IronCAP™ Post-Quantum Cybersecurity

Spring - 2025

Tomorrow's Cyber Security, Today

IRONCAP

Q-Day Attention Heated UP!

Google
Willow achieved a major breakthrough in Dec 2024

Microsoft
Stated that 2025 is the year to move on your quantum strategy

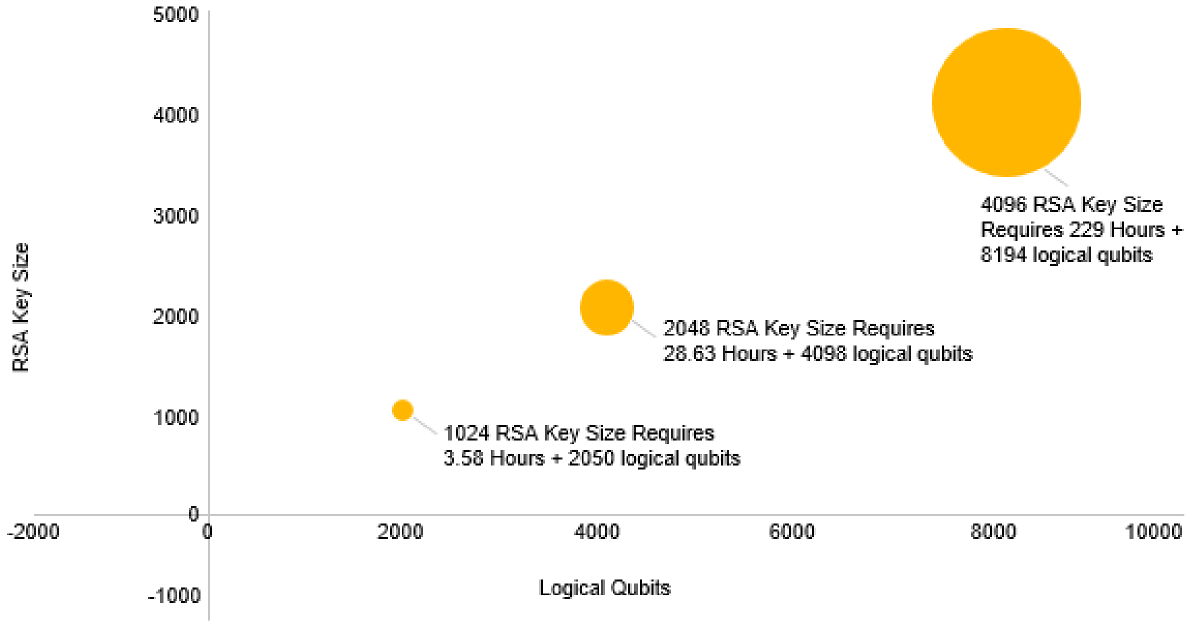
IBM Roadmap
Predicts Kookaburra with 4158 Qubits in 2025

Gartner Research
2025 is the year to get started on quantum strategy

SandBox AQ
Urging companies to transition immediately to PQC-compliant protocol

Q-Day has Arrived!

Figure 2 – RSA Key Size vs Qubits requirement in breaking



Source: Quantum Computing: Progress & Prospects (2019) Emily Grumbling and Mark Horowitz

HNDL Attack

(Harvest Now, Decrypt Later)

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?

Q-Day Preparation - NIST

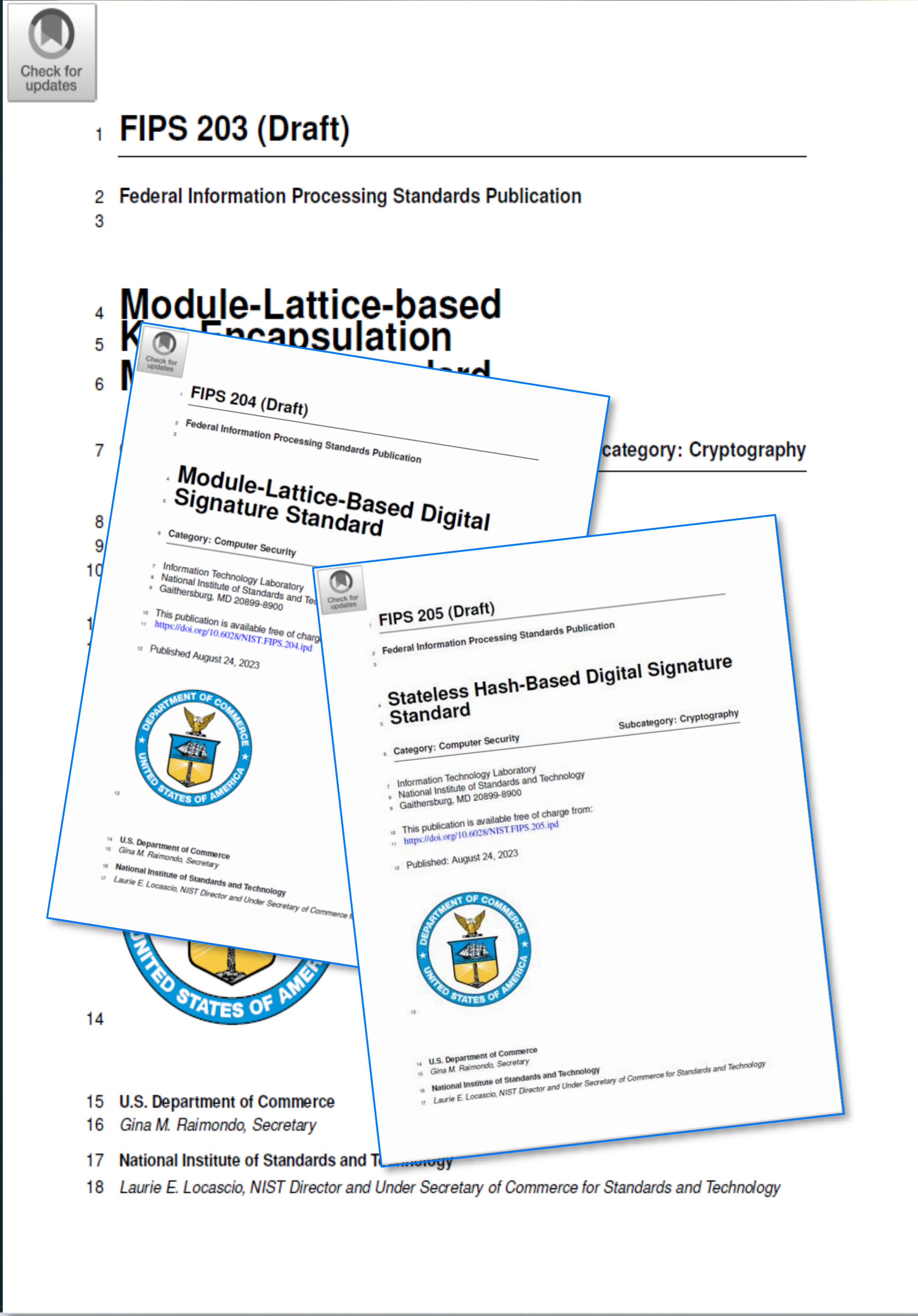
NIST 4th Round PQC – March 2025

❑ HQC selected

* Already offered by IronCAP engine since 2022 (expected to be part of ISO)

** To be included into next version of IronCAP

Algorithm	Algorithm Class
Classic McEliece*	Code-based
HQC (selected)**	Code-based
BIKE (out)	Code-based



Check for updates

FIPS 203 (Draft)

Federal Information Processing Standards Publication

Module-Lattice-based

Encapsulation

category: Cryptography

U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and T

Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology

Check for updates

FIPS 204 (Draft)

Federal Information Processing Standards Publication

Module-Lattice-Based Digital Signature Standard

Category: Computer Security

Information Technology Laboratory
National Institute of Standards and Tec
Gaithersburg, MD 20899-8900

This publication is available free of charg
https://doi.org/10.6028/NIST.FIPS.204.ipd

Published August 24, 2023

U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Under Secretary of Commerce f

Check for updates

FIPS 205 (Draft)

Federal Information Processing Standards Publication

Stateless Hash-Based Digital Signature Standard

Category: Computer Security Subcategory: Cryptography

Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8900

This publication is available free of charge from:
https://doi.org/10.6028/NIST.FIPS.205.ipd

Published: August 24, 2023

U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology

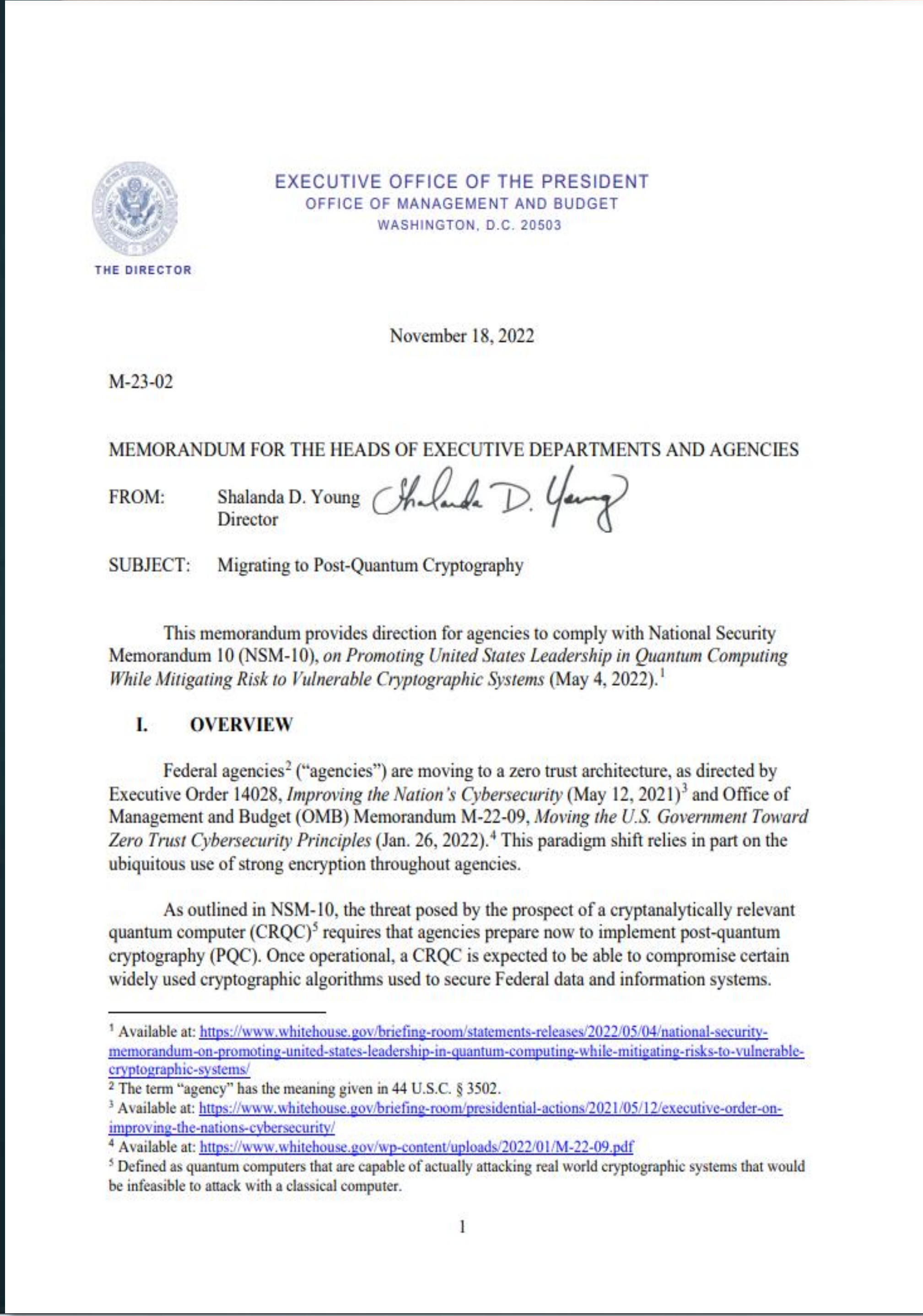
Source: https://csrc.nist.gov/News/2023/three-draft-fips-for-post-quantum-cryptography

Q-Day Preparation – US Gov

Executive Office of the President – November 2022

- ❑ Provided more specific directions for agencies to comply with NSM-10 (submit funding assessment by Oct 18, 2023)
- ❑ Reminded agencies to be mindful that encrypted data can be recorded now and decrypted at a later date by operators of a future CRQC (Cryptanalytically Relevant Quantum Computer)
- ❑ Set out preparatory steps for agencies to undertake as they begin their PQC transition, starting with a prioritised inventory of cryptographic systems
- ❑ Provided additional transitional guidance to agencies in the period before PQC standards are finalised by the NIST

Source: https://www.whitehouse.gov/wp-content/uploads/2022/11/M-23-02-M-Memo-on-Migrating-to-Post-Quantum-Cryptography.pdf



EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

THE DIRECTOR

November 18, 2022

M-23-02

MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Shalanda D. Young Shalanda D. Young
Director

SUBJECT: Migrating to Post-Quantum Cryptography

This memorandum provides direction for agencies to comply with National Security Memorandum 10 (NSM-10), *on Promoting United States Leadership in Quantum Computing While Mitigating Risk to Vulnerable Cryptographic Systems* (May 4, 2022).[1]

I. OVERVIEW

Federal agencies[2] ("agencies") are moving to a zero trust architecture, as directed by Executive Order 14028, *Improving the Nation's Cybersecurity* (May 12, 2021)[3] and Office of Management and Budget (OMB) Memorandum M-22-09, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles* (Jan. 26, 2022).[4] This paradigm shift relies in part on the ubiquitous use of strong encryption throughout agencies.

As outlined in NSM-10, the threat posed by the prospect of a cryptanalytically relevant quantum computer (CRQC)[5] requires that agencies prepare now to implement post-quantum cryptography (PQC). Once operational, a CRQC is expected to be able to compromise certain widely used cryptographic algorithms used to secure Federal data and information systems.

[1] Available at: https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/

[2] The term "agency" has the meaning given in 44 U.S.C. § 3502.

[3] Available at: https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

[4] Available at: https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf

[5] Defined as quantum computers that are capable of actually attacking real world cryptographic systems that would be infeasible to attack with a classical computer.

1

Q-Day Preparation – Apple

Apple's iMessage to be Quantum-Safe – February 2024

Cupertino announced that PQ3—its post-quantum cryptographic protocol — is included in iMessage. The update will launch in iOS and iPad OS 17.4 and macOS 14.4 after previously being deployed in the beta versions of the software. Apple, which published the news on its security research blog, says the change is the "most significant cryptographic security upgrade in iMessage history."

Source: https://www.wired.com/story/apple-pq3-post-quantum-encryption/
Blog: https://security.apple.com/blog/imessage-pq3/

IronCAP Patents

Patent Portfolio

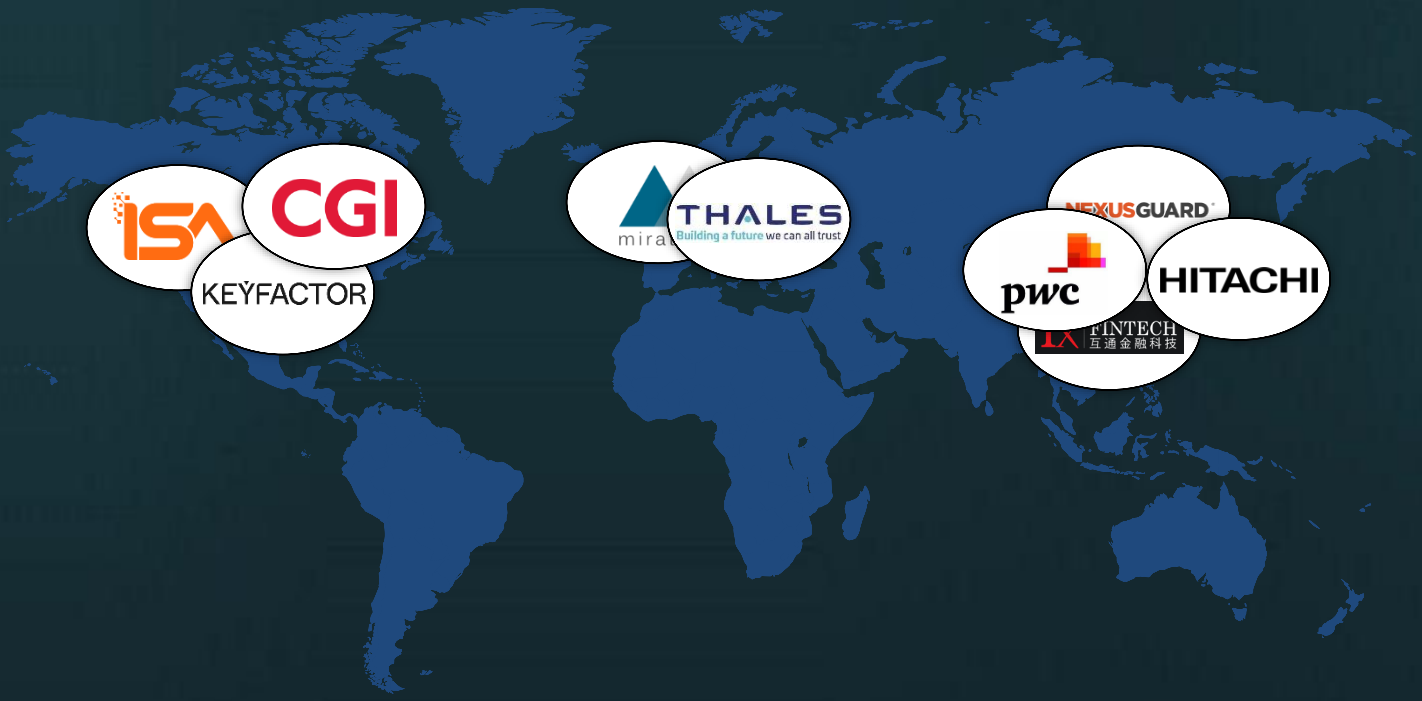
US#11,271,715: cryptographic system incorporating advanced post-quantum cryptographic technology

US#11,669,833:
Quantum-Safe blockchain endpoints and crypto Wallets

Patent-pending

- ❑ Email security related
- ❑ PQC related
- ❑ Secure AI platform

Global Partnerships

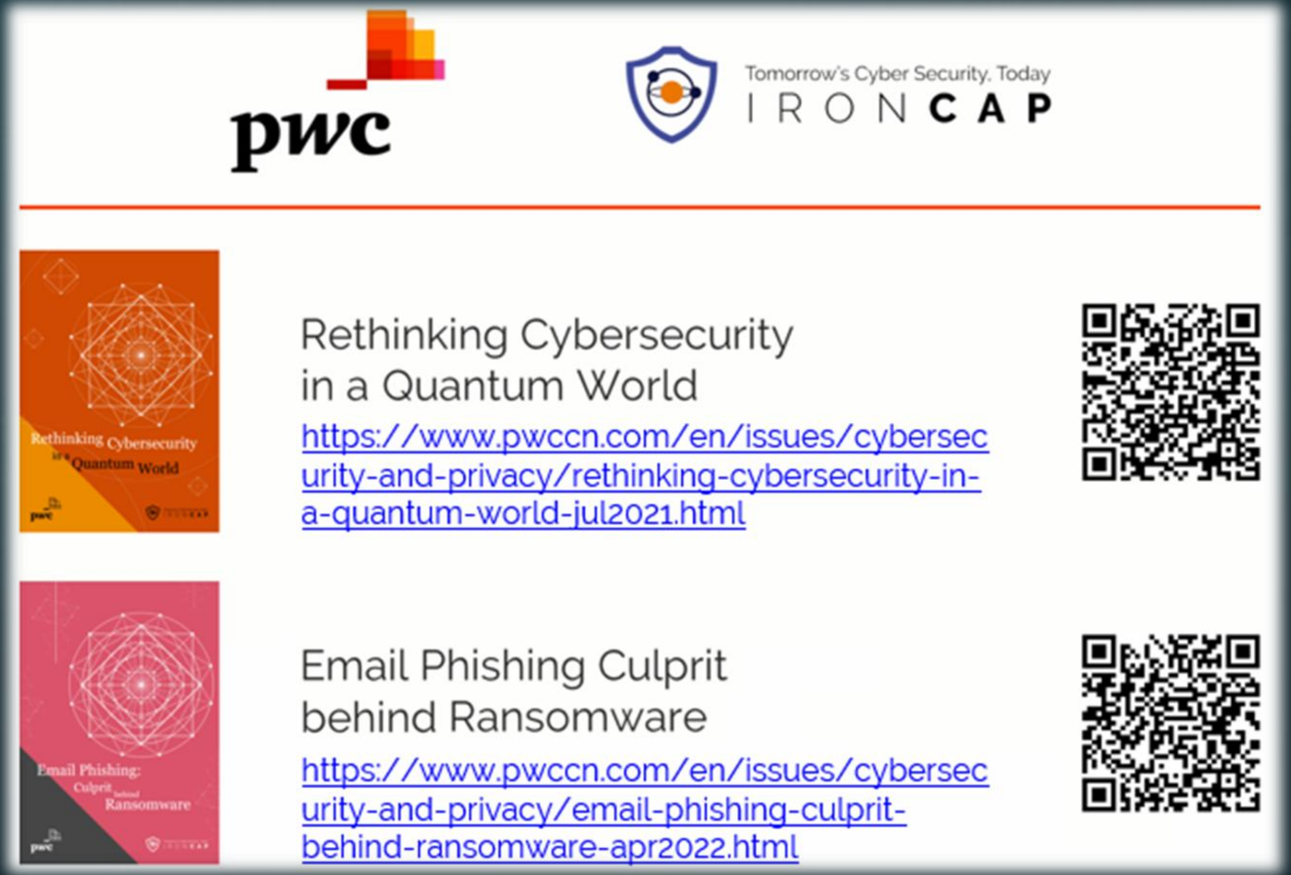


CGI - Innovation Center

IronCAP Demo

https://ironcap.ca/demo/cgi/

PwC - Thought Leadership Papers



pwc

Tomorrow's Cyber Security, Today

IRONCAP

Rethinking Cybersecurity in a Quantum World

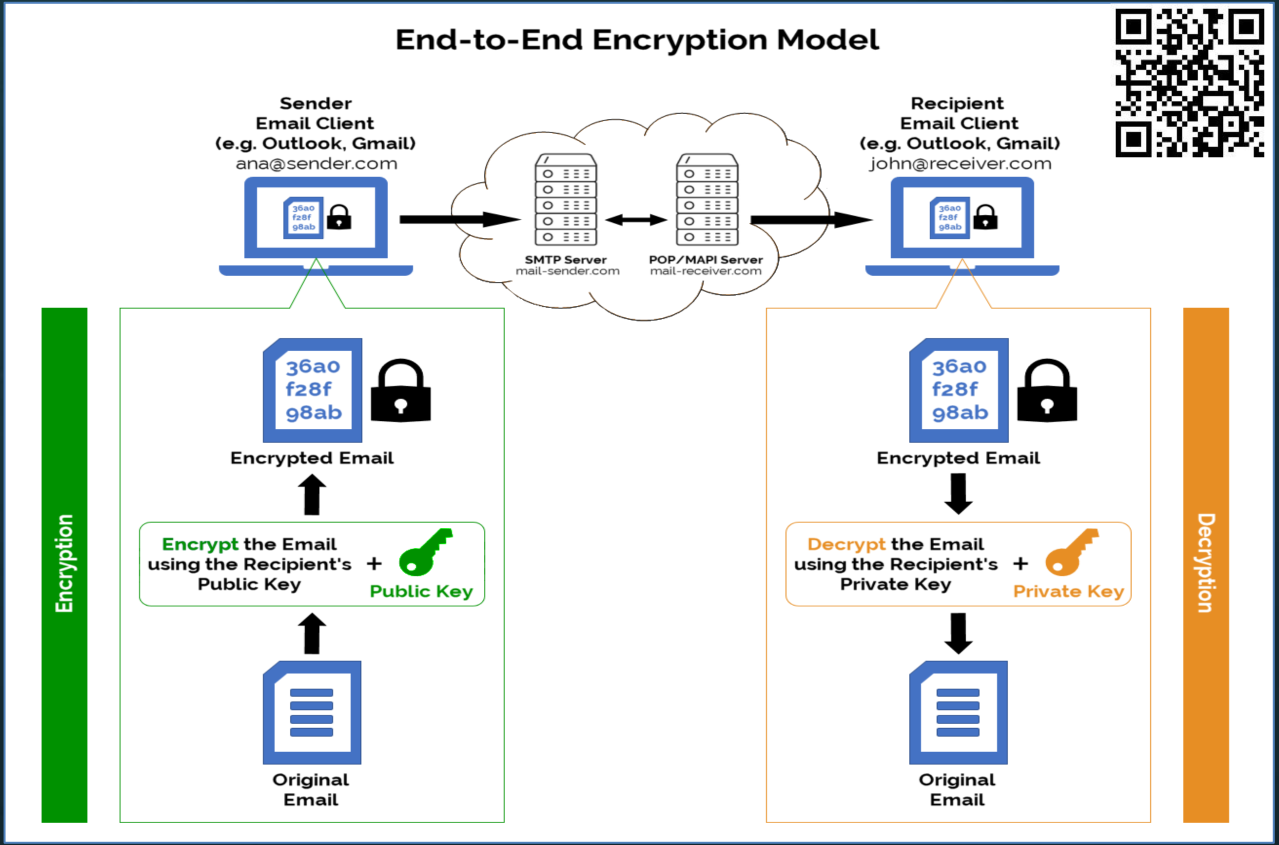
https://www.pwccn.com/en/issues/cybersecurity-and-privacy/rethinking-cybersecurity-in-a-quantum-world-jul2021.html

Email Phishing Culprit behind Ransomware

https://www.pwccn.com/en/issues/cybersecurity-and-privacy/email-phishing-culprit-behind-ransomware-apr2022.html

Use Case #1 – Email Security

https://ironcap.ca/ironcap-x/



End-to-End Encryption Model

Sender Email Client (e.g. Outlook, Gmail) ana@sender.com

SMTP Server mail-sender.com

POP/MAPI Server mail-receiver.com

Recipient Email Client (e.g. Outlook, Gmail) john@receiver.com

Encryption

Original Email

Encrypt the Email using the Recipient's Public Key + Public Key

Encrypted Email

Decryption

Encrypted Email

Decrypt the Email using the Recipient's Private Key + Private Key

Original Email

Use Case #1 – Email Security

IronCAP X^{TM} Illustration Video — Ctrl-click to Play

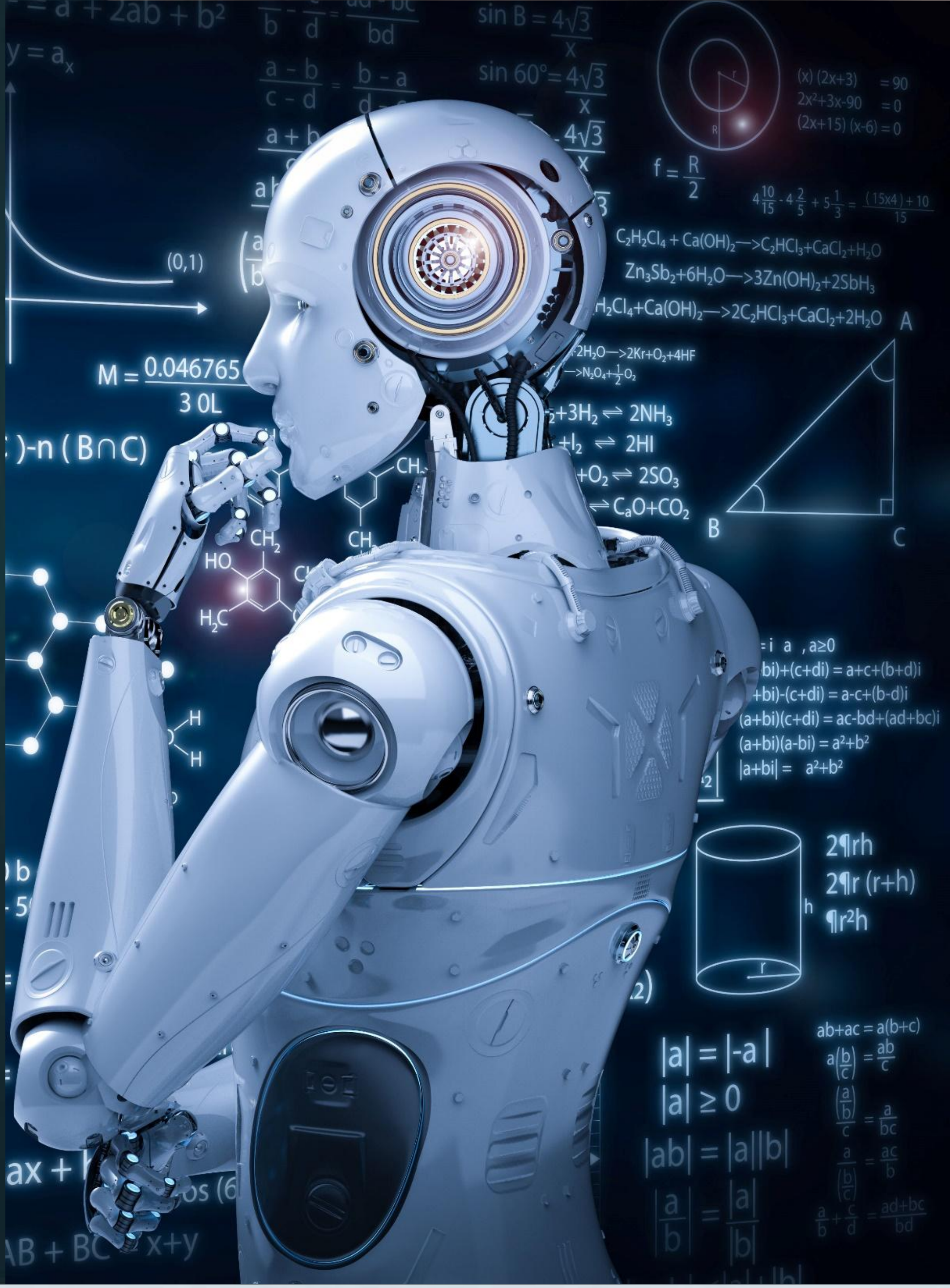
IronCAP X^{TM} Demo Video — Ctrl-click to Play

Use Case #2 – AI

End-to-End Quantum-Safe Machine Learning
(Learning ⇔ Knowledge ⇔ Query)

Typical users:

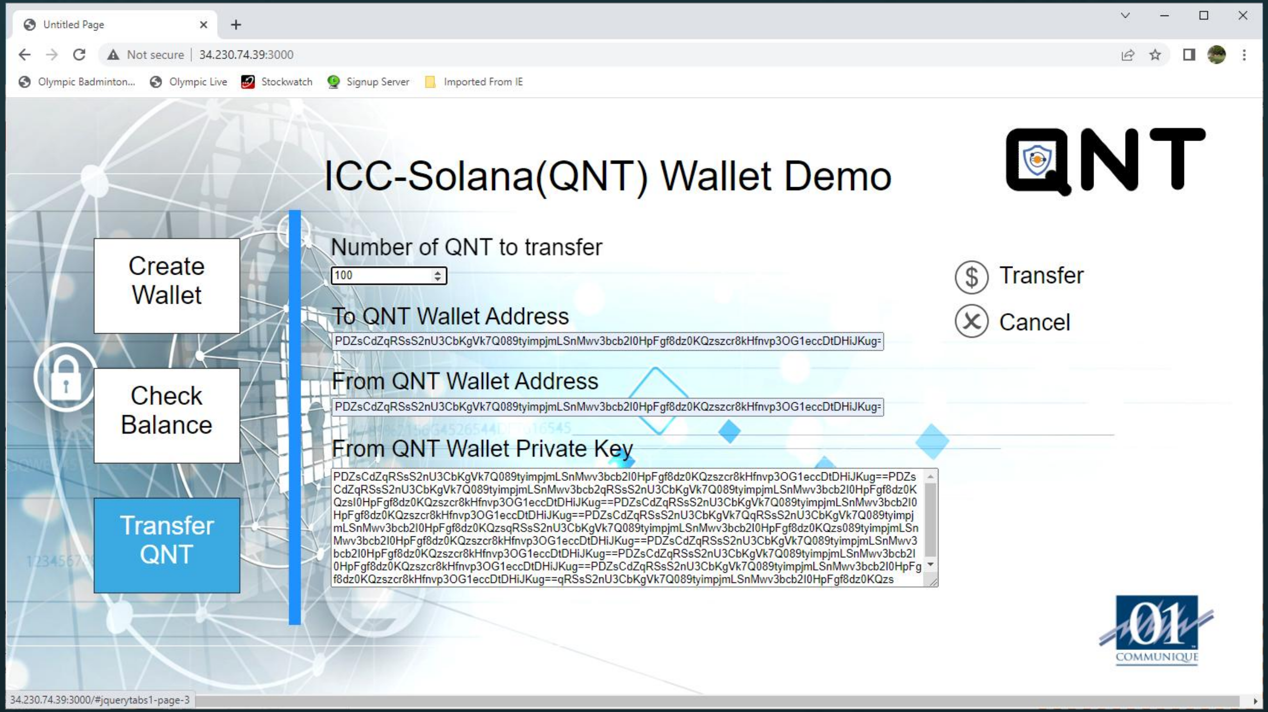
- Secure multi-party Computation
- Private Set Intersection
- Outsourcing ML
- Privacy-preserved ML
- Medical Records Learning
- Financial Model Learning
- Image Recognition
- Anomaly Detection
- Supply Chain Optimization
- Blockchain | Smart Contract



Use Case #3 - Cryptocurrency

Proof-of-Concept on Solana

https://qnt-demo.ironcap.ca



ICC-Solana(QNT) Wallet Demo

Number of QNT to transfer

100

To QNT Wallet Address

PDZsCdZqRSsS2nU3CbKgVk7Q089tyimpjmLSnMwv3bcb2I0HpFgf8dz0KQzszcr8kHfnvp3OG1eccDtDHiJKug=

From QNT Wallet Address

PDZsCdZqRSsS2nU3CbKgVk7Q089tyimpjmLSnMwv3bcb2I0HpFgf8dz0KQzszcr8kHfnvp3OG1eccDtDHiJKug=

From QNT Wallet Private Key

```
PDZsCdZqRSsS2nU3CbKgVk7Q089tyimpjmLSnMwv3bcb2I0HpFgf8dz0KQzszcr8kHfnvp3OG1eccDtDHiJKug==PDZs
CdZqRSsS2nU3CbKgVk7Q089tyimpjmLSnMwv3bcb2qRSsS2nU3CbKgVk7Q089tyimpjmLSnMwv3bcb2I0HpFgf8dz0K
QzsI0HpFgf8dz0KQzszcr8kHfnvp3OG1eccDtDHiJKug==PDZsCdZqRSsS2nU3CbKgVk7Q089tyimpjmLSnMwv3bcb2I0
HpFgf8dz0KQzszcr8kHfnvp3OG1eccDtDHiJKug==PDZsCdZqRSsS2nU3CbKgVk7QqRSsS2nU3CbKgVk7Q089tyimpj
mLSnMwv3bcb2I0HpFgf8dz0KQzsqRSsS2nU3CbKgVk7Q089tyimpjmLSnMwv3bcb2I0HpFgf8dz0KQzs089tyimpjmLSn
Mwv3bcb2I0HpFgf8dz0KQzszcr8kHfnvp3OG1eccDtDHiJKug==PDZsCdZqRSsS2nU3CbKgVk7Q089tyimpjmLSnMwv3
bcb2I0HpFgf8dz0KQzszcr8kHfnvp3OG1eccDtDHiJKug==PDZsCdZqRSsS2nU3CbKgVk7Q089tyimpjmLSnMwv3bcb2I
0HpFgf8dz0KQzszcr8kHfnvp3OG1eccDtDHiJKug==PDZsCdZqRSsS2nU3CbKgVk7Q089tyimpjmLSnMwv3bcb2I0HpFg
f8dz0KQzszcr8kHfnvp3OG1eccDtDHiJKug==qRSsS2nU3CbKgVk7Q089tyimpjmLSnMwv3bcb2I0HpFgf8dz0KQzs
```

Use Case #4 - DAEM

Digital Asset Exchange Machine

ixFintech launched the world's first quantum-safe DAEM at Cyberport, Hong Kong. DAEM allows trading of digital assets using cash and digital wallets. Secure transactions are done by utilizing IronCAP's cryptographic technology for its key generation, encryption, decryption, digital signature, verification and other quantum-safe crypto functions.

DAEM adopts 2 layers of authentication to ensure end-to-end security between:

1. User's device and DAEM.
2. DAEM and the host application.

First Hong Kong DeFi-DAEM (Digital Asset Exchange Machine) installed with post quantum computing security. IxFintech strive to build the best next generation digital asset financial framework. The device you see here can not only give you an experience to purchase and sell digital asset, but also installed with patented IronCap technology from 01 Communique, an Ontario Canada Fintech company with 40 years of unhacked history. Every transaction here is tri-protected by network security, time protected token (example OTP) and cryptography technology which supercomputer cannot hack.

香港第一台安裝了超級電腦保安系統的DeFi–數碼資產交易站。互通金融科技致力於打造最佳的新一代數碼資產金融框架。您在此看到的這台設備不僅可以為您提供買賣數碼資產的體驗，這台設備同時也安裝了獲得專利的IronCap科技，該科技來自01 Communique，這是一家擁有40年未被侵入歷史的位於加拿大安大略省的金融科技公司。該自動櫃員機上的每一筆交易都受到網絡安保，時間保護令牌（例如OTP）以及超級電腦也無法侵入的加密技術的三重保護。

IRONCAP

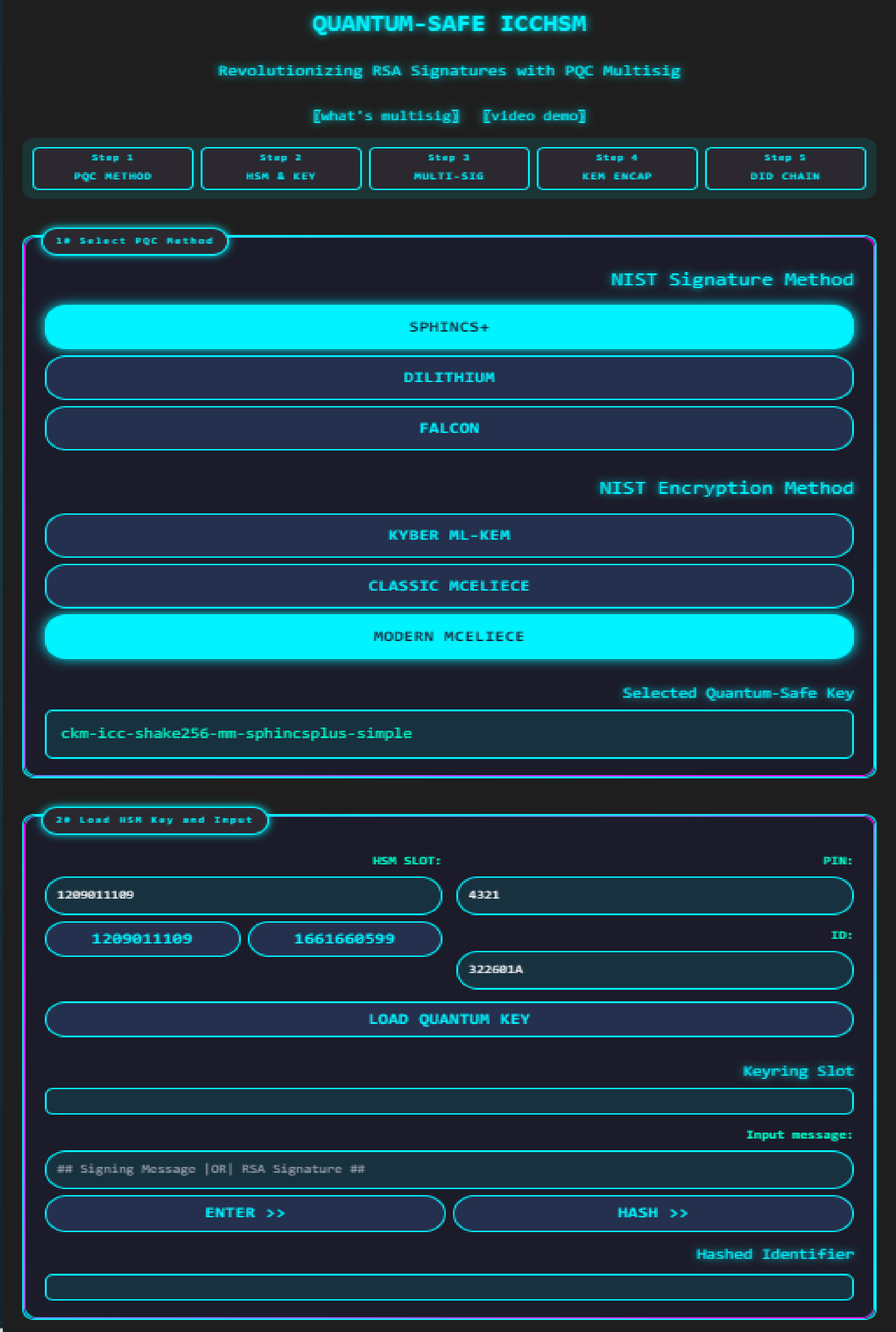
Use Case #5 – Multi-Signature

Partnership with Real Matter

Quantum-Safe Multi-Signature

QSMS is an innovative technology built on top of the existing digital signature framework (RSA). It introduces an optional QSMS Blockchain Ledger layer that enhances security with quantum-safe additional signatures while preserving the independence of the existing RSA framework. Both systems can operate separately without interference.

Demo:
https://quantumsafe-multisig-pin4321.web.app/



QUANTUM-SAFE ICCHSM

Revolutionizing RSA Signatures with PQC Multisig

[what's multisig] [video demo]

1# Select PQC Method

NIST Signature Method: SPHINCS+ (selected)

NIST Encryption Method: MODERN MCELIECE (selected)

Selected Quantum-Safe Key: ckm-icc-shake256-mm-sphincsplus-simple

2# Load HSM Key and Input

HSM SLOT: 1209011109

PIN: 4321

ID: 322601A

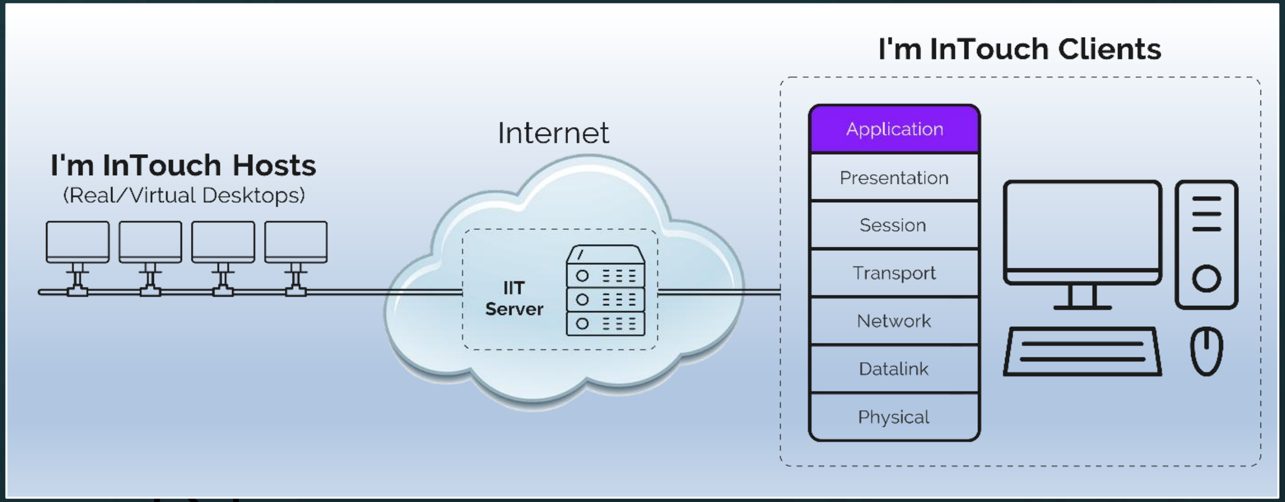
Keyring Slot:

Input message: ## Signing Message |OR| RSA Signature ##

Hashed Identifier:

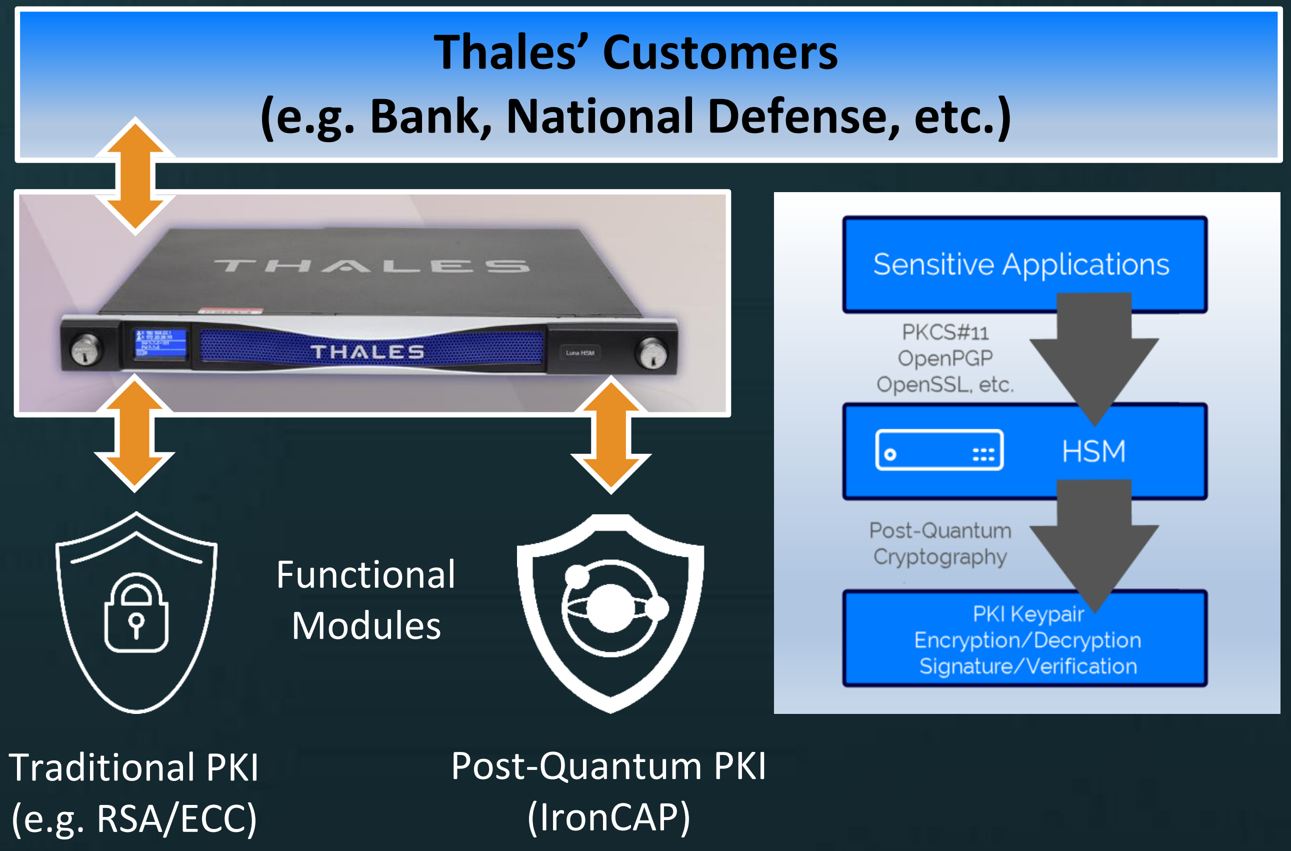
Use Case #6 - Remote Access

Quantum-Safe + Zero Trust



No access to corporate LAN

Use Case #7 – Thales Luna HSM



Thales' Customers
(e.g. Bank, National Defense, etc.)

Functional Modules

Traditional PKI
(e.g. RSA/ECC)

Post-Quantum PKI
(IronCAP)

Sensitive Applications

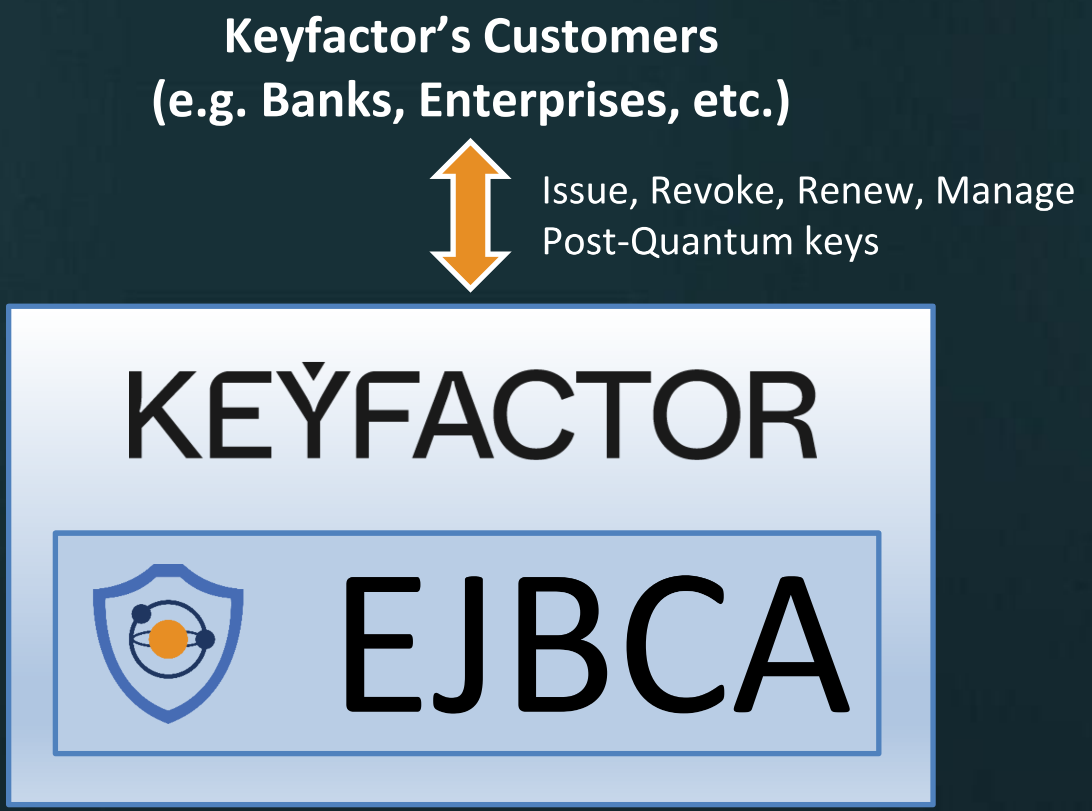
PKCS#11
OpenPGP
OpenSSL, etc.

HSM

Post-Quantum Cryptography

PKI Keypair
Encryption/Decryption
Signature/Verification

Use Case #8 – Keyfactor EJBCA



Keyfactor's Customers
(e.g. Banks, Enterprises, etc.)

Issue, Revoke, Renew, Manage
Post-Quantum keys

IRONCAP

By combining both NIST-approved PQC algorithms as well as our own patent-protected quantum-safe technologies, IronCAP™ has extensive hands-on experience in Post-Quantum Cybersecurity to help you transform your systems to become quantum-safe.

For more information:

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

IronCAP Partners:

CGI pwc KEYFACTOR THALES Building a future we can all trust
Hitachi Solutions Create REAL MATTER ISA mirata ltd

01 COMMUNIQUE

Take Away:

- Quantum Threat is here
- Everything is vulnerable
- Need to act now
- IronCAP is the Solution