Aliro™

A Future-Proof Cybersecurity Posture

Aliro

www.alirotech.com

A Future-Proof Cybersecurity Posture

Summary

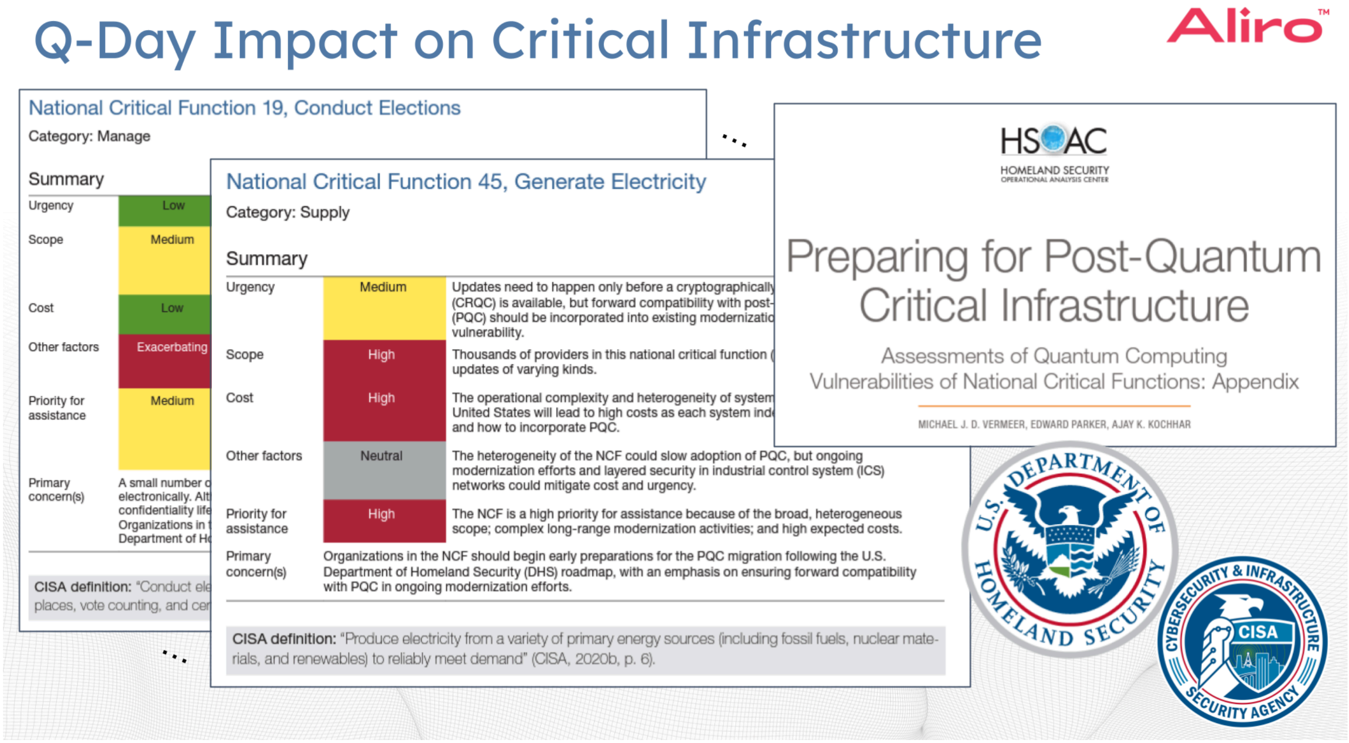
The advent of quantum computing is poised to revolutionize many aspects of technology, but it also brings significant challenges to the world of cybersecurity. As quantum computers become more powerful, traditional cryptographic systems like RSA and Diffie-Hellman are at risk of being rendered obsolete. In this white paper, we aim to provide a clear understanding of the practical considerations involved in implementing a hybrid classical/quantum security architecture, including hardware maturity, market readiness, and regulatory compliance. As we move further into the quantum era, it is imperative for organizations to begin their journey toward a quantum-safe future. This white paper offers an approach for ensuring that your organization's security posture remains resilient, adaptable, and future-proof.

In the rapidly evolving landscape of cybersecurity, the threat posed by quantum computing necessitates a robust and future-proof approach to protecting sensitive information. We propose a hybrid architecture, combining Post-Quantum Cryptography (PQC) with Quantum Secure Communication (QSC) to provide comprehensive defense against both current and future cybersecurity threats. We also compare the 3 most relevant strategies for securing networks against quantum attacks (PQC, QKD, and QSC), unpack the challenges of integrating these emerging technologies, and show how this hybrid approach offers a path to achieving a resilient and secure cybersecurity posture. Government agencies, financial institutions, and enterprises handling sensitive data will benefit from these essential insights into building a security architecture that can protect data today from the threats of tomorrow.

The Threat Against Public Key Crypto Systems

Q-Day is defined as the day when a quantum computer will be able to crack algorithms, such as RSA and Diffie-Hellman, that we rely on for public key cryptography. This quote from a report by the Department of Homeland Security gets to the core of Q-Day and the problem with legacy crypto systems: “The security of the U.S. information and communication infrastructure is currently predicated on the assumption that it is impractically hard for computers to solve certain mathematical problems, such as integer factorization and finding the discrete logarithm of elliptic curves.”

Digital security in the US and abroad, all of the existing communication infrastructure, is currently predicated on this assumption that certain math problems are very hard to crack, and specifically math problems like integer factorization and the discrete logarithm problem for elliptic curves. These are math problems that were presumed to be very hard for any computer to crack, and that's what security in today's systems relies upon – but that is no longer an assumption we can afford to make. These math problems are now vulnerable to attack by quantum computers. This is a big problem that impacts all of our communication systems, but perhaps more urgently, it impacts our critical infrastructure. A report put out by the Department of Homeland Security in collaboration with the RAND Corporation and CISA assessed dozens of these National Critical Functions. These are important digital systems, such as the ability to generate and distribute electricity and the ability to conduct trustworthy elections.



Q-Day Impact on Critical Infrastructure

National Critical Function 19, Conduct Elections

Category: Manage

Summary

Urgency	Low
Scope	Medium
Cost	Low
Other factors	Exacerbating
Priority for assistance	Medium
Primary concern(s)	A small number o electronically. Alt confidentiality life Organizations in t Department of H

CISA definition: "Conduct ele
places, vote counting, and cer

National Critical Function 45, Generate Electricity

Category: Supply

Summary

Urgency	Medium	Updates need to happen only before a cryptographically (CRQC) is available, but forward compatibility with post- (PQC) should be incorporated into existing modernizatio vulnerability.
Scope	High	Thousands of providers in this national critical function (updates of varying kinds.
Cost	High	The operational complexity and heterogeneity of system United States will lead to high costs as each system inde and how to incorporate PQC.
Other factors	Neutral	The heterogeneity of the NCF could slow adoption of PQC, but ongoing modernization efforts and layered security in industrial control system (ICS) networks could mitigate cost and urgency.
Priority for assistance	High	The NCF is a high priority for assistance because of the broad, heterogeneous scope; complex long-range modernization activities; and high expected costs.
Primary concern(s)	Organizations in the NCF should begin early preparations for the PQC migration following the U.S. Department of Homeland Security (DHS) roadmap, with an emphasis on ensuring forward compatibility with PQC in ongoing modernization efforts.	

CISA definition: "Produce electricity from a variety of primary energy sources (including fossil fuels, nuclear materials, and renewables) to reliably meet demand" (CISA, 2020b, p. 6).

HSOAC
HOMELAND SECURITY
OPERATIONAL ANALYSIS CENTER

Preparing for Post-Quantum Critical Infrastructure

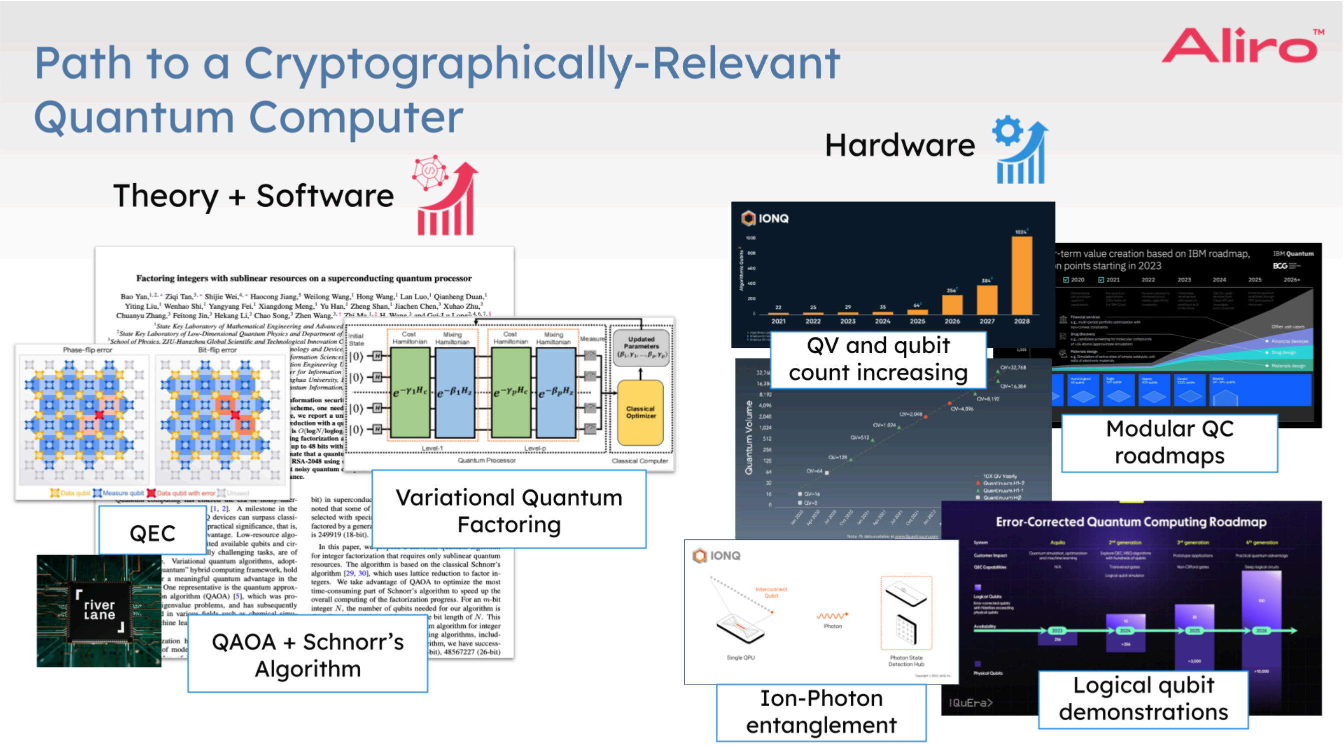
Assessments of Quantum Computing Vulnerabilities of National Critical Functions: Appendix

MICHAEL J. D. VERMEER, EDWARD PARKER, AJAY K. KOCHHAR

Each of the critical functions identified in the report have different urgencies, and different scopes of migration. In addition, the report highlights which parts of our digital infrastructure we should prioritize in terms of migration to a quantum-safe solution. It is imperative that we prepare and begin the migration to a quantum-safe critical infrastructure to maintain these systems.

A Timeline to Q-Day

At some point, a quantum computer will break the existing crypto systems that we depend on to keep our data private and our infrastructure secure. Only a cryptographically relevant quantum computer (CRQC), a quantum computer that is large enough, fast enough, and with high enough fidelity, will be able to crack algorithms like RSA. When will a CRQC come online? The timeline according to experts in the field varies from a few years to decades from now. No one really knows when, but the estimate is continually shrinking because with every advancement in both theory and hardware, a CRQC becomes more attainable.


Path to a Cryptographically-Relevant Quantum Computer

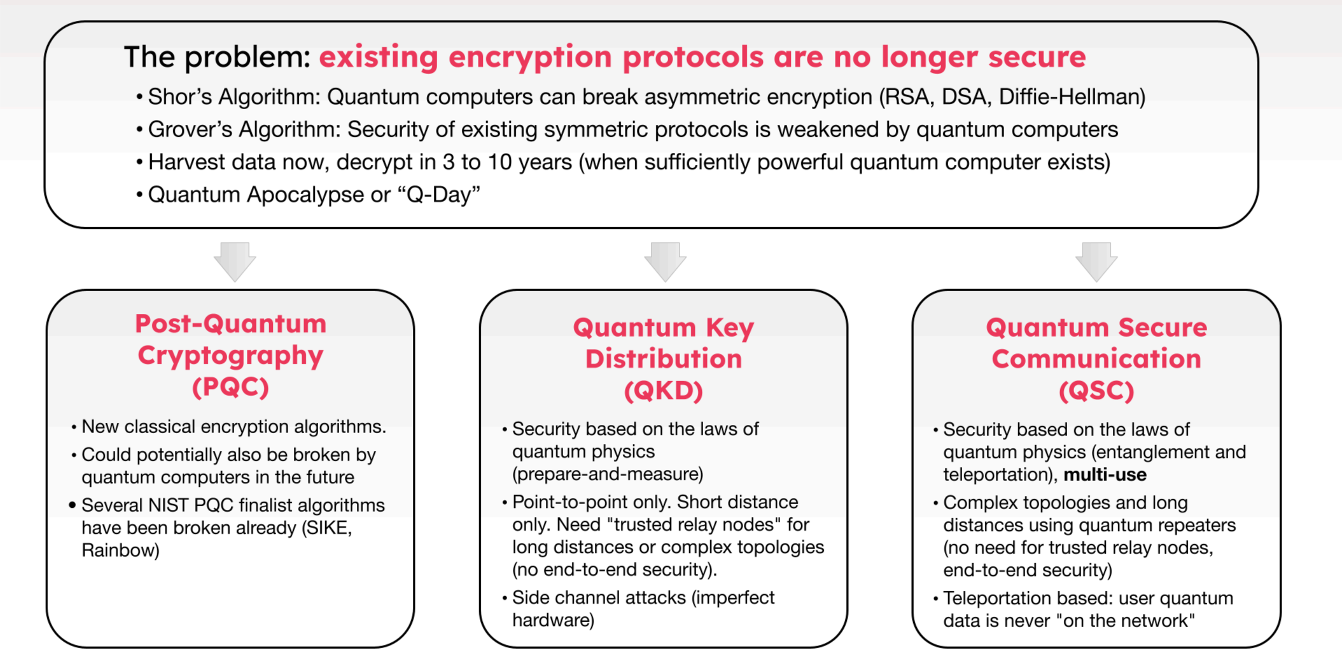
Aliro™
Theory + Software
Hardware
QEC
Variational Quantum Factoring
QAOA + Schnorr's Algorithm
QV and qubit count increasing
Modular QC roadmaps
Ion-Photon entanglement
Logical qubit demonstrations
Factoring integers with sublinear resources on a superconducting quantum processor
IONQ
Error-Corrected Quantum Computing Roadmap
river lane

Some recent advancements that are bringing us closer to a CRQC include:

- Lower Physical Qubit Requirements. Recent advancements in quantum algorithms have significantly reduced the number of physical qubits required to run Shor's algorithm, which is essential for breaking asymmetric encryption and public key cryptography

schemes. Previously, it was believed that millions of qubits would be necessary, but these advancements have lowered that threshold significantly.
- More Efficient Error-Correcting Codes. The development of more efficient error-correcting codes is crucial for maintaining the fidelity of qubits, which is essential for the reliable operation of quantum computers.
- Development of Variational Algorithms. Algorithms such as Variational Quantum Factoring (VQF) allow quantum and classical computers to work together. These algorithms enable operations like factoring large integers into primes, further reducing the requirements for a CRQC in terms of qubit number, fidelity, and overall resources.
- Advancements in Quantum Computing Hardware. Periodic updates and innovations in quantum computing hardware by vendors and manufacturers have accelerated progress. These include the move towards modular architectures, where multiple processors work together, resembling the evolution seen in high-performance computing. This requires the development of interconnects between processors, such as ion-photon entanglement.
- Improvement in Qubit Quality. Ongoing improvements in qubit quality, such as increased quantum volume and qubit count, and increased gate fidelities, are essential for advancing towards CRQC.
- Logical Qubits and Fault-Tolerant Quantum Computing. Demonstrations of logical qubits and small-scale fault-tolerant quantum computers are promising steps toward achieving utility-scale quantum computing, which is critical for the development of a CRQC.

These factors collectively contribute to the accelerated development of a CRQC, bringing us closer to the capability of breaking current cryptographic systems. **When it comes to cybersecurity, a lens of risk is necessary. From a risk standpoint, if there is a 10% chance that a CRQC will be available in the next five years, is that level of risk something an organization is willing to accept?**



The problem: **existing encryption protocols are no longer secure**

- Shor’s Algorithm: Quantum computers can break asymmetric encryption (RSA, DSA, Diffie-Hellman)
- Grover’s Algorithm: Security of existing symmetric protocols is weakened by quantum computers
- Harvest data now, decrypt in 3 to 10 years (when sufficiently powerful quantum computer exists)
- Quantum Apocalypse or “Q-Day”

Post-Quantum Cryptography (PQC)

- New classical encryption algorithms.
- Could potentially also be broken by quantum computers in the future
- Several NIST PQC finalist algorithms have been broken already (SIKE, Rainbow)

Quantum Key Distribution (QKD)

- Security based on the laws of quantum physics (prepare-and-measure)
- Point-to-point only. Short distance only. Need "trusted relay nodes" for long distances or complex topologies (no end-to-end security).
- Side channel attacks (imperfect hardware)

Quantum Secure Communication (QSC)

- Security based on the laws of quantum physics (entanglement and teleportation), **multi-use**
- Complex topologies and long distances using quantum repeaters (no need for trusted relay nodes, end-to-end security)
- Teleportation based: user quantum data is never "on the network"

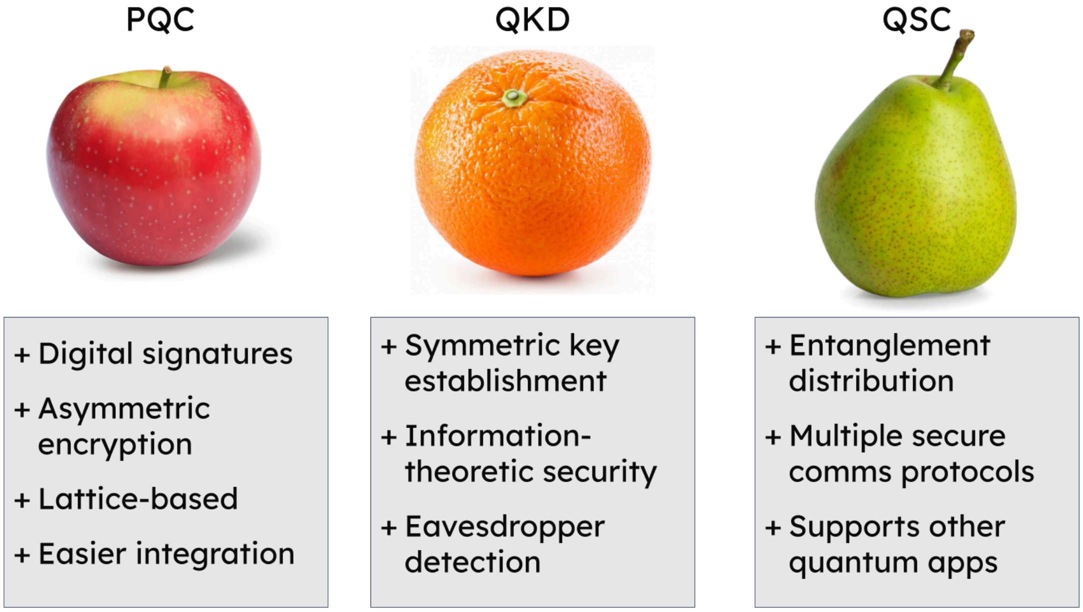
The problem we’re confronting is clear: existing encryption protocols are no longer secure. Asymmetric algorithms like RSA, DSA, and Diffie-Hellman can all be cracked by Shor's algorithm on a quantum computer. So what solutions are there to protecting data from quantum attacks like Shor’s algorithm? There are three primary families of solutions out there:

1. Post Quantum Cryptography (PQC). PQC is an encryption solution that replaces discrete log and integer factorization. PQC uses new math problems. This is a purely classical technology, but these new math problems employed by PQC are intended to be resistant to attacks by supercomputers, classical computers, as well as quantum computers. The National Institute of Standards and Technology (NIST) is responsible for standardizing these new algorithms in the United States, and those standards were released in August of 2024.
2. Quantum Key Distribution (QKD). QKD relies on quantum physics for security. Quantum signals are used to communicate between two nodes on a network and establish a shared symmetric key.
3. Quantum Secure Communication (QSC). Quantum Secure Communication also leverages quantum physics for security. However, this solution relies on quantum entanglement, which can be used for a variety of cryptosystems, as well as a wide variety of other applications.

Which is better: PQC, QKD, or QSC?

Aliro is frequently asked this question: when it comes to solutions to protect against Q-Day, what is a better solution? In some ways this is a fair question, and in other ways it's not a level comparison. It is an objective question to some degree, but it is also rather subjective and dependent on an organization's specific security needs and the applications it wants to enable on the network. There are certain protections and capabilities these technologies can provide in a crypto system that other solutions cannot provide.

Comparing PQC, QKD, and Quantum Secure Communications (QSC)



PQC	QKD	QSC
+ Digital signatures + Asymmetric encryption + Lattice-based + Easier integration	+ Symmetric key establishment + Information-theoretic security + Eavesdropper detection	+ Entanglement distribution + Multiple secure comms protocols + Supports other quantum apps

When comparing Post-Quantum Cryptography (PQC), Quantum Key Distribution (QKD), and Quantum Secure Communication (QSC), it's important to recognize that each technology offers distinct advantages that cater to different security needs. PQC, as a classical technology, is more straightforward to integrate into existing systems, making it an attractive option for organizations looking to enhance their security with minimal disruption. On the other hand, QKD and QSC offer the unparalleled advantage of information-theoretic security, which remains robust regardless of advancements in computational power. These quantum-based solutions also provide unique capabilities like eavesdropper detection, a critical feature that identifies any attempt at interception, ensuring the highest levels of communication security. Ultimately, the choice between these technologies hinges on an organization's specific requirements, including the nature of the threats they face, the sensitivity of their data, and the complexity of their network infrastructure.

Given these differing strengths, the decision between PQC, QKD, and QSC should be guided by the specific security priorities and operational contexts of an organization. Let's take a closer look at each of the options.

PQC

PQC employs algorithms based on lattice problems. These lattice-based algorithms have been well-studied, and they can be used to establish public and private key pairs on a network. These lattice problems are presumed to be very difficult for both classical computers as well as quantum computers to crack. That being said, the security of PQC is still a conjecture. There is no provable guarantee that a future computational system would not be able to crack lattice-based problems. Using PQC makes it possible to retain a lot of the cryptographic notions and primitives that are already in place today, such as digital signatures, certificates, and trusted authorities. These are capacities that PQC can provide to your crypto system that QKD and QSC may not provide.

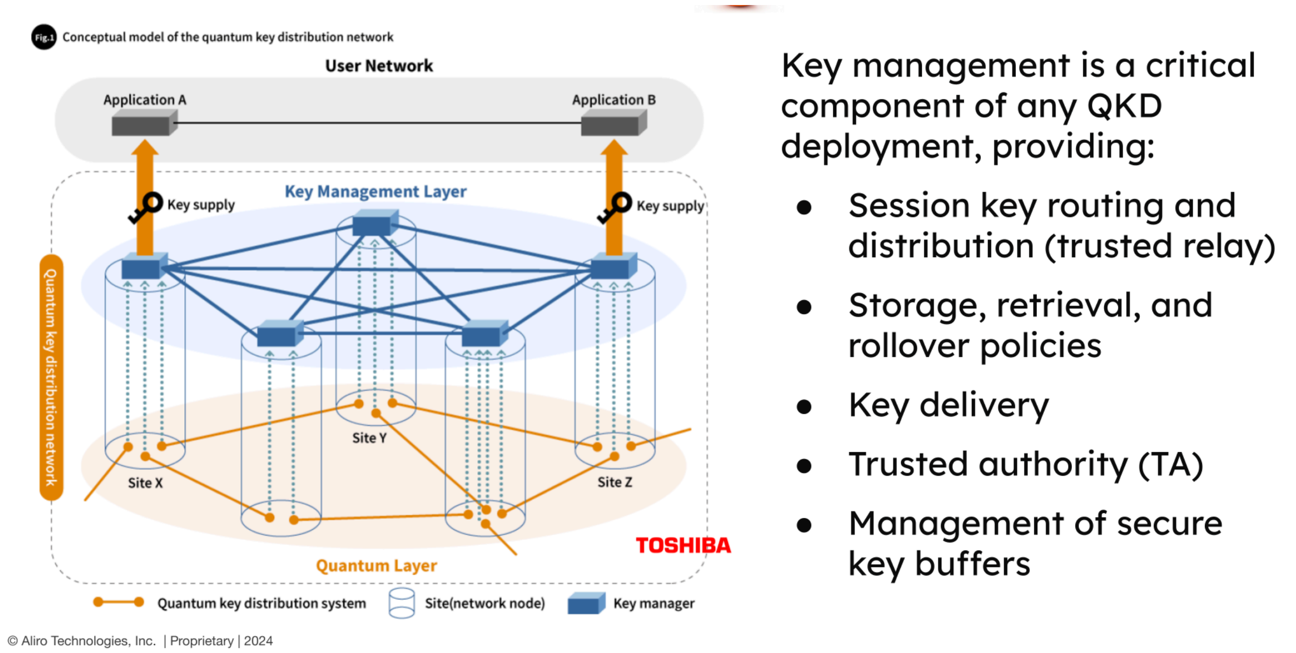
Although there exist multiple classes of candidate algorithms for PQC, most are based on the conjectured difficulty of **lattice problems** related to SVP, CVP, and LWE.

- SVP: Shortest Vector Problem–find the vector in a lattice with smallest magnitude
- CVP: Closest Vector Problem–find the lattice vector closest to a given vector
- LWE: Learning With Errors–solve a linear system with added noise
- The public key is derived from the lattice, the private key is related to the problem solution

QKD

QKD is a technology that has been theorized for decades, with the first protocol dating back to the 1980s. QKD uses single photons traversing a quantum channel to establish a symmetric cryptographic key between two directly connected parties in a point-to-point system. QKD is information-theoretically secure, so any eavesdropper or man-in-the-middle, regardless of their computational capabilities, will not be able to crack the key. The technology has been theorized for many decades, and has been implemented and deployed in networking systems for a little over 20 years now. There are robust commercial products and a market for QKD being deployed across the globe.

QKD does have some drawbacks when it comes to scalability. While very effective for point-to-point systems between just two parties, scaling QKD to a more complex network topology requires what are called trusted relay nodes. Trusted relay nodes are responsible for relaying the cryptographic key established on one link to other parties in the network. To do this, the network must trust that relay functionality. This highlights the importance of the Key Management layer in QKD networks today and in QKD networks of the future, especially as upgrades and new deployments are implemented. The Key Management layer is responsible for functions like session key routing and distribution, and policies on managing crypto keys in the network. These policies might include how long to store the crypto keys, how often crypto keys roll over, and any other storage or retrieval policies fall to this key management layer. QKD also suffers from photon loss. As photons travel through optical fiber, they are susceptible to loss, and the probability of successful transmission decreases exponentially with distance.



Key management is a critical component of any QKD deployment, providing:

- Session key routing and distribution (trusted relay)
- Storage, retrieval, and rollover policies
- Key delivery
- Trusted authority (TA)
- Management of secure key buffers

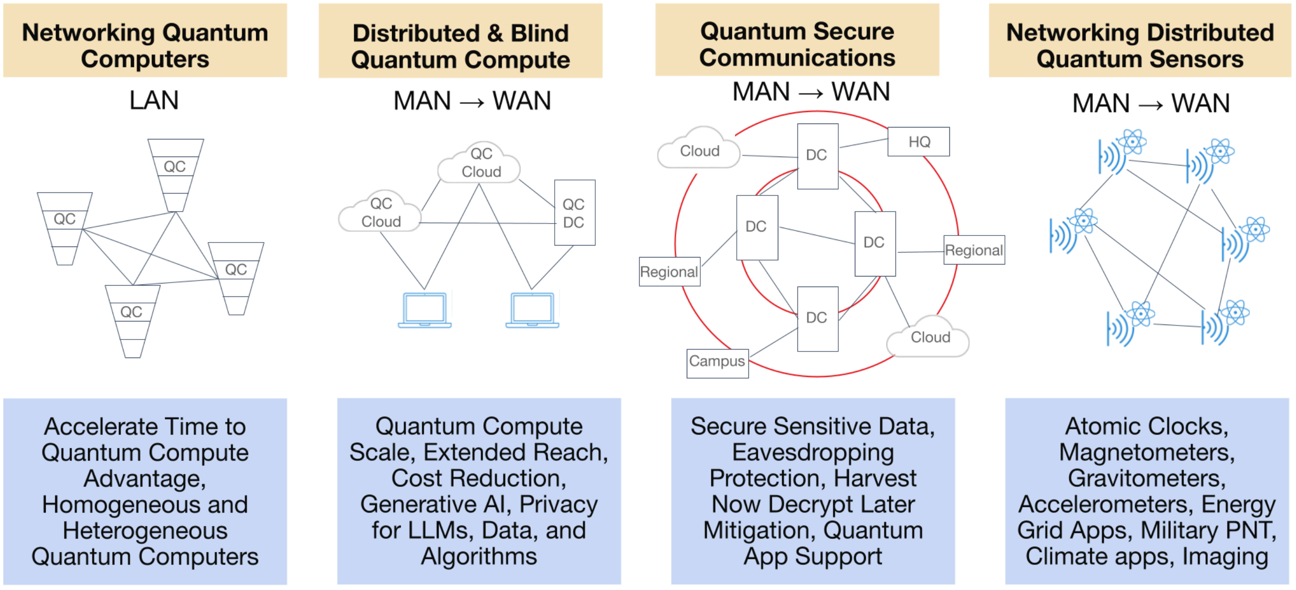
© Aliro Technologies, Inc. | Proprietary | 2024

QSC

Quantum Secure Communication provides arguably the most advanced level of security of these three solutions because QSC uses entanglement. Entanglement enables an entire suite of key distribution protocols beyond the prepare-and-measure BB84-style QKD protocols. Entanglement enables the next generation of key distribution protocols: E91, BBM92, and Device Independent QKD all rely on establishing end-to-end entanglement.

Using entanglement eliminates the need for trusted relay nodes, which introduce insider security risks. Eliminating trust in specific nodes or certain actors in the network is a more secure approach. In addition to eliminating risk, entanglement-based quantum networks are multi-use platforms. Where QKD networks can only enable the distribution of key material, entanglement-based quantum networks can also be used for other applications, enabling other cryptographic use cases beyond symmetric keys, including Quantum Secure Direct Communication (QSDC) protocols. QSDC protocols use entangled photons to encode sensitive data in the photons themselves.

Entanglement also enables protocols such as quantum teleportation, where information can be received at a destination on the network without the need to send the information on the network itself.


Networking Quantum Computers
LAN
QC
QC
QC
QC
Accelerate Time to Quantum Compute Advantage, Homogeneous and Heterogeneous Quantum Computers
Distributed & Blind Quantum Compute
MAN → WAN
QC Cloud
QC Cloud
QC DC
Quantum Compute Scale, Extended Reach, Cost Reduction, Generative AI, Privacy for LLMs, Data, and Algorithms
Quantum Secure Communications
MAN → WAN
Cloud
DC
HQ
DC
DC
Regional
Regional
DC
Cloud
Campus
Secure Sensitive Data, Eavesdropping Protection, Harvest Now Decrypt Later Mitigation, Quantum App Support
Networking Distributed Quantum Sensors
MAN → WAN
Atomic Clocks, Magnetometers, Gravitometers, Accelerometers, Energy Grid Apps, Military PNT, Climate apps, Imaging

Entanglement-based quantum networks enable QSC, but they can also simultaneously enable a variety of applications in addition to the security applications. This includes networking quantum computers together to scale up quantum computing power, enable distributed quantum computing, and facilitate blind quantum computing.

There are some challenges to distributing entanglement with quantum networks. Currently, there are low entanglement generation rates, which equates to low secret key rates. The reason for this is quantum protocols are stochastic, which impacts how efficiently entanglement can be distributed. Fidelity is also a limiting factor in entanglement-based quantum networks. Fidelity, the quality and strength of the entanglement being generated, decays over time as it's interacting with the environment.

Attack Profiles for PQC, QKD, and QSC

The security offered by PQC, QKD, and QSC can be divided into two categories: theoretical security and implementation security. Theoretical security, or “protocol security,” refers to the protection of a system against adversaries whose capabilities adhere to a certain set of assumptions. Using these mathematical frameworks, cryptographic protocols can be proven to be mathematically secure against known attacks by the adversary. Implementation security, on the other hand, concerns the real-world deployment of these protocols, where factors such as hardware imperfections, side-channel attacks (i.e., any attacks not in scope of the security proof), and operational errors come into play.

For example, QKD protocols have been proven theoretically secure against any computational attack, including those from quantum computers. However, in practice, QKD systems have been shown to be vulnerable to side-channel attacks, where attackers exploit weaknesses in the hardware rather than the underlying protocol. Similarly, PQC algorithms, while theoretically resistant to quantum attacks, might still be compromised by advances in algorithmic theory or by implementation flaws such as electromagnetic interference or side-channel attacks.

The landscape of cryptographic attacks is continually evolving, driven by advances in quantum computing and cryptanalysis. As these technologies develop, the attack profiles for PQC, QKD, and QSC will also change. For instance, the advent of a powerful quantum computer would render RSA obsolete almost instantly, as it would be easily cracked by Shor's algorithm. In contrast, PQC might hold up longer but could still be vulnerable to future computational breakthroughs.

Understanding these evolving attack profiles underscores the need for a hybrid approach to cybersecurity. No single technology can provide complete protection against all potential threats. Instead, a combination of PQC, QKD, and QSC can create a layered defense, where the strengths of each technology compensate for the weaknesses of the others. This approach also allows for greater flexibility and adaptability, ensuring that as new threats emerge, organizations can adjust their security measures accordingly.

Practical Considerations: Hardware Maturity and Market Readiness

When considering the implementation of quantum-safe cryptographic systems, organizations must also weigh factors such as hardware maturity, market readiness, and cost. PQC, as a purely classical technology, has the advantage of easier integration with existing legacy systems, making it more scalable in the short term. However, as the technology matures, QKD and QSC will likely offer superior protection, especially in critical applications where security is paramount.

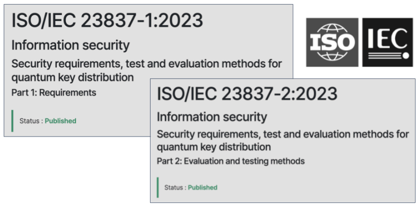
The development of quantum hardware, such as quantum repeaters and equipping satellites with quantum components, will play a crucial role in extending the range and effectiveness of QSC. These advancements will lower the barriers to long-distance entanglement distribution and increase the scalability of these networks. Organizations must carefully consider the urgency of their migration to any system. Contributing factors in this decision are an organization’s needs and use cases for the network, the type of data traffic on the network, and the network architecture. These factors influence the urgency of the migration, the scope of migration, and how to prioritize implementation.

Side-Channel Attacks: A Shared Vulnerability

One of the most pressing challenges across all three technologies—PQC, QKD, and QSC—is the threat of side-channel attacks. These attacks target the physical implementation of cryptographic systems rather than the underlying algorithms, making them a significant concern for real-world security. For instance, a side-channel attack on a QKD system might involve shining a bright light into a photon detector to extract information, while a similar attack on a PQC system might exploit electromagnetic emissions to gain insights into the cryptographic process.

QKD Side-Channel Attacks

1. Vakhitov, Makarov, and Hjelme, **Large pulse attack** as a method of conventional optical eavesdropping in quantum cryptography, Journal of Modern Optics 48, 2001.
2. Makarov and Hjelme, **Faked states attack** on quantum cryptosystems, Journal of Modern Optics, vol. 52, 2005.
3. Ferenczi, Grangier, Grosshans, **Calibration Attack** and Defense in Continuous Variable Quantum Key Distribution, CLEO-IQEC, 2007.
4. Zhao, Fung, Qi, Chen, and Lo, Experimental demonstration of **time-shift attack** against practical quantum key distribution systems, Physical Review A vol. 78, 2008.
5. Scarani and Kurtsiefer, The black paper of quantum cryptography: Real implementation problems, Theoretical Computer Science (560) 2014.



ISO/IEC 23837-1:2023

Information security

Security requirements, test and evaluation methods for quantum key distribution

Part 1: Requirements

Status : Published

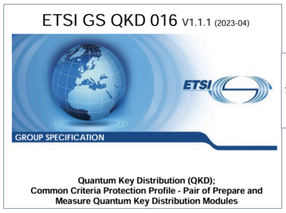
ISO/IEC 23837-2:2023

Information security

Security requirements, test and evaluation methods for quantum key distribution

Part 2: Evaluation and testing methods

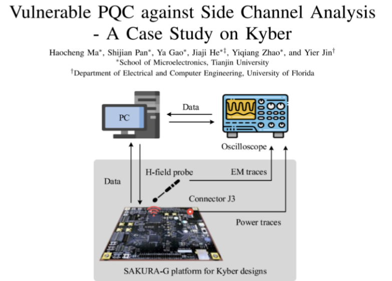
Status : Published



ETSI GS QKD 016 V1.1.1 (2023-04)

Quantum Key Distribution (QKD);
Common Criteria Protection Profile - Pair of Prepare and
Measure Quantum Key Distribution Modules

BSI



Vulnerable PQC against Side Channel Analysis - A Case Study on Kyber

Haocheng Ma*, Shijian Pan*, Ya Gao*, Jiaji He*‡, Yiqiang Zhao*, and Yier Jin†
*School of Microelectronics, Tianjin University
†Department of Electrical and Computer Engineering, University of Florida

Fig. 2: The overview of the experimental setup.

Quantum Algorithms for Lattice Problems

Yilei Chen, Tsinghua University, Shanghai Artificial Intelligence Laboratory, Shanghai Qi Zhi Institute

*not peer-reviewed

To mitigate these risks, ongoing research and standardization efforts are crucial. Organizations such as ISO, IEC, and ETSI are continuously updating protection profiles, security requirements, and evaluation methods to safeguard against side-channel attacks. By staying informed and implementing the latest security measures, organizations can enhance the implementation security of their crypto systems.

Hybrid Architectures: A Future-proof Cybersecurity Posture

The ideal future-proof approach to cybersecurity would provide:

- Layered defense-in-depth, where any adversary or attacker on the network would have to break multiple protocols and crypto systems in order to gain access to the cryptographic key or decrypt any data on the network.
- Diversified with math & physics, where security relies on both types of protection.
- Multiple use cases possible, such as enabling the creation of symmetric keys, use of digital signatures and certificates, and the ability to support applications beyond cybersecurity.
- A cryptographically agile strategy, capable of changing which cryptographic algorithms are employed and which attacks the network is protected from.

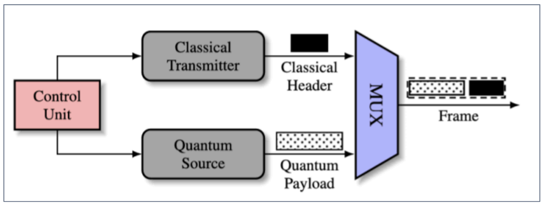
The crux of modern network security lies in not relying solely on any single technology or protocol. As we anticipate the quantum era, it's clear that a hybrid approach—combining Post-Quantum Cryptography (PQC) with Quantum Key Distribution (QKD) and / or Quantum Secure Communication (QSC)—is essential for comprehensive security. This is not a case of choosing between one technology or another; rather, it's about integrating these solutions to harness their collective strengths. This integration occurs across multiple layers of the network architecture: the physical layer, the cryptographic layer, the network architecture layer, and the application layer. Each layer offers unique intersection points where quantum and classical technologies can complement each other to create a robust, future-proof security system.

Physical Integration

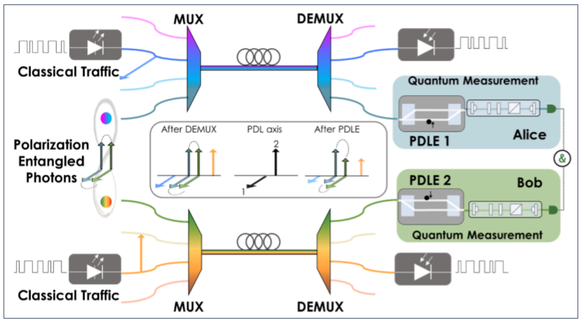
At the physical layer, where data transmission occurs, the intersection of quantum and classical signals can provide valuable cybersecurity benefits. For instance, when quantum and classical signals traverse the same channel, hybrid data packets can be employed. In these packets, classical headers guide the information, while quantum payloads ensure the security of the data. This integration at the physical layer enables advanced security features like eavesdropper detection, where any attempt at unauthorized interception can be immediately identified due to the perturbation of the quantum state.

Physical Layer Integrations

- Multiplexing (time, wavelength)
- Quantum components:
  - High-rate photon generation at telecom wavelength
  - Room temp
  - Compatible with OTN gear (e.g. optical cross-connects)
  - Atomic clocks?
- Hybrid data packet structures



DiAdamo, Stephen, et al. "Packet switching in quantum networks: A path to the quantum Internet." Physical Review Research 4.4 (2022): 043064.



Security

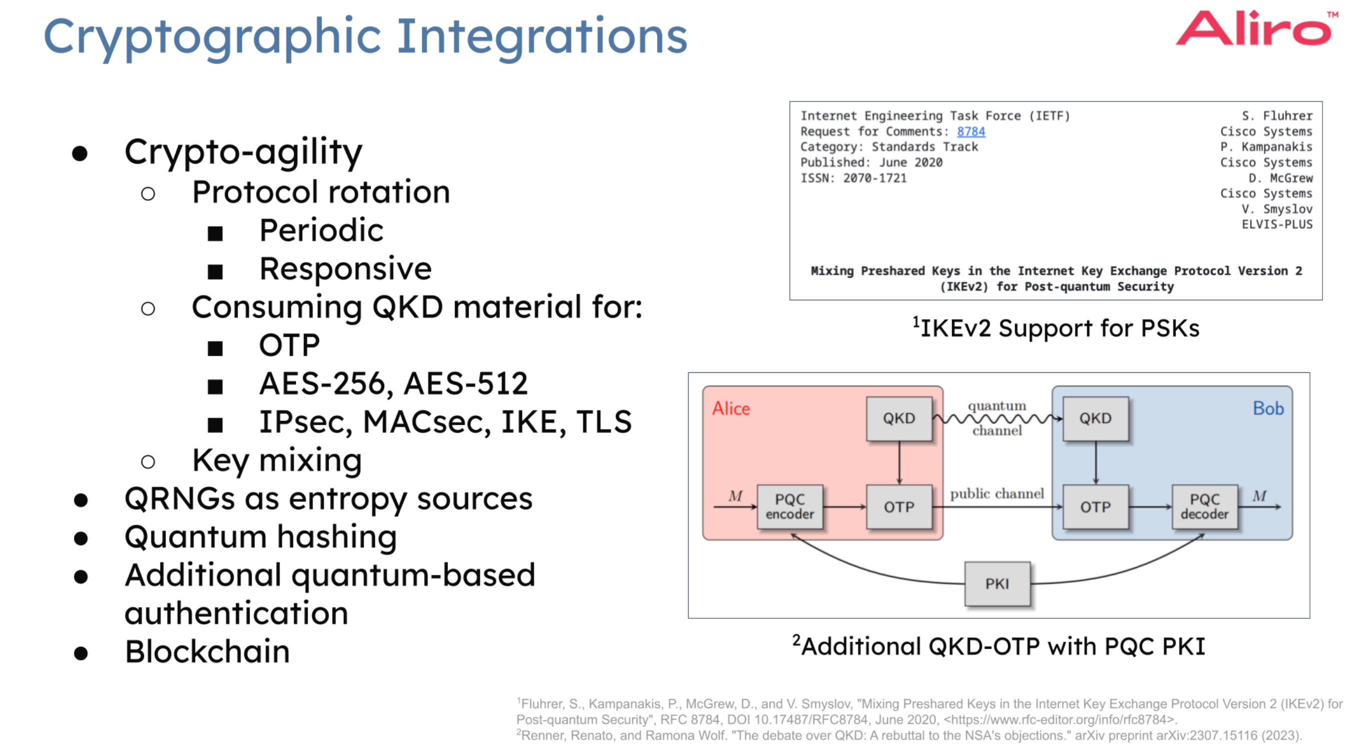
- Eavesdropper detection & fast mitigation
- Quantum sensors
- Quantum alarms
- Position verification

Lu, Hsuan-Hao, et al. "Procrustean entanglement concentration in quantum-classical networking." arXiv preprint arXiv:2401.01311 (2024).

Moreover, quantum signals can be utilized for fast mitigation of attacks on the link, and for applications like quantum sensors and quantum alarms, which provide additional layers of security by verifying the physical presence and location of network participants. For example, quantum signals can be used to confirm that "Alice" is where they claim to be, or that "Bob" is located where the network expects them to be. These capabilities are foundational to building a secure and resilient network infrastructure.

Cryptographic Integration

Moving to cryptographic integration, the focus shifts to the integration of PQC algorithms with methods like QKD and QSC. The interplay between these technologies is crucial for achieving crypto agility—a key requirement in a rapidly evolving threat landscape. Crypto agility refers to the ability to dynamically switch and rotate cryptographic protocols in response to emerging threats or changes in the network environment. This might involve periodic rotations of key establishment or distribution protocols, or even responsive adjustments based on real-time network state and detected attacks.



Cryptographic Integrations

Aliro™

- Crypto-agility
  - Protocol rotation
    - Periodic
    - Responsive
  - Consuming QKD material for:
    - OTP
    - AES-256, AES-512
    - IPsec, MACsec, IKE, TLS
  - Key mixing
- QRNGs as entropy sources
- Quantum hashing
- Additional quantum-based authentication
- Blockchain

```
Internet Engineering Task Force (IETF)                        S. Fluhrer
Request for Comments: 8784                                 Cisco Systems
Category: Standards Track                                  P. Kampanakis
Published: June 2020                                       Cisco Systems
ISSN: 2070-1721                                                D. McGrew
                                                           Cisco Systems
                                                              V. Smyslov
                                                              ELVIS-PLUS


   Mixing Preshared Keys in the Internet Key Exchange Protocol Version 2
                     (IKEv2) for Post-quantum Security
```

[1]IKEv2 Support for PSKs

[2]Additional QKD-OTP with PQC PKI

[1]Fluhrer, S., Kampanakis, P., McGrew, D., and V. Smyslov, "Mixing Preshared Keys in the Internet Key Exchange Protocol Version 2 (IKEv2) for Post-quantum Security", RFC 8784, DOI 10.17487/RFC8784, June 2020, <https://www.rfc-editor.org/info/rfc8784>.
[2]Renner, Renato, and Ramona Wolf. "The debate over QKD: A rebuttal to the NSA's objections." arXiv preprint arXiv:2307.15116 (2023).

At this layer, entanglement-based protocols can be used to generate symmetric cryptographic keys, which can then be consumed by various algorithms, such as AES-256 or AES-512. The integration points extend to other cryptographic methods, including one-time pads, IPsec, Macsec, IKE, and TLS, ensuring that the keys generated in entanglement-based quantum networks used for QSC can be effectively utilized across a wide range of security protocols. Additionally, the concept of key mixing—combining multiple sources of entropy, like those provided by quantum random number generators (QRNGs), and methods for key establishment—further enhances security by making it significantly more difficult for adversaries to compromise the cryptographic keys.

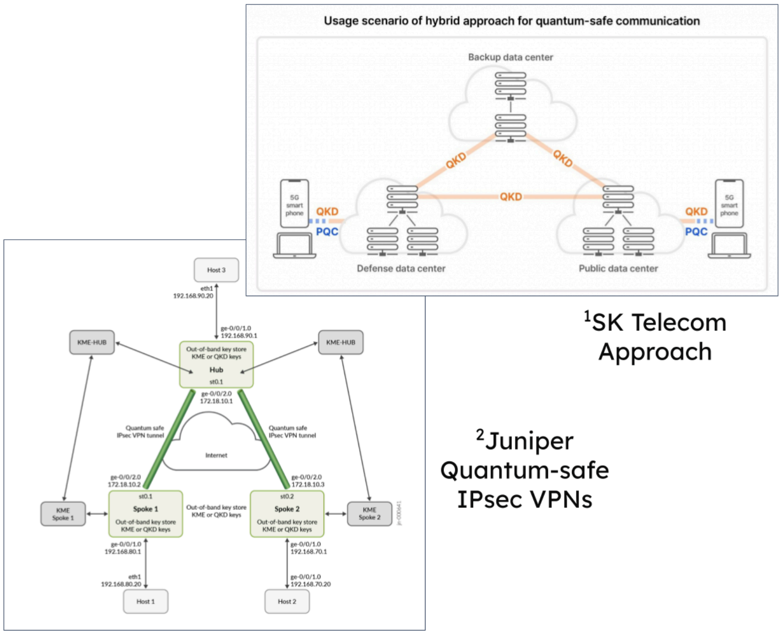
Network Architecture Integration

At the network architecture level of integration, the focus is on the overall design and structure of the network. Here, the intersection of quantum and classical technologies can be seen in the topology of the network, the distribution of data centers, and the placement of edge devices. The critical backbones of the network, which handle the highest data rates and the most sensitive information, are ideal candidates for quantum security solutions like QSC. These backbones are typically connected by fiber optic channels, making them well-suited for the deployment of quantum technologies.

Network Integrations

Architectural considerations:

- Topology
- Free-space <> terrestrial
- Key management
- Gateway functions
- Protocol integration on routers & switches
- Quantum "backbones" for high datarate links
- PQC at the edge (IoT)



[1]SK Telecom Approach

[2]Juniper Quantum-safe IPsec VPNs

[1]https://www.sktelecom.com/en/press/press_detail.do?idx=1579
[2]https://www.juniper.net/documentation/us/en/software/junos/vpn-ipsec/topics/topic-map/quantum-safe-ipsec-vpn.html

However, the edge of the network, where Internet of Things (IoT) devices and wireless communication dominate, presents a different set of challenges. The deployment of quantum technologies in these environments is more complex and less feasible at this stage. As a result, PQC plays a more prominent role in securing the last mile of the network, where classical cryptographic methods are still more practical due to their smaller form factors.

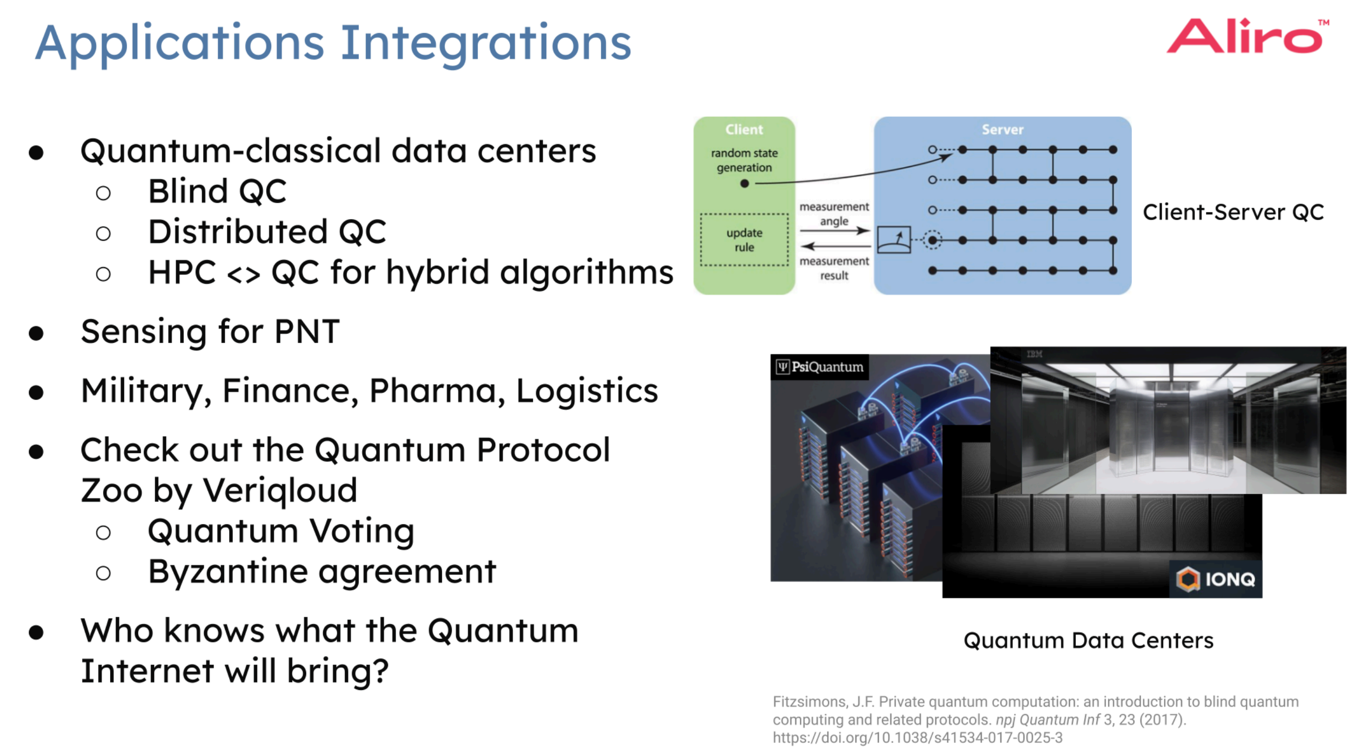
Gateway functions are another critical intersection point at this layer. These gateways manage the transition between quantum-enabled links and purely classical links, ensuring that the security provided by quantum technologies is maintained across network boundaries. The hybrid architecture must be designed to seamlessly integrate these different layers, ensuring that the entire network remains secure, regardless of where the data is flowing.

Application Integration

At the highest layer, the application layer, the intersection of quantum and classical technologies becomes even more apparent. Quantum-enabled data centers are already being built by companies like IBM and IonQ, which are leading the way in developing modular quantum computers that coexist with classical systems. These data centers raise important questions about how quantum computing will be consumed by end users—whether it will be primarily accessed through the cloud or deployed on-premises.

In cloud-based quantum computing scenarios, protocols for blind quantum computing and distributed quantum computing become valuable to end users. These protocols allow quantum computations to be performed without revealing the underlying data to the cloud providers, ensuring that sensitive information, such as intellectual property or personal data, remains private throughout the process. This capability is critical for industries that handle highly confidential information, such as finance, healthcare, and scientific research.

In the domain of sensing, quantum technologies offer new opportunities for applications in position, navigation, and timing (PNT). Quantum sensors, connected through entanglement-based quantum networks, can provide unparalleled accuracy and security for military and critical infrastructure applications. As we continue to explore the potential of entanglement-based quantum networks, new applications will emerge, ranging from trustworthy voting systems to quantum-secure financial transactions and beyond.



Applications Integrations

Aliro™

- Quantum-classical data centers
  - Blind QC
  - Distributed QC
  - HPC <> QC for hybrid algorithms
- Sensing for PNT
- Military, Finance, Pharma, Logistics
- Check out the Quantum Protocol Zoo by Veriqloud
  - Quantum Voting
  - Byzantine agreement
- Who knows what the Quantum Internet will bring?

Client-Server QC

Quantum Data Centers

Fitzsimons, J.F. Private quantum computation: an introduction to blind quantum computing and related protocols. *npj Quantum Inf* 3, 23 (2017). https://doi.org/10.1038/s41534-017-0025-3

Challenges of Implementing a Hybrid Classical/Quantum Architecture for Future-Proof Cybersecurity

As we move towards integrating quantum technologies with classical cryptographic systems, hybrid architectures emerge as a promising approach for future-proof cybersecurity. However, this approach is not without its challenges. The technologies involved—Post-Quantum Cryptography (PQC), Quantum Key Distribution (QKD), and Quantum Secure Communication (QSC)—have not reached the peak of their potential, with new hardware, components, and companies constantly emerging.

One of the primary challenges in implementing a hybrid classical/quantum architecture is the lack of a comprehensive suite of standards. While there is ongoing activity in developing protection profiles integration standards, there is no universal, one-size-fits-all approach to integrating these technologies across different layers of network architecture – yet. While classical internet protocols have well-established standards, the quantum domain remains in its early stages of standardization. This lack of uniform standards can make integration complex and daunting, as organizations must navigate a landscape where different solutions may not yet be fully interoperable. Reaching out and working with experienced partners and vendors can make this task less daunting. Additionally, the absence of rigid standards also offers a degree of flexibility. It allows for more agile development and adaptation as the technologies mature. As quantum computing and cryptographic methods mature, so too will the algorithms, hardware, and protocols that underpin these systems. Organizations must be prepared to invest in a migration strategy that anticipates these changes and stays ahead of emerging trends, ensuring that their security architecture remains resilient against new threats.

Crypto agility, the ability to dynamically adapt and rotate cryptographic protocols in response to evolving threats, is crucial in a hybrid architecture. However, there is still no clear definition or framework for what it means to be truly crypto-agile. This ambiguity poses a challenge for organizations trying to implement agile systems that can respond to both current and future threats. The ability to rotate protocols, adjust key distribution methods, and integrate new quantum-generated entropy sources are all aspects of crypto agility that need to be further defined and standardized. Moreover, as government regulations like GDPR, other privacy laws, and quantum technology export controls evolve, organizations must ensure that their security measures are not only agile but also compliant with these legal frameworks. Balancing the need for dynamic security with regulatory compliance adds another layer of complexity to the implementation of hybrid architectures.

The business case for adopting a hybrid classical/quantum architecture is a potential challenge that needs careful consideration. While the case for enhanced security is clear, the economics of migrating to these new systems must be evaluated from both a risk management and cost perspective. Organizations need to assess their current infrastructure, the sensitivity of the data they handle, and the specific threats they face. This assessment will inform the urgency and scope of their migration to quantum-safe systems. The architectural design of the network, including decisions on where and how to implement quantum technologies, will depend heavily on these factors. For instance, the integration of quantum solutions might be prioritized in the most sensitive parts of the network, while classical cryptographic methods continue to be used in less critical areas. The strategic allocation of resources, combined with a clear understanding of business incentives, will be key to successful implementation.

The effectiveness of a hybrid classical/quantum architecture also depends on the specific use cases and constraints of an organization. The sensitivity of the data, the expected attack profiles, and the geographic footprint of the organization's network can all influence the design of the security architecture. For example, a financial institution may prioritize the integration of quantum technologies to protect high-value transactions, while a government agency may focus on securing communications in compliance with national security regulations. These use case dependencies mean that there is no one-size-fits-all solution. Each organization will need to tailor its hybrid architecture to meet its unique security requirements, making the design process more complex but ultimately more effective.

The Promise of Hybrid Architectures

Despite these challenges, the potential benefits of hybrid architectures make them a worthy endeavor. By combining the strengths of classical cryptographic methods like PQC with quantum-based security measures, organizations can achieve a level of security that was previously unattainable. The integration of quantum technologies introduces notions of information-theoretic security, making it practically impossible for adversaries to crack encryption even with future advances in quantum computing.

Furthermore, the dynamic nature of a crypto-agile system allows organizations to rotate and update their security protocols in response to evolving threats, providing a resilient defense against both current and future cyber attacks. This adaptability is particularly valuable in a landscape where new threats are constantly emerging.

Embracing the Future of Cybersecurity

In conclusion, while there are challenges to implementing a hybrid architecture, the potential rewards are immense. The continuous evolution of quantum technologies, combined with the growing need for robust cybersecurity solutions, makes this an exciting and necessary field to explore. By investing in hybrid architectures that combine classical methods like PQC with quantum-based security measures like QSC, organizations can strengthen their security posture and prepare for the quantum era while also investing in its potential. Organizations that start their quantum networking journey today will be best positioned to face the challenges, and embrace the upsides of tomorrow's quantum world.

A full-stack solution for entanglement-based Quantum Secure Communication

Entanglement-based quantum networks are being built today by a variety of organizations for a variety of use cases – benefiting organizations internally, as well as providing great value to an organization’s customers. Telecommunications companies, national research labs, and systems integrators are just a few examples of the organizations Aliro is helping to leverage the capabilities of quantum secure communications.

Building entanglement-based quantum networks that use entanglement is no easy task. It requires:

- Emerging hardware components necessary to build the network.
- The software necessary to design, simulate, run, and manage the network.
- A team with expertise in the fundamental science of entanglement-based quantum networks and classical networking.
- Years of hard work and development.

This may seem overwhelming, but Aliro is uniquely positioned to help you build your quantum network. The steps you can take to ensure your organization is meeting the challenges and leveraging the benefits of the quantum revolution are part of a clear, unified solution already at work in networks like the EPB Quantum Network℠ powered by Qubitekk in Chattanooga, Tennessee.

AliroNet™, the world's first full-stack entanglement-based network solution, consists of the software and services necessary to ensure customers will fully meet their advanced secure networking goals. Each component within AliroNet™ is built from the ground up to be compatible and optimal for with entanglement-based networks of any scale and architecture. AliroNet™ is used to simulate, design, run, and manage quantum networks as well as test, verify, and optimize quantum hardware for network performance. AliroNet™ leverages the expertise of Aliro personnel in order to ensure that customers get the most value out of the software and their investment.

Depending on where customers are in their quantum networking journeys, AliroNet™ is available in three modes that create a clear path toward building full-scale entanglement-based secure networks: (1) Emulation Mode, for emulating, designing, and validating entanglement-based quantum networks, (2) Pilot Mode for implementing a small-scale entanglement-based quantum network testbed, and (3) Deployment Mode for scaling entanglement-based quantum networks and integrating end-to-end applications. AliroNet™ has been developed by a team of world-class experts.

To get started on your Quantum Networking journey, reach out to the Aliro team for additional information on how AliroNet™ can enable secure communications.

www.alirotech.com

References

Vermeer, Michael J. D., et al. Preparing for Post-Quantum Critical Infrastructure. RAND Corporation, 2022, www.rand.org/content/dam/rand/pubs/research_reports/RRA1300/RRA1367-6/RAND_RRA1367-6.pdf.

DiAdamo, Stephen, et al. "Packet Switching in Quantum Networks: A Path to the Quantum Internet." Physical Review Research, vol. 4, no. 4, 2022, p. 043064, https://doi.org/10.1103/PhysRevResearch.4.043064.

Lu, Hsuan-Hao, et al. "Procrustean Entanglement Concentration in Quantum-Classical Networking." arXiv, 2024, https://arxiv.org/abs/2401.01311.

National Institute of Standards and Technology. “Post-Quantum Cryptography FIPS Approved.” NIST, 2024, https://csrc.nist.gov/news/2024/postquantum-cryptography-fips-approved.

Fluhrer, S., et al. "Mixing Preshared Keys in the Internet Key Exchange Protocol Version 2 (IKEv2) for Post-Quantum Security." RFC 8784, RFC Editor, June 2020, https://www.rfc-editor.org/info/rfc8784.

Renner, Renato, and Ramona Wolf. "The Debate over QKD: A Rebuttal to the NSA's Objections." arXiv, 2023, https://arxiv.org/abs/2307.15116.

SK Telecom. "SK Telecom to Launch Quantum Cryptography Communication in Malaysia and Thailand." SK Telecom, 2024, https://www.sktelecom.com/en/press/press_detail.do?idx=1579.

Juniper Networks. “Quantum-Safe IPSec VPN.” Juniper Networks, https://www.juniper.net/documentation/us/en/software/junos/vpn-ipsec/topics/topic-map/quantum-safe-ipsec-vpn.html.

Fitzsimons, J. F. "Private Quantum Computation: An Introduction to Blind Quantum Computing and Related Protocols." npj Quantum Information, vol. 3, 2017, p. 23, https://doi.org/10.1038/s41534-017-0025-3.