# Beyond quadratic speedups in quantum attacks on symmetric schemes

Xavier Bonnetain, André Schrottenloher, Ferdinand Sibleyras

# Beyond quadratic speedups in quantum attacks on symmetric schemes

## Extended abstract

Xavier Bonnetain[1], André Schrottenloher[2] and Ferdinand Sibleyras[3]

[1] Université de Lorraine, CNRS, Inria, Nancy, France
[2] Cryptology Group, CWI, Amsterdam, The Netherlands
[3] NTT Social Informatics Laboratories

## Context

Since Shor showed that quantum computers could break the RSA and Diffie-Hellman cryptosystems [13], the most widely used asymmetric schemes to day, the cryptographic community has focused on the design and analysis of suitable quantum-resistant replacements.

In symmetric cryptography, the situation was different. Grover's algorithm [8] gives a quadratic speedup for the exhaustive search of a secret key. From this generic result came the folklore belief that "doubling the key length is sufficient". Indeed, doubling the length of the key makes the quantum attack with Grover's search at least as costly, in number of operations, as the classical exhaustive search of the original key.

In this paper, we focus on the case of key-recovery attacks on a block cipher $E_k$ (instantiated with a secret key $k$) to which the attacker has only black box access.

**Superposition Attacks.** When the quantum adversary makes only classical queries, that is, gets classical tuples $(x, E_k(x))$, all quantum attacks known to date have reached at most a quadratic speedup on their classical counterparts. However, Kuwakado and Morii [10] first showed that a quantum adversary could do better in the *superposition query* model. Here, the adversary can query a quantum oracle $|x\rangle|0\rangle \mapsto |x\rangle|E_k(x)\rangle$. Some classically secure constructions, such as the Even-Mansour cipher, become completely broken in this model [11], due to a quantum-only structural attack. These attacks rely on Simon's period-finding algorithm [14], which solves the following problem.

**Problem 1** (Boolean period-finding)**.** *Given access to a two-to-one function $f$ such that $\forall x, y, f(x) = f(y) \iff y \in \{x, x \oplus s\}$ for some value $s$ (the period), then find $s$.*

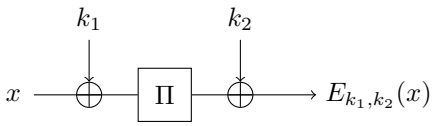


**Figure 1:** The Even-Mansour cipher [6]. The permutation $\Pi$ is a public component drawn uniformly at random.

The attack on the Even-Mansour cipher (Figure 1) then runs as follows: given quantum query access to the cipher $E_{k_1,k_2}(x) = k_2 \oplus \Pi(k_1 \oplus x)$ where $\Pi$ is a public permutation, we can query the function $f(x) = E_{k_1,k_2}(x) \oplus \Pi(x)$, which admits $k_1$ as a period[1]. Simon's

[1] This function might not be two-to-one, but this is not an issue as long as it is periodic [9, 4].

algorithm retrieves $k_1$ in $\mathcal{O}(n)$ quantum queries to $f$ (hence to the cipher) and about $\mathcal{O}(n^3)$ computations.

**Offline-Simon.** In [5], the authors introduced the offline-Simon algorithm (presented at QIP 2020), which was the first use of Simon's algorithm in the *classical* query model. It targets the following problem:

**Problem 2** (Finding a periodic function)**.** *Let $f$ and $(g_i, i \in I)$ be injective functions from $\{0,1\}^n$ to $\{0,1\}^m$ for some $n, m$, where $(g_i)$ is a family indexed by $i \in I$, such that for a single $i_0 \in I$, $x \mapsto f(x) \oplus g_i(x)$ is periodic. Given quantum access to $f$ and $G(i,x) = g_i(x)$, find $i_0$.*

In previous work, this problem was solved with a Grover search over $I$, in which Simon's algorithm checks if $f \oplus g_i$ is periodic [12]. This method requires to query $f$ and $G$ at each iteration. In offline-Simon, $f$ is queried only $\mathcal{O}(n)$ times, at the beginning of the algorithm (hence the *offline* denomination), and these queries are reused during the search iterates.

Because they are computed only once, it becomes possible to construct them using a large number of classical queries $(x, f(x))$. This technique yields improved time-memory trade-offs in quantum attacks on several cipher constructions, such as Even-Mansour. However, it still reaches a quadratic speedup in time at best.

## Contributions

In this paper, we present the first key-recovery attack on a block cipher construction that, with classical queries only, reaches a more than quadratic quantum speedup. This attack is based on an extension of offline-Simon and allows to target several constructions with a speedup of a factor 2.5 instead of 2.

Our main example is the *double-XOR Cascade construction* (2XOR in what follows), introduced by Gazi and Tessaro [7]. This construction (Figure 2) takes an ideal $n$-bit block cipher $E$ and increases its key by $n$ bits, using a new whitening key $z$.

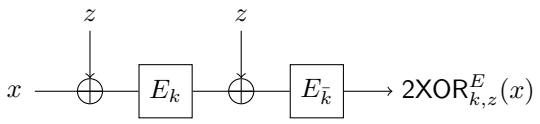


**Figure 2:** The 2XOR construction of [7]. $E$ is an ideal $n$-bit block cipher, $z$ is an $n$-bit key, $k$ is a $\kappa$-bit key and $\bar{k}$ is $\pi(k)$ for some chosen permutation without fixpoints.

On the one hand, the 2XOR construction has a classical security proof. In this paper, we also give a self-contained proof of a variation we called EFX. When the internal key $k$ has $2n$ bits, any classical adversary having black-box access to $E$ and a permutation $P$ that is either $\mathsf{2XOR}^E_{k,z}(x)$ for a random choice of $k, z$, or a random permutation, must make at least $\Omega(2^{5n/2})$ queries to $E$ to distinguish the two cases with constant advantage. Note that an adversary that recovers the key $k$ can distinguish, as it can then recover $z$ and compute the result of any query to $\mathsf{2XOR}^E_{k,z}(x)$ without actually querying it.

On the other hand, we show that, in this precise case, a quantum adversary can recover the key in time $\widetilde{\mathcal{O}}(2^n)$. For this, we extend offline-Simon to solve the following problem.

**Problem 3** (Finding a periodic function)**.** *Let $f : \{0,1\}^n \to \{0,1\}^m$ be an injective function, $(g_i : \{0,1\}^n \to \{0,1\}^m, i \in I)$ a family of functions such that for a single $i_0 \in I$, $g_i$ is periodic. Let $U$ be a unitary operator such that $U|i\rangle \sum_{x\in\{0,1\}^n} |x\rangle |f(x)\rangle = |i\rangle \sum_{y\in\{0,1\}^n} |y\rangle |g_i(y)\rangle$. Given classical access to $f$ and quantum access to $U$ and $U^\dagger$ find $i_0$.*

In the case of 2XOR, we instantiate Problem 3 with $f(x) = \mathsf{2XOR}^E_{k,z}(x)$, and

$$g_i(x) = E_{\bar{i}}^{-1}\big(\mathsf{2XOR}^E_{k,z}(x)\big) \oplus E_i(x).$$

We define

$$U\,|i\rangle\,|x\rangle\,|f(x)\rangle = |i\rangle\,|x\rangle\,|E_{\bar{i}}^{-1}(f(x)) \oplus E_i(x)\rangle\,.$$

Note that this operator is indeed easy to compute, as it requires only to first compute in-place $E_{\bar{i}}^{-1}$, and then to add $E_i(x)$ to the third register, with $i$ and $x$ in the first two.

It is easy to see that $g_k$ is periodic, as this reduces to the Even-Mansour quantum attack.

**Attack details.** We use $2^n$ classical queries to build, in a first step, the offline queries that offline-Simon requires:

$$\sum_{x\in\{0,1\}^n} |x\rangle\,|\mathsf{2XOR}^E_{k,z}(x)\rangle$$

They will be reused during the quantum search on $k$.

Then, for the second step, the periodicity check on $i$ is done by first applying $U$ on $|i\rangle \sum_x |x\rangle\,|\mathsf{2XOR}^E_{k,z}(x)\rangle$, and then applying Simon's algorithm on $g_i$.

This first step costs $\widetilde{\mathcal{O}}(2^n)$ time, as does the second if $k$ has $2n$ bits. This also matches a lower bound which can be obtained easily.

**Attack tradeoffs.** This attack also works for other key sizes, and with a smaller number of queries. However, the largest gap, 2.5, is only reached when $k$ has $2n$ bits and the adversary does $\mathcal{O}(2^n)$ classical queries.

## Implications

Apart from solving a long-standing open question in quantum cryptanalysis, our result shows that generic key-length extension techniques, which might be a first choice for ensuring post-quantum security, should be analyzed with care. Indeed, the 2XOR construction is shown to offer roughly as much security as its internal component $E$ itself.

The problems that we are trying to solve, that is, recovering the key of a block cipher construction (with an ideal component inside), can also be studied from the point of view of query complexity. Indeed, we can consider the number of quantum queries to the component ($E$ in the case of 2XOR) made by a quantum adversary, compared to the number of classical queries made by a classical adversary. Our result then becomes a separation between the quantum and classical query complexities of a certain function of $E$, which corresponds to performing the key-recovery attack. However, there is no connection with the studies in the query complexity of total functions [3], because we considered average-case algorithms. In this case, no general relation is known between the quantum and randomized query complexities [1]. However, it is still possible that a polynomial relation holds in our case, and this is an interesting open question.

Another question is by how much this gap may be increased. The algorithm that we used, offline-Simon, does not seem capable of reaching more than a 2.5 gap. A cubic separation could be achievable by replacing Simon's algorithm by another quantum algorithm (e.g. solving $k$-forrelation [2]), but to date, we have not identified any such problem of cryptographic interest.

## References


[1] Ambainis, A., de Wolf, R.: Average-case quantum query complexity. In: STACS. Lecture Notes in Computer Science, vol. 1770, pp. 133–144. Springer (2000)

[2] Bansal, N., Sinha, M.: $k$-forrelation optimally separates quantum and classical query complexity. Electron. Colloquium Comput. Complex. 27, 127 (2020)

[3] Beals, R., Buhrman, H., Cleve, R., Mosca, M., de Wolf, R.: Quantum lower bounds by polynomials. J. ACM 48(4), 778–797 (2001)

[4] Bonnetain, X.: Tight bounds for Simon's algorithm. In: Longa, P., Ràfols, C. (eds.) LATINCRYPT 2021. Lecture Notes in Computer Science, Springer (2021)

[5] Bonnetain, X., Hosoyamada, A., Naya-Plasencia, M., Sasaki, Y., Schrottenloher, A.: Quantum attacks without superposition queries: The offline simon's algorithm. In: ASIACRYPT (1). Lecture Notes in Computer Science, vol. 11921, pp. 552–583. Springer (2019)

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

[7] Gazi, P., Tessaro, S.: Efficient and optimally secure key-length extension for block ciphers via randomized cascading. In: EUROCRYPT. Lecture Notes in Computer Science, vol. 7237, pp. 63–80. Springer (2012)

[8] Grover, L.K.: A fast quantum mechanical algorithm for database search. In: STOC. pp. 212–219. ACM (1996)

[9] Kaplan, M., Leurent, G., Leverrier, A., Naya-Plasencia, M.: Breaking symmetric cryptosystems using quantum period finding. In: CRYPTO (2). Lecture Notes in Computer Science, vol. 9815, pp. 207–237. Springer (2016)

[10] Kuwakado, H., Morii, M.: Quantum distinguisher between the 3-round feistel cipher and the random permutation. In: ISIT. pp. 2682–2685. IEEE (2010)

[11] Kuwakado, H., Morii, M.: Security on the quantum-type even-mansour cipher. In: ISITA. pp. 312–316. IEEE (2012)

[12] Leander, G., May, A.: Grover meets simon - quantumly attacking the fx-construction. In: ASIACRYPT (2). Lecture Notes in Computer Science, vol. 10625, pp. 161–178. Springer (2017)

[13] Shor, P.W.: Algorithms for quantum computation: Discrete logarithms and factoring. In: FOCS. pp. 124–134. IEEE Computer Society (1994)

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