NANYANG TECHNOLOGICAL UNIVERSITY SINGAPORE

Security and Quantum Computing: An Overview

Prasanna Ravi,
Anupam Chattopadhyay,
Shivam Bhasin.

NTU Singapore

LATS 2022
5th September 2022

Contents

- **Security Threats from Quantum Architectures**
  - Public-Key Cryptography
  - Private-Key Cryptography
  - Post-Quantum Cryptography
- **Quantum-enabled Security**
  - Quantum Key Distribution
  - Quantum TRNG
  - New Attacks

Contents

- **Security Threats from Quantum Architectures**
  - Public-Key Cryptography
  - Private-Key Cryptography
  - Post-Quantum Cryptography
- **Quantum-enabled Security**
  - Quantum Key Distribution
  - Quantum TRNG
  - New Attacks

Quantum Computing Architectures: Now

- **2017-18**
  - Google announces 72-qubit ‘Bristlecone’
  - Intel develops 49-qubit ‘Tangle Lake’
  - IBM announces 50-qubit quantum computer
  - 160-qubit quantum computer from IonQ
- **2021**
  - IBM announces 127-qubit IBM Eagle processor
  - Anticipating 1121-qubit processor named “Condor” in 2023
- **2022**
  - NIST recently announced the first standards for quantum-resistant cryptography.

Administration

BRIEFING ROOM

National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems

MAY 04, 2022 • STATEMENTS AND RELEASES

Quantum Architectures

- Universal Quantum computers (IBM, Intel, Google, IonQ)
  - Akin to a general-purpose processor
  - Relevant to the security threats

- Quantum Annealing (D-Wave)
  - Akin to an ASIC, designed to solve a hard optimization problem
  - No evidence of quantum speed-up over entire dataset[1]
  - Demonstrated speed-up over Simulated Annealing, and Quantum Monte Carlo[2]

1. T. F. Ronnow et al, “Defining and detecting quantum speedup”, Science 2014
2. H. Neven, “When can Quantum Annealing win?”, Google AI Blog, 2015

In 1994....

Algorithms for Quantum Computation: Discrete Logarithms and Factoring

Peter W. Shor
AT&T Bell Labs
Room 2D-149
600 Mountain Ave.
Murray Hill, NJ 07974, USA

Abstract

A computer is generally considered to be a universal computational device; i.e., it is believed able to simulate any physical computational device with a cost in computation time of at most a polynomial factor. It is not clear whether this is still true when quantum mechanics is taken into consideration. Several researchers, starting with David Deutsch, have developed models for quantum mechanical computers and have investigated their computational properties. This paper gives Las Vegas algorithms for finding discrete logarithms and factoring integers on a quantum computer that take a number of steps which is polynomial in the input size, e.g., the number of digits of the integer to be factored. These two problems are generally considered hard on a classical computer and have been used as the basis of several proposed cryptosystems. (We thus give the first examples of quantum cryptanalysis.)

[1, 2]. Although he did not ask whether quantum mechanics conferred extra power to computation, he did show that a Turing machine could be simulated by the reversible unitary evolution of a quantum process, which is a necessary prerequisite for quantum computation. Deutsch [9, 10] was the first to give an explicit model of quantum computation. He defined both quantum Turing machines and quantum circuits and investigated some of their properties.

The next part of this paper discusses how quantum computation relates to classical complexity classes. We will thus first give a brief intuitive discussion of complexity classes for those readers who do not have this background. There are generally two resources which limit the ability of computers to solve large problems: time and space (i.e., memory). The field of analysis of algorithms considers the asymptotic demands that algorithms make for these resources as a function of the problem size. Theoretical computer scientists generally classify algorithms as efficient when the number of steps of the algorithms grows as a polynomial in the size of the input. The class of prob-

Why worry?

- Shor's algorithms can solve *discrete logarithm problem*, and *number factorization problem* in polynomial time[1]
  - These are basis for ECC and RSA cryptosystem respectively
  - Practical demonstration of factorization[2,3]

- Several symmetric-key cryptosystems are under the scrutiny of 'quantum cryptanalysis'[4]

- **Question**: How realistic these attacks are?
- **Question**: What alternatives do we have?

1. P. Shor, "Algorithms for quantum computation: discrete logarithms and factoring", Proceedings of FOCS, 1994
2. E. Martin-Lopez et al, "Experimental realization of Shor's quantum factoring algorithm using qubit recycling", Nature Photonics, 2012
3. Note: Several demonstrations used adiabatic quantum computing to reduce factorization to an optimization problem
4. M. Grassl, "Applying Grover's Algorithm to AES: Quantum Resource Estimates", PQCrypto 2016

Asymmetric/Public-Key Cryptography

- Largest RSA factored using classical computer– RSA-768[1]
- RSA-2048 has 2048 bit
  - Could be broken by a 20 Million Noisy-Qubit Quantum computer in 8 hours[2]

- Modular exponentiation is the most complex block in Shor's factorization algorithm
  - $2000n^2$ depth, $9n + 2$ 'logical' qubits[3]
  - Include other blocks
  - Include Quantum Error Correction
  - Include Logical → Physical Qubits

- **Recap**: we are at 100s of qubits now

1. T. Kleinjung et al, "Factorization of a 768-Bit RSA Modulus", Crypto 2010
2. C. Gidney et al, "How to Factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits", Quantum Journal, 2021
3. A. Pavlidis et al, " Fast quantum modular exponentiation architecture for Shor's factoring algorithm", QIC, 2014

Symmetric/Private-Key Cryptography

- Basic Idea
  - Search over all possible keys using Grover's search[1] algorithm, where the symmetric-key algorithm is a blackbox.

- Grover's search is $O\left(\sqrt{N}\right)$ runtime for a database of size N,
  - e.g., AES-128 will need $K2^{64}$ iterations. After considering the AES-128 circuit implementation, the overall depth is obtained as 1.16×2^{81}
  - Further search-space reduction using side-channel knowledge

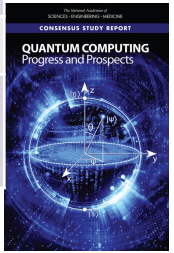
	#gates		depth		#qubits
k	T	Clifford	T	overall	
128	$1.19 \cdot 2^{86}$	$1.55 \cdot 2^{86}$	$1.06 \cdot 2^{80}$	$1.16 \cdot 2^{81}$	2,953
192	$1.81 \cdot 2^{118}$	$1.17 \cdot 2^{119}$	$1.21 \cdot 2^{112}$	$1.33 \cdot 2^{113}$	4,449
256	$1.41 \cdot 2^{151}$	$1.83 \cdot 2^{151}$	$1.44 \cdot 2^{144}$	$1.57 \cdot 2^{145}$	6,681

- **Note**: Classical cryptanalysis for AES-128 provides 85-bit security if 2^{43} encryptions are available through time-memory-data trade-off attack

1. L. Grover, "A fast quantum mechanical algorithm for database search", Proceedings of STOC, 1996
2. M. Grassl, "Applying Grover's Algorithm to AES: Quantum Resource Estimates", PQCrypto 2016

Attack Complexity Estimates

Cryptosystem	Category	Key Size	Quantum Algorithm	# Logical Qubits Required	# Physical Qubits Required	Time Required to Break System
AES-GCM	Symmetric-Key Encryption	128	Grover's Algorithm	2,953	4.61×10^6	2.61×10^{12} years
		192		4,449	1.68×10^7	1.97×10^{22} years
		256		6,681	3.36×10^7	2.29×10^{32} years
RSA	Asymmetric-Key Encryption	1024	Shor's Algorithm	2,050	8.05×10^6	3.58 hours
		2048		4,098	8.56×10^6	28.63 hours
		4096		8,194	1.12×10^7	229 hours
ECC Discrete-log problem	Asymmetric-Key encryption	256	Shor's Algorithm	2,330	8.56×10^6	10.5 hours
		384		3,484	9.05×10^6	37.67 hours
		521		4,719	1.13×10^6	55 hours



1. Quantum Computing: Progress and Prospects (2019). Consensus Study Report. National Academies Press, 2019.

In a Possible Future with Quantum Computers

Post-Quantum Cryptography:
Cryptography designed to be secure against an attacker (not the user) with a large scale quantum computer

Operations are performed on a classical device!!!

Post-Quantum Cryptography

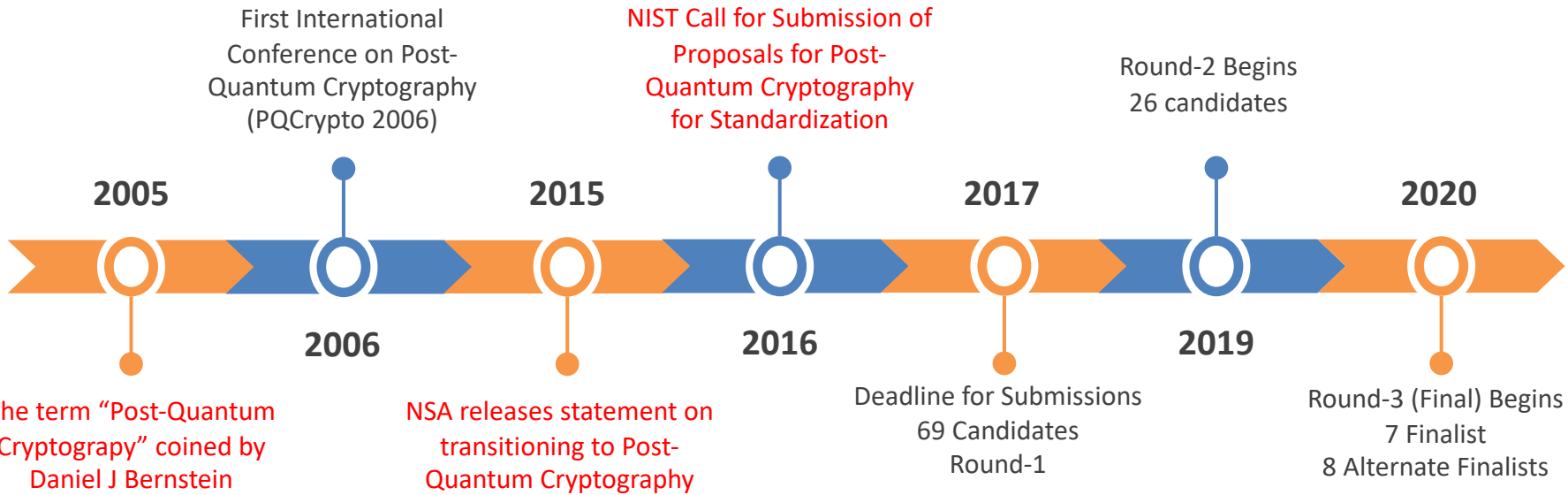
- Instead of waiting for a Quantum computer ***to actually break*** the current e-commerce, we prepare for that by designing new public-key cryptographic primitives that are resistant against Quantum-enabled attackers

- **Why start now??**
  - Attacker can store communication transcripts today, and decrypt at a later time.

- **Idea:** Base security on a hard computational problem 'without efficient Quantum algorithm'

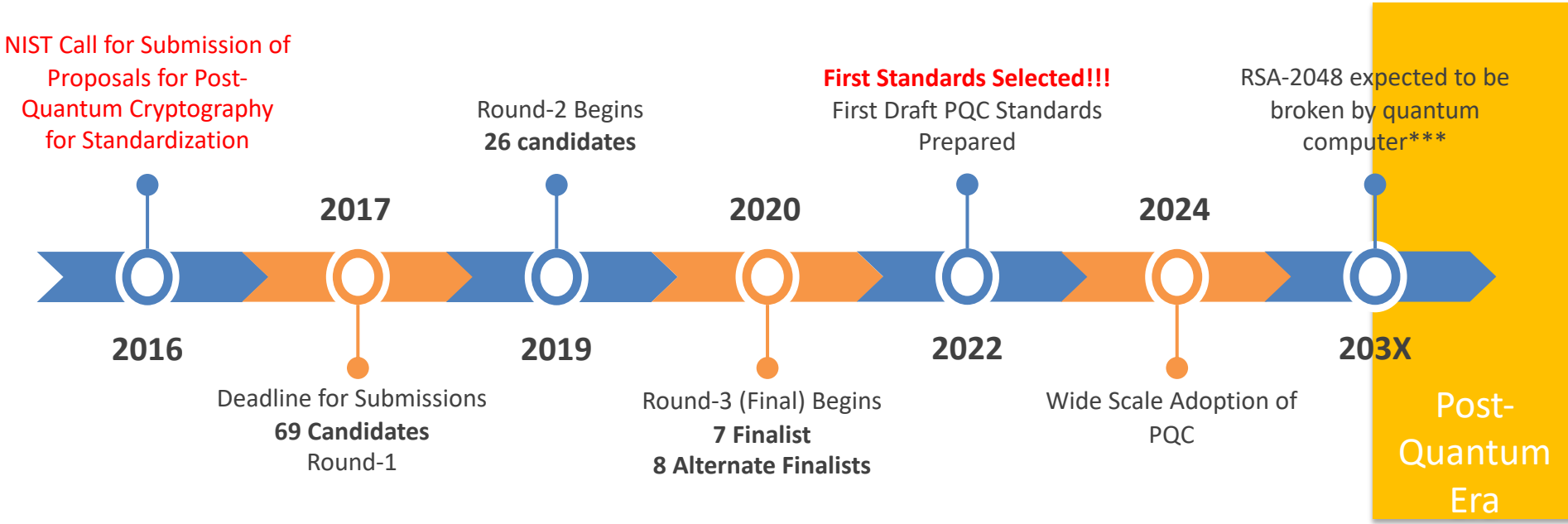
- Lattice-based: Closest-vector problem, Shortest-vector problem
- Hash-based: Security of one-way hash functions
- Multivariate Cryptography: Multivariate Quadratic Equation Solving problem
- Code-based: Syndrome decoding problem

PQC: Timeline



Alagic, Gorjan, Gorjan Alagic, Jacob Alperin-Sheriff, Daniel Apon, David Cooper, Quynh Dang, Yi-Kai Liu et al. *Status report on the first round of the NIST post-quantum cryptography standardization process*. Washington, DC: US Department of Commerce, National Institute of Standards and Technology, 2019.

PQC: Timeline



Alagic, Gorjan, Gorjan Alagic, Jacob Alperin-Sheriff, Daniel Apon, David Cooper, Quynh Dang, Yi-Kai Liu et al. *Status report on the first round of the NIST post-quantum cryptography standardization process*. Washington, DC: US Department of Commerce, National Institute of Standards and Technology, 2019.

NIST PQC Call

Round 3 (Aug 2020-July 2022):

Type	Signature	KEM/Encryption	Finalist (Alternate)
Lattice Based	2	3 (2)	5 (2)
Code-Based	-	1 (2)	1 (2)
Multivariate	1 (1)	-	1 (1)
Hash-Based	- (2)	-	- (2)
Isogeny based	-	- (1)	- (1)
Total	3 (3)	4 (5)	7 (8)

Moody, Dustin, Gorjan Alagic, Daniel C. Apon, David A. Cooper, Quynh H. Dang, John M. Kelsey, Yi-Kai Liu et al. "Status report on the second round of the NIST post-quantum cryptography standardization process." (2020).

NIST PQC Call

- **Criteria for Standardization:**
  - Theoretical Security (Classical, Post-Quantum)
  - Implementation Performance on HW/SW platforms
  - Integration into existing protocols/ Resistance against Side-Channel Attacks and Fault Attacks.

- **Selected Standards (July 2022):**
  - **KEMs:**
    - Kyber (Lattice-based)
  - **Signatures:**
    - Dilithium (Lattice-based)
    - Falcon (Lattice-based)
    - SPHINCS+ (Hash-based)

- **There is also a fourth round for the NIST PQC process (starting at end of 2022)**

Take with a Pinch of Salt!

Type	Signature	KEM/Encryption	Finalist (Alternate)
Lattice Based	2	3 (2)	5 (2)
Code-Based	-	1 (2)	1 (2)
Multivariate[1]	1 (1)	-	1 (1)
Hash-Based	- (2)	-	- (2)
Isogeny based[2]	-	- (1)	- (1)
Total	3 (3)	4 (5)	7 (8)

1. Beullens, Ward. "Breaking rainbow takes a weekend on a laptop." *Cryptology ePrint Archive* (2022).

2. Castryck, Wouter, and Thomas Decru. "An efficient key recovery attack on SIDH (preliminary version)." *Cryptology ePrint Archive* (2022).

Take with a Pinch of Salt!

Type	Signature	KEM/Encryption	Finalist (Alternate)
Lattice Based	2	3 (2)	5 (2)
Code-Based	-	1 (2)	1 (2)
~~**Multivariate**[1]~~	~~1 (1)~~	~~-~~	~~1 (1)~~
Hash-Based	- (2)	-	- (2)
~~**Isogeny based**[2]~~	~~-~~	~~- (1)~~	~~- (1)~~
Total	3 (3)	4 (5)	7 (8)

1. Beullens, Ward. "Breaking rainbow takes a weekend on a laptop." *Cryptology ePrint Archive* (2022).

2. Castryck, Wouter, and Thomas Decru. "An efficient key recovery attack on SIDH (preliminary version)." *Cryptology ePrint Archive* (2022).

PQC is not enough: Side-Channel Attacks

- Side-channel resistance is essential criteria of cryptographic implementations
  - Several attacks and countermeasures are known for classical cryptographic primitives[1,2,3]
  - PQC is relatively unexplored

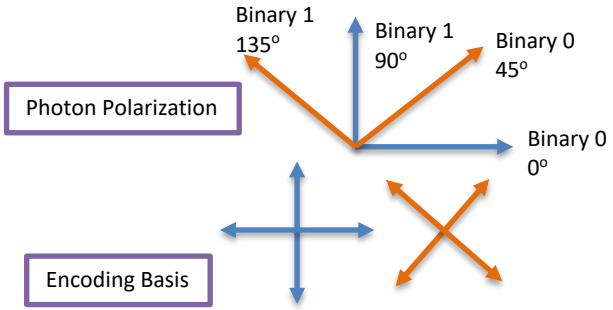
1. Ravi, Prasanna, Debapriya Basu Roy, Shivam Bhasin, Anupam Chattopadhyay, and Debdeep Mukhopadhyay. "Number “not used” once-practical fault attack on pqm4 implementations of NIST candidates." In *International Workshop on Constructive Side-Channel Analysis and Secure Design*, pp. 232-250. Springer, Cham, 2019.
2. Ravi, Prasanna, Anupam Chattopadhyay, and Anubhab Baksi. "Side-channel and Fault-injection attacks over Lattice-based Post-quantum Schemes (Kyber, Dilithium): Survey and New Results." *Cryptology ePrint Archive* (2022).
3. Guo, Qian, Thomas Johansson, and Alexander Nilsson. "A key-recovery timing attack on post-quantum primitives using the Fujisaki-Okamoto transformation and its application on FrodoKEM." In *Annual International Cryptology Conference*, pp. 359-386. Springer, Cham, 2020.

Contents

- Security Threats from Quantum Architectures
  - Public-Key Cryptography
  - Private-Key Cryptography
  - Post-Quantum Cryptography
- **Quantum-enabled Security**
  - Quantum Key Distribution
  - Quantum TRNG
  - New Attacks

Quantum Key Distribution

- **BB84** Protocol[1]



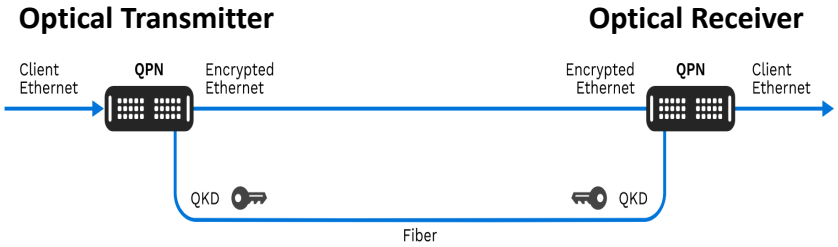
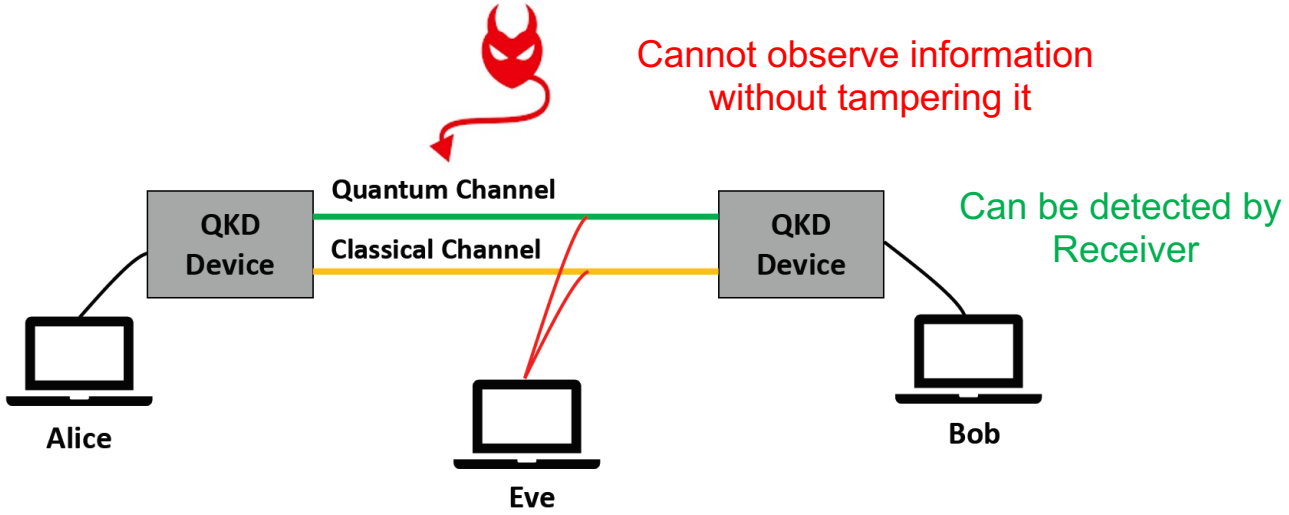


Image source: MagiQ

- Commercial offerings by
  - ID-Quantique, NuCrypt, MagiQ
- **Unconditional Security:** Secure against any attacker !!!
  - All cryptographic algorithms are only conditionally secure (attacker's capability)
- **Implementation:** Off-the shelf telecommunication components (No Quantum Computer)

1. C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing", *IEEE CSSP, 1984*
2. A. Nordrum, "China Demonstrates Quantum Encryption By Hosting a Video Call", IEEE Spectrum, 2017

Quantum Key Distribution



- **Important:** QKD requires an authenticated classical channel (cannot be used in standalone manner)
- **Challenges:**
  - Distance-Rate Trade-off Limitations
  - New Infrastructure Required - Cost

Quantum Key Distribution: Attacks

- Man-in-the-Middle Attack: Needs 3rd Party, or *unconditionally secure authentication*
- Intercept and Resend: Eavesdropper detected with high probability
- Implementation Attacks[1,2]
  - Utilizes the functioning of Avalanche Photo Diodes (APD) to operate in a different mode and mount ‘intercept and resend’ attack without being detected.

1. L. Lydersen et al, ”Hacking commercial quantum cryptography systems by tailored bright illumination”, Nature Photonics, 2010
2. I. Gerhardt et al, “Full-field implementation of a perfect eavesdropper on a quantum cryptography system”, Nature Communications, 2011.

Quantum True Random Number Generation

- Based on Smartphone camera
  - Counting photons on individual pixels[1]
- Based on EM field at Vacuum
  - Measuring the fluctuations of phase and amplitude[2]
- Attacks
  - Prone to classical noise from environment, measurement setup, and exploiting these by an attacker
  - Machine Learning attacks

1. B. Sanguinetti et al, “Quantum Random Number Generation on a Mobile Phone”, Physical Review X, 2014
2. J. Y. Haw et al, “Maximization of Extractable Randomness in a Quantum Random-Number Generator”, Physical Review A, 2015

Summary

- Quantum threat to Security
  - Is real - estimates on timeframe varies
  - Relies on Qubit quality, Error Correction Codes, Efficient Circuits

- PQC and Symmetric-Key Crypto are safer options
  - Implementation aspects, larger key sizes to be accommodated

- QKD, QTRNG to pave new protocols
  - Implementation issues remain


Post-Quantum
Cryptography
Thank
you!!!
Quantum
Computer

Contents

- Security Threats from Quantum Architectures
  - Public-Key Cryptography
  - Private-Key Cryptography
  - Post-Quantum Cryptography
  - New Attacks
- Quantum-enabled Security
  - Quantum Key Distribution
  - Quantum TRNG
  - New Attacks
- **Robust Quantum Circuits**
  - Error Correction Codes
  - Noisy Intermediate Scale Quantum Computing

Robust Quantum Computing

- Quantum computing is susceptible to
  - Error in gate control
  - Environmental Decoherence
  - Initialization/Measurement Error
  - Qubit loss/leakage error

- Three aspects
  - Fault-Tolerant Quantum Computing, e.g.[1]
  - Quantum Error Correction Codes, e.g.[2,3]
  - Error Suppression Techniques (e.g., decoherence-free subspace)

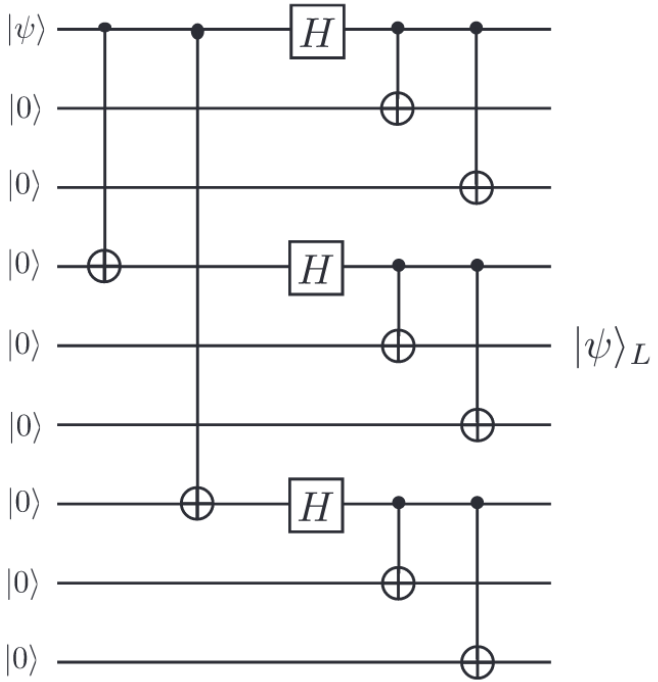
- Integrated approach: Error correction in a fault-tolerant manner implementations done for *concatenated codes*, and *topological codes*

1. P.W. Shor, "Fault-Tolerant quantum computation", Proc. 37th IEEE Symp. on Foundations of Computer Science., pages 56–65, 1996.
2. A.M. Steane. "Error Correcting Codes in Quantum Theory", Phys. Rev. Lett., 77:793, 1996.
3. A.R. Calderbank and P.W. Shor, "Good Quantum Error-Correcting codes exist", Phys. Rev. A., 54:1098,1996.
4. E. Knill, "Quantum computing with realistically noisy devices", Nature, 434:39, 2005.

Robust Quantum Computing (contd.)

- Quantum Error Correction
  - Errors from diverse sources are converted to a discrete and probabilistic error
  - Set of discrete ‘correctable’ errors are dependent the code used

- Shor’s 9 physical-qubit QEC code that can correct arbitrary 1 logical-qubit single bit-flip, or phase-flip error



Quantum Threshold Theorem

- Essentially states that for a *general local noise model*, if the error in a gate/qubit is smaller than a constant threshold then, *fault tolerant computation can be performed* using universal set of gates.[1]

- Randomized benchmarking to estimate gate fidelity as function of number of gates.[2]

1. D. Aharonov and M. Ben-Or, “Fault-Tolerant Quantum Computation with Constant Error Rate”, Siam J. Computing, 2008
2. X. Xue et al, “Benchmarking Gate Fidelities in a Si/SiGe Two-Qubit Device”, Physical Review X, 2019

Logical and Physical Qubits

- **Question**: Better Qubit, or Better QEC[1]

- One logical qubit realization needs > 1 physical qubit. Ratio depends on
  - Which errors to correct
  - Code used
  - Measurement/Qubit used

- Example
  - Surface code with depolarizing error probability $p < 10^{-3}$ per elementary gate needs 10^4 physical qubits per logical qubit[1]
  - Factoring $N = 2000$ bit number using surface codes need $130\ Million - 1\ Billion$ physical qubits[2]

1. E. Campbell et al, “Roads towards fault-tolerant universal quantum computation”, Nature, 2017
2. A. Fowler et al, “Surface codes: Towards practical large-scale quantum computation”, Physical Review A, 2012

Noisy Intermediate Scale Quantum (NISQ) Computing

- Exciting possibility suggested by J. Preskill[1]
  - "Quantum computers with *50-100 qubits* may be able to perform tasks which surpass the capabilities of today's classical digital computers, but *noise* in quantum gates will limit the size of quantum circuits that can be executed reliably"

- Primary Challenges
  - Identifying 'high-impact' applications solvable with NISQ
  - Designing Low-depth Quantum Circuits
  - Prudent mapping to avoid noisy Qubits

1. J. Preskill, "Quantum Computing in the NISQ era and beyond", Quantum Journal, 2018