The ISC Int'l Journal of Information Security

January 2023, Volume 15, Number 1 (pp. 27–39)

http://www.isecure-journal.org

Quantum Cryptanalysis of Symmetric Primitives by Improving Relaxed Variants of Simon's Algorithm

Ali Khosravi [1], and Taraneh Eghlidos [2,*]

[1] *Sharif University of Technology, Department of Electrical Engineering, Tehran, Iran.*

[2] *Electronics Research Institute, Sharif University of Technology, Tehran, Iran.*

ARTICLE INFO.

Article history:

Received: –

Revised: –

Accepted: –

Published Online: –

Keywords:

Modes of Operation, Quantum Cryptanalysis, Quantum Distinguishers, Quantum Key Recovery Attack, Quantum Related Key Attack, Quantum Slide Attack, Symmetric Cipher

Type: –

doi: --

dor: --

ABSTRACT

Computing the period of the periodic functions is the main reason of using Simon's algorithm to attack symmetric-key cryptographic primitives. However, if the target function does not satisfy Simon's promise completely or if the number of superposition queries of the adversary is limited, Simon's algorithm cannot compute the actual target period, unambiguously. These problems may lead to the failure of period-finding-based quantum attacks.Our main aim in this paper is to relax Simon's algorithm so that quantum adversaries can still carry out the mentioned attacks without any assumptions (Simon's promise) on the target function. To that end, we use two different methods, each of which is suitable for some of the period-finding-based quantum attacks. In the first method, as a complement to Kaplan's suggestion, we first show that using Simon's algorithm, one can find the proper partial periods of Boolean vector functions so that the probability of their establishment, independent of the target function, is directly related to the number of the attacker's quantum queries. Next, we examine how one can use the partial period instead of the actual one. The advantage of this method is twofold: It enables the attackers to perform the quantum period-finding-based distinguishers with a smaller number of quantum queries than those of the previous relaxation method. On the other hand, it generalizes the previous forgery attacks on modes of operation for message authentication codes. In the second method, we use Grover's algorithm to complement Simon's algorithm in quantum key recovery attacks. This ensures that the time complexity of the mentioned attacks is less than that of a quantum brute-force attack.

1 Introduction

Quantum computers can solve some complex problems much more efficiently than their classical counterparts. Cryptanalysis of classical ciphers is no exception to this rule. For a notable example, Shor's algorithm [1] can be used to break some asymmetric ciphers, such as Elgamal and RSA, whose security is based on the difficulty of solving discrete logarithms and integer factorization, respectively. As another well-known example, Grover's algorithm [2] is one of the most famous quantum algorithms which can pro-

* Corresponding author.

Email addresses: ali.khosravi@alum.sharif.edu, teghlidos@sharif.edu

ISSN: 2008-2045

vide a quadratic speedup compared to the exhaustive classical search.

Simon's algorithm [3] is one of the most widely used quantum algorithms in quantum shortcut attacks on symmetric cryptosystems. Computing period [4–6] or linear structure [7] of Boolean vector functions, which are the two main pillars of most quantum cryptanalysis, are the main aim of Simon's algorithm. In fact, assuming access to the quantum oracle of the target primitive, one can use Simon's algorithm to analyze some symmetric primitives with linear complexity. For example, Kuwakado *et al.* [8] have shown that using Simon's algorithm, one can recover the key of Even-Mansour construction [9] with linear complexity. The security of the mentioned cipher has been proved in the random permutation model [9]. As another significant work based on Simon's algorithm, we can refer to [6], which has proposed a quantum distinguisher for three rounds of the Feistel family for the first time. Kaplan *et al.* [5] have shown that assuming access to quantum oracle, one can perform forgery attacks on various modes of authentication and authenticated encryption, with linear complexity. Also, Simon's algorithm is the cornerstone of the quantized version of related key [10] and slide attacks [5, 11]. Using Grover's algorithm as a complement to Simon's algorithm, Leander *et al.* [12] have shown that whitening keys do not significantly affect the security of the block ciphers.

In general, computing the period of the target primitive is the main reason for using Simon's algorithm in most quantum cryptanalyses of symmetric ciphers. However, if the target function does not satisfy Simon's promise, that is, the target function has other collisions in addition to the target period, or if the number of quantum queries of the adversary is restricted, there is no guarantee that Simon's algorithm can find the period, unambiguously. This issue may lead to the failure of quantum period-finding-based cryptanalysis. To deal with this problem, Ito *et al.* [4] eliminate the need to recover the actual period in quantum distinguishers by focusing on the dimension of the space spanned by the resulting vectors of Simon's algorithm. As mentioned by Ito *et al.*, their technique cannot be applied to quantum key recovery attacks and forgery attacks on authentication and authenticated encryption schemes since these attacks aim at recovering the actual period.

1.1 Author's Contribution

Our main goal in this paper is to relax Simon's algorithm such that quantum attackers can launch period-finding-based attacks without any assumptions about the target function, even if the number of his quantum queries is restricted to a given small positive integer. In this regard, we use two methods to fix the mentioned flaws of Simon's algorithm in the period-finding-based quantum attacks. In the first method, as a complement to Kaplan *et al.*'s [5] suggested method, we first show that using Simon's algorithm, one can find proper partial periods of Boolean vector functions, such that the corresponding probabilities, independent of the target function, are directly related to the number of quantum queries. Then we look at how the partial period can be used instead of the actual period in some period-finding-based attacks. As a result, compared to Ito *et al.*'s relaxation method [4], using the partial period is not only applicable to quantum forgery attacks on modes of operation for MACs but also improves the success probability of quantum distinguishers, assuming quantum adversaries are restricted to a specific small number of quantum queries. In the case of quantum key recovery attacks, such as a quantum-related key attack, we propose another method, the summary of which is as follows. First, using Simon's algorithm the attacker finds some candidates for the key of the target block cipher and then uses Grover's algorithm to search for the key among them.

The rest of this paper is organized as follows. In Section 2 we give the basic notations and definitions. In Section 3, the required quantum algorithms are described. Section 4 is devoted to examining the behavior of Simon's algorithm, provided that Simon's promise is not fully satisfied. Section 5 is dedicated to how to launch quantum period-finding-based attacks without any assumption on the target periodic function. Finally, in Section 6, we conclude the paper and present some suggestions for further work.

2 Preliminaries

In this section, we introduce the notations and definitions used throughout the paper.

2.1 Notations

Table 1. Notations

Symbol	definition
$\oplus$	bit wise exclusive-or
$A\|\|B$	concatenation of A and B
$Tranc_L^q(T)$	q most significant bit(s) of T
$Tranc_R^q(T)$	q least significant bit(s) of T
$\|M\|$	cardinality of the set M
$Cost(S)$	The cost of process S

The notation F_2 denotes a finite field of characteris-

tic 2, and F_2^n is an n-dimensional vector space over F_2. Let $perm(l)$ denotes the set of all possible permutations on F_2^l. We use $\pi \xleftarrow{\$} perm(l)$ to represent uniform sampling of the $perm(l)$. For a Bolean vector function g, we use f^g to represent a specific function, which is efficiently executable by a classical algorithm, with access to function(s) g (and g^{-1}, in case g is invertible). The other notations are given in Table 1.

2.2 Definitions

Definition 2.1 (Quantum oracle function [13]). Any Boolean vector function $f : F_2^n \to F_2^m$, say the target cryptosystem, with a defined circuit is efficiently implementable as a quantum unitary $\mathcal{O}_f : |x\rangle |y\rangle \to |x\rangle |y \oplus f(x)\rangle$ on $n+m$ qubits.

Definition 2.2 (Query model [14]). In general, quantum attacks are divided into the following models, according to the adversary's access to the oracle of the target algorithm.

i) *Q1 model*: The quantum adversaries (i.e., attackers who access quantum computers) are allowed to perform only classical queries [15]. As a notable example, this model is used in a quantized version of online-offline meet-in-the-middle attack [15] and in running Simon's algorithm with only classical query [16].

ii) *Q2 model*: The quantum adversaries have access to the classical and quantum oracles and perform quantum superposition queries [14]. For example, this scenario is used in [4–6, 8, 17].

iii) *Q3 model*: The quantum adversaries are allowed to make quantum superposition queries under related key differences [14]. This model is too strong and has been used in quantum-related-key attacks [10].

Definition 2.3 ((Q2, AnyD)-Pseudorandom permutation (PRP) [18]). For query models $Q2$ and arbitrary polynomially-bounded n, an (Q2, AnyD)-Pseudorandom permutation is a family of efficient keyed permutations $P_k : F_2^n \times F_2^{|k|} \to F_2^n$ and ${P_k}^{-1}$, if for all probabilistic polynomial-time distinguisher $\mathcal{D}$, there exists a negligible function $negl(n)$ such that:

$$Pr[C] \leqslant negl(n),$$

where $Pr[C]$ is defined as follows:

$$|Pr[\mathcal{D}^{P_k,P_k^{-1}} = 1 : k \xleftarrow{\$} F_2^{|k|}] - Pr[\mathcal{D}^{\pi,\pi^{-1}} = 1 : \pi \xleftarrow{\$} perm(n)]|$$

In fact, $Pr[C]$ can be used as a measure to indicate the deviation of the function P_k from a random permutation π. In this paper, we are going to compare the efficiency of our proposed distinguisher and that of Ito [4]. For this purpose, we compare the corresponding $Pr[C]$s under the same conditions.

Definition 2.4 (Period of Boolean vector function [17]). A vector s is called period (actual period [4]) of a vector function $f : F_2^n \to F_2^m$, if

$$f(x) = f(x \oplus s), \forall x \in F_2^n.$$

In this paper, any function that satisfies the above condition is called periodic function.

Definition 2.5 (Simon promise [17]). For a given periodic Boolean vector function $f : F_2^n \to F_2^m$, with period $s \in F_2^n \backslash \{0\}^n$, if there is no collision other than the actual period s (i.e. $f(x) = f(y) \Leftrightarrow y = x \oplus s$), the function f is called to satisfy Simon's promise [17].

Definition 2.6 (Partial period [4]). In periodic functions, if there are other collisions in addition to s , (i.e., $\exists s' \neq s, x \in F_2^n : x' = x \oplus s', f(x) = f(x')$), the vector $t \neq s$ is called partial period, if $f(x) = f(x \oplus t)$ holds for some x.

Definition 2.7 (Maximum probability of partial period [5]). For any periodic function $f : F_2^n \to F_2^m$, the maximum probability of partial period is defined as follows:

$$\varepsilon_{f,s} = \max_{t \in F_2^n \backslash \{0,s\}} Pr_x[f(x) = f(x \oplus t)]$$

This parameter shows how much the function f deviates from Simon's promise.

Definition 2.8 (Set of irregular permutations [4]). For any permutation $\pi \in perm(l)$ and a specified function $f^\pi : F_2^n \to F_2^m$, the parameter ϵ_f^π is defined as follows:

$$\epsilon_f^\pi = \max_{t \in F_2^n \backslash \{0,s\}} Pr_x[f^\pi(x) = f^\pi(x \oplus t)]$$

Let us consider $0 \leqslant \delta < 1$ as an arbitrary constant. A permutation π is called irregular, if $\epsilon_f^\pi > 1 - \delta$. Furthermore, the set of all irregular permutations irr_f^δ is defined as follows [4]:

$$irr_f^\delta = \{\pi \in perm(l) : \epsilon_f^\pi > 1 - \delta\}$$

3 Required Quantum Algorithms

Throughout this section, we assume that the reader is familiar with the basic concepts of quantum processing.

3.1 Simon's Algorithm

Assuming access to the quantum oracle of Boolean vector functions $f : F_2^n \to F_2^n$ (i.e. unitary operator $\mathcal{O}_f : |x\rangle |y\rangle \to |x\rangle |y \oplus f(x)\rangle$), one can compute the period of f with linear complexity, provided that f

satisfies Simon's promise. In fact, Simon proposed the circuit S_f, which computes an orthogonal vector to period s in each execution.

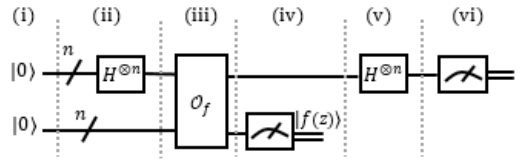

Figure 1. Subroutine quantum circuit S_f of Simon's algorithm

As shown in Figure 1, S_f is described as $(measure \otimes I^n) \cdot (H^{\otimes n} \otimes I^n) \cdot (I^n \otimes measure) \cdot \mathcal{O}_f \cdot (H^{\otimes n} \otimes I^n)$ and works as follows:

(1) *Prepare* $(2n)$ *qubits in state* $|0^n\rangle |0^n\rangle$;
(2) *Apply the Hadamard transform to the* n *most significant qubits which leads to state* $2^{(-n/2)} \sum_{x \in F_2^n} |x\rangle |0^n\rangle$;
(3) *Apply the unitary operator* $\mathcal{O}_f$ *to obtain the state* $2^{(-n/2)} \sum_{x \in F_2^n} |x\rangle |f(x)\rangle$;
(4) *Measure the second register in the computational basis;*
Executing this step yields an n-vector $f(z)$, then the first register collapses to the state $(1/\sqrt{2})(|z\rangle + |z \oplus s\rangle)$.
(5) *Apply the Hadamard operator to the first register again, giving*

$$\frac{1}{\sqrt{2}} \frac{1}{\sqrt{2^n}} \sum_{y \in F_2^n} (-1)^{z \cdot y} \left[1 + (-1)^{s \cdot y}\right] |y\rangle \quad (1)$$

(6) *Measure the above register in the computational basis;*

Note that the amplitude of each y vanishes, if $s \cdot y = 1$. As a result, by measuring the above state on the computational basis, it is obtained a vector orthogonal to s. By $O(n)$ times executing quantum circuit S_f as a subroutine of Simon's algorithm, one obtains $n-1$ independent vectors, orthogonal to s with high probability. Then s can be computed using basic linear algebra. In summary, to compute the period of the periodic function f, Simon has proposed the following algorithm:

Algorithm 1 Simon's algorithm

1: Initialize $U := \varnothing$;
2: Choose a positive integer c;
3: **for** $i = 1, \ldots, cn$, **do**
4: Run the quantum circuit S_f to obtain an n-bit vector u_i;
5: Set $U := U \cup \{u_i\}$;
6: **end for**
7: Compute the system of linear equations $s \cdot u_i = 0, \forall u_i \in U$ for s;
8: Return s;

3.2 Grover's Algorithm

Grover's algorithm [2] and its generalized variants are widely used in quantum cryptanalysis of symmetric ciphers. For example, those are the basis of the quantum online-offline meet-in-the-middle (MitM) attacks [15] and also the cornerstone of the quantum preimage [19], multi-target preimage [13, 20] and collision [13, 20] attacks on hash functions.

In this section, according to our attack strategy, we describe the following generalizations of Grover's algorithm.

Theorem 1 ([21]). *Let* X *represent the target search space. (not necessarily* $\{0,1\}^n$*). Consider the test function* $f : F_2^n \to F_2$*, such that* $f(x) = 1$ *if* $x \in M$*, for a specific marked subset* $M \subset X : |M| \geqslant 1$*, otherwise* $f(x) = 0$*. There exists a quantum algorithm, say AlgorithmA, which finds a marked element* $x \in M$*, at cost of the order*

$$\sqrt{|X|/|M|}(Cost(Setup) + Cost(Checking))$$

where Setup and Checking represent the process of constructing a uniform superposition of all elements in X *and process of applying quantum unitary operator* $\mathcal{O}_f$*, respectively.*

In the special case, where the target search space is the set of all possible vectors (i.e., $\{0,1\}^n$), the cost of the setup step is low and can be neglected, therefore the following theorem results.

Theorem 2 ([15]). *For a specific set* X*, let* $g : F_2^n \to F_2$ *be a Boolean function, such that* $g(x) = 1$ *if* $x \in X$ *and* $g(x) = 0$*, otherwise. There exists a quantum algorithm, say AlgorithmB, that finds an element* $x \in F_2^n : g(x) = 1$ *with* $O(\sqrt{2^n/|X|})$ *times execution of unitary operator* $\mathcal{O}_g$*.*

Note that the setup of *AlgorithmA* itself can be a separate quantum algorithm, for example, *AlgorithmB* without its final measurement. As a notable example, this method has been used in [13, 21].

4 Relaxation of Simon's Algorithm

As mentioned in Section 3.1, if the target function completely satisfies Simon's promise (i.e. $f(x) = f(y) \Leftrightarrow y = x \oplus s$), Simon's algorithm can compute the period of the target function with linear complexity [3]. In this section, we examine what happens if Simon's promise is partially fulfilled (i.e. $f(x) = f(y) \Leftarrow y = x \oplus s$). In fact, our main goal in this section is to investigate the impact of unwanted collisions on the result of Simon's algorithm. The following theorem is inspired by Theorem 1 of [7], shows that, even with numerous unwanted collisions, the result vector of the quantum circuit S_f is orthogonal to the period of the target periodic function f.

Theorem 3. *For any periodic Boolean vector function $f : F_2^n \to F_2^m$, even with a large number of unwanted collisions, the result vector of each execution of the quantum circuit S_f is definitely orthogonal to the period s.*

Proof. Let $f(z)$ indicate the measurement result of the second register in item 4 of the quantum circuit S_f, described in Section 3.1. In addition to the period s, f may have other collisions at $f(z)$. Suppose that $T = \{t_1, t_1 \oplus s, \ldots, t_q, t_q \oplus s\}$ represents the set of such unwanted collisions. Note that, since the function, f is a periodic function, $\forall t_i \in T$ we have $t_i \oplus s \in T$. Hence, for each $\alpha \in \{\{s, 0\} \cup T\}$, we have $f(z) = f(z \oplus \alpha)$. Therefore, after item 4 of circuit S_f, the first register collapses to the following state:

$$\frac{1}{\sqrt{2(q+1)}}(|z\rangle + |z \oplus s\rangle + \sum_{t_i \in T} |z \oplus t_i\rangle + |z \oplus t_i \oplus s\rangle) \quad (2)$$

Let $T' = \{t_0, t_1, \ldots, t_q : t_0 = 0^n, t_1, \ldots, t_q \in T\}$. The Equation 2 can be rewritten as follows:

$$\frac{1}{\sqrt{2(q+1)}} \sum_{t_i \in T'} |z \oplus t_i\rangle + |z \oplus t_i \oplus s\rangle$$

By applying the Hadamard operator, in the item 5 of quantum circuit S_f, the state of the first register changes as follows:

$$\frac{1}{\sqrt{2^n}} \frac{1}{\sqrt{2(q+1)}} \sum_{y \in F_2^n} \left(\sum_{t_i \in T'} (-1)^{(z \oplus t_i) \cdot y} \right) [1 + (-1)^{s \cdot y}] \, |y\rangle$$

The result of measuring the above register, on the computational basis is orthogonal to the period. □

Let $U = \{u_1, \ldots, u_{cn}\}$ indicates the set of all vectors obtained from cn times executing quantum circuit S_f. According to Theorem 3, all members of the set U are orthogonal to the period of the function f. Therefore, if the dimension of $spam(U) = n - 1$, one can unambiguously calculate the period s by solving the system of equations $x \cdot u_i = 0, \forall u_i \in U$. Otherwise, a set of candidates is obtained for the period s. The following theorem shows the success probability of Simon's algorithm in the computing period unambiguously.

Theorem 4 ([5]). *For any periodic boolean vector function $f : F_2^n \to F_2^m$, if $\varepsilon_{f,s} \leqslant p_0 < 1$, the probability that Simon's algorithm returns s uniquely after cn quantum queries is greater than $1 - (2(\frac{1+p_0}{2})^c)^n$.*

According to Theorem 4, if the target function has numerous collisions other than the actual period or if the number of quantum queries is limited to a given small integer, one cannot compute the period s unambiguously. As a result, this issue may lead to the failure of period-finding-based quantum attacks. Therefore, to make the aforementioned attacks more practical we aim at using the partial period instead of the actual one. To find a suitable partial period, it is necessary to introduce the following lemma from Kaplan.

Lemma 1 ([5]). *For a fixed Boolean vector function $f : F_2^n \to F_2^m$ and any $t \in F_2^n$, let $p_t = Pr_x[f(x) = f(x \oplus t)]$. Then the probability of obtaining 'u' such that $u \cdot t = 0$, after executing the quantum circuit S_f, is $\frac{(1+p_t)}{2}$.*

The following theorem, inspired by Xie *et al.* [22, 23], shows that any vector that is orthogonal to all vectors returned by $\mathcal{Z}$ times execution of the quantum circuit S_f, i.e. u_i's, is the appropriate partial period.

Theorem 5. *For any periodic Boolean vector function $f : F_2^n \to F_2^m$, let $U = \{u_1, \ldots, u_\mathcal{Z}\}$ represents the set of all vectors obtained from $\mathcal{Z}$ times execution of quantum circuit S_f, as a subroutine of Simon's algorithm, and A be the set of solution(s) of the system of equations $x \cdot u_i = 0, \forall u_i \in U$. Then for all $a \in A$ and all ϵ satisfying $0 < \epsilon < 1$, we have:*

$$Pr[Pr_x[f(x) = f(x \oplus a)] > 1 - \epsilon] > \max\left\{ \left(1 - e^{-\frac{\mathcal{Z}\epsilon^2}{2}}\right), \left(1 - \left(2\left(1 - \frac{\epsilon}{2}\right)^{\frac{\mathcal{Z}}{n}}\right)^n\right) \right\} \quad (3)$$

Proof. First, we prove that the left side of the Equation 3 is greater than the first element inside the accolade. For $a \in A$, let $p_a = Pr_x[f(x) = f(x \oplus a)]$ and $q_a = \frac{1+p_a}{2}$. We define the random variable Y as follows:

$$Y(u) = \begin{cases} 0 & if \ u \cdot a = 0 \\ 1 & if \ u \cdot a \neq 0 \end{cases}$$

According to Lemma 1 the expectation of Y is $1 - q_a$. By $\mathcal{Z}$ times executing of quantum circuit S_f as a subroutine of Simon's algorithm, one can get $\mathcal{Z}$ independent identical random variables $Y_1, \ldots, Y_\mathcal{Z}$. By Hoeffding's inequality [24] we have

$$Pr[((1 - q_a) - \frac{1}{\mathcal{Z}} \sum_{i \in \{1,\ldots,\mathcal{Z}\}} Y_i) \geqslant \epsilon] \leqslant e^{-2\mathcal{Z}\epsilon^2}$$

Since $a \in A$, by the definition of random variable Y, we have $\sum_{i \in \{1,\ldots,\mathcal{Z}\}} Y_i = 0$. As a result

$$Pr[(1 - q_a) \geqslant \epsilon] \leqslant e^{-2\mathcal{Z}\epsilon^2}$$

$$Pr[1 - q_a < \epsilon] > 1 - e^{-2\mathcal{Z}\epsilon^2}$$

$$Pr[q_a > 1 - \epsilon] > 1 - e^{-2\mathcal{Z}\epsilon^2}$$

According to the definition of $q_a = \frac{1+p_a}{2}$, the above relation can be rewritten as follows:

$$Pr[\frac{1 + p_a}{2} > 1 - \epsilon] > 1 - e^{-2\mathcal{Z}\epsilon^2}$$

$$Pr[1 + p_a > 2 - 2\epsilon] > 1 - e^{-2\mathcal{Z}\epsilon^2}$$

Let $\epsilon' = 2\epsilon$

$$Pr[p_a > 1 - \epsilon'] > 1 - e^{\frac{-\mathcal{Z}\epsilon'^2}{2}}$$

Using $p_a = Pr_x[f(x) = f(x \oplus a)]$, the proof of the left part of the *max*-term is completed, as follows:

$$Pr[Pr_x[f(x) = f(x \oplus a)] > 1 - \epsilon] > 1 - e^{-\frac{\mathcal{Z}\epsilon^2}{2}} \quad (4)$$

In a special case where $\mathcal{Z} > 2n$, let $\epsilon = \sqrt{\frac{2n}{\mathcal{Z}}}$, therefore, with overwhelming probability (i.e., $1 - e^{-n}$) we have

$$Pr_x[f(x) = f(x \oplus a)] > 1 - \sqrt{\frac{2n}{\mathcal{Z}}} \quad (5)$$

We remind the proof of the Equation 3 for the second element inside the accolade by Kaplan *et al.* [5] as follows:

For a fixed Boolean vector function $f : F_2^n \to F_2^m$ and vector t from its domain, let $p_t = Pr_x[f(x) = f(x \oplus t)]$. According to Lemma 1, all independent vectors obtained from $\mathcal{Z}$ times executing of quantum circuit S_f are orthogonal to t with probability $(\frac{1+p_t}{2})^{\mathcal{Z}}$. As a result, the probability that Simon's algorithm returns a vector t such that $p_t \leqslant p_0 < 1$ is bounded as follows:

$$Pr[p_t \leqslant p_0] \leqslant \sum_{t:p_t \leqslant p_0} \left(\frac{1+p_t}{2}\right)^{\mathcal{Z}} \leqslant 2^n \times \left(\frac{1+p_0}{2}\right)^{\mathcal{Z}} = \left(2\left(\frac{1+p_0}{2}\right)^{\frac{\mathcal{Z}}{n}}\right)^n$$

$$\Rightarrow \quad Pr[p_t > p_0] > 1 - \left(2\left(\frac{1+p_0}{2}\right)^{\frac{\mathcal{Z}}{n}}\right)^n$$

Let $p_t = Pr_x[f(x) = f(x \oplus t)]$, we have

$$Pr[Pr_x[f(x) = f(x \oplus t)] > p_0] > 1 - \left(2\left(\frac{1+p_0}{2}\right)^{\frac{\mathcal{Z}}{n}}\right)^n \quad (6)$$

In a special case where $\mathcal{Z} > 3n$, according to Theorem 2 of [5], by placing $\frac{\mathcal{Z}}{n} = \frac{3}{1-p_0}$, we have

$$Pr\left[Pr_x[f(x) = f(x \oplus t)] > 1 - \frac{3n}{Z}\right] \approx 1 \quad (7)$$

By placing $p_0 = 1 - \epsilon$ in Equation 6, we have

$$Pr\left[Pr_x[f(x) = f(x \oplus t)] > 1 - \epsilon\right] > 1 - \left(2\left(1 - \frac{\epsilon}{2}\right)^{\frac{\mathcal{Z}}{n}}\right)^n \quad (8)$$

Thus the Equation 3 holds for the second element inside the accolade.

Consequently, by considering Equation 4 and Equation 8 at the same time, the proof of this theorem is completed. □

Ito *et al.* [4] have shown that if the target function $f : F_2^n \to F_2^m$ has no period, most likely no vector appears in the output of Simon's algorithm. More precisely, if $U = \{u_1, \ldots, u_{\mathcal{Z}}\}$ represents the set of all vectors obtained by $\mathcal{Z}$ times executing quantum circuit S_f, they have shown that the dimension of $span(U)$ is n with high probability. Therefore, the system of equations $x \cdot u_i = 0, \forall u_i \in U$ has no solution.

Theorem 6 ([4]). *For a random permutation $\pi \xleftarrow{\$} perm(l)$ and given function $f^\pi : F_2^n \to F_2^m$, let $U = \{u_1, \ldots, u_{\mathcal{Z}}\}$ represents the set of vectors resulting from $\mathcal{Z}$ times executions of quantum circuit S_f. Then the following relation holds:*

$$Pr[dim(span(U)) < n] \leqslant 2^n \cdot e^{-\delta \mathcal{Z}/2} + Pr_\pi[\pi \in irr_f^\delta].$$

5 Applications of Improved Relaxation Method

The period of boolean vector functions is one of the most widely used concepts in the quantum cryptanalysis of symmetric ciphers. Assuming access to the quantum oracle of the target periodic function f, its period can be computed with one of the Simon's [3] or Bernstein-Vazirani's [17] algorithms. In both algorithms, the target period can be retrieved ambiguously, if there are multiple collisions other than the actual one or the access to quantum oracle corresponding to the target function f is limited. In practice, this issue challenges the period-finding-based quantum attacks. Dealing with this problem is our main goal in this paper.

Throughout this section, we assume that the number of quantum queries of the attacker is restricted to a given positive integer, say $\mathcal{Z}$.

5.1 Forgery Attack on Modes of Operation for MAC

Analysis of modes of operation for message authentications [5], encryptions [25] and authenticated encryptions [5] are some important applications of Simon's algorithm. For example, Kaplan *et al.* [5] have shown that, in Q2 model, adversaries can launch forgery attacks on some of the authentication and authenticated encryption schemes with linear complexity. In the following, we describe their forgery attack on the CBC_MAC shown in Figure 2.

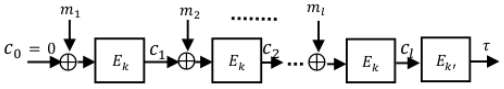

Figure 2. Construction of CBC_MAC

According to Figure 2, the output tag corresponding to the r concatenated block messages $M = m_1 \| m_2 \| \cdots \| m_r$ is generated as follows:

$c_0 = 0$, $c_i = E_k(c_{i-1} \oplus m_i)$, $CBC\_MAC(M) = E_{k'}(c_r)$

For two arbitrary vectors $t_0, t_1 \in F_2^n$, consider the function $f^{CBC\_MAC} : F_2 \times F_2^n \to F_2^n$, which is defined as follows:

$$(b, x) \to CBC\_MAC(t_b \| x)$$

$$f^{CBC\_MAC}(b, x) = E_{k'}\Big(E_k(x \oplus E_k(t_b))\Big)$$

It can be easily verified that the function f^{CBC_MAC} has period $s = 1 \| E_k(t_0) \oplus E_k(t_1)$, because

$$f^{CBC\_MAC}(b \oplus 1, x \oplus E_k(t_0) \oplus E_k(t_1)) = f^{CBC\_MAC}(b, x), \forall b, x \in F_2 \times F_2^n$$

Kaplan *et al.* [5] analyzed the CBC_MAC in the following steps:

(1) *Run Simon's algorithm to find the period* $s = 1 \| E_k(t_0) \oplus E_k(t_1)$*, using unitary operator* $\mathcal{O}_{f^{CBC\_MAC}}$*;*
(2) *Query the tag of* $(t_b \| m)$*, i.e.,* $\tau = f^{CBC\_MAC}(t_b \| m)$*, for arbitrary block message* $m \in F_2^n$ *and* $b \in F_2$*;*
(3) *Return the* τ*-value as a valid tag for the message* $t_{b \oplus 1} \| m \oplus E_k(t_0) \oplus E_k(t_1)$*;*

According to Theorem 4, if the number of the allowed quantum queries are limited or if the number of unwanted collisions of the function f^{CBC_MAC} is large, Simon's algorithm cannot compute the period s unambiguously. However, according to Theorem 5, each vector $\alpha \| \beta \in F_2 \times F_2^n$ derived from the Simon's algorithm is the suitable partial period that satisfies the following equation.

$$Pr\Big[Pr_{b,m}[CBC\_MAC(t_{b\oplus\alpha} \| m \oplus \beta) = CBC\_MAC(t_b \| m)] > 1 - \epsilon\Big] > \max\left\{\left(1 - e^{-\frac{\mathcal{Z}\epsilon^2}{2}}\right), \left(1 - \left(2\left(1 - \frac{\epsilon}{2}\right)^{\frac{\mathcal{Z}}{n}}\right)^n\right)\right\} \quad (9)$$

In fact, Equation 9 means that for every $\lceil \frac{1}{1-\epsilon} \rceil$ random messages, on average, one satisfies the relation $CBC\_MAC(t_{b\oplus\alpha} \| m \oplus \beta) = CBC\_MAC(t_b \| m)$, with probability greater than $\max\{(1 - e^{-\frac{\mathcal{Z}\epsilon^2}{2}}), (1 - (2(1 - \frac{\epsilon}{2})^{\frac{\mathcal{Z}}{n}})^n)\}$.

Note that Equation 9 is valid for all $0 < \epsilon < 1$. Therefore, in a special case where $\mathcal{Z} > 2n$, let fix $\epsilon = \sqrt{\frac{2n}{\mathcal{Z}}}$. Hence, according to Equation 5 we have

$$Pr_{b,m}[CBC\_MAC(t_{b\oplus\alpha} \| m \oplus \beta) = CBC\_MAC(t_b \| m)] > 1 - \sqrt{\frac{2n}{\mathcal{Z}}} \quad (10)$$

That is, the tag corresponding to any message $(t_b \| m) \in \{t_1, t_2\} \times F_2^n$ is also a valid tag for the message $(t_{b\oplus\alpha} \| m \oplus \beta)$, with probability greater than $1 - \sqrt{\frac{2n}{\mathcal{Z}}}$.

Note that, according to Equation 5 and Equation 7, if the number of quantum queries of an adversary is greater than $3n$, i.e., $\mathcal{Z} > 3n$, Equation 10 can be improved as follows:

$$Pr_{b,m}[CBC\_MAC(t_{b\oplus\alpha} \| m \oplus \beta) = CBC\_MAC(t_b \| m)] > \max\left\{\left(1 - \sqrt{\frac{2n}{\mathcal{Z}}}\right), \left(1 - \frac{3n}{\mathcal{Z}}\right)\right\} \quad (11)$$

According to Equation 11, the success probability of the proposed algorithm, independent of the subroutine block cipher E_k depends on the number of quantum queries of the adversary and block size of the E_k. For the two prevalent block sizes of 64 and 128 bits, Figure 3 shows a relation between the number of adversary's quantum queries and a lower bound for the success probability of the proposed method. According to Figure 3, as the number of quantum queries increases, the success probability of the attacker tends to 1.

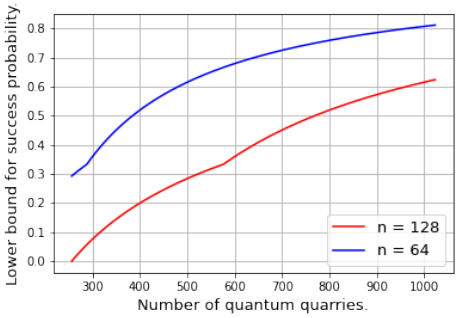

Figure 3. The result of the proposed method

Dealing with Nonce

Many modes of operation for MACs use a nonce value, N, to guarantee independence of the MAC outputs. Let P_N represents a specific mode of operation for the MAC, such as $GMAC$, under a random nonce $N \in F_2^n$. In general, Kaplan *et al.* [5] have suggested the following steps for analyzing P_N.

(1) *Define the function* f^{P_N}*, such that it is a special case of* P_N *having a known period* s*, where* s *is independent of nonce* N*;*
(2) *Run Simon's Algorithm to recover* s*, using unitary operator* $\mathcal{O}_{f^{P_N}} : |x\rangle |y\rangle \to |x\rangle |y \oplus f^{P_N}(x)\rangle$*;*
(3) *Query the tag of message* m*, (i.e.* $\tau = f^{P_N}(m)$*) for an arbitrary classical massage* m *under a random nonce* N*;*
(4) *Return* τ *as a valid tag for the message* $m \oplus s$ *with the same nonce* N*;*

For example, their forgery attack on the $GMAC$ is as follows. For two arbitrary vectors $t_0, t_1 \in F_2^n : t_0 \neq t_1$, consider the function $f^{GMAC_N} : F_2 \times F_2^n \to F_2^n$, which is defined as follows:

$$(b, x) \to GMAC(N, t_b \| x)$$

$$f^{GMAC_N}(b, x) = t_b \cdot H^2 \oplus x \cdot H \oplus E_k(N \| 1)$$

where $H = E_k(0)$. As shown by Kaplan *et al.*, the function f^{GMAC_N} has period $s = 1 \| (t_0 \oplus t_1) \cdot H$. Because $f^{GMAC_N}(b, x) = f^{GMAC_N}(b \oplus 1, x \oplus t_0 \oplus t_1)$.

Using the above algorithm we can find the appropriate partial period for f^{GMAC_N}. For this purpose, it suffices to show that the output distribution of circuit $S_{f^{GMAC_N}}$ is independent of the nonce N. For a fixed vector $\alpha \| \beta \in F_2 \times F_2^n$ and two distinct vectors $N, N' \in F_2^{n-1}$, let $p^N_{\alpha\|\beta}$ and $p^{N'}_{\alpha\|\beta}$ represent $Pr_{b,x}[f^{GMAC_N}(b, x) = f^{GMAC_N}(b \oplus \alpha, x \oplus \beta)]$ and $Pr_{b,x}[f^{GMAC_{N'}}(b, x) = f^{GMAC_{N'}}(b \oplus \alpha, x \oplus \beta)]$, respectively. It is easy to verify that $p^N_{\alpha\|\beta} = p^{N'}_{\alpha\|\beta}$. Since the effect of the nonce in the output difference of f^{GMAC_N} is eliminated. Set $p_{\alpha\|\beta} = p^N_{\alpha\|\beta} = p^{N'}_{\alpha\|\beta}$. According to Lemma 1, each vector obtained by execution of quantum circuit $S_{f^{GMAC_N}}$ is orthogonal to the vector $\alpha \| \beta$, with probability $\frac{1+p_{\alpha\|\beta}}{2}$, which is independent of nonce N and N'. Therefore, the same attack proposed for the analysis of CBC_MAC can be used for other authentication modes, analyzed by Kaplan [5].

5.2 Quantum Distinguishers

Using Grover's algorithm [2] and quantum counting, Kaplan *et al.* [21] have introduced quantum linear, differential and truncated differential distinguishers. They have shown that by accessing quantum oracle and an appropriate differential characteristic (or linear approximation), the distinguishers are significantly superior to their classical counterparts.

In a seminal work, Kuwakado and Morii [6] have shown that if the internal round functions, used in the three-round Feistel structure $E_k : F_2^{\frac{n}{2}} \times F_2^{\frac{n}{2}} \to F_2^{\frac{n}{2}} \times F_2^{\frac{n}{2}}$, are random permutations, assuming access to quantum oracle, then the quantum adversary can distinguish it from a completely random permutation with linear complexity. The main idea of their attack is as follows:

Let $\mathcal{O} : F_2^n \to F_2^n$ be either a 3-round Feistel structure E_k or a random permutation $\pi \xleftarrow{\$} perm(n)$. Suppose that the quantum oracle $\mathcal{O}$ is given. The main goal of attacker in this attack is to distinguish whether $\mathcal{O} = E_k$ or $\mathcal{O} = \pi$.

According to Figure 4, the following relation holds:

$$Tranc_R^{\frac{n}{2}}(E_k(X_L, X_R)) = X_L \oplus P_2(X_R \oplus P_1(X_L))$$

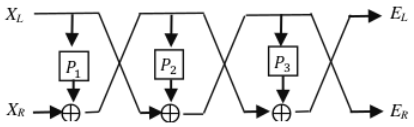

Figure 4. Three round Feistel

For two arbitrary vectors $t_0, t_1 \in F_2^n : t_0 \neq t_1$ consider the function f^{E_k} defined as follows:

$$f^{E_k} : F_2 \times F_2^{\frac{n}{2}} \to F_2^{\frac{n}{2}}$$

$$f^{E_k}(b, x) = Tranc_R^{\frac{n}{2}}(E_k(t_b, x)) \oplus t_b = P_2(x \oplus P_1(t_b))$$

It can be easily verified that the function f^{E_k} has period $s = 1 \| P_1(t_1) \oplus P_1(t_2)$. Since, the following relation holds for all $(b, x) \in F_2 \times F_2^{\frac{n}{2}}$

$$f^{E_k}(b, x) = f^{E_k}(b \oplus 1, x \oplus P_1(t_1) \oplus P_1(t_2)) \quad (12)$$

Kaplan *et al.* [5] and Kuwakado *et al.* [6] have shown that if the internal round functions P_1, P_2 and P_3 are random functions/random permutations, respectively, the number of unwanted collisions of the function f^{E_k} can be neglected. Therefore, according to Theorem 4, one can compute the period s using Simon's algorithm. As a result, to distinguish the status of the given oracle $\mathcal{O}$, the attacker asks for two values $\mathcal{O}(m)$ and $\mathcal{O}(m \oplus s)$ for the desired value m. According to Equation 12, if $\mathcal{O}(m) = \mathcal{O}(m \oplus s)$, then $\mathcal{O} = E_k$. Else $\mathcal{O} = \pi$.

In practice, it is possible that the round functions used in the 3-round Feistel structure do not behave like a completely random function or random permutation. As a result, the function f^{E_k} may have several unwanted collisions. Therefore, by Theorem 4, Simon's algorithm may not be able to compute the period s, which is the basis of the described distinguisher. To deal with this problem, Ito *et al.* [4] have focused on the dimension of the space spanned by the resulting vectors of Simon's algorithm. This method eliminates the need for recovering the actual period. As mentioned in Theorem 6, if the target function has no period, the dimension of the space spanned by the resulting vectors is equal to n with a high probability. Therefore, the distinguisher can detect the status $\mathcal{O} = \pi$ with a high probability. In the next section, we briefly describe the general form of Ito's relaxation method:

5.2.1 General Description of Ito's Distinguishers

Let $\mathcal{O} : F_2^l \to F_2^l$ be either a random permutation $\pi \xleftarrow{\$} perm(l)$ or a specified block cipher $E_k : F_2^l \to F_2^l$. Assuming that there exists a function $f^{E_k} : F_2^n \to F_2^m$ with key-dependent period s, Ito *et al.* [4], have proposed the following steps for distin-

guishing the status of the oracle $\mathcal{O}$:

(1) *Run the quantum circuit $S_{f^{\mathcal{O}}}$, $\mathcal{Z}$ times and add the result of each execution to a set U;*
(2) *If $dim(span(U)) = n$, then the distinguisher $\mathcal{D}$ guesses $\mathcal{O} = \pi$ and returns 0. Else $\mathcal{D}$ guesses $\mathcal{O} = E_k$ and outputs 1;*

Note that if the real status of the given oracle $\mathcal{O}$ is E_k, then the dimension of $span(U)$ is obviously smaller than n, because, by Theorem 1, all members of the set U are orthogonal to the period of the function f^{E_k}. As a result, by Theorem 6, we have

$$Pr[C] > 1 - 2^n \cdot e^{-\frac{\delta\mathcal{Z}}{2}} - Pr_\pi[\pi \in irr_f^\delta] \qquad (13)$$

5.2.2 Our Proposed Distinguisher

In this section, to deal with the described shortcomings of Simon's algorithm, we use the partial period instead of the actual one in period-finding-based quantum distinguishers. In the following, we use $\mathcal{Z}c$ and $\mathcal{Z}q$ to represent the number of classical and quantum queries of the attacker from the given quantum oracle $\mathcal{O}$, respectively. Note that, since the number of queries to quantum oracle $\mathcal{O}$ is restricted to $\mathcal{Z}$, we have $\mathcal{Z} = \mathcal{Z}c + \mathcal{Z}q$.

Let $\delta : 0 < \delta \leqslant 1$ be a value, say 0.5, such that $Pr[\exists t' : Pr_x[f^\pi(x) = f^\pi(x \oplus t')] > 1 - \delta]$ is small, provided that the permutation π is randomly selected. To know how to choose a suitable value for δ, we refer the reader to [4]. For distinguishing between E_k and a random permutation $\pi \xleftarrow{\$} perm(l)$, we suggest Algorithm 2 as follows. Just like Ito's method, we assume that for block cipher E_k there exists a function $f^{E_k} : F_2^n \to F_2^m$, so that it has a key-dependent period s.

Algorithm 2 Modified quantum distinguisher

1: Initialize the sets $U := \varnothing$ and $H := \varnothing$;
2: **for** $i = 1, \ldots, \mathcal{Z}q$, **do**
3: Run the quantum circuit $S_{f^{\mathcal{O}}}$ to get an n-bit vector u_i;
4: Set $U = U \cup \{u_i\}$;
5: **end for**
6: Compute the system of equations $x \cdot u_i = 0, \forall u_i \in U$ for x, store the solution(s) in an auxiliary variable A;
7: $a \xleftarrow{\$} A$;
8: **for** $i = 1, \ldots, \frac{\mathcal{Z}c}{2}$, **do**
9: $x_i \xleftarrow{\$} F_2^n$;
10: Compute $f^{\mathcal{O}}(x_i)$ and $f^{\mathcal{O}}(x_i \oplus a)$, store them in H;
11: **end for**
12: Compute the value $P' = \frac{|\{x_i : f^{\mathcal{O}}(x) = f^{\mathcal{O}}(x \oplus a)\}|}{\mathcal{Z}c/2}$ for member of H; (*In fact, P' is an estimation of* $P = Pr_x[f^{\mathcal{O}}(x) = f^{\mathcal{O}}(x \oplus a)]$)
13: **if** $P' > 1 - \delta + \frac{\epsilon}{2}$, **then**
14: Guess $\mathcal{O} = E_k$ and output 1;
15: **else**
16: Guess $\mathcal{O} = \pi$ and output 0;
17: **end if**

Note that the reason for using ϵ in step 13 of 2 is to decrease the error of estimating P. Below we explain how to choose a suitable ϵ.

Considering $\mathcal{Z}q$ and $\mathcal{Z}c$ as quantum and classical queries used in step 3 and 10, respectively, the data complexity of the attack is equal to

$$\mathcal{Z}q + \mathcal{Z}c = \mathcal{Z}$$

To compare the efficiency of our proposed distinguisher with Ito's, we compute $Pr[C]$, which is described in 2.3, as follows. To that end, let us first compute the probability that the attacker mistakenly returns 1, whereas the actual status of a given oracle is a random permutation π.

$$\begin{aligned}
&Pr\left[\mathcal{D}^{\pi,\pi^{-1}} = 1 |\ \pi \xleftarrow{\$} perm(n)\right] \\
&= Pr\left[\mathcal{D}^{\pi,\pi^{-1}} = 1 |\ \pi \xleftarrow{\$} perm(n), \pi \in irr_f^\delta\right] \cdot Pr_\pi[\pi \in irr_f^\delta] \\
&+ Pr\left[\mathcal{D}^{\pi,\pi^{-1}} = 1 |\ \pi \xleftarrow{\$} perm(n), \pi \notin irr_f^\delta\right] \cdot Pr_\pi[\pi \notin irr_f^\delta] \\
&\leqslant Pr_\pi[\pi \in irr_f^\delta] + Pr\left[\mathcal{D}^{\pi,\pi^{-1}} = 1 |\ \pi \xleftarrow{\$} perm(n), \pi \notin irr_f^\delta\right]
\end{aligned}$$

According to the definition, given in 2.8, for any permutation that is not a member of the set irr_f^δ, there exists no vector t so that $Pr_x[f^\pi(x) = f^\pi(x \oplus t)] > 1 - \delta$. As a result, $Pr[\mathcal{D}^{\pi,\pi^{-1}} = 1 |\ \pi \xleftarrow{\$} perm(n), \pi \notin irr_f^\delta] \leqslant Pr[P' - P \geqslant \frac{\epsilon}{2}]$. Therefore, according to Hoeffding's inequality [24] we have

$$\begin{aligned}
&Pr[\mathcal{D}^{\pi,\pi^{-1}} = 1 |\ \pi \xleftarrow{\$} perm(n)] \\
&\qquad \leqslant Pr_\pi[\pi \in irr_f^\delta] + e^{-\frac{\mathcal{Z}c\epsilon^2}{2}} \qquad (14)
\end{aligned}$$

On the other hand, the probability $Pr[\mathcal{D}^{E_k,E_k^{-1}} = 1 : k \xleftarrow{\$} F_2^{|k|}]$ is bounded as follows:

$$\begin{aligned}
&Pr[\mathcal{D}^{E_k,E_k^{-1}} = 1 |\ k \xleftarrow{\$} F_2^{|k|}] \geqslant \\
&\qquad Pr[P \geqslant 1 - \delta + \epsilon, (P - P') < \frac{\epsilon}{2}] \\
&= Pr[P \geqslant 1 - (\delta - \epsilon)] \cdot Pr[(P - P') < \frac{\epsilon}{2}] \qquad (15)
\end{aligned}$$

Consequently, according to Equation 14, Equation 15, Theorem 5 and Hoeffding's inequality, we have

$$Pr[C] > P_L - Pr_\pi[\pi \in irr_f^\delta] \qquad (16)$$

where we use P_L to indicate the following relation

$$\begin{aligned}
P_L = \max\left\{1 - \left(e^{-\frac{\mathcal{Z}q(\delta-\epsilon)^2}{2}}\right), 1 - \left(2(1 - \frac{\delta - \epsilon}{2})^{\frac{\mathcal{Z}q}{n}}\right)^n\right\} \\
\cdot \left(1 - e^{-\frac{\mathcal{Z}c\epsilon^2}{2}}\right) - e^{-\frac{\mathcal{Z}c\epsilon^2}{2}} \qquad (17)
\end{aligned}$$

Note that, Equation 16 is valid for all $\mathcal{Z}c$ and ϵ, therefore enjoy optimal performance, we should optimize it for both values $\mathcal{Z}c$ and ϵ. As a result

$$Pr[C] > \max_{\epsilon,\mathcal{Z}c}\{P_L\} - Pr_{\pi}[\pi \in irr_f^{\delta}] \qquad (18)$$

5.2.3 Comparison with Ito's Method

As shown in Table 2, the advantages of using the partial period over Ito's relaxation method is twofold: First, it applies not only to quantum distinguishers, but also to forgery attack on modes of operation for $MACs$. Second, it improves the success probabilities of quantum period-finding-based distinguishers, provided that the adversary is limited to a specified small number of queries. To show the second advantage, we compare the success probability of our proposed method with that of Ito's in terms of the number of quantum queries. If our proposed lower bound for $Pr[C]$ in Equation 18 is greater than that of Ito's in Equation 13, then our proposed attack would be stronger than Ito's. For this purpose, the value $\max_{\epsilon,\mathcal{Z}c}\{P_L\}$ in Equation 18 should be greater than the value $1 - 2^n \cdot e^{-\frac{\delta\mathcal{Z}}{2}}$ in Equation 13, that is

$$\max_{\epsilon,\mathcal{Z}c}\{P_L\} > 1 - 2^n \cdot e^{-\frac{\delta\mathcal{Z}}{2}} \qquad (19)$$

Let fix $\delta = 0.5$ and $n = 128$. As it can be seen in Figure 5, the Equation 19 holds for $\mathcal{Z} < 366$.

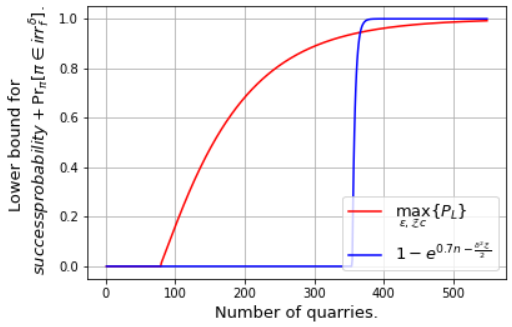

Figure 5. Investigate the establishment of Equation 19, for a special case, where $n = 128$ and $\delta = 0.5$

In conclusion, the attacker must check whether Equation 19 holds, according to the parameters used in the attack. If it holds, then our method is superior to Ito's, otherwise, Ito's is recommended.

5.3 Quantum Key Recovery Attack

In quantum key recovery attacks, just like the classical examples, the main target of the adversary is to recover the key of the underlying algorithm. Assuming access to the quantum oracle or quantum related-key oracle of the target function, the power of the quantum adversaries is surprisingly high in some types of mentioned attacks. For example, despite the fact that the security of Even-Mansour construction has been proved in random permutation model, Kuwakado *et al.* [8], has introduced a quantum key recovery attack, which works only with linear complexity. In another outstanding work, Roetteler *et al.* [10] have shown that by performing quantum related key attack, quantum adversaries are able to recover the key of block ciphers with linear complexity. In the following, we briefly describe their method.

5.3.1 Quantum Related-Key Attack

For block cipher $E_k : F_2^n \to F_2^n, k \in F_2^{|k|}$, consider the related-key oracle $\mathcal{O}_{E_k}$, which for block message $m \in F_2^n$ and bitmask $L \in F_2^{|k|}$ as input, returns the value $E_{k\oplus L}(m)$. In this attack, it is assumed that the attacker is allowed to query the oracle $\mathcal{O}_{E_k}$ with a superposition of keys. Let $m_1, \ldots, m_r : m_i \in F_2^n$ represent r arbitrary block message, so that m_i's are pairwise different. In the following, we use $\overrightarrow{M}$ and $E_k(\overrightarrow{M})$ to indicate $m_1\|\cdots\|m_r$ and $E_k(m_1)\|\cdots\|E_k(m_r)$, respectively. As shown by Roetteler *et al.* [10], according to the strict key avalanche criterion, if $r > \lceil\frac{2|k|}{n}\rceil$, the following relation holds.

$$E_k(\overrightarrow{M}) \neq E_{k'}(\overrightarrow{M}), \forall k, k' \in F_2^{|k|} : k \neq k'$$

Consider the function $f^{E_k} : F_2^{|k|} \to F_2^{2rn}$, which is defined as follows:

$$f^{E_k}(x) = \Big(\min\Big(E_x(\overrightarrow{M}), E_{x\oplus k}(\overrightarrow{M})\Big), \max\Big(E_x(\overrightarrow{M}), E_{x\oplus k}(\overrightarrow{M})\Big)\Big)$$

It is easy to verify that the function f^{E_k} is a periodic function with period $s = k$. Because

$$f^{E_k}(x) = f^{E_k}(x') \Leftrightarrow x' = x \oplus k$$

Consequently, one can recover the secret key k by performing Simon's algorithm.

In general, the main idea of period-finding-based quantum key recovery attacks, for analysis of E_k, is as follows:

(1) *Define the function f^{E_k} so that it has period k;*
(2) *Run Simon's algorithm to recover $s = k$, using unitary operator $\mathcal{O}_{f^{E_k}}$ to retrieve the period k;*

According to Theorem 4, if the function f^{E_k} has other collisions in addition to k or if $\mathcal{Z}$ is small, Simon's algorithm cannot recover the period $s = k$. This issue may lead to the failure of the quantum key recovery attacks. Note that, since quantum key recovery attacks aim at recovering the key of the target cipher, i.e. the actual period of the function f^{E_k}, one cannot use the concept of the partial period in

Table 2. Comparison between the results of the relaxation methods

Relaxation methods	modes of operation for MACs	Quantum distinguishers	Quantum key recovery attack
Focusing on the dimension of the space [4].	Not applicable	Preferred for a large number of quantum queries	Not applicable
Using partial period	$Pr_s > \max\left\{\left(1-\sqrt{\frac{2n}{\mathcal{Z}}}\right),\left(1-\frac{3n}{\mathcal{Z}}\right)\right\}$	Preferred for a small number of quantum queries	Not applicable
Using Grover's algorithm as a complement of Simon's algorithm	Not applicable	Not applicable	$T \leqslant O(\sqrt{2^{\lvert k\rvert-1}})$

the aforementioned attacks. Therefore, we suggest the following algorithm. In this section, we show that even if Simon's algorithm cannot compute the period $s = k$, it reduces the key space of the target cryptosystem. Therefore, the attacker can search in the remaining space with the help of Grover's algorithm.

5.3.2 Modified Quantum Key-Recovery Attacks

According to Theorem 3, each execution of the quantum circuit $S_{f^{E_k}}$, as a subroutine of Simon's algorithm, produces a vector u_i orthogonal to the key of the target algorithm (i.e. period of f^{E_k}). Let $U = \{u_1, \ldots, u_{\mathcal{Z}}\}$, Dim and B represent the set of all vector obtained from $\mathcal{Z}$ times execution of quantum circuit $S_{f^{E_k}}$, as subroutine of Simon's algorithm, dimension of $span(U)$ and a basis for subspace $span(U)$, respectively. As a result, running Simon's algorithm with $\mathcal{Z}$ quantum query, leaks Dim-bits information about the target key to the attacker. Therefore, he can search the remaining key space using Grover's algorithm. In summary, we propose the following algorithm.

Algorithm 3 Modified quantum key recovery attack

1: Initialize the set $U := \varnothing$;
2: **for** $i = 1, \ldots, \mathcal{Z}$, **do**
3: Run the quantum circuit $S_{f^{E_k}}$ to get a $|k|$-bit vector u_i;
4: Set $U = U \cup u_i$;
5: **end for**
6: compute the value of $dim(span(U))$, store the result in auxiliary variable Dim;
7: **if** $Dim == |k|-1$, **then**
8: Solve the system of equations $x \cdot u_i = 0, \forall u_i \in U$;
9: Return the result of step 7 as the target key and finish the algorithm;
10: **else**
11: Find a basis for $span(U)$ and store the result in an auxiliary set B;
12: Apply the generalized Grover's algorithm, where
- Setup: Construct the state $\frac{1}{\sqrt{2^{|k|-dim}}}\sum_{x:x\cdot b=0,\forall b\in B}|x\rangle$, using Grover's algorithm without any measurement.
- Checking: Check if input x is the key of E_k.

13: **end if**

Considering 3 uses the quantum oracle function $\mathcal{Z}$ times, the data complexity is $\mathcal{Z}$. According to Theorem 2, the cost of *setup* in step 12 of 3 is $\sqrt{\frac{2^{|k|}}{2^{|k|-Dim}}} \cdot T_{dot} = \sqrt{2^{-Dim}} \cdot T_{dot}$, where T_{dot} indicates the time required to execute an inner product. Therefore, according to Theorem 1, the total cost of 3 is equal to

$$\begin{aligned}&\sqrt{|X|/|M|}(Cost(setup) + Cost(Checking)) + \mathcal{Z}\\ &= \sqrt{2^{|k|-Dim}}(\sqrt{2^{-Dim}} \cdot T_{dot} + T_{f^E}) + \mathcal{Z}\\ &= \sqrt{2^{|k|}}T_{dot} + \sqrt{2^{|k|-Dim}}T_{f^E} + \mathcal{Z} \qquad (20)\end{aligned}$$

Where T_{f^E} indicates the time required to execute the function E in a superposition of states.
Note that in Equation 20 for the small value of Dim, the second term is dominant compared to the first and third terms in view of computation complexity of 3. Therefore the complexity of the algorithm is almost equal to the second term. Otherwise, if the value of Dim is large, the attacker can search for the target key k in the candidate subspace classically. Therefore, the time complexity is obtained as follows:

$$\min\left\{\left(\sqrt{2^{|k|}}T_{dot} + \sqrt{2^{|k|-Dim}}T_{f^E} + \mathcal{Z}\right), \left(2^{|k|-Dim}T_{f^E}\right)\right\}$$

Note that, for a fixed $\mathcal{Z}$, the value of the Dim is completely related to the target algorithm E_K, but certainly is greater than 0. This ensures that the time complexity of the attack is less than that of a quantum brute-force attack.

In conclusion, 3 can be used in the following quantum attacks.

- Key recovery attack on Even-Mansour construction introduced by Kuwakado *et al.* [8].
- Quantum Slide attack introduced by Kaplan *et al.* [5].
- Quantum related key attack introduced by Roetteler *et al.* [10].
- Quantum slide attacks introduced by Bonnetain *et al.* [11].

6 Conclusions

Period-finding is one of the most widely used concepts in quantum cryptanalysis of symmetric primitives using specific structures, which can be computed by Simon's quantum algorithm, assuming access to the quantum oracle of the target primitive. Nevertheless, unwanted collisions of the target periodic function or limitations on the number of quantum queries of the adversary can be a bottleneck for the correct operation of Simon's algorithm. This issue can lead to the failure of period-finding-based quantum attacks. In this paper, we have relaxed Simon's algorithm using two different methods. In the first method, we have used the partial period instead of the actual one. This method not only improves the success probability of the period-finding-based quantum distinguishers, provided that the adversary is limited to a specified small number of queries, but also relaxes quantum forgery attacks on modes of operation for MACs. On the other hand, in the case of quantum key recovery attacks, we have used Grover's algorithm as a complement to Simon's algorithm. As a result, even if Simon's promise is not satisfied and the target function has numerous collisions other than the target period, the complexity of the attack, independent of the target primitive, is certainly less than the complexity of the quantum brute force attack.

Note that our proposed quantum distinguisher makes some classical queries to the given quantum oracle. Considering the quantum counting algorithm, using a quantum query, provides quadradic speed up, it seems that using this algorithm can improve the success probability of our proposed distinguisher. On the other hand, based on some primary research in quantum differential attacks, it seems that the partial period has great potential for computing an appropriate differential characteristic. These ideas can be considered for future works.

Acknowledgment

The authors would like to thank Saba Karimani, Masroor Hajari, Abbas Rabbani, Mohammadreza Khosravi and Mahdi Rahimi for the interesting discussions that we shared.

References

[1] Peter W Shor. Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings 35th annual symposium on foundations of computer science*, pages 124–134. IEEE, 1994.

[2] Lov K Grover. A fast quantum mechanical algorithm for database search. In *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*, pages 212–219, 1996.

[3] Daniel R Simon. On the power of quantum computation. *SIAM journal on computing*, 26(5):1474–1483, 1997.

[4] Gembu Ito, Akinori Hosoyamada, Ryutaroh Matsumoto, Yu Sasaki, and Tetsu Iwata. Quantum chosen-ciphertext attacks against feistel ciphers. In *Cryptographers' Track at the RSA Conference*, pages 391–411. Springer, 2019.

[5] Marc Kaplan, Gaëtan Leurent, Anthony Leverrier, and María Naya-Plasencia. Breaking symmetric cryptosystems using quantum period finding. In *Annual international cryptology conference*, pages 207–237. Springer, 2016.

[6] Hidenori Kuwakado and Masakatu Morii. Quantum distinguisher between the 3-round feistel cipher and the random permutation. In *2010 IEEE International Symposium on Information Theory*, pages 2682–2685. IEEE, 2010.

[7] Huiqin Xie and Li Yang. Quantum miss-in-the-middle attack. *arXiv preprint arXiv:1812.08499*, 2018.

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

[9] Shimon Even and Yishay Mansour. A construction of a cipher from a single pseudorandom permutation. *Journal of cryptology*, 10(3):151–161, 1997.

[10] Martin Roetteler and Rainer Steinwandt. A note on quantum related-key attacks. *Information Processing Letters*, 115(1):40–44, 2015.

[11] Xavier Bonnetain, María Naya-Plasencia, and André Schrottenloher. On quantum slide attacks. In *International Conference on Selected Areas in Cryptography*, pages 492–519. Springer, 2019.

[12] Gregor Leander and Alexander May. Grover meets simon–quantumly attacking the fx-construction. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 161–178. Springer, 2017.

[13] André Chailloux, María Naya-Plasencia, and André Schrottenloher. An efficient quantum collision search algorithm and implications on symmetric cryptography. In *International Conference on the Theory and Application of Cryptology and Information Security*, volume 10625, pages 211–240. Springer, 2017.

[14] María Naya-Plasencia. Preparing symmetric crypto for the quantum world. In *FSE 2019-26th Annual Fast Software Encryption Conference*, 2019.

[15] Akinori Hosoyamada and Yu Sasaki. Cryptanalysis against symmetric-key schemes with online classical queries and offline quantum computa-

tions. In *Cryptographers' Track at the RSA Conference*, volume 10808, pages 198–218. Springer, 2018.

[16] Xavier Bonnetain, Akinori Hosoyamada, María Naya-Plasencia, Yu Sasaki, and André Schrottenloher. Quantum attacks without superposition queries: the offline simon's algorithm. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 552–583. Springer, 2019.

[17] Xuexuan Hao, Fengrong Zhang, Yongzhuang Wei, and Yong Zhou. Quantum period finding based on the bernstein-vazirani algorithm. *Quantum Inf. Comput.*, 20(1&2):65–84, 2020.

[18] Mark Zhandry. A note on quantum-secure prps. *arXiv preprint arXiv:1611.05564*, 2016.

[19] Ping Wang, Shengping Tian, Zhiwei Sun, and Ning Xie. Quantum algorithms for hash preimage attacks. *Quantum Engineering*, 2(2):e36, 2020.

[20] Gilles Brassard, Peter Høyer, and Alain Tapp. Quantum cryptanalysis of hash and claw-free functions. In *Latin American Symposium on Theoretical Informatics*, pages 163–169. Springer, 1998.

[21] Marc Kaplan, Gaëtan Leurent, Anthony Leverrier, and María Naya-Plasencia. Quantum differential and linear cryptanalysis. *arXiv preprint arXiv:1510.05836*, 2015.

[22] Huiqin Xie and Li Yang. Using bernstein–vazirani algorithm to attack block ciphers. *Designs, Codes and Cryptography*, 87(5):1161–1182, 2019.

[23] Hongwei Li and Li Yang. A quantum algorithm to approximate the linear structures of boolean functions. *Mathematical Structures in Computer Science*, 28(1):1–13, 2018.

[24] W Hoeffding. Probability inequalities for sums of bounded random variables, amer. ž. *Statist. Assoc. J*, 1329, 1963.

[25] 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*, pages 44–63. Springer, 2016.

Ali Khosravi received his B.Sc. degree in Electronic Technology from the Shamsipour Technical and Vocational College and the M.Sc. degree in Telecommunications (Cryptography and Secure Communication) from the Sharif University of Technology, Tehran, Iran, in 2018 and 2020, respectively. His current research interests include quantum cryptanalysis of symmetric cryptosystems and quantum secure symmetric primitives.

Taraneh Eghlidos received her B.Sc. degree in mathematics from the University of Shahid Beheshti, Tehran, Iran, in 1986, and the M.Sc. degree in industrial mathematics from the University of Kaiserslautern, Germany, in 1991. She received her Ph.D. degree in mathematics from the University of Giessen, Germany, in 2000. She joined the Sharif University of Technology (SUT) in 2002, as a faculty member, and is currently an Associate Professor with the Electronics Research Institute at SUT. Her research interests include interdisciplinary research areas, such as symmetric and asymmetric cryptography, applications of coding theory in cryptography, and mathematical modeling for representing and solving real-world problems. Her current fields of research include lattice-based and code-based cryptography.