

# POST-QUANTUM CRYPTO: THE EMBEDDED CHALLENGE

Joppe Bos

JANUARY 7, 2022



SECURE CONNECTIONS  
FOR A SMARTER WORLD

PUBLIC

NXP, THE NXP LOGO AND NXP SECURE CONNECTIONS FOR A SMARTER WORLD ARE TRADEMARKS OF NXP B.V.  
ALL OTHER PRODUCT OR SERVICE NAMES ARE THE PROPERTY OF THEIR RESPECTIVE OWNERS. © 2021 NXP B.V.



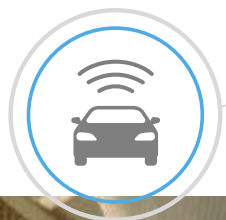


# SECURE CONNECTIONS FOR A SMARTER WORLD

**OUR DIGITALLY ENHANCED WORLD IS EVOLVING TO ANTICIPATE AND AUTOMATE**

NXP Semiconductors N.V. (NASDAQ: NXPI) is a global semiconductor company creating solutions that enable secure connections and infrastructure for a smarter world. NXP focuses on research, development and innovation in its target markets.

**AUTOMOTIVE**



**INDUSTRIAL & IOT**



**MOBILE**



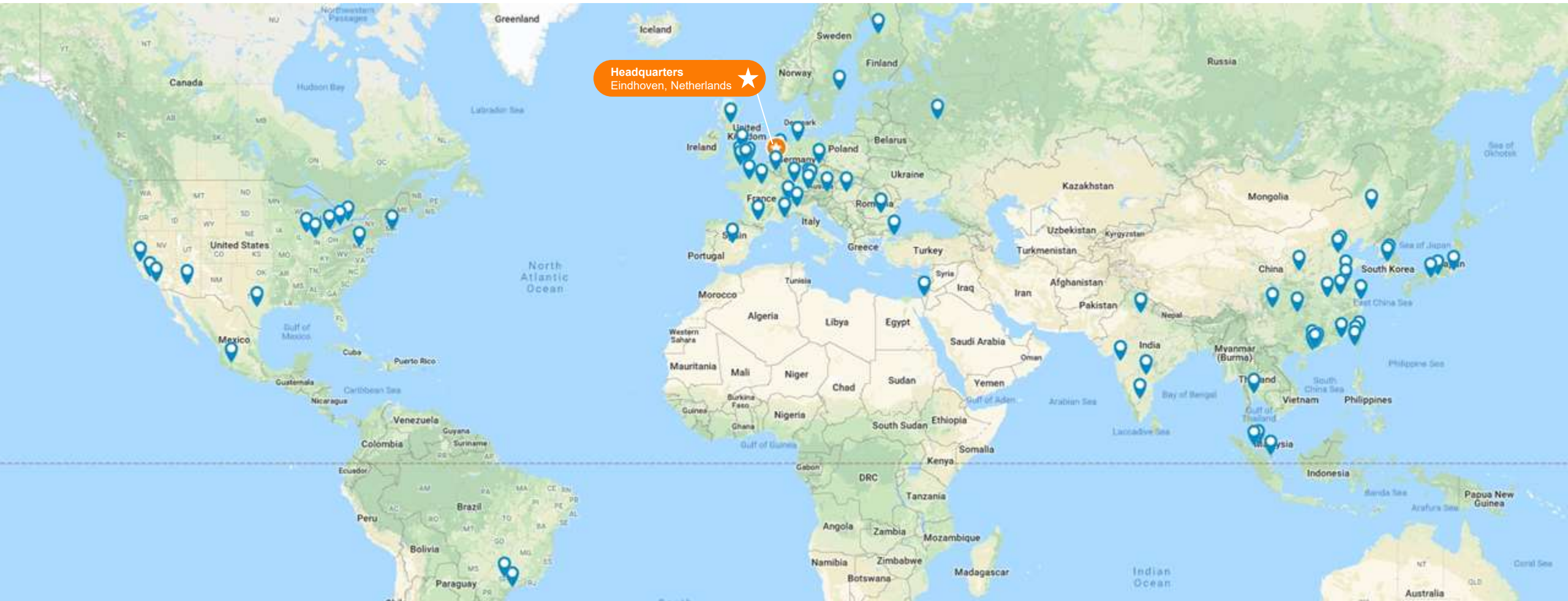
**COMMUNICATION  
INFRASTRUCTURE**





## NXP LOCATIONS

~29,000 employees with operations  
in more than 30 countries



# NXP GERMANY AT A GLANCE

## Hamburg

- NXP CEO and CTO Office
- Automotive R&D, Marketing:
  - Infotainment / V2X / Radar
  - Functional Safety
  - Secure Car Access
  - Sensors
- Security R&D
- Industrial IoT R&D, Marketing
- NFC / Ultra-Wideband (UWB) R&D, Marketing
- Secure Identity / Payment



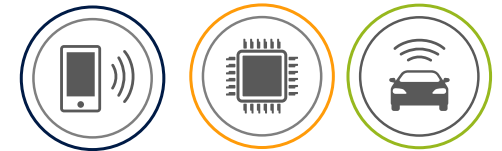
## Wiesbaden, Nuremberg, Boeblingen

- Sales Offices



## Munich

- Automotive:
  - Infotainment / Radar
  - Battery Management Systems
  - Microcontroller
- NFC
- Industrial IoT
- Sales



## Dresden

- Infotainment R&D



## Karlsruhe

- WiFi R&D
- Sales

# WORK ON REAL PRODUCTS WITH REAL IMPACT

## Explore our opportunities in Germany

Are you ready for some "real world" experience working with the latest in automotive, IoT, mobile or communication infrastructure technologies?

Do you want to meet and work with industry leaders and innovators in these fields?

Check out our open jobs via [www.nxp.com/careers](http://www.nxp.com/careers)!



### Working student

Gain experience through a part time occupation alongside your studies

Usually between **8 and 18 hours** weekly

Available in all our locations

### Fulltime internship

An excellent learning opportunity as part of your education

Duration depends on study regulations

Voluntary internships possible in Dresden & Munich

### Thesis

Put your learning into practice and get the best kickoff of your career

Approximate duration of the assignment is **6 months**

Available in all our locations

### PhD assignment

Start your research career in one of our highly innovative teams

Duration is about **3 to 4 years**

Most PhD assignments are driven by our collaboration with Universities across the region

### Graduate opportunity

Explore a wealth of graduate opportunities in our different domains and disciplines

Opportunities available in all our locations



# BACK TO THE TECHNICAL TOPIC POST-QUANTUM CRYPTO: THE EMBEDDED CHALLENGE



SECURE CONNECTIONS  
FOR A SMARTER WORLD

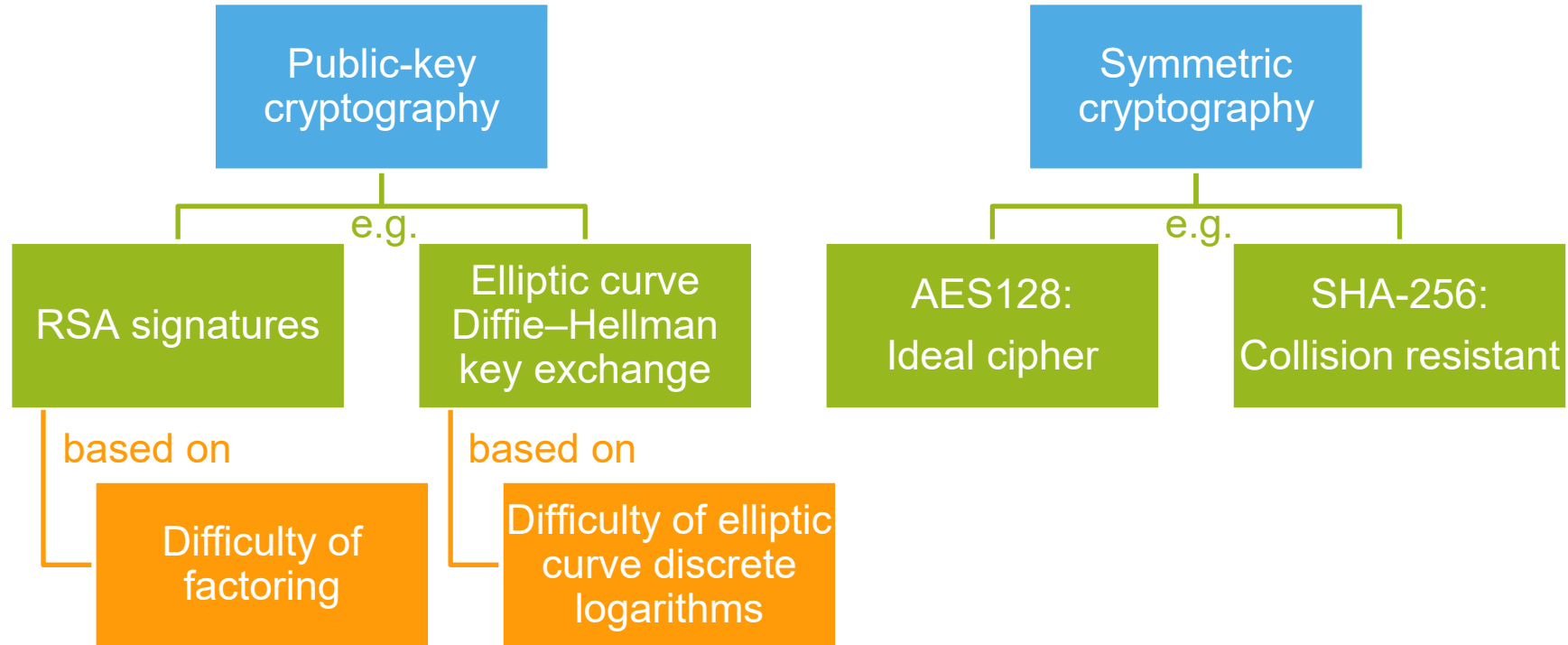
PUBLIC

NXP, THE NXP LOGO AND NXP SECURE CONNECTIONS FOR A SMARTER WORLD ARE TRADEMARKS OF NXP B.V.  
ALL OTHER PRODUCT OR SERVICE NAMES ARE THE PROPERTY OF THEIR RESPECTIVE OWNERS. © 2021 NXP B.V.



# CONTEMPORARY CRYPTOGRAPHY

## E.G. TLS-ECDHE-RSA-AES128-GCM-SHA256





Microsoft is collaborating with some of the world's top mathematicians to build a scalable, fault-tolerant, universal quantum computer. Research breakthroughs to develop both the quantum hardware and the software are essential to this effort.

Microsoft is making these investments because the team knows a quantum computer will revolutionize computing.

Overview Publications Videos Groups Projects Events Contact

The roots of Microsoft's quantum computing effort go back nearly a decade to the company's investment in topological quantum computing. Over time, the team has brought together mathematicians and computer scientists to investigate the complex mathematical theory behind topological quantum computing. In 2012, the "Station Q" lab was established in 2005 on the campus of the University of California, Santa Barbara and is now the center of Microsoft's research in quantum computing.



WIRED

BACKCHANNEL BUSINESS CULTURE GEAR IDEAS SCIENCE SECURITY

# 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

## 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.

for simulating molecules on a quantum computer.

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

Machines

## Bets It Can Turn Everyday Silicon into Quantum Computing's Wonder Material

Intel, the world's largest chip company, sees a novel path toward quantum computing of immense power.

by Tom Simonite December 21, 2016



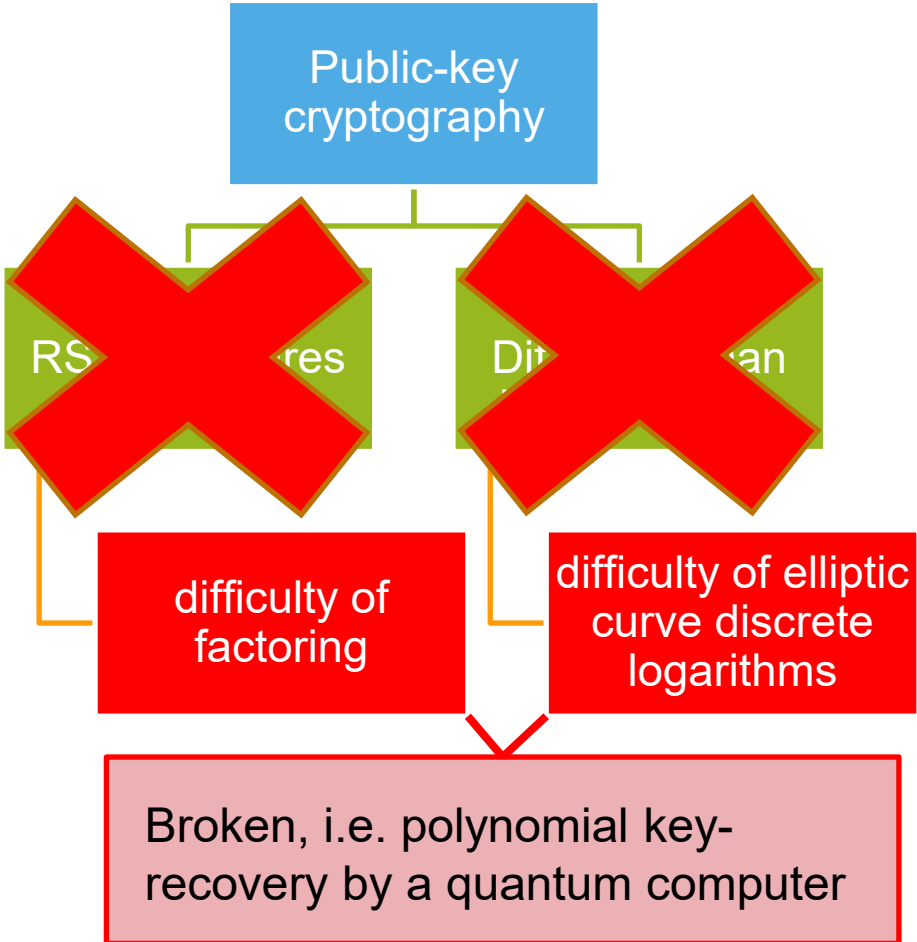
Intel is testing quantum computing devices at

ing you in the face all along. Intel is in the race to build a quantum computer that will offer immense processing power and new mechanics.

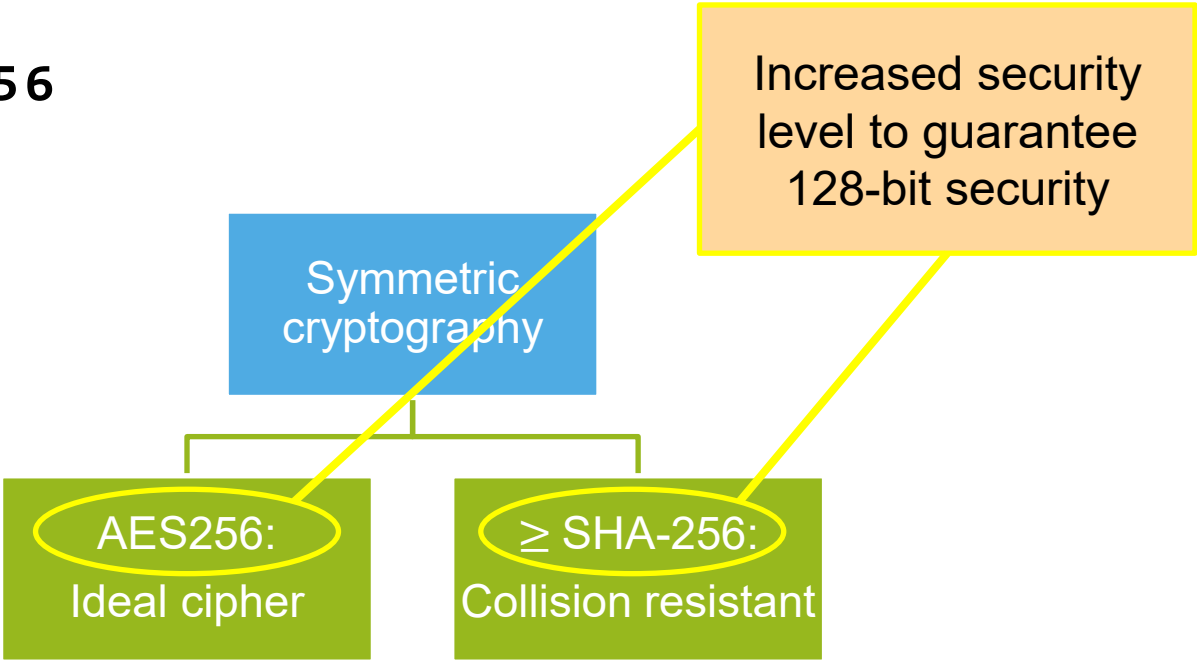
are all developing quantum computing components that are different from the ones crunching data in today's



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



Shor's algorithm (1994)



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



Grover's algorithm (1996)

## WHAT NOW?

### POST-QUANTUM CRYPTOGRAPHY

- We need to update our cryptographic primitives to protect applications from a potential quantum adversary
- **Post-quantum cryptography** is based on mathematical problems not vulnerable to (known) quantum attacks



Hash-  
based  
Crypto

Code-  
based  
Crypto

Multivariate  
Crypto

Lattice-  
based  
Crypto

Isogeny-  
based  
Crypto



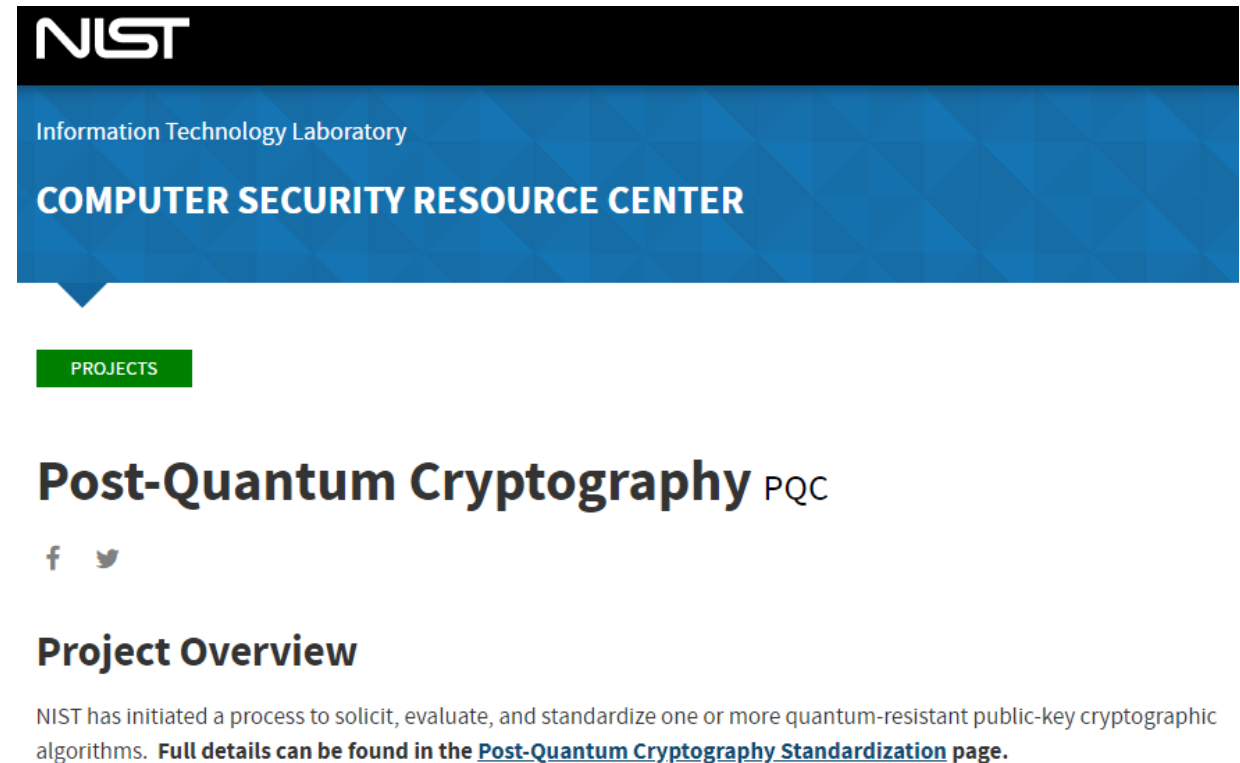
**POST-QUANTUM CRYPTO STANDARDS ARE COMING**  
(IT DOESN'T MATTER IF YOU BELIEVE IN QUANTUM COMPUTERS OR NOT)

**HOW ARE EXISTING SYSTEMS IMPACTED?**



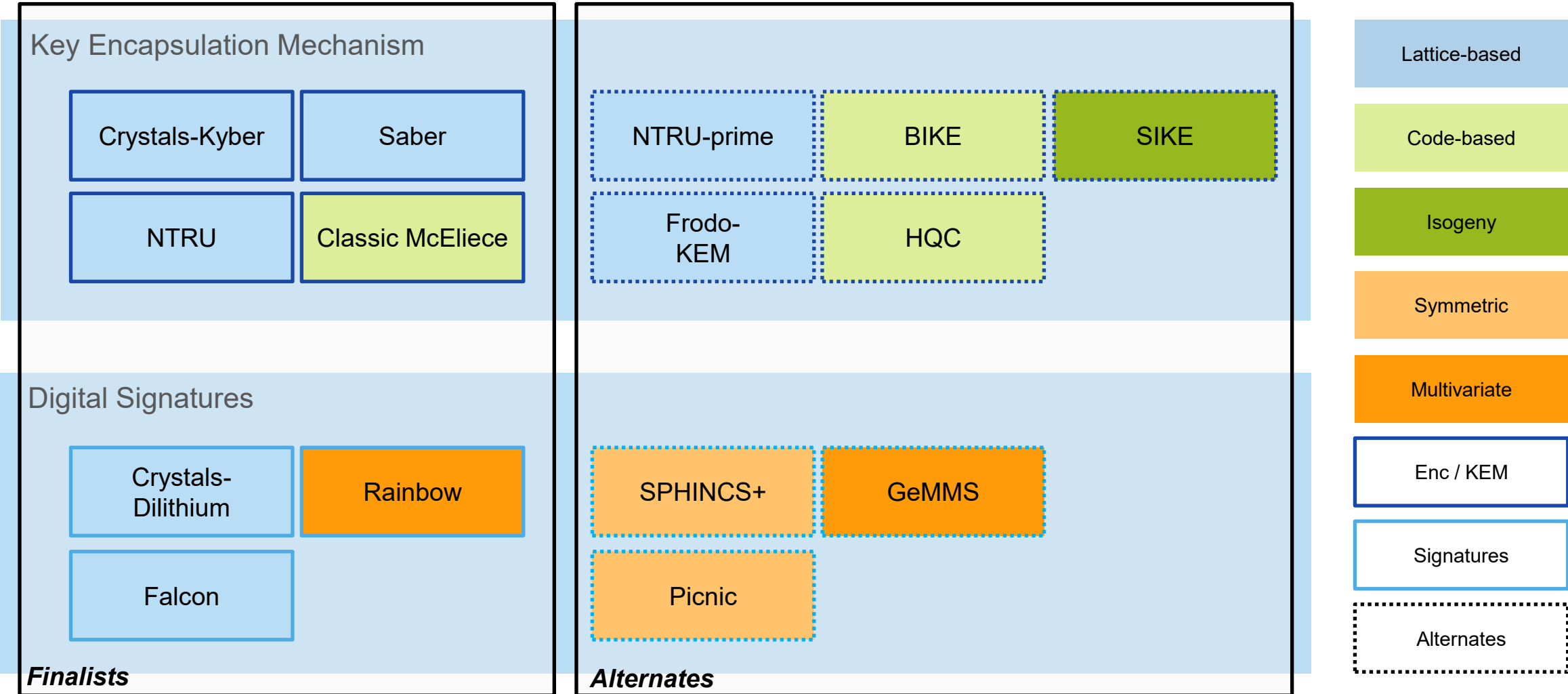
## STANDARDS – LONG TERM – NIST ROUND 3

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	<b>Analysis phase</b> <b>Jan 2019: Round 2</b> <b>July 2020: Round 3 announced</b> <b>Early 2022: Winners</b>
2 years later (2022/2024)	Draft standards ready

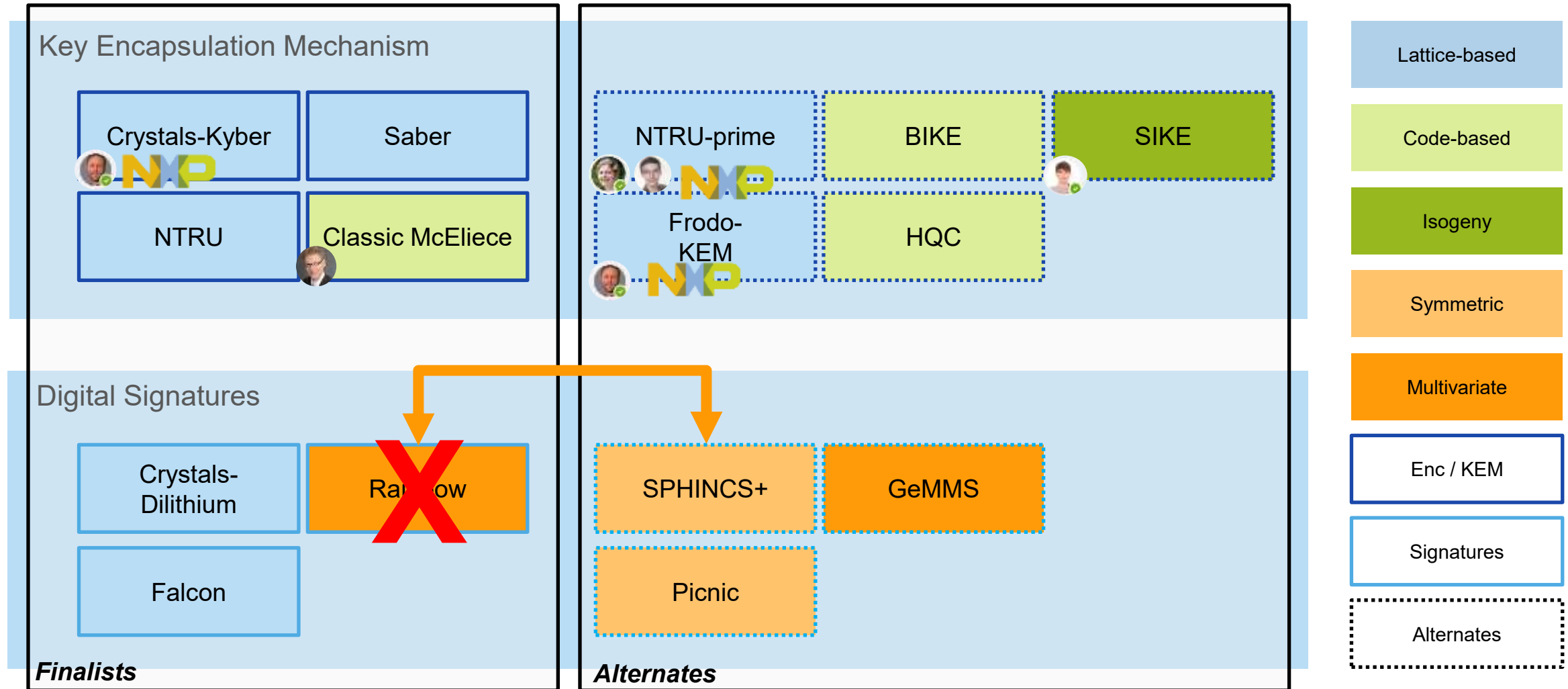


The screenshot shows the NIST Information Technology Laboratory's Computer Security Resource Center page for Post-Quantum Cryptography (PQC) projects. The header features the NIST logo and the text 'Information Technology Laboratory' and 'COMPUTER SECURITY RESOURCE CENTER'. Below this is a green button labeled 'PROJECTS'. The main heading is 'Post-Quantum Cryptography PQC', followed by social media icons for Facebook and Twitter. A section titled 'Project Overview' contains the text: 'NIST has initiated a process to solicit, evaluate, and standardize one or more quantum-resistant public-key cryptographic algorithms. Full details can be found in the [Post-Quantum Cryptography Standardization](#) page.'

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



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





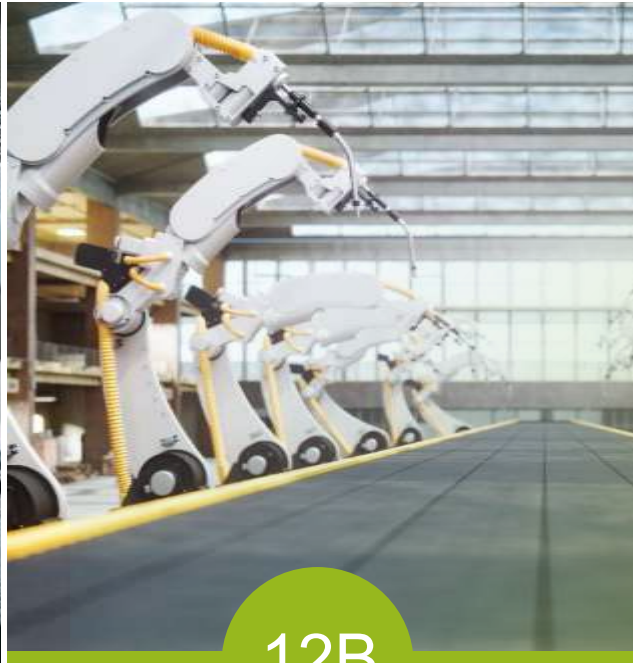
# POST-QUANTUM CRYPTO IS ON THE HORIZON

## AUTOMOTIVE



**70%** connected cars by 2025

## INDUSTRIAL & IOT



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

## MOBILE



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

## COMMUNICATION INFRASTRUCTURE



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

What is the impact on the billions of embedded devices?



## 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

Is this even possible?  
What is the impact?



## HOW TO PREPARE FOR HURRICANE SEASON Quantum



### MAKE A PLAN

Amren should create an emergency plan and/or checklist:

- obtain supplies
- update personal documents
- secure household
- research evacuation options/routes
- update prescriptions



### CREATE A GO-BAG

Prepare supplies ahead of a hurricane. These can include:

- Food/water
- Additional clothes
- Personal documents
- Travel supplies
- Prescriptions



### KNOW YOUR WING GUIDANCE

Whether preparing for a hurricane or evacuating, know your wing or installation's guidance. Routinely check for updates from leadership and maintain communication with your chain of command.



### RECOGNIZE WARNINGS & ALERTS

Have several ways to receive alerts. Download real-time alert apps. Sign up for community alerts in your area and be aware of the Emergency Alert System (EAS) and Wireless Emergency Alert (WEA), which requires no sign up.



### STAY SAFE

Practice good hygiene and safety measures during any part of a hurricane evacuation or impact. Keep family considerations in mind and don't be afraid to contact leadership for guidance.

## PREPARATION FOR THIS NEW STANDARD

### General challenges

Key sizes

Stack usage

Memory requirements

Bandwidth

### Re-use existing hardware

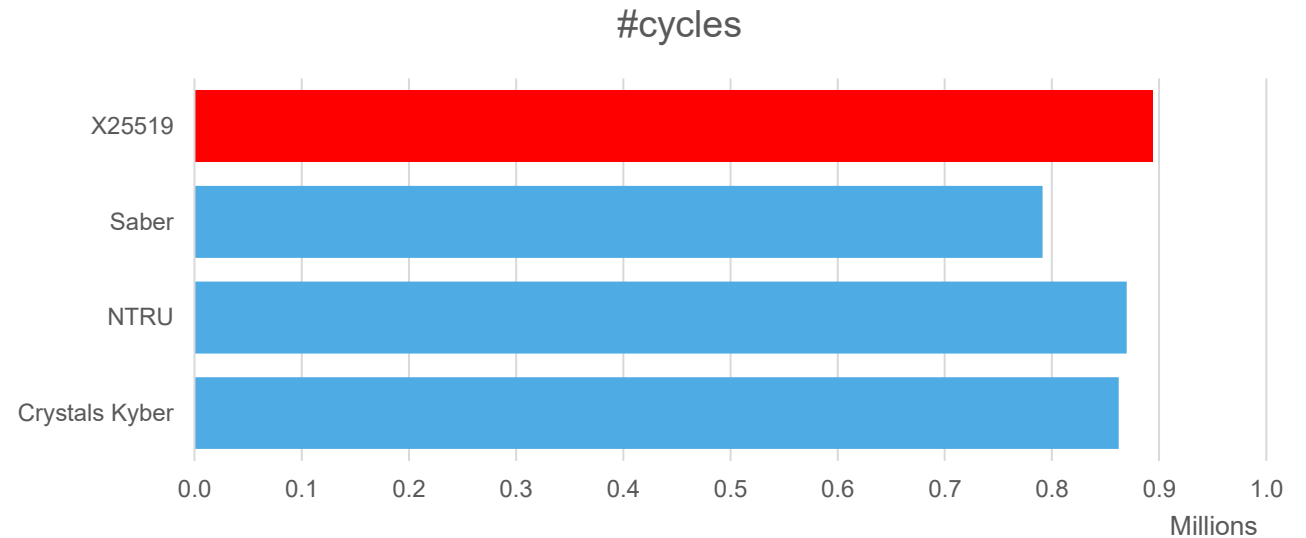
Co-processors for hashing

Co-processors for big  
number arithmetic





## 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]

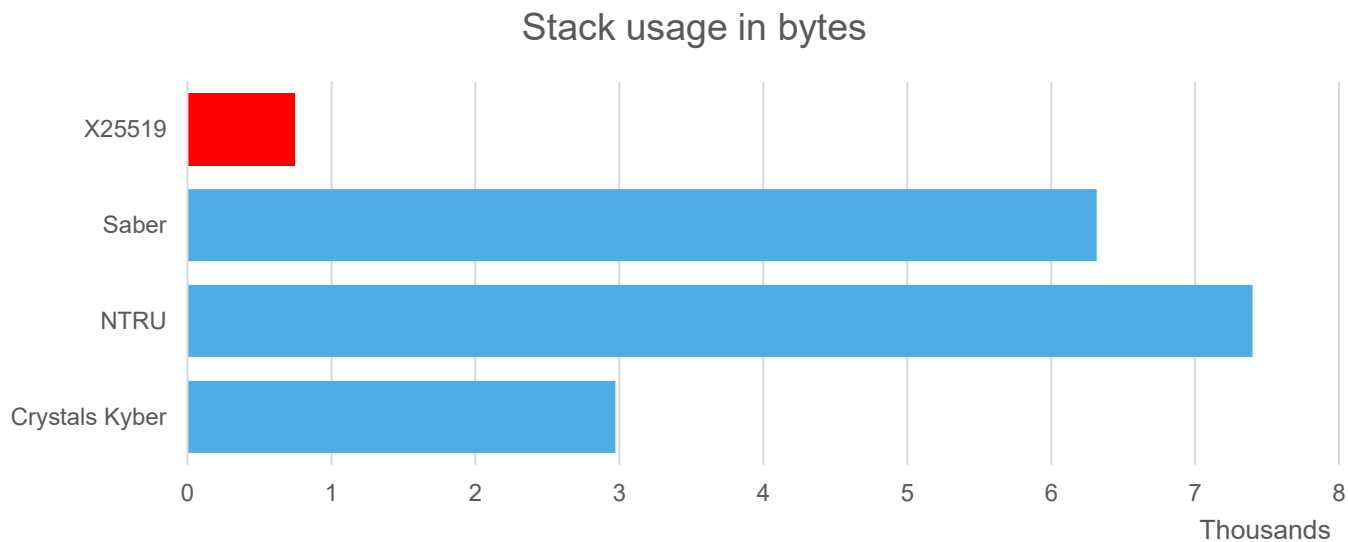
Note: Cortex-M4 is high-end for many embedded applications

[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.

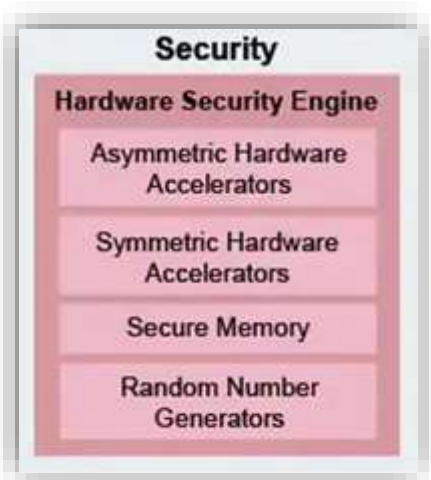
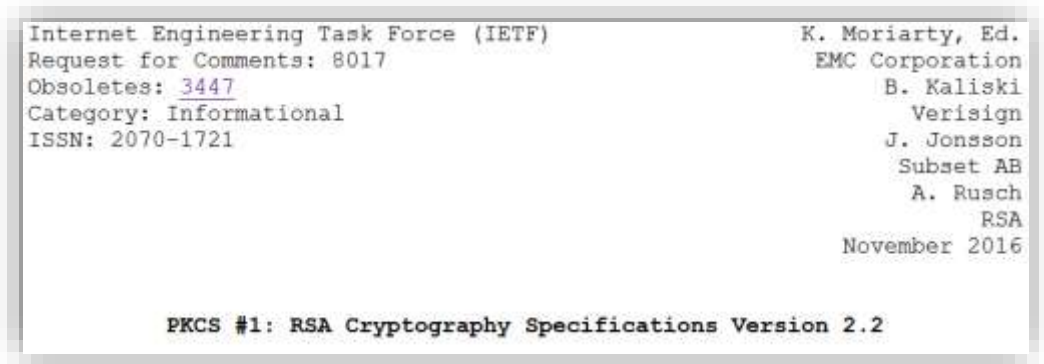


## CLASSIC VS LATTICES IN PRACTICE (2/2)

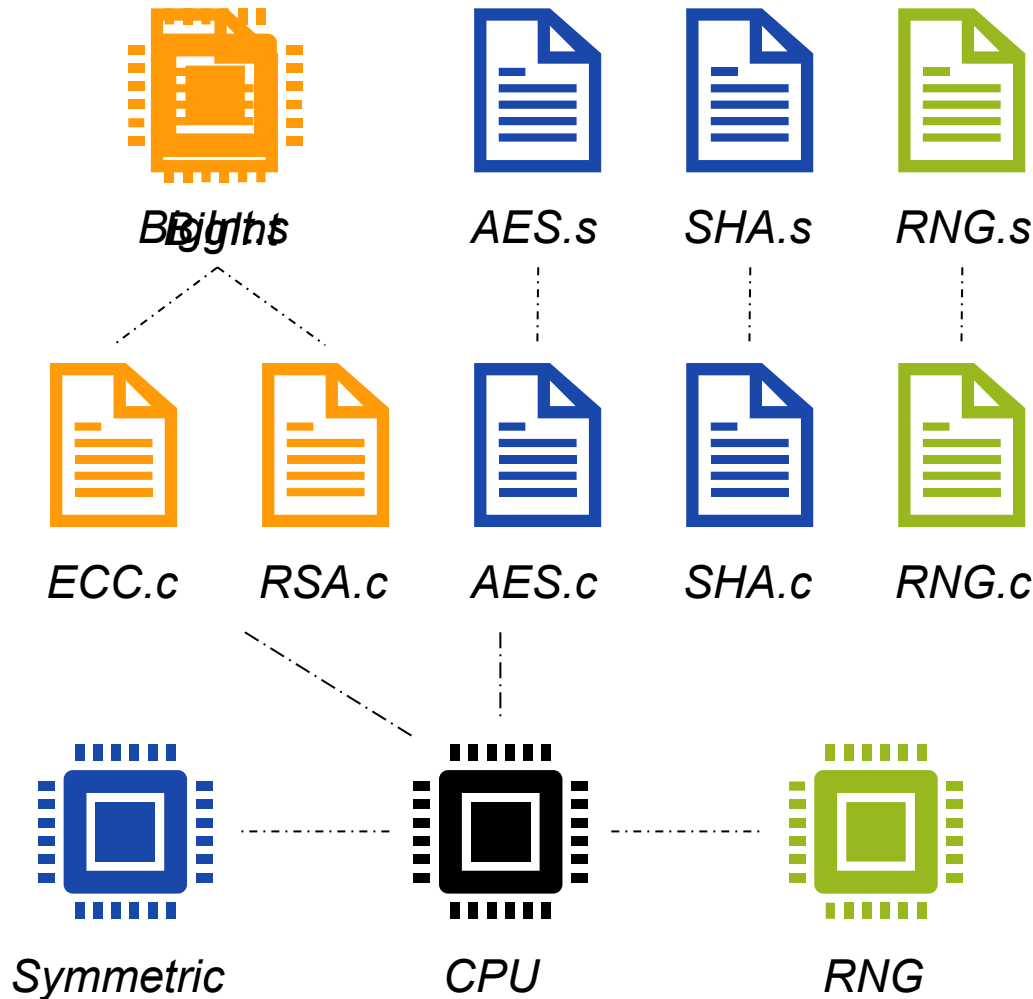


- This ignores RAM / flash memory for key material
- Typical max. stack requirements:  
1k, 2k, 4k bytes → serious challenge

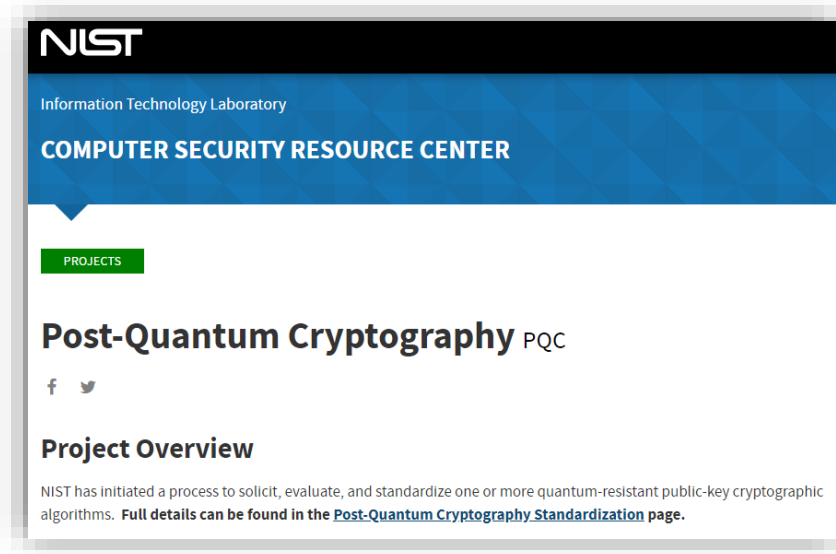
# IMPLEMENTING CLASSICAL CRYPTOGRAPHY



*S32G2 automotive processor spec*



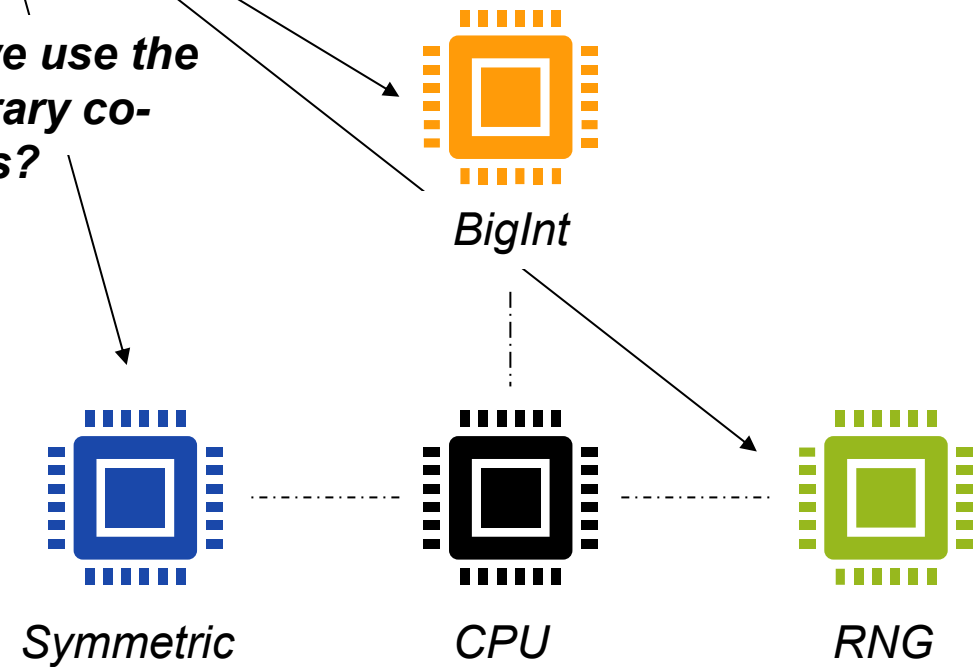
# IMPLEMENTING POST-QUANTUM CRYPTOGRAPHY



- ▶ For the lattice KEMs, the main decision will be Kyber/NTRU/Saber
- ▶ Similarly for lattice signatures, the main decision will be Dilithium/Falcon

-- Dustin Moody (NIST R3 Status Update)

**How can we use the contemporary co-processors?**





## REUSING EXISTING COPROCESSORS



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

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

“Basic” idea for 128-bit coprocessors

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

Ensure sufficient “space” is reserved to avoid overflow

# KRONECKER SUBSTITUTION: POLYNOMIAL MULTIPLICATION WITH INTEGER MULTIPLIERS

*Polynomial domain*

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

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

×

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

*Kronecker domain (with evaluation point 100)*

$$f(100) = 4030201$$

$$g(100) = 8070605$$

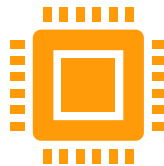
×

$$fg(100) = \underline{32526160341605}$$

Grundzüge einer arithmetischen Theorie der  
algebraischen Grössen.

(Von L. Kronecker.)

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



## HOW TO DO INTEGER MULTIPLICATIONS?

- First proposed by [A] for Kyber & NewHope
- **Saber**:  $R_{8192}[X]/(X^{256} + 1)$ 
  - Evaluate at  $2^{32} \rightarrow$  **8192-bit** integer multiplication
- **Q**: How should we do the multiplication?
  - **A**: It depends on the size of the multiplier..

This allows to re-use existing arithmetic co-processors designed for RSA / ECC.

Table. Number of  $w$ -bit multiplications for a polynomial multiplication in Saber

Multiplier width	8192	4096	2048	1024	512
Schoolbook	1	4	16	64	256
Karatsuba (rec.)	1	3	9	27	81
Toom-Cook- $t$	1	3	7	15	31
<b>Kronecker+ [C]</b>	<b>1</b>	<b>2</b>	<b>4</b>	<b>8</b>	<b>16</b>

*“Regular” Kronecker substitution*

*“Multipoint Kronecker substitution” [B]*

[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; Journal of Symbolic and Algebraic Computation 2007

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



## CONCLUSIONS

- Irrelevant if the quantum threat is real or not  
→ Post-quantum crypto is already being requested
- Standards are coming
- **Exciting times to work on crypto & security solutions!**

I am in the  
**Competence Center Crypto & Security**  
working on Long Term Innovation Projects  
We have a great team in Hamburg! We are always  
looking for good Master / PhD interns as well as  
PhD candidates. Interested?

Just contact me:  
[joppe.bos@nxp.com](mailto:joppe.bos@nxp.com)  
Or more generally  
[careers.germany@nxp.com](mailto:careers.germany@nxp.com)



# THANK YOU.

QUESTIONS?



SECURE CONNECTIONS  
FOR A SMARTER WORLD



SECURE CONNECTIONS  
FOR A SMARTER WORLD