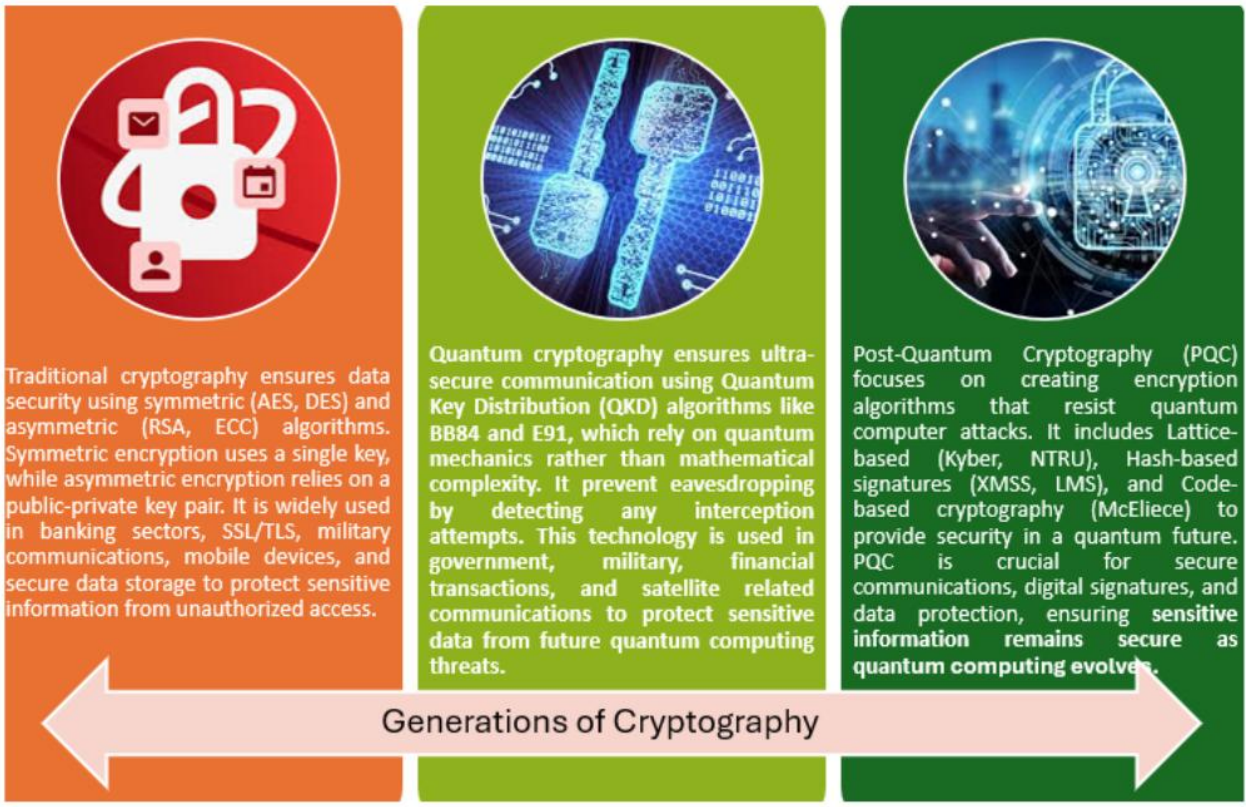
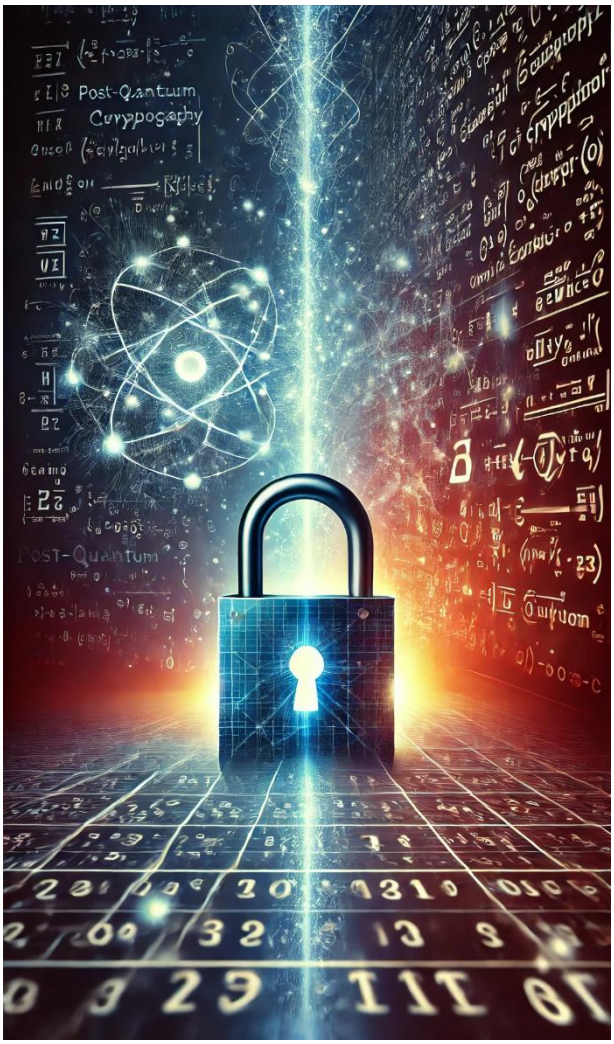
Ensuring Future-Proof Security With Post Quantum Cryptography

This newsletter highlights the risks quantum computing poses to traditional cryptography and the need for stronger security measures. As quantum technology advances, existing encryption methods become vulnerable and it becomes important to validate your traditional cryptographic algorithms. Implementing post-quantum cryptography ensures long-term data protection, safeguards critical infrastructure.

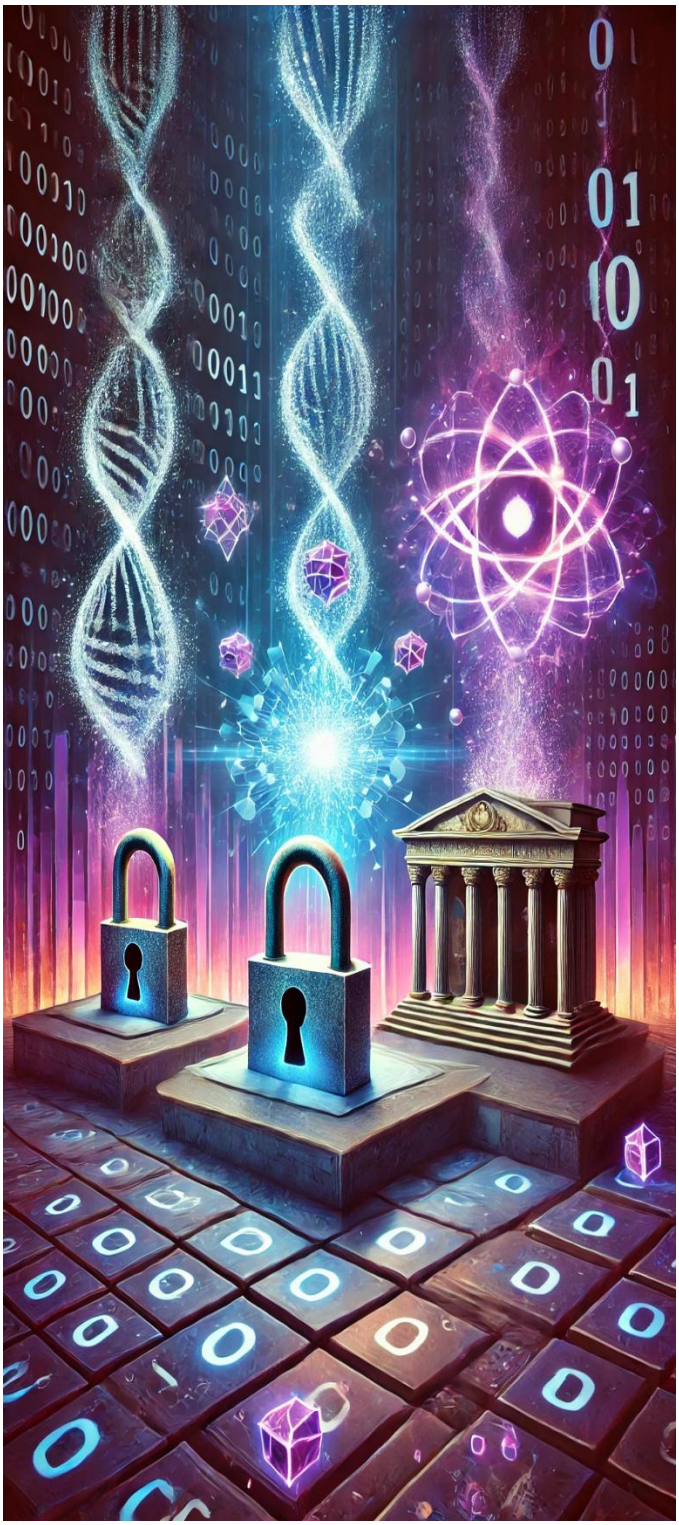


Challenges in traditional cryptography due to quantum attacks



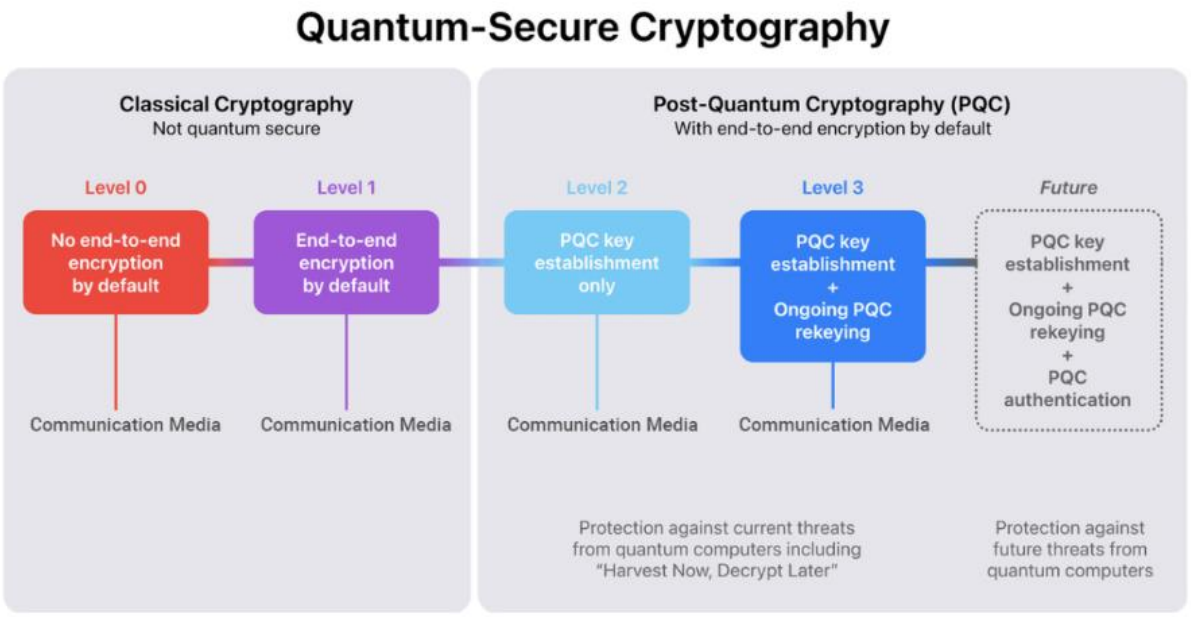
Traditional cryptography faces significant challenges due to quantum attacks, primarily because of the immense computational power of quantum computers. Here are the main challenges: Quantum computers can efficiently solve problems that traditional computers cannot, such as factoring large prime numbers (used in RSA) and computing discrete logarithms (used in ECC). Shor's algorithm, for example, can break these encryption methods quickly, rendering them insecure. While symmetric key encryption algorithms like AES are not completely broken by quantum computers, Grover's algorithm can effectively halve their security strength. This means that a 256-bit key would provide the equivalent security of a 128-bit key, necessitating larger key sizes to maintain security. Quantum computers can also undermine digital signatures, which rely on asymmetric key cryptography for verifying authenticity. This can compromise the integrity and authenticity of digital documents and communications. Traditional methods of key exchange over public channel, such as Diffie-Hellman, are vulnerable to quantum attacks, making it easier for an attacker with a quantum computer to intercept and decrypt communications. These challenges necessitate the development of quantum-resistant cryptographic algorithms to secure communications against future quantum attacks. Therefore Organization can switch to Post Quantum Cryptography to save themselves from future attack that can cause financial and data loss and may result in loss that might not be able to recover.

Why organizations should switch to Post-Quantum Cryptography



Quantum cryptography uses QKD, where the security of key exchange relies on the principles of quantum mechanics, such as the no-cloning theorem and Heisenberg's uncertainty principle. Any attempt to intercept the key would disturb the quantum state, alerting the parties involved and preventing the attack. Since quantum states change when observed, QKD ensures that any eavesdropping attempt can be detected, making the key exchange process highly secure. Post-quantum cryptography develops new algorithms that are secure against quantum attacks. These include lattice-based, hash-based, code-based, and multivariate polynomial-based algorithms, which are resistant to quantum computer capabilities like those exploited by Shor's and Grover's algorithms. By adopting quantum-resistant algorithms, post-quantum cryptography ensures that data encrypted today remains secure even when quantum computers become widely available. Why Organizations Should Switch to Quantum and Post-Quantum Cryptography Data encrypted today with traditional methods can be intercepted and stored, potentially to be decrypted in the future when quantum computers are available. Switching to quantum-resistant cryptography protects sensitive information from future breaches. As governments and industries recognize the risks posed by quantum computers, there will likely be new regulations requiring the use of quantum-resistant cryptography to safeguard critical data. Proactively adopting post-quantum cryptography reduces the risk of data breaches and protects against future threats, providing a competitive edge and enhancing trust with customers and partners. By adopting quantum and post-

quantum cryptography, organizations can ensure their security infrastructure remains robust against both current and future threats.



Change in media encryption due to Post Quantum Cryptography

Future-proofing security with TASL: Safeguarding data against cryptographic attacks

As quantum computing advances, traditional cryptographic algorithms face an increasing risk of becoming obsolete and vulnerable to sophisticated attacks. At TASL, we proactively help organizations stay ahead of these emerging threats by thoroughly assessing their encryption infrastructure and identifying potential weaknesses before they can be exploited. Our team of experts conducts an in-depth evaluation of your existing cryptographic algorithms, ensuring they meet the latest quantum-resistant standards. We assist in a seamless transition to post-quantum cryptographic (PQC) solutions by integrating hybrid encryption models that allow for a phased and secure migration. To further enhance security, we implement Quantum Key Distribution (QKD), a cutting-edge technology that provides unparalleled protection against quantum threats. In addition to fortifying encryption, we ensure full compliance with evolving PQC regulations, helping organizations navigate the complexities of future security frameworks. Our tailored roadmap equips businesses with the necessary strategies to safeguard their sensitive data and critical infrastructure against the rapidly evolving risks posed by quantum computing. With TASL as your trusted partner, you can confidently secure your digital assets and maintain resilience in the face of future quantum challenges.