POST-QUANTUM CRYPTO: THE EMBEDDED CHALLENGE

Joost Renes

SEPTEMBER 2021

SECURE CONNECTIONS FOR A SMARTER WORLD

PUBLIC

AUTOMOTIVE

70%

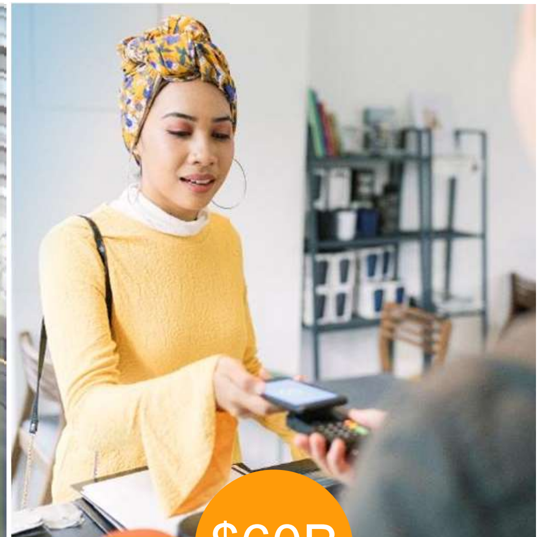
70% connected cars by 2025

INDUSTRIAL & IOT

$12B

IoT Edge & end nodes from **6B units** in 2021 to **12B units** in 2025

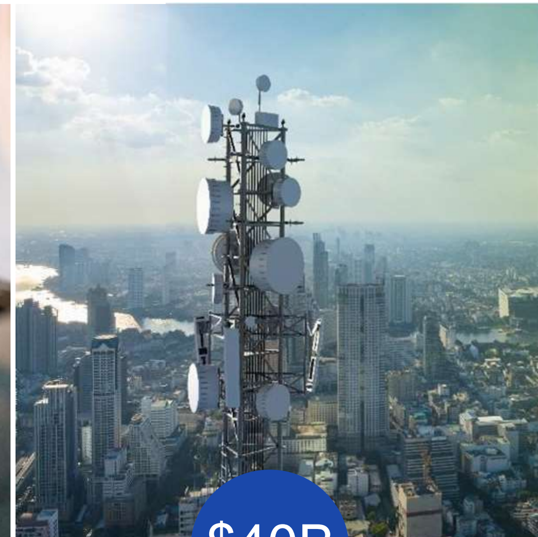
MOBILE



$60B

Tagging **60B products** per year by 2025

COMMUNICATION INFRASTRUCTURE

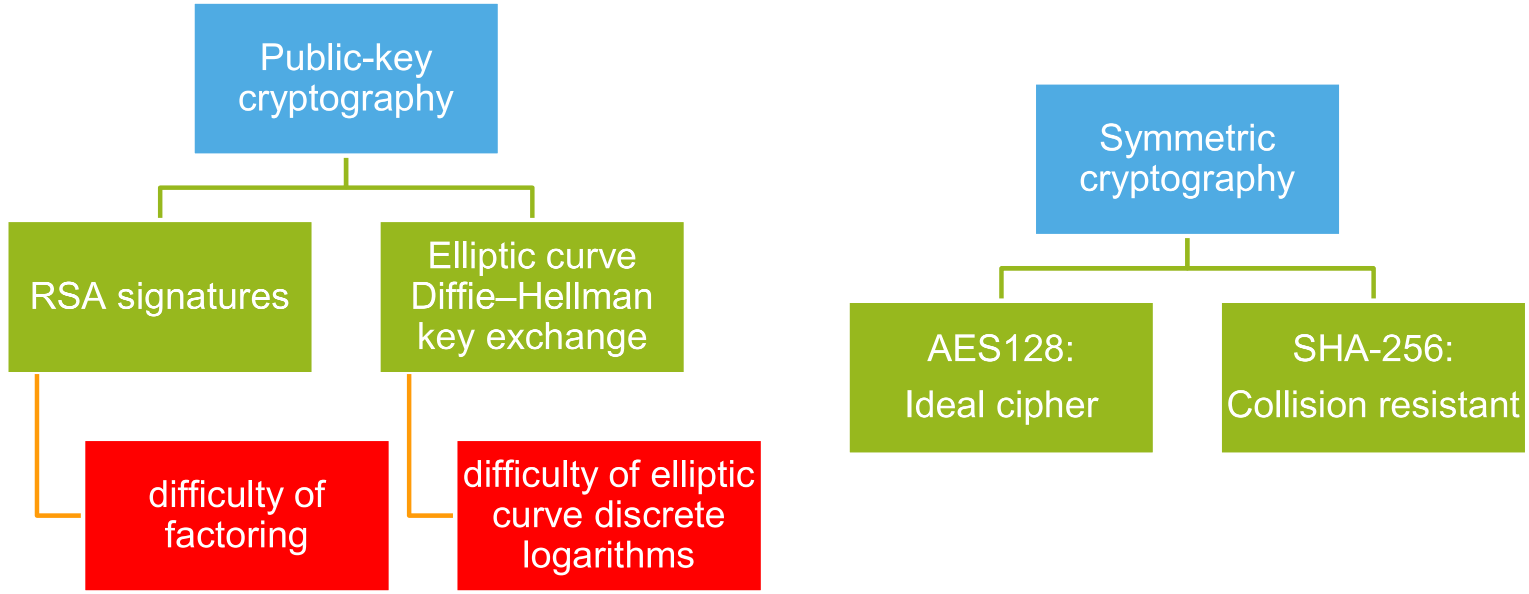


$40B

Secure anchors & services for **40B processors**

1. Source: NXP, Strategy Analytics, Evercore, Ericsson, IDTechex,

CONTEMPORARY CRYPTOGRAPHY
E.G. TLS-ECDHE-RSA-AES128-GCM-SHA256



CONTEMPORARY CRYPTOGRAPHY
E.G. TLS-ECDHE-RSA-AES128-GCM-SHA256

Public-key cryptography

- RS… …res
  - difficulty of factoring
- Di… …an
  - difficulty of elliptic curve discrete logarithms

Broken, i.e. polynomial key-recovery by a quantum computer

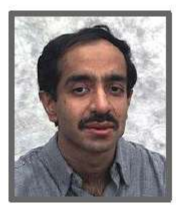
Shor's algorithm (1994)

Increased security level to guarantee 128-bit security

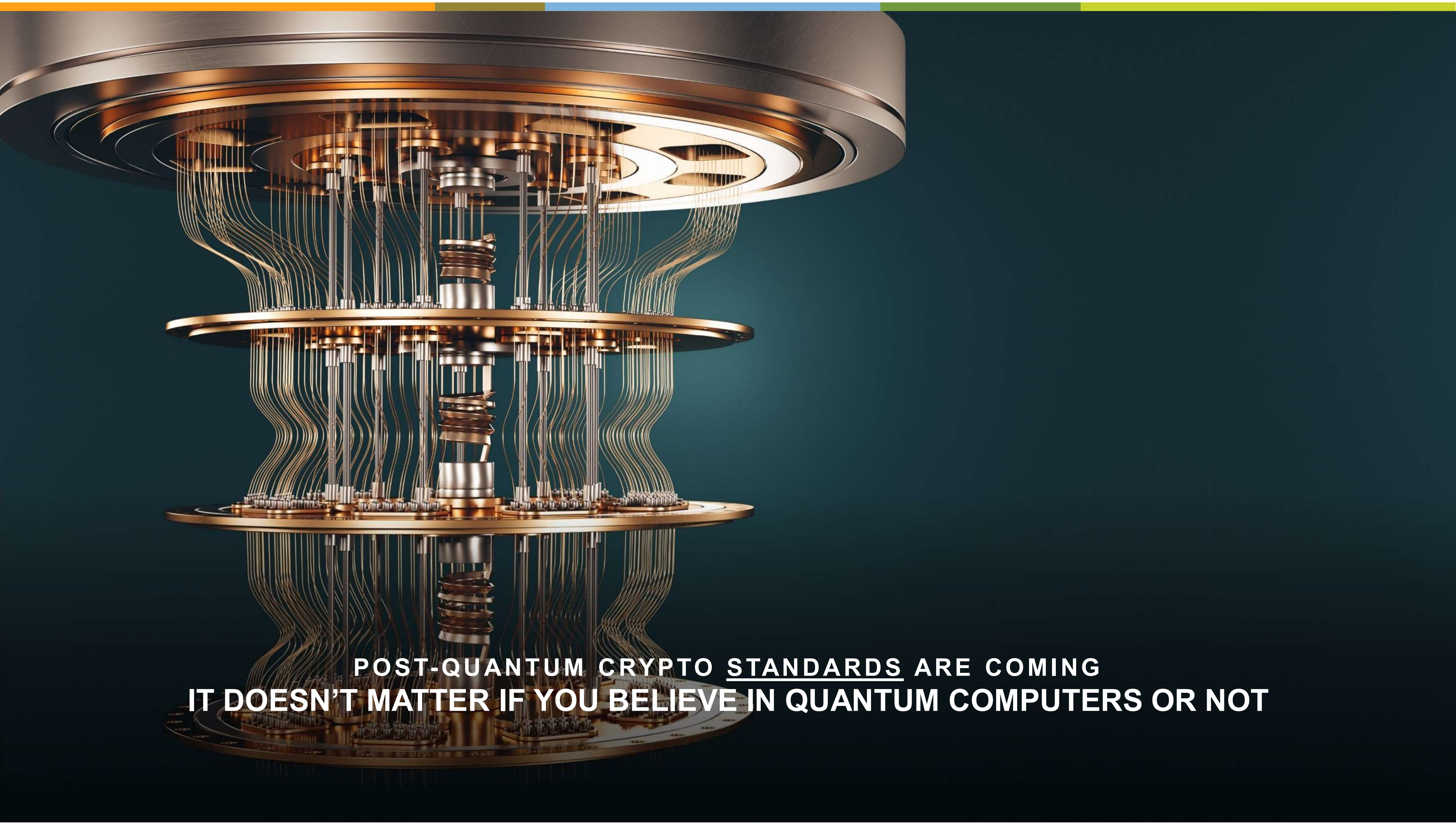
Symmetric cryptography

- AES256: Ideal cipher
- ≥ SHA-256: Collision resistant

With the invention of a full-scale, available quantum computer our security paradigm is undermined



Grover's algorithm (1996)

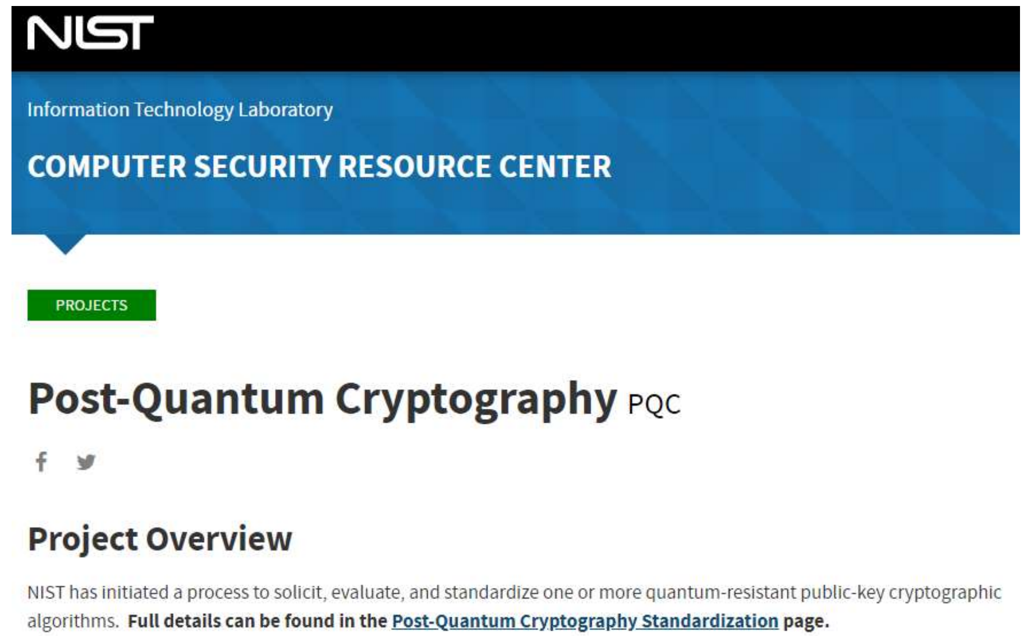


POST-QUANTUM CRYPTO STANDARDS ARE COMING

IT DOESN’T MATTER IF YOU BELIEVE IN QUANTUM COMPUTERS OR NOT

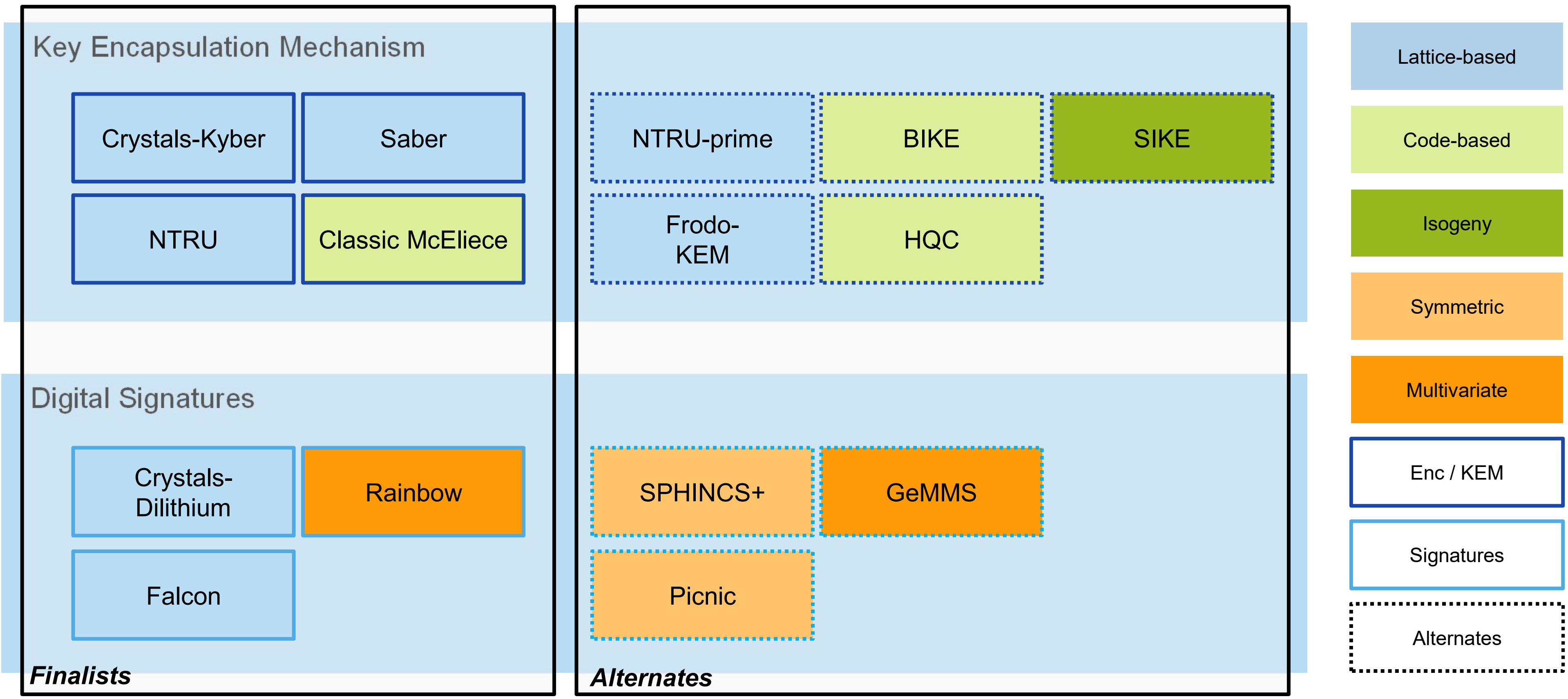
LONG TERM STANDARDS (2022/2024)– NIST (ROUND 3, JULY 2020)

September 16, 2016	Feedback on call for proposals
Fall 2016	Formal call for proposals
November 2017	Deadline for submissions
Early 2018	Workshop – submitters' presentations
3-5 years	**Analysis phase** **Jan 2019: Round 2** **July 2020: Round 3 announced** **2021/2022: Winners**
2 years later (2022/2024)	Draft standards ready



NIST update summer 2021:
Winners will be announced by the end of <u>this</u> year

LONG TERM STANDARDS (2022/2024)– NIST (ROUND 3, JULY 2020)



EMBEDDED USE CASES

Digital signatures (verification)

Secure boot

Mobile. Firmware integrity

Over-the-air updates

Automotive. Firmware authentication, smart car access

Key-Exchange

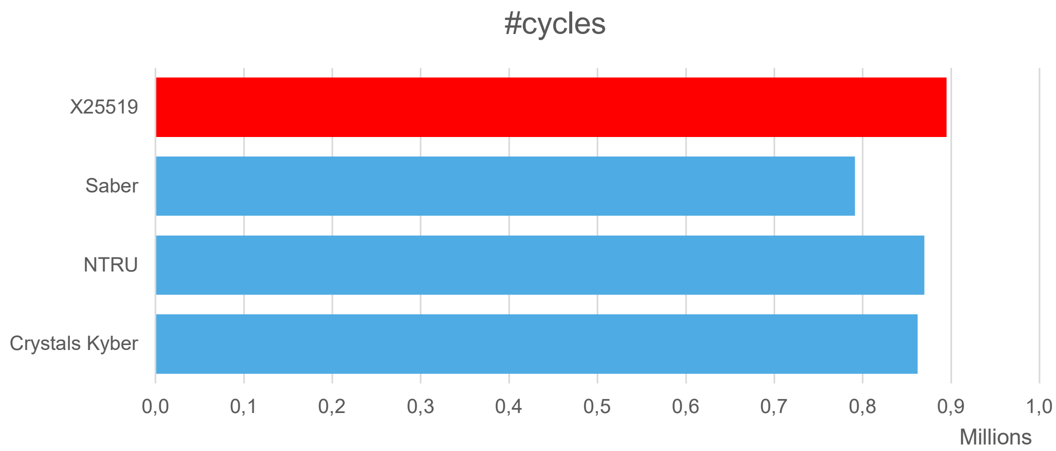
Secure element communication

Industrial & IoT. Communication within IoT devices

Trust provisioning

Industrial & IoT. Communication by IoT devices

CLASSIC VS LATTICES IN PRACTICE (1/2)

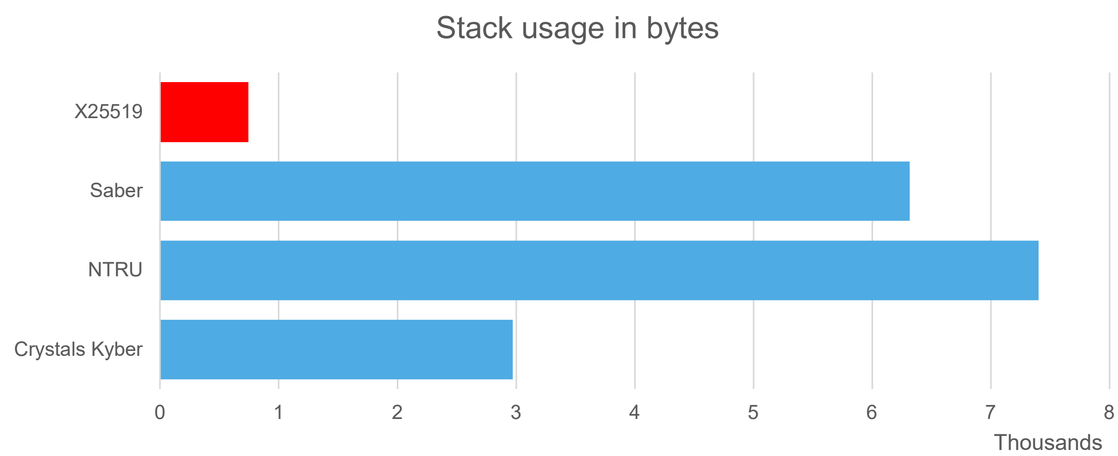


- KEM finalists example excluding Classic McEliece (public key sizes range from 255 KiB to 1,326 KiB)
- Numbers from pqm4 library on Cortex-M4 [A]
- X25519 numbers from [B]

Note: Cortex-M4 is high-end for many embedded applications

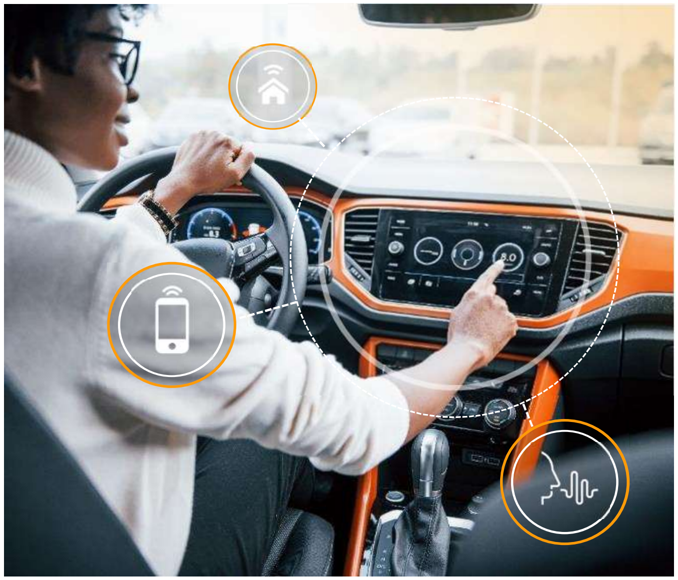
[A] Kannwischer, Rijneveld, Schwabe, Stoffelen. pqm4: Testing and Benchmarking NIST PQC on ARM Cortex-M4. PQC standardization Conference, 2019.
[B] Fujii, Aranha: *Curve25519 for the Cortex-M4 and beyond*. LatinCrypt 2017.

CLASSIC VS LATTICES IN PRACTICE (2/2)



- This ignores RAM / flash memory for key material
- Typical max. stack requirements:
  1k, 2k, 4k bytes → serious challenge

REUSING EXISTING COPROCESSORS



Grundzüge einer arithmetischen Theorie der algebraischen Grössen.

(Von *L. Kronecker.*)

(Abdruck einer Festschrift zu Herrn *E. E. Kummers* Doctor-Jubiläum, 10. September 1881.)

- Idea [A]: Re-use contemporary coprocessors
- Can do better: Combine symbolic NTTs with Kronecker substitution in a smart way
- Reduces number of operations required on the coprocessor

[A] Albrecht, Hanser, Hoeller, Pöppelmann, Virdia, Wallner: Implementing RLWE-based schemes using an RSA co-processor. TCHES 2019

[B] Harvey. Faster polynomial multiplication via multipoint Kronecker substitution. J. Sym. Comp. 2009.

[C] Bos, Renes and Vredendaal: Polynomial Multiplication with Contemporary Co-Processors: Beyond Kronecker, Schönhage-Strassen & Nussbaumer. USENIX 2022

STANDARDS – SHORT TERM (2020/2021)
STATEFUL HASH-BASED SIGNATURE SCHEMES: XMSS

```
Internet Research Task Force (IRTF)                          A. Huelsing
Request for Comments: 8391                                 TU Eindhoven
Category: Informational                                        D. Butin
ISSN: 2070-1721                                            TU Darmstadt
                                                              S. Gazdag
                                                             genua GmbH
                                                            J. Rijneveld
                                                     Radboud University
                                                             A. Mohaisen
                                         University of Central Florida
                                                               May 2018


                XMSS: eXtended Merkle Signature Scheme
```

XMSS signatures
RFC 8391 (2018)
NIST SP 800-208 (2020)
Support from industry and government (e.g., BSI)

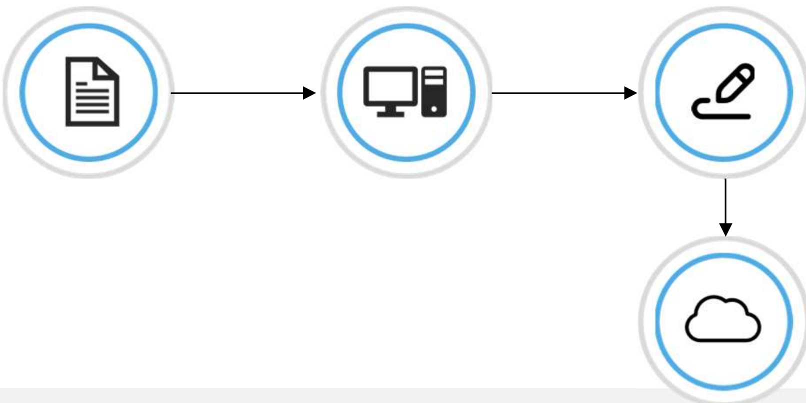
Not for all use-cases → need to keep a state
Main operation: thousands of hashes per signature generation / verification

NIST Special Publication 800-208

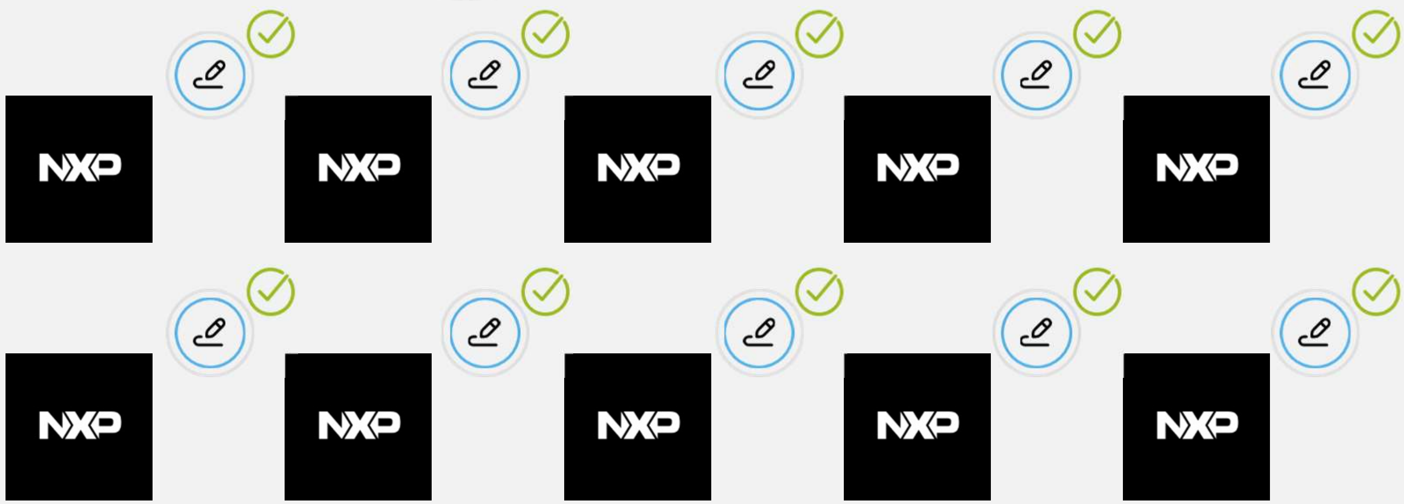
Recommendation for Stateful Hash-Based Signature Schemes

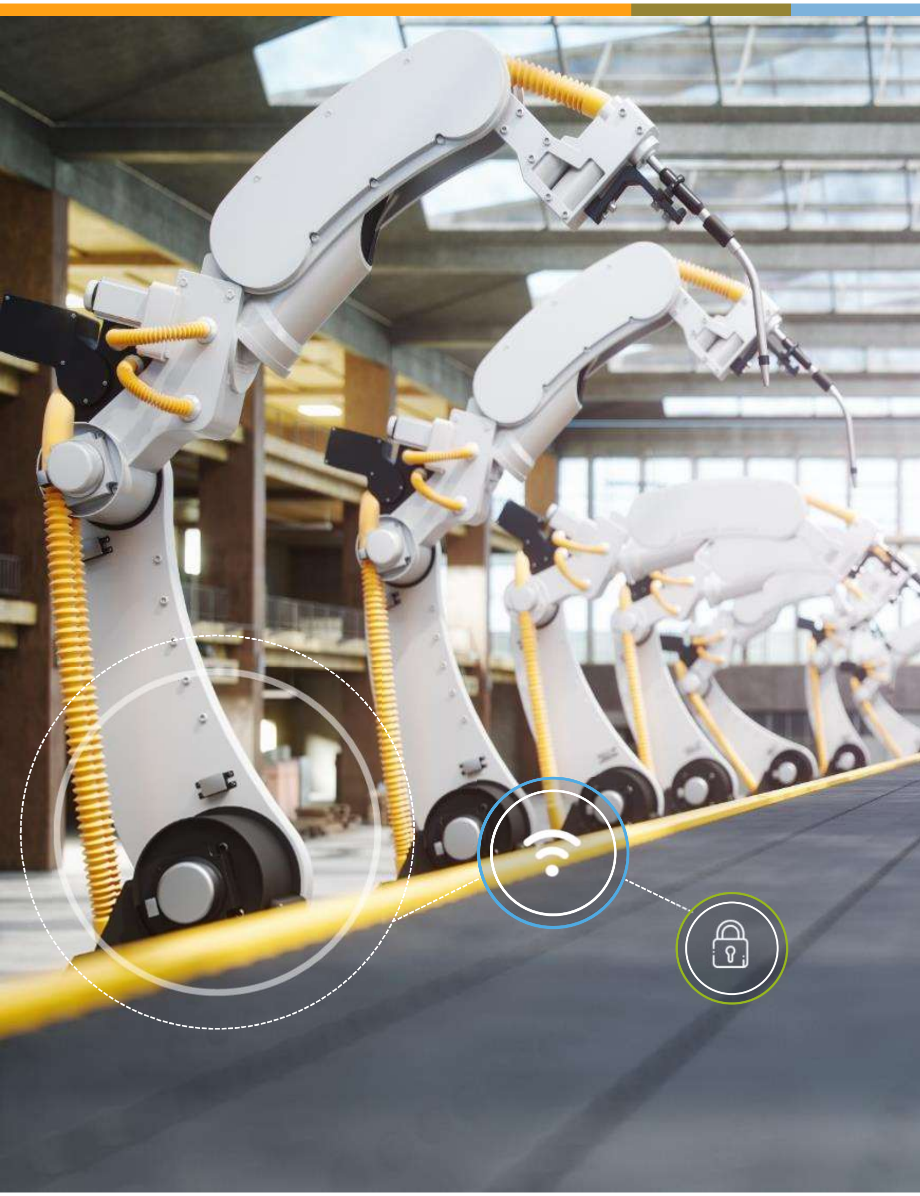
David A. Cooper
Daniel C. Apon
Quynh H. Dang
Michael S. Davidson
Morris J. Dworkin
Carl A. Miller

USE-CASE: OVER-THE-AIR UPDATES



Signature **verification** done **many times** by **low-resource** devices. Speed it up by allowing a performance loss for signing on a **powerful server**.





FASTER SIGNATURE VERIFICATION

Use / extend trade-off technique from [A]

New proof of security

New statistical analysis of the speed-up provided

Fully compatible with the standard

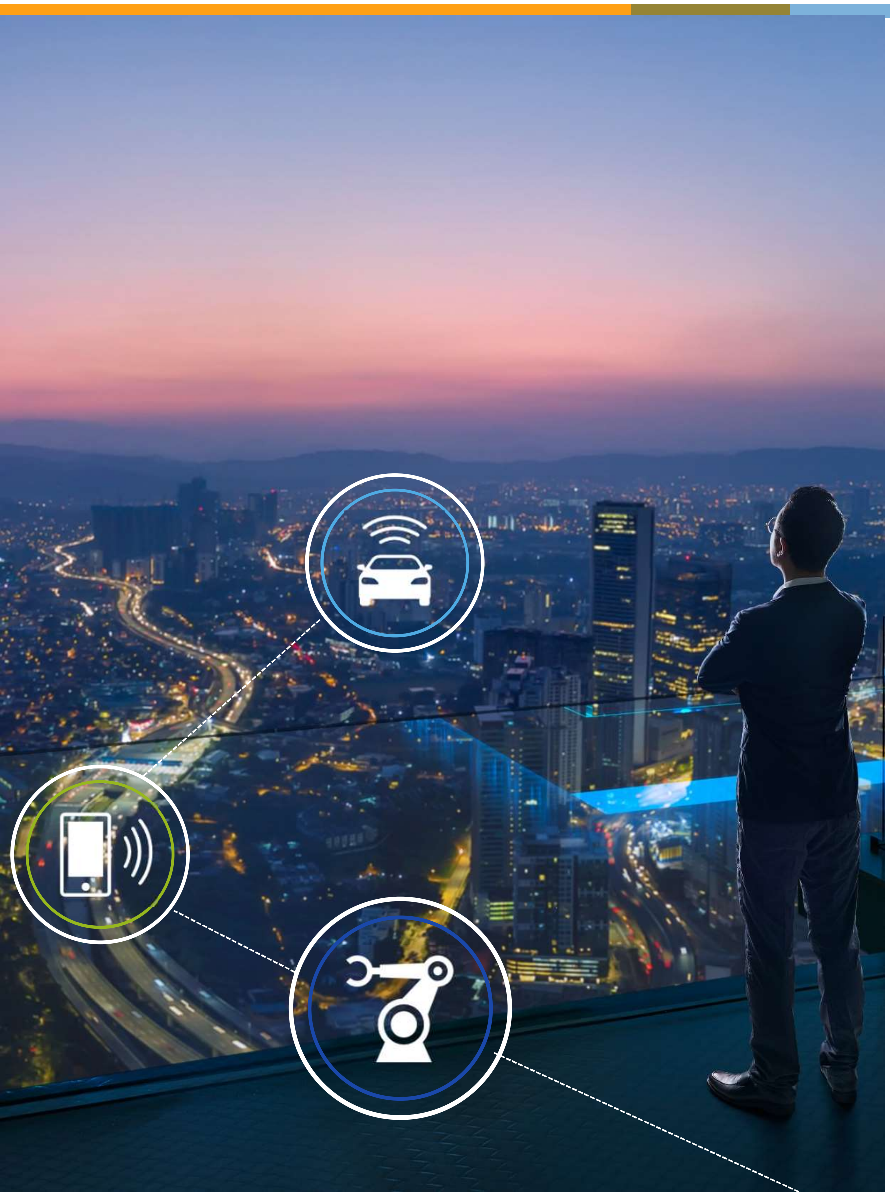
Uses hash-precomputation from [B]

Implementation	Signature Verification (10^6 cycles)	Signature generation (seconds)
Ref	13.85	< 0.01
New (t=10)	7.87	0.04
New (t=27)	**6.56**	60

[A] Perin, Zambonin, Martins, Custódio, Martina: *Tuning the Winternitz hash-based digital signature scheme*. IEEE ISCC 2018.

[B] Campos, Kohlstadt, Reith, Stöttinger: *LMS vs XMSS: Comparison of Stateful Hash-Based Signature Schemes on ARM Cortex-M4*. AFRICACRYPT 2020

[C] Bos, Hülsing, Renes, van Vredendaal: Rapidly Verifiable *XMSS Signatures*. TCHES 2021



CONCLUSIONS

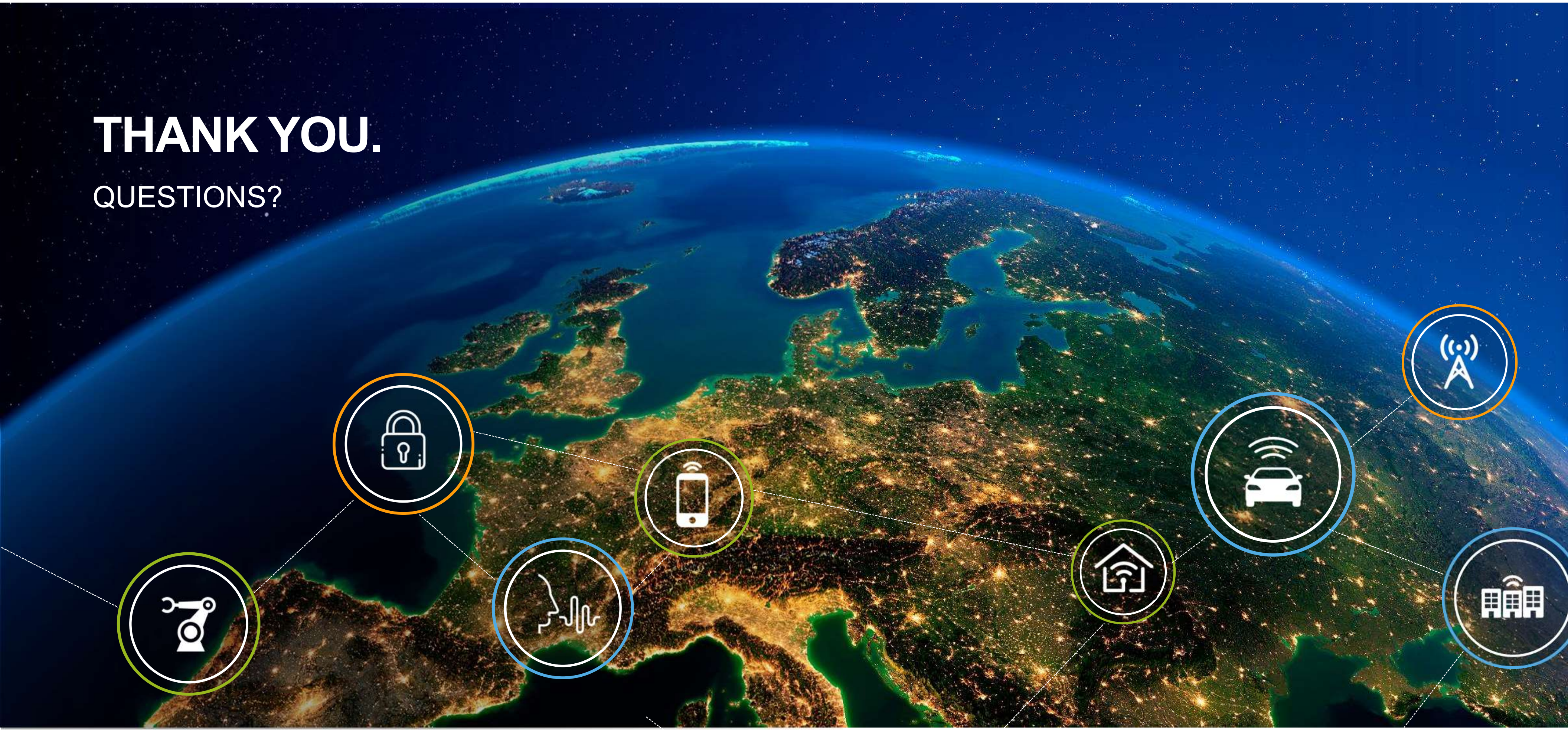
- Irrelevant if the quantum threat is real or not
  → Post-quantum crypto support is already being requested
- Standards are coming
- We didn’t even talk about hardened implementations

Short term (2020)
Stateful-hash signature schemes

Long term (2022/2024)
NIST standards → KEM, digital signatures
Possibly multiple winners per category

THANK YOU.

QUESTIONS?



SECURE CONNECTIONS
FOR A SMARTER WORLD

SECURE CONNECTIONS
FOR A SMARTER WORLD