Quantum Threat – Impact on Certification Authorities

APKIC Symposium
Bangaluru, 28 November 2023

Tomorrow's Cyber Security, Today
IRONCAP

Agenda

Quantum Computer and the Quantum Threat

NIST PQC Update

PQC Use Cases

Impact on Certification Authorities

Summary

01 Communique

(TSX-V: ONE)

One Qubit	Two Qubits	Three Qubits
1	1 0	1 0 1

- Based on Super-positioning and Entanglement
- On and Off states can co-exist
- Processing power equivalent to having millions of traditional computers working in parallel

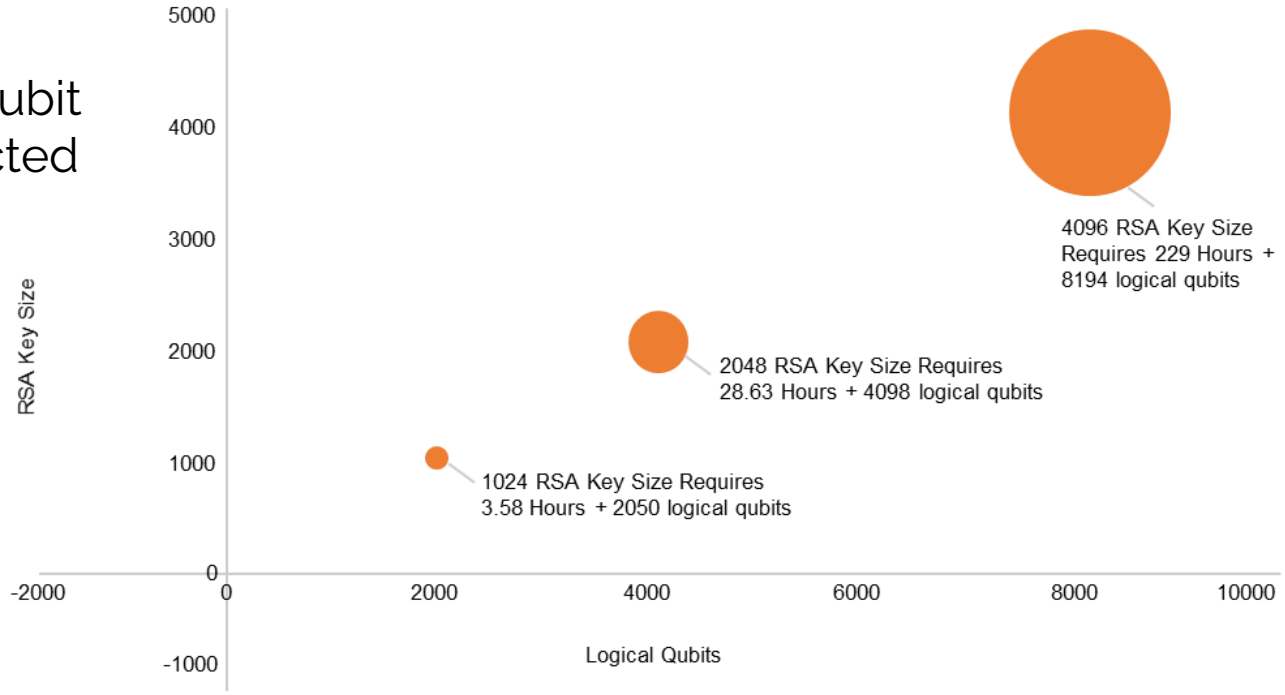
- ➢ Performs computation in a way fundamentally different from classical computing
- ➢ Uses quantum “superposition” and “entanglement” effects
- ➢ Unique properties of a quantum computer makes it more powerful than a classical computer; with the information stored in superposition, some problems can be solved exponentially faster compared to a classical computer

The **Shor's algorithm** could be used by quantum computers to break those encryption which is based upon Integer Factorisation; e.g. RSA.

Such disruption is believed to happen when quantum power reached around 1,000 logical qubit (i.e. approx. 1 million qubit with fully error-corrected capability).

"Q-Day is not coming, it has arrived! It is just a matter of time before someone finds a way to make this consumer grade. Right now it is still at professional grade. But the problem is the professionals are in the business of criminal activity especially when it pertains to the cyber."

Ajay Sood, Country Manager (Canada), Rapid7



Source:
Quantum Computing: Progress and Prospects (2019) Emily Grumbling and Mark Horowitz
https://nap.nationalacademies.org/catalog/25196/quantum-computing-progress-and-prospects

Mosca's Theoerm

If X + Y > Z then ***Checkmate!***

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?

HNDL Attack

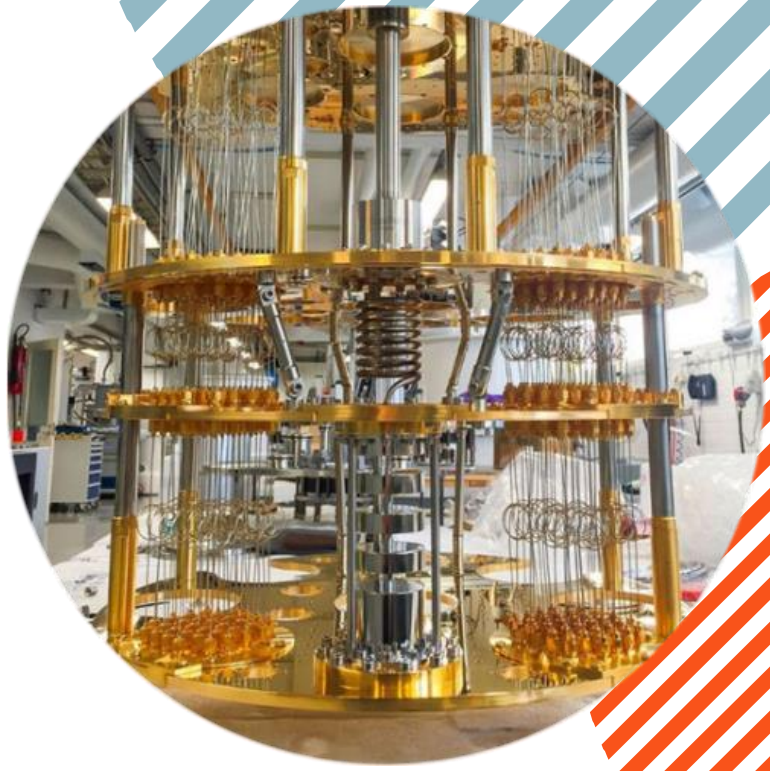
(Harvest Now, Decrypt Later)

Reference:
Professor Michele Mosca, co-founder of the Institute for Quantum Computing, University of Waterloo
https://csrc.nist.gov/csrc/media/events/workshop-on-cybersecurity-in-a-post-quantum-world/documents/presentations/session8-mosca-michele.pdf

Q-Day has Arrived!

2019 – 27 Qubits
2022 – Osprey with 433 Qubits
2023 – Condor with 1121 Qubits
2024 – Flamingo with 1386 Qubits
2025 – Kookaburra with 4158+ Qubits
2026 – 100,000+ Qubits

IBM's quantum computers roadmap (May 2022)



Jan 2023: Researchers in China claimed breakthrough in quantum computing, outlining an approach to break the RSA public-key encryption system using a quantum computer of 372 qubits

https://therecord.media/chinese-researchers-claim-to-have-broken-rsa-with-a-quantum-computer-experts-arent-so-sure/

Agenda

Quantum Computer and the Quantum Threat

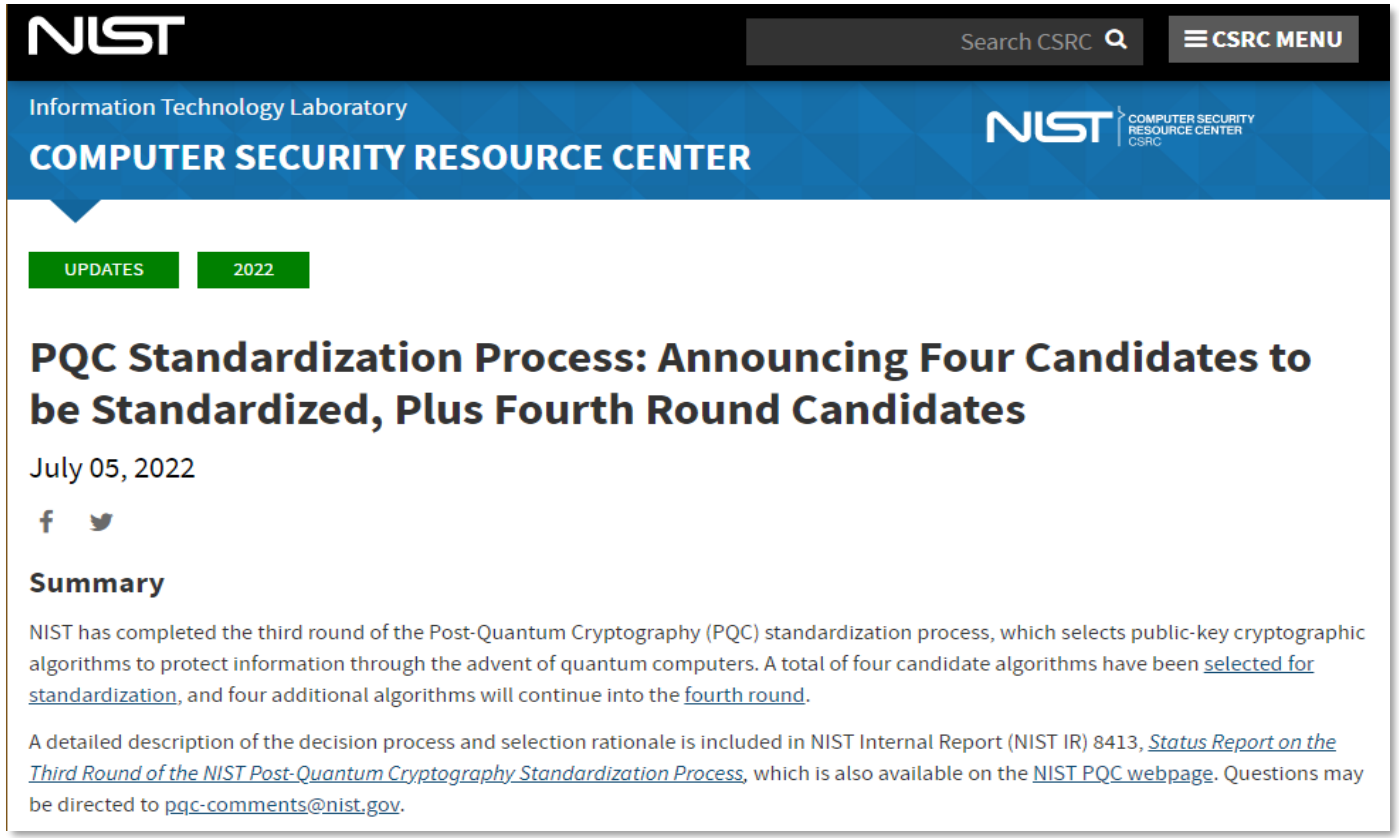
NIST PQC Update

PQC Use Cases

Impact on Certification Authorities

Summary

NIST PQC Initiative



NIST Search CSRC CSRC MENU

Information Technology Laboratory

COMPUTER SECURITY RESOURCE CENTER

NIST COMPUTER SECURITY RESOURCE CENTER CSRC

UPDATES 2022

PQC Standardization Process: Announcing Four Candidates to be Standardized, Plus Fourth Round Candidates

July 05, 2022

Summary

NIST has completed the third round of the Post-Quantum Cryptography (PQC) standardization process, which selects public-key cryptographic algorithms to protect information through the advent of quantum computers. A total of four candidate algorithms have been selected for standardization, and four additional algorithms will continue into the fourth round.

A detailed description of the decision process and selection rationale is included in NIST Internal Report (NIST IR) 8413, *Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process*, which is also available on the NIST PQC webpage. Questions may be directed to pqc-comments@nist.gov.

Third Round Candidates to be Standardized

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

Fourth Round Candidates

Public-Key Encryption/KEMs
BIKE
Classic McEliece
HQC
SIKE

Source: https://csrc.nist.gov/News/2022/pqc-candidates-to-be-standardized-and-round-4

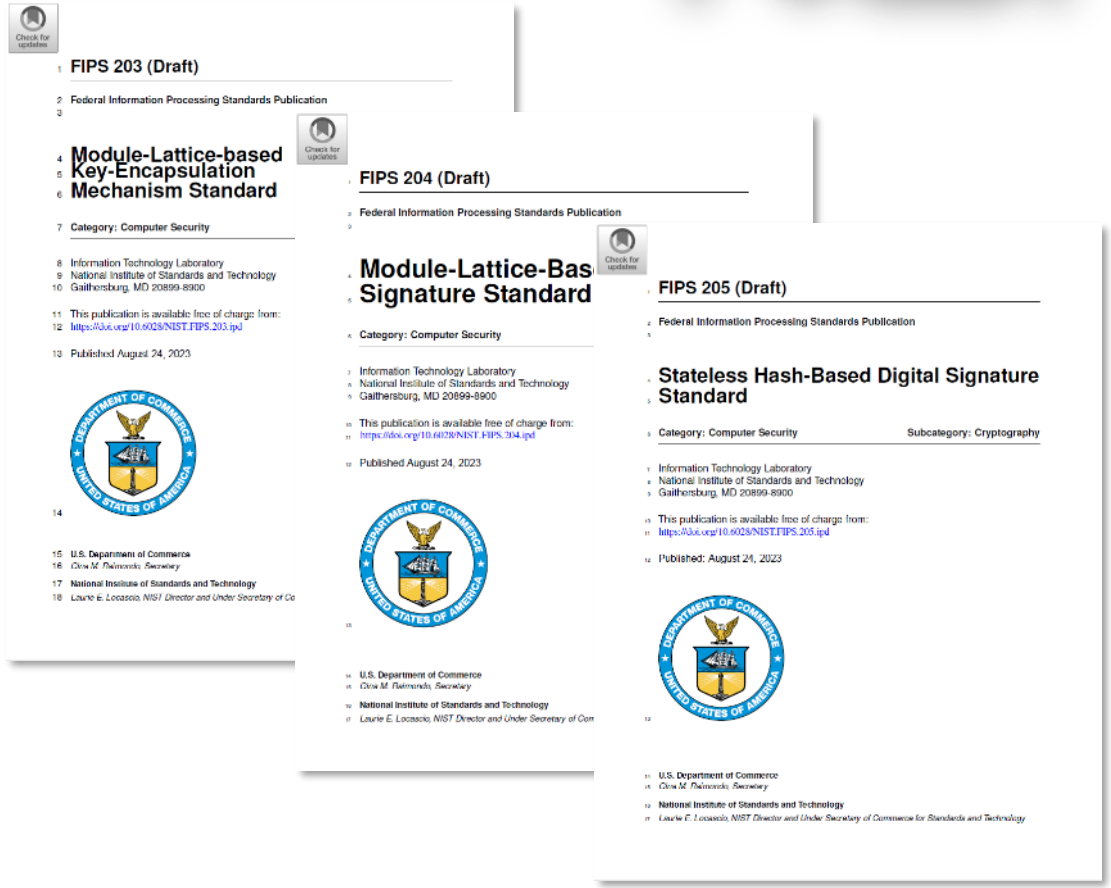
Draft Standards Published

NIST Standards – August 24, 2023

- ❑ Published FIPS 203, FIPS 204, and FIPS 205

Third Round Candidates to be Standardized

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



Coming Soon…

- ❑ Draft standard for Falcon

Source: https://csrc.nist.gov/News/2023/three-draft-fips-for-post-quantum-cryptography

Agenda

Quantum Computer and the Quantum Threat

NIST PQC Update

PQC Use Cases

Impact on Certification Authorities

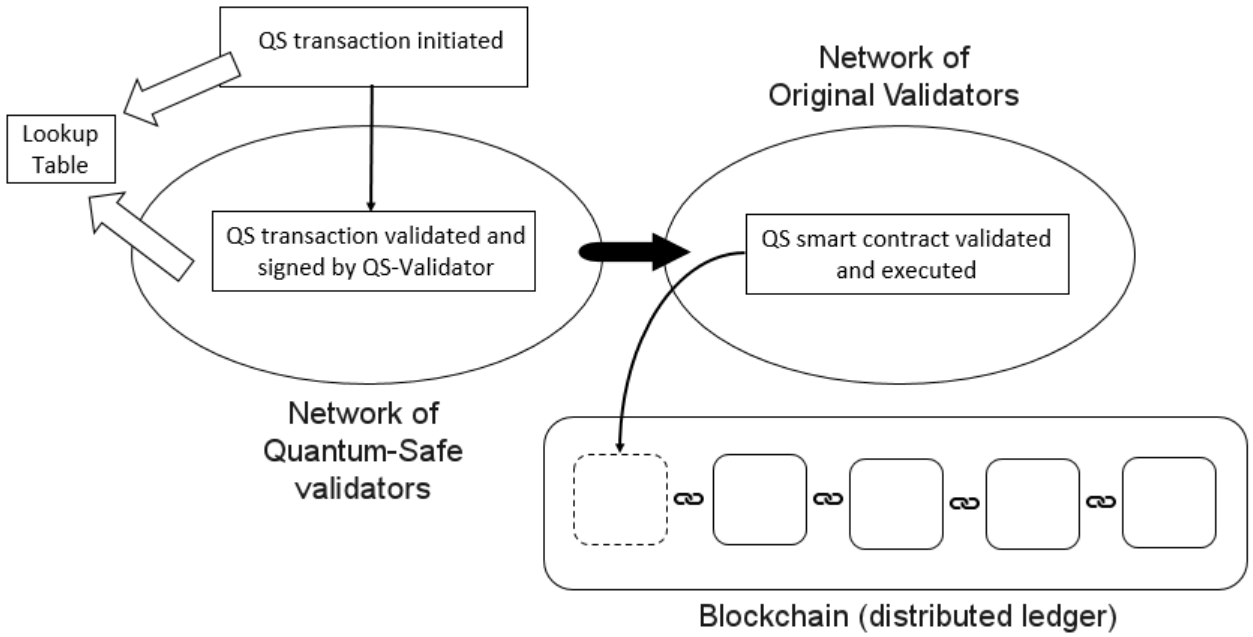
Summary

Quantum-Safe HSM

THALES
Building a future we can all trust

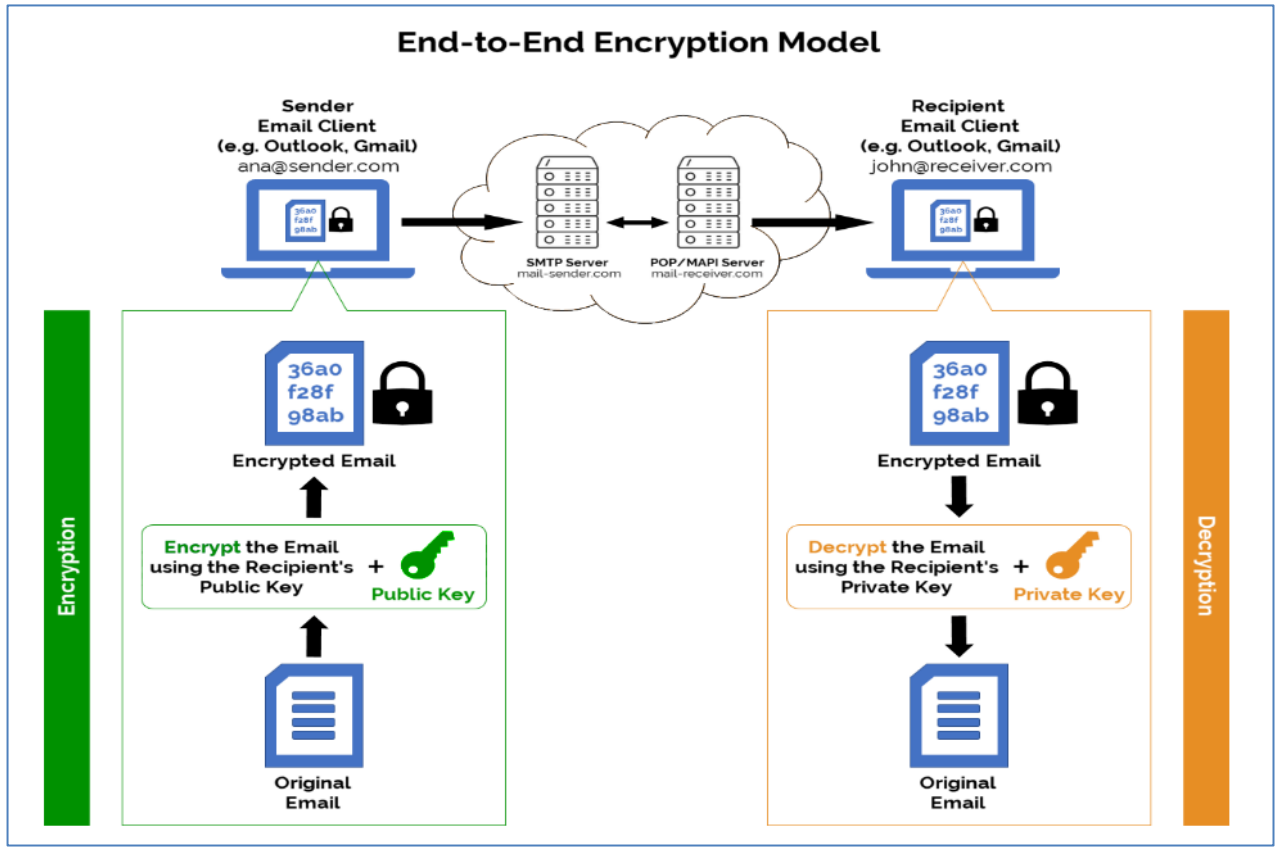
Quantum-Safe Blockchain

US Patent: #11,698,833



IRONCAP

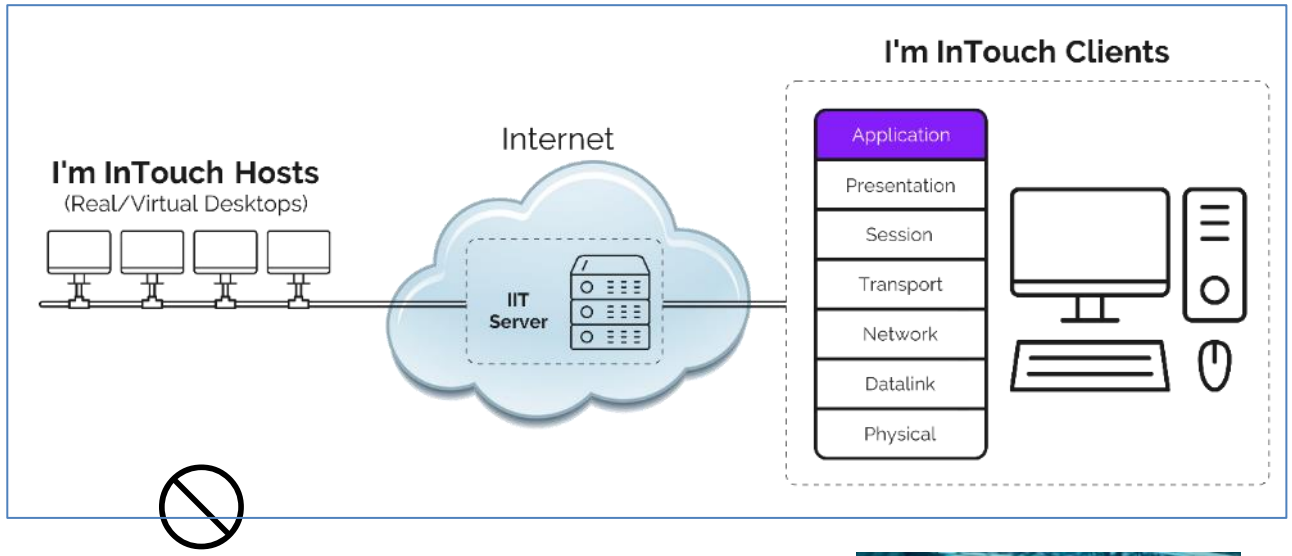
Email Security



IRONCAP

Remote Access

Quantum-Safe + Zero Trust



No access to corporate LAN

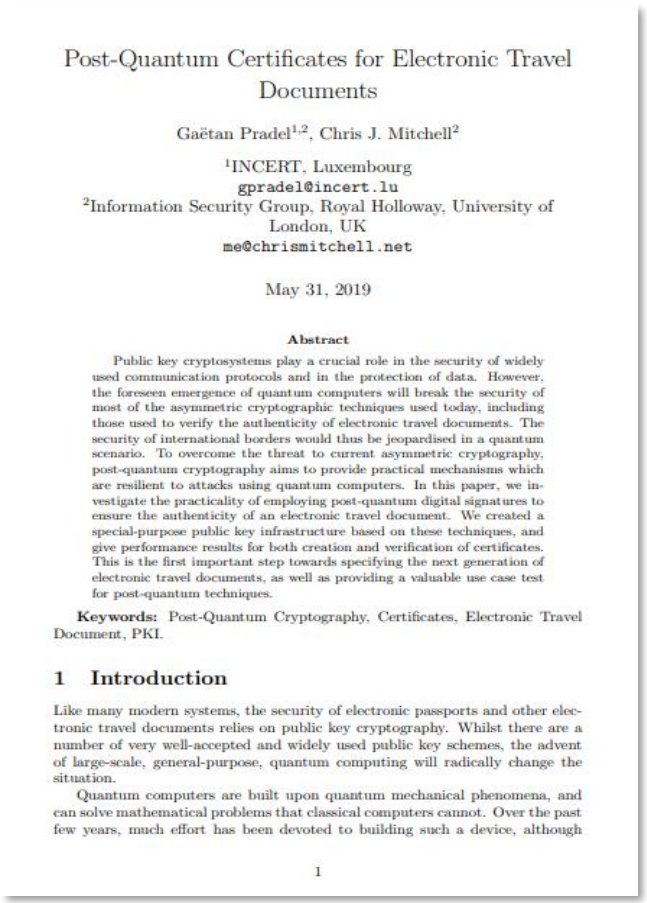
IRONCAP

Steganography

- Watermark steganography – **18th Century**
- Quantum-safe Steganography – **21st Century**
- IronCAP Goppa-code error vectors – **proven**
- International Patent Application – **filed**
- Applications: e-wallets recovery, NFTs, etc.

Industry Q-Day Preparations

"Looking ahead, each passing year brings the payments industry closer to a truly post-quantum world… EMVCo continues to explore and evaluate potential risks …



Post-Quantum Certificates for Electronic Travel Documents

Gaëtan Pradel[1,2], Chris J. Mitchell[2]

[1]INCERT, Luxembourg
gpradel@incert.lu
[2]Information Security Group, Royal Holloway, University of London, UK
me@chrismitchell.net

May 31, 2019

Abstract

Public key cryptosystems play a crucial role in the security of widely used communication protocols and in the protection of data. However, the foreseen emergence of quantum computers will break the security of most of the asymmetric cryptographic techniques used today, including those used to verify the authenticity of electronic travel documents. The security of international borders would thus be jeopardised in a quantum scenario. To overcome the threat to current asymmetric cryptography, post-quantum cryptography aims to provide practical mechanisms which are resilient to attacks using quantum computers. In this paper, we investigate the practicality of employing post-quantum digital signatures to ensure the authenticity of an electronic travel document. We created a special-purpose public key infrastructure based on these techniques, and give performance results for both creation and verification of certificates. This is the first important step towards specifying the next generation of electronic travel documents, as well as providing a valuable use case test for post-quantum techniques.

Keywords: Post-Quantum Cryptography, Certificates, Electronic Travel Document, PKI.

1 Introduction

Like many modern systems, the security of electronic passports and other electronic travel documents relies on public key cryptography. Whilst there are a number of very well-accepted and widely used public key schemes, the advent of large-scale, general-purpose, quantum computing will radically change the situation.

Quantum computers are built upon quantum mechanical phenomena, and can solve mathematical problems that classical computers cannot. Over the past few years, much effort has been devoted to building such a device, although

1

Source:
EMV Co 2023 Priorities
HHS Quantum Cryptography and the Health Sector
Bank of International Settlement Project Leap
ICAO - Study on Post-Quantum Certificates for Electronic Travel Documents

Agenda

Quantum Computer and the Quantum Threat

NIST PQC Update

PQC Use Cases

Impact on Certification Authorities

Summary

Who will be Impacted?

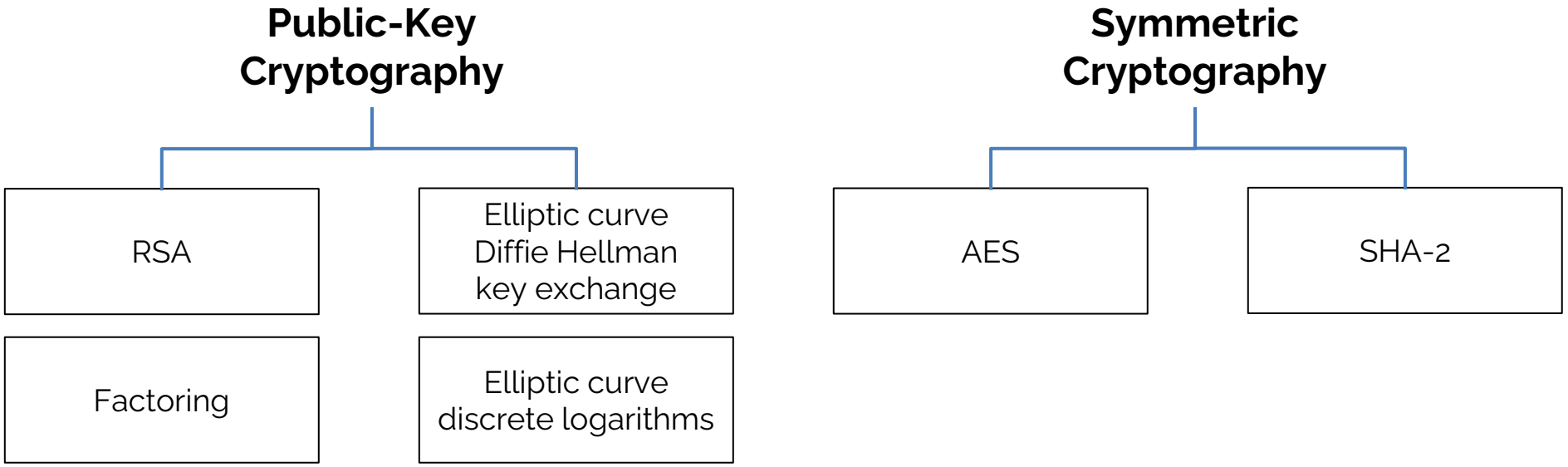
Financial World

- ❑ Financial transactions; Payment systems
- ❑ Cryptocurrencies, CBDC, etc.
- ❑ Smart card infrastructure

World of Internet

- ❑ **PKI**
- ❑ AI Privacy
- ❑ Email security
- ❑ IoT
- ❑ Website authenticity

Impact on today's cryptographic systems



Can be solved efficiently by a large scale quantum computer so need to seek replacement

(Shor's Algorithm 1994)

Impacted by quantum computing but can be mitigated by increasing (at least doubling) key sizes

(Grover's Algorithm 1996)

Practical Implications of PQC Upgrade

NIST PQC Encryption Algorithms -- Public Key & Ciphertext Sizes

Encryption Algorithm	Public Key (bytes)	Ciphertext (bytes)
RSA-2048	256	256
NIST Round 3 Selection		
CRYSTALS-Kyber	800	768
NIST Round 4 Candidates		
Classic McEliece	261,120	128
BIKE	12,323	12,579
HQC	2,249	4,481
~~SIKE (compressed)~~	~~300 (197)~~	~~346 (236)~~

Reference:
https://cryptobook.nakov.com/digital-signatures/rsa-signatures
https://pq-crystals.org/kyber/data/kyber-specification-round3-20210131.pdf
https://bikesuite.org/files/v5.0/BIKE_Spec.2022.10.04.1.pdf
https://pqc-hqc.org/doc/hqc-specification_2023-04-30.pdf
https://csrc.nist.gov/CSRC/media/Presentations/classic-mceliece-round-2-presentation/images-media/classic-mceliece-persichetti.pdf
https://csrc.nist.gov/CSRC/media/Presentations/sike-round-3-presentation/images-media/session-6-sike-de-feo.pdf

Practical Implications of PQC Upgrade

NIST PQC Encryption Algorithms -- Public Key & Signature Sizes

Encryption Algorithm	Public Key (bytes)	Signature (bytes)
RSA-2048	256	256
ECC-P256	32	64
NIST Round 3 Selections		
CRYSTALS-Dilithium	1,312	2,420
Falcon	897	666
Sphincs+	32	7,856

Reference:
https://openquantumsafe.org/liboqs/algorithms/sig/dilithium
https://openquantumsafe.org/liboqs/algorithms/sig/falcon
https://openquantumsafe.org/liboqs/algorithms/sig/sphincs.html

Key Implications for Public Key Infrastructures

- **Uncertain timeline vs. imminent threat**
- **Time needed for transition**
- **Achieving cryptographic agility**
- **Jurisdiction laws and regulations**
- **Interoperability**

"Regardless of unpredictable timelines, organizations should think about their transition to quantum-safe cryptography now, as the process will take time."

WEF Transitioning to a Quantum-Secure Economy, September 2022

"… all secret and private keys that are protected using the current public-key algorithms—and all available information protected under those keys—will be subject to exposure. We need to determine where, why, and with what priority vulnerable public-key algorithms will need to be replaced, and we need to understand the constraints that apply to specific use cases. These initial steps in developing and implementing algorithm migration playbooks can and should begin immediately."

NIST, Getting Ready for Post-Quantum Cryptography, April 2021

Agenda

Quantum Computer and the Quantum Threat

NIST PQC Update

PQC Use Cases

Impact on Certification Authorities

Summary

Tomorrow's Cyber Security, Today
IRONCAP

Summary

- ❑ Q-Day has arrived + transitional challenge = no time to wait
- ❑ Everything needs to be quantum-safe (e.g. financial transactions, health care, IoT, general cybersecurity, email, remote access, etc.)
- ❑ Some pioneer Post-quantum end-user products can be found in the market already (e.g. email security, blockchain, remote access, etc.)
- ❑ Opportunities for new services where robust security is needed

01 COMMUNIQUE

Andrew Cheung

Founder, President and CEO of
01 Communique Laboratory Inc.

email: andrew.cheung@01com.com

William Gee

Senior Advisor, Policy and
Government Liaison

email: william.gee@ironcap.ca

Tomorrow's Cyber Security, Today

IRONCAP

www.ironcap.ca | www.01com.com
+1 905-795-2888 (tel)
+1 800-668-2185 (toll-free)
Sales@ironcap.ca

(TSX-V: ONE | OTCQB: OONEF)