Post-Quantum Cryptography – an overview

Johannes Buchmann, CYSEC, TU Darmstadt, Germany

Public key cryptography is indispensable

In the late 1970ies, public-key cryptography was invented. The two most important public-key building blocks are public-key encryption and digital signatures.

The first of these building blocks simplifies key distribution in open computer networks. It allows senders of secret messages to encrypt them with a public key while the receivers can decrypt them with their corresponding private key. Since the private key cannot be computed from the public key, the public key can be made accessible in a public directory. So no key exchange is required prior to exchanging secret messages. Instead, senders of secret messages can obtain encryption keys from the public directory.

The digital signature of a document – the second public-key building block - is generated using a secret key. It can be verified using the corresponding public key, thereby proving the authenticity of the signed document. Again, the public verification key is kept in a public directory. Therefore, anybody can validate the authenticity of the document.

The first to come up with public-key encryption and digital signature schemes were Rivest, Shamir, and Adleman in their seminal work where they proposed the RSA schemes. Alternative schemes have been proposed since. However, RSA is still most important in practice. Today, RSA protects billions of Internet communications daily via the TLS protocol. Also, RSA protects the authenticity of billions of software downloads daily, for example updates of antivirus software.

So it is fair to say that without public-key cryptography current and future IT-infrastructures would collapse.

Quantum computers threaten today's public-key cryptography

The security of the public-key schemes used today relies on the hardness of certain algorithmic problems in number theory, most importantly the integer factorization problem and the discrete logarithm problem in certain finite abelian groups. Unfortunately, these problems will not remain hard when sufficiently powerful quantum computers are available. In fact, in his famous work of 1994, Peter Shor [5] presented polynomial time algorithms for factoring integers and imputing discrete logarithms in all the relevant groups on a quantum computer. Therefore, the advent of large quantum computers will render current public-key cryptography insecure.

Post-quantum cryptography

In view of the importance of public-key cryptography and the quantum computer threat against current public-key algorithms it is necessary to come up with quantum safe public-key cryptography. Such algorithms are referred to as post-quantum cryptography algorithms.

Quantum-hard problems

The realization of post-quantum cryptography requires coming up with algorithmic problems that are hard even in the presence of quantum computers and, at the same time, can serve as the security basis of public-key cryptography algorithms. Currently, there are four such problems which are

considered very promising. Correspondingly, there are four types of post-quantum public-key cryptography:

1. Lattice-based public-key cryptography. Its security is based on the hardness of finding short or close vectors in lattices.
2. Multivariate public-key cryptography. Its security is based on the hardness of solving systems of nonlinear multivariate equations over finite fields.
3. Code-based public-key cryptography. Its security is based on the hardness of decoding linear codes, for example, Goppa-codes.
4. Hash-based signatures. Their security is based on the hardness of finding collisions of cryptographic hash functions.

It is important to note that none of the computational problems mentioned above are guaranteed to resist quantum computer attacks. However, this is a problem that post-quantum cryptography shares with classical cryptography. None of the problems that guarantee the security of classical public-key cryptography, such as the integer factorization problem or the discrete logarithm problem is guaranteed to resist attacks with classical computers. In fact, there is not a single algorithmic problem relevant for cryptography that is probably intractable. The only thing we can do is to identify good candidates and to thoroughly study their hardness.

The role of quantum cryptography

Since post-quantum cryptography still relies on mathematically unproven assumptions regarding the hardness of certain algorithmic problems, it is sometimes suggested to realize post-quantum cryptography using quantum cryptography. However, currently the most practical quantum cryptography components are random number generators and quantum key distribution. It is unclear whether quantum cryptography can implement public-key encryption and digital signatures. Therefore, quantum cryptography cannot be expected to replace classical public-key cryptography.

What is needed is an intelligent combination of classical and quantum cryptography to achieve the goal of everlasting security. The strength of quantum key distribution is to protect exchanged keys forever. Therefore, quantum key distribution can be the basis of everlasting confidentiality protection for data in transit. This will become very important in the future when data are communicated that require confidentiality protection for a very long time. At the same time, such communication also requires proofs of authenticity. But such proofs must only be verifiable when the communication actually happens, i.e. for a much shorter time. A combination of quantum key distribution and post-quantum signatures can be expected to provide the required security.

State of the art

From a practical perspective, it would be desirable to have secure and efficient public-key schemes as soon as possible.

In this respect, hash-based signatures and code-based public-key encryption are most advanced. The two best hash-based schemes are XMSS [3] and SPHINCS [1]. They have strong security proofs, implementations that show their performance, and there is even a standard draft for them (see [4]). Goppa-code-based public-key cryptography has resisted all attacks including quantum attacks since its invention in the late 1970ties. Also, several efficiency improvements now permit their use in practice (see [2]).

Lattice-based cryptography is very interesting since it allows for very strong security proofs, highly efficient schemes, and the realization of advanced functionality such as fully homomorphic encryption. However, the underlying problems appear to require more investigation. Multivariate

cryptography is interesting because it allows for extremely efficient realizations in hardware, for example on smartcards. Again, more research is required to strengthen the confidence in the hardness of the underlying problems.

[1] Daniel J. Bernstein, Daira Hopwood, Andreas H ulsing, Tanja Lange, Ruben Niederhagen, Louiza Papachristodoulou, Michael Schneider, Peter Schwabe, and Zooko Wilcox-O'Hearn. SPHINCS: Practical Stateless Hash-Based Signatures. In Elisabeth Oswald and Marc Fischlin, editors, Advances in Cryptology - EUROCRYPT 2015 - 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Sofa, Bulgaria, April 26-30, 2015, Proceedings, Part I, volume 9056 of Lecture Notes in Computer Science, pages 368-397. Springer, 2015

[2] Daniel J. Bernstein, Tung Chou, and Peter Schwabe. McBits: Fast Constant-Time Code-Based Cryptography. In Guido Bertoni and Jean-S ebastien Coron, editors, Cryptographic Hardware and Embedded Systems - CHES 2013 - 15th International Workshop, Santa Barbara, CA, USA, August 20-23, 2013. Proceedings, volume 8086 of Lecture Notes in Computer Science, pages 250{272. Springer, 2013.

[3] Johannes A. Buchmann, Erik Dahmen, and Andreas H ulsing. XMSS - A Practical Forward Secure Signature Scheme Based on Minimal Security Assumptions. In Bo-Yin Yang, editor, Post-Quantum Cryptography - 4th International Workshop, PQCrypto 2011, Taipei, Taiwan, November 29 - December 2, 2011. Proceedings, volume 7071 of Lecture Notes in Computer Science, pages 117{129. Springer, 2011.

[4] Andreas Hülsing, Denis Butin, Stefan Gazdag, and Aziz Mohaisen. XMSS: Extended Hash-Based Signatures. Crypto Forum Research Group Internet-Draft, 2015. https: //datatracker.ietf.org/doc/draft-irtf-cfrg-xmss-hash-based-signatures/

[5] Peter W. Shor. Algorithms for quantum computation: Discrete logarithms and factoring. In 35th Annual Symposium on Foundations of Computer Science, Santa Fe, New Mexico, USA, 20-22 November 1994, pages 124{134. IEEE Computer Society, 1994.