POST-QUANTUM CRYPTO: THE EMBEDDED CHALLENGE

Joppe Bos

JANUARY 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

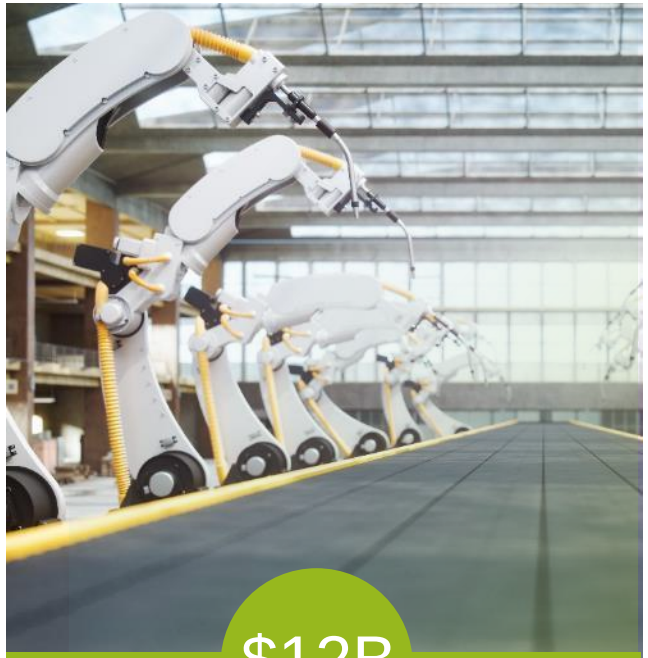
POST-QUANTUM CRYPTO IS ON THE HORIZON

AUTOMOTIVE

70%

70% connected cars by 2025

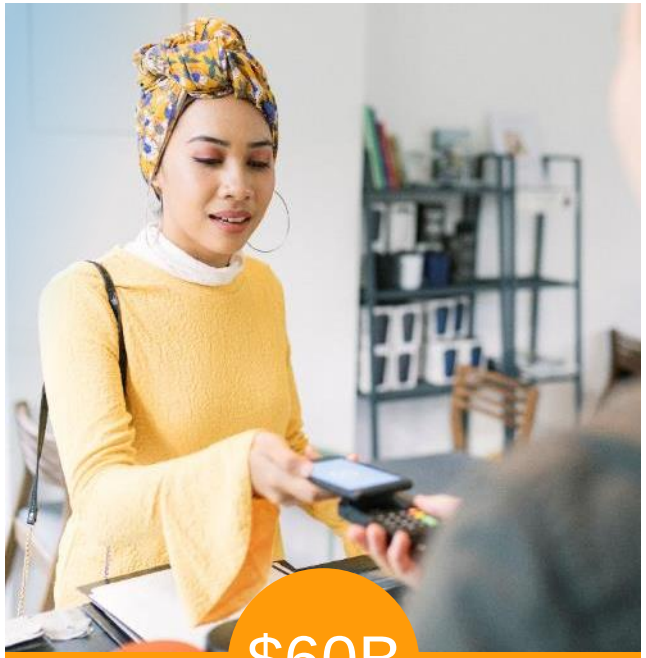
INDUSTRIAL & IOT



$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

Secure boot

Industrial & IoT. Firmware integrity for IoT devices

Over-the-air updates

Automotive. Firmware authentication, smart car access

Key-Exchange

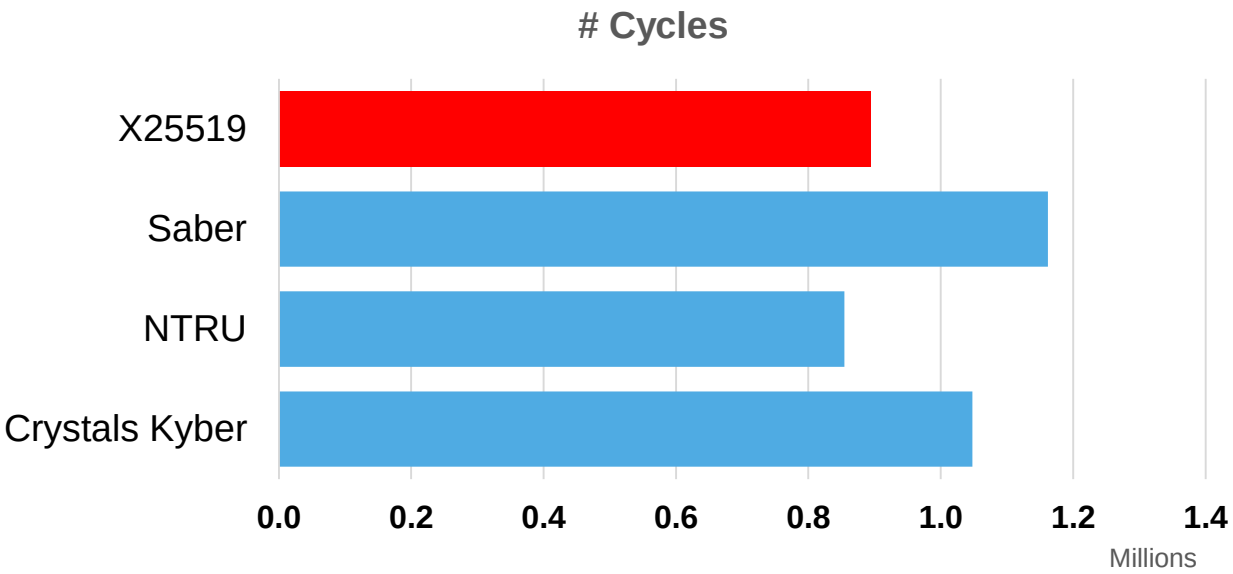
Secure element communication

Industrial & IoT. Communication within IoT devices

Trust provisioning

Industrial & IoT. Communication by IoT devices

CLASSIC VS LATTICES IN PRACTICE (1/2)

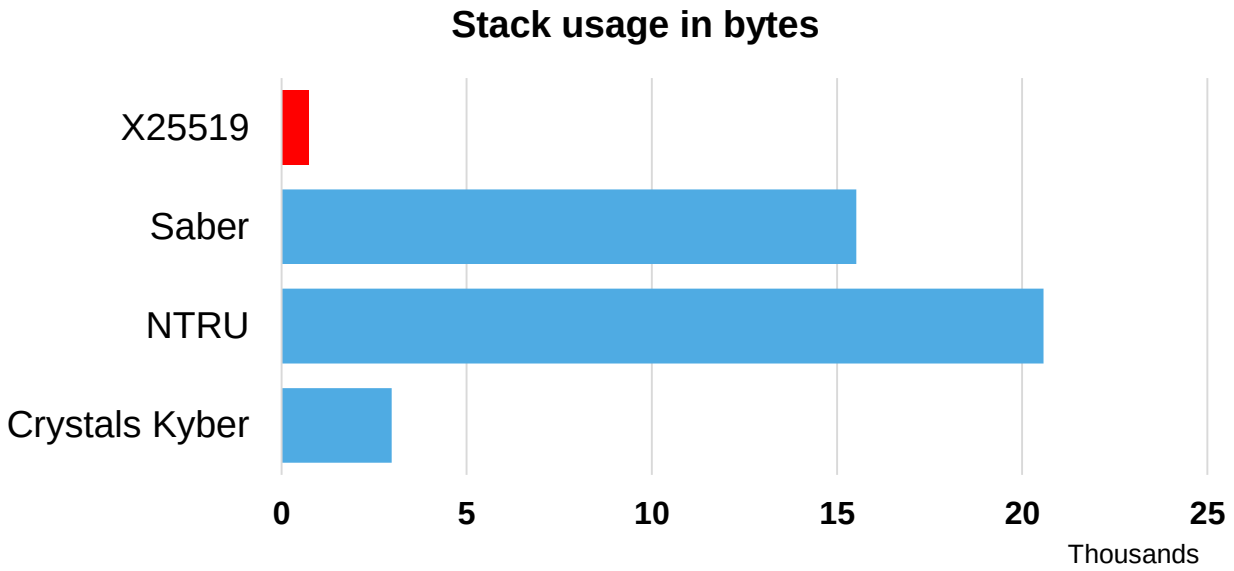


- KEM finalists example
- Numbers from pqm4 library on Cortex-M4 [A]
- X25519 numbers from [B]

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)



- Cortex-M4 is high-end for many embedded applications
- This ignores RAM / flash memory for key material
- Typical max. stack requirements:
  1k, 2k, 4k bytes → serious challenge

REUSING EXISTING COPROCESSORS (1/3)

Approach	Core	Structure	Size
RSA	Modular multiplication	$(\mathbb{Z}/n\mathbb{Z})^*$	n is 3072-bit
ECC	Elliptic curve scalar multiplication	$\mathrm{E}(\mathbb{F}_p)$	p is 256-bit
Lattice	Polynomial multiplication	$(\mathbb{Z}/q\mathbb{Z})[X]/(X^n+1)$	q is 16-bit n is 256

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

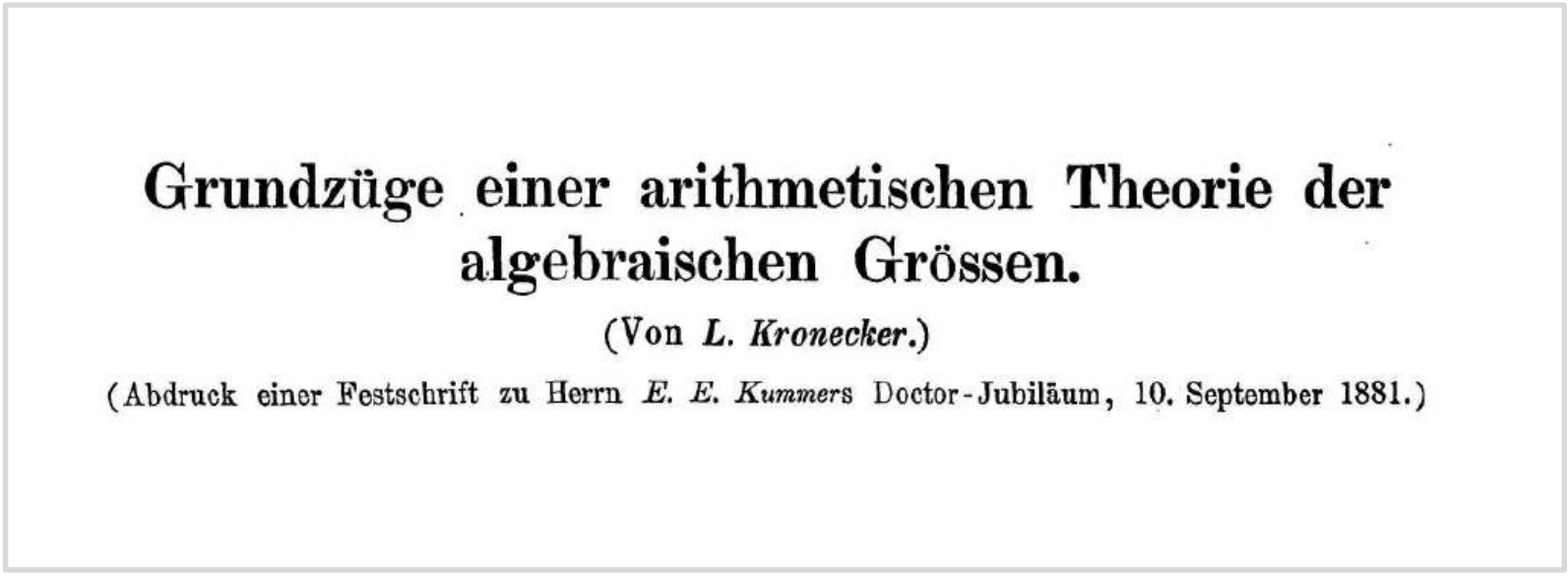
Lattice cryptography uses 16-bit coefficients, how to use our bignum coprocessors?

"Basic" idea [A] for 128-bit coprocessors

Pack multiple 16-bit coefficients in large 128-bit register

Ensure sufficient "space" is reserved to avoid overflow

REUSING EXISTING COPROCESSORS (2/3)



Grundzüge einer arithmetischen Theorie der algebraischen Grössen.

(Von *L. Kronecker.*)

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

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

Lattice cryptography uses 16-bit coefficients, how to use our bignum coprocessors?

“Basic” idea [A] for 128-bit coprocessors

Pack multiple 16-bit coefficients in large 128-bit register

Ensure sufficient “space” is reserved to avoid overflow

REUSING EXISTING COPROCESSORS (3/3)

Lattice	**Polynomial multiplication**	$(\mathbb{Z}/q\mathbb{Z})[X]/(X^n+1)$	**q is 16-bit** **n is 256**

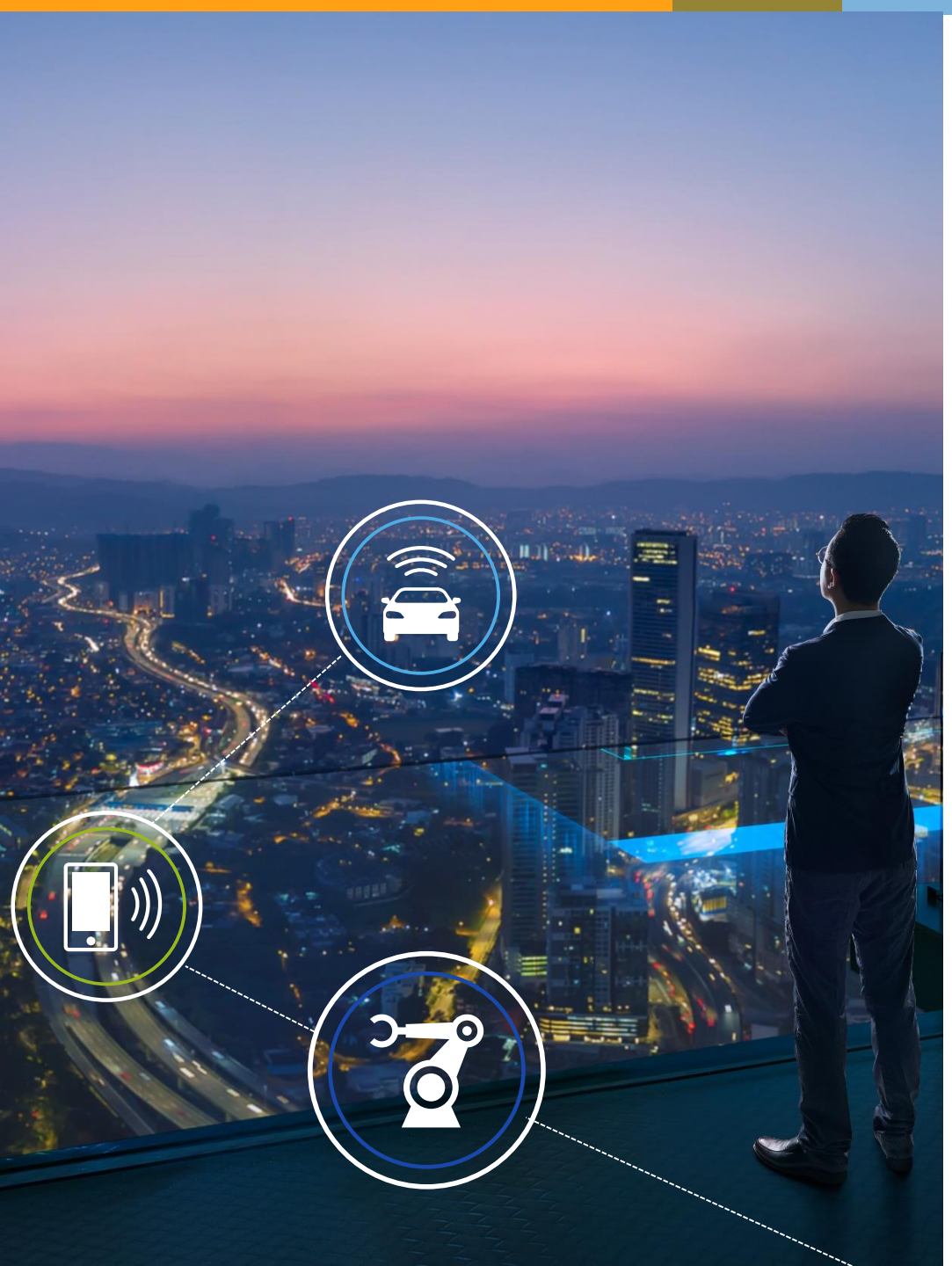
Can we do better?

Combine Schönhage-Strassen with Kronecker in a smart way

Use the fact that there exists roots of unity modulo $X^n + 1$ to construct fast symbolic NTTs

*Harvey. Faster polynomial multiplication via multipoint Kronecker substitution. J. Sym. Comp. 2009.
New: Bos, Renes and Vredendaal: Polynomial Multiplication with Contemporary Co-Processors: Beyond Kronecker, Schönhage-Strassen & Nussbaumer. Cryptology ePrint Archive, Report 2020/1303, IACR, 2020.

Kronecker	1 x 8192-bit multiplication	4096 x 128-bit multiplications
Harvey*	2 x 4096-bit multiplication	2048 x 128-bit multiplications
Harvey* / New	4 x 2048-bit multiplication	1024 x 128-bit multiplications
New	8 x 1024-bit multiplication	512 x 128-bit multiplications
New	16 x 512-bit multiplication	256 x 128-bit multiplications



CONCLUSIONS

- Post-quantum crypto support is already being requested
  → Irrelevant if the quantum threat is real or not

Short term (now)
Stateful-hash signature schemes

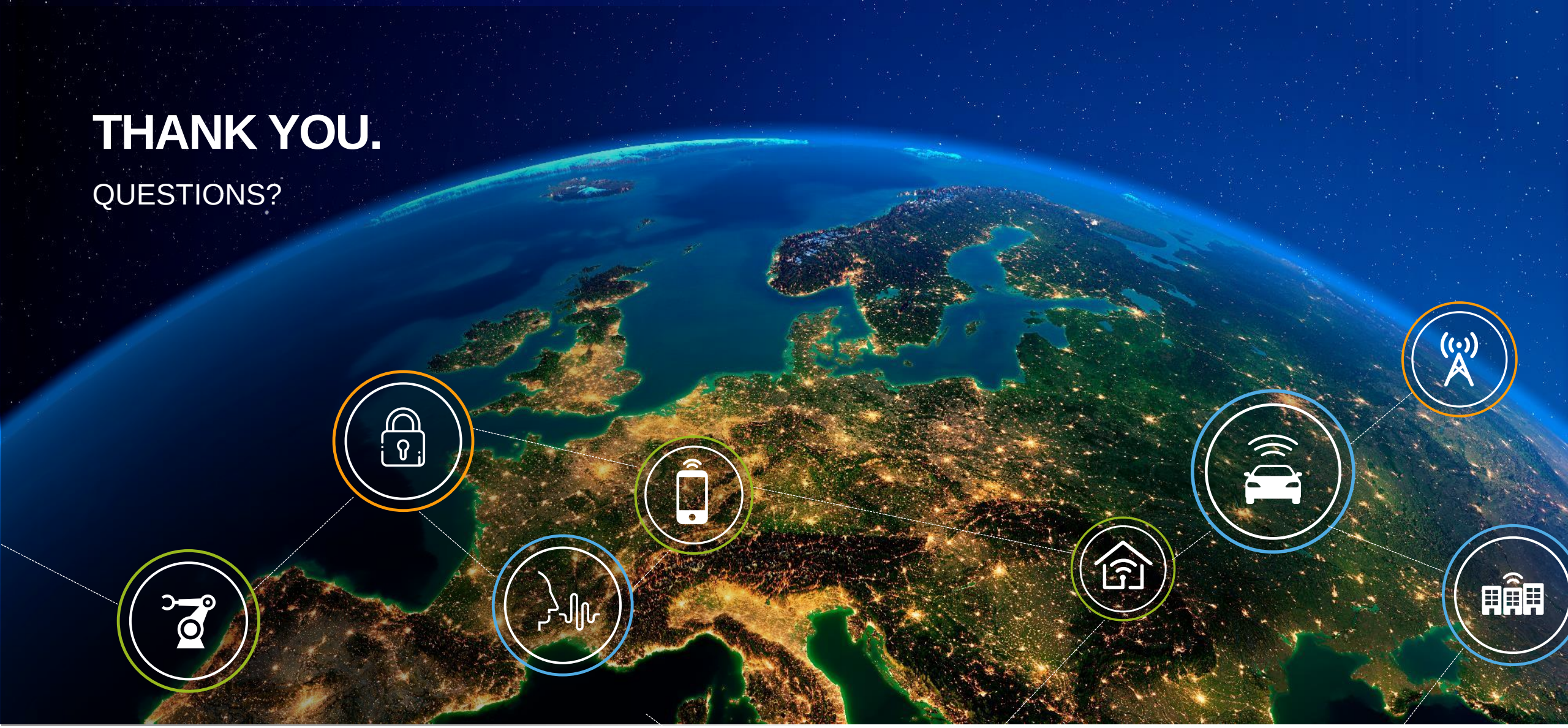
Long term (2022/2024)
NIST standards → KEM, digital signatures
Possibly multiple winners per category

We didn't even talk about hardened implementations

Interesting times ahead.

THANK YOU.

QUESTIONS?



SECURE CONNECTIONS
FOR A SMARTER WORLD

SECURE CONNECTIONS
FOR A SMARTER WORLD