QKD and PQ: Approaching Security as an Onion

Quantum Communication Conclave
New Delhi

Bruno Huttner ; ID Quantique

March 2023

1

The Quantum Threat

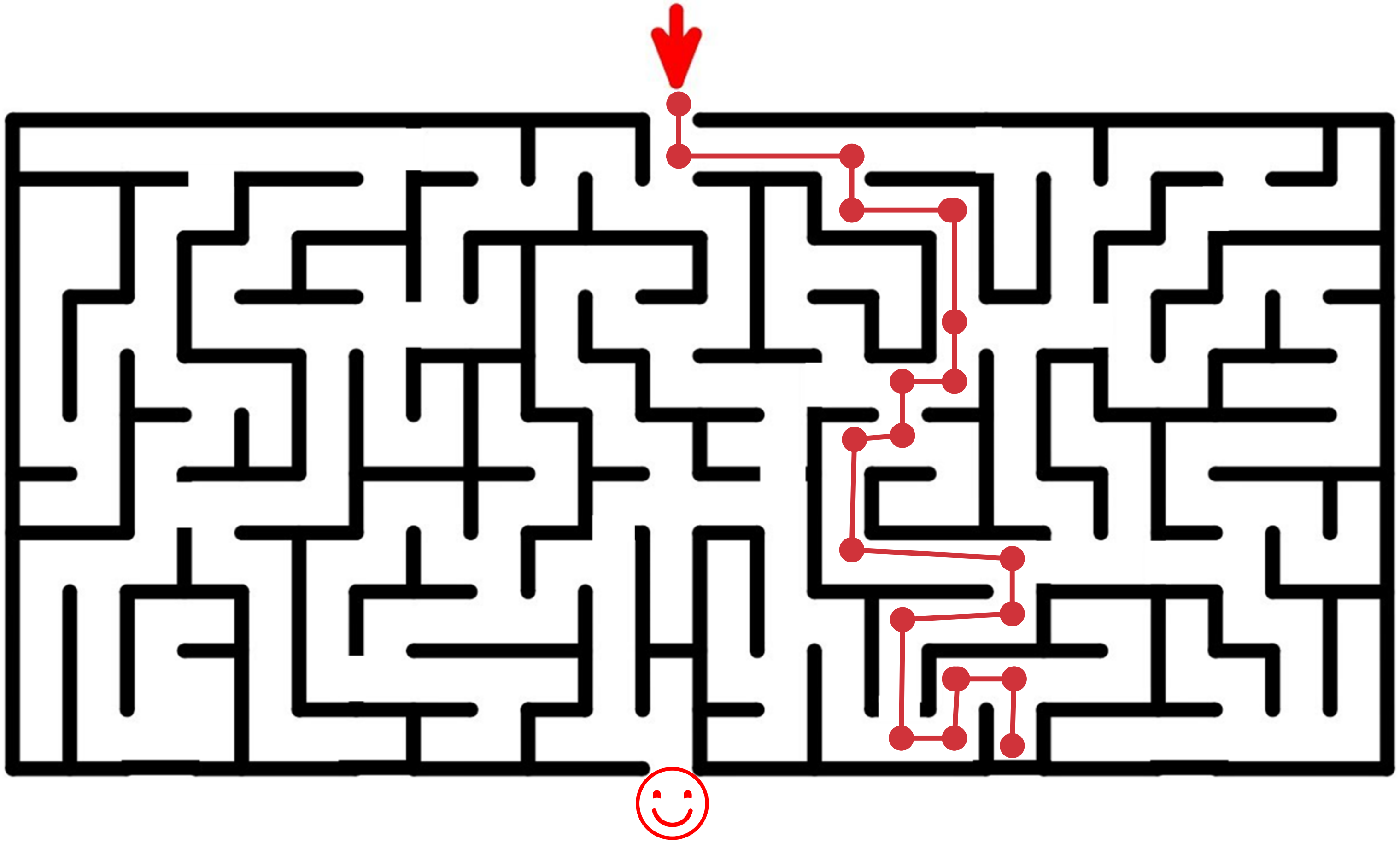
The Quantum Computer

- Computation with Qubits.
- Main difference: build coherent superposition of states.

- Behaves like a massively parallel computer.
- Solves problems in much fewer steps.

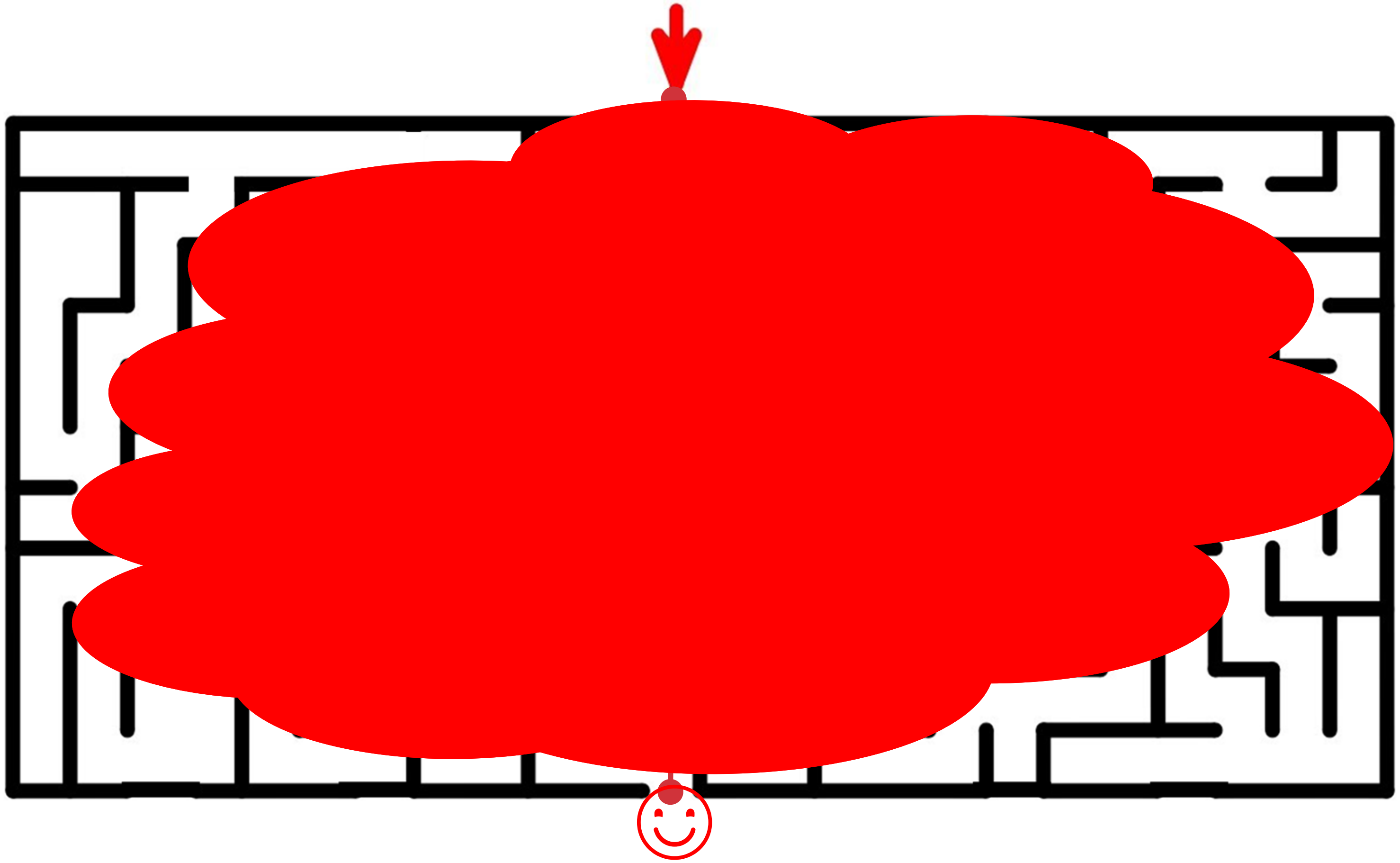
- Some “intractable” (Hard) computations become feasible (Easy).

Computation as a Maze: classical case



Classically: Explore one path at a time...

Computation as a Maze: quantum case



With QC: Explore many paths together; paths may interfere with one another.

The two sides of the Quantum Computer

Opportunities

Threats

What is at risk for crypto?

✓ Symmetric cryptography (secret key)

Encryption

✓ Hash-based functions

Hash-based signature

✗ Most asymmetric cryptography (public/private keys)

Key Exchange Mechanism

Signature schemes

A Time-bomb on security

- ❑ Full-scale quantum computer may be available before the end of the decade

- ❑ Data encrypted with current public Key protocols already vulnerable to « **harvest now, decrypt later** » attacks

2

Possible Solutions:

Towards Quantum-Safe Security

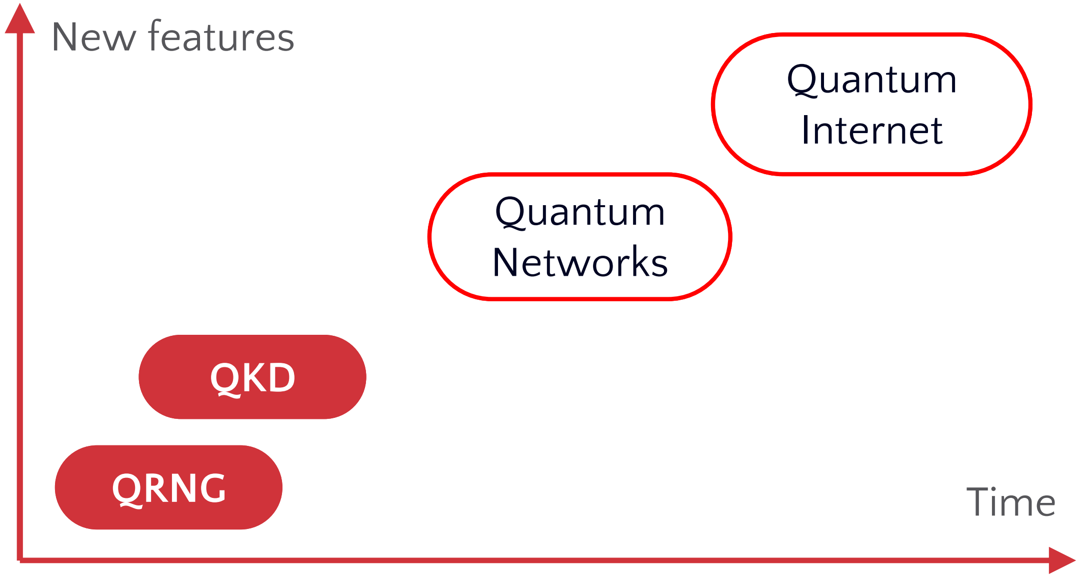
How to address the quantum threats? Quantum-Safe Solutions

Classical solutions

- Post-Quantum Cryptography (PQC).
- Find classical algorithms to replace current ones
- Choose mathematical problems known/believed to be resistant to the Quantum Computer
- The NIST process is exactly doing this now…

Quantum vs. Quantum

Use quantum systems and properties against the Quantum Computer



Classical & Quantum solutions: we need both!

Different solutions for different needs…

Crypto function	Solution
Randomness – Entropy generation	Quantum (QRNG)
Authentication – Signature	Maths (PQC) & Physical (PUF…)
Key Exchange Mechanism	Maths (PQC) & Quantum (QKD)
Encryption	Maths

Two approaches to Quantum-Safe Cryptography

Both technologies, algorithmic-based (PQC) and physics-based (QKD) will co-exist in different use cases

	PQC	QKD
Security	Algorithms will undergo years of study to determine reliability. However, there is no guarantee that nobody could eventually find a way to break them. In addition, for all computational security, security decreases with time	Quantum mechanics guarantees that a quantum channel cannot be successful intercepted without Detection. Security does not decrease with time.
Implementation	Most implementations will use existing communication infrastructure with added SW. End-points (for example IoT) may require specific HW (higher processing and memory requirements)	Initial implementations will require specialized HW. Future aaS offers will use the new quantum infrastructure.
Communication 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 mostly software based	Higher initial cost because hardware and a new communications infrastructure will be required
Global reach	Fully compatible with current global digital technology	Can achieve global reach with Trusted Nodes today (possibly with satellites) and will be able to offer trustless global reach after the development of quantum memories and quantum repeaters
Mobile device compatibility	Fully compatible with any type of communications used by a mobile device	Limited, but could provide KaaS to mobile users with some type of recharging stations, similar to an ATM today.
Cryptographic functions	Both authentication/signature and key exchange	Only key exchange , authentication required by other means

Both technologies have different features as can be seen from the table. Each will have valid use cases

QKD will likely be the right approach for highly sensitive applications, where confidentiality needs to be guaranteed under all circumstances and for a long period of time, e.g. government, military, healthcare and financial service industries.

QKD comes at the disadvantage of higher costs as well as the need for a new quantum infrastructure.

PQC targets applications that put emphasis on mobility, cost and minimizing changes to the hardware infrastructure

However, PQC comes at the clear disadvantage of not providing the long-term security guarantees as the QKD approach

QKD and Authentication Issues

1. QKD is a Key Exchange Mechanism (KEM)
2. One element in a complete cybersecurity system
3. Requires discussion over an **authenticated channel** (service channel)

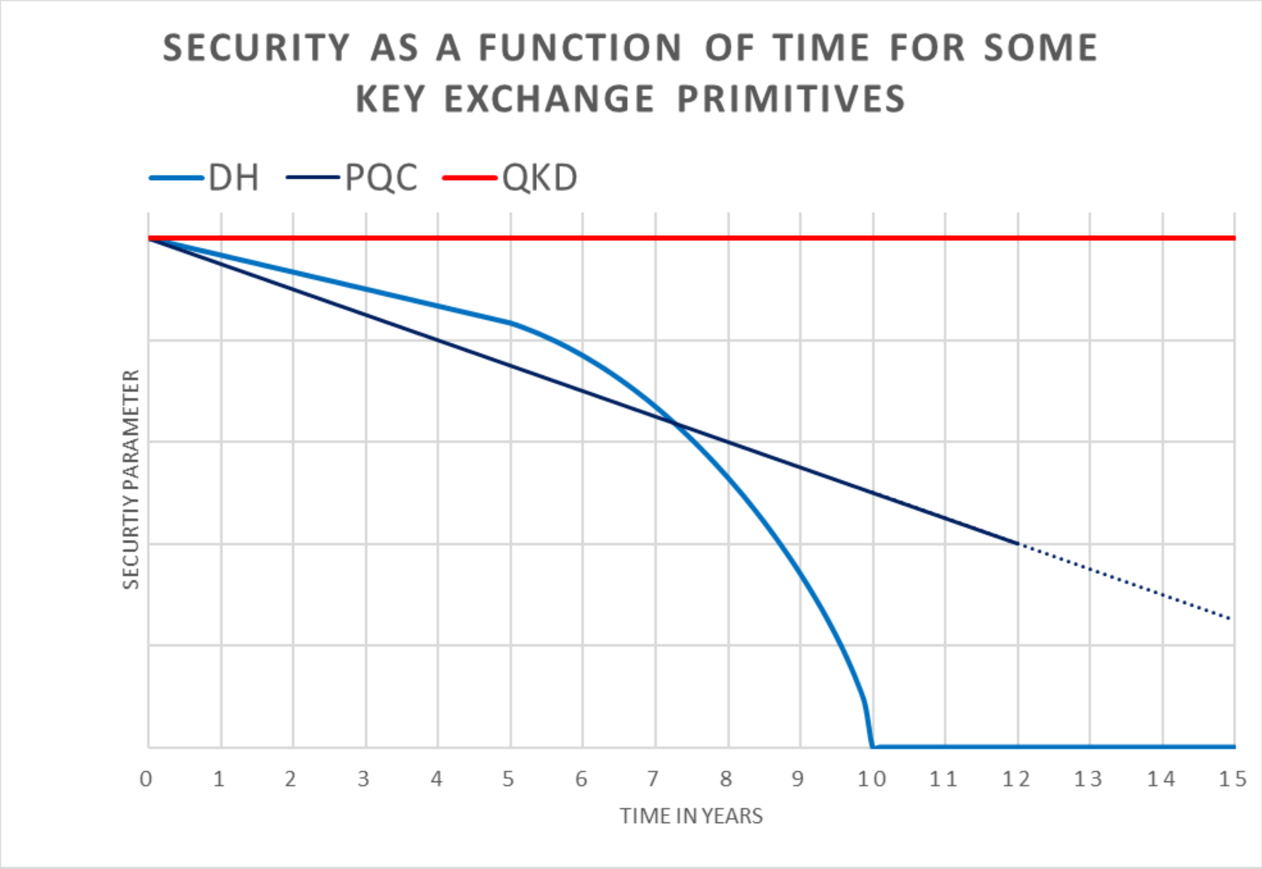
Solutions:

- Initial pre-shared key, which will be renewed with QKD
- Good for single point-to-point operation
- ITS

OR

- Use of quantum-safe signatures (e.g. Hash-based signatures)
- Use Physically Unclonable Functions
- **Good for QKD Networks**

QKD vs. PQC: Time-Dependence is the Essence!



- All **computational security** comes with an expiry date
- Integrate QKD as Key Exchange Mechanism for high-valued information with long-term confidentiality requirements
- Adds one extra layer of security

Quantum-Resistant Algorithms (QRAs)

Name of method	Application	Resilience against Quantum Computer
RSA	KEM, signature	No
ECC	KEM, signature	No
AES	Encryption	Widely believed
Hash-functions	Signature	Widely believed
Lattice-based CRYSTALS-KYBER	KEM	Believed
Lattice-based CRYSTALS-DILITHIUM; FALCON	Signature	Believed
Hash-based SPHINCS+	Signature	Widely Believed
Code-based (Classic Mc Eliece) BIKE	KEM	Believed
HQC; ~~SIKE~~	KEM	Believed

High level of confidence

NIST Selected to be standardized

NIST Round 4 candidates; Under investigation

Risk associated with Quantum Resistant Algorithms

Classical Risks

No security proof (complexity theory).

Asymptotic security well understood – issues with choice of parameters (Matzov attack on Kyber).

Possible attacks with new classical algorithms (Rainbow; Sike)

Progress in computing power.

Quantum Risks

Shor not applicable – What about others? (see Soliloquy).

Grover: double key size for symmetric crypto

Unpredictable new vulnerabilities… A timely reminder!

“As is the norm, an unexpected problem occurred today.”

Summary: Key points

1 The Quantum Computer will break existing Cybersecurity

2 Need to start moving NOW

3 PQC (Algorithmic solutions) are being developed to replace existing algorithms

4 Quantum Solutions (QRNG, QKD, Quantum Networks) add a valuable layer for high security requirements

5 Both have a role to play to achieve Quantum-Safe Security

ID Quantique

Quantum.
Trust enabled for the future

Q & A

bruno.huttner@idquantique.co
m | www.idquantique.com

ID Quantique

Founded in 2001

3 Product lines:

1. Quantum Random Number Generation
2. Quantum-Safe Security
3. Quantum Sensing

High-quality engineering

Best-in-class performance

Trust

Operational simplicity