POST-QUANTUM CRYPTOGRAPHY: A NEW CYBERSECURITY ERA

Joppe Bos, Senior Principal Cryptographer
Competence Center Crypto & Security

OCTOBER 2022

NXP | SECURE CONNECTIONS FOR A SMARTER WORLD

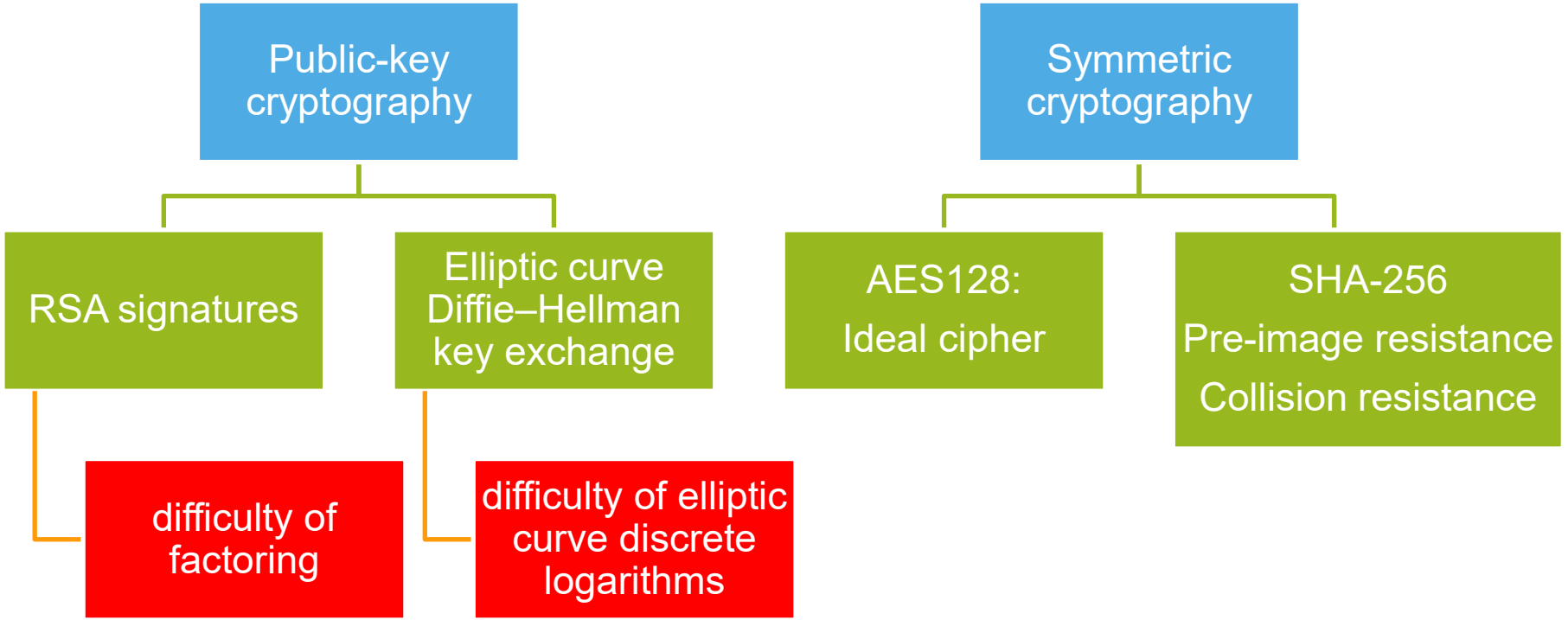
PUBLIC

AGENDA

- Quantum computing
  - Opportunities
  - Threats
- Post-quantum cryptography standards
  - Winners
  - Timeline
- Impact assessment (example on the S32G)
  - Re-using hardware
  - Secure boot

CONTEMPORARY CRYPTOGRAPHY

TLS-ECDHE-RSA-AES128-GCM-SHA256



Microsoft is collaborating with some of the world's top mathemati
build a scalable, fault-tolerant, universal quantum computer. Resea
breakthroughs to develop both the quantum hardware and the sof

Microsoft is making these investments because the team knows a
computing.

Overview Publications Videos Groups Projects Events C

The roots of Microsoft's quantum computing effort go back nearly
investigate the complex mathematical theory behind topological q

Over time, the team has brought together mathematicians and cor
"Station Q" lab was established in 2005 on the campus of the Univ
physicists and start experimentally investigating the topological eff

The Santa Barbara lab became the center of Microsoft's research in
fractional Quantum Hall effect.

Google AI Blog

The latest news from Google AI

Quantum Supremacy Using a Programmable Superconducting Processor

Wednesday, October 23, 2019

Posted by John Martinis, Chief Scientist Quantum Hardware and Sergio Boixo, Chief Scientist Quantum Computing Theory, Google AI Quantum

technologyreview.com/s/603163/intel-bets-it-can-turn-everyday-silicon-into-quantum-computings-wonder-material

Machines

Bets It Can Turn Everyday n into Quantum Computing's ler Material

largest chip company sees a novel path toward of immense power.

nite December 21, 2016

his to test quantum computing devices at

WIRED BACKCHANNEL BUSINESS CULTURE GEAR IDEAS SCIENCE SECURITY

TOM SIMONITE BUSINESS 12.03.2020 02:00 PM

China Stakes Its Claim to Quantum Supremacy

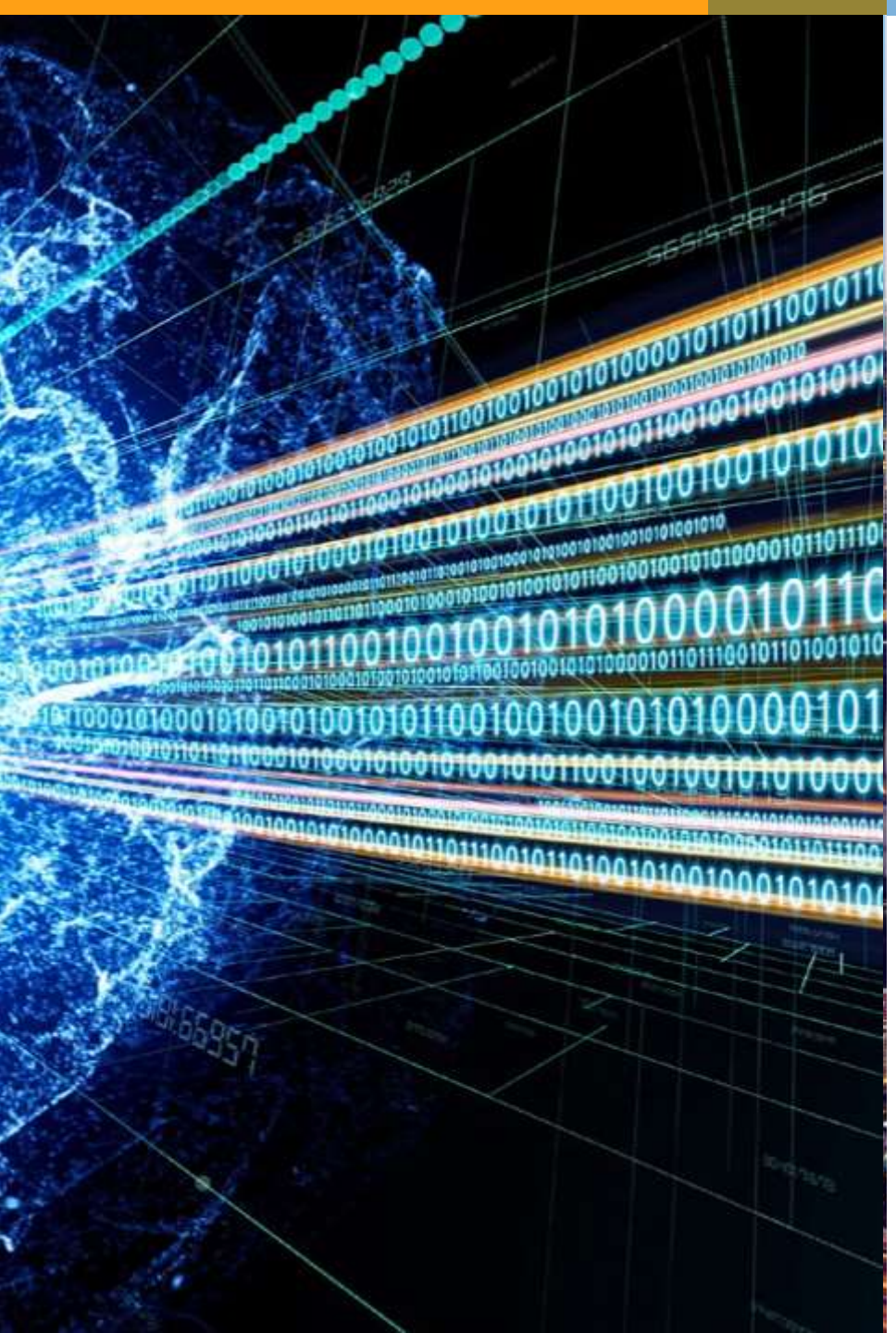
Google trumpeted its quantum computer that outperformed a conventional supercomputer. A Chinese group says it's done the same, with different technology.

g you in the face all along.
in the race to build
l offer immense processing
ı mechanics.

for simulating molecules on a quantum computer.

The breakthrough, outlined in a research paper to be published in the scientific journal

e all developing quantum components that are different from the ones crunching data in today's



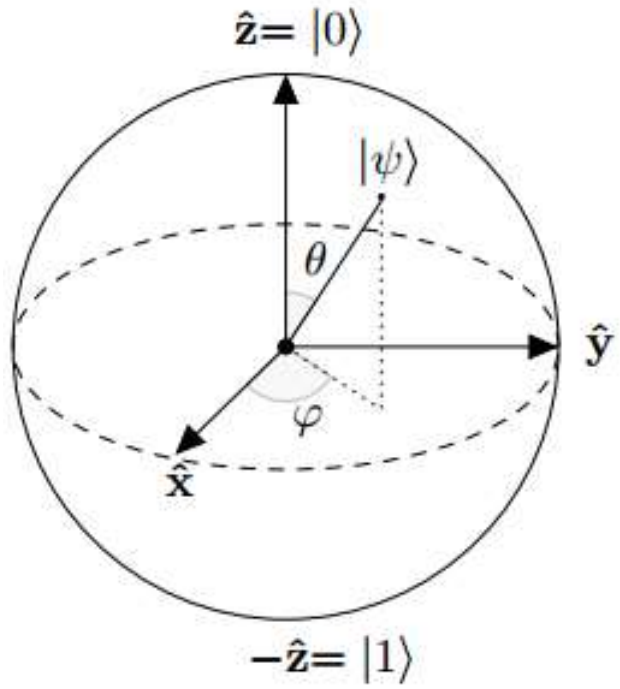
ADVANCES IN QUANTUM COMPUTING

Quantum computers hold the promise of being able to take on certain problems exponentially faster compared to a normal computer

- Healthcare and pharmaceuticals
- Materials
- Sustainability solutions
- Financial trading
- Big data and many other complex problems and simulations

QUANTUM COMPUTING

Computer systems and algorithms based on principles of quantum mechanics
- Superposition
- Interference
- Entanglement



- A classical bit can only be in the state corresponding to 0 or the state corresponding to 1
- A qubit may be in a superposition of both states
  → when measured it is always 0 or 1

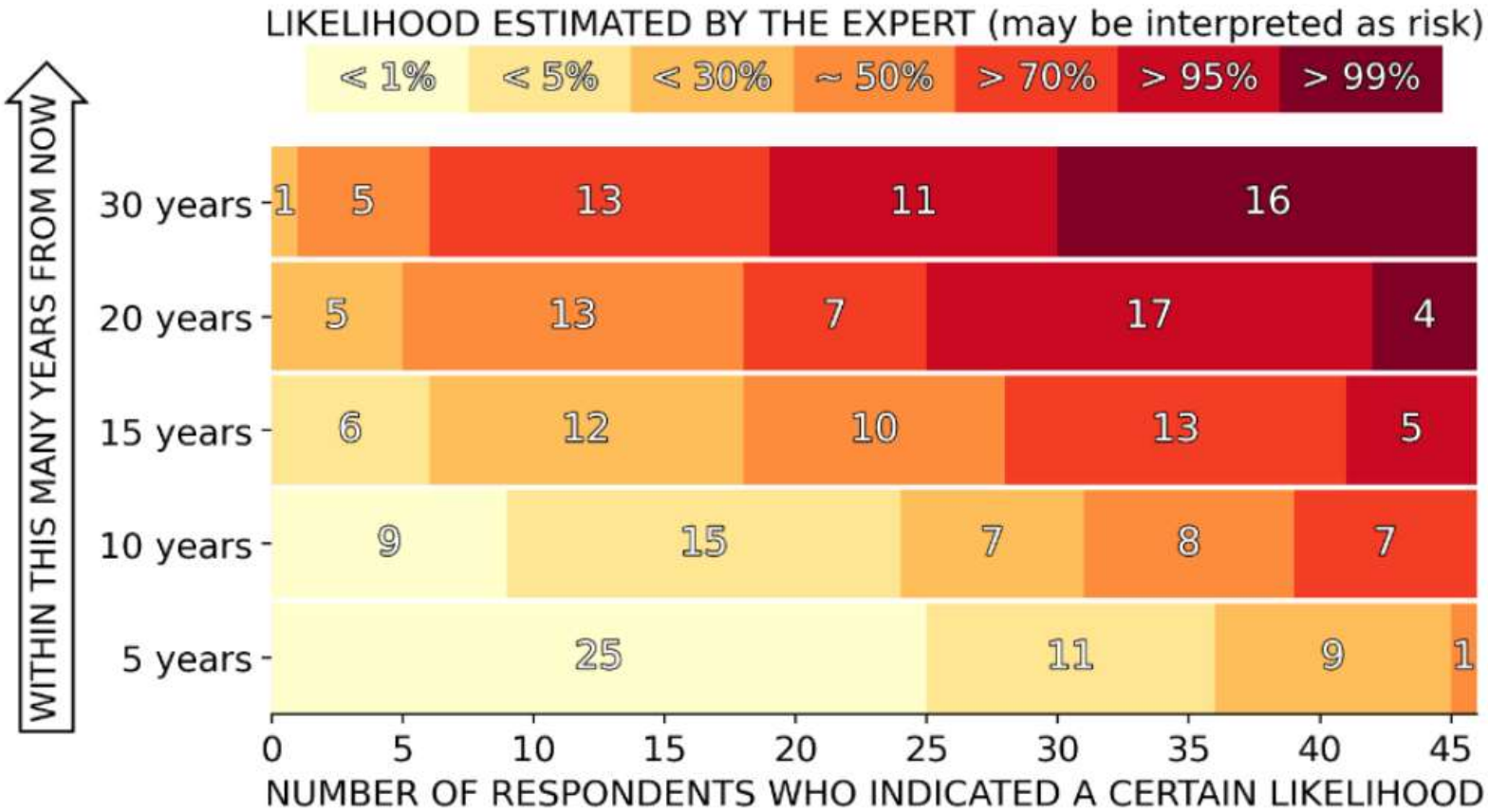
Shor's quantum algorithm (1994).
Polynomial time algorithm to factor integers.
Impact. If we assume the availability of a large quantum computer, then one can break RSA instantly.

State-of-the-art.
IBM's 127-Qubit Quantum Processor
Break RSA-3072:
~10,000 qubits are needed

SO, WHEN IS IT GOING TO BE HERE ?

EXPERTS' ESTIMATES OF THE LIKELIHOOD OF A QUANTUM COMPUTER ABLE TO BREAK RSA-2048 IN 24 HOURS

The experts were asked to indicate their estimate for the likelihood of a quantum computer that is cryptographically relevant—in the specific sense of being able to break RSA-2048 quickly—for various time frames, from a short term of 5 years all the way to 30 years.

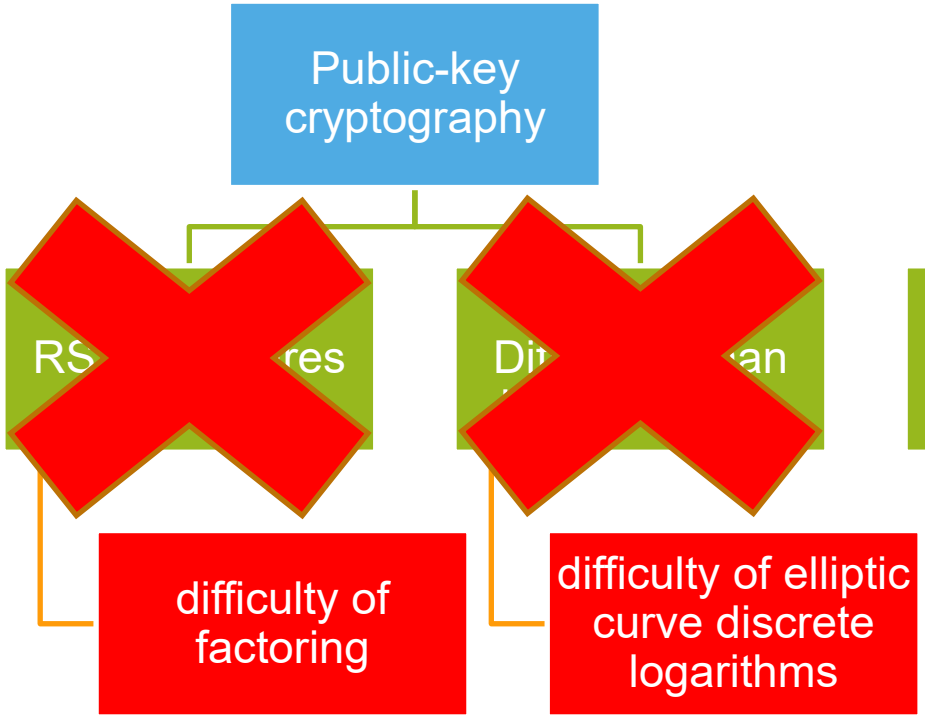


© https://globalriskinstitute.org/publications/2021-quantum-threat-timeline-report/

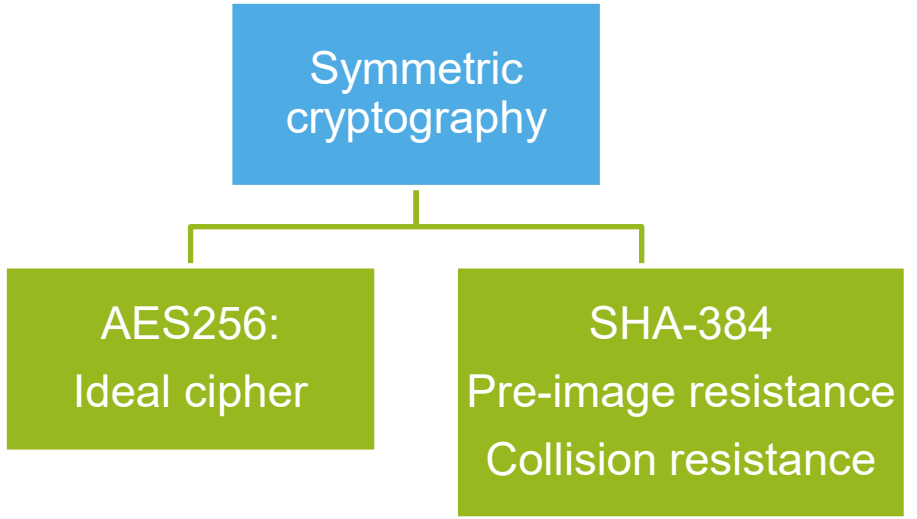
CONTEMPORARY CRYPTOGRAPHY

TLS-~~ECDHE-RSA~~-AES256-GCM-SHA384

"Double" the key sizes



Shor's algorithm (1994)



Grover's algorithm (1996)

Quantum Potential To destroy Security As We know it

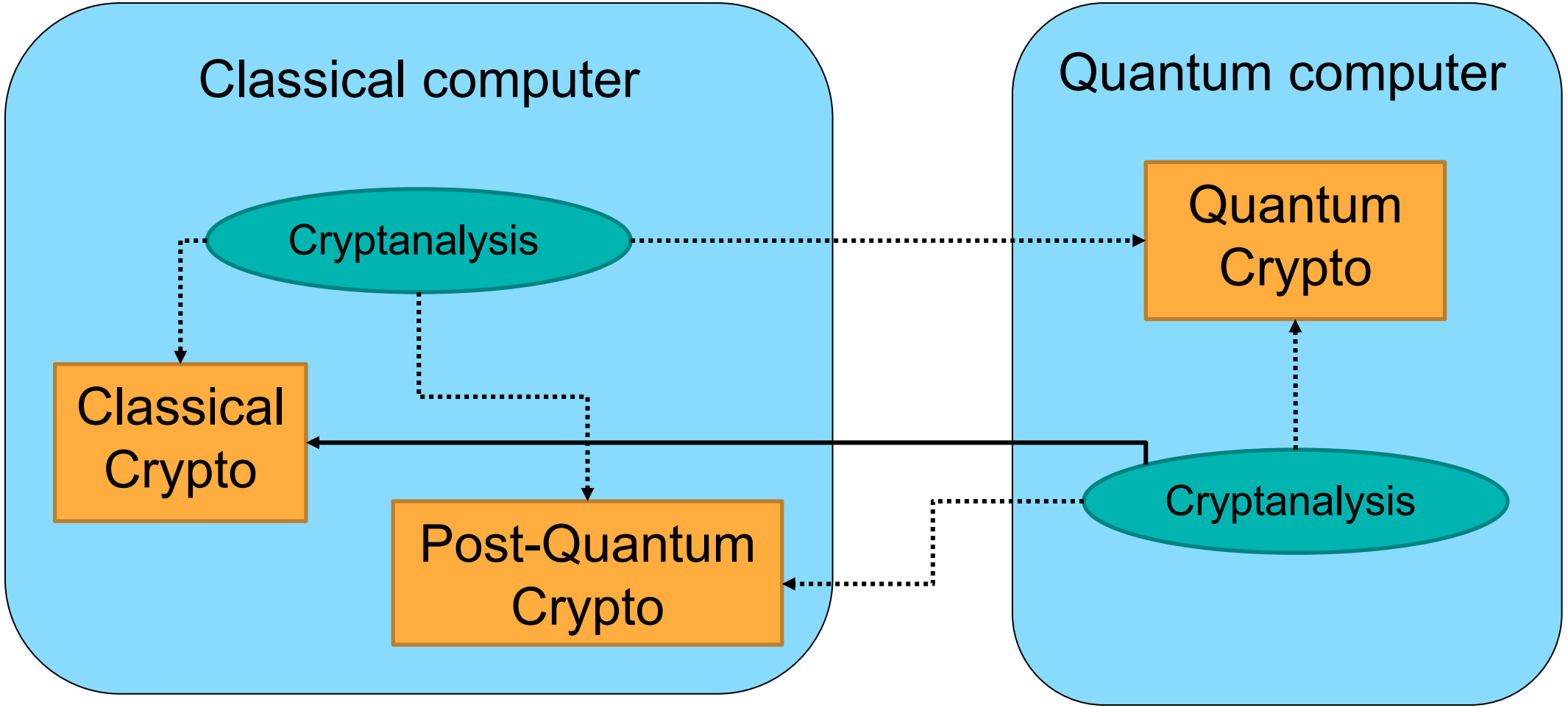
Confidential email messages, private documents, and financial transactions
Secure today but may be compromised in the future, even if recorded & encrypted

Firmware update mechanisms in vehicles
May be circumvented and allow dangerous modifications

Critical industrial and public service infrastructure (for healthcare, utilities, and transportation using internet and virtual private networks)
Could become exposed – potentially destabilize cities

Audit trails and digitally signed documents associated with safety (auto certification and pharmaceutical authorizations)
Could be retrospectively modified

The integrity of blockchains
Could be retrospectively compromised - could include fraudulent manipulation of ledger and cryptocurrency transactions


Classical computer
Cryptanalysis
Classical Crypto
Post-Quantum Crypto
Quantum computer
Quantum Crypto
Cryptanalysis

POST-QUANTUM CRYPTO STANDARDS ARE COMING

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

POST-QUANTUM CRYPTO STANDARDIZATION

2016
- Formal call for proposals

2017
- Deadline for submissions
- 69 candidates received

2019
- Second Round Candidates announced: 26 remaining candidates

2020
- Third Round Candidates announced: 7 Finalists and 8 Alternates

2022
- Announcement of Winners to be Standardized

2024 - 2030
- Standards Available
- Migration timeline

AUTOMOTIVE | EGOVERNMENT | BANK CARDS | SMART MOBILITY (MIFARE) CARDS | TAGS & AUTHENTICATION | READERS | MOBILE

STANDARDS – NIST

Winners	Secondary Winners	Round 4 Candidates	Digital Signature Competition
CRYSTALS-Kyber	Falcon	HQC	Proposals due '23
CRYSTALS-Dilithium	SPHINCS+	BIKE	
		Classic McEliece	
		SIKE	

2024 | 2025? | 2028? | 2030?

NIST PQC Standard (Key Exchange + Digital Signatures)

PQC Standard #2 (Digital Signatures)

Q&A on PQC + Standards

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 ‘21 to 12B units in ‘25

MOBILE

60B

Tagging 60B products per year by 2025

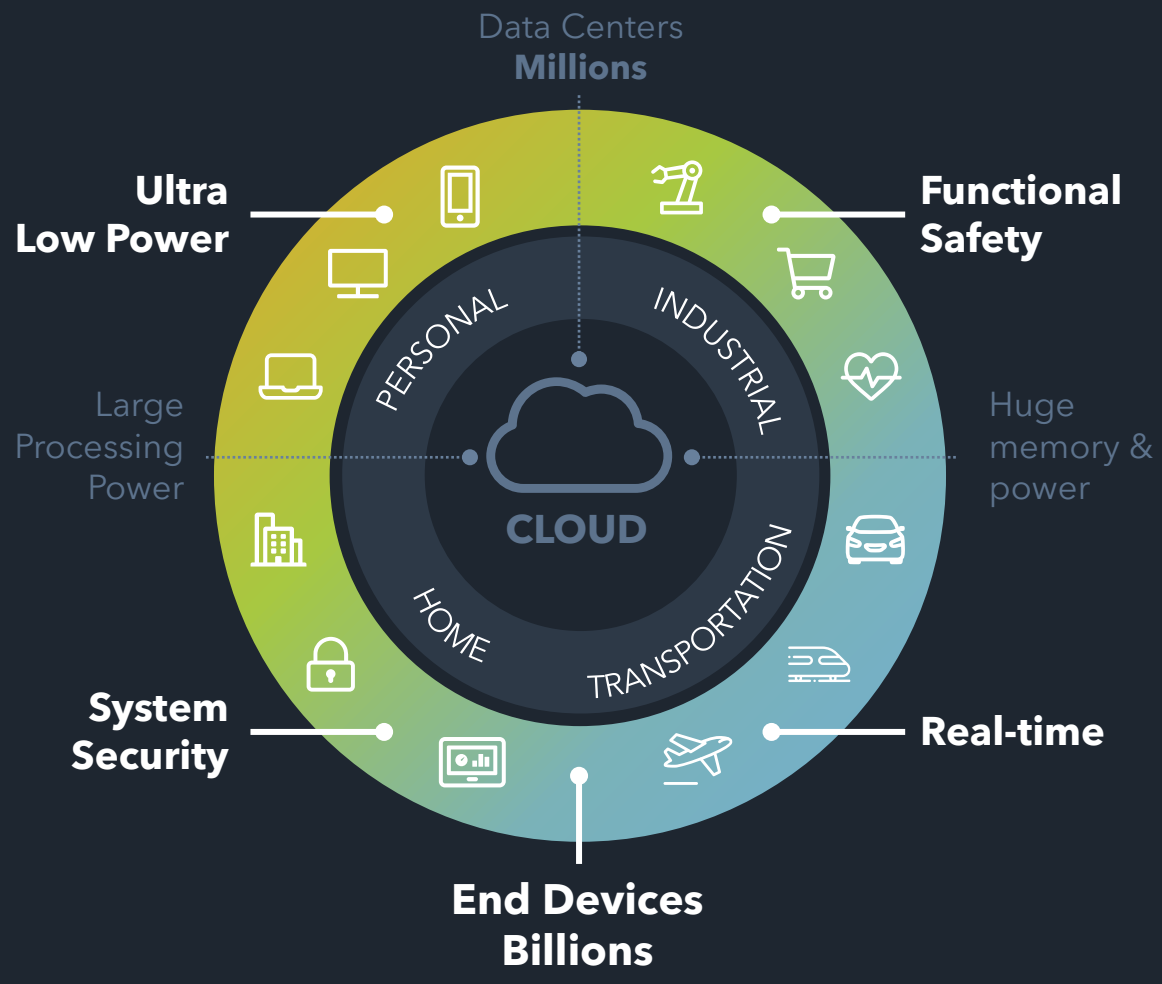
COMMUNICATION INFRASTRUCTURE

40B

Secure anchors & services for 40B processors

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

IMPACT PQC ON OUR ECO-SYSTEM



Data collection, processing and decisions at the edge
Devices securely connected to the cloud

No Silver Bullet

If a crypto scheme was better, we would have standardized this already

Cryptographic Keys

Orders of magnitude larger.
In the final: up to 1.3MB
Winners: up to 4.8KB
(ECC: 32 bytes, RSA: 384 bytes)

Performance

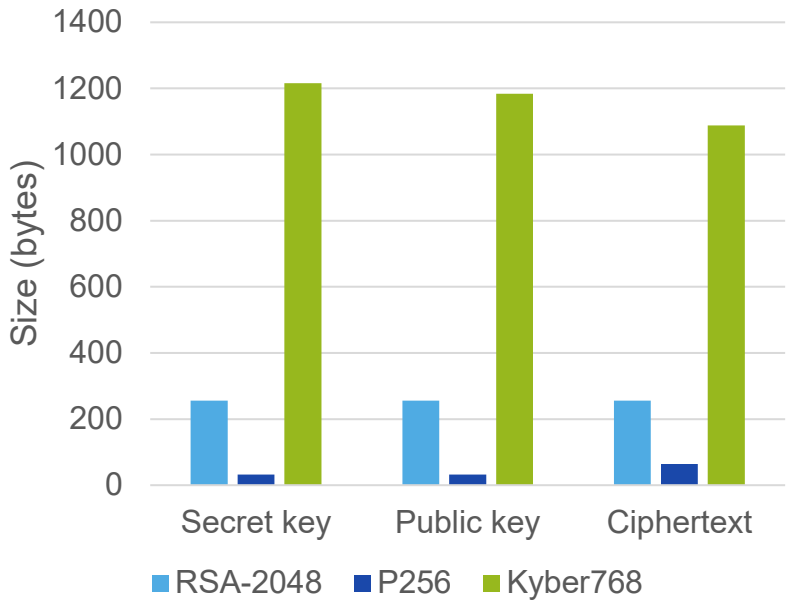
Varies: some faster some significantly slower.
SHA-3 is a dominating component (~80%)
→ HW co-processor

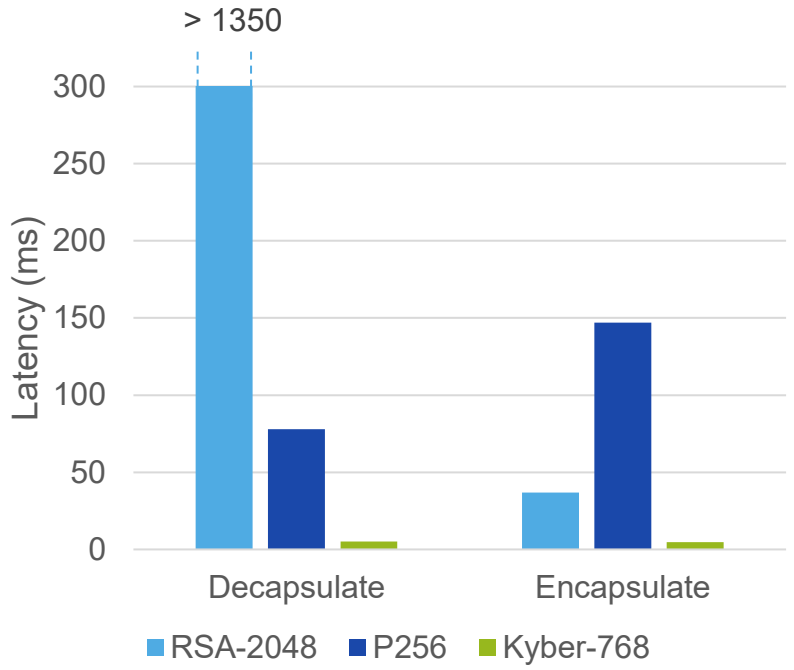
Memory

Orders of magnitude more:
up 100KB memory of RAM when executing
NXP has dedicated implementations reaching
~16KB of RAM

Bandwidth & Power

Larger signatures (up to 4.6KB)
→ more bandwidth required
→ increase in power usage



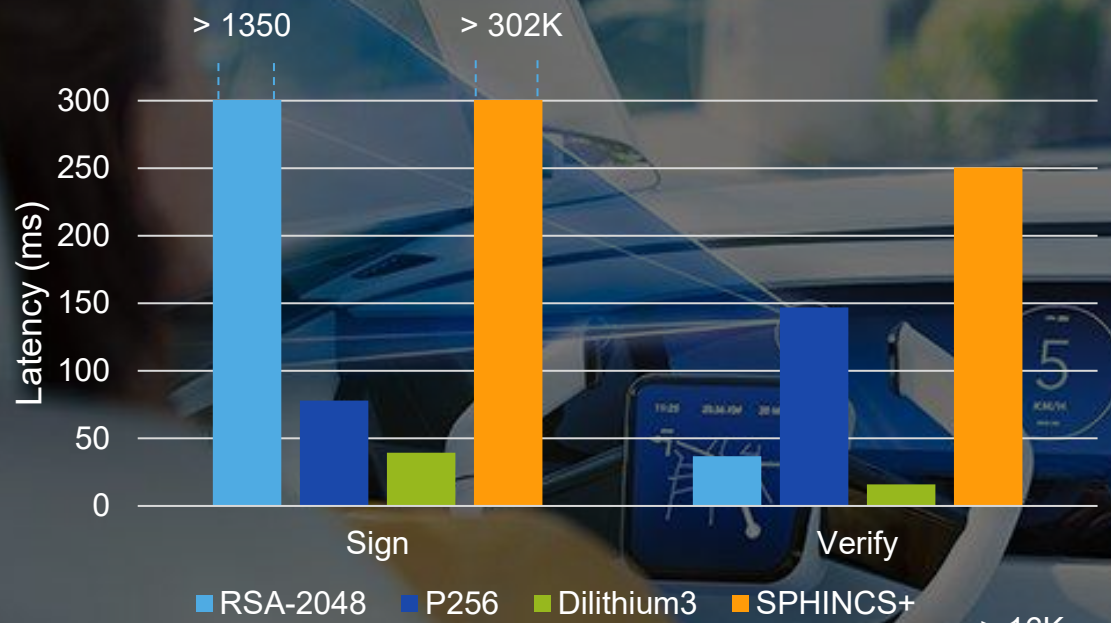


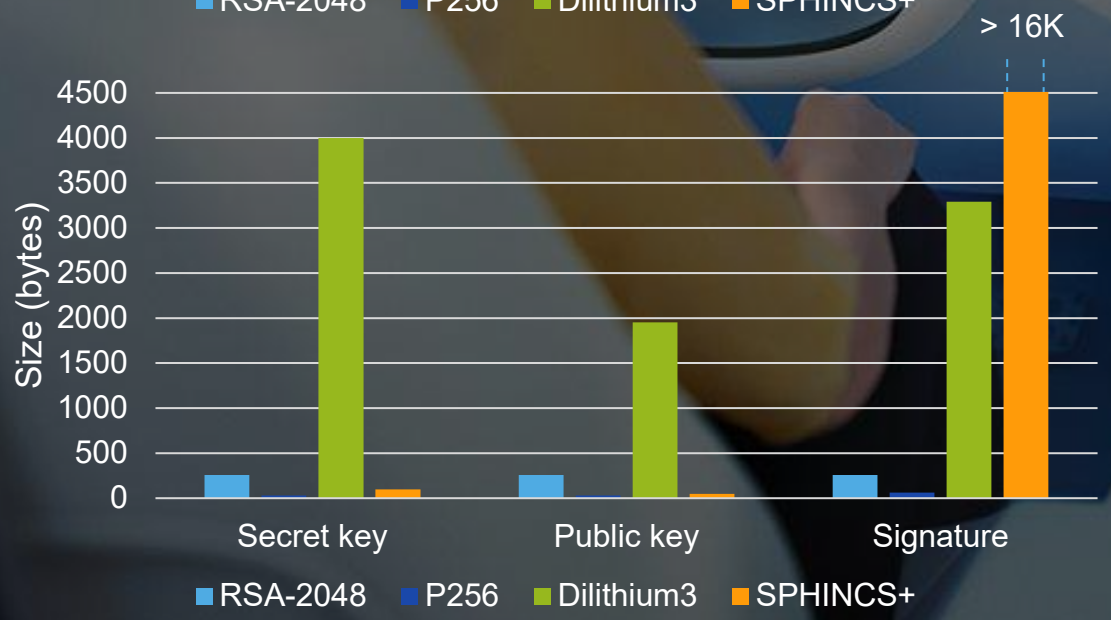
KEY-EXCHANGE IMPACT

Kyber **co-designed by NXP** with IBM, ARM and academic partners

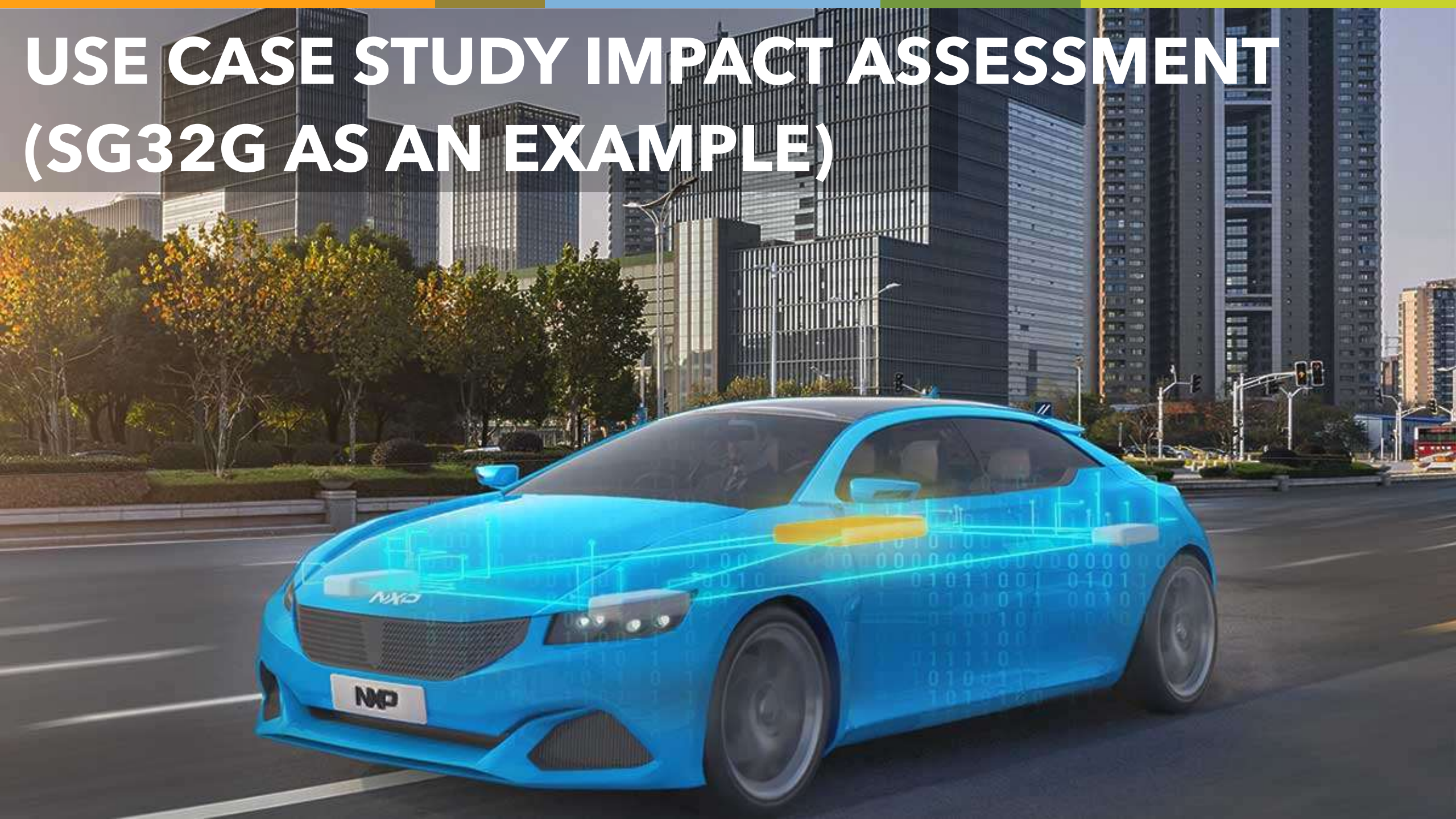
- Measurements on Cortex-M4 @ 168MHz from pqm4 framework
- Functional implementation only (not hardened)
- **70 ~ 80 percent** of run-time in SHA-3

DIGITAL SIGNATURE IMPACT

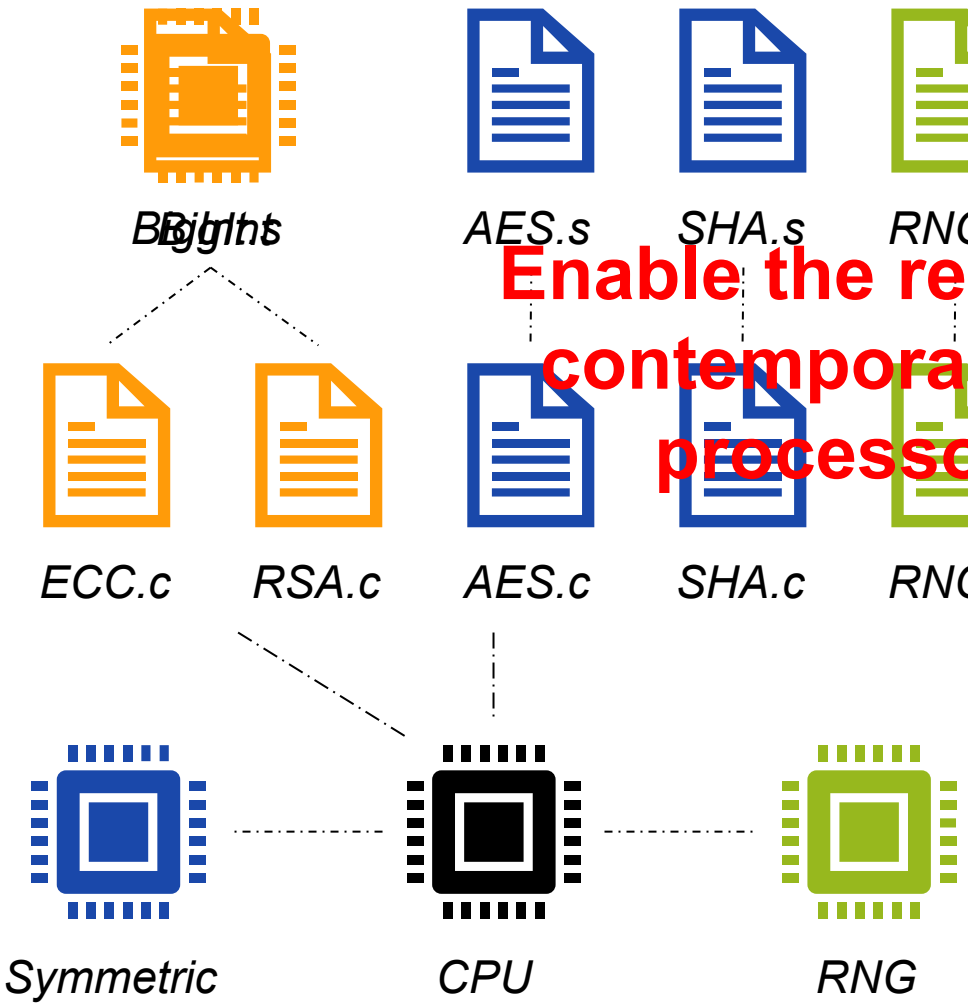




USE CASE STUDY IMPACT ASSESSMENT (SG32G AS AN EXAMPLE)

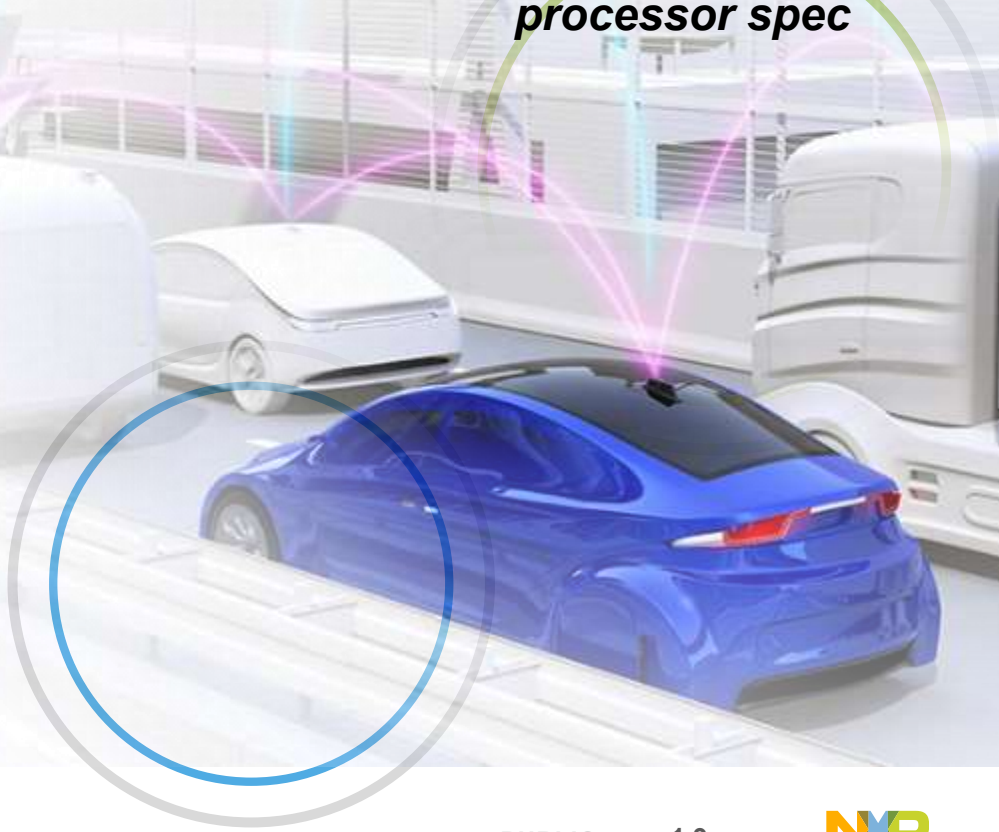


IMPLEMENTING CLASSICAL CRYPTOGRAPHY



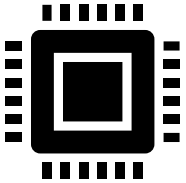
Enable the re-use of contemporary co-processors

S32G2 automotive processor spec

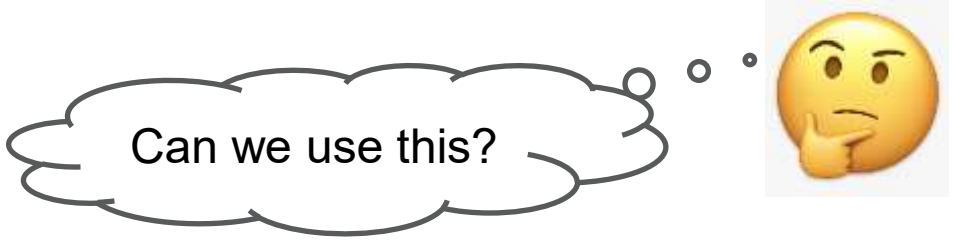


RE-USING EXISTING HW

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



Co-pro present in current hardware



KRONECKER SUBSTITUTION

Polynomial domain

$$f = 1 + 2x + 3x^2 + 4x^3$$

$$g = 5 + 6x + 7x^2 + 8x^3$$

✖

$$fg = 5 + 16x + 34x^2 + 60x^3 + 61x^4 + 52x^5 + 32x^6$$

Grundzüge einer arithmetischen Theorie der algebraischen Grössen.

(Von *L. Kronecker.*)

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

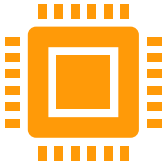
Kronecker domain (with evaluation point 100)

$$f(100) = 4030201$$

$$g(100) = 8070605$$

✖

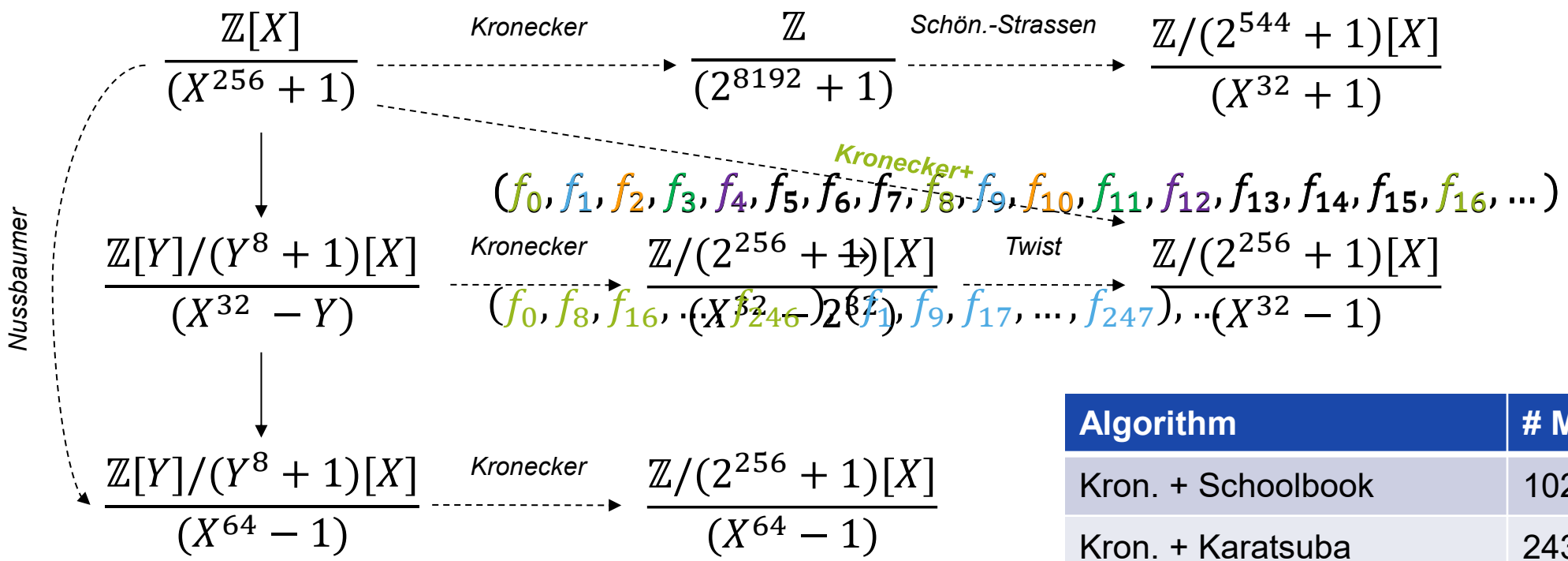
$$fg(100) = 32526160341605$$



POLYNOMIAL MULTIPLICATION TECHNIQUES

Multiplication with a 256-bit multiplier

Kronecker evaluation at 2^{32}



All methods include transformational overhead (additions, number-theoretic transforms, etc..). Become dominant cost for small multipliers, optimal choice depends on platform.

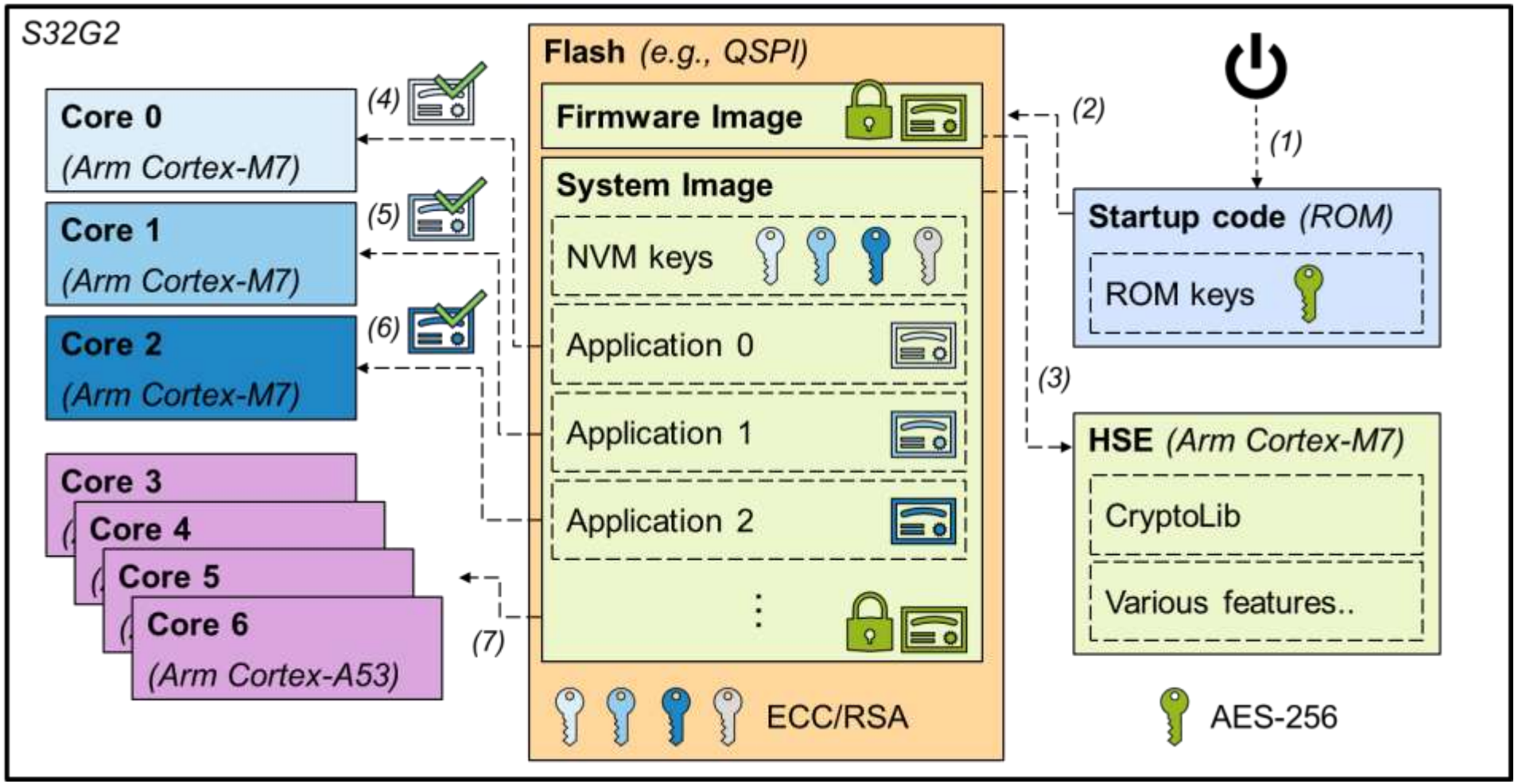
Algorithm	# Muls	# Bits
Kron. + Schoolbook	1024	256
Kron. + Karatsuba	243	256
Kron. + Toom-Cook	63	256
Kron. + Schön.-Strassen	32	544
Nussbaumer + Kron.	64	256
Kronecker+	**32**	**256**

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

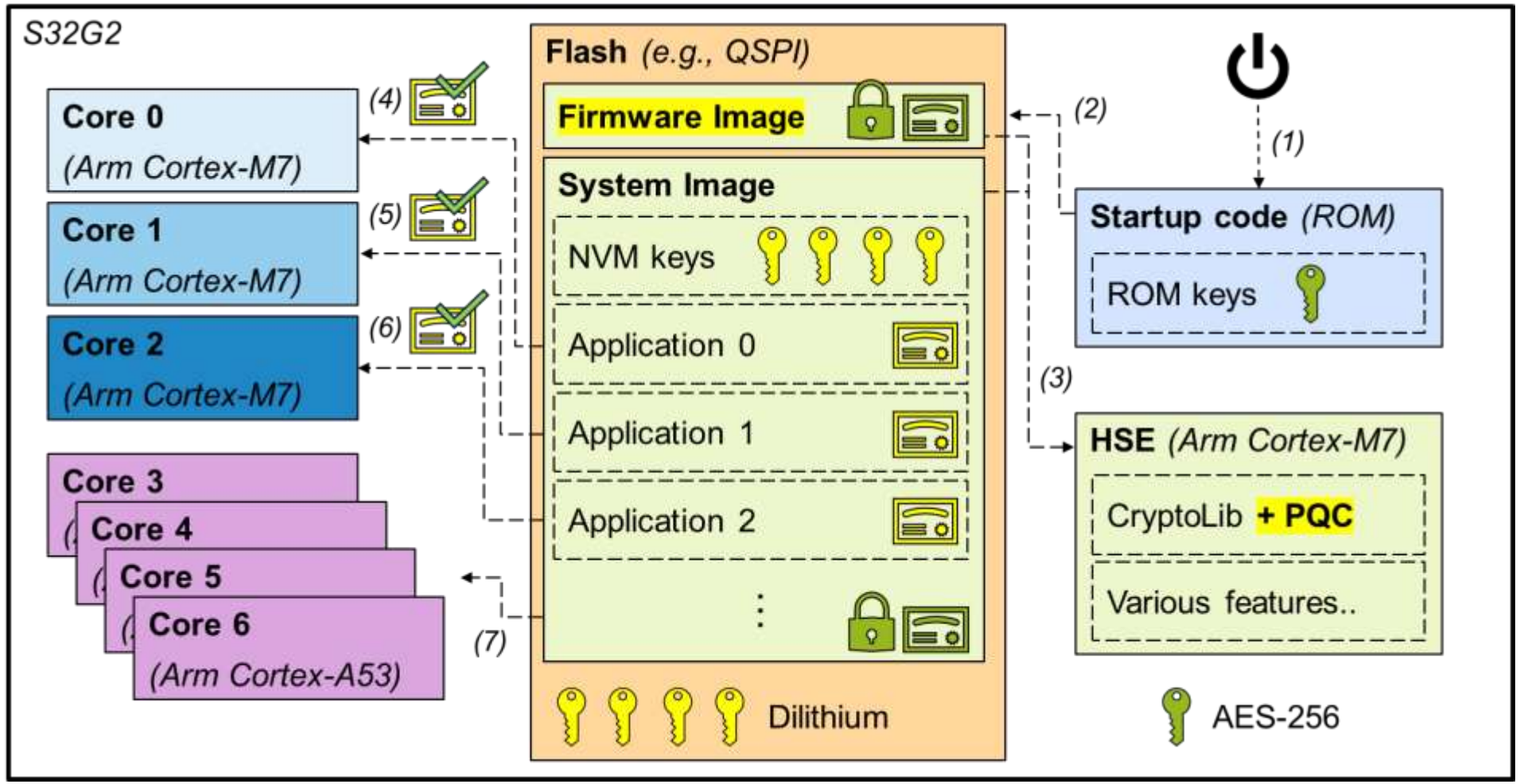
[B] Harvey. Faster polynomial multiplication via multipoint Kronecker substitution. J. of Sym. Comp. 2009.

[C] **Bos**, Renes, van Vredendaal; Post-Quantum Cryptography with Contemporary Co-Processors: Beyond Kronecker, Schönhage-Strassen & Nussbaumer; USENIX 2022

PQC DEMO: HSE SECURE BOOT OVERVIEW



PQC DEMO: HSE SECURE BOOT OVERVIEW



BENCHMARKS FOR AUTHENTICATION OF FW SIGNATURE ON THE S32G2

Alg.	Size		Performance (ms)			
			1 KB		128 KB	
	PK	Sig.	Inst.	Boot	Inst.	Boot
RSA 4K	512	512	2.6	0.0	2.7	0.2
ECDSA-p256	64	64	6.2	0.0	6.4	0.2
Dilithium-3	**1952**	**3293**	**16.7**	**0.0**	**16.9**	**0.2**

- Demonstrator only, further optimizations are possible (such as hardware accelerated SHA-3)
- Signature verification only required once for installation!
- During boot the signature verification can be replaced with a check of the Reference Proof of Authenticity

To appear:
J. W. Bos, B. Carlson, J. Renes, M. Rotaru, D. Sprenkels, G. P. Waters: Post-Quantum Secure Boot on Vehicle Network Processors. Embedded Security in Cars (escar) 2022

Conclusions

- New public-key standards are coming
  - irrelevant if the quantum threat is real or not
- Significant impact on *all* cybersecurity use-cases
- Migration will take years / decades

- Current dedicated cryptographic hardware can be re-used to a certain extend
- Lots of opportunities for new PQC hardware designs!

- We didn't even talk about hardened implementations

CONTACT: PQC@NXP.COM | NXP.COM/PQC

SECURE CONNECTIONS
FOR A SMARTER WORLD