# Chapter 9
# Quantum Key Distribution


**Jasper Rödiger**

## 9.1 Introduction

A new class of computers, so-called quantum computers, will soon be able to crack common encryption algorithms. Quantum Key Distribution (QKD) is a promising solution to stay secure in the quantum computer age, which is progressively getting industrialized in recent years. Worldwide, point-to-point QKD links are combined into larger and larger testbed networks, which approach more commercially usable networks. Topics like certification and standardization have become increasingly important for QKD. Since Switzerland is strong in the field of QKD in terms of academia and industry, it has the opportunity to produce QKD technology within the country successfully.

## 9.2 Analysis

### *9.2.1 Definition*

Quantum computers will soon thus endanger secure data traffic. Entirely new methods will therefore be needed to secure data transmission in the future. Nowadays, two leading families of cryptographic techniques are used to protect telecommunications. The first is symmetric encryption, see Chap. 2, such as AES, and the other is public-key cryptography, also known as asymmetric cryptography. The asymmetric cryptographic methods are often used to distribute the symmetric

J. Rödiger (✉)
Rohde und Schwarz, Cologne, Germany
e-mail: jasper.roediger@rohde-schwarz.com



V. Mulder et al. (eds.), *Trends in Data Protection and Encryption Technologies*,
https://doi.org/10.1007/978-3-031-33386-6_9

keys needed for symmetric cryptographic methods to the communication partners. The sender and receiver each use different keys in these methods: a public key and a private key. With conventional computers, it takes much effort to deduce the private key from the public key and thus break the encryption. However, as soon as quantum computers with the necessary computing power are available, the Shor algorithm can calculate the private key quickly for many methods used today [1].

QKD uses the quantum states of individual photons, i.e., light particles, to send so-called qubits from one communication partner to the other and thus generate a symmetric and secure key [2]. This exploits the fact that individual photons cannot be copied due to the no-cloning theorem of quantum physics and that the measurement of photons leads to measurement errors due to the quantum mechanical uncertainty principle. By cleverly applying these laws and if an authenticated communication channel exists between the communication parties, they can gain an information-theoretic advantage over potential attackers. Furthermore, by suitable post-processing of the measured qubits, they can generate a sequence of coinciding bits only known to them, which they can then use as a key, e.g., in symmetric cryptography methods.

Since the quantum key exchange is based on physical laws and not on the complexity of specific mathematical problems, the keys generated in this way can be used securely regardless of the computing power of quantum or classical computers and are thus future-proof.

### *9.2.2 Trends*

There are many different QKD protocols in existence, which, based on the above-described principles, use different degrees of freedom and state preparation and measurement mechanisms. The maturity of the implementation and theoretical assessment of the different QKD protocols are vastly different. Some implementations of those protocols are already quite mature, can be purchased as QKD solutions for point-to-point secure communication by different vendors, or are close to being purchasable. Worldwide, those point-to-point solutions are combined to testbed networks, which approach more commercially usable networks.

The largest of those QKD networks is the quantum backbone network built in China from 2013 to 2017, which spans over 2000 km of fiber between Beijing and Shanghai, including the satellite Micius offering satellite-based QKD links [3]. It is being expanded in 2017 to cover China by 2025. In the EU, since 2019, the EuroQCI initiative aims to build a secure quantum communication infrastructure (QCI) that will span the whole EU, including its overseas territories through fiber and satellite links [4]. All 27 EU member states have signed the EuroQCI declaration, committing themselves to the EuroQCI initiative. EuroQCI's goal is to have a fully operational QCI by 2027. The US company Battelle and the swiss company IDQuantique implemented a QKD network in the US in 2013 between

Columbus and Dublin in Ohio, namely the Battelle Quantum Network (BQN) [5]. It is their declared goal to extend the BQN to span 700 km.

Another sign that QKD is progressively getting industrialized can be observed by examining standardization endeavors. The most critical standardization organizations regarding QKD are ETSI and ITU. The first standardization activity was already started in 2008 by the ETSI by establishing the Industry Specification Group on QKD. Later, the ITU started in the realm of QKD and remained very active. Additionally, cybersecurity authorities, like, e.g., the German BSI or the French ANSSI, will play an essential role in the certification of QKD products [6]. However, governmental agencies still point out the lack of scalability [7] or even oppose its use for business-critical networks [8].

## 9.3 Consequences for Switzerland

Academically, Switzerland is one of the leading countries worldwide in the QKD [9]. This also affects the know-how transfer into the industry. One prominent example is the company IDQuantique, one of the first companies to bring QKD products to the market in 2004 and has remained an essential company in this area.

### *9.3.1 Implementation Possibilities: Make or Buy*

Since there is already much know-how in Switzerland, both academically and in the private industry, Switzerland is in an excellent position to produce QKD technology within the country if QKD technology is further fostered. Due to the expected demand, the QKD market is currently massively growing. Therefore, it is reasonable to expect more QKD vendors to emerge, exploring the different possible technologies including continuous-variable (CV) and discrete-variable (DV) QKD modules. The best technologies may be depending on the exact use case (Table 9.1).

### *9.3.2 Variations and Recommendation*

Since the QKD market is growing, Switzerland can keep its advantages in the field of QKD if the field is further supported [10].

**Table 9.1** Implementations possibilities for different sectors

| | Make | | Buy | |
|---|---|---|---|---|
| | Pros | Cons | Pros | Cons |
| **Military** | Full control over development | The Market is still developing and changing | A lot of different vendors and technologies expect to emerge in the next five years | Less control over products |
| **Civil Society** | Switzerland is in a good position, academically and industry-wise | None | A lot of different vendors and technologies expect to emerge in the next five years | None |
| **Economy** | Switzerland is in a good position, academically and industry-wise | None | Switzerland is in a good position already | None |

## 9.4 Conclusion

The QKD market is developing. Industrialization takes place in terms of publicly funded projects and private actors. Since Switzerland is vital in the field of QKD in terms of academia and industry, it has the opportunity to produce and export QKD technology. However, it is necessary to know that influential cybersecurity authorities do not recommend using this technology at a broader level as there are cheaper alternatives for the mass market.

## References

1. Craig Gidney and Martin Ekerå. How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits. *Quantum*, 5:433, April 2021. arXiv:1905.09749 [quant-ph].
2. S. Pirandola, S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. L. Pereira, M. Razavi, J. Shamsul Shaari, J. Shamsul Shaari, M. Tomamichel, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi, and P. Wallden. Advances in quantum cryptography. *Advances in Optics and Photonics*, 12(4):1012–1236, December 2020. Publisher: Optica Publishing Group.
3. *An Assessment of the U.S. and Chinese Industrial Bases in Quantum Technology*. RAND Corporation, 2022.

4. The European Quantum Communication Infrastructure (EuroQCI) Initiative | Shaping Europe's digital future. https://digital-strategy.ec.europa.eu/en/policies/european-quantum-communication-infrastructure-euroqci.
5. Alex Morrow and Matthieu Legré. Battelle QKD Test Bed. In *2012 IEEE Conference on Technologies for Homeland Security (HST)*, Waltham, MA, USA, November 2012. IEEE.
6. Marius Loeffler, Christian Goroncy, Thomas Länger, Andreas Poppe, Alexander Neumann, Matthieu Legré, Imran Khan, Christopher Chunnilall, Diego López, Marco Lucamarini, Andrew Shields, Elisabetta Spigone, Martin Ward, and Vicente Martin. Current Standardisation Landscape and existing Gaps in the Area of Quantum Key Distribution. page 31.
7. Should Quantum Key Distribution be Used for Secure Communications? https://www.ssi.gouv.fr/publication/should-quantum-key-distribution-be-used-for-secure-communications/, November 2022. ANSSI.
8. Quantum security technologies. https://www.ncsc.gov.uk/whitepaper/quantum-security-technologies, November.
9. Lutz Bornmann, Robin Haunschild, Thomas Scheidsteger, and Christoph Ettl. Quantum technology – a bibliometric analysis of a maturing research field, August 2019.
10. Cathal J. Mahon and SSC secretariat. White Paper: Quantentechnologie in der Schweiz, 2020.