



THE END OF CRYPTOGRAPHY

AS WE KNOW IT

ABOUT ISARA

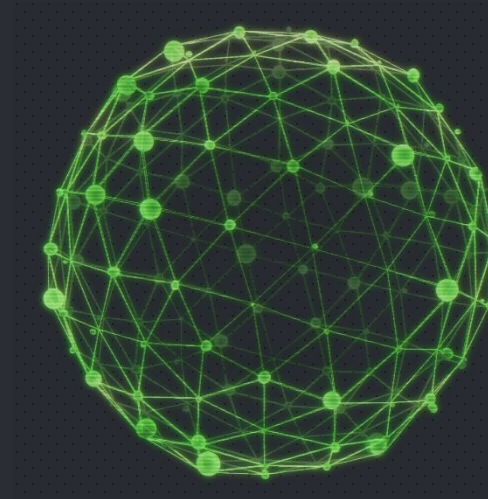
Security Measures For
The Quantum Age

About ISARA



—
Founded in 2015,
ISARA is affiliated with
the rich academic and
research ecosystem of
Quantum Valley, a high-
tech hub in Waterloo,
Ontario, Canada

—
Founded



—
Consumers,
governments and
organizations should
benefit from the power
of quantum computing
without compromising
data security.

—
Vision

About ISARA



—
We have a highly experienced management team with backgrounds in wireless, encryption, security solutions, sales and standards/certification.

Team



—
We're building quantum safe solutions, starting with the launch of our ISARA Quantum Resistant Toolkit.

Solutions

01

02

03



Threat



Solutions



Standards

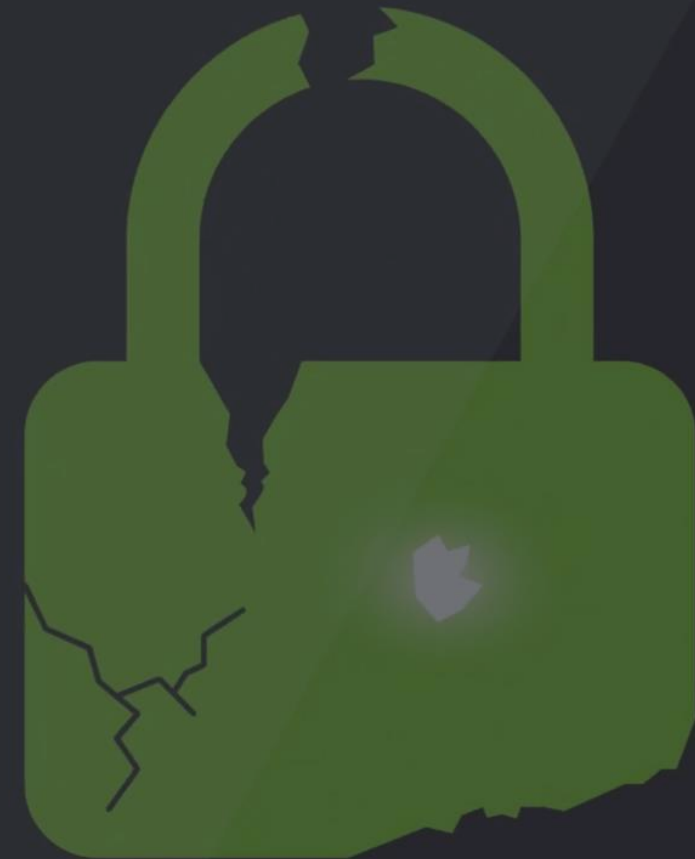
Quantum Computing Threat



Cryptographic Challenges For A Post Quantum World

Today's security solutions rely on the complexity of the underlying mathematical problems that form the foundation for modern cryptographic systems.

The massive processing capabilities found in quantum computers will challenge our current beliefs around complexity.



When Does The Clock Run Out?

Understanding the risks means balancing multiple factors.

The answer depends on who you are, what secrets you need to keep and what the impact is if your secrets are no longer secrets.

In some cases, it's already too late.

When Do You Need To Worry?

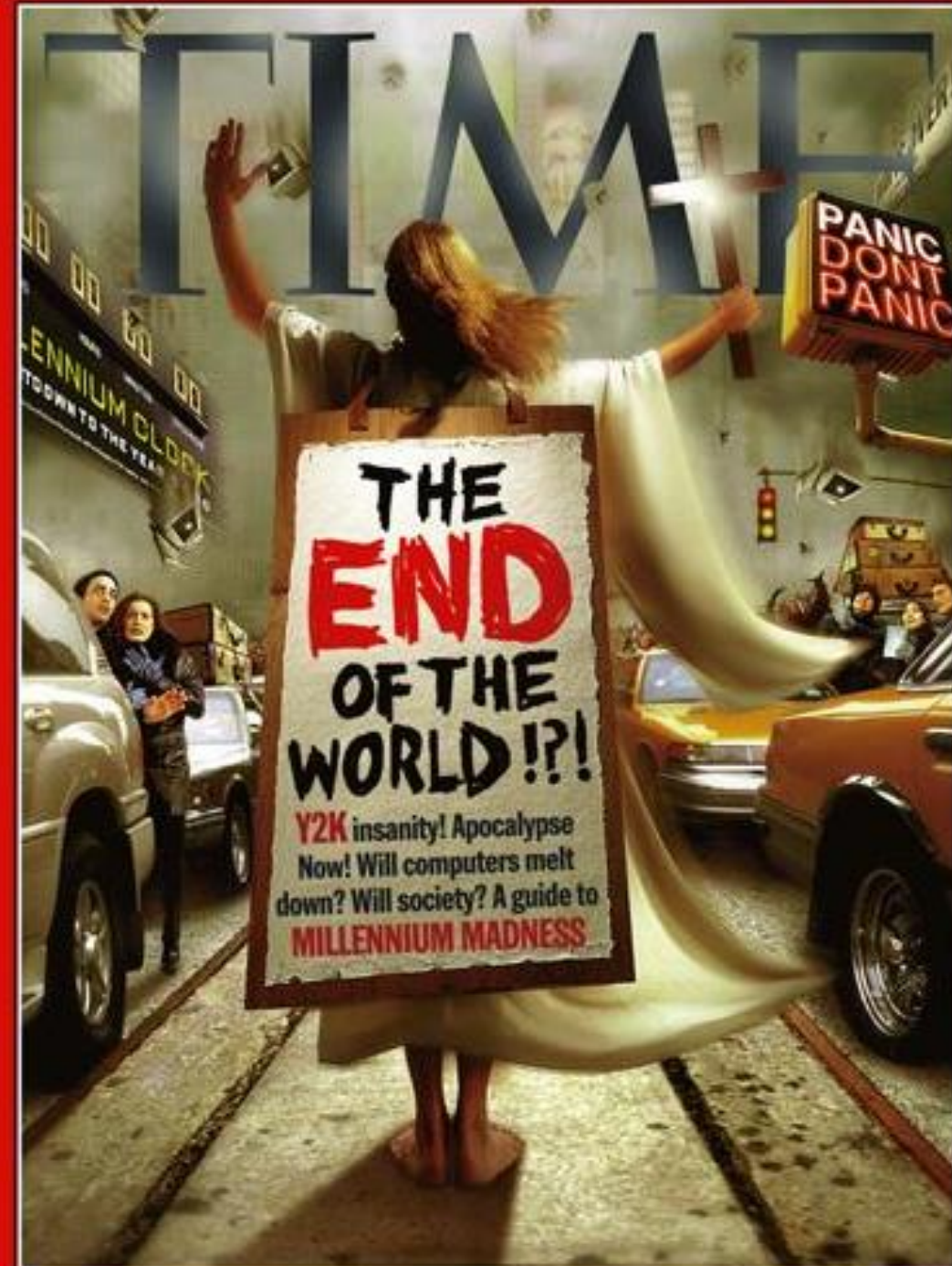
(It Depends...)



Years To Quantum

Y2Q: The scope of the change required is akin to Y2K.

To do a risk management assessment, all protocols, clients and servers need an in-depth review. This requires coordination between vendors, OEMs and customers to catch all of the interactions.



What Does All This Mean For Crypto?

“A collection of just 50 qubits operated that way will likely be the first computer to demonstrate “quantum supremacy”—the power to solve a computational problem immensely difficult and perhaps practically impossible for conventional machines.”

Scott Aaronson

“With a quantum computer built of just 50 qubits, none of today’s TOP500 supercomputers could successfully emulate it, reflecting the tremendous potential of this technology.”

IBM

“The potential impact is enormous. Everything we are encrypting today that is stored somewhere will be decrypted by quantum computers when we have them.”

Ray LaFlamme

“There is an emerging consensus that *the best practical approach to quantum security is to evolve current security applications and packet-based communication protocols towards adopting post-quantum public key cryptography. Software or firmware implementations of post-quantum cryptography should be easier to develop, deploy and maintain, have lower lifecycle support costs, and have better understood security threats than QKD-based solutions.*”

*From Quantum Key Distribution – A CESG Whitepaper
Published: February 2016*



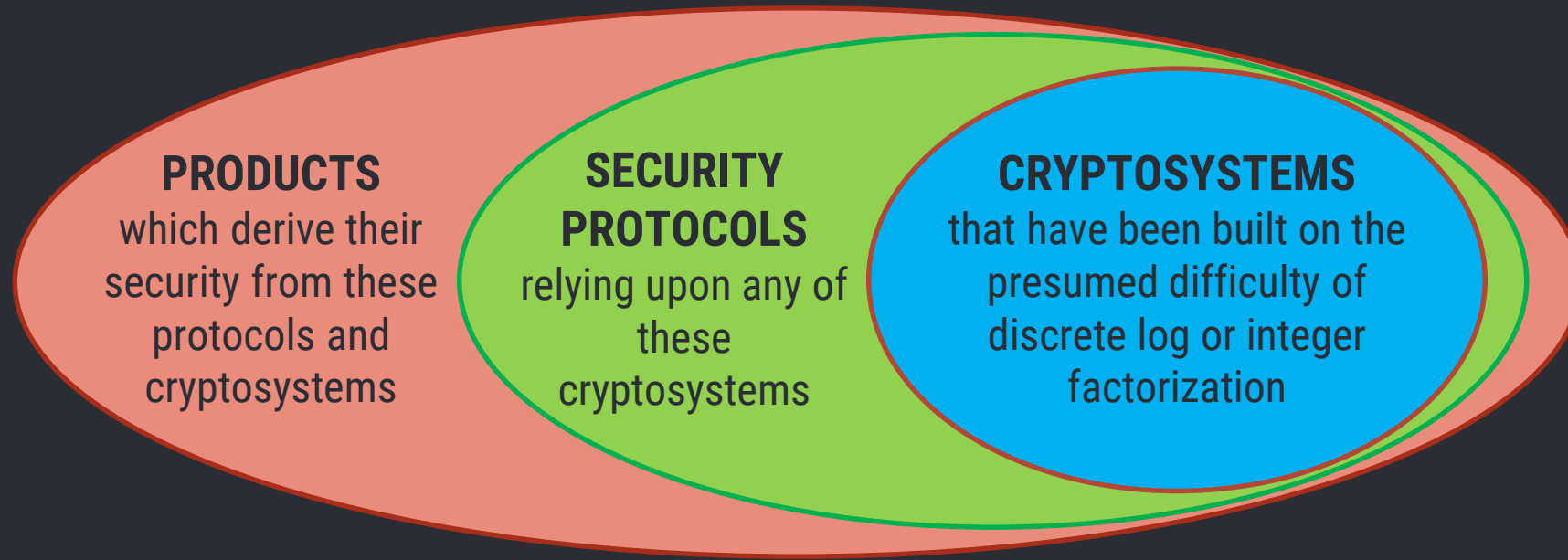
What needs to be protected today?

Any encrypted data where key establishment is communicated or stored along with it will not remain confidential beyond Y2Q.

Any digital documents signed today that must maintain their authenticity beyond Y2Q.

Any signed software that needs to remain authentic at crossover point.

So, What Is Vulnerable?

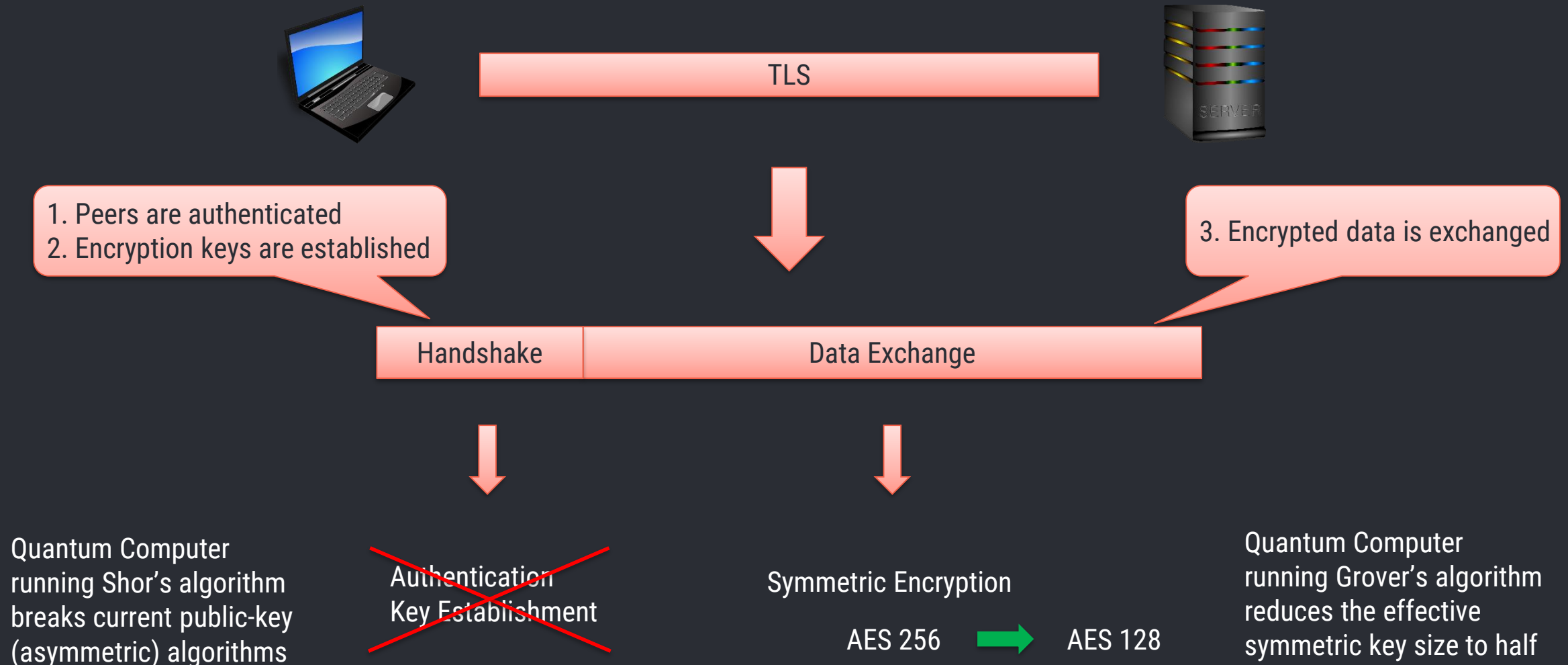


This is the case for anything that is encrypted after a large-scale quantum computer has been built, anything we encrypt today, and anything we encrypted in the past!

Why Can't We Just Make Longer Keys?

Algorithm	Key Length	Classical Bit Strength	Quantum Bit Strength
RSA 1024	1024 bits	80 bits	0 bits
RSA 2048	2048 bits	112 bits	0 bits
ECC 256	256 bits	128 bits	0 bits
ECC 521	521 bits	256 bits	0 bits
AES 128	128 bits	128 bits	64 bits
AES 256	256 bits	256 bits	128 bits
SHA 256	256 bits	256 bits	128 bits

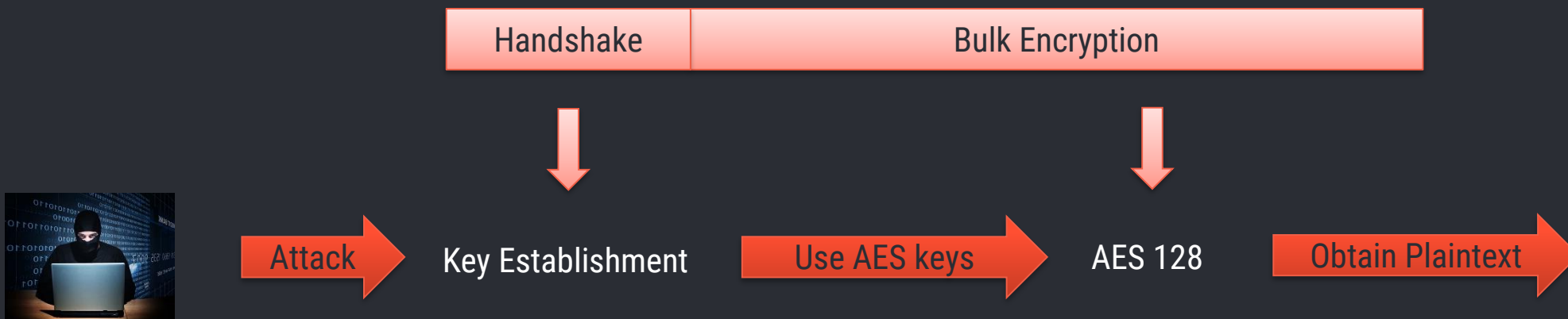
Example: How is TLS vulnerable?



Harvest & Decrypt: How Does it Work?

Communication session is intercepted and saved for later analysis when quantum computers are available.

Quantum computer running Shor's algorithm is used to attack the key establishment algorithm to obtain the symmetric encryption keys which are then used to decrypt the data.



Key Establishment: Deployment Options

Quantum-resistant algorithms can be used as a straight drop-in replacement for classic key agreement algorithms like DH.

Although the mathematics behind many new algorithms is well-studied, there is a concern about using them before NIST standardization.

As an alternative to straight drop-in replacement, new key agreement algorithms can be used in a hybrid mode.

In a hybrid mode, the peers establish a classic secret based on DH and a quantum-resistant secret (say, based on New Hope), and the two shared secrets are XOR'd before being used in a key derivation.

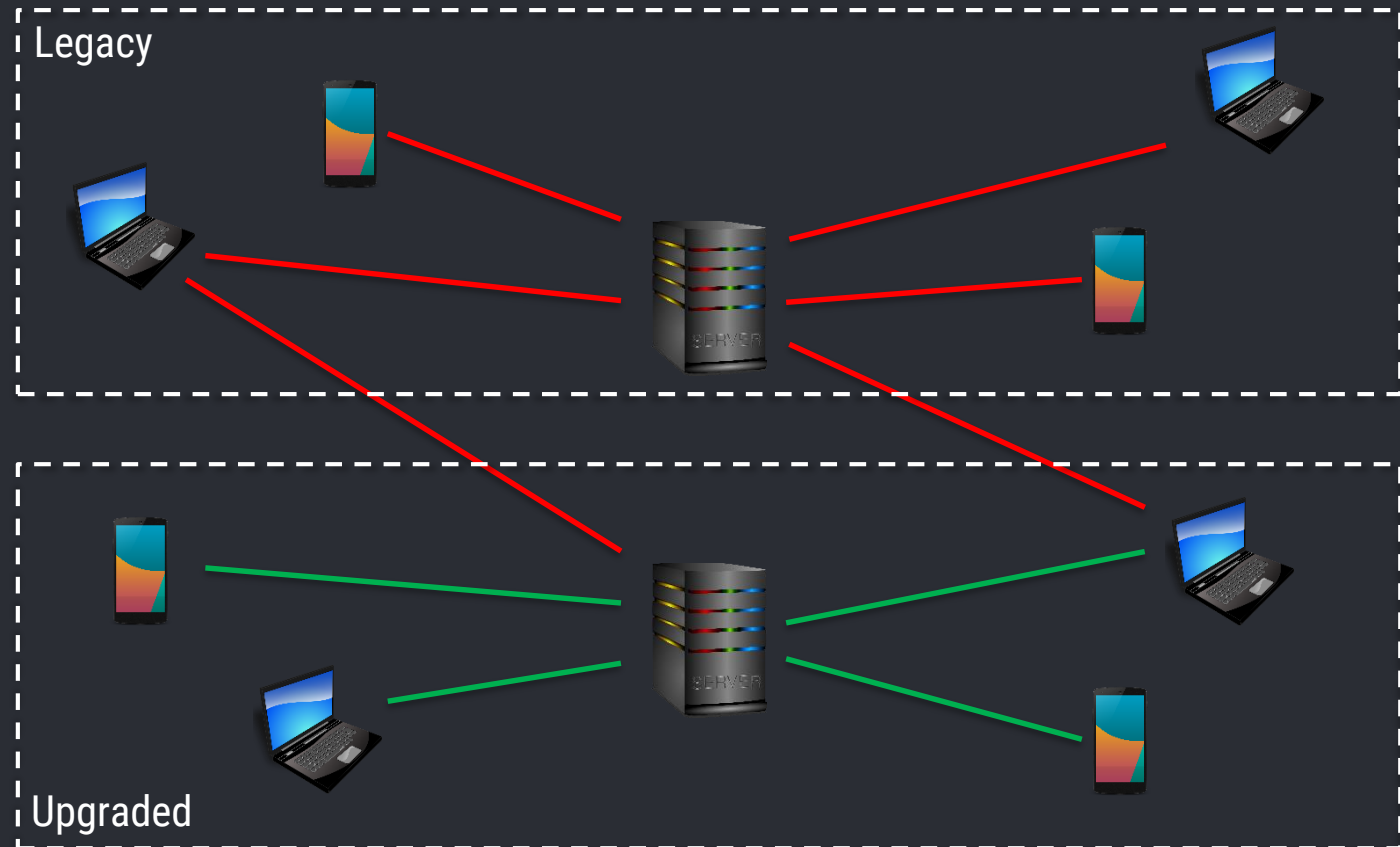
Key Establishment: Deployment Options

Moderate deployment effort with a phased deployment possible.

Timeline: 2 - 3 years.

Classic
Connection

Quantum-Safe
Connection



Authentication: Deployment Options

Complex deployment effort with a parallel deployment possible.

Phased deployment possible using emerging solutions.

Timeline: 3 - 5 years.



Quantum Safe Cryptography Solutions

Quantum Resistant Cryptography



- **Hash:** Signature
- **Lattice:** Encryption, Signature, Key Exchange
- **Error Correcting Code:** Encryption, Signature
- **Isogeny:** Encryption, Signature, Key Exchange
- **Multivariate:** Encryption, Signature



Hash-Based Signatures

“One-Time Signatures”

Very large private keys, small public key

Introduced by Merkle in 1979

Fast signing and verifying

Stateful



Merkle Trees

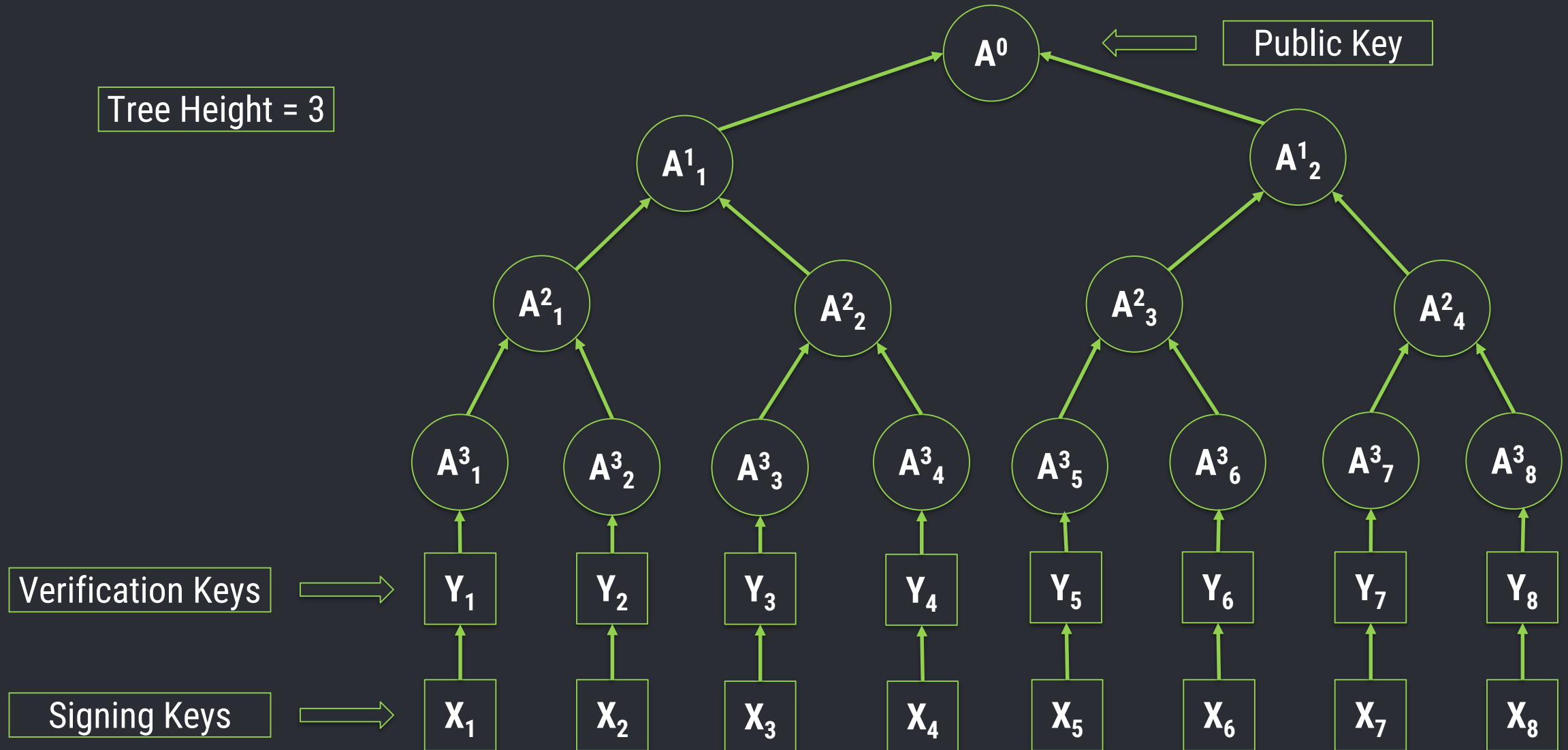


Leighton-Micali Signatures (LMS)

SPHINCS

eXtended Merkle Signature Scheme (XMSS)

Merkle Tree



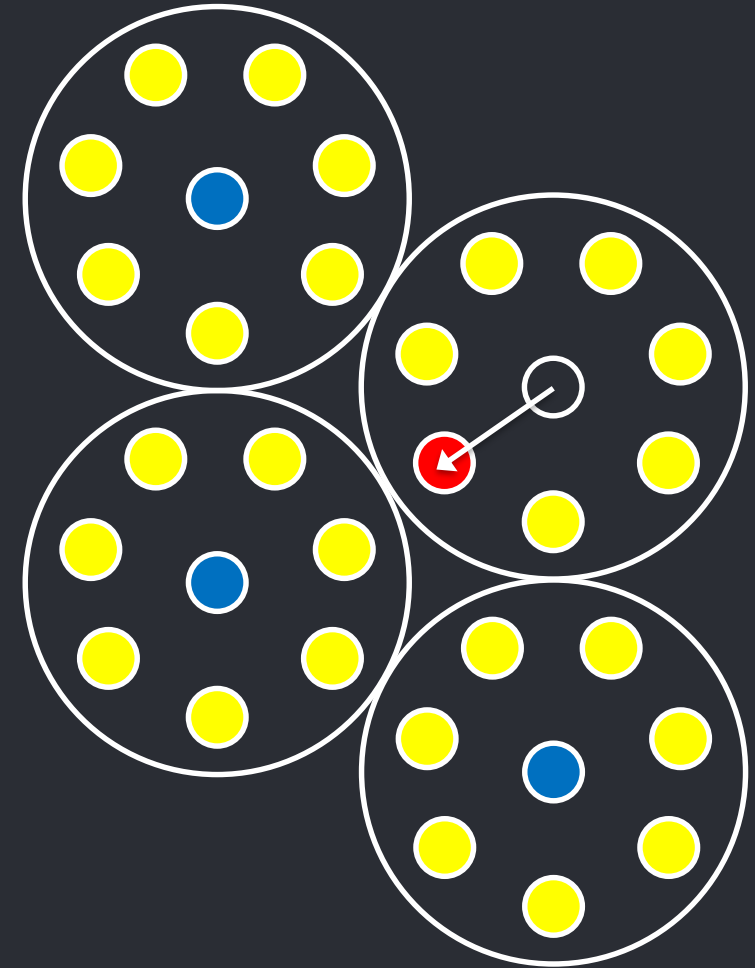
Code-Based Encryption

Introduced by McEliece in 1978

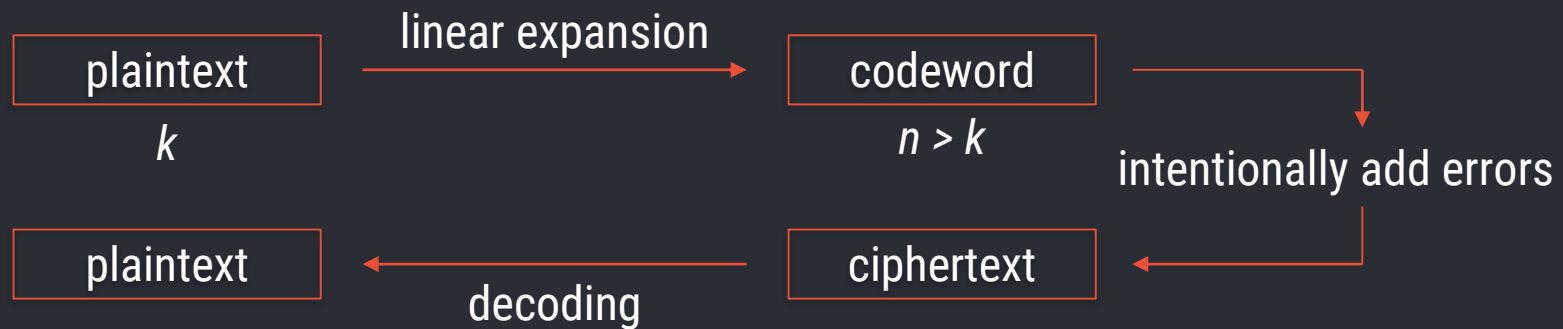
Relies on hardness of decoding unknown codes

Very large public keys

Fast encryption and decryption



Code-Based Encryption



Code-Based Encryption

McEliece with Goppa Codes

Quasi-cycle Medium Density Parity Check (QC-MDPC)

McBits

Neidereitter

Code-Based Encryption

Let G be a $k \times n$ generator matrix of code C , for which there is an efficient algorithm Dec_C that can decode any codeword with up to t errors. Let S be a random non-singular $k \times k$ matrix, and let P be a random $n \times n$ permutation matrix.

(Generalized) McEliece cryptosystem (MECS) is defined as follows:

Secret Key: (Dec_C, S, P)

Public Key: $(G' = S \cdot G \cdot P)$

Encryption: Let m be a k -bit message, and let e be a random n -bit vector with $w_H(e) \leq t$. Then $c = m \cdot G' + e$ is a ciphertext.

Decryption: Decryption is given by the following algorithm:

$$1: c' \leftarrow c \cdot P^{-1}$$

$$2: m' \leftarrow Dec_C(c')$$

$$3: m \leftarrow m' \cdot S^{-1}$$

Lattice Cryptography

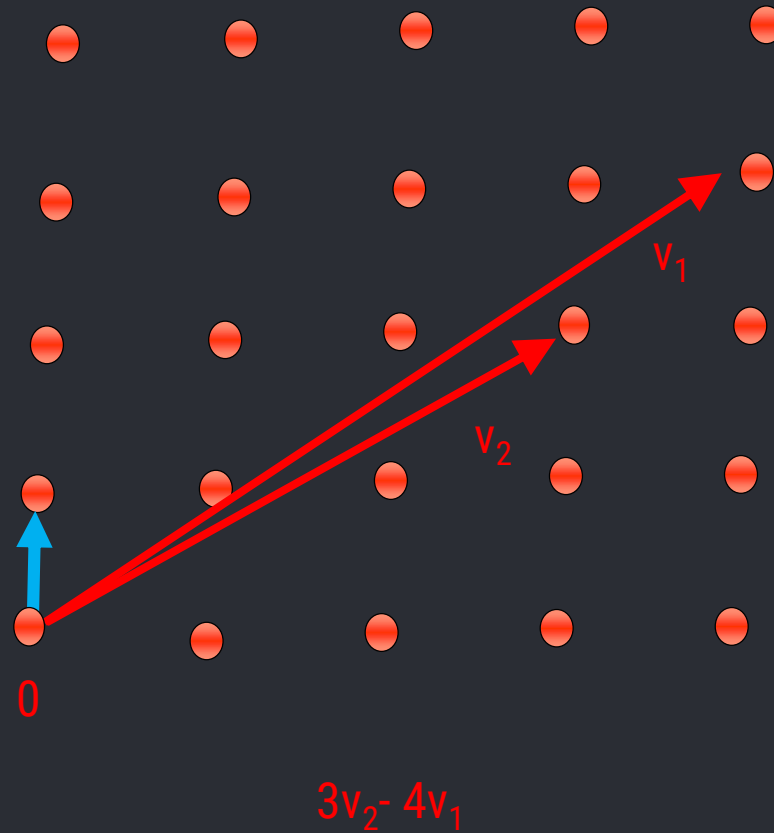
First commercial version was NTRU (1996)

Hard Problems

- Shortest Integer Solution (SIS)
 - Short Integer Solution (SIS):
 - Given: $A = (a_1, \dots, a_m) \in \mathbb{Z}_q^{n \times m}$, $a_i \in \mathbb{Z}_q^n$
 - Goal: Find $x \in \mathbb{Z}_q^m$ with $|x| \leq \beta$ such that $Ax = 0 \pmod{q}$
- Learning With Errors (LWE)
 - Let X be some error distribution on \mathbb{Z}_q
 - Given: $A = (a_1, \dots, a_m)^T \in \mathbb{Z}_q^{m \times n}$, $a_i \in \mathbb{Z}_q^n$ and $b = As + e \pmod{q}$ with $s \in \mathbb{Z}_q^n$, $e \leftarrow X_m$
 - Goal: Find s

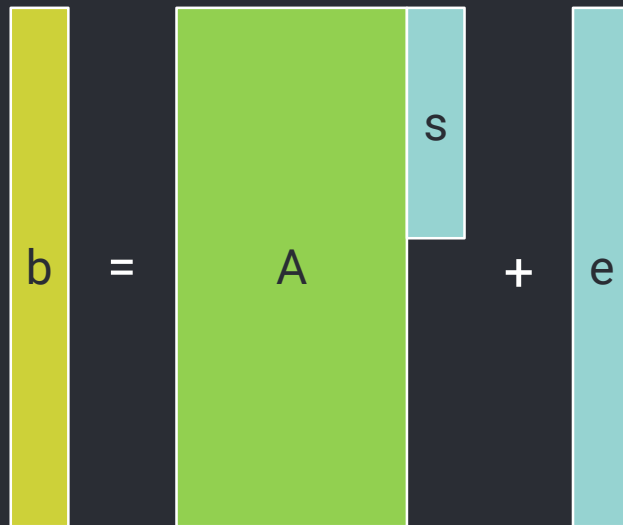
Competitive key sizes and fast operations

Lattice Cryptography



Lattice Cryptography

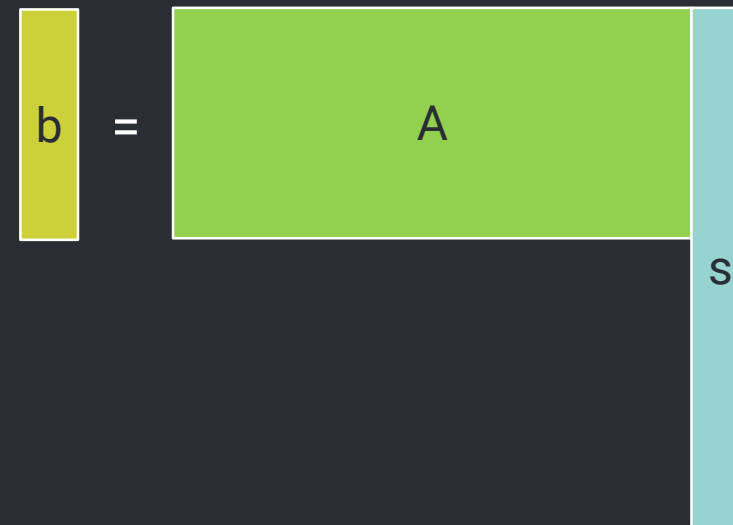
LWE



The diagram illustrates the Learning With Errors (LWE) equation. On the left is a yellow vertical rectangle labeled b . To its right is an equals sign. Next is a green rectangle labeled A , followed by a light blue vertical rectangle labeled s . To the right of these is a plus sign, followed by another light blue vertical rectangle labeled e .

$$b = [A \mid s] + e$$

SIS



The diagram illustrates the Short Integer Solution (SIS) equation. On the left is a yellow vertical rectangle labeled b . To its right is an equals sign. Next is a green rectangle labeled A , followed by a light blue vertical rectangle labeled s .

$$b = [A \mid s]$$

Lattice Cryptography

Key Exchange

- NTRU (SIS)
- New Hope (R-LWE)
- Frodo (LWE)

Signatures

- BLISS (SIS)
- Ring-TESLA (R-LWE)

Lattice Cryptography

Parameters: $q = 12289 < 2^{14}, n = 1024$

Error Distribution: ψ_{16}

Alice (server)

$seed \xleftarrow{\$} \{0,1\}^{256}$

$a \leftarrow \text{Parse}(\text{SHAKE} - 128(\text{seed}))$

$s, e^{\$} \leftarrow \psi_{16}^n$

$b \leftarrow as + e \xrightarrow{(b, seed)}$

$v' \leftarrow us \xleftarrow{(u, r)}$

$v \leftarrow \text{Rec}(v', r)$

$\mu \leftarrow \text{SHA3} - 256(v)$

Bob (client)

$s', e', e'' \xleftarrow{\$} \psi_{16}^n$

$a \leftarrow \text{Parse}(\text{SHAKE} - 128(\text{seed}))$

$u \leftarrow as' + e'$

$v \leftarrow bs' + e''$

$r \xleftarrow{\$} \text{HelpRec}(v)$

$v \leftarrow \text{Rec}(v, r)$

$\mu \leftarrow \text{SHA3} - 256(v)$

Isogeny-Based Cryptography

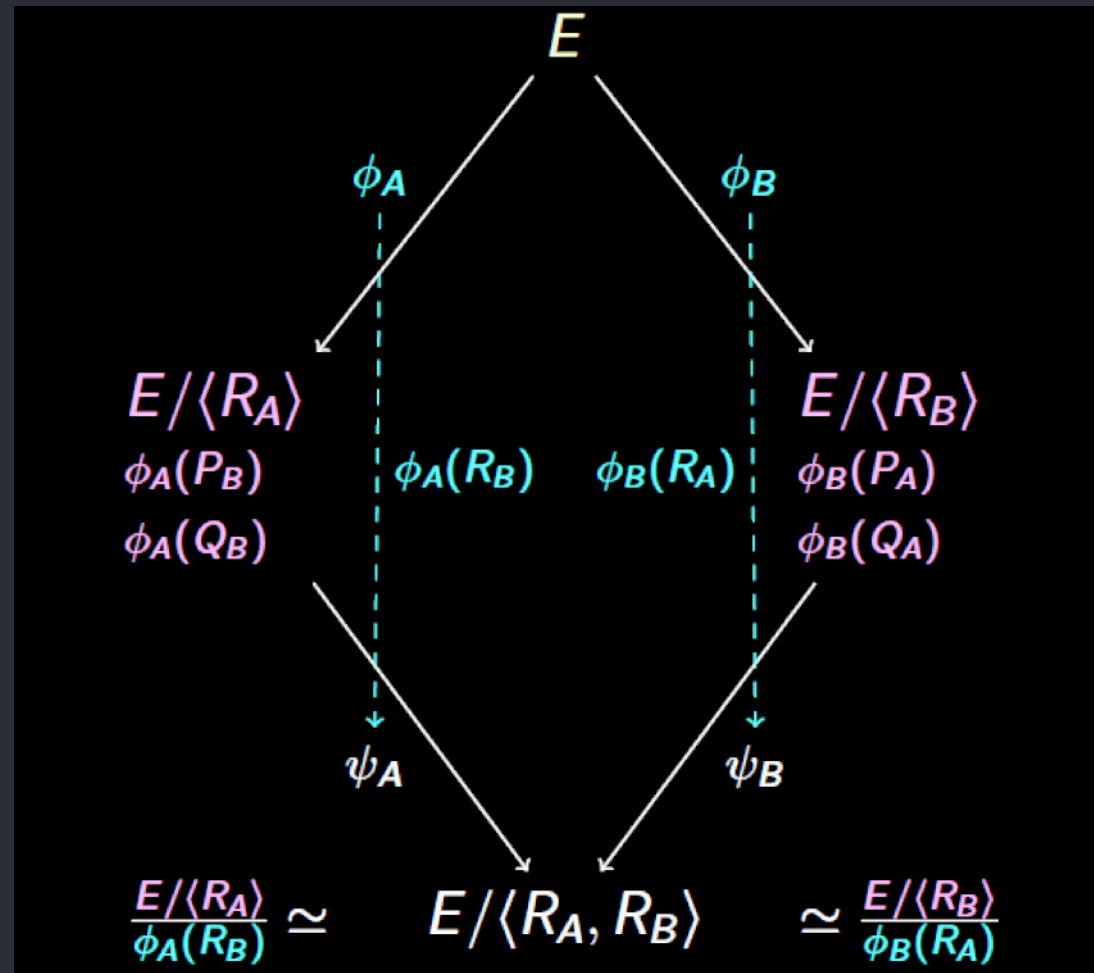
Introduced by Jao in 2009

Relies on difficulty of finding isogenies (mappings) between Elliptic Curves

Competitive key sizes

Efficient encryption and decryption

Isogeny-Based Cryptography



Isogeny-Based Cryptography

Key Exchange

- Jao, De Feo, Plut
- Supersingular Isogeny Diffie Hellman (SIDH) - Costello, Longa, Naehrig

Signature

- Some early constructions using zero knowledge ideas

Multivariate Public Key Cryptography

Introduced by Matsumoto and Imai in 1988

- Based on the fact that solving n randomly chosen (non-linear) equations in n variables is NP-complete

Can be formulated into signatures, key exchange and key transport

Often trade offs between key size and public/private key operation speeds

Multivariate Public Key Cryptography

The public key is given as:

$$G(x_1, \dots, x_n) = (G_1(x_1, \dots, x_n), \dots, G_m(x_1, \dots, x_n)).$$

Here the $G(x_1, \dots, x_n)$ are multivariate polynomials over a finite field.

Multivariate Public Key Cryptography

Any plaintext $M = (x'_1, \dots, x'_n)$ has the ciphertext:

$$G(M) = G(x'_1, \dots, x'_n) = (y'_1, \dots, y'_m).$$

To decrypt the ciphertext (y'_1, \dots, y'_m) , one needs to know a secret (**the secret key**), so that one can invert the map: G^{-1} to find the plaintext (x'_1, \dots, x'_n) .

$$M = (x'_1, \dots, x'_n) = G^{-1}(y'_1, \dots, y'_m).$$

Multivariate Public Key Cryptography

Simple Matrix

- Encryption

Hidden Field Equations - HFE(+,-,v)

- Encryption and Signatures

Unbalanced Oil and Vinegar (UOV)

- Signatures

Rainbow

- Signatures

Quantum Computing Standards



Why standardize?

Standardization is needed for cryptographic systems for the same reason it was needed for wireless systems to be deployed on an extremely large scale.

Challenges to Quantum-Safe Security

It takes several years of cryptanalysis for cryptographers to gain confidence in the security of new algorithms.

Some network security protocols may be too rigid to accommodate the increased key lengths or changes in ciphers required to make them quantum-safe.

New standards for protocols are needed.

Many people perceive quantum-safe cryptography as “not urgent,” despite the lead times required to analyze new cryptosystems and implement them in security protocols and products.

“Based on experience in deploying Suite B, we have determined to start planning and communicating early about the upcoming transition to quantum resistant algorithms.[...]For those partners and vendors that have not yet made the transition to Suite B elliptic curve algorithms, we recommend not making a significant expenditure to do so at this point but instead to prepare for the upcoming quantum resistant algorithm transition.”

From NSA website, August 2015



NIST Timeline



Fall 2016: Formal call for quantum-resistant public key crypto standards

November, 2017: Deadline for submissions

3-5 years later: Analysis phase

2 years later: Draft standards ready

ETSI



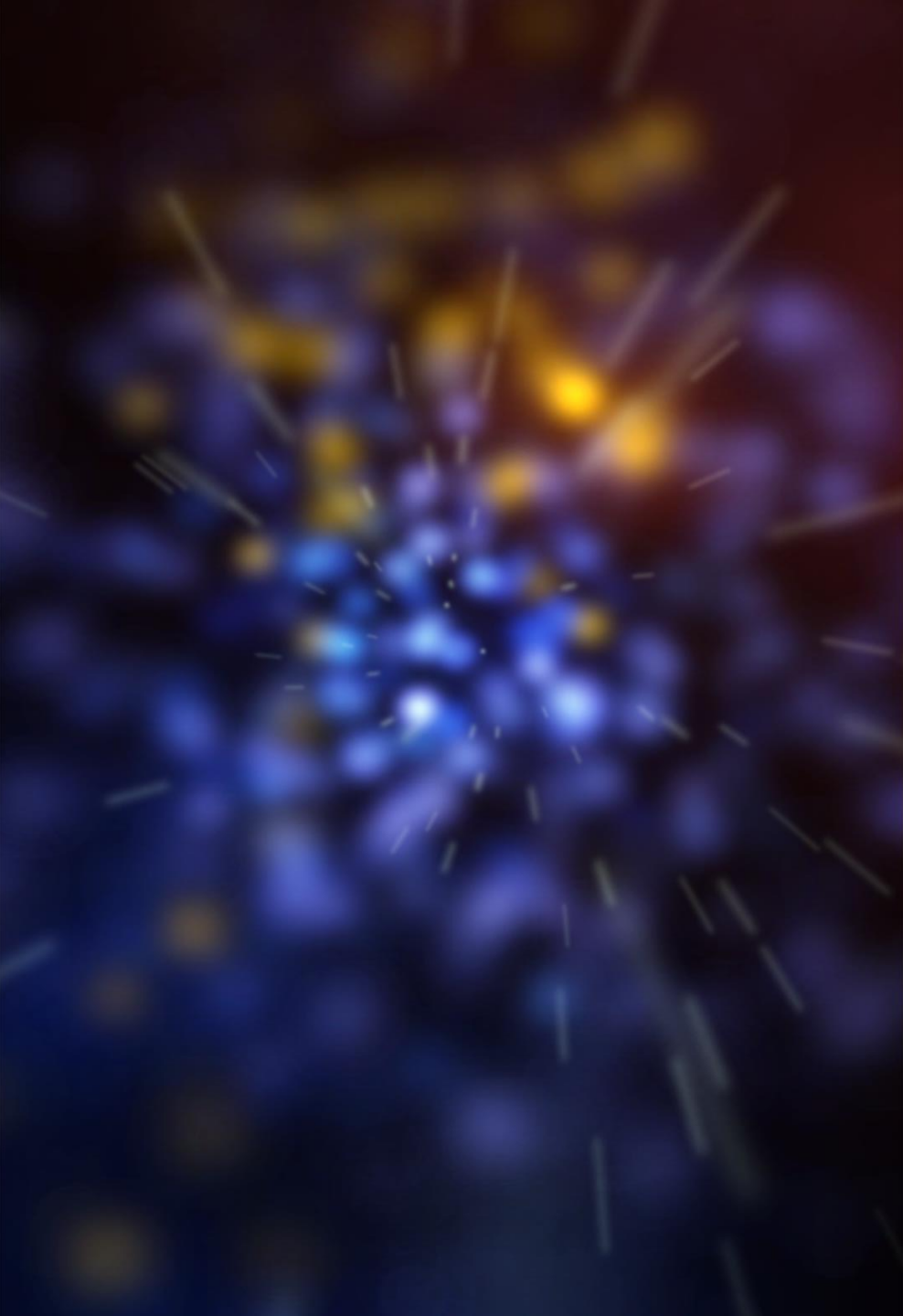
European Telecommunications Standards Institute

Industry Specifications Groups

- Quantum Safe Cryptography (QSC)
- Quantum Key Distribution (QKD)

Focus on practical implementation of quantum safe primitives

- performance considerations
- implementation capabilities
- benchmarking
- practical architectural considerations



Quantum Computing Conclusions

When Does The Clock Run Out?

While this seems enormous, its like drinking the ocean...

We do have viable solutions today and more are coming.

Start planning your transition today!

UNIVERSITY OF
WATERLOO

- science
- mathematics
- computer science
- engineering
- philosophy

LAURIER 
Innovation &
Entrepreneurship
MBA

accelerator  centre®

INRS
Université d'avant-garde

**Venture Capital
Funds**

New Start-ups

PRIVATE
PHILANTHROPY

EXPERIMENTATION

IQC

PI

BASIC RESEARCH

**Quantum Valley
Investments**

COMMERCIALIZATION

PRIVATE SECTOR

Canada 
 **Ontario**


SUPPORT & SUSTAINABILITY

 **WATERLOO INSTITUTE FOR
nanotechnology**


Region of Waterloo

THE CITY OF
Waterloo


KITCHENER


**CANADA
CAMBRIDGE**
It's all right here

COMMUNITECH



Thank you!



www.isara.com



mike@isara.com