CR04 report – Breaking Symmetric Cryptosystems using Quantum Period Finding

Arthur Blot

January 3, 2017

1 Introduction

Quantum computers are a severe threat to our modern cryptography, as with Shor's algorithm [14], assymetric cryptography may not be secure anymore.

However, the problem has been less studied for symmetric cryptography in the past. Using Grover's algorithm [5], one can find the private key of an encryption scheme using $\mathcal{O}(\sqrt{n})$ operations instead of an optimal $\mathcal{O}(n)$ in the classical setting (where n is the number of possible keys). This means that in the general case, doubling the key size could be enough to restore the same level of security as before. But is this result still optimal for schemes of symmetric cryptography?

The paper [6] proves that it is not the case: using Simon's algorithm [15] and some properties of its behavior in the non-ideal case that we are going to detail next, the authors manage to break the security of some symmetric cryptographic constructions, followed by many widely used message authentication and authenticated encryption modes (ie, algorithms used to forge authentication codes supposedly unforgeable by an unauthenticated user). The complexity of the attack goes from an exponential one in the classical setting to a linear one. It ends by detailing how to speed-up a known attack strategy in the quantum setting: slide attacks.

2 Simon's algorithm and attack strategy

2.1 Simon's algorithm and results

As we already know, Simon's problem [15] is given by:

Given $f : \{0,1\}^n \to \{0,1\}^n$ such that there exists $s \in \{0,1\}^n$ which verifies for all $x, y \in \{0,1\}^n$, $[f(x) = f(y)] \Leftrightarrow [x \oplus y \in \{0^n, s\}]$, find s.

We will call the hypothesis over f of this problem **Simon's promise**.

It can be solved using quantum circuits in $\mathcal{O}(n)$, with high probability. For the record, the algorithm works by returning in $\mathcal{O}(1)$ time a vector orthogonal to s.

However, the condition on the function may not always be met. We will suppose that there is always a s respecting the condition, but that it may not be the only one. In that

case, we define ε, which will be bigger if there are more "collisions" (ie, x, y such that $f(x) = f(y)$):

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

In the perfect case where all the collisions have difference s, we have $\varepsilon(f, s) = 0$, and ε will go up to 1, which is the only value for which s can never be recovered.

In order to exploit Simon's algorithm in the non-ideal case, we use the following theorem:

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

If we have no bound on $\varepsilon(f, s)$, we can still establish the following result:

Theorem 2. *After cn steps of Simon's algorithm, if t is orthogonal to all the vectors returned by the different steps of the algorithm, then for all p_0, $\Pr_x[f(x \oplus t) = f(t)] \geq p_0$ with probability at least $1 - \left(2\left(\frac{1+p_0}{2}\right)^c\right)^n$.*

2.2 Attack strategy

The general attack strategy will rely on applying Simon's algorithm on a function handcrafted from the encryption system, which we shall name Simon's function, such that there exists s which verifies:

- $f(x) = f(x \oplus s)$ for all x
- we have $\varepsilon(f, s) < 1$
- s gives some information which helps break the cryptosystem

The function f will always be such that it can be computed by a quantum circuit, although we are not going to detail it here.

3 Three-round Feistel, Even-Mansour construction

3.1 Three-round Feistel

The Feistel scheme is a classical algorithm used to build a random permutation out of random functions or permutations, proved secure in the classical setting [11].

A three-round Feistel scheme takes (x_L, x_R) as an input and gives $(y_L, y_R) = E(x_L, x_R)$ as an output, with:

$$(u_0, v_0) = (x_L, x_R) \quad (u_i, v_i) = (v_{i-1} \oplus R_i(u_{i-1}), u_{i-1}), \quad (y_L, y_R) = (u_3, v_3)$$

The attack was described by Kuwakado and Morii [8] in the case where the R_i are permutations, which is the case we are going to consider first. It uses the following as

Simon's function, where $\alpha_0 \neq \alpha_1$ are arbitrary constants:

$$\begin{aligned} f : \{0,1\} \times \{0,1\}^n &\to \{0,1\}^n \\ b, x &\mapsto y_R \oplus \alpha_b \quad \text{where } (y_R, y_L) = E(\alpha_b, x) \end{aligned}$$

which gives:

$$f(b,x) = R_2(x \oplus R_1(\alpha_b))$$

Then, we can prove that:

$$f(b',x') = f(b,x) \Leftrightarrow \begin{cases} x' \oplus x = 0 & \text{if } b' = b \\ x' \oplus x = R_1(\alpha_0) \oplus R_1(\alpha_1) & \text{if } b' \neq b \end{cases}$$

Applying Simon's algorithm on this function with $s = 1 \parallel R_1(\alpha_0) \oplus R_1(\alpha_1)$ gives $R_1(\alpha_0) \oplus R_1(\alpha_1)$, which makes it distinguishable from a random permutation, because applying Simon's algorithm on a random permutation gives 0 with overwhelming probability [3] (this is a consequence of Theorem 2).

Moreover, the article shows that the result extends when the R_i are random functions in general. In order to do this, we just need to prove that $\varepsilon(f,s) < 1$: actually, we have $\varepsilon(f,s) < 1/2$, which can be proven using Theorem 1 and the fact that random functions have few enough collisions [3].

3.2 Even-Mansour construction

The Even-Mansour construction [4] is a way to build a block cipher from a public permutation P:

$$E_{k_1,k_2}(x) = P(x \oplus k_1) \oplus k_2$$

This construction is secure in the classical setting, requiring $2^{n/2}$ queries, where n is the size of x.

However, it was shown by Kuwakado and Morii [9] that the construction is broken in the quantum setting, using this function:

$$\begin{aligned} f : \{0,1\} &\to \{0,1\}^n \\ x &\mapsto E_{k_1,k_2}(x) \oplus P(x) = P(x \oplus k_1) \oplus P(x) \oplus k_2 \end{aligned}$$

It can again be shown that we have $f(x \oplus k_1) = f(x)$ (ie, what we want with $s = k_1$) and $\varepsilon(f,k_1) < 1/2$. Therefore, Simon's algorithm gives us k_1, which obviously breaks the construction.

4 LRW construction

The LRW construction [10] turns a block cipher into a family of unrelated block ciphers. Given a universal hash function h (which is part of the key), we define:

$$\widetilde{E}_{t,k}(x) = E_k(x \oplus h(t)) \oplus h(t)$$

We will use the following function as Simon's function:

$$\begin{aligned} f : \{0,1\}^n &\to \{0,1\}^n \\ x &\mapsto \widetilde{E}_{t_0,k}(x) \oplus \widetilde{E}_{t_1,k}(x) \end{aligned}$$

which gives

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

The function satisfies $f(x) = f(x \oplus s)$ with $s = h(t_0) \oplus h(t_1)$, and it can again be shown that it satisfies $\varepsilon(f, s) \leq 1/2$ with overwhelming probability, assuming E_k behaves as a random permutation (which is a reasonable assumption, since it is needed for the security of the construction).

This gives a distinguisher between the LRW construction and an ideal block cipher, which would give 0 with overwhelming probability as seen for the three-round Feistel scheme.

Moreover, h is often of the form $h(t) = f(t) \cdot L$, where L is a secret offset, that $h(t_0) \oplus h(t_1)$ reveals. This is the case of MACs and authenticated encryption we are going to see later.

5 Block cipher modes of operation

The most popular block-cipher based MACs and message authentication schemes are broken in the quantum setting: the article presents attacks for CBC-MAC and some variants, GMAC, PMAC, GCM, OCB and some CAESAR candidates. In all cases, a classical attack would take $\mathcal{O}(2^{n/2})$ operations in the classical cases, but only takes $\mathcal{O}(n)$ in the quantum case.

We will consider a single block cipher E_k acting on blocks of size n and associated with the key k, and that the message is M composed of l blocks of size n: $M = m_1 \parallel \ldots \parallel m_l$. Also, we will consider that the output is of size n.

5.1 CBC-MAC

A MAC (Message Authentication Code) is a code associated to a message used to guarantee its authenticity. Its security is therefore defined by the unability to forge a code for a message by someone with no access to k. More precisely, the attacker must produce $q + 1$ valid tags after only q queries to an oracle producing the MACs, ie, the attacker must produce a valid tag for an input for which he could not query the oracle.

CBC-MAC is one of the first MAC constructions to be created. Here, we will consider the Encrypted-CBC-MAC variant [1] of CBC-MAC (because the original one is unsafe in the classical case). It is defined as (where the key is composed of k and k'):

$$x_0 = 0 \quad x_i = E_k(x_{i-1} \oplus m_i) \quad \text{CBC-MAC}(M) = E_{k'}(x_l)$$

Again, we will define Simon's function, for two arbitrary message blocks $\alpha_0 \neq \alpha_1$:

$$\begin{aligned} f : \{0,1\} \times \{0,1\}^n &\to \{0,1\}^n \\ b, x &\mapsto \text{CBC-MAC}(\alpha_b \parallel x) = E_{k'}(E_k(x \oplus E_k(\alpha_b))) \end{aligned}$$

Which verifies:

$$f(b', x') = f(b, x) \Leftrightarrow \begin{cases} x' \oplus x = 0 & \text{if } b' = b \\ x' \oplus x = E_k(\alpha_0) \oplus E_k(\alpha_1) & \text{if } b' \neq b \end{cases}$$

ie, Simon's promise for $s = 1 \parallel E_k(\alpha_0) \oplus E_k(\alpha_1)$.

We can therefore get $E_k(\alpha_0) \oplus E_k(\alpha_1)$ using Simon's algorithm and forge messages using the following scheme:

1. Compute the tag of $\alpha_0 \parallel m_1$ for any m_1,
2. Use it for $\alpha_1 \parallel m_1 \oplus E_k(\alpha_0) \oplus E_k(\alpha_1)$.

Let us define q' the number of (quantum) queries made by Simon's algorithm to learn $E_k(\alpha_0) \oplus E_k(\alpha_1)$. By running the previous forging scheme $q' + 1$ times for different m_1 (which needs $q' + 1$ additional (classical) queries, one for each $\alpha_0 \parallel m_1$), we can forge $2(q' + 1)$ tags, by only using a total of $q' + (q' + 1) = 2q' + 1$ queries (q' for Simon's algorithm, $q' + 1$ for the $\alpha_0 \parallel m_1$). So the security of the code is indeed broken, because we produced more tags ($2(q' + 1)$) than we made queries ($2q' + 1$).

5.2 PMAC

PMAC [12] is a parallelizable MAC which uses secret offsets Δ_i part of the secret key to turn a block cipher into a tweakable block cipher. It is defined as:

$$c_i = E_k(m_i \oplus \Delta_i) \quad \text{PMAC}(M) = E_k^*(m_l \oplus \sum c_i)$$

where E_k^* is a tweakable block cipher.

Similarly to the attack of LRW, we can get the difference of two Δ_i by using:

$$\begin{aligned} f : \{0,1\}^n &\to \{0,1\}^n \\ x &\mapsto \text{PMAC}(m \parallel m \parallel 0^n) = E_k^*(E_k(m \oplus \Delta_0) \oplus E_k(m \oplus \Delta_1)) \end{aligned}$$

which satisfies $f(m \oplus s) = f(m)$ for $s = \Delta_0 \oplus \Delta_1$. It can be shown that $\varepsilon(f, s) \leq 1/2$ when E is a good cipher, and Simon's algorithm can be used to get the value of $\Delta_0 \oplus \Delta_1$.

Valid tags can hence be forged, similarly as for CBC-MAC, because the tag for $m_1 \parallel m_1$ for an arbitrary m_1 is also valid for $m_1 \oplus \Delta_0 \oplus \Delta_1 \parallel m_1 \oplus \Delta_0 \oplus \Delta_1$. Moreover, for PMAC, offsets are defined as $\Delta_i = \gamma(i) \cdot L$, where γ is a Gray encoding. L can thus be recovered from $\Delta_0 \oplus \Delta_1$, giving the ability to recover all the Δ_i.

5.3 OCB

OCB [13] [12] [7] is an authenticated encryption mode: out of a message M (which will be encrypted) and an associated data A (which will only be authenticated), we will return the encrypted message, along with an authentication tag τ. It will require a nonce N, which is a non-repeating input which we will suppose chosen randomly by the oracle in our security definitions.

Then, by finding a f_N which depends on the nonce N but such that $f_N(M) = f_N(M \oplus \Delta)$ for any nonce N, we can use the previous strategy with a random nonce to recover Δ. If Δ is correctly chosen to be secret, this will provide a valid attack.

OCB is built from the LRW construction previously described. More precisely, it takes as an input a nonce N, a message $M = m_1 \parallel \ldots \parallel m_l$ and associated data $A = a_1 \parallel \ldots \parallel a_@$ and returns a ciphertext $C = c_1 \parallel \ldots \parallel c_l$ and a tag τ:

$$c_i = E_k(m_i \oplus \Delta_i^N) \quad \tau = E_k(\Delta_l'^N \oplus \sum m_i) \oplus \sum b_i \quad b_i = E_k(a_i \oplus \Delta_i)$$

which gives, when the message is empty, the tag:

$$\mathrm{OCB}_k(N, \varepsilon, A) = \phi_k(N) \oplus \sum b_i \quad b_i = E_k(a_i \oplus \Delta_i)$$

which can be seen as a random variant of PMAC.

Moreover, the Δ_i are independent from the nonce N, so we can apply the same strategy as for PMAC and produce forgery attacks by using:

$$\begin{aligned} f_N : \{0,1\}^n &\to \{0,1\}^n \\ x &\mapsto \mathrm{OCB}_k(N, \varepsilon, x \parallel x) = E_k(x \oplus \Delta_0) \oplus E_k(x \oplus \Delta_1) \oplus \phi_k(N) \end{aligned}$$

which verifies $f_N(a \oplus \Delta_0 \oplus \Delta_1) = f_N(a)$ and $\varepsilon(f_N, \Delta_0 \oplus \Delta_1) \leq 1/2$ in the same conditions as for the PMAC, which allows us to apply the same forgery attack even by using a random nonce N.

6 Slide attacks

Slide attacks [2] is a class of attacks appliable to some cryptosystems, whose complexity goes from $\mathcal{O}(2^{n/2})$ in the classical setting to $\mathcal{O}(n)$ in the quantum setting.

It can be applied to block ciphers made of r applications of the same round function R, parametrized by the same key k. The attack works independently of r, and only works in the case R is vulnerable to plaintext attacks.

In the classical setting, the attacker must collect $2^{n/2}$ encryptions of plaintexts, and must find among it a pair of couples plaintext-ciphertext (P_0, C_0) and (P_1, C_1) such that $R(P_0) = P_1$, which implies that $R(C_0) = C_1$ (R is supposed to make these couples recognizable easily). A plaintext attack therefore breaks the scheme. This attack is therefore faster than a bruteforce attack by a quadratic speed-up.

Using Simon's algorithm, the attack can even become of linear complexity. In order to do this, we will denote P the unkeyed round function, and E_k the whole encryption function. We then define:

$$\begin{aligned} f : \{0,1\} \times \{0,1\}^n &\to \{0,1\}^n \\ b, x &\mapsto \begin{cases} P(E_k(x)) \oplus x & \text{if } b = 0 \\ E_k(P(x)) \oplus x & \text{if } b = 1 \end{cases} \end{aligned}$$

The slide property (which is basically the property saying that we get the same circuit by "shifting" the series of R) gives that $P(E_k(x)) \oplus k = E_k(P(x \oplus k))$, hence:

$$f(0, x) = P(E_k(x)) \oplus x = E_k(P(x \oplus k)) \oplus k \oplus x = f(1, x \oplus k)$$

Therefore, f satisfies what we want with $s = 1 \parallel k$. It can be proved that $\varepsilon(f, s) \leq 1/2$, and thanks to Simon's algorithm, k can be recovered in $\mathcal{O}(n)$.

7 Conclusion

The article is really a breakthrough into the analysis of security of our current symmetric cryptographic schemes in the post-quantum world. It shows that most of the symmetric cryptography modes are completely broken in the quantum setting. Moreover, slide attacks received an exponential speedup, also breaking cryptosystems which are sensitive to it in the classical setting. More constructions might be broken in the quantum setting, so, in the same way as post-quantum assymetric cryptography, post-quantum symmetric cryptography will be very different from the one in the classical setting.

However, the article mostly deals with constructions based on already existing block ciphers (with the three-round Feistel, LRW) and authenticated modes, the attacks on authenticated encryption often being based on techniques close to the ones on authenticated modes. Symmetric encryption algorithms such as AES, which is probably the most used nowadays, are not referred to in the article, and so, remain for now unattacked.

References

[1] M. Bellare, J. Kilian, and P. Rogaway. The security of the cipher block chaining message authentication code. *J. Comput. Syst. Sci.*, 61(3):362–399, Dec. 2000.

[2] A. Biryukov and D. Wagner. Slide attacks. In L. R. Knudsen, editor, *Fast Software Encryption, 6th International Workshop, FSE '99, Rome, Italy, March 24-26, 1999, Proceedings*, volume 1636 of *Lecture Notes in Computer Science*, pages 245–259. Springer, 1999.

[3] J. Daemen and V. Rijmen. Probability distributions of correlation and differentials in block ciphers. *J. Mathematical Cryptology*, 1(3):221–242, 2007.

[4] S. Even and Y. Mansour. A construction of a cipher from a single pseudorandom permutation. *J. Cryptology*, 10(3):151–162, 1997.

[5] L. K. Grover. A fast quantum mechanical algorithm for database search. In G. L. Miller, editor, *Proceedings of the Twenty-Eighth Annual ACM Symposium on the Theory of Computing, Philadelphia, Pennsylvania, USA, May 22-24, 1996*, pages 212–219. ACM, 1996.

[6] M. Kaplan, G. Leurent, A. Leverrier, and M. Naya-Plasencia. Breaking symmetric cryptosystems using quantum period finding. In M. Robshaw and J. Katz, editors, *Advances in Cryptology - CRYPTO 2016 - 36th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2016, Proceedings, Part II*, volume 9815 of *Lecture Notes in Computer Science*, pages 207–237. Springer, 2016.

[7] T. Krovetz and P. Rogaway. The software performance of authenticated-encryption modes. In A. Joux, editor, *Fast Software Encryption - 18th International Workshop, FSE 2011, Lyngby, Denmark, February 13-16, 2011, Revised Selected Papers*, volume 6733 of *Lecture Notes in Computer Science*, pages 306–327. Springer, 2011.

[8] H. Kuwakado and M. Morii. Quantum distinguisher between the 3-round feistel cipher and the random permutation. In *IEEE International Symposium on Information Theory, ISIT 2010, June 13-18, 2010, Austin, Texas, USA, Proceedings*, pages 2682–2685. IEEE, 2010.

[9] H. Kuwakado and M. Morii. Security on the quantum-type even-mansour cipher. In *Proceedings of the International Symposium on Information Theory and its Applications, ISITA 2012, Honolulu, HI, USA, October 28-31, 2012*, pages 312–316. IEEE, 2012.

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

[11] M. Luby and C. Rackoff. How to construct pseudorandom permutations from pseudorandom functions. *SIAM J. Comput.*, 17(2):373–386, 1988.

[12] P. Rogaway. Efficient instantiations of tweakable blockciphers and refinements to modes OCB and PMAC. In P. J. Lee, editor, *Advances in Cryptology - ASIACRYPT 2004, 10th International Conference on the Theory and Application of Cryptology and Information Security, Jeju Island, Korea, December 5-9, 2004, Proceedings*, volume 3329 of *Lecture Notes in Computer Science*, pages 16–31. Springer, 2004.

[13] P. Rogaway, M. Bellare, J. Black, and T. Krovetz. OCB: a block-cipher mode of operation for efficient authenticated encryption. In M. K. Reiter and P. Samarati, editors, *CCS 2001, Proceedings of the 8th ACM Conference on Computer and Communications Security, Philadelphia, Pennsylvania, USA, November 6-8, 2001.*, pages 196–205. ACM, 2001.

[14] P. W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput.*, 26(5):1484–1509, 1997.

[15] D. R. Simon. On the power of quantum computation. *SIAM J. Comput.*, 26(5):1474–1483, 1997.