BOSCH

Combating the Quantum Hackers:
A Secure Tomorrow Starts Now

Software
Digital
Solutions

Table of contents

1 ABSTRACT/ SUMMARY

2 QUANTUM RESILIENT SECURITY: THE BACKBONE OF OUR MODERN DIGITAL ECOSYSTEM

3 THE QUANTUM THREAT

4 ENTERING THE POST-QUANTUM AGE: A SECURE FUTURE WITH QRSC

5 CHALLENGES IN ADOPTING QUANTUM-RESILIENT SECURITY

6 IMPLEMENTING QUANTUM-RESILIENT SECURITY: A PRACTICAL APPROACH

7 QUANTUM-RESILIENT MARKET LANDSCAPE

8 QUANTUM-PROOFING DIGITAL ASSETS WITH BOSCH

> In an era of sophisticated malicious actors with access to quantum computers which will annihilate the traditional public-key infrastructure (PKI), an essential component of cybersecurity, quantum resilient security controls (QRSC) are our only hope towards ensuring security of our assets."

Abstract/Summary

While quantum hacking may seem a distant threat, it is prudent to be proactive and prepare for potential future challenges now. Quantum computers, advanced machines capable of solving complex problems at unprecedented speeds, promise to do good but can also cause harm. Though their existence remains years or even decades away, these sophisticated computers have the potential to reshape security in our digitally connected ecosystems. Powerful quantum computers can simultaneously calculate and consider countless solutions to a problem, breaking virtually any password, and rendering existing encryption algorithms useless.

However, if these computers are still hypothetical, do we need to start worrying now? The answer is, yes. New cyberattack strategies like “Store Now, Decrypt Later” (SNDL) have already emerged in our digital landscape. The hackers are stealing our precious data today, storing it for as long as they need to, until they finally get access to quantum computers that are powerful enough to decrypt it. It is clearer now, more than ever, that we must start preparing for a post-quantum world.

In an era of sophisticated malicious actors with access to quantum computers that can annihilate the traditional public-key infrastructure (PKI), quantum-resilient security controls (QRSC) can become a pillar of modern cybersecurity. They can be our only hope to ensure the security of our assets in the future.

Quantum Resilient Security: The Backbone of Our Modern Digital Ecosystem

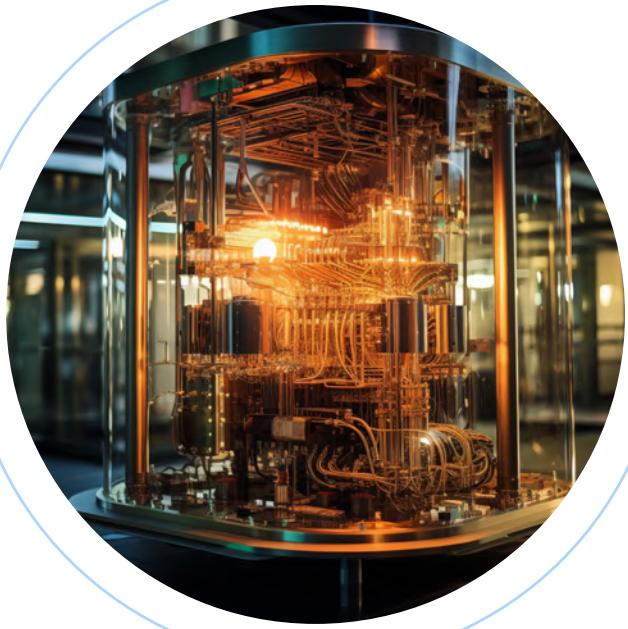
The functionality of the digitally connected ecosystem, including financial transactions, healthcare records, connected vehicles, smart cities, and critical infrastructure, relies on fundamental security objectives like entity identification, data integrity, data authenticity, and data confidentiality. These objectives are achieved using various security controls and protocols, the essential components of which are digital certificates and public key infrastructure (PKI). The security guarantees of these two components rely on asymmetric cryptographic algorithms, traditionally RSA and ECDSA. Such traditional algorithms, however, can be broken entirely once cryptographically relevant quantum computers (CRQC) become available.

Post-quantum cryptography (PQC), a domain of cryptography that deals with the design and analysis of cryptographic algorithms, can be used in classical systems to secure itself against both quantum and classical adversaries. In recent years, awareness of the potential threats posed by future quantum computers to current cybersecurity infrastructure has become more widespread.

The Quantum Threat

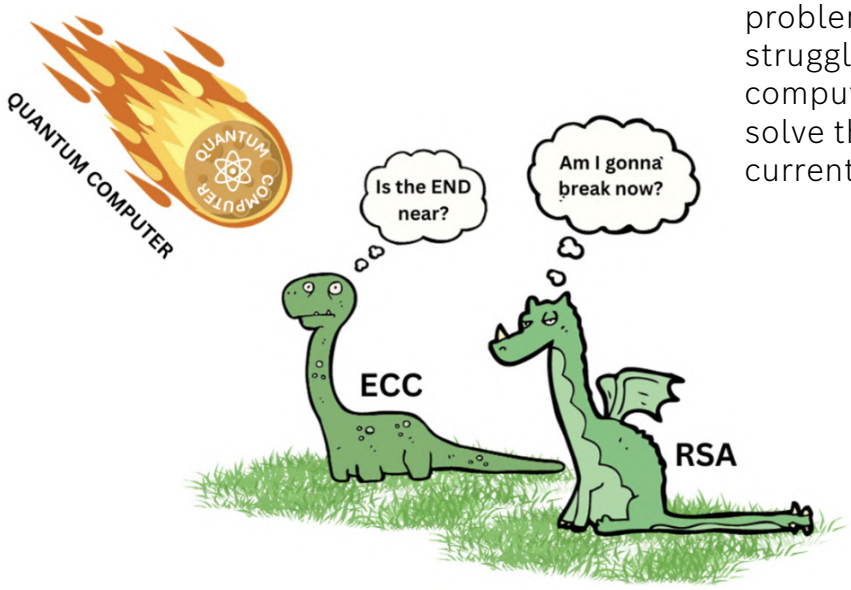
Quantum Computing Advancements

Though still in its preliminary stages, quantum computing is rapidly progressing, with governments and private enterprises making significant investments. Milestones like IBM's quantum roadmap indicate advancements toward practical quantum machines capable of solving complex problems at unprecedented speeds. Microsoft, leveraging its Azure Quantum platform and recent breakthroughs in topological qubits, is expanding the boundaries of scalable quantum systems. Google, on the other hand, continues to lead with its Sycamore processor by demonstrating how quantum systems can perform better than classical supercomputers in specific tasks. Holistically, these advancements anticipate a future where today's encryption methods might be considered obsolete and hint towards profound cybersecurity implications.



How CRQCs Will Break Traditional Cryptographic Algorithms

Digital security today relies on asymmetric cryptography, primarily RSA and ECDSA algorithms, whose security are based on complex mathematical problems, such as integer factorization or discrete logarithm problems. While classical computers struggle with these computations, quantum computers running Shor's algorithm can solve them exponentially faster, rendering current encryption obsolete.



Entering the Post-Quantum Age: A Secure Future With QRSC

Recognizing the imminent threat posed by quantum computers, the National Institute of Standards and Technology (NIST) initiated a global effort to standardize post-quantum cryptographic (PQC) algorithms to help stakeholders migrate to the quantum era safely. NIST has recently selected a set of PQC algorithms: ML-KEM (Kyber), ML-DSA (Dilithium), SLH-DSA (SPHINCS+), HQC, XMSS, and LMS. However, these algorithms will require substantial optimization of resources such as memory, bandwidth, CPU cycles, etc., and extensive testing before they can be practically deployed in the real-world applications. This has prompted more cybersecurity solution providers to accelerate their efforts in developing and deploying quantum-resilient security controls (QRSC). These can be integrated with the existing hardware and interoperate with existing communications protocols and networks, ensuring security against quantum and classical adversaries.

Hardware Migration

Migration to quantum-resistant systems may involve upgrading physical devices with new cryptographic modules or designing hardware accelerators specifically optimized for PQC algorithms. These upgrades must be secure while maintaining system performance, as the added computational load from PQC algorithms can impact efficiency.

Software Migration

Organizations must update cryptographic libraries, communication protocols, and authentication mechanisms to support post-quantum algorithms. The actual challenge, however, lies in ensuring backward compatibility with current systems during the transition. To achieve this, software solutions must be modular, allowing for the seamless integration of PQC algorithms without disrupting the integrity of existing systems.

Challenges in adopting Quantum-Resilient Security

While shifting to post-quantum cryptography (PQC) is essential, organizations may face several challenges in adopting quantum-resilient security solutions. These challenges span technical, operational, and regulatory aspects, making widespread adoption complex and resource-intensive.

Performance Trade-offs

Unlike traditional cryptography, quantum-resistant algorithms have substantially different computational requirements. They often require specific optimizations at both software and hardware levels to ensure efficient execution without compromising system performance.

Compatibility with Existing Infrastructure

Contemporary security frameworks, including public key infrastructure, digital certificates, and secure communication protocols, like TLS, are built around classical cryptographic algorithms. Replacing these with quantum-resistant alternatives may require significant updates to hardware, software, and communication protocols.

Regulatory and Compliance Challenges

Beyond governmental and regulatory guidelines, organizations must align their security strategies with emerging post-quantum standards to avoid non-compliance risks.

Adoption Costs and Resource Constraints

Transitioning to post-quantum security requires significant investment in research, development, and workforce training. Enterprises must allocate resources to test, validate, and integrate quantum-resistant cryptographic solutions into their infrastructure.

Implementing Quantum-Resilient Security: A Practical Approach

To address these challenges, organizations must adopt a structured approach to implementing quantum-resilient security. The first step in adopting PQC is to comprehensively assess existing security frameworks, and distinctly identify areas that rely on vulnerable cryptographic algorithms.

Hybrid PQC integration in Security Architecture

Organizations are integrating PQC by incorporating hybrid cryptographic models that combine classical and quantum-resilient algorithms. Given the unpredictable advancements in quantum computing, adopting a flexible and adaptive security strategy is crucial. Cryptographic agility allows organizations to switch between cryptographic methods as new threats emerge dynamically. This allows for a smooth transition without replacing existing security mechanisms, offering a practical starting point.

Testing and Benchmarking Performance

Before fully deploying PQC, organizations must conduct extensive testing to evaluate the impact of quantum-resistant algorithms on system performance. This includes evaluating encryption and decryption latency, key length, total computational overhead, and server-side and client-side processing time.

Collaboration with Industry and Regulatory Bodies

Organizations should actively participate in industry forums, regulatory discussions, and standardization efforts to stay ahead of PQC developments. Collaborating with cybersecurity firms, government agencies, and industry peers can help organizations draw on their varied expertise. This collective effort will help them cover all aspects of PQC implementation, including cryptographic protocols, software, hardware, and libraries, ensuring robust defense mechanisms against potential quantum attacks.

Quantum-Resilient Market Landscape

As storage assets become more deeply Quantum-resilient technology currently accounts for approximately **1.52 billion USD** in the market, and by 2029, it is estimated to surpass **9.4 billion USD**. The global market size of quantum-resilient technology is growing at a staggering rate of **44.2% CAGR**. This growth is fueled by the urgent need to protect critical information from the potential threats posed by quantum computing advancements.

Global Landscape and Industry Initiatives

Several countries have launched national strategies to address the quantum cybersecurity challenge. The U.S. National Institute of Standards and Technology (NIST) has led global efforts by standardizing PQC algorithms. Leading technology firms and startups such as PQShield, ID Quantique, and SandboxAQ are actively developing quantum-resilient solutions. Meanwhile, cybersecurity giants like IBM, Intel, Apple, Microsoft, and Google are embedding PQC into their products and cloud infrastructures, ensuring future-proof security.

India's Initiatives in Quantum-Resilience

The Government of India has launched several initiatives to advance post-quantum cryptography. In April 2023, the Union Cabinet approved the National Quantum Mission (NQM) with a budget of ₹6,003.65 crore (approximately 730 million USD) for 2023–2031. This mission aims to foster scientific and industrial research and development, establishing a robust and dynamic quantum technology (QT) ecosystem. A key initiative under NQM is the development of Quantum Key Distribution (QKD) satellites by the Indian Space Research Organization (ISRO), ensuring secure and quantum-resilient communication channels.

EU’s Quantum Flagship Program

Launched in 2018 with a budget of €1 billion over 10 years (2018-2028), the European Union’s Quantum Flagship program is a major driver for research and development in quantum communication and encryption technologies and other quantum domains. One of the key aspects of this approach is the European Quantum Communication Infrastructure (EuroQCI) initiative, striving to create a secure quantum communication network across the EU. It integrates Quantum Key Distribution (QKD) and several other terrestrial and space-based quantum technologies. The European Telecommunications Standards Institute (ETSI) also plays a vital role in developing quantum-safe cryptography standards while actively working on standardizing PQC algorithms and QKD protocols.

Besides these, several other individual member states are also complementing EU-level efforts with significant national investments. For example, France announced a €1.8 billion investment plan, and Germany committed €2 billion to quantum technologies with a strong focus on security and industrial applications. In 2019, the Netherlands published a National Agenda on Quantum Technologies, implemented through the Quantum Delta NL program, focusing on research, ecosystem development, human capital, and societal dialogue.

Other countries investing in Quantum-Resilience

China is investing heavily in quantum technologies as a strategic priority. It has also made significant advances in quantum key distribution (QKD), including the launch of Micius, the world's first quantum communication satellite. China is also building out a national quantum communication backbone spanning thousands of kilometers.

Japan, through its Moonshot R&D Program and collaborations between government, academia, and companies like Toshiba and NTT, is focusing on quantum cryptography and secure communications. The country also aims to deploy QKD networks in critical infrastructure sectors, including finance and defense.

The United Kingdom established the National Quantum Technologies Programme in 2014 and followed that up with a National Quantum Strategy in 2023, charting a 10-year plan to realize the potential of quantum technologies.

Quantum-Proofing Digital Assets with Bosch

For the last decade, Bosch SDS has invested in continuous research, development, integration, and deployment of cybersecurity controls to mitigate the threats posed by quantum computing. Our Quantum-Resilient Security Controls (QRSC) provide end-to-end protection, by seamlessly integrating with existing hardware and communication protocols to safeguard device integrity, secure access, trusted updates, and encrypted communications in a post-quantum world.

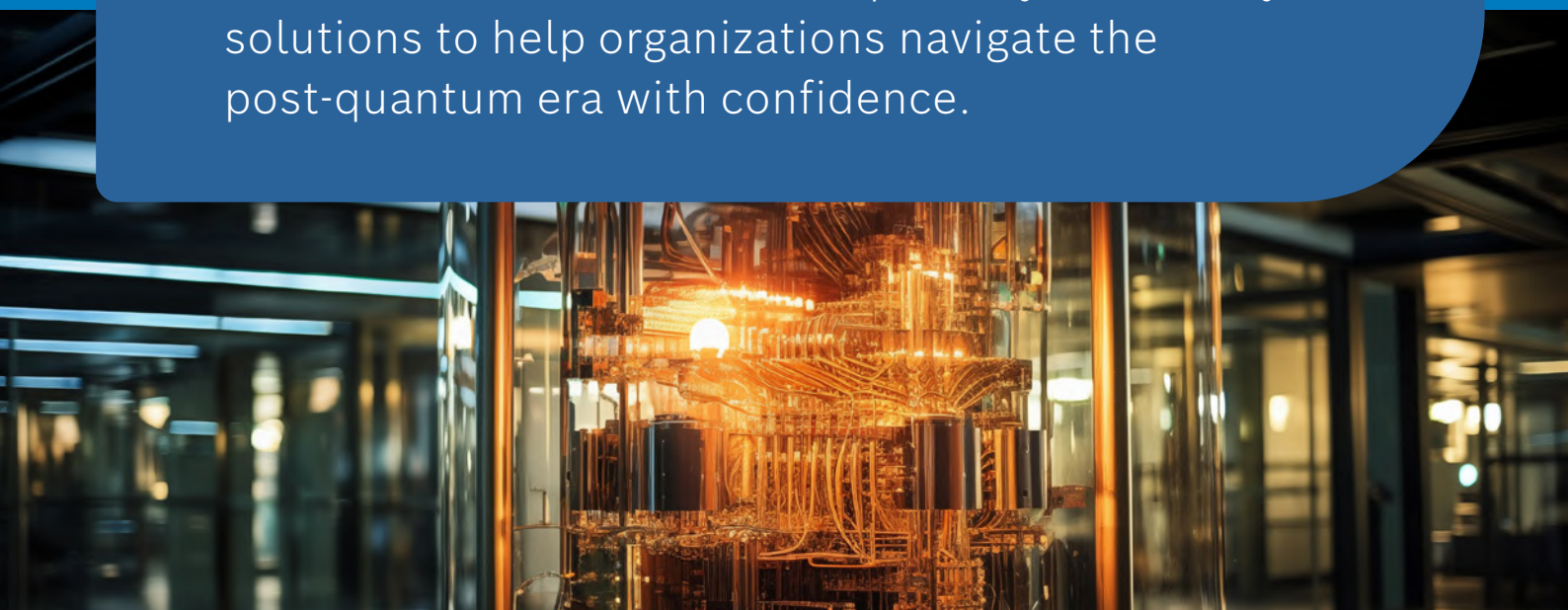
Built on NIST-standardized post-quantum cryptographic algorithms, our solutions are optimized for real-world performance, ensuring efficiency across diverse operational environments. Our security stack is available in both Software-as-a-Product (SaaP) and Software-as-a-Service (SaaS) models, enabling enterprises to adopt quantum resilience without costly infrastructure overhauls.

The comprehensive approach of Bosch SDS incorporates stand-alone PQC, mixed PQC, and hybrid classical-and-PQC schemes at various levels of the certificate chain to meet each customer's specific needs.

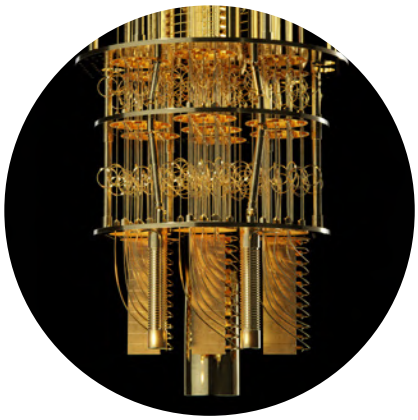
We ensure seamless integration across hardware and software, helping clients maintain cryptographic agility and implement state-of-the-art security. This enables them to meet regulatory compliances, industry best practices, and market demands in an efficient, flexible, and scalable manner.

By implementing quantum-resilient security today, businesses can ensure compliance with upcoming regulatory mandates, mitigate future cyber risks, and maintain operational security across long product lifecycles.

Bosch SDS stands ready to lead the way, providing scalable, efficient, and future-proof cybersecurity solutions to help organizations navigate the post-quantum era with confidence.



Traditional/Classical Security Controls



Quantum-Resilient (QR) Security Controls

Secure Boot

Secure Update

DH
ECDSA
RSA

Secure Access

Secure TLS

VULNERABLE

QR Boot

QR Update

Kyber
Dilithium
SPHINCS+
Falcon
XMSS

QR Access

QR TLS

SECURE

Author Details

Dr. Vishal Saraswat
(Head – Research & Innovation,
Cybersecurity Practice, Bosch SDS.)

Established in 1886, the Bosch Group is a leading global partner for technology and services. Bosch Software and Digital Solutions (Bosch SDS) is a global digitalization provider of consulting, engineering, and IT services. We help enterprises switch to Smarter Digital, a forward-looking approach to digitalization that is centered on the user. From creating new digital business models, enabling resilient future-proof enterprises and accelerating sustainability goals, Bosch SDS is a trusted partner for a multitude of industries across the world. As a global technology partner, Bosch SDS operates in North America, Europe, the UK, the Middle East, and Asia Pacific markets through a network of on-shore, near-shore and off-shore delivery centers.

Bosch Software and Digital Solutions
NA | UK | EU | ME | SE | JP

www.bosch-sds.com

connect.sds@bosch.com

linkedin.com/company/bosch-software-digital-solutions/