Communication Security Challenges in the Post-Quantum World

Mark Pecen

Co-founder and past chairman

ETSI Working Group for Quantum-Safe Cryptography (WG QSC)

3 – 5 November, 2021 • IFEMA, Madrid, Spain

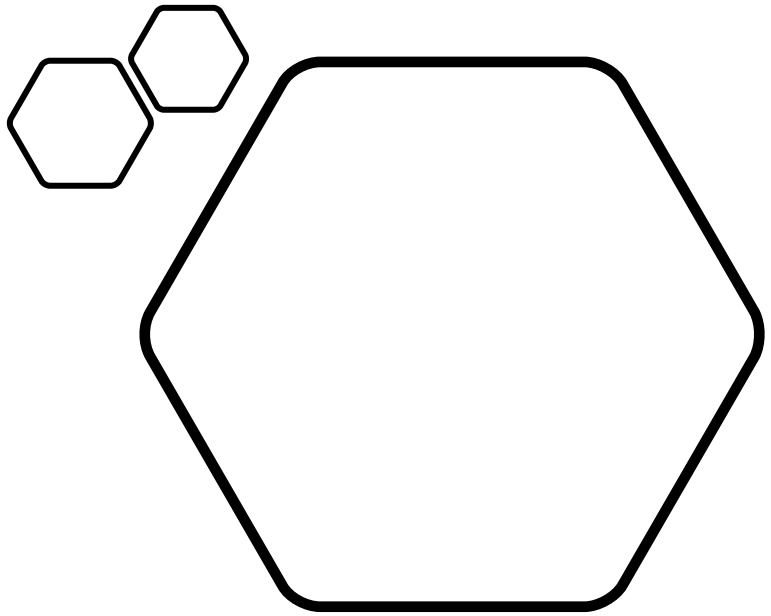
www.critical-communications-world.com/madrid

TCCA Critical Communications World 2021

Agenda

- About quantum computing
- The impact of quantum computing on security
- Quantum computers are not the ONLY security threat
- Industry response to quantum-based security threats – emerging standards
- Landscape of quantum-safe security mechanisms
- Conclusions

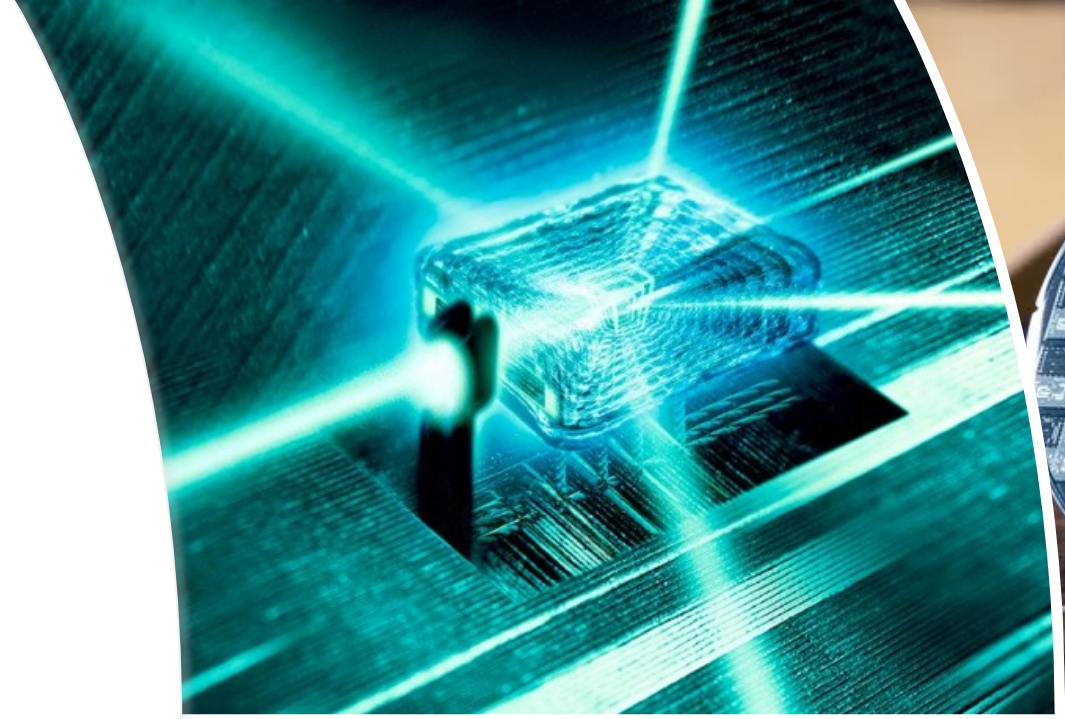
About Quantum Computing

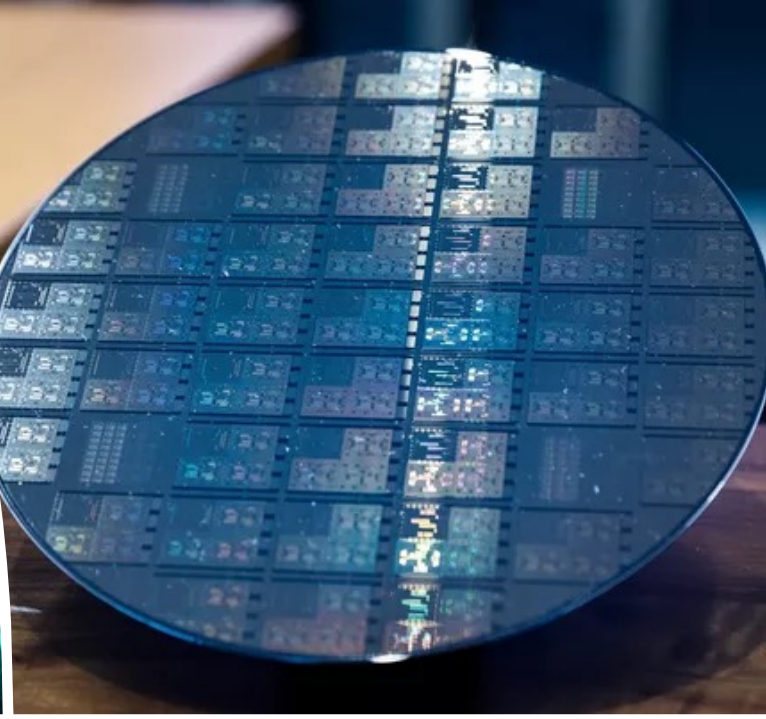


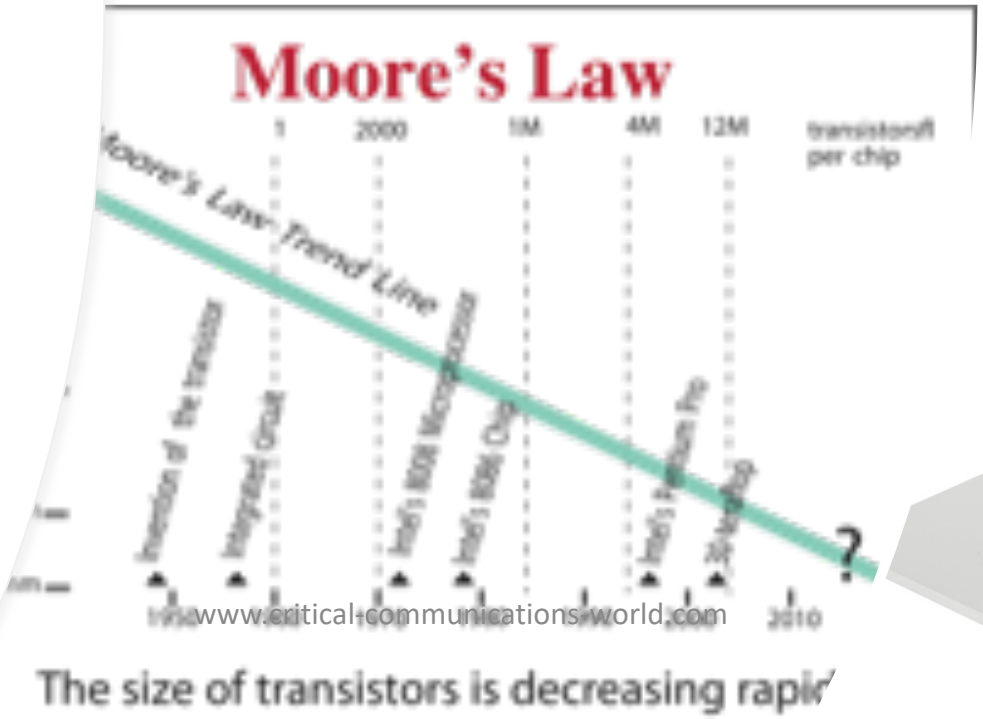
Quantum Computing is the Marriage of…

Information Theory, and

Quantum Mechanics







By combining the two domains we can calculate with certainty using physical effects that are highly uncertain

A Classical Bit is Either 1 or 0

- A classical bit is like a light bulb that's either on or off
- In a standard Von Neumann processor, we get one set of states per clock tick

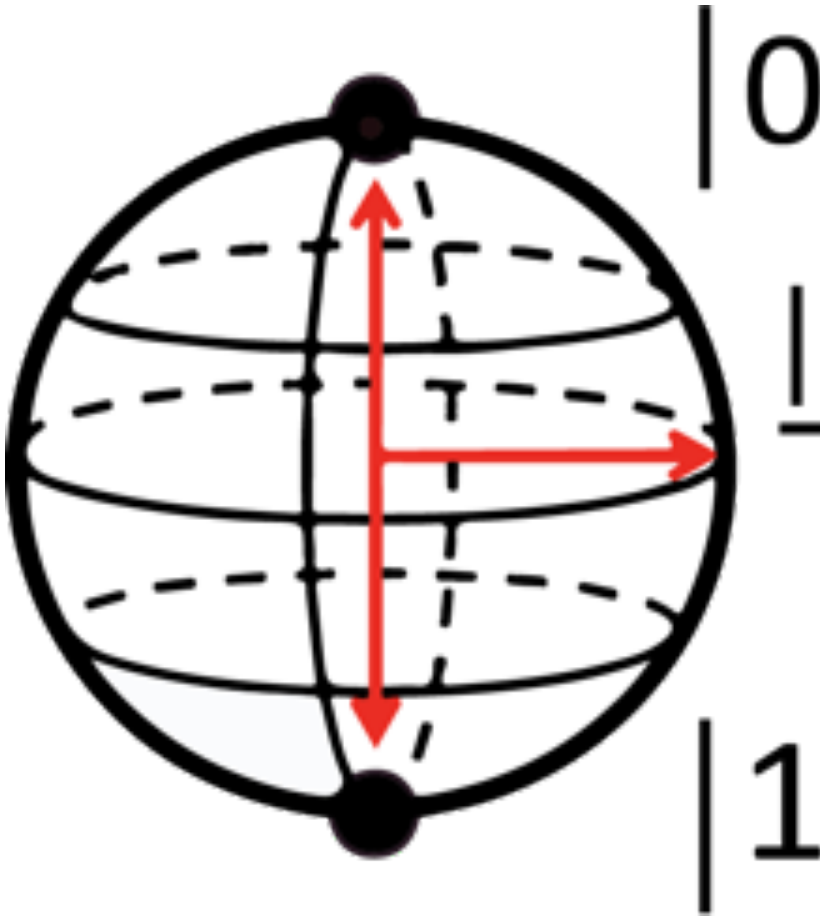
0

"Off"

or

1

"On"



A Quantum Bit (qubit) is Different

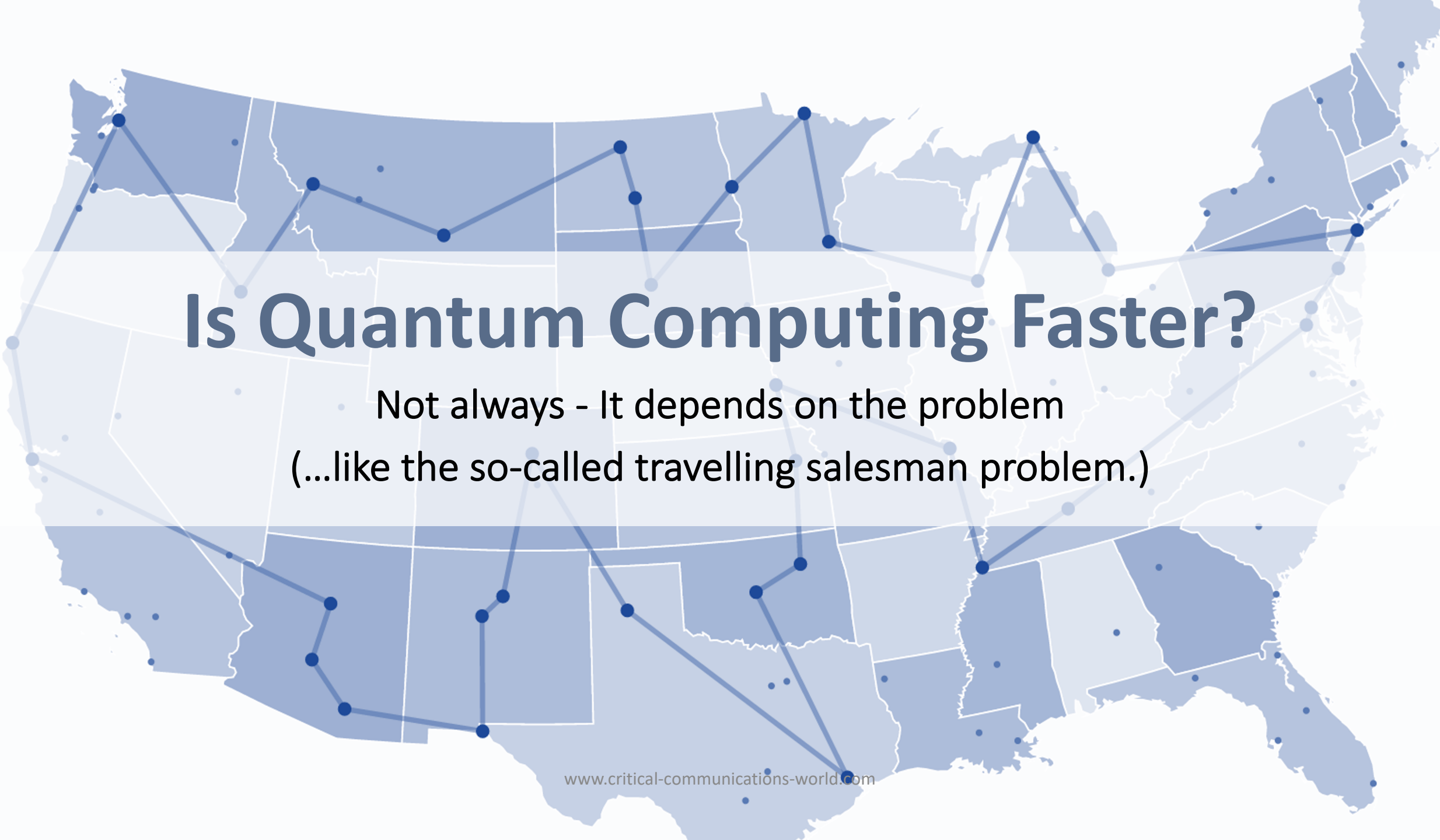
- A quantum bit can exist in **multiple states simultaneously**, like a light bulb that's on and off at the same time.
- Number of states = 2^N , where N = number of qubits
- Example: A system with 16 qubits can be in 2^{16} = **65,536** states at once!

How is this even possible?

There's a Better Question…

- How can we use this interesting property of being in many states at once to **solve important problems?**

- Because the quantum computer lends itself to solving certain types of problems extremely easily



Is Quantum Computing Faster?

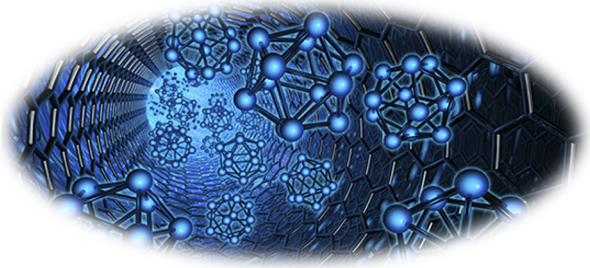
Not always - It depends on the problem

(…like the so-called travelling salesman problem.)

The **Quantum** Race is On!

A New Realm of Possibilities

- Quantum Computing will solve today's unsolvable problems and revolutionize many industries



MATERIAL DESIGN

CRYPTOGRAPHY

BIG DATA

WEATHER SERVICES

CHEMISTRY

MACHINE LEARNING

The **Challenge** of Quantum Computers:

Security

Quantum Computing will break today's public key encryption standards.

Type	Algorithm	Key Strength Classic (bits)	Key Strength Quantum (bits)	Quantum Attack
Asymmetric	RSA 2048	112	0	Shor's Algorithm
	RSA 3072	128		
	ECC 256	128		
	ECC 521	256		
Symmetric	AES 128	128	64	Grover's Algorithm
	AES 256	256	128	

Impact on Secure Communications

Secure Communication Protocol

Handshake | **Data Exchange**

Shor's algorithm **breaks** current public-key algorithms

Authentication

Key Establishment

Symmetric Encryption

AES 256 → AES 128

Grover's algorithm **reduces** the effective symmetric key size to half

Impact on Software Updates

Embed a Root of Trust at Manufacture

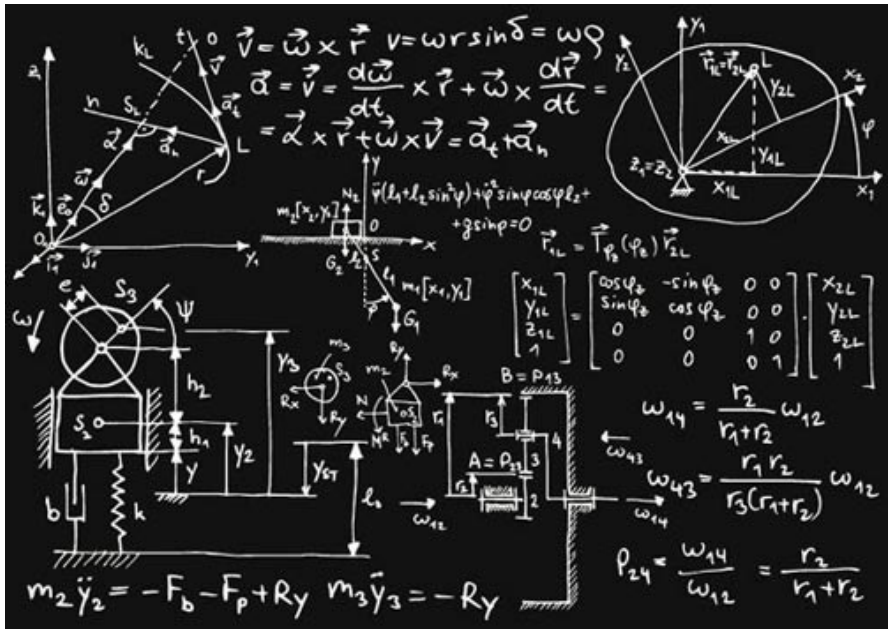
Digital Signature | Software Update

- Receive software update
- Verify ECDSA or RSA digital signature
- Apply software update

→ **broken using Shor's algorithm**

Pathways to Quantum Safety

Quantum Key Distribution



Quantum-Safe Cryptography

Quantum Key Distribution

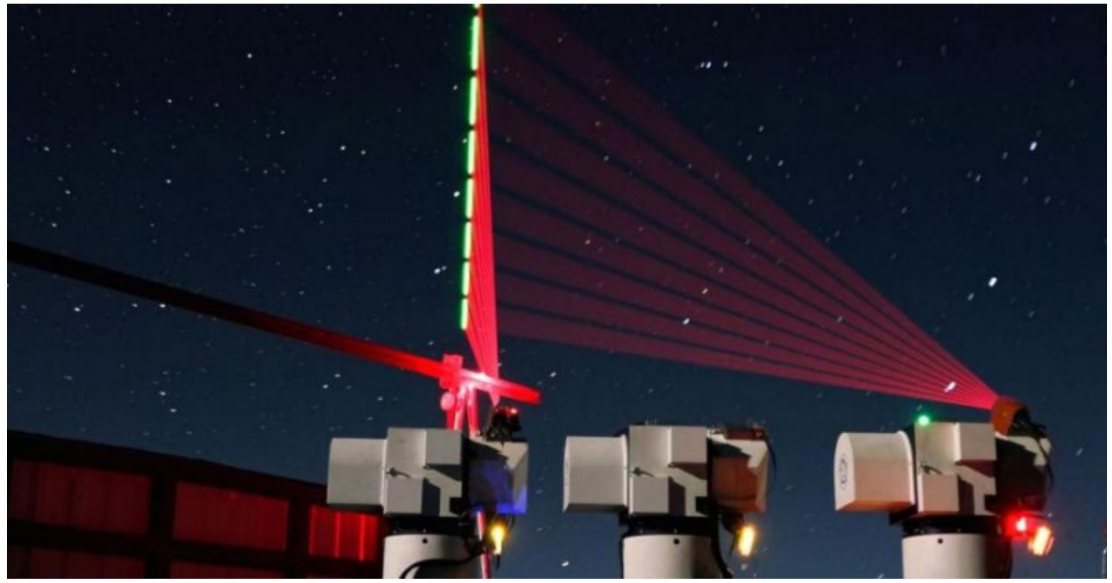
- Utilize basic physical properties to protect information
- Requires a fibre optic connection or line of sight
- Serious distance restrictions
- Side channels risks
- Still requires an authentic channel protected by quantum-resistant cryptography

finance.yahoo.com

China uses a quantum satellite to transmit potentially unhackable info for the first time ever

Arjun Kharpal

4-5 minutes

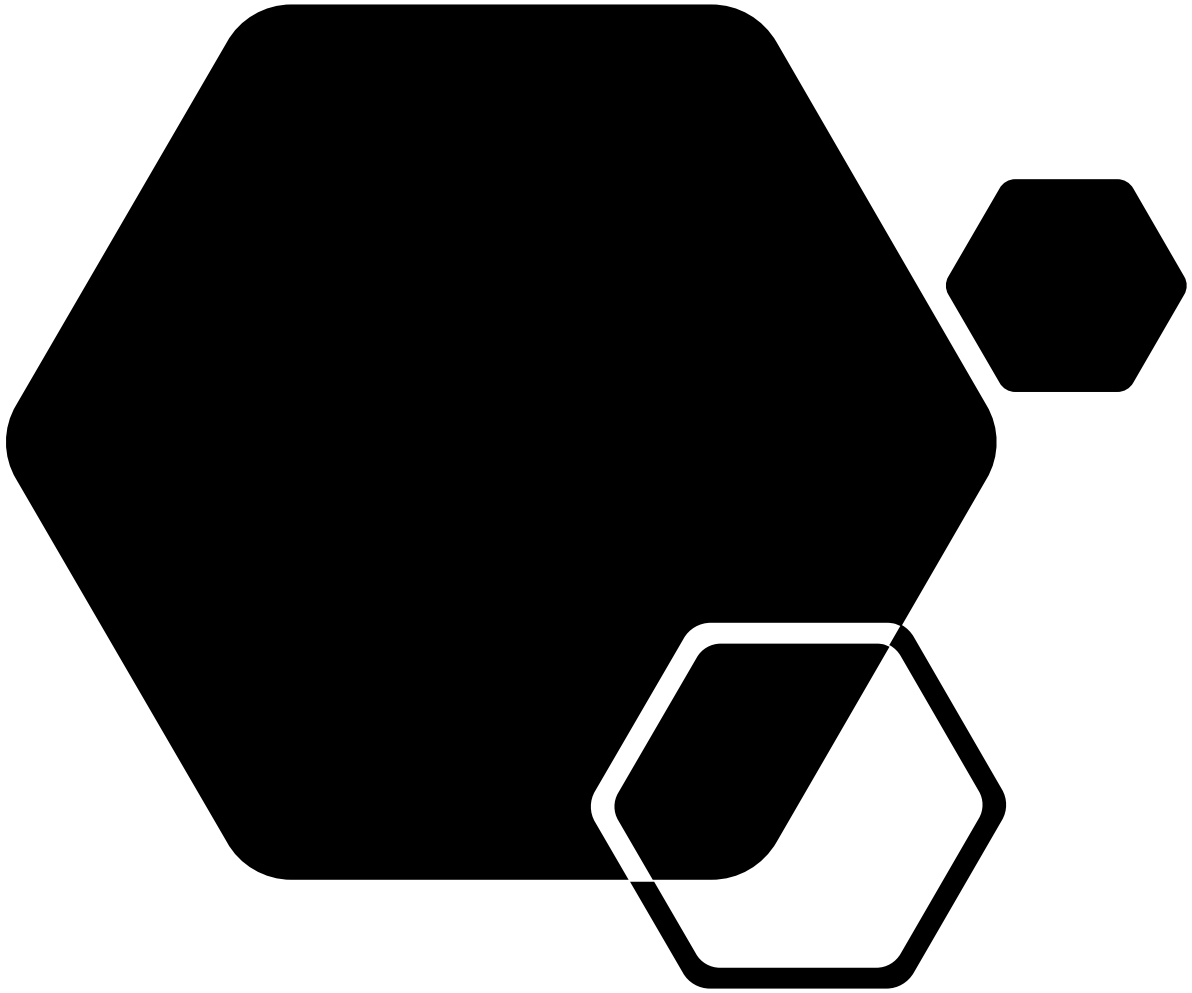


www.critical-communications-world.com

Quantum-Safe Cryptography

- Uses **different classes of mathematical problems** to protect information
- Also resistant, not just to attacks by quantum computers, but to **attacks by conventional computers**
  - ECC and RSA are both **aging cryptosystems**
  - Conventional super-computing is continuously improving
  - Attackers have had much experience in devising newer and more efficient algorithms to compromise these systems

Industry response includes creation of various Standards Working Groups



Standards Organizations in Quantum-Safe Cryptography

European Telecommunications Standards Institute (ETSI) Working Group for Quantum-Safe Cryptography (QSC)

- Founded March 2015 as ETSI Industry Specification Group and converted to WG of TC Cyber in March 2017
- Focus is on the practical implementation of quantum safe primitives, including performance considerations, implementation capabilities, protocols, benchmarking, parameter selection and practical architectural considerations for specific applications
- Work has fed into other ETSI groups and projects as 3GPP and other standards bodies such as International Telecommunication Union (ITU), IETF, etc.
- Objectives DON'T include the development of cryptographic primitives, but rather how to implement and use the primitives coming from advanced research organisations and academia
- Also in ETSI is ISG QKD, founded 2008, whose focus is the hardware-based QKD approach

- https://www.etsi.org

National Institute of Standards & Technology (NIST – in US)

- Focus on evaluating quantum-safe primitives
- Started work on post-quantum algorithms in 2015 April
- Enlisted the research of universities globally
- Established a competition to evaluate the security and usefulness of various quantum-safe mathematical primitives
- Ongoing process, multiple rounds of candadate evaluation
- Currently on round 3

- https://csrc.nist.gov/projects/post-quantum-cryptography

International Telecommunications Institute (ITU) Telecom Sector Study Group 17 (Security)

Quantum-safe cryptography and quantum key distribution have been a part of the ITU-T SG17 work program since 2017

https://www.itu.int/ITU-T/workprog/wp_search.aspx?sg=17&q=15

Internet Engineering Task Force (IETF)

Amazon Web Services and others have been participants in the development of post-quantum Transport Layer Security (TLS)

https://aws.amazon.com/fr/blogs/security/post-quantum-tls-now-supported-in-aws-kms/

https://docbox.etsi.org/Workshop/2017/201709_ETSI_IQC_QUANTUMSAFE/TECHNICAL_TRACK/S02_JOINT_GLOBAL_EFFORTS/IRTF_PATERSON.pdf

American National Standards Institute (ANSI) WG X.9

ANSI X.9 is a specialized standardization group with a focus on payment systems

Recent guidelines published in 2021 by X.9 on quantum-safe cryptography and associated requirements: https://x9.org/quantum-computing/

International Standards Organisation (ISO)

ISO has two technical organizations with a focus on quantum-safe cryptography:

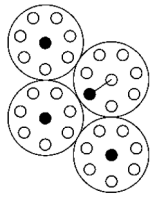
- ISO/IEC JTC 1/SC 27/WG 2 Cryptography and security mechanisms
- ISO/TC 68/SC 2/WG 11 Encryption algorithms used in banking applications

https://www.iso.org/organization/5984715.html

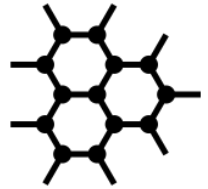
Quantum Safe Cryptography: The “New” Math

QSC: The “New” Math domains for crypto

Hash-based

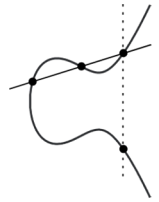


Code-based



Lattice-based

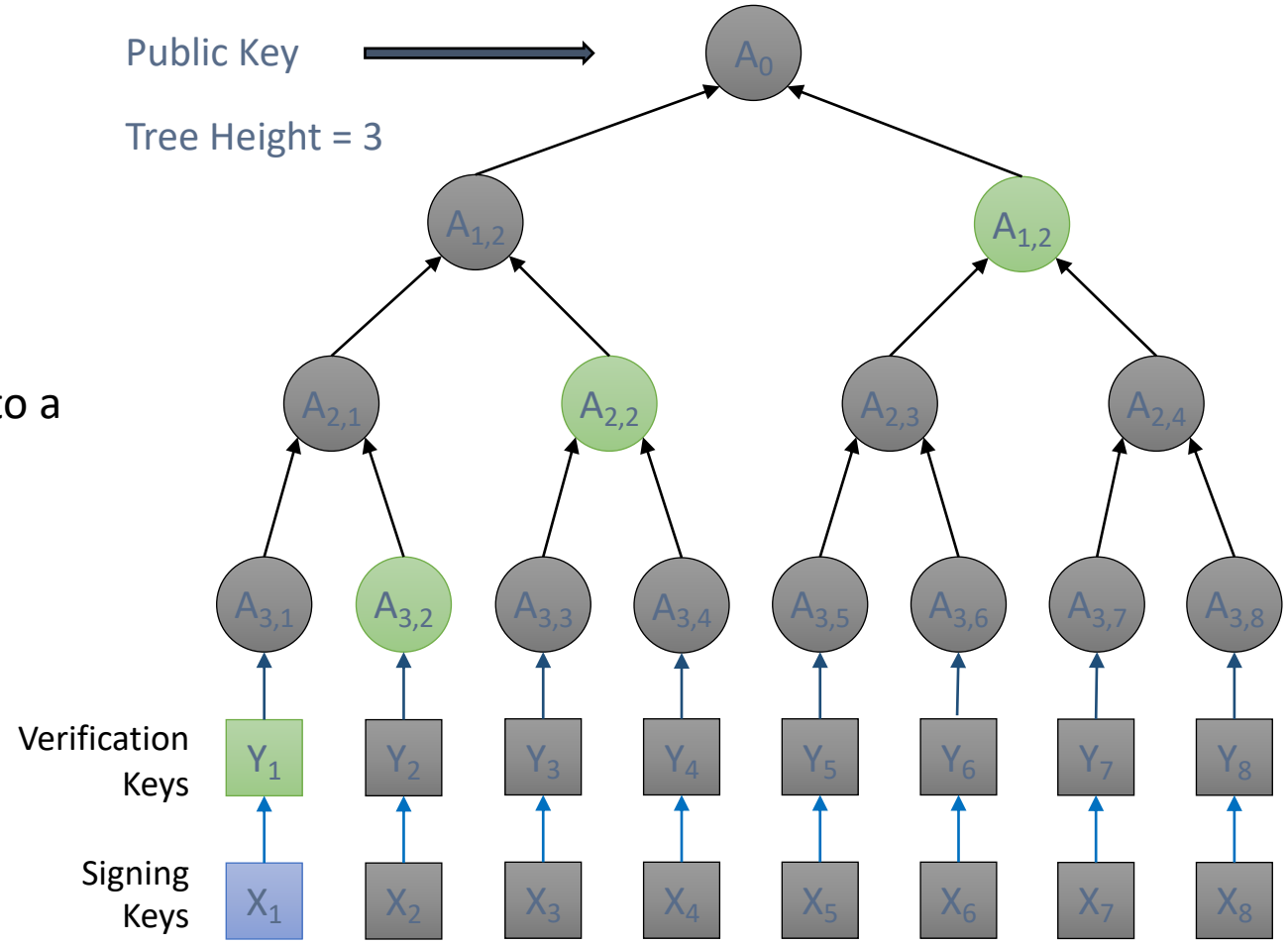
Multivariate-based



Isogeny-based

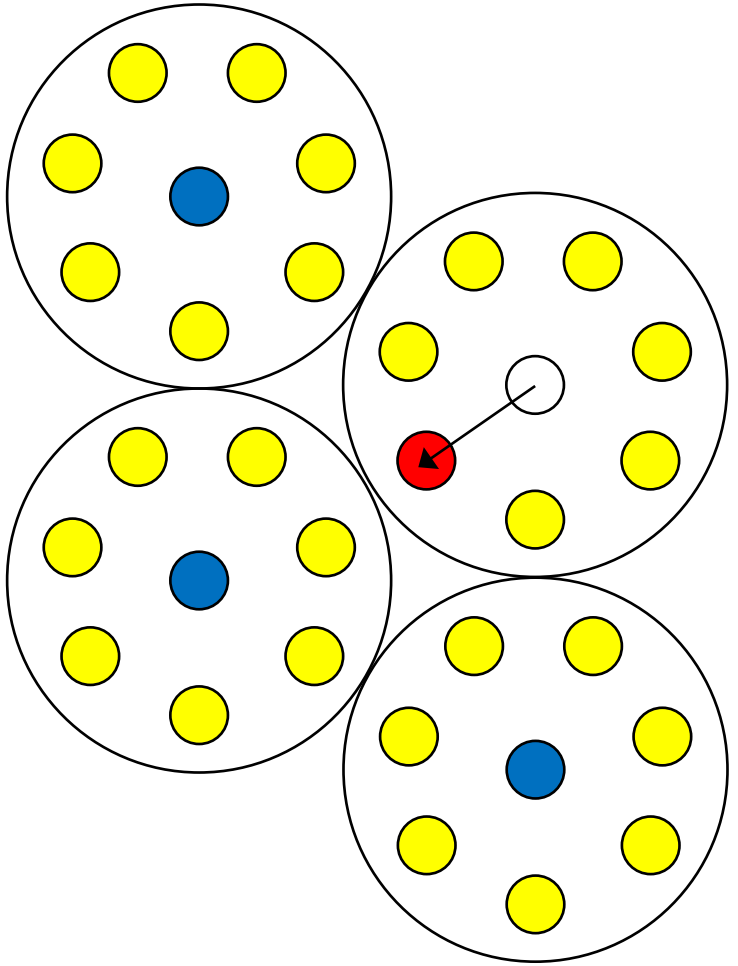
Hash-Based Cryptography

- Introduced by Merkle in 1979
- “One-Time Signatures”
- Small public key but very large private key
- Fast signing & verifying
- Stateful
- Became practical by combining all verification keys into a single Public Key
- And it happens to be Quantum-Safe
- Candidates
  - Leighton-Micali Signatures (LMS)
  - eXtended Merkle Signature Scheme (XMSS)
  - SPHINCS



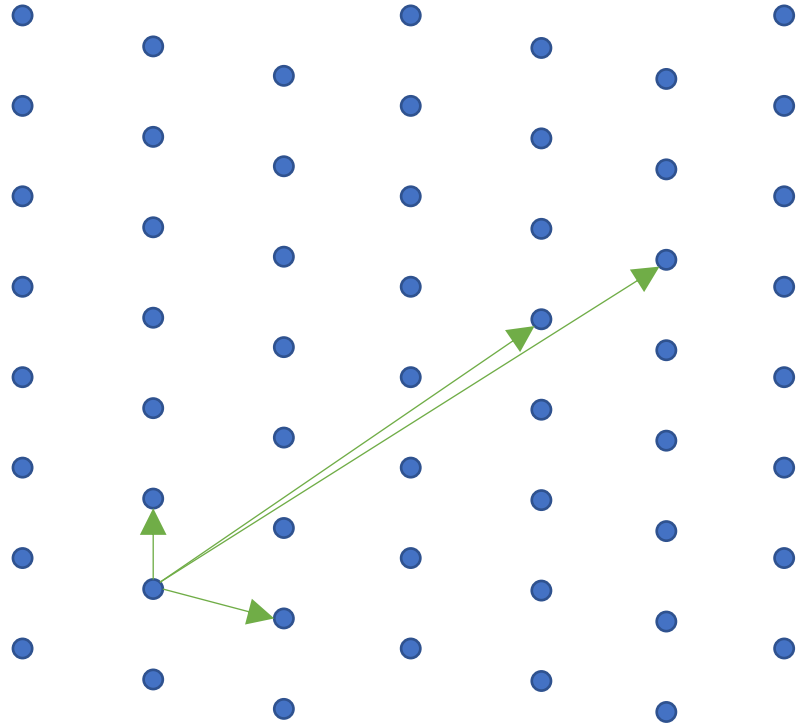
Code-Based Cryptography

- Introduced by McEilece in 1978
- Relies on hardness of decoding unknown codes
- Very large public keys
- Fast encryption and decryption
- Smaller variants – QC-MDPC, McBits, others



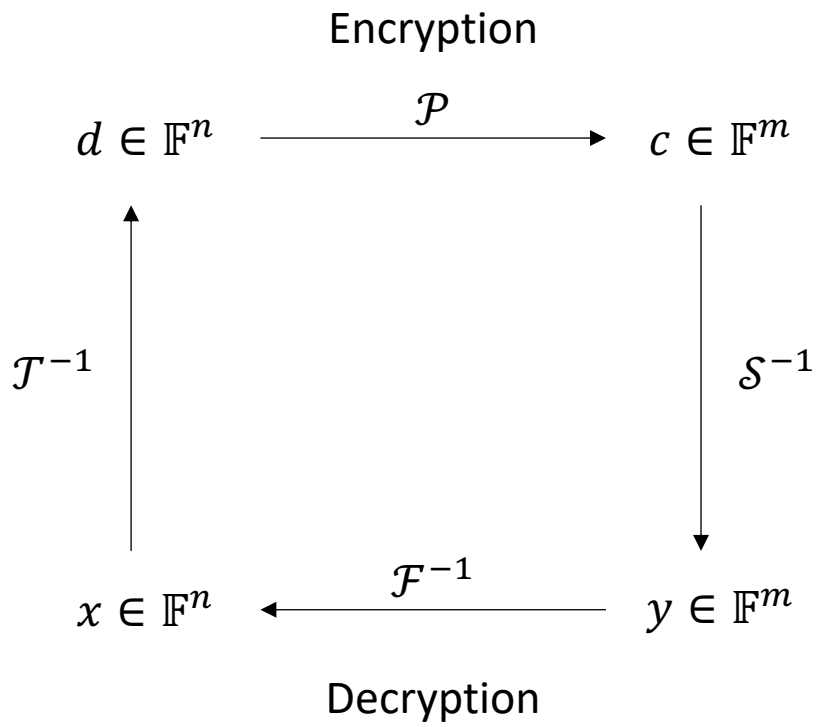
Lattice-Based Cryptography

- First commercial version was NTRU (1996)
- Hard Problems
  - Shortest Integer Solution (SIS)
  - Learning With Errors (LWE)
- Competitive key sizes and fast operations
- Open questions around tightness of reductions
- Risks when used in a static or static/ephemeral environment
- Google public experiments with NewHope in Chrome Canary



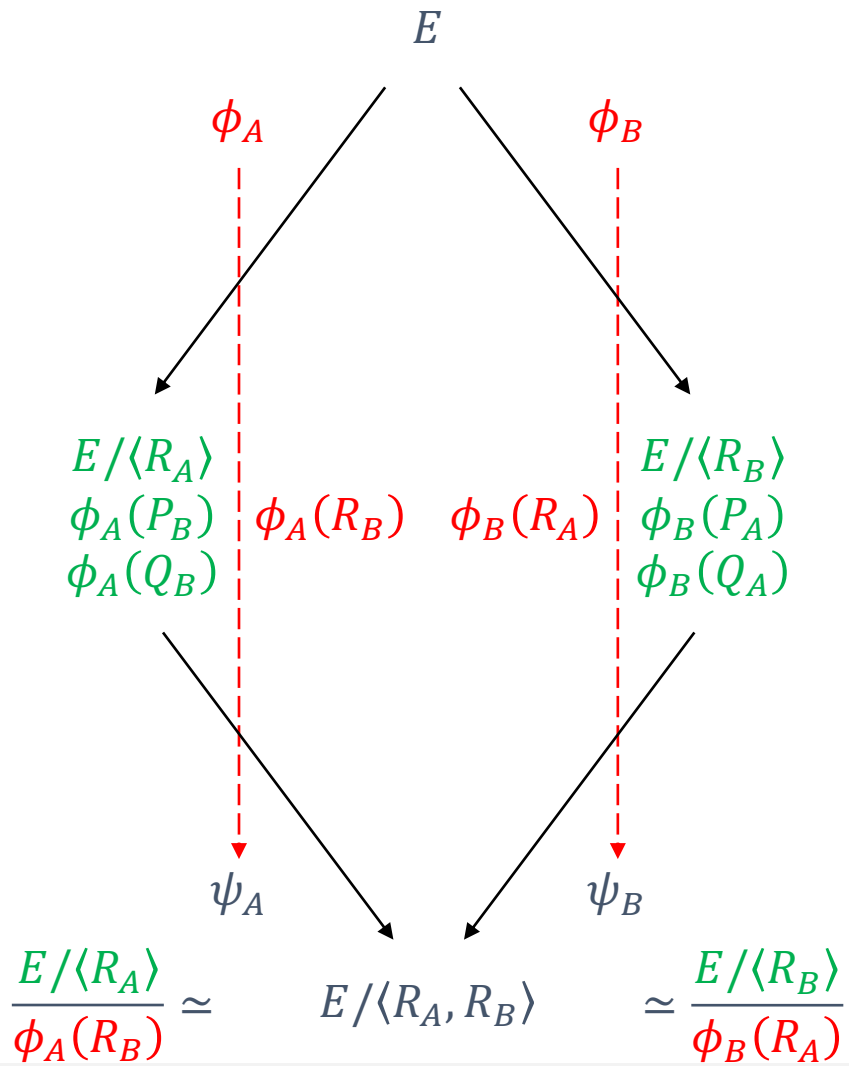
Multivariate-Based Cryptography

- Introduced by Matsumoto and Imai in 1988
- Based on the fact that solving n randomly chosen (non-linear) equations in n variables is NP-complete
- Can be formulated into signatures, key exchange and key transport
- Often trade offs between key size and public/private key operation speeds

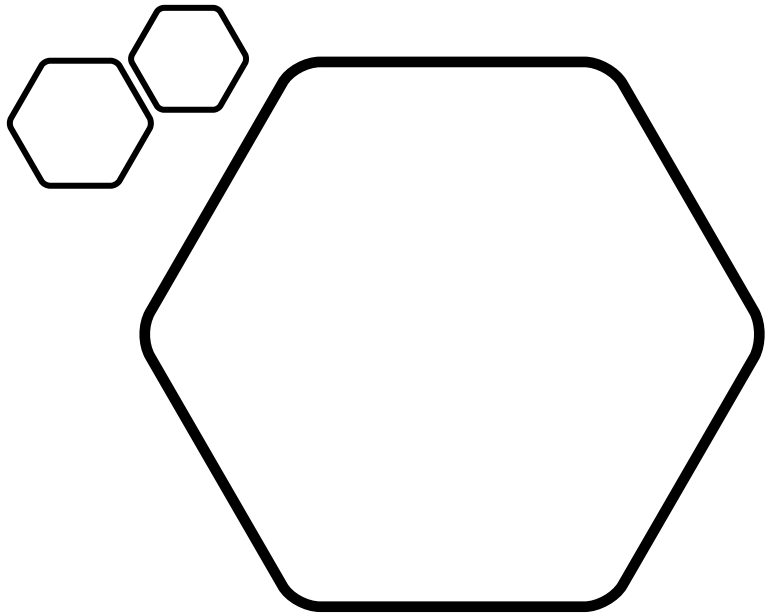


Isogeny-Based Cryptography

- Introduced by Jao in 2009
- Relies on difficulty of finding isogenies (mappings) between Elliptic Curves
- Competitive key sizes
- Slower operations
- Risks when used in a static or static/ephemeral way



Migration to quantum-safe systems



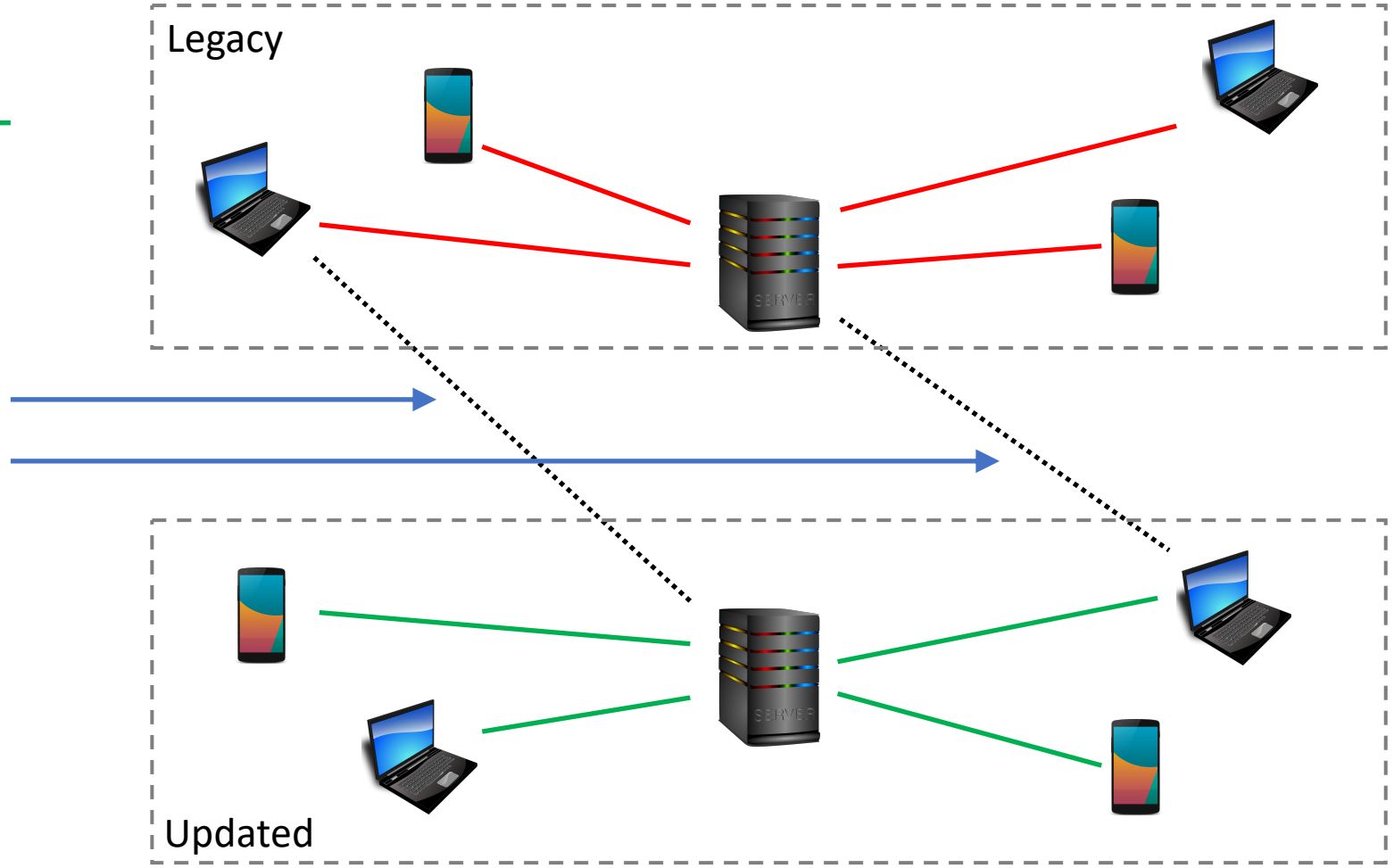
Migration Could Take Years…

Classic Connection

Quantum-Safe Connection

Peers typically can negotiate **key establishment** algorithms

Authentication uses a single algorithm that is used by the PKI-issued certificates



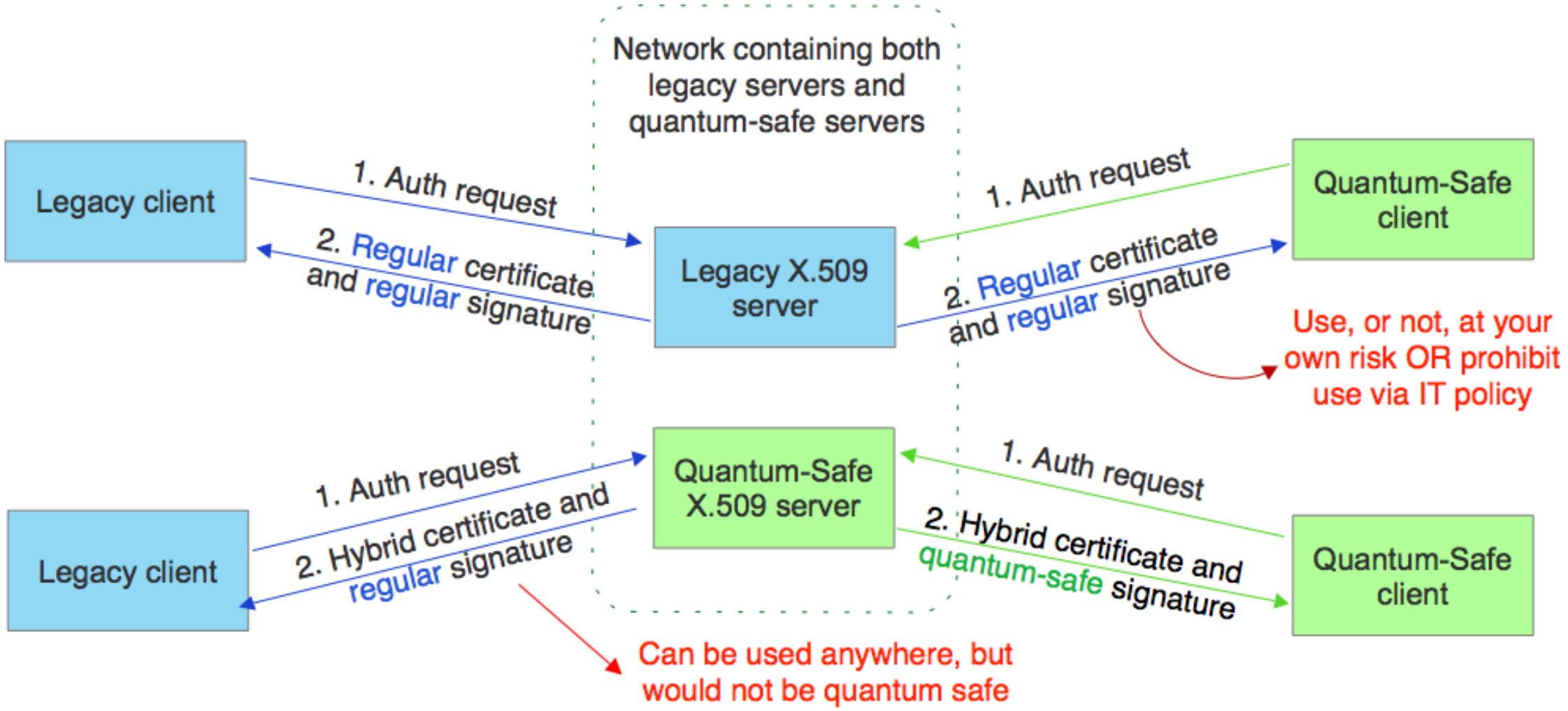
What's Needed is Crypto-Agility

- The concept of crypto-agility is the notion that a given system or subsystem is specified and implemented in such a manner that different cryptographic techniques may be added or removed based on security requirements

X.509 certificate standard made crypto-agile

- The X.509 certificate standard is the most widely-used cryptographic standard in the world
- Recently, the ITU-T SG17 accepted a proposal to update the next version of the ITU Rec. X.509 certificate to be crypto-agile
- The certificate is now able to support multiple signing algorithms, some of which may be quantum-safe

How does a crypto-agile certificate work?

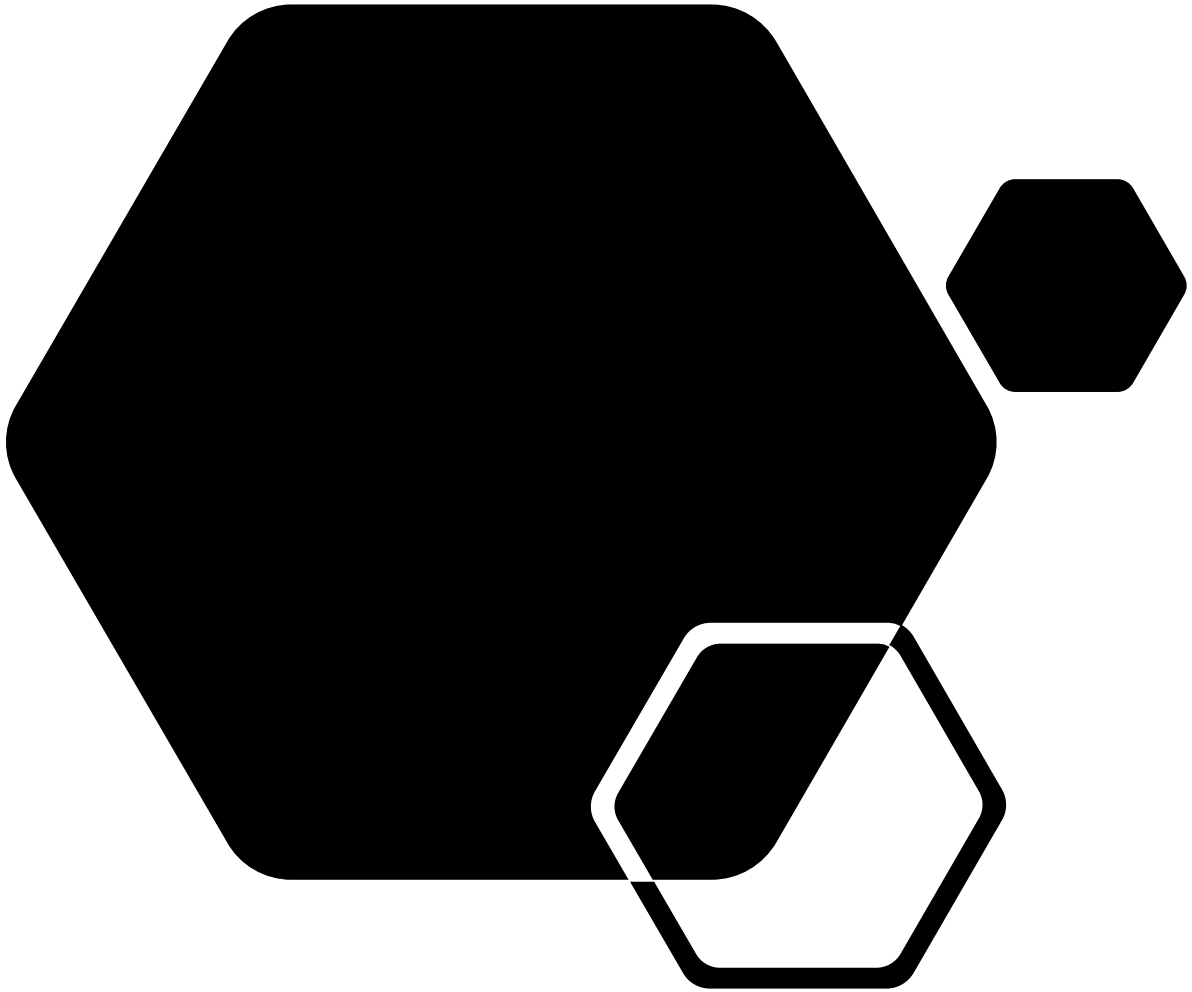


Conclusions

- Quantum computing will absolutely have an impact on communications security
  - Quantum computers are still primitive, but global investment is large
  - Academic research has begun to address quantum attacks over more than 20 years, but now industry is showing increasing interest over the past 10 years or so
- Existing public key infrastructure is based on aging cryptosystems, which themselves are more at risk from attack by conventional computers

- The communications industry has responded recently by creating collaborative environments, such as working groups in global standards bodies to address a way forward for quantum safety
- There exist 5 basic algorithm families that are believed to be quantum-safe
  1. Hash-based
  2. Code-based
  3. Lattice-based
  4. Quadratic multivariate-based
  5. Isogeny-based
- Migration of conventional systems to quantum-safe security will require more attention as we move forward

Questions & Comments?



Contact me:
mpecen@approachinfinity.ca

Mark Pecen

- MARK PECEN is a senior technology executive and head of a specialised technology advisory group, Approach Infinity, Inc., with a focus on research, standardisation, intellectual property and commercialisation of advanced technologies.
- He recently served 5 years as chairman and was a founding member of the European Telecommunication Standards Institute (ETSI) Working Group for Quantum Safe Cryptography (Cyber QSC) in Sophia Antipolis, FRANCE.
- Pecen is a retired senior executive of BlackBerry, Ltd. where he founded the Advanced Technology Research Centre and helped to develop a significant portion of BlackBerry's wireless and networking patent portfolio.

- Pecen has served on over 20 governance and advisory boards for both public and private companies in Canada, Europe and the U.S. and is currently serving on two Canadian university governance boards. He also serves as an advisor to the Canadian government and European Commission on ICT R&D and technology standardization.
- He is a named inventor on more than 100 fundamental patents in wireless communication, networking and computing, and is a graduate of the University of Pennsylvania, Wharton School of Business and the School of Engineering and Applied Sciences.