Post-Quantum Cryptography (PQC) Initiatives and Key Insights

Dr. Vishal Saraswat
Bosch Cybersecurity University
Vishal.Saraswat@bosch.com

CYBERSECURITY.ONE -Cybersmart in Connected World-

BGSW alt_future

BOSCH CYBERSECURITY UNIVERSITY

BOSCH

Dr. Vishal Saraswat

Personal

Role : Crypto Expert
NE/Dept : BGSW / MS / ECL3
✉ Saraswat.Vishal@in.bosch.com
☎ +91-970-357-2379 (Mobile)

Education

- Ph.D. (Cryptography, UMN, USA)
- M.S. (Mathematics & CSE, UMN, USA)
- Certified Blockchain Expert™

Work Experience

- **01/2019 – *Present* : Bosch Global Software Technologies (BGSW)**
  - Research & Innovation (PQC, Privacy Preservation, Crypto V&V, Reusabilty)
  - Competency Development (Bosch Cybersecurity University)
  - Security Consulting (TARA, Security Concepts, Crypto SME)
  - Security Reviewing (PROSO)
  - **Distinguished Expert, Board of Academics (Math.), MNNIT Allahabad**
- **IIT Jammu, IIT Hyderabad, IIT Palakkad, ISI Kolkata, Univ. of Hyderabad, SPJainSGM, NIIT Univ.**: Adjunct / External / Visiting Faculty
- **Securacy:** Chief Cryptographer
- **AIMSCS:** Faculty Member, Lead Cryptographer
- **University of Minnesota:** Lecturer, Research Assistant, Teaching Assistant, etc.
- **TIFR Bombay:** Research Scholar

Professional Summary

24+ years experience (9 years in USA)
- R&D and Innovation
- Teaching and Training

12+ years leadership experience
- Crypto consulting
- Competency development for academia and industry
- Advanced cybersecurity program development:
  - M.Tech: Information Security, IIT Hyderabad
  - M.Tech: Cyber Security, Univ. of Hyderabad
  - M.Tech: Cyber Security, SPJainSGM
  - P.G.Diploma: Automotive Cybersecurity, BITS Pilani
- Establishing and research and analysis labs
- Consulting
- Mentoring

Research Expertise

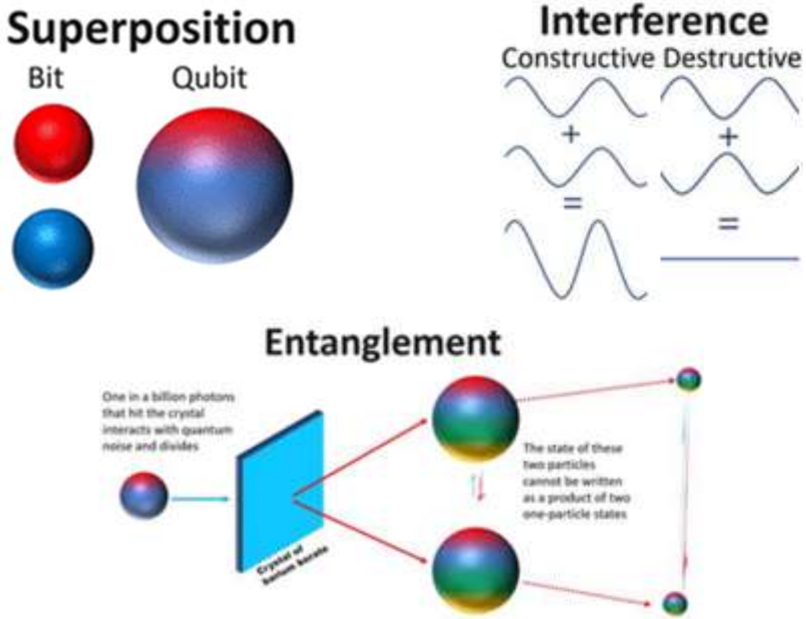
- Post-quantum crypto
- CPS, OT, IIoT, & CI security
- Anonymity and privacy in communication protocols
- Searchable encryption for the cloud-based services
- Lightweight cryptography for IoT devices
- Blockchain security
- Hardware security
- Active and passive cryptanalysis

BOSCH

Quantum Computing

For some problems, supercomputers aren’t that super

- **Quantum Computing** is a rapidly-emerging technology that harnesses the laws of quantum mechanics to solve problems too complex for classical computers.



[McKinsey Quantum Monitor June 2025]

Market size and value at stake: QC companies began a shift toward revenue generation, earning an estimated $650-$750 million in 2024.

Investments and ecosystem +XX% **Compared to previous year**

$8.5B +25% YOY
total cumulative global QT start-up investment

367 +5% YOY
start-ups in the QT ecosystem

$42B +26% YOY
total government investment announced

Quantum technology market size scenarios for 2035 and 2040
Based on existing development road maps and assumed adoption curve

	Quantum computing	Quantum communication	Quantum sensing
2035	$28B–$72B	$11B–$15B	$7B–$10B
2040	$45B–$131B	$24B–$36B	$18B–$31B

Potential economic value[2] from quantum computing in 2035:

~$0.9T–$2.0T

Potential value driven by four industries by 2035: global energy and materials, pharmaceuticals and medical products, financial industry, and travel, transport, and logistics

1. QS approach through clusters of use cases based on recent development, announcements, and breakthroughs.
2. Economic value is defined as the additional revenue and saved costs that the application of QC can unlock.
3. Per annum.

BOSCH

Evolution of Quantum Computers

- QC has already evolved from theoretical research to an engineering enterprise with a potential to save the industry millions of dollars in production and post-production costs.
- **Denso** claims a 15% efficiency in their Automated Guided Vehicle (AGV) routing.
- **BMW** is exploring QC/QT to schedule robots to seal automotive seams to achieve manufacturing efficiency as it scales.
- **Ford** is exploring QC/QT to reduce wear on commercial vehicles by optimizing routes.
- **Volkswagen** is exploring QC/QT to help customers configure a functional and satisfying vehicle by reducing configuration errors.
- **Toyota & Denso & Volkswagen & AirBus** are using QC/QT for real time traffic management systems and fleet routes & dispatch management.
- **EMEA** claims a 30% increase in paint line capacity and a deferring of $1B investment in a new paint line.
- **German Aerospace Center** is exploring QC/QT to optimize airport flight/gate assignment to reduce passenger travel time.

BOSCH

Benefits

Quantum Simulation	Artificial Intelligence and Machine Learning	Optimization Problems	Traffic Optimization
Financial Modeling	Climate Modeling	Pharmaceutical Research	Bio-engineering
Material Science	Quantum Cryptography	Post-Quantum Cryptography	…

BOSCH

Post-Quantum Cryptography (PQC)

- Post-Quantum Cryptography (PQC) is the study of cryptosystems that
  - run on classical computers; and yet
  - are secure against attacks by quantum computers.

Post Quantum Crypto is NOT Quantum Cryptography

- PQC Techniques
  - Code based (e.g., McEliece'78)
  - Hash based (e.g., Merkle trees'79)
  - Lattice based (e.g., NTRU'95, LWE'05)
  - Multivariate based (e.g., HFE'96)
  - Isogeny based (e.g., SIDH'11)

FIPS 203: ML-KEM (**Kyber**)

FIPS 204: ML-DSA (**Dilithium**)

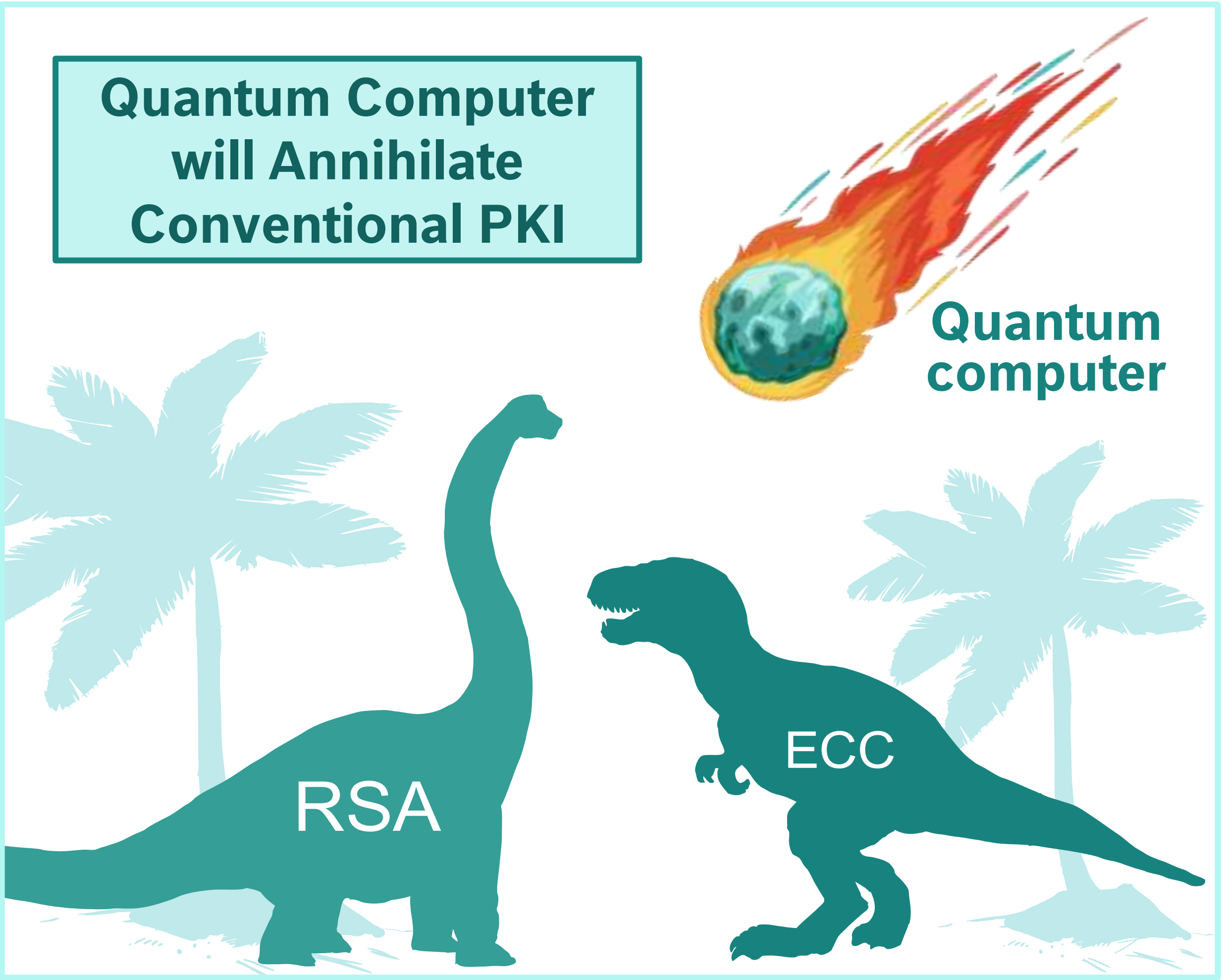
FIPS 205: SH-DSA (**Sphincs+**)

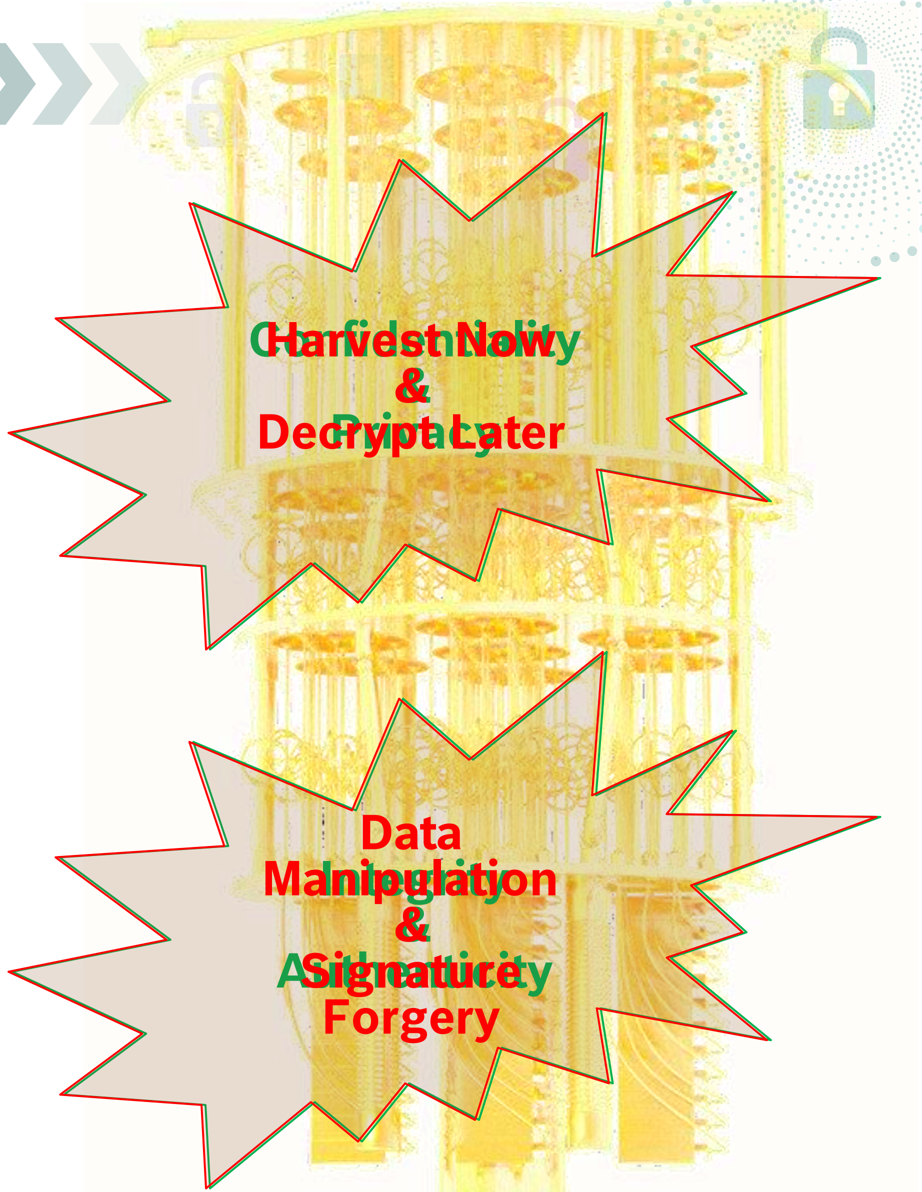
Round 4 KEMs: BIKE, Classic McEliece, HQC, and SIKE

Additional Digital Signature Schemes

XMSS, LMS

Quantum-Resilient Security Controls





McKinsey Quantum Monitor June 2025

Quantum-Resilient Security Controls

Quantum Threat Timeline

Quantum hype bubble?

IBM Quantum Processors

- **2021** Eagle
  - 127 qubits
  - Error Rate: 1%

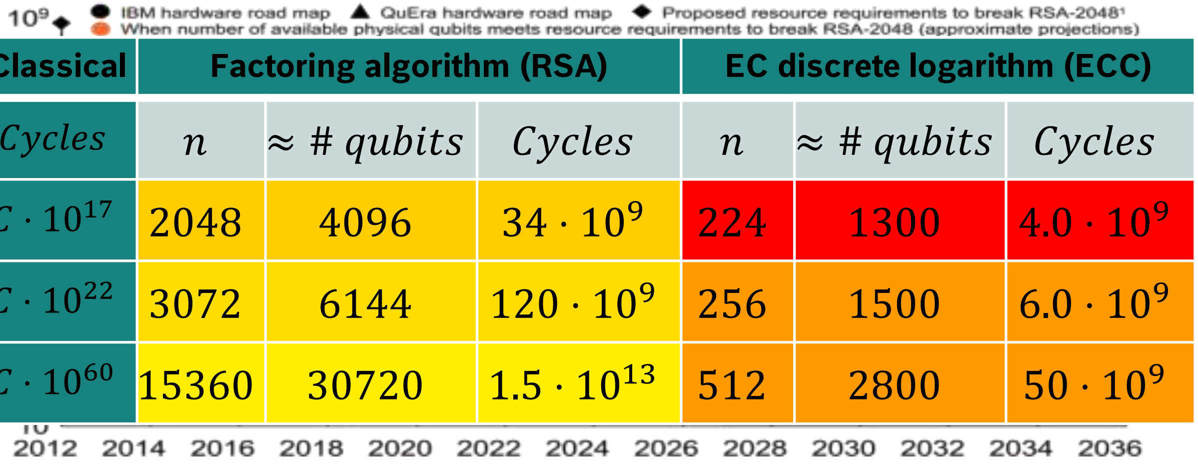
- **2022** Osprey
  - 433 qubits
  - Qiskit

- **2023** Condor
  - 1121 qubits
  - Q. System Two

- **2024** Flamingo
  - 1386 qubits

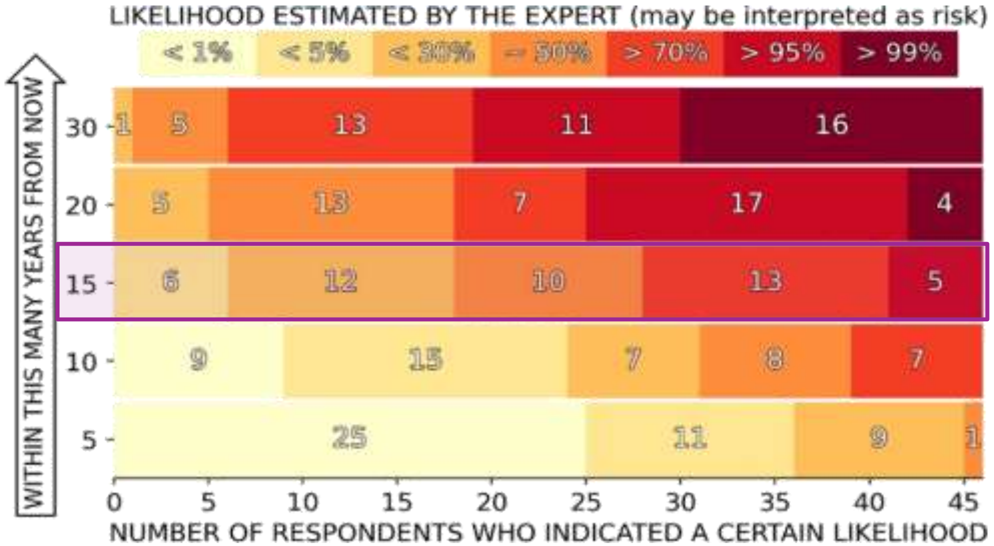
- **2025** Kookaburra
  - 4000 qubits
  - Error Rate: 0.0001%

100k qubits system* beyond 2026



Classical	Factoring algorithm (RSA)			EC discrete logarithm (ECC)		
Cycles	n	$\approx$ # *qubits*	*Cycles*	n	$\approx$ # *qubits*	*Cycles*
$C \cdot 10^{17}$	2048	4096	$34 \cdot 10^9$	224	1300	$4.0 \cdot 10^9$
$C \cdot 10^{22}$	3072	6144	$120 \cdot 10^9$	256	1500	$6.0 \cdot 10^9$
$C \cdot 10^{60}$	15360	30720	$1.5 \cdot 10^{13}$	512	2800	$50 \cdot 10^9$

- **Likelihood of a QC able to break RSA- 2048 in 24 hours**
  - **Directly proportional to the risk**
  - **Within this many years from 2021**



Mosca, M.; Piani, M. (2022): 2021 Quantum Threat Timeline Report.
https://globalriskinstitute.org/publications/2021-quantum-threat-timeline-report/

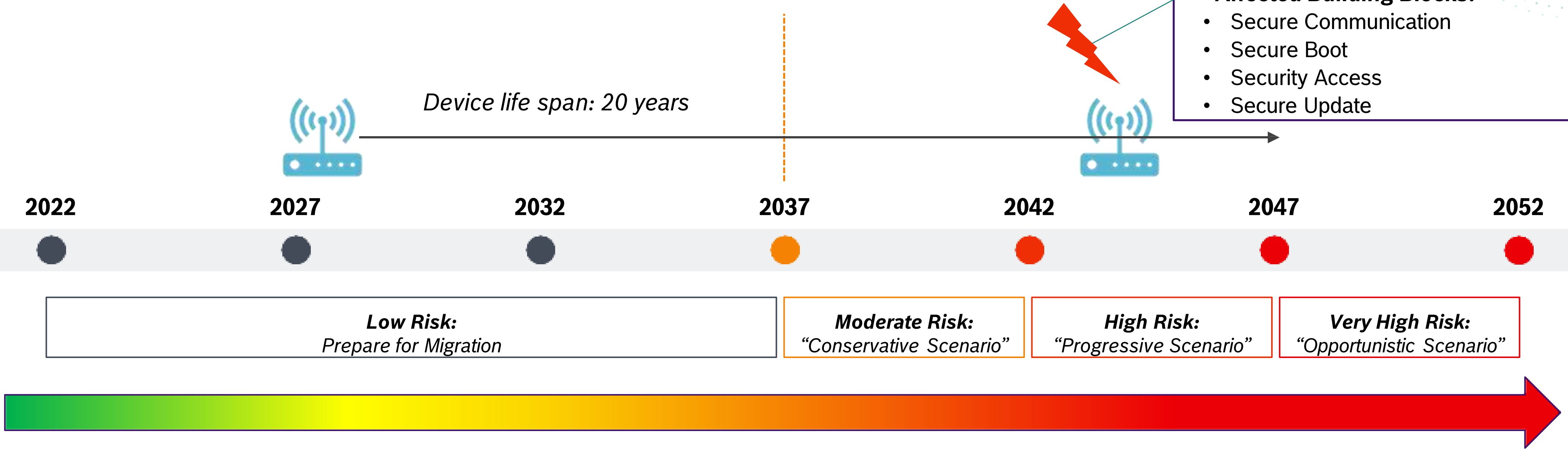
Post-Quantum Cryptography @ CR, Sebastian Paul (CR/APT5), Matthias Meier (CR/APT5) Paul Duplys (CR/ADI1.2) Philipp Mundhenk (CR/PJ-ICT) Frederic Stumpf (M/NET)

BOSCH

Quantum-Resilient Security Controls

Risk Assessment for Security Assets

- **Affected Products:**
  - Internet communication
  - (Connected) Devices
- **Affected Building Blocks:**
  - Secure Communication
  - Secure Boot
  - Security Access
  - Secure Update



Migration Challenges:

- PQC requires redesign of security building blocks
- Overcome resource constraints in devices ➔ HW vs. SW impl.
- Long lead times ➔ 10 years(!) in case of HW changes
- Identify suitable PQC schemes ➔ Select standards
- Distribution of SW updates often challenging

Public-key cryptography (RSA + ECC) broken with probability 50% – 83%[1]

[1] Mosca, M.; Piani, M. (2022): 2021 Quantum Threat Timeline Report. https://globalriskinstitute.org/publications/2021-quantum-threat-timeline-report/

BOSCH

Quantum-Resilient Security Controls

Why worry now?

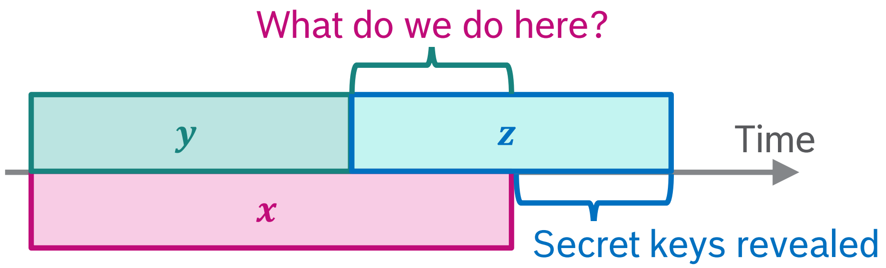
"By completing their transition before *December 31, 2030, stakeholders – particularly cryptographic module …"*

"We want people to take note of these requirements to plan and budget for the expected transition"

"a cryptographically relevant quantum computer will be available in the early 2030s; BSI believes that it is already urgently necessary to take appropriate measures to switch to quantum-safe scheme"

"For high-risk use cases, quantum-vulnerable public-key mechanisms shall not be used stand-alone after the end of 2030, analogously after the end of 2035 for medium-risk use cases"

- Time needed for a large enough quantum computer to become a reality?
  - **x years (~ 15 years from now)**
- Time needed to deploy a quantum safe solution?
  - **y years (~ 5-10 years)**
- Time for which the information needs to be secure?
  - **z years (~ 15 years)**
- **Theorem**: If $x < y + z$, then we need to worry now.



Mosca's Theorem

Do I need PQ Encryption?

For your general day-to-day product / project discussions on slack / internal chat?

For your general online transactions?

In between??

- Analysis required
- Till when do you need the confidentiality?

An extra-marital affair?

For strategic “HARD/GRAY” business decisions?

BOSCH

Do I need PQ Authentication?

For your general (online) logins?

- To your email / bank / org / etc.

In between??

- Analysis required
- Till when do you need the same authentication credentials?

For access of products in the field with long life?

- Cars
- Satellites
- Manufacturing plants
- Critical Infrastructure
- …

Boot

Update

Communication

…

Our QR Solutions

QR-Guide
PQC Migration Training & Advisory Services

Expert-led training and consulting built on a strong post-quantum cryptography research foundation, offering proven best practices and technical disclosure of real-world PQC prototypes.

QR-Inspect
Quantum-Readiness Infrastructure Evaluation

A unified platform offering comprehensive crypto discovery and assessment across applications, networks, and databases

QR-Bridge
Cryptographic Overlay Migration Solution

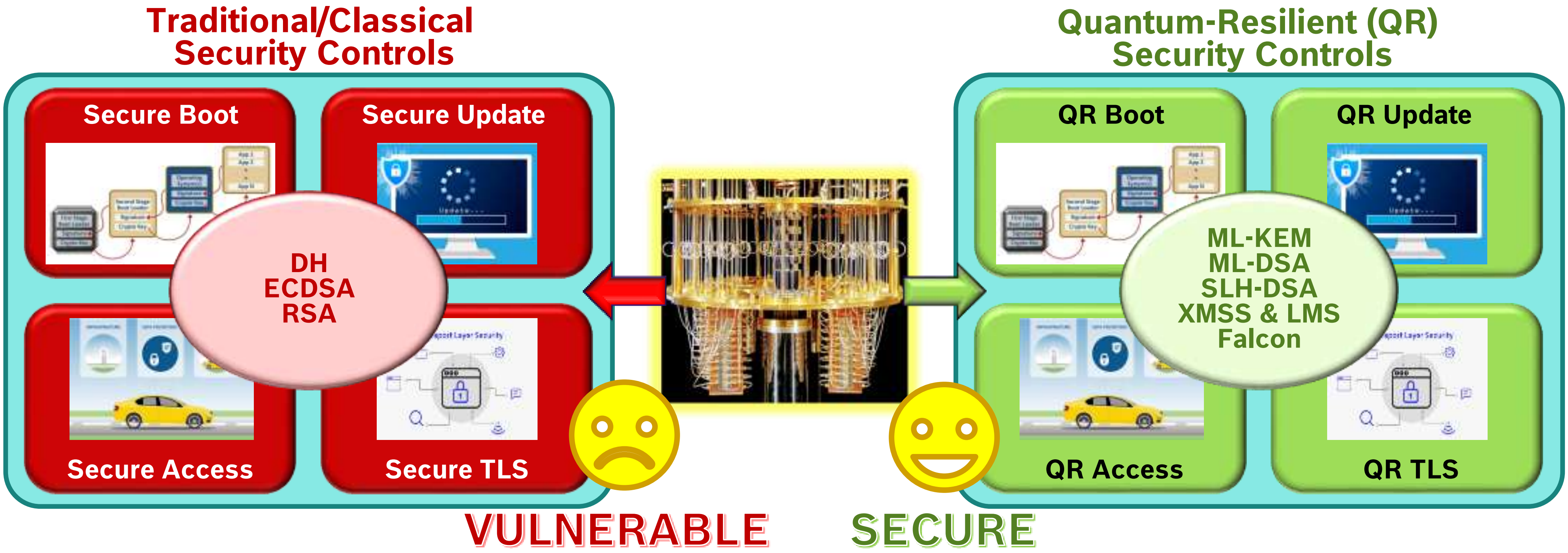
A plug-and-play overlay enabling post-quantum cryptography migration with full backward compatibility, requiring no modifications to existing codebases.

QR-Shield
High-Performance PQC Hardware & Software Designs

Delivers high-performance, quantum-secure IP cores that are hardened against physical attacks, offering best-in-class protection for embedded systems and secure hardware platforms.

BOSCH

Our Assets



BOSCH

Our offerings

Crypto Discovery > Transient Migration > Core Migration

Features	Features
• Real-Time Network Analysis • Active Network Vulnerability Analysis • Filesystem Cryptography Analysis • Application Cryptography Analysis • Data Sensitivity Tracking Mechanisms • Privacy Preserving Features	• Support for NIST Standardized PQC Algorithms • Efficient Hardware Implementations • Enterprise Software Implementations (Infrastructure, Cloud) • Embedded Software Implementations • Physical Attack Resistance • Formally Verified Implementations

Benchmarking

Security Controls	Platforms/controllers	Algorithms	Hybrid PoCs purely software AND/OR exploit whatever HSMs are available. e.g.,
Secure Boot	X86	XMSS_SHA2_10_256,	For classical algorithms, we use HSM whenever available.
Secure Access	ArmV7	XMSS_SHA2_10_512,	For XMSS / Sphincs+, we use hash accelerators whenever available.
Secure Update	Aarch64 (ArmV8)	Falcon_1, Falcon_5,	On FPGA, we use our optimized NTT implementation of Dilithium/Kyber.
Secure TLS	TC37xx > TC38xx > TC39xx	DIL_2, DIL_3, DIL_5,	
	STM SR6x	SPX_MODE_1, SPX_MODE_5,	
	Agilex7 FPGA	KYBER_1, KYBER_3.	

Benchmarking: QR-Access

Category	Signature Scheme	Size (bytes)	Time (ms)
Non PQC	ECDSA	Public key : 64 Private Key : 32 Signature : 64	~800
	ECDSA with HW ECC accelerator		~20
PQC	XMSS with SHA-256	Public key: 64 Private key: 132 Signature: 2,532 (incl. 32B of Msg)	~70
	DILITHIUM (SHAKE128)	Public Key: 1312 Private Key: 2528 Signature: 2,452 (incl. 32B of Msg)	~100

Controller: IFX 3 40nm (TC37x) with HSM activated

Benchmarking

Secure Boot			
Library	QR Algorithm (Digital Signature)	Total Signature Time (ms)	Total Verification Time (ms)
pq-wolfSSL*	Dilithium	17.764	24.06

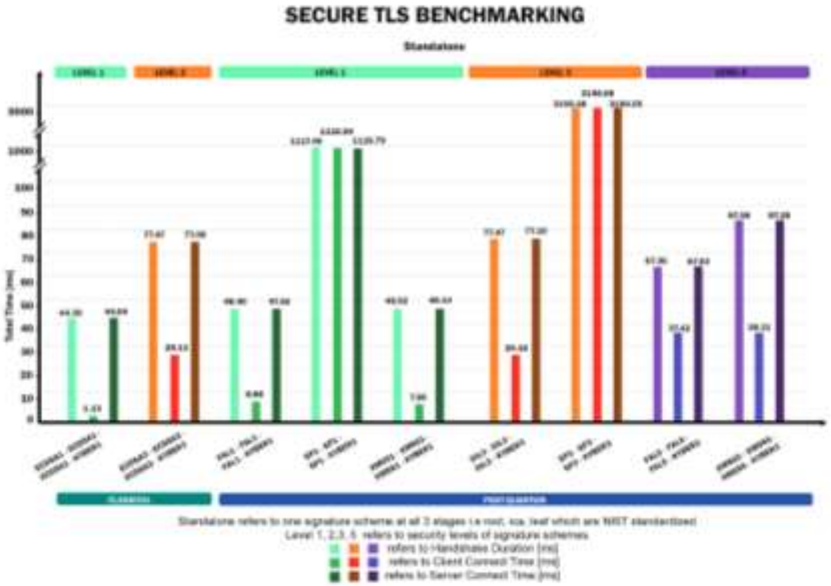
Secure Update						
Library	QR Algorithm (KEM)	QR Algorithm (Digital Signature)	KEM Time (ms)	DEM Time (ms)	Sign. Gen. Time (ms)	Sign. Verification Time (ms)
pq-wolfSSL*	Kyber	Dilithium	3.58	3.41	242.02	99.77

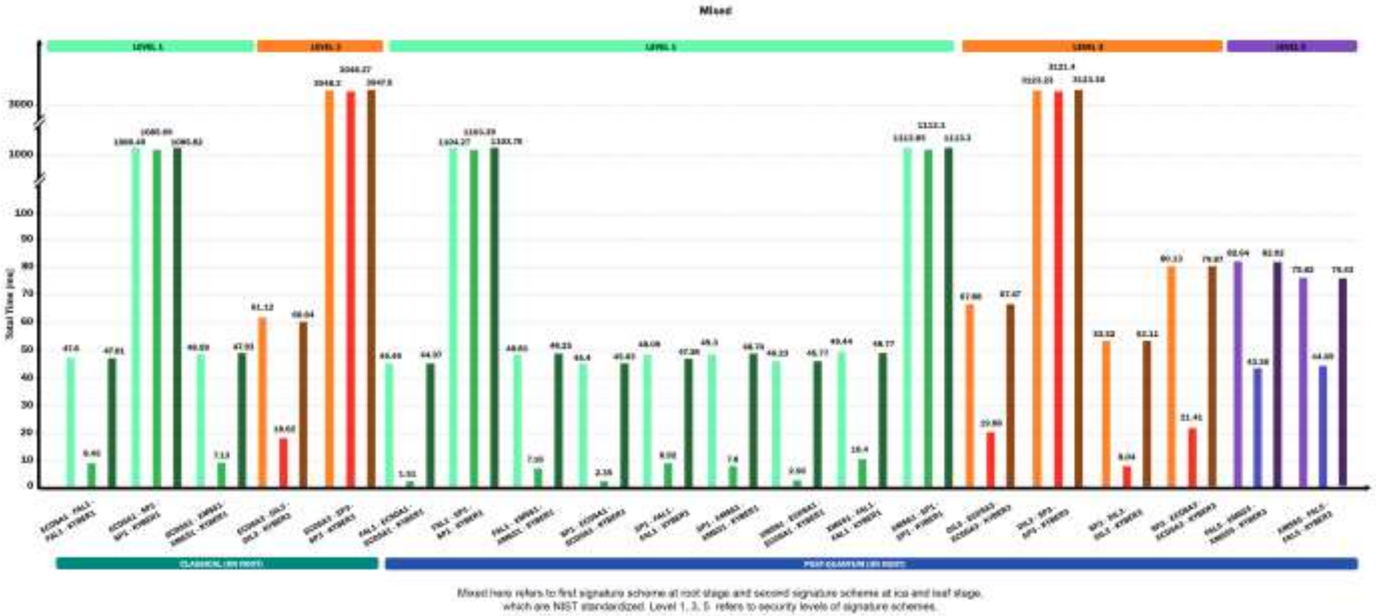
Secure TLS				
Library	QR Algorithm (KEM)	QR Algorithm (Digital Signature)	Server Time (ms)	Client Time (ms)
pq-wolfSSL	Kyber	Dilithium	48.14	7.66

BOSCH

Quantum-Resilient Security Controls

Benchmarking





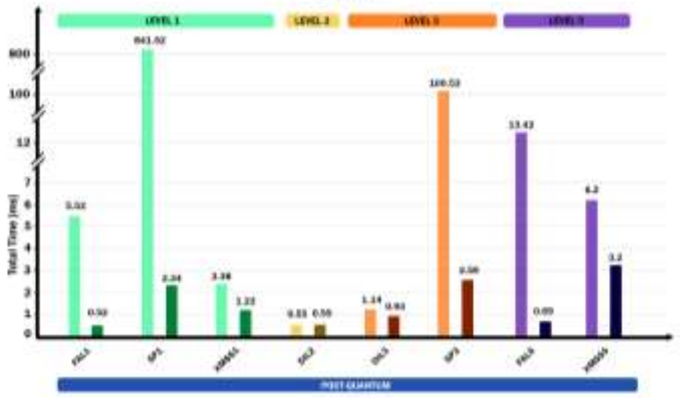
BOSCH

Quantum-Resilient Security Controls

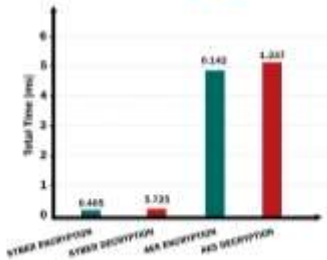
Benchmarking

SECURE UPDATE BENCHMARKING

Standalone



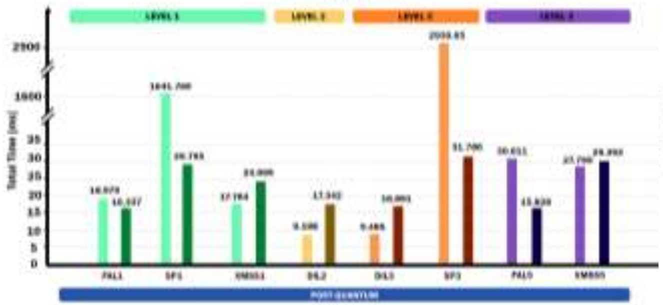
Standalone refers to one signature scheme at all 3 stages i.e root, ica, leaf which are NIST standardized.
Level 1, 2,3, 5 refers to security levels of signature schemes.
Light Shade represents Signature Generation Time [ms]
Dark Shade represents Signature Verification Time [ms]



This graph refers the respective encryption and decryption times during the secure update process.

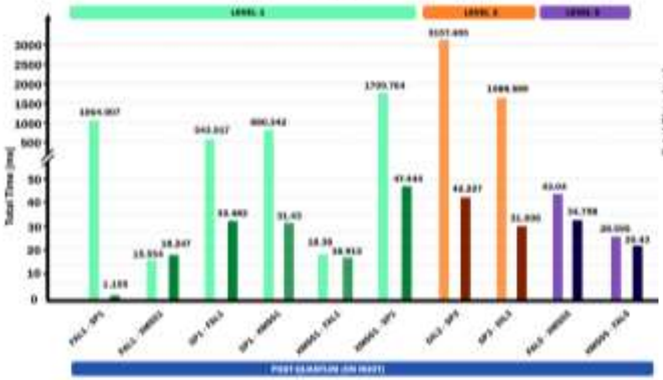
SECURE BOOT BENCHMARKING

Standalone



Standalone refers to one signature scheme at all 3 stages i.e root, ica, leaf which are NIST standardized.
Level 1, 2,3, 5 refers to security levels of signature schemes.
Light Shade represents Total Signing Time [ms] = RootSig + ICASign + ServerSign
Dark Shade represents Total Verification Time [ms] = RootVer + ICA ver + ServerVer

Mixed



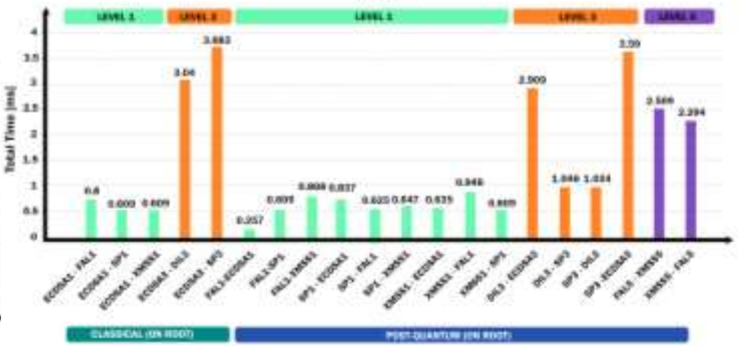
Mixed here refers to first signature scheme at root stage and second signature scheme at ica and leaf stage, which are NIST standardized. Level 1, 3, 5 refers to security levels of signature schemes.

SECURE ACCESS BENCHMARKING

Standalone

Standalone refers to one signature scheme at all 3 stages i.e root, ica, leaf which are NIST standardized.
Level 1, 2,3, 5 refers to security levels of signature schemes.
Total Certificate Verification Time = Root to ICA [ms] + ICA to Server [ms]

Mixed



Mixed here refers to first signature scheme at root stage and second signature scheme at ica and leaf stage, which are NIST standardized. Level 1, 3, 5 refers to security levels of signature schemes.

BOSCH

Thank You

Dr. Vishal Saraswat
Bosch Cybersecurity University
Vishal.Saraswat@bosch.com