Quantum Cryptography: a view from classical cryptography

Quantum Cryptography: a view from classical cryptography

Johannes Buchmann Johannes Braun Denise Demirel
Matthias Geihs
Technische Universität Darmstadt
E-Mail: buchmann, jbraun, ddemirel, mgeihs@cdc.tu-darmstadt.de

1 Introduction

Cryptography is essential for the protection of our increasingly digitized world. Fundamental protection goals that cryptography achieves are data confidentiality, integrity, and authenticity. Confidentiality guarantees that only authorized parties are able to access the data. Integrity means that illegitimate and accidental changes of the data can be discovered. Authenticity refers to the origin of the data being identifiable. For example, consider medical data. Confidentiality protects the privacy of the involved individuals. Data integrity is important because changes may lead to incorrect treatment with serious health consequences, and authenticity is required for liability reasons.

The oldest cryptographic technique is encryption. It achieves confidentiality. Before the digital era, encryption was mostly used to protect military and governmental communication. Today, the use of encryption is ubiquitous, in particular on the Internet. Other fundamental cryptographic techniques include cryptographic hash functions and digital signature schemes. They are used to protect data integrity and authenticity. In addition to achieving the above mentioned security goals, cryptography serves many more tasks. For example, multiparty computation allows parties to jointly compute a function over their inputs, for instance the average, while keeping those inputs private.

What has been discussed so far is referred to in the title of this contribution as classical cryptography. In contrast, quantum cryptography started with the seminal work of Bennet and Brassard [1]. The security guarantees of quantum cryptography components are very strong: their security is based on the laws of quantum physics which are beliefved to be valid forever. On the other hand, there are only a few quantum cryptography components most of which are rather resource intensive. In this paper we adress the following question: how can classical and quantum cryptography be combined in order to address important cybersecurity challenges. Our answer to this question ist twofold. First, classical cryptography and quantum key distribution (QKD) can collaborate in order to protect the confidentiality of digital communication in the long-term. Second, quantum technology can be used for the generation of secure random numbers, one of the most fundamental tasks in cryptography.

The paper is organized as follows. In Section 2 we specify the problem of long-term confidentiality protection. Section 3 eplains how QKD enables long-term confidentiality of digital communication. Section 4 discusses the importance of quantum randum number generation. Finally, Section 5 looks into the relevance of other quantum cryptography techniques from the view point of classical cryptography.

Bit length of prime number instance	Secure until until year
2048	2040
3106	2065
4096	2085
5120	2103
6144	2116

Tabelle 1: Security of instances of the discrete logarithm problem according to Lenstra and Verheul [11, 10].

2 The challenge: long-term confidentiality

A very serious challenge that classical cryptography faces today is to provide long-term confidentiality. For example, such protection is required for medical data. They may have to be kept as long as the respective patients are alive or even beyond this time. The required protection period may be more than 100 years. Other examples for sensitive long-lived data are genome data, governmental secrets, and tax data. Since required protection periods vary, we define long-term protection as protection for an indefinite time period.

Cryptographic algorithms currently used in practice do not provide long-term confidentiality since they are complexity-based. This means that their security relies on the intractability of certain algorithmic problems. This implies that complexity-based cryptosystems only remain secure for a certain time period. And this time period is hard to predict.

Consider, for example, the Diffie-Helman key exchange protocol (DH) [7]. It is used in the Transport Layer Security protocol (TLS) [6] to protect the confidentiality of Internet communication. More precisely, DH is used to exchange keys for the symmetric AES cipher [19]. The security of original DH relies on the hardness of computing discrete logarithms in the multiplicative group of a finite prime field GF(p) where the prime number p is its cardinality. When DH is used, this prime p is selected. The corresponding DH instance is secure as long as the discrete logarithm problem (DLP) in GF(p) with the chosen p remains intractable. Table 1 shows predictions for the hardness of instances of the DLP as estimated by Lenstra and Verheul [11, 10]. They are based on Moore's law [12] ("the computing speed doubles every 18 months") and on anticipated algorithmic progress. However, such predictions may be too optimistic. Peter Shor [18] proved in 1997 that quantum computers can solve the DLP in the multiplicative group of a finite field in polynomial time. So as soon as there sufficiently large quantum computers can be built, DH based on such a DLP will be useless. In fact, Shor's algorithm and variants of it provide polynomial-time solutions for all versions of the DLP that are relevant for cryptography. Since progress in quantum computer development is hard to predict, it remains unclear how long DH can be used. But just replacing DH when it becomes insecure by a quantum-secure key exchange protocol is not an option when long-term confidentiality of communicated data is required. This is because adversaries may store encrypted data now and decrypt them later when the used DH instance becomes insecure and the corresponding keys can be reconstructed. This may happen during the lifetime of the protected data. Technologically, storing encrypted data appears to be quite feasible. For instance, the Utah Data Center of the NSA has an estimated capacity of 4 to 12 Exabytes (10^{18} bytes) which allows to store huge amounts of encrypted data for a long time.

3 Quantum key distribution - enabler of long-term confidential communication

From our view point, one of the most important use cases for quantum cryptography is enabling long-term confidentiality. This is explained in this section. For more details we refer to [2].

In 1949 Claude Shannon presented his model of *information-theoretic confidentiality* protection [17] which is much stronger than complexity-based security. Intuitively, information-theoretic protection means that even computationally unbounded adversaries are unable to learn anything from ciphertexts. This means that there is no use in storing ciphertexts. In [17], Shannon proved that *one-time-pad encryption* (OTP) provides such protection. So a combination of OTP with information-theoretic secure key exchange solves the problem of long-term confidentiality protection. This is where Quantum Key Distribution (QKD) is needed. It is by far the most advanced option for long-term secure key-exchange, both theoretically and experimentally. Alternatives are key exchange by couriers and schemes based on the *bounded storage*, *noisy channel*, or *limited access* models (see [4, 21, 13]). However, QKD appears to have the strongest security: based on the laws of physics (e.g., see [16]). Also QKD backbones are being deployed in many countries such as Austria, China, Japan, Switzerland, and the USA (see [15]). In addition, in [3] a secure long-term storage system is presented that uses QKD.

There is still some way to go until OTP+QKD-based long-term confidentiality protection of communication becomes practical. OTP keys are as long as the protected data and can only be used once. So one issue is the possible QKD key rate which is currently rather limited. Also, the maximum distance between communication partners is currently limited to 300 km. For longer distances trustworthy repeaters are required. However, there is progress. Much larger key rates can be expected in the near future. Also, quantum repeaters are being developed that do not require to be trusted.

What can be done until QKD performance is satisfactory? Hybrid solutions are an option and are already being deployed. By this we mean confidentiality protection by classical symmetric encryption where QKD instead of DH takes care of the key distribution. As of today, such hybrid solutions are considered to be safe against quantum adversaries. This is because modern symmetric encryption such as AES is believed to be secure against quantum attacks except that key lengths may have to be doubled. However, such hybrid solutions still do not provide confidentiality protection for an indefinite time period as long as complexity-based encryption is used.

4 Quantum random numbers - enabler of cryptography

There is no secure cryptography without random numbers. In particular, the generation of cryptographic keys requires a reliable source of randomness. These random numbers are either used directly as keys or they are the seeds for secure random number generators. The random key generation must be implemented in such a way that adversaries cannot predict the keys. This is a real challenge. For example, in [9] the authors report on an experiment where they collected over six million public RSA keys from the Internet. Such keys are the product of two large random prime numbers. They found that almost thirteen thousand of them had a prime factor in common. Computing their gcds, the authors were able to factor these moduli and to compute the corresponding secret keys. This result means that the involved prime factors were not random. It illustrates how important true randomness is for cryptography.

A natural way of generating random numbers is to use quantum effects. In fact, companies offer quantum based devices that generate true random numbers. There are even developments that

allow for quantum random number generation on smart phones (see [14]). As is true for all cryptographic hardware, the users must trust in the proper functioning of the devices. For this, evaluation procedures must be in place. The big advantage of quantum based random number generators over other such generators is that the laws of quantum mechanics guarantee true randomness.

5 The usefulness of other quantum crypto techniques

Encouraged by the unconditional security of QKD, researchers have developed other quantum-based cryptographic schemes. Examples include quantum signature schemes [8], quantum commitment, and quantum oblivious transfer (OT) protocols [5]. Commitment schemes are used for instance in zero knowledge proofs, and secure multi-party computation.

The usefulness of these buildng blocks is less obvious than that of quantum random generation and QKD. True randomness is essential for most cryptography applications and quantum thechnology is very approprioate for this task. QKD enables long-term confidentiality and appears to be superior to its competitors, both theoretically and experimentally. For signatures, oblivious transfer, and commitments there are classical alternatives which so far outperform their quantum counterparts significantly. Also, the security of classical signatures and commitments can be prolonged, thereby providing indefinite protection (see [20]). So the security guarantees provided by quantum signatures and commitments are not required to allow for long-term security.

Literatur

[1] Charles Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, 1984.

[2] Johannes Braun, Johannes Buchmann, Ciaran Mullan, and Alex Wiesmaier. Long term confidentiality: a survey. *Designs, Codes and Cryptography*, 71(3):459–478, 2014.

[3] Johannes Braun, Johannes A. Buchmann, Denise Demirel, Mikio Fujiwara, Matthias Geihs, Shiho Moriai, Masahide Sasaki, and Atsushi Waseda. A qkd-based digital archiving solution providing everlasting confidentiality and integrity. *IACR Cryptology ePrint Archive*, 2016:742, 2016.

[4] Christian Cachin and Ueli Maurer. Unconditional security against memory-bounded adversaries. In *Annual International Cryptology Conference*, pages 292–306. Springer, 1997.

[5] Ivan B Damgård, Serge Fehr, Louis Salvail, and Christian Schaffner. Cryptography in the bounded-quantum-storage model. *SIAM Journal on Computing*, 37(6):1865–1890, 2008.

[6] T. Dierks and E. Rescorla. The Transport Layer Security (TLS) Protocol Version 1.2. RFC 5246 (Proposed Standard), August 2008. Updated by RFCs 5746, 5878, 6176, 7465, 7507, 7568, 7627, 7685.

[7] Whitfield Diffie and Martin Hellman. New directions in cryptography. *IEEE transactions on Information Theory*, 22(6):644–654, 1976.

[8] Daniel Gottesman and Isaac Chuang. Quantum digital signatures. *arXiv preprint quant-ph/0105032*, 2001.

[9] Arjen Lenstra, James P Hughes, Maxime Augier, Joppe Willem Bos, Thorsten Kleinjung, and Christophe Wachter. Ron was wrong, whit is right. Technical report, IACR, 2012.

[10] Arjen K Lenstra. Key lengths. In *The Handbook of Information Security*. Wiley, 2004.

[11] Arjen K. Lenstra and Eric R. Verheul. Selecting cryptographic key sizes. *Journal of Cryptology*, 14(4):255–293, 2001.

[12] Gordon E. Moore. *Understanding Moore's law: four decades of innovation*, chapter Moore's law at 40. Chemical Heritage Foundation, 2006.

[13] Michael O Rabin. Provably unbreakable hyper-encryption in the limited access model. In *IEEE Information Theory Workshop on Theory and Practice in Information-Theoretic Security, 2005.*, pages 34–37. IEEE, 2005.

[14] Bruno Sanguinetti, Anthony Martin, Hugo Zbinden, and Nicolas Gisin. Quantum random number generation on a mobile phone. *Physical Review X*, 4(3):031056, 2014.

[15] M. Sasaki et al. Field test of quantum key distribution in the tokyo qkd network. *Opt. Express*, 19(11):10387–10409, May 2011.

[16] Valerio Scarani, Helle Bechmann-Pasquinucci, Nicolas J. Cerf, Miloslav Dušek, Norbert Lütkenhaus, and Momtchil Peev. The security of practical quantum key distribution. *Rev. Mod. Phys.*, 81:1301–1350, Sep 2009.

[17] C. E. Shannon. Communication theory of secrecy systems. *The Bell System Technical Journal*, 28(4):656–715, Oct 1949.

[18] Peter W Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM review*, 41(2):303–332, 1999.

[19] NIST-FIPS Standard. Announcing the advanced encryption standard (AES). *Federal Information Processing Standards Publication*, 197:1–51, 2001.

[20] Martín A. Gagliotti Vigil, Johannes A. Buchmann, Daniel Cabarcas, Christian Weinert, and Alexander Wiesmaier. Integrity, authenticity, non-repudiation, and proof of existence for long-term archiving: A survey. *Computers & Security*, 50:16–32, 2015.

[21] Aaron D Wyner. The wire-tap channel. *The bell system technical journal*, 54(8):1355–1387, 1975.