PQCRYPTO
ICT-645622

Horizon 2020

PQCRYPTO

Post-Quantum Cryptography for Long-Term Security

Project number: Horizon 2020 ICT-645622

Task 3.1 Cloud: Security Risks in Secret-key Cryptography

Due date of deliverable: M12
Actual submission date: 17. March 2016

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)	

Task 3.1 Cloud: Security Risks in Secret-key Cryptography

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

17. March 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 document provides the first deliverable for WP3 (Post-quantum cryptography for the cloud) under the PQCRYPTO project. It serves as a progress report on Task 3.1 ("encrypt at home"). The main purpose of this document is to describe recent research on the impact of quantum computers on the security of secret-key cryptography, much of which was and is performed by project members.

Keywords: Post-quantum cryptography, secret-key encryption, secret-key authentication, secret-key cryptanalysis

1 Quantum-Cryptanalysis

Quantum computers would have a tremendous impact on the security of asymmetric cryptography, because Shor's algorithm can factor integers and compute discrete logarithms in polynomial time on a quantum computer. On the other hand, their impact on symmetric cryptography seem to be smaller, but this topic has received much less attention, and is not as well understood.

It is known that quantum computers can speed up generic attacks like exhaustive search and collision finding. These algorithms usually only give polynomial speedups and it would be sufficient to increase the key size to restore the desired security level. However, these are basic quantum algorithms which do not exploit any specific structure of the underlying primitives. This leaves the big open question of finding new and improving more advanced cryptanalysis techniques using quantum computing. We first describe the generic attack due to Grover, and subsequently more recent work that (1) applies Grover's algorithm as a building-block in non-generic attacks, (2) finds non-generic attacks that go beyond what Grover's algorithm can do.

1.1 Security Models

Quantum attacks against asymmetric crypto-systems require only the public key, and use quantum computations to recover the secret key from the public key much faster than is possible with a classical computer.

For symmetric crypto-systems, the situation is different. 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 [5], and a corresponding notion for authenticated encryption schemes has been studied by Soukharev, Jao, and Seshadri[11]. 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.

1.2 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 [3].

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 [6]:
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.

1.3 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 [9].

2 General considerations for symmetric-key crypto, and recent progress

We now give a quick review of the main known attacks against symmetric crypto-systems using quantum computers.

2.1 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[10].

2.2 Cryptanalysis of 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 [8]. 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 [9]. Surprisingly, slide attacks can receive an exponential speed-up in the quantum setting, using Simon's algorithm, with complexity $O(n)$ rather than $O(2^{n/2})$.

2.3 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. [1] 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. [9] 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 [7] 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.

3 Future work

Due to recent progress discussed above it is clear that more research is needed to establish confidence in currently used designs and design approaches in symmetric-key cryptography. In addition to exploring then above-mentioned works more, the following topics are interesting: **Multi-target attacks.** The standard AES-128 block cipher has held up well against more than a decade of cryptanalysis, allowing only slight brute-force-like "biclique" speedups in key searches[4]. However, one should not think that attacking AES-128 has a cost anywhere near 2^{128}. Generic "multi-target" attacks mean that the security level of a cipher drops as the cipher is used to encrypt more and more data. Furthermore, Grover's algorithm potentially finds an AES key using just 2^{64} quantum AES queries, and there are multi-target variants of Grover's algorithm that use even fewer queries, although the circuit complexity of those variants is still an open question. Another open question in this area, is the use of Grover's algorithm in parallel quantum computation for multi-target attacks. In the work of Beals et al [2] an improvement in the search using distributed quantum computing is shown and the authors present the Multi-Grover search algorithm.

The maximum key size allowed by the AES standard is 256 bits. Multi-target Grover breaks AES-256 using considerably fewer than 2^{128} queries. This motivates designs that support more than 256-bit of key size.

Authenticated ciphers. 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.

References

[1] 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.

[2] Robert Beals, Stephen Brierley, Oliver Gray, Aram W Harrow, Samuel Kutin, Noah Linden, Dan Shepherd, and Mark Stather. Efficient distributed quantum computing. In

Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences, volume 469, page 20120686. The Royal Society, 2013.

[3] 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.

[4] Andrey Bogdanov, Dmitry Khovratovich, and Christian Rechberger. Biclique cryptanalysis of the full AES. In Dong Hoon Lee and Xiaoyun Wang, editors, *Advances in Cryptology - ASIACRYPT 2011*, volume 7073 of *LNCS*, pages 344–371. Springer, 2011.

[5] 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/.

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

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

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

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

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

[11] 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.