An Update on Post Quantum Cryptography

Mike Brown, CTO & Co-founder,
ISARA Corporation

Founded | 2015

Headquarters | Waterloo, Ontario, Canada

Initial Funding from Quantum Valley Investments | $11.5M

Series A from Shasta Ventures | $10M

Canadian Government Strategic Funding (April 2019) | $5.5M

Full-time employees | 33 (9 PhDs)

Visionary Leadership Team

Combined **150+** years experience and extensive global business experience and networks.

Master Practitioners, Quantum-safe Experts

Specialize in **quantum-safe** crypto. Deep knowledge of **lightweight crypto** for IoT.

Standards-based Approach

Collaboratively setting standards with **ETSI, ITU-T, X9, IETF, and NIST**.

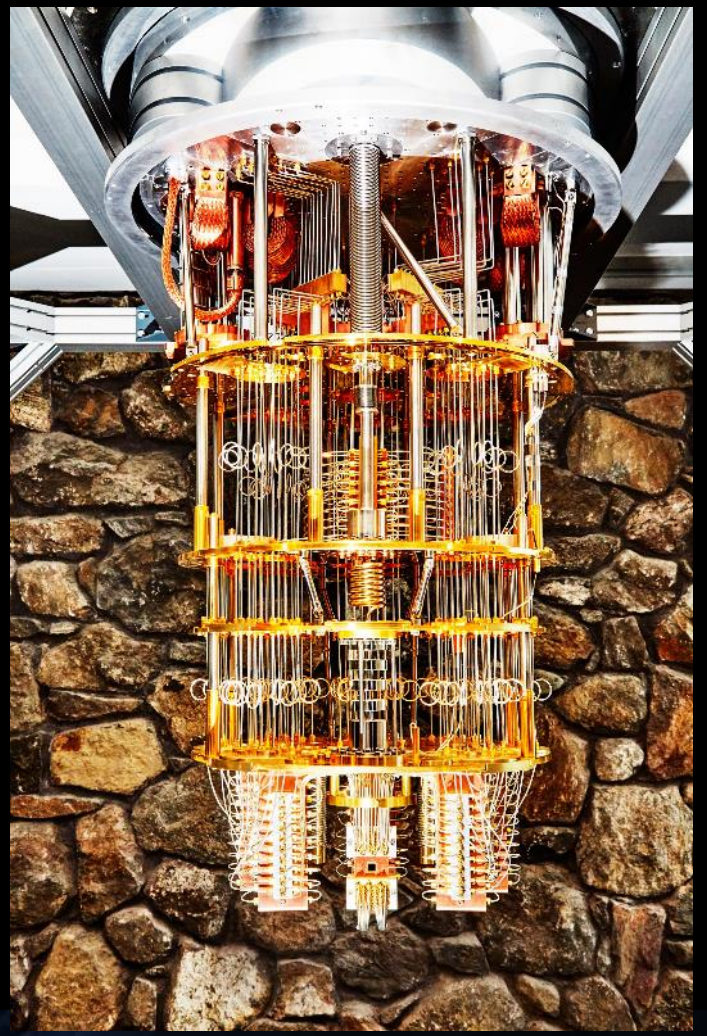
WHAT IS QUANTUM COMPUTING?

Quantum computing harnesses the unique properties of quantum physics to break barriers currently limiting the speed of today's "classical" computers, as they're now called.

Quantum computing **will not replace** current computers; you won't have a quantum computer smartphone in your pocket.

They will, however, be able to **solve very specific, hard problems** that even the fastest supercomputers couldn't solve in a reasonable amount of time today.

The first real use for them will likely be in advancements in areas such as material design, pharmaceuticals, and optimizing the power grid.



Major Industry Players

Google

intel

IBM

rigetti

ISARA

THE QUANTUM RACE IS ON






Microsoft

Google

rigetti

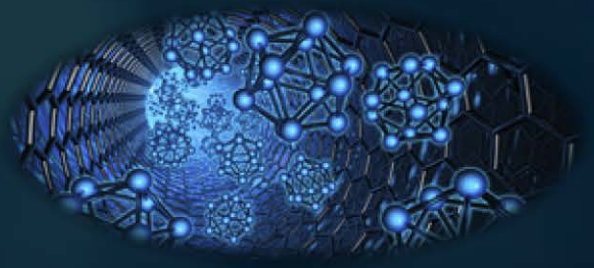
IBM

D:wave
The Quantum Computing Company™

intel

ISARA

POSITIVE DISRUPTIONS



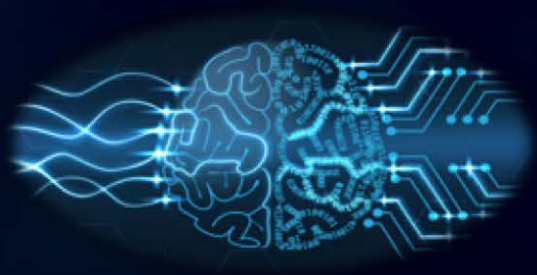
MATERIAL DESIGN

CHEMICAL DISCOVERY

DRUG DESIGN

OPTIMIZATION

SEARCH/ BIG DATA



MACHINE LEARNING

ISARA

Timeline to Quantum

ANALOG QC

NOISY QC

UNIVERSAL QC

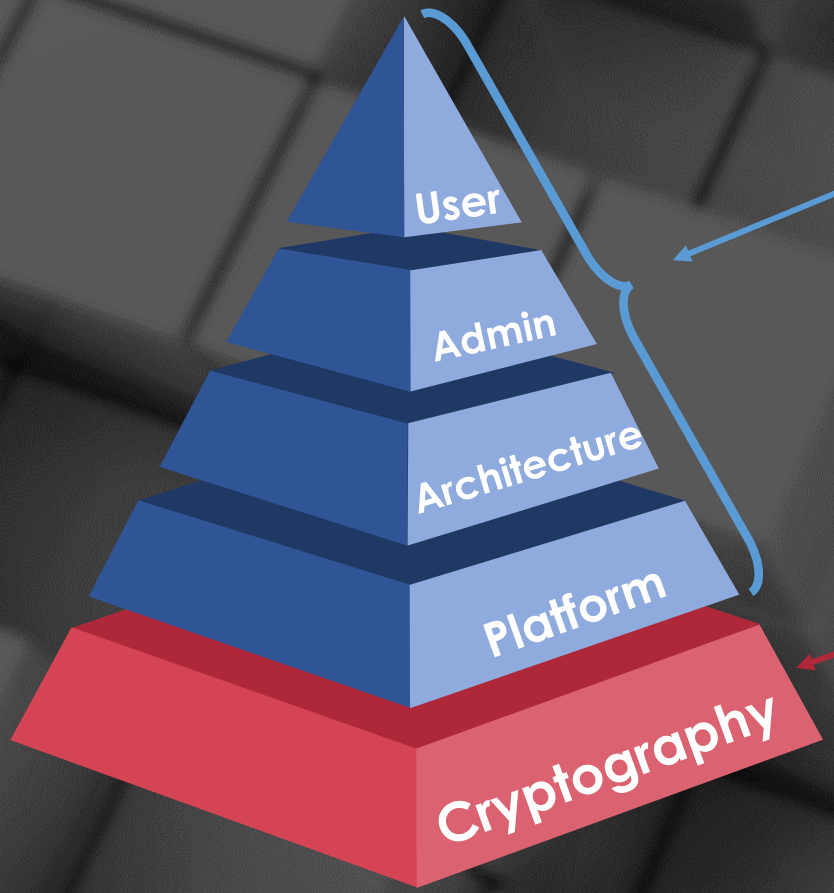
ISARA

The Quantum Effect on Public Key Cryptography

Type	Algorithm	Key Strength Classic (bits)	Key Strength Quantum (bits)	Quantum Attack
Asymmetric	RSA 2048	112	0	Shor's Algorithm
	RSA 3072	128		
	ECC 256	128		
	ECC 521	256		
Symmetric	AES 128	128	64	Grover's Algorithm
	AES 256	256	128	

ISARA

MITIGATING AN UNPRECEDENTED THREAT



Today, data breaches occur outside of cryptography, and the costs of those breaches is **growing**.

A complete break of public key cryptography is **unprecedented.**

In our connected world, everything that **protects data, authorizes or authenticates must be updated** to be quantum-safe.

This magnitude of change has never been required **on such a large scale**.

ISARA


IBM
= Less than 20 years
ETSI
= Less than 10 years
NIST
= Less than 11 years
Microsoft
= Less than 11 years
European Commission
= Sometime after 2025
Future
The dawn of large-scale quantum computers
By 2026, the risk becomes too high to ignore

The best time to start is now

How many years does the connected device need to be secured for?

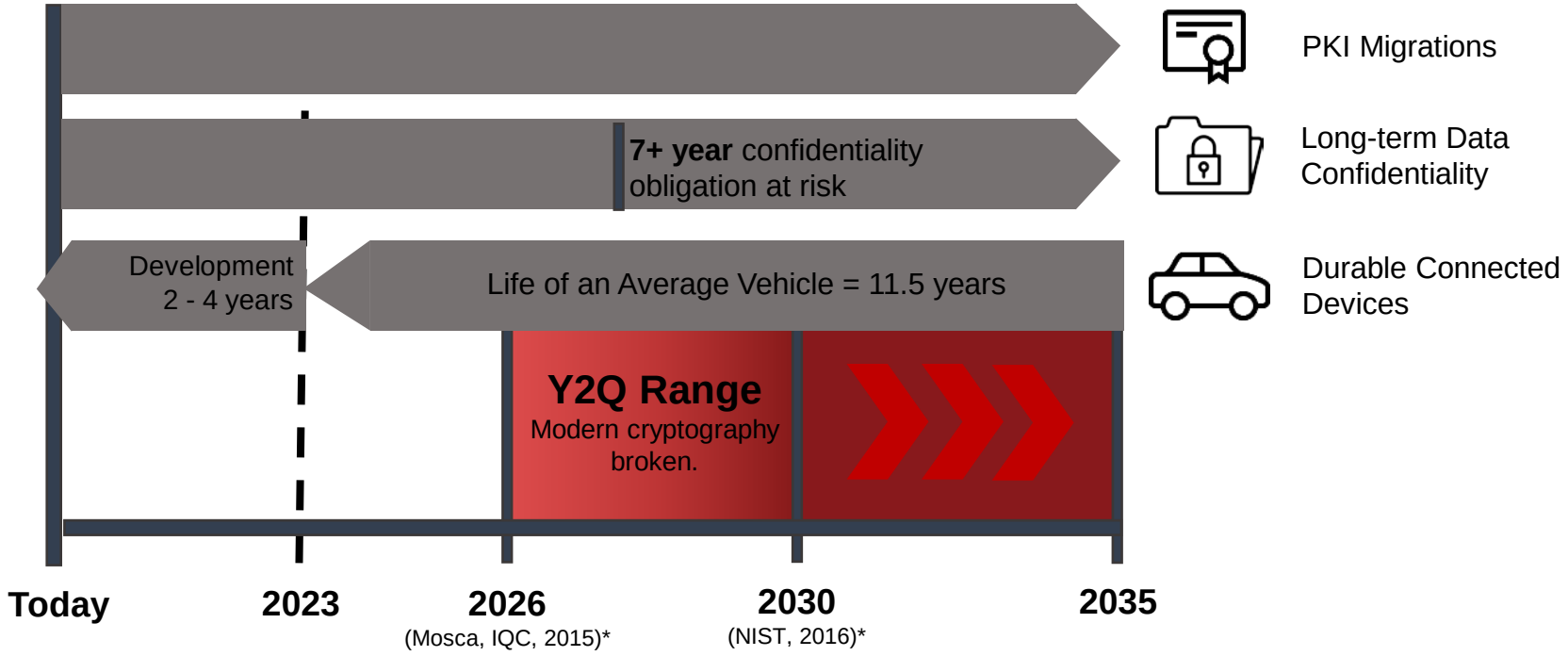
If 7+ years, you need to start preparing today

How long does the information need to remain confidential?

If 7+ years, you need to start preparing today

Does the device require strong security?

- PKI and digital certificates
- Hardware security modules (HSMs)
- Physically embedded roots of trust



*Mosca, Michele., Institute for Quantum Computing. 2015. "Cybersecurity in an era with quantum computers: will we be ready?". https://eprint.iacr.org/2015/1075.pdf

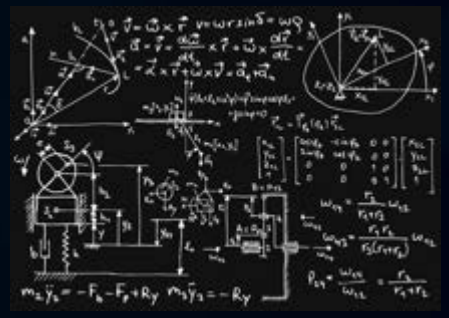
*NIST. April 2016. "Report on Post-Quantum Cryptography". http://dx.doi.org/10.6028/NIST.IR.8105

*https://www.popsci.com/environment/article/2009-06/next-grid

ISARA

TWO PATHS TO QUANTUM-SAFE SECURITY

Quantum Key Distribution



Quantum-Safe Cryptography

ISARA

THE "NEW" MATH

Hash-based

Ready to Use Today

Undergoing NIST Evaluation

Code-based

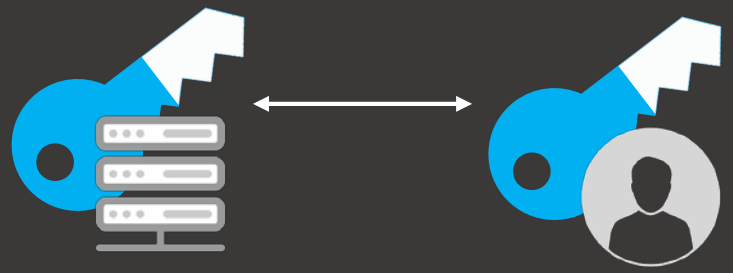
Lattice-based

Multivariate-based

Isogeny-based

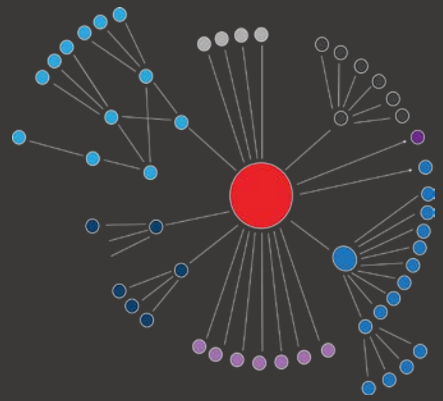
ISARA

THE MIGRATION CHALLENGE
KEY ESTABLISHMENT VS. AUTHENTICATION



Key establishment can be **easily upgraded** because the client and server negotiate which algorithm to use.

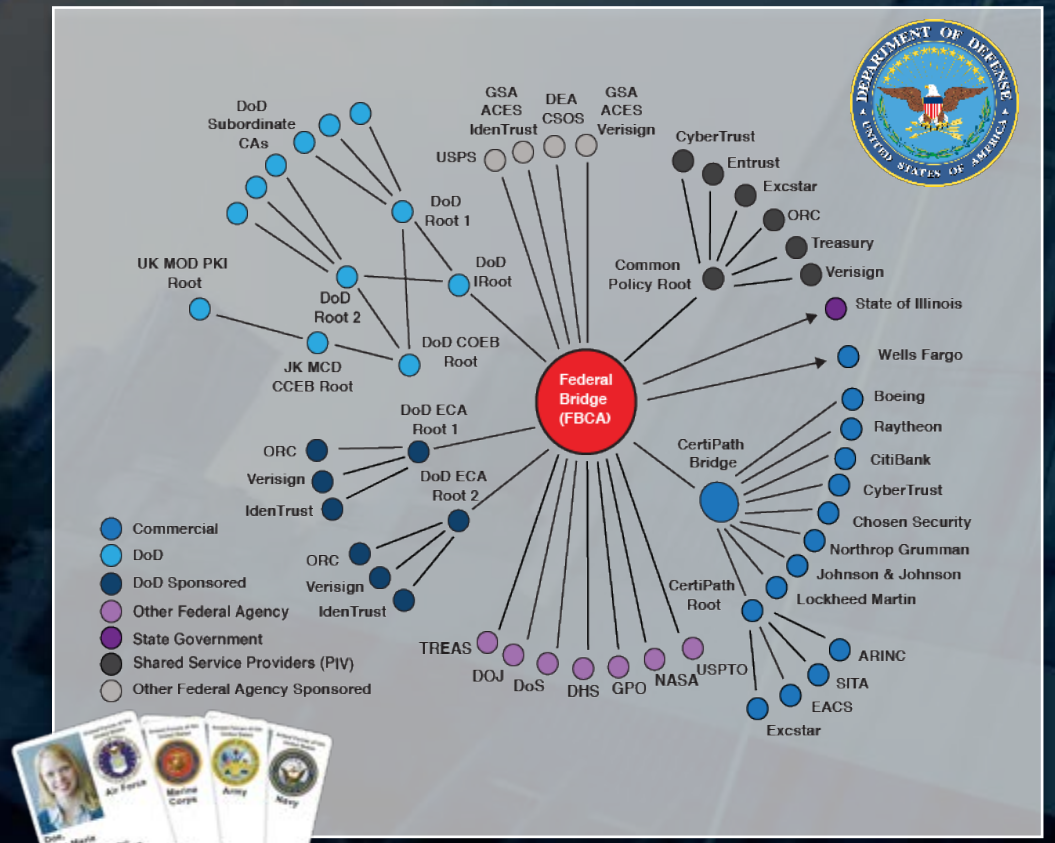
1) Use quantum-safe **key transport** or **key agreement** algorithms
2) Use **hybrid keys**, a mix of both classic and quantum-safe algorithms



The complexity and interconnectivity of public key infrastructure demands action today in order to be ready for the quantum age, and difficult to do while maintaining backward compatibility.

ISARA

DoD PKI MIGRATION EXAMPLE



There's more than

4.5 million active users

in the DoD identity management system.

Creating a quantum-safe duplicate infrastructure is time-consuming and cost prohibitive.

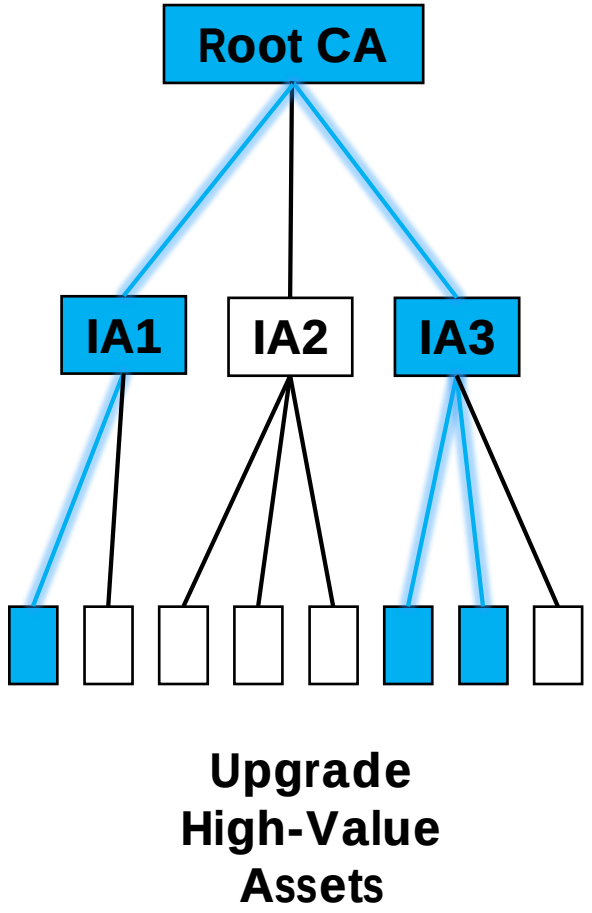
ISARA

Bridging the Gap
Using Crypto-Agility

ISARA

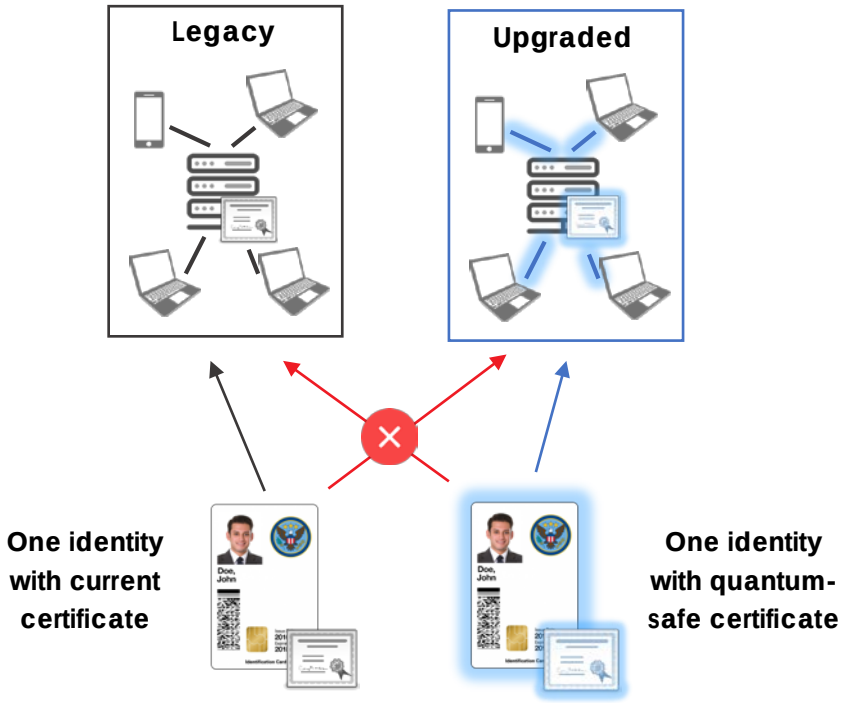
HYBRID PKI & PHASED MIGRATION

- Hybrid Root certificates can be created today and embedded into systems today
- Stateful hash-based signatures are perfectly suited for certificate signing and are ready to be used today
- Code signing end systems can also be upgraded today
- Communication systems are ready to be upgraded to use hybrid algorithms or leading NIST candidates

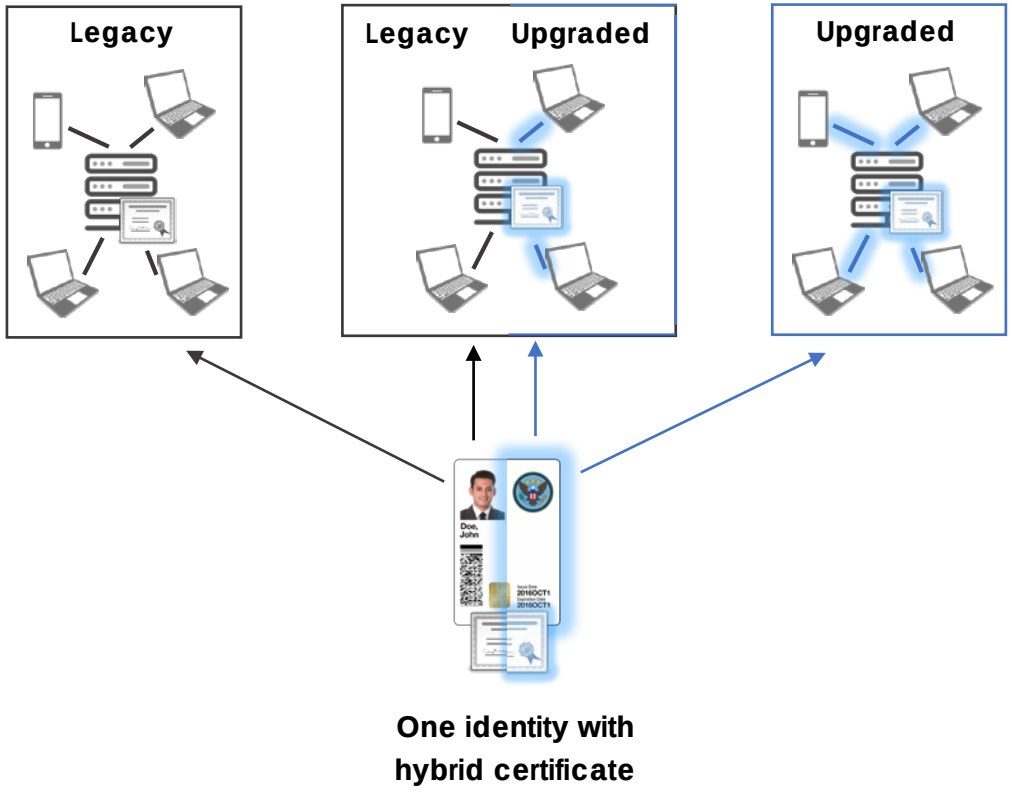


PKI MIGRATION APPROACHES

Duplicate Infrastructure



Hybrid Infrastructure



Hybrid and Standards

- ITU-T
  - A contribution submitted by ISARA Corporation (Canada) was approved that proposes the inclusion of optional support for multiple public-key algorithms in **Recommendation ITU-T X509 | ISO/IEC 9594-8**
- IETF
  - Two proposals
    - *"Composite" – IETF draft* ***Composite Public Keys and Signatures*** *(draft-pala-composite-crypto)*
    - *"Catalyst" - IETF draft* ***Multiple Public-Key Algorithm X.509 Certificates*** *(draft-truskovsky-lamps-pq-hybrid-x509)*
  - Both expired

HIGH RISK:
Authenticated Software Over-The-Air (OTA) Updates

What's at risk?

Durable connected devices (IoT) **with long in-field lives**

What's The Attack

Forged software updates by quantum-enabled adversaries

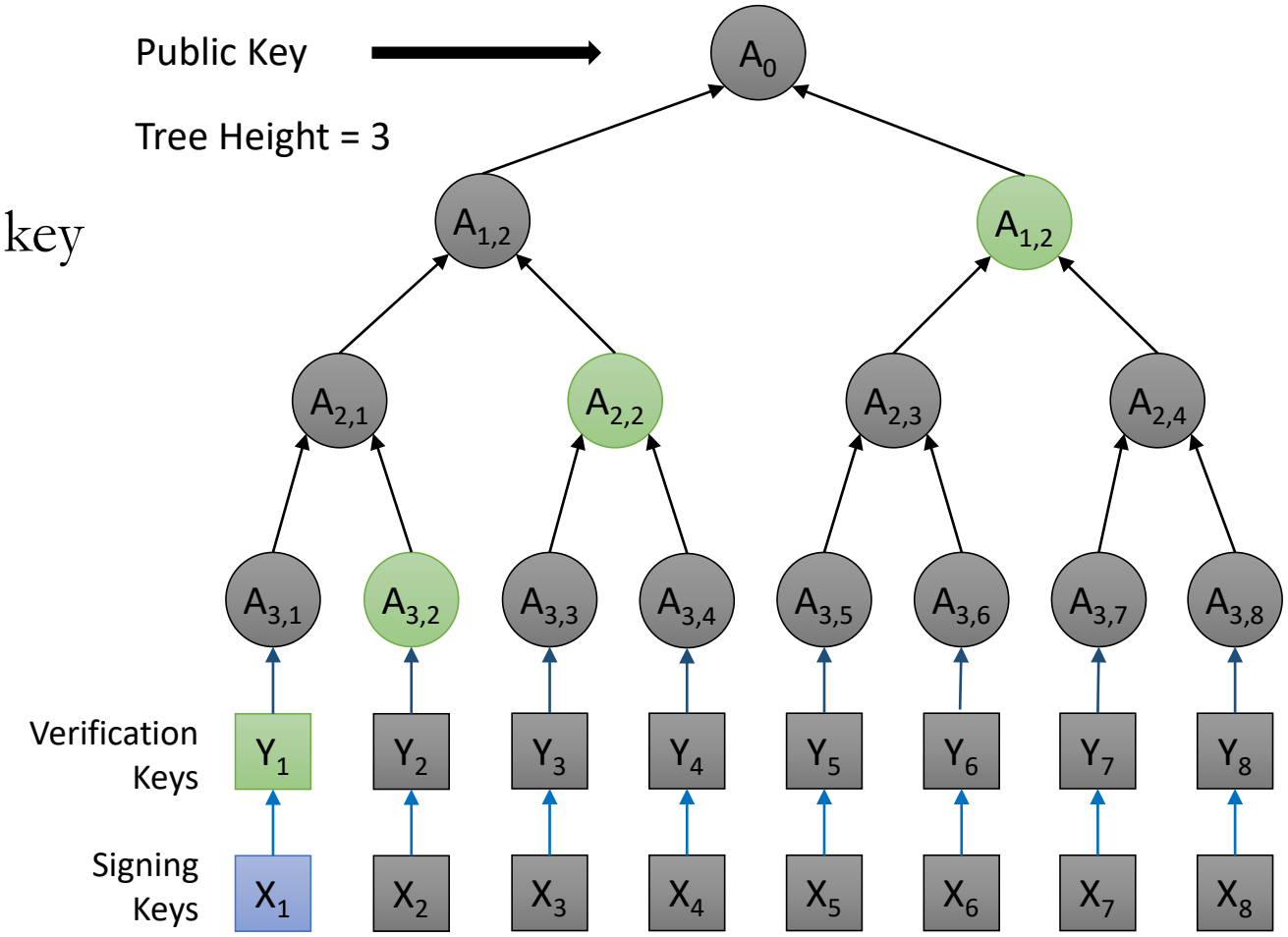
What's Affected

- Digital Signatures
- Code Signing
- Embedded Roots of Trust

Protection: Physically embed stateful hash-based roots of trust today

Hash-Based Cryptography 101

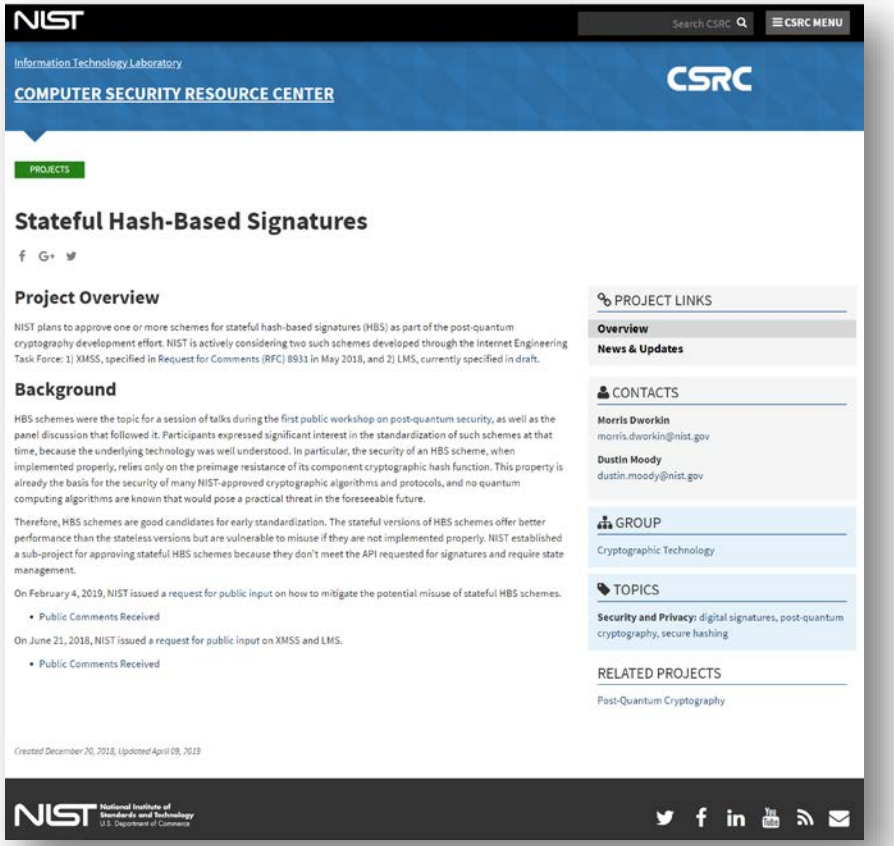
- Introduced by Merkle in 1979
- "One-Time Signatures"
- Small public key but very large private key
- Fast signing & verifying
- Stateful
- Candidates:
  - Leighton-Micali Signatures (LMS)
  - eXtended Merkle Signature Scheme (XMSS)
  - SPHINCS



ISARA

NIST on Stateful Hash-based Signatures (HBS)

1. HBS schemes are good candidates for early standardization because they're **trusted, mature, and well understood**
2. NIST is actively reviewing **XMSS and LMS** (HSS) for early approval outside their Post-Quantum Cryptography Standardization Process
3. Under consideration for specific use-cases, such as **code-signing**
4. The security of an HBS scheme **relies on the same basis** as many current NIST-approved cryptographic algorithms and protocols, and no known quantum algorithms pose a practical threat



https://csrc.nist.gov/Projects/Stateful-Hash-Based-Signatures

ISARA

Stateful HBS Operational Implications

1. **Running out of keys**: The private key of a stateful HBS scheme is an "exhaustible" resource, so careful planning is required
2. **Growing signatures**: Signature size grows as the size of the private key grows
3. **New implementation considerations**: Private key splitting and state management is not something the industry has had to deal with before
4. **Special considerations for high-value roots**: For extremely high-value root keys that don't produce many signatures during their validity a manual process for state management may be required

Global Standards Focus

ISARA

NIST Standardization Update

- 17 KEM Candidates
  - BIKE
  - Classic McEliece
  - Kyber
  - Frodo
  - HQC
  - LAC
  - LEDAcrypt
  - NewHope
  - NTRU
  - NTRU Prime
  - NTS-KEM
  - ROLLO
  - Round5
  - RQC
  - SABER
  - SIKE
  - Three Bears
- 9 Signature Candidates
  - Dilithium
  - Falcon
  - GeMSS
  - LUOV
  - MQDSS
  - Picnic
  - qTESLA
  - Rainbow
  - SPHINCS+

NIST Standardization Update

- Timelines
  - Round 2 ends June 2020
  - Round 3 begins after with reduced list
  - Final standards 2022-2024(ish)
  - Potential additional algorithms standardized post Round 3
- Request more merging
- Hybrid modes of operation
- Complexity of implementation


We leverage decades of real-world cybersecurity expertise to protect today's computing ecosystems in the quantum age using practical, standardized technologies for a seamless migration.
ISARA
CLEARING THE PATH TO QUANTUM-SAFE SECURITY
www.isara.com
quantumsafe@isara.com