ECRYPT CSA

H2020-ICT-2014 – Project 645421

ECRYPT – CSA

ECRYPT – Coordination & Support Action

Whitepaper on Post-Quantum Cryptography

Due date of deliverable: None. This is an extra document
Actual submission date: 08 April 2018

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

Lead contractor: Technische Universiteit Eindhoven (TUE) Revision 1.1

Change log

Version	Contents
1.0	Short document fulfilling industry demand
1.1	Typo fixes, some small rewrites

Project co-funded by the European Commission within the H2020 Programme		
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)	

Whitepaper on Post-Quantum Cryptography

Editor
Tanja Lange (TUE)

Contributors
Daniel J. Bernstein (TUE), Wouter Castryck (KUL), Tim Güneysu (RUB),
Andreas Hülsing (TUE) Eike Kiltz (RUB), Alexander May (RUB),
Christof Paar (RUB), Frederic Vercauteren (KUL).

08 April 2018

Revision 1.1

The work described in this report has in part been supported by the Commission of the European Communities through the H2020-ICT program under contract H2020-ICT-2014 no. 645421. 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.

1 What is post-quantum cryptography and why should I care?

Post-quantum cryptography is an area of cryptography in which systems are studied under the security assumption that the attacker has a quantum computer. This attack model is interesting because Shor has shown a quantum algorithm that breaks RSA, ECC, and finite field discrete logarithms in polynomial time. This means that in this model all commonly used public-key systems are no longer secure.

Symmetric cryptography is also affected but significantly less. For systems that do not rely on mathematical structures the main effect is that an algorithm due to Grover halves the security level, i.e., breaking AES-128 takes 2^{64} quantum operations while current attacks take 2^{128} steps. While this is a big change, it can be managed quite easily by doubling the key sizes, e.g., by deploying AES-256. The operations needed in Grover's algorithm are inherently sequential which has led some to doubt that even 2^{64} quantum operations are feasible, but since the remedy of changing to larger key sizes is very inexpensive it is generally recommended to do so.

At this moment the quantum computers that exist are not large enough to pose a threat against current cryptography. However, rolling out new cryptographic systems takes a lot of time and effort, and it is thus important to have replacements in place well before large, powerful quantum computers exist.

What makes matters worse is that any ciphertext intercepted by an attacker today can be decrypted by the attacker as soon as he has access to a large quantum computer. The Snowden revelations have shown that the NSA is casually recording all Internet traffic in their datacenters such as in Bluffdale, Utah, and that they select encrypted traffic as interesting and worth storing. This means that any data encrypted using any of the standard public-key systems today will need to be considered compromised once a quantum computer exists and there is no way to protect it retroactively, because a copy of the ciphertext is in the hands of the attacker. This means that data that needs to remain confidential after the arrival of quantum computers need to be encrypted with alternative means.

Signatures can be updated and old keys can be revoked when a signature system is broken; however, not all development in the area of building quantum computers is public and it is fairly likely that the first fully-functional large quantum computer will not be publicly announced but sit in the basement of some government agency. Timing the roll-over of signature keys thus remains guesswork. On top of that, one important use case for signatures is operating-system upgrades. If a post-quantum signature system is not in place by the time an attacker has a quantum computer, then the attacker can take control of the operating system through a fake upgrade and prevent any future upgrades from fixing the problem.

2 Does quantum help against quantum?

The proponents of quantum cryptography like to portray quantum cryptography as a solution to the threat of quantum computers. However, the main problem that quantum computers create is that they break public-key cryptography. Despite the name, quantum key distribution is most akin to an authenticated cipher, in that it requires the communicating parties to have a (short) shared secret to begin with and then generates a long shared secret from that. That means it does nothing to solve the problem of how these parties obtain the shared secret, one of the main tasks of public-key cryptography and the task that needs alternatives

because of Shor's attack. On top of that, it is not possible to build signatures on quantum cryptography.

In short, the answer is that quantum cryptography does not help in dealing with the threat of quantum computers.

3 What systems will survive?

There would not be much point to speak about post-quantum systems if there were none that survive attacks by quantum computers. The usual disclaimers apply as with all of cryptography: It might be possible that more powerful attacks (quantum or not) exist that have not yet been found. Apart from that possibility, research over the last 15–20 years has built confidence in the following four areas that lead to secure systems in a post-quantum world.

Code-based: Code-based cryptography uses the theory of error-correcting codes. For some specially constructed codes it is possible to correct many errors while for random linear codes this is a difficult problem. Code-based encryption systems go back to a proposal by McEliece from 1978 and are among the most studied post-quantum schemes. Some code-based signature systems have been designed and offer short signatures but at the expense of very large key sizes. Systems based on binary Goppa codes are generally considered secure; systems based on quasi-cyclic medium-density parity checks have held up to analysis for five years and are gaining confidence.

Hash-based: Hash functions are one-way functions that map strings of arbitrary length to strings of fixed length. In the simplest version a hash-based signature on one bit is as follows. Pick two random strings, hash each of them, and publish the outputs. Reveal the first preimage to sign 0 and the second to sign 1. This signature scheme, due to Lamport from 1979, is a one-time signature scheme – once the secret is revealed it cannot be used a second time. Starting from this basic idea hash-based signatures on longer strings and on multiple messages have been built. The designs fall into stateless and stateful versions – the former work as normal signatures while for the latter the signer needs to keep track of some information, e.g., how many signatures were already made with a given key. For typical hash functions the strongest quantum attacks are well understood.

Lattice-based: On a high level, the descriptions of lattices look much like those of codes – elements are length-n vectors in some space and get error vectors added to them – but where codes typically have entries 0 or 1, lattices work with much larger numbers in each entry and errors can move away further. The problems underlying the cryptographic constructions are to find the original vector given a disturbed one. Lattices offer more parameters than codes which means that they might offer solutions better adapted to a given situation, but also offer more attack surface. Lattice-based cryptography goes back to 1996 and the designs of Ajtai and of Hoffstein, Pipher, and Silverman. Both encryption and signature systems exist.

Multivariate-system based: Finding solutions to systems of linear equations is taught in linear algebra and takes polynomial time. Changing the degree from linear to quadratic makes the problem much harder, so much so that cryptosystems and signatures have

been built on it. For encryption the polynomials are typically built with some secret trapdoor information that gets hidden by some transformation. For signature systems it is possible to start with random systems but systems built with trapdoors enjoy particularly short signatures.

A more recent suggestion for post-quantum systems is isogeny-based cryptography which uses a graph related to elliptic curves.

Much more information on the technical details, attacks used for estimating key sizes, and implementation issues can be found at the pages for the 2017 schools Executive School on Post-Quantum Cryptography, organized by ECRYPT-CSA, and Summer School on Post-Quantum Cryptography, organized by PQCRYPTO.

4 What can I do now?

If you encrypt data that needs to be kept confidential for more than 10 years and an attacker could gain access to the ciphertext you should upgrade your encryption systems to include one of the post-quantum schemes. If you build devices that will be hard to reach or to upgrade later you should include a post-quantum signature scheme now. There are many candidates submitted to NIST's competition on post-quantum cryptography and the European project PQCRYPTO has issued some recommendations. Using a hybrid solution, one that combines a post-quantum system with one of the currently common public-key systems in a way that is as strong as the strongest of the two, makes the transition and possible auditing easier.

Otherwise, you should start to prepare for migration by making a catalog of where you currently use public-key cryptography and for what purpose. Make sure to include software updates and third party products in your overview. Figure out whether you fit into one of the use cases that NIST builds – even better, get involved in the NIST discussions to make sure your use case is covered. Then wait for the outcome of the NIST competition (or quantum computers getting dangerously close, whichever comes first) to update your systems.