Making networks quantum-safe

The quantum threat

Privacy of communication is fundamental to society and essential for the protection of businesses. Cryptographic methods such as hashing, and encryption are well established techniques for securely authenticating parties involved in a communication and protecting privacy and integrity.

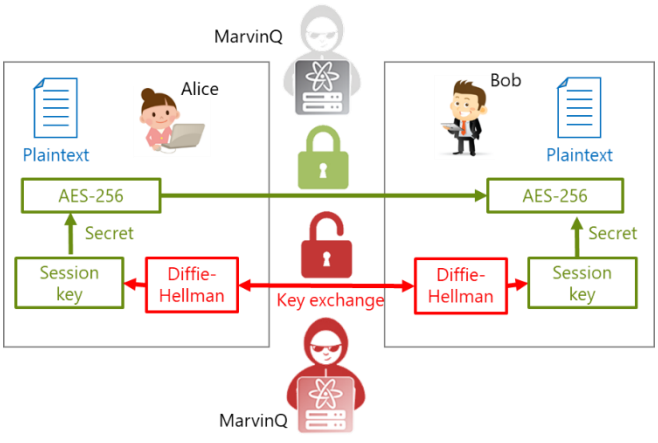
Public key exchange protocols leverage proven asymmetric encryption algorithms, such as RSA or Diffie-Hellman, to securely exchange secrets for authentication and to establish session keys. Session keys are used for encrypting large amounts of data with high-performance symmetrical ciphers, such as AES-256. Today's encryption and hashing algorithms offer high levels of security built on rigorous mathematical analysis and extensive use. They have never been breached and have proven to be secure even against attacks from the most powerful supercomputers. Alice and Bob don't need to worry about Marvin being able to compromise their communication, even if he has help from most powerful machines.

However, this situation will change with the emergence of quantum computers. Most experts believe that in 15 years from now there will be a quantum computer powerful enough to break RSA2048 within 24 hours. rendering existing cryptography insecure. As such, quantum computing is a threat to established methods of securing communication networks.

Quantum computers – a game changer in network security

Quantum bits – so-called qubits – are represented by quantum states. The behavior of a quantum state does not follow the rules of mechanical physics. It may represent the logical value of "0" or "1" but it could also represent a superposition of both, which is why it can carry much more information than a classical bit. Certain complex problems can be represented and processed by quantum computers in a fast and efficient way.

Asymmetric encryption algorithms are among the mathematical problems that can be solved by a quantum computer within hours or days – something classical supercomputers couldn't achieve in any reasonable period. Known as Shor's algorithm, quantum computers can apply methods for breaking established and commonly used public key algorithms.

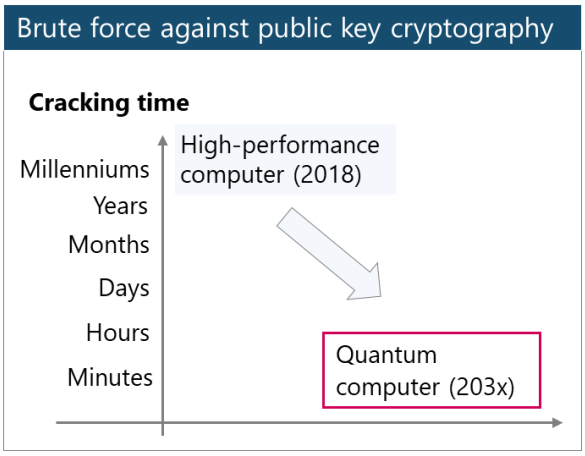


Luckily, the situation is much better with symmetrical encryption algorithms. While quantum computers have some advantage in attacking those algorithms, a widely applied key length of 256 is considered to be sufficiently long to make AES-256 quantum-safe.

The network diagram shows Alice and Bob using AES-256 to encrypt their communication and Diffie-Hellmann as a key exchange protocol. With the power of a quantum computer, MarvinQ can now decrypt the session keys. With those keys, he can read Alice and Bob's communication. He is, however, not able to directly break the communication secured with a symmetrical cipher.

Quantum computers do not exist yet – do we need to care?

Until today, there is no quantum computer large enough to run Shor's algorithm that could break currently applied cryptographic solutions. However, a lot of research money is going into the development of quantum computers and it's reasonable to expect their advent within the next 10 to 15 years.



This doesn't mean that we should sit by and wait for it to happen. For several reasons, action needs to be taken now:

- By applying a "store now, decrypt later" approach, attackers might eavesdrop on a secure communication link and store the encrypted traffic including the key exchange messages. As soon as a quantum computer becomes available, they will be able to process this data, decrypt the session keys and gain access.

- Security protocols are implemented in hardware, which stays in networks for many years. This includes cable modems, which use public key cryptography for secure authentication, and which are frequently deployed for 10 years and more. Today's installed hardware should be quantum-safe to avoid expensive hardware swaps when quantum computers become available.

- Public key cryptography is used in many applications as it's an essential technology for secure identification. As such, it's also applied with blockchain technology and cryptocurrencies. A quantum-resistant solution is vital to protect related assets.

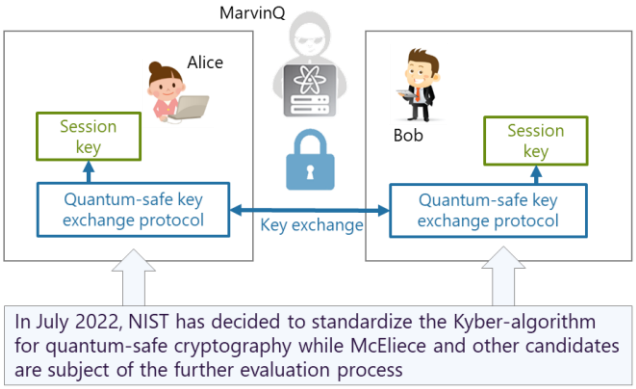
While there is no immediate risk from quantum attacks, the risk and associated cost from applying solutions vulnerable to the emerging quantum threat can be highly significant.

National security agencies/authorities – such as the NSA in the US and the Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik, BSI) in Germany – have initiated activities to make quantum-safe cryptography available, initiating projects to identify, evaluate and eventually standardize security solutions for the post-quantum era.

Quantum-safe cryptography

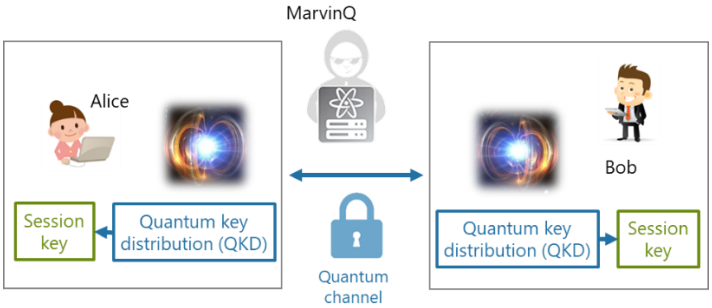
There are different ways to mitigate the vulnerabilities of public key algorithms and secure networks against quantum computer attacks. Two very different protective measures can be applied:

Making public key algorithms quantum-safe: Currently applied cryptographic schemes build on computational difficulty. While factorizing large prime products or solving polynomial equations is quite a challenge for a classical computer, these mathematical problems can easily be solved by quantum computers. Luckily, there are other mathematical challenges that are extremely hard even for the most powerful quantum computers. Algorithms like the one based on the McEliece cryptosystem have shown resistance to such attacks.



This is known as post-quantum cryptography (PQC) and a range of promising protocols currently undergo extensive security assessment by the global security expert community. In July 2022, NIST has decided to standardize the Kyber-algorithm for quantum-safe cryptography while McEliece and other candidates are subject of the further evaluation process. Until this process is finalized, security can be optimized by using pre-shared keys, preferably in combination with crypto-agile implementations upgradable to emerging standardized post-quantum algorithms.

Distributing keys in a quantum-safe way: A very different approach to quantum-safe cryptography is turning the attacking quantum technology into a weapon for defense. Quantum random number generators (QRNG) and quantum key distribution (QKD) are applying quantum physics to protect the integrity of key creation and key exchange.



As QKD uses quantum physics, this method is future-proof. There is no risk that new algorithms or more powerful computers might break this method as the security builds on fundamental physical principles. The implementation requires a careful design of the quantum optical channel. Optical amplification cannot be used as the replication of a quantum changes its status and related information. To bridge long distances, multiple QKD links need to be daisy-chained by means of trusted nodes. In future, quantum repeaters might simplify implementation over multiple spans. This technology is in an early conceptual phase.

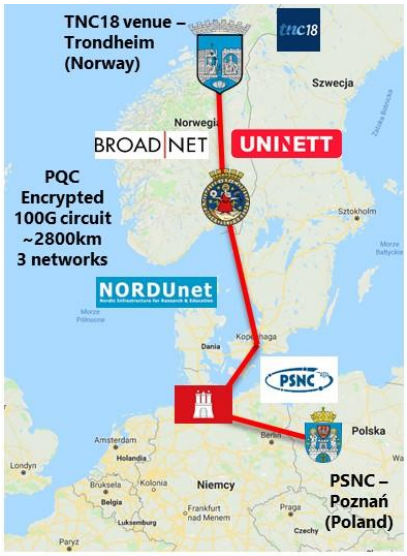
On the other hand, a post-quantum algorithm is relatively easy to implement as classical computers can be applied. However, new classical or quantum algorithms might be able to break security controls that are considered quantum-safe today. Implementations should be crypto-agile allowing algorithms to be updated at a later point in time.

Towards post-quantum secure transport networks

As early as 2014, ADVA started to research quantum-safe technologies and developed demonstrators for QKD-enabled WDM encryptors as well as for post-quantum key exchange. We demonstrated essential achievements in 2018. Since then, our focus has moved to productization.

With our technology partners ID Quantique and Toshiba, we showcased QKD solutions in live networks that meet operational service requirements. As quantum states cannot be multiplied without changing the information, optical amplifiers are not applicable on a QKD link. Hence, the distance between key recovery sites was in the order of 40 to 80km, depending on the fiber quality and other border conditions. Ongoing innovation allows to increase distances.

Based on our extensive experience with implementing security controls and certifying our protective controls, our customers could benefit from robust quantum-safe DWDM solutions as early as 2021. They can decide between QKD or PQC for securely establishing session keys. Both solutions use our certified and approved quantum-resistant AES-GCM-256 encryption for protecting large amounts of user data in real-time and with lowest latency. For QKD, a standardized key exchange protocol is already available with our ADVA's FSP 3000. This allows quantum-based key generation from third-party suppliers such as ID Quantique or Toshiba to be easily combined with our high-capacity optical transport system.



As early as in 2018, we also implemented a PQC solution using a McEliece-type algorithm in our high-bitrate optical transport system and demonstrated a quantum-safe 100Gbit/s transmission over 2800km on a live-traffic carrying fiber network. Our PQC solution combines classical with quantum-safe algorithms and can be further security-hardened with QKD. Such hybrid models leverage our extensive experience with implementing proven protocols with the additional level of protection required to defend against quantum attacks.

ADVA has been pioneering lowest-latency high-bitrate transmission systems and is now taking a major step towards quantum-safe security. Recently launched products leverage our experience from early demos. ADVA is the first company to commercialize a quantum-safe optical transport solution as well as introduce a crypto-agile packet network product. Both solutions can be operated with post-quantum cryptography and upgraded to NIST-selected PQC algorithms. Our pioneering engagement with quantum-safe high-bandwidth transport gives our customers a unique opportunity to implement quantum-safe networks today. By integrating all security functions into a crypto module, we're creating a truly future-proof security solution, removing any quantum risk and allowing our customers to leverage the true value of this powerful emerging technology.