In-flight data protection for the quantum age

Chris Janson

Nokia

October 2024

© 2024 Nokia

In-flight data protection for the quantum age

Agenda

1. The quantum threat, HNDL, timelines
2. Government and industry initiatives and responses
3. Defining a Quantum-Safe Network
4. Tools in the chest: crypto ciphers, key distribution, key material
5. A quantum-safe network blueprint: build today, evolve with the threat

© 2024 Nokia

Let’s make sense of the soup!

MACsec

QKD

RS

PQC

Q-day

CRQC

SSL TLS

IPsec

PKI

AES

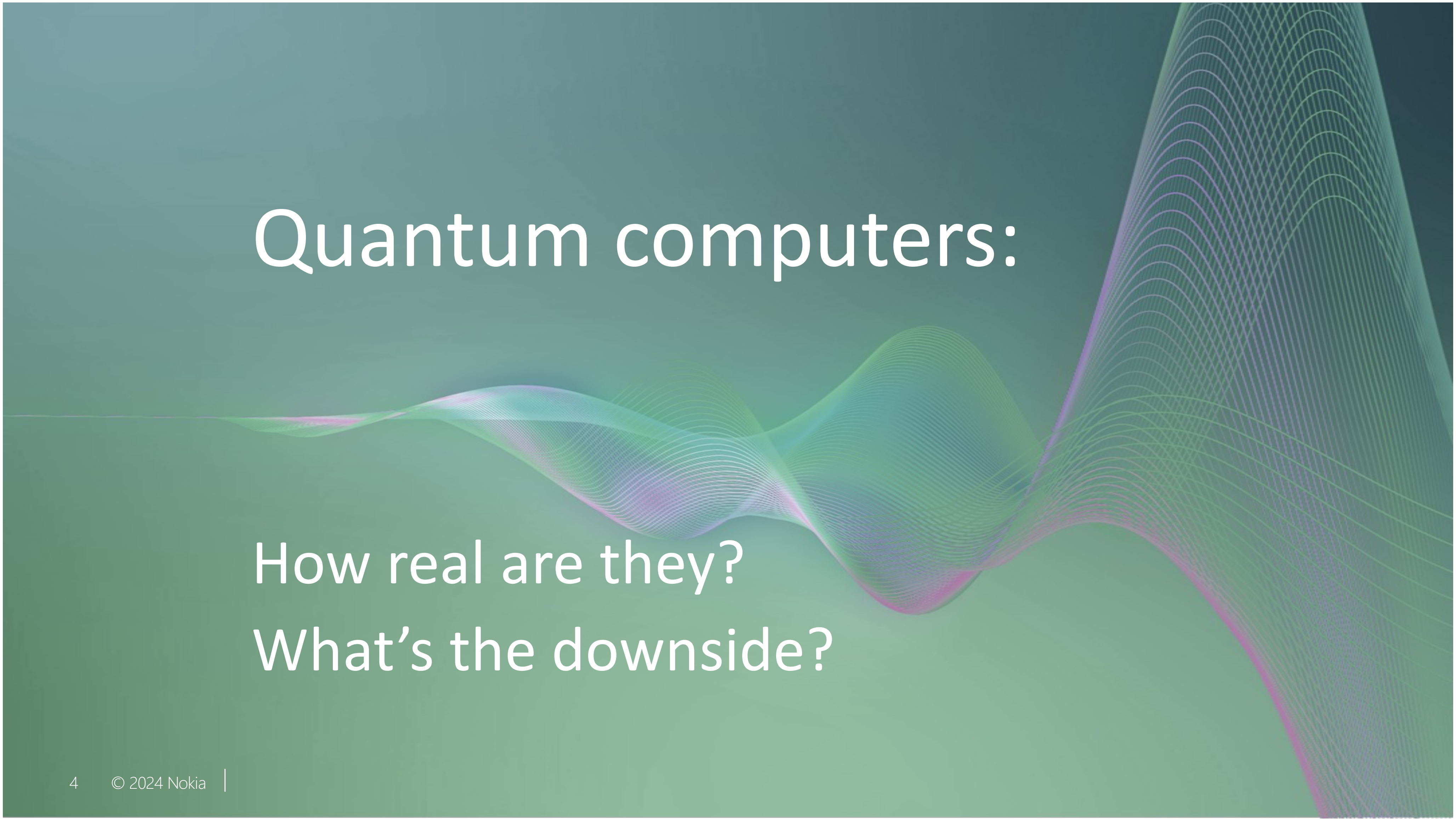
PKC

OTNsec

QCI

QSN

RSA



Quantum computers:

How real are they?

What’s the downside?

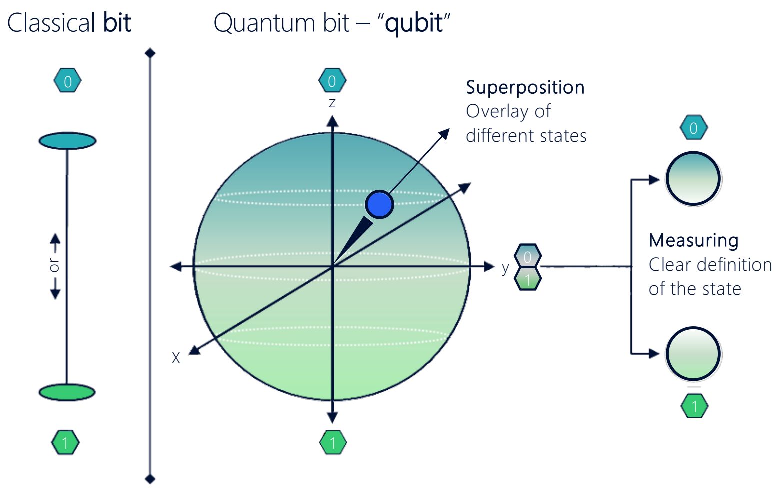
© 2024 Nokia

Quantum computing

Massively different, massively powerful

- Quantum computer: a machine that can perform quantum computations using particles subject to quantum physics– eg: photons or superconducting materials to create logical gates

- Qubits: fundamental unit of computation. Allows multiple states at once (superposition) and correlation (entanglement)



Classical bit

Quantum bit – "qubit"

Superposition
Overlay of different states

Measuring
Clear definition of the state

Source: IBM presentation at Quantum World Congress, Sept. '23, Washington, DC

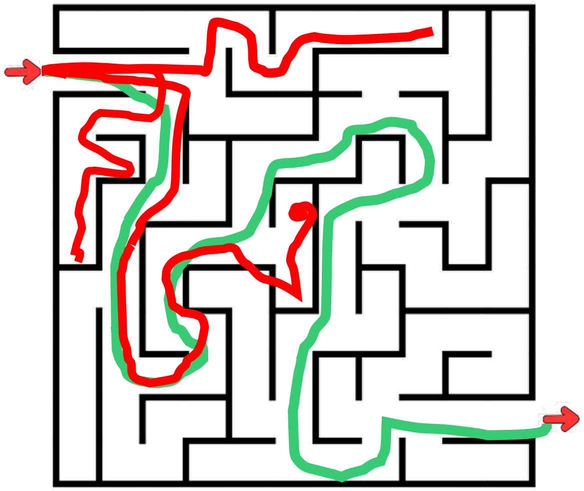
© 2024 Nokia

Quantum computing

Massively different, massively powerful

Parallel processing at exponential scale:

M. Kaku describes it as capable of finding the path out of a maze in a single path calculation



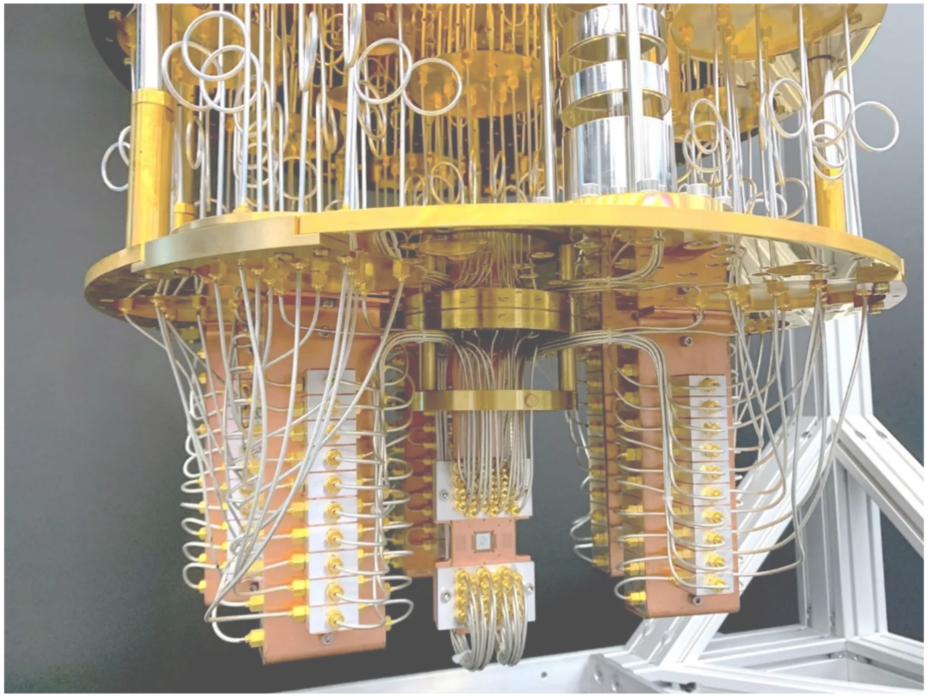


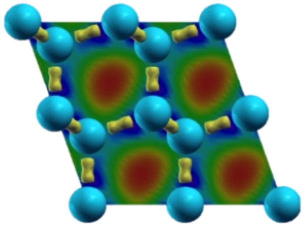
Photo journey inside an IBM quantum computer

© 2024 Nokia

Quantum computing

What's driving their development?

- **Computational speed:** exponential increase
- **Complex problems:** materials research, drug discovery, energy optimization, AI
- **Basic research** and curiosity
- **Information security**

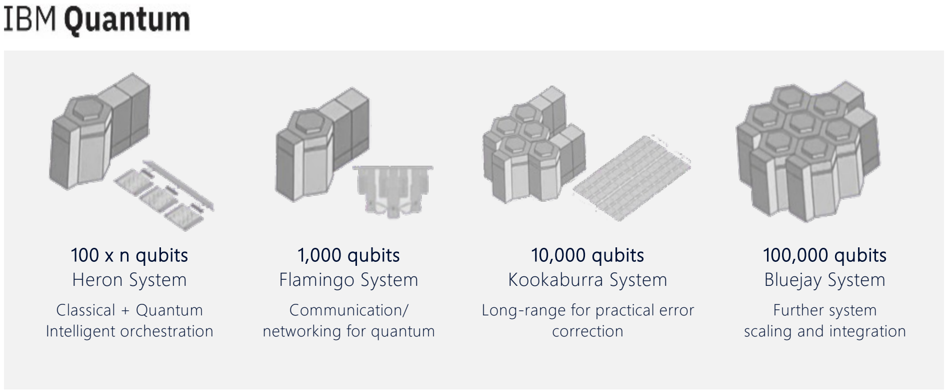


© 2024 Nokia

Quantum computing

How real are they? Not just a science project anymore

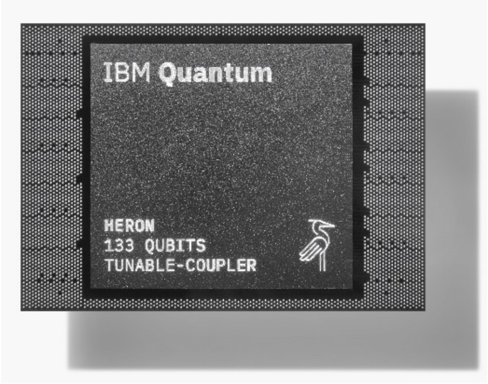
- **Many technical barriers**: qubit stability, error correction, scaling, supercooling
- **$B's invested** over past few years, globally; public and private funding
- **Clear progress** reported in multiple papers at SC23
- **IBM** announced their System 2, modular quantum architecture in Dec '23
    - Roadmap to a 100K Qubit system



IBM Quantum

100 x n qubits Heron System	1,000 qubits Flamingo System	10,000 qubits Kookaburra System	100,000 qubits Bluejay System
Classical + Quantum Intelligent orchestration	Communication/ networking for quantum	Long-range for practical error correction	Further system scaling and integration

Source: IBM presentation at Quantum World Congress, Sept. '23, Washington, DC



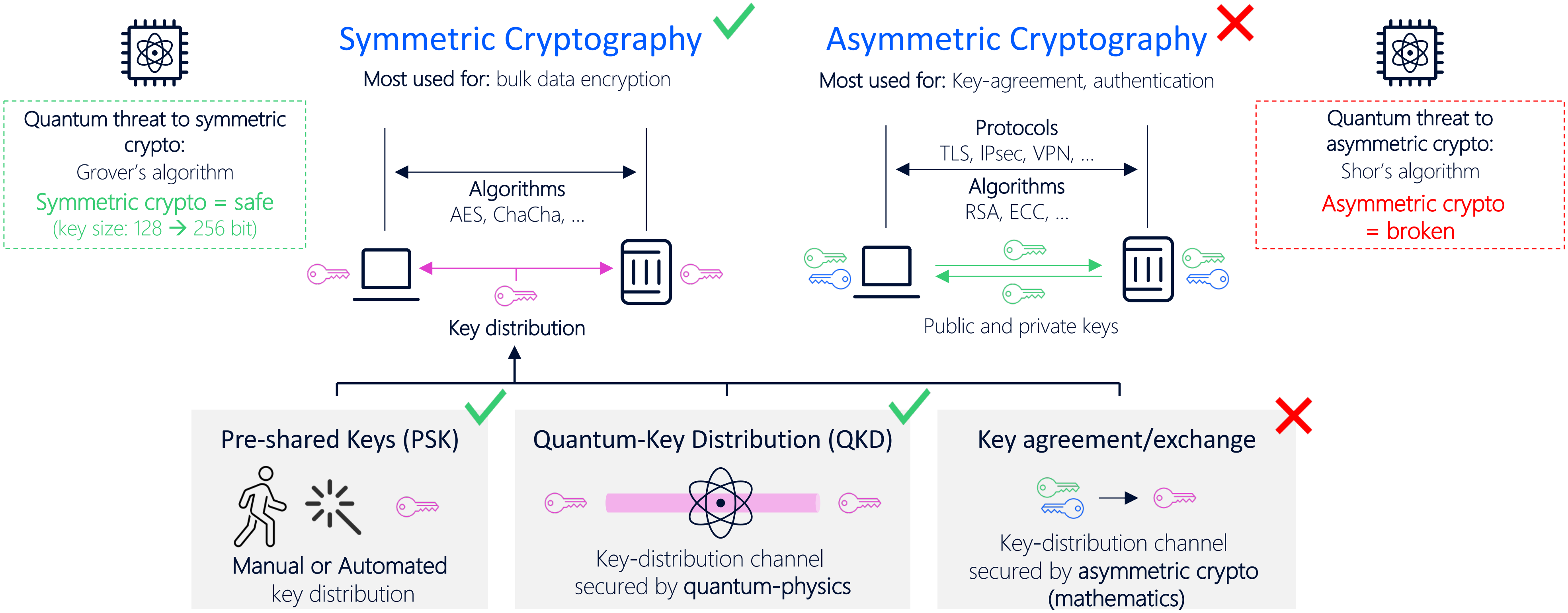
What's the downside?

Quantum computing breaks a decades-long approach to network security.

© 2024 Nokia

Quantum computers break widely-used asymmetric crypto

Symmetric crypto solutions are still safe



Quantum threat to symmetric crypto:
Grover's algorithm
Symmetric crypto = safe
(key size: 128 → 256 bit)

Symmetric Cryptography ✓

Most used for: bulk data encryption

Algorithms
AES, ChaCha, …

Key distribution

Asymmetric Cryptography ✗

Most used for: Key-agreement, authentication

Protocols
TLS, IPsec, VPN, …

Algorithms
RSA, ECC, …

Public and private keys

Quantum threat to asymmetric crypto:
Shor's algorithm
Asymmetric crypto = broken

Pre-shared Keys (PSK) ✓

Manual or Automated key distribution

Quantum-Key Distribution (QKD) ✓

Key-distribution channel secured by **quantum-physics**

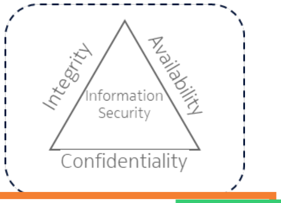
Key agreement/exchange ✗

Key-distribution channel secured by **asymmetric crypto (mathematics)**

© 2024 Nokia

First, let’s consider some network security basics….

Cryptography is a powerful tool to contain these risks



Eavesdropping

Collect sensitive data, system commands and login info

Confidentiality breached

Man-in-the-middle

Command spoofing with inverted logic of system configuration

Integrity compromised

Denial of service

Flood with illicit control traffic with legitimate IP and TCP/UDP header to overwhelm the system

Availability down

Confidentiality, integrity and availability

Threatened by quantum computing

Integrity
Availability
Information Security
Confidentiality

Eavesdropping

Collect sensitive operational data including system commands and system login info

Confidentiality breached

Man-in-the-middle

Command spoofing with inverted logic (e.g. from close position to open) of system configuration

Integrity compromised

Denial of service

Flood with illicit control traffic with legitimate IP and TCP/UDP header to overwhelm the system

Availability down

Why act now?

CRQC and the HNDL threat

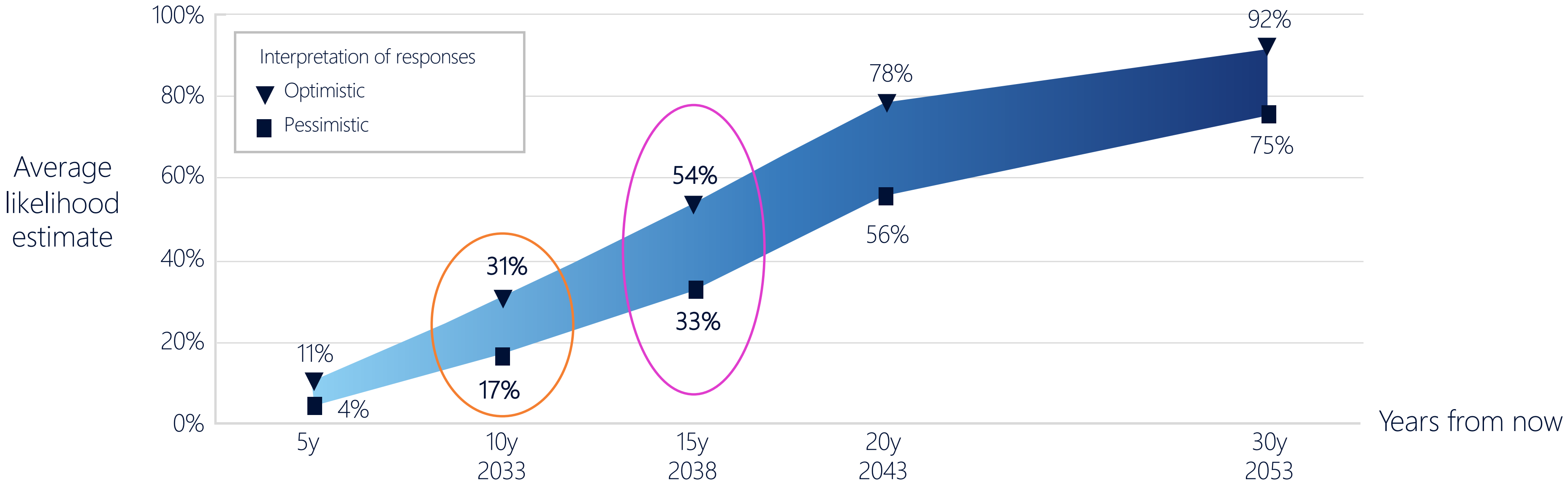
A Quantum computer with a sufficient number of qubits is defined as a **Cryptographically Relevant Quantum Computer (CRQC)** and can decrypt asymmetric security protocols

Harvest Now, Decrypt Later (HNDL) a clear and present danger

Growing CRQC threats: Time for Action

Global Risk Institute View

Expert survey on the likelihood of a Quantum Computer breaking RSA-2048 in 24h (2023)



Source: Global Risk Institute, Quantum Threat Timeline Report 2023

Policy makers are responding to the security impact

Is your cybersecurity ready to take the quantum leap?

EU urged to prepare for quantum cyberattacks with coordinated action plan

The US is worried that hackers are stealing data today so quantum computers can crack it in a decade*

Singapore to build national quantum-safe network that provides robust cybersecurity for critical infrastructure

South Korea plans large scale quantum cryptography adoption

*The US government is starting a generation-long battle against the threat next-generation computers pose to encryption.

OK, OK ....there’s a threat!

What can we do about it?
How hard is this going to be?

Soup’s up!: ABC’s of cryptography

Integrity
Availability
Information Security
Confidentiality

Public key crypto

DHKE, ECCA, RSA

Asymmetric, public key (PKI) paired with math calculation

Pre-shared key crypto

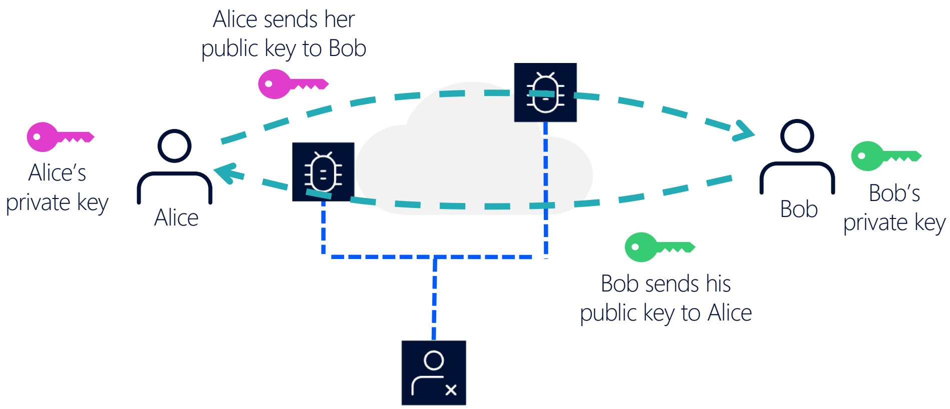
3DES, AES 128/256

Symmetric, pre-shared key (PSK)

Public key cryptography

Public key to encrypt, private key to decrypt

Alice and Bob share their public keys



Alice sends her public key to Bob

Alice's private key

Alice

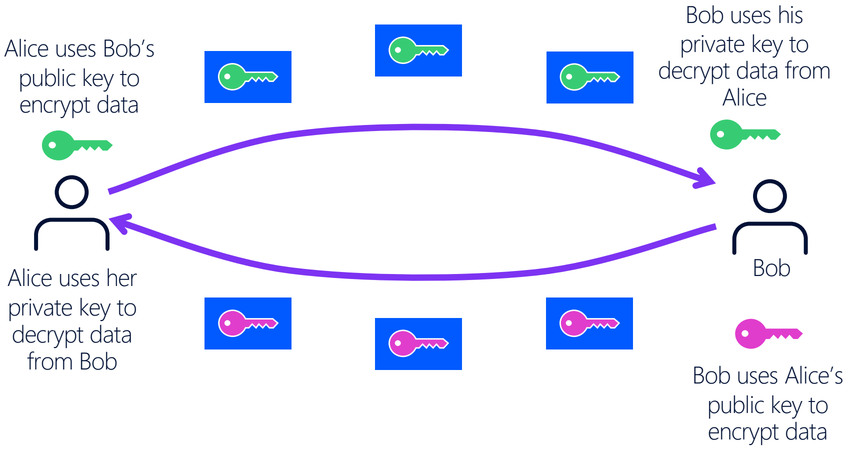
Bob

Bob's private key

Bob sends his public key to Alice

VULNERABILITY:
Eavesdropping was harmless, until now

Alice and Bob send encrypted data using each other's public keys



Alice uses Bob's public key to encrypt data

Bob uses his private key to decrypt data from Alice

Alice uses her private key to decrypt data from Bob

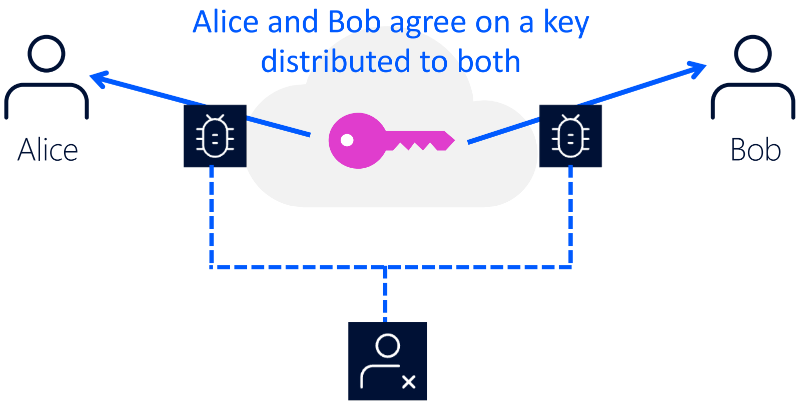
Bob

Bob uses Alice's public key to encrypt data

© 2024 Nokia

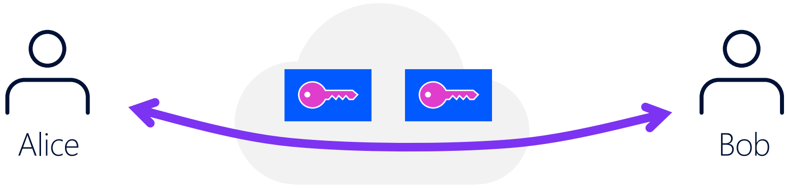
Symmetric key cryptography

Using one secret key to encrypt to decrypt

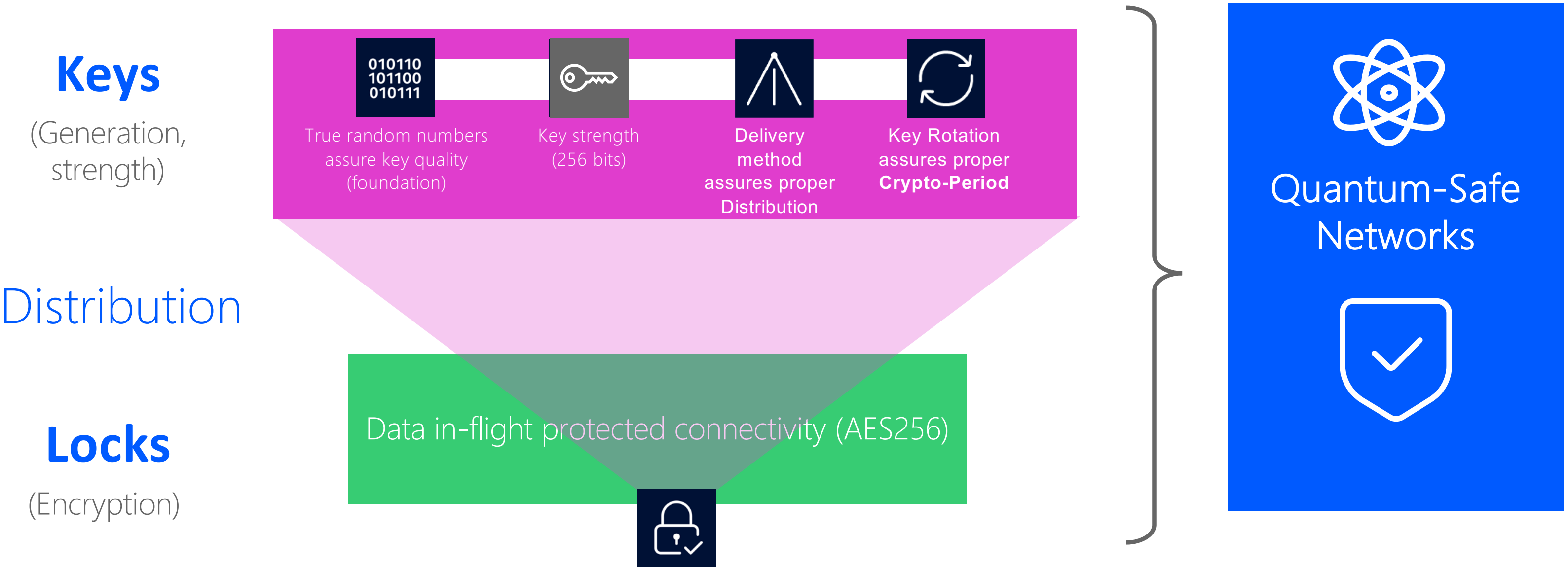

Alice and Bob agree on a key distributed to both

VULNERABILITY:
Eavesdropping during key distribution- but safe if key is removed from data path

After receiving the key, they start exchange encrypted data



Ingredients of Quantum-Safe Networks


Keys
(Generation, strength)
010110
101100
010111
True random numbers assure key quality (foundation)
Key strength (256 bits)
Delivery method assures proper Distribution
Key Rotation assures proper **Crypto-Period**
Distribution
Locks
(Encryption)
Data in-flight protected connectivity (AES256)
Quantum-Safe Networks

A Defense-in-depth approach

An additive approach with layered cryptography

Mathematics & Physics based Cryptosystems

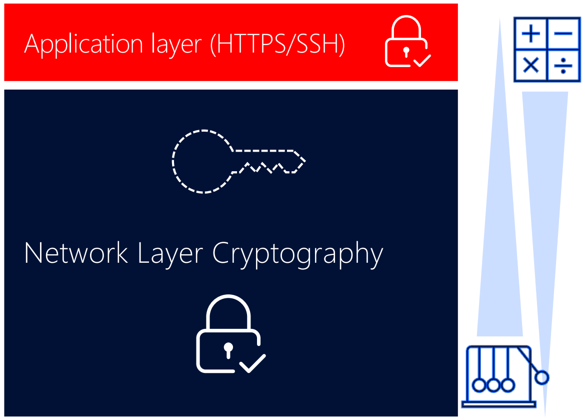
Mathematics

- Public Key Cryptography
- Key exchange approach
- Authentication and encryption

Physics

- Symmetric keys
- Key distribution approach
- Authentication and encryption

Adapt, Scale and Evolve your infrastructure security with defense in-depth



Application layer (HTTPS/SSH)

Network Layer Cryptography

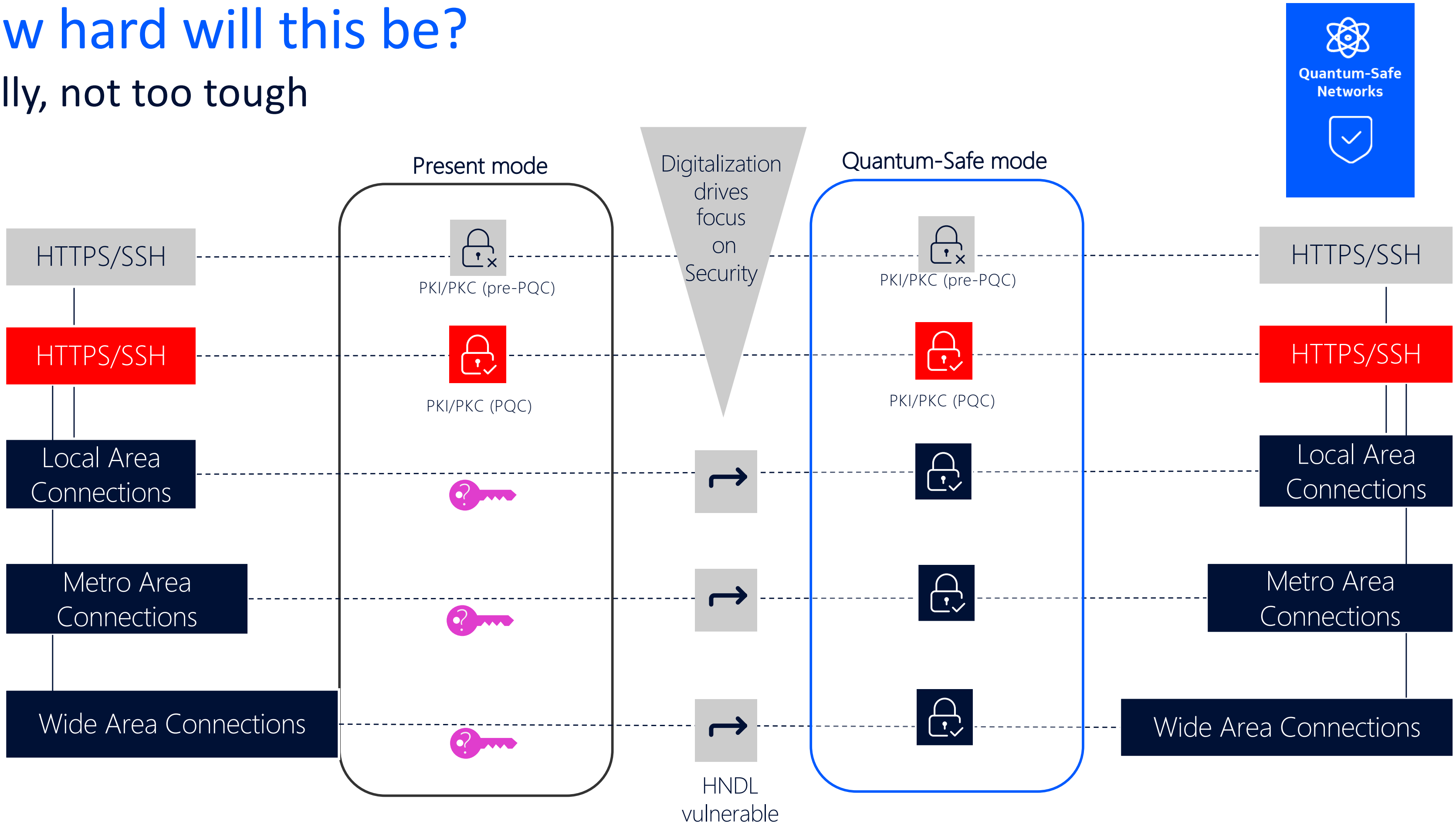
Start today with an additive approach

1+1 or 1+2 or 1+N

- Application layer (HTTPS/SSH)
- Network layer (ANYsec/IPsec)
- MPLS layer (ANYsec)
- Data link layer (MACsec)
- Physical layer (OTNsec)

How hard will this be?

Really, not too tough



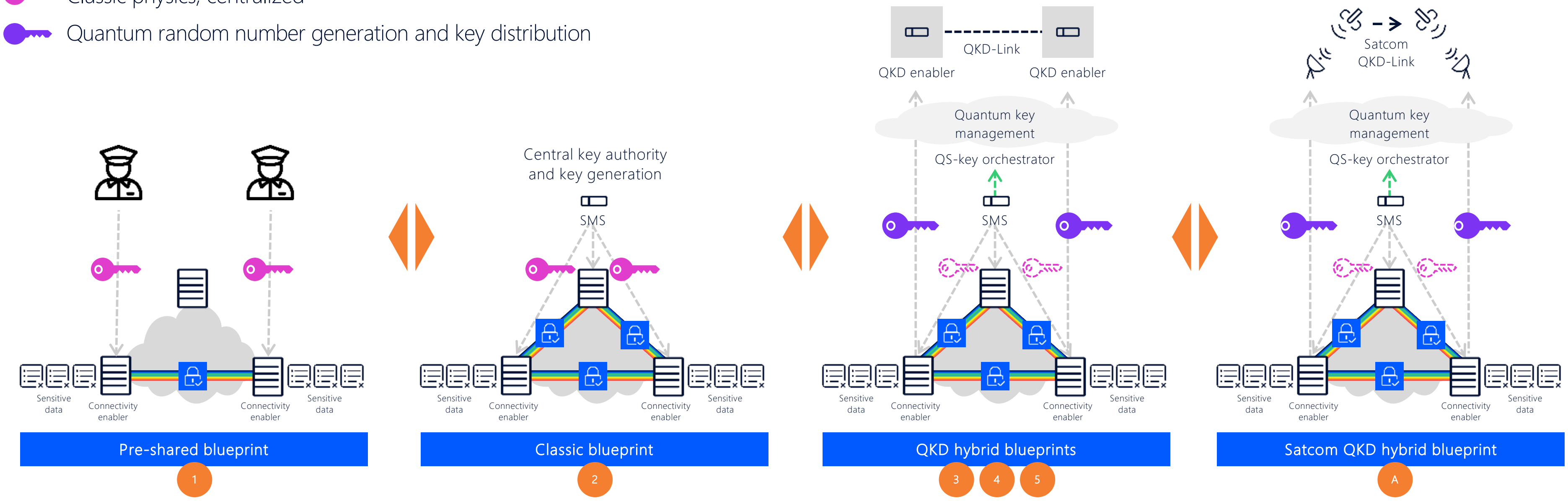
Quantum-Safe Network evolution

Example of PSK evolution

Your Quantum-Safe roadmap: Begin today and adapt to tomorrow's innovations

Classic physics, centralized

Quantum random number generation and key distribution



Central key authority and key generation

SMS

QKD-Link

QKD enabler

QKD enabler

Quantum key management

QS-key orchestrator

Satcom QKD-Link

Sensitive data

Connectivity enabler

Pre-shared blueprint

1

Classic blueprint

2

QKD hybrid blueprints

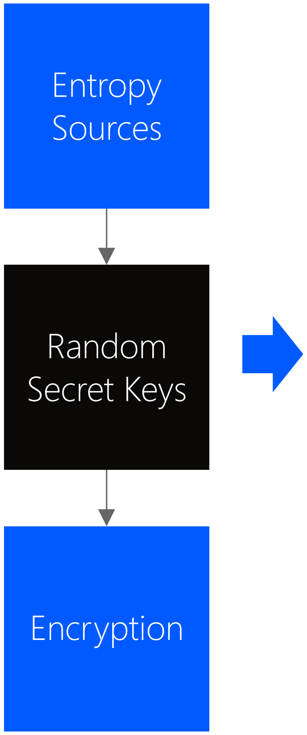
3 4 5

Satcom QKD hybrid blueprint

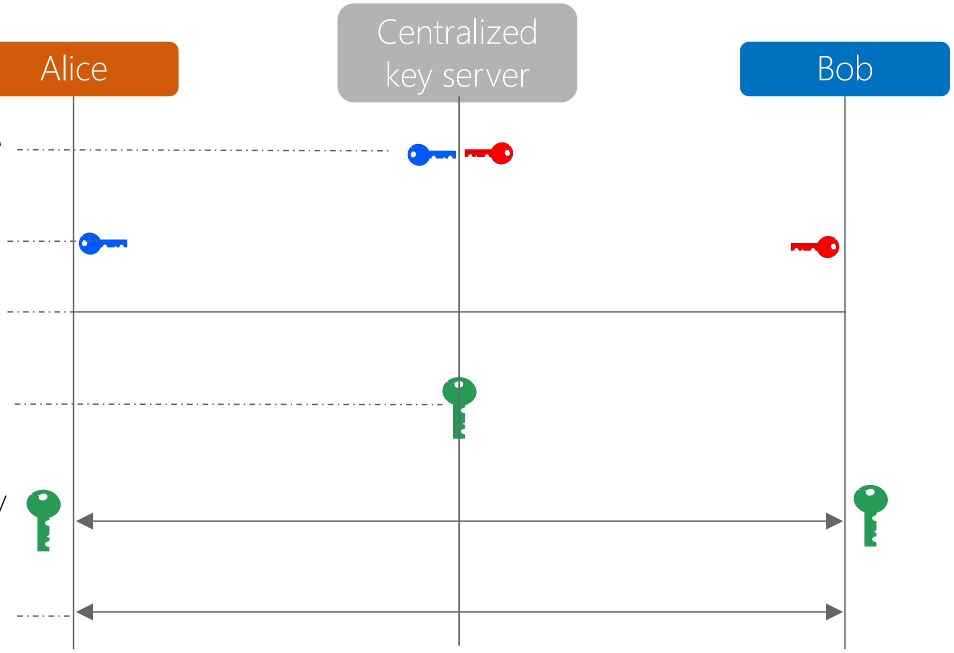
A

Key distribution

Automated PSK distribution



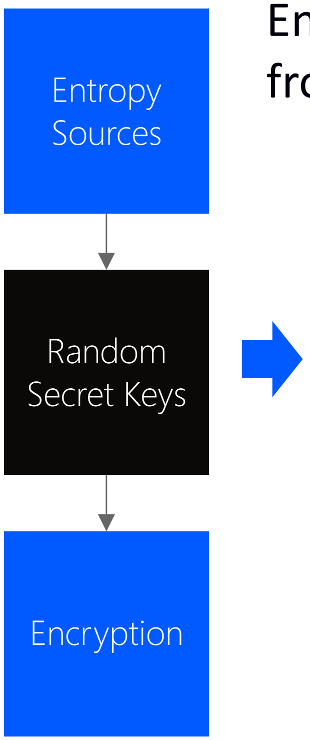
1. Server generates PSK from a TRNG to secure control path to NE
2. PSK from server is installed on the NE at commissioning
3. Alice and Bob configure SNMPv3 (UDP) for the control path with the PSK
4. Server follows security policy and produces session Key for Alice and Bob
5. Server initiates PSK rotation, validates the Key and monitors the NE for Key mismatches
6. Bulk data is encrypted with Session Key



© 2024 Nokia

Key distribution

Hybrid Multi-Vendor Quantum Key Distribution solution



Entropy Sources

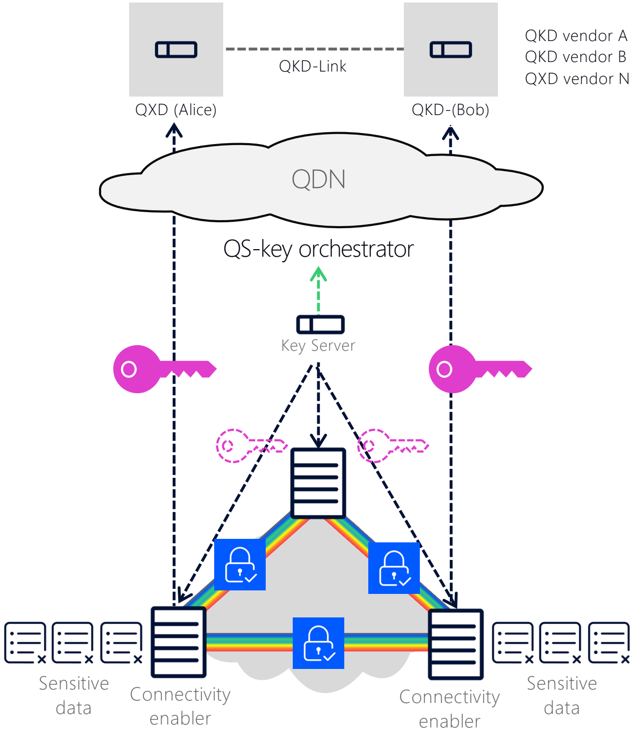
Random Secret Keys

Encryption

Enable support of **QKD multi-vendor** from single key orchestrator

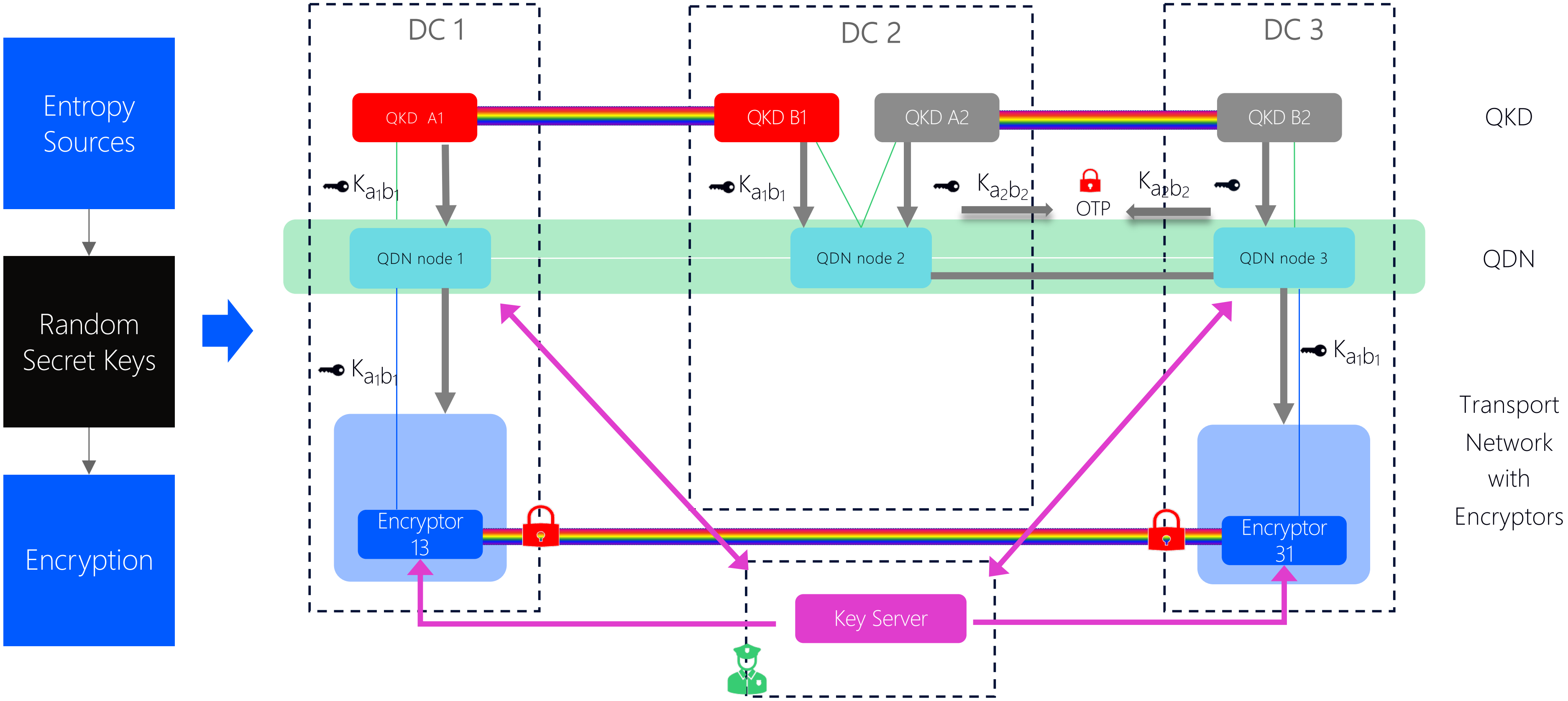
Hybrid

Classic Key Distribution Network	Quantum Key Distribution Network



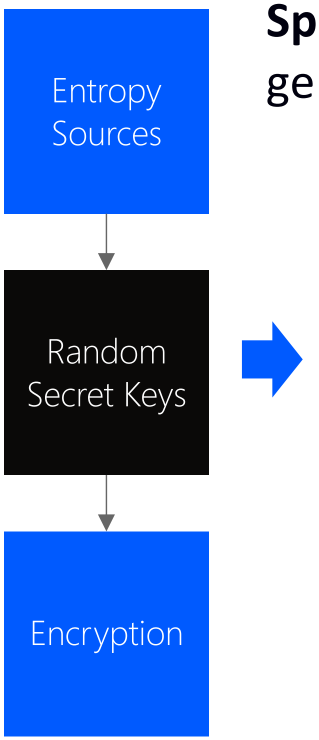
Hybrid Quantum Key distribution 3 node example

Multi-Vendor scenario



Key distribution

Hybrid Multi-Vendor Satcom Quantum Key Distribution solution


Entropy Sources

Random Secret Keys

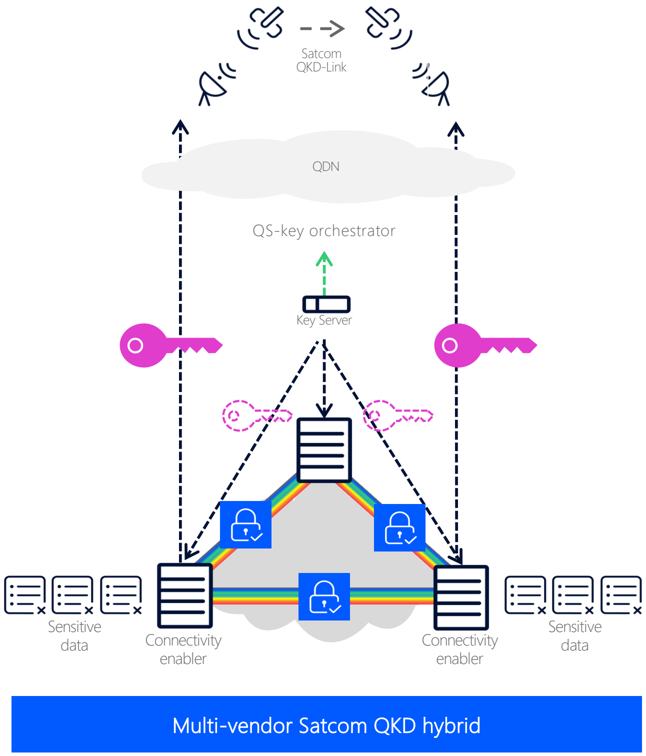
Encryption

Space-based quantum-key generation and distribution

Hybrid

Classic Key Distribution Network

Quantum Key Distribution Network



© 2024 Nokia

Respond to the threat:

You need to act now

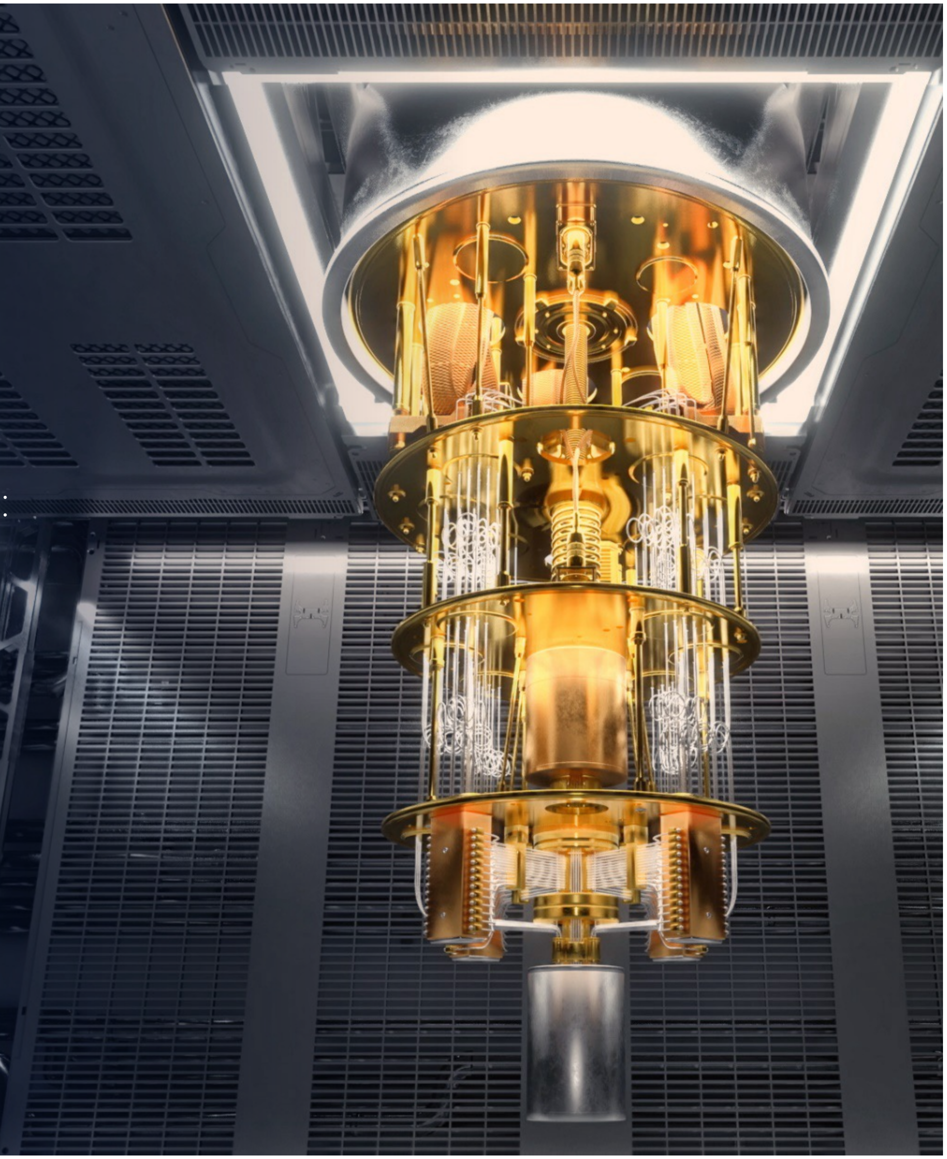
Impossible to “time the threat”

- 5 or 15 years until Q-day? We won’t know

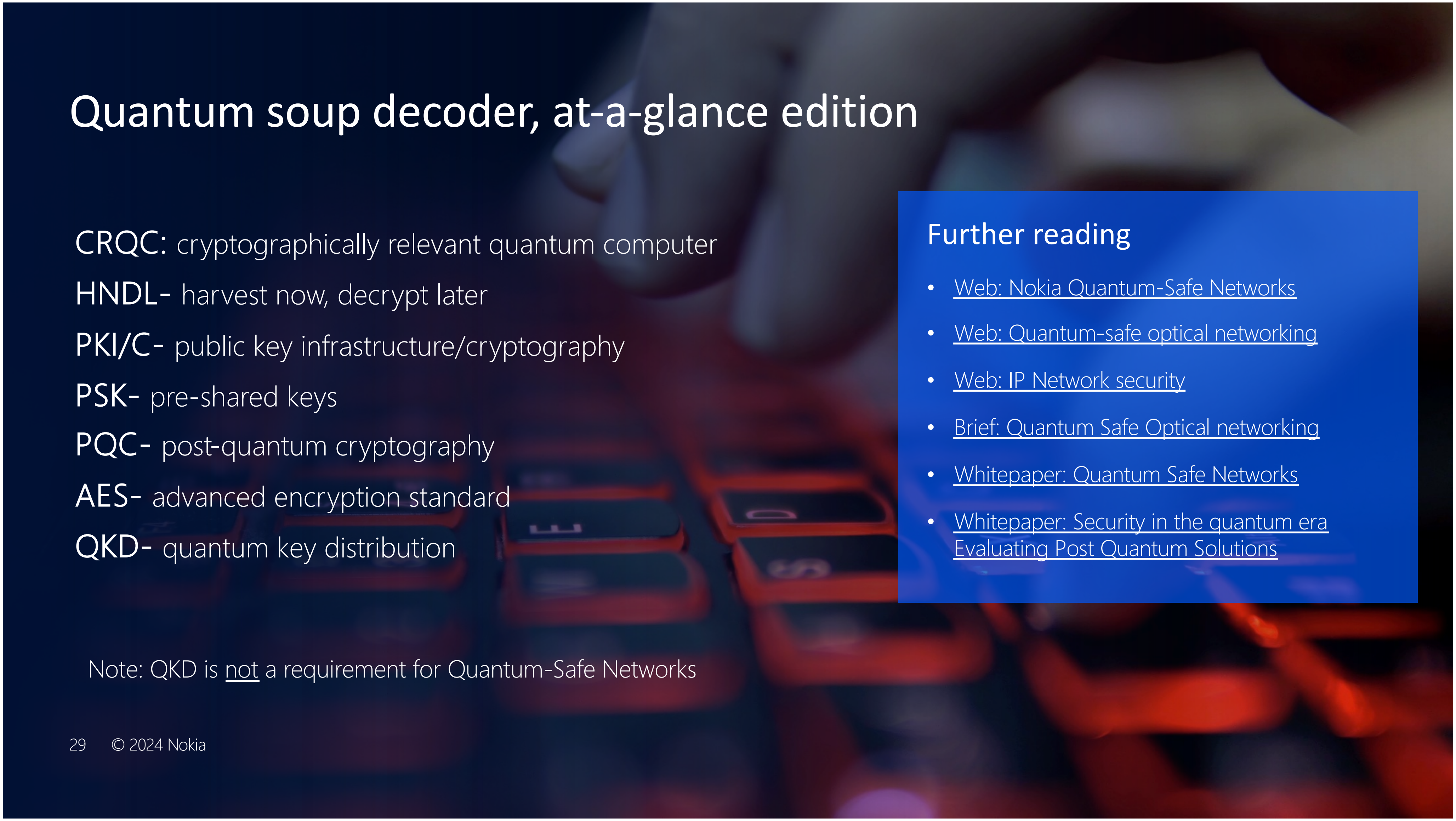
New ciphers, new commercial products, system change-outs: all take time.

Act now

- Develop a plan to adopt quantum-safe protections. Implement as part of your refresh cycle.



© 2024 Nokia



Quantum soup decoder, at-a-glance edition

CRQC: cryptographically relevant quantum computer

HNDL- harvest now, decrypt later

PKI/C- public key infrastructure/cryptography

PSK- pre-shared keys

PQC- post-quantum cryptography

AES- advanced encryption standard

QKD- quantum key distribution

Note: QKD is not a requirement for Quantum-Safe Networks

Further reading

- Web: Nokia Quantum-Safe Networks
- Web: Quantum-safe optical networking
- Web: IP Network security
- Brief: Quantum Safe Optical networking
- Whitepaper: Quantum Safe Networks
- Whitepaper: Security in the quantum era Evaluating Post Quantum Solutions

Thank you!
Q&A?