Bell Labs Consulting

NOKIA BELL LABS

Quantum-safe communications

Quick take

The advent of quantum computing threatens to obsolete our current cryptographic systems, which rely on complex mathematical problems that quantum computers will be able to break. To address this challenge, quantum-safe cryptographic algorithms have been proposed, which are designed to resist attacks from either classical or quantum computers. By adopting post-quantum cryptography (PQC) into their systems and applications, organizations will be able to safeguard their networks and protect their sensitive data in the quantum era. In this note, we assess the issue of quantum-safe communications, the risks associated with the advent of quantum computing, and the countermeasures organizations should take to limit the threats, vulnerabilities and attacks it may pose to their networks and applications.

Bell Labs Consulting

In today's digital landscape, cybersecurity is fundamental to network and system design. While traditional authentication and encryption techniques have effectively protected against conventional computing threats, the emergence of quantum computing presents an unprecedented challenge. The exponential computational power of quantum systems threatens to obsolete current cryptographic protocols, necessitating a transition to quantum-safe networks that are communication frameworks designed to resist quantum computational capabilities.

The deployment of quantum-safe measures requires careful risk assessment across multiple dimensions:

1. Technical risks (compatibility issues, performance impact, integration challenges and potential vulnerabilities)
2. Operational risks (implementation complexity, staff training and expertise, service disruption, maintenance and support)
3. Financial risks (initial investment, operation costs, return on investment, resource trade-offs)
4. Strategic risks (timing of deployment, technology selection and vendor lock-in, competitiveness and regulatory compliance).

At Bell Lab Consulting (BLC), we combine technical and business expertise to advise and guide organizations through this critical transition, helping implement robust security measures that protect sensitive information against both current and quantum-based threats. Our risk assessment methodology ensures a balanced approach to quantum-safe deployment, aligning security needs with business objectives and resource constraints.

Security principles

The five fundamental principles of network security that need to be satisfied when one party communicates with another in a secure manner are confidentiality, integrity, availability, authentication, and non-repudiation. They form the cornerstones of secure network design:

1. Confidentiality ensures that sensitive information remains private and accessible only to authorized users
2. Integrity guarantees that data remains unaltered during transmission or storage
3. Availability ensures systems and data are accessible when needed by legitimate users
4. Authentication verifies the identity of users and systems accessing the network
5. Non-repudiation provides proof of data origin and delivery, preventing users from denying their actions.

Together, these principles create a comprehensive framework for protecting networks against unauthorized access, data breaches and service disruptions.

Implementation of security principles

To implement these principles, organizations employ various strategies:

- Confidentiality is achieved through encryption techniques like SSL/TLS to secure data transmission
- Integrity is maintained using checksums, digital signatures and intrusion detection systems to detect and prevent unauthorized modifications
- Availability is ensured by redundant systems, backups and disaster recovery plans
- Authentication is enforced through strong passwords, multi-factor authentication and biometric verification
- Non-repudiation is established using digital signatures and timestamping to prove the origin and authenticity of digital documents.

By implementing these measures, organizations can significantly enhance the security of their networks and protect sensitive information.

Quantum computers and conventional cryptography

Common encryption algorithms like RSA and ECC, which are used in public-key cryptography, and AES, which is used in symmetric-key cryptography, are currently secure against classical computers. These algorithms rely on complex mathematical problems that are computationally intensive to solve. However, the advent of quantum computing poses a significant threat to these algorithms.

Quantum computers can potentially break these encryption schemes by leveraging quantum algorithms like Shor's algorithm, which can efficiently factor large numbers and solve discrete logarithm problems. This would compromise the security of many current cryptographic systems.

While Grover's algorithm can accelerate brute-force attacks on symmetric-key encryption, doubling the key length can mitigate this threat. However, asymmetric-key cryptography, which is essential for key exchange and digital signatures, remains vulnerable.

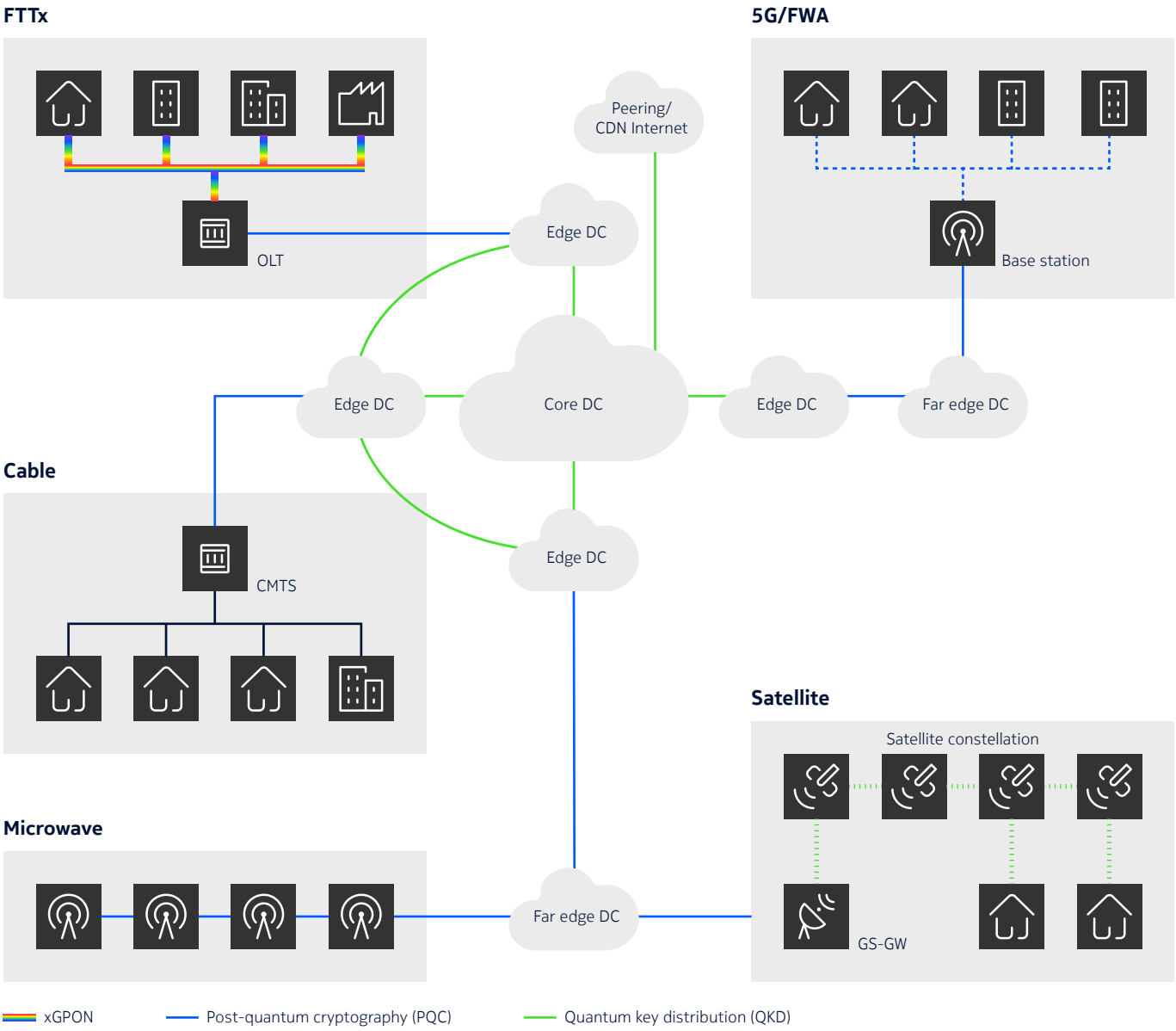
To address this challenge, quantum-safe cryptographic algorithms have been proposed, and they are designed to be resistant to attacks from both classical and quantum computers. By adopting quantum-safe cryptography, organizations can protect their sensitive data and secure their digital communications in the quantum era.

Why do we need quantum safety?

We need quantum-safe networks because the advent of quantum computing threatens to render our current cryptographic systems obsolete. The immense computational power of quantum computers could potentially break the encryption methods we currently rely on to secure sensitive data, such as financial transactions, medical records and government communications. This could have devastating consequences for individuals, businesses and governments alike.

Quantum-safe networks, on the other hand, are designed to be resilient against quantum attacks. They employ advanced cryptographic techniques that are believed to be secure even in the face of quantum computing power. By adopting and implementing quantum-safe networks, we can safeguard our digital infrastructure and protect our sensitive information from future threats.

Figure 1. Example of PQC/QKD hybrid implementation



Providing quantum safety

To provide quantum-safe networking and safeguard the digital infrastructure and communications generally, the development and deployment of quantum-safe networks are becoming increasingly crucial. Multiple approaches are being considered, developed and implemented.

Post-quantum cryptography (PQC)

New cryptographic algorithms have been developed that are believed to be resistant to attacks from both classical and quantum computers. These algorithms are based on mathematical problems that are believed to be intractable for both classical and quantum computers.

Organizations like the National Institute of Standards and Technology (NIST) have standardized several PQC algorithms, providing a solid foundation for their widespread adoption. These include CRYSTALS-Kyber for general encryption, CRYSTALS-Dilithium, FALCON, and SPHINCS+ for digital signatures.

Many organizations are beginning to integrate PQC algorithms into their systems and applications. Ongoing research and development are focused on improving the performance and security of PQC algorithms.

Quantum key distribution (QKD)

Quantum key distribution (QKD) leverages the principles of quantum mechanics to securely exchange cryptographic keys between two parties. Any attempt to eavesdrop on the quantum channel will inevitably alter the quantum state of the signal, alerting the legitimate parties to the intrusion. This ensures unconditional security, meaning the system is theoretically secure against any attack, including those from quantum computers.

While QKD offers significant security advantages, practical implementation challenges exist. Establishing a dedicated quantum channel over long distances can be difficult. Quantum repeaters are being developed to extend the range of QKD networks, and satellite-based QKD is being explored for ultra-long-haul secure communication.

Several countries and organizations are actively deploying QKD networks to secure critical infrastructure and sensitive communications. Researchers are continuously working to improve the range, scalability and integration of QKD systems with existing classical networks.

While PQC offers a more practical solution for securing existing networks, QKD provides the ultimate level of security. A hybrid approach, combining PQC and QKD, may be the most effective way to secure future networks. The combination of QKD and PQC offers a robust and flexible solution. QKD can be used to securely distribute cryptographic keys, while PQC can be used to encrypt and authenticate data.

Key challenges and future directions

The practical implementation of quantum-safe networks faces several challenges. Long-distance QKD requires quantum repeaters to amplify signals. Standardization of protocols and devices is essential for widespread adoption. Quantum-resistant hardware, like random number generators, is crucial for security. Policy and regulatory frameworks are needed to guide development and deployment. Ensuring seamless interoperability between different quantum-safe technologies and systems is vital. Scalable solutions are required for large-scale deployments. Cost-effectiveness is crucial for widespread adoption. Finally, maintaining the security and trustworthiness of quantum-safe networks is paramount.

It's important to note that the development of quantum-safe networks is an ongoing process. As quantum computing technology advances, organizations may need to continue to adapt and evolve their security measures. By combining these strategies and addressing the challenges, providers could build a quantum-safe future where digital communications remain secure in the face of quantum computing advancements.

Bell Labs Consulting Services

Bell Labs Consulting employs a risk-based approach to security consulting, leveraging a proven threat modeling methodology and a deep understanding of threats, vulnerabilities, attacks and countermeasures. This knowledge is derived from years of global risk assessments across various technologies, including 5G, cloud, networking, IT applications and AI.

A formal, structured risk-based approach is essential for assessing the quantum threat to encryption and selecting appropriate protective measures, such as post-quantum cryptography (PQC) and quantum key distribution (QKD). Proactive security measures are crucial to address the “harvest now, decrypt later” threat. A phased approach to adopting evolving security countermeasures, combined with a defense-in-depth strategy, are recommended.

Quantum-safe networking is relevant to both service providers and service users. Service providers can benefit from offering quantum-safe networking services, while enterprises can procure these services and implement quantum-safe measures within their own networks and applications.

For further information please contact us at info.query@bell-labs-consulting.com

Learn more about Bell Labs Consulting at https://www.bell-labs.com/consulting/

Nokia OYJ
Karakaari 7
02610 Espoo
Finland
Tel. +358 (0) 10 44 88 000

Document code: 1155203 (December) CID#214406