Post Quantum Cryptography

Creative Convergence of Quantum Assistive and Resistant Methods!

Gokul Alex

Twitter @gokulgaze

Founder - GigameshGarages, QuantumQuixote
Chief Architect - Somish Labs, Spathion Labs

Gokul Alex is an Engineer, Economist and Educator experimenting with emerging and enigmatic technologies. He loves the creative convergence of programming, philosophy, poetry, psychology, physics with passion and perspectives.

Gokul Alex has started working on Quantum Computers during his career in IBM in 2012. He has designed and developed Quantum Blood Filters in IBM Qiskit. He has built the first Quantum Computing Research Lab in Kerala during his career in UST Global. He has collaborated with Russian Quantum Centre, MIT Media Lab, Malta Digital Innovation Authority, CSIR India, West Bengal Government etc. on Quantum Computing Researches.

He is advisor to the one for the first Quantum Randomness StartUp from Asia, Haqien Inc which is incubated in the New York Luminate Accelerator. He is the reviewer of a Pakt Publisher Book on Quantum Machine Learning. He is currently working on Quantum Computing based optimisation algorithms for machine learning and mathematical modelling problems in finance and transportation sector.

He is also experimenting with Quantum Randomness based identity and integrity infrastructure systems. He is one of the first adopters of Quantum Resistant Ledger in Asia. He has pitched Quantum Resistant Cryptography for 5G Network Deployment in Europe through R3 Corda Accelerator.

Let us begin with a poem ...

If computers that you build are quantum,

Then spies of all factions will want ‘em.

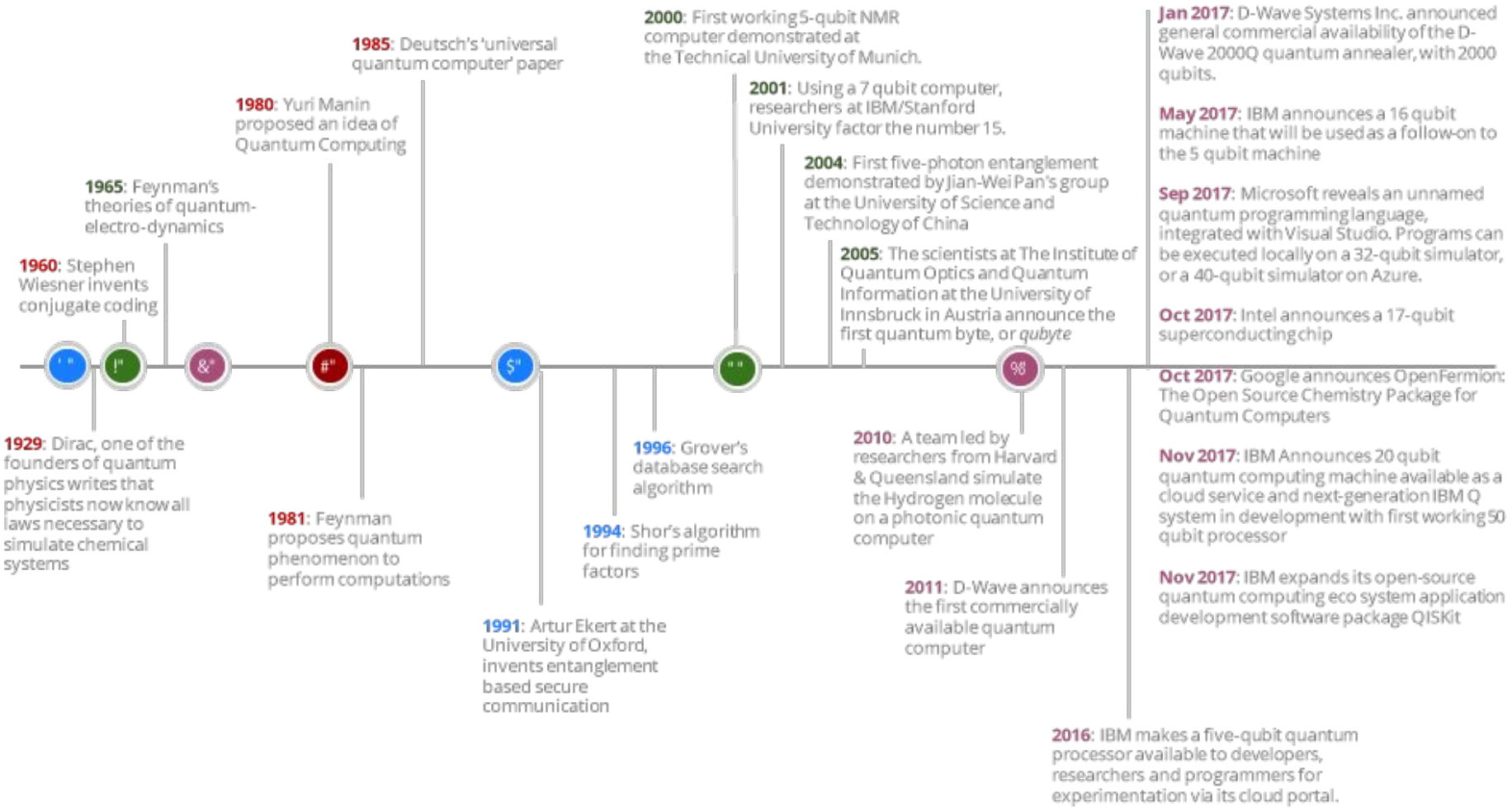
Our codes will all fail,

And they’ll read our email,

Till we’ve crypto that’s quantum, and daunt ‘em.

(by Jennifer and Peter Shor)

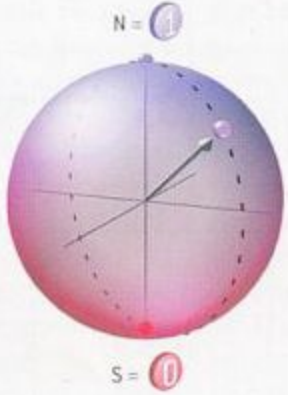
In 1994, Peter Shor Presented his Famous Factoring Algorithm for Quantum Machines!

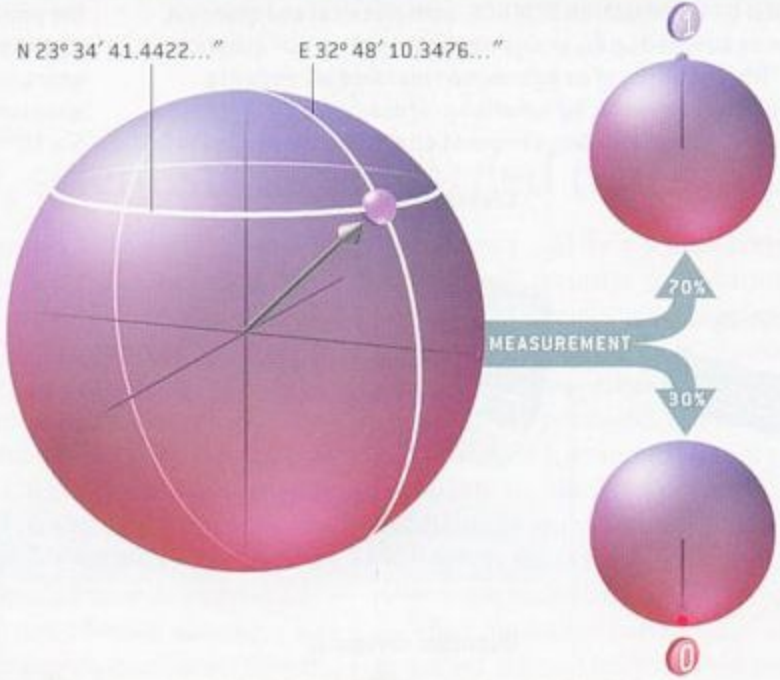

1929: Dirac, one of the founders of quantum physics writes that physicists now know all laws necessary to simulate chemical systems
1960: Stephen Wiesner invents conjugate coding
1965: Feynman's theories of quantum-electro-dynamics
1980: Yuri Manin proposed an idea of Quantum Computing
1981: Feynman proposes quantum phenomenon to perform computations
1985: Deutsch's 'universal quantum computer' paper
1991: Artur Ekert at the University of Oxford, invents entanglement based secure communication
1994: Shor's algorithm for finding prime factors
1996: Grover's database search algorithm
2000: First working 5-qubit NMR computer demonstrated at the Technical University of Munich.
2001: Using a 7 qubit computer, researchers at IBM/Stanford University factor the number 15.
2004: First five-photon entanglement demonstrated by Jian-Wei Pan's group at the University of Science and Technology of China
2005: The scientists at The Institute of Quantum Optics and Quantum Information at the University of Innsbruck in Austria announce the first quantum byte, or qubyte
2010: A team led by researchers from Harvard & Queensland simulate the Hydrogen molecule on a photonic quantum computer
2011: D-Wave announces the first commercially available quantum computer
2016: IBM makes a five-qubit quantum processor available to developers, researchers and programmers for experimentation via its cloud portal.
Jan 2017: D-Wave Systems Inc. announced general commercial availability of the D-Wave 2000Q quantum annealer, with 2000 qubits.
May 2017: IBM announces a 16 qubit machine that will be used as a follow-on to the 5 qubit machine
Sep 2017: Microsoft reveals an unnamed quantum programming language, integrated with Visual Studio. Programs can be executed locally on a 32-qubit simulator, or a 40-qubit simulator on Azure.
Oct 2017: Intel announces a 17-qubit superconducting chip
Oct 2017: Google announces OpenFermion: The Open Source Chemistry Package for Quantum Computers
Nov 2017: IBM Announces 20 qubit quantum computing machine available as a cloud service and next-generation IBM Q system in development with first working 50 qubit processor
Nov 2017: IBM expands its open-source quantum computing eco system application development software package QISKit

QUBITS EXPLAINED

A BIT can have one of two states: 0 or 1. A bit can be represented by a transistor switch set to "off" or "on" or abstractly by an arrow pointing up or down.

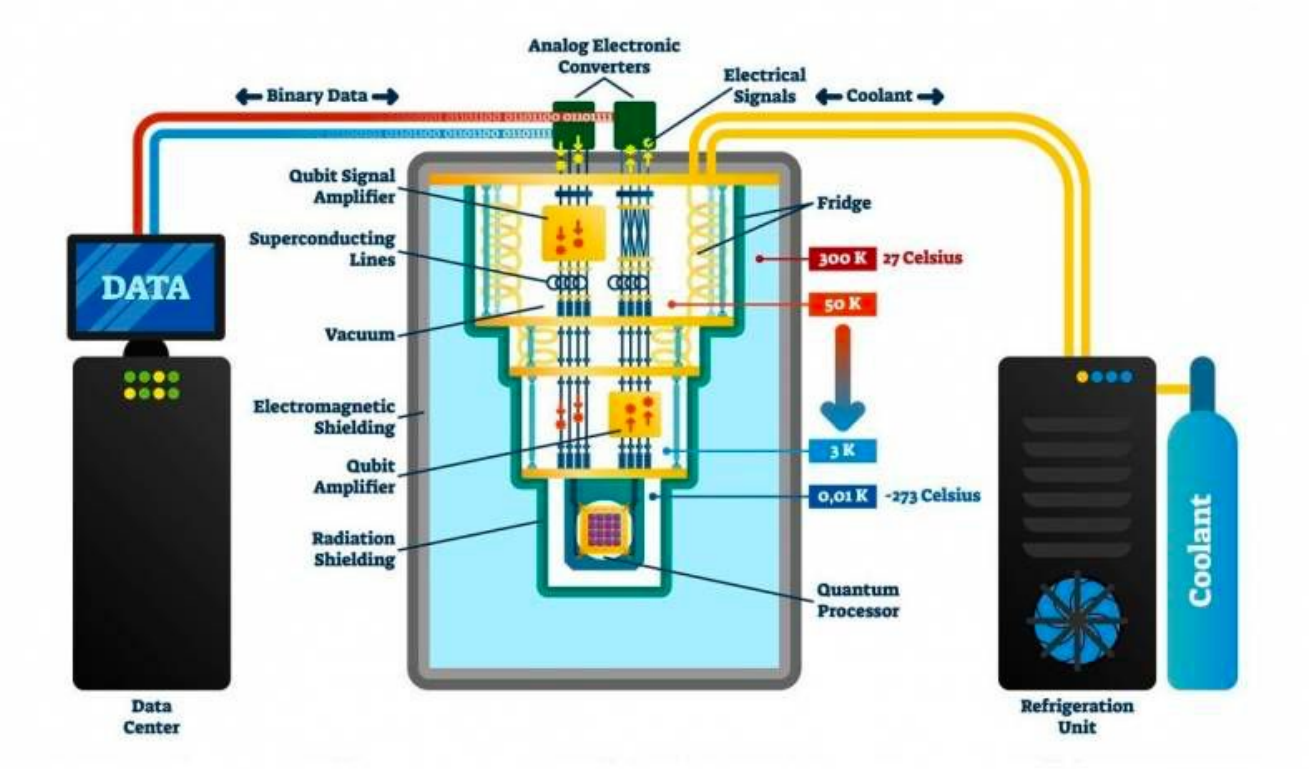
A QUBIT, the quantum version of a bit, has many more possible states. The states can be represented by an arrow pointing to a location on a sphere. The north pole is equivalent to 1, the south pole to 0. The other locations are quantum superpositions of 0 and 1.



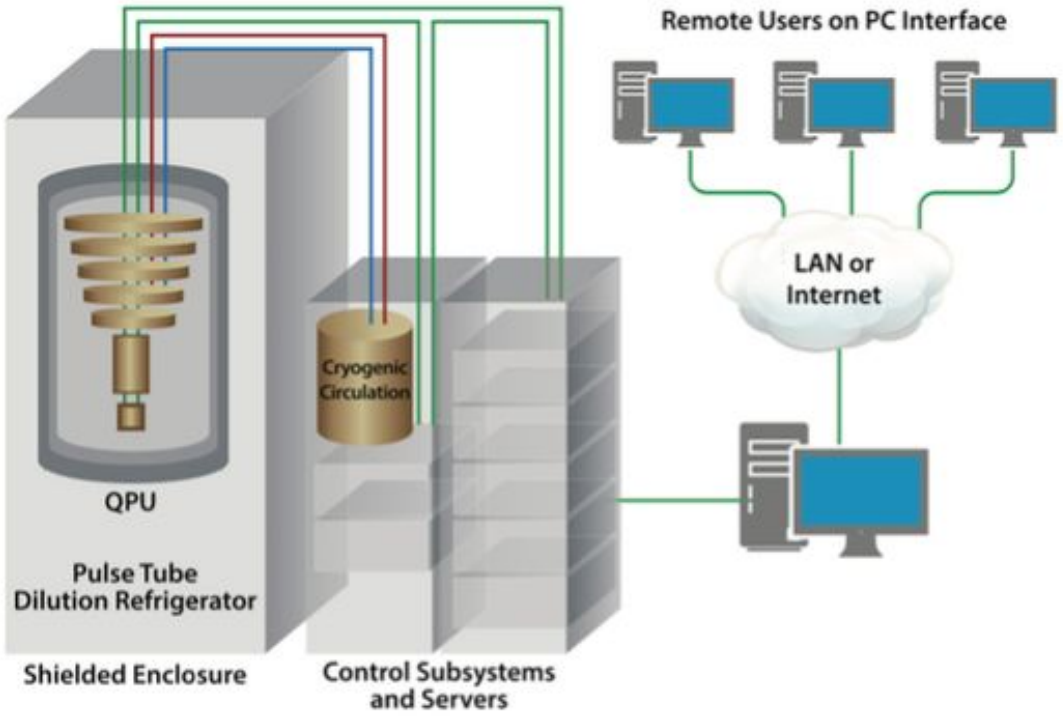


A QUBIT MIGHT SEEM TO CONTAIN an infinite amount of information because its coordinates can encode an infinite sequence of digits. But the information in a qubit must be extracted by a measurement. When the qubit is measured, quantum mechanics requires that the result is always an ordinary bit—a 0 or a 1. The probability of each outcome depends on the qubit's "latitude."

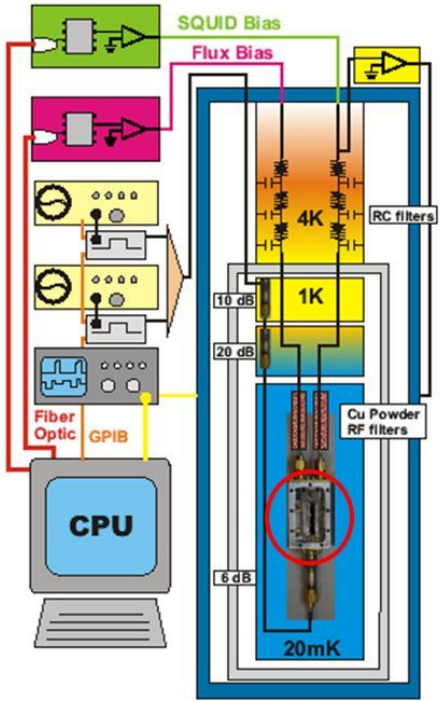
A simple schematic of the quantum computer!



Quantum Annealing Computer by D-Wave



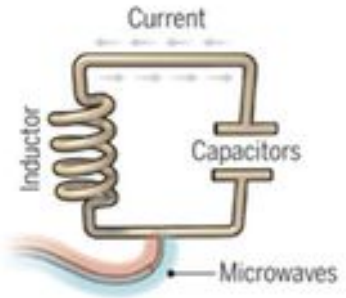
Superconducting Qubit Models



- Ante
  - Dilution Refrigerator
    - Low temperature, < 50 mK
  - RF measurement
    - Low power ~ 1 photon of energy in cavity
- <u>Improves coherence</u>
  - Removes quasiparticles in superconductor
  - Reduces thermal radiation
- <u>Hurts coherence:</u>
  - Low-energy, two-level excitations in amorphous materials

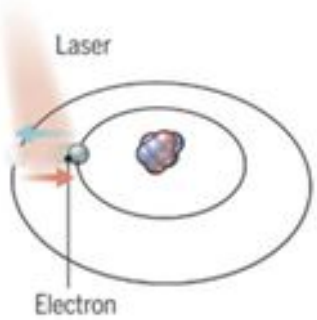
NIST
National Institute of Standards and Technology
Technology Administration, U.S. Department of Commerce

Quantum Computing Construction Models



Superconducting loops

A resistance-free current oscillates back and forth around a circuit loop. An injected microwave signal excites the current into superposition states.

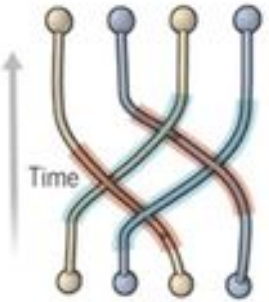


Trapped ions

Electrically charged atoms, or ions, have quantum energies that depend on the location of electrons. Tuned lasers cool and trap the ions, and put them in superposition states.

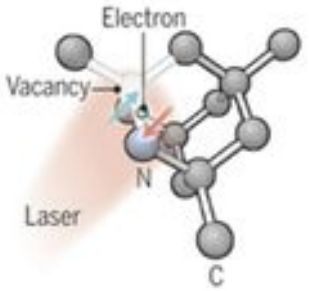
Silicon quantum dots

These "artificial atoms" are made by adding an electron to a small piece of pure silicon. Microwaves control the electron's quantum state.



Topological qubits

Quasiparticles can be seen in the behavior of electrons channeled through semiconductor structures. Their braided paths can encode quantum information.



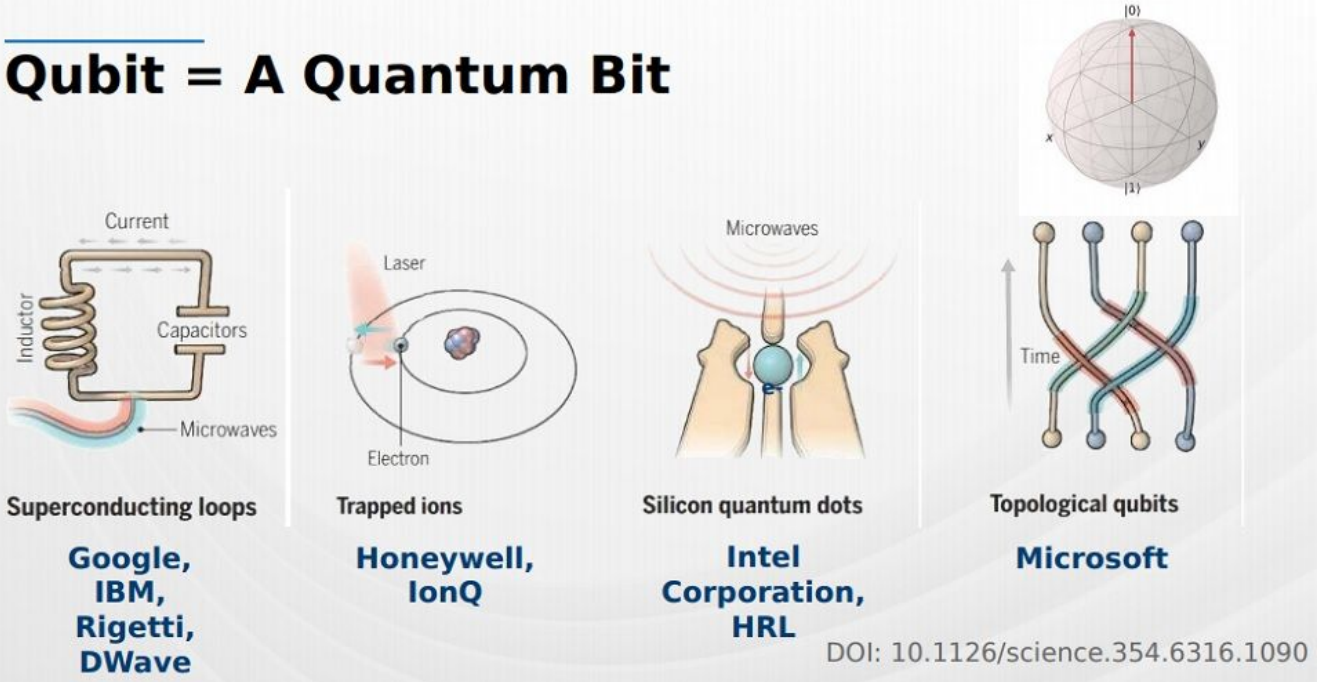
Diamond vacancies

A nitrogen atom and a vacancy add an electron to a diamond lattice. Its quantum spin state, along with those of nearby carbon nuclei, can be controlled with light.

Longevity (seconds)				
0.00005	>1000	0.03	N/A	10
Logic success rate				
99.4%	99.9%	~99%	N/A	99.2%

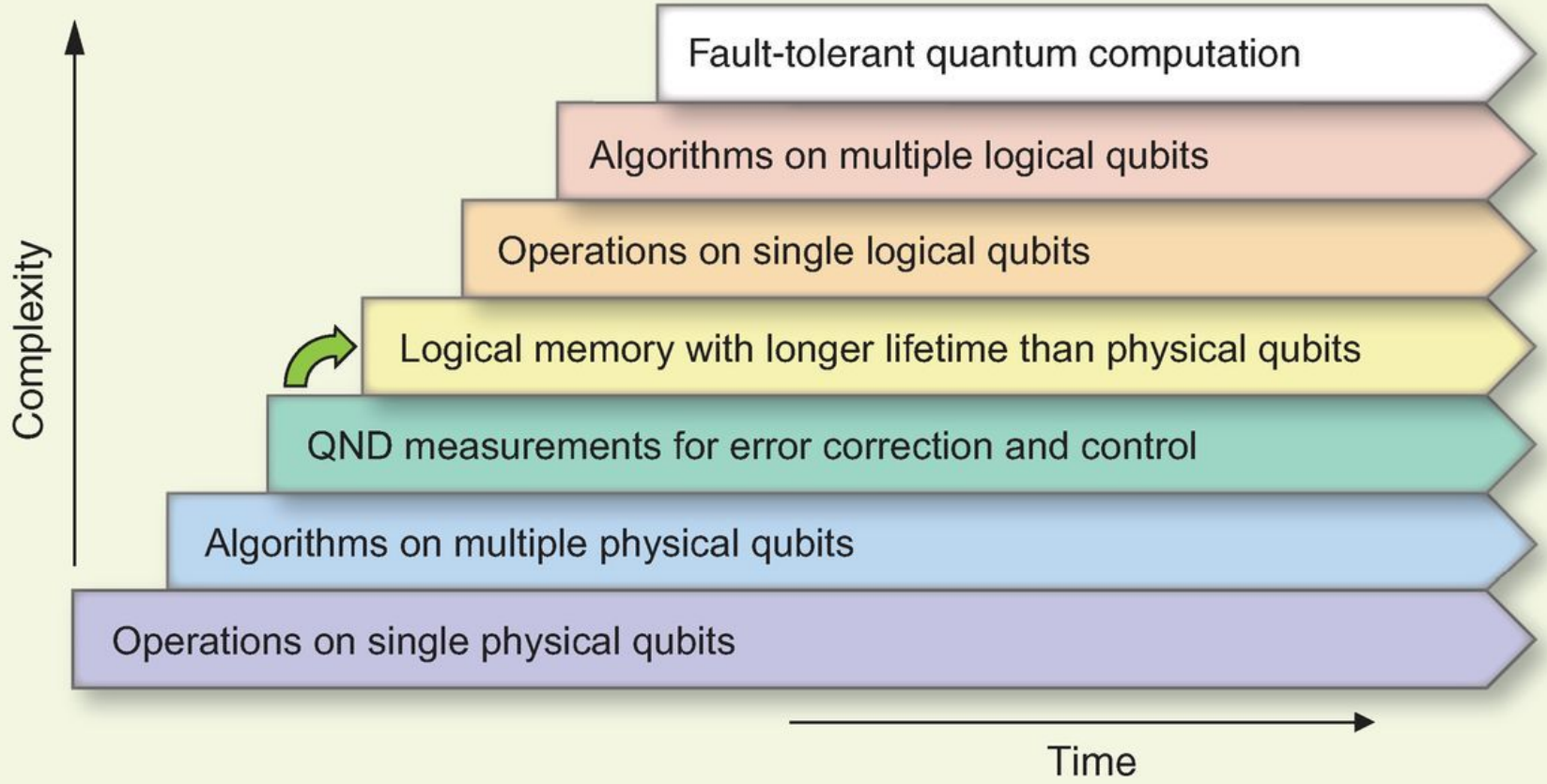
Quantum Computing and Industry Innovators

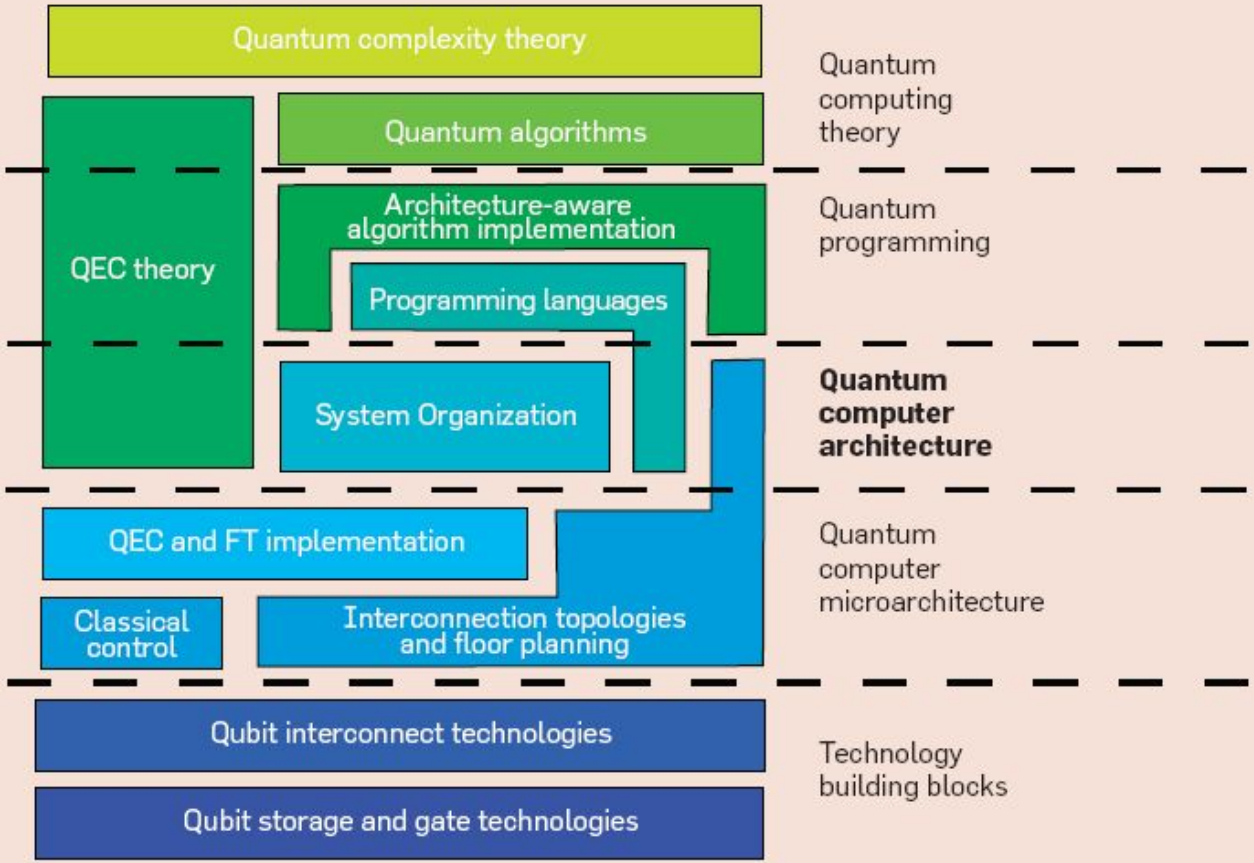
Qubit = A Quantum Bit

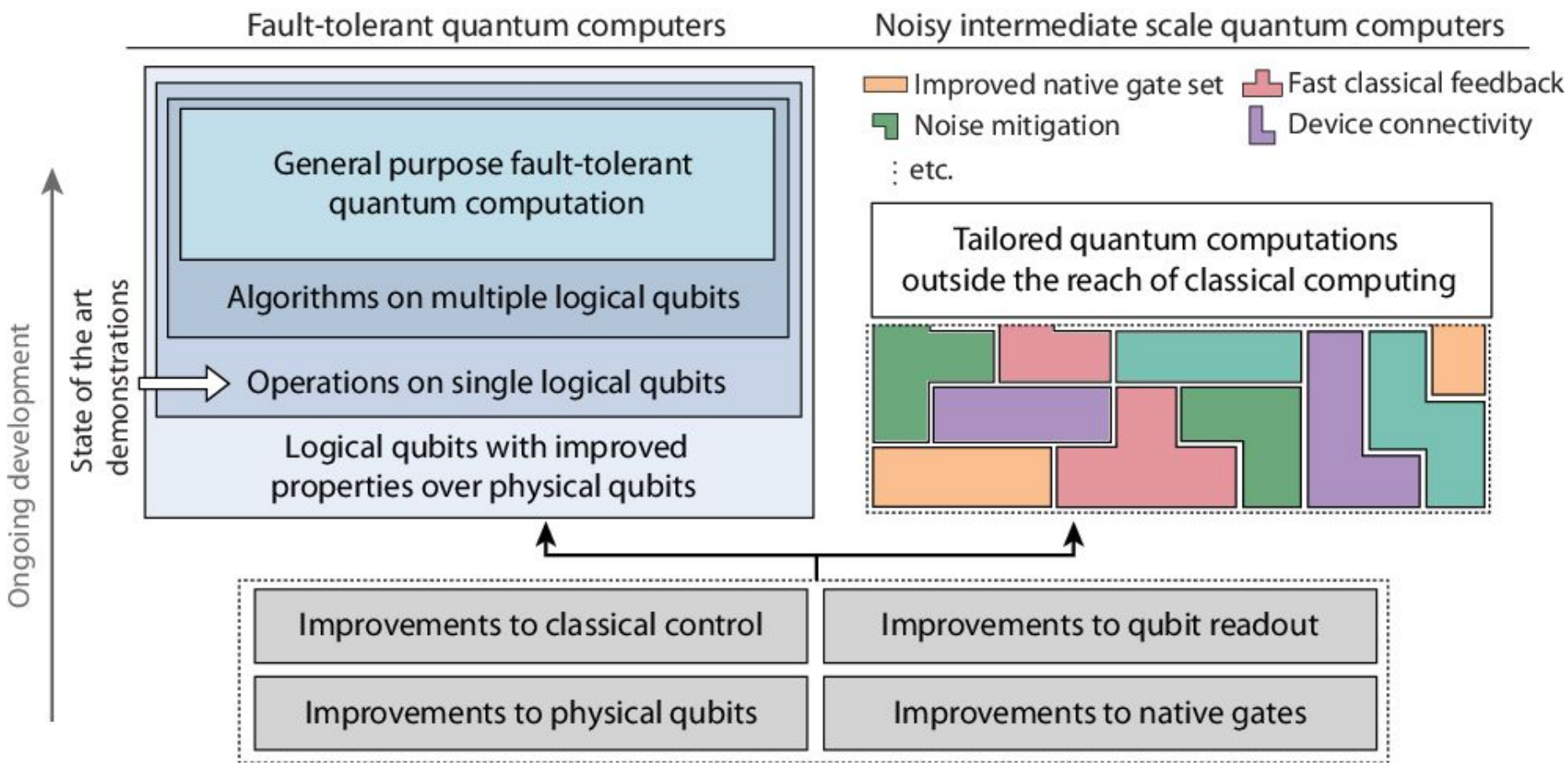


Superconducting loops	Trapped ions	Silicon quantum dots	Topological qubits
Google, IBM, Rigetti, DWave	Honeywell, IonQ	Intel Corporation, HRL	Microsoft

DOI: 10.1126/science.354.6316.1090


Fault-tolerant quantum computation
Algorithms on multiple logical qubits
Operations on single logical qubits
Logical memory with longer lifetime than physical qubits
QND measurements for error correction and control
Algorithms on multiple physical qubits
Operations on single physical qubits
Complexity
Time

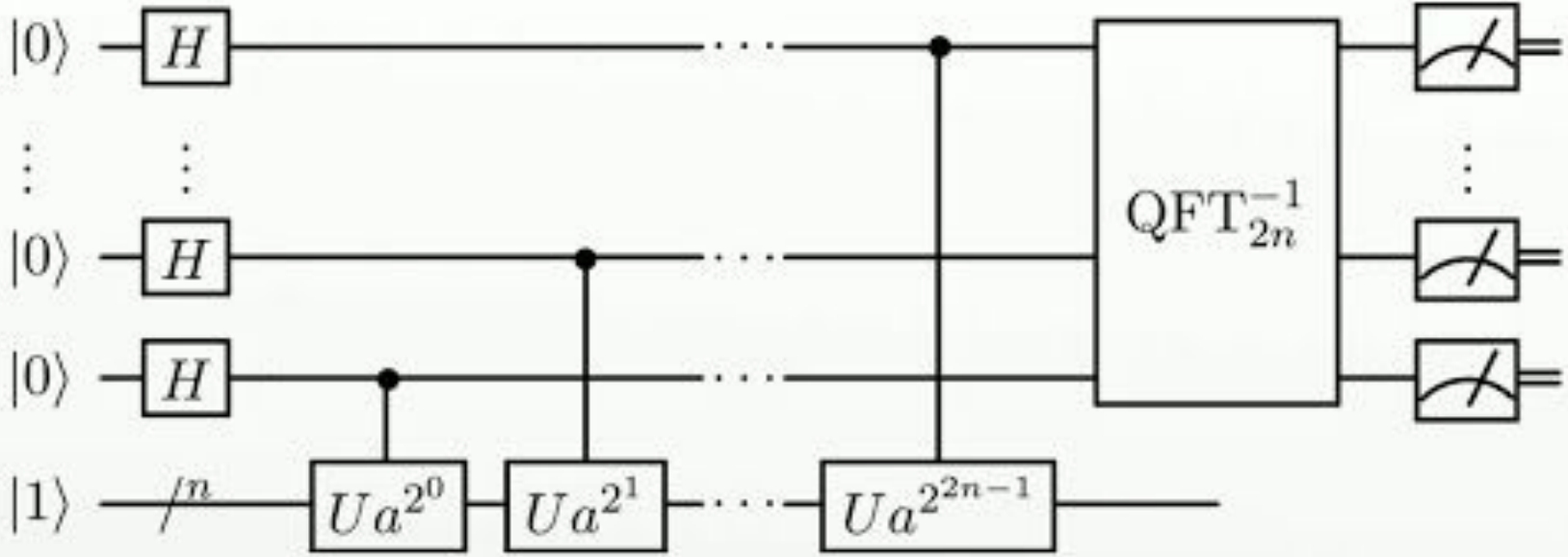

Quantum complexity theory
Quantum algorithms
Quantum computing theory
QEC theory
Architecture-aware algorithm implementation
Programming languages
Quantum programming
System Organization
Quantum computer architecture
QEC and FT implementation
Classical control
Interconnection topologies and floor planning
Quantum computer microarchitecture
Qubit interconnect technologies
Qubit storage and gate technologies
Technology building blocks


Fault-tolerant quantum computers
Noisy intermediate scale quantum computers
Improved native gate set
Fast classical feedback
Noise mitigation
Device connectivity
etc.
General purpose fault-tolerant quantum computation
Algorithms on multiple logical qubits
Operations on single logical qubits
Logical qubits with improved properties over physical qubits
Tailored quantum computations outside the reach of classical computing
State of the art demonstrations
Ongoing development
Improvements to classical control
Improvements to qubit readout
Improvements to physical qubits
Improvements to native gates

History

- In 1994, Peter Shor published an algorithm that is able to efficiently solve some problems that are used in asymmetric cryptography that are considered hard for classical computers.
- **Shor's algorithm**, named after mathematician Peter Shor, is a quantum algorithm (an algorithm that runs on a quantum computer) for integer factorization formulated in 1994. Informally it solves the following problem: given an integer N, find its prime factors.

Shor's algorithm

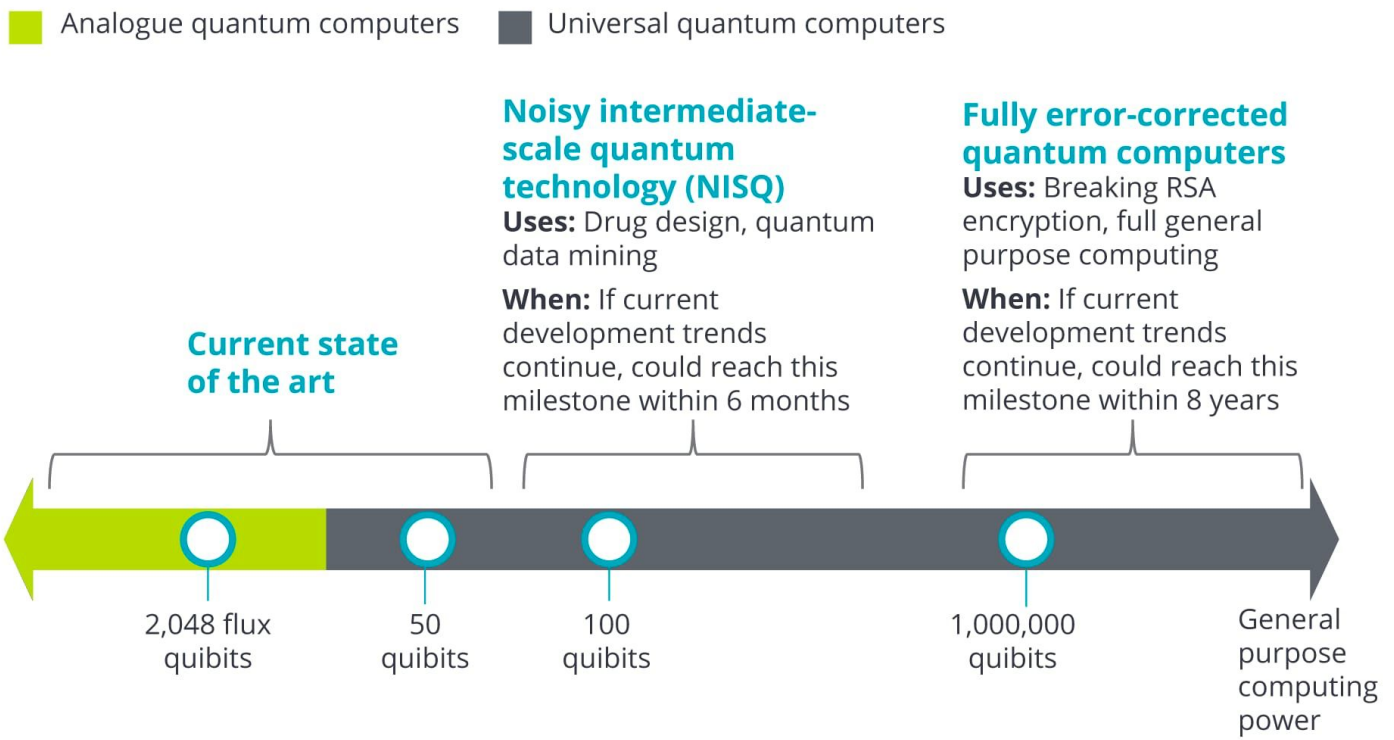


https://en.wikipedia.org/wiki/File:Shor's_algorithm.svg

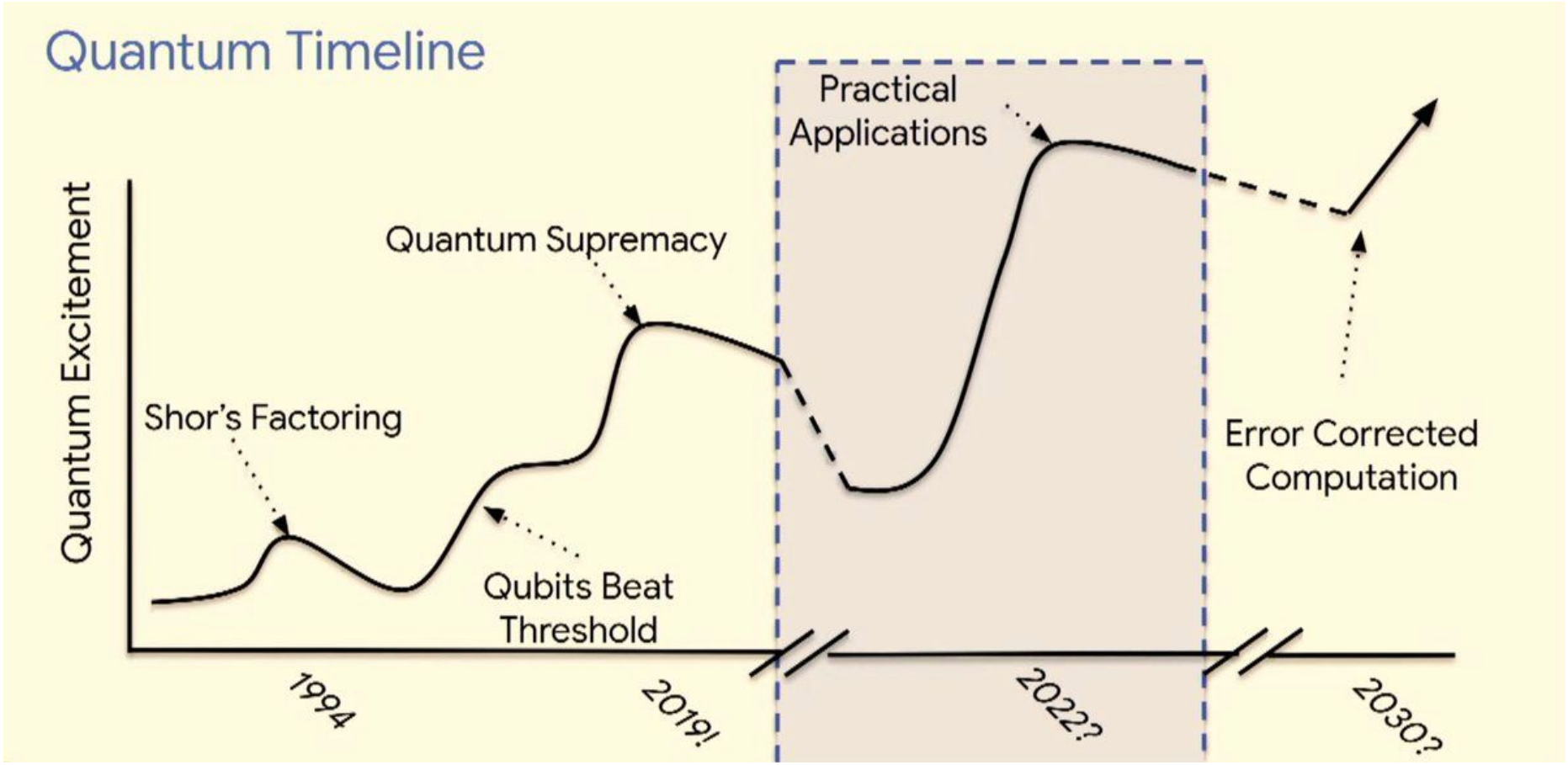
Peter Shor showed that it is possible to factor a number into its primitives efficiently on a quantum computer. This problem is believed to be hard with a conventional computer.

Shor's algorithm was the first demonstration that Quantum Computers are fundamentally more powerful than conventional computers, launching an explosion of both theoretical and experimental interests in the field.

Quantum computers vary in how they can be used



Source: Deloitte analysis.


Quantum Timeline
Quantum Excitement
Shor's Factoring
Quantum Supremacy
Qubits Beat Threshold
Practical Applications
Error Corrected Computation
1994
2019!
2022?
2030?

Problem Statement

Most popular public key algorithms can be efficiently broken by sufficiently strong hypothetical quantum computers

The reasons being that most of them relied on three hard mathematical problems:

- Integer Factorisation Problem
- Discrete Logarithm Problem
- Elliptic Curve Discrete Logarithm Problem

Traditional Crypto Assumptions

Factoring:

Given N = pq, find p, q –

- RSA Given N = pq, e, x^e mod N, find x. •

Discrete Log:

Given g^x mod p, find x. –

- Diffie-Hellman Assumptions (g^x , g^y , g^xy), (g^x , g^y , g^z)

Algorithmic Advances of Quantum Era!

Factoring : Best Algorithm Time 2^O(n^⅓) to factor n-bit number

Discrete Log : Best Algorithm 2 ^O(n^⅓) for groups Zp*, where p is in bits

Shor's Algotithm solves both factoring and discrete log in quantum polynomial time (O(n^2)).

Broken & Impacted Algorithms

The emergence of quantum computers would break all asymmetric public key cryptography and signature algorithms used today - the type of cryptography that protects communications over the internet.

The size of symmetric keys is also halved, meaning the strength of 256-bit keys . This is the type of cryptography used for Full Disk Encryption, when data is encrypted with a passphrase,

All current generation symmetric cryptographic authentication modes such as CBC-MAC, PMAC, GMAC, GCM, and OCB are completely broken.

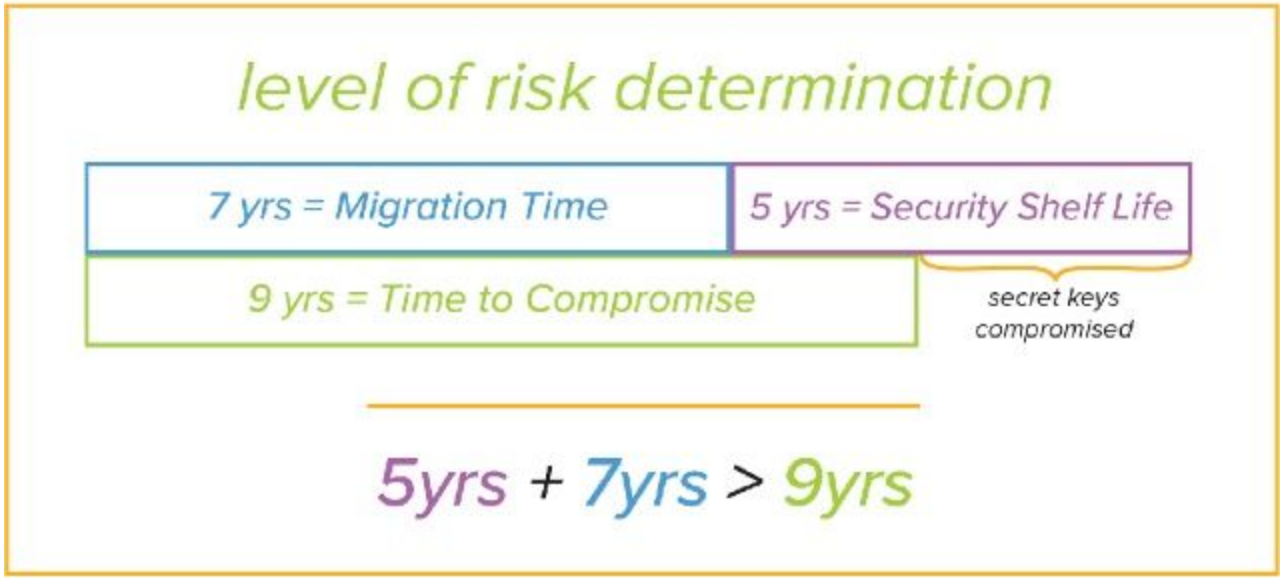
Table 1: Security Comparison						
Type of Attack	Symmetric Encryption			Public Key Encryption		
		Key Length	Bits of Security		Key Length	Bits of Security
Classical Computers	AES-128	128	128	RSA-2048	2048	112
	AES-256	256	256	RSA-15360	15,360	256
Quantum Computers	AES-128	128	64	RSA-2048	2048	25
	AES-256	256	128	RSA-15360	15,360	31

Type	Algorithm	Key Strength Classic (bits)	Key Strength Quantum (bits)	Quantum Attack
Asymmetric	RSA 2048	112	o	Shor's Algorithm
	RSA 3072	128		
	ECC256	128		
	ECC 521	256		
Symmetric	AES128	128	64	Grover's Algorithm
	AES 256	256	128	

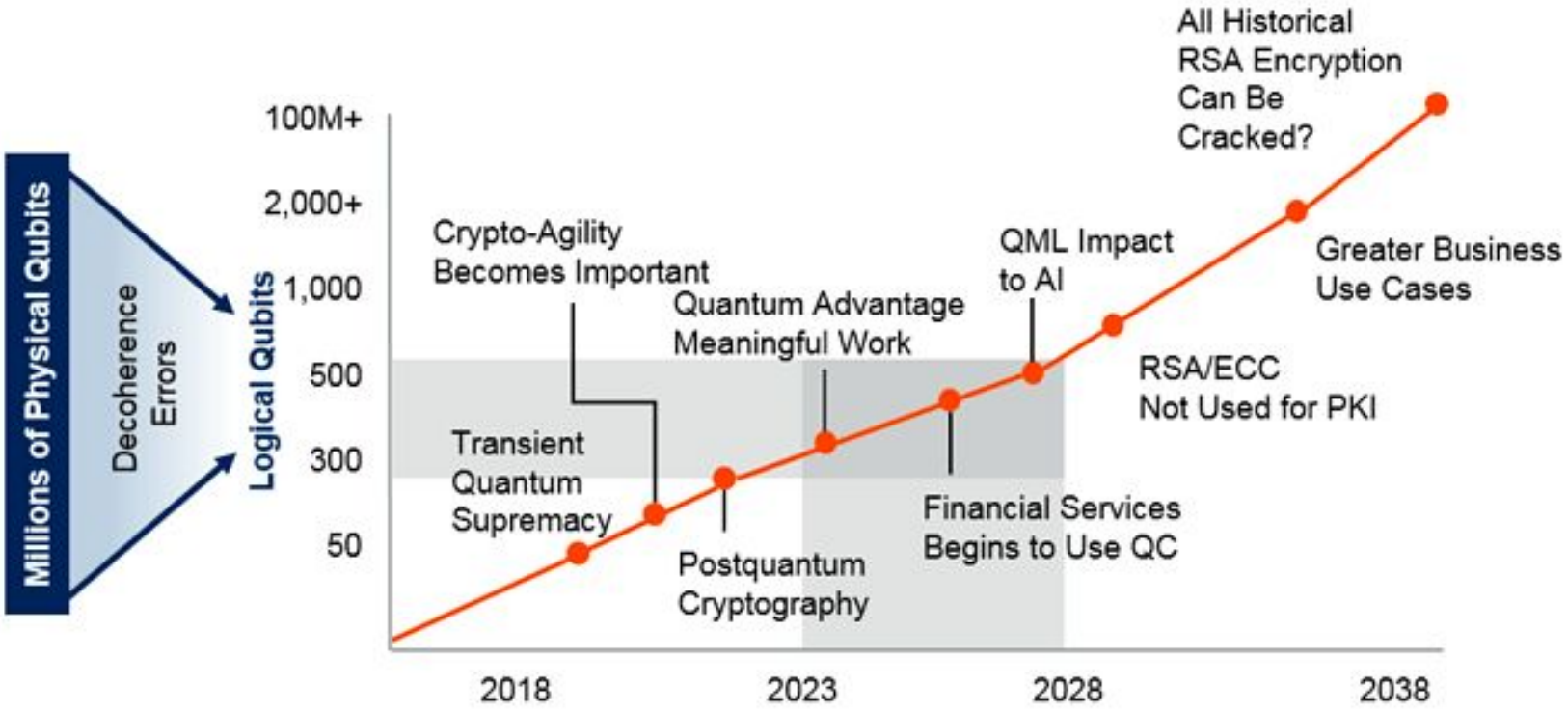
Cryptosystem	Category	Key Size	Security Parameter	Quantum Algorithm Expected to Defeat Cryptosystem	# Logical Qubits Required	# Physical Qubits Required	Time Required to Break System	Quantum-Resilient Replacement Strategies
AES-GCM	Symmetric encryption	128 192 256	128 192 256	Grover's algorithm	2,953 4,449 6,681	4.61×10^6 1.68×10^7 3.36×10^7	2.61×10^{12} yrs 1.97×10^{22} yrs 2.29×10^{32} yrs	
RSA	Asymmetric encryption	1024 2048 4096	80 112 128	Shor's algorithm	2,290 4,338 8,434	2.56×10^6 6.2×10^6 1.47×10^7	3.58 hours 28.63 hours 229 hours	Move to NIST-selected PQC algorithm when available
ECC Discrete -log problem	Asymmetric encryption	256 386 512	128 192 256	Shor's algorithm	2,330 3,484 4,719	3.21×10^6 5.01×10^6 7.81×10^6	10.5 hours 37.67 hours 95 hours	Move to NIST-selected PQC algorithm when available
SHA256	Bitcoin mining	N/A	72	Grover's algorithm	2,403	2.23×10^6	1.8×10^4 years	
PBKDF2 with 10,000 iteration	Password hashing	N/A	66	Grover's algorithm	2,403	2.23×10^6	2.3×10^7 years	Move away from passwordbased authentication

“There is a 1 in 7 chance that some fundamental public-key crypto will be broken by quantum by 2026, and a 1 in 2 chance of the same by 2031.”

- Dr. Michele Mosca, U. of Waterloo

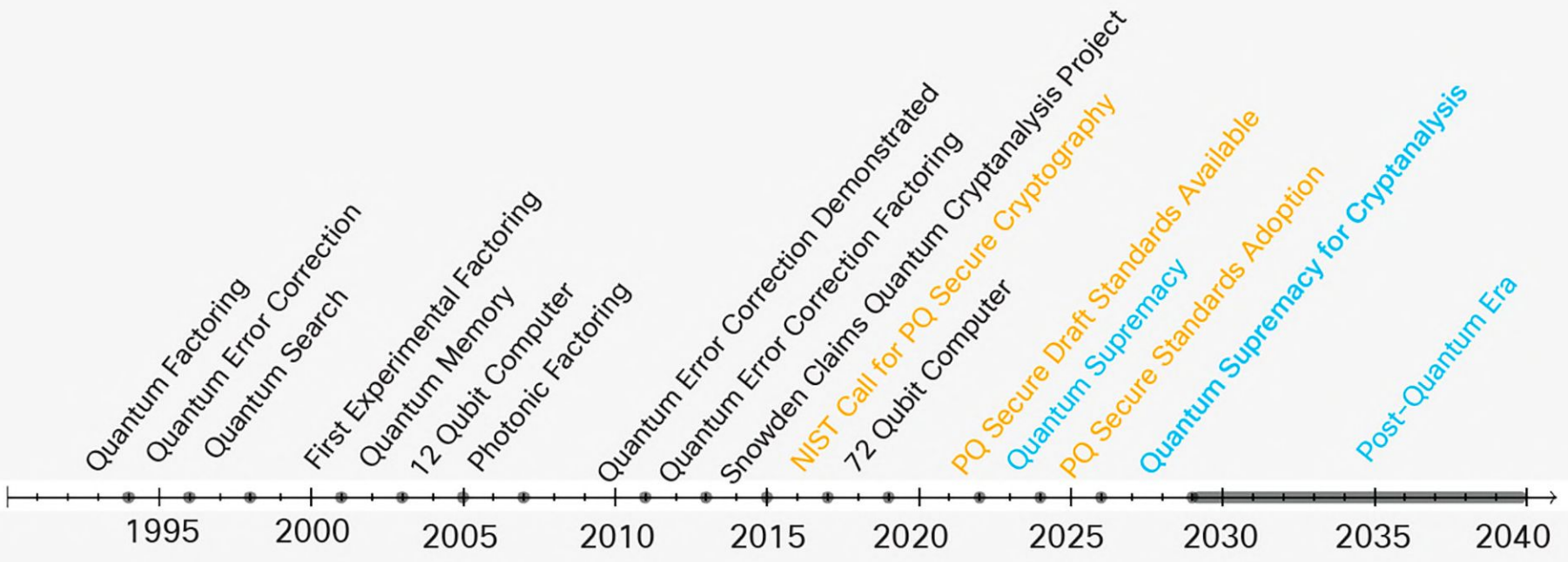

level of risk determination
7 yrs = Migration Time
5 yrs = Security Shelf Life
9 yrs = Time to Compromise
secret keys compromised
5yrs + 7yrs > 9yrs

Qubit Timeline Estimates



Note: Dates are speculative
ID: 374252

Hypothetical PQ-Secure Crypto Standard Timeline



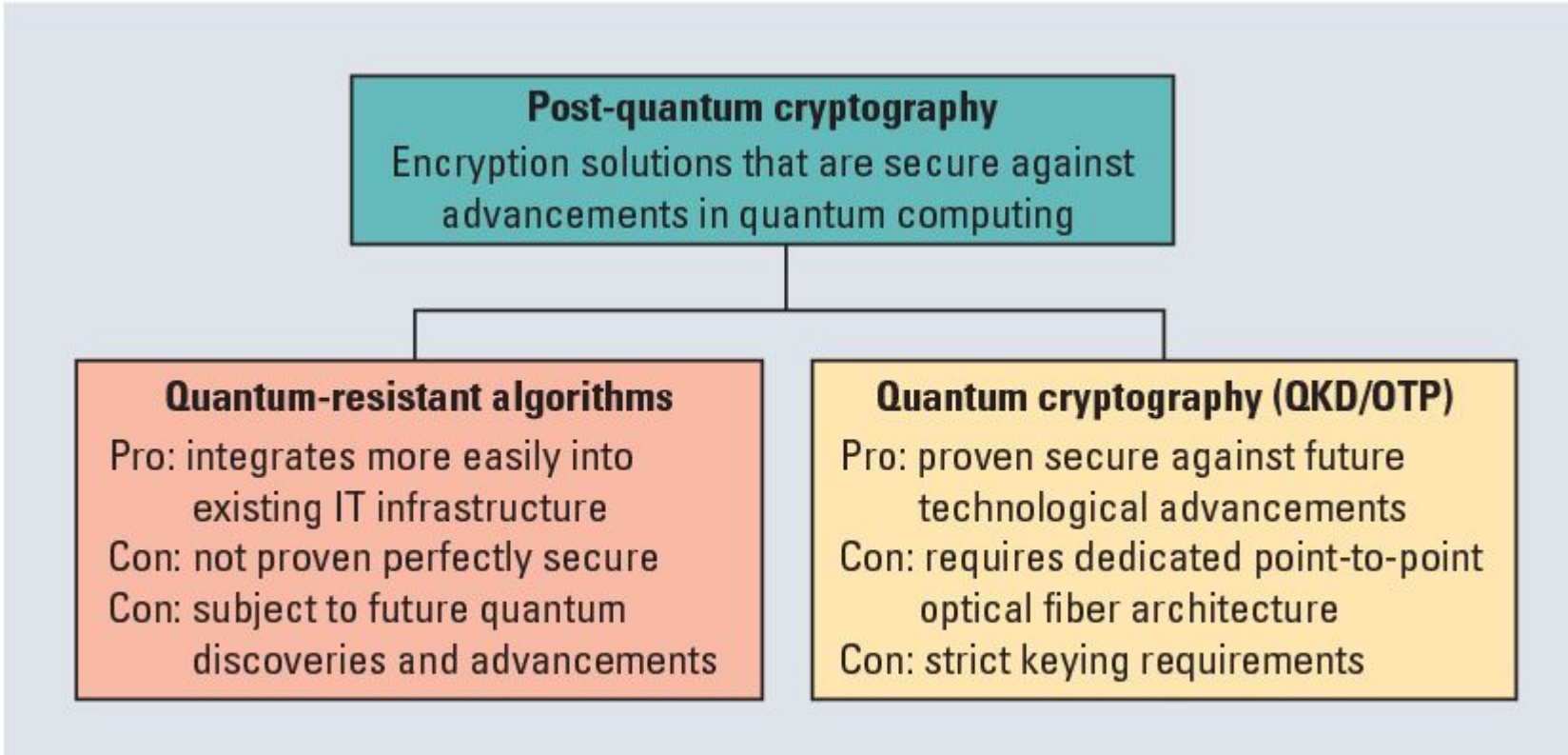
Twin Towers of Post Quantum Cryptography

Post-Quantum Cryptography & Quantum Key Distribution

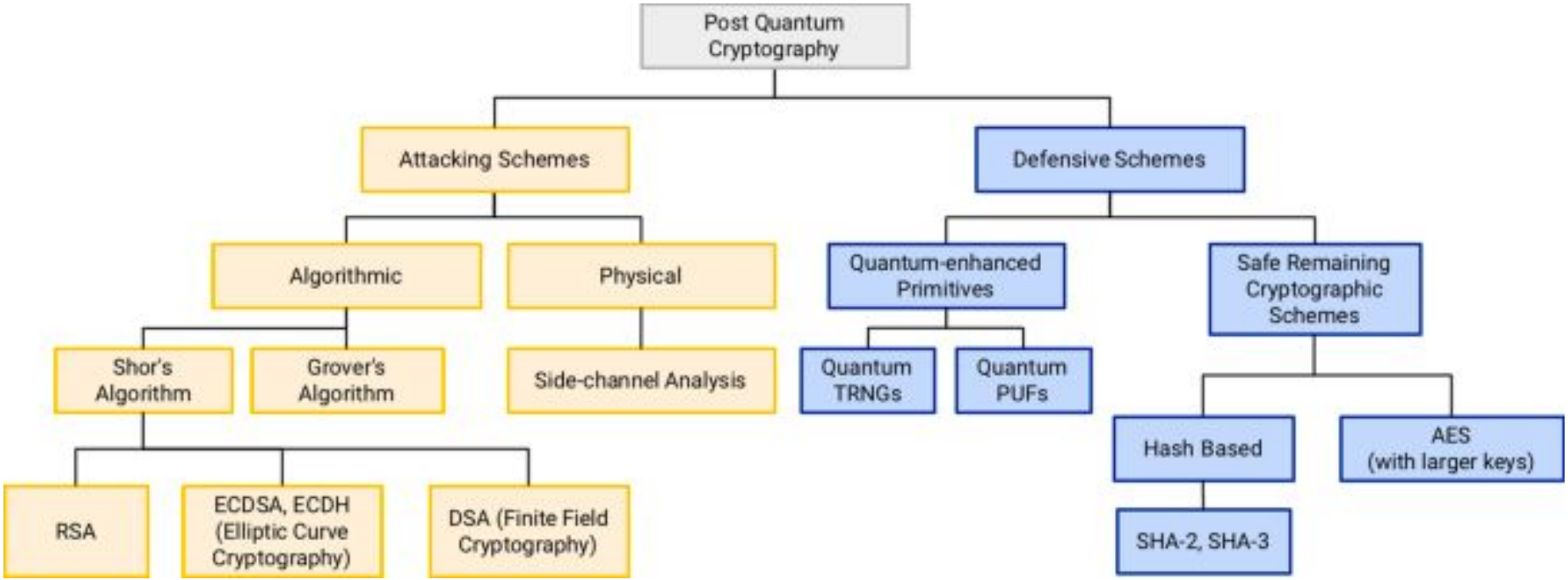
Two different efforts – Why both are not the same?

- **Post-Quantum Cryptography (PQC)**
  - Traditional cryptographic schemes deployable on classical computers and known to be quantum-resistant.
  - Assures mathematical hardness when compared with public-key cryptosystems
  - Security against quantum attacks and impacts of Grover's and Shor's algorithms.

- **Quantum Key Distribution (QKD)**
  - Secure communication using Quantum superposition and entanglements.
    - Encoding information in quantum states and transmission of particles (Over a Physical Quantum channel
    - Generate and secure distribution of keys (Over a QKD link)
  - QKD is not based on traditional computations – It is intrinsically sage
    - Not vulnerable to Shor and Grover.


Post-quantum cryptography
Encryption solutions that are secure against advancements in quantum computing
Quantum-resistant algorithms
Pro: integrates more easily into existing IT infrastructure
Con: not proven perfectly secure
Con: subject to future quantum discoveries and advancements
Quantum cryptography (QKD/OTP)
Pro: proven secure against future technological advancements
Con: requires dedicated point-to-point optical fiber architecture
Con: strict keying requirements

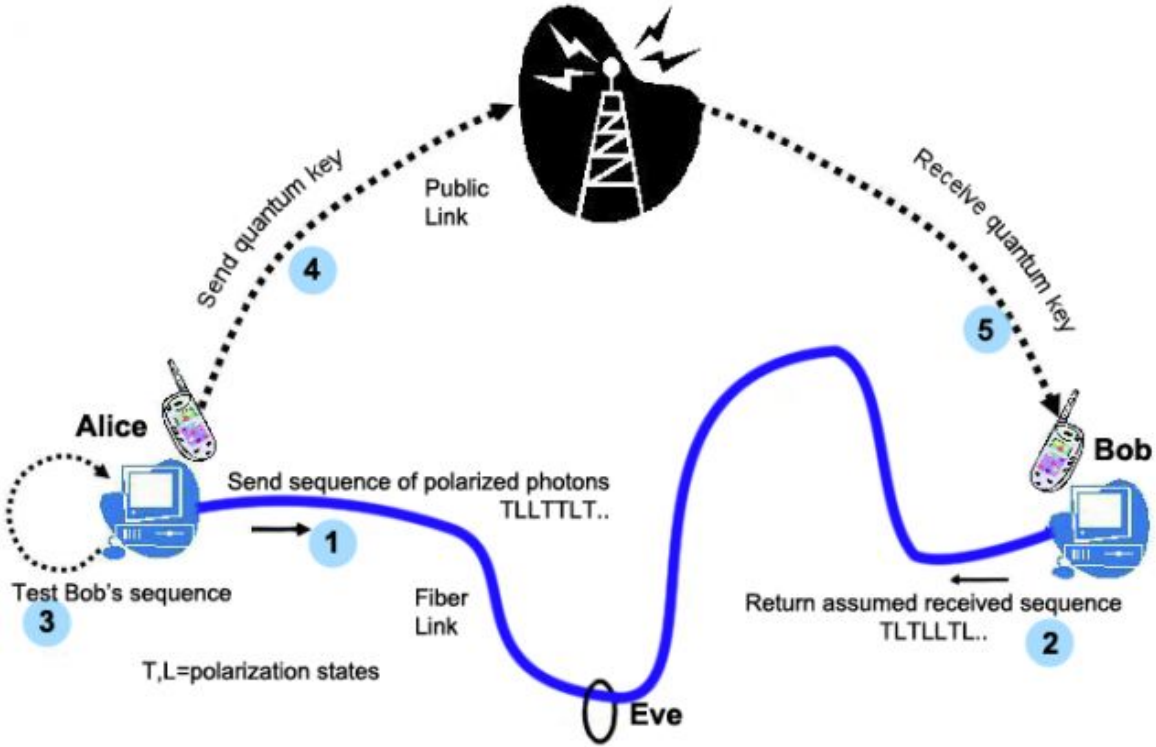
A Different perspective on post quantum crypto!



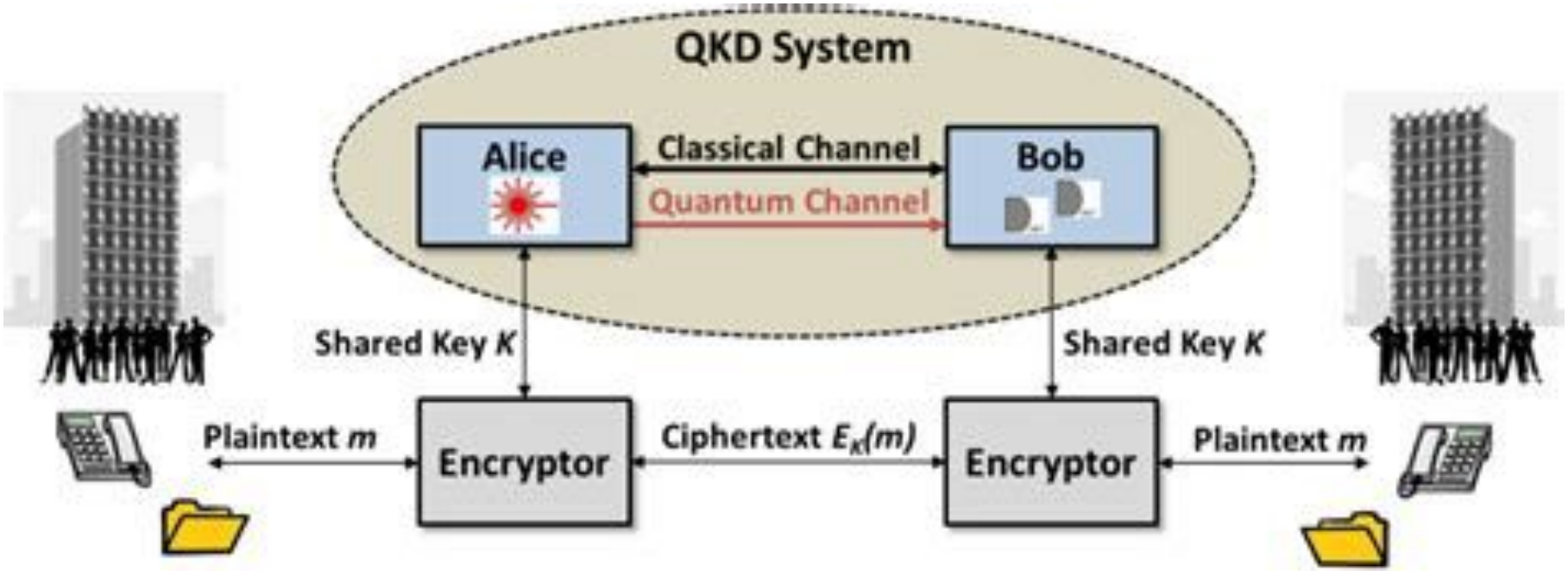
Comparison Metric	PQC	QKD
Security	Algorithms will undergo years of study to determine reliability. However, there is no 100% guarantee that someone would eventually find a way to break it.	Quantum mechanics guarantees that a quantum channel cannot be successful intercepted without detection.
Implementation	Most implementations will be software only. Will not require specialized hardware.	Implementations will required specialized hardware.
Communications Media	Can be used with any type of digital communications media including RF, wired networks, optical communications.	Only works with optical communications; either optical fiber or free space optical.
Cost	Relatively low cost since the solutions will be software based	Higher cost because hardware and a new communications infrastructure will be required
Repeater Compatibility	Full compatible with current digital repeater technology.	Repeater possible by receiving a quantum channel, decoding to classical bits, and re-encrypting and retransmitting to another quantum channel. However, this does create a security risk of interception when the data is in a classical state at the repeater.
Mobile Device Compatibility	Fully compatible with any type of communications used by a mobile device.	Very limited. Could only be used with line-of-sight nodes.
Digital Signature Compatibility	Variations of the standards are being developed specifically for digital signature applications.	Could potentially be used for digital signatures, but use is unlikely for other reasons.

Quantum Assisted Cryptography

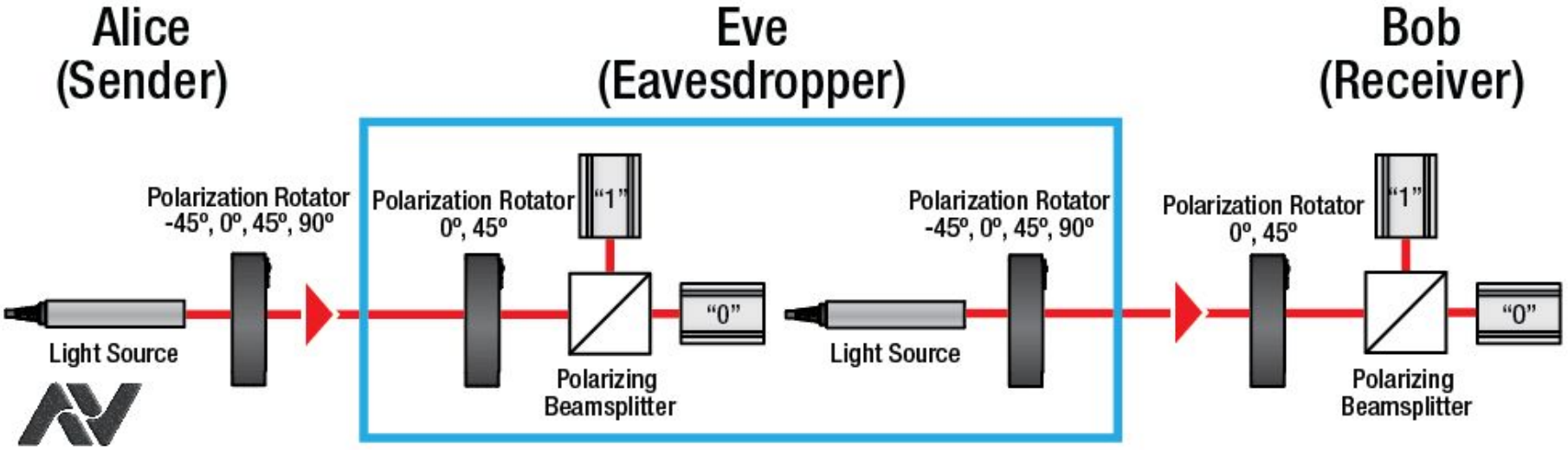
Quantum Cryptography & Communication



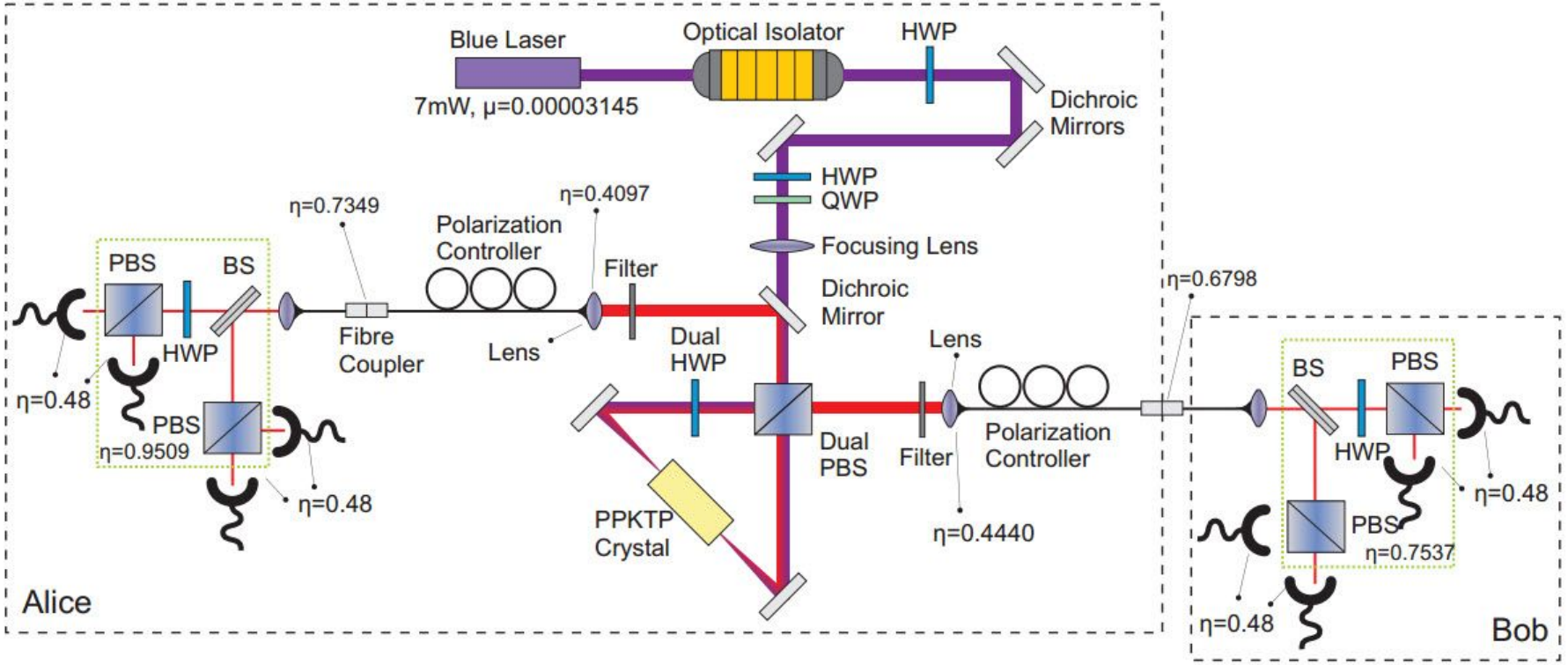
Quantum Key Distribution System



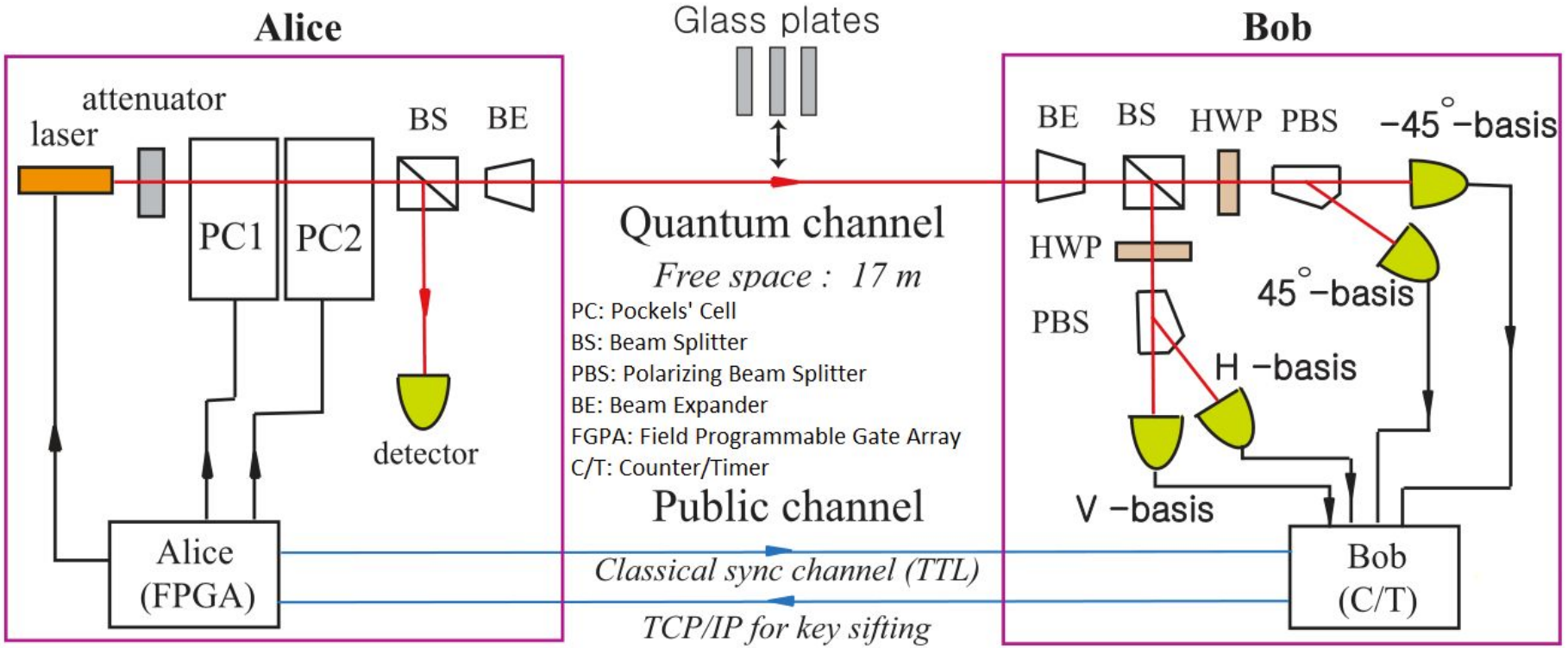
Quantum Cryptography Construction

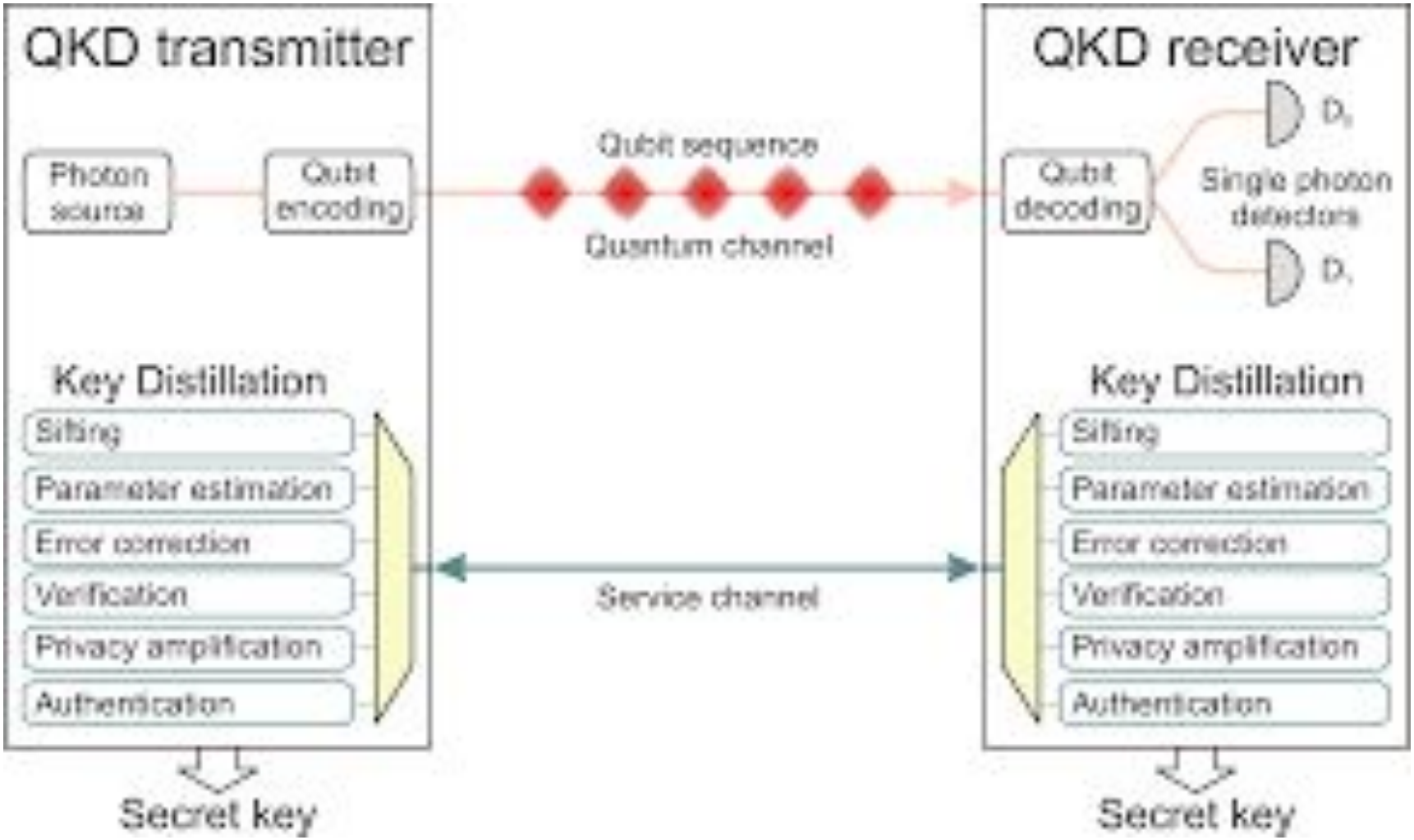


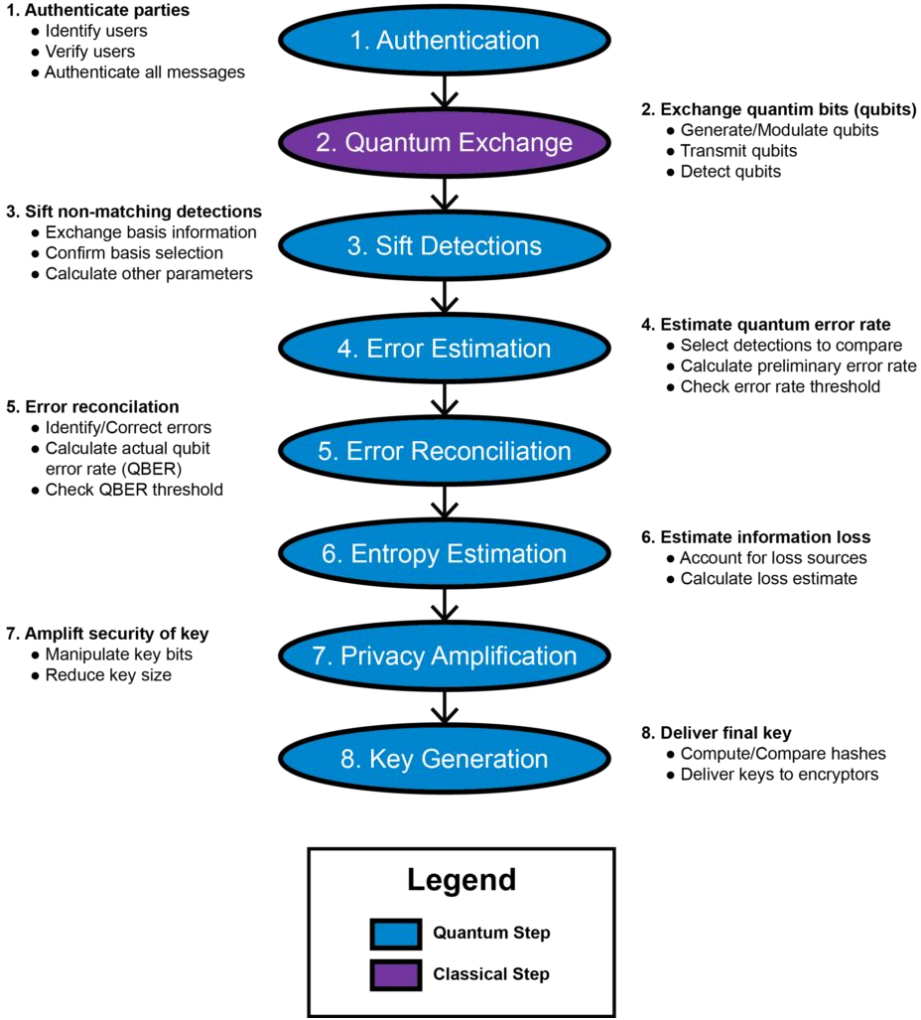
Quantum Optics Implementation



Quantum Circuits and Channels




QKD transmitter
Photon source
Qubit encoding
Qubit sequence
Quantum channel
QKD receiver
Qubit decoding
Single photon detectors
Key Distillation
Sifting
Parameter estimation
Error correction
Verification
Privacy amplification
Authentication
Service channel
Key Distillation
Sifting
Parameter estimation
Error correction
Verification
Privacy amplification
Authentication
Secret key
Secret key


1. Authenticate parties
• Identify users
• Verify users
• Authenticate all messages
1. Authentication
2. Quantum Exchange
2. Exchange quantim bits (qubits)
• Generate/Modulate qubits
• Transmit qubits
• Detect qubits
3. Sift non-matching detections
• Exchange basis information
• Confirm basis selection
• Calculate other parameters
3. Sift Detections
4. Error Estimation
4. Estimate quantum error rate
• Select detections to compare
• Calculate preliminary error rate
• Check error rate threshold
5. Error reconcilation
• Identify/Correct errors
• Calculate actual qubit error rate (QBER)
• Check QBER threshold
5. Error Reconciliation
6. Entropy Estimation
6. Estimate information loss
• Account for loss sources
• Calculate loss estimate
7. Amplift security of key
• Manipulate key bits
• Reduce key size
7. Privacy Amplification
8. Key Generation
8. Deliver final key
• Compute/Compare hashes
• Deliver keys to encryptors
Legend
Quantum Step
Classical Step

Quantum Resistant Cryptography

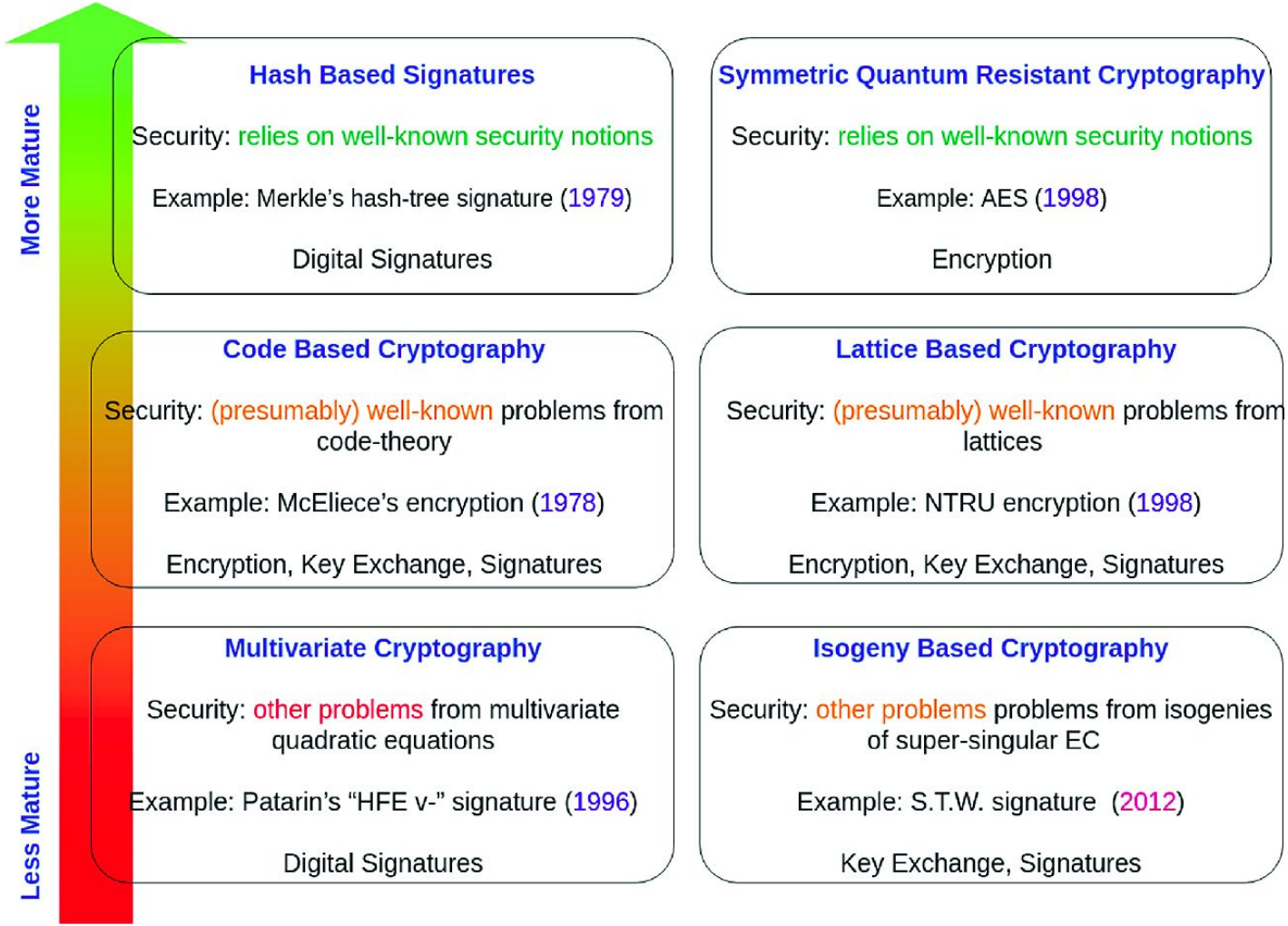
Early Engineering Implementations of PQC

- McElice - Code based Cryptography
- Niederreiter - Code based Cryptography
- NTRU - Lattice Based Cryptography
- Ring LWE - Lattice Based Cryptography
- BLISS - Lattice Based Cryptography
- Rainbow - Multivariate Cryptography
- Lamport Signature - Hash based Cryptography
- Merkle Signature - Hash based Cryptography

Post-Quantum Asymmetric Crypto Algorithms

Known PQC Implementations

PQC Algorithm	Encryption or Key Exchange	Signatures	Known Implementations
Hash-based	-	Yes.	SPHINCS, XMSS
Multi-Variate	-	Yes.	-
Code-based	Yes.	-	QC-MDPC
Supersingular EC Isogeny	Yes	Yes	-
Lattice based	Yes	Yes	NTRU Key Exchange: OQSKEM, Kyber, New Hope, Signatures: Dilithium, BLISM, Tesla


More Mature
Less Mature
Hash Based Signatures
Security: relies on well-known security notions
Example: Merkle's hash-tree signature (1979)
Digital Signatures
Symmetric Quantum Resistant Cryptography
Security: relies on well-known security notions
Example: AES (1998)
Encryption
Code Based Cryptography
Security: (presumably) well-known problems from code-theory
Example: McEliece's encryption (1978)
Encryption, Key Exchange, Signatures
Lattice Based Cryptography
Security: (presumably) well-known problems from lattices
Example: NTRU encryption (1998)
Encryption, Key Exchange, Signatures
Multivariate Cryptography
Security: other problems from multivariate quadratic equations
Example: Patarin's "HFE v-" signature (1996)
Digital Signatures
Isogeny Based Cryptography
Security: other problems problems from isogenies of super-singular EC
Example: S.T.W. signature (2012)
Key Exchange, Signatures

Algorithm	Digital Signature	Key Encapsulation	Key Agreement	Source	Math
HSS	✓			IETF	Stateful Hash-Based
XMSS – XMSSmt	✓			IETF	Stateful Hash-Based
SPHINCS+	✓			NIST	Stateless Hash-Based
Rainbow	✓			NIST	Multivariate-Based
Dilithium	✓			NIST	Lattice-Based
FrodoKEM		✓		NIST	Lattice-Based
NTRU Prime		✓		NIST	Lattice-Based
Kyber		✓		NIST	Lattice-Based
SIKE		✓		NIST	Supersingular Isogeny-Based
Classic McEliece		✓		NIST	Code-Based
NewHopeDH			✓	NIST Variant	Lattice-Based
SIDH			✓	NIST Variant	Supersingular Isogeny-Based
FrodoDH			✓	NIST Variant	Lattice-Based

Code Based Cryptography

The McEliece method uses code-based cryptography. Its foundation is based on the difficulty in decoding a general linear code and is faster than RSA for encryption and decryption.

The McEliece method uses linear codes that are used in error correcting codes, and involves matrix-vector multiplication. An example of a linear code is Hamming code

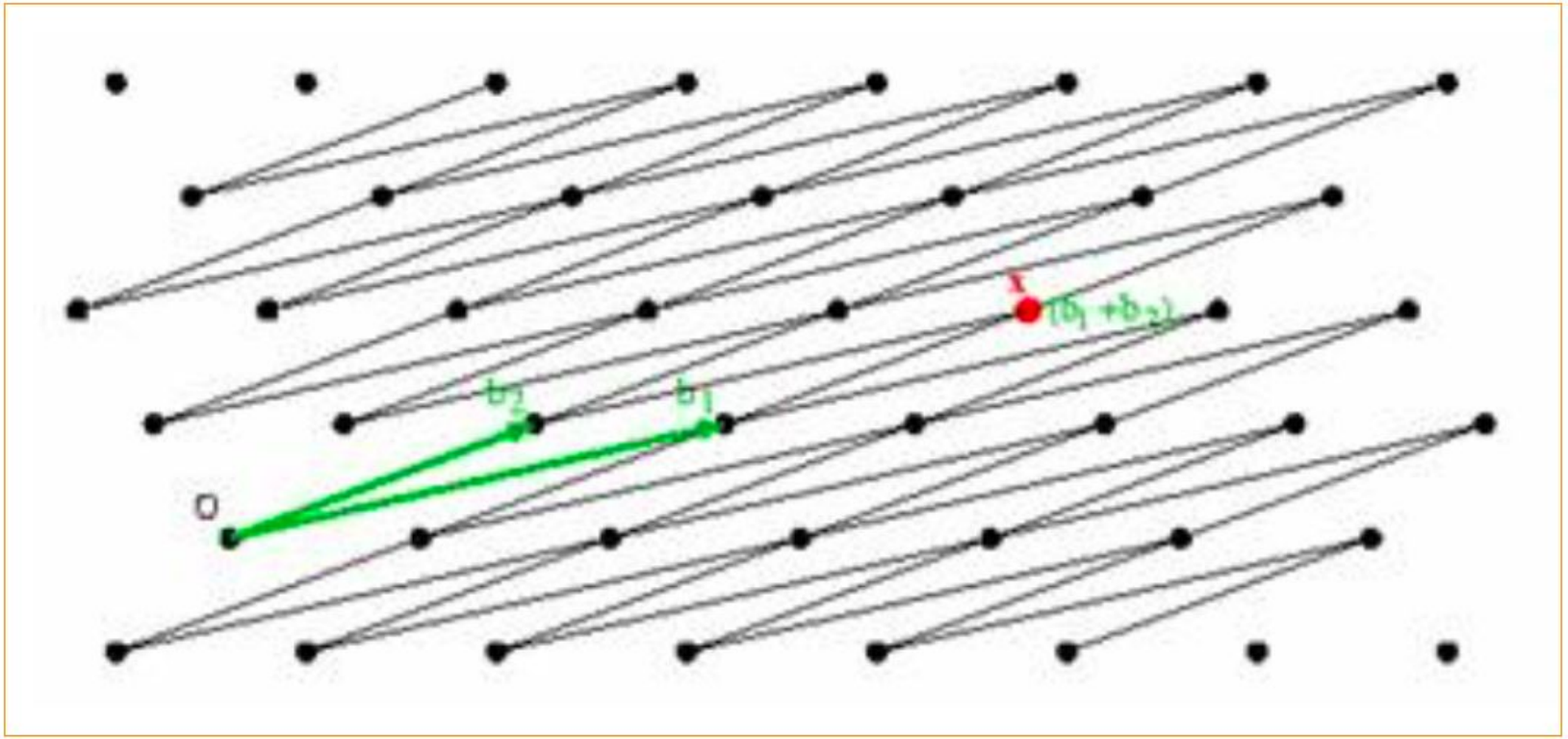
Within this method, we have a probabilistic key generation method, which is then used to produce the public and the private key.

A Public-Key Cryptosystem Based On Algebraic Coding Theory

R. J. McEliece
Communications Systems Research Section

Using the fact that a fast decoding algorithm exists for a general Goppa code, while no such exists for a general linear code, we construct a public-key cryptosystem which appears quite secure while at the same time allowing extremely rapid data rates. This kind of cryptosystem is ideal for use in multi-user communication networks, such as those envisioned by NASA for the distribution of space-acquired data

Lattice Cryptography



Introduction to Lattices

An n-dimensional lattice L is an additive discrete subgroup of R^n.

A basis $\boldsymbol{B} \in R^{n \times n}$ defines a lattice L($\boldsymbol{B}$) in the following way:

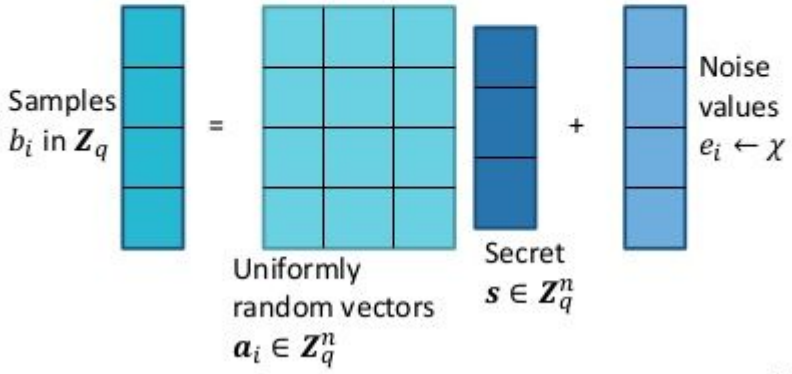
L(B) = { v ∈ R^n s.t. V = Bz for some z ∈ Z^n}

Integer linear combination of the basis vectors

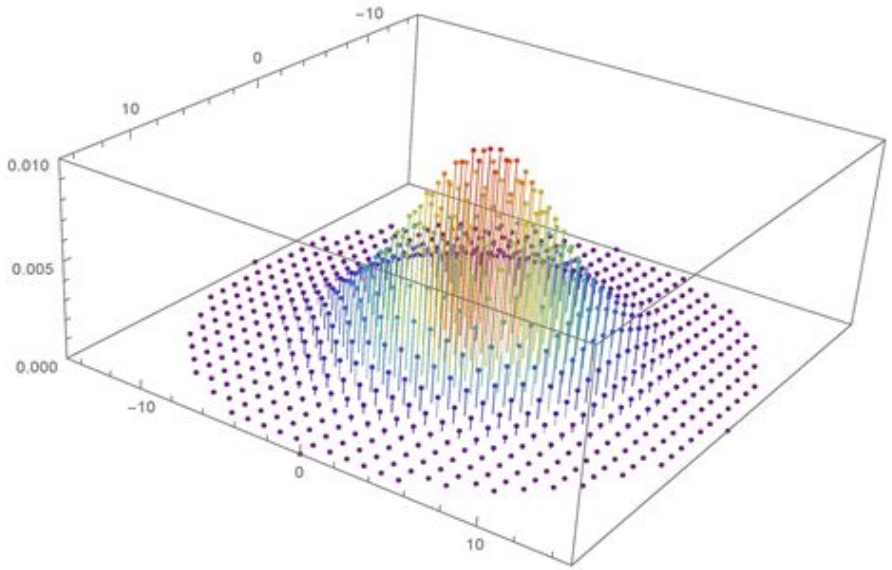
Learning With Errors from Lattices

$$b_i = \langle \boldsymbol{a}_i, \boldsymbol{s} \rangle + e_i$$

$$\boldsymbol{b} = A\boldsymbol{s} + \boldsymbol{e}$$



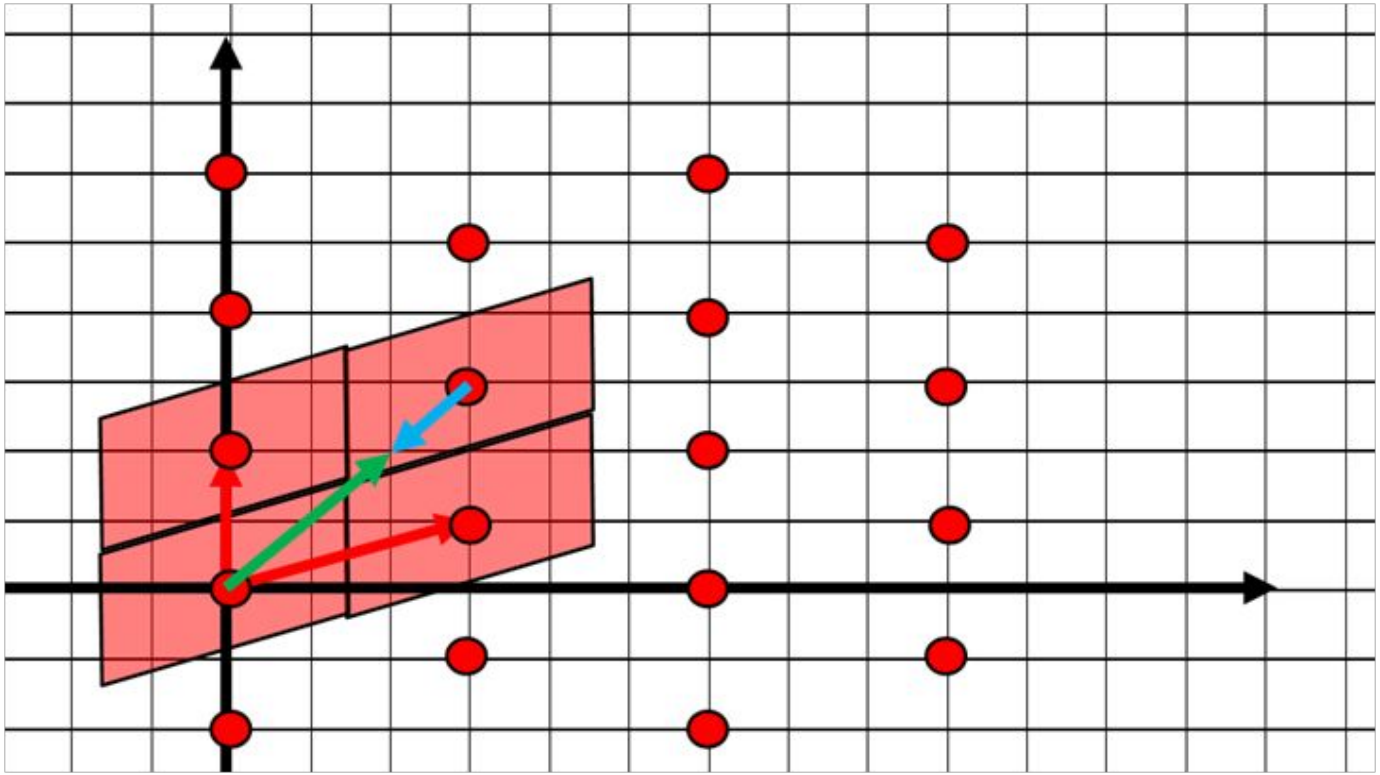
Visualisation of Lattices



Hard Lattice Problems

- All are parameterized by approximation factor y > 1
- Shortest Vector Problem (SVP) :
  - Given a basis B, find a non-zero vector v ∈ L(B) whose length is atmost y
  - λ1 (L(B)
- Shortest Independent Vector Problem (SIVP)
  - Given a basis B, find a linearly independent set {v1, ..., vn} such that all vectors have length at most $\boldsymbol{\gamma}$. λ(n)(L(B)).
- Gap Shortest Vector Problem (GapSVP):
  - Given a basis B, and a radius r>0
    - Return YES, if λ1 (L(B)) ≤ r
    - Return NO if λ1 (L(B)) ≥ $\boldsymbol{\gamma}$. r.

Navigating through the Lattice



Lamport Signature Scheme

- Lamport Signatures are an elegant use of cryptographically-secure hash functions.
  - Functions that may be applied to data which generate an output of a known size, which is unique to the input, without revealing anything useful about the input itself, and without being able to deliberately design an input to get a desired output.
- While the hash of a certain piece of data may be a constant thing, you cannot theoretically determine what data has been hashed unless you have a copy of the original data to compare against on hand.
  - You cannot (with any reasonable amount of effort) find an alternative input which generates the same hash output, except through a level of brute-force trial-and-error which would take longer than a human lifespan at least with exceptionally powerful computing resources at your disposal.

Lamport Signature Scheme

- In order to use this to generate a secure digital signature scheme, the Lamport Signature scheme uses hashes to declare knowledge of a set of secret numbers, some of which are then revealed along with a message that is intended to be signed.
- Specifically, the scheme uses large sets of pairs of numbers, and reveals one from each pair depending on the value of the message to be signed.
- Readers can then compare the message, the secret numbers, and the previously and publicly disclosed hashes of the secret keys, to prove that the message could only have been signed by a person who knew all of the secret numbers; ergo, the "owner" of the private key.

SIKE

- SIKE is a family of post-quantum key encapsulation mechanisms based on the Supersingular Isogeny Diffie-Hellman (SIDH) key exchange protocol.
- The algorithms use arithmetic operations on elliptic curves defined over finite fields and compute maps, so-called isogenies, between such curves.
- The security of SIDH and SIKE relies on the hardness of finding a specific isogeny between two such elliptic curves, or equivalently, of finding a path between them in the isogeny graph.
- This problem is different from that of computing discrete logarithms on a single elliptic curve and is believed to be hard to solve with both classical and quantum computers.

NTRU

- Nth degree truncated polynomial ring public key method
- It uses shortest vector problem in a lattice
- Related to the difficulty in factoring polynomials
  a. Bob and Alice agree to share N, p and q
  b. Bob generates two short polynomials (f and g) and generates his key pair from this.
  c. Alice receives this, and she generates a random polynomial
  d. Alice encrypts some data for Bob.
  e. Bob then decrypts the message with his private key.
  f. We generate the public and private key from N, p and q:

Post-Quantum Asymmetric Crypto Algorithms

Quantum-resistant Crypto schemes without factorization and discrete logarithms

☑ Lattice-based Cryptography

- Proposed by M.Ajtai 1996, one of the early cryptographic schemes relied on the hardness of computational lattice problems
- In 2005, Regev introduced the Learning With Errors (LWE) based on Lattice problem which serves as the basis for a variety of public-key encryption and signature schemes
- Following LWE, in 2010, Lyubashevsky, Peikert, and Regev introduced the Ring-Learning With Errors (Ring-LWE) which used an additional structure that allows for smaller key sizes.

☑ Multi-variate Cryptography

- Based on the difficulty of solving non-linear usually quadratic, polynomial over a finite field.
- The hardness of the system depends on the size of the finite field, variables and the degree of the system. .
- For building asymmetric public key system, the public key is a set of multivariate quadratic polynomials and the private key is the knowledge of a trapdoor that allows solving the multi-variate system.

qTESLA

qTESLA is a family of efficient post-quantum digital signature schemes, with security based upon the hardness of the decisional Ring Learning With Errors (R-LWE) problem, which in turn relates to hard problems in lattices.

qTESLA is the result of a long line of research, beginning with a signature scheme proposed by Bai and Galbraith in 2014, which is based on the Fiat-Shamir construction of Lyubashevsky (2012).

This construction was used as the basis for an LWE-based instantiation called TESLA (2017) which then was modified and adapted to the setting of the decisional Ring Learning With Error problem, and finally led to the design of the signature scheme qTESLA.

PQ VPN

This project takes a fork of the OpenVPN software and combines it with post-quantum cryptography.

	Signatures	Key Exchange	Fast?
Elliptic Curves	64 bytes	32 bytes	✓
Lattices	2.7kb	1 kb	✓
Isogenies	✗	330 bytes	✗
Codes	✗	1 mb	✓
Hash functions	41 kb	✗	✓

Table 1: Comparison of classical ECC vs post-quantum schemes submitted to NIST

Open Quantum Safe Project

Integrations for OpenSSL and OpenSSH

TLS 1.2 prototype and available as a fork for OpenSSL

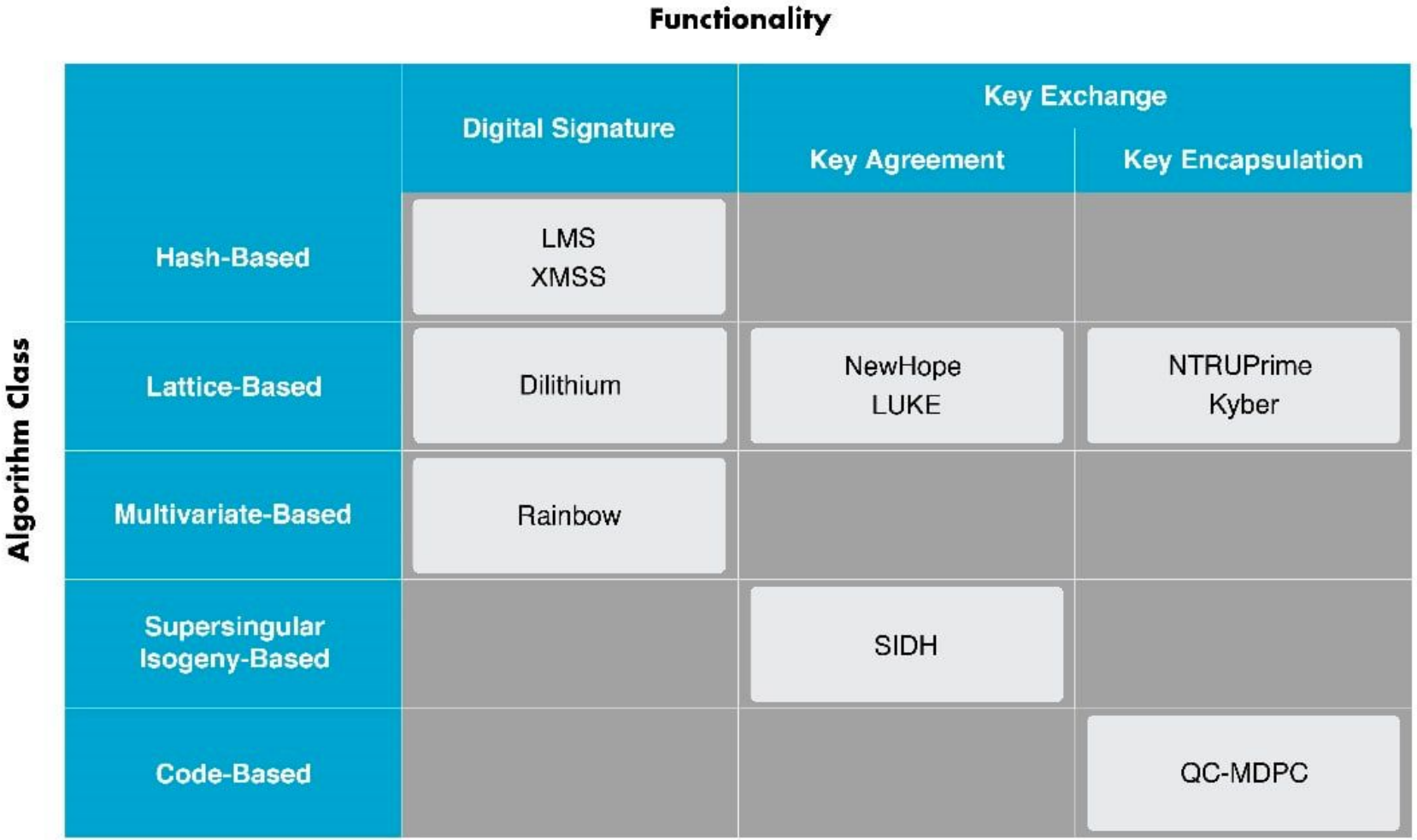
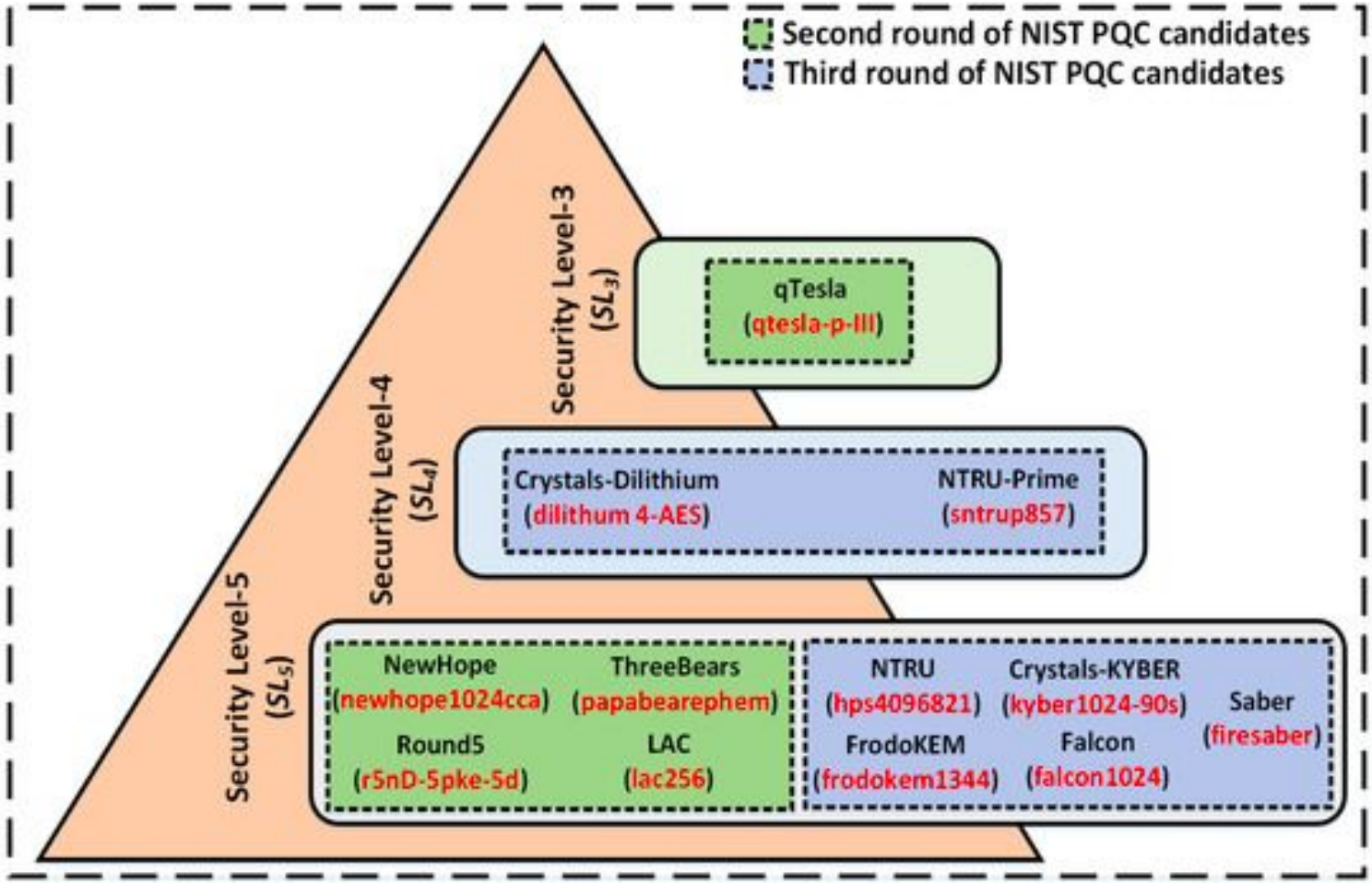
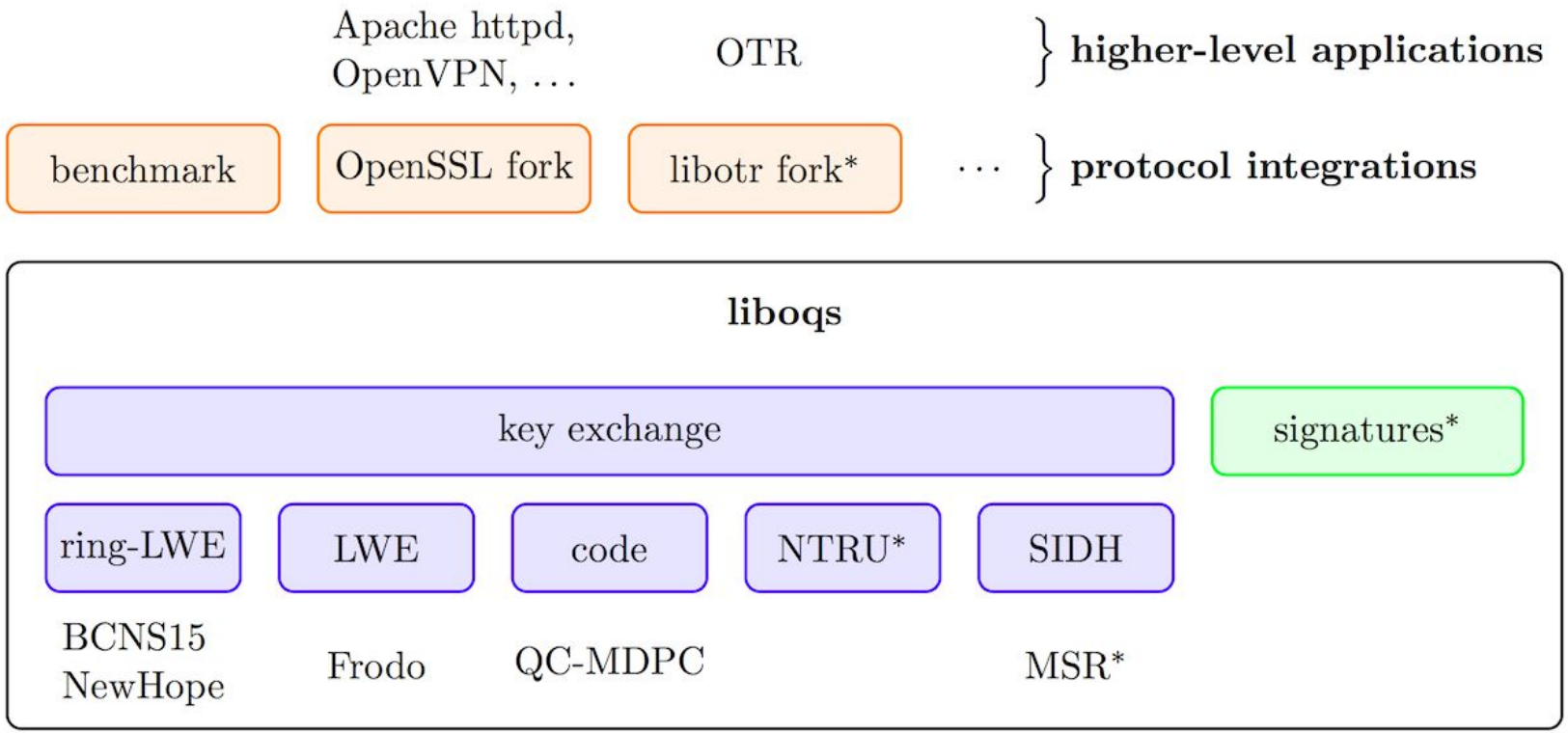

Functionality
Algorithm Class
Digital Signature
Key Exchange
Key Agreement
Key Encapsulation
Hash-Based
LMS
XMSS
Lattice-Based
Dilithium
NewHope
LUKE
NTRUPrime
Kyber
Multivariate-Based
Rainbow
Supersingular
Isogeny-Based
SIDH
Code-Based
QC-MDPC

Table 1: A Comparison of Public Key Cryptographic Algorithms at the 80 Bit Security Level

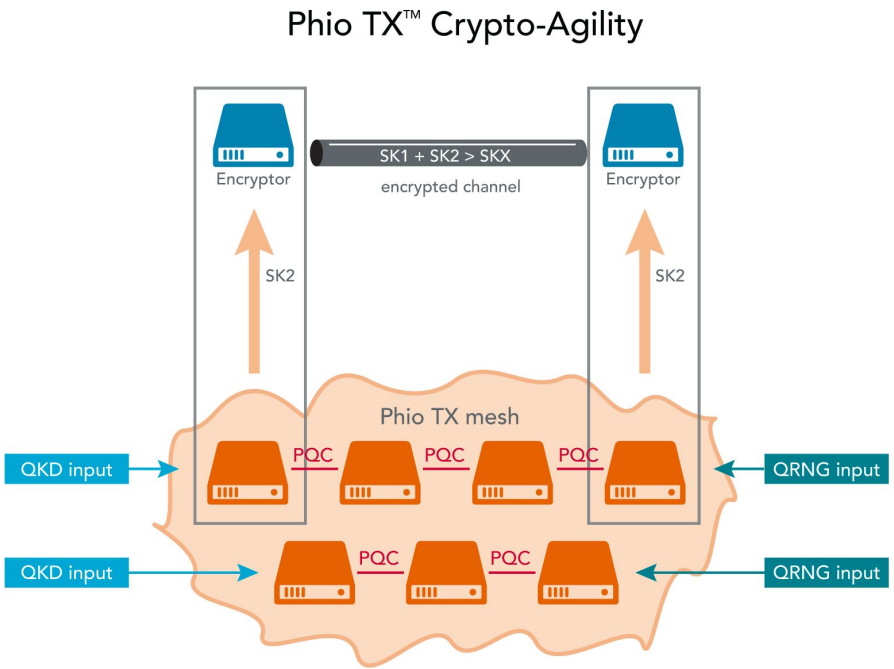
	Estimated Time (PC)						
	Setup (ms)	Public Key Operation (ms)	Private Key Operation (ms)	Limited Lifetime?	Public Key Size (kbits)	Private Key Size (kbits)	Message Size (kbits)
Lamport Signature	1	1	1	1 signature	~10	~10	~10
Lamport w/Merkle	1	1	1	2^{40} signatures	0.08	~250	~50
McEliece Encryption	0.1	0.01	0.1	no	500	1000	1
McEliece Signature	0.1	0.01	20,000	no	4000	4000	0.16
NTRUEncrypt	0.1	0.1	0.1	no	2	2	2
NTRUSign	0.1	0.1	0.1	2^{30} signatures	2	2	4
RSA	2000	0.1	5	no	1	1	1
DSA	2	2	2	no	2	0.16	0.32
Diffie-Hellman	2	2	2	no	2	0.16	1
ECC	2	2	2	no	0.32	0.16	0.32


Second round of NIST PQC candidates
Third round of NIST PQC candidates
Security Level-3 (SL_3)
Security Level-4 (SL_4)
Security Level-5 (SL_5)
qTesla
(qtesla-p-III)
Crystals-Dilithium
(dilithum 4-AES)
NTRU-Prime
(sntrup857)
NewHope
(newhope1024cca)
ThreeBears
(papabearephem)
Round5
(r5nD-5pke-5d)
LAC
(lac256)
NTRU
(hps4096821)
Crystals-KYBER
(kyber1024-90s)
FrodoKEM
(frodokem1344)
Falcon
(falcon1024)
Saber
(firesaber)

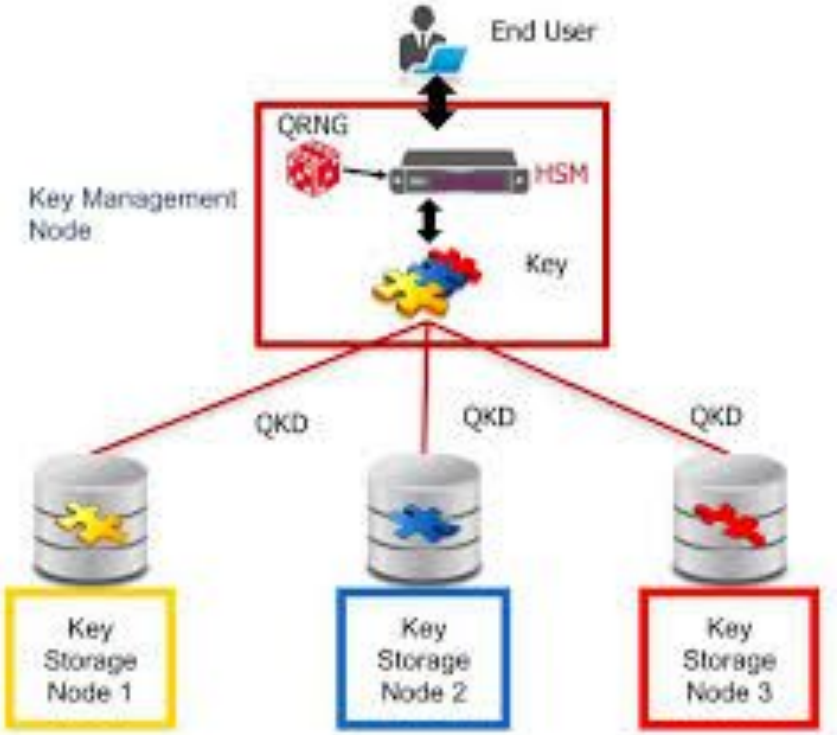
Reference Implementation approaches



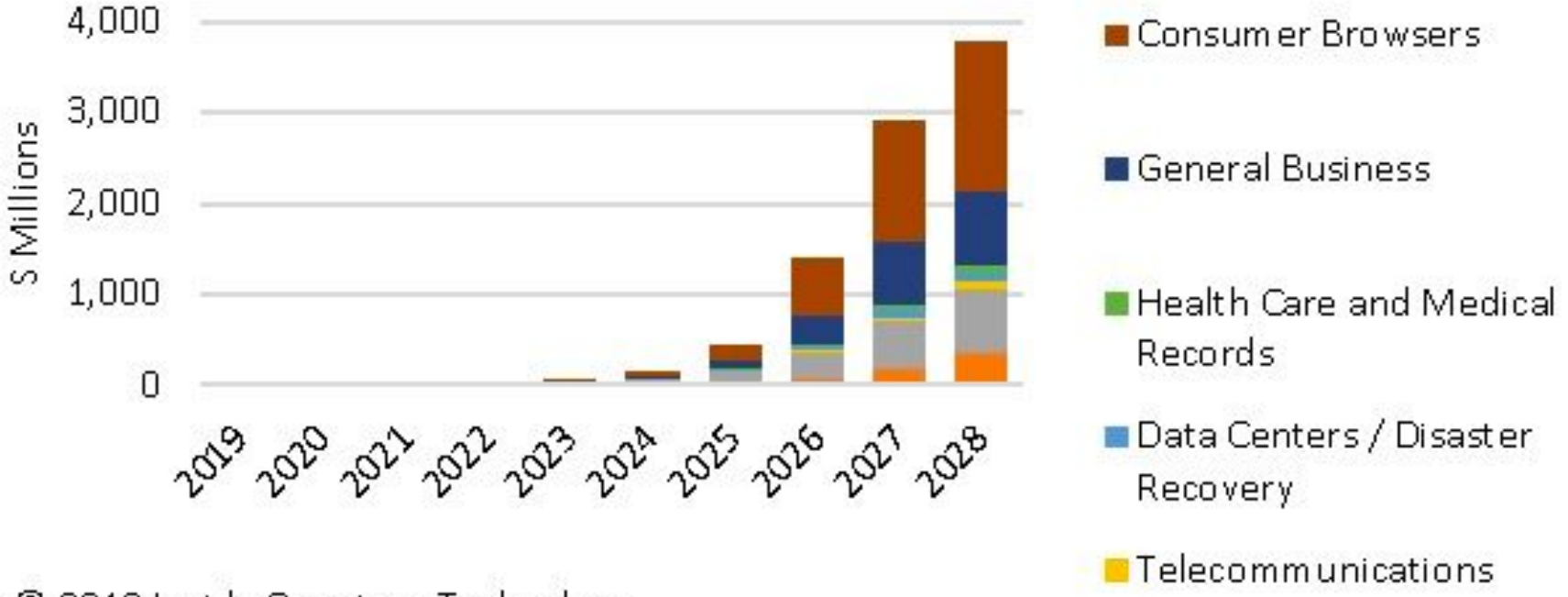
Convergence of QRNG, QKD and PQC !



Convergence of QRNG and QKD



Total Post Quantum Cryptography Opportunity by Market Segments ($ Millions)



Current of Quantum Cryptography

- Classical Quantum Cryptography
- Quantum Cryptography
  - Quantum Key Distribution
  - Quantum Random Number Generators
  - Quantum Channels
  - Quantum Blind Computation