks after the last lecture
  - Complete 3 modules + 1 final project (see Monica Dey for details)
- For CrytoWorks21 Qualification:
  - A quiz will be given (format & time TBD)

What is this module about?

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

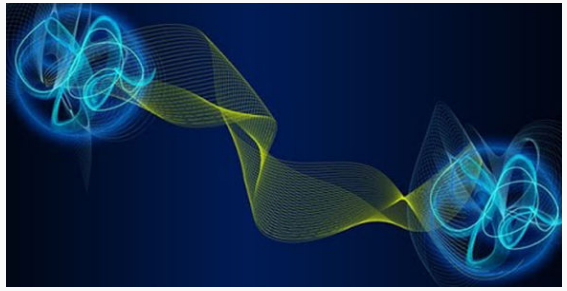
Physicists: quantum weirdness

Quantum **superposition**

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

Quantum Entanglement

- Non-classical correlation

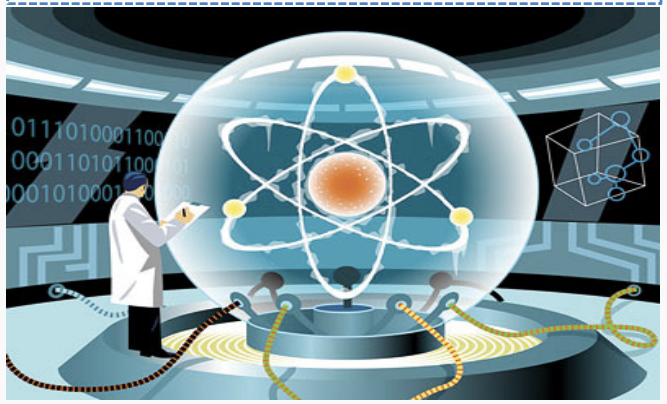


"Spooky action at a distance"
– A. Einstein

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

X

- Computational assumption:
hard for **quantum** computer

Need: Re-examine every link against quantum attackers

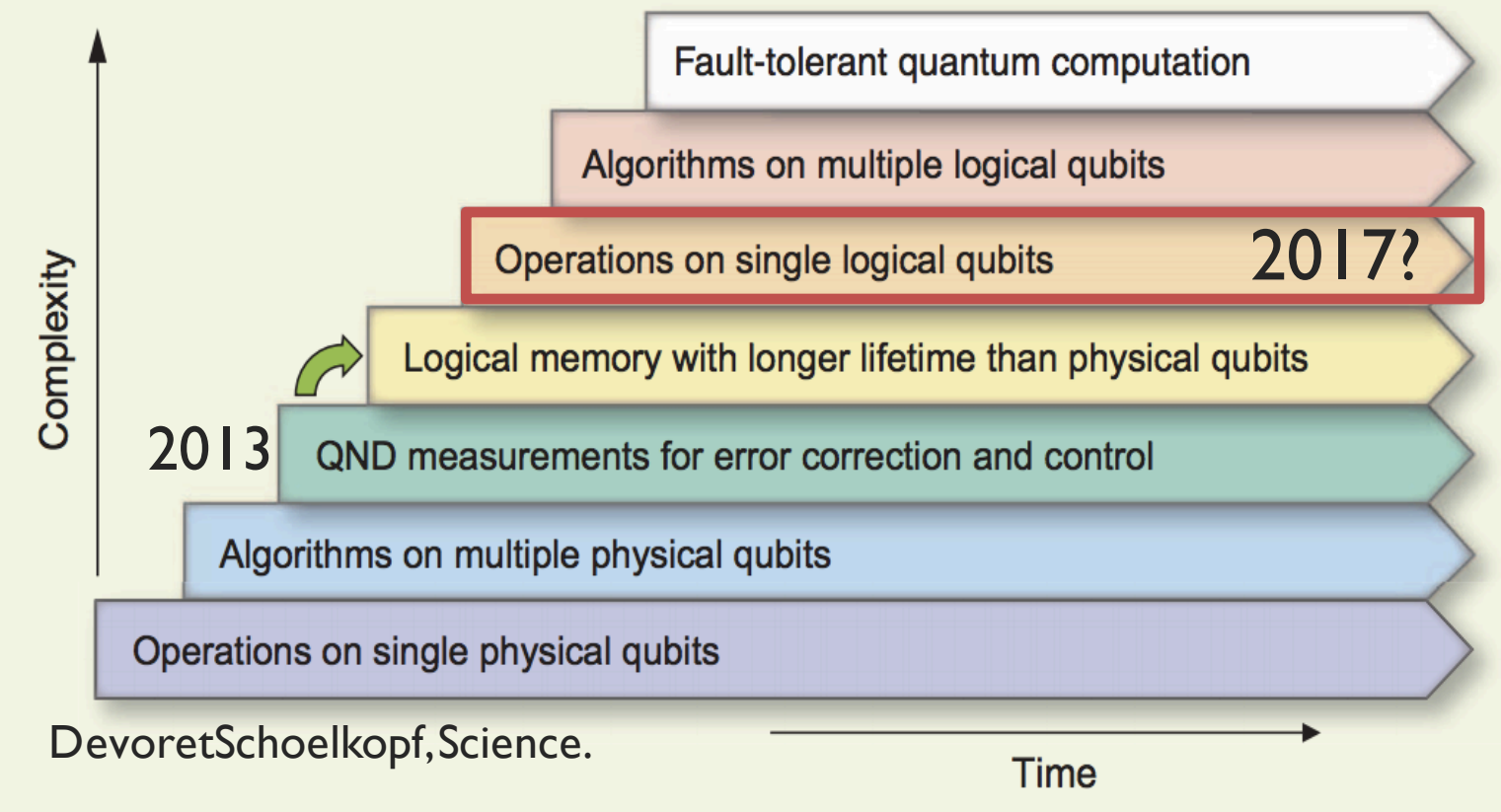
Question: How to obtain quantum-safe cryptosystems?

Should I really care?

	Task	Need	Availability
1	Run quantum factoring algorithm (to break public key crypto)	Full-scale fault-tolerant QC 	?

How far is a quantum computer away?

- Hardware



UCSB + Google

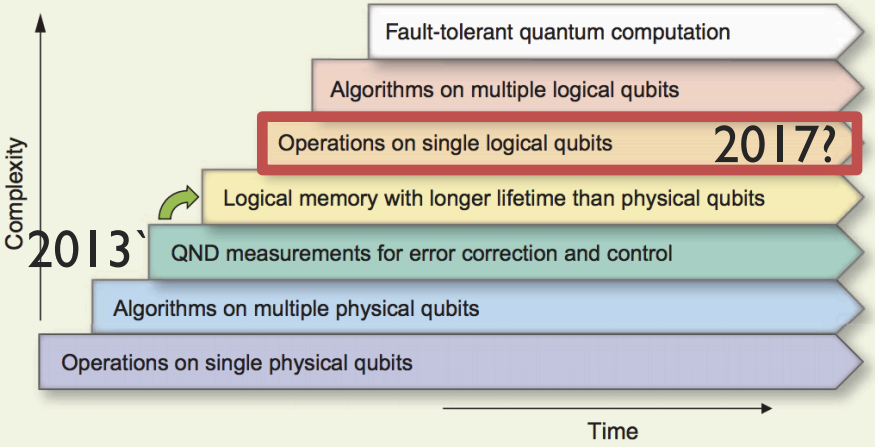
IBM

…

- 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

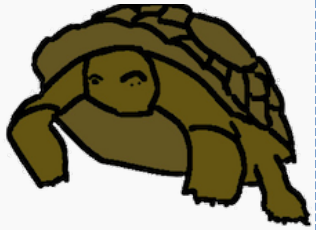
ETSI

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**."

This Module

Will see

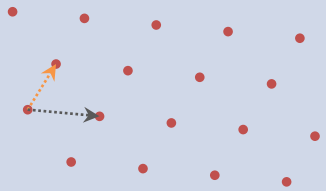
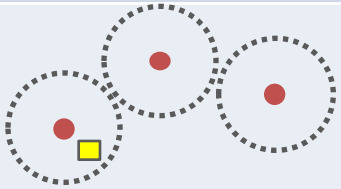
- Key theoretical ideas for PQC
- (My hope) A unified framework to think about various schemes
  → inspire future research
- (Challenges of) provable quantum security
- **Focus**: public-key signature & encryption

Won't see or very little (my apologies)

- Key-exchange, symmetric-key crypto (block cipher etc.)
- Implementations, concrete parameters, efficiency…

Major directions of post-quantum crypto

Hash **signature**	Looks solid & promising [revival of an early brilliant idea!]

	Foundation	**Functionalities**	**Security**
Lattice		• ID, PRFs, CRHF… • Signature, PKE, • FHE, IBE, FE, obfuscation…	• Worst-case hard problems • **Worst-case ≡ avg-case** • Provable security: common
Code		• ID, PRG • Signature, PKE	• Worst-case hard problems • Obfuscate easy instances • Provable security: few
Multivariate	$p_i(x_1, \dots, x_k) = y_i$ p_i: quadratic $(x_i x_j)$	• Signature, PKE	• Worst-case hard problems • Obfuscate easy instances • Provable security: none?
Isogeny	$i: E \mapsto F$	• Key-exchange, Sign, PKE	• Extensions of discrete Log

Provable **Quantum** Security: largely missing!

Tentative schedule

1. Overview of PQC
   - Major candidate directions & central problems
2. Public-key **signature**
   - Hash-based signature & Hash+(Identification+FiatShamir)
   - Trapdoor function
     - ☹ "Text-book" RSA signature & post-quantum siblings
     - Full-domain Hash
3. Public-key **encryption**
   - 😐 "Text-book" RSA encryption & post-quantum siblings (weak security)
   - Getting IND-CPA (&stronger) security
     - Generic: OAEP & FujisakiOkamoto
     - Direct constructions
4. Quantum security
   - Hardness of candidate problems
   - Analyzing security formally against quantum attacks