Breaking Symmetric Cryptosystems using Quantum Period Finding

M. Kaplan G. Leurent A. Leverrier M. Naya-Plasencia

Abstract

Due to Shor's algorithm, quantum computers are a severe threat for public key cryptography. This motivated the cryptographic community to search for quantum-safe solutions. On the other hand, the impact of quantum computing on secret key cryptography is much less understood. In this paper, we consider attacks in the *quantum chosen plaintext* model, in which an adversary can query an oracle implementing a cryptographic primitive in a quantum superposition of different states. The adversary is then very powerful, but recent results show that it is nonetheless possible to design secure cryptosystems.

We introduce new applications of a quantum procedure called *Simon's algorithm* (the simplest quantum period finding algorithm) in order to attack symmetric cryptosystems in this model. Following previous works in this direction, we show that several classical attacks based on finding collisions can be dramatically sped up using Simon's algorithm: finding a collision requires $\Omega(2^{n/2})$ queries in the classical setting, but when collisions happen with some hidden periodicity, they can be found with only $O(n)$ queries in the quantum model.

We obtain attacks with very strong implications. First, we show that the most widely used modes of operation for authentication and authenticated encryption (*e.g.* CBC-MAC, PMAC, GMAC, GCM, and OCB) are completely broken in this security model. Our attacks are also applicable to many CAESAR candidates: CLOC, AEZ, COPA, OTR, POET, OMD, and Minalpher.

Second, we show that slide attacks can also be sped up using Simon's algorithm. This is the first exponential speed up of a classical symmetric cryptanalysis technique in the quantum model.

1 Introduction

In this paper, we show that Simon's algorithm can be used to break symmetric cryptosystems. We consider an attack model in which, in addition to local quantum operations, an adversary is granted an access to a remote cryptographic oracle in superposition of the inputs, and obtains the corresponding superposition of outputs. In past works, this model have been called *superposition attacks* [4] or *quantum chosen message attacks* [3].

We prove the following results. **(i)** We first analyze Simon's algorithm with an approximate promise, and improve the analysis of previous applications of Simon's algorithm in symmetric cryptography.

(ii) We then show an attack against the LRW construction, used to turn a block-cipher into a tweakable block cipher [7]. Like the results against 3-round Feistel and Even-Mansour, this is an example of construction with provable security in the classical setting that becomes insecure against a quantum adversary.

(iii) Next, we study block cipher modes of operation. We show that some of the most common modes for message authentication and authenticated encryption are completely broken in this setting. We describe forgery attacks against standardized modes (CBC-MAC, PMAC, GMAC, GCM, and OCB), and against several CAESAR candidates, in linear complexity in the size of the block. In particular, this partially answers an open question by Boneh and Zhandry: "Do the CBC-MAC or NMAC constructions give quantum-secure PRFs?" [3].

Those results are in stark contrast with a recent analysis of encryption modes in the same setting: Anand *et al.* show that some classical encryption modes are secure against a quantum adversary when using a quantum-secure PRF [1]. Our results imply that some authentication and authenticated encryption schemes remain insecure with *any* block cipher.

(iv) The last application is a quantization of slide attacks, a popular family of cryptanalysis that is independent of the number of rounds of the attacked cipher. Our result is the first exponential quantum speed up of a classical cryptanalysis technique, with complexity dropping from $O(2^{n/2})$ to $O(n)$, where n is the size of the block.

These results imply that for the symmetric primitives we analyze, doubling the key length as suggested by attacks based on Grover's search, may not be sufficient to restore security against more clever quantum adversaries. A significant effort on quantum cryptanalysis of symmetric primitives is thus crucial for our long-term trust in these cryptosystems.

2 Simon's algorithm with approximate promise

For $f : \{0,1\}^n \to \{0,1\}^n$ such that $f(x \oplus s) = f(x)$ for all x, define

$$\varepsilon(f,s) = \max_{t \in \{0,1\}^n \setminus \{0,s\}} \Pr_x[f(x) = f(x \oplus t)]. \tag{1}$$

This parameter measures how far the function is from satisfying Simon's promise perfectly. For a random function, one expects $\varepsilon(f,s) = \Theta(n2^{-n})$; for a constant function, $\varepsilon(f,s) = 1$ and it is impossible to recover s.

Theorem 1. *If $\varepsilon(f,s) \leq p_0 < 1$, then Simon's algorithm returns s with cn queries, with probability at least $1 - \left(2\left(\frac{1+p_0}{2}\right)^c\right)^n$.*

In particular, choosing $c > (1 - \log_2(1+p_0))^{-1}$ ensures that the failure probability decreases exponentially with n. For our results, it is sufficient to bound $\varepsilon(f,s)$ by a constant. In general, if this is not satisfied, it implies the existence of a classical distinguisher for the underlying block cipher.

3 Application to the LRW construction

The LRW construction, introduced by Liskov, Rivest and Wagner [7], turns a block cipher E_k into a tweakable block cipher, *i.e.* a family of uncorrelated block ciphers $\widetilde{E}_{t,k}$. The tweakable block cipher is a very useful primitive to build modes for encryption, authentication, or authenticated encryption. In particular, tweakable block ciphers and the LRW construction were inspired by the first version of OCB, and later versions of OCB use the tweakable block ciphers formalism. The LRW construction uses a (almost) universal hash function h (which is part of the key), and is defined as : $\widetilde{E}_{t,k}(x) = E_k(x \oplus h(t)) \oplus h(t)$. We consider that the cryptographic oracle queried by the adversary $\widetilde{E}_{t,k}$ takes two inputs: the block x to be encrypted and the tweak t.

For the quantum attack, fix two arbitrary tweaks t_0, t_1, with $t_0 \neq t_1$, and consider the function

$$f(x) = E_k\big(x \oplus h(t_0)\big) \oplus h(t_0) \oplus E_k\big(x \oplus h(t_1)\big) \oplus h(t_1).$$

Given a superposition access to an oracle for an LRW tweakable block cipher, we can build a circuit implementing this function. It is easy to see f satisfies the promise of Simon's problem: $f(x) = f(x \oplus s)$ with $s = h(t_0) \oplus h(t_1)$. Furthermore, we bound the quantity $\varepsilon(f,s) = \max_{t \in \{0,1\}^n \setminus \{0,s\}} \Pr[f(x) = f(x \oplus t)]$. If $\varepsilon(f,s) > 1/2$, there exists some t with $t \notin \{0,s\}$ such that $\Pr[f(x) = f(x \oplus t)] > 1/2$, *i.e.*,

$$\Pr[\widetilde{E}_k\big(x\big) \oplus \widetilde{E}_k\big(x \oplus s\big) \oplus \widetilde{E}_k\big(x \oplus t\big)\big) \oplus \widetilde{E}_k\big(x \oplus t \oplus s\big) = 0] > 1/2$$

where $\widetilde{E}_k(x) = E_k(x \oplus h(t_0))$. We show that if it was the case, there would be a simple distinguisher for E with $O(2^{3n/4})$ queries.

Therefore, $\varepsilon(f,s) \leq 1/2$ if E is a well-chosen block cipher, and running Simon's algorithm with the function f returns $h(t_0) \oplus h(t_1)$. On the other hand, with an ideal tweakable block cipher, f is a pseudo-random function, and Simon's algorithm returns 0. We can thus distinguish the LRW construction from an ideal tweakable block cipher with $O(n)$ quantum queries to $\widetilde{E}$.

This attack is important, because many recent modes of operation are inspired by the LRW construction, and the XE and XEX instantiations, such as CAESAR candidates AEZ, COPA, OCB, OTR, Minalpher, OMD, POET. The details of these attacks can be found in the full version of the paper.

4 Simon's algorithm applied to slide attacks

In 1999, Wagner and Biryukov introduced the technique called *slide attack* [2]. It can be applied to a block cipher $\widetilde{E}_K$ that consist of r applications of an identical round function R, each one parametrized by the same key K. In this case, the cipher is simply $\widetilde{E}_K = R_K \circ \ldots \circ R_K$

The attacker collects $2^{n/2}$ encryptions of plaintexts. Amongst these couples of plaintext-ciphertext, with large probability, he gets a "slid" pair, that is, a pair of couples (P_0, C_0) and (P_1, C_1), where C_i is the ciphertext corresponding to P_i, and such that $R(P_0) = P_1$. This immediately implies that $R(C_0) = C_1$. For the attack to work, the function R needs to allow for an efficient recognition of such pairs, which in turns makes the key extraction from R easy.

We illustrate our technique with the key-alternate cipher with blocks of n bits, identical subkeys and no round constants. In this case, $R = E_k$ for some ideal cipher E_K. The complexity of the classical slide attack is $O(2^{n/2})$, equivalent to a quantum attack based on Grover's algorithm. For a quantum adversary, define the following function:

$$f : b, x \quad \mapsto \begin{cases} P(E_k(x)) \oplus x & \text{if } b = 0, \\ E_k(P(x)) \oplus x & \text{if } b = 1. \end{cases}$$

The slide property shows that all x satisfy $P(E_k(x)) \oplus k = E_k(P(x \oplus k))$. This implies that f satisfies the promise of Simon's problem with $s = 1 \,\|\, k$. In order to apply Simon's algorithm, we bound $\varepsilon(f, 1 \,\|\, k)$. If $\varepsilon(f, 1 \| k) > 1/2$, there exist (τ, t) with $(\tau, t) \notin \{(0, 0), (1, k)\}$ such that: $\Pr[f(b, x) = f(b \oplus \tau, x \oplus t)] > 1/2$. For $\tau = 0$ (resp. $\tau = 1$), this implies that there is a differential in $P \circ E_k$ or $E_k \circ P$ (resp. $E_k \circ P$) with probability $1/2$ which does not happen for a random permutation. In both cases, this implies the existence of an efficient disinguisher.

Finally we conclude that $\varepsilon(f, 1 \,\|\, k) \leq 1/2$, unless $E_k \circ P$ or $P \circ E_k$ have differentials with probability $1/2$. Therefore, we can apply Simon's algorithm to get k.

5 Conclusion

We have showed that symmetric cryptography is far from ready for the post quantum world. We have found exponential speed-ups on attacks on symmetric cryptosystems. In consequence, some cryptosystems that are believed to be safe in a classical world become vulnerable in a quantum world. We successfully applied our technique in the following cases. For 3-round **Feistel** and **Even-Mansour**, we have extended and fixes previous attacks by Kuwakado and Morii [6, 5]. We have found a distinguisher for **LRW**. We found forgery attacks for the following message authentication code: **CBC-MAC**, **PMAC** and **GMAC**. Interestingly, these attacks also make legitimate use of the nonces of the cryptosystem. In the case of authenticated encryption, we show how to forge tags for **GCM** and **OCB**. Finally, we have showed that a number of CAESAR candidates can be attacked using Simon's algorithm: **CLOC**, **AEZ**, **COPA**, **OTR**, **POET**, **OMD** and **Minalpher**.

With the speed-up on slide attacks, we provided the first known exponential quantum speed-up of a classical attack. This attack now becomes very powerful. An interesting follow-up would be to seek other such speed-ups of cryptanalytic techniques. For authenticated encryption, we have shown that many modes of operations that are believed to be secure in the classical world, become completely broken in the post-quantum world. More constructions might be broken following the same ideas.

Full version: The full version of this work can be found at the address: `http://arxiv.org/abs/1602.05973`.

References

[1] M. V. Anand, E. E. Targhi, G. N. Tabia, and D. Unruh. Post-quantum security of the CBC, CFB, OFB, CTR, and XTS modes of operation. In *PQCrypto 2016*, 2016. to appear.

[2] Alex Biryukov and David Wagner. Slide attacks. In *Fast Software Encryption, 6th International Workshop, FSE '99*, pages 245–259, 1999.

[3] Dan Boneh and Mark Zhandry. Secure signatures and chosen ciphertext security in a quantum computing world. In *Advances in Cryptology - CRYPTO 2013*, pages 361–379, 2013.

[4] Ivan Damgård, Jakob Funder, Jesper Buus Nielsen, and Louis Salvail. Superposition attacks on cryptographic protocols. In *ICITS*, pages 142–161, 2013.

[5] H. Kuwakado and M. Morii. Quantum distinguisher between the 3-round feistel cipher and the random permutation. In *International Symposium on Information Theory Proceedings*, pages 2682–2685, 2010.

[6] H. Kuwakado and M. Morii. Security on the quantum-type even-mansour cipher. In *International Symposium on Information Theory and its Applications*, pages 312–316, 2012.

[7] M. Liskov, R. L. Rivest, and D. Wagner. Tweakable block ciphers. *J. Cryptology*, 24(3):588–613, 2011.