Challenges and Opportunities from Quantum-Safe Cryptography

Tjerand Silde, PONE Biometrics

PONE
BIOMETRICS

Introduction

Associate Professor in Cryptology at NTNU

Working on quantum-safe cryptography and privacy

Security and Cryptography Expert at Pone Biometrics

Teaching a course on “Secure Cryptographic Implementations”

Working on FIDO, secure authentication, biometrics

Supervising master’s and PhD students in cryptography

Outline

Cryptography today

Quantum computing

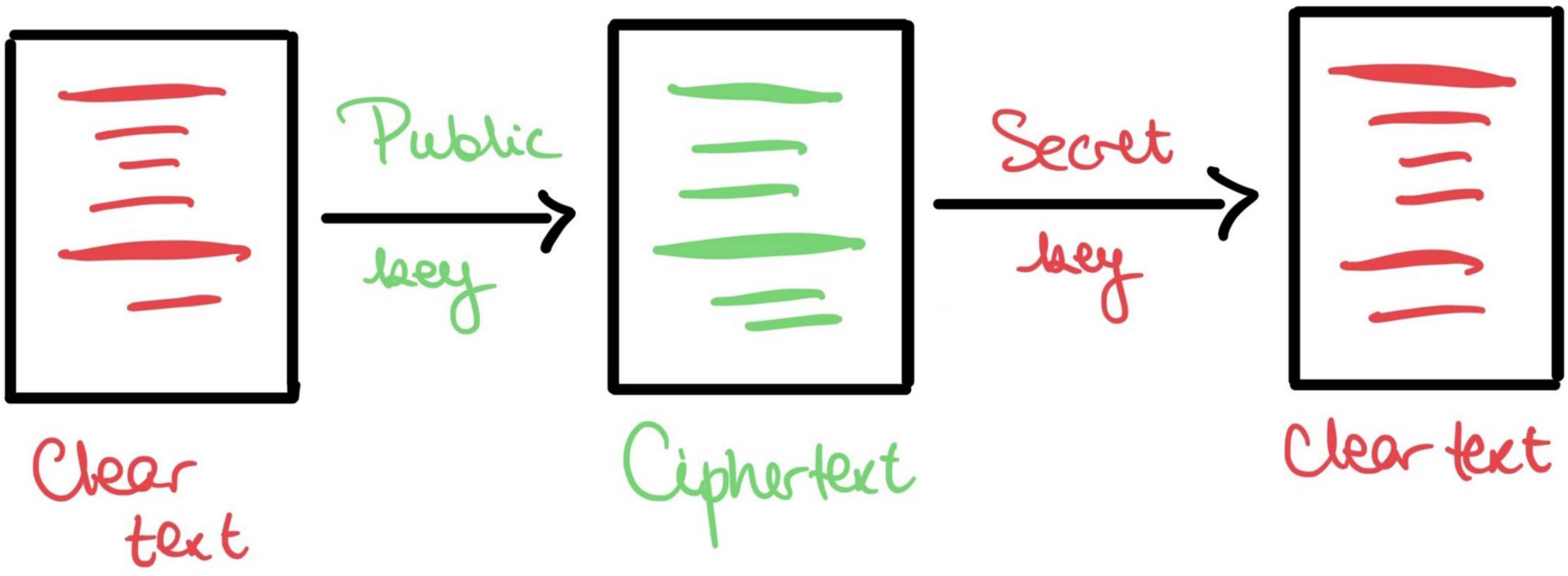
Quantum-safe cryptography

"Store now, decrypt later"

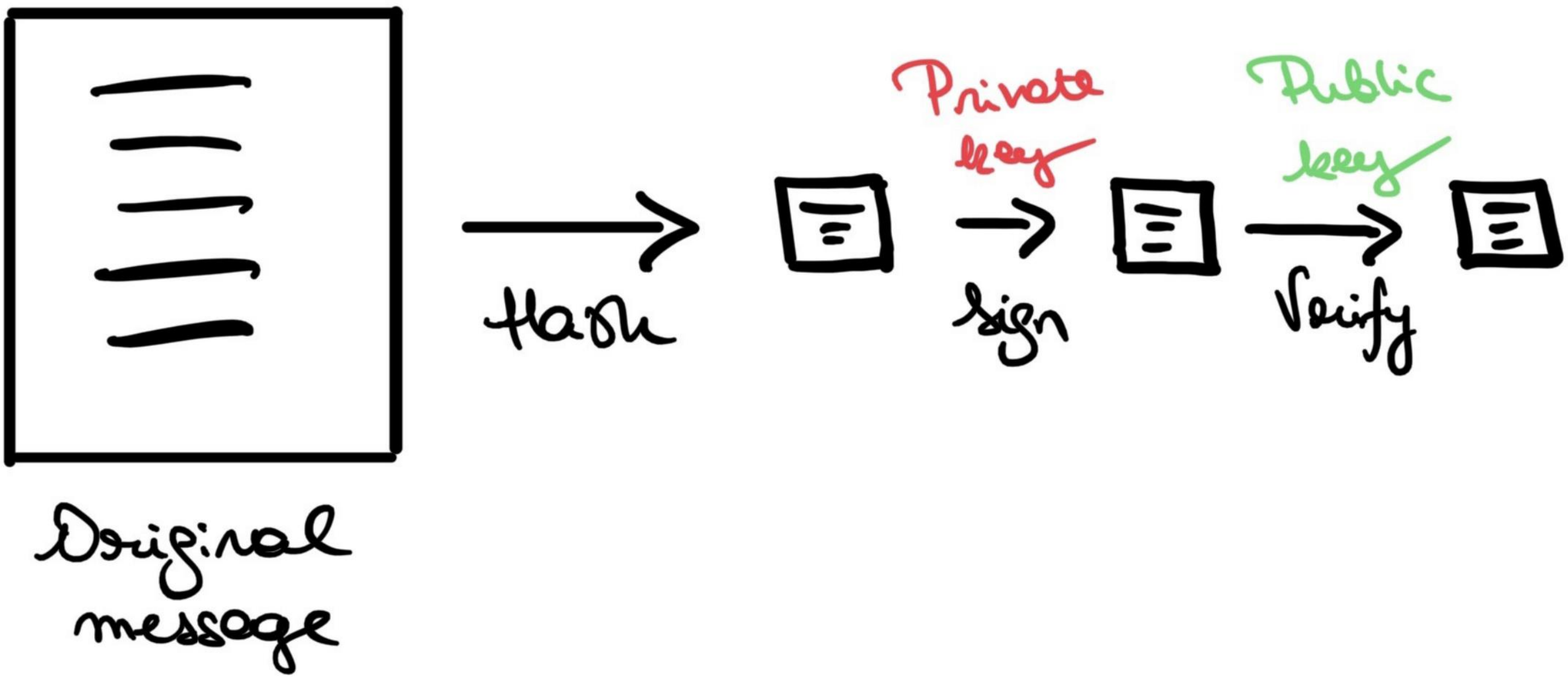
Challenges with PQC

Opportunities with PQC

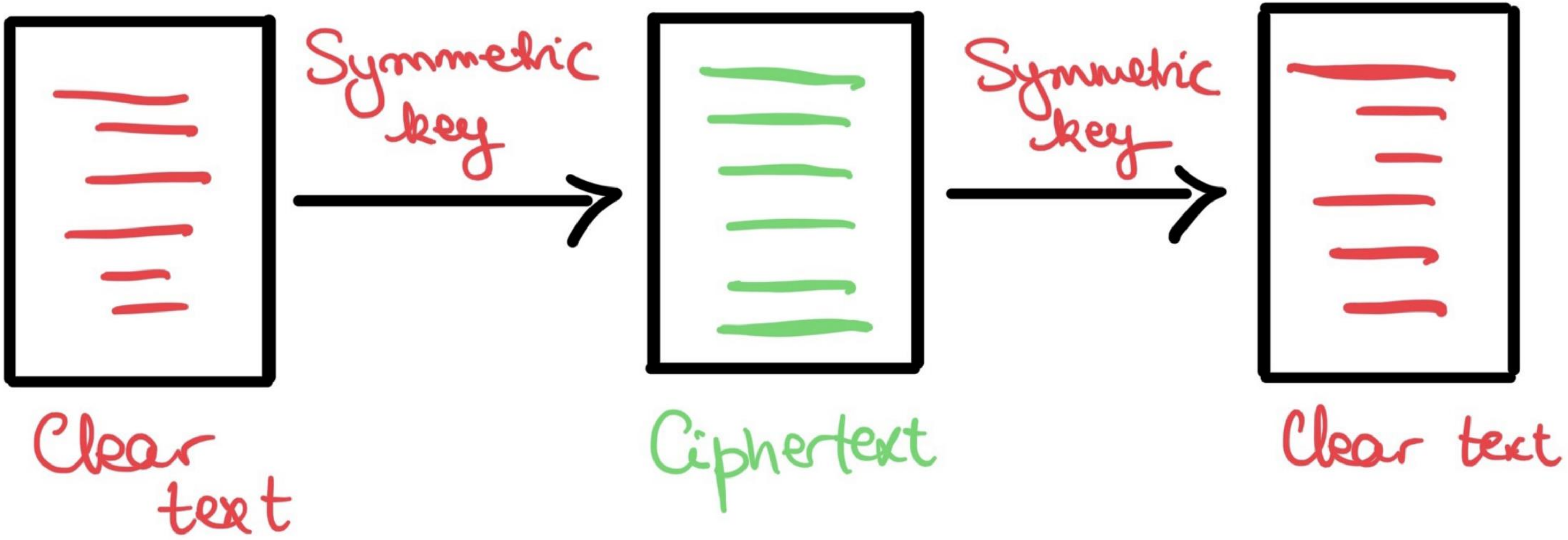
Cryptography Today – Public Key Enc



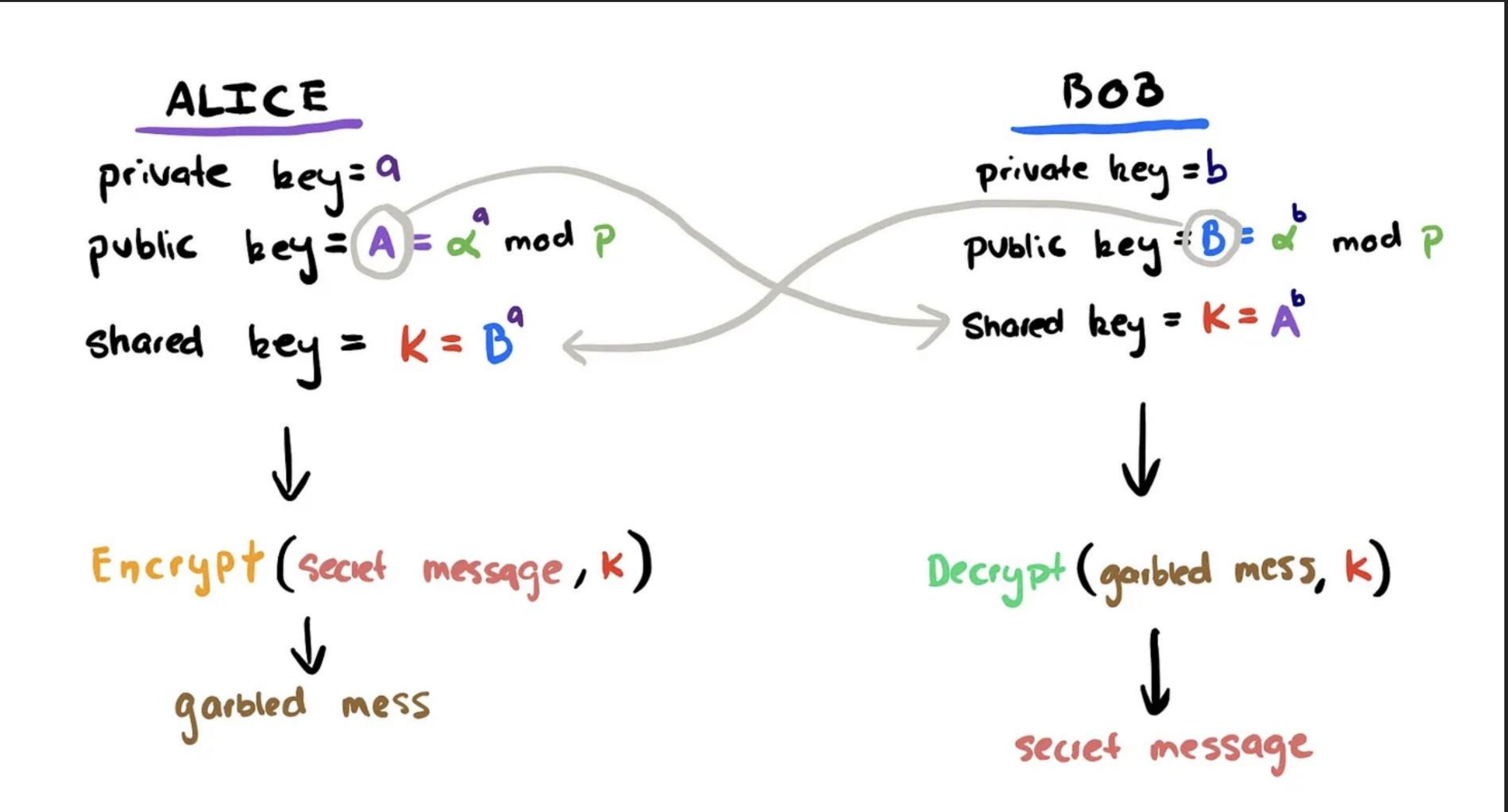
Cryptography Today – Digital Signatures



Cryptography Today – Symmetric Key



Cryptography Today – DH + AES



Cryptography Today - Algorithms

RSA Encryption and Signatures,
(EC) Diffie-Hellman Key Exchange,
(EC) Digital Signature Algorithm,
(EC) ElGamal Encryption, Pairings.

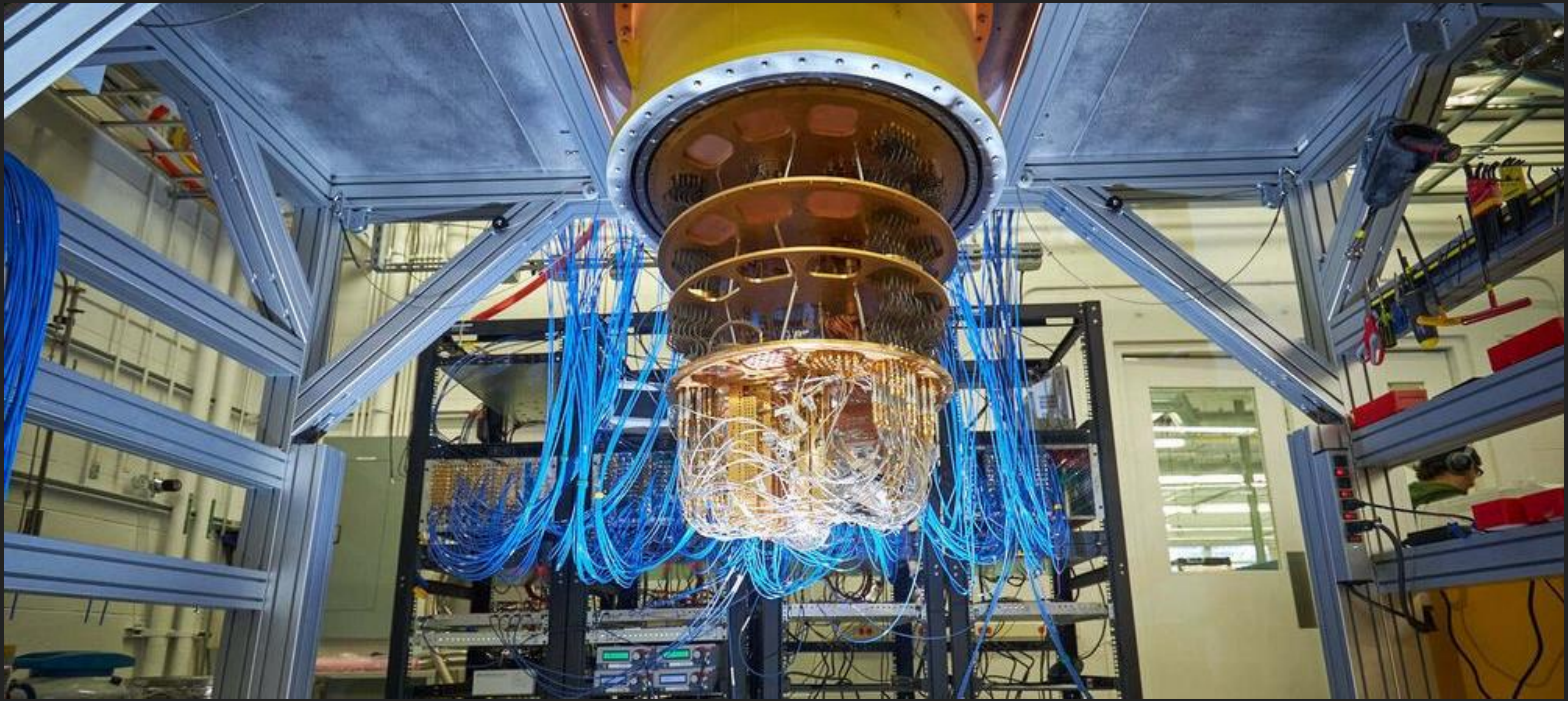
Symmetric encryption like AES,
Hash functions like SHA2/3,
MAC schemes like HMAC.

Cryptography Today - Use Cases

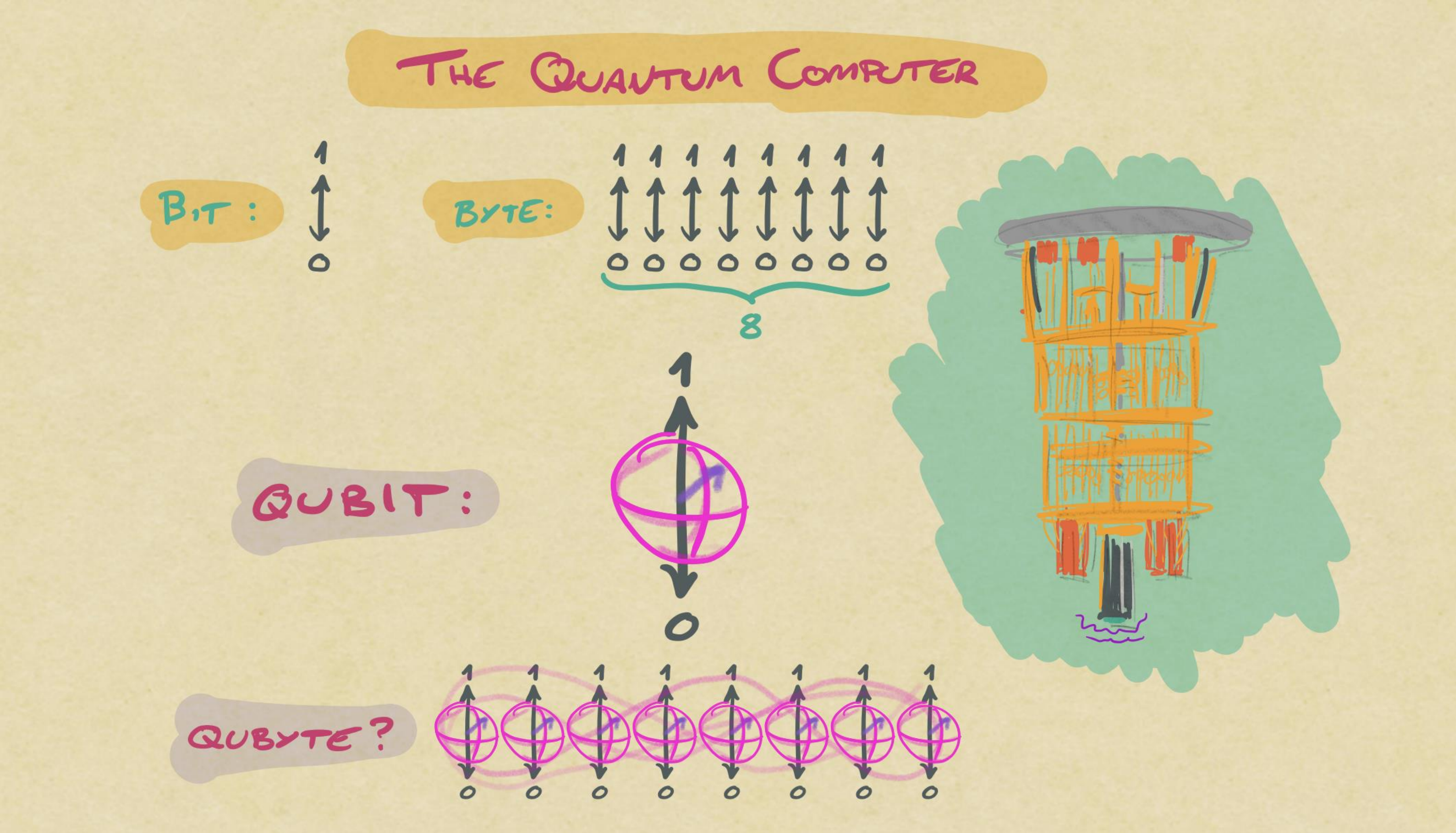
Secure messaging:	Signal, WhatsApp, iMessage
Secure connections:	TLS, SSH, IPsec
Digital authentication:	FIDO, Bank ID, Buypass ID
Payments:	Venmo, VISA / Mastercard, Apple / Google Pay, Vipps

Will these protocols be secure in the future?

Tomorrow: Quantum Computers



Quantum Computing



Quantum Algorithms

Shor's Algorithm can be used to efficiently find the periodicity of a function and can be applied to factoring and computing discrete logarithms.

Grover's Algorithm can be used to speed up unstructured search and can be applied to finding symmetric keys and hash collisions.

Cryptography Today - Algorithms

RSA Encryption and Signatures,
(EC) Diffie-Hellman Key Exchange,
(EC) Digital Signature Algorithm,
(EC) ElGamal Encryption, Pairings.

Symmetric encryption like AES,
Hash functions like SHA2/3,
MAC schemes like HMAC.

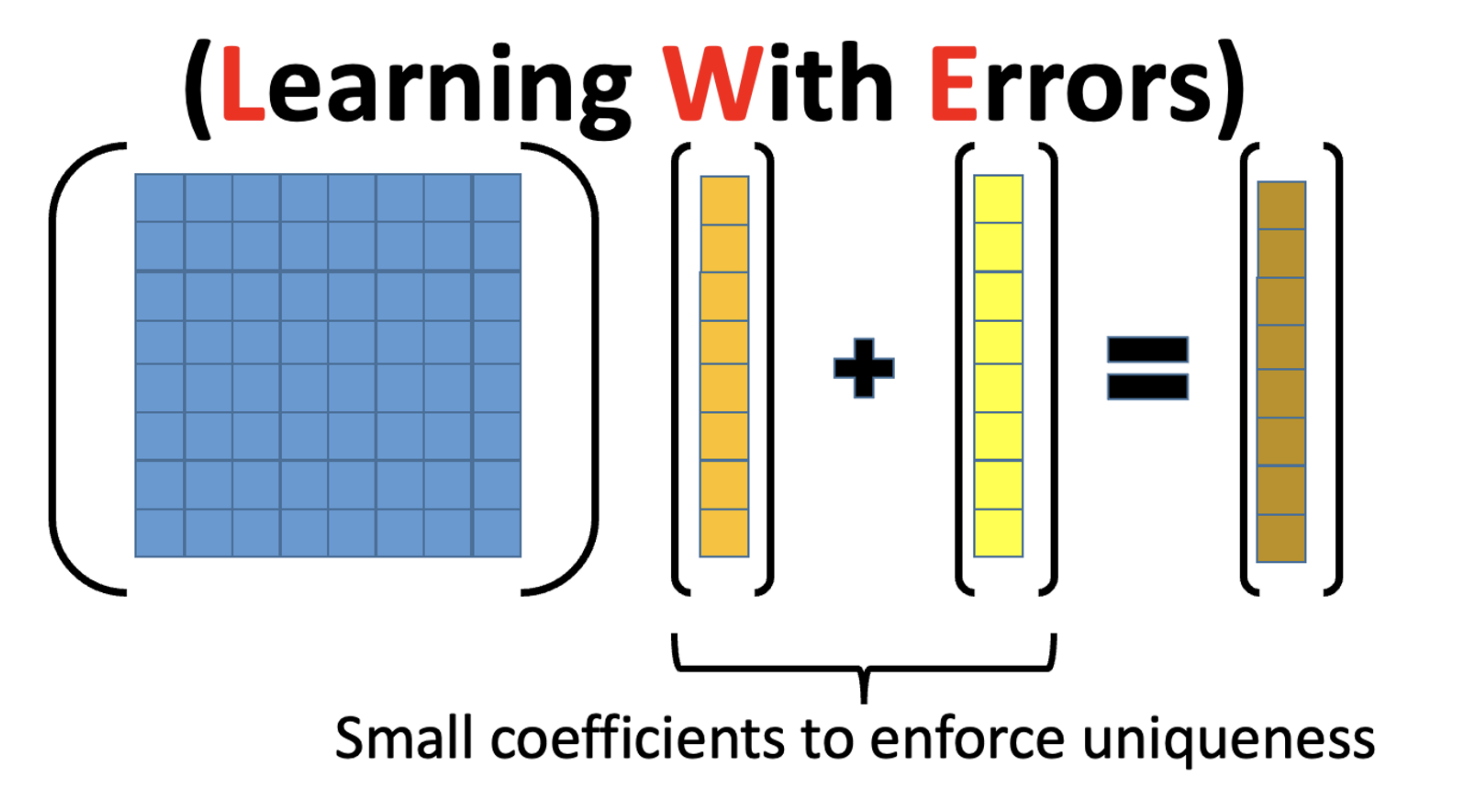
Quantum-Safe Cryptography

Cryptographic algorithms that we run on classical computers

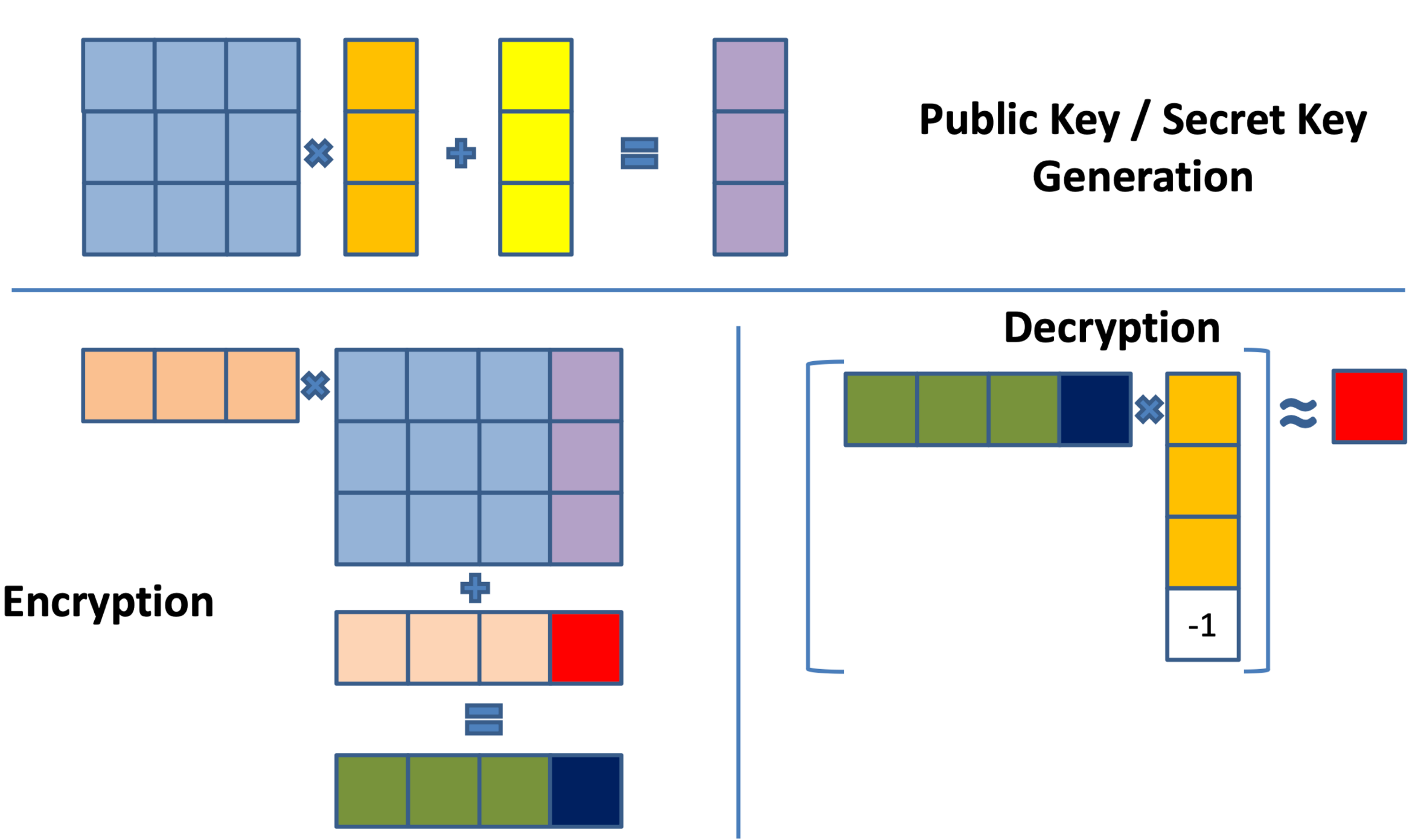
Based on mathematical problems (other than factoring and DLOG) that are hard to break even for quantum computers

For example: lattices, codes, isogenies, symmetric schemes

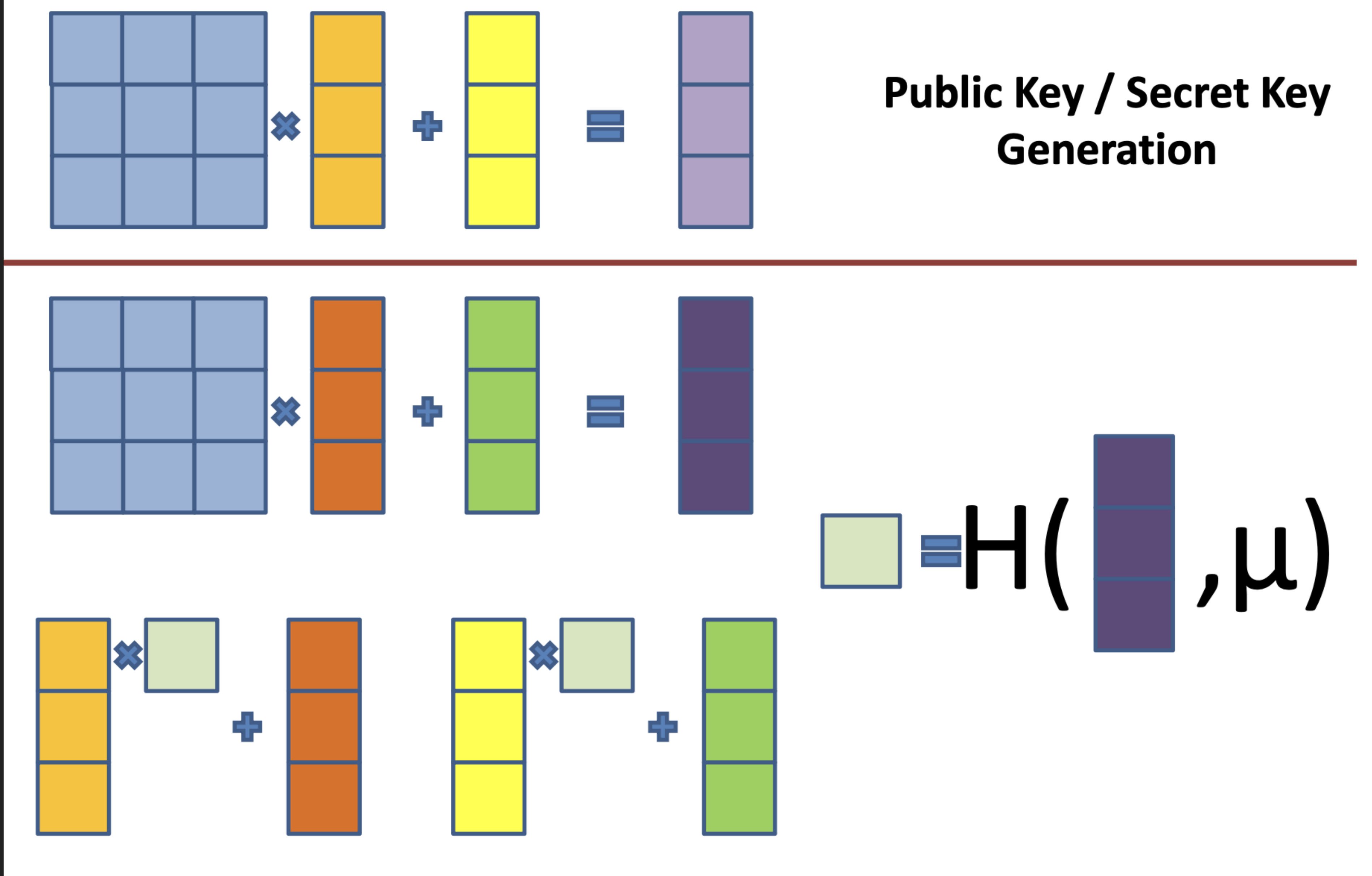
Lattice-Based Cryptography



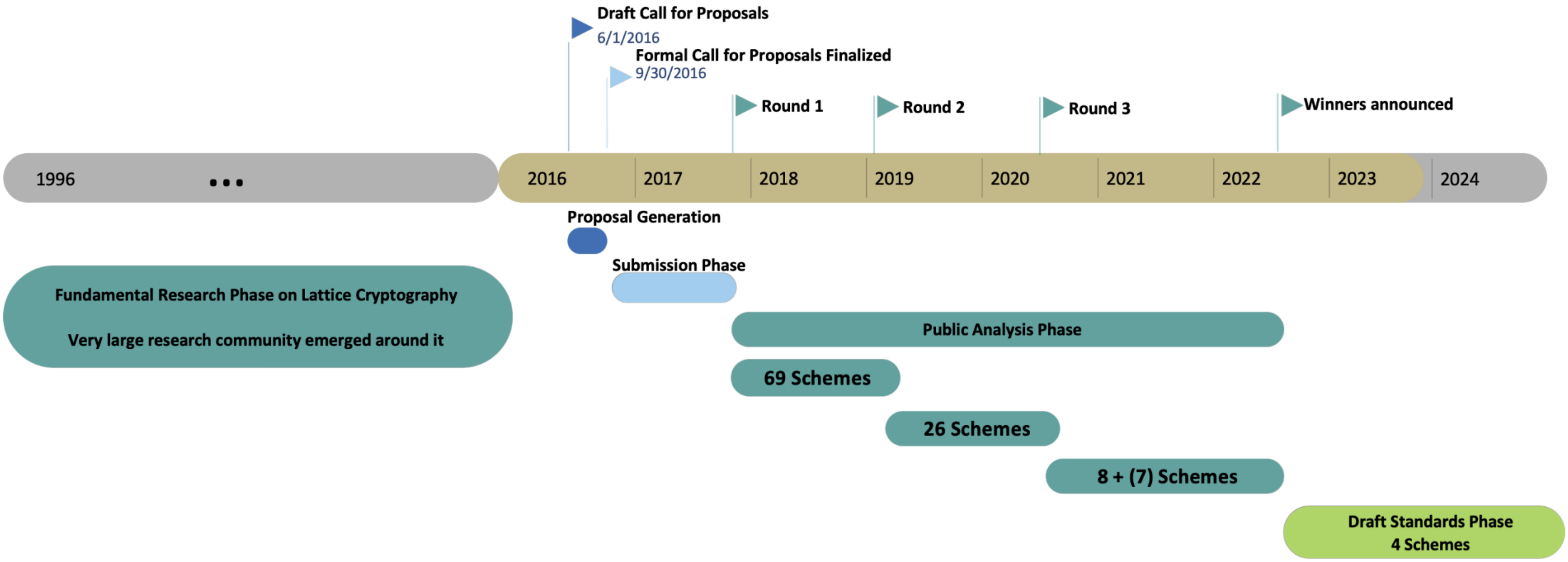
Lattice-Based Encryption



Lattice-Based Signatures



Quantum-Safe Cryptography Timeline



New Cryptographic Standards

FIPS 203

Federal Information Processing Standards Publication

Module-Lattice-Based Key-Encapsulation Mechanism Standard

Category: Computer Security **Subcategory: Cryptography**

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

New Cryptographic Standards

	encapsulation key	decapsulation key	ciphertext	shared secret key
ML-KEM-512	800	1632	768	32
ML-KEM-768	1184	2400	1088	32
ML-KEM-1024	1568	3168	1568	32

Table 3. Sizes (in bytes) of keys and ciphertexts of ML-KEM

nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.203.ipd.pdf

New Cryptographic Standards

FIPS 204

Federal Information Processing Standards Publication

Module-Lattice-Based Digital Signature Standard

Category: Computer Security **Subcategory: Cryptography**

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

New Cryptographic Standards

	Private Key	Public Key	Signature Size
ML-DSA-44	2528	1312	2420
ML-DSA-65	4000	1952	3293
ML-DSA-87	4864	2592	4595

Table 2. Sizes (in bytes) of keys and signatures of ML-DSA.

nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.204.ipd.pdf

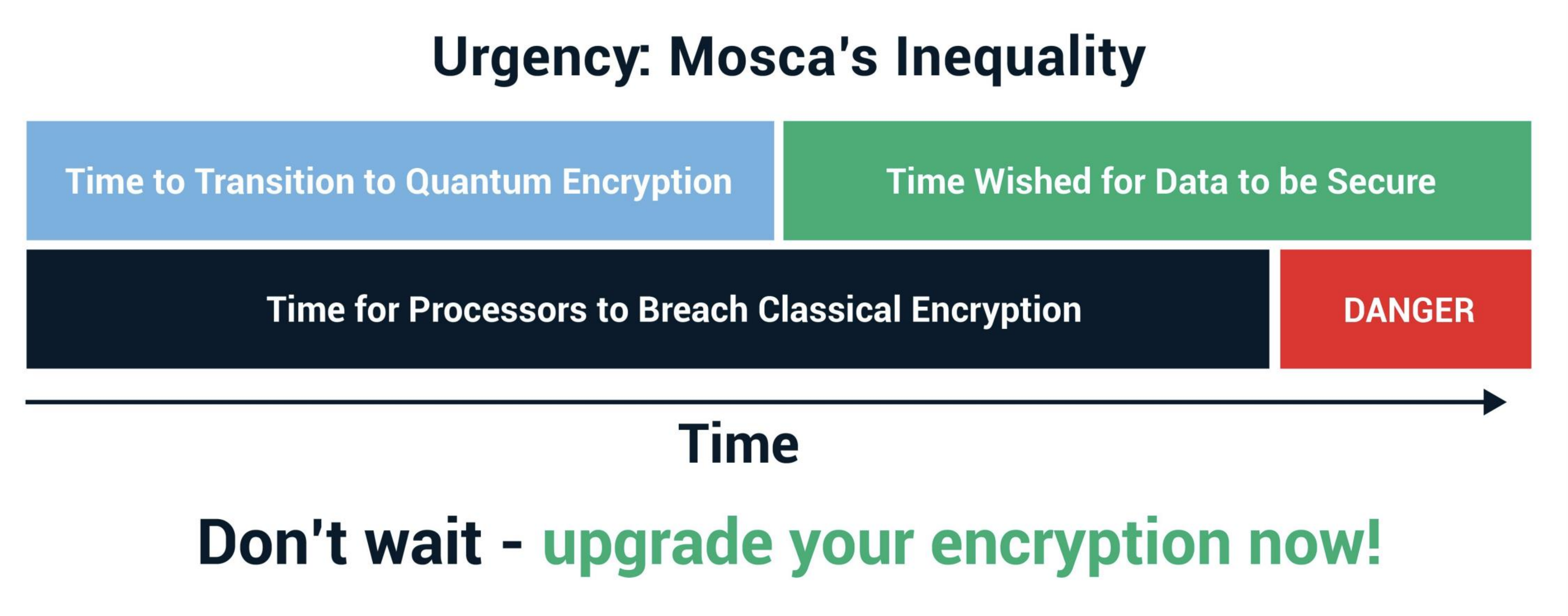
Transition to PQC

NIST Internal Report
NIST IR 8547 ipd

Transition to Post-Quantum Cryptography Standards

https://doi.org/10.6028/NIST.IR.8547.ipd

Why This Matters Today

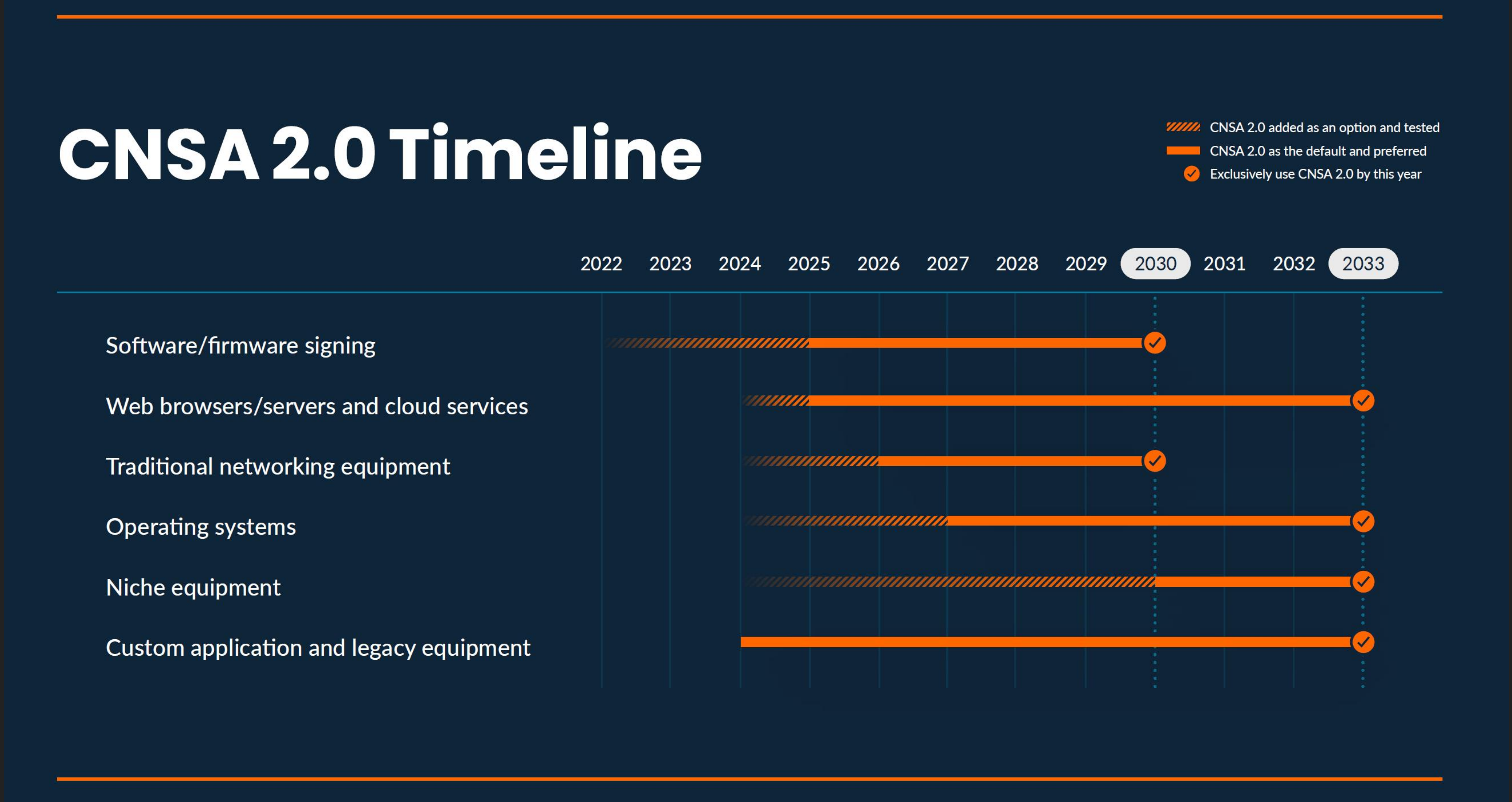


Why This Matters Today


Scott Hanselman
@shanselman
Follow

HTTPS & SSL doesn't mean "trust this." It means "this is private." You may be having a private conversation with Satan.

Quantum-Safe Cryptography Timeline



Hybrid PQC

Are PQC algorithms mature enough to replace all classical algorithms today? Can we implement them securely?

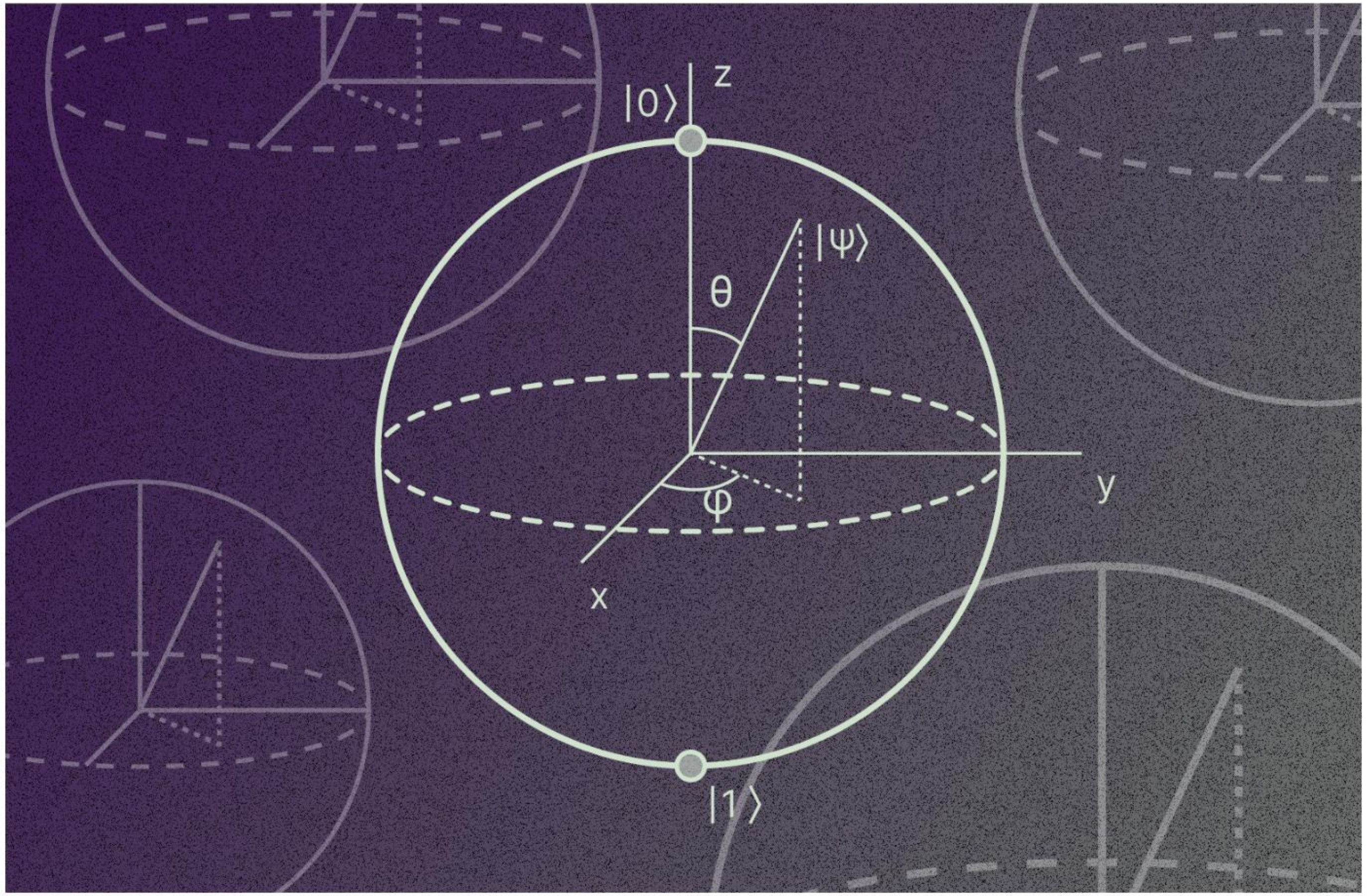
Possible solution: hybrid classical-PQ cryptography.

Enc: Use two schemes for KEX / KEM, encrypt with AES.
Sign: Use two schemes, and both signatures must verify.

Hybrid PQC in Practice

Quantum Resistance and the Signal Protocol

ehrenkret on 19 Sep 2023



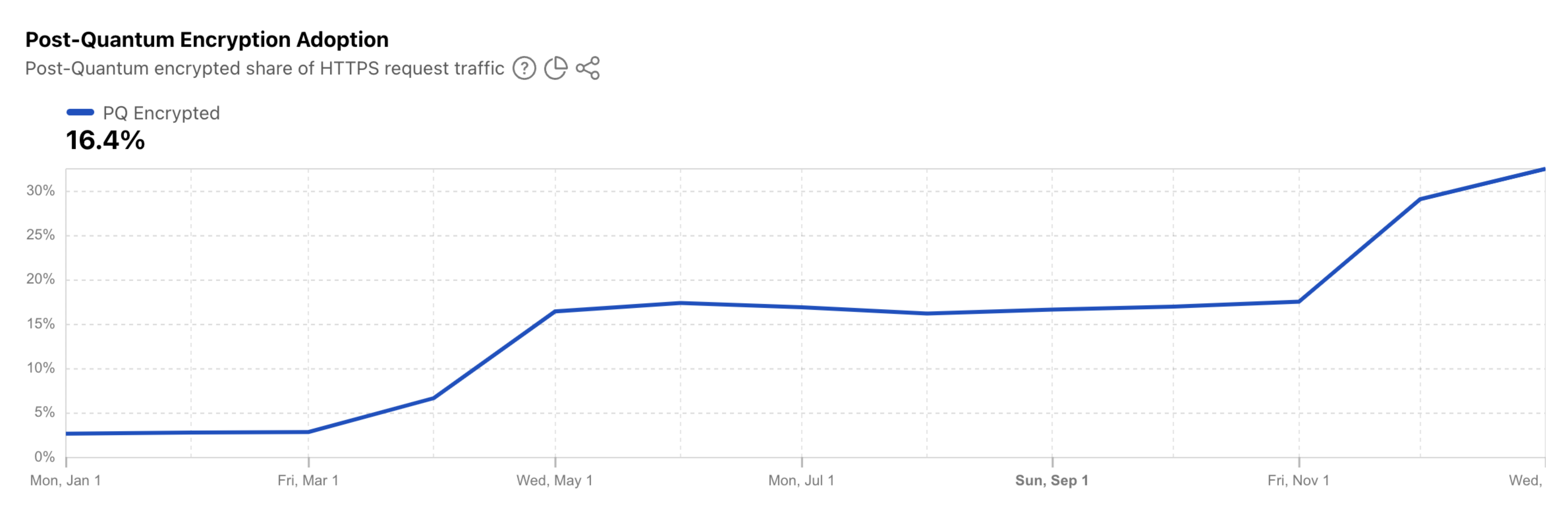
Hybrid PQC in Practice

February 21, 2024

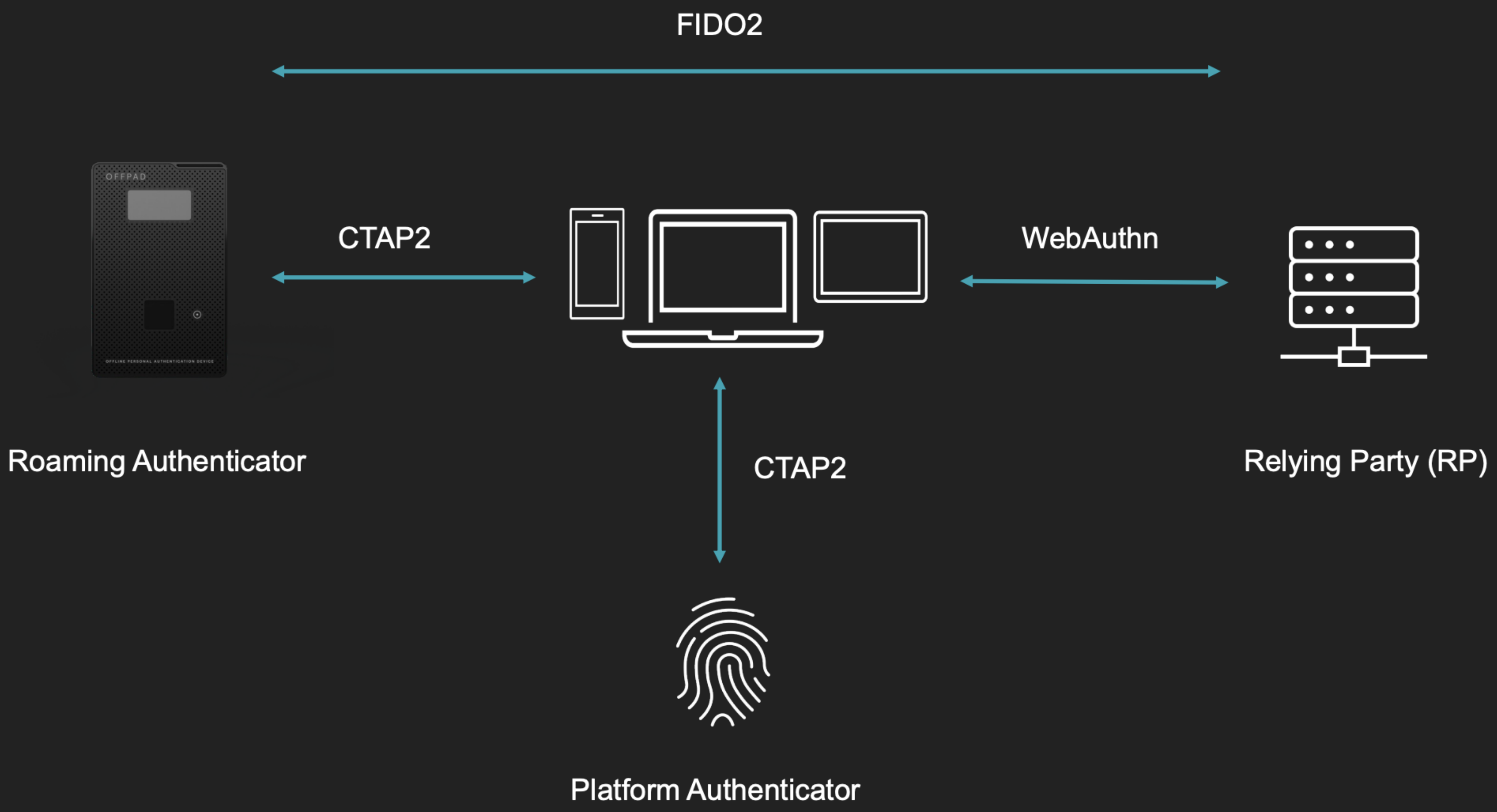
iMessage with PQ3: The new state of the art in quantum-secure messaging at scale

Posted by Apple Security Engineering and Architecture (SEAR)

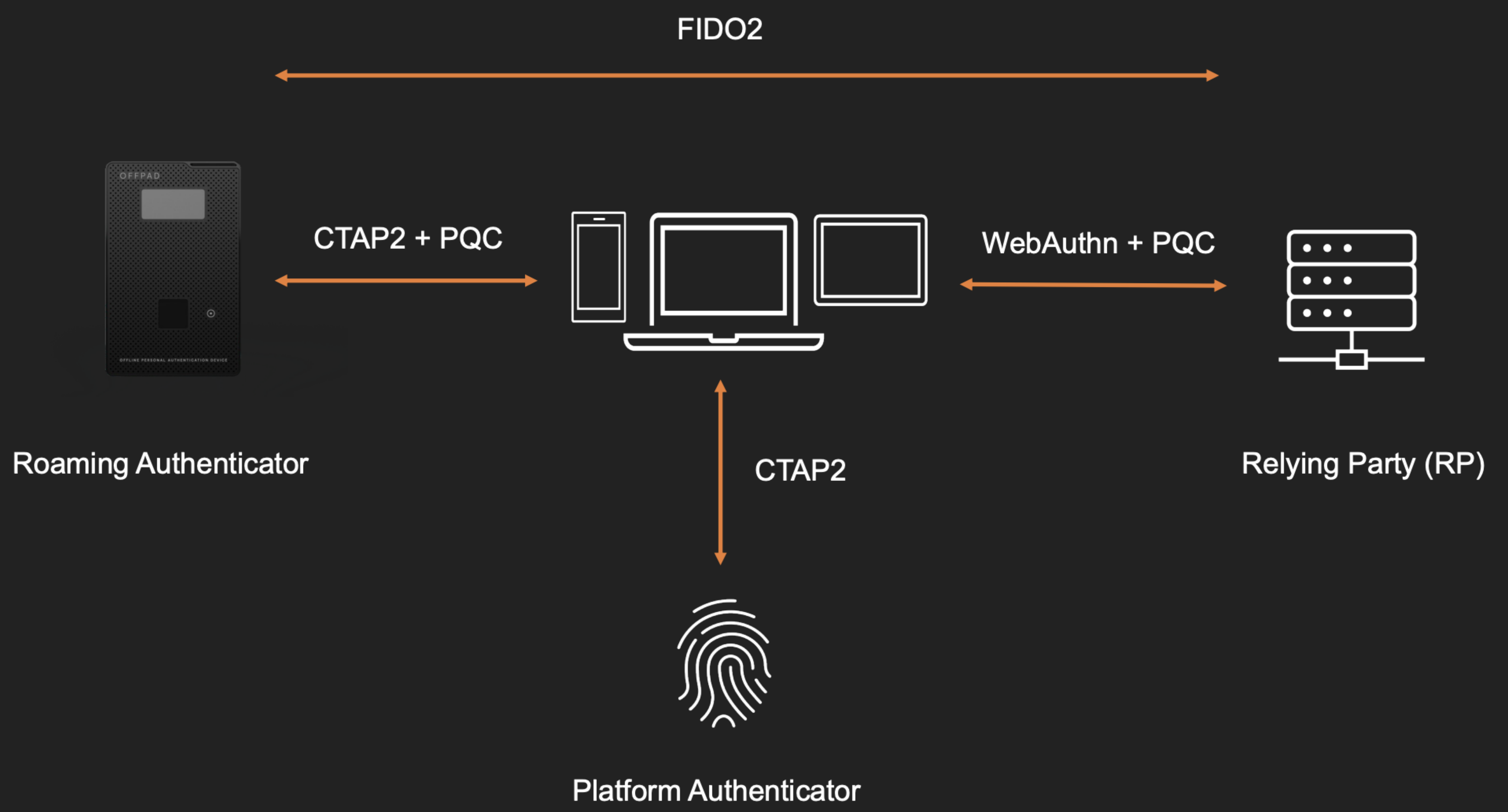
Hybrid PQC in Practice



Hybrid PQC in Practice



Hybrid PQC in Practice



PONE BIOMETRICS

Challenges with PQC

Performance: larger ciphertexts and signatures, larger memory requirements, sometimes slower

Foundations: new assumptions, models, and analysis

Variations: different use cases, combinations, national and international standards, recommendations

Opportunities with PQC

Be at the front: PQC skills and knowledge will make you a leading actor in the cybersecurity space

Clean up: opportunity to get an overview of cryptographic algorithms and remove old stuff (SHA-1, 3DES, RSA-1024)

Opportunities with PQC

Implementation: 25+ years side-channel experience, avoid large-integer arithmetic, linear algebra > elliptic curves

New applications: lattice-based cryptography allows for computation on encrypted data for privacy applications

The state of the post-quantum Internet

CLOUDFLARE

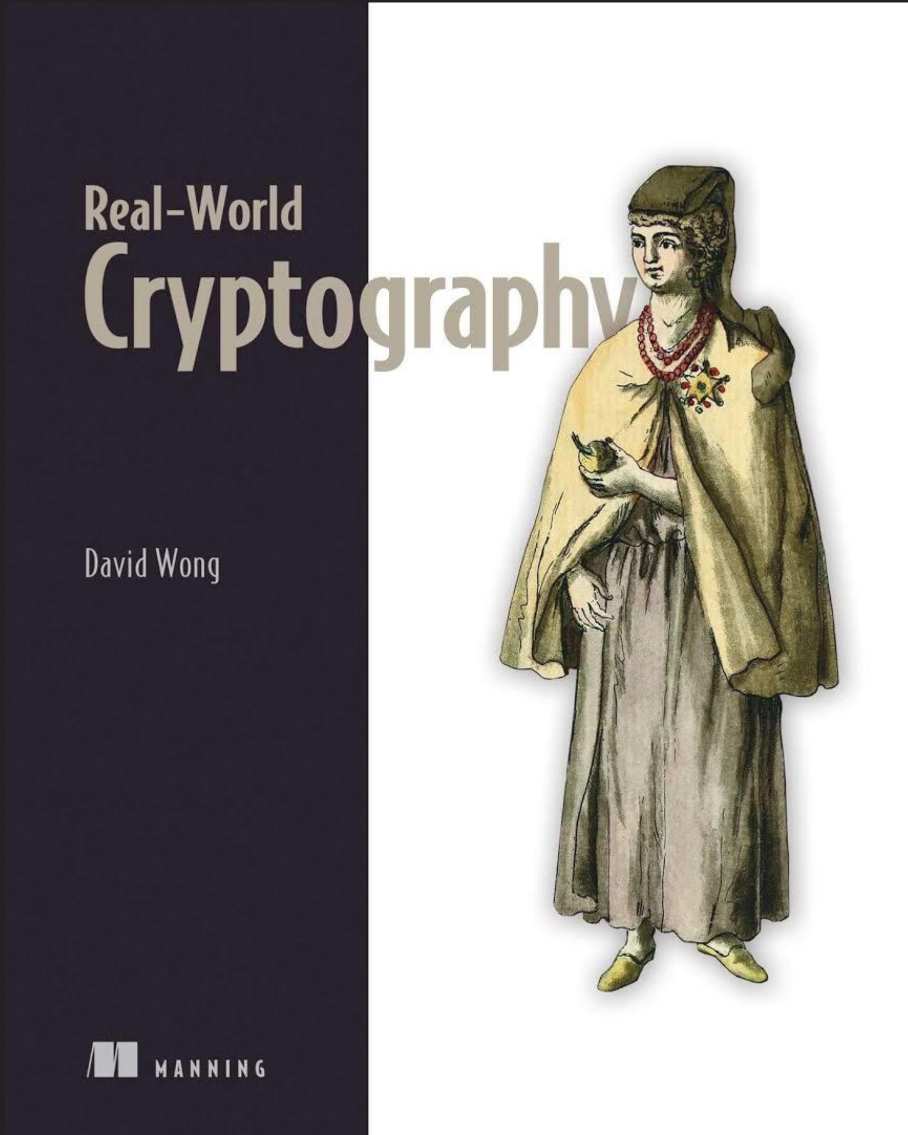
The state of the post-quantum Internet

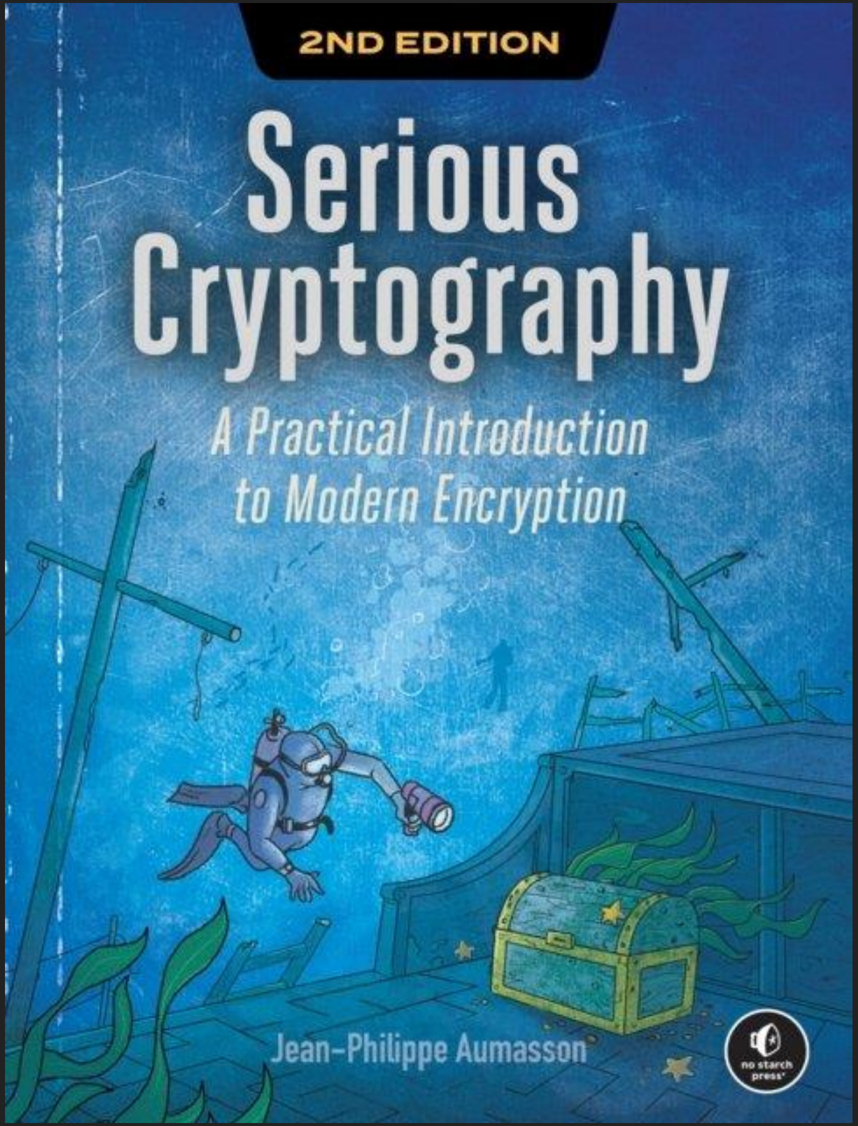
2024-03-05

Bas Westerbaan

33 min read

Modern Cryptography





PONE Biometrics PQC White Paper

ponebiometrics.com/post-quantum-cryptography

Thank you!
Questions?

Tjerand Silde, PONE Biometrics

PONE BIOMETRICS