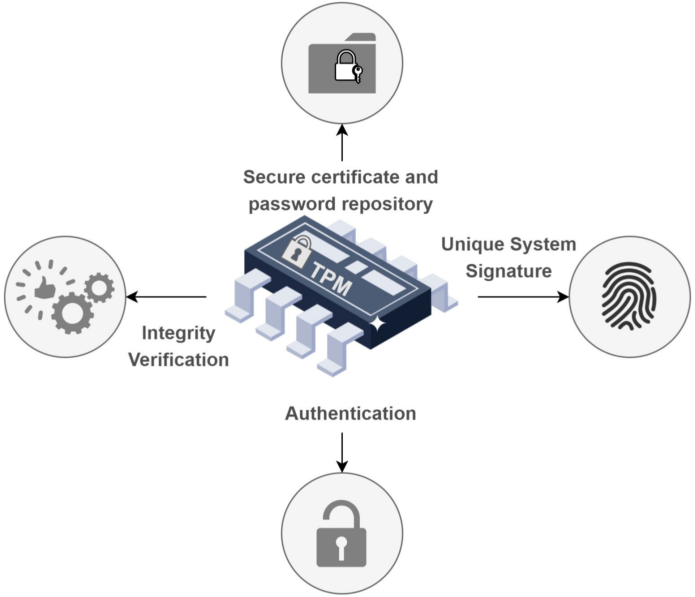
Requirements for a hybrid TPM based on optimized ML-DSA post-quantum signature

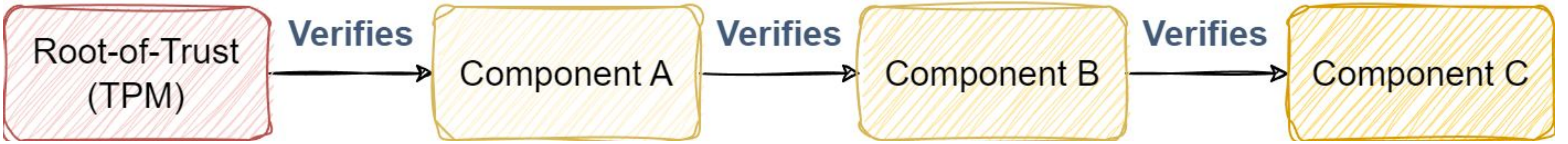
Felipe José Aguiar Rampazzo
Rodrigo de Meneses
Caio Teixeira
Marco A. Amaral Henriques

Trusted Platform Module (TPM)

- Dedicated secure hardware used to attest system integrity and secure key storage
- Provides:
  - A set of cryptographic and security functions
  - Tamper-proof
- Can be used as a **Root of Trust**



Root of Trust



Cryptographic algorithms available in TPM

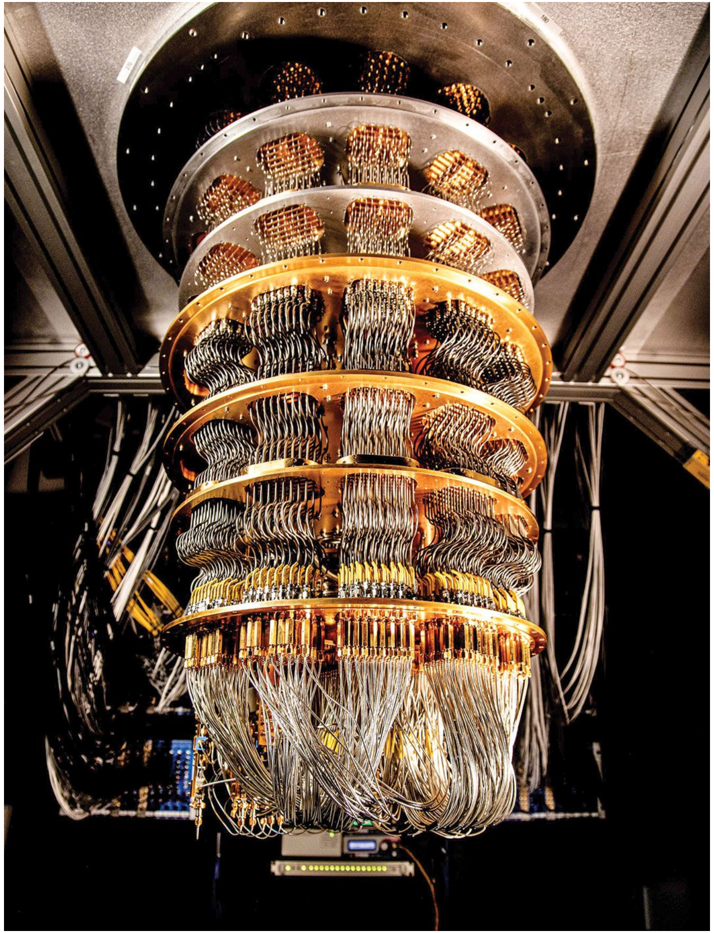
- Elliptic curves
- RSA
- AES
- SHA family: SHA-1, SHA-2 and SHA-3
- Others.

Cryptographic algorithms available in TPM

- **Elliptic curves**
- **RSA**
- AES
- SHA family: SHA-1, SHA-2 and SHA-3
- Others.

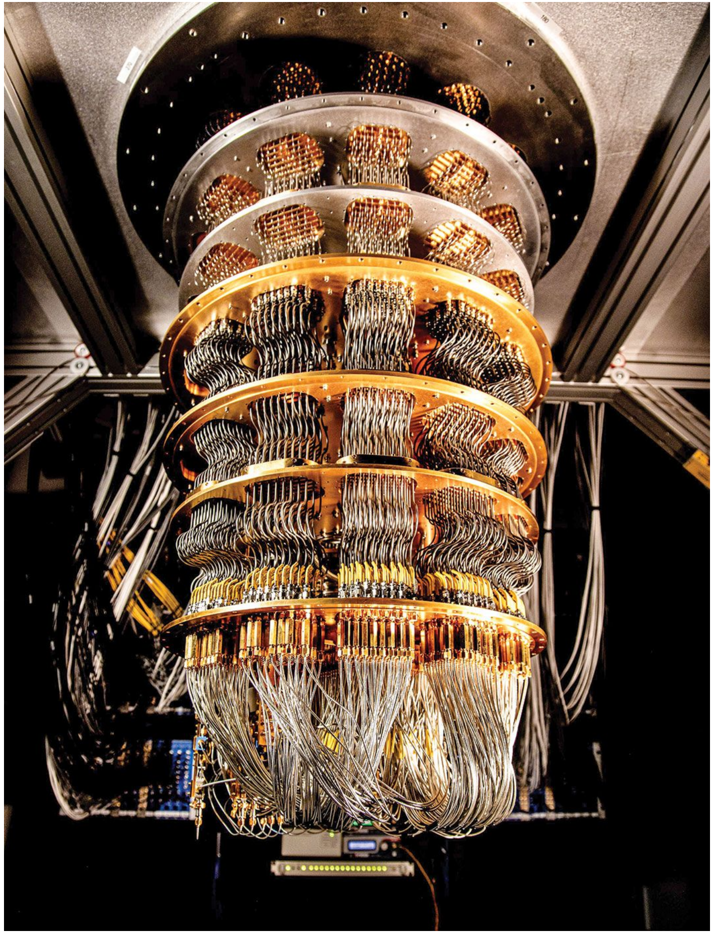
Vulnerable to the Quantum Computer

- Cryptographically Relevant Quantum Computers (CRQC) will break Public Key algorithms (**RSA** and **ECC**).



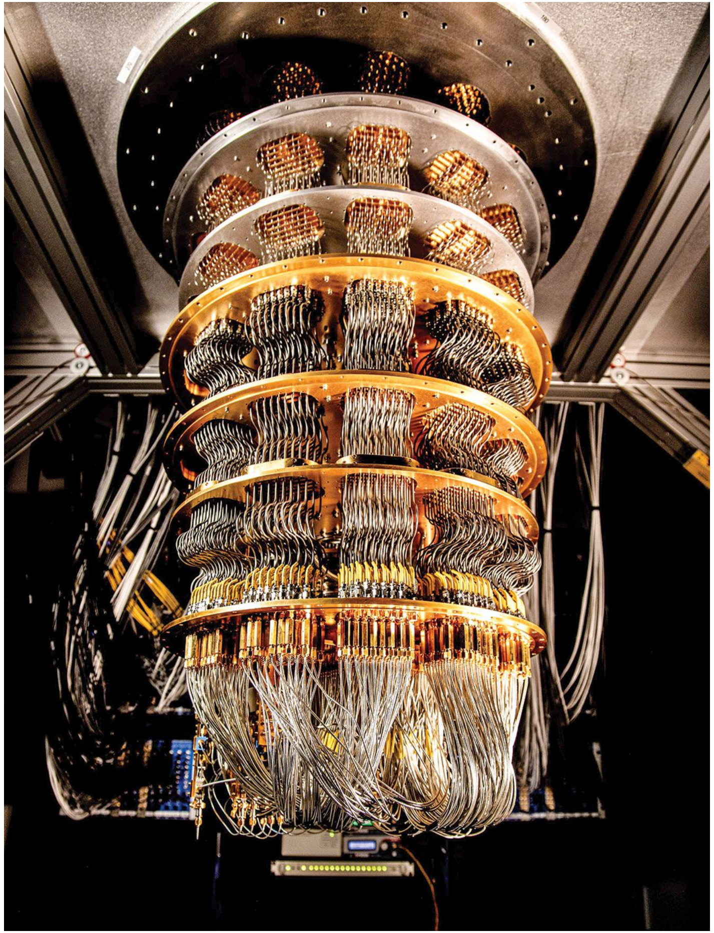
Fonte: https://www.science.org/content/article/quantum-computers-take-key-step-toward-curbing-errors

- Cryptographically Relevant Quantum Computers (CRQC) will break Public Key algorithms (**RSA** and **ECC**).
- Schemes resistant to CRQC attacks are needed to keep the root of trust secure.



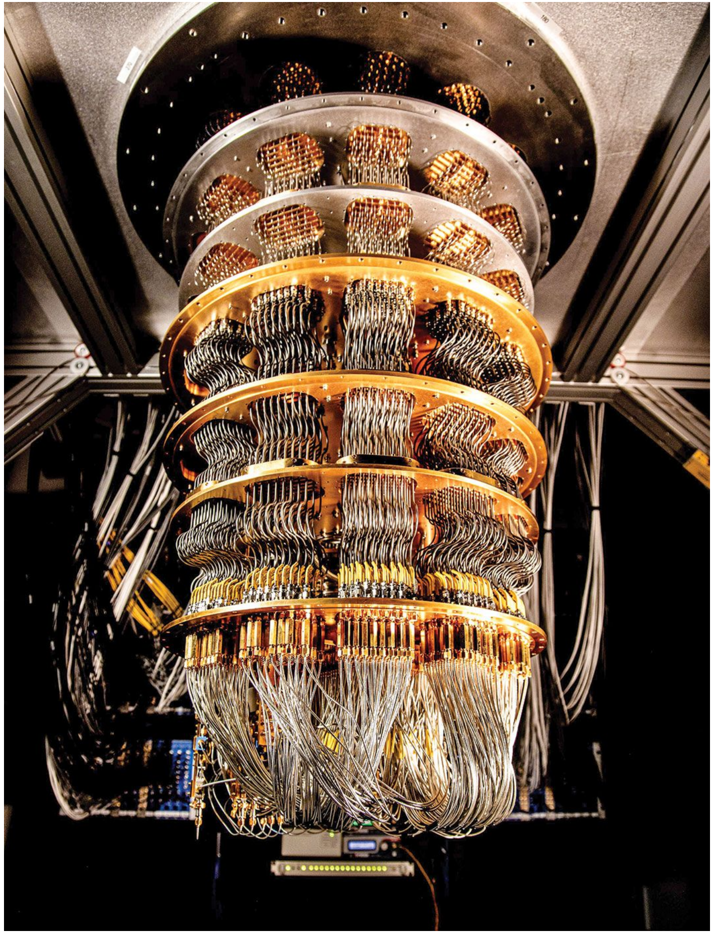
Fonte: https://www.science.org/content/article/quantum-computers-take-key-step-toward-curbing-errors

- Cryptographically Relevant Quantum Computers (CRQC) will break Public Key algorithms (**RSA** and **ECC**).
- Schemes resistant to CRQC attacks are needed to keep the root of trust secure.
- A CQCR could emerge in ~10 years.



Fonte: https://www.science.org/content/article/quantum-computers-take-key-step-toward-curbing-errors

- Cryptographically Relevant Quantum Computers (CRQC) will break Public Key algorithms (**RSA** and **ECC**).
- Schemes resistant to CRQC attacks are needed to keep the root of trust secure.
- A CQCR could emerge in ~10 years.
    - Important to protect data now.



Fonte: https://www.science.org/content/article/quantum-computers-take-key-step-toward-curbing-errors

What is a Hybrid scheme?

A hybrid cryptographic scheme is formed by a traditional and a post-quantum algorithm.

Why is a Hybrid necessary?

Hybrids are safe now...

No presence of a **Cryptographically Relevant Quantum Computers** (CRQC)

... and recommended

- Classical computers **might break PQC**:
  - “Breaking Rainbow Takes a Weekend on a Laptop” (Beullens, 2022).
- Avoid the "save now, decrypt later" attack.

Objectives

- Measuring the impacts of **Hybrid** protocols on TPM;

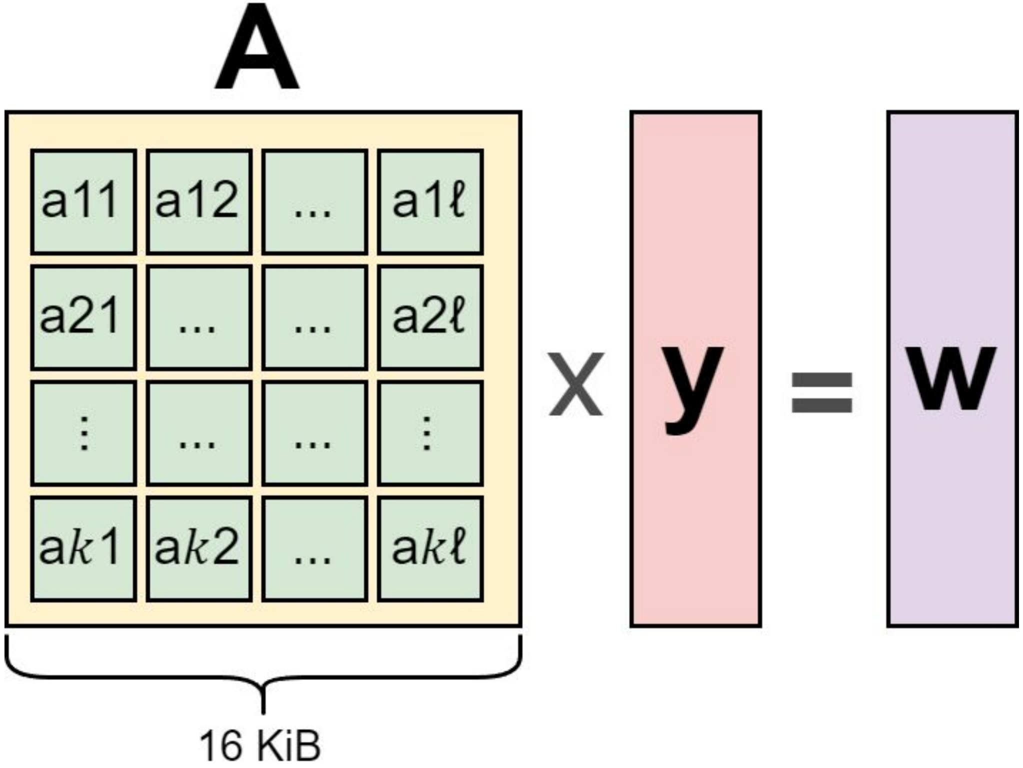
- Apply strategies to reduce memory usage of PQC algorithms.

Context

- **Hybrid scheme:**
  - **ML-DSA** + ECC (based on **Ed25519**)
- Adoption of memory optimization in ML-DSA;
- **TPM Software Stack (TSS)**: interface to pass commands to the TPM;
- **SW-TPM:** emulator of TPM specifications in software:
  - Used for prototyping.

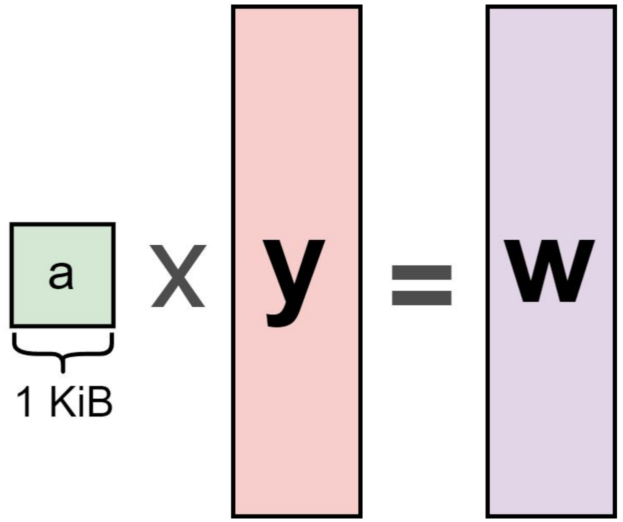
Memory optimization

Instead of storing in memory a 4x4 matrix **A** (ML-DSA-44), with 256 4-byte polynomials (totaling 16KiB)...

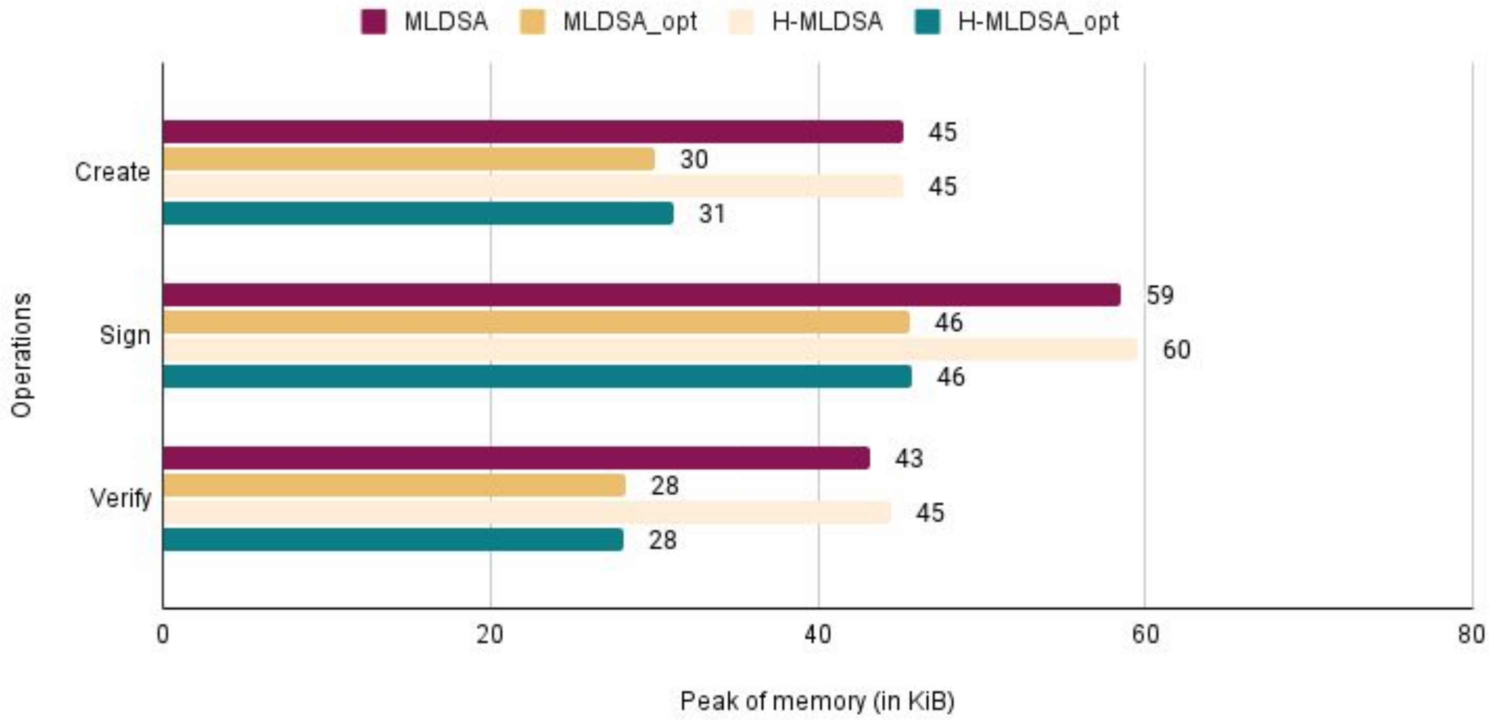


Memory optimization

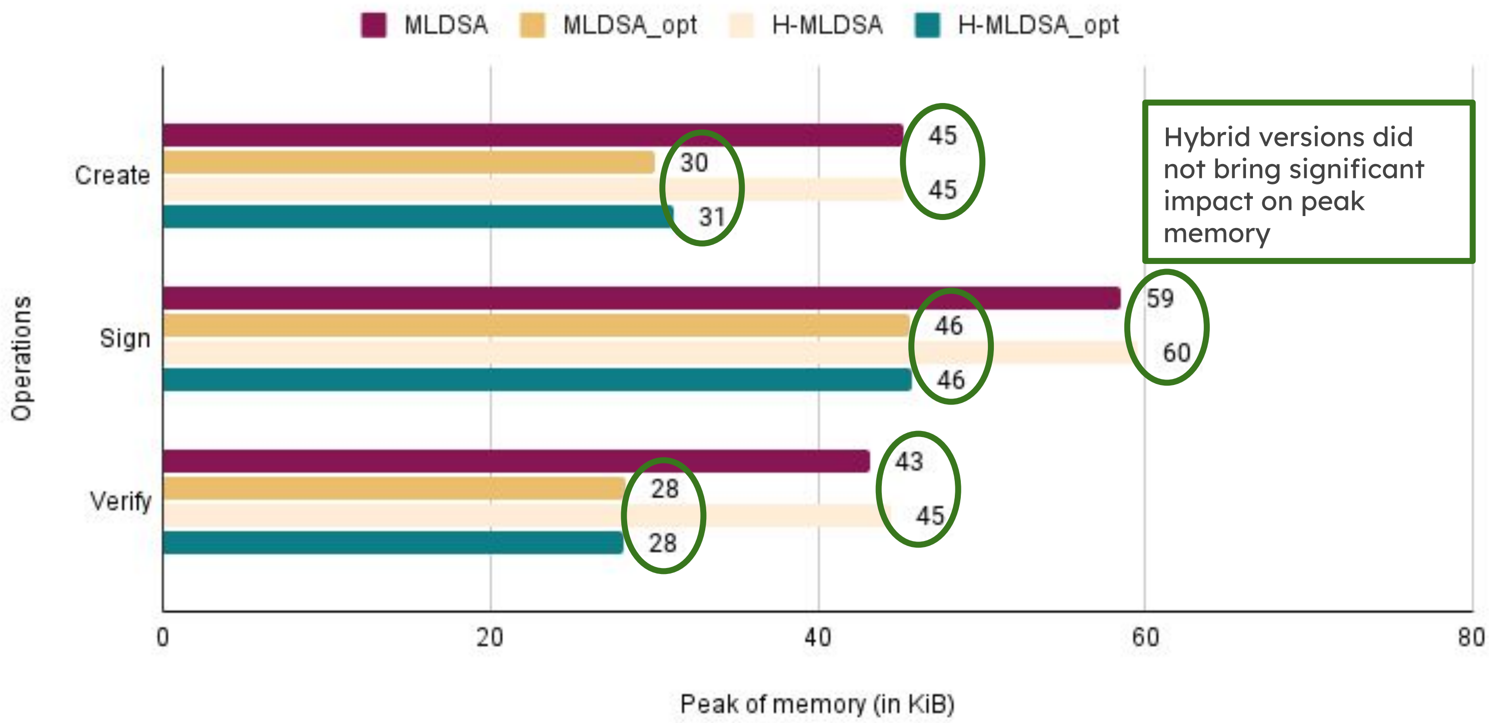
… we generate each polynomial of A, multiply by the y and accumulate results in w, constructing it after all entries are processed.



Memory Usage

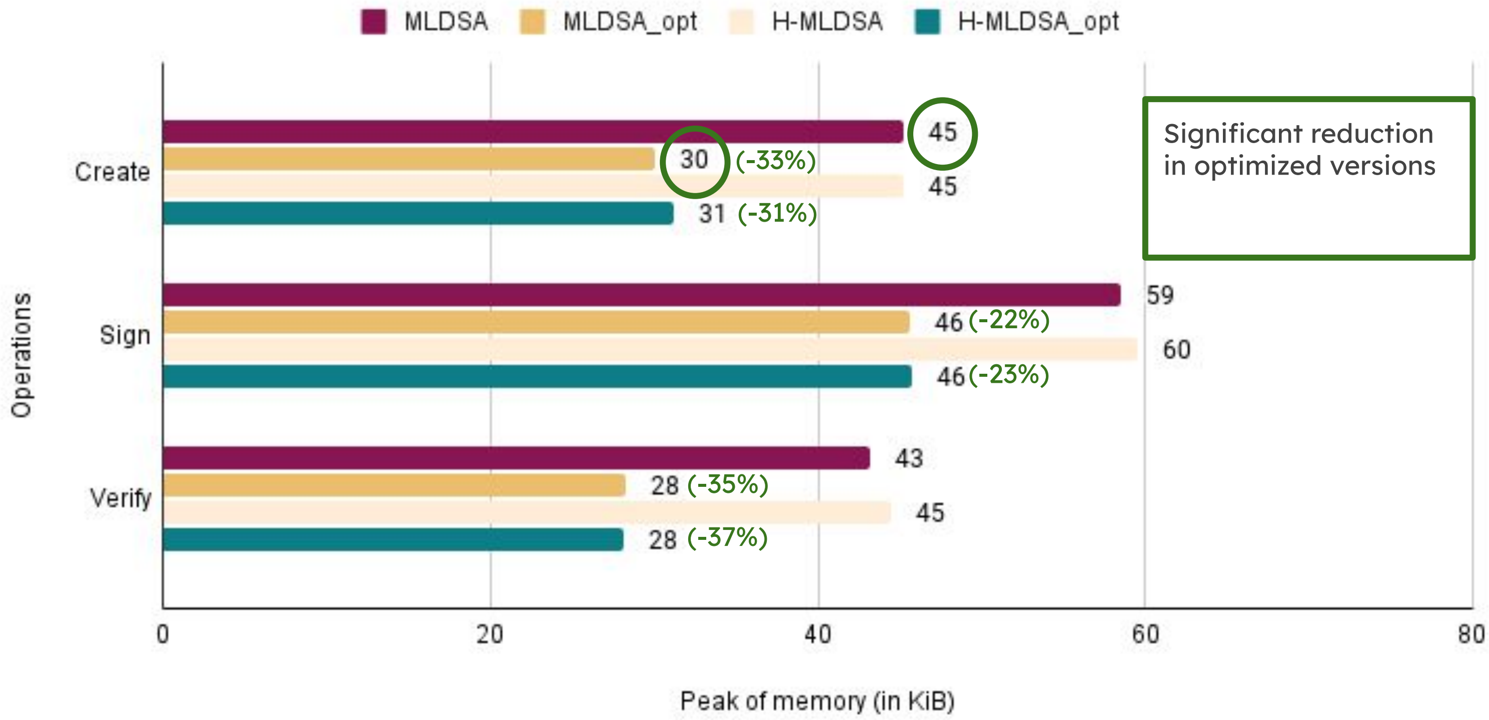


Memory Usage



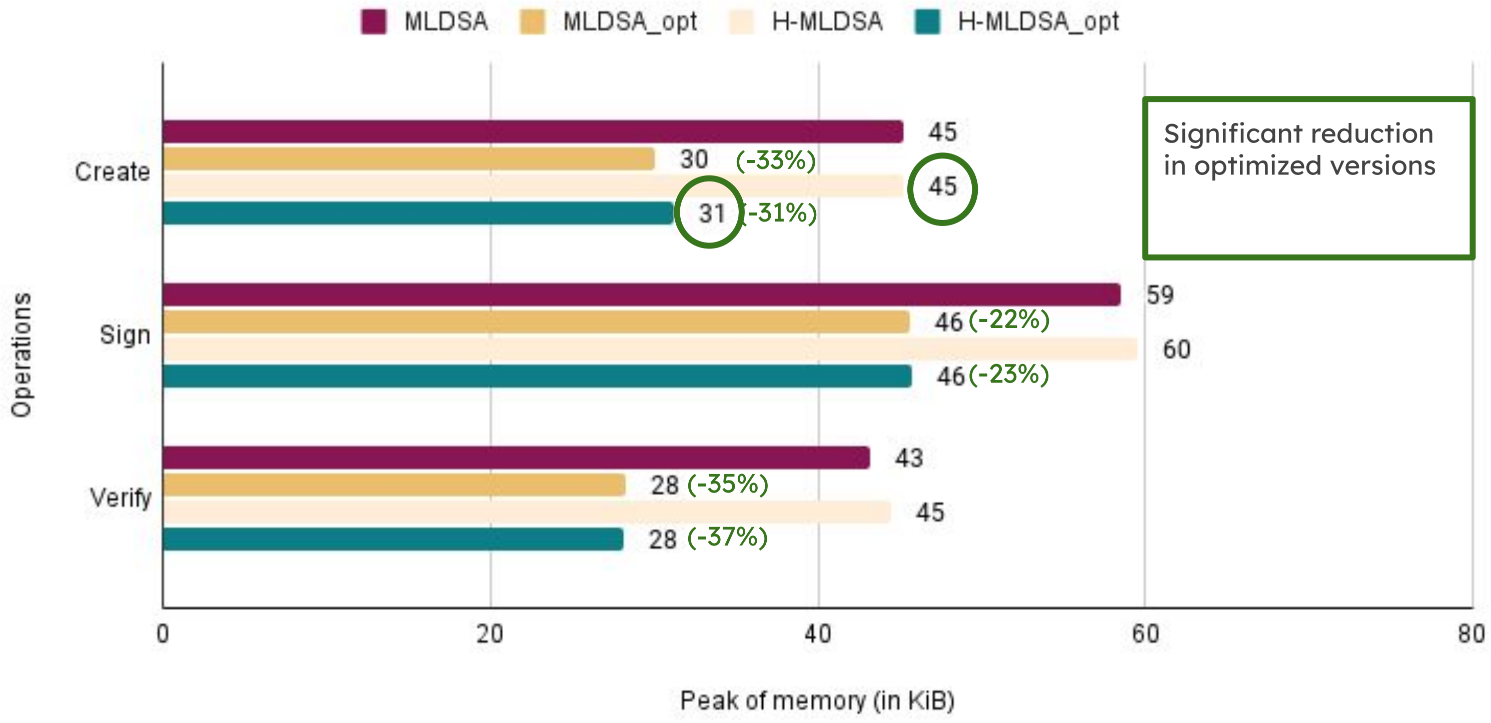
Hybrid versions did not bring significant impact on peak memory

Memory Usage



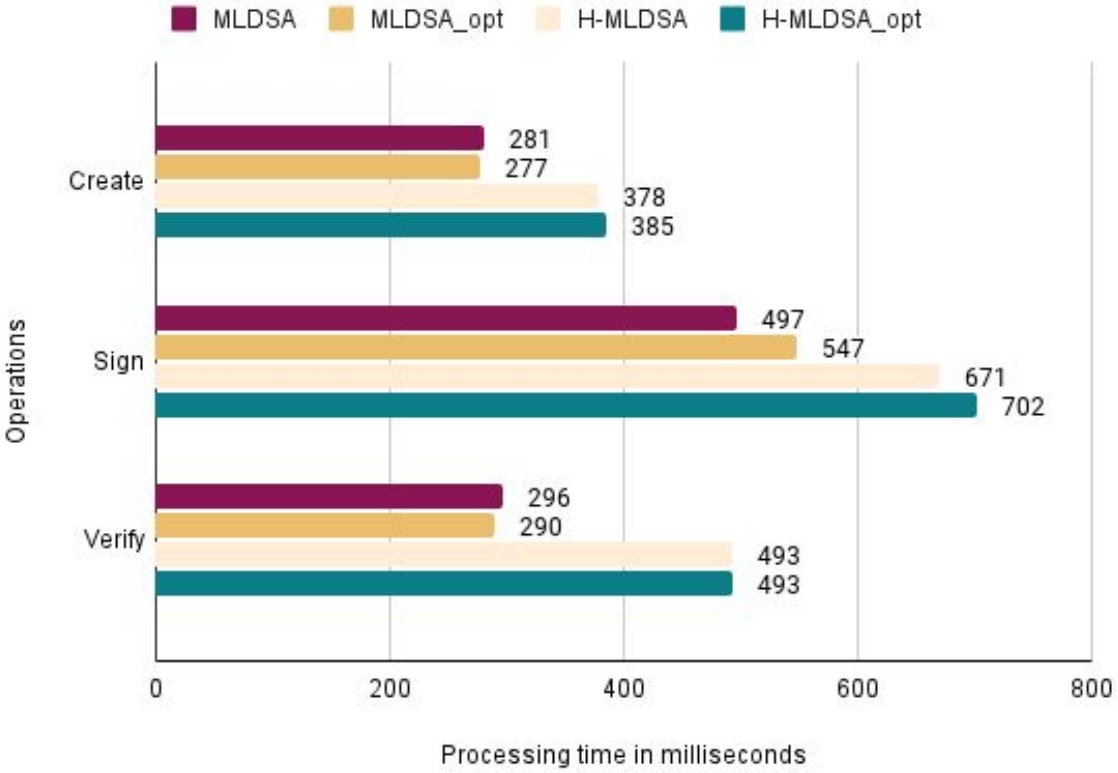
Significant reduction in optimized versions

Memory Usage

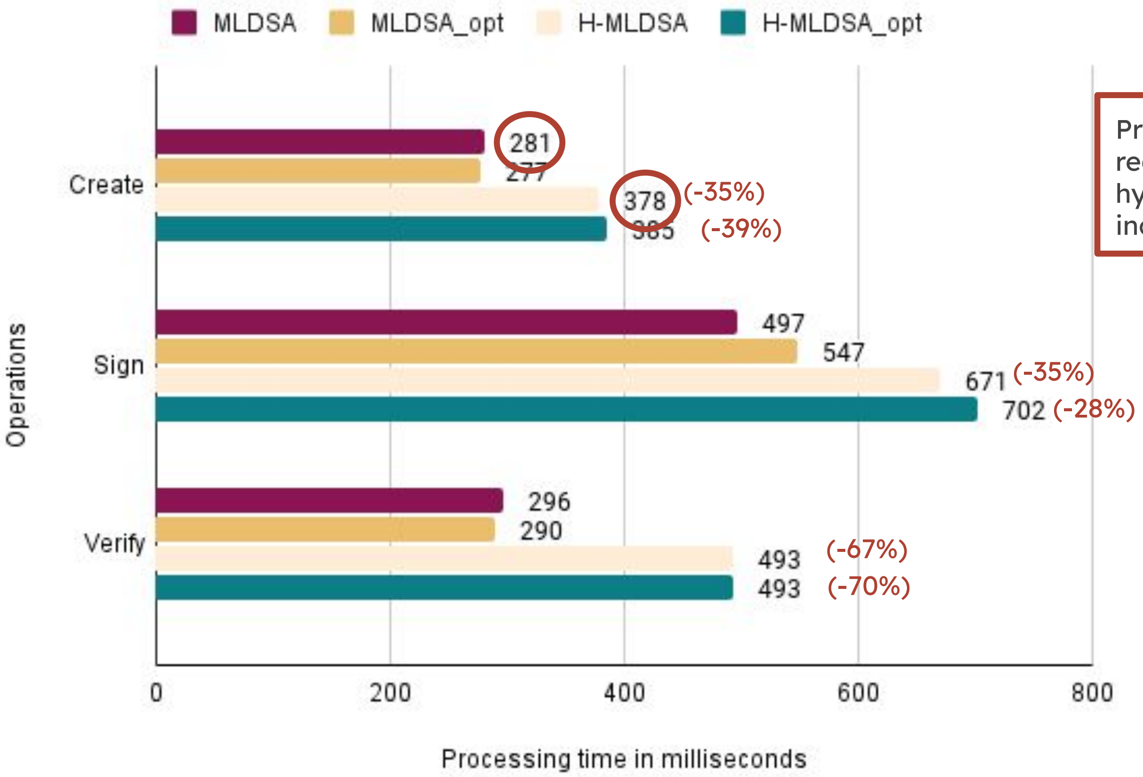


Significant reduction in optimized versions

Processing time

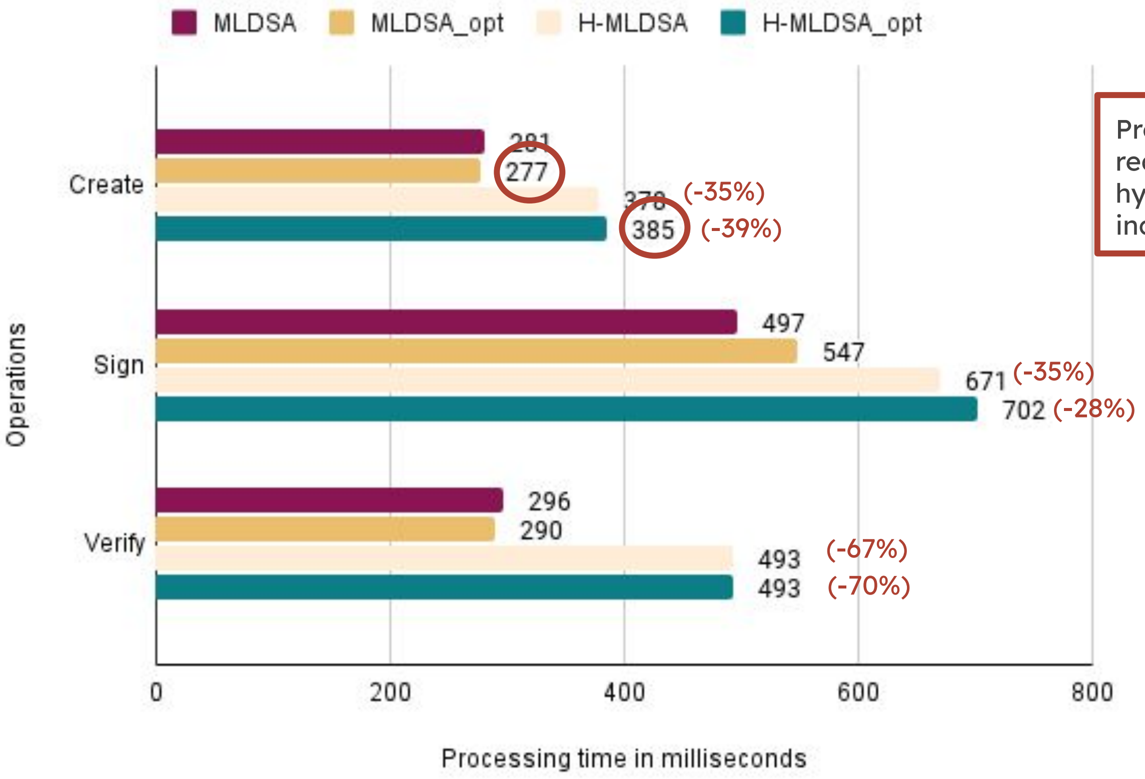


Processing time



Processing and request time for hybrid protocols has increased

Processing time



Processing and request time for hybrid protocols has increased

Conclusions

- ML-DSA optimization makes it easier to implement in TPM;
- Hybrid versions showed no significant memory peak increase compared to the PQC version;
- Hybrid versions resulted in longer processing time.

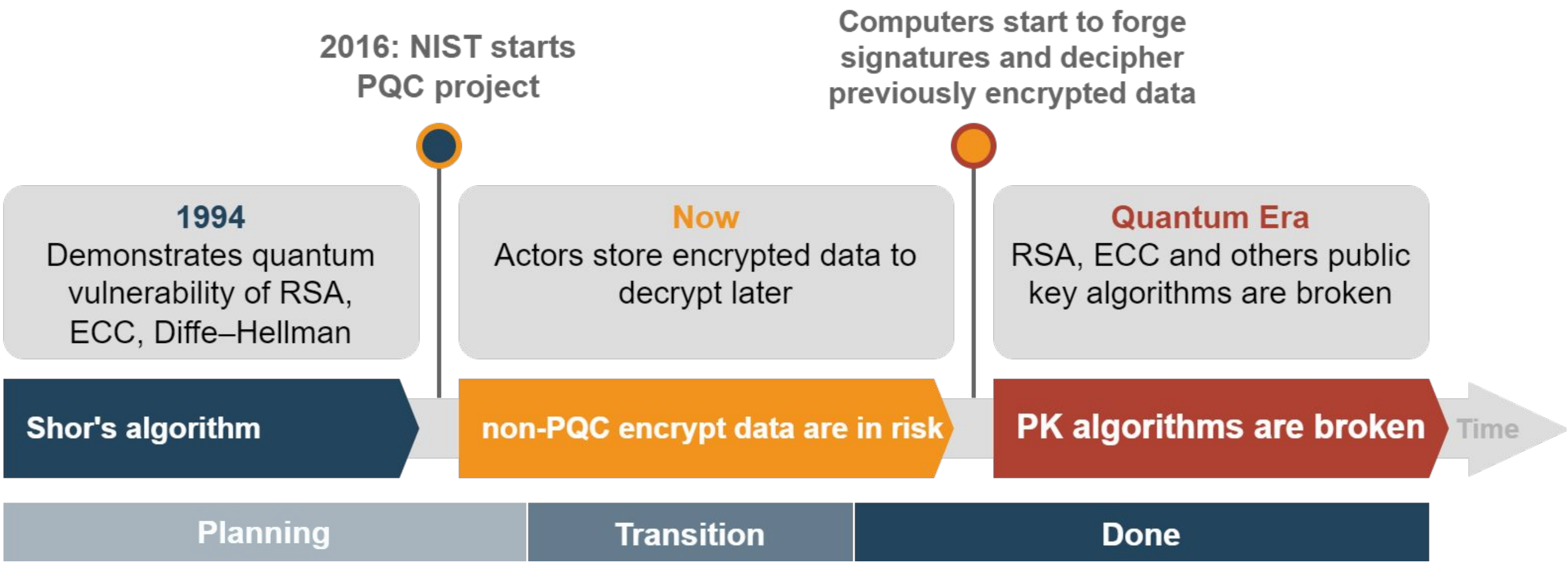
Future Work

- Further reduce the memory and processing requirements of Hybrid and PQC protocols;
- Implement a PQC and Hybrid version of ML-KEM;
- Explore new hybrid combinations.

Obrigado!

- Felipe J. A. Rampazzo
- f233261@dac.unicamp.br

Slides Extras



1994
Demonstrates quantum vulnerability of RSA, ECC, Diffe–Hellman

Shor's algorithm

2016: NIST starts PQC project

Now
Actors store encrypted data to decrypt later

non-PQC encrypt data are in risk

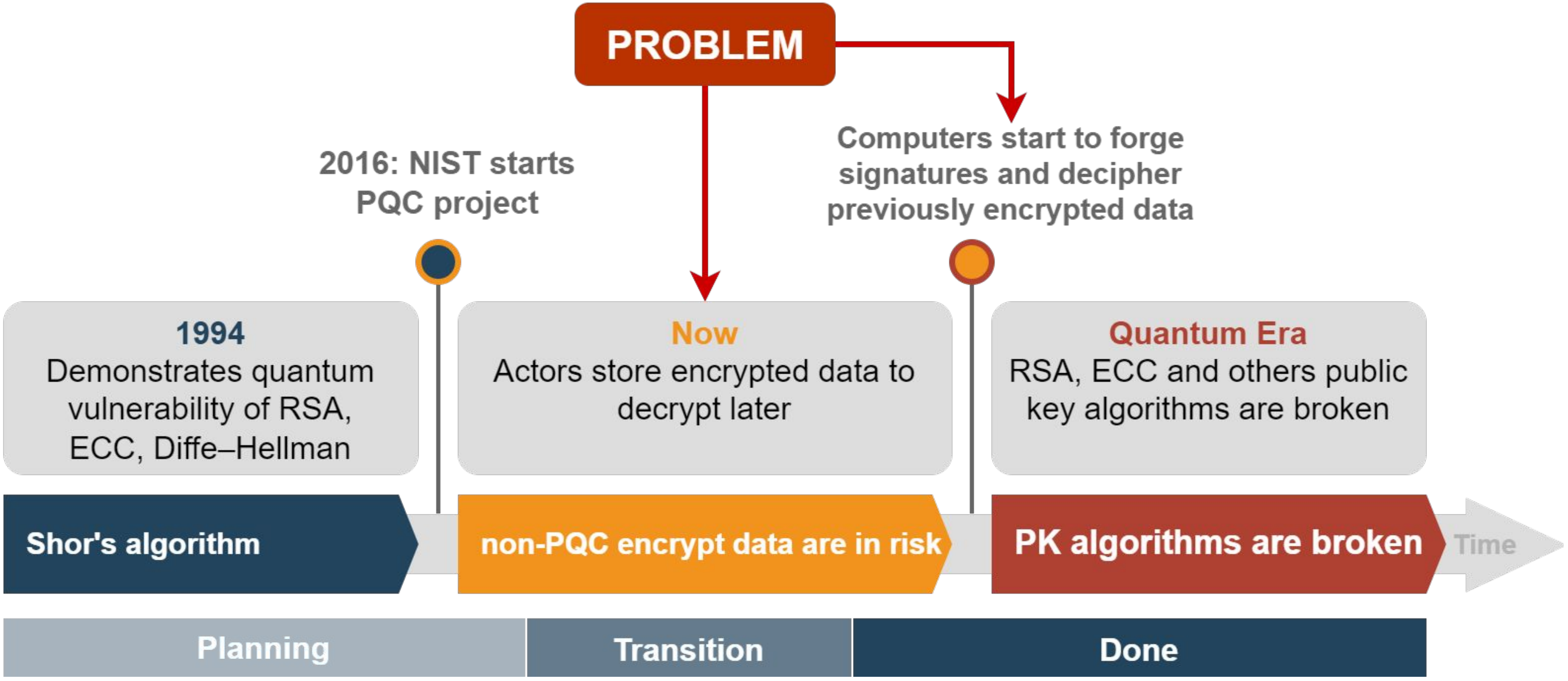
Computers start to forge signatures and decipher previously encrypted data

Quantum Era
RSA, ECC and others public key algorithms are broken

PK algorithms are broken

Time

Planning | **Transition** | **Done**



PROBLEM

2016: NIST starts PQC project

Computers start to forge signatures and decipher previously encrypted data

1994
Demonstrates quantum vulnerability of RSA, ECC, Diffe–Hellman

Now
Actors store encrypted data to decrypt later

Quantum Era
RSA, ECC and others public key algorithms are broken

Shor's algorithm

non-PQC encrypt data are in risk

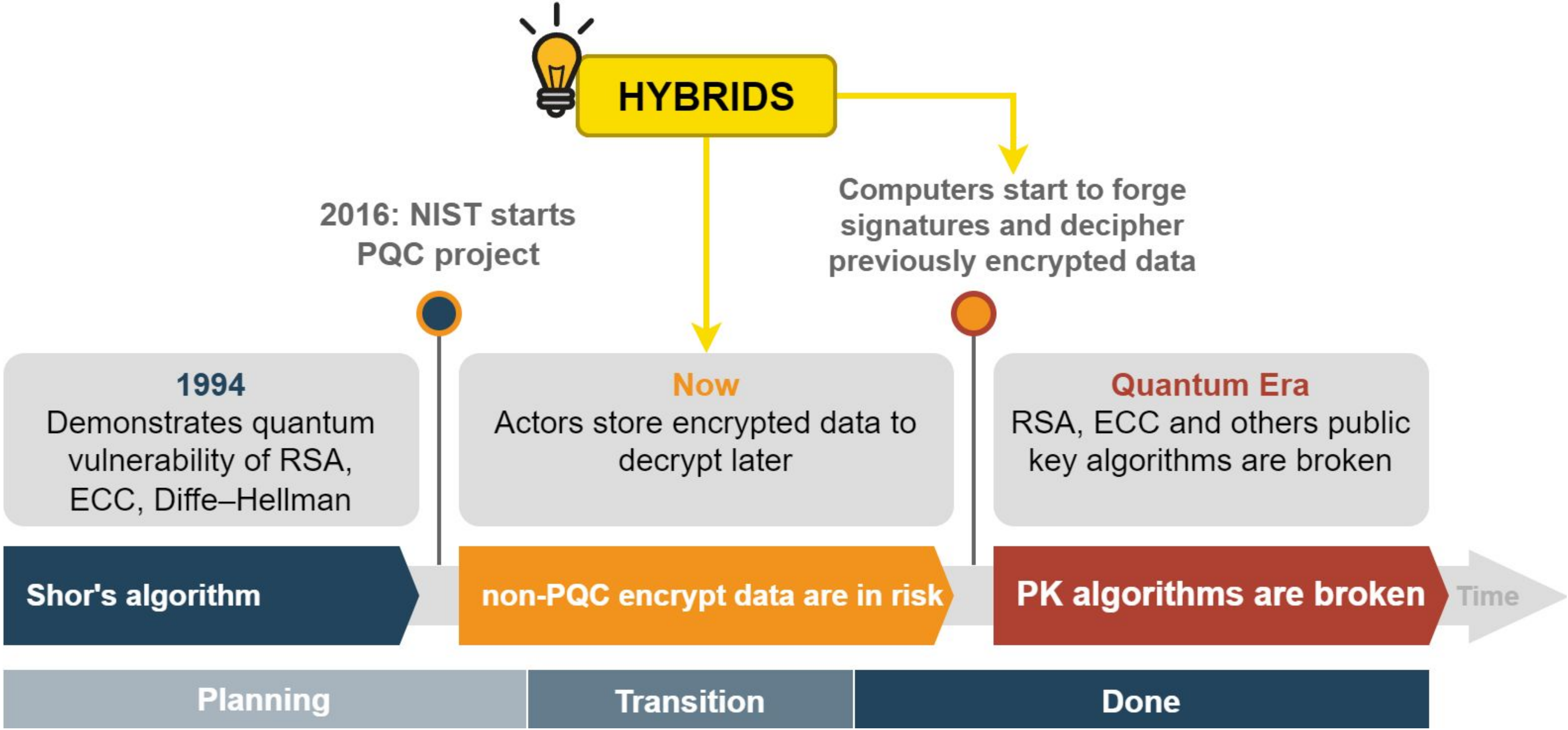
PK algorithms are broken

Time

Planning

Transition

Done



HYBRIDS

2016: NIST starts PQC project

Computers start to forge signatures and decipher previously encrypted data

1994
Demonstrates quantum vulnerability of RSA, ECC, Diffe–Hellman

Now
Actors store encrypted data to decrypt later

Quantum Era
RSA, ECC and others public key algorithms are broken

Shor's algorithm

non-PQC encrypt data are in risk

PK algorithms are broken

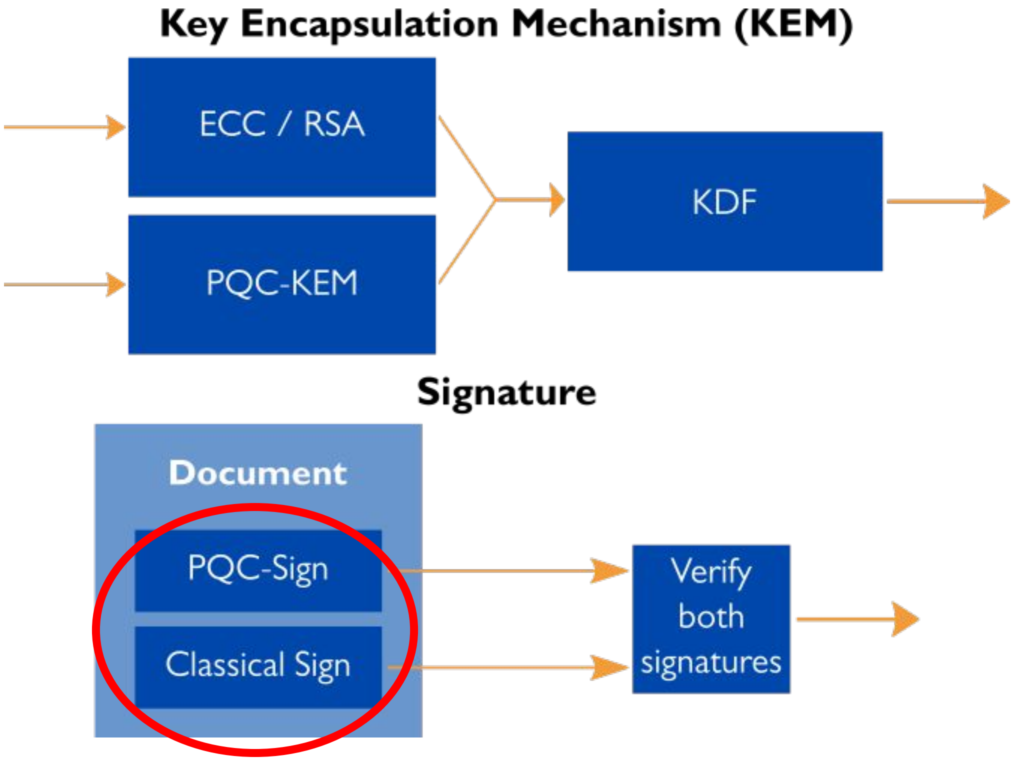
Time

Planning

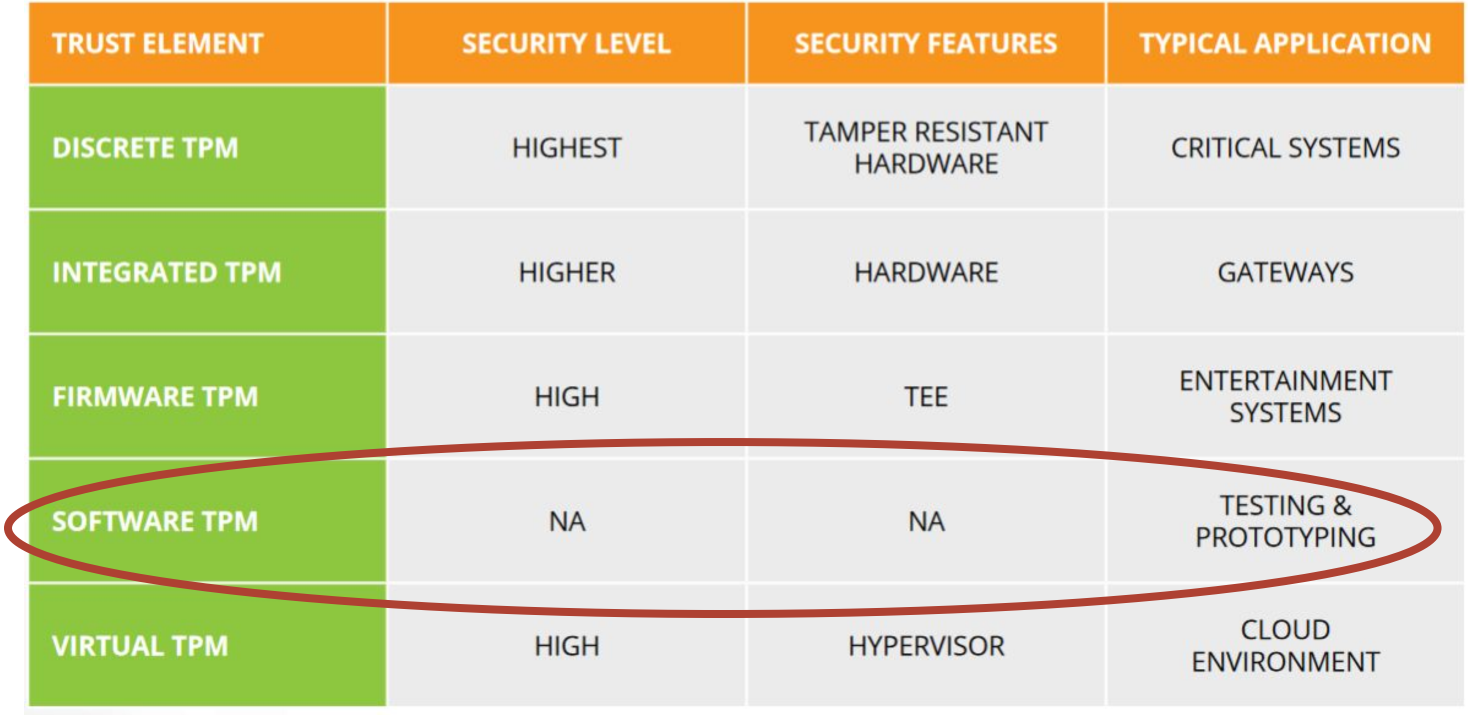
Transition

Done

What is a Hybrid scheme?



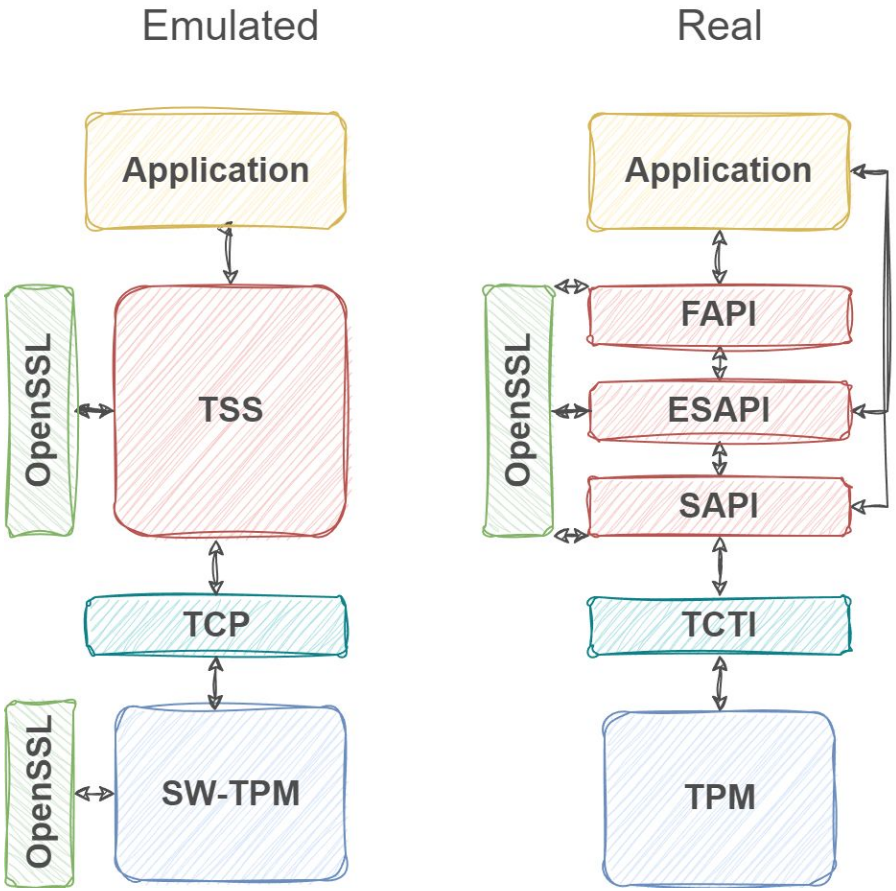
Emulated TPM



TRUST ELEMENT	SECURITY LEVEL	SECURITY FEATURES	TYPICAL APPLICATION
DISCRETE TPM	HIGHEST	TAMPER RESISTANT HARDWARE	CRITICAL SYSTEMS
INTEGRATED TPM	HIGHER	HARDWARE	GATEWAYS
FIRMWARE TPM	HIGH	TEE	ENTERTAINMENT SYSTEMS
SOFTWARE TPM	NA	NA	TESTING & PROTOTYPING
VIRTUAL TPM	HIGH	HYPERVISOR	CLOUD ENVIRONMENT

Tool stack

- **TPM Software Stack (TSS)**: interface to pass commands to the TPM;
- **sw-tpm**: emulator of TPM specifications in software:
  - Used for prototyping.


Emulated
Real
Application
OpenSSL
TSS
TCP
OpenSSL
SW-TPM
Application
OpenSSL
FAPI
ESAPI
SAPI
TCTI
TPM