ENISA Briefing: Quantum Key Distribution

enisa
European Network and Information Security Agency

ENISA Briefings are short descriptions of emerging issues in security aimed at policy and decision makers. They give a brief introduction to the topic, areas of debate and propose a reasoned opinion on controversial points.

About ENISA: *The European Network and Information Security Agency (ENISA) is an EU agency created to advance the functioning of the internal market. ENISA is a centre of excellence for the European Member States and European institutions in network and information security, giving advice and recommendations and acting as a switchboard for information on good practices. Moreover, the agency facilitates contacts between European institutions, the Member States, and private business and industry actors. Internet: http://www.enisa.europa.eu/*

Contact details:

This report has been edited by: Giles Hogben, email: Giles.hogben@enisa.europa.eu

Acknowledgements:

We would like to thank the following for their input and advice:

- Rainer Plaga, BSI, Germany
- Johannes Skaar, Norwegian University of Science and Technology

ENISA Briefing: Quantum Key Distribution

The purpose of this briefing is to give an introduction to the possibilities offered by quantum key distribution (QKD), as well as its limitations and the main issues of disagreement between experts in the field. The algorithms and their basis in quantum mechanical theory are not covered in detail, but those interested can find suggestions for further reading in [Sources and further reading].

Key points

- The main use-case for QKD is the sharing of very long keys which may be used to provide message confidentiality using one-time-pad encryption. Due to its high cost, this means its main area of application is very high assurance applications (particularly related to national security and government use-cases).
- QKD provides future-proof secrecy – because the security of key material does not depend on the computational intractability of the algorithm used, but on physical properties which do not change over time.
- QKD relies on a security mechanism which is completely separate from traditional methods used for key exchange. It is therefore useful to develop as an alternative method which could be an essential fall-back in case other regimes become unusable (for example in case quantum computers become practical for factorisation problems, rendering traditional encryption useless).

Introduction

Quantum Key Distribution (QKD) is a method for remotely agreeing encryption keys between two parties. The most important feature of QKD is that it can be used to distribute *very long secret keys* in such a way that it is known *that no eavesdropping could be successful*.

QKD enables the encryption of data using random keys of the same length as the data being transmitted, in other words, using a true one-time-pad encryption (1). Encryption using a one-time-pad can only be provably unbreakable provided that the key generation algorithm uses a true random number generator and randomness is not lost in key agreement. As an aside, truly random key generation can also be achieved using techniques based on quantum mechanical properties (see (2)).

The use of one-time-pads for encryption, in combination with eavesdrop protection based on QKD promises unconditionally secure transmission of messages – i.e. an attacker can gain no knowledge

about the message. This can now be achieved at speeds which make it practical for certain real-world applications.

QKD uses the physical property of quantum mechanical states, that they are *altered by certain acts of observation*. At a small scale (approximately single photons or the wavelength of light), such alterations and therefore the observation (eavesdropping) that caused them, can be reliably detected. QKD provides protocols (e.g. BB84, E91) and implementations (see (2)) for using this property to detect eavesdropping of secret key material. In QKD, a secret key is encoded as a set of quantum mechanical states, such that any act of observation which might lead to knowledge about the message is detected through its effect on those states. Only parts of the message which are known not to have been observed are retained.

QKD relies on physical properties rather than the intractability of a mathematical property (asymmetric cryptography, for example, relies on the intractability of certain mathematical problems, such as the factorisation of large numbers). This means that, unlike current classical cryptography techniques, the message security provided by QKD does not have a "sell-by-date" determined by the inexorable progress in computing power. In other words, it provides "forward security".

What it is not

- QKD is not an encryption technique. Quantum Key Distribution is sometimes described as "quantum cryptography" but it is not a technique for encrypting data, only for distributing keys in such a way that any eavesdropping is known. Given knowledge of eavesdropping, only key material which is known not to have been eavesdropped is then used to encrypt data.
- QKD is not exclusively quantum mechanical - it requires an initial secret, which must be established using a classical method (such as PKI) in order to authenticate both parties. This initial secret is then "grown" using QKD into a secret which is suitable for one-time-pad encryption.
- QKD is not possible over unlimited distances, with current implementations. The current maximum range is of the order of 100km. This problem could be solved using repeaters, but repeaters which do not have to be trusted (i.e. do not read and re-encode the key material) are not currently available. Therefore such a repeater has to be trusted and such "QKD networking devices" are in the early stages of development.
- It does not replace end-to-end security. QKD represents one link in a chain of security measures used for encrypting data. If, for example, initial authentication of the parties is compromised, the vetting of the staff with access to the secrets is not sufficient, or the

equipment used has back-doors, then the investment in security provided by QKD is wasted. In other words, QKD is only one link in a chain and if the other links are of unequal strength, it may not be a rational investment.

- QKD has nothing to do with Quantum Computing or Quantum Cryptanalysis – other than the encoding of information using quantum states. Quantum computing and quantum cryptanalysis use information encoded in quantum states to process information. This can be used to perform certain computing operations (such as factorisation) much more efficiently than classical computing machines.

- QKD cannot be used to transmit specific predetermined information, only to *agree on* a randomised secret. Since vulnerable parts of the message are routinely discarded as part of the BB84 algorithm (a process known as “sifting”), any predetermined message would be corrupted.

Implementations and weaknesses

There are currently a number of (high cost) commercial implementations of the theory. These implementations use either :

- Discrete Variable measurements: this is typically based on the measurement of the polarisation of individual photons. This was the first type of system to be implemented and therefore may be considered *more mature* in terms of implementation security and robustness. However, compared to continuous variable systems, the *data transmission rate is much lower*, because of the need to isolate individual particles (of the order of KB/Sec).

- Continuous Variable measurements: this is typically based on the measurement of the phase and amplitude of a laser beam to encode information. This is a relatively recent development and therefore has less maturity in terms of security testing, but promises considerably higher data transmission (of the order of MB/Sec). Another advantage of continuous variable approaches is that they are possible using off-the-shelf equipment.

There are a number of well-documented attacks against implementations, although these generally only show a slight weakening of the unconditional security offered and not a practical attack. For more information, see: (3) (4) .

Areas of controversy and open issues.

The following are important areas of uncertainty and debate in this area:

- Which use-cases justify the cost and complexity of implementation? Given that the security of QKD lies in its ability to exchange very large keys in a way which provides so-called "forward security" – i.e. Given that QKD only grows keys, at what point does it become worthwhile to invest in QKD equipment rather than, for example, the exchange of very large keys e.g. stored on hard drives.
- The concept of "unconditional security": when the models used to prove unconditional security will always rely on a set of assumptions, which is necessarily incomplete. Attacks on QKD all rely on inaccurate modelling of theory in implementation because of hidden assumptions. It is clearly impossible for any implementation to be immune to the discovery of a new assumption which was not previously considered.
- Is it worth having one link in the security chain so strong when all the other links are weaker?

Future trends and research

The following are areas where significant developments can be expected in QKD:

- Range – the distance over which key agreement is possible can be expected to increase. Quantum repeaters are one way of achieving this. These are devices which can increase the range of transmission without having to be trusted. Although quantum states cannot be cloned (5), they can be stored and retransmitted without being observed. Quantum repeaters use this possibility, but practical commercial implementations are not yet available.
- Bandwidth – the bit-rate of transmission can be expected to increase.
- Cost – the cost of equipment can be expected to decrease.
- Quantum Random Number Generation: keys used for one-time pads are only unconditionally secure if the process used to generate the keys is perfectly random. Measurements of quantum states can be used to create perfectly random strings (see (2)).

Sources and further reading

1. Anderson, Ross. *Security Engineering.* s.l. : Wiley, 2008. pp. 132-134. 9780470068526.

2. Assche, Gilles Van. *Quantum Cryptography and Secret-Key Distillation.* s.l. : Cambridge University Press, 2006. ISBN-13: 9780521864855.

3. Vadim Makarov, Andrey Anisimov, Sebastien Sauge. Quantum hacking: adding a commercial actively-quenched module to the list of single-photon detectors controllable by Eve. [Online] http://arxiv.org/PS_cache/arxiv/pdf/0809/0809.3408v2.pdf.

4. Bing Qi, Chi-Hang Fred Fung, Yi Zhao, and Xiongfeng Ma. Quantum hacking: attacking practical quantum key distribution systems. [Online] 2007. http://spiedl.aip.org/getabs/servlet/GetabsServlet?prog=normal&id=PSISDG006710000001671001000001&idtype=cvips&gifs=yes.

5. *A Single Quantum Cannot be Cloned, Nature.* **Zurek, W.K. Wootters and W.H.** 1982, Nature, Vol. 299, pp. 802–803.

6. Quantum Cryptography, Quantum Teleportation, Quantum Computation, Bouwmeester, Dirk; Ekert, Artur K.; Zeilinger, Anton (Eds.) 2000, ISBN: 978-3-540-66778-0

7. "The case for quantum key distribution" by Stebila et al, arXiv:0902.2839.