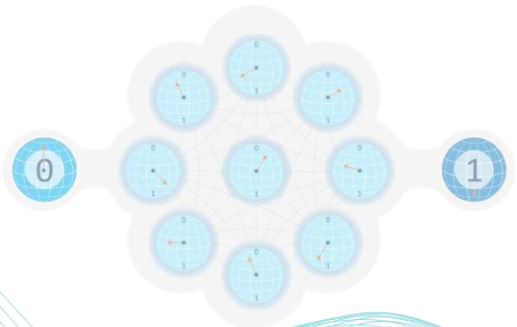
Future-Proofing Security: Embracing Crypto Agility and Post-Quantum Cryptography



Dr. Vishal Saraswat
Bosch Cybersecurity University
Bosch Global Software Technologies
Vishal.Saraswat@bosch.com

Dr. Vishal Saraswat

Personal

Role : Program Manager & 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)**
  - Security Consulting (TARA, Security Concepts, Crypto SME)
  - Security Reviewing (PROSO)
  - Innovation (PQC, Crypto V&V, Reusable Repository)
  - Competency Development (Bosch Cybersecurity University)
  - Adjunct Faculty – NIIT University: Faculty of **OT & ICS Security**
- **IIT Jammu, IIT Hyderabad, IIT Palakkad, ISI Kolkata, Univ. Hyderabad, SPJain, 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

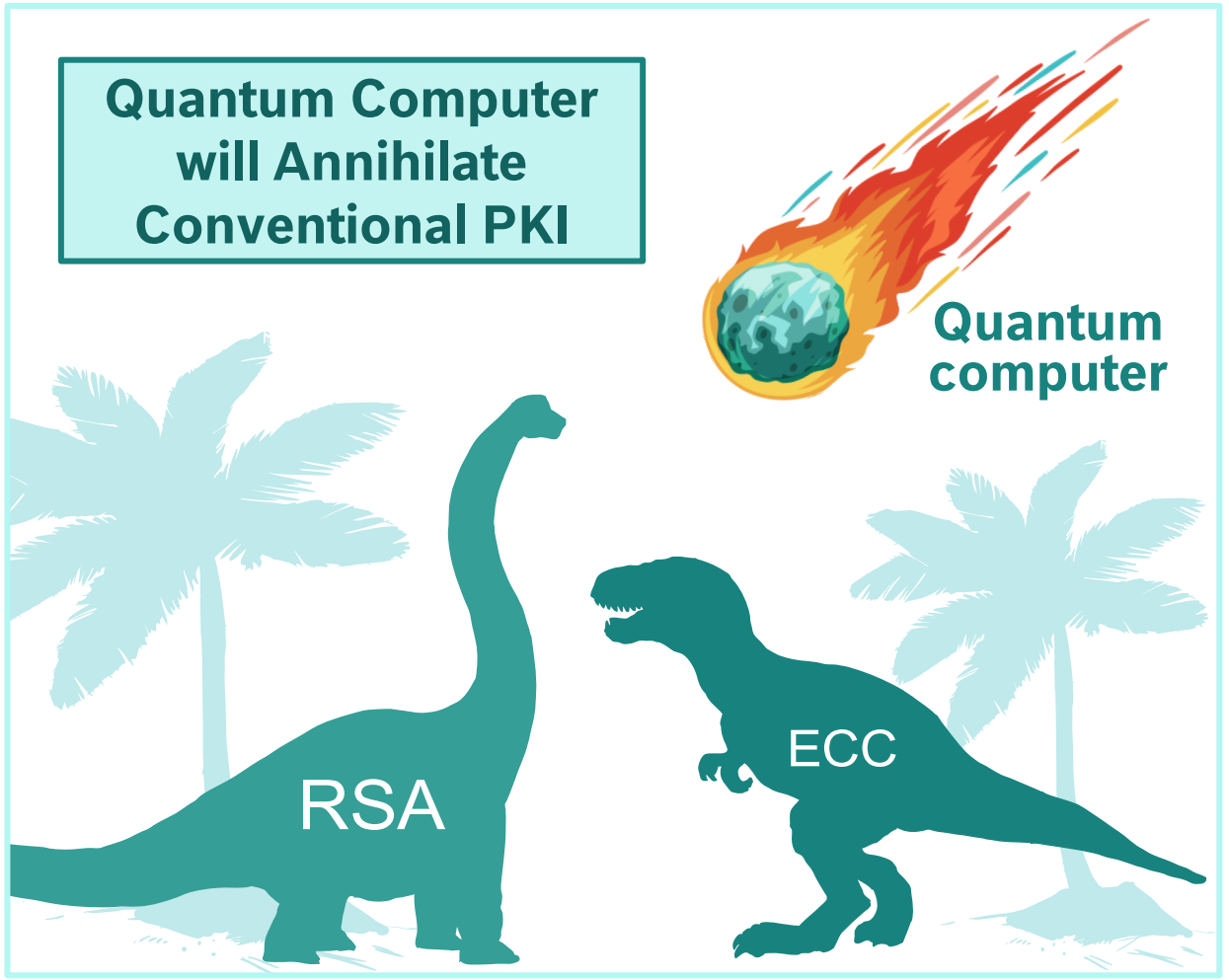
12+ years leadership experience
- Crypto consulting
- Competency development for academia and industry
  - M.Tech: Information Security, IIT Hyderabad
  - M.Tech: Cyber Security, CU Hyderabad
  - M.Tech: Cyber Security, SPJain
  - P.G.Diploma: Automotive Cybersecurity, BITS Pilani
- Establishing and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

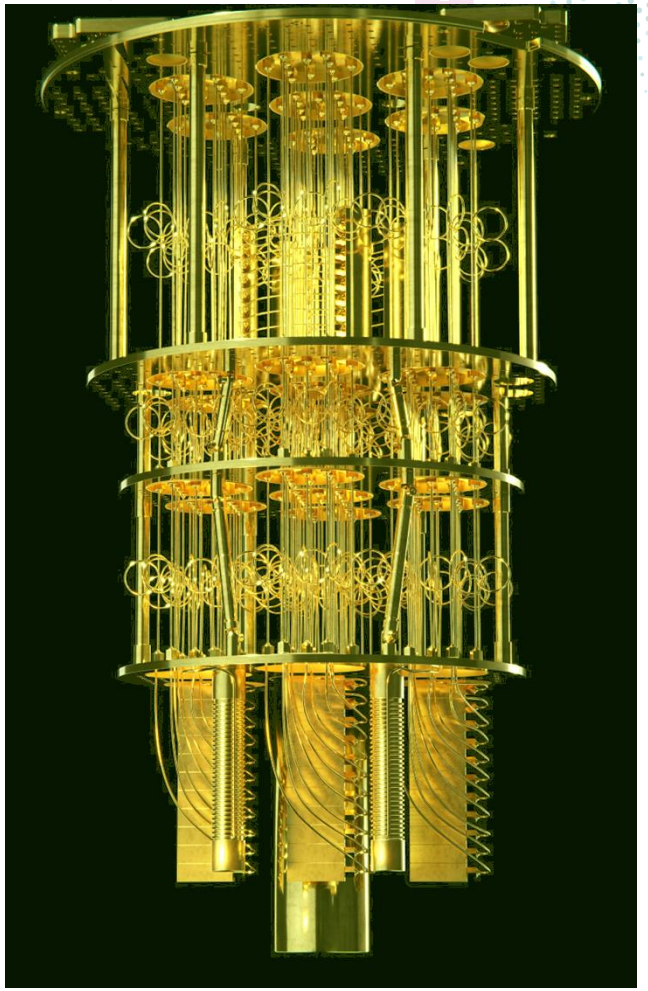
Research Interests

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

BOSCH

Quantum-Resilient Security Controls



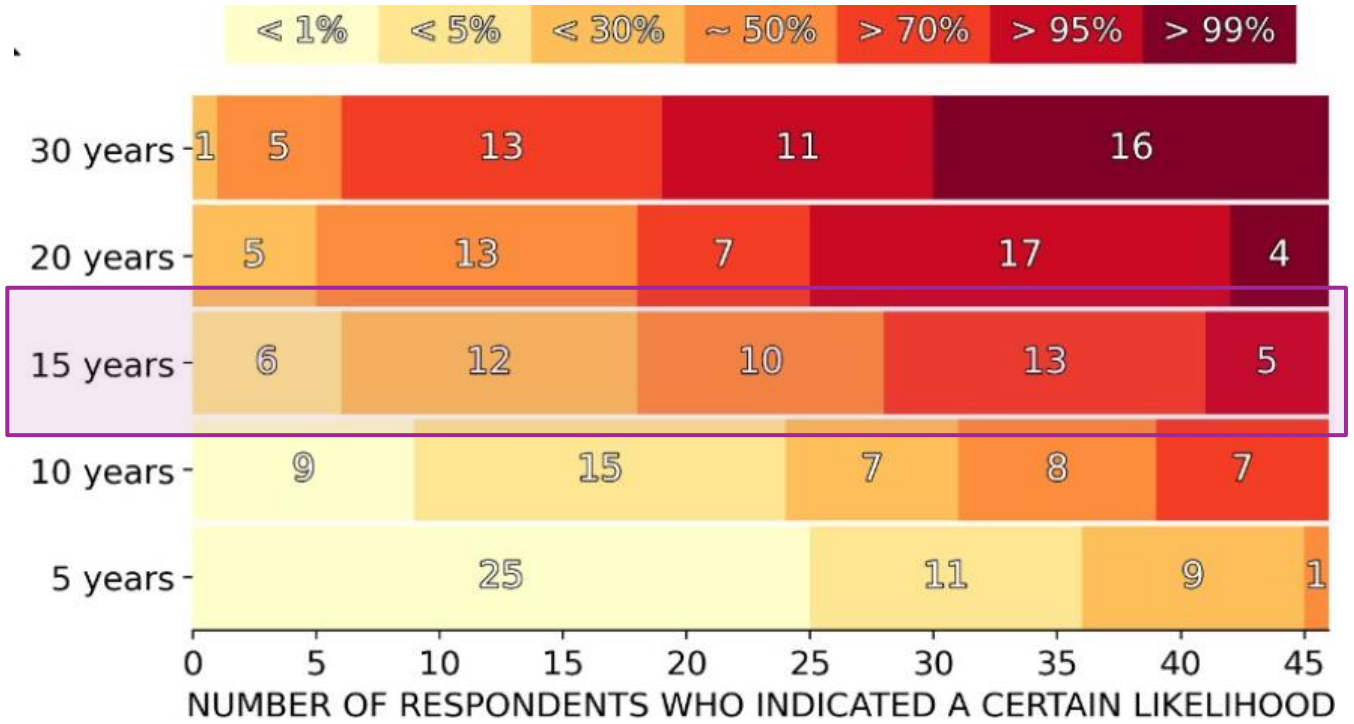


BOSCH

Quantum Threat Timeline

Quantum hype bubble?

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

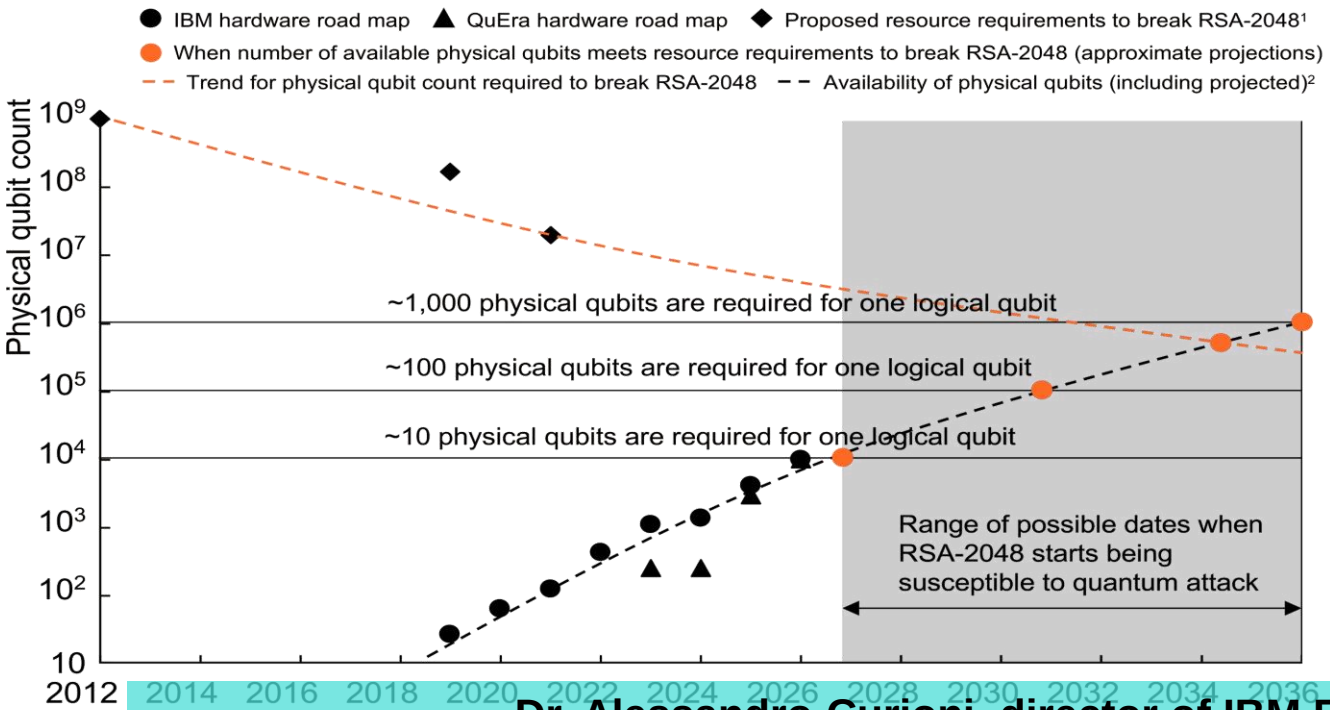


Mosca, M.; Piani, M. (2022): 2021 Quantum Threat Timeline Report.
https://globalriskinstitute.org/publications/2021-quantum-threat-timeline-report/

Timelines for susceptibility to quantum attack depend on qubit hardware development and implementation.

Illustrative

Quantum resource availability and requirements by year, 2012–2036



The date by which commonly used cryptosystems (eg, RSA, ECC) are susceptible to quantum attack depends on the availability of quantum resources (eg, number of physical qubits) and qubit implementations (eg, number of physical qubits needed to operate a logical qubit).[3]

To break RSA-2048 in reasonable time (~days), schemes requiring ~10^3–10^4 logical qubits have been proposed; ~10^3 physical qubits are required for one logical qubit, though more recently announced techniques reduce the number of physical qubits per logical qubit to 10–100, which is an active area of research by companies such as Alice & Bob, AWS, IBM, and QuEra.

Decrypting RSA-2048 would then require at minimum ~10^4 and up to ~10^7 physical qubit,s which provide the timeline range based on the road maps for availability of physical qubits by major QC players.

Dr. Alessandro Curioni, director of IBM Research at Zurich:
"We do know that a quantum computing machine, probably before the end of the decade, will be powerful enough to break the standard cryptographic technology that is used today."

[1]From *Quantum*: https://doi.org/10.22331/q-2021-04-15-433
[2]Historical for pre-year
[3]Not considering

Source: Alice & Bob; Google; IBM; Microsoft; QuEra; McKinsey analysis

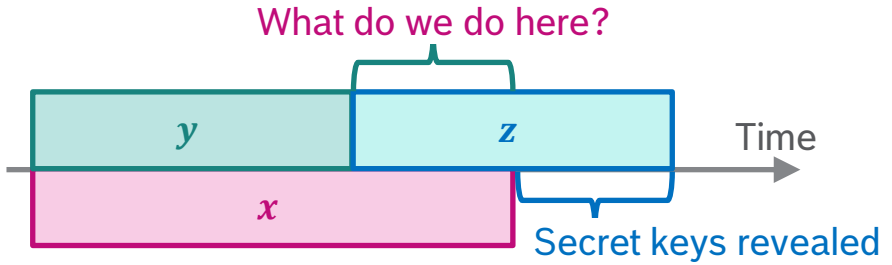
McKinsey & Company 88

Why worry now?

IBM Quantum Processors

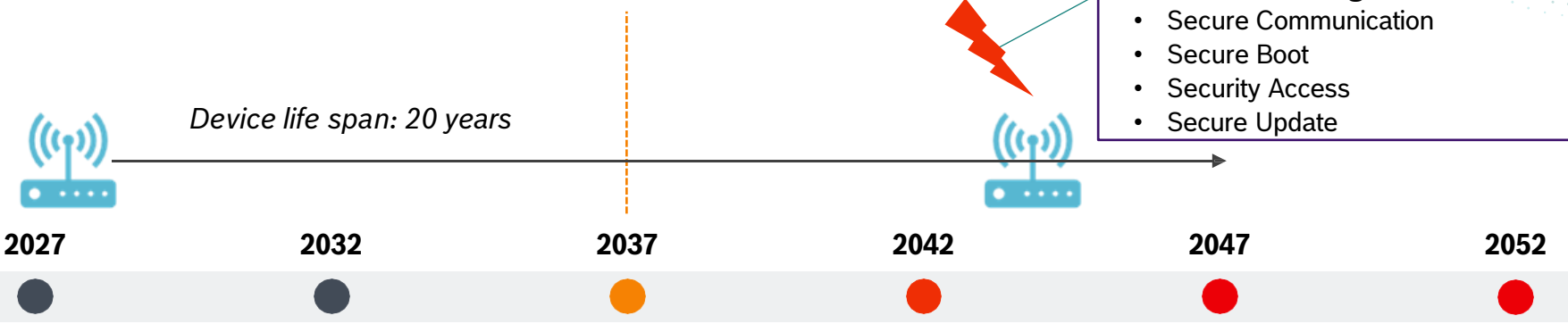
Classical	Factoring algorithm (RSA)			EC discrete logarithm (ECC)		
$Cycles$	n	$\approx \#\ qubits$	$Cycles$	n	$\approx \#\ qubits$	$Cycles$
$C \cdot 10^{17}$	2048	4096	$34 \cdot 10^9$	224	1300	$4.0 \cdot 10^9$
$C \cdot 10^{22}$	3072	6144	$120 \cdot 10^9$	256	1500	$6.0 \cdot 10^9$
$C \cdot 10^{60}$	15360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

- 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.



Risk Assessment for Security Assets

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



Low Risk: *Prepare for Migration*	***Moderate Risk:*** *"Conservative Scenario"*	***High Risk:*** *"Progressive Scenario"*	***Very High Risk:*** *"Opportunistic Scenario"*

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/

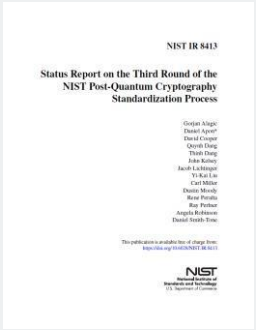
BOSCH

PQC Standardization and Recommendations

- FIPS 203: ML-KEM
- FIPS 204: ML-DSA
- FIPS 205: SH-DSA
- Round 4 KEMs: BIKE, Classic McEliece, HQC, and SIKE
- Additional Digital Signature Schemes

PQC Standardization and Recommendations

- FIPS 203: ML-KEM
- FIPS 204: ML-DSA
- FIPS 205: SH-DSA
- Round 4 KEMs: BIKE, Classic McEliece, HQC, and SIKE
- Additional Digital Signature Schemes



NIST

Selected four algorithms to become first **PQC standards**

"NIST hopes for **rapid adoption** of first standardized algorithms."

"The **transition** will undoubtedly have **many complexities**, and there will be challenges for some use cases, such as IoT devices."

NIST (2022): Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process.

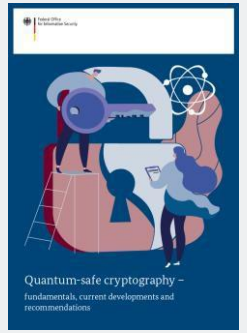
NSA

Recommended Timeline:

"Software and firmware signing: **begin transition immediately**"

"Constrained devices: support and prefer **PQC by 2030**."

NSA (2022): Announcing the Commercial National Security Algorithm Suite 2.0.

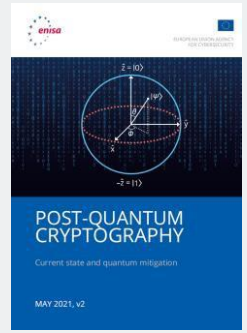


BSI

"The question of "if" or "when" there will be quantum computers is no longer in the foreground.

Post-Quantum Cryptography will become the standard in the long term."

BSI (2022): Quantum-safe cryptography – fundamentals, current developments and recommendations.



EU

"Given recent developments in the Quantum Computing race among industries and nation states, it seems prudent for Europe to **start considering mitigation strategies now**."

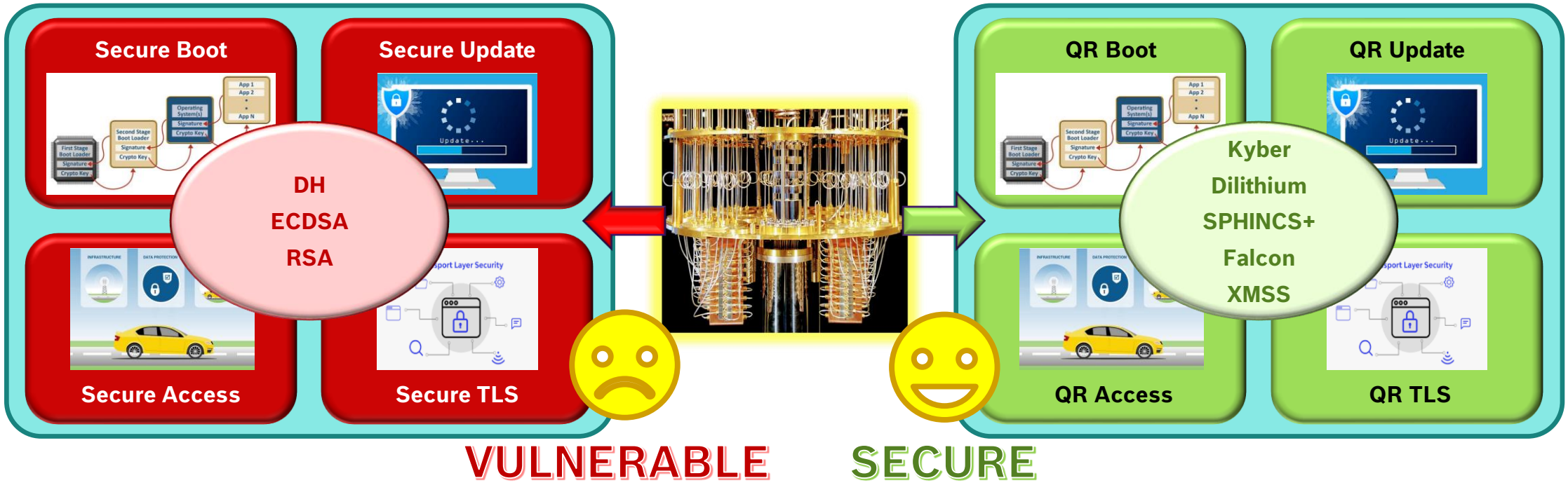
ENISA (2021): Post-Quantum Cryptography: Current state and quantum mitigation.

BOSCH

Our Assets

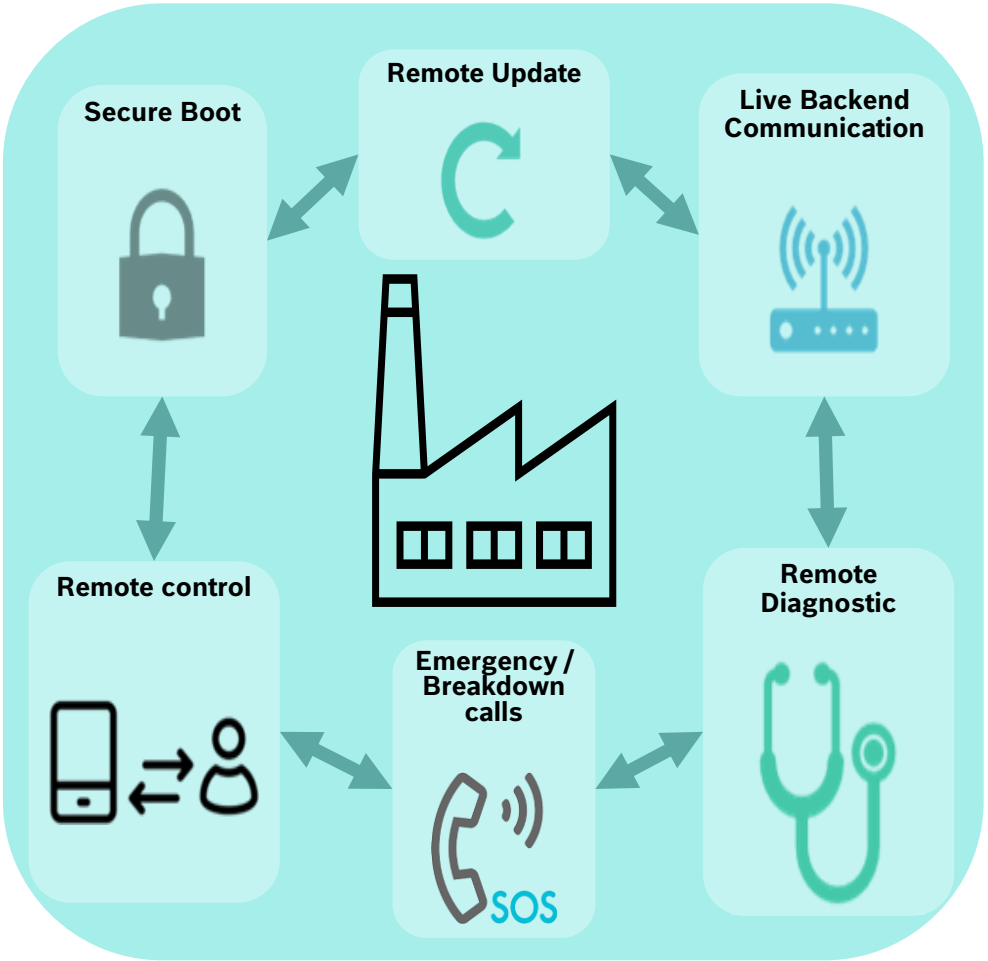
Traditional/Classical Security Controls

Quantum-Resilient (QR) Security Controls



BOSCH

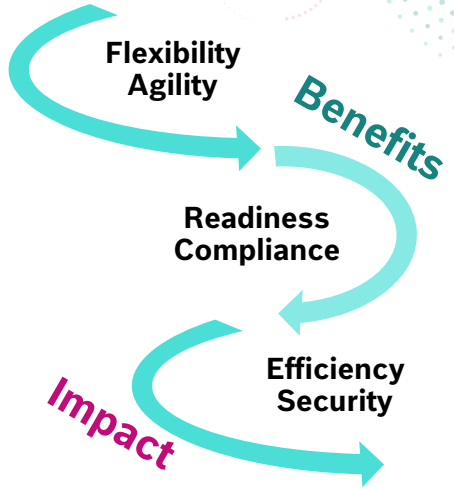
Quantum-Resilient Security Controls



- QR-Boot & QR-Access & QR-OTA & QR-TLS
- Hybrid Certificates

Proof of Concepts
- SW & HW

IP
- Multiple Patent Filings



Efficiency: Much faster than RSA and ECDSA (certain usecases)

Flexibility: Trade-offs possible without affecting security

Security: Tighter bounds; stronger guarantees; weaker assumptions

Crypto Agility: To maintain the current levels of security through lifecycle

Compliance: CNSA? FIPS 140-4? ...

Thank You

Dr. Vishal Saraswat
Bosch Cybersecurity University
Bosch Global Software Technologies
Vishal.Saraswat@bosch.com