IDEMIA
SECURE
TRANSACTIONS

Crypto Agility for Smart Cards

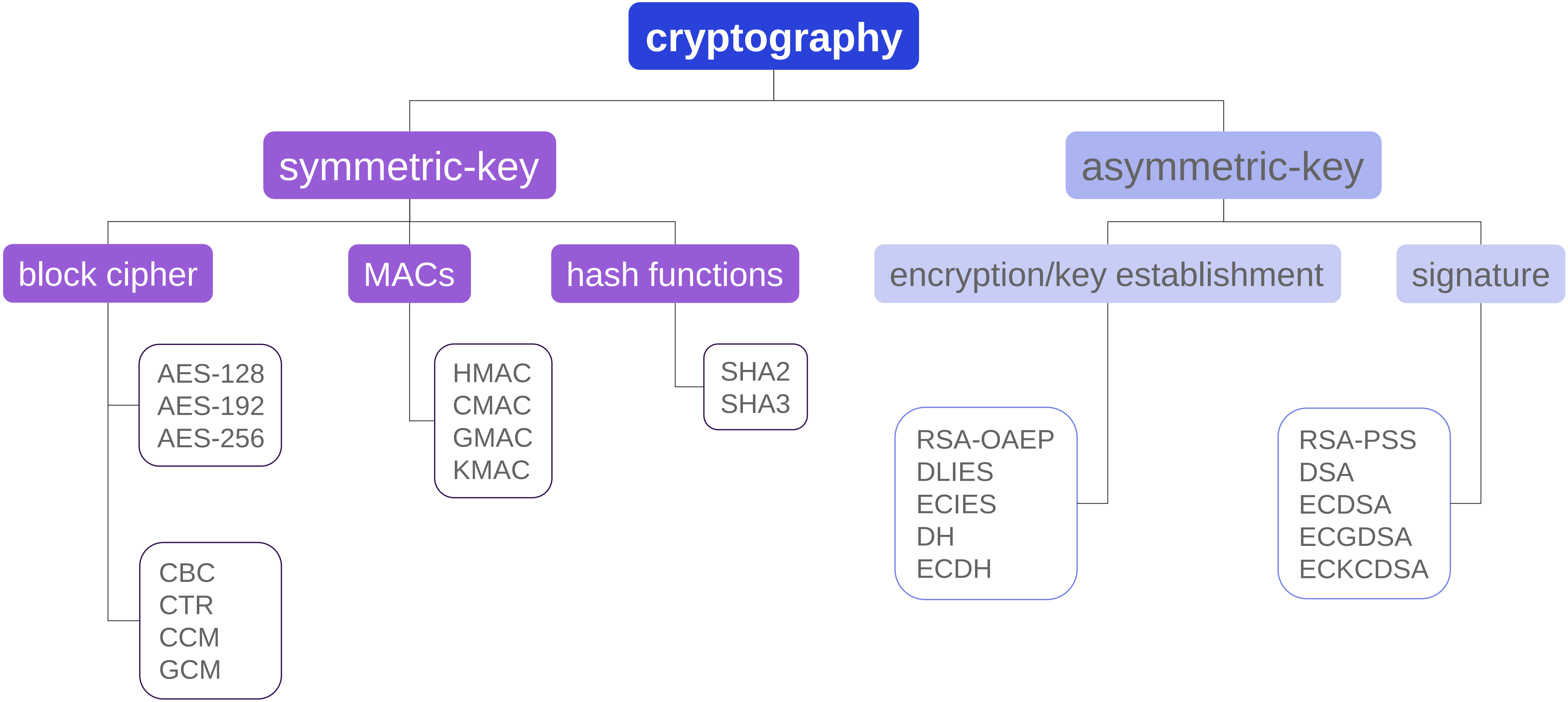
Christophe Giraud

SUMMARY

- Motivations
- Crypto-agility
- Practical use-case

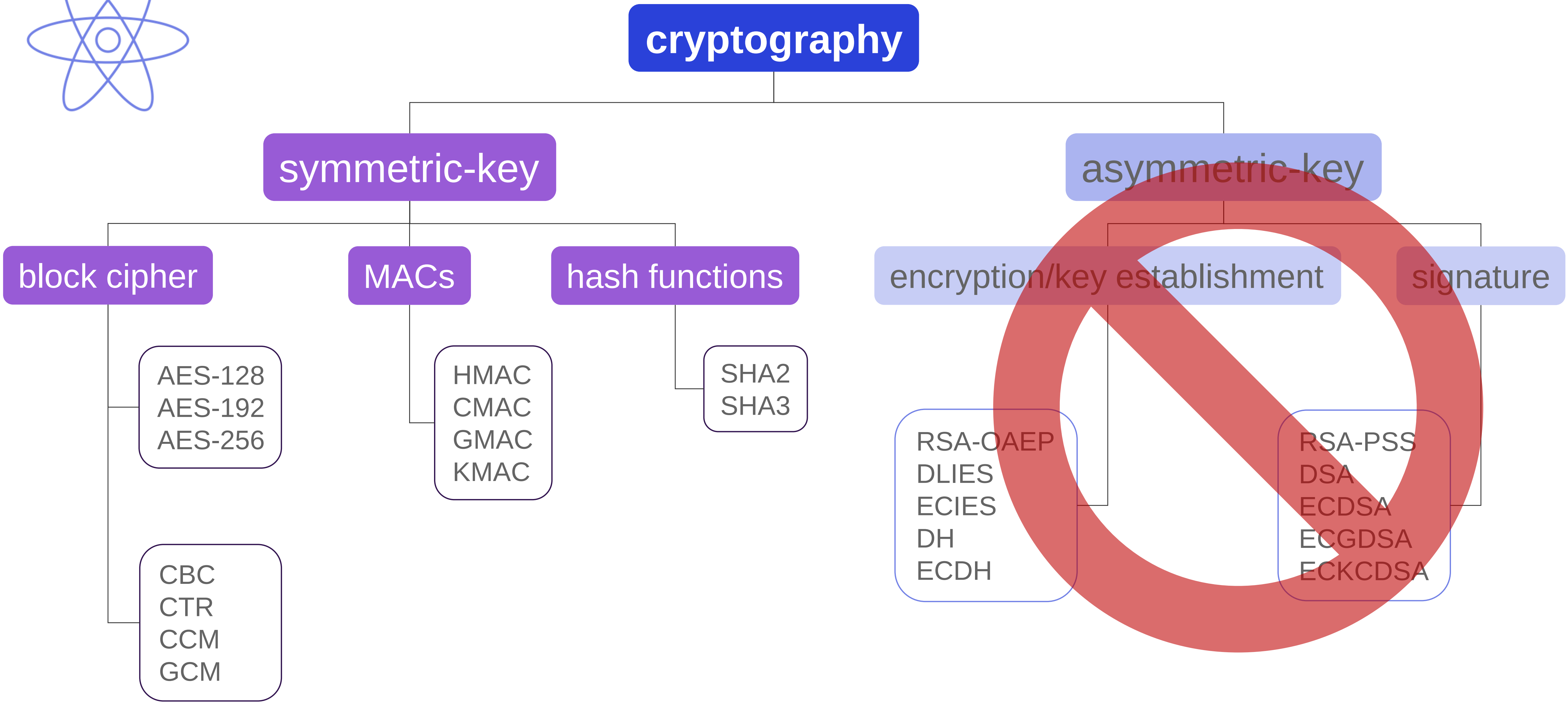
IDEMIA SECURE TRANSACTIONS

MOTIVATIONS



IDEMIA
SECURE TRANSACTIONS

QUANTUM THREAT



POST-QUANTUM CRYPTOGRAPHY

Check for updates

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

This publication is available free of charge from:
https://doi.org/10.6028/NIST.FIPS.203

Published August 13, 2024

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

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

Check for updates

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

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

Published August 13, 2024

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

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

Check for updates

FIPS 205

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

Published: August 13, 2024

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

FALCON: Fast-Fourier Lattice-based Compact Signatures over NTRU

Specification v1.2 — 01/10/2020

Pierre-Alain Fouque Jeffrey Hoffstein Paul Kirchner
Vadim Lyubashevsky Thomas Pornin Thomas Prest Thomas Ricosset
Gregor Seiler William Whyte Zhenfei Zhang

falcon@ens.fr

Hamming Quasi-Cyclic (HQC)

Fourth round version

Updated version 19/02/2025

HQC is an IND-CCA2 KEM running for standardization to NIST's competition in the category "post-quantum public key encryption scheme". Parameters sets are given for the three categories 1, 3 and 5. The main features of the HQC submission are:
- *IND-CCA2 KEM*
- *Small public key size*
- *Precise DFR analysis*
- *Efficient implementations based on classical decoding algorithms*

Principal Submitters (by alphabetical order):
- Carlos AGUILAR MELCHOR (SandboxAQ)
- Nicolas ARAGON (Univ. of Limoges)
- Slim BETTAIEB (TII)
- Loïc BIDOUX (TII)
- Olivier BLAZY (Ecole Polytechnique)
- Jurjen BOS (Worldline)
- Jean-Christophe DENEUVILLE (ENAC)
- Arnaud DION (ISAE Supaero)
- Philippe GABORIT (Univ. of Limoges)
- Jérôme LACAN (ISAE Supaero)
- Edoardo PERSICHETTI (Florida Atlantic Univ.)
- Jean-Marc ROBERT (Univ. of Toulon)
- Pascal VÉRON (Univ. of Toulon)
- Gilles ZÉMOR (Univ. of Bordeaux)

Inventors: Same as submitters
Developers: Same as submitters

IDEMIA
SECURE TRANSACTIONS

HOW TO TRANSITION?

- PQ algorithms are still “young”
- Time is needed to gain sufficient confidence

RÉPUBLIQUE FRANÇAISE

Post-quantum cryptography

The maturity level of the post-quantum algorithms should not be overestimated.

- ≈ the maturity level of RSA in the mid 90’s
- Multifaceted immaturity: difficulty of the underlying problem in the classical and quantum computation models, dimensioning, integration of schemes in protocols, secure implementations
- Immaturity will **not cease immediately with the publication of NIST standards**

Acknowledging this immaturity is important,

but it should not serve as an argument for postponing the first deployments.

➔ Hybrid cryptography

➔ Crypto-agility

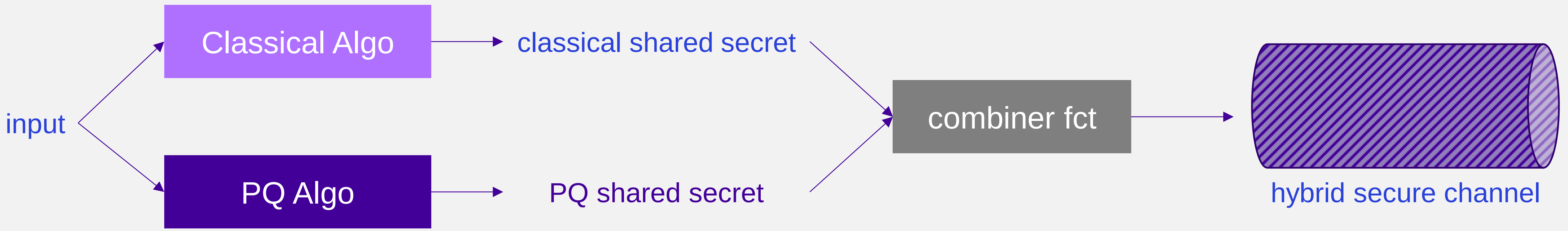
HYBRID CRYPTOGRAPHY

Hybridation

Post-quantum mechanisms **+** a recognised pre-quantum scheme.

- Preservation of the pre-quantum security.
- Extra protection against the quantum threat.
- Low performance penalty over drop-in replacement.

Example



IDEMIA
SECURE TRANSACTIONS

CRYPTO AGILITY

CRYPTO-AGILITY: DEFINITION(S)

Bundesamt für Sicherheit in der Informationstechnik

A cryptosystem is considered crypto-agile if its components, for example cryptographic algorithms, key lengths, key generation schemes or technical implementation, can be replaced by other components **without having to make significant changes to the rest of the overall system**.

National Cyber Security Centre
Ministry of Justice and Security

Crypto-agility means that cryptographic protocols, products and systems are implemented in such a way that it takes **minimal effort** to modify the associated cryptographic algorithms.

NIST

- The ability for machines to select their security algorithms in real time and based on their combined security functions;
- The ability to add new cryptographic features or algorithms to existing hardware or software, resulting in new, stronger security features;
- The ability to **easily** retire cryptographic systems that have become either vulnerable or obsolete.

ANSSI

A product is said crypto-agile if it includes the possibility to update its cryptographic algorithms **without recalling it or substituting it with a new one**.

CRYPTO-AGILITY: SUMMARY

Goal: Make cryptographic functionalities **as flexible and future-proof as possible**

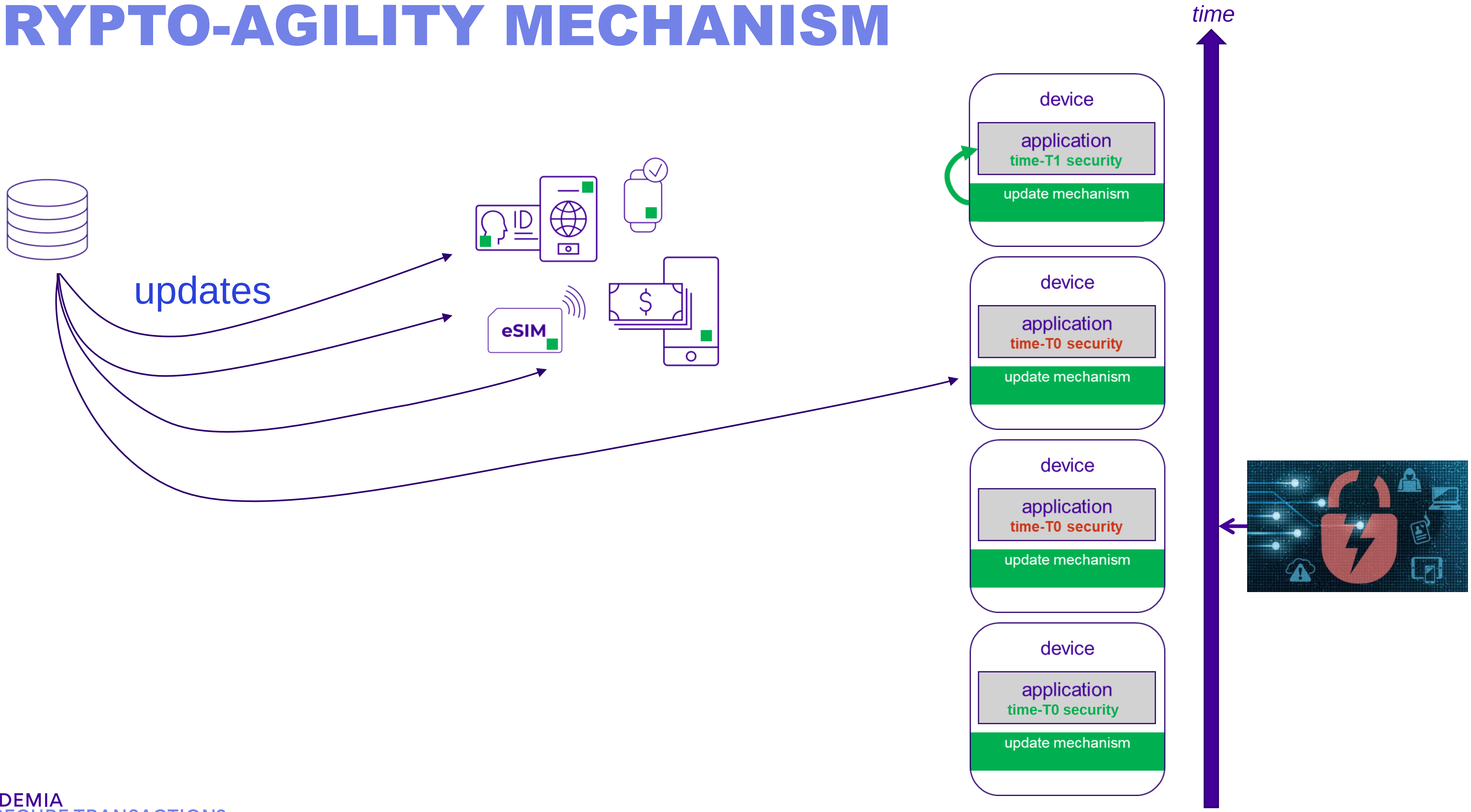
To enable:

- Updating **implementations** when side-channel or fault attacks are discovered
- Updating **parameters** when the current security margin is insufficient
- Adding **new algorithms** when old ones are broken or better standards emerge
- Updating **applications** to replace old algorithms seamlessly
- Updating **protocols**, for example, to adjust hybrid cryptographic behavior

It should be simple and doable**.**

This is essential for overall security, but **critical for Post-Quantum migration.**

CRYPTO-AGILITY MECHANISM



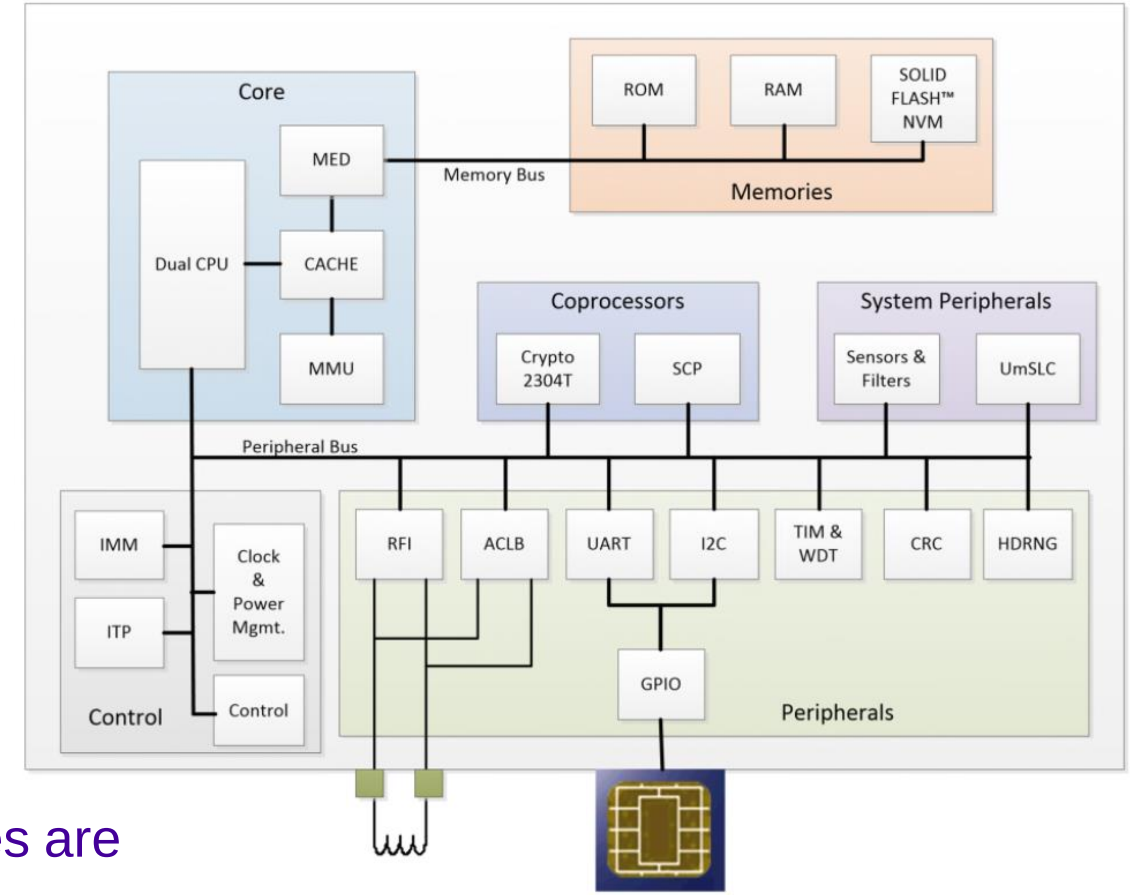
CRYPTO-AGILITY: SMART-CARDS CHALLENGES

Smart-card are highly constrained devices

Example
- 32-bit processor (~ Cortex M3)
- up to 100 MHz
- up to few MB of flash memory
- up to 48 KB of RAM

Crypo-agility is challenging to implement

Updating or replacing an algo:
- difficult if not enough RAM/NVM available
- possibly impact on user experience if performances are different (e.g. contactless payments)

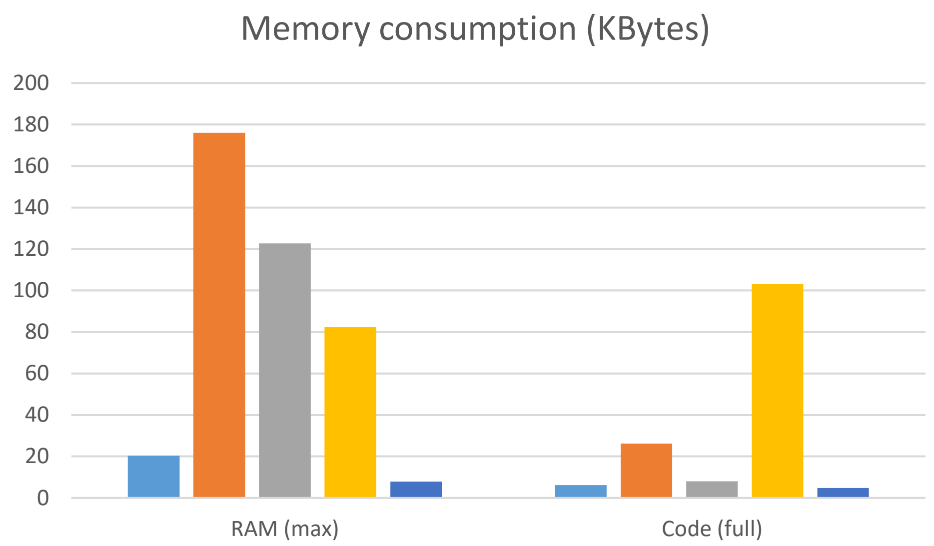


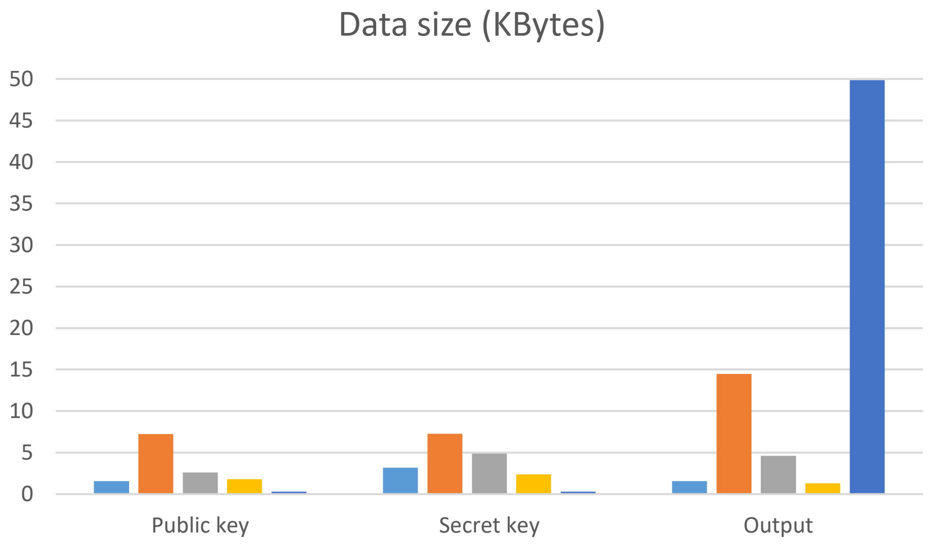
https://www.commoncriteriaportal.org/files/epfiles/1110V6b_pdf.pdf

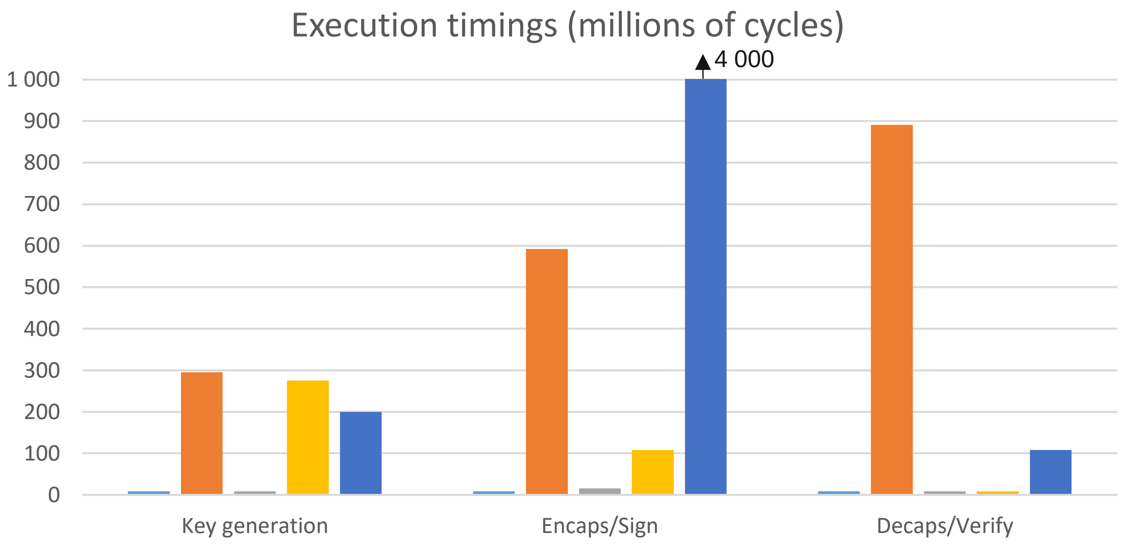
HIGH VARIABILITY

PQ algorithms:

- **are more demanding than classic ones**
- **have varied RAM, performance, and data size needs.**







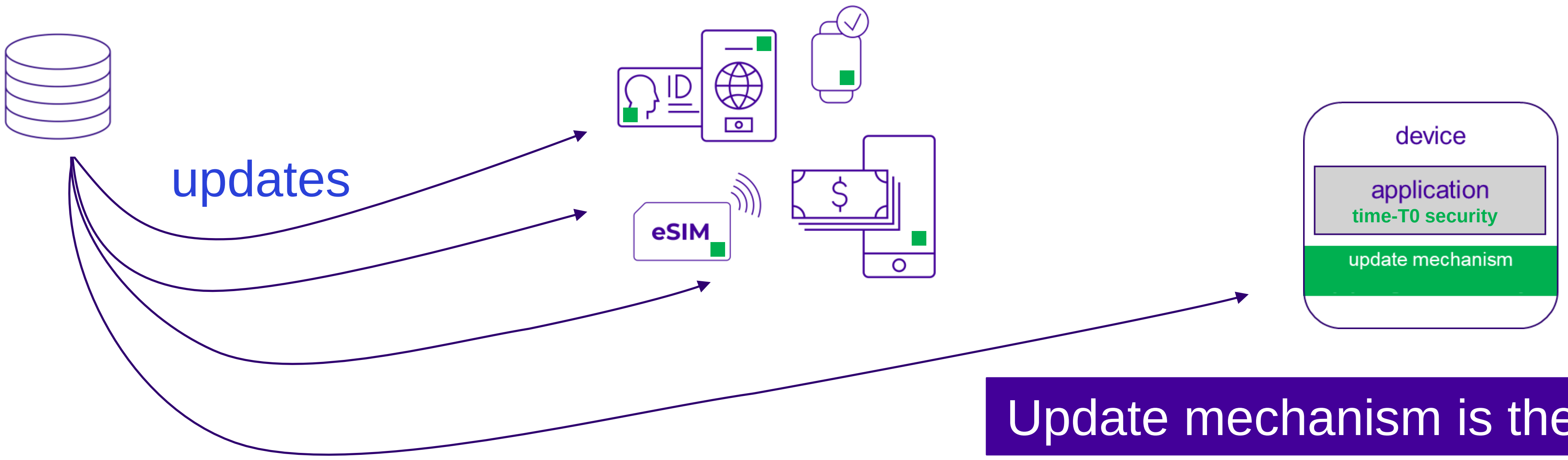
ML-KEM-1024 clean HQC-256 clean ML-DSA-87 clean Falcon-1024 ref SLH-DSA-SHAKE-256f-simple clean

IDEMIA SECURE TRANSACTIONS

Source: https://github.com/mupq/pqm4/blob/master/benchmarks.md

PRACTICAL USE-CASE

CRYPTO-AGILITY MECHANISM



Update mechanism is the root of trust

Crypto-agility requires a post-quantum, highly and long-term secure mechanism to:

1. Authenticate the provenance of the update
   → Hash-Based Signature XMSS (next slide)

2. Protect data (code IP, credentials)
   → AES-256 based protection

HASH-BASED SIGNATURES

NIST Special Publication 800-208

Recommendation for Stateful Hash-Based Signature Schemes

David A. Cooper
Daniel C. Apon
Quynh H. Dang
Michael S. Davidson
Morris J. Dworkin
Carl A. Miller
Computer Security Division
Information Technology Laboratory

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-208

October 2020

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Walter Copan, NIST Director and Under Secretary of Commerce for Standards and Technology

- Over 40 years of history (Lamport 1979).
- Security relies solely on hash functions (no new mathematical problem).

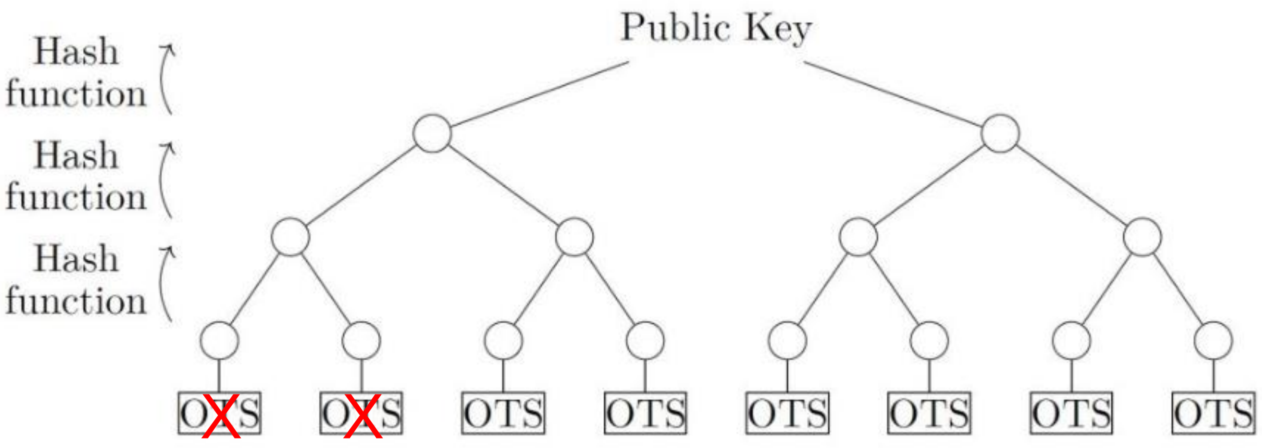
➔ Quantum-resistant.

- **XMSS** and **LMS**: Standardized by NIST in a separated process in 2020, also IETF RFC 8391

Highly trusted

Recommended (included in non-hybrid protocols):
→ by BSI
→ by ANSSI
→ by NSA (included in Suite 2.0)

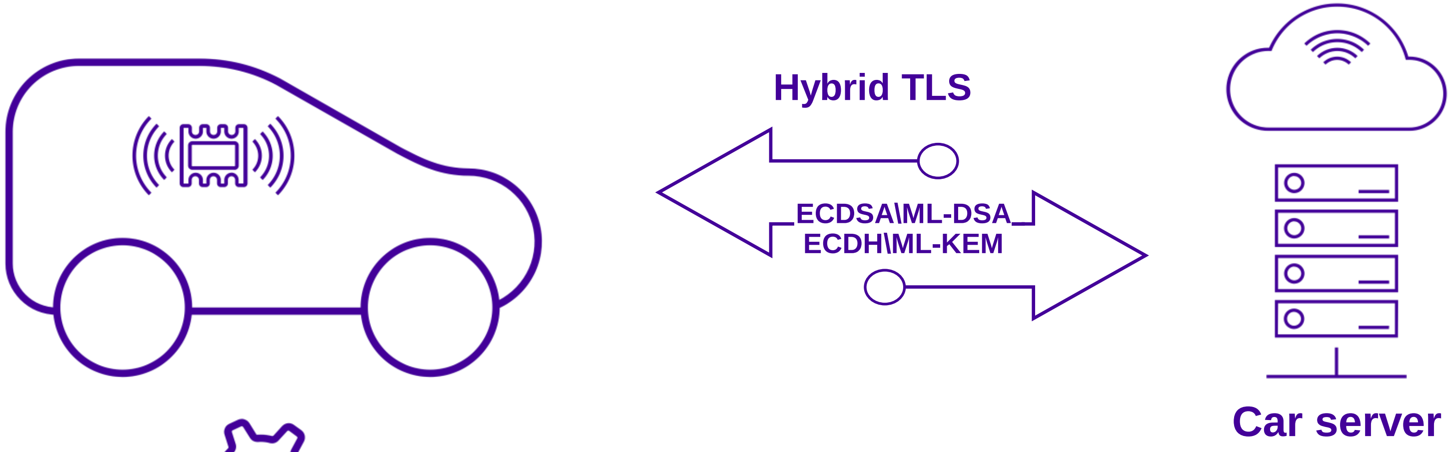
Downside: Stateful signature schemes:
- limited number of signatures can be done
- decided at key generation
- careful management of the secret key required



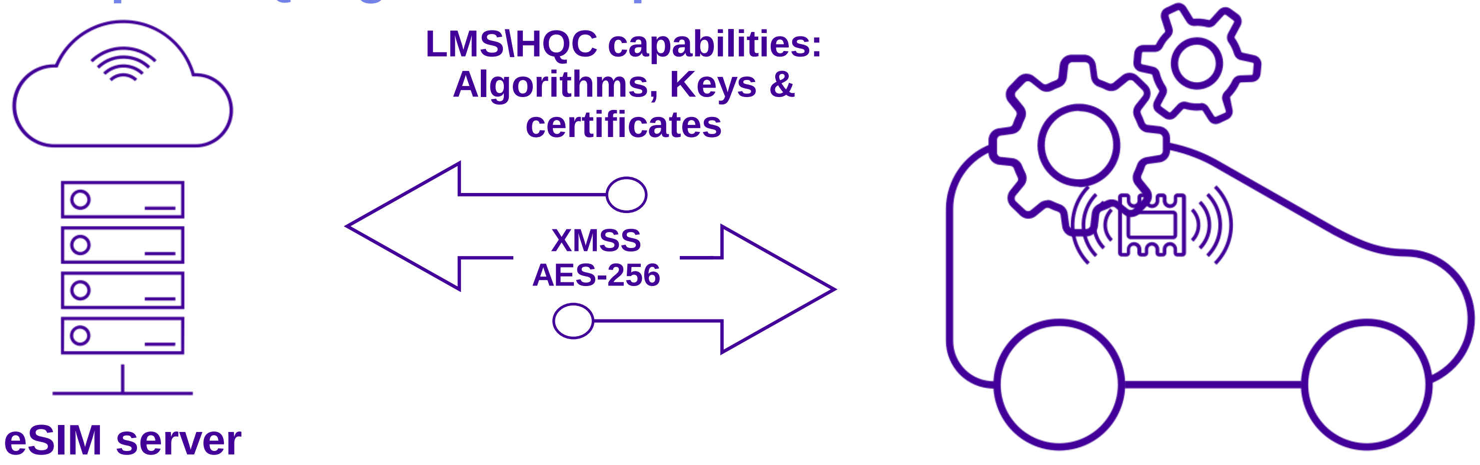
REAL-CASE EXAMPLE

▪ Step 1: PQ hybrid communication

Target
A TLS-like protocol providing:
- mutual authentication
- and key exchange



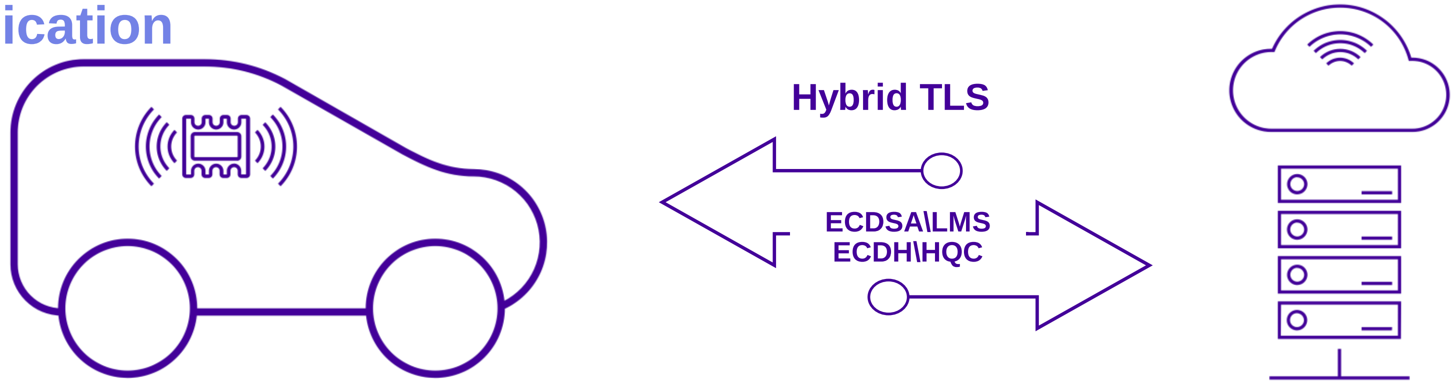
▪ Step 2: PQ algorithms update



Content
- Installation of the new crypto algos
- New credentials (keys and hybrid certificates)
- Protection overhead (encryption and signature)

▪ Step 3: Updated PQ hybrid communication

Results
~ 82 KB for the update
~ 22 sec to install



CONCLUSION

- **Crypto-agility demonstrated on a real product**
- **Integrated with a robust post-quantum (PQ) mechanism**
- **Proves feasibility, even on constrained platforms like smart cards**

- **Key Takeaways**
  - **Resource needs vary** widely and are difficult to anticipate
  - **Coordinated migration** across the entire system is essential

THANK YOU FOR YOUR ATTENTION

Christophe GIRAUD
Cryptography & Product Security Manager
Cryptography & Security Labs

christophe.giraud@idemia.com

IDEMIA GROUP

www.idemia.com