Post-Quantum

Cryptography Conference

Quantum Resistance through Symmetric Key Cryptography

Pasqualle Verwoerdt

Board of Directors at Compumatica

Quantum Resistance through Symmetric Key Cryptography

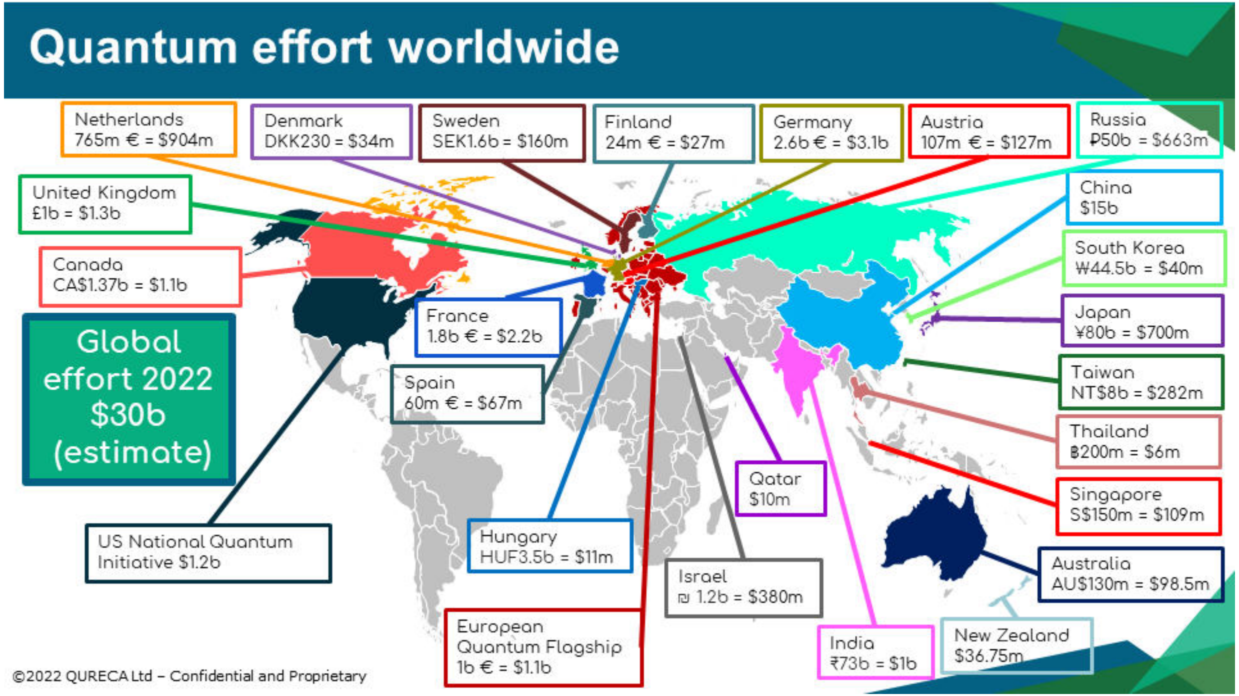
"A different approach"

Pasqualle Verwoerdt | *Board of Directors*

pasqualle.verwoerdt@compumatica.com

06 1268 2780

Quantum Computer (public) Investments



Quantum effort worldwide

Netherlands
765m € = $904m

Denmark
DKK230 = $34m

Sweden
SEK1.6b = $160m

Finland
24m € = $27m

Germany
2.6b € = $3.1b

Austria
107m € = $127m

Russia
₽50b = $663m

United Kingdom
£1b = $1.3b

China
$15b

Canada
CA$1.37b = $1.1b

South Korea
₩44.5b = $40m

Japan
¥80b = $700m

France
1.8b € = $2.2b

Global effort 2022 $30b (estimate)

Spain
60m € = $67m

Taiwan
NT$8b = $282m

Thailand
฿200m = $6m

Qatar
$10m

Singapore
S$150m = $109m

US National Quantum Initiative $1.2b

Hungary
HUF3.5b = $11m

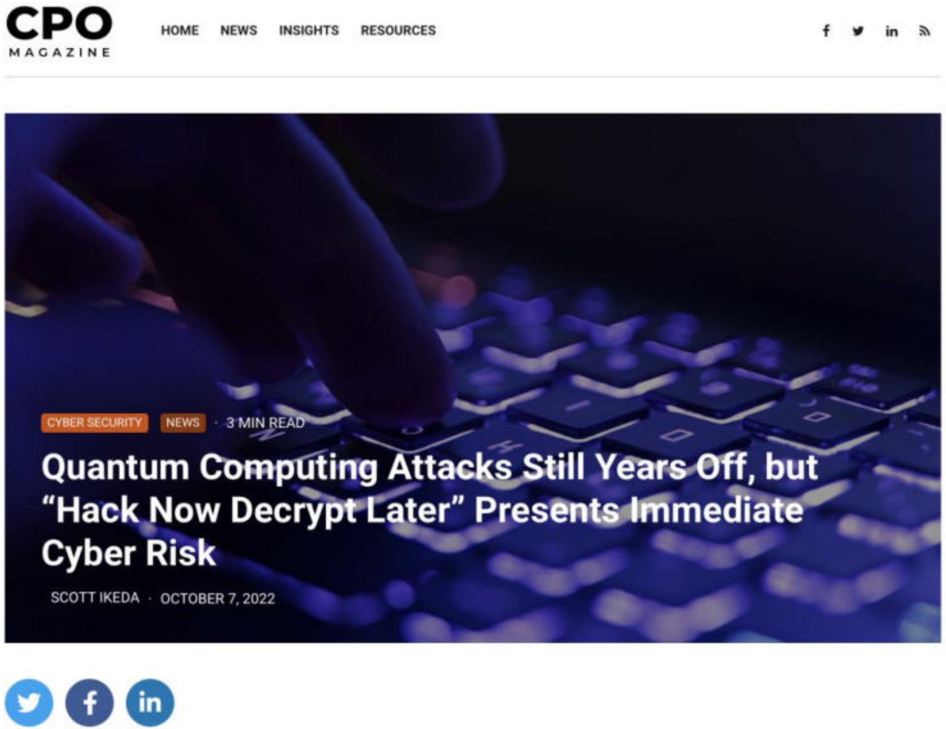
Australia
AU$130m = $98.5m

Israel
₪ 1.2b = $380m

European Quantum Flagship
1b € = $1.1b

India
₹73b = $1b

New Zealand
$36.75m

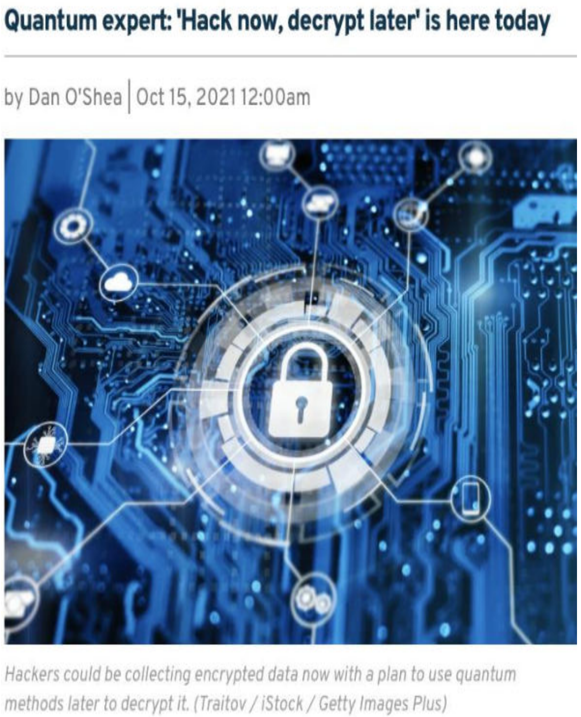


CPO MAGAZINE

CYBER SECURITY · NEWS · 3 MIN READ

Quantum Computing Attacks Still Years Off, but "Hack Now Decrypt Later" Presents Immediate Cyber Risk

SCOTT IKEDA · OCTOBER 7, 2022

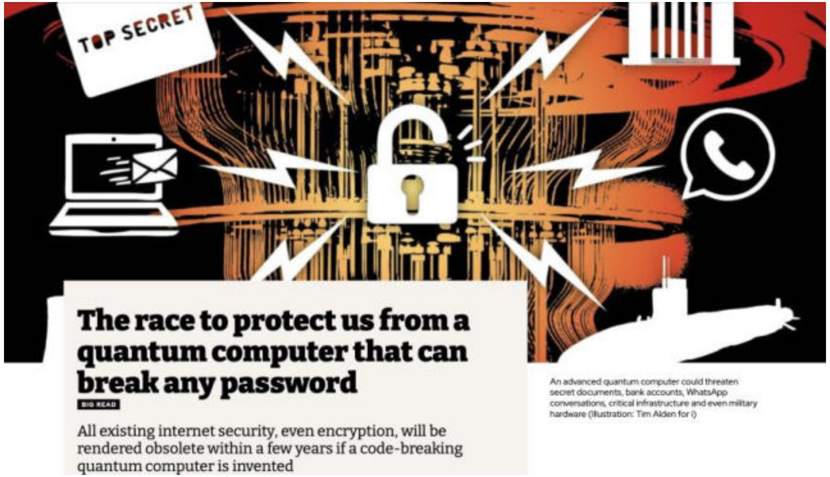


Quantum expert: 'Hack now, decrypt later' is here today

by Dan O'Shea | Oct 15, 2021 12:00am

Hackers could be collecting encrypted data now with a plan to use quantum methods later to decrypt it. (Traitov / iStock / Getty Images Plus)

Quantum security Threats (now)



The race to protect us from a quantum computer that can break any password

BIG READ

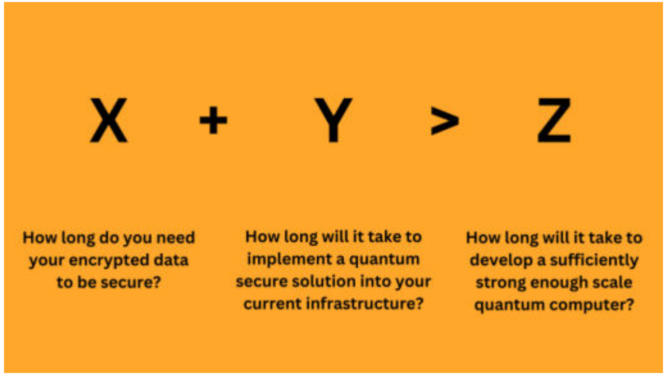
All existing internet security, even encryption, will be rendered obsolete within a few years if a code-breaking quantum computer is invented

An advanced quantum computer could threaten secret documents, bank accounts, WhatsApp conversations, critical infrastructure and even military hardware (Illustration: Tim Alden for i)

Quantum security Threats (future)

Do you need to act Now?

Mosca’s Theorem

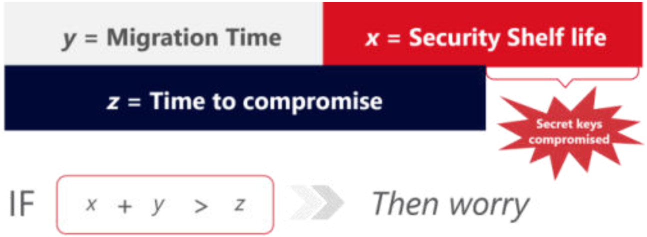


X + Y > Z

How long do you need your encrypted data to be secure?

How long will it take to implement a quantum secure solution into your current infrastructure?

How long will it take to develop a sufficiently strong enough scale quantum computer?



y = Migration Time

x = Security Shelf life

z = Time to compromise

Secret keys compromised

IF $x + y > z$ *Then worry*

What is Quantum resilience?

“The idea of quantum resilience is that regardless of whatever happens, even with a quantum computing attack, your communications remain secure”

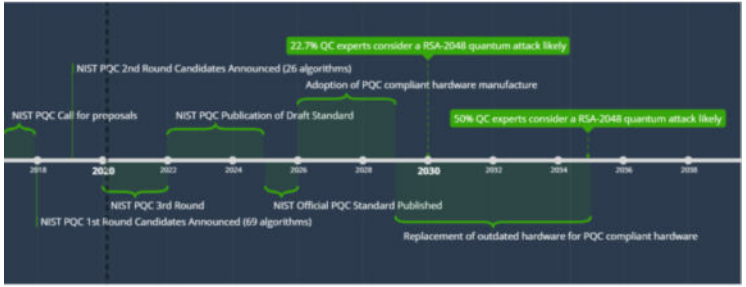
How to prepare for Quantum resilience

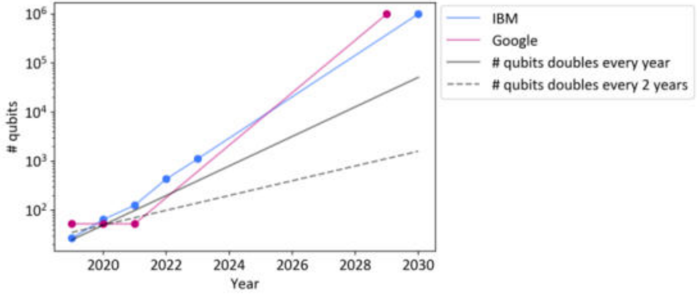
1. Assess based on **Riskmanagement and apply Mosca’s Theorem**

2. Make sure you implement a **hybrid quantum security strategy** (classical algorithms in combination with post quantum proof algorithms (both asymmetric) and asymmetric in combination with symmetric encryption)

3. Make sure your hybrid quantum security strategy is **Crypto agile**

1. Assess based on **Riskmanagement and apply Mosca’s Theorem**

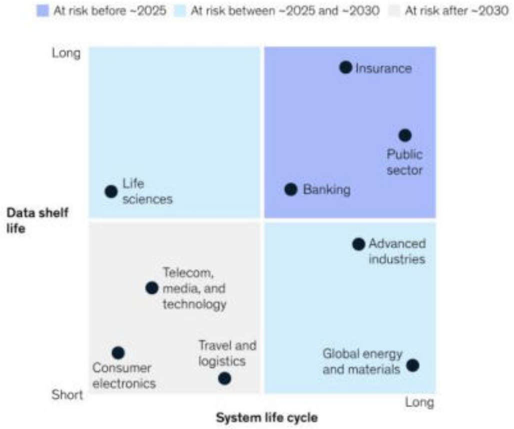

22.7% QC experts consider a RSA-2048 quantum attack likely
NIST PQC 2nd Round Candidates Announced (26 algorithms)
Adoption of PQC compliant hardware manufacture
NIST PQC Call for proposals
NIST PQC Publication of Draft Standard
50% QC experts consider a RSA-2048 quantum attack likely
2018
2020
2022
2024
2026
2028
2030
2032
2034
2036
2038
NIST PQC 3rd Round
NIST Official PQC Standard Published
NIST PQC 1st Round Candidates Announced (69 algorithms)
Replacement of outdated hardware for PQC compliant hardware



X

Industries should prepare for post-quantum cryptography based on data shelf life and system lifetime.

Risk of quantum-powered attack by industry

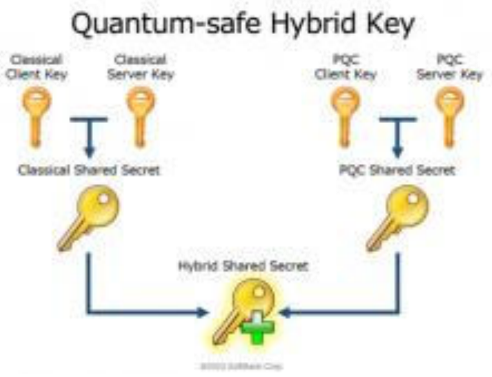


McKinsey & Company

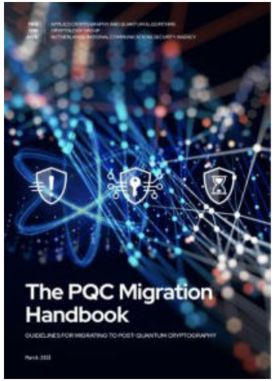
2. Make sure you implement a **hybrid quantum security strategy**

2a. **Classical algorithms** in combination with **post quantum algorithms** (both asymmetric)

2b. **Asymmetric encryption** in combination with **symmetric encryption**



©2023 SoftBank Corp.

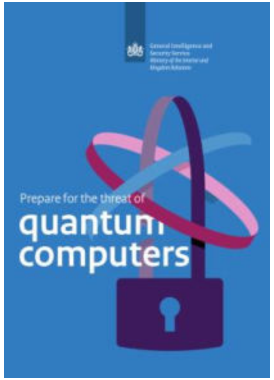


TNO CWI AIVD
APPLIED CRYPTOGRAPHY AND QUANTUM ALGORITHMS
CRYPTOLOGY GROUP
NETHERLANDS NATIONAL COMMUNICATIONS SECURITY AGENCY

The PQC Migration Handbook

GUIDELINES FOR MIGRATING TO POST-QUANTUM CRYPTOGRAPHY

March 2023



General Intelligence and Security Service
Ministry of the Interior and Kingdom Relations

Prepare for the threat of quantum computers

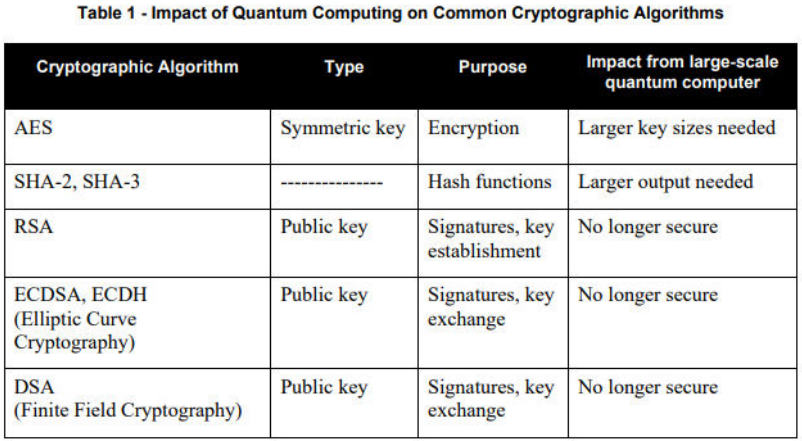


Table 1 - Impact of Quantum Computing on Common Cryptographic Algorithms

Cryptographic Algorithm	Type	Purpose	Impact from large-scale quantum computer
AES	Symmetric key	Encryption	Larger key sizes needed
SHA-2, SHA-3	---------------	Hash functions	Larger output needed
RSA	Public key	Signatures, key establishment	No longer secure
ECDSA, ECDH (Elliptic Curve Cryptography)	Public key	Signatures, key exchange	No longer secure
DSA (Finite Field Cryptography)	Public key	Signatures, key exchange	No longer secure

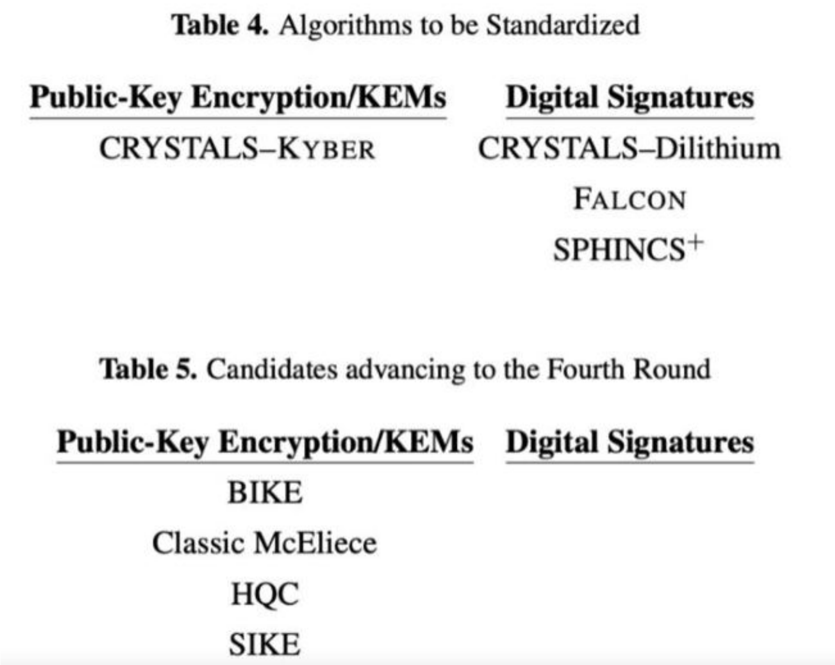
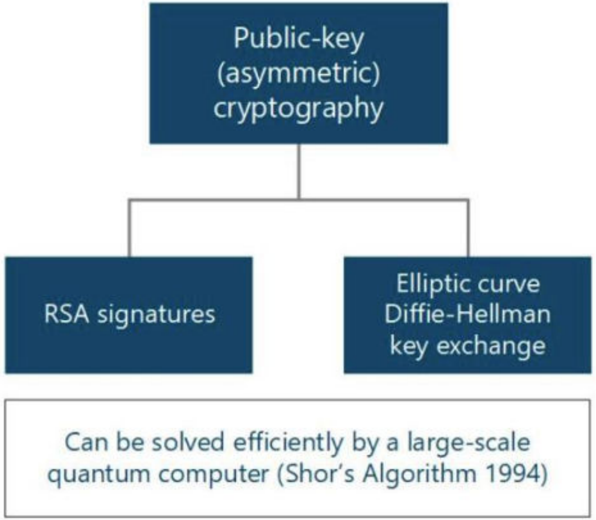


Table 4. Algorithms to be Standardized

Public-Key Encryption/KEMs	Digital Signatures
CRYSTALS–KYBER	CRYSTALS–Dilithium
	FALCON
	SPHINCS$^+$

Table 5. Candidates advancing to the Fourth Round

Public-Key Encryption/KEMs	Digital Signatures
BIKE	
Classic McEliece	
HQC	
SIKE	



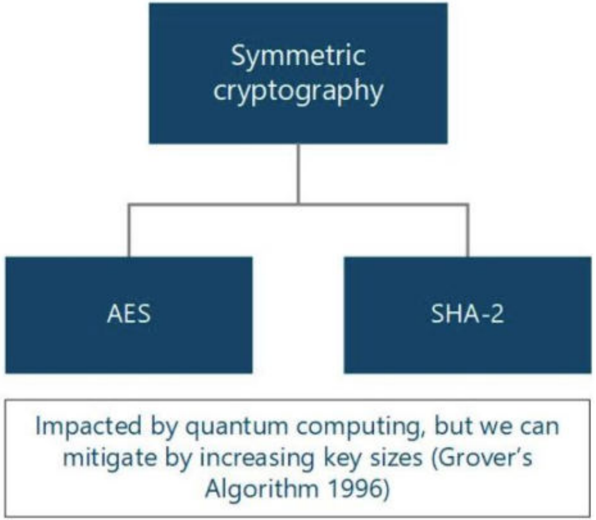
Public-key (asymmetric) cryptography

RSA signatures

Elliptic curve Diffie-Hellman key exchange

Can be solved efficiently by a large-scale quantum computer (Shor's Algorithm 1994)

“The significant impact is on asymmetric encryption. Using Shor’s algorithm, quantum computing breaks all public-key cryptography. ***Public-key solutions like RSA, Diffie-Hellman, and ECC will all need replacements. Among other things, this has a severe effect on key exchanges for TLS”***



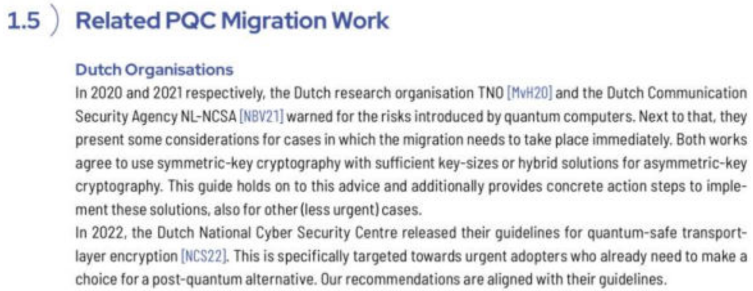
Symmetric cryptography

AES

SHA-2

Impacted by quantum computing, but we can mitigate by increasing key sizes (Grover's Algorithm 1996)

“While Grover’s algorithm can reduce the time necessary to guess symmetric keys, widely accepted solutions with sufficient key size are believed to be quantum-resistant. Lane Wagner, writingOpens a new window for Qvault, reports that Grover’s algorithm can effectively reduce the attack time against AES-128 to achieve reasonably successful key guessing once quantum computers reach the necessary power levels. ***However, the AES-256 keyspace is sufficiently large to remain resistant to quantum-enabled attacks.”***

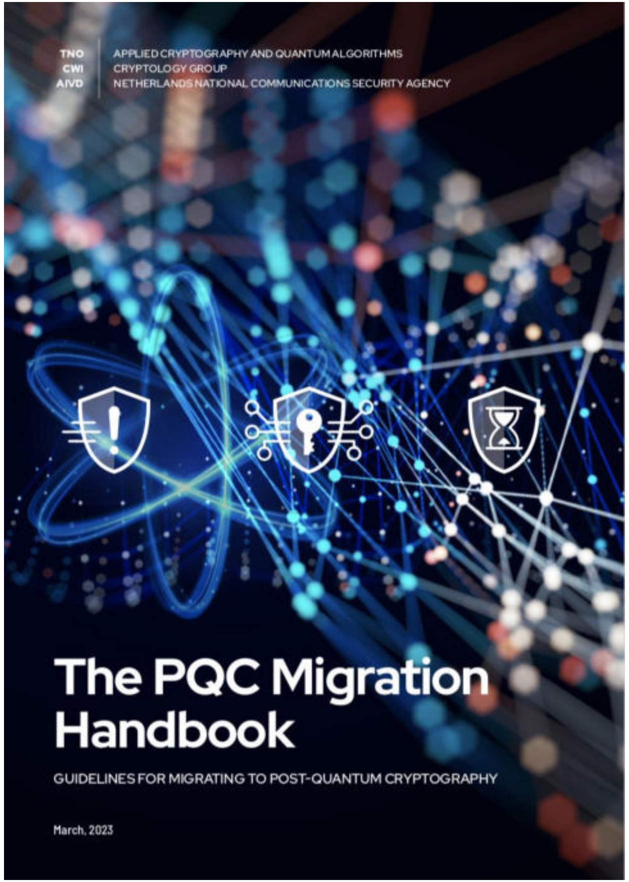


1.5) Related PQC Migration Work

Dutch Organisations

In 2020 and 2021 respectively, the Dutch research organisation TNO [MvH20] and the Dutch Communication Security Agency NL-NCSA [NBV21] warned for the risks introduced by quantum computers. Next to that, they present some considerations for cases in which the migration needs to take place immediately. Both works agree to use symmetric-key cryptography with sufficient key-sizes or hybrid solutions for asymmetric-key cryptography. This guide holds on to this advice and additionally provides concrete action steps to implement these solutions, also for other (less urgent) cases.

In 2022, the Dutch National Cyber Security Centre released their guidelines for quantum-safe transport-layer encryption [NCS22]. This is specifically targeted towards urgent adopters who already need to make a choice for a post-quantum alternative. Our recommendations are aligned with their guidelines.



TNO APPLIED CRYPTOGRAPHY AND QUANTUM ALGORITHMS
CWI CRYPTOLOGY GROUP
AIVD NETHERLANDS NATIONAL COMMUNICATIONS SECURITY AGENCY

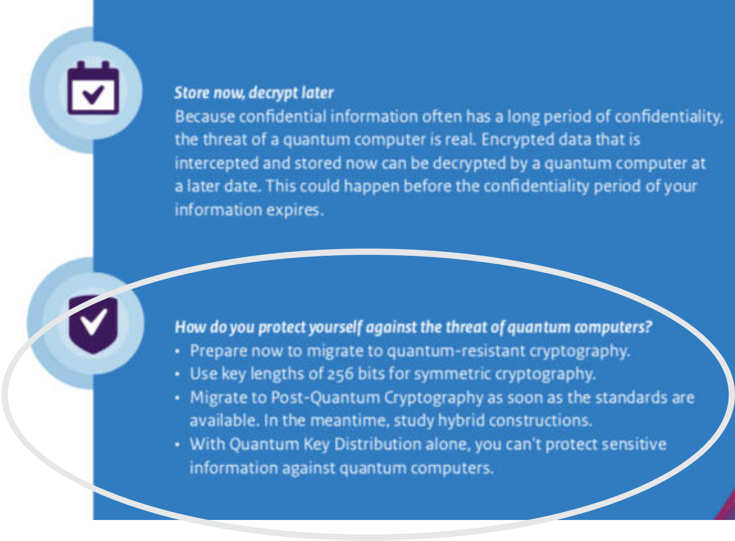
The PQC Migration Handbook

GUIDELINES FOR MIGRATING TO POST-QUANTUM CRYPTOGRAPHY

March, 2023

Prepare for the threat of

quantum computers

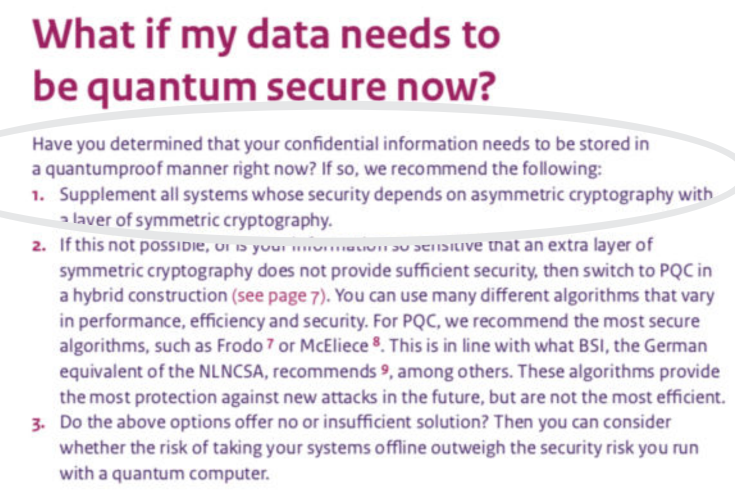


Store now, decrypt later

Because confidential information often has a long period of confidentiality, the threat of a quantum computer is real. Encrypted data that is intercepted and stored now can be decrypted by a quantum computer at a later date. This could happen before the confidentiality period of your information expires.

How do you protect yourself against the threat of quantum computers?

- Prepare now to migrate to quantum-resistant cryptography.
- Use key lengths of 256 bits for symmetric cryptography.
- Migrate to Post-Quantum Cryptography as soon as the standards are available. In the meantime, study hybrid constructions.
- With Quantum Key Distribution alone, you can't protect sensitive information against quantum computers.



What if my data needs to be quantum secure now?

Have you determined that your confidential information needs to be stored in a quantumproof manner right now? If so, we recommend the following:

1. Supplement all systems whose security depends on asymmetric cryptography with a layer of symmetric cryptography.
2. If this not possible, or is your information so sensitive that an extra layer of symmetric cryptography does not provide sufficient security, then switch to PQC in a hybrid construction (see page 7). You can use many different algorithms that vary in performance, efficiency and security. For PQC, we recommend the most secure algorithms, such as Frodo [7] or McEliece [8]. This is in line with what BSI, the German equivalent of the NLNCSA, recommends [9], among others. These algorithms provide the most protection against new attacks in the future, but are not the most efficient.
3. Do the above options offer no or insufficient solution? Then you can consider whether the risk of taking your systems offline outweigh the security risk you run with a quantum computer.

3. Make sure your hybrid quantum security strategy is **Crypto agile**

“Cryptoagility is a practice in designing the information systems which encourages support of new crypto primitives and crypto algorithms without making significant changes to system infrastructure. A plan is considered to be cryptoagile if the existing cryptographic algorithms and other parameters can be changed with ease without leaving gaps in implementation”

Conclusion

(Classical asymmetric encryption + Post quantum asymmetric encryption)
+ Post quantum symmetric encryption
=
Crypto agile quantum security strategy

Questions?

Pasqualle Verwoerdt | *Board of Directors*

pasqualle.verwoerdt@compumatica.com

06 1268 2780

Post-Quantum

Cryptography Conference

Quantum Resistance through Symmetric Key Cryptography

Pasqualle Verwoerdt

Board of Directors at Compumatica