POST-QUANTUM CRYPTO: THE EMBEDDED CHALLENGE

Joost Renes

MARCH 2021

SECURE CONNECTIONS FOR A SMARTER WORLD

POST-QUANTUM CRYPTO STANDARDS ARE COMING

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

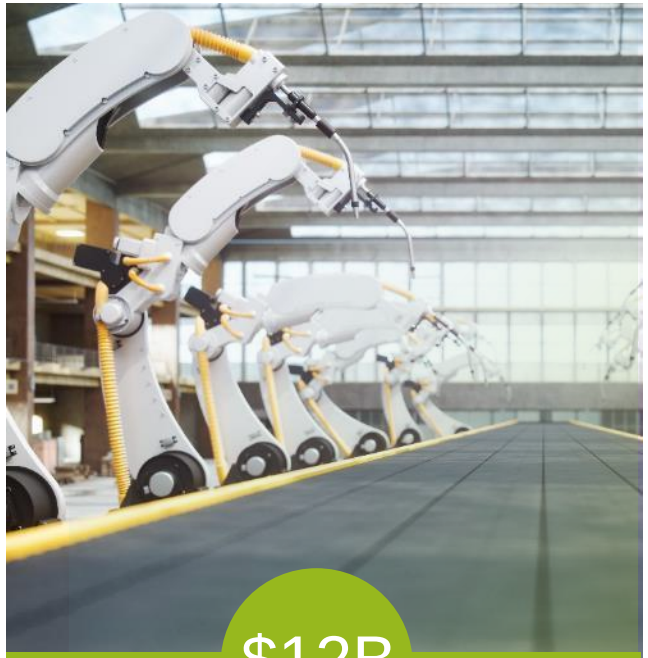
POST-QUANTUM CRYPTO IS ON THE HORIZON

AUTOMOTIVE

70%

70% connected cars by 2025

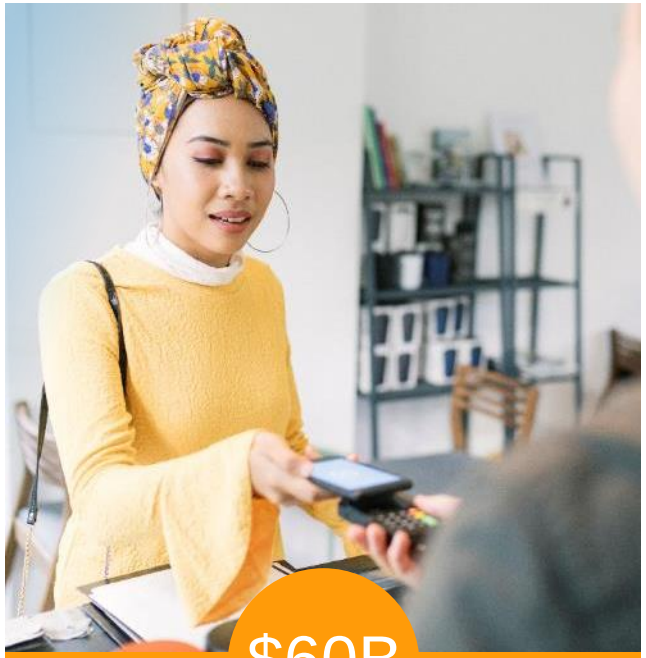
INDUSTRIAL & IOT



$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**

What is the impact on the billions of embedded devices?

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

EMBEDDED USE CASES

Digital signatures (verification)

Secure boot

Mobile. Firmware integrity for payment terminals

Over-the-air updates

Automotive. Firmware authentication, smart car access

Key-Exchange

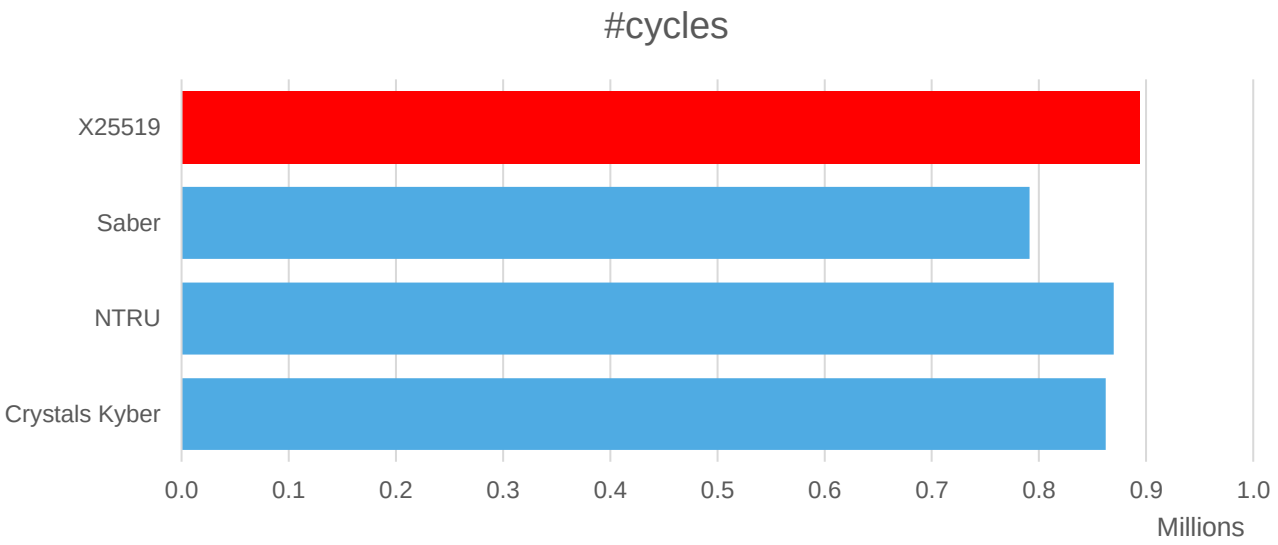
Secure element communication

Industrial & IoT. Communication within IoT devices

Trust provisioning

Industrial & IoT. Communication by IoT devices

CLASSIC VS LATTICES IN PRACTICE (1/2)



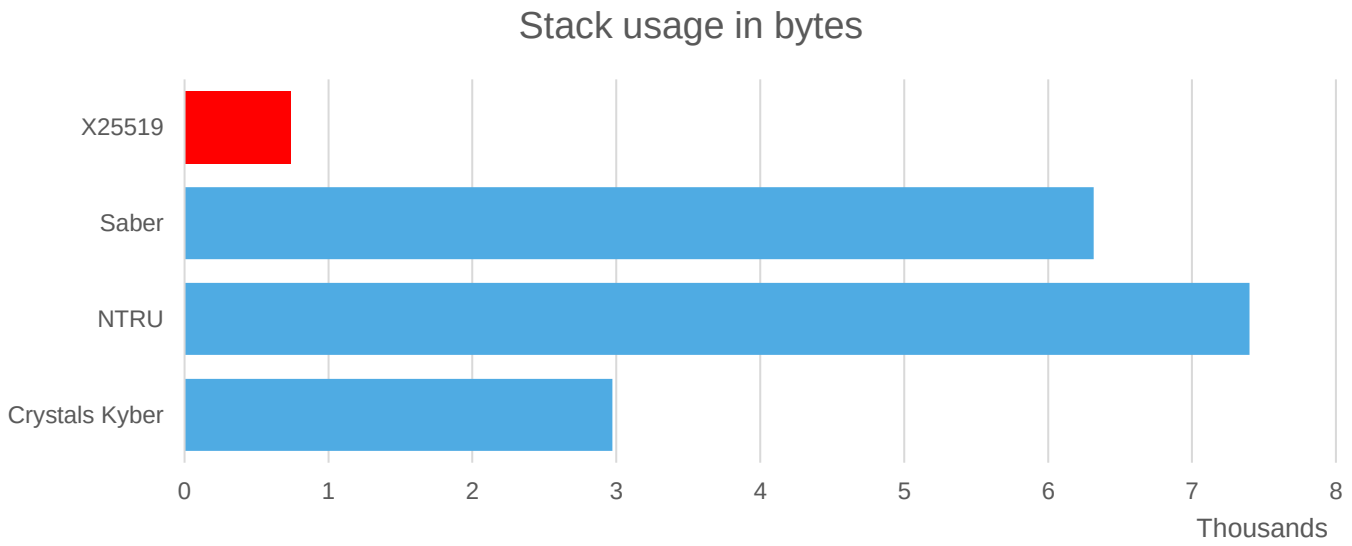
- KEM finalists example excluding Classic McEliece (public key sizes range from 255 KiB to 1,326 KiB)
- Numbers from pqm4 library on Cortex-M4 [A]
- X25519 numbers from [B]

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

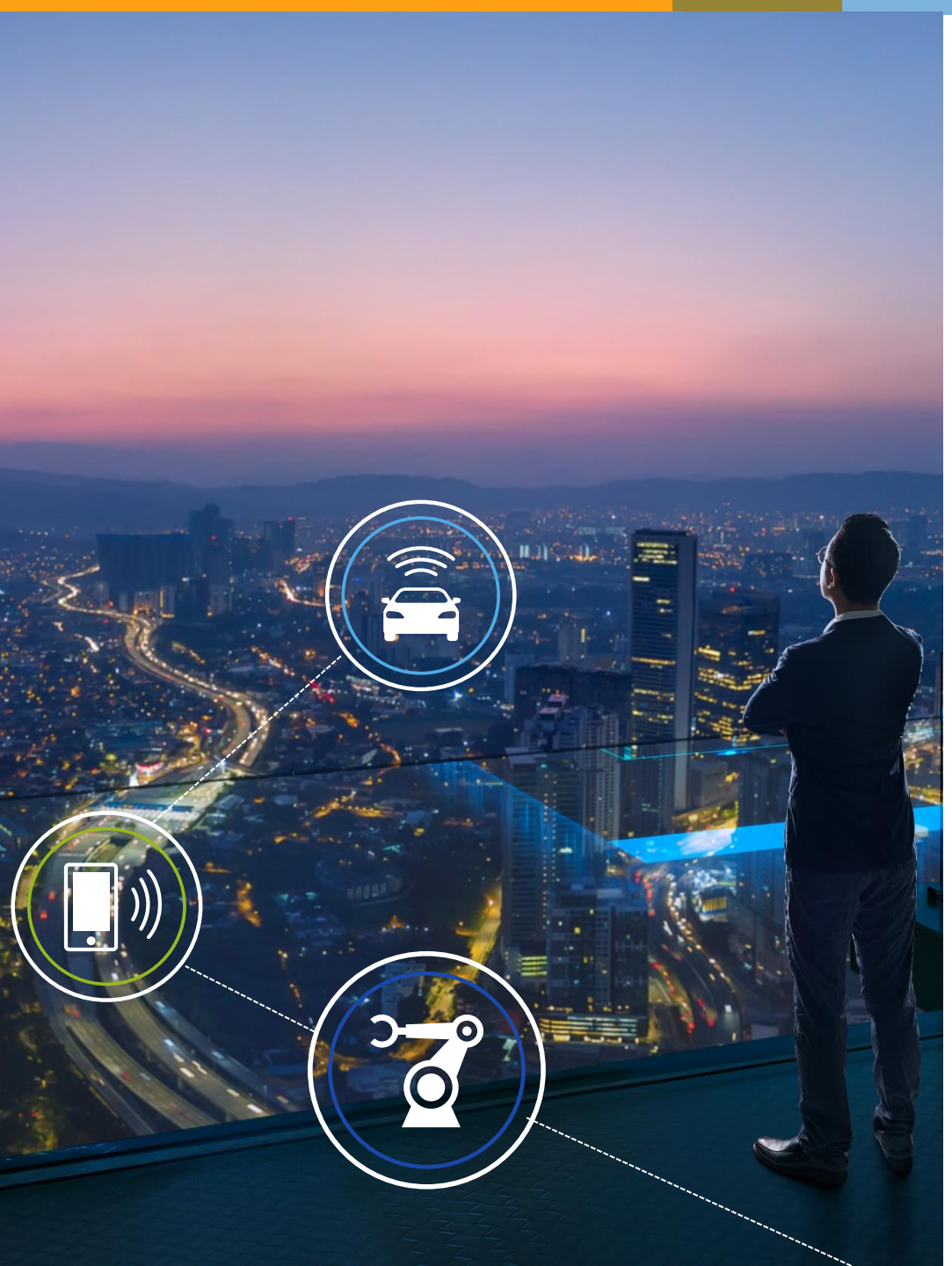
Grundzüge einer arithmetischen Theorie der algebraischen Grössen.

(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. Cryptology ePrint Archive, Report 2020/1303, IACR, 2020.



CONCLUSIONS

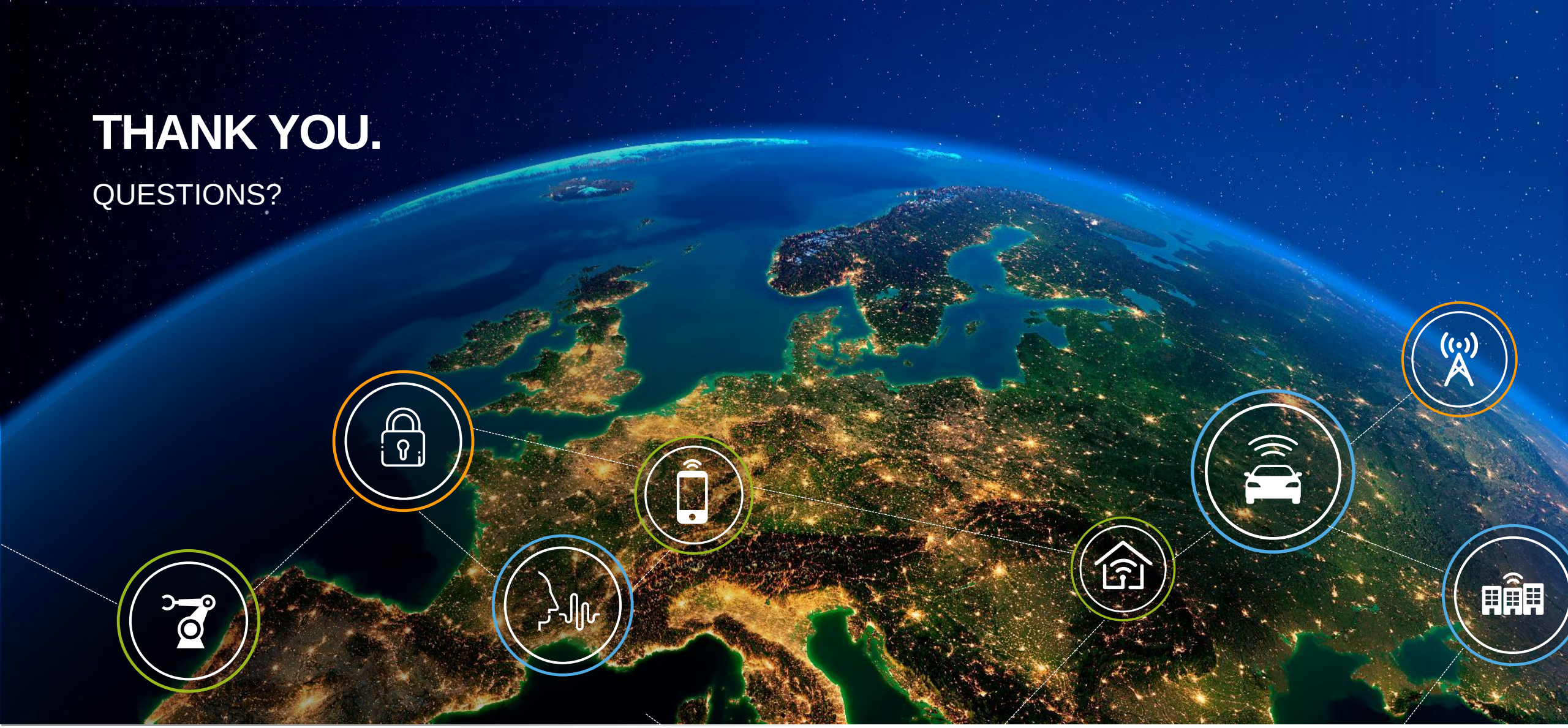
- Irrelevant if the quantum threat is real or not
  → Post-quantum crypto support is already being requested
- Standards are coming
- We didn't even talk about hardened implementations

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