Quantum-Safe Security Working Group

What is Quantum Key Distribution?

The Need for Key Distribution

Encryption is an essential part of data security. It provides a fundamental layer of protection that shields confidential data from exposure to attacks. It is needed to protect information transferred across telecommunications networks, as well as residing in files and databases.

The most secure and widely used methods to protect the confidentiality and integrity of data transmission are based on symmetric cryptography. Even better security is delivered with a mathematically unbreakable form of encryption called a one-time pad, whereby data is encrypted using a truly random key of the same length as the data being encrypted. In both cases, the main practical challenge is how to securely share the keys between the concerned parties.

Current Key Distribution Approaches

Key distribution is the process of sharing cryptographic keys between two or more parties to allow them to securely share information.

A simple though non-scalable method for sharing symmetric keys is for the parties to physically meet in a secure environment and agree on shared secret keys. Current key distribution techniques are more pragmatic than that, and can be performed at any distance. They almost universally use public key ciphers, such as RSA, Diffie-Hellman, and ECC to agree upon and exchange symmetric keys. These secret keys can then be used for encryption, for example with AES or OTP encryption systems.

The Challenges of Conventional Key Distribution

The security of the public key ciphers that are used to distribute symmetric keys relies on the strength of mathematical problems and limiting assumptions on the capabilities of the attacker. These ciphers are based upon mathematical calculations that are simple to compute, but require an infeasible amount of processing power to invert. For example, it is easy to calculate the product of two large prime numbers, but much harder to factor the product to derive the primes.

This key distribution approach presents multiple challenges. Its security is threatened by weak random number generators, advances to CPU power, new attack strategies, and the emergence of quantum computers. Quantum computers will ultimately render much of today's encryption unsafe. A particular concern is that data encrypted today can be intercepted and stored for decryption by quantum computers in the future. In 1977, a seminal article on public key cryptography in Scientific American estimated that it would take 40 quadrillion years to crack a message asymmetrically encrypted with the RSA-129 cipher. In actuality, it was cracked less than 20 years later, within six short months, by using a distributed network of computers. To stay ahead of the trend, ever increasingly larger asymmetric keys are required to securely distribute symmetric keys.

All these factors, especially the continued progress in quantum information processing, make it necessary to rethink how to securely distribute cryptographic keys.

What is Quantum Key Distribution?

Quantum Key Distribution (QKD) addresses these challenges by using quantum properties to exchange secret information -- such as a cryptographic key, -- which can then be used to encrypt messages that are being communicated over an insecure channel. The security of QKD relies on fundamental laws of nature, which are invulnerable to increasing computational power, new attack algorithms or quantum computers. It is secure against the most arbitrarily powerful eavesdroppers.

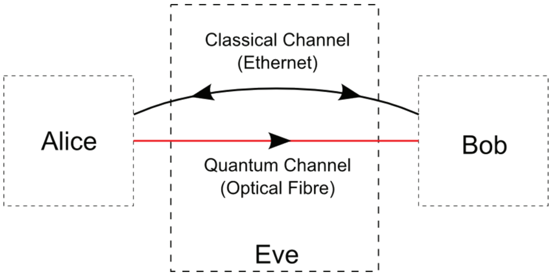
QKD effectively addresses the challenges confronting classic key distribution approaches, by providing a provably secure cryptographic building block for remote parties to share cryptographic keys. For the highest security requirements, QKD even enables the continuous generation and sharing of truly random one-time pad keys.

How does QKD Work?

The security of QKD is based on a fundamental characteristic of quantum mechanics: The act of measuring a quantum system disturbs the system. Thus, an eavesdropper trying to intercept a quantum exchange will inevitably leave detectable traces. The legitimate exchanging parties can decide either to discard the corrupted information, or reduce the information available to the eavesdropper to nought by distilling a shorter key.

A QKD implementation typically includes the following components:

- A fiber or free-space quantum channel to send quantum states of light between the transmitter (Alice) and receiver (Bob). This channel does not need to be secured
- A public but authenticated communication link between the two parties to perform post-processing steps and distill a correct and secret key
- A key exchange protocol that exploits quantum properties to ensure security by detecting eavesdropping or errors, and by calculating the amount of information that has been intercepted or lost



Both errors and potential information leakage are removed during subsequent error correction and privacy amplification post-processing steps, leaving Bob and Alice with a shared key known only to them.

Types of Quantum Key Distribution

Since QKD first appeared as a promising theoretical concept, a variety of protocols have emerged and been demonstrated in many real-world scenarios.

The first approach is Discrete Variable QKD, which encodes quantum information in discrete variables and uses single photon detectors to measure the received quantum states. Examples are the BB84 protocol[1] and the E91[2] protocol.

A second approach is continuous-variable QKD (CV-QKD). In this approach, the quantum information is encoded onto the amplitude and phase quadratures of a coherent laser, and can then be measured by the receiver using homodyne detectors. Example protocols include Silberhorn (2002)[3] and Grangier (2003)[4].

Both of these approaches have been proven to be information-theoretically secure[5,6] even in the presence of an attacker or eavesdropper.

The Path Forward

Since practical protocols emerged starting in the 1980’s and 1990’s, QKD has evolved into a thriving experimental field, and is rapidly becoming a solid commercial proposition. Multiple QKD networks have been implemented around the globe, and more are in progress. The technology has been steadily improving, expanding the distances and information rates achieved. Recent COW[7] (Coherent One Way) deployments have exceeded 300 km[8].

The Quantum-Safe Security Working Group (QSSWG) was formed within the Cloud Security Alliance to help promote the adoption of technologies that will protect data even after quantum computing becomes readily available. QKD is one of the technologies recommended by the QSSWG to protect and future-proof data against developments to computer power, new attack strategies, weak random number generators, and the emergence of quantum computers.

References

[1] C.H. Bennett and G. Brassard, Proceedings of IEEE International Conference on Computers Systems and Signal Processing, Bangalore India, December 1984, pp 175-179.

[2] Artur Eckert , Physical Review Letters **67**, p. 661 (1991)

[3] Ch. Silberhorn, T. C. Ralph, N. Lutkenhaus, and G. Leuchs, Phys. Rev. Lett. **89**, 167901 (2002).

[4] F. Grosshans et al., Nature (London) **421**, 238 (2003).

[5] H.-K. Lo and H. F. Chau Science **283**, 2050 (1999).

[6] R. Renner and J. I. Cirac, Phys. Rev. Lett. **102**, 110504 (2009). A. Leverrier and P. Grangier, Phys. Rev. Lett. **102**, 180504 (2009).

[7] Damien Stucki, Nicolas Brunner, Nicolas Gisin, Valerio Scarani, Hugo Zbinden. Appl. Phys. Lett. 87, 194108 (2005).

[8] Korzh et al. Nature Photonics 9, 163–168 (2015).