ETSI

The Standards People

Overview of Quantum Computing, Quantum-Safe Cryptography and ETSI WG QSC

Presented by: **Mark Pecen, Chairman**
ETSI TC Cyber WG QSC

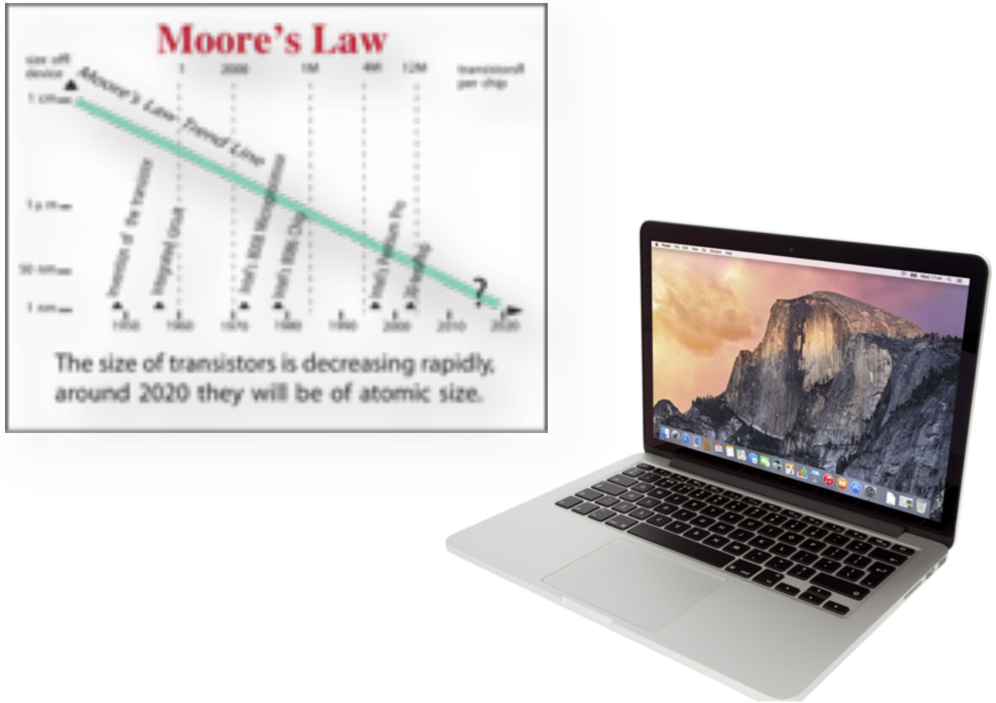
For: **ETSI Webcast**

June 2020

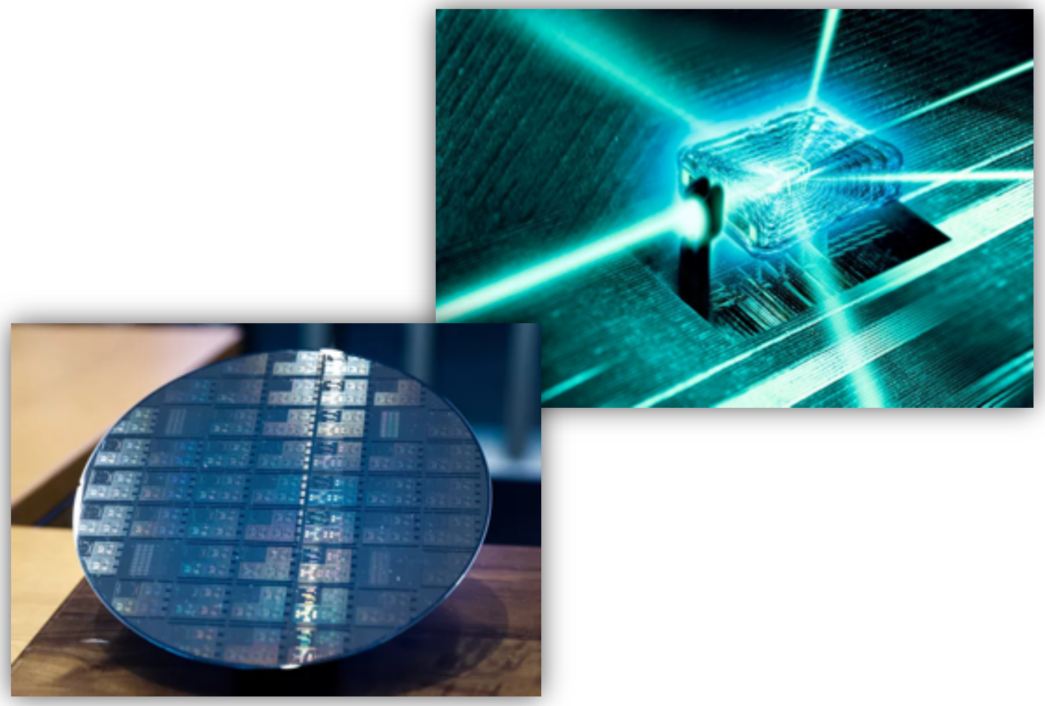
Agenda

- About quantum computing
- The impact of quantum computing on security
- Industry response to quantum-based security threats
- Landscape of quantum-safe security mechanisms
- About the ETSI WG for Quantum-Safe Cryptography

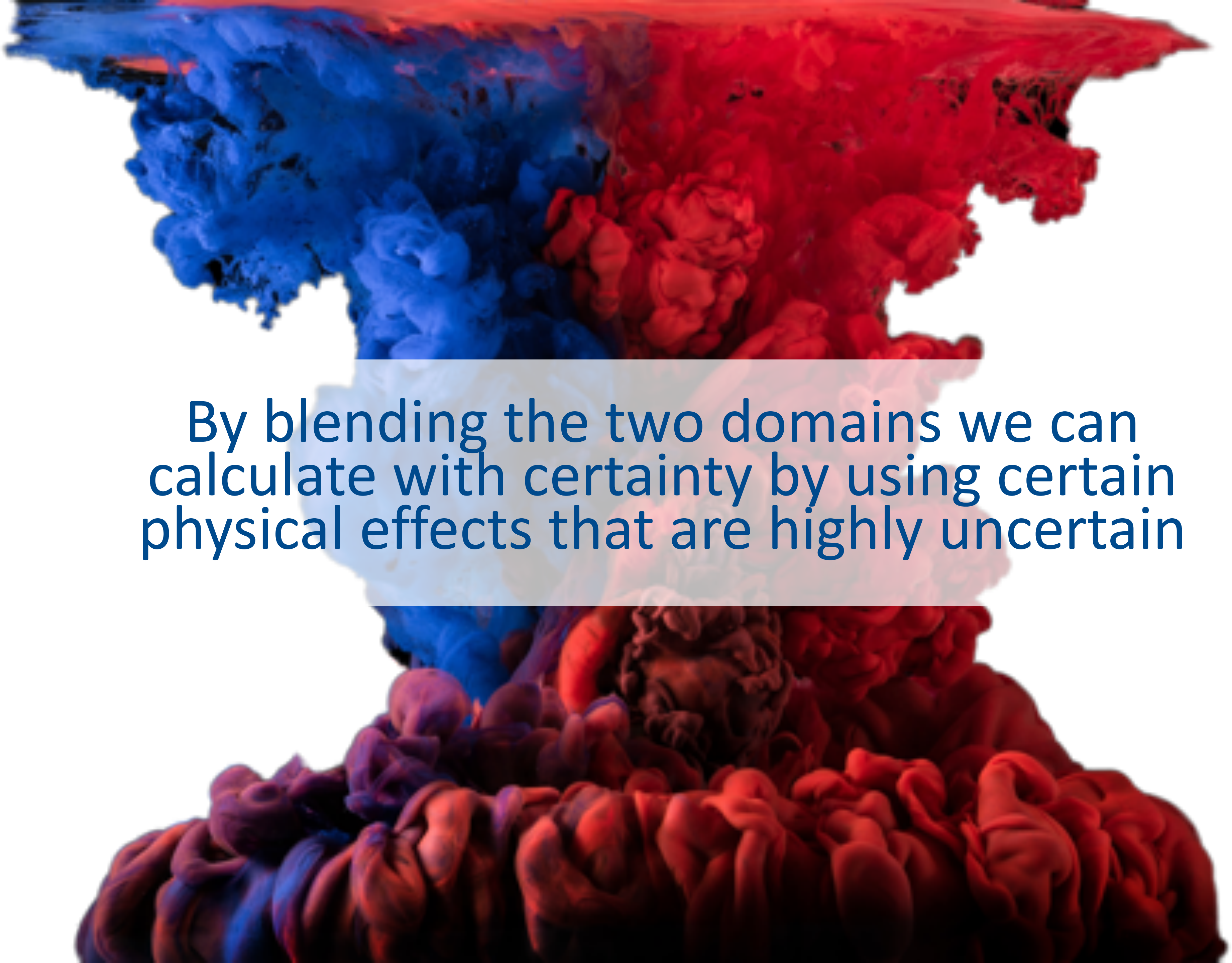
Quantum Computing is the Marriage of...


Moore's Law
Moore's Law Trend Line
The size of transistors is decreasing rapidly, around 2020 they will be of atomic size.

Information Theory



Quantum Mechanics



By blending the two domains we can calculate with certainty by using certain 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

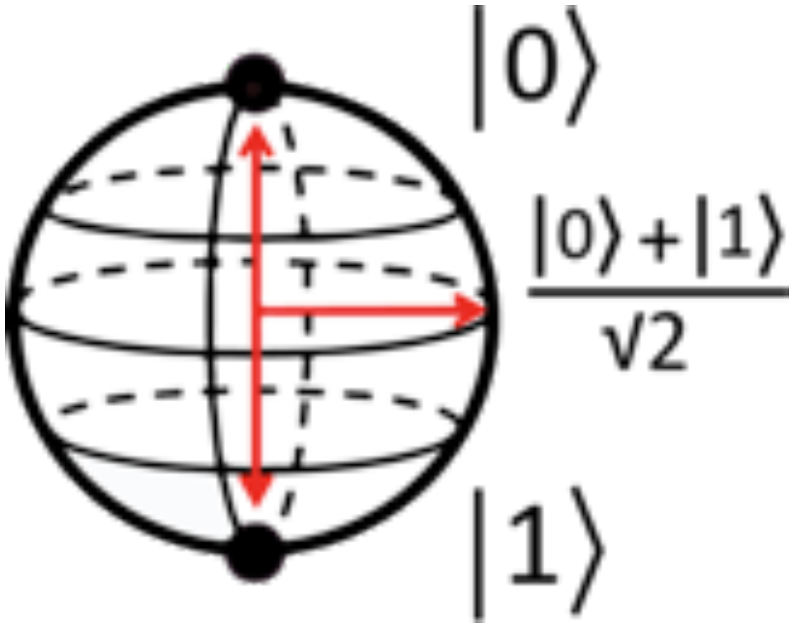
or

0
“Off”

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!

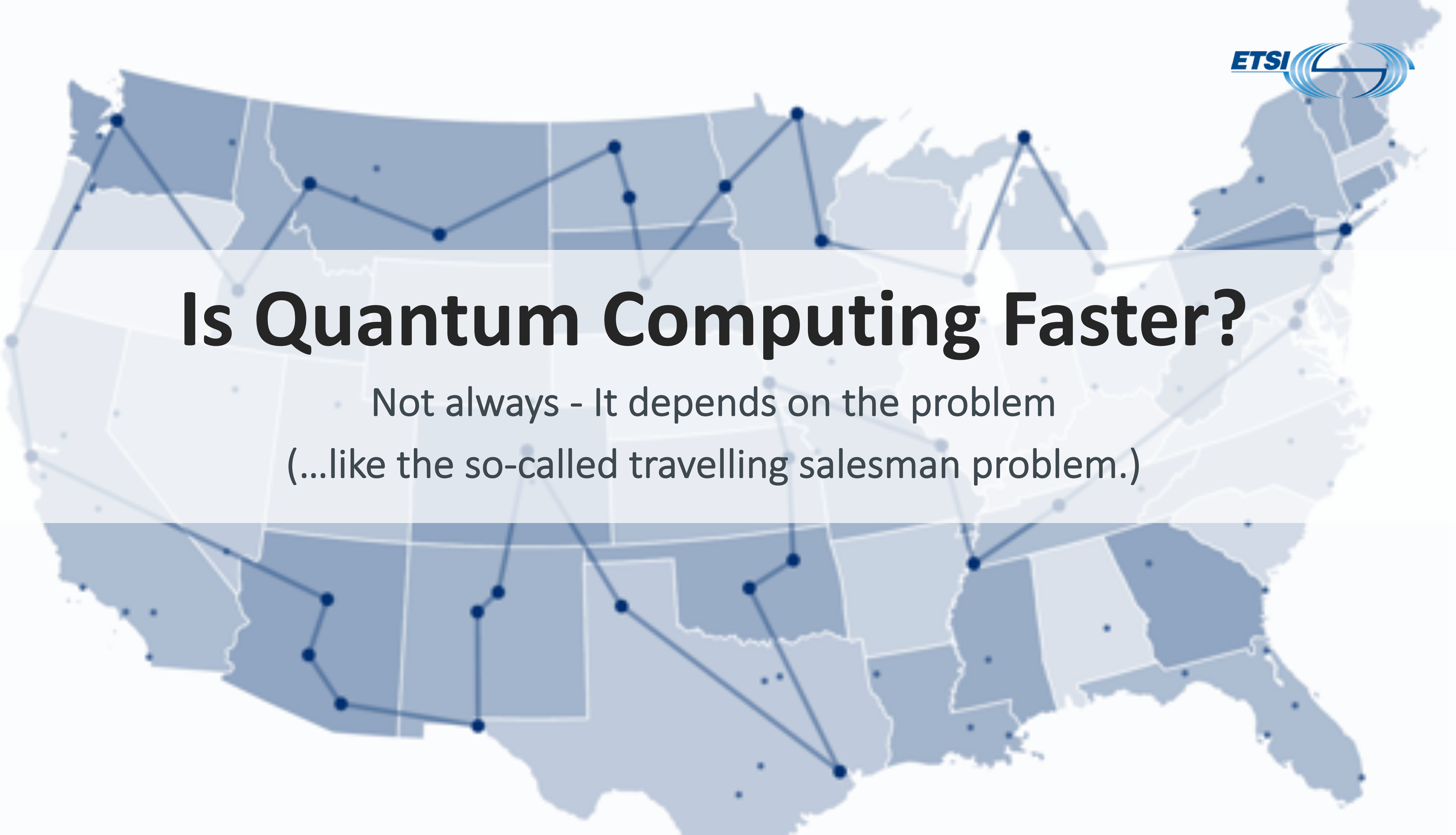


How is This Possible?

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

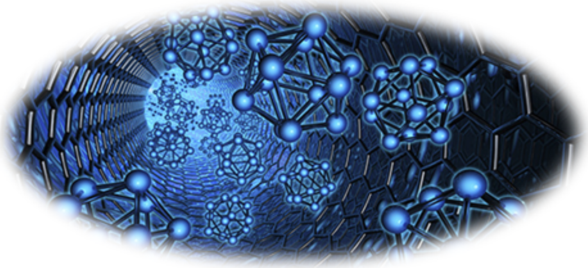
(…like the so-called travelling salesman problem.)

The **Quantum** Race is On!

Microsoft
Google
rigetti
D:Wave
The Quantum Computing Company™
IBM
intel®

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

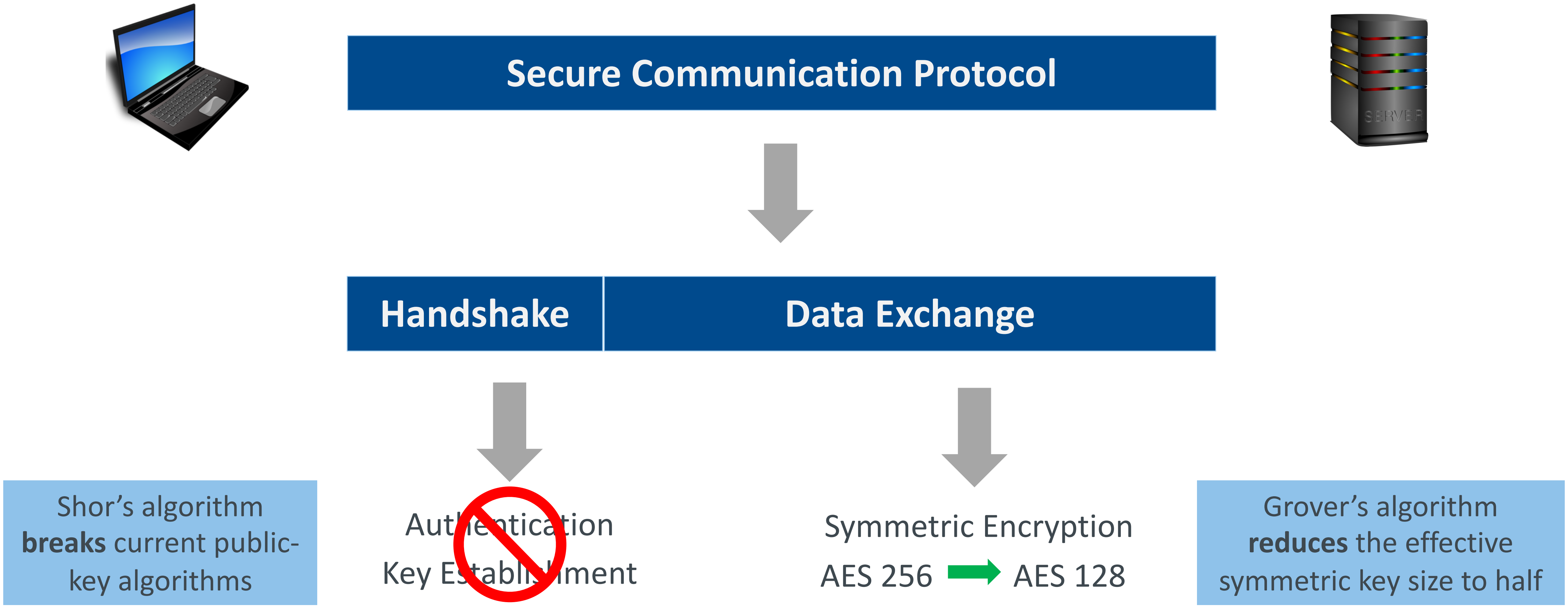
The **Challenge** of Quantum Computers:

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

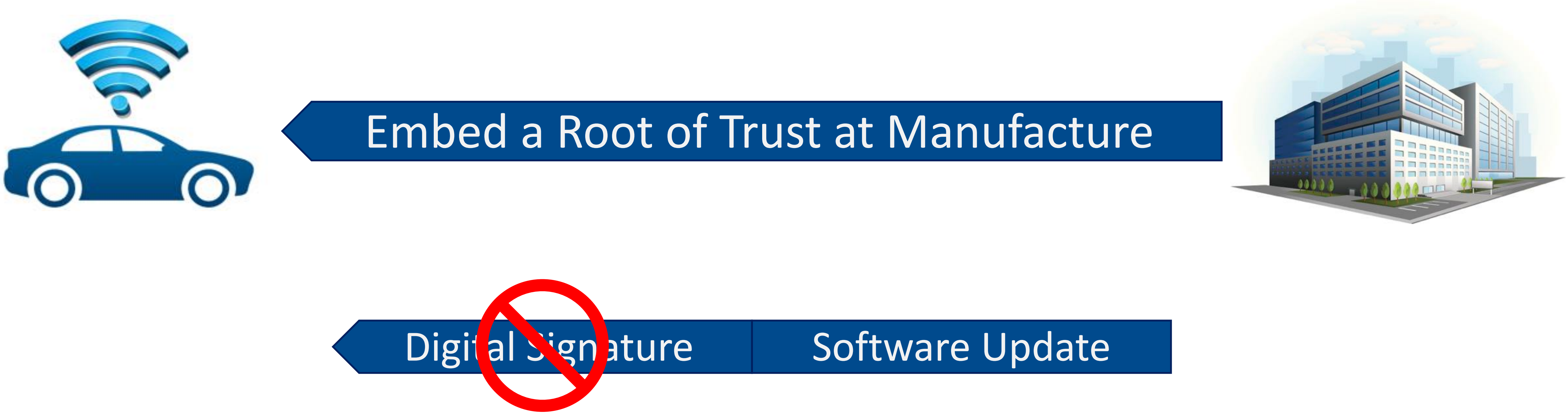
Key Establishment

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

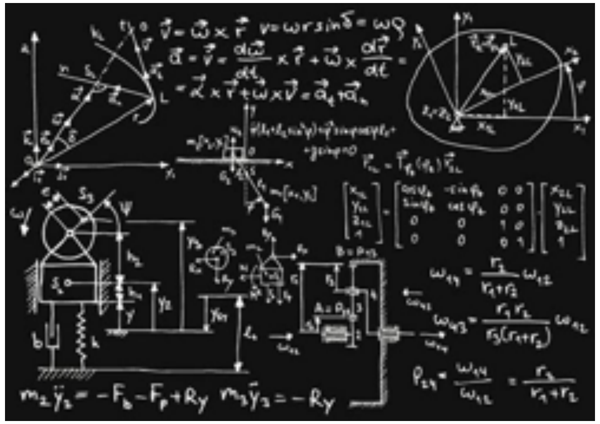
Digital Signature

Software Update

- Receive software update
- Verify ECDSA or RSA digital signature → **broken using Shor’s algorithm**
- Apply software update

Pathways to Quantum Safety

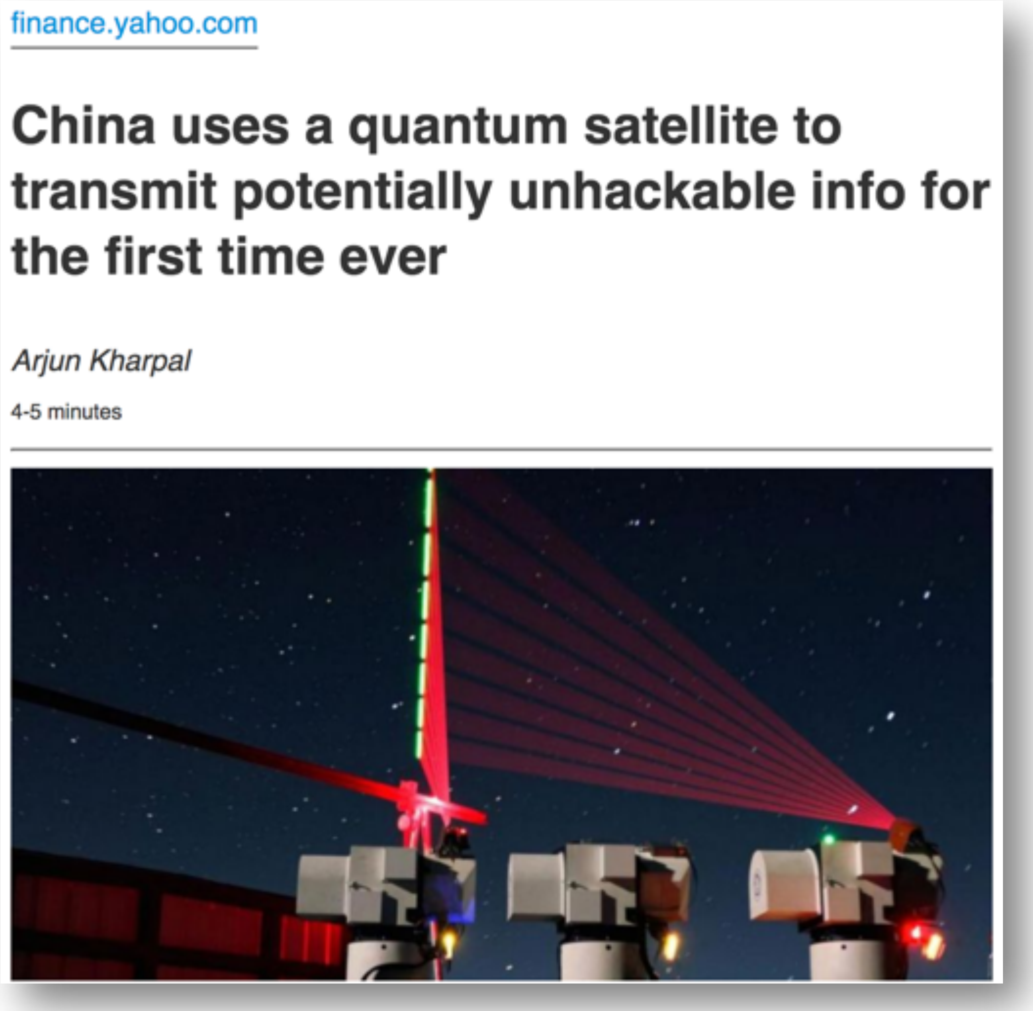
Quantum Key Distribution



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

Quantum Safe Cryptography: The “New” Math

QSC: The “New” Math

Hash-based

Code-based

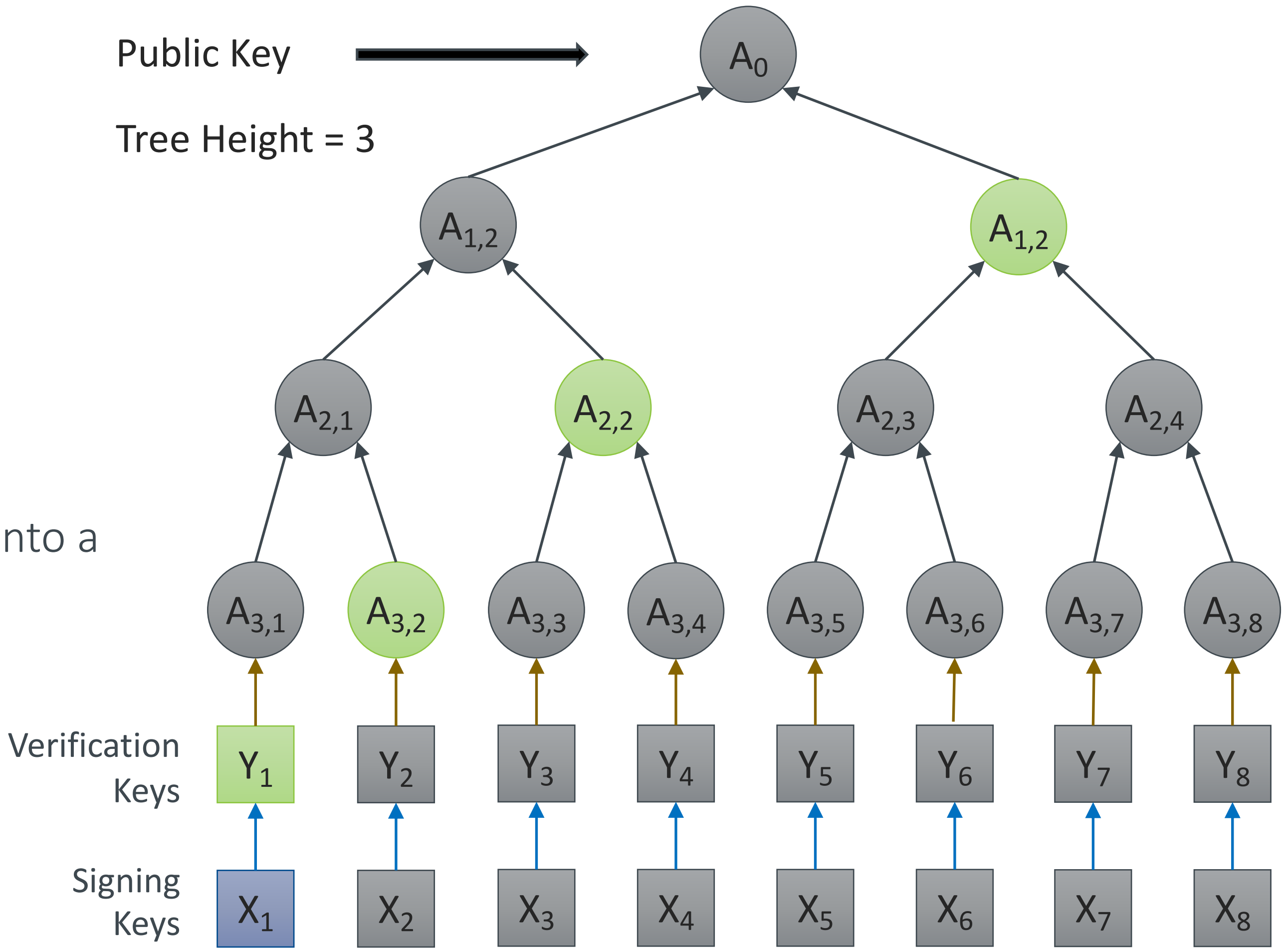
Lattice-based

Multivariate-based

Isogeny-based

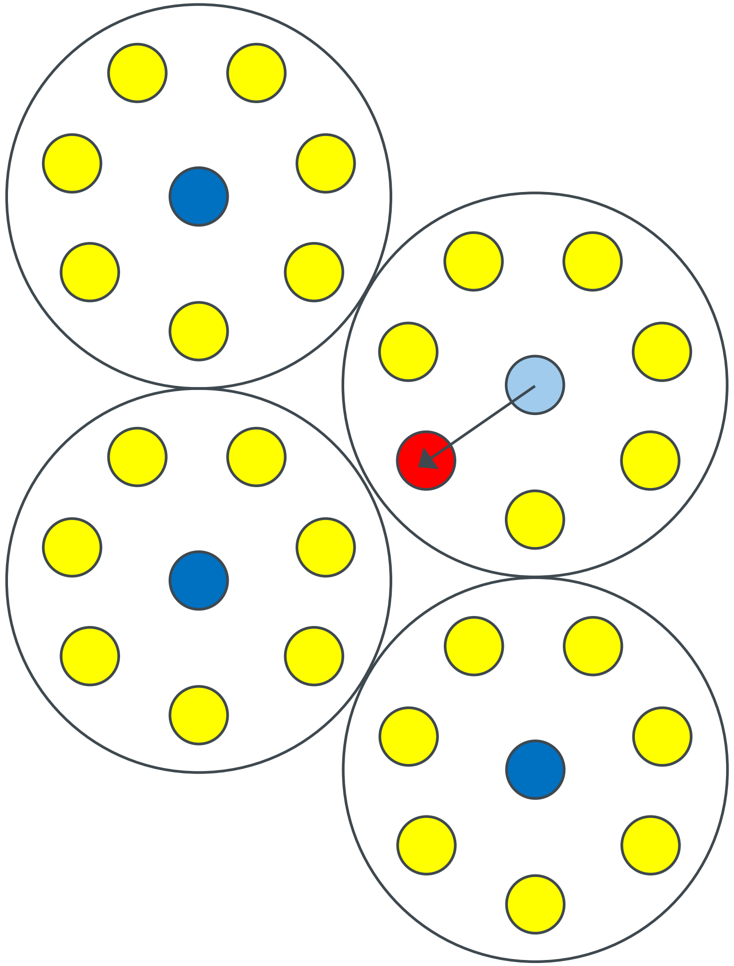
Hash-Based Cryptography

- 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



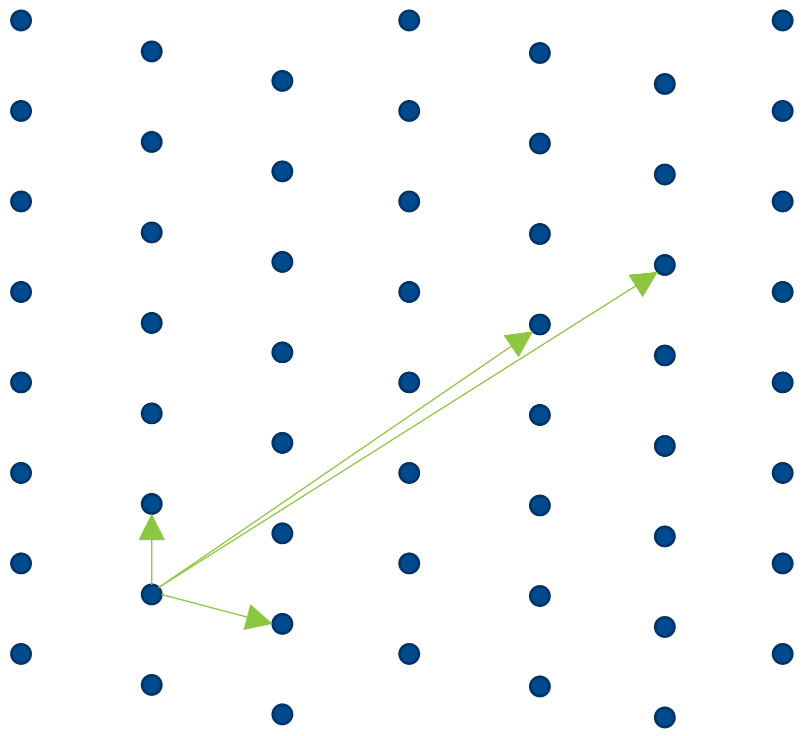
Code-Based Cryptography

- 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
- Recent attacks mitigated through ephemeral use



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

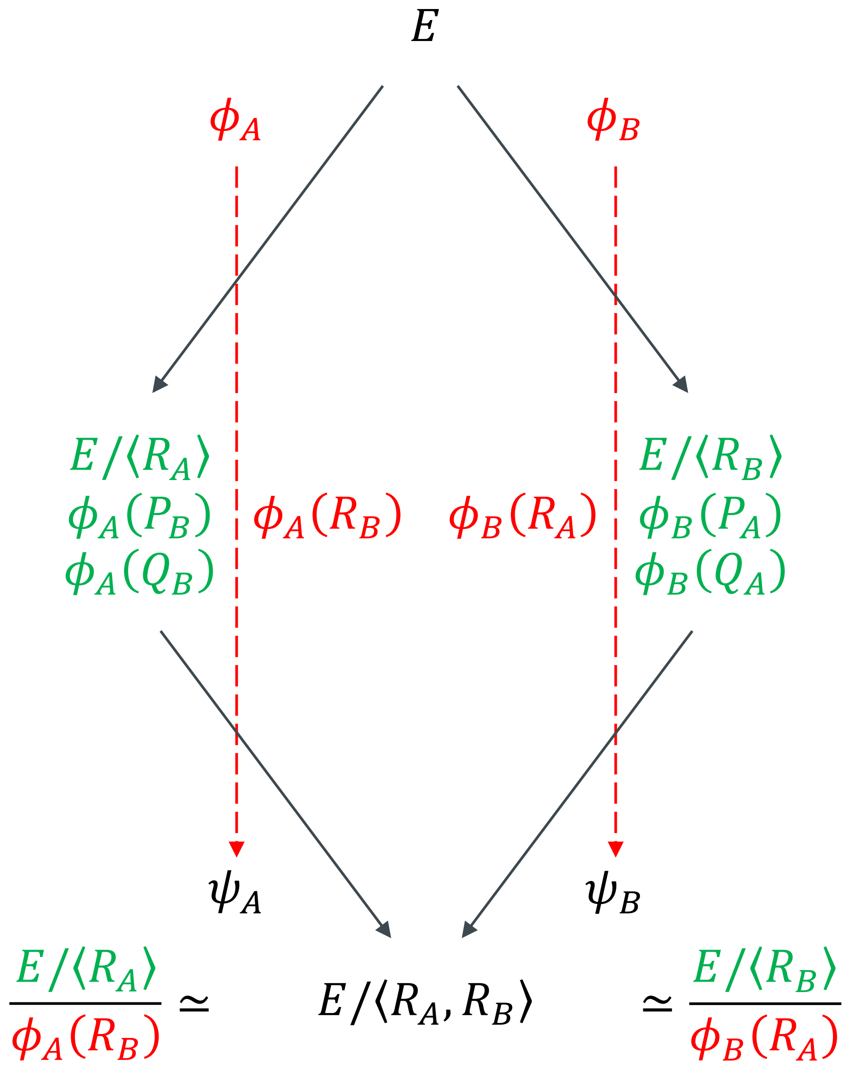
Encryption

$$\begin{tikzcd} d \in \mathbb{F}^n \arrow[r, "\mathcal{P}"] & c \in \mathbb{F}^m \arrow[d, "\mathcal{S}^{-1}"] \\ x \in \mathbb{F}^n \arrow[u, "\mathcal{T}^{-1}"] & y \in \mathbb{F}^m \arrow[l, "\mathcal{F}^{-1}"'] \end{tikzcd}$$

Decryption

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



Success
Requires
Standards

Standards Organizations in Quantum-Safe Cryptography

NIST
National Institute of Standards and Technology

ETSI
World Class Standards

Accredited Standards Committee X9 Inc.
Financial Industry Standards

About the Technical Committee Cyber (TC Cyber) 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
- Our 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
- Our work may feed into other ETSI groups and projects as 3GPP and other standards bodies such as International Telecommunication Union (ITU), IETF, etc.
- Our objectives DON'T include the development of cryptographic primitives
  - This is a proposition best left to academia and other groups who specialise in the area

Progress Thus Far in WG QSC

- The following documents have been published:
  - ETSI GR QSC001 Analysis of Quantum-Safe Primitives
  - ETSI GR QSC003 Quantum-Safe Case Studies & Use Cases
  - ETSI GR QSC004 Quantum-Safe Threat Analysis
  - ETSI GR QSC006 Limits of Quantum Computing on Symmetric Key Cryptography
  - ETSI TR 103 570 Quantum-Safe Key Exchanges, Implementation Analysis
  - ETSI TR 103 617 Quantum-Safe Virtual Private Network (VPN)
  - ETSI TR 103 618 Quantum-Safe Identity-Based Encryption (IBE)
- Ongoing Work Items:
  - QSC-008: Quantum-Safe Cryptographic Signature assessment, (INRIA)
  - QSC-13: Migration Techniques to Quantum-Safe Systems, (Cadzow Communication)
  - QSC-14: Quantum-Safe Hybrid Key Exchange TS (Amazon)

New Work Item Proposals

- In addition to the ongoing work, the following work is being contemplated by the QSC
  - Creation of Stage 1, 2, 3 for a VPN TS
  - Creation of additional Stage 1, 2, 3 for Hybrid Key Exchange TS
  - Secure updating of automotive firmware, software downloads
  - Various discussion documents regarding migration methods
  - Potential WI for Quantum-Safe authentication protocol for quantum key exchange (QKD) systems

Migration to quantum-safe systems

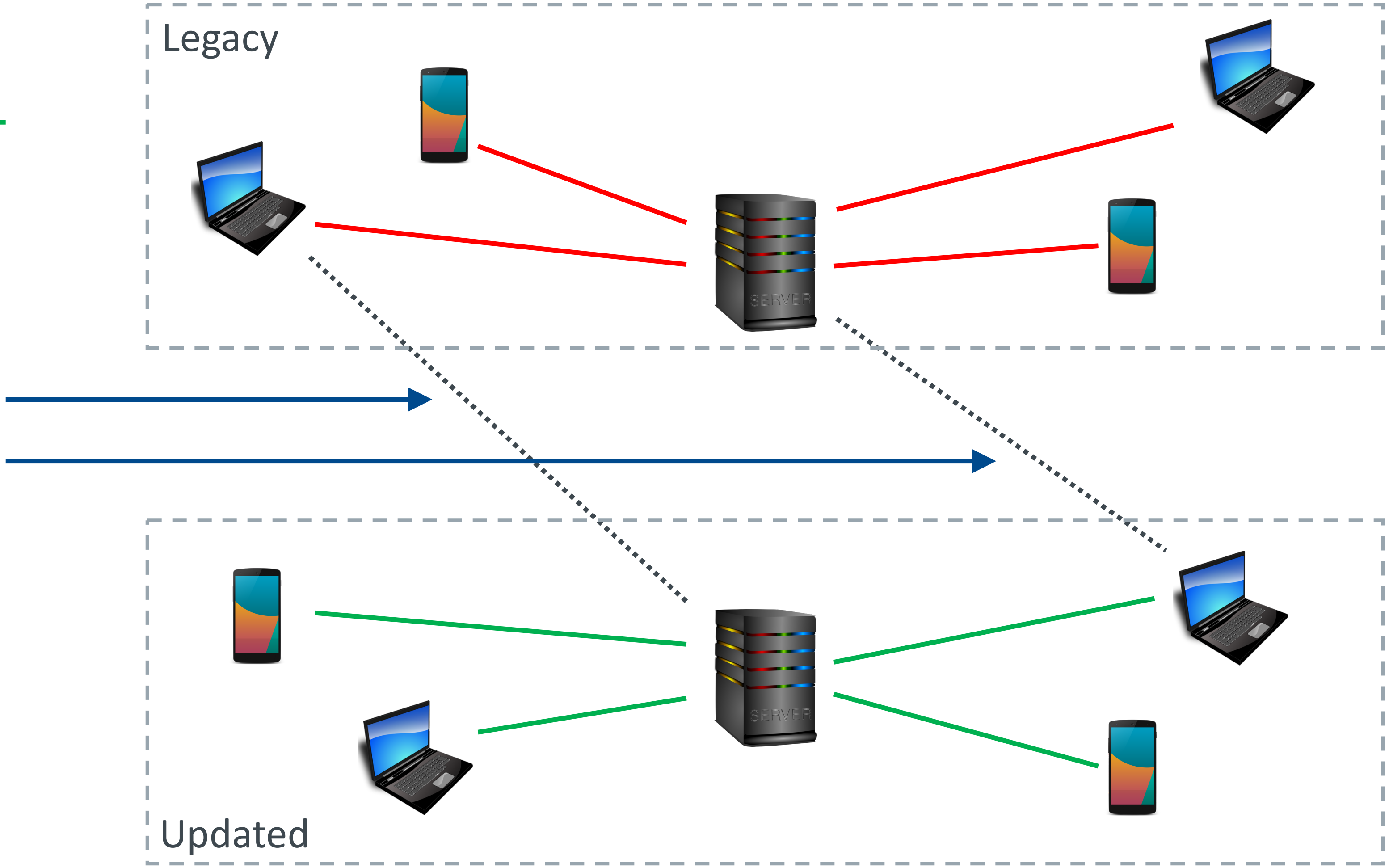
Migration Could Take Years…

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

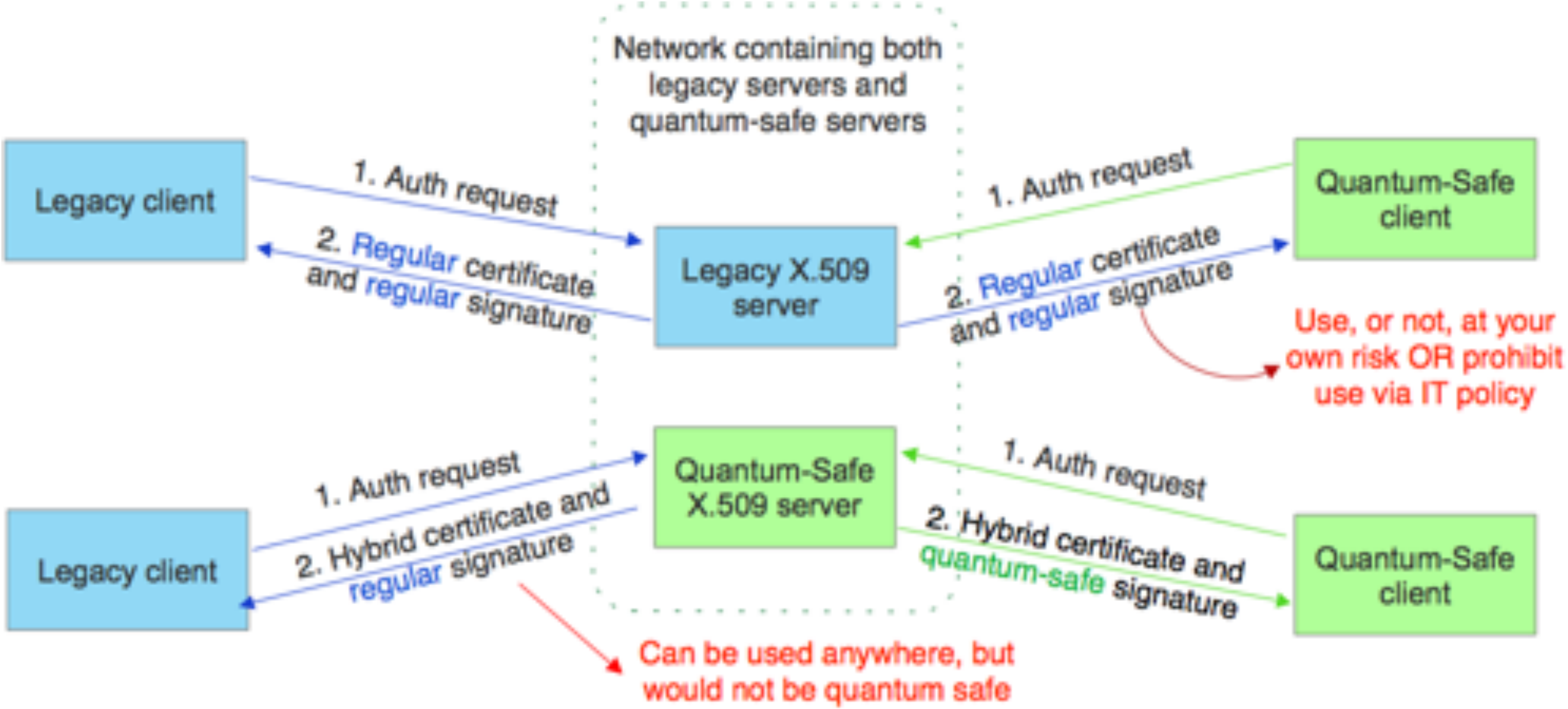
Engagements with other groups

- As result of the work in GR QSC-001, GR QSC-003 and GR QSC-004, the concept of a hybrid cryptographic certificate was introduced to ITU-T SG17 Q.11 by ETSI QSC member ISARA Corporation
- A hybrid certificate definition was accepted as an optional feature into the next version of the Rec. X.509 certificate standard based on this work
- This is a type of cryptographic certificate that eases migration from conventional to quantum-safe, by allowing certificate servers to use both conventional and quantum-safe certificates at the same time, until full network migration is achieved

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?


Network containing both legacy servers and quantum-safe servers
Legacy client
1. Auth request
2. Regular certificate and regular signature
Legacy X.509 server
1. Auth request
2. Regular certificate and regular signature
Quantum-Safe client
Use, or not, at your own risk OR prohibit use via IT policy
Legacy client
1. Auth request
2. Hybrid certificate and regular signature
Quantum-Safe X.509 server
1. Auth request
2. Hybrid certificate and quantum-safe signature
Quantum-Safe client
Can be used anywhere, but would not be quantum safe

Introduction to published specifications

ETSI GR QSC001 Analysis of Quantum-Safe Primitives

This Group Report discusses the basic principles of quantum-safe cryptography, the range of options available for implementation and usage as well as certain performance considerations and constraints such as cryptographic key-lengths and computational requirements

- Primitive families, Primitive types, Application-specific or restricted-use cases, Other mechanisms
- We introduce an asessment framework to include security (classical, provable, quantum and forward security), efficiency and deployment and implementation issues
- In-depth analysis on the 5 basic families of quantum-safe classes (Hash-based, Code-based, Lattice-based, Quadratic multivariate and Isolgeny-based)

ETSI GR QSC003 Quantum-Safe Case Studies & Use Cases

A practical analysis of the consequences of implementing and deploying certain quantum-safe methods

- Network security protocols: TLS, the notion of Drop-in replacements, Hybrid schemes, re-engineering, integration into network protocol stack and the handling of large key sizes
- Offline services & secure email, as well as credentials for these services
- Internet of Things (IoT) and the consequences and limitations of quantum-safe technology and its deployment on inexpensive equipment
- Satellite communication and streaming secure data in broadcast (1-to-many) environments such as sending video from drones
- Key-distribution centres, authentication and some of the more exotic techniques such as Attribute Based Encryption (ABE) and Identity Based Encryption (IBE)

ETSI GR QSC004 Quantum-Safe Threat Analysis

An overview of what is vulnerable over time to quantum attacks

- Includes introduction to Shor’s and Grover’s algorithms and the requirements of quantum computation to enable widespread use of these techniques
- Discussions of network security protocols such as TLS, IPSec, S/MIME, Public Key Infrastructures, etc. and their vulnerabilities
- Range of industry-specific applications relative to the requirements of
  - banking and finance
  - intelligent transportation systems
  - Internet of Things
  - digital media content protection
  - eHealth

ETSI GR QSC006 Limits of Quantum Computing on Symmetric Key Cryptography

This is the only effort addressing Symmetric Key Cryptography thus far, presenting a theoretical survey framwork for the following:

- Asymmetric cryptography & symmetric cryptography and their vulnerabilities to quantum computing
- About quantum computers, number of qubits, implementation level taken to the limits of the physical atoms
- Speculation on the power of quantum computers in the future
  - Learning curves such as Moores Law
  - Directions for commercial quantum computers
  - Worst-case for quantum computation
  - Upper bounds for computing quantum computing budgets
- Discussion of key lengths, hashes and parameter selection

ETSI TR 103 570 Quantum-Safe Key Exchanges, Implementation Analysis

- This Technical Report (TR) covers a range of quantum-safe key exchange mechanisms, such as Learning with Errors (LWE), Ring Learning with Errors (RLWE), supersingular isogenies, SIDH, Niederreiter, and others with regard to parameter selection, performance and implementation constraints , including
  - Key validation, Key generation, Key extraction, Reconciliation
  - Invalid key attacks, public parameters, parameter selection
- Also analysed and discussed
  - Performance on a 64-bit processor
  - Performance on a 32-bit embedded processor
  - Performance on 32-bit microcontrollers

ETSI TR 103 617 “Quantum-Safe Virtual Private Networks

This Technical Report (TR) explores protocol requirements necessary to add quantum resistance to VPN technologies, including client, server and architectural considerations

- Includes a general discussion on VPN requirements – what are the basic ingredients ?
- Specific requirements around protocols and key establishment are considered, based on the multitude of systems that are at risk and require security updates before quantum computers that can attack commercial cryptography are developed
  - Internet Key Exchange (IKE)
  - Transport Layer Security (TLS)
  - Secure Shell (SSH)
  - Medium Access Control Security (MACSec)
- Also included are analysis of experimental results on message fragmentation and impacts to protocols

Questions & Comments?

Contact me:

mpecen@approachinfinity.ca

Mark Pecen

- MARK PECEN serves as Senior Advisor to Quantum Valley Ideas Lab, a specialized advanced technology research centre with focus on quantum 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.