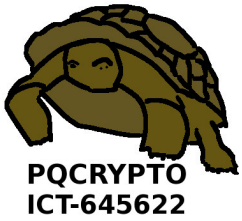

PQCRYPTO

Post-Quantum Cryptography for Long-Term Security

Project number: Horizon 2020 ICT-645622

Initial recommendations of long-term secure post-quantum systems

Due date of deliverable: none
Actual submission date: 7. September 2015

Start date of project: 1. March 2015 Duration: 3 years

Coordinator:
Technische Universiteit Eindhoven
Email: coordinator@pqcrypto.eu.org
www.pqcrypto.eu.org

Revision 1

Project co-funded by the European Commission within Horizon 2020		
Dissemination Level		
PU	Public	X
PP	Restricted to other programme participants (including the Commission services)	
RE	Restricted to a group specified by the consortium (including the Commission services)	
CO	Confidential, only for members of the consortium (including the Commission services)	

Initial recommendations of long-term secure post-quantum systems

Daniel Augot, Lejla Batina, Daniel J. Bernstein, Joppe Bos, Johannes Buchmann, Wouter Castryck, Orr Dunkelman, Tim Güneysu, Shay Gueron, Andreas Hülsing, Tanja Lange, Mohamed Saied Emam Mohamed, Christian Rechberger, Peter Schwabe, Nicolas Sendrier, Frederik Vercauteren, Bo-Yin Yang

7. September 2015
Revision 1

The work described in this report has in part been supported by the Commission of the European Communities through the Horizon 2020 program under project number 645622. The information in this document is provided as is, and no warranty is given or implied that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability.

Abstract

This document provides the PQCRYPTO project's initial recommendations for post-quantum cryptographic algorithms for symmetric encryption, symmetric authentication, public-key encryption, and public-key signatures. These recommendations are chosen for confidence in their long-term security, rather than for efficiency (speed, bandwidth, etc.). Research in the following years should lead to confidence in the security of some systems (either preexisting or developed in the project) that provide better efficiency and usability.

Keywords: Post-quantum cryptography, initial recommendations, public-key encryption, public-key signatures, secret-key encryption, secret-key authentication

1 Introduction

The EU and governments around the world are investing heavily in building quantum computers. Society needs to be prepared for the consequences, including cryptanalytic attacks accelerated by these computers. In particular, Shor's algorithm [16] shatters the foundations for deployed public-key cryptography: RSA and the discrete-logarithm problem in finite fields and elliptic curves. Long-term confidential documents such as patient health-care records and state secrets have to guarantee security for many years, but information encrypted today using RSA or elliptic curves and stored until quantum computers are available will then be as easy to decipher as Enigma-encrypted messages are today.

The PQCRYPTO project's mission is to allow users to switch to post-quantum cryptography: cryptographic systems that are not merely secure for today but that will also remain secure long-term against attacks by quantum computers. During the project, PQCRYPTO will design a portfolio of high-security post-quantum public-key systems, and will improve the speed of these systems, adapting to the different performance challenges of mobile devices, the cloud, and the Internet of Things.

This document provides PQCRYPTO's initial recommendations of long-term secure post-quantum systems. These systems were selected for confidence in their security against cryptanalytic attacks, including quantum cryptanalysis: Shor's algorithm, Grover's algorithm [9], quantum walks [1, 12], etc.

Beyond these recommendations, this document also lists some further examples of systems that are currently under evaluation, but this document does not mention any new systems under construction inside or outside PQCRYPTO. This document focuses on cryptographic primitives to be used inside higher-level cryptographic protocols and security protocols; it does not give specific recommendations for those protocols.

2 Symmetric encryption

Symmetric systems are usually not affected by Shor's algorithm, but they are affected by Grover's algorithm. Under Grover's attack, the best security a key of length n can offer is $2^{n/2}$, so AES-128 offers only 2^{64} post-quantum security. PQCRYPTO recommends thoroughly analyzed ciphers with 256-bit keys to achieve 2^{128} post-quantum security:

- AES-256 [8].
- Salsa20 [3] with a 256-bit key.

Example of another choice under evaluation: Serpent-256 [6].

3 Symmetric authentication

Some message-authentication codes provide "information-theoretic security", guaranteeing that they are as secure as the underlying cipher (within a negligible mathematically guaranteed forgery probability), even against an adversary with unlimited computing power. These authentication mechanisms are not affected by quantum computing. PQCRYPTO recommends the following mechanisms:

- GCM [13] using a 96-bit nonce and a 128-bit authenticator.

- Poly1305 [2].

4 Public-key encryption

For public-key encryption the currently used algorithms based on RSA and ECC are easily broken by quantum computers. Code-based cryptography has been studied since 1978 and has withstood attacks very well, including attacks using quantum computers. PQCRYPTO recommends the following parameters as included in McBits [4] to achieve 2^{128} post-quantum security:

- McEliece with binary Goppa codes using length $n = 6960$, dimension $k = 5413$ and adding $t = 119$ errors.

Examples of other choices under evaluation: (1) Quasi-cyclic MDPC codes [14] for McEliece with parameters at least $n = 2^{16} + 6, k = 2^{15} + 3, d = 274$ and adding $t = 264$ errors. (2) The Stehlé–Steinfeld version [17] of the NTRU [10] lattice-based cryptosystem.

5 Public-key signatures

Similar to encryption, currently used signatures are based on problems that become easy to solve with a quantum computer. Signatures use cryptographic hash functions in order to hash the message and then sign the hash. Hash-based signatures use nothing but such a hash function and thus assume the minimum requirement necessary to build signatures. PQCRYPTO recommends the following two hash-based systems to achieve 2^{128} post-quantum security:

- XMSS [7] with any of the parameters specified in [11]. XMSS requires maintaining a state.
- SPHINCS-256 [5]. SPHINCS is stateless.

Example of another choice under evaluation: the HFEv- [15] multivariate-quadratic signature system.

References

[1] Andris Ambainis. Quantum walk algorithm for element distinctness. In *45th Symposium on Foundations of Computer Science (FOCS 2004), 17-19 October 2004, Rome, Italy, Proceedings*, pages 22–31. IEEE Computer Society, 2004.

[2] Daniel J. Bernstein. The Poly1305-AES Message-Authentication Code. In Henri Gilbert and Helena Handschuh, editors, *Fast Software Encryption: 12th International Workshop, FSE 2005, Paris, France, February 21-23, 2005, Revised Selected Papers*, volume 3557 of *Lecture Notes in Computer Science*, pages 32–49. Springer, 2005.

[3] Daniel J. Bernstein. The Salsa20 Family of Stream Ciphers. In Matthew J. B. Robshaw and Olivier Billet, editors, *New Stream Cipher Designs - The eSTREAM Finalists*, volume 4986 of *Lecture Notes in Computer Science*, pages 84–97. Springer, 2008.

[4] Daniel J. Bernstein, Tung Chou, and Peter Schwabe. McBits: Fast Constant-Time Code-Based Cryptography. In Guido Bertoni and Jean-Sébastien 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.

[5] Daniel J. Bernstein, Daira Hopwood, Andreas Hülsing, 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, Sofia, Bulgaria, April 26-30, 2015, Proceedings, Part I*, volume 9056 of *Lecture Notes in Computer Science*, pages 368–397. Springer, 2015.

[6] Eli Biham, Ross J. Anderson, and Lars R. Knudsen. Serpent: A new block cipher proposal. In Serge Vaudenay, editor, *Fast Software Encryption, 5th International Workshop, FSE '98, Paris, France, March 23-25, 1998, Proceedings*, volume 1372 of *Lecture Notes in Computer Science*, pages 222–238. Springer, 1998.

[7] Johannes A. Buchmann, Erik Dahmen, and Andreas Hülsing. 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.

[8] Joan Daemen and Vincent Rijmen. *The Design of Rijndael: AES - The Advanced Encryption Standard*. Information Security and Cryptography. Springer, 2002.

[9] Lov K. Grover. A fast quantum mechanical algorithm for database search. In Gary L. Miller, editor, *Proceedings of the Twenty-Eighth Annual ACM Symposium on the Theory of Computing, Philadelphia, Pennsylvania, USA, May 22-24, 1996*, pages 212–219. ACM, 1996.

[10] Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman. NTRU: A ring-based public key cryptosystem. In Joe Buhler, editor, *Algorithmic Number Theory, Third International Symposium, ANTS-III, Portland, Oregon, USA, June 21-25, 1998, Proceedings*, volume 1423 of *Lecture Notes in Computer Science*, pages 267–288. Springer, 1998.

[11] 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/.

[12] Frédéric Magniez, Ashwin Nayak, Jérémie Roland, and Miklos Santha. Search via quantum walk. In David S. Johnson and Uriel Feige, editors, *Proceedings of the 39th Annual ACM Symposium on Theory of Computing, San Diego, California, USA, June 11-13, 2007*, pages 575–584. ACM, 2007.

[13] David A. McGrew and John Viega. The Security and Performance of the Galois/Counter Mode of Operation (Full Version). Cryptology ePrint Archive, Report 2004/193, 2004. https://eprint.iacr.org/2004/193.

[14] Rafael Misoczki, Jean-Pierre Tillich, Nicolas Sendrier, and Paulo S. L. M. Barreto. MDPC-McEliece: New McEliece variants from Moderate Density Parity-Check codes. In *Proceedings of the 2013 IEEE International Symposium on Information Theory, Istanbul, Turkey, July 7-12, 2013*, pages 2069–2073. IEEE, 2013.

[15] Jacques Patarin. Hidden fields equations (HFE) and isomorphisms of polynomials (IP): two new families of asymmetric algorithms. In Ueli M. Maurer, editor, *Advances in Cryptology - EUROCRYPT '96, International Conference on the Theory and Application of Cryptographic Techniques, Saragossa, Spain, May 12-16, 1996, Proceeding*, volume 1070 of *Lecture Notes in Computer Science*, pages 33–48. Springer, 1996.

[16] 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.

[17] Damien Stehlé and Ron Steinfeld. Making NTRU as Secure as Worst-Case Problems over Ideal Lattices. In Kenneth G. Paterson, editor, *Advances in Cryptology - EUROCRYPT 2011 - 30th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tallinn, Estonia, May 15-19, 2011. Proceedings*, volume 6632 of *Lecture Notes in Computer Science*, pages 27–47. Springer, 2011.