symmetry

IMPACT FACTOR 2.940

CITESCORE 4.3

Article

Quantum Related-Key Attack Based on Simon's Algorithm and Its Applications

Ping Zhang

MDPI

https://doi.org/10.3390/sym15050972

symmetry

MDPI

Article

Quantum Related-Key Attack Based on Simon's Algorithm and Its Applications

Ping Zhang

School of Computer Science, Nanjing University of Posts and Telecommunications, Nanjing 210023, China; zhgp@njupt.edu.cn

Abstract: With the development of quantum technology, quantum computing has an increasingly significant impact on cryptanalysis. Several quantum algorithms, such as Simon's algorithm, Grover's algorithm, the Bernstein–Vazirani algorithm, Shor's algorithm, and the Grover-meets-Simon algorithm, have been proposed successively. However, almost all cryptanalysis is based on the quantum chosen-plaintext attack (qCPA) model. This paper focuses on a powerful cryptanalytic model, quantum related-key attack (qRKA), and proposes a strategy of qRKAs against symmetric ciphers using Simon's algorithm. We construct a periodic function to efficiently recover the secret key of symmetric ciphers if the attacked symmetric ciphers satisfy Simon's promise, and present the complexity analysis on specific symmetric ciphers. Then, we apply qRKA to the Even–Mansour cipher and SoEM construction, recover their secret keys, and show their complexity comparison in the distinct attack models. This work is of great significance for the qRKA cryptanalysis of existing provably secure cryptographic schemes and the design of future quantum secure cryptographic schemes.

Keywords: quantum cryptography; quantum cryptanalysis; quantum related-key attack; quantum algorithm; symmetric ciphers

Citation: Zhang, P. Quantum Related-Key Attack Based on Simon's Algorithm and Its Applications. *Symmetry* **2023**, *15*, 972. https://doi.org/10.3390/sym15050972

Academic Editor: Aviv Gibali

Received: 10 March 2023
Revised: 13 April 2023
Accepted: 22 April 2023
Published: 24 April 2023

1. Introduction

In recent years, countries all over the world have been vigorously promoting the research and development of quantum computing and quantum computers. This has brought great security threats to existing cryptosystems. Compared with classical computing (classical computers), quantum computing (quantum computers) has shown great advantages in solving the large integer factorization problem, the discrete logarithm problem, the key brute force search problem and other problems. For example, Shor's algorithm can break RSA and ECC ciphers in polynomial time [1]. In order to resist the security threats brought by quantum computing and quantum computers, countries around the world are accelerating the research, development, and standardization of post-quantum cryptography. Currently, the standardization of post-quantum cryptography carried out by National Institute of Standards and Technology (NIST) has entered the fourth round. Therefore, the quantum cryptanalysis of existing cryptographic schemes becomes increasingly important.

Quantum algorithms are important tools for achieving quantum cryptanalysis of cryptographic schemes. There exist many quantum algorithms in symmetric-key ciphers, such as Grover's algorithm [2], Simon's algorithm [3], Bernstein–Vazirani (BV) algorithm [4], HHL algorithm [5], and their generalization and hybrid algorithms [6,7]. Grover's algorithm is a widely used quantum search algorithm which provides a quadratic speed-up for searching the secret key from a key space [2,8,9]. This threatens the security of symmetric cryptography. For example, in 2021, Bathe et al. presented key-recovery attacks against ChaCha by Grover's search algorithm [10]. Simon's algorithm is a period finding algorithm in polynomial time and has been widely used in cryptanalysis of symmetric ciphers [6,11–23]. For example, Kuwakado and Morii used Simon's algorithm to distinguish a three-round Feistel structure with a random permutation in 2010 [19], and then recovered the key of

the Even–Mansour cipher in 2012 [24]. In 2020, Dong et al. presented quantum analyses on Feistel structure and generalized Feistel structure based on Simon's algorithm [14,25]. In 2021, Cui et al. used Simon's algorithm to launch quantum attacks on Feistel variant schemes [13]. In 2022, Mao et al. used Simon's algorithm to launch quantum attacks on Lai–Massey structure [26]. The Bernstein–Vazirani algorithm can be used to find the linear structures of a Boolean function, which enables quantum attacks against block ciphers. Xie and Yang proposed new quantum distinguishers for the three-round Feistel scheme, recovered a partial key of the Even–Mansour construction, and found high-probability differentials by the Bernstein–Vazirani algorithm [4]. The Bernstein–Vazirani algorithm can be utilized to find the period of the function [27]. Therefore, it also has the capability of Simon's algorithm. The HHL algorithm can be used to solve linear systems of equations quickly and achieve exponential acceleration [28]. Liu and Gao utilized the HHL algorithm to analysis quantum security of Grain-128/Grain-128a stream cipher [5]. For some constructions, such as FX and SoEM22, a single quantum algorithm does not work. Leander and May proposed a Grover-meets-Simon algorithm and presented a quantum key-recovery attack on FX construction [29]. Grover-meets-Simon algorithm was later used in SoEM22 [6] and 5-round Feistel structure [15]. Recently, Guo et al. introduced three general frameworks—F1, F2, and F3—for n-to-n-bit pseudorandom functions (PRFs) based on public random permutations, and showed that F1 is not secure with $O(n)$ quantum queries by Simon's algorithm while its PRFs achieve $n/2$-bit security in the classical setting, and F2 and F3 are not secure with $O(n \cdot 2^{n/2})$ quantum queries by Grover-meets-Simon algorithm while their PRFs, such as SoEM22, PDMMAC, and pEDM, achieve $2n/3$-bit security in the classical setting [30]. Nan et al. presented quantum key recovery attack against pEDM and pPMAC-plus by the Grover-meets-Simon algorithm [31]. The Grover-meets-BV algorithm proposed by Zhou and Yuan combined the Bernstein–Vazirani algorithm and Grover's algorithm to achieve quantum key-recovery attacks on 5 or more rounds Feistel structures [7]. Variational quantum algorithms (VQAs) use a classical optimizer to train a parameterized quantum circuit. Wang et al. used VQA to study the security of symmetric encryption algorithm S-DES under VQA attacks and obtained the encrypted key.

However, all of the attacks described above are based on the quantum chosen-plaintext attack (qCPA) model. If we give an adversary more ability than qCPA, can we utilize Simon's algorithm to recover the secret key of cryptographic schemes? Further, can we recover the secret key of cryptographic schemes that provide enough security under the qCPA model by Simon's algorithm?

Our contributions. This paper focuses on the quantum related-key attack (qRKA) model and presents positive responses for the above problems. The qRKA model was first introduced by Roetteler and Steinwandt [32] and had already made some progress in quantum cryptanalysis [33,34]. In this paper, based on Simon's algorithm, we propose a strategy of quantum key recovery attacks against symmetric ciphers under the qRKA model. We first construct a periodic function based on the attacked symmetric cipher and then apply Simon's algorithm to recover the secret key. The complexity of the attack is polynomial in terms of the key bits and the complexity comparison on specific symmetric ciphers is presented. Finally, we apply qRKA to two instances of symmetric ciphers: the Even–Mansour cipher and the SoEM construction (including all variants of SoEM: SoEM1, SoEM21, and SoEM22), present their key recovery attacks under the qRKA model, and show their complexity comparison under the distinct attack models. SoEM22 enjoys enough security against $O(n \cdot 2^{n/2})$ quantum queries under the qCPA model, but its secret key can be recovered in $O(n)$ quantum queries under the qRKA model, which is the greatest significance of our work.

Related works. The classical RKA is a powerful attack model, which gives the adversary more ability than the classical CPA. In classical RKA, the adversary can query encryption and decryption oracles under different keys derived from the target key by a known mathematical relationship. The bit-flip is a common mathematical relationship. The qRKA is a more powerful attack model than RKA, which gives the adversary to query the

encryption and decryption oracles with a quantum superposition. Roetteler and Steinwandt first recovered the key of block ciphers under the qRKA model [32]. In 2017, Hosoyamada and Aoki introduced qRKA and proposed a quantum algorithm that recovers the key of the two-round iterated Even–Mansour cipher [33]. In 2020, Xie and Yang focused on the qRKA based on the BV algorithm, described a strategy for attacking general block ciphers using the BV algorithm, and applied it to the Even–Mansour cipher [34]. Later, Malviya et al. concluded several latest quantum cryptanalysis techniques including qRKA for attacking symmetric cryptography [21]. In 2023, Sun et al. introduced an improved BV-based algorithm to realize a quadratic speedup and presented qRKAs on iterated Even–Mansour ciphers and i-round Feistel ciphers with independent round keys [35].

Organizations of this paper. The preliminaries are presented in Section 2. The strategy of qRKAs against block ciphers is shown in Section 3. In Section 4, we describe two applications under the qRKA model. Section 5 presents the conclusions.

2. Preliminaries

2.1. Notations

Let $\oplus$ denote the XOR operation. Let $E : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ be a block cipher with block size n and key size k. Given a key $K \in \{0,1\}^k$, E_K is a permutation from $\{0,1\}^n$ to $\{0,1\}^n$ and $D_K = E_K^{-1}$. We assume that there exists a polynomial-time quantum circuit to efficiently implement E. Define the following unitary operator U_E:

$$U_E : \sum_{m,x,y} |x\rangle|m\rangle|y\rangle \to \sum_{m,x,y} |x\rangle|m\rangle|y \oplus E_x(m)\rangle \tag{1}$$

Equation (1) shows that the quantum circuit of U_E does not include the key K. Therefore, it can be queried by anyone, including malicious adversaries. The malicious adversary can integrate U_E into its circuits.

Let $|E|_Q$ be the number of universal gates (including Hadamard gate H, controlled-NOT gate $CNOT$, phase gate $Phase$, etc.) in the quantum circuit implementing E, that is, $|E|_Q$ is a polynomial of parameter n [34].

2.2. Quantum Related-Key Attack Model [32,34]

The so-called related-key attack is that the adversary does not know the key K, but knows that the key K satisfies a mathematical relationship $\Phi(K)$. To adapt Simon's algorithm to achieve exponential acceleration, here, we restrict the relationship $\Phi(K)$ as bit-flips, i.e., $\Phi(K) = K \oplus x$, where x is a bitmask.

In the classical related-key attack model, with a fixed secret key K, the adversary can query encryption and decryption oracles:

- $\mathcal{E}$: It takes a plaintext $m \in \{0,1\}^n$ and a bitmask $x \in \{0,1\}^k$ as input, and outputs $E_{K\oplus x}(m)$.
- $\mathcal{D}$: It takes a ciphertext $c \in \{0,1\}^n$ and a bitmask $x \in \{0,1\}^k$ as input and outputs $D_{K\oplus x}(c)$.

After querying these oracles, the adversary obtains a guess key K'. If $K' = K$, the adversary succeeds in obtaining the correct key.

In the quantum related-key attack model, wirh a fixed secret key K, the adversary is allowed to query the quantum encryption oracle $O_{\mathcal{E}}$ and the quantum decryption oracle $O_{\mathcal{D}}$ with superpositions of keys, i.e.,

$$O_{\mathcal{E}} : \sum_{m,x,y} |x\rangle|m\rangle|y\rangle \to \sum_{m,x,y} |x\rangle|m\rangle|y \oplus E_{K\oplus x}(m)\rangle \tag{2}$$

$$O_{\mathcal{D}} : \sum_{c,x,y} |x\rangle|c\rangle|y\rangle \to \sum_{c,x,y} |x\rangle|c\rangle|y \oplus D_{K\oplus x}(c)\rangle. \tag{3}$$

In particular, if the adversary is just allowed to query the quantum encryption oracle $O_{\mathcal{E}}$ with the superposition state $\sum_{m,y} |0^k\rangle|m\rangle|y\rangle$ and discard the first register, then $O_{\mathcal{E}}$ will correspond to cryptographic primitive O_{E_K}, i.e.,

$$O_{E_K} : \sum_{m,y} |m\rangle|y\rangle \rightarrow \sum_{m,y} |m\rangle|y \oplus E_K(m)\rangle. \tag{4}$$

Furthermore, if the adversary is also allowed to query the quantum decryption oracle $O_{\mathcal{D}}$ with the superposition state $\sum_{m,y} |0^k\rangle|c\rangle|y\rangle$ and discard the first register, then $O_{\mathcal{D}}$ will correspond to the cryptographic inverse primitive O_{D_K}, i.e.,

$$O_{D_K} : \sum_{c,y} |c\rangle|y\rangle \rightarrow \sum_{c,y} |c\rangle|y \oplus D_K(c)\rangle. \tag{5}$$

Therefore, the quantum related-key attack model can be seen as an extension of the quantum chosen-plaintext and chosen-ciphertext attack models.

As quantum attacks in this paper do not involve quantum decryption oracle $O_{\mathcal{D}}$ queries, the quantum related-key attack model we consider is just in the quantum encryption oracle $O_{\mathcal{E}}$. The adversary can integrate the quantum encryption oracle $O_{\mathcal{E}}$ into its circuits.

2.3. Simon's Algorithm [3,18,21,33]

Simon's algorithm is a quantum algorithm that efficiently solves the period finding problem of a function in polynomial times.

Definition 1 (Period finding problem)**.** *Given a Boolean function $f : \{0,1\}^k \rightarrow \{0,1\}^n$, assume that there exists some non-zero $s \in \{0,1\}^k \setminus \{0^k\}$ such that $f(x \oplus s) = f(x)$ holds for any $x \in \{0,1\}^k$. The goal is to find s.*

Simon's algorithm finds s with high probability by performing polynomial quantum queries ($O(k)$) and quantum bit memory ($O(k)$). The details of Simon's algorithm are shown in Algorithm 1.

Algorithm 1 Simon's Algorithm.

1: Initialize $2k$ qubits state $|0^k\rangle|0^k\rangle$.
2: Apply Hadamard transform $H^{\otimes k}$ to the first k qubits to obtain quantum superposition $\frac{1}{\sqrt{2^k}} \sum_{x\in\{0,1\}^k} |x\rangle|0^n\rangle$.
3: A quantum query to the function f maps this to the state $\frac{1}{\sqrt{2^k}} \sum_{x\in\{0,1\}^k} |x\rangle|f(x)\rangle$.
4: Measuring the second register in the computational basis yields a value $f(z)$ and collapses the first register to the state: $\frac{1}{\sqrt{2}}(|z\rangle + |z \oplus s\rangle)$.
5: Applying again the Hadamard transform $H^{\otimes k}$ to the first register gives: $\frac{1}{\sqrt{2}} \frac{1}{\sqrt{2^k}}$ $\sum_{y\in\{0,1\}^k} |(-1)^{y\cdot z}(1 + (-1)^{y\cdot s})\rangle|y\rangle$.
6: The vectors y such that $y \cdot s = 1$ have amplitude 0. Therefore, measuring the state in the computational basis yields a random vector y such that $y \cdot s = 0$.
7: By repeating the above steps $O(k)$ times, one obtains $k-1$ independent vectors orthogonal to s with high probability, and s can be recovered using basic linear algebra.

To resolve unwanted collisions, Kaplan et al. introduced the following index [18]:

$$\epsilon(f, s) = \max_{t\in\{0,1\}^k\setminus\{0,s\}} Pr_x[f(x) = f(x \oplus t)]. \tag{6}$$

It represents the maximum probability of unwanted additional collisions.

Proposition 1 (Simon [3], Kaplan et al. [18], Guo et al. [16])**.** *Let p_0 and c be positive integers. If $\epsilon(f,s) \leq p_0 < 1$, then Simon's algorithm finds s with ck queries, with probability of at least $1-(2(\frac{1+p_0}{2})^c)^k$.*

Later, Hosoyamada and Aoki further considered the period finding problem of a function with constant addition [33].

Definition 2 (Period finding problem with constant addition)**.** *Given a Boolean function $f:\{0,1\}^k \to \{0,1\}^n$, assume that there exists some non-zero $s \in \{0,1\}^k \setminus \{0^k\}$ and $r \in \{0,1\}^n$ such that $f(x \oplus s) = f(x) \oplus r$ for any $x \in \{0,1\}^k$. The goal is to find s and r.*

Hosoyamada and Aoki considered the difference of f [33]:

$$(\Delta_u f)(x) = f(x) \oplus f(x \oplus u). \tag{7}$$

Take $u \in \{0,1\}^k$ arbitrarily, for $\forall x \in \{0,1\}^k$, there exist $w \in \{0,1\}^k$ such that

$$(\Delta_u f)(x \oplus w) = (\Delta_u f)(x). \tag{8}$$

Then, $(\Delta_u f)(x)$ is a double-period function with a double period $w = \{s, u\}$. After performing Simon's algorithm, they finds s with high probability. Then, $r = f(x \oplus s) \oplus f(x)$ is also recovered.

Proposition 2 (Hosoyamada and Aoki [33])**.** *Let p_0 and c be positive integers. If $\epsilon(\Delta_u f, w) \leq p_0 < 1$, then, after performing Simon's algorithm, (s,r) can be found by ck queries, with probability of at least $1-(2(\frac{1+p_0}{2})^c)^k$.*

3. Strategy of Quantum Related-Key Attacks

3.1. Description of Quantum Related-Key Attacks

The strategy of quantum attacks against symmetric ciphers using Simon's algorithm usually consists of two steps:

- Construct a periodic function F with/without constant addition based on the cipher E so that F meets (1) the adversary has quantum oracle access to F; (2) the period of F with/without constant addition includes the information of the secret key or even the secret key itself;
- Apply Simon's algorithm to F or the differential of F, obtain the period of F with/without constant addition, and then recover the secret key.

The traditional quantum attacks against symmetric ciphers are achieved by constructing a periodic function with/without constant addition that takes plaintexts or tweaks as input and the secret key or its partial information as period. In other words, they are based on the quantum chosen-plaintext attack model (qCPA). However, it is a little different under the quantum related-key attack model (qRKA). We construct a periodic function with/without constant addition that takes a bit-mask of the key as input and the secret key or its partial information as period.

Let $E:\{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ be a symmetric cipher, $K \in \{0,1\}^k$ be the secret key, and $m \in \{0,1\}^n$ be an arbitrary plaintext, then, for any $x \in \{0,1\}^k$, we construct a function

$$F_K^m(x) = E_x(m) \oplus E_{x \oplus K}(m). \tag{9}$$

We find that: (1) For any $x \in \{0,1\}^k$, $F_K^m(x)$ is a periodic function with period K, i.e.,

$$F_K^m(x \oplus K) = F_K^m(x). \tag{10}$$

(2) The adversary has quantum oracle access to F_K^m, which can be obtained by first querying $Q_{\mathcal{E}} : |x, m, y\rangle \rightarrow |x, m, y \oplus E_{K\oplus x}(m)\rangle$ and then computing $U_E : |x, m, y\rangle \rightarrow |x, m, y \oplus E_x(m)\rangle$.

Therefore, according to Proposition 1, under the condition $\epsilon(F_K^m, K) \leq p_0 < 1$, the secret key K is recovered. Similarly, we can also construct a periodic function with constant addition and recover the secret key using Proposition 2.

3.2. Simon's Promise

To use Simon's algorithm, we need to verify the Simon's promise $\epsilon(F_K^m, K) \leq p_0 < 1$. Simon presented a simple distinguishing attack if this Simon's promise is not satisfied [18]. For a specific symmetric cipher, we can verify whether it meets the Simon's promise. Bounding p_0 usually utilize the Hoeffding inequality. Here, we present a simple analysis if the Simon's promise is not satisfied.

$$\epsilon(F_K^m, K) = \max_{t\in\{0,1\}^k\setminus\{0,K\}} Pr_x[F_K^m(x) = F_K^m(x \oplus t)] \tag{11}$$

$$= \max_{t\in\{0,1\}^k\setminus\{0,K\}} Pr_x[E_x(m) \oplus E_{x\oplus K}(m) \oplus E_{x\oplus t}(m) \oplus E_{x\oplus t\oplus K}(m) = 0]. \tag{12}$$

According to Equation (12), as $t \in \{0,1\}^k \setminus \{0, K\}$, therefore x, $x \oplus t$, $x \oplus K$, and $x \oplus t \oplus K$ are always four distinct keys. After going through all possible values of x, the exclusive value of the ciphertexts of m under these four distinct keys is 0 with a probability close to 1, which should not exist for a well-constructed symmetric cipher. If Simon's promise is not satisfied, we can construct a polynomial-time distinguisher of the symmetric cipher.

For any constant $\varepsilon(\varepsilon \ll 1)$, there exists $t \in \{0,1\}^k \setminus \{0, K\}$ such that

$$Pr_x[E_x(m) \oplus E_{x\oplus K}(m) \oplus E_{x\oplus t}(m) \oplus E_{x\oplus t\oplus K}(m) = 0] \geq 1 - \varepsilon, \tag{13}$$

i.e.,

$$\frac{|\{x \in \{0,1\}^k \mid E_x(m) \oplus E_{x\oplus K}(m) \oplus E_{x\oplus t}(m) \oplus E_{x\oplus t\oplus K}(m) = 0\}|}{2^k} \geq 1 - \varepsilon. \tag{14}$$

Similar to [34], according to Equation (14), we choose a constant $\varepsilon(\varepsilon \ll 1)$ and then show a simple distinguish attack against the symmetric cipher E as follows:

1. Randomly choose $x_1, x_2, \cdots, x_p$ from $\{0,1\}^k$, where $p = O(k)$. Then, using the quantum circuit of U_E, we compute $E_{x_1}(m), \cdots, E_{x_p}(m)$, $E_{x_1\oplus t}(m), \cdots, E_{x_p\oplus t}(m)$;
2. Query $E_{x_1\oplus K}(m), \cdots, E_{x_p\oplus K}(m)$, $E_{x_1\oplus t\oplus K}(m), \cdots, E_{x_p\oplus t\oplus K}(m)$ using the quantum encryption circuit of $O_{\mathcal{E}}$. Then, using the quantum encryption circuits of U_E and $O_{\mathcal{E}}$, we compute $Z_i = E_{x_i}(m) \oplus E_{x_i\oplus K}(m) \oplus E_{x_i\oplus t}(m) \oplus E_{x_i\oplus t\oplus K}(m)$ for $i = 1, \cdots, p$. From Equation (14), the probability that $Z_i = 0$ is greater than $1 - \varepsilon$;
3. According to the Hoeffding inequality, except for a negligible probability, the probability of random variable $Z = E_x(m) \oplus E_{x\oplus K}(m) \oplus E_{x\oplus t}(m) \oplus E_{x\oplus t\oplus K}(m)$ whose value is equal to 0 in the set $\{Z_i \mid i = 1, \cdots, p\}$ is greater than $1 - 2\varepsilon$.

While, for a random permutation, the probability that $Z = 0$ in the set $\{Z_i \mid i = 1, \cdots, p\}$ is greater than $1 - 2\varepsilon$ is negligible. Therefore, the above attack can distinguish the symmetric cipher from a random permutation.

3.3. Complexity Analysis

Under the qRKA model, the quantum gate of $F_K^m(x)$ runs Simon's algorithm once to execute $2k$ Hadamard gates, one unitary operator U_E, and one quantum encryption oracle $O_{\mathcal{E}}$. Thus, $F_K^m(x)$ needs $2k$ qubits, $(2k + |E|_Q)O(k)$ universal gates, and $O(k)$ quantum queries. To visually demonstrate the advantages of exponential acceleration of our strategy, the comparison of previous attacks and our attacks on specific symmetric ciphers is shown in Table 1. Table 1 shows that qRKA based on Simon's algorithm is the best.

Table 1. Complexity comparison on specific symmetric ciphers.

Scheme	Classical Attack	Bernstein–Vazirani Algorithm	Simon's Algorithm
AES-128	2^{126} [36]	128^2 [34]	128
DES	2^{39}–2^{41} [37]	64^2 [34]	56
PRESENT-80	$2^{79.34}$ [38]	64^2 [34]	80
SIMON 128/256	2^{248} [39]	128^2 [34]	256

4. Applications

In this section, we present two applications and prove that the secret keys of the Even–Mansour cipher and SoEM construction can be efficiently extracted under the quantum related-key attack model.

4.1. Application to the Even–Mansour Cipher

Let $K = (K_1, K_2)$ be a tuple of two n-bit keys. Let P be a public n-bit random permutation. Given a plaintext m, the Even–Mansour cipher is defined as

$$E_K(m) = P(m \oplus K_1) \oplus K_2. \tag{15}$$

Theorem 1. *There exists a quantum related-key attack against the Even–Mansour cipher that recovers the secret keys K_1 and K_2 with $O(n)$ qubits and $O(n)$ quantum queries.*

Proof. For an arbitrary plaintext $m \in \{0,1\}^n$, let $x = (x_1, x_2) \in \{0,1\}^{2n}$, we construct a function

$$\begin{aligned} F_K^m(x) =& E_x(m) \oplus E_{x\oplus K}(m) && (16)\\ =& P(m \oplus x_1) \oplus P(m \oplus x_1 \oplus K_1) \oplus K_2. && (17) \end{aligned}$$

As $F_K^m(x)$ is a function independent of x_2, then, for any $x \in \{0,1\}^{2n}$, one has

$$F_K^m(x \oplus K) = F_K^m(x) \Longleftrightarrow F_K^m(x_1 \oplus K_1, *) = F_K^m(x_1, *). \tag{18}$$

Therefore, $F_K^m(x)$ is a periodic function with period K (or, more precisely, K_1).

Next, we need to verify the condition $\epsilon(F_K^m; K) \leq p_0 < 1$ for some constant p_0. For $t = (t_1, t_2) \in \{0,1\}^k \setminus \{0, K\}$ and any $m \in \{0,1\}^n$, we consider the following probability:

$$\begin{aligned} & Pr_x[F_K^m(x) = F_K^m(x \oplus t)] && (19)\\ =& Pr_x[E_x(m) \oplus E_{x\oplus K}(m) \oplus E_{x\oplus t}(m) \oplus E_{x\oplus t\oplus K}(m) = 0] && (20)\\ =& Pr_{x_1}[P(m \oplus x_1) \oplus P(m \oplus x_1 \oplus K_1) \oplus P(m \oplus x_1 \oplus t_1) && \\ & \oplus P(m \oplus x_1 \oplus K_1 \oplus t_1) = 0] && (21)\\ \overset{m=0}{=}& Pr_{x_1}[P(x_1) \oplus P(x_1 \oplus K_1) \oplus P(x_1 \oplus t_1) \oplus P(x_1 \oplus K_1 \oplus t_1) = 0] && (22)\\ =& \frac{|\{x_1 \mid P(x_1) \oplus P(x_1 \oplus K_1) \oplus P(x_1 \oplus t_1) \oplus P(x_1 \oplus K_1 \oplus t_1) = 0\}|}{2^n} && (23)\\ \leq& \frac{5}{6}, && (24) \end{aligned}$$

where the last inequality comes from the works of Xie and Yang [34].

Therefore, the condition $\epsilon(F_K^m; K) \leq \frac{5}{6} < 1$ is satisfied. According to Proposition 1, we can find K_1 with overwhelming probability by Simon's algorithm and then compute $K_2 = F_K^m(x) \oplus P(m \oplus x_1) \oplus P(m \oplus x_1 \oplus K_1)$. □

To summarize, the Even–Mansour cipher enjoys $n/2$-bit security in the classical setting [40], however, its secret keys can be recovered by $O(n)$ quantum queries in the quantum setting (the qCPA and qRKA models).

4.2. Application to SoEM

Let $K = (K_1, K_2)$ be a tuple of two n-bit keys. Let P_1 and P_2 be two public n-bit random permutations. Given a plaintext m, SoEM is defined as

$$E_K(m) = P_1(m \oplus K_1) \oplus K_1 \oplus P_2(m \oplus K_2) \oplus K_2. \tag{25}$$

Theorem 2. *There exists a quantum related-key attack against SoEM that recovers the secret keys K_1 and K_2 with $O(n)$ qubits and $O(n)$ quantum queries.*

Proof. For an arbitrary plaintext $m \in \{0,1\}^n$, let $x = (x_1, x_2) \in \{0,1\}^{2n}$, we construct a function

$$\begin{aligned} F_K^m(x) =& E_x(m) \oplus E_{x\oplus K}(m) && (26)\\ =& P_1(m \oplus x_1) \oplus P_2(m \oplus x_2) \oplus P_1(m \oplus x_1 \oplus K_1) \oplus P_2(m \oplus x_2 \oplus K_2) \\ & \oplus K_1 \oplus K_2. && (27) \end{aligned}$$

Then, for any $x \in \{0,1\}^{2n}$, it holds that

$$F_K^m(x \oplus K) = F_K^m(x). \tag{28}$$

Therefore, $F_K^m(x)$ is a periodic function with period $K = (K_1, K_2)$.

Next, we need to verify the condition $\epsilon(F_K^m; K) \leq p_0 < 1$ for some constant p_0. For $t = (t_1, t_2) \in \{0,1\}^{2n} \setminus \{0, K\}$ and any $m \in \{0,1\}^n$, we consider the following probability:

$$\begin{aligned} & Pr_x[F_K^m(x) = F_K^m(x \oplus t)] && (29)\\ =& Pr_x[E_x(m) \oplus E_{x\oplus K}(m) \oplus E_{x\oplus t}(m) \oplus E_{x\oplus t\oplus K}(m) = 0] && (30)\\ =& Pr_x[P_1(m \oplus x_1) \oplus P_1(m \oplus x_1 \oplus K_1) \oplus P_1(m \oplus x_1 \oplus t_1) \\ & \oplus P_1(m \oplus x_1 \oplus K_1 \oplus t_1) = P_2(m \oplus x_2) \oplus P_2(m \oplus x_2 \oplus K_2) \\ & \oplus P_2(m \oplus x_2 \oplus t_2) \oplus P_2(m \oplus x_2 \oplus K_2 \oplus t_2)] && (31)\\ \overset{m=0}{=}& Pr_x[P_1(x_1) \oplus P_1(x_1 \oplus K_1) \oplus P_1(x_1 \oplus t_1) \oplus P_1(x_1 \oplus K_1 \oplus t_1) \\ & = P_2(x_2) \oplus P_2(x_2 \oplus K_2) \oplus P_2(x_2 \oplus t_2) \oplus P_2(x_2 \oplus K_2 \oplus t_2)] && (32)\\ =& \sum_{a\in\{0,1\}^n} Pr_{x_1}[P_1(x_1) \oplus P_1(x_1 \oplus K_1) \oplus P_1(x_1 \oplus t_1) \oplus P_1(x_1 \oplus K_1 \oplus t_1) = a] \\ & \cdot Pr_{x_2}[P_2(x_2) \oplus P_2(x_2 \oplus K_2) \oplus P_2(x_2 \oplus t_2) \oplus P_2(x_2 \oplus K_2 \oplus t_2) = a] && (33)\\ \leq& \frac{5}{6} \times \frac{5}{6} + \frac{1}{6} \times \frac{1}{6} = \frac{13}{18}, && (34) \end{aligned}$$

where the penultimate equation comes from the fact that P_1 and P_2 are two random and independent permutations, and the last inequality is bounded by the extreme cases that a is equal to 0 and a is not equal to 0.

Therefore, the condition $\epsilon(F_K^m; K) \leq \frac{13}{18} < 1$ is satisfied. According to Proposition 1, we can find $K = (K_1, K_2)$ with overwhelming probability by Simon's algorithm, performing polynomial quantum queries and quantum bit memory. □

Note: this attack can be applied to all variants of SoEM, including SoEM1, SoEM21, and SoEM22. SoEM22 enjoys $2n/3$-bit security in the classical setting [41]. However, the keys of SoEM22 can be recovered with $O(n \cdot 2^{\frac{n}{2}})$ quantum queries by the Grover-meets-Simon algorithm under the qCPA model [6]. Theorem 2 shows that we can recover the keys of SoEM with $O(n)$ quantum queries and quantum bit memory under the qRKA model. The complexity comparison of the Even–Mansour cipher (EM for short), SoEM1, SoEM21, and SoEM22 in the different attack models is concluded in Table 2.

Table 2. Complexity comparison of the Even–Mansour cipher (EM for short), SoEM1, SoEM21, and SoEM22 in the classical setting (classical CPA and RKA models) and quantum setting (qCPA and qRKA models).

Scheme	Classical Setting		Quantum Setting	
	CPA	**RKA**	**qCPA**	**qRKA**
EM	$O(2^{n/2})$ [40]	$O(2^{n/2})$ [42]	$O(n)$ [18]	$O(n)$
SoEM1	$O(2^{n/2})$ [41]	-	$O(n)$ [6]	$O(n)$
SoEM21	$O(2^{n/2})$ [41]	-	$O(n)$ [6]	$O(n)$
SoEM22	$O(2^{2n/3})$ [41]	-	$O(n \cdot 2^{n/2})$ [6]	$O(n)$

Table 2 shows that: (1) In the quantum setting, the adversary has stronger attack capabilities and can break these cryptographic schemes in polynomial time, compared with the classical setting; (2) Cryptographic schemes that can be broken in polynomial time under the qCPA model can also be broken in polynomial time under the qRKA model, such as EM, SoEM1, and SoEM21; (3) Cryptographic schemes that cannot be broken in polynomial time under the qCPA model may be broken in polynomial time under the qRKA model, such as SoEM22.

5. Conclusions

This paper focuses on the quantum related-key attack model, proposes a strategy of quantum related-key attacks based on Simon's algorithm, and presents two applications. This work is of great significance. Quantum related-key attacks have more ability than quantum chosen-plaintext attacks. SoEM22 ensures enough security in the quantum chosen-plaintext attack model but is broken in the quantum related-key attack model. In other words, quantum related-key attacks may threaten existing cryptographic schemes that have proven security in the classical setting or even in the quantum chosen-plaintext attack model. One of the future goals is to cryptanalyze existing cryptographic schemes in the quantum related-key attack model. The classical related-key security of SoEM is still an open problem. Another future work direction is to research its classical related key security. This research is cutting-edge and targeted and has significant theoretical value and practical guidance for promoting the design of future quantum secure cryptographic schemes, advancing China's quantum computing technology, and standardizing post-quantum cryptographics.

Funding: This research was supported by National Natural Science Foundation of China (Grant Nos.: 61902195 and 62272238), Natural Science Fund for Colleges and Universities in Jiangsu Province (General Program, Grant No.: 19KJB520045), and NUPTSF (Grant No.: NY219131).

Data Availability Statement: The data used to support the findings of the study are available within the article.

Acknowledgments: I would like to express my sincere thanks to editors and the anonymous reviewers for the valuable comments and suggestions.

Conflicts of Interest: The author declares no conflict of interest.

References

1. Shor, P.W. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *SIAM J. Comput.* **1997**, *26*, 1484–1509. [CrossRef]
2. Grover, L.K. A Fast Quantum Mechanical Algorithm for Database Search. In Proceedings of the Twenty-Eighth Annual ACM Symposium on the Theory of Computing, Philadelphia, PA, USA, 22–24 May 1996; Miller, G.L., Ed.; ACM: New York, NY, USA, 1996; pp. 212–219. [CrossRef]
3. Simon, D.R. On the Power of Quantum Computation. *SIAM J. Comput.* **1997**, *26*, 1474–1483. [CrossRef]
4. Xie, H.; Yang, L. Using Bernstein-Vazirani algorithm to attack block ciphers. *Des. Codes Cryptogr.* **2019**, *87*, 1161–1182. [CrossRef]
5. Liu, W.; Gao, J. Quantum security of Grain-128/Grain-128a stream cipher against HHL algorithm. *Quantum Inf. Process.* **2021**, *20*, 343. [CrossRef]

6. Shinagawa, K.; Iwata, T. Quantum attacks on Sum of Even-Mansour pseudorandom functions. *Inf. Process. Lett.* **2022**, *173*, 106172. [CrossRef]
7. Zhou, B.; Yuan, Z. Quantum key-recovery attack on Feistel constructions: Bernstein-Vazirani meet Grover algorithm. *Quantum Inf. Process.* **2021**, *20*, 330. [CrossRef]
8. Wu, X.; Li, Q.; Li, Z.; Yang, D.; Yang, H.; Pan, W.; Perkowski, M.A.; Song, X. Circuit optimization of Grover quantum search algorithm. *Quantum Inf. Process.* **2023**, *22*, 69. [CrossRef]
9. Chakraborty, K.; Maitra, S. Application of Grover's algorithm to check non-resiliency of a Boolean function. *Cryptogr. Commun.* **2016**, *8*, 401–413. [CrossRef]
10. Bathe, B.N.; Anand, R.; Dutta, S. Evaluation of Grover's algorithm toward quantum cryptanalysis on ChaCha. *Quantum Inf. Process.* **2021**, *20*, 394. [CrossRef]
11. Bonnetain, X. Quantum Key-Recovery on Full AEZ. In Proceedings of the Selected Areas in Cryptography—SAC 2017—24th International Conference, Ottawa, ON, Canada, 16–18 August 2017; Adams, C., Camenisch, J., Eds.; Revised Selected Papers; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2017; Volume 10719, pp. 394–406. [CrossRef]
12. Bonnetain, X.; Naya-Plasencia, M.; Schrottenloher, A. Quantum Security Analysis of AES. *IACR Trans. Symmetric Cryptol.* **2019**, *2019*, 55–93. [CrossRef]
13. Cui, J.; Guo, J.; Ding, S. Applications of Simon's algorithm in quantum attacks on Feistel variants. *Quantum Inf. Process.* **2021**, *20*, 117. [CrossRef]
14. Dong, X.; Dong, B.; Wang, X. Quantum attacks on some feistel block ciphers. *Des. Codes Cryptogr.* **2020**, *88*, 1179–1203. [CrossRef]
15. Dong, X.; Wang, X. Quantum key-recovery attack on Feistel structures. *Sci. China Inf. Sci.* **2018**, *61*, 102501:1–102501:7. [CrossRef]
16. Guo, T.; Wang, P.; Hu, L.; Ye, D. Attacks on Beyond-Birthday-Bound MACs in the Quantum Setting. In Proceedings of the Post-Quantum Cryptography—12th International Workshop, PQCrypto 2021, Daejeon, Republic of Korea, 20–22 July 2021; Cheon, J.H., Tillich, J., Eds.; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2021; Volume 12841, pp. 421–441. [CrossRef]
17. Ito, G.; Hosoyamada, A.; Matsumoto, R.; Sasaki, Y.; Iwata, T. Quantum Chosen-Ciphertext Attacks Against Feistel Ciphers. In Proceedings of the Topics in Cryptology—CT-RSA 2019—The Cryptographers' Track at the RSA Conference 2019, San Francisco, CA, USA, 4–8 March 2019; Matsui, M., Ed.; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2019; Volume 11405, pp. 391–411. [CrossRef]
18. Kaplan, M.; Leurent, G.; Leverrier, A.; Naya-Plasencia, M. Breaking Symmetric Cryptosystems Using Quantum Period Finding. In Proceedings of the Advances in Cryptology—CRYPTO 2016—36th Annual International Cryptology Conference, Santa Barbara, CA, USA, 14–18 August 2016; Robshaw, M., Katz, J., Eds.; Proceedings, Part II; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2016; Volume 9815, pp. 207–237. [CrossRef]
19. Kuwakado, H.; Morii, M. Quantum distinguisher between the 3-round Feistel cipher and the random permutation. In Proceedings of the IEEE International Symposium on Information Theory, ISIT 2010, Austin, TX, USA, 13–18 June 2010; IEEE: Piscataway, NJ, USA, 2010; pp. 2682–2685. [CrossRef]
20. Liu, H.; Yang, L. Quantum key recovery attack on SIMON32/64. *Cybersecurity* **2021**, *4*, 23. [CrossRef]
21. Malviya, A.K.; Tiwari, N.; Chawla, M. Quantum cryptanalytic attacks of symmetric ciphers: A review. *Comput. Electr. Eng.* **2022**, *101*, 108122. [CrossRef]
22. Ni, B.; Ito, G.; Dong, X.; Iwata, T. Quantum Attacks Against Type-1 Generalized Feistel Ciphers and Applications to CAST-256. In Proceedings of the Progress in Cryptology—INDOCRYPT 2019—20th International Conference on Cryptology in India, Hyderabad, India, 15–18 December 2019; Hao, F., Ruj, S., Gupta, S.S., Eds.; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2019; Volume 11898, pp. 433–455. [CrossRef]
23. Xu, Y.; Liu, W.; Yu, W. Quantum forgery attacks on COPA, AES-COPA and marble authenticated encryption algorithms. *Quantum Inf. Process.* **2021**, *20*, 131. [CrossRef]
24. Kuwakado, H.; Morii, M. 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, 28–31 October 2012; Springer: Berlin/Heidelberg, Germany, 2012; pp. 312–316.
25. Dong, X.; Sun, S.; Shi, D.; Gao, F.; Wang, X.; Hu, L. Quantum Collision Attacks on AES-Like Hashing with Low Quantum Random Access Memories. In Proceedings of the Advances in Cryptology—ASIACRYPT 2020—26th International Conference on the Theory and Application of Cryptology and Information Security, Daejeon, Republic of Korea, 7–11 December 2020; Moriai, S., Wang, H., Eds.; Proceedings, Part II; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2020; Volume 12492, pp. 727–757. [CrossRef]
26. Mao, S.; Guo, T.; Wang, P.; Hu, L. Quantum Attacks on Lai-Massey Structure. In Proceedings of the Post-Quantum Cryptography—13th International Workshop, PQCrypto 2022, Virtual Event, 28–30 September 2022; Cheon, J.H., Johansson, T., Eds.; Lecture Notes in Computer Science; Springer: Cham, Switzerland, 2022; Volume 13512, pp. 205–229. [CrossRef]
27. Hao, X.; Zhang, F.; Wei, Y.; Zhou, Y. Quantum period finding based on the Bernstein-Vazirani algorithm. *Quantum Inf. Comput.* **2020**, *20*, 65–84. [CrossRef]
28. Harrow, A.W.; Hasidim, A.; Lloyd, S. Quantum algorithm for linear systems of equations. *Phys. Rev. Lett.* **2009**, *103*, 150502. [CrossRef]

29. Leander, G.; May, A. Grover Meets Simon—Quantumly Attacking the FX-construction. In Proceedings of the Advances in Cryptology—ASIACRYPT 2017—23rd International Conference on the Theory and Applications of Cryptology and Information Security, Hong Kong, China, 3–7 December 2017; Takagi, T., Peyrin, T., Eds.; Proceedings, Part II; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2017; Volume 10625, pp. 161–178. [CrossRef]
30. Guo, T.; Wang, P.; Hu, L.; Ye, D. Quantum Attacks on PRFs Based on Public Random Permutations. In Proceedings of the Progress in Cryptology—INDOCRYPT 2022—23rd International Conference on Cryptology in India, Kolkata, India, 11–14 December 2022; Isobe, T., Sarkar, S., Eds.; Lecture Notes in Computer Science; Springer: Cham, Switzerland, 2022; Volume 13774, pp. 566–591. [CrossRef]
31. Nan, J.; Hu, H.; Zhang, P.; Luo, Y. Quantum attacks against BBB secure PRFs or MACs built from public random permutations. *Quantum Inf. Process.* **2023**, *22*, 26. [CrossRef]
32. Rötteler, M.; Steinwandt, R. A note on quantum related-key attacks. *Inf. Process. Lett.* **2015**, *115*, 40–44. [CrossRef]
33. Hosoyamada, A.; Aoki, K. On Quantum Related-Key Attacks on Iterated Even-Mansour Ciphers. *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.* **2019**, *102-A*, 27–34. [CrossRef]
34. Xie, H.; Yang, L. A quantum related-key attack based on the Bernstein-Vazirani algorithm. *Quantum Inf. Process.* **2020**, *19*, 240. [CrossRef]
35. Sun, H.; Wei, C.; Cai, B.; Qin, S.; Wen, Q.; Gao, F. Improved BV-based quantum attack on block ciphers. *Quantum Inf. Process.* **2023**, *22*, 9. [CrossRef]
36. Tao, B.; Wu, H. Improving the Biclique Cryptanalysis of AES. In Proceedings of the Information Security and Privacy—20th Australasian Conference, ACISP 2015, Brisbane, QLD, Australia, 29 June–1 July 2015; Foo, E., Stebila, D., Eds.; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2015; Volume 9144, pp. 39–56. [CrossRef]
37. Junod, P. On the Complexity of Matsui's Attack. In Proceedings of the Selected Areas in Cryptography, 8th Annual International Workshop, SAC 2001, Toronto, ON, Canada, 16–17 August 2001; Vaudenay, S., Youssef, A.M., Eds.; Revised Papers; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2001; Volume 2259, pp. 199–211. [CrossRef]
38. Sereshgi, M.H.F.; Dakhilalian, M.; Shakiba, M. Biclique cryptanalysis of MIBS-80 and PRESENT-80 block ciphers. *Secur. Commun. Netw.* **2016**, *9*, 27–33. [CrossRef]
39. Chen, H.; Wang, X. Improved Linear Hull Attack on Round-Reduced Simon with Dynamic Key-Guessing Techniques. In Proceedings of the Fast Software Encryption—23rd International Conference, FSE 2016, Bochum, Germany, 20–23 March 2016; Peyrin, T., Ed.; Revised Selected Papers; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2016; Volume 9783, pp. 428–449. [CrossRef]
40. Even, S.; Mansour, Y. A Construction of a Cipher from a Single Pseudorandom Permutation. *J. Cryptol.* **1997**, *10*, 151–162. [CrossRef]
41. Chen, Y.L.; Lambooij, E.; Mennink, B. How to Build Pseudorandom Functions from Public Random Permutations. In Proceedings of the Advances in Cryptology—CRYPTO 2019—39th Annual International Cryptology Conference, Santa Barbara, CA, USA, 18–22 August 2019; Boldyreva, A., Micciancio, D., Eds.; Proceedings, Part I; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2019; Volume 11692, pp. 266–293. [CrossRef]
42. Farshim, P.; Procter, G. The Related-Key Security of Iterated Even-Mansour Ciphers. In Proceedings of the Fast Software Encryption—22nd International Workshop, FSE 2015, Istanbul, Turkey, 8–11 March 2015; Leander, G., Ed.; Revised Selected Papers; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2015; Volume 9054, pp. 342–363. [CrossRef]