Preparing for Tomorrow: Post-Quantum Cryptography and Crypto Agility in Automotive Security

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

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

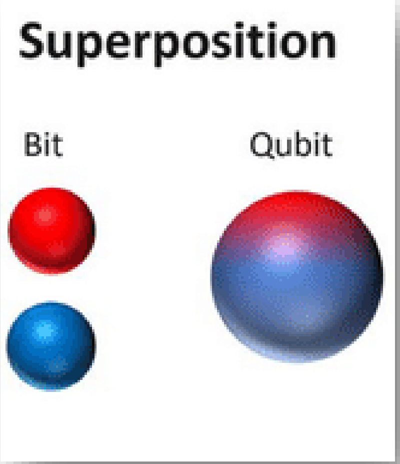
Research Expertise

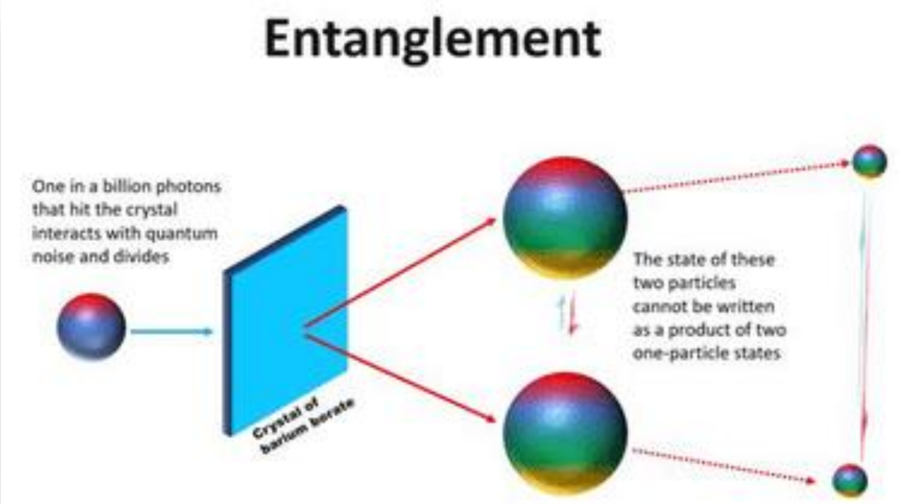
- Post-quantum crypto
- CPS, OT, IIoT, & CI security
- Anonymity and privacy in communication protocols
- Searchable encryption for the cloud-based services
- Lightweight cryptography for IoT devices
- Blockchain security
- Hardware security
- Active and passive cryptanalysis

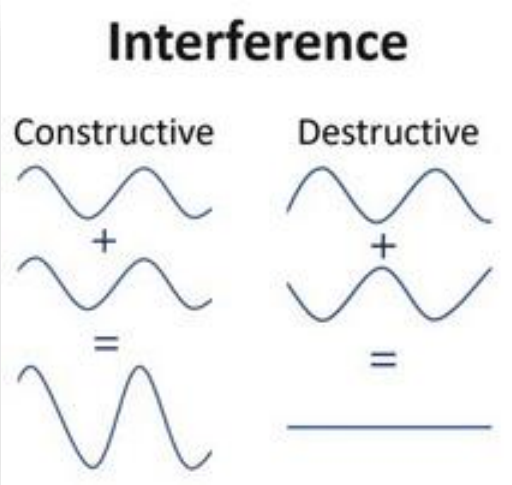
BOSCH

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.







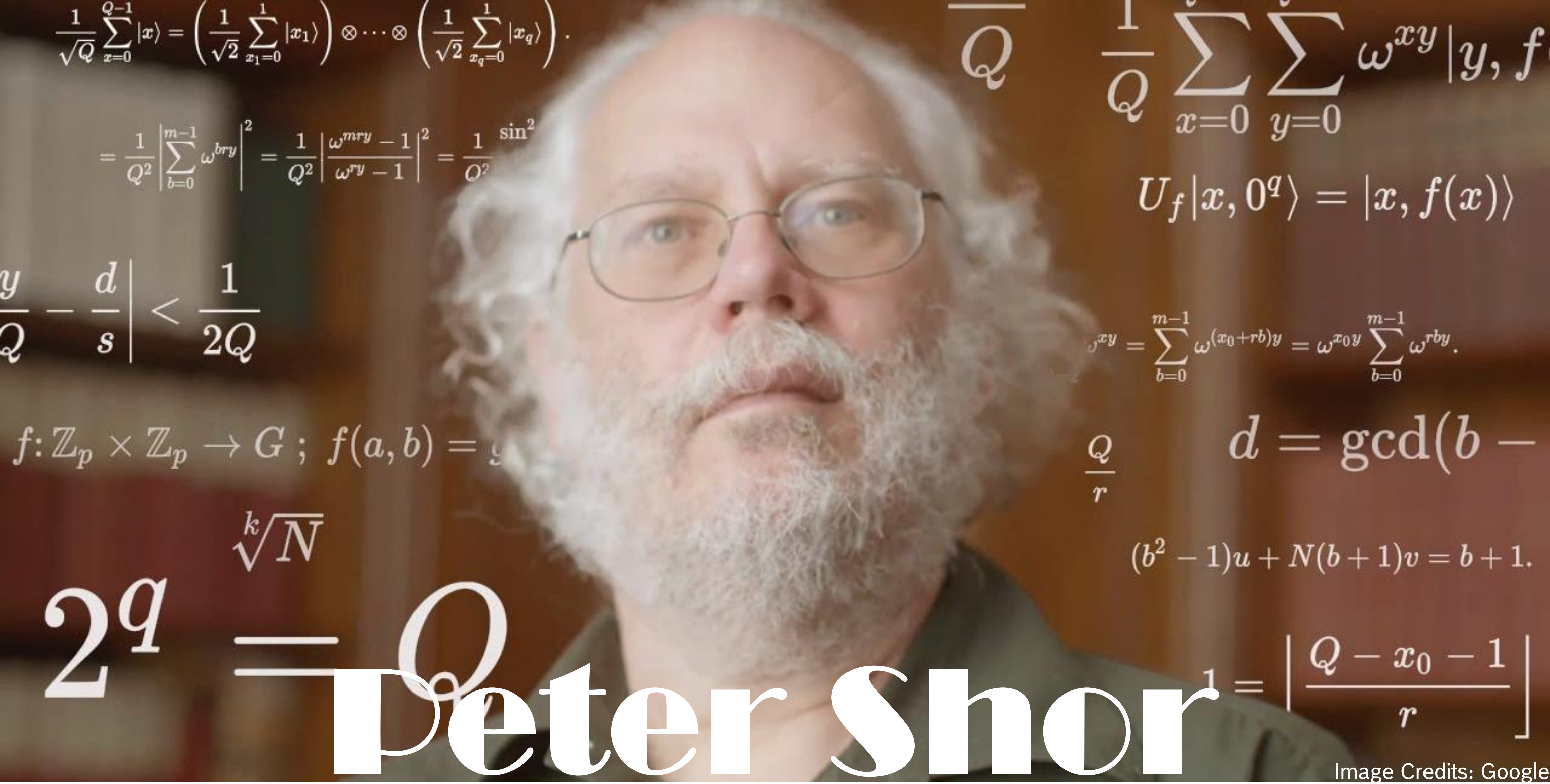
Benefits

- 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
- …

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

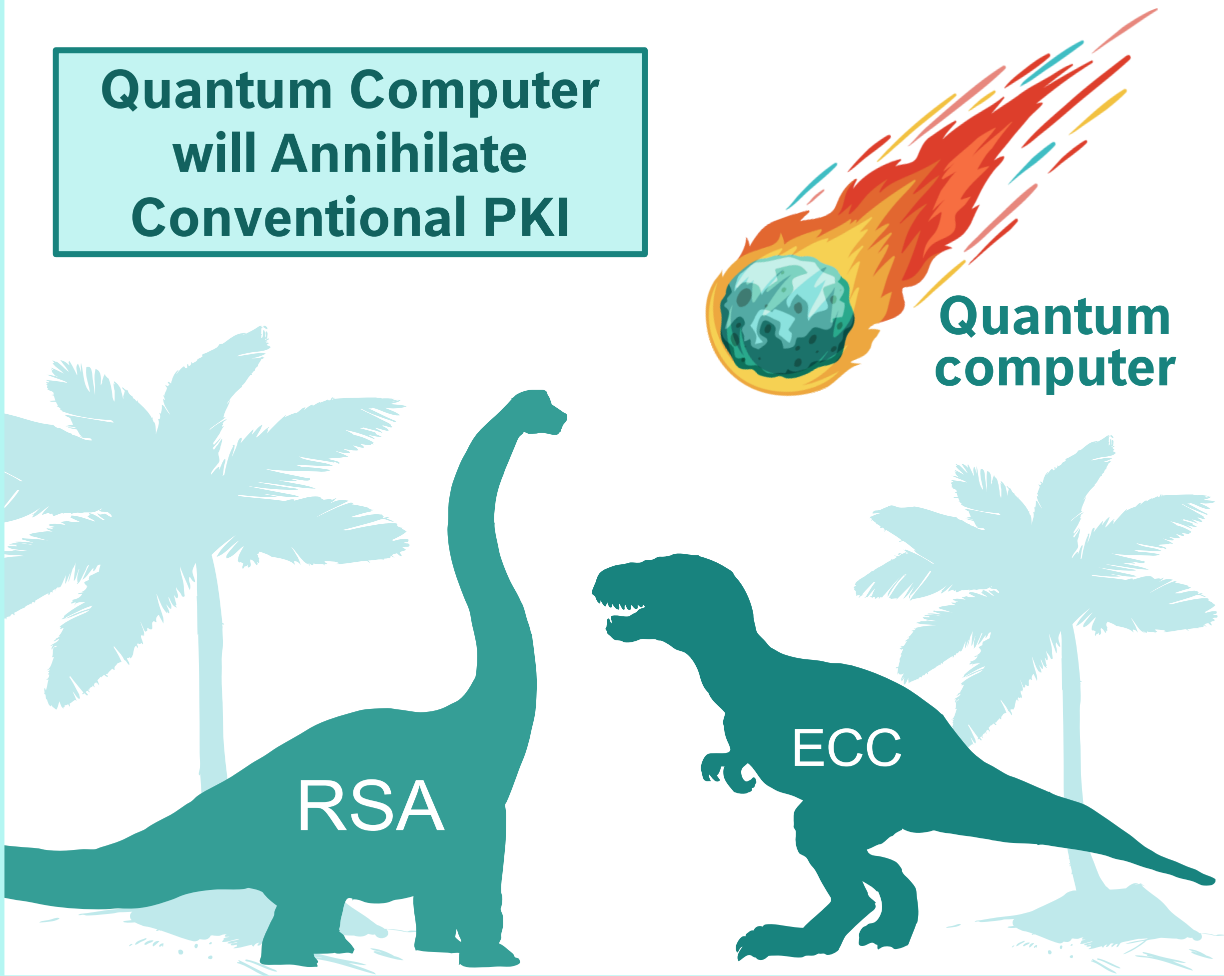


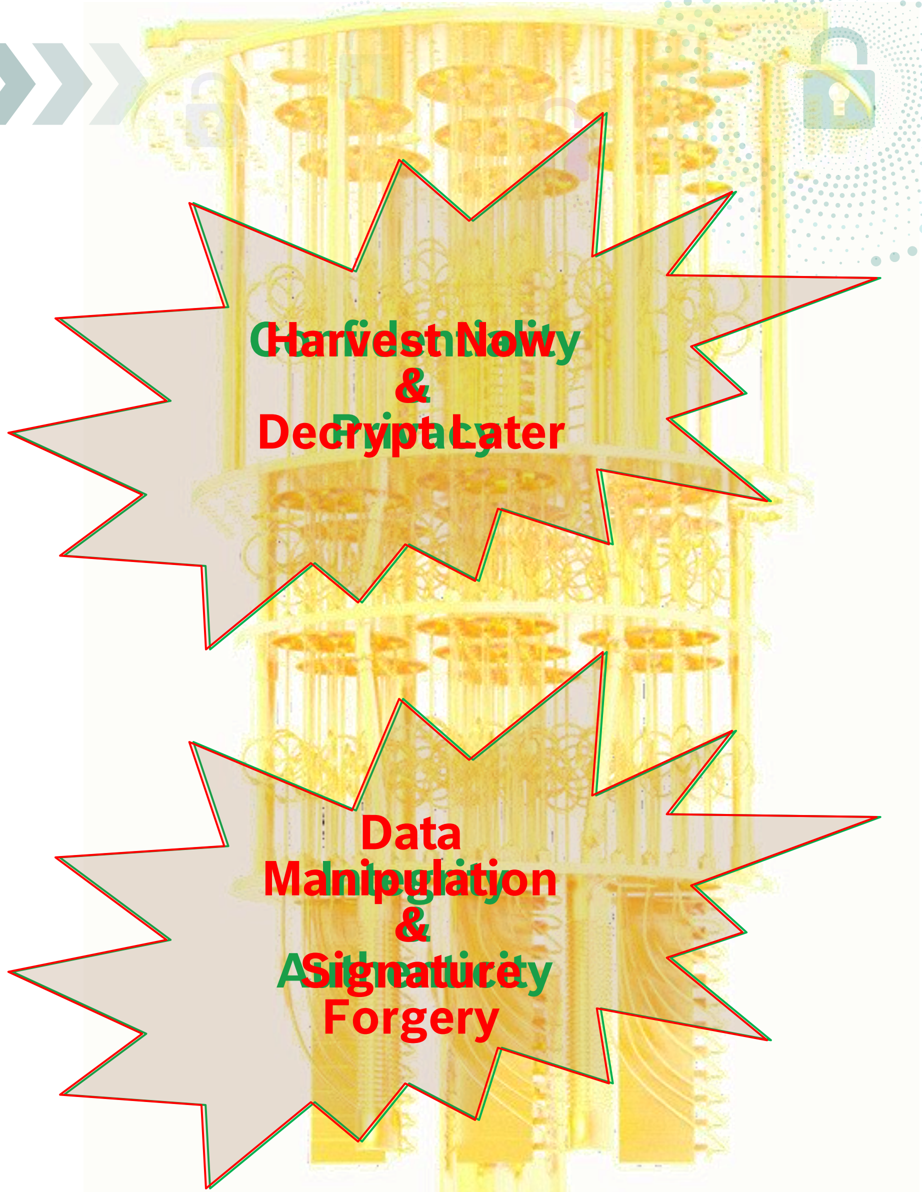
Peter Shor

Image Credits: Google

1994: “Algorithms for quantum computation: Discrete logarithms and factoring”

Quantum Computer will Annihilate Conventional PKI

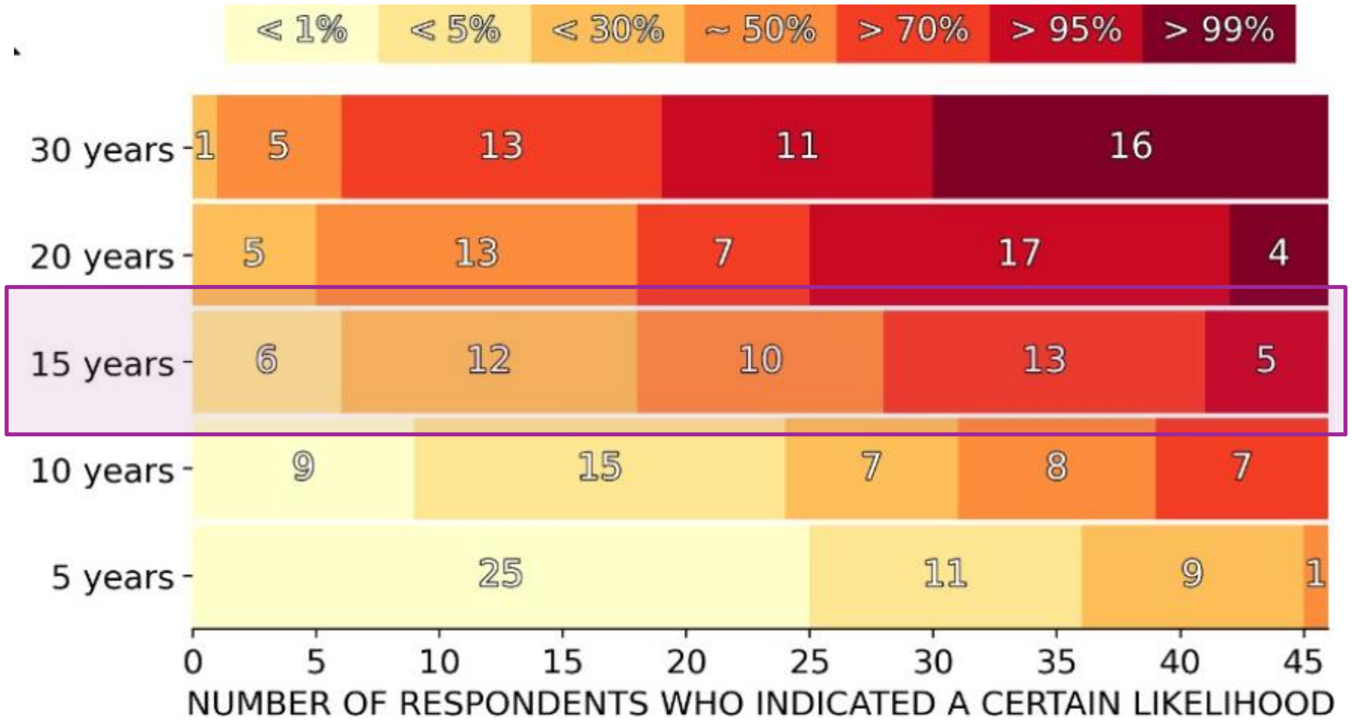




Quantum Threat Timeline

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**



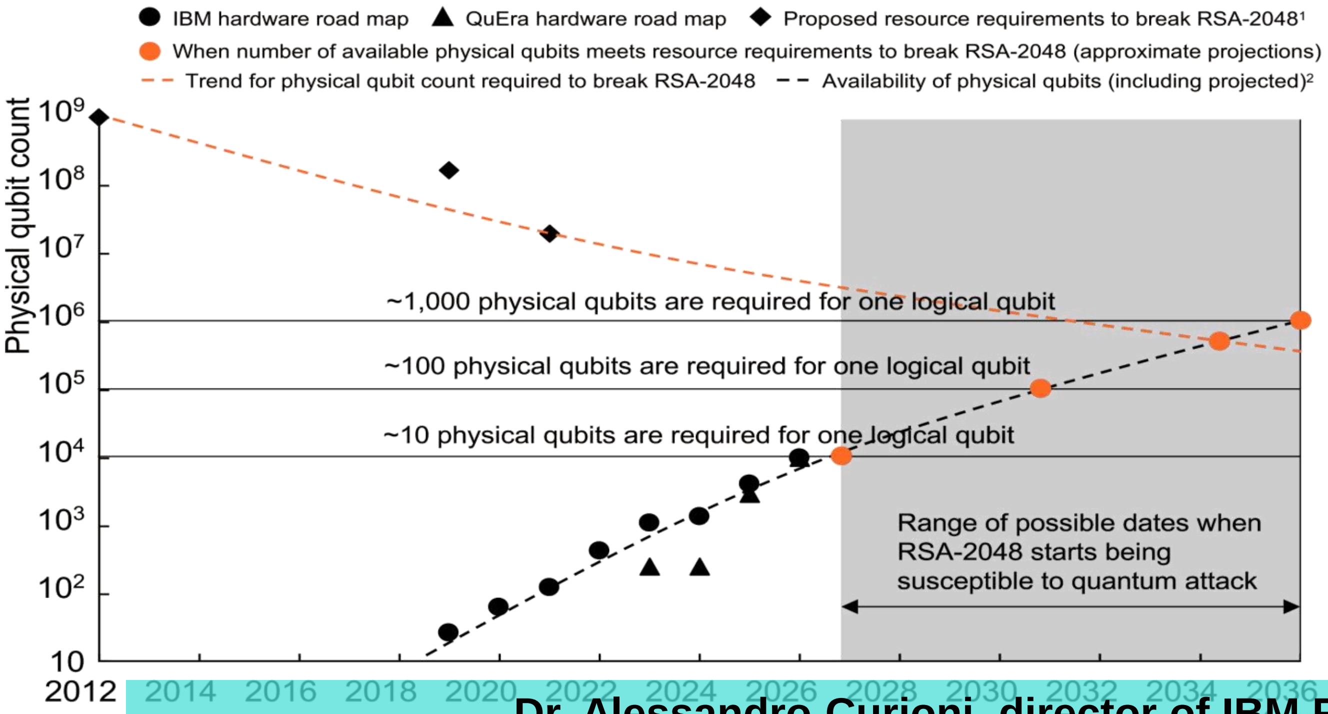
Mosca, M.; Piani, M. (2022): 2021 Quantum Threat Timeline Report.
https://globalriskinstitute.org/publications/2021-quantum-threat-timeline-report/

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)

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."

¹From Quantum: https://doi.org/10.22331/q-2021-04-15-433.
²Historical for pre-year ...
³Not considering harvest now, decrypt later attacks that have an earlier time horizon but actual decryption date.

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

McKinsey & Company 88

BOSCH

Why worry now?

IBM Quantum Processors

2021
Eagle
- 127 qubits
- Error Rate: 1%

2022
Osprey
- 433 qubits
- Qiskit

2023
Condor
- 1121 qubits
- Q. System Two

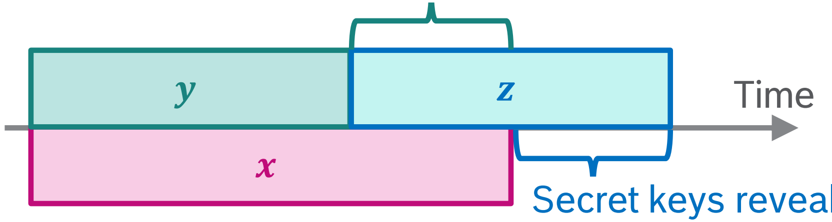
2024
Flamingo
- 1386 qubits

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	$50 \cdot 10^{9}$

- 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.



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.

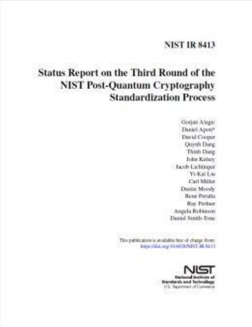
- Post-Quantum Cryptosystems
  - are secure against both quantum and classical computers,
  - and can interoperate with existing communications protocols ar net

- 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)

Post Quantum Crypto
is NOT
Quantum Crypto

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.

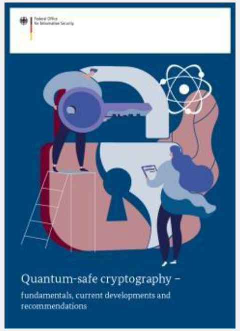
NSA

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.

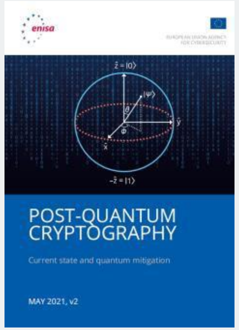


BSI

"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.

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

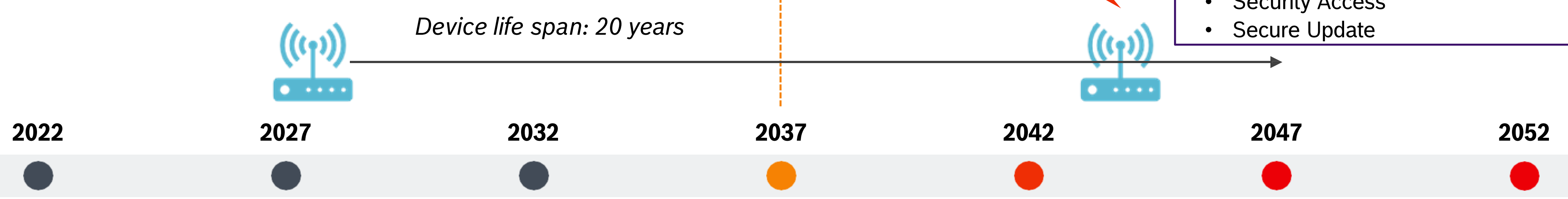
Communication

…

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



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/

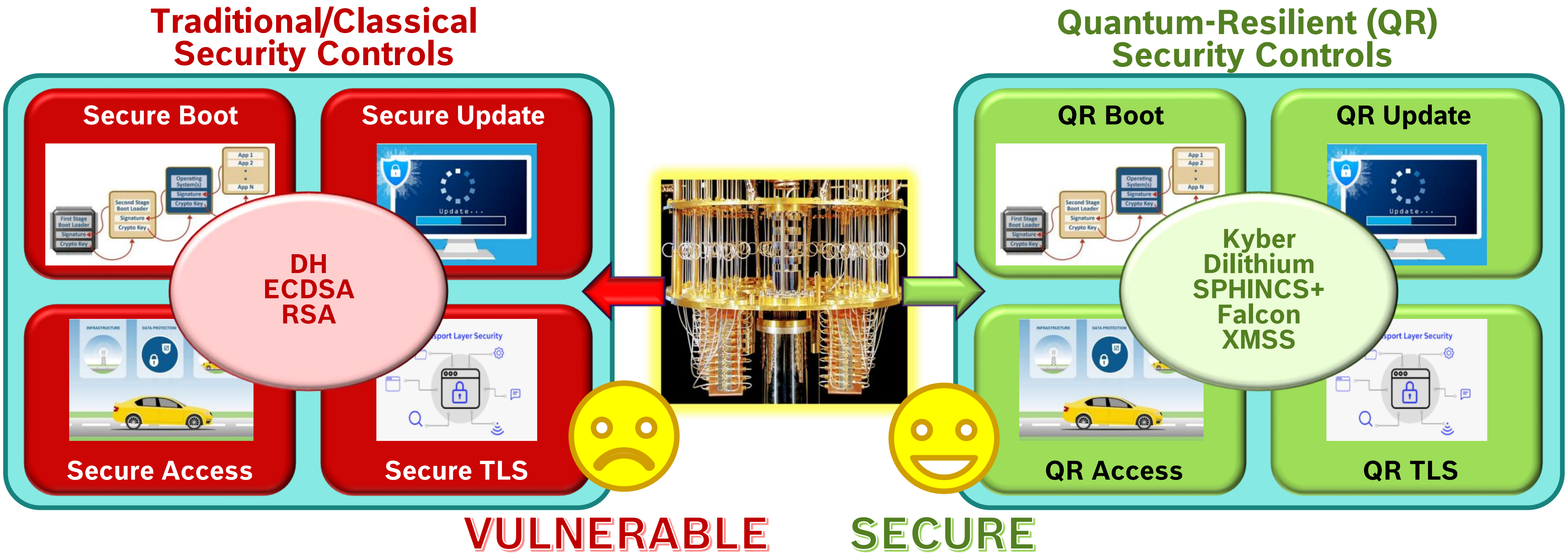
Post-Quantum Cryptography @ CR, Sebastian Paul (CR/APT5), Matthias Meier (CR/APT5) Paul Duplys (CR/ADI1.2) Philipp Mundhenk (CR/PJ-ICT) Frederic Stumpf (M/NET)

BOSCH

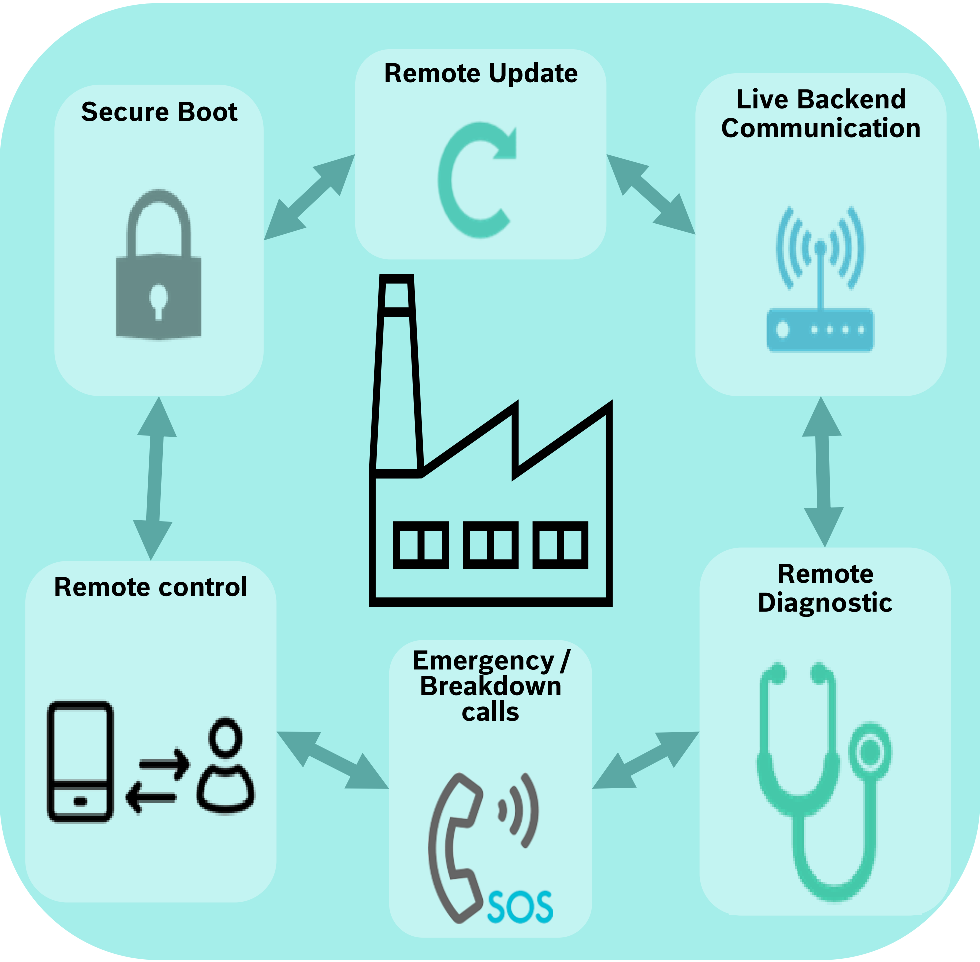
PQC Architecture and Solution Deployment

CRYPTO DISCOVERY → TARA	TRANSIENT MIGRATION	CORE MIGRATION	SECURITY MANAGEMENT
QVision	**QTunnel**	**QCore**	**QAlly**
Crypto Inventory Management Platform	Overlay Solution	PQC HW/SW Designs	Training and Consulting on PQC Migration
Assess Quantum Readiness USP: Comprehensive Discovery scanning Application, Network, Database	Siloed Migration with No-Code Change USP: Plug and Play with Backwards Compatibility	Best-in-class IPs USP: High Performance, Protected Against Physical Attacks	Best Practices in Cryptography USP: Strong PQC Research Background, Technology Disclosure of PQC Prototypes

Our Assets


Traditional/Classical Security Controls
Secure Boot
Secure Update
Secure Access
Secure TLS
DH
ECDSA
RSA
VULNERABLE
Quantum-Resilient (QR) Security Controls
QR Boot
QR Update
QR Access
QR TLS
Kyber
Dilithium
SPHINCS+
Falcon
XMSS
SECURE

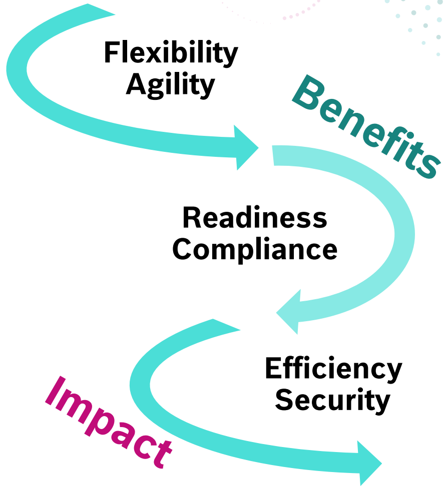
Quantum-Resilient Security Controls



- 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? ...

BOSCH

Thank You

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

BGSW
alt_future

BOSCH CYBERSECURITY UNIVERSITY

BOSCH