FUTUREMATTERS™
CENTRE OF EXCELLENCE

PREPARING FOR A QUANTUM-SAFE TOMORROW

Contributors:

Thomas Moser
Alternate Member of the Governing Board,
Swiss National Bank

Andreas Wehrli
Advisor to the Head of Department III,
Swiss National Bank

POINT ZERO FORUM™
Policymakers | Leaders | Investors

Content

Introduction

Quantum computers evolved from theoretical concepts in the 1980s to experimental realisations in the 2000s and are now in the early stages of practical application. Although many technical challenges remain, the field is advancing rapidly towards practical, large-scale quantum computing. Significant breakthroughs are expected in the coming years.

Quantum computers offer great opportunities to solve complex problems that remain intractable for classical computers. However, this capability also poses a threat to the security of public key cryptosystems, which are widely used today to ensure the confidentiality and integrity of digital communications. For the financial sector, a specific threat is that quantum computers can forge the digital signatures used to ensure the integrity and authenticity of financial transactions.

How close are we to Q-Day, the day when quantum computers will be powerful enough to break public key cryptosystems widely used today? Which strategies should we adopt to protect our financial infrastructures before Q-Day arrives? How urgent is the transition to quantum-resistant cryptosystems? What measures should organisations take?

These questions set the context for the roundtable, “Preparing for a quantum-safe tomorrow,” held in Zürich on 3 July 2024, as part of the Point Zero Forum. The Swiss National Bank hosted the session with Thomas Moser, Alternate Member of the Governing Board, serving as the moderator. The roundtable brought together experts from private-sector research companies, academia, international standard setters, and the financial industry. Participants included Raphael Auer (BIS), August Benz (Swiss Bankers Association), Marco Brenner (IBM), Klaus Ensslin (ETH Zurich), Frederik Flöther (QuantumBasel), Esther Haenggi (Lucerne University of Applied Sciences and Arts), Heike Riel (IBM), and Sven Stucki (Procivis).

This report summarises key points of the discussion and proposes four practical action points for financial institutions and other organisations to consider when looking for ways to ensure the security of their businesses and those of their customers.

Quantum computing in the financial sector

The state of quantum computing

Quantum computing represents a fundamental shift in computational technology, utilising principles of quantum mechanics like superposition, entanglement, and interference, which differ significantly from the classical physics that underpin traditional computing. As a result, quantum computers have the potential to solve problems that are beyond the capabilities of classical computers. This is particularly notable in fields that require large amounts of computational power, such as model simulations or search and optimisation problems.

Recent years have seen significant advances in both quantum hardware and algorithms, pushing the boundaries of what was thought to be possible. Governments and academic institutions worldwide are heavily investing in quantum research, and tech companies such as IBM, Google, Microsoft, and Intel have made significant advances in developing quantum computing. In 2016, IBM launched the 'IBM Quantum Platform', providing a cloud-based access to its five-qubit quantum computer – the largest at that time – for researchers and the public.[1]

While classical computers are not able to simulate a quantum computer with more than a few dozen qubits, today there are already quantum processors with more than 1,000 qubits, and there are plans to reach multiple thousands of qubits by 2030.[2] We have already reached a state of quantum utility, the state in quantum computing development where quantum computers can serve as a scientific tool to explore a new scale of problems that classical methods may not be able to solve This scale, combined with advances in algorithms, is fundamental to enabling quantum advantage; the point where quantum computers can faithfully run one of more tasks providing business or scientific value with more accuracy, efficiency, or cost-effectiveness than with classical computation alone. Looking ahead, we can expect further progress as major technological trends like artificial intelligence, cloud computing, distributed ledger technology, and quantum computing are partly interdependent and mutually reinforcing.

Despite these advances, a real scaling up of quantum computing has not yet occurred as significant challenges persist. There are several challenges research and development is working on like scaling the number of qubits, as well as reducing and mitigating errors as qubits are highly susceptible to them. Additionally, there is no definitive architecture for quantum hardware; various novel types, such as superconducting qubits, neutral atoms and ion traps, are being explored.

1. Qubits, or quantum bits, are the smallest unit of date in quantum computing. Unlike a classical bit which is in one of two states (either 0 or 1), a qubit can be in a combination of both states simultaneously (superposition).

2. See for instance IBM's roadmap for quantum computing: https://www.ibm.com/roadmaps/quantum/

The promise of quantum computing: A powerful tool for complex tasks

While quantum computing is not a panacea, it is a powerful tool for specific, complex tasks. It holds immense potential, particularly in fields where classical computing approaches fall short. While quantum computers are not poised to replace classical computers universally, they promise to excel in areas that require parallel processing and complex problem-solving at a previously unmanageable scale.

In finance, promising applications of quantum computing include portfolio optimisation, risk analysis and risk management, algorithmic trading, prediction analytics and fraud detection. These areas could benefit from quantum computing's ability to handle vast amounts of data (although efficiently loading large volumes of classical data remains challenging for quantum computers) and perform complex calculations at unprecedented speeds.

For instance, optimisation problems, whose complexity tends to rise exponentially with the number of choice variables, can be solved more efficiently using quantum algorithms. Quantum computers can potentially also accelerate certain machine learning tasks.

The threat of quantum computing: Implications for cryptosystems

Quantum computing poses significant challenges for cryptosystems because of its potential to break widely used cryptographic protocols that are currently considered secure. The security of many algorithms that underlie much of today's applied cryptography rely on the difficulty of specific mathematical problems, such as integer factorisation (e.g., RSA) and discrete logarithms (e.g., Elliptic Curve Cryptography), which large-scale quantum computers will be able to efficiently solve.

Given that such algorithms are foundational to today's secure communication protocols, digital signatures, and public key infrastructure systems, potential damage to the financial sector and the economy is huge if the risk is not mitigated in time. Sensitive financial data could be exposed and digital signatures forged, leading to large-scale fraud, unauthorised fund transfers, and identity theft. Loss of customer confidence could cause market instability. Financial firms could face legal repercussions and hefty fines for conditions potentially outside of their control. The broader economy could suffer from disrupted markets and increased volatility. Transitioning to quantum-safe cryptosystems is essential to mitigate these risks.

How much time do we have until Q-day?

How many years remain until quantum computers can break a significant part of commonly used cryptography? An anecdotal audience poll at the roundtable discussion yielded an almost even distribution of responses ranging from one to fifteen years.

While predictions about the pace of technological advancement are often wrong, there was a strong consensus among roundtable participants that significant developments in quantum computing will occur within the next decade. In any case, given recent rapid advancements, Q-Day is closer today than was thought possible just a few years ago.

Arguably, the precise date of Q-Day is irrelevant from a risk management perspective. The probability of it happening in any given year from now is not zero, and the business impact would be huge. Even a 5% risk is too high to ignore.

Solutions and challenges in achieving quantum-safety

What solutions are available to achieve quantum-safety?

Quantum security requires cryptographic algorithms and protocols that are designed to be secure not only against the capabilities of classical computers, but also those of quantum computers. To achieve this, there are two approaches that are not mutually exclusive: The migration to cryptosystems using (i) post-quantum cryptography and (ii) quantum cryptography.

Post-quantum cryptography focuses on quantum-safe classical algorithms. Its security relies on problems that are considered intractable even for quantum computers. The U.S. National Institute of Standards and Technology (NIST) is leading efforts to standardise post-quantum cryptographic algorithms. In August 2024, NIST released a first set of encryption algorithms[3] designed to withstand cyberattacks from a quantum computer.

Quantum cryptography uses the principles of quantum mechanics itself. Unlike post-quantum cryptography, quantum cryptography does not rely on computational assumptions but provides theoretically unconditional security based on the laws of quantum mechanics. Quantum key distribution is an example already in use. However, quantum cryptography requires specialised hardware, which can be expensive and challenging to deploy on a large scale and still requires end-point security.

Implementing quantum-safe algorithms is not merely a technical challenge. It extends to business processes and the intricate links within our digital ecosystems, requiring a comprehensive approach to ensure that all interconnected silos remain secure. For most applications, post-quantum cryptography is the more practical and immediate solution today. It can be more easily integrated into existing systems and requires fewer significant changes in infrastructure.

Challenges in implementing quantum safety: Not plug and play

There is a common misconception that quantum safety can be achieved simply by exchanging the relevant algorithms. Unfortunately, it is much more complex in practice. While technical solutions for quantum safety exist, implementing them in an organisation's IT infrastructure remains challenging.

The transition to quantum-safe cryptography is not confined to individual applications, it affects entire communication systems and business ecosystems. As cryptography touches all elements of digital business models, replacing the underlying mathematical structures of these requires comprehensive planning and execution. Differences in the resource footprints of the newly proposed algorithms further complicate this transition as additional capacity is required. Updating legacy systems is arduous and generally involves surmounting a steep organisational learning curve.

3. https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards

Case studies highlight this complexity. Project Leap, recently undertaken by the BIS Innovation Hub, involved connecting private and public clouds with a layer of post-quantum cryptography.[4] The project revealed several practical challenges and performance impacts, underscoring the difficulty of updating legacy infrastructures. Similarly, Project Tourbillon showed that replacing classic cryptography with post-quantum cryptography may impair performance.[5] These examples indicate that migration requires time to get new systems up and running and that it is therefore better to start early.

Practical action points to achieve quantum safety

To achieve quantum safety within a limited time frame, organisations must take proactive steps to safeguard their systems against emerging quantum threats. Specifically, there are four practical action points:

Identify quantum-competent staff in your organisation. Ensure that your organisation has at least one person who understands quantum computing and its potential impacts. If this is not feasible, collaborate with other organisations to share expertise. This person should stay informed about developments in quantum computing and standards, and inform the organisation on specific implications to its practices and infrastructure.

Assess vulnerabilities in your systems. Conduct a thorough assessment of your organisation's systems to identify where vulnerable cryptography is used. This includes evaluating the security of financial data and other critical information that must remain confidential for years.

Develop a plan to achieve quantum safety. Create a comprehensive plan to transition to quantum-safe cryptosystems. This plan should include timelines, resource allocations, and strategies for implementing new cryptographic standards as they are finalised. Start building skills within your team to handle these future changes.

Establish regular dialogue with key stakeholders. Achieving quantum safety is not just a technical issue, but also a strategic imperative requiring collaboration among authorities, academia, the financial industry, and tech companies. Regular dialogue ensures the exchange of crucial information, classification of developments, and derivation of necessary measures to address emerging challenges and enhance organisational quantum safety.

4. See "Project Leap: quantum-proofing the financial system": https://www.bis.org/about/bisih/topics/cyber_security/leap.htm
5. Project Tourbillon: exploring privacy, security and scalability for CBDCs: https://www.bis.org/publ/othp80.htm

Contributors

Thomas Moser
Alternate Member of the Governing Board,
Swiss National Bank

Thomas Moser is alternate member of the governing board of the SNB and responsible for the operational management of the Money Market and Foreign Exchange, Asset Management, Banking Operations, and Information Technology divisions, as well as for the Singapore branch office. Additionally, he is a member of the Managing Committee of the Swiss Institute of Banking and Finance at the University of St. Gallen and a visiting professor at the Faculty of Economics and Management at the University of Lucerne.

Andreas Wehrli
Advisor to the Head of Department III,
Swiss National Bank

Andreas (Tres) Wehrli is advisor to governing board members of the SNB and his current work focuses on issues related to payments and digital innovation. On these topics, he contributes to SNB projects, publications and speeches by senior management.