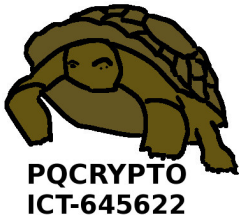

PQCRYPTO

Post-Quantum Cryptography for Long-Term Security

Project number: Horizon 2020 ICT-645622

D3.3

Cloud: Long-term authenticated ciphers

Due date of deliverable: February 28, 2018
Actual submission date: April 13, 2018

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: Long-term authenticated ciphers

Gustavo Banegas, Gaetan Leurent, Stefan Kölbl, Martin M. Lauridsen,
Christian Rechberger, Peter Schwabe

April 13, 2018
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 concludes Task 3.1 on authenticated encryption and specifies authenticated ciphers that are designed to last for 50 years. The current document will present an analysis of impact of quantum computer on the most widely used authenticated encryption schemes and provides recommendations for authenticated ciphers with long-term security.

Keywords: authenticated encryption, block ciphers

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 3.1 is dedicated to authenticated encryption.

The central challenge in Task 3.1 was to understand the impact of quantum computers upon the security of secret-key cryptography. Large parts of this deliverable hence detail what is known in this domain including new insights gained in the course of the work of WP3. This security analysis is now guiding WP3s contribution to the design of new authenticated ciphers that gives some assurance to remain safe far into the future. Hence towards the end of the deliverable we apply various criteria to candiate authenticated encryption schemes and we conclude with a recommendation of a AE system co-designed by WP3, including links to implementations.

2 State of Authenticated Encryption

Secret-key cryptography has a tradition for holding open competitions to identify new and better designs for current problems in the field. The CAESAR (Competition for Authenticated Encryption: Security, Applicability, and Robustness) competition is an ongoing NIST-sponsored competition to identify a portfolio of authenticated ciphers. The portfolio will offer advantages over the current standard AES-GCM (AES in Galois/Counter mode), and will be suitable for widespread adoption. In a nutshell, an authenticated cipher is a secret-key cryptographic primitive which provides confidentiality, integrity and authenticity in a combined solution, rather than combining encryption with a MAC (which is usually referred to as generic composition). Future work includes new designs that reflect all what is expected from a good CAESAR candidate while at the same time offering more than 256-bits of key size and resistance also against quantum versions of cryptanalytic attacks.

3 Post-Quantum Security of Authenticated Encryption

In the classical setting, the main security notion is against chosen plaintext attacks (IND-CPA): an adversary is given access to an oracle implementing a cryptographic algorithm, and must distinguish the oracle's output from random values, or recover the secret key. There are several ways to extend this scenario to a quantum setting. In the weakest model, the adversary has the same classical oracle, and can use a quantum computer to perform computations on the data collected from the classical oracle. However this model assumes that there is no quantum interaction between the attacker and the oracle, which might be a strong assumption when quantum computers are available. In order to understand the impact of such interactions, a stronger model has been proposed, where the adversary can send superposition queries to the oracle, and receive the corresponding superposition of outputs. There are several difficulties to reach a good security definition that captures interesting attacks but still allows secure schemes: a security notion for encryption schemes has been formalized as IND-qCPA by Boneh and Zhandry [BZ13], and a corresponding notion for authenticated encryption schemes has been studied by Soukharev, Jao, and Seshadri[SJS16]. This model is very powerful for the adversary, but it is still possible build secure systems. In particular, aiming for security in this model is more significant than with only classical queries.

3.1 Grover's algorithm

Consider a function F mapping n-bit values to a single bit, and where there is just a single input v such that $F(v) = 1$. Say we would like to determine the unique value v which maps to 1 under F. In classical computing, the best one can do, without using any knowledge about the structure of F, is to try each input to F and see if it is the sought value. In other words, the complexity for solving this problem is $O(2^n)$. Grover's algorithm, attributed to Lov Grover, is a quantum algorithm which allows to solve this problem in just $O(2^{n/2})$ *quantum queries* to F. This asymptotic bound has been proven optimal in 1997 [BBBV97].

To use Grover's algorithm, one needs a quantum implementation of F, i.e. an implementation which operates on quantum states. In the scope of our function F, a quantum state is essentially a superposition of all 2^n inputs to F itself. If we denote the 2^n inputs to F by $x_1, \ldots, x_{2^n}$, we would write such a quantum state in *ket notation* as

$$|x\rangle = 2^{-n/2}(|x_1\rangle + |x_2\rangle + \cdots + |x_{2^n}\rangle). \tag{1}$$

By applying quantum operations on $|x\rangle$, the quantum state would approach the pure state $|v\rangle$, thus increasing the probability that when measured, the state would collapse into the correct state v, representing the correct answer to the inversion of the function F. This algorithm can be used to get a quadratic speedup for finding preimages or generic key recovery attacks.

We can summarize Grover's algorithm as presented in Masahito et al [HIK+14]:
Input: a function $F : \{0,1\}^n \to \{0,1\}$, where it has a unique solution $x_0 \in \{0,1\}^n$ of $f(x_0) = 1$.
Output: the unique solution $x_0 \in \{0,1\}^n$ satisfying the above equation.

For simplicity, the initial qubit sequence will be $|0^n\rangle |1\rangle$, and let θ be the value satisfying $\sin\theta = \sqrt{\frac{1}{N}}$.

1. Apply the Hadamard transform $\mathbf{H}$ to the $n+1$ qubits.
2. Iterate steps 3 and 4, $\lfloor \frac{\pi}{4\theta} \rfloor$ times.
3. Apply U_f to whole of the $n+1$ qubits.
4. Apply the diffusion matrix D_n to the first n qubits.
5. Output classical n bits obtained by measuring the first n qubits.

3.2 Simon's algorithm

This algorithm gives an exponential speedup for finding collisions, if they occur with some periodicity. Consider a function $F : \{0,1\}^n \to \{0,1\}^n$ and the promise that there exists $s \in \{0,1\}^n$ such that for any $x, y \in \{0,1\}^n$, $f(x) = f(y)$ holds if and only if $x \oplus y \in \{0^n, s\}$. The target is to find s. In the classical setting this can be solved by searching for collisions, which has a complexity of $\Theta(2^{n/2})$, while Simon's algorithm allows to solve this problem in $O(n)$.

The main problem in the direct application of this algorithm is that it requires that only a very specific class of collisions occur, which is in general not true for cryptographic primitives. However, some first applications have been found recently [KLLN16].

3.3 Brute-force key-recovery

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. More precisely, the attack requires just a few known plaintext/ciphertext pairs, so that an attacker can implement a function F to test a key candidate. By building a quantum circuit implementing F, he can apply Grover's algorithm to F. SAT solvers are often described as doing intelligent brute-force search. There is however evidence that some classes of problems steming from cryptography could enjoy more than square-root, perhaps even exponential speed- up[Mon16].

3.4 Multi-Target Attacks

The most important pre-quantum threat to symmetric cryptography, in special AES-128, is the 1994 van Oorschot–Wiener "parallel rho method", a low-communication parallel pre-quantum multi-target preimage-search algorithm. This algorithm uses a mesh of p small processors, each running for approximately $2^{128}/pt$ fast steps, to find one of t independent AES keys $k_1, \ldots, k_t$, given the ciphertexts $\mathrm{AES}_{k_1}(0), \ldots, \mathrm{AES}_{k_t}(0)$ for a shared plaintext 0. The paper from Banegas and Bernstein [BB17] introduces a different quantum algorithm for multi-target preimage search. This algorithm shows, in the same realistic parallel setting, that quantum preimage search benefits asymptotically from having multiple targets. The new algorithm requires a revision of NIST's AES-128, AES-192, and AES-256 security claims.

The parallelization of Grover's algorithm raises several problems and in the paper they tackle some of these problems, i.e., reversibility and communication between the processes. In the paper, the authors describe two settings that they called free of communication and realistic model. The free of communication gives an analysis when it is not considered costs for the the network that the processors are running. However, that is not a realistic scenario for parallel computation and this costs should be demonstrated when a quantum algorithm is used in parallel. The advantages for the algorithm from [BB17] is that they use a really small amount of memory for their computations. [BB17] shows that the free communication model has a cost of $\sqrt{N/pt}$ and in the realistic model $\sqrt{N/pt^{1/2}}$, where N is the size of database, p number of parallel instances of Grover and t the number of pre-images to search.

4 Security of Cryptographic Primitives

Since cryptanalysis is the main way we evaluate the security of symmetric primitives, it is important to understand the impact of quantum computers on cryptanalysis.

Recently, a paper studying the influence of quantum computing on two of the most important attacks on symmetric primitives, namely differential and linear cryptanalysis, has been published [KLLN15]. For both techniques the authors show that one can get a quadratic speed-up if the attacker can query the secret function with superposition states. In particular, differential and linear cryptanalysis can be more efficient than brute-force key-recovery with Grover's algorithm when there is a differential trail with probability $p \gg 2^{-n}$ (leading to a quantum attack with complexity $O(1/\sqrt{p})$), or a linear trail with bias $\varepsilon \gg 2^{-n/2}$ (leading to a quantum attack with complexity $O(1/\varepsilon)$). If the attacker has only access to a classical oracle, the main part of the attack is usually the data collection, with complexity $O(1/p)$ or $O(1/\varepsilon^2)$, so that there is no speed up on quantum computers. However, if the block-size is smaller than the key size, like in AES-256, quantum differential cryptanalysis and quantum

linear cryptanalysis can be faster than Grover's algorithm. The work also show that truncated differential cryptanalysis, a variant of differential cryptanalysis, receives a smaller speed-up in the quantum model. In particular, the optimal quantum attack is not always a quantum version of the optimal classical attack.

Another work has studied the impact of quantum computing on slide attacks, a class of attacks exploiting a special iterative structure in some block ciphers [KLLN16]. Surprisingly, slide attacks can receive an exponential speed-up in the quantum setting, using Simon's algorithm, with complexity $O(n)$ rather than $O(2^{n/2})$.

5 Security of Modes of Operation

There are also several recent works studying the security of modes of operation in the quantum setting. In particular, these works illustrate the importance of defining the right security model.

First, a paper by Anand et al. [ATTU16] investigated the security of various modes of operations for encryption against superposition attacks. They show that OFB and CTR remain secure, while CBC and CFB are not secure in general (with attacks involving Simon's algorithm), but are secure if the underlying PRF is quantum secure.

More surprisingly, a very recent work by Kaplan et al. [KLLN16] shows that the most common authentication and authentication modes are *not* secure against superposition queries. Using Simon's algorithm, they show how to build forgeries for CBC-MAC, PMAC, GCM, OCB, and several CAESAR candidates with complexity $O(n)$. This shows that the impact of quantum computer on symmetric cryptography can be much higher than previously thought.

Another work by Kaplan [Kap14] studies the impact of quantum attacks on iterated block ciphers. This suggests that the time-space tradeoffs for meet- in-the-middle attacks are different in the quantum setting and also indicates that bigger gains over classic attacks can be expected if the block cipher is iterated more times.

6 CAESAR Competition

CAESAR [1] (Competition for Authenticated Encryption: Security, Applicability, and Robustness) is a new competition in order to create a portfolio of authenticated encryption schemes. This includes both modes of operation, which can be used with any suitable (tweakable) block cipher or permutation, and dedicated designs.

The competition was announced in 2013 receiving a total of 56 submissions and is currently in the final round before the final portfolio will be released. The remaining schemes in the competition are: ACORN, AEGIS, Ascon, COLM, Deoxys-II, MORUS and OCB.

ACORN is a dedicated authenticated encryption scheme based on linear feedback shift registers (LFSR) and its main design criteria is to be efficient in hardware. ACORN only supports a key size of 128 bits and a tag size of 128 bits. Due to the limited key size it is not suited for long-term security in the post-quantum setting.

AEGIS is based on the AES round function and optimized for current platforms. There are several variants of AEGIS and from those only AEGIS-256 provides a 256-bit key and is therefore suitable for long-term use.

[1] For more information see https://competitions.cr.yp.to/index.html.

Ascon is a permutation based authenticated encryption scheme using the sponge construction and well suited for hardware implementations while also performing well on 64-bit platforms. The only key size supported is 128 bits and therefore it is not well suited for a long-term secure scheme. Various implementations for Ascon are publicly availabe at https://ascon.iaik.tugraz.at/.

COLM is a mode of operation to construct an authenticated encryption scheme from a block cipher. COLM provides nonce-misuse resistance, but the current proposal only considers an instantiation with AES-128.

Deoxys-II is an authenticated encryption scheme based on tweakable block ciphers. It is based on a tweakable variant of AES, supports 256-bit keys and provides nonce-misuse resistant.

Morus is another dedicated authenticated encryption scheme optimized for hardware and current platforms. There are several variants and for the post-quantum setting only MORUS-1280-256 would provide long-term security.

OCB (RFC 7253[2]) is a mode for authenticated encryption based on a block cipher. A variant instantiated with AES-256 would provide a sufficient level of security.

For the final round the schemes have been chosen for different use-cases:

- Lightweight applications: Schemes that are suitable for resource-constraint enviroments (e.g. Internet of Things). Prioritizes low-cost implements in hardware and microcontrollers over the performance.
- High performance: Schemes designed to have a high performance on current general purpose computers. This could be seen as in line with currently widely used schemes like AES-GCM.
- Defense in depth: Schemes which are more robust and harder to misuse in practice. This schemes provide security against nonce-misuse and ideally security should only degrade gracefully.

A list of all CAESAR finalists, their category and post-quantum security level is given in Table 6.1. A broad performance comparison of all the schemes on various platforms can be found at https://bench.cr.yp.to/results-caesar.html, including optimized implementations for those schemes.

7 Recommendations

For any long-term security against an adversary with a quantum computer the size of the secret keys used in an authenticated encryption scheme should be at least 256 bits, ideally more to mitigate multi-target attacks.

The currently most widely used authenticated encryption scheme GCM can be used in combination with AES-256 to achieve this and is already widely deployed. Other valid choices include Salsa20–Poly1305 with a 256-bit key, which was already included in PQCRYPTO's initial recommendations; and its variant ChaCha20–Poly1305 with a 256-bit key, which is now widely deployed in TLS. The candidates of the final round of the CAESAR depict the current state of research on authenticated encryption, however one has to be careful as several of the finalists do not support a key size of 256-bit.

[2]See https://tools.ietf.org/html/rfc7253

Table 6.1: List of the candidates for the final round of the CAESAR competition. Case 1 is for lightweight applications resource (resource constraint enviroments), Case 2 for high-performance applications and Case 3 for defense in-depth. The security level refers to the costs for an adversary to recover the secret key. Note that authenticity might be broken at lower costs if a small tag size is used.

	Design	Post-Quantum Security Level
Case 1	ACORN	64-bit
	Ascon	64-bit
Case 2	AEGIS	128-bit (only AEGIS-256)
	MORUS	128-bit (only MORUS-1280-256)
	OCB	128-bit (with AES-256)
Case 3	COLM	64-bit
	Deoxys-II	128-bit

Out of the final CAESAR candidates Deoxys-II seems to be good choice for a post-quantum secure authenticated encryption scheme as it is both robust against nonce-misuse and supports a 256-bit key. Deoxys-II however requires a tweakable block cipher and there are currently no dedicated standards. At the moment Deoxys-II is proposed with a tweakable variant of AES. Alternatively, Deoxys-II could also be instantiated with the lightweight tweakable block cipher Skinny [BJK+16] co-designed by project members, which would be better suited for resource-constraint enviroments.

Skinny is a lightweight tweakable block cipher and has one of the smallest hardware footprint among all block ciphers. It further comes with strong security guarantees against all known cryptanalytical attacks, provides a high security margin and also allows efficient implementations protected against side-channel attacks. Implementations for a large set of platforms, including both hardware and software, of the Skinny cipher have been made publicly available on the project website[3].

References

[ATTU16] Mayuresh Vivekanand Anand, Ehsan Ebrahimi Targhi, Gelo Noel Tabia, and Dominique Unruh. Post-quantum security of the CBC, CFB, OFB, CTR, and XTS modes of operation. In *Post-Quantum Cryptography - 7th International Workshop, PQCrypto 2016, Fukuoka, Japan, February 24-26, 2016, Proceedings*, pages 44–63, 2016.

[BB17] Gustavo Banegas and Daniel J. Bernstein. Low-communication parallel quantum multi-target preimage search. In *SAC*, volume 10719 of *Lecture Notes in Computer Science*, pages 325–335. Springer, 2017.

[BBBV97] Charles H. Bennett, Ethan Bernstein, Gilles Brassard, and Umesh Vazirani. Strengths and weaknesses of quantum computing. *SIAM Journal on Computing*, 26(5):1510–1523, 1997.

[3] https://sites.google.com/site/skinnycipher/home

[BJK+16] Christof Beierle, Jérémy Jean, Stefan Kölbl, Gregor Leander, Amir Moradi, Thomas Peyrin, Yu Sasaki, Pascal Sasdrich, and Siang Meng Sim. The SKINNY family of block ciphers and its low-latency variant MANTIS. In *CRYPTO (2)*, volume 9815 of *Lecture Notes in Computer Science*, pages 123–153. Springer, 2016.

[BZ13] Dan Boneh and Mark Zhandry. Secure signatures and chosen ciphertext security in a quantum computing world. Cryptology ePrint Archive, Report 2013/088, 2013. http://eprint.iacr.org/.

[HIK+14] Masahito Hayashi, Satoshi Ishizaka, Akinori Kawachi, Gen Kimura, and Tomohiro Ogawa. *Introduction to Quantum Information Science*. Springer, 2014.

[Kap14] Marc Kaplan. Quantum attacks against iterated block ciphers. 2014. arXiv:1410.1434.

[KLLN15] Marc Kaplan, Gaëtan Leurent, Anthony Leverrier, and María Naya-Plasencia. Quantum Differential and Linear Cryptanalysis. 2015. arXiv:1510.05836.

[KLLN16] Marc Kaplan, Gaëtan Leurent, Anthony Leverrier, and María Naya-Plasencia. Breaking Symmetric Cryptosystems using Quantum Period Finding. 2016. arXiv:1602.05973.

[Mon16] Ashley Montanaro. Quantum walk speedup of backtracking algorithms. 2016. arXiv:1509.02374.

[SJS16] Vladimir Soukharev, David Jao, and Srinath Seshadri. Post-quantum security models for authenticated encryption. In *Post-Quantum Cryptography - 7th International Workshop, PQCrypto 2016, Fukuoka, Japan, February 24-26, 2016, Proceedings*, pages 64–78, 2016.