Quantum Technology for Securing Financial Messaging

July 2024

Acknowledgments

Thank you to the Quantum Economic Development Consortium (QED-C®) Use Cases Technical Advisory Committee. Additionally, this report would not have been possible without the leadership and contributions of the members of the workshop organizing committee.

Peter Bordow, Wells Fargo
Scott Buchholz, Deloitte
John Buselli, IBM
Terry Cronin, Toshiba
Carl Dukatz, Accenture
Mehdi Namazi, Qunnect
Simon Patkovic, ID Quantique
Bruno Huttner, ID Quantique
John Prisco, Safe Quantum
Tahereh Rezaei, Wells Fargo
Keeper Sharkey, ODE, L3C
Catherine Simondi, ID Quantique
Colin Soutar, Deloitte
Jeff Stapleton, Wells Fargo

Thank you to Accenture for providing workshop facilities.

The National Institute of Standards and Technology (NIST) provided financial support for this study.

About QED-C

QED-C is an industry-driven consortium managed by SRI. With a diverse membership representing industry, academia, government, and other stakeholders, the consortium seeks to enable and grow the quantum industry and associated supply chain. For more about QED-C, visit our website at quantumconsortium.org.

Suggested Citation

Quantum Economic Development Consortium (QED-C®). *Quantum Technology for Securing Financial Messaging*. Arlington, VA. May 2024. https://quantumconsortium.org/financial24.

Government Purpose Rights

Agreement No.: OTA-2019-0001
Contractor Name: SRI International
Contractor Address: 333 Ravenswood Avenue, Menlo Park, CA 94025
Expiration Date: Perpetual
Use, duplication, or disclosure is subject to the restrictions as stated in the Agreement between NIST and SRI.

Non-US Government Notice

Disclaimer
This publication of the Quantum Economic Development Consortium, which is managed by SRI International, does not necessarily represent the views of SRI International, any individual member of QED-C, or any government agency.

Table of Contents

Executive Summary

The financial industry depends on secure messaging in transactions sent between banks, merchants, customers, and government agencies; credit card authorizations; wire transfers; account information; and other types of communications. The monetary and systemic value of financial messaging makes it especially vulnerable to cybersecurity attacks. Cryptography is therefore central to trust in the financial system and critical to the financial industry and to the economies that rely on it.

The advent of quantum computing creates a new cybersecurity challenge for financial institutions, as quantum computers will one day become powerful enough to break many of the cryptographic algorithms currently used to protect data and communications. Most notable is the ability for quantum computers to run Shor's algorithm, which threatens many of the commonly deployed encryption methods used to protect messaging. Running Shor's algorithm requires a cryptographically relevant quantum computer (CRQC), which is likely still years in the future. However, the concept of "harvest now, decrypt later" means that encrypted data taken today compound overall risk. Furthermore, the technology upgrade path to post-quantum security readiness will take many years. Financial institutions need to take steps *today* to mitigate future risks.

There are two technologies that provide different forms of security against a CRQC: post-quantum cryptography (PQC) and quantum key distribution (QKD); we describe each. They offer different benefits and, if combined, may provide increased protection.

The two technologies have potential applications in the following high-feasibility, high-impact use cases identified by stakeholders in quantum security and financial services:

- more secure cross-border transactions,
- security-enabling physical infrastructure,
- third-party validation of financial institutions' quantum security posture,
- post-quantum transport layer security, and
- quantum communications service providers.

Three important themes emerged during this study:

1. The threat posed by a future CRQC requires immediate evaluation of exposure risk to a cybersecurity breach due to the threat posed by harvest now, decrypt later.
2. Combined approaches that employ multiple technologies may increase security.

3. Third-party service providers can help ensure timely risk mitigation by smaller institutions.

In addition, three recommendations are suggested for advancing security in the financial industry:

1. **Support the financial industry in implementation of PQC standards:** Federal agencies should support migration to PQC algorithms by sharing information and resources with financial institutions and by providing grants to help institutions implement the new algorithms. Grants to state and local government entities that handle sensitive financial information should also be considered. While large financial institutions will have the financial and technological resources to swiftly implement the change, small, community-based banks and credit unions — of which there are thousands in the United States — are more vulnerable as they have fewer resources and thus will be less prepared. Federal grants or loans to small and medium-sized financial institutions to support PQC technology adoption could be vital to maintaining a robust, quantum-resistant financial industry.
2. **Increase quantum expertise at financial institutions:** The financial industry should grow in-house quantum expertise to raise awareness of the implications of quantum technologies in terms of both benefits and risks. Financial institutions should hire quantum networking and security experts to assist with conducting an inventory of quantum-vulnerable cryptographic assets and implementing PQC standards. Financial institutions can also partner with companies developing QKD to trial this technology as it grows in its capabilities. Investment banks can further stay at the forefront of quantum technology by investing in companies that offer quantum communications and security as a service.
3. **Explore QKD + PQC combined approaches:** While QKD and PQC each have advantages and limitations, using both technologies in a combined approach could lead to higher levels of security than either approach on its own. The United States government has prioritized deploying PQC but should also fund R&D in QKD-related technologies to ensure that the nation stays competitive and protected. Federal agencies should invest today in research that aims to make QKD more scalable and practical. Investments in R&D on approaches that combine QKD, PQC, and classical cryptography will drive innovation in ways that support cryptographic defense-in-depth. The financial services sector stands ready to collaborate with telecommunications companies, researchers, and government to help assess and advance combined approaches for possible implementation before a CRQC becomes available.

Introduction

The financial sector is the driving force behind many innovative developments in information technologies and services. With over $100 trillion in assets at stake,[1] the industry depends on and invests in cutting-edge cybersecurity systems and protocols to protect itself and its customers. While appropriately cautious and conservative about adopting novel technologies, financial institutions are constantly assessing technological advances that could be the basis of new products and business — or that pose new threats.

Cyberthreats and data breaches create risks to the stability of the financial system and threaten customer trust. The problems can be compounded by the complexity of the systems involved. Financial services firms have not only technological debt from legacy systems but also complex information technology (IT) landscapes comprising internally developed and third-party applications, cloud storage and software, software-as-a-service (SaaS) capabilities, and other integrated technologies that create a large attack surface for malicious actors to attempt to exploit. Examples of attacks include:

- credit card skimmers at an ATM or gas station pose a threat to customers through a physical device,
- phishing emails to a bank employee could download malware and harvest a financial institution's data, and
- weak points in a fiberoptic network could be leveraged by cybercriminals for ransom or data exfiltration.

Merchants, customers, wire transactions, financial institution data, and network infrastructure are all targets of cybersecurity threats. In 2023 distributed denial-of-service (DDoS) attacks — cyberattacks that attempt to make a server or network unavailable to users by overwhelming it with internet traffic — targeted the financial services sector as never before.[2]

As the threat landscape continues to evolve, so does the solution space. The ability to control the quantum properties and behavior of materials, devices, and systems is at the heart of quantum computers, quantum sensors, quantum networks, and communication technologies, and these technologies create both benefits and risks for businesses' cybersecurity.

---

[1] Heredia, Lubasha, Simon Bartletta, Joe Carrubba, Dean Frankle, Chris McIntyre, Edoardo Palmisani, Anastasios Panagiotou, Neil Pardasani, Kedra Newsom Reeves, Thomas Schulte, and Ben Sheridan. 2021. *The $100 Trillion Machine*. Boston Consulting Group, July 2021, https://web-assets.bcg.com/79/bf/d1d361854084a9624a0cbce3bf07/bcg-global-asset-management-2021-jul-2021.pdf

[2] FS-ISAC. 2024. *DDoS: Here to Stay*. Reston, VA. https://www.fsisac.com/hubfs/Knowledge/DDoS/FSISAC_DDoS-HereToStay.pdf

The rapid progression of quantum computing capabilities poses a new foundational risk to the financial industry and the classical encryption protocols that enable virtually all digital transactions. A cryptographically relevant quantum computer (CRQC) would break widespread data encryption methods, such as public-key cryptography. According to current best estimates, the likelihood that a quantum computer capable of breaking RSA-2048 within 24 hours will emerge within the next ten years is materially high.[3] Furthermore, any classically encrypted communication transmitted through an unprotected network, such as the internet, is at risk today, and possibly already subject to exfiltration. Through "harvest now, decrypt later" attacks, an adversary can intercept and store encrypted data until a CRQC is available. This makes the quantum threat one of the most important cybersecurity issues facing the financial system, potentially exposing all financial transactions and much of the existing stored financial data to attack.

The stakes are high, given that data protection mechanisms for internet communications, digital signatures, passwords, contracts, and other documents would become instantly obsolete as soon as a sufficiently powerful quantum computer became operational. As just one example, a CRQC could destroy the integrity of today's digitally signed contracts because the validity of the signer's identity could no longer be ensured.[4] The implications extend to the foundation of financial messaging infrastructure, which relies on cryptography to secure ledgers and protect records in transit. An attacker with access to a CRQC could manipulate previously encrypted data, tamper with records, rewrite asset ownership rules, and generate fraudulent transactions. Even where long-term confidentiality is not a serious concern, expected migration times for many complex digital systems are already starting to exceed the potential timelines for a CRQC. The scale of the threat to the global financial sector requires the community to focus *today* on ensuring cybersecurity in the future quantum world.

This report reviews the challenges and threats posed by CRQCs and considers two primary technologies for addressing them:

1. *Post-quantum cryptography (PQC)* is software-based and involves upgrading existing mathematical cryptographic algorithms with new algorithms that are believed to be resistant to attack by a quantum computer.
2. *Quantum key distribution (QKD)* is a hardware-based approach that creates highly secure communication channels by using the principles of quantum mechanics to establish a shared secret key between two parties.

---

[3] Mosca, Michele, and Marco Piani. 2022. *Quantum Threat Timeline Report 2022*. Toronto: Global Risk Institute. https://globalriskinstitute.org/publication/2022-quantum-threat-timeline-report/

[4] Bank for International Settlements. 2023. *Project Leap: Quantum-Proofing the Financial System.* Basel. https://www.bis.org/publ/othp67.pdf

PQC and QKD are both considered quantum-resistant (also known as quantum-safe) for their ability to resist attacks from a future quantum computer. This report considers the strengths and weaknesses of each approach and assesses strategies for achieving security across the financial sector using these technologies. It is based on a workshop that brought together experts from the financial services industry, QKD technology providers, PQC suppliers/integrators, and other quantum technology stakeholders. The workshop methodology is described in Appendix A, the list of 60 quantum security use cases generated by the participants is in Appendix B, and the workshop attendees are listed in Appendix C.

Quantum-Resistant Security Approaches

Cybersecurity is an evolving challenge of protecting information against a variety of ever-changing threats. Emerging quantum technologies include quantum computers, which present novel and sophisticated threats, and quantum communication techniques, which can provide protection in the face of these threats.

The primary threat to security from quantum computers is rooted in their ability to process complex calculations that classical computers cannot. Many currently used security protocols that rely on public-key cryptography, such as Rivest-Shamir-Adleman (RSA), either will no longer be secure or will be greatly weakened by the processing capabilities of CRQCs.[5] For example, Shor's algorithm, a quantum algorithm designed by Peter Shor in 1994, provides a method for efficiently factoring large numbers. The limitations of classical computers to perform this complex calculation are the mathematical foundation of public-key cryptography in use today.

The field of cryptography has been aware of the threat posed by quantum computers, and two technologies have been developed to address it: post-quantum cryptography and quantum key distribution. Each approach has the potential to substantially benefit institutions seeking to improve the security of their information and assets. Furthermore, a combined approach that layers QKD and PQC technologies on top of existing security protocols could further increase the security of financial messages and data.

Current Cryptography Tools

Most encryption used in the financial services industry today relies on hash functions, symmetric cryptography, and/or asymmetric cryptography. Hash functions process an input to yield an output that cannot be used to recover the input. While hash functions are known to be quantum-resistant, it may be necessary to double the size of the input to be resistant to a quantum computer attack using Grover's algorithm.[6]

Symmetric or secret-key cryptography is used mostly for data encryption and sometimes for authentication and integrity (i.e., verification that the data have not been altered). The same secret key is used for encryption/signature on one side and for decryption/verification on the other side. Since it relies on shared secret keys, symmetric cryptography requires a complementary key exchange protocol to

[5] Quantum Economic Development Consortium (QED-C). 2021. *Guide to a Quantum-Safe Organization*. Arlington, VA. https://quantumconsortium.org/guide-to-a-quantum-safe-organization/

[6] Preston, Richard H. 2022. Applying Grover's Algorithm to Hash Functions: A Software Perspective. *IEEE Transactions on Quantum Engineering* PP(99): 1–12. doi: 10.1109/TQE.2022.3233526

distribute the keys from one party to the other. These keys are typically too long to remember, and great care must be taken in how they are shared. There are a few potential methods for key exchange: a written key can be physically carried in a locked suitcase with armed guards in a bulletproof vehicle from one location to another; or it can be implemented technically by using software-/firmware-based asymmetric cryptography, over a separate trusted network, or by using QKD.

The widely used transport layer security (TLS) protocol uses asymmetric cryptography for the exchange of secret session keys for connections to internet websites. For faster encryption, dedicated hardware known as link encryptors — an approach to communications security that encrypts and decrypts all network traffic at each network routing point — can reach encryption speeds of hundreds of gigabits. Importantly, asymmetric cryptography is used both for key exchange (in conjunction with symmetric cryptography for encryption) to protect the data being sent and for digital signature to verify the identity of the sender and receiver.

Traditional cryptographic algorithms, such as RSA and Diffie-Helmann, create security by relying on a mismatch in the computational difficulty of certain problems, such as those involving factorization and discrete logarithms. These problems are relatively easy to compute in one direction, and exceedingly expensive for classical computers to reverse.[7] Algorithms for quantum computers that leverage the principles of quantum mechanics, such as Shor's algorithm for integer factorization, can undermine the computational complexity of the factorization challenge. Therefore, the currently used asymmetric algorithms must be replaced by new PQC quantum-resistant ones.

Post-Quantum Cryptography

PQC is a mathematical upgrade to asymmetric algorithms that is used to protect IT systems and can run on existing, everyday classical computers. PQC involves the use of cryptographic building blocks, called "primitives," to construct more complex cryptographic protocols based on hard mathematical problems that will be able to resist attacks from both classical and quantum computers. PQC is a software-based approach and, although "quantum" is in its name, does not leverage quantum technology.

A challenge of PQC is the identification of such hard mathematical problems that are impervious (according to current knowledge) to decryption with classical and quantum computers. Quantum computing as a field is young, and there remain unknowns about what algorithms may be developed. Moreover, new algorithms that

[7] Xu, Guobin, Jianzhou Mao, Eric Sakk, and Shuangbao Paul Wang. 2023. An Overview of Quantum-Safe Approaches: Quantum Key Distribution and Post-Quantum Cryptography. IEEE 57th Annual Conference on Information Sciences and Systems.
https://ieeexplore.ieee.org/abstract/document/10089619

run on classical computers also may hold surprises in their ability to break problems thought to be computationally expensive.

Contenders for hard mathematical problems that can replace existing methods to generate cryptographic primitives include lattice-based, hash-based, code-based, and multivariate cryptography and isogeny of elliptic curves.[8] Each category offers a distinct approach to the next generation of security that can protect digital information against quantum threats.

Lattice-based cryptography relies on problems derived from lattice theory, such as finding the shortest vector in a high-dimensional lattice. Hash-based cryptography is a family of algorithms that transform data of arbitrary size into fixed-size strings, i.e., hash values. Code-based cryptography is based on error-correcting codes, multivariate cryptography is based on solving multivariate quadratic equations over a finite field known to be NP-hard, and isogeny-based cryptography involves computing the isogeny given two elliptic curves.

Four initial algorithms have been chosen by the National Institute of Standards and Technology (NIST) for standardization of PQC, three of which are lattice-based (CRYSTALS-Kyber, CRYSTALS-Dilithium, and Falcon) and one hash-based (SPHINCS+).[9] The multiple PQC standards have a range of requirements and trade-offs; different standards will work in different use cases.

PQC is expected to be widely adopted because it is accessible to classical computers and can be implemented on current hardware or with few infrastructure additions.[10] NIST is in the process of finalizing the initial PQC standards, and CRYSTALS-Kyber and CRYSTALS-Dilithium are being prepared for release this year for key encapsulation and signature, respectively (Falcon and SPHINCS+ will come later). Both algorithms involve lattice cryptography, which offers substantial advantages, including serving as a building block for identification-based encryption. These algorithms facilitate extremely efficient and fast implementations when compared to RSA encryption, and, critically, they can support hybrid cloud and edge use cases.

NIST is also continuing to explore new PQC schemes to add to this initial set. The objective is to enable additional general-purpose signature schemes and key encapsulation mechanisms for secret key exchange that are not solely lattice-based and that may provide even faster performance and smaller key sizes.

---

[8] Dam, Duc-Thuan, Thai-Ha Tran, Van-Phuc Hoang, Cong-Kha Pham, and Trong-Thuc Hoang. 2023. A Survey of Post-Quantum Cryptography: Start of a New Race. *Cryptography* 7(3): 40. https://www.mdpi.com/2410-387X/7/3/40

[9] National Institute of Standards and Technology, 2024. Post-Quantum Cryptography: Selected Algorithms 2022. https://csrc.nist.gov/projects/post-quantum-cryptography/selected-algorithms-2022

[10] QED-C (2021), op. cit. https://quantumconsortium.org/guide-to-a-quantum-safe-organization/

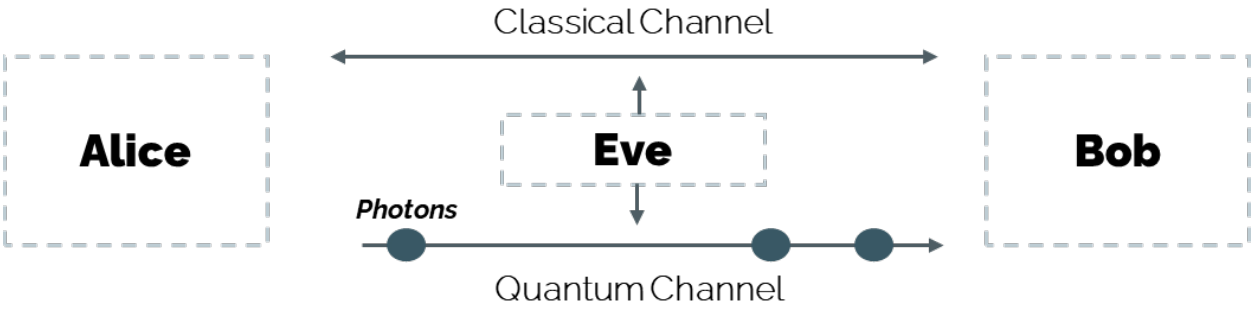
Quantum Key Distribution

Generally, data transmitted on current networks can be copied by anyone who can capture the information through techniques such as interception, sniffing, and spoofing. Cryptography is used to make data unintelligible without knowing the keys, mitigating the risk of theft of data in transit.

Quantum physics offers another approach for preventing the theft of information. QKD establishes a key shared between two parties by leveraging the principles of quantum mechanics, such as the superposition and entanglement of quantum states, to protect against eavesdropping attempts. When a key transmission is intercepted, the quantum effects produce evidence of tampering that cannot be avoided regardless of the computational resources of the eavesdropper.[11] Implementation of QKD does not require a quantum computer, but it does require special technology for transmitting and receiving data.

QKD involves sending information in the form of both photons and bits through quantum and classical channels, respectively. The quantum channel used to send the stream of photons is typically either an optical fiber or free space, and a crucial characteristic of the channel is the ability to preserve the quantum properties of the photon. The classical channel is used to share the information necessary to correlate and authenticate the information sent in the quantum channel (see Figure 1). The principles of quantum mechanics mean that an attacker attempting to eavesdrop on the quantum channel would perturb the stream of photons through the act of measurement, and thus the eavesdropping would be detectable as a disruption to the key sharing.

Figure 1: Illustration of a QKD system between two parties



Commercial key distribution services are available and many protocols for QKD have been proposed, including BB84 and its variants, B92 and E91, and the more recently developed coherent one-way protocol.[12] In 2022 Toshiba and BT launched a

[11] Alléaume, R., C. Branciard, J. Bouda, T. Debuisschert, M. Dianati, et al. 2014. Using Quantum Key Distribution for Cryptographic Purposes: A Survey. *Theoretical Computer Science* 560, part 1: 62–81. https://www.sciencedirect.com/science/article/pii/S0304397514006963

[12] Xu et al. (2023), op. cit. https://ieeexplore.ieee.org/abstract/document/10089619

metropolitan network in London that uses QKD and can be deployed over existing fiber networks; EY and HSBC have both signed up to trial the network.[13] Similarly, ID Quantique (IDQ) is collaborating with telecommunications operators Singtel in Singapore and SK Telecom in Korea, as well as other European telecommunications operators, to create nationwide quantum networks to provide quantum-safe-as-a-service to their enterprise customers.[14] IDQ is also directly engaged in projects with the Fidelity Center for Applied Technology, JPMC, Hanwha Bank, and other banks in Europe.

Although QKD is relatively mature, there remain practical challenges to its implementation. First, it requires specialized hardware, including single-photon sources and detectors, which adds to implementation and maintenance costs. Second, since quantum principles prevent the use of optical amplifiers on the quantum channel, point-to-point QKD links can function only over relatively short distances, typically about 100 kilometers. To offer long-distance security, QKD links must be connected by trusted nodes (TNs) in QKD networks. Quantum-protected keys hop from one TN to another but are not protected by quantum within the node, creating a potential point of attack. TNs may be replaced in the future by quantum repeaters, a technology that is the subject of current research, to enable secure long-distance distribution of quantum-protected keys. Another option for long-distance key distribution is via satellite, whereby the satellite serves as a TN. Finally, QKD cannot be used for authentication, integrity, and nonrepudiation actions, which means that it must be implemented alongside other quantum-resistant security methods.[15]

Based on these challenges and the imminent announcement of PQC standards, some governments are not recommending QKD at this time. The US National Security Agency released a statement that QKD would not be certified for use in national security systems because of hardware and infrastructure costs and limitations as well as challenges in securing, validating, and authenticating when using QKD.[16] Several European countries' security agencies have also recently urged prioritization of PQC over QKD given the latter's limitations and the need to act now to strengthen cybersecurity.[17]

---

[13] Pearce, James. 2023. HSBC trials quantum cyber defence system with BT, Toshiba and AWS. *TechInformed*, July 6. https://techinformed.com/hsbc-trials-quantum-cyber-defence-system-with-bt-toshiba-and-aws/

[14] ID Quantique. 2022. IDQ and SK Broadband complete phase one of nation-wide Korean QKD Network, July 19. Geneva. https://www.idquantique.com/idq-and-sk-broadband-complete-phase-one-of-nation-wide-korean-qkd-network/

[15] QED-C (2021), op. cit. https://quantumconsortium.org/guide-to-a-quantum-safe-organization/

[16] National Security Agency. Quantum Key Distribution (QKD) and Quantum Cryptography (QC). Fort Meade, MD. https://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC/

[17] French Cybersecurity Agency, Federal Office for Information Security [Germany], Netherlands National Communications Security Agency, and Swedish National Communications Security Authority.

Combined Methods

In this report we use the word "combined" broadly to mean cryptographic systems that combine multiple protocols. Such an approach could use one or more PQC algorithms for encryption and authentication as well as QKD for key distribution.[18] PQC addresses the challenge of securing data against quantum attacks, while QKD provides a quantum-resistant and eavesdropping-proof means of distributing encryption keys. Classical cryptographic techniques can also be part of a combined solution.

In a World Economic Forum report,[19] developed in collaboration with Deloitte, PQC and QKD were described as follows (p. 24):

> In today's nascent quantum cybersecurity market, several efforts are ongoing to develop technologies to mitigate the quantum threat. These technologies do not represent a silver bullet, but they can be used individually or in combination for certain applications…to mitigate the risk posed by quantum to public-key cryptography that have been garnering the majority of attention:
>
> - Post-quantum cryptography (PQC) uses new mathematics-based public-key cryptography algorithms that are designed to be impervious to attacks by Shor's algorithm. PQC will fundamentally update what will become insecure cryptographic algorithms.
> - Quantum key distribution (QKD) develops physics-based quantum techniques to generate secure communication channels which can be used to distribute encryption keys. QKD can complement the use of PQC and other cryptographic algorithms by providing a secure key distribution method.

Further security can be achieved by adding layers of software-based cryptography.

Combined approaches have the potential to enhance security by incorporating the strengths of each. By layering with classical cryptography tools such as pre-shared keys and symmetric cryptography, combined approaches provide a transition pathway to post-quantum methods. Moreover, combining protocols may provide defense in depth by creating layers of protection. For example, an approach that

---

2024. Position Paper on Quantum Key Distribution, January 26, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Crypto/Quantum_Positionspapier.pdf?__blob=publicationFile&v=4

[18] Marchsreiter, Dominik, and Johanna Sepúlveda. 2023. A PQC and QKD Hybridization for Quantum-Secure Communications. IEEE 26th Euromicro Conference on Digital System Design (DSD). https://ieeexplore-ieee-org.sri.idm.oclc.org/abstract/document/10456851

[19] World Economic Forum, in collaboration with Deloitte. 2022. *Transitioning to a Quantum-Secure Economy*, 24. Geneva. https://www3.weforum.org/docs/WEF_Transitioning%20to_a_Quantum_Secure_Economy_2022.pdf

implements PQC, QKD, and symmetric key technologies would resist attacks even if the selected PQC algorithm were broken.

However, when implementing combined solutions, it will be important to assess the potential to create new points of attack as well as the benefits of multiple layers or protocols.

Combined solutions could be particularly valuable to the financial industry, given its critical need to protect sensitive financial data with greater security and resilience to quantum and classical attacks.

Current and Emergent Technologies

PQC and QKD are at different stages of development and readiness for full-scale implementation. NIST has been leading the PQC standards effort since 2016.[20] Following a thorough evaluation process, four PQC algorithms (noted above) have been selected from 82 submitted by the cryptography community.[21] Robustness to attack by a quantum computer is the primary consideration; however, practical implementation is also a factor, and the four algorithms offer a range of requirements. As when cryptographic standards have been upgraded in the past, institutions will need to update their security systems when they migrate to the new standards. Transitioning to the PQC standards is expected to take time and resources and organizations are encouraged to start now by assessing the most critical data and systems for prioritization. The NIST Cybersecurity Center of Excellence has published a fact sheet with steps to take in preparation for migration to PQC.[22]

Although commercially available, QKD continues to be an area of research and development. Desired improvements include faster key generation rates, an extended range of secure communication, and enhanced practicality and scalability of QKD systems. Research is also needed to improve options for integrating QKD into existing network infrastructure. For example, QKD could be used in conjunction to RFC 8784, which is used by most network hardware vendors to enable pre-shared post-quantum keys.

Implementing new measures of security and resilience is not optional as progress is made toward a CRQC. Quantum computing experts believe it is not a matter of whether there will be a CRQC but when, and security experts affirm that PQC, QKD, and combined approaches offer the current best levels of protection against the

---

[20] NIST Computer Security Resource Center. 2024. Post-Quantum Cryptography, last modified May 28. https://csrc.nist.gov/projects/post-quantum-cryptography

[21] IBM. 2023. *Security in the Quantum Computing Era*. Armonk, NY. https://www.ibm.com/thought-leadership/institute-business-value/en-us/report/quantum-safe-encryption

[22] Cybersecurity & Infrastructure Security Agency, National Security Agency, and NIST. 2023. Quantum-readiness: Migration to post-quantum cryptography, August 17. https://www.nccoe.nist.gov/sites/default/files/2023-08/quantum-readiness-fact-sheet.pdf

eventuality of a CRQC. By using a combined approach, institutions can mitigate the risk of a single point of failure and increase resilience to a wider range of threats than any one quantum-resistant security measure could provide in isolation.

Migrating an enterprise's information security systems and infrastructures from a quantum-vulnerable to a quantum-resistant state can be enormously complicated and costly. Depending on the enterprise, a quantum-resistant migration program may take a decade or longer to complete. While not a primary objective of the workshop, discussions touched on the need for new methods for cryptographic remediation. "Crypto-agility" is a characteristic of a flexible information security system that can pivot to a variety of encryption methods without significant disruption. According to NIST, crypto-agility is imperative to preparing for a quantum-resistant future.

Furthermore, implementing the four selected PQC algorithms should not be considered a permanent. failproof solution. It is difficult to predict what cyberattacks will be possible in the future, but it is almost certain that new threats beyond Shor's algorithm will exist. Algorithmic solutions, such as PQC, will need to continually evolve to sustain protection against cyberattacks. Quantum physics-based solutions, such as QKD, can support defense-in-defense as new cyberthreats emerge.

In summary, advances in quantum computing will leave contemporary cryptography insecure, meaning that the technology that financial services firms rely on to protect data will no longer safeguard information. To prepare for these risks, companies must anticipate future requirements of encrypted systems and begin the process of transitioning to post-quantum cryptography by reviewing their data holdings and developing a plan to prioritize and protect sensitive and critical data.

The remainder of this report explores the potential benefits and challenges of quantum technology use cases related to the pressing security concerns that quantum threats pose to the financial industry.

Key Themes of Use Cases

Financial services and quantum experts at the workshop discussed the potential impact of quantum computing, networking, and communications in the financial sector and identified 60 uses cases for applying quantum-resistant technologies. For each use case idea, participants were asked to identify a delivery channel (e.g., customers, merchants) and pick a technology approach (e.g., QKD, PQC, combined) that could be a primary method of addressing that use case.[23] The findings presented in this section are based on the workshop process that required participants to pick a primary approach to facilitate the workshop activities; the approach selected for each case is not necessarily the *only* possible approach.

Several themes emerged among the identified use cases. First, despite the expectations that a CRQC is likely a decade or more in the future, the threat posed by future systems exists today through the method of harvest now, decrypt later. Second, an approach combining both PQC and QKD is worth further exploration. Third, given the magnitude of the threat and the diversity of institutions that must migrate to new security systems and protocols, quantum security as a service is seen as a potential solution to expedite migration to quantum-resistant security in the financial sector.

Theme 1: Current Threat

The estimated timeline for the emergence of a cryptographically relevant quantum computer ranges from within ten years to several decades. However, most experts acknowledge that there is an immediate risk to financial messaging from harvest now, decrypt later threats, where information encrypted with current public-key or asymmetric key protocols is collected now in its encrypted form, under the assumption it will be possible and expedient to break the encryption with a future CRQC.[24]

While certain data have a relatively short lifespan, other types have a much longer shelf life, spanning several decades. For example, the financial details of a ten-year loan might not be of high value, but the social security numbers and other personally identifiable information on the loan document could have longevity well beyond the duration of the loan. Similarly, compromised data about trading strategies could lead to financial losses, identity theft, fraud, and reputational damage for the institution

[23] See Appendix A for the workshop methodology and the matrix that participants used to categorize their ideas, which are listed in Appendix B.
[24] Soutar, Colin, Scott Buchholz, Doug Dannemiller, and Mohak Bhuta. 2023. Industry Spending on Quantum Computing Will Rise Dramatically. Will It Pay Off? Deloitte. https://www2.deloitte.com/us/en/insights/industry/financial-services/financial-services-industry-predictions/2023/quantum-computing-in-finance.html

where the breach occurred. Such risks must be taken into consideration when determining the lifetime and sensitivity of documents and information.

Furthermore, migration to quantum-resistant technologies is expected to take a long time, so even getting signatures migrated before the arrival of a CRQC is becoming urgent. Given near- and long-term threats, there are agreed upon measures that should be taken now.[25,26] The first steps for a financial institution are to perform a comprehensive inventory of all data assets and to start to map out the institution's cryptography landscape. It should then plan the implementation of selected solutions and finally execute the plan to ensure post-quantum security.

Theme 2: Combined Systems

Many security use cases to address the threat posed by CRQCs may benefit from a combined solution. Among the 60 use cases identified during this workshop, participants chose combined technology as the primary approach to explore for 17 of them. The complexity and diversity of the technology used in financial messaging, as well as the sensitivity of the content, argue for a multilayered security approach to mitigate the threat.

Combined systems can take many forms to bolster cryptographic defense-in-depth. To name a few examples, elliptic curve cryptography from classical approaches can be combined with Kyber, a PQC algorithm; several PQC algorithms can be used in a standard session; and one or more PQC algorithms can be paired with a QKD-based key.

PQC and QKD each have advantages and drawbacks. PQC is software-based, can be implemented now, is relatively affordable, and can be upgraded in the future, but PQC algorithms may eventually be compromised by classical or quantum computers. QKD does not rely on computationally hard problems and will not be vulnerable to advances in computation. However, it is hardware-based and therefore more costly. Also, it is not useful for authentication and so must be used in combination with other approaches. Given the complementary aspects of PQC and QKD, a combined solution may offer more robust protection, especially when further combined with pre-shared keys and symmetric cryptography. Combined approaches will be critical to implement in sectors with large institutions whose business could be highly impacted, such as finance.

---

[25] ETSI. 2020. *Migration strategies and recommendations to Quantum Safe schemes*. Technical Report 103 619. Valbonne, France. https://www.etsi.org/deliver/etsi_tr/103600_103699/103619/01.01.01_60/tr_103619v010101p.pdf

[26] White House. 2022. National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems, May 4. https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/

Theme 3: Quantum-Resistant Security as a Service

Concerns were raised about the inadequacy of relying solely on individual financial institutions to address the significant threat posed by quantum computers to the security of financial messaging. Quantum-resistant security offered as a service, especially for smaller financial institutions, may be a more practical approach.

Of the five use cases examined in greater detail during the workshop, two lend themselves to a service-based model: One centered around third-party services to help companies meet quantum-resistant standards, while another focused on telecom providers offering quantum-safe networks. Two others, examining cross-border transactions and physical infrastructure, presupposed established quantum-safe networks, sometimes provided by entities other than financial institutions.

The financial sector is highly interconnected, involving communications and transactions among tens of thousands of institutions globally. The security of the network and of the data transmitted on it depends on security at each networked institution. A vulnerability anywhere in the network can threaten both security throughout the network and customer trust in the financial sector. Relying solely on individual institutions to secure the data that they send and receive is a potential weak link. While larger entities may have the financial means to implement robust safeguards independently, smaller institutions may lack the necessary resources. Quantum security as a service helps address this gap by providing cost-effective security solutions tailored to the specific needs and capacities of diverse stakeholders, thus bolstering the entire financial ecosystem against quantum threats.

Impact and Feasibility of Selected Use Cases

In breakout groups at the workshop, participants prioritized two or three use case ideas to present to the full group, resulting in nine consolidated use cases (see Figure 2 and Table 1). These nine were then ranked by the group on impact and feasibility (see Appendix A for the methodology). The most impactful use case was *money movement*; however, it did not rank high on feasibility, likely because of the requirement of large-scale coordination among banks and network providers. When this concept was expounded on in subsequent workshop activities, its scope was narrowed to cross-border transactions, which is seen as more tractable.[27] Cross-border transactions are growing in number but generally considered not only less secure by stakeholders because of control and ownership boundary changes but also more costly and slower than domestic transactions; they would thus be a prime area for improvement in the broad category of money movement.

The use case ranked most feasible was c*onnecting to customers using post-quantum transport layer security.* TLS is an existing encryption protocol that secures the connection between a web server and a web application, and it applies to most data exchanged over the internet. PQC is the principal approach recommended by the workshop participants for achieving *post-quantum TLS*. Its high feasibility ranking stems from the fact that PQC is designed to work on current devices and network infrastructure.

[27] Bank of England. 2023. "Cross-border payments." Last modified January 31. https://www.bankofengland.co.uk/payment-and-settlement/cross-border-payments

Figure 2: Impact and feasibility of the nine consolidated use cases

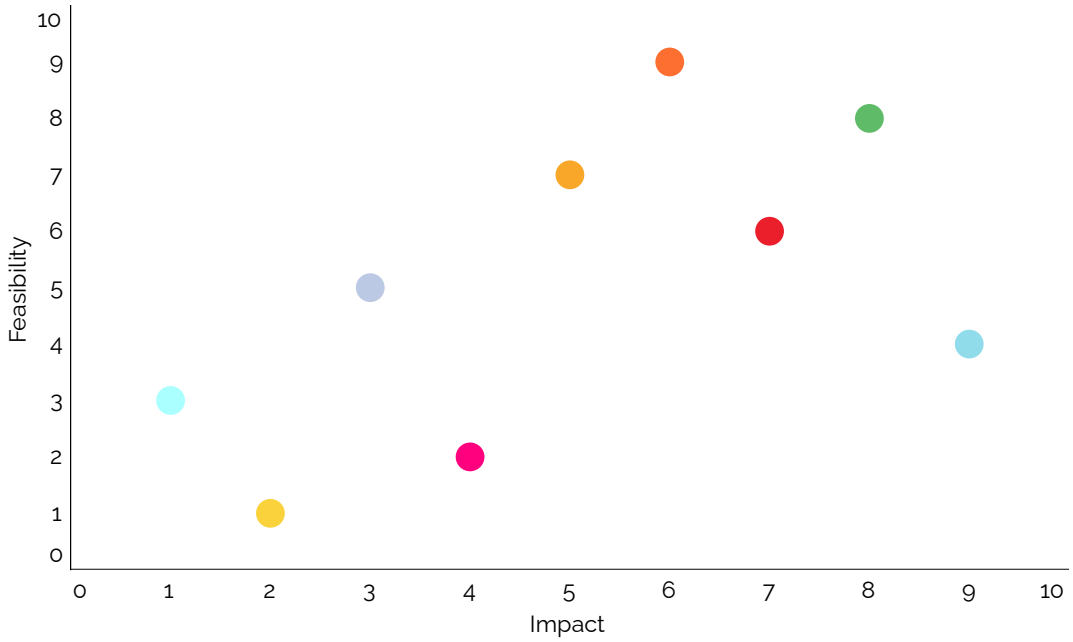


Table 1: Legend for categories displayed in Figure 2

	3rd-party risk: enable out-of-band key services; cloud provider
	Connecting to customers using post-quantum TLS; Europay, Visa, and Mastercard credit cards; prepaid/credit cards; payment tokenization with PQC-based authorization
	Email negotiations; account information can be changed; hybrid and pre-shared key
	Preventive measures; hybrid protection for cybersecurity for detecting fraud
	Physical critical infrastructure: protecting fiber backbone between data centers (DC) and customers, banks, and other DCs; decrypting high-value networks; data center backbone; critical infrastructure for secure FedWire
	QKD for embedded devices: Internet of Things (IoT), supervisory control and data acquisition (SCADA), point of sale (POS), automated teller machines (ATM); communications security (BB84 QKD embedded in the telecommunications backbone, for all optical-based connections)
	Money movement: bank-to-bank transfer protected by QKD network defense
	Secure bidding using quantum auctions
	Shared QKD infrastructure; privately owned QKD links can be offered to others as a service

Classification

The workshop participants classified the 60 use cases by primary technology approach (QKD, PQC, a combined method, symmetric, or other) and delivery channel (customer, merchant, financial, operations, or other). Again, the classification chosen should not be considered the only possible technological approach or the only relevant delivery channel, but instead as the primary approach that participants were interested in exploring during the workshop activities.

The most frequently selected technology for a given use case was QKD, followed by combined QKD + PQC approaches, and then PQC. Overall, though, there was a balance of technology approaches selected, and the frequency should not be interpreted as the participants' preference for or recommendation of one technology over another. The most common delivery channels selected for the use cases were customer, financial, and other, the latter of which captured many ideas for infrastructure development. Only one use case was classified as merchant-related. Of the use cases in the high-impact, high-feasibility quadrant (shown in Appendix A), there was no trend in the selected technology approach or delivery channel.

Implementation Details of Selected Use Cases

Five of the consolidated use cases that were voted as most feasible and impactful were further developed. For each, workshop participants expanded on the use case description and discussed desired features and functionalities, timelines, and critical stakeholders for implementation based on the security approach selected in the previous activity.

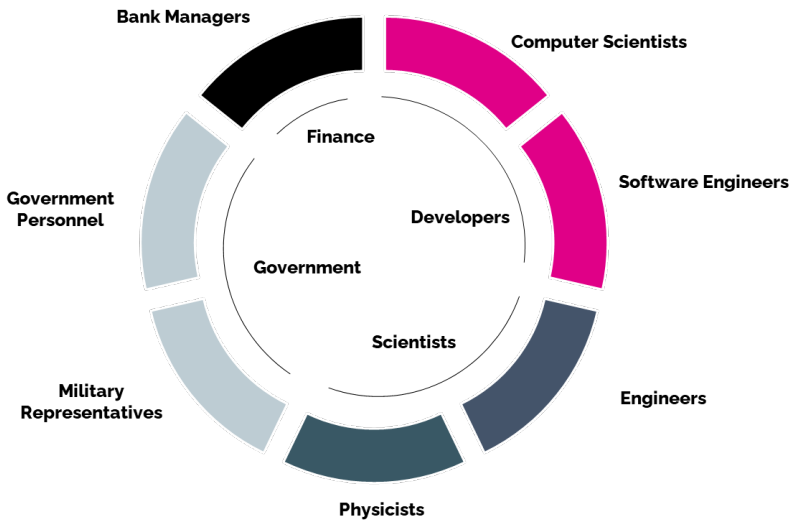
Cross-Border Transactions

The concept of cross-border transactions, honed from the money movement use case, includes bank transfers, credit card payments, and other types of financial transactions between entities in different countries, which are more vulnerable than transactions within one country. There is potential for using QKD to assist in the secure movement of money, primarily the end-to-end exchange of symmetric keys for international payments and messaging systems. This would create a quantum-secure key exchange and key management system, in addition to the traditional public-key mechanism, that would detect misbehavior in areas otherwise invisible to the transferring party.

To increase the security of cross-border transactions, there would need to be a resilient, heterogeneous network of fiber and free-space QKD links. Long-distance quantum networks for key distribution will require trusted nodes in the short term until quantum repeaters become available. There would also need to be redundancy built in by involving multiple providers.

Using QKD for cross-border transactions can enhance security against the potential threat from quantum computers, bolster financial stability, and reduce cyberattacks and fraud, though it likely would not improve transaction speed. Establishing the necessary infrastructure and systems is a principal barrier to realizing this use case. It would require international agreement and collaboration, which could take time to develop but would strengthen alliances among like-minded countries and could eventually lead to global standards. Creating such a system would entail substantial cost that could be justified by the reduced cross-border transaction risks and costs. Figure 3 illustrates the key personnel who are expected to be involved in the development and implementation of this use case.

Figure 3: Key personnel for cross-border transactions



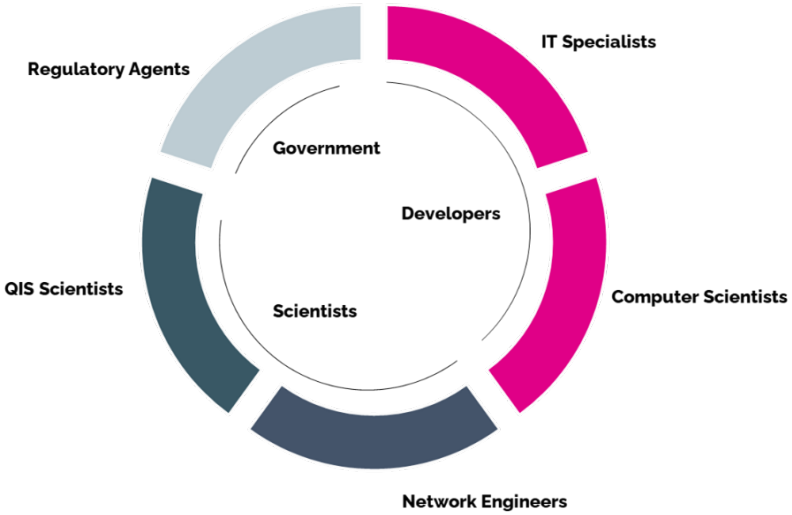
Physical Infrastructure

A promising idea that experts believe is quite technologically feasible today involves using quantum networking technology to construct critical physical infrastructure with fiber connections that can serve as a secure backbone for financial communications between banks and data centers as well as for other financial transactions. A hybrid QKD-classical system would facilitate the secure transfer of large volumes of information, with QKD providing security and classical providing the bulk transfer. The primary users of this system would be the infrastructure owners themselves, in this case financial institutions, with the potential for adoption by nonfinancial entities that offer services to banks.

The proposed system would employ dark fiber links (fiberoptic cables that do not have service or traffic running through them) and QKD integrated with a new wide area network equipped with routers that feature key management entities (KME). Ideal features of this proposed system include continuous availability, physical security, redundancy, low latency, adherence to established standards, and transparency. The success of this concept hinges on achieving these features with minimal or no security breaches.

Figure 4 illustrates the key personnel who are expected to be involved in the implementation of this use case. The timeframe for researching and developing this concept is anticipated to be relatively short. Although this use case ranked high in both impact and feasibility, there may be challenges in terms of project cost and financing, geographical distance, and regulatory obstacles.

Figure 4: Key personnel for physical infrastructure

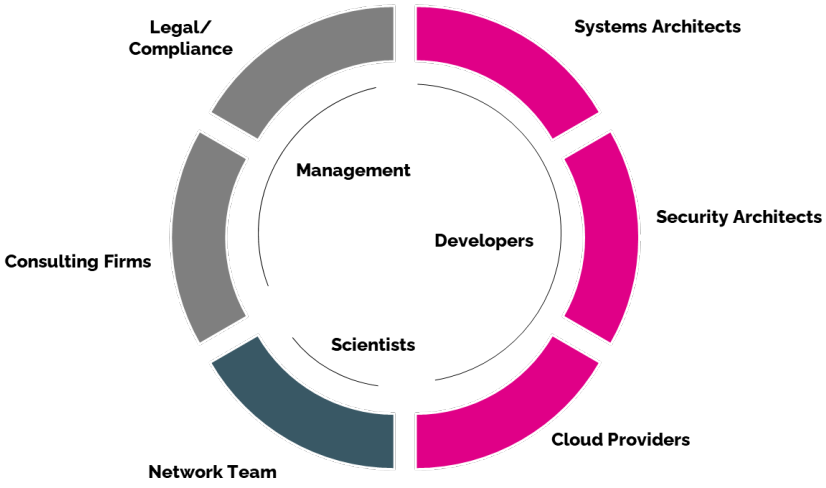


Quantum Security as a Service

Security is incredibly important in financial services, but for many institutions it is not their core business. As a result, developing in-house capabilities to implement QKD, PQC, or combined systems will not be a top priority. Third-party service providers will be available to support financial institutions by deploying and managing the daily operations of the systems implementing quantum-resistant techniques. Financial services companies will use contractual agreement mechanisms to transfer and mitigate risk. The third party would employ auditors to produce reports that assess the efficacy of a company's quantum security. The audits should evaluate adherence to industry standards through acquisition, testing, and deployment of a suite of tools. Third-party servicers will need to develop an easy-to-use approach that is interoperable among financial institutions, easy to deploy, and cost efficient, all while ensuring levels of security comparable to today's standards vis-à-vis data transmission, storage, and usage.

Before implementation can begin, standards must be developed and adopted. Financial institutions must ensure that their entire value chain and their partners follow and implement the adopted standards, which can be a challenge if awareness and acceptance of the risk is low in the sector. Additionally, institutions and their partners may have conflicting timelines and/or lack technical capabilities, hardware, and access to a qualified quantum workforce, any of which could prevent successful implementation. Figure 5 illustrates the key personnel who are expected to be involved in the development and implementation of this use case.

Figure 5: Key personnel for cloud service providers

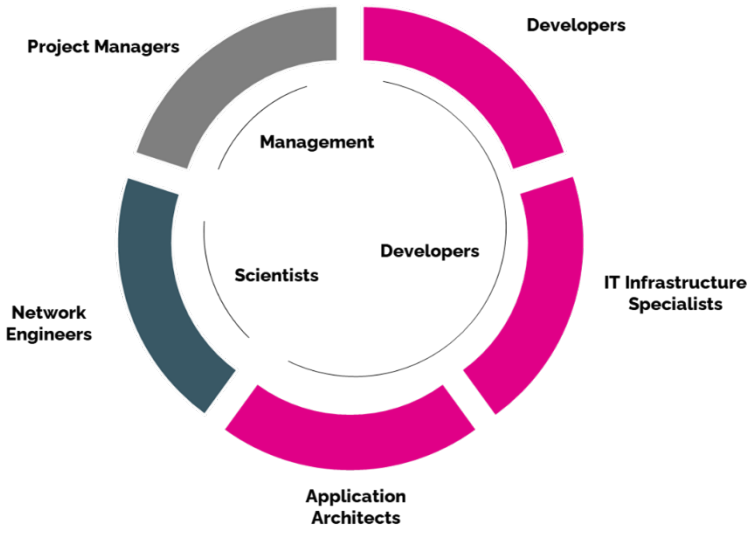


Post-Quantum TLS: Connecting Customers

TLS is a cryptographic protocol that secures the connection between a web server and a web application using data encryption. It applies to all data exchanged over the network, including emails, web browsing sessions, and file transfers, and prevents hackers from accessing users' sensitive data such as login credentials and credit card numbers.[28] A next generation of TLS, quick UDP internet connections (QUIC), has been widely deployed. Both TLS and QUIC protocols now have implementations that use PQC. Upgraded TLS and QUIC will benefit all internet service end users (i.e., customers) and especially the hard-to-reach places in the financial services industry, such as millions of point-of-sale (POS) systems and automated teller machines (ATMs).

Post-quantum TLS is currently deployed by major internet browsers and infrastructure providers such as Google, Microsoft, and Amazon Web Services, and it will be the primary deployment channel for the PQC standards from NIST. Once NIST delivers these standards (expected in July 2024), upgraded TLS could be deployed and integrated into important financial services within 12 months. Figure 6 illustrates the key personnel who will likely need to be involved in the development and implementation of this use case.

Figure 6: Key personnel for quantum transport layer security



[28] Dinda, Sopha M. 2023. *What Is TLS? Understanding Transport Layer Security and How It Works.* Hostinger Tutorials, May 14. https://www.hostinger.com/tutorials/what-is-tls

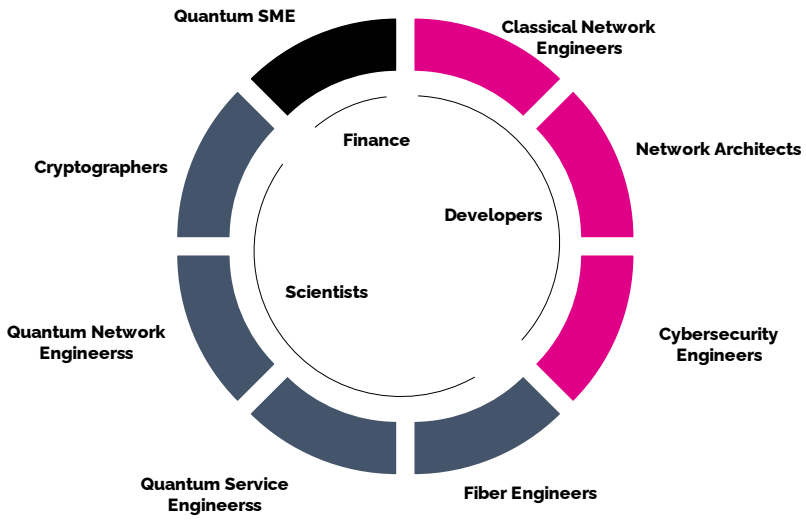
Quantum Communications Service Provider

Though experts don't expect this to have a significant impact on financial sector security, an idea with potentially broad applicability is for major telecommunications operators to build out a national quantum network. This could be done via fiberoptic cable and/or free-space networks (without fiberoptic cable, through laser communication). For example, Verizon fiber networks could connect two banks, which could use the common fiberoptic cable infrastructure via the link of the quantum service provider. Entanglement-based quantum networks are likely the most viable for this application because the user can verify the sender and receiver without having to trust a network partner.

Development of this application would require collaboration among satellite providers, fiber infrastructure owners, photonics companies, and the quantum service providers; see Figure 7 for the key personnel involved in the development of this use case. Customers would need to verify the trust of the sender; the service provider would distribute entanglement; and users would rent the necessary equipment. The provider could differentiate tiers of service by quantum analogs of traditional performance metrics, such as bandwidth, throughput, and attack detection latency. To use the service, bank branches would need network-to-network compatibility. While quantum as a service would initially be limited geographically, with the development of quantum repeater technology it could eventually spread across the nation, connecting thousands of parties.

The timeline for implementing this use case is long, estimated at 11 years: It is expected to take about four years to deploy nationally owned quantum satellites, another five years to deploy quantum repeaters to enable long-distance networks, and about two years for final deployment.

Figure 7: Key personnel for quantum service provider



Recommendations

The following recommendations for advancing security in the financial industry are based on inputs from the workshop and subsequent discussions with experts in the field. Their implementation will likely enhance security in other sectors as well.

1. **Support the financial industry in implementation of PQC standards:** NIST is expected to release standardized post-quantum cryptography algorithms as early as July 2024. These algorithms will augment existing cryptographic algorithms to improve security and resistance to attacks by a quantum computer, but they can take substantial time, labor, and money to implement. Financial institutions need to inventory their network protocols, software, applications, and other assets that are vulnerable to quantum computing attacks and then prioritize assets for migration to PQC algorithms.

   Federal agencies such as NIST, the Federal Deposit Insurance Corporation, National Credit Union Administration, and Community Development Financial Institutions Fund should support this migration by sharing information and resources with financial institutions and providing grants to help institutions implement the new algorithms. In particular, while large financial institutions will have the financial and technological resources to swiftly implement the change, small, community-based banks and credit unions — of which there are thousands in the United States — have fewer resources and thus will be less prepared and more vulnerable.

   Similarly, grants to state and local government entities that handle sensitive financial information should be considered. As tax collectors, most state, county, and city governments collect data on citizens' and businesses' investment transactions, incomes and expenditures, and other sensitive information that is tied directly to a social security number or employer identification number. As public entities, these agencies also typically have limited resources to shore up their technology security. Federal grants or loans to small and medium-sized financial institutions and state and local government agencies to support adoption of quantum-resistant technologies could be vital to maintaining a robust, resilient financial industry.

2. **Increase quantum expertise at financial institutions:** The financial industry has a strong record of being early adopters of new technologies. It should continue this trend by growing in-house quantum expertise to raise awareness of the implications of quantum technologies in terms of both benefits and risks. Financial institutions should hire quantum networking and security experts to assist with conducting an inventory of quantum-vulnerable cryptographic assets and implementing PQC standards. Where there are workforce shortages, financial institutions can help train quantum workers by

partnering with academic institutions that have strong cybersecurity and quantum programs.

Financial institutions can also partner with companies developing QKD to trial this technology as it grows in its capabilities. Layering QKD with PQC and classical cryptography approaches could one day increase defense-in-depth, but getting to that point will take investments in network infrastructure and deployment pilots. Investment banks can further stay at the forefront of quantum technology by investing in companies that offer quantum communications and security as a service.

3. **Explore QKD + PQC combined approaches:** While QKD and PQC each have advantages and limitations, using both technologies in a combined approach could lead to higher levels of security than either approach on its own. All European Union member states have signed onto the European Quantum Communication Infrastructure (EuroQCI) Initiative, which supports deployment of QKD networks,[29] and China has deployed satellites to provide QKD.[30] The United States government has prioritized PQC deployment, but it should also fund R&D in QKD-related technologies to ensure that the nation stays competitive and protected. Several financial institutions are already trialing QKD networks (see **Quantum Key Distribution** section), and the number of financial use cases for QKD generated by workshop participants indicates significant interest in continued QKD innovation.

   Federal agencies should invest today in research that aims to make QKD more scalable and practical. These investments in R&D on approaches that combine QKD, PQC, and classical cryptography will drive innovation in ways that support cryptographic defense-in-depth. Furthermore, government agencies should use this report to gauge interest in different security research topics. Innovation is needed not just for deploying PQC algorithms but also for developing post-quantum blockchains, making pre-shared keys and symmetric cryptography more scalable, developing quantum repeaters to make long-distance QKD networks viable, and effectively implementing combined cryptography approaches.

   The financial services sector stands ready to collaborate with telecommunications companies, researchers, and government to help assess and advance combined approaches for possible implementation *before* a

[29] European Commission. 2024. The European Quantum Communication Infrastructure (EuroQCI) Initiative. https://digital-strategy.ec.europa.eu/en/policies/european-quantum-communication-infrastructure-euroqci

[30] Jones, Andrew. 2023. China is developing a quantum communications satellite network. *SpaceNews*, March 10. https://spacenews.com/china-is-developing-a-quantum-communications-satellite-network/

CRQC becomes available. Government should engage financial services stakeholders through groups such as QED-C, FS-ISAC, and the Department of Homeland Security's Financial Services Sector Council.

Appendix A: Methodology

This report explores quantum security as it relates to secured financial messaging and is informed by an in-person workshop organized by the QED-C Use Cases Technical Advisory Committee. The event took place February 22, 2024, in New York City — a hub of the financial industry — and was attended by 48 stakeholders from finance, quantum technology, government, and academia.

Participants looked at a variety of security approaches (primarily cryptography and quantum key distribution) and their ability to solve problems facing the financial industry, and identified 60 specific use cases (listed in Appendix B). Several use cases focused on addressing transaction-related problems such as wire transfers and person-to-person payments. A few focused on infrastructure development, though participants noted that existing infrastructure likely just needs updating to support quantum-secure financial messaging.

Workshop Goals: Surface High-Impact, Feasible Ideas

- Capture many ideas on how to use quantum technology to solve current challenges in the financial sector and create a diverse set of concepts to investigate.
- Clearly define and refine popular ideas and match to quantum approaches for future exploration, including timeline to realization.
- Isolate the ideas with the highest impact and feasibility and identify a path to bring these ideas to fruition.

Structure: Encourage Collaboration, Fresh Thinking

The workshop was designed to maximize collaboration opportunities among attendees with knowledge of finance and those familiar with quantum technologies. Facilitators and attendees from the quantum sector were invited to a briefing on the workshop structure and tools several days before the event to ensure smooth operations. All participants were sent the following reading materials beforehand describing how quantum might help with securing financial messaging and transactions:

- Defense Advanced Research Projects Agency. 2023. A network security revolution enhanced by quantum communication, June 13. https://www.darpa.mil/news-events/2023-06-13
- Guarrera, David, and Khalid Khan. 2023. Preparing financial services cybersecurity for quantum computing. EY, April 12, https://www.ey.com/en_us/strategy/financial-services-cybersecurity-for-quantum-computing
- Deloitte, 2024. FSI Predictions 2024. https://www2.deloitte.com/xe/en/insights/industry/financial-services/financial-services-industry-predictions.html#industry-spending

- FS-ISAC, 2023. Preparing for a Post-Quantum World by Managing Cryptographic Risk. https://www.fsisac.com/knowledge/pqc
- National Security Agency. Quantum Key Distribution (QKD) and Quantum Cryptography (QC). Fort Meade, MD. https://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC/
- Shields, Andrew. Without quantum encryption, the financial sector will not be secure for long. Toshiba. https://www.toshiba.eu/quantum/insights/without-quantum-encryption-the-financial-sector-will-not-be-secure-for-long/
- Bank for International Settlements. 2023. *Project Leap: Quantum-Proofing the Financial System.* Basel. https://www.bis.org/publ/othp67.pdf
- Singh, Mandeep, and Albert H. Carlson. 2024. Exploring Polymorphic Algorithms and Their Use in Cryptography. IEEE 14th Annual Computing and Communication Workshop and Conference (CCWC). https://ieeexplore.ieee.org/document/10427812

The workshop began with presentations from groups that are working actively on cryptography and/or increasing the security of financial messaging to provide context and foundational information on the state of security and financial services. Whitfield Diffie, a mathematician and early pioneer of public-key cryptography, gave a keynote talk that provided an overview of the evolution of cryptography. To start, he explained that cryptography is a security technique best applied to messaging and communications across large distances and networks. He then stressed that quantum computing threatens to break current key management systems, thereby putting the security of nearly all financial transactions and data at risk of theft, corruption, and interception.

Michele Mosca, cofounder and CEO of EvolutionQ, discussed the role of quantum networks in strengthening cryptographic defenses. He emphasized the importance of a dual-track program for quantum readiness in the financial industry that focuses on both potential and risk. He also highlighted the key features of quantum networks used for communications and the limitations of those networks. For example, quantum communication networks are currently much more limited by distance compared to classical networks; however, solutions like satellite networks and repeaters circumvent some of the challenges of establishing long-distance entanglement to better enable quantum networks. Mosca also noted that because classical and quantum networks both rely on optical fiber and free-space media (satellites), there is a high likelihood that quantum communication networks can be established using existing communications infrastructure. Because of the potential for shared infrastructure and the unprecedented economic risks, some telecommunications companies have already begun trialing QKD technologies for financial communications and messaging to test their readiness and security.

Steve Silberstein, CEO of FS-ISAC, gave an overview of financial communications and messaging and discussed current and projected security challenges that quantum solutions can address. He argued that the biggest challenge in financial services is the individual security of customers, and the most at-risk financial institutions are the smaller, less established, less regulated organizations. He believes that quantum solutions, like QKD, will add important layers of security for financial messaging but should not replace baseline practices that are not always commonly adopted across institutions and users, such as strong passwords and multifactor authentication.

Peter Bordow, managing director and PQC/Quantum Systems & Emerging Technologies Leader for Cybersecurity at Wells Fargo, detailed the risk landscape and potential mitigation strategies for PQC. He reported that large amounts of encrypted data are being harvested currently with the intention of decrypting the data once quantum technologies make it feasible to do so. He also emphasized the importance of considering data longevity and type (in motion, at rest, and in use) when conducting risk assessments for potentially at-risk data. Bordow then shared the PQC solution stack used by Wells Fargo, which encourages greater randomness and therefore better security. He also discussed the possibility that quantum technologies will make it impossible to secure data and communications using mathematical algorithms, and projected that data will eventually need to be secured using physics.

Following the presentations, workshop participants were divided into groups that were balanced among attendees from the financial industry, the quantum technology industry, and academic and government representatives.

Value Chain Matrix: A Bidirectional Flow

The primary tool to guide conversations during the ideation session was a secured financial messaging value chain matrix (shown below).

The two columns on the left describe at-risk delivery channels that can support or benefit from quantum-secured financial messaging: customers, merchants, financial, operations. This organizational structure was not intended to restrict thought but rather to provide participants with starting points to think of specific use cases that could benefit from quantum-secured financial messaging. The delivery channels did not necessarily have to be considered independent of each other; attendees were encouraged to think about how the categories interact and which processes and operations touch multiple delivery channels.

The top of the matrix shows the categories of quantum security approaches: quantum communications (e.g., QKD protocol), post-quantum cryptography (PQC), symmetric pre-shared keys, and a combination of approaches (e.g., QKD and PQC).

Quantum Security

Risk Factors - Delivery Channels		Quantum Communications Type (ex. QKD protocol)			Hybrid	PQC	Symmetric	Other
		Prepare & Measure (bb84)	Entangled (bbm92)	Continuous Variable (GG02)	PQC + QKD + QRNG	Asymmetric (ex. Crystals)	Pre-shared key, Manual seed	
Customers	**Online presence (customer)**							
	Mobile presence							
	Automated Teller Machines (ATM) (Operation)							
	Issue debit or credit cards							
	Prepaid cards							
	Person-to-person payments (P2P)							
	Originating automated clearing house (ACH) payments							
Merchants	Merchant remote deposit capture (RDC)							
	Merchant acquirer (sponsor merchants or card processor activity into the payment system)							
Financial	Originating wholesale payments (e.g., Clearing House Interbank Payments System [CHIPS])							
	Wire transfers							
	Global remittances							
	Treasury services and clients							
	Trust services							
	Act as a correspondent bank (Interbank transfers)							
Operations	Host IT services for other organizations (either through joint systems or administrative support)							
Other								

Workshop Process: Idea Generator

The workshop was designed to create as many ideas as possible up front, methodically select ideas that the participants considered the most important, and develop the ideas into meaningful and actionable concepts.

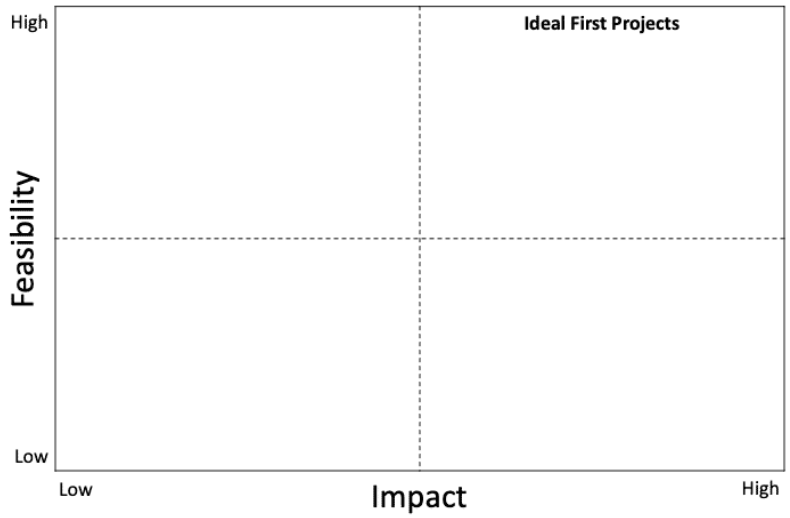
Brainstorm, analysis, selection

Workshop participants were assigned to small groups for a 35-minute ideation session. First they individually generated ideas in a 15-minute brainstorm and placed their ideas on the value chain matrix under the delivery channel and technological approach they felt was most applicable. The groups then took 15 minutes to discuss the generated ideas, and finally 5 minutes to vote for the ideas they thought had the most potential. To indicate their vote, participants were given three sticky dots to put on the ideas on the value matrix; they could put all their dots on one idea or split them across ideas. Visualizing the votes helped the group members prioritize choices together and make decisions at the end of a work session with minimal effort.

The groups came up with 60 ideas. The ideas were well distributed across the grid areas, but most ideas focused on communications and messaging between financial institutions and between financial institutions and customers. Each group then determined the two or three top ideas based on the ones with the most dots. This culminated in nine top use cases across all groups, after some consolidation of like ideas.

A flexible rating system to promote expansive thinking

The top use case ideas from each group where evaluated by the collective group. Through a facilitated discussion, the workshop participants ranked the nine top ideas based on their impact and feasibility in comparison with each other. Factors influencing *why* participants thought one idea was more feasible or impactful than another were not necessarily apparent during the discussions.



Concept Posters: How to Execute

The participants then focused on the five concepts that ranked the highest on impact and feasibility to develop them as concepts in the direction they felt best. The concept posters included a description of the concept, how it works, the problem space it occupies, key features, personae affected by the concept (e.g., network providers, infrastructure owners), and key metrics and outcomes to measure success. The posters also identified potential team members and suggested a timeline to complete the project.

Concept Poster & Collaboration Plan

Concept Name	Description
Persona	
How it works	Features
Problem Space	Success Metrics/Outcomes

Team Members:

Timeline:

	Start	_	_	_	_	_	_	_	Finish
Research									
Solve									
Develop									

Appendix B: Quantum Security Use Cases for Financial Services

This table lists all 60 ideas developed by the workshop participants regardless of the opinion of the group. The security approach and delivery channel noted for each is as the individual participants assigned them as the primary topic they wished to explore. Ideas have been only lightly edited.

Idea	Proposed Security Approach	Delivery Channel
Email negotiations; social media with post-quantum techniques	Combined	Customers
Mobile phone communications, for financial protections with post-quantum techniques	Combined	Customers
PQC as authentication for point-to-point QKD communications	Combined	Customers
Entanglement-based QKD + PQC for end-of-day settlements	Combined	Financial
Global remittances using post-quantum remediation	Combined	Financial
Trust services using quantum authentication	Combined	Financial
Interbank transfers using point-to-point communications with pre-shared keys and QKD	QKD	Financial
Central management, ownership, and operations of QKD infrastructure for financial transactions between partners	QKD	Operations
Data center backbone using QKD	QKD	Operations
Atomic power generation control to prevent financial network outages with QKD	QKD	Other
Pharmaceuticals purchase verification and fraud prevention with QKD	QKD	Other
Secure leader election for increased objectivity in financial processes with QKD	QKD	Other
Quantum byzantine agreement for blockchain using QKD to resist failures	QKD	Other
Quantum magnetometers for detecting insider trading fraud	Other	Operations
Secure quantum communications in remote locations during times of national emergency, resilient from active intercepts	Other	Other

Idea	Proposed Security Approach	Delivery Channel
Drone logistics communications to reduce fraud and decrease insurance liability with post-quantum techniques	Combined	Other
Peer-to-peer (P2P)/business-to-business (B2B) transactions validated by entanglement (Bell test) using QKD	QKD	Customers
PQC efficiently added to cryptocurrencies, ideally through soft forks	PQC	Customers
Leverage PQC for connections to customers and identity providers	PQC	Customers
Protect infrastructure communications by enabling secure connections with QKD (+ PQC) to protected backend	Combined	Customers
Quantum random number generation (QRNG) for creating unique transaction session keys	Combined	Financial
Bank-to-bank transfer protected by QKD, extended by PKK for network defense	QKD	Financial
Enable out-of-band key services (QKD/PKK) to protect against 3rd-party risk through cloud providers	QKD	Operations
End-to-end post-quantum protections for financial networks using defense-in-depth using PQC and QKD	Combined	Customers
EMV; credit cards, debit cards; payment tokenization; PQC-based authorization	PQC	Customers
Encapsulate older technology with PQC to upgrade and extend security	PQC	Customers
Leverage satellites and quantum memory to extend quantum networks for financial transactions	QKD	Merchants
Increase virtual network security by leveraging PQC for authentication and QKD for secret sharing	Combined	Financial
Enhance SWIFT with post-quantum techniques	Combined	Financial
Increase the limited range of QKD for larger regional transfer networks	QKD	Financial
Network-level threat detection with QKD for critical financial messages	QKD	Operations
Increase ecosystem engagement and investment by educating government and society about QKD and PQC to encourage adoption	Other	Other
Leverage QKD as a nonrepudiation technology for consumers	QKD	Customers

Idea	Proposed Security Approach	Delivery Channel
Enable PQC and QKD solutions for critical infrastructure including Fedwire and Fedwire/CHIPS refurbishment	Combined	Financial
Benchmark PQC and QKD to understand their impact on financial transaction SLAs	Combined	Other
Leverage point-to-point QKD instead of quantum key management for multimode QKD implementation to enable financial messaging	QKD	Other
Q-auction secure bidding	QKD	Other
Conduct cost-benefit analysis of QKD to confirm implementation viability for messaging and transactions	QKD	Customers
Increase ATM and POS security with low-cost QKD when viable	QKD	Customers
Leverage PQC for IoT wireless authorized for transactions and purchasing	PQC	Customers
Evaluate where QRNG can provide advantages in entropy-starved systems	Combined	Customers
Use PQC for authentication in P2P payments	PQC	Customers
Embed BB84 QKD in telecom backbones where optical connectivity is available	QKD	Financial
Update internal high-value networks with QKD for increased messaging security	QKD	Financial
Leverage QKD for key services for high-value banking partners	QKD	Financial
Enhance systems of record with QKD-based clock synchronization through entangled quantum networks and atomic clocks	Combined	Other
Enhance POS systems with PQC to safeguard consumer data and purchase records	PQC	Customers
Increase ATM endpoint security with PQC, specifically for reduced-cost ATM key loading	PQC	Customers
Add PQC to mobile banking authentication and multifactor for customers	PQC	Customers
Add PQC to online banking for browser connections	PQC	Customers
Combine PQC and PUF (physically unclonable function) technologies for IoT devices	Other	Customers
Add QKD for intercontinental transactions	QKD	Financial
Add QKD to mainframe systems which are connected to distributed networks	QKD	Financial

Idea	Proposed Security Approach	Delivery Channel
Enhance POS systems connected to credit card networks with PQC for token transaction fields	PQC	Financial
Combine PQC and PUF (physically unclonable function) technologies for IoT devices	Symmetric	Financial
Leverage CV-QKD for longer-distance financial services messaging systems and for shorter optical links	QKD	Operations
Create QKD networks with BBM92 for critical messaging backbones such as data center to large campus; data center to data center (replication, data transfer); fiber backbone, data center to bank, and Fed to bank	QKD	Other
Increase security at MPC data centers and their interconnect with post-quantum technologies	Combined	Other
Leverage post-quantum pre-shared keys (PPKs) for IOT devices to increase smart home transaction security	Symmetric	Other
Leverage post-quantum pre-shared keys (PPKs for long-distance complex to data center interconnects	Symmetric	Other

Appendix C: Workshop Attendees

Thank you to the following workshop participants for sharing their time and perspectives.

Khushi Advani, Deloitte

Matthew Aleksich, Aleksco

Clark Alexander, ODE L3C

Omar Amer, JP Morgan

Peter Bordow, Wells Fargo

John Buselli, IBM

Nico Choksi, Qunnect

Eric Clemons, National Security Agency

Michael Cubeddu, Aliro Quantum

Whitfield Diffie

Carl Dukatz, Accenture

Jon Felbinger, QED-C

John Geraci, Accenture

Muhammad Ghani, DHS Cybersecurity and Infrastructure Security Agency

Jacob Gottlieb, SRI

Sandra Guasch, SandboxAQ

Victoria Hazoglou, Accenture

Reza Hedayati, NubisAI

Masashi Hirose, Nanofiber Quantum Technologies, Inc.

Young Kim, Maxxen Group

Daniel Koch, Air Force Research Laboratory

Claire Lecornu, SRI

Xinhua Ling, Amazon Web Services

Corey McClelland, Qubitekk

Alan Migdall, National Institute of Standards and Technology

Shay Moore, SRI

Michele Mosca, evolutionQ

Mehdi Namazi, Qunnect

Tommaso Occhipinti, QTI s.r.l.

Simon Patkovic, ID Quantique

Marco Pistoia, JP Morgan

John Prisco, Safe Quantum, Inc.

Emma Rose, SRI

Ashish Sardesai, Verizon

Tsuyoshi Sasano, Toshiba International Corporation

Benjamin Shapiro, Deloitte

Keeper Sharkey, ODE L3C

Rajeev Sharma, Vanguard

Steven Silberstein, FS-ISAC

Manish Singh, memQ Inc.

Roland Stephen, SRI

Peter Tsahalis, Wells Fargo

Brandon van Hoff, SRI

Tom Walsh, Federal Bureau of Investigation

Geoff Warner, MITRE

Brian Williams, Oak Ridge National Laboratory

Annie Wyhof, SRI


QED·C