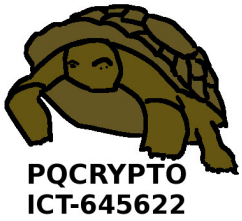

PQCRYPTO

Post-Quantum Cryptography for Long-Term Security

Project number: Horizon 2020 ICT-645622

D3.2

Cloud: Security risks in public-key cryptography

Due date of deliverable: September 2016
Actual submission date: 8. November 2016

WP contributing to the deliverable: WP3

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)	

Cloud: Security risks in public-key cryptography

Nicolas Sendrier, André Chailloux, Andreas Hüsling, Stefan Kölbl, Christian Rechberger

8. November 2016
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 PQCRYPTO. 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 deliverable serves as a progress report on Task 3.2 ("share files") of the work package 3 ("Post-quantum cryptography for the cloud ") of the PQCRYPTO project. The main purpose of this task is to identify some of the most promising techniques for public key cryptography for long term security in particular against a quantum adversary. The current document will present some preliminary results, mostly on the cryptographic techniques we wish to promote, and raise some issue concerning their security.

Keywords: public key cryptography, post-quantum, code-based, hash-based, lattice-based , multivariate

Contents

1 Introduction

The main objectives of WorkPackage 3 is to understand the means to provide very long term (50 years) protection for users data in the cloud. The Task 3.2 is dedicated to public-key cryptography, namely public-key digital signatures and public-key encryption and key exchange mechanisms.

The present deliverable makes a first assessment of the situation, reports the findings of the project participants, and raises some issues to be explored within the project lifetime and beyond. The task is focused on two target systems, hash-based digital signatures and the McEliece public-key encryption scheme. However, beyond that, the project and its participants are concerned with any research, applied and fundamental, aiming at a better understanding and a better design of cryptographic solutions for long term security, in particular in the presence of an adversary endowed with quantum computing capabilities.

During the 18 months of the reported period and within the scope of the task 3.2, the participants of the PQCRYPTO project have produced 16 research publications which have appeared in relevant international conferences and journals. In addition, they have produced 10 preprints. This preliminary report categorizes those works and explains how they coherently aggregate towards the project goals.

2 Digital Signature

2.1 Hash-Based Signatures

In the area of hash-based signatures, the participants produced several important results during the first 18 project months. Project members were and are involved in the ongoing standardization of XMSS, a stateful hash-based signature scheme, within IRTF [HBGM15], the analysis of the security of hash-based signatures [HRS16b], research on the feasibility of implementations (of hash-based signatures) on resource-constrained devices [HRS16a], and the construction of short, fixed-length input hash functions [KLMR16, GM16].

Project members are authoring an Internet-Draft within the *crypto forum research group* (CFRG) of the *Internet research task force* (IRTF). The draft is currently in last call and awaits a document shepherd for publication as *request for comments* (RFC). Besides authoring the Internet Draft, project members presented a tightened security reduction for the scheme described in the draft [HRS16b]. Compared to previous versions of the scheme, this tightened security analysis justifies to select shorter hash function output lengths, reducing the signature size, while preserving the security level. It also justifies to use a 256-bit hash function for the 256-bit classical and 128-bit quantum security level. The results can also be applied to the stateless hash-based signature scheme SPHINCS, proposed by several project members [BHH+15].

In the same work [HRS16b], project members present lower bounds on the complexity of generic quantum attacks against the security properties of hash functions underlying XMSS. This was the first work formally justifying post-quantum security claims of XMSS, as long as a hash function is used that does not have specific quantum weaknesses. The latter is assumed to apply to all "engineered" hash functions like SHA2, or SHA3.

The only practical proposal for stateless hash-based signatures so far is SPHINCS. While it achieves reasonable speed on standard CPUs (14ms on Intel Haswell CPUs) and also signature sizes reasonable on normal platforms (41KB), speed and sizes might become an issue on

resource-constrained devices. To evaluate the feasibility of using SPHINCS on such resource-constrained devices, project members did an implementation [HRS16a] on an ARM Cortex M3 with only 16KB working memory[1]. Although it was possible to demonstrate feasibility, the results also show that, on such constrained devices, a lot of struggle can be avoided if the specific setting permits the use of stateful hash-based signature schemes.

The hash-functions used within hash-based signature schemes map short, fixed-length inputs to short outputs. This is not the typical setting today's hash functions are designed for and they often achieve good performance only for long variable-length inputs. Hence, the performance of hash based signatures can be improved constructing dedicated hash functions for the short, fixed-length input setting. Project members proposed two such dedicated hash functions: Haraka [KLMR16] and Simpira [GM16]. The first benchmarks for SPHINCS using Haraka suggest that one can expect a speed-up of factor 1.99/1.87/2.86 for key generation/signing/verification on Intel Skylake CPUs.

Both Haraka and Simpira utilize AES-NI and are therefore limited to standard CPUs on newer platforms. However, recent ARM platforms (ARMv8) also come with AES specific instructions which might also allow a very efficient implementation. This aspects needs to be evaluated for both candidates. For more constrained devices it could still be interesting to explore other design strategies, if the main limiting factor are not the memory requirements.

2.2 Other Signatures

In complement to our efforts to improve and promote hash-based signatures, we had several contributions, one for lattice-based signatures [ABB+16] and one for multivariate signatures [PCY+15].

In addition, we are exploring other promising directions, namely digital signature schemes based on Zero-Knowledge (ZK) protocols. Since Fiat and Shamir seminal work [FS87], ZK protocols can be transformed into signature scheme. The so-called Non-Interactive Zero-Knowledge (NIZK) protocols can be derived from various quantum resistant primitives, in particular from multivariate crypto [CHR+16] and code-based crypto [Sen16], but also lattice-based crypto. Those construction have some merits but they have security issues which are discussed in §5.

3 Public-Key Encryption / Key Exchange Mechanisms

3.1 McEliece Encryption Scheme

The original McEliece public-key encryption scheme, using binary Goppa codes, has successfully resisted to almost 40 years of cryptanalysis efforts. It enjoys numerous interesting features: its security is well understood and can be accurately estimated in the current state of the art and it can be efficiently and securely implemented [BCS13][2]. This system can be considered as mature and, during this eighteen months period, no researcher within the project or outside has found results changing the state of the art.

One limitation of the scheme comes from the size of the public keys, which make it less suitable for some applications, as key exchange mechanisms with forward secrecy in which a public key has to be transmitted at every instance of the scheme. To improve this aspect

[1] This work was performed within WP1, we mention it here for the sake of completeness

[2] http://www.win.tue.nl/~tchou/mcbits/

a quasi-cyclic variant, namely QC-MDPC-McEliece has been proposed recently [MTSB13], with similarly good security arguments and an easy implentation [HvMG13, Cho16]. A very recent result[3] points out the existence of decryption failure and how to use them to recover the secret key. This side channel attack do not threaten all applications, in particular key exchange mechanisms can avoid it. However, this issue must be addressed and the design failure-free variants of QC-MDPC-McEliece is one of the challenges that the project participants intend to solve. A first step has already been made [CS16].

3.2 Other techniques

Multivariate crypto also offers some interesting lines of work to produce really public-key encryption schemes [SDP15].

Last but not least, in the first 18 months of the project, some of our contributions to produce key exchange mechanisms based on lattices have recieved at lot of attention [ADPS16, BCD+16b] and is likely to produce secure and practical primitives. We definitely intend to pursue this research direction.

4 Security Assessment

4.1 Generic Techniques

This category of security arguments relates to the underlying hard algorithmic problems. Those problems are essentially, finding short vectors (lattice-based crypto), decoding in a linear code (code-based crypto), or solving polynomial systems (multivariate crypto). They are of major importance for selecting secure parameters for the considered schemes. The key issues are to keep track and to contribute to the state of the art for the design of algorithms solving those problems, and, in the case of this project, to find their best quantum variants.

The participants have contributed in lattice-based cryptography with two papers, the first improves the state of the art for computing short vectors in ideal lattices [BNvdP16], the second proves that instances of LWE with binary errors can be solved more efficiently than expected [BGPW16].

We also have two results for code-based cryptography, the first one explores the case where the error weight is small compared with the code length and concludes that all recent improvements of generic decoding techniques are inefficient in that case [CTS16]. This is important in practice since the QC-MDPC-McEliece variant falls into this category. Another work deals with generic decoding for the rank metric [HT15]. Rank metric is an alternative to the Hamming metric for designing code-based cryptosystems, the research community needs to explore the possibilities and limitations of this technique.

4.2 Structural Attacks

This second category of security arguments relates to attacks or properties which target a specific variant of the schemes.

Two of our contributions relate to lattices, more specifically to Ring-LWE, and expose weaknesses of particular variants [CIV16b, CIV16a].

[3] Thomas Johansson, Paul Stankovski and Qian Guo, *A Key Recovery Attack on MDPC with CCA Security Using Decoding Errors*, to appear at ASIACRYPT, in December 2016

Two other contributions prove that some specific constructions of code-based cryptography are unsafe, one breaks a variant of McEliece using polar codes [BCD+16a] and the other breaks a digital signature scheme based on LDGM (Low Density Generator Matrix) codes [PT16].

Other results [FOP+16b, FOP+16a, CCP14] relate to code-based cryptography, and though they do not break a specific proposed scheme, they help to understand the limits of what is secure and what is not when designing code-based public-key schemes.

5 Some Issues with Protocols in a Quantum Setting

The Fiat-Shamir construction [FS87] is a way to transform a zero-knowledge protocol into a signature scheme. Even if the underlying computational assumptions are secure against quantum adversaries, the security proof itself doesn't directly imply security against quantum adversaries. Some proof techniques, such as *rewinding* or the use of a *random oracle*, do not translate immediately to the quantum setting and require more work.

Quantum rewinding. When considering for example zero-knowledge protocols, we need to construct an efficient simulator that will simulate the distribution of transcripts between the prover and the verifier. In order to do so, we often ask this simulator to perform backtracking also called in this setting rewinding. Some outcomes of the simulator will be invalid transcripts and we ask the simulator to go back to a previous step of the simulation and start again with new randomness. In the quantum setting, we would also ask the quantum simulator to rewind to a previous state in the computation. This rewinding can depend on some outcomes *i.e.* measurements of the simulator and therefore its reversibility is lost. An additional complication is that the simulator has access to a single copy of prior knowledge, an auxiliary quantum state, that he uses for the simulation so this quantum rewinding should not destroy this state.

Quantum random oracle model In the random oracle model, hash functions used in some cryptographic protocol are replaced by idealized random functions, which sometimes helps in proving security of the protocol. In order to prove security, it is often required to tweak the random oracle depending on past inputs. In the quantum setting, queries to the random oracle can be made in superposition. When the input of the random oracle is not a well defined string, those tweaking techniques do not necessarily apply and therefore proving security is more challenging and requires techniques tailored for this quantum setting.

In [Unr15], Unruh showed how solve these problems specifically for the Fiat Shamir construction. However several other constructions are still not known to be secure against quantum adversaries.

References

[ABB+16] Sedat Akleylek, Nina Bindel, Johannes Buchmann, Juliane Krämer, and Giorgia Azzurra Marson. An efficient lattice-based signature scheme with provably secure instantiation. In David Pointcheval, Abderrahmane Nitaj, and Tajjeeddine Rachidi, editors, *Progress in Cryptology – AFRICACRYPT 2016*, volume 9646 of *LNCS*, pages 44–60. Springer, 2016. https://www.cdc.informatik.tu-darmstadt.de/fileadmin/user_

upload/Group_CDC/An_Efficient_Lattice-Based_Signature_Scheme_with_Provably_Secure_Instantiation.pdf.

[ADPS16] Erdem Alkim, Léo Ducas, Thomas Pöppelmann, and Peter Schwabe. Post-quantum key exchange – a new hope. In *Proceedings of the 25th USENIX Security Symposium*. USENIX Association, 2016. https://cryptojedi.org/papers/#newhope.

[BCD+16a] Magali Bardet, Julia Chaulet, Vlad Dragoi, Ayoub Otmani, and Jean-Pierre Tillich. Cryptanalysis of the McEliece public key cryptosystem based on polar codes. In Tsuyoshi Takagi, editor, *PQCrypto 2016*, volume 9606 of *LNCS*, pages 118–143. Springer, 2016. https://hal.inria.fr/hal-01240856.

[BCD+16b] Joppe Bos, Craig Costello, Léo Ducas, Ilya Mironov, Michael Naehrig, Valeria Nikolaenko, Ananth Raghunathan, and Douglas Stebila. Frodo: Take off the ring! practical, quantum-secure key exchange from LWE. Cryptology ePrint Archive, Report 2016/659, 2016. http://eprint.iacr.org/2016/659.

[BCS13] Daniel J. Bernstein, Tung Chou, and Peter Schwabe. McBits: Fast constant-time code-based cryptography. In Guido Bertoni and Jean-Sébastien Coron, editors, *CHES 2013*, volume 8086 of *LNCS*, pages 250–272. Springer, 2013.

[BGPW16] Johannes Buchmann, Florian Göpfert, Rachel Player, and Thomas Wunderer. On the hardness of LWE with binary error: Revisiting the hybrid lattice-reduction and meet-in-the-middle attack. Cryptology ePrint Archive, Report 2016/089, 2016. http://eprint.iacr.org/2016/089.

[BHH+15] Daniel J. Bernstein, Daira Hopwood, Andreas Hülsing, Tanja Lange, Ruben Niederhagen, Louiza Papachristodoulou, Peter Schwabe, and Zooko Wilcox-O'Hearn. SPHINCS: practical stateless hash-based signatures. In Marc Fischlin and Elisabeth Oswald, editors, *Advances in Cryptology – EUROCRYPT 2015*, volume 9056 of *LNCS*, pages 368–397. Springer, 2015. Document ID: 5c2820cfddf4e259cc7ea1eda384c9f9, http://cryptojedi.org/papers/#sphincs.

[BNvdP16] Joppe W. Bos, Michael Naehrig, and Joop van de Pol. Sieving for shortest vectors in ideal lattices: a practical perspective. *International Journal of Applied Cryptography*, 2016. to appear, http://eprint.iacr.org/2014/880.

[CCP14] Alain Couvreur, Irene Marquez Corbella, and Ruud Pellikaan. A polynomial time attack against algebraic geometry code based public key cryptosystems. *CoRR*, abs/1401.6025, 2014. https://arxiv.org/abs/1401.6025, revised 2016.

[Cho16] Tung Chou. QcBits: Constant-time small-key code-based cryptography. In Benedikt Gierlichs and Axel Y. Poschmann, editors, *CHES 2016*, volume 9813 of *LNCS*, pages 280–300. Springer, 2016. http://www.win.tue.nl/~tchou/papers/qcbits.pdf.

[CHR+16] Ming-Shing Chen, Andreas Hülsing, Joost Rijneveld, Simona Samardjiska, and Peter Schwabe. From 5-pass MQ-based identification to MQ-based signatures.

Cryptology ePrint Archive, Report 2016/708, 2016. http://eprint.iacr.org/2016/708.

[CIV16a] Wouter Castryck, Ilia Iliashenko, and Frederik Vercauteren. On error distributions in ring-based LWE. Cryptology ePrint Archive, Report 2016/240, 2016. http://eprint.iacr.org/2016/240.

[CIV16b] Wouter Castryck, Ilia Iliashenko, and Frederik Vercauteren. Provably weak instances of Ring-LWE revisited. In Marc Fischlin and Jean-Sébastien Coron, editors, *Advances in Cryptology - EUROCRYPT 2016*, volume 9665 of *LNCS*, pages 147–167. Springer, 2016. https://eprint.iacr.org/2016/239.

[CS16] Julia Chaulet and Nicolas Sendrier. Worst case QC-MDPC decoder for McEliece cryptosystem. In *IEEE Conference, ISIT 2016*, pages 1366–1370. IEEE Press, 2016. https://arxiv.org/abs/1608.06080.

[CTS16] Rodolfo Canto-Torres and Nicolas Sendrier. Analysis of information set decoding for a sub-linear error weight. In Tsuyoshi Takagi, editor, *PQCrypto 2016*, volume 9606 of *LNCS*, pages 144–161. Springer, 2016. https://hal.inria.fr/hal-01244886.

[FOP+16a] Jean-Charles Faugère, Ayoub Otmani, Ludovic Perret, Frédéric de Portzamparc, and Jean-Pierre Tillich. Folding alternant and Goppa codes with non-trivial automorphism groups. *IEEE Trans. Information Theory*, 62(1):184–198, 2016. http://arxiv.org/abs/1405.5101.

[FOP+16b] Jean-Charles Faugère, Ayoub Otmani, Ludovic Perret, Frédéric de Portzamparc, and Jean-Pierre Tillich. Structural cryptanalysis of McEliece schemes with compact keys. *Des. Codes Cryptography*, 79(1):87–112, 2016. https://hal.inria.fr/hal-00964265.

[FS87] A. Fiat and A. Shamir. How to prove yourself: Practical solutions to identification and signature problems. In A.M. Odlyzko, editor, *Advances in Cryptology - CRYPTO '86*, volume 263 of *LNCS*, pages 186–194. Springer, 1987.

[GM16] Shay Gueron and Nicky Mouha. Simpira v2: A family of efficient permutations using the AES round function. Cryptology ePrint Archive, Report 2016/122, 2016. http://eprint.iacr.org/2016/122.

[HBGM15] Andreas Hülsing, Denis Butin, Stefan-Lukas Gazdag, and Aziz Mohaisen. XMSS: Extended hash-based signatures. Internet Draft, IETF Crypto Forum Research Group, 2015. https://datatracker.ietf.org/doc/draft-irtf-cfrg-xmss-hash-based-signatures/.

[HRS16a] Andreas Hülsing, Joost Rijneveld, and Peter Schwabe. ARMed SPHINCS. In Chen-Mou Cheng, Kai-Min Chung, Giuseppe Persiano, and Bo-Yin Yang, editors, *Public-Key Cryptography – PKC 2016: 19th IACR International Conference on Practice and Theory in Public-Key Cryptography, Taipei, Taiwan, March 6-9, 2016, Proceedings, Part I*, pages 446–470, Berlin, Heidelberg, 2016. Springer Berlin Heidelberg. https://cryptojedi.org/papers/#armedsphincs.

[HRS16b] Andreas Hülsing, Joost Rijneveld, and Fang Song. Mitigating multi-target attacks in hash-based signatures. In Chen-Mou Cheng, Kai-Min Chung, Giuseppe Persiano, and Bo-Yin Yang, editors, *Public-Key Cryptography – PKC 2016: 19th IACR International Conference on Practice and Theory in Public-Key Cryptography, Taipei, Taiwan, March 6-9, 2016, Proceedings, Part I*, pages 387–416, Berlin, Heidelberg, 2016. Springer Berlin Heidelberg. https://eprint.iacr.org/2015/1256.

[HT15] Adrien Hauteville and Jean-Pierre Tillich. New algorithms for decoding in the rank metric and an attack on the LRPC cryptosystem. In *IEEE Conference, ISIT 2015*, pages 2747–2751. IEEE Press, 2015. https://arxiv.org/abs/1504.05431.

[HvMG13] Stefan Heyse, Ingo von Maurich, and Tim Güneysu. Smaller keys for code-based cryptography: QC-MDPC McEliece implementations on embedded devices. In Guido Bertoni and Jean-Sébastien Coron, editors, *CHES*, volume 8086 of *LNCS*, pages 273–292. Springer, 2013.

[KLMR16] Stefan Kölbl, Martin M. Lauridsen, Florian Mendel, and Christian Rechberger. Haraka v2 - efficient short-input hashing for post-quantum applications. Cryptology ePrint Archive, Report 2016/098, 2016. http://eprint.iacr.org/2016/098.

[MTSB13] 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 *IEEE Conference, ISIT 2013*, pages 2069–2073, Instanbul, Turkey, July 2013.

[PCY+15] Albrecht Petzoldt, Ming-Shing Chen, Bo-Yin Yang, Chengdong Tao, and Jintai Ding. Design principles for hfev- based multivariate signature schemes. In Tetsu Iwata and Jung Hee Cheon, editors, *Advances in Cryptology - ASIACRYPT 2015*, volume 9452 of *LNCS*, pages 311–334. Springer, 2015. http://www.iis.sinica.edu.tw/papers/byyang/19342-F.pdf.

[PT16] Aurélie Phesso and Jean-Pierre Tillich. An efficient attack on a code-based signature scheme. In Tsuyoshi Takagi, editor, *PQCrypto 2016*, volume 9606 of *LNCS*, pages 86–103. Springer, 2016. https://hal.inria.fr/hal-01244640.

[SDP15] Alan Szepieniec, Jintai Ding, and Bart Preneel. Extension field cancellation: a new central trapdoor for multivariate quadratic systems. Cryptology ePrint Archive, Report 2015/1184, 2015. http://eprint.iacr.org/2015/1184.

[Sen16] Nicolas Sendrier. Stern-based NIZK digital signatures. presented at PQCRYPTO miniworkshop, June 2016. https://pqcrypto.eu.org/miniws/szks.pdf.

[Unr15] Dominique Unruh. Non-interactive zero-knowledge proofs in the quantum random oracle model. In Elisabeth Oswald and Marc Fischlin, editors, *Advances in Cryptology - EUROCRYPT 2015*, volume 9057 of *LNCS*, pages 755–784. Springer, 2015.