GEVALLENSTUDIES WISKUNDIGE INGENIEURSTECHNIEKEN

Joppe Bos

MARCH 2023

SECURE CONNECTIONS
FOR A SMARTER WORLD

PUBLIC

WHOAMI

Joppe W. Bos

Cryptographic Researcher at NXP Semiconductors

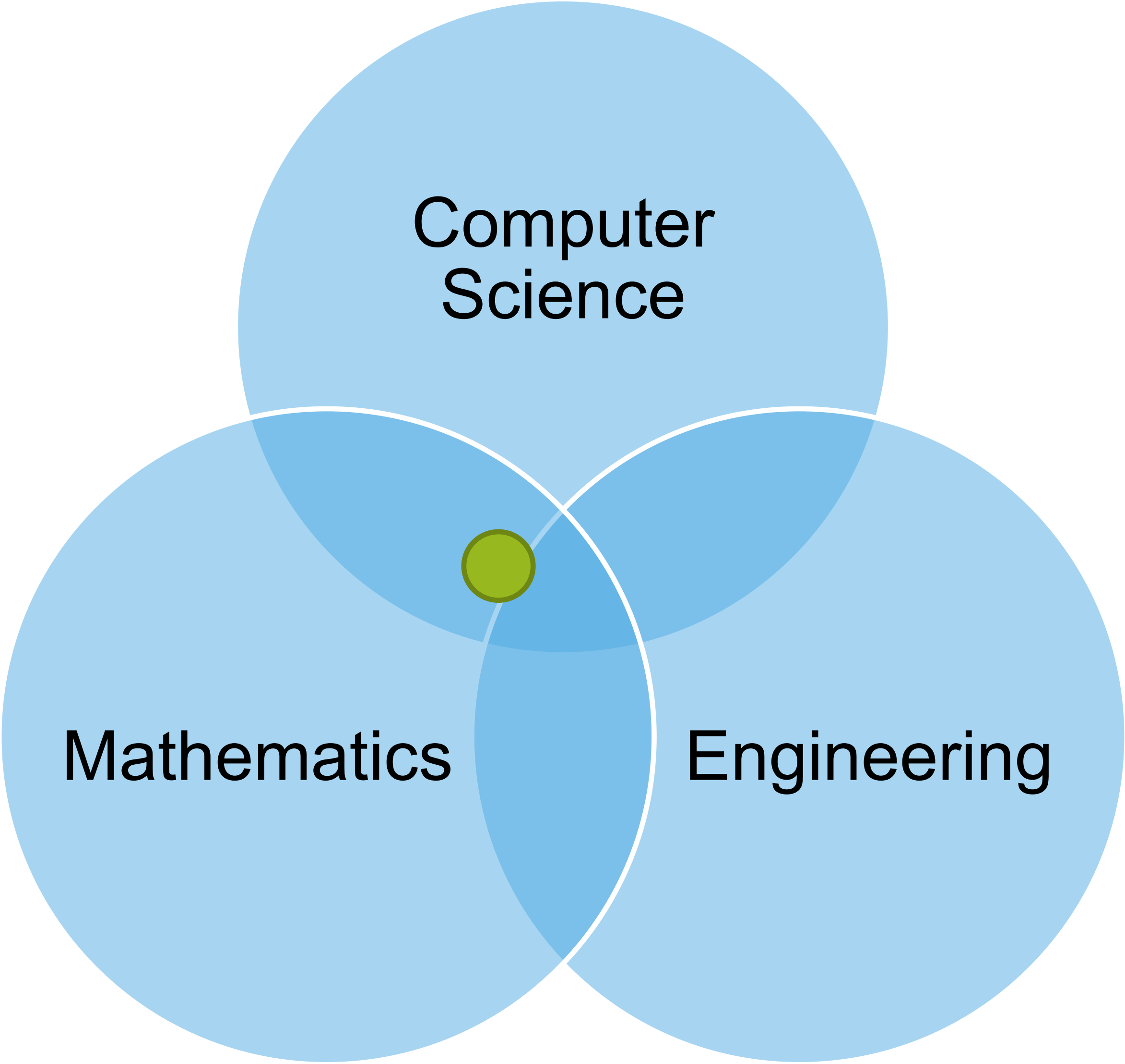
Secretary of the IACR (2017-2019, 2020-2022)

Editor of the Cryptology ePrint Archive (2019-today)

- Cryptographic researcher
  - in the competence center crypto & security at NXP Semiconductors, Leuven
  - Lead the PQC team
  - Lead security + crypto funded projects & university relations
- Post-doc
  - Cryptography Research Group at Microsoft Research, Redmond, USA.
- PhD in Cryptology
  - EPFL, Lausanne, Switzerland
- Bachelor / Master in Computer Science
  - University of Amsterdam

Public Key Cryptography

- Computational number theory
- Number theoretic transform



BREAKING ECC

112-bit ECDLP solved using 224 PlayStation 3 game consoles.

PUBLIC-KEY CRYPTOGRAPHY

In **public-key** cryptography the theoretical foundation of the schemes used are problems which are **believed** to be hard

- Integer factorization problem (RSA)
- Discrete logarithm problem (DSA, ElGamal)

One of the main ingredients to these problems is a group

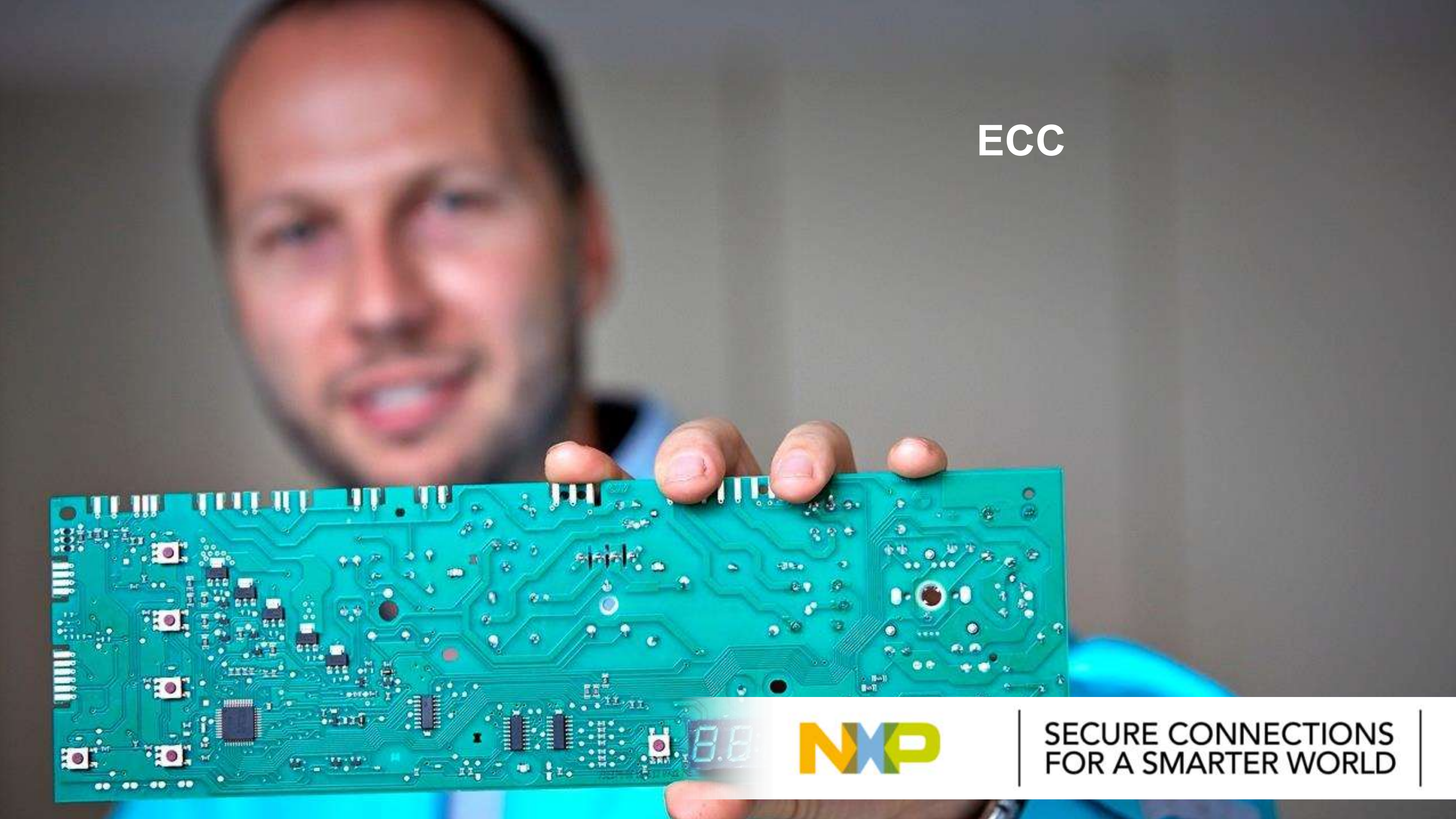
RSA → $(\mathbb{Z}/N\mathbb{Z})^{\times}$→ integers $[\,1, 2, \dots, N-1]$ which are co-prime to N

DSA/ElGamal → $\mathbb{F}_p^{\times} = (\mathbb{Z}/p\mathbb{Z})^{\times}$ → integers $[\,1, 2, \dots, p-1]$ where p is prime

Elliptic Curve Cryptography → $E/\mathbb{F}_p$ → point on $E(\mathbb{F}_p)$ where p is prime

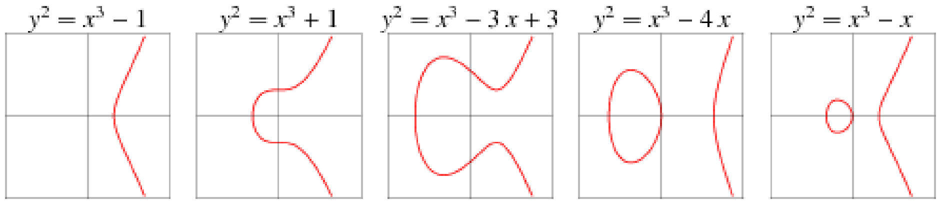
<table>
<tr><td>Application</td><td colspan="3">Encryption Scheme, Signature Scheme, Identification Scheme, etc.</td></tr>
<tr><td>Cryptosystem</td><td colspan="2">DSA, ElGamal, Schnorr, etc.</td><td>RSA, Rabin, etc.</td></tr>
<tr><td>Computational Problem</td><td colspan="2">The Discrete Logarithm Problem in a Group of prime Order</td><td>The Factoring Problem</td></tr>
<tr><td>Algebraic Structure</td><td>The multiplicative group of integers modulo a prime</td><td>Elliptic Curve Group over a Finite Field</td><td>The set of integers modulo the product of two primes</td></tr>
</table>

ECC



EXAMPLE: ELLIPTIC CURVES

What is an elliptic curve?



Not an ellipse!

<u>Mathematical perspective</u>
Smooth, projective algebraic curve of genus one which together with a point “at infinity” forms an abelian variety

<u>Practical perspective</u>
When defined over a large prime field an elliptic curve simply is

$$E/\mathbb{F}_p: y^2 = x^3 + ax + b \qquad \text{such that} \qquad 4a^3 + 27b^2 \neq 0$$

Number of points

How many points can we expect?

$$E(\mathbb{F}_p) : y^2 = x^3 + ax + b$$

Number of points

How many points can we expect?

$E(\mathbb{F}_p) : y^2 = x^3 + ax + b$

Estimate:

- there are p different values for x
- for approximately $\frac{p}{2}$ a square root exists
- if it exists, we have two solutions
- $\rightarrow \text{estimate } 2 \cdot \frac{p}{2} = p$ points

Number of points

How many points can we expect?

$$E(\mathbb{F}_p) : y^2 = x^3 + ax + b$$

Estimate:

- there are p different values for x
- for approximately $\frac{p}{2}$ a square root exists
- if it exists, we have two solutions
- $\rightarrow$ estimate $2 \cdot \frac{p}{2} = p$ points

Hasse's theorem on elliptic curves

$$\#E(\mathbb{F}_p) = p + 1 - t$$

with $|t| < 2\sqrt{p}$

Number of points

How many points can we expect?

$E(\mathbb{F}_p): y^2 = x^3 + ax + b$

Estimate:

- there are p different values for x
- for approximately $\frac{p}{2}$ a square root exists
- if it exists, we have two solutions
- $\rightarrow$ estimate $2 \cdot \frac{p}{2} = p$ points

Hasse's theorem on elliptic curves

$$\#E(\mathbb{F}_p) = p + 1 - t$$

with $|t| < 2\sqrt{p}$

Can we use any elliptic curve in cryptography? No!
When $\#E(\mathbb{F}_p) = n = \prod_{i=1}^{m} p_i$ with p_i prime then
solving the DLP in $E(\mathbb{F}_p)$ can be done by solving m easier DLPs (*Pohlig–Hellman*)

Number of points

How many points can we expect?

$$E(\mathbb{F}_p) : y^2 = x^3 + ax + b$$

Estimate:

- there are p different values for x
- for approximately $\frac{p}{2}$ a square root exists
- if it exists, we have two solutions
- $\rightarrow$ estimate $2 \cdot \frac{p}{2} = p$ points

Hasse's theorem on elliptic curves

$$\#E(\mathbb{F}_p) = p + 1 - t$$

with $|t| < 2\sqrt{p}$

Can we use any elliptic curve in cryptography? No!
When $\#E(\mathbb{F}_p) = n = \prod_{i=1}^{m} p_i$ with p_i prime then
solving the DLP in $E(\mathbb{F}_p)$ can be done by solving m easier DLPs (*Pohlig–Hellman*)

For ECC we require large prime order subgroups
(almost all curves in the current standards have prime order)

HOW TO MEASURE SECURITY?

Asymptotically run-time of crypto attacks is measured using (for $n \to \infty$)

$$L_n(\alpha, c) = \exp\left((c + o(1))(\ln(n)^{\alpha})(\ln(\ln(n))^{1-\alpha})\right)$$

Where $c > 0$ and $0 \leq \alpha \leq 1$.

HOW TO MEASURE SECURITY?

Asymptotically run-time of crypto attacks is measured using (for $n \to \infty$)

$$L_n(\alpha, c) = \exp\left(\left(c + o(1)\right)(\ln(n)^\alpha)(\ln(\ln(n))^{1-\alpha})\right)$$

Where $c > 0$ and $0 \leq \alpha \leq 1$.

Why? Because this allow one to measure
<u>sub-exponential</u> runtimes

$L_n(0, c) = (\ln(n))^{c+o(1)}$: polynomial in $\ln(n)$
$L_n(1, c) = n^{c+o(1)}$: exponential in $\ln(n)$

- When $0 < \alpha < 1$: **<u>sub-exponential</u>**

HOW TO MEASURE SECURITY?

- Factoring integers $\rightarrow$ breaking RSA
- Breaking RSA $\stackrel{?}{\rightarrow}$ factoring integers

Best publicly known factorization algorithm:

Number Field Sieve: $L_n\left(\mathbf{\frac{1}{3}}, \sqrt[3]{\frac{64}{9}}\right)$

HOW TO MEASURE SECURITY?

- Factoring integers $\rightarrow$ breaking RSA
- Breaking RSA $\overset{?}{\rightarrow}$ factoring integers

Best publicly known factorization algorithm:

Number Field Sieve: $L_n\left(\mathbf{\frac{1}{3}}, \sqrt[3]{\frac{64}{9}}\right)$

✓ **Idea**: $n = p \cdot q = \left(\frac{p+q}{2}\right)^2 - \left(\frac{p-q}{2}\right)^2$,
find integers $x^2 \equiv y^2 \pmod{n}$ s.t. $x \not\equiv y \pmod{n}$

✓ This can be done by finding “relations” and relies on the fact that we can break down $x \in (\mathbb{Z}/n\mathbb{Z})^*$ in elementary pieces (find the prime divisors).

Elliptic curve discrete logarithm problem

Given $\mathrm{P}, \mathrm{Q} \in E(\mathbb{F}_p)$ of prime order n find the integer k such that $k \cdot P = Q$.

Elliptic curve discrete logarithm problem

Given $\mathrm{P}, \mathrm{Q} \in E(\mathbb{F}_p)$ of prime order n find the integer k such that $k \cdot P = Q$.

Best publicly known algorithm are the “generic” ones

Pollard rho: $L_n\left(\mathbf{1}, \frac{1}{2}\right) = \mathcal{O}(\sqrt{n})$ exponential in $\ln(n)$

- No equivalent of prime divisors for elliptic curve points (known)

HOW TO MEASURE SECURITY?

Elliptic curve discrete logarithm problem

Given $\mathrm{P}, \mathrm{Q} \in E(\mathbb{F}_p)$ of prime order n find the integer k such that $k \cdot P = Q$.

Best publicly known algorithm are the "generic" ones

Pollard rho: $L_n\left(\mathbf{1}, \frac{1}{2}\right) = \mathcal{O}(\sqrt{n})$ exponential in $\ln(n)$

- No equivalent of prime divisors for elliptic curve points (known)

Consequence

- Key sizes grow much slower compared to RSA
- Smaller keys
  → less storage and smaller intermediate results

ECC KEYS

Domain parameters

$$(p, a, b, G, n, h)$$

- $p \in \mathbb{Z}$ prime number which defines $\mathbb{F}_p$
- $a, b \in \mathbb{F}_p$ define $y^2 = x^3 + ax + b$
- $G = (x, y) \in E(\mathbb{F}_p)$
- $n \in \mathbb{Z}$ prime order of G
- $h \in \mathbb{Z}$ co-factor, $h = \#E(\mathbb{F}_p)/n$

Private key: $d \in \mathbb{Z}/n\mathbb{Z}$
Public key: $P = d \cdot G \in E(\mathbb{F}_p)$

ECC KEYS

Domain parameters

$$(p, a, b, G, n, h)$$

- $p \in \mathbb{Z}$ prime number which defines $\mathbb{F}_p$
- $a, b \in \mathbb{F}_p$ define $y^2 = x^3 + ax + b$
- $G = (x, y) \in E(\mathbb{F}_p)$
- $n \in \mathbb{Z}$ prime order of G
- $h \in \mathbb{Z}$ co-factor, $h = \#E(\mathbb{F}_p)/n$

These domain parameters are publicly available through named identifiers

Private key: $d \in \mathbb{Z}/n\mathbb{Z}$
Public key: $P = d \cdot G \in E(\mathbb{F}_p)$

NIST	SEC	ANSI X9.62	OpenSSL
Curve P-192	secp192r1	prime192v1	prime192v1
Curve P-224	secp224r1		secp224r1
Curve P-256	secp256r1	prime256v1	prime256v1
Curve P-384	secp384r1		secp384r1
Curve P-521	secp521r1		secp521r1

Key Agreement: ECDH

Elliptic Curve Diffie–Hellman is an anonymous key agreement protocol that allows two parties, each having an elliptic curve public/private key pair, to establish a shared secret over an insecure channel

Key Agreement: ECDH

Elliptic Curve Diffie–Hellman is an anonymous key agreement protocol that allows two parties, each having an elliptic curve public/private key pair, to establish a shared secret over an insecure channel.

Assuming shared domain parameters

Alice		**Bob**
$P_a \ (= d_a \cdot G)$		$P_b \ (= d_b \cdot G)$
	$\overset{P_b}{\longleftarrow}$ and $\overset{P_a}{\longrightarrow}$	
$d_a \cdot P_b$		$d_b \cdot P_a$

$$d_a \cdot P_b = d_a \cdot d_b \cdot G = d_b \cdot P_a$$

Key Agreement: ECDH

Elliptic Curve Diffie–Hellman is an anonymous key agreement protocol that allows two parties, each having an elliptic curve public/private key pair, to establish a shared secret over an insecure channel.

Assuming shared domain parameters

Alice		Bob
$P_a \ (= d_a \cdot G)$		$P_b \ (= d_b \cdot G)$
	$\overset{P_b}{\longleftarrow}$ and $\overset{P_a}{\longrightarrow}$	
$d_a \cdot P_b$		$d_b \cdot P_a$

$$d_a \cdot P_b = d_a \cdot d_b \cdot G = d_b \cdot P_a$$

So-called **static** public keys which needs to be trusted (e.g. through a certificate)

If someone breaks your key they can read all your messages from the past and future!

Key Agreement: ECDHE

<u>Ephemeral</u> Diffie-Hellman

Each instance or run of the protocol uses a different public key

Instead of using P_a $(= d_a \cdot G)$ pick a fresh random $r \in [1, \ldots n-1]$ and use

$$r \cdot P_a \;(= (r \cdot d_a) \cdot G)$$

Key Agreement: ECDHE

<u>Ephemeral</u> Diffie-Hellman

Each instance or run of the protocol uses a different public key

Instead of using $P_a \ (= d_a \cdot G)$ pick a fresh random $r \in [1, \dots n-1]$ and use

$$r \cdot P_a \ (= (r \cdot d_a) \cdot G)$$

Advantage	Disadvantage
Compromise of the server's long term signing key d_a ***does not*** jeopardize the privacy of past sessions	Increased computation costs. Two elliptic curve scalar multiplications required

Key Agreement: ECDHE

<u>Ephemeral</u> Diffie-Hellman

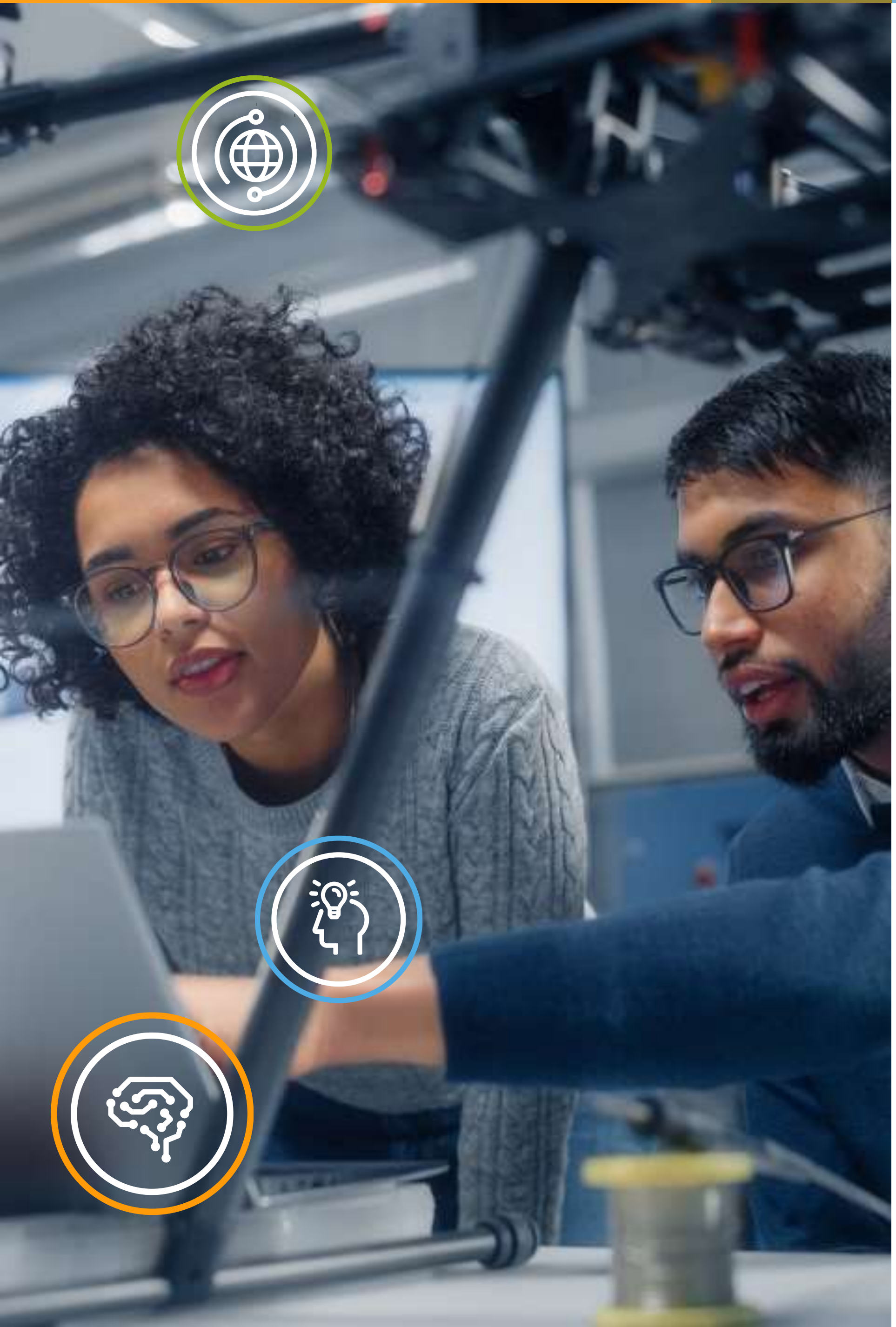
Each instance or run of the protocol uses a different public key

Instead of using P_a $(= d_a \cdot G)$ pick a fresh random $r \in [1, \ldots n-1]$ and use

$$r \cdot P_a \ (= (r \cdot d_a) \cdot G)$$

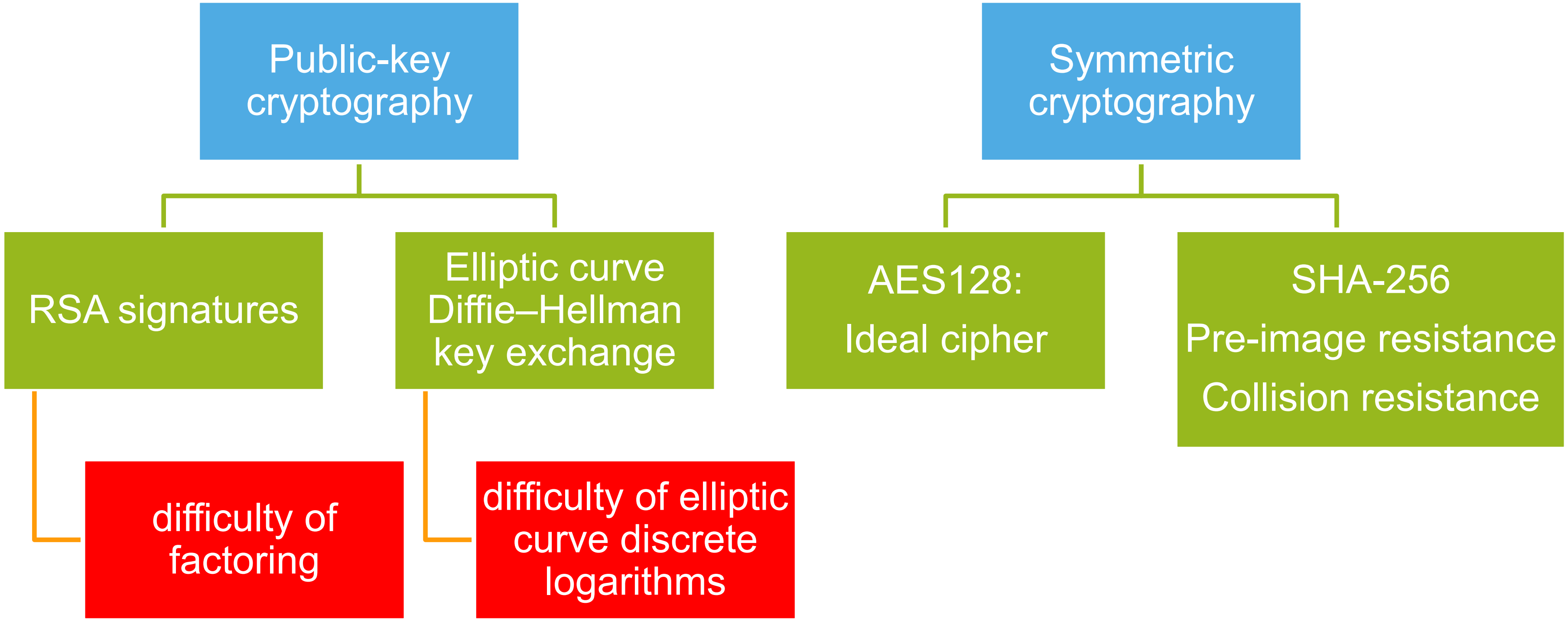
Advantage	Disadvantage
Compromise of the server's long term signing key d_a ***does not*** jeopardize the privacy of past sessions	Increased computation costs. Two elliptic curve scalar multiplications required

This feature is known as *Perfect Forward Secrecy (PFS)*



Transition: From ECC + RSA to PQC

CONTEMPORARY CRYPTOGRAPHY
TLS-ECDHE-RSA-AES128-GCM-SHA256



microsoft.com/en-us/research/lab/quantum

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 con
"Station Q" lab was established in 2005 on the campus of the Unive
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/603165/intel-bets-it-can-turn-everyday-silicon-into-quantum-computings-wonder-material

Machines

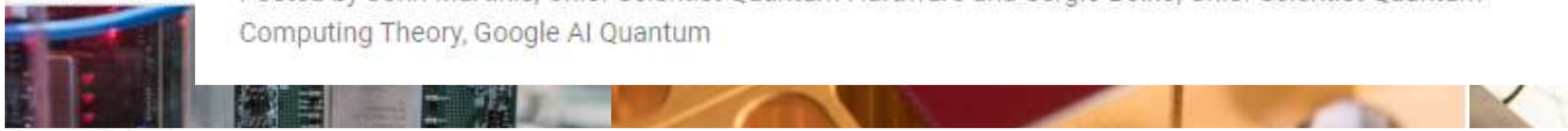
...Bets It Can Turn Everyday ...n into Quantum Computing's ...ler Material

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

...onite December 21, 2016

...his to test quantum computing devices at

Bloomberg L.P. [US] bloomberg.com



WIRED BACKCHANNEL BUSINESS CULTURE GEAR IDEAS SCIENCE SECURITY

TOM SIMONITE BUSINESS 12.03.2020 02:00 PM

China Stakes Its Claim to Quantum Supremacy

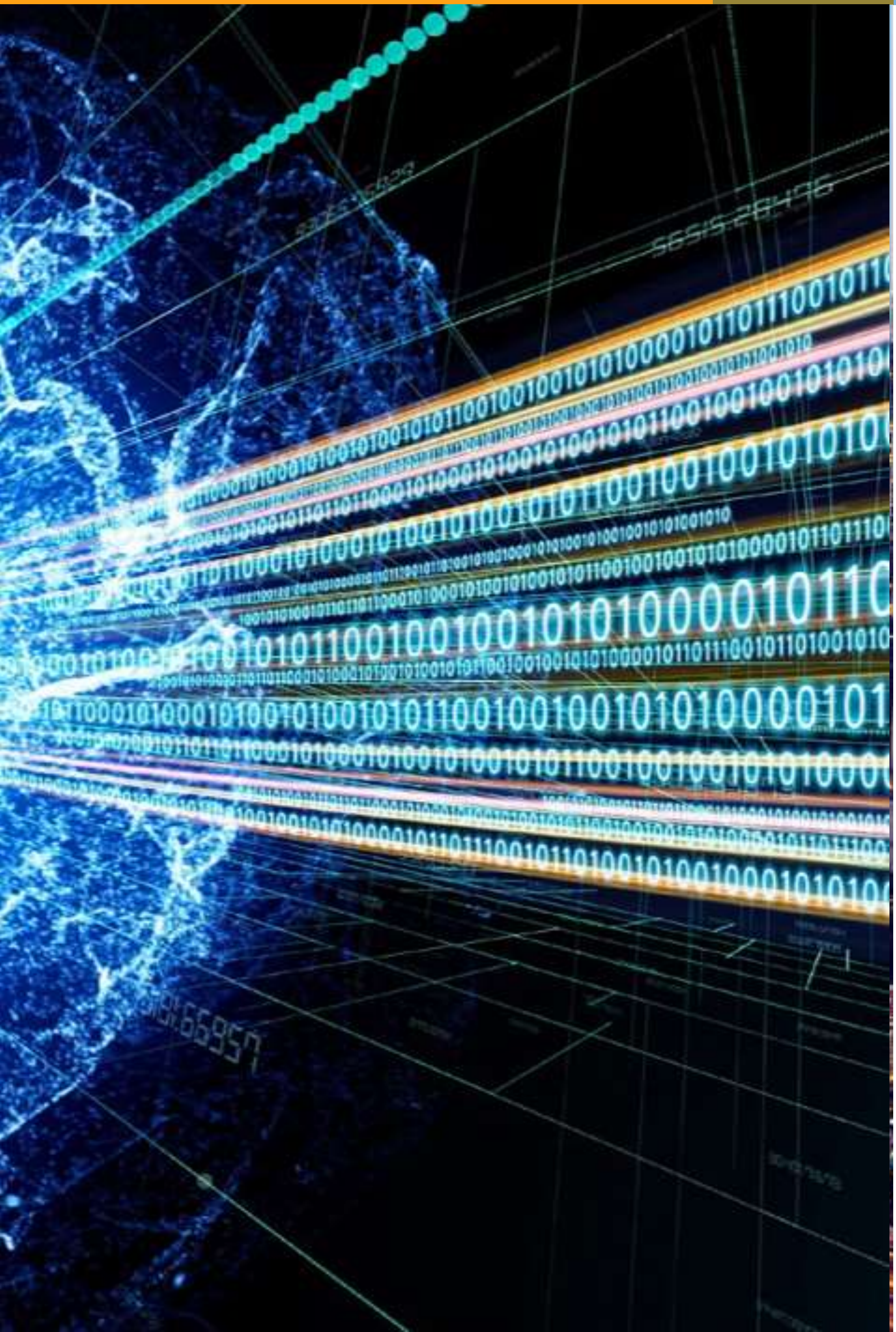
Google trumpeted its quantum computer that outperformed a conventional supercomputer. A Chinese group says it's done the same, with different technology.

...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

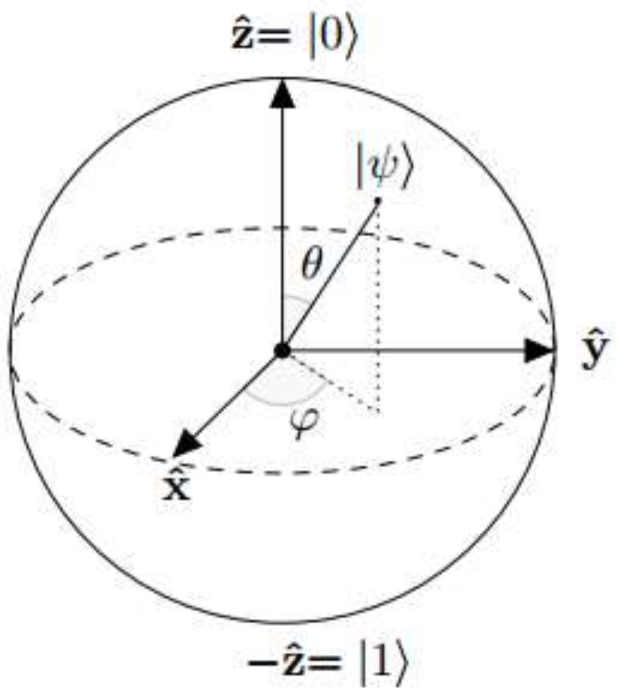
Quantum computers hold the promise of being able to take on certain problems exponentially faster compared to a normal computer

- 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

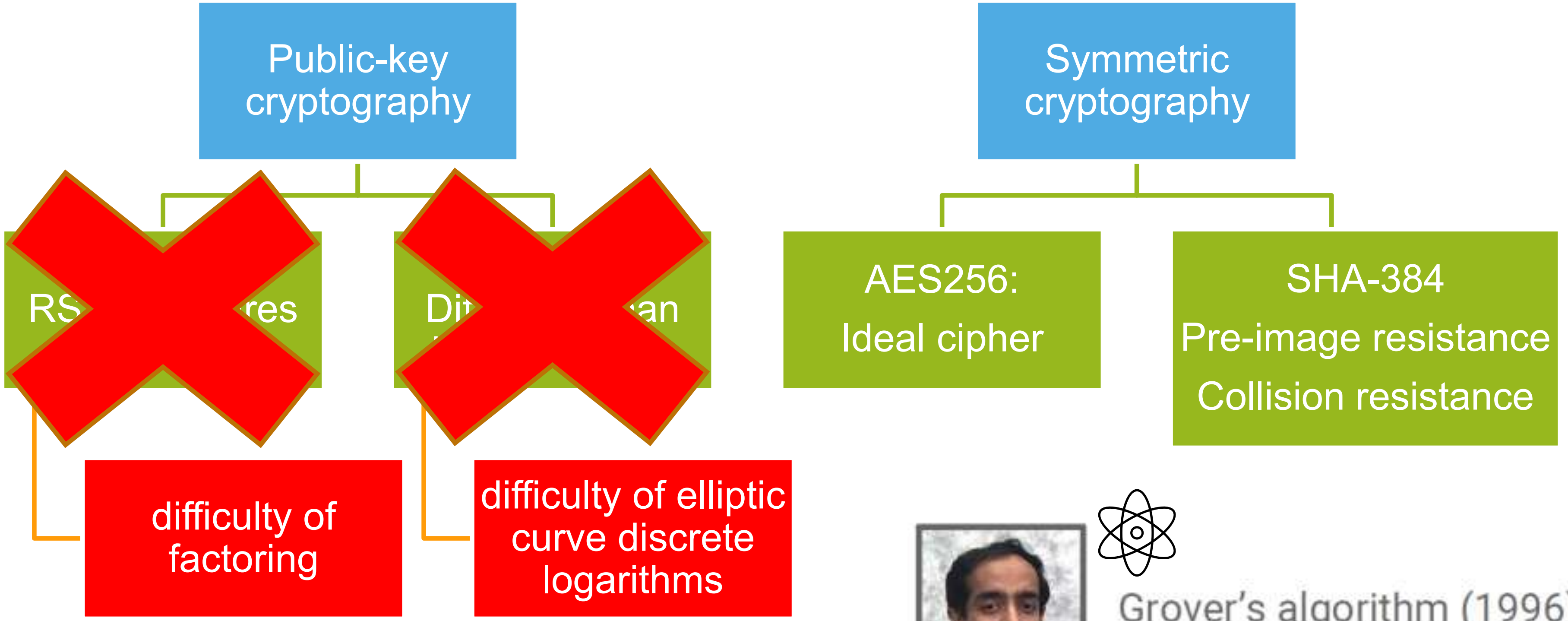
State-of-the-art.
IBM's 127-Qubit Quantum Processor
Break RSA-3072:
~10,000 qubits are needed

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.

CONTEMPORARY CRYPTOGRAPHY

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

"Double" the key sizes



Grover's algorithm (1996)

Shor's algorithm (1994)

Quantum Potential To destroy Security As We know it

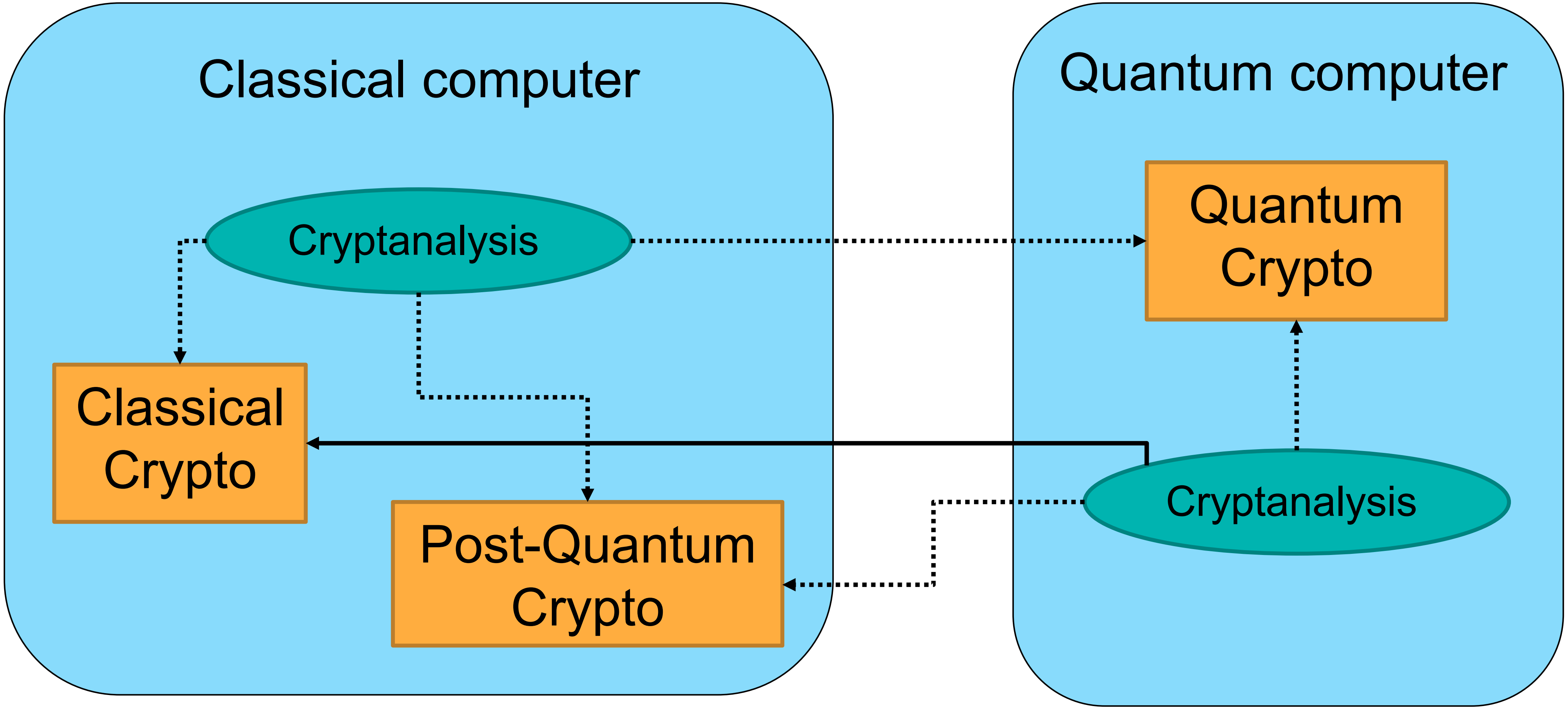
Confidential email messages, private documents, and financial transactions
Secure today but may be compromised in the future, even if recorded & encrypted

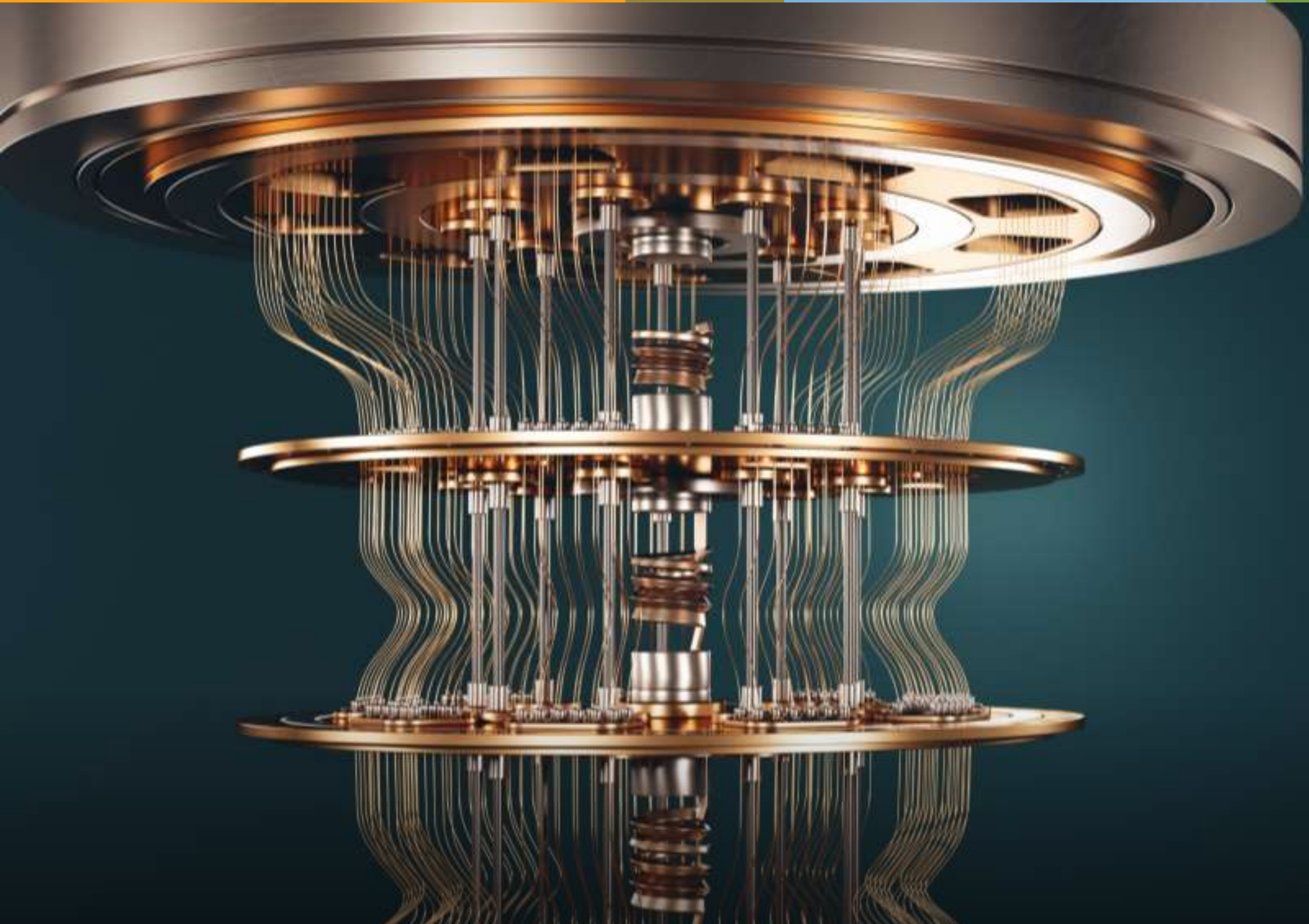
Firmware update mechanisms in vehicles
May be circumvented and allow dangerous modifications

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 to PQC

AUTOMOTIVE

EGOVERNMENT

BANK CARDS

MIFARE

SMART MOBILITY (MIFARE) CARDS

TAGS & AUTHENTICATION

READERS

MOBILE

LEARNING WITH ERROR PROBLEM

SOLVING SYSTEMS OF LINEAR EQUATIONS

$$\underset{\mathbb{Z}_{13}^{7\times 4}}{\begin{bmatrix} 4 & 1 & 11 & 10 \\ 5 & 5 & 9 & 5 \\ 3 & 9 & 0 & 10 \\ 1 & 3 & 3 & 2 \\ 12 & 7 & 3 & 4 \\ 6 & 5 & 11 & 4 \\ 3 & 3 & 5 & 0 \end{bmatrix}} \times \underset{\mathbb{Z}_{13}^{4\times 1}}{\overset{\text{secret}}{\begin{bmatrix} \; \\ \; \\ \; \\ \; \end{bmatrix}}} = \underset{\mathbb{Z}_{13}^{7\times 1}}{\begin{bmatrix} 4 \\ 8 \\ 1 \\ 10 \\ 4 \\ 12 \\ 9 \end{bmatrix}}$$

Linear system problem: given **blue**, find **red**

SOLVING SYSTEMS OF LINEAR EQUATIONS

secret

$$\underset{\mathbb{Z}_{13}^{7\times 4}}{\begin{bmatrix} 4 & 1 & 11 & 10 \\ 5 & 5 & 9 & 5 \\ 3 & 9 & 0 & 10 \\ 1 & 3 & 3 & 2 \\ 12 & 7 & 3 & 4 \\ 6 & 5 & 11 & 4 \\ 3 & 3 & 5 & 0 \end{bmatrix}} \times \underset{\mathbb{Z}_{13}^{4\times 1}}{\begin{bmatrix} 6 \\ 9 \\ 11 \\ 11 \end{bmatrix}} = \underset{\mathbb{Z}_{13}^{7\times 1}}{\begin{bmatrix} 4 \\ 8 \\ 1 \\ 10 \\ 4 \\ 12 \\ 9 \end{bmatrix}}$$

Easily solved using Gaussian elimination (Linear Algebra 101)

Linear system problem: given **blue**, find **red**

LEARNING WITH ERRORS PROBLEM

random $\mathbb{Z}_{13}^{7\times 4}$ × secret $\mathbb{Z}_{13}^{4\times 1}$ + small noise $\mathbb{Z}_{13}^{7\times 1}$ = $\mathbb{Z}_{13}^{7\times 1}$

$$\begin{pmatrix} 4 & 1 & 11 & 10 \\ 5 & 5 & 9 & 5 \\ 3 & 9 & 0 & 10 \\ 1 & 3 & 3 & 2 \\ 12 & 7 & 3 & 4 \\ 6 & 5 & 11 & 4 \\ 3 & 3 & 5 & 0 \end{pmatrix} \times \begin{pmatrix} 6 \\ 9 \\ 11 \\ 11 \end{pmatrix} + \begin{pmatrix} 0 \\ -1 \\ 1 \\ 1 \\ 1 \\ 0 \\ -1 \end{pmatrix} = \begin{pmatrix} 4 \\ 7 \\ 2 \\ 11 \\ 5 \\ 12 \\ 8 \end{pmatrix}$$

LEARNING WITH ERRORS PROBLEM

$$\underset{\text{random}\ \mathbb{Z}_{13}^{7\times 4}}{\begin{pmatrix} 4 & 1 & 11 & 10 \\ 5 & 5 & 9 & 5 \\ 3 & 9 & 0 & 10 \\ 1 & 3 & 3 & 2 \\ 12 & 7 & 3 & 4 \\ 6 & 5 & 11 & 4 \\ 3 & 3 & 5 & 0 \end{pmatrix}} \times \underset{\text{secret}\ \mathbb{Z}_{13}^{4\times 1}}{\begin{pmatrix} \ \\ \ \\ \ \\ \ \end{pmatrix}} + \underset{\text{small noise}\ \mathbb{Z}_{13}^{7\times 1}}{\begin{pmatrix} \ \\ \ \\ \ \\ \ \\ \ \\ \ \\ \ \end{pmatrix}} = \underset{\mathbb{Z}_{13}^{7\times 1}}{\begin{pmatrix} 4 \\ 7 \\ 2 \\ 11 \\ 5 \\ 12 \\ 8 \end{pmatrix}}$$

Computational LWE problem: given **blue**, find **red**

TOY EXAMPLE VERSUS REAL-WORLD EXAMPLE

$\mathbb{Z}_{13}^{7\times 4}$

4	1	11	10
5	5	9	5
3	9	0	10
1	3	3	2
12	7	3	4
6	5	11	4
3	3	5	0

$\mathbb{Z}_{2^{15}}^{752\times 8}$

8

752

2738	3842	3345	2979	…
2896	595	3607		
377	1575			
2760				
…				

752 × 8 × 15 bits = **11 KiB**

RING LEARNING WITH ERRORS PROBLEM

random

$\mathbb{Z}_{13}^{7\times 4}$

4	1	11	10
10	4	1	11
11	10	4	1
1	11	10	4
4	1	11	10
10	4	1	11
11	10	4	1

Each row is the cyclic shift of the row above

RING LEARNING WITH ERRORS PROBLEM

random
$\mathbb{Z}_{13}^{7\times 4}$

4	1	11	10
3	4	1	11
2	3	4	1
12	2	3	4
9	12	2	3
10	9	12	2
11	10	9	12

Each row is the cyclic shift of the row above

…

with a special wrapping rule: x wraps to $-x$ mod 13.

RING LEARNING WITH ERRORS PROBLEM

random
$\mathbb{Z}_{13}^{7\times 4}$

4	**1**	**11**	**10**

Each row is the cyclic
shift of the row above
…
with a special wrapping rule:
x wraps to –*x* mod 13 (→ $\mathbb{Z}_{13}[x]/\langle x^4+1\rangle$)

So I only need to tell you the first row.

RING LEARNING WITH ERRORS PROBLEM

$$\mathbb{Z}_{13}[x]/\langle x^4 + 1 \rangle$$

	$4 + 1x + 11x^2 + 10x^3$	random
$\times$	$6 + 9x + 11x^2 + 11x^3$	secret
$+$	$0 - 1x + 1x^2 + 1x^3$	small noise
$=$	$10 + 5x + 10x^2 + 7x^3$	

RING LEARNING WITH ERRORS PROBLEM

$\mathbb{Z}_{13}[x]/\langle x^4 + 1 \rangle$

	$4 + 1x + 11x^2 + 10x^3$	**random**
×		**secret**
+		**small noise**
=	$10 + 5x + 10x^2 + 7x^3$	

Computational ring-LWE problem: given **blue**, find **red**

BASIC RING-LWE-DH KEY AGREEMENT

- Reformulation of Peikert's ring-LWE KEM (*PQCrypto 2014*)

public: "big" a in $R_q = \mathbf{Z}_q[x]/(x^n+1)$

Alice

secret:
random "small" s, e in R_q

Bob

secret:
random "small" s', e' in R_q

$b = a \bullet s + e$ →

← $b' = a \bullet s' + e'$

Alice

shared secret:
$s \bullet b' = s \bullet (a \bullet s' \bullet e') \approx s \bullet a \bullet s'$

Bob

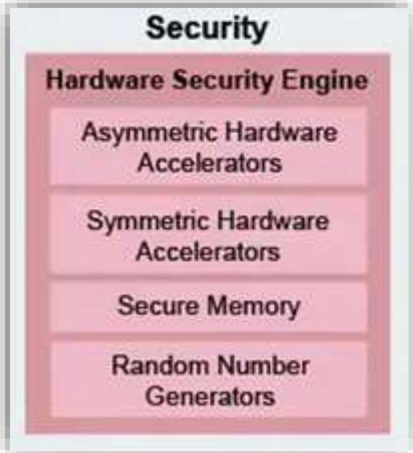
shared secret:
$b \bullet s' \approx s \bullet a \bullet s'$

These are only approximately equal ⇒ need rounding

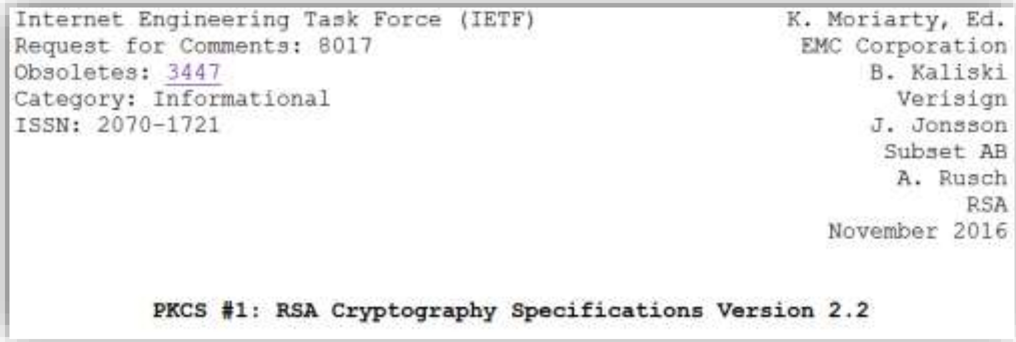
Example of what we do at NXP

Joppe W. Bos, Joost Renes and Christine van Vredendaal: *Polynomial Multiplication with Contemporary Co-Processors: Beyond Kronecker, Schönhage-Strassen & Nussbaumer*. USENIX Security Symposium 2022.

IMPLEMENTING CLASSICAL CRYPTOGRAPHY

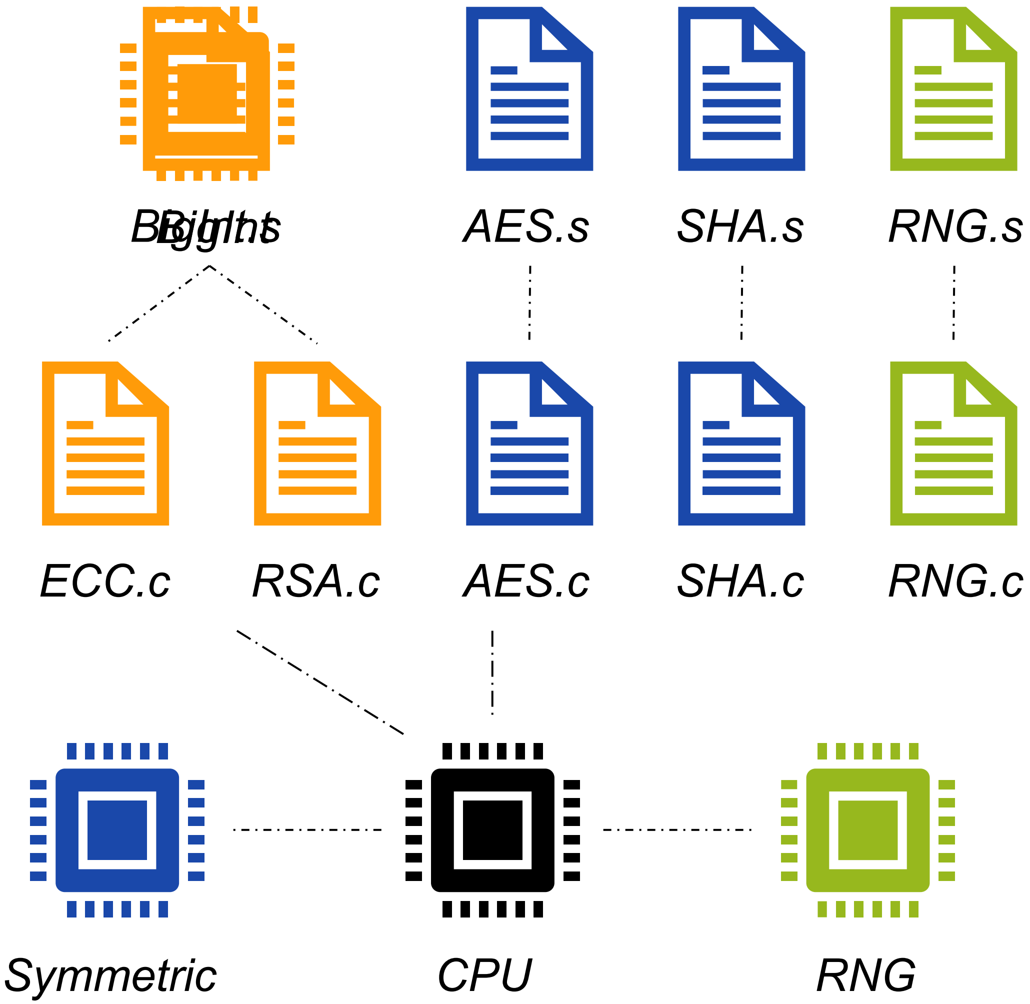


S32G2 automotive processor spec



```
Internet Engineering Task Force (IETF)                 K. Moriarty, Ed.
Request for Comments: 8017                              EMC Corporation
Obsoletes: 3447                                              B. Kaliski
Category: Informational                                        Verisign
ISSN: 2070-1721                                              J. Jonsson
                                                              Subset AB
                                                               A. Rusch
                                                                    RSA
                                                          November 2016

          PKCS #1: RSA Cryptography Specifications Version 2.2
```

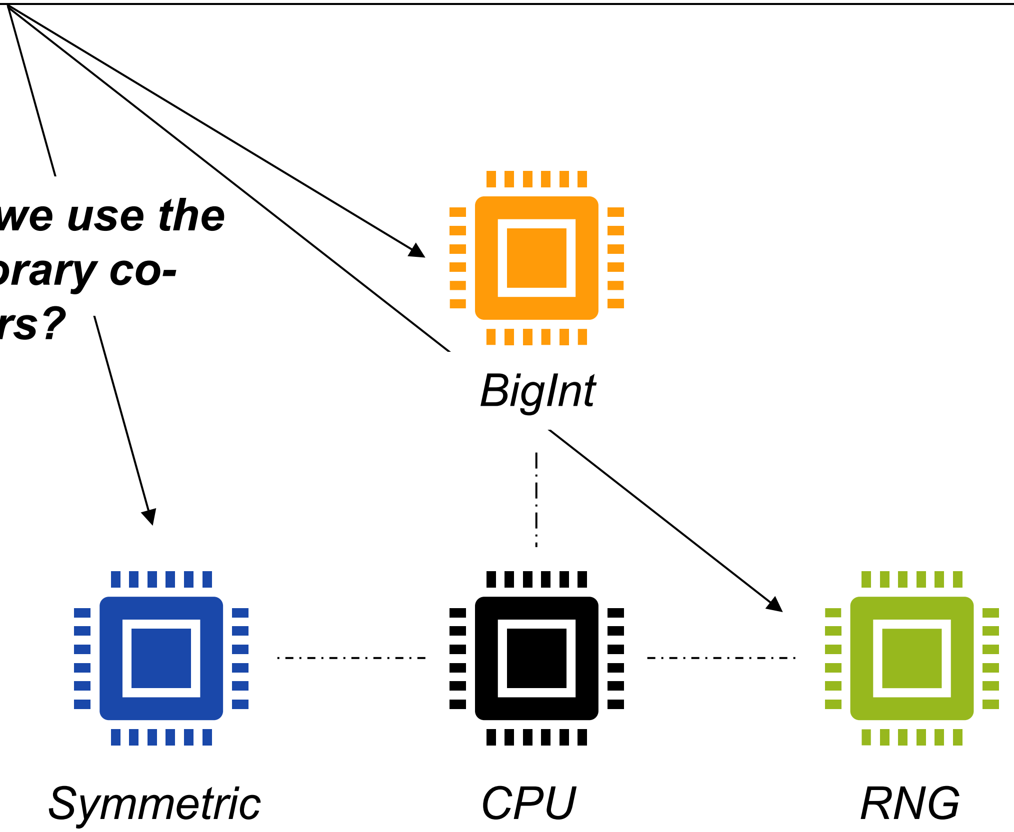


1. https://www.nxp.com/products/processors-and-microcontrollers/arm-processors/s32g-vehicle-network-processors:S32G-PROCESSORS

IMPLEMENTING POST-QUANTUM CRYPTOGRAPHY

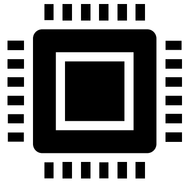
Lattice-based winners: **Kyber, Dilithium, Falcon** (Saber, NTRU, FrodoKEM)

How can we use the contemporary co-processors?



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 chips

Can we use this?

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)

$$f(100) = 4030201$$

$$g(100) = 8070605$$

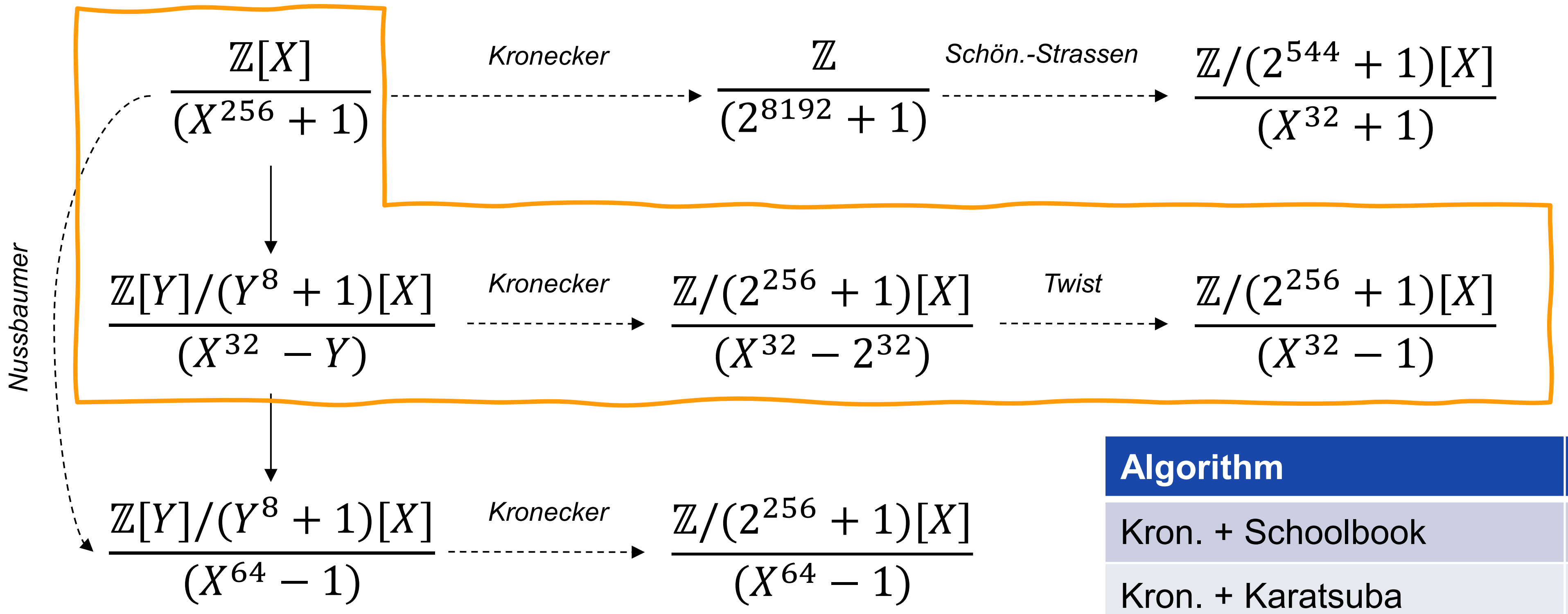
✖

$$fg(100) = 32526160341605$$

POLYNOMIAL MULTIPLICATION TECHNIQUES

Kronecker evaluation at 2^{32}

Multiplication with a 256-bit multiplier



Kronecker+

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.

CONCLUSIONS

- We are always looking for talented young people in math / crypto!
- Need to have an applied interest as well.
- New mathematical techniques to map algorithms to resource constrained devices.

- Software / hardware skills are a plus
- Crypto / number theory knowledge is a must!

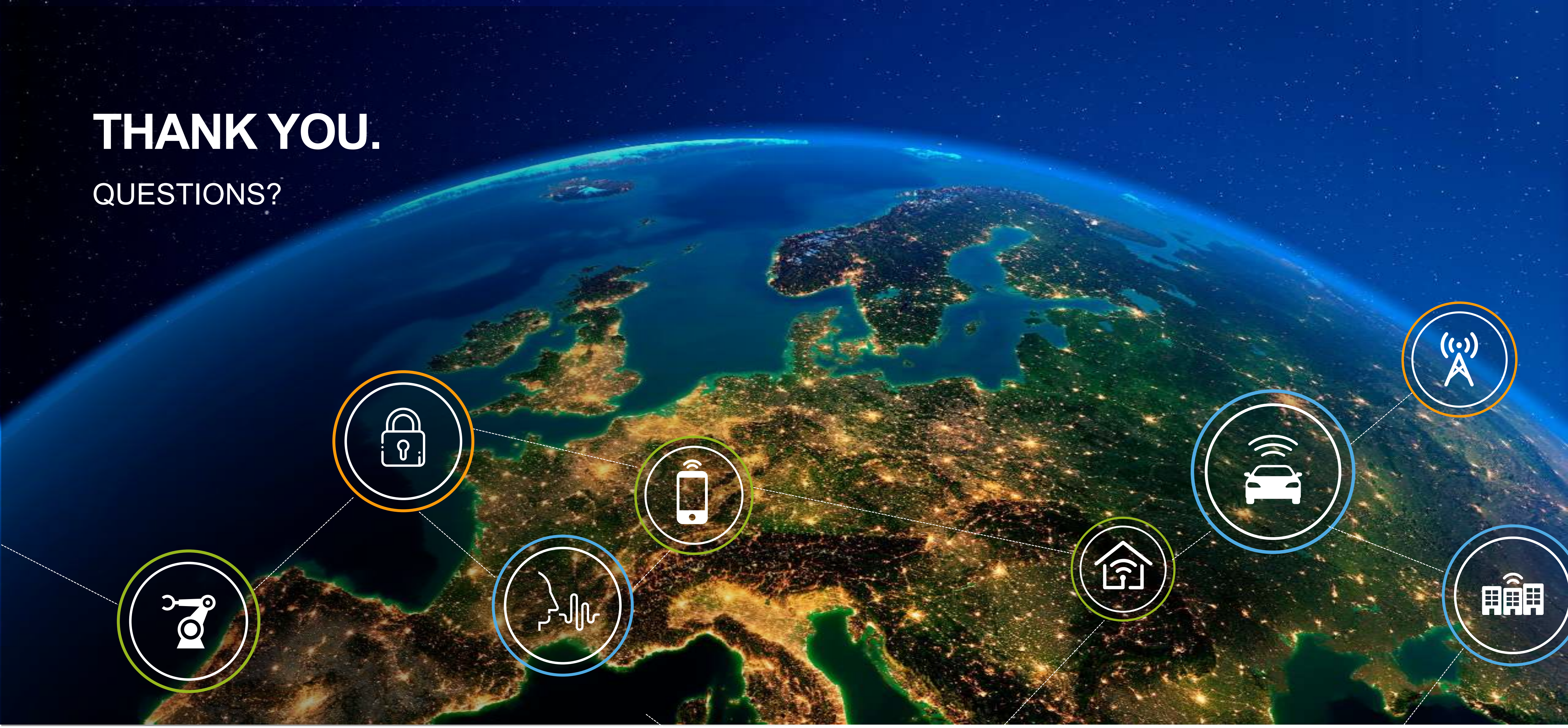
Experience shows it is easier to teach software development skills to an applied mathematician than number theory to an engineer ☺

Interested? Job? Internship? Industry PhD with KU Leuven?

Contact me: joppe.bos@nxp.com

THANK YOU.

QUESTIONS?



SECURE CONNECTIONS
FOR A SMARTER WORLD

SECURE CONNECTIONS
FOR A SMARTER WORLD