entropy

MDPI

Article

Quantum Attacks on Sum of Even–Mansour Construction with Linear Key Schedules

Ping Zhang

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

Abstract: Shinagawa and Iwata are considered quantum security for the sum of Even–Mansour (SoEM) construction and provided quantum key recovery attacks by Simon's algorithm and Grover's algorithm. Furthermore, quantum key recovery attacks are also presented for natural generalizations of SoEM. For some variants of SoEM, they found that their quantum attacks are not obvious and left it as an open problem to discuss the security of such constructions. This paper focuses on this open problem and presents a positive response. We provide quantum key recovery attacks against such constructions by quantum algorithms. For natural generalizations of SoEM with linear key schedules, we also present similar quantum key recovery attacks by quantum algorithms (Simon's algorithm, Grover's algorithm, and Grover-meet-Simon algorithm).

Keywords: quantum attacks; sum of Even–Mansour construction; linear key schedule; quantum algorithms

Citation: Zhang, P. Quantum Attacks on Sum of Even–Mansour Construction with Linear Key Schedules. *Entropy* **2022**, *24*, 153. https://doi.org/10.3390/e24020153

Academic Editors: Durdu Guney and David Petrosyan

Received: 27 December 2021
Accepted: 18 January 2022
Published: 20 January 2022

1. Introduction

Since 1981, when Richard Feynman, winner of the Nobel Prize in Physics, proposed the concept of a quantum computer, the research of the quantum computer has deeply influenced the scientific research circle. Classical computers are often attacked by malicious viruses that crash the computer and can lead to personal information being stolen. However, in quantum computers, these problems will not exist because of the quantum no-cloning principle and Heisenberg's uncertainty principle. Quantum computers have good properties, such as fast running speed, a strong information processing ability, and powerful parallel computing capability. Therefore, quantum computers have great applications in cryptanalysis and other fields. Quantum algorithms are the most important software components of quantum computers to realize quantum computation.

The importance of information security is self-evident. In 2021, there were multiple breaches of sensitive information and cyber attacks, causing a large number of property losses and even endangering personal security and social stability. Modern cryptography is one of the core technologies to protect information security.

The design and analysis of cryptographic schemes that resist quantum computing have become increasingly important. Among them, the public key cryptographic scheme is the typical representative. Difficult mathematical problems of public key cryptography can be solved by efficient quantum algorithms. Therefore, public key cryptographic schemes, such as RSA and ECC, are insecure in the quantum scenario [1]. While, for symmetric cryptographic schemes (such as AES and IDEA), the influence is limited and Grover's algorithm [2] has been regarded for a long time as the best method to search for the secret key. It is only in recent years that quantum analyses of symmetric cryptographic schemes have made some progress.

Simon's algorithm [3] is a vital quantum algorithm for the quantum analyses of symmetric cryptographic schemes. Its goal is to efficiently find a period of a period function. It was first utilized to the security analyses of the 3-round Feistel cipher [4] and then extended to the Even–Mansour cipher [5,6], Feistel and its variants [7–11], and the

Luby–Rackoff construction [12]. Grover-meet-Simon algorithm [13] was first introduced by Leander and May, and combined Simon's algorithm and Grover's algorithm to achieve the key recovery attack against FX-construction. Currently, Simon's algorithm, Grover's algorithm, and Grover-meet-Simon algorithm have been extended to the Sum of Even–Mansour construction [14], encryption schemes [15–20], hash schemes [21–23], message authentication codes (MACs) [18,24], and authenticated encryption schemes [18,25,26]. There exist other quantum algorithms (such as HHL algorithm and BTH algorithm) and relevant quantum cryptanalysis. We will not go into the details here.

Problem Statement. The sum of Even–Mansour (SoEM) construction [14] is built by the exclusive or (XOR) of two instances of Even–Mansour cipher. According to whether the keys or permutations used in the two instances are equal, SoEM is divided into three variants: SoEM1 for the case where permutations used in the two instances are identical, SoEM21 for the case where permutations used in the two instances are independent but keys used in the two instances are identical, and SoEM22 for the case where permutations used in the two instances are independent and keys used in the two instances are independent. They are pseudorandom functions designed by random permutations and designers give security results in the classical scenario.

Shinagawa and Iwata considered the quantum security for SoEM construction, providing quantum key recovery attacks by Simon's algorithm and Grover's algorithm, and applied the similar quantum key recovery attacks to natural generalizations of SoEM in [27]. For some variants of SoEM, they found that their quantum attacks are not obvious and left it as an open problem to consider the security of such constructions.

Our Contributions. This paper focuses on the open problem and provides quantum key recovery attacks against such constructions by quantum algorithms. First, we consider a variant of SoEM21 given in Shinagawa and Iwata, which is described as:

$$C = SoEM21_K^{P_1,P_2}(M) = P_1(M \oplus K) \oplus K \oplus P_2(M \oplus 2 \cdot K) \oplus 2 \cdot K,$$

where P_1 and P_2 are two public n-bit random permutations, K is an n-bit key, M is a plaintext, and C is the corresponding ciphertext. Here SoEM21 is generated by the XOR-sum of two instances of Even–Mansour cipher with simple key schedules. We prove that this variant is insecure under the quantum scenario and recover its key by quantum algorithms.

Then we consider a generalized construction of SoEM21 with linear key schedules (a linear key schedule means that it is linear with respect to the key) and rename it as SoEM21L, which is described as:

$$C = SoEM21L_K^{P_1,P_2}(M) = P_1(M \oplus a \cdot K) \oplus P_2(M \oplus b \cdot K) \oplus c \cdot K,$$

where a, b, c are three integers and $(a, b, c) \neq (0, 0, 0)$. We also achieve a quantum key recovery attack against SoEM21L by quantum algorithms.

Finally, we consider natural generalizations of SoEM with linear key schedules and present similar quantum key recovery attacks by quantum algorithms (Simon's algorithm, Grover's algorithm, and Grover-meet-Simon algorithm).

Organizations of This Paper. Notations and some preliminaries are presented in Section 2. Quantum algorithms are shown in Section 3. In Section 4, we describe quantum key recovery attacks for SoEM21 and SoEM21L. In Section 5, we present natural generalizations of SoEM with linear key schedules and their quantum key recovery attacks. Finally, we present a conclusion in Section 6.

2. Preliminaries

Notations. Given an integer $n \geq 1$, let $\{0,1\}^n$ be a set of all strings whose bit-lengths are n, and $Perm(n)$ be a set of all permutations over $\{0,1\}^n$. For any two finite strings $x \in \{0,1\}^n$ and $y \in \{0,1\}^n$, let $x \oplus y$ stand for their bit-wise XOR.

Finite Field. The finite field $GF(2^n)$ can be viewed as the set $\{0,1\}^n$ and $GF(2^n) = GF(2)/(f(x))$, where $f(x)$ is an irreducible polynomial of degree n over $GF(2)$. For any integer $0 \leq a \leq 2^n - 1$, it can be seen as an n-bit string over $GF(2^n)$, i.e., $a = a_{n-1} \cdots a_1 a_0 \in \{0,1\}^n$, where $a_i \in \{0,1\}$ for $0 \leq i \leq n-1$. It also corresponds to a polynomial with a degree of at most $n-1$ over $\{0,1\}$, i.e., $a(x) = a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$. For example, 2 (10) corresponds to x, 3 (11) corresponds to $x+1$, and 7 (111) corresponds to $x^2 + x + 1$. The addition over $GF(2^n)$ can be defined by the addition of polynomials over $\{0,1\}$ or the bit-wise XOR over $\{0,1\}^n$ and the multiplication over $GF(2^n)$ is defined by the polynomial multiplication over $\{0,1\}$ reduced modulo $f(x)$, i.e., for any $a, b \in GF(2^n)$, then $a + b = a(x) + b(x)\ mod\ 2 = a \oplus b$ and $a \cdot b = a(x) \cdot b(x) \bmod f(x)$. Therefore, if $n = 128$ and $f(x) = x^{128} + x^7 + x^2 + x + 1$, then:

$$2 \cdot a = x \cdot a(x) \mod f(x), 3 \cdot a = (x+1) \cdot a(x) \mod f(x) = 2 \cdot a \oplus a,$$
$$4 \cdot a = x^2 \cdot a(x) \mod f(x) = 2^2 \cdot a, 5 \cdot a = (x^2+1) \cdot a(x) \mod f(x) = 2^2 \cdot a \oplus a,$$
$$6 \cdot a = (x^2 + x) \cdot a(x) \mod f(x) = 2^2 \cdot a \oplus 2 \cdot a,$$
$$7 \cdot a = (x^2 + x + 1) \cdot a(x) \mod f(x) = 2^2 \cdot a \oplus 2 \cdot a \oplus a,$$
$$8 \cdot a = x^3 \cdot a(x) \mod f(x) = 2^3 \cdot a, \ldots$$
$$2^2 \cdot a = 2 \cdot 2 \cdot a = x^2 \cdot a(x) \mod f(x) = 4 \cdot a, 2 \cdot 3 \cdot a = x(x+1) \cdot a(x) \mod f(x) = 6 \cdot a, \ldots$$
$$3^2 \cdot a = (x+1)^2 \cdot a(x) \mod f(x) = (x^2+1) \cdot a(x) \mod f(x) = 5 \cdot a, \ldots$$

Sum of Even–Mansour Construction (SoEM) [14]. SoEM introduced by Chen et al. is a provably secure pseudorandom function in the classical security model. It is built by the XOR of two distinct instances of the Even–Mansour cipher. The specification of SoEM is shown as follows. Let P_1 and P_2 be two public n-bit permutations. Let K_1 and K_2 be two n-bit keys. For a plaintext M and the corresponding ciphertext C, SoEM: $\{0,1\}^{2n} \times \{0,1\}^n \to \{0,1\}^n$ can be expressed as:

$$C = SoEM^{P_1,P_2}_{K_1,K_2}(M) = P_1(M \oplus K_1) \oplus K_1 \oplus P_2(M \oplus K_2) \oplus K_2.$$

SoEM can be divided into three variants, SoEM1, SoEM21, and SoEM22, according to the number of underlying permutations and keys. SoEM1, SoEM21, and SoEM22 are respectively shown as follows.

SoEM1: The permutations used in the two instances are identical (two instances utilize the same permutation), i.e., $P_1 = P_2 = P$. Then SoEM1: $\{0,1\}^{2n} \times \{0,1\}^n \to \{0,1\}^n$ can be expressed as:

$$C = SoEM1^{P}_{K_1,K_2}(M) = P(M \oplus K_1) \oplus K_1 \oplus P(M \oplus K_2) \oplus K_2.$$

Note that, in this case, it makes no sense to subdivide again as the same key will make SoEM1 zero.

SoEM21: The permutations used in the two instances are independent but keys used in the two instances are identical, i.e., $K_1 = K_2 = K$. Then SoEM21: $\{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ can be expressed as:

$$C = SoEM21^{P_1,P_2}_{K}(M) = P_1(M \oplus K) \oplus P_2(M \oplus K) \oplus K.$$

SoEM22: The permutations used in the two instances are independent and keys used in the two instances are independent, i.e., SoEM22 is SoEM. Then SoEM22: $\{0,1\}^{2n} \times \{0,1\}^n \to \{0,1\}^n$ can be expressed as:

$$C = SoEM22^{P_1,P_2}_{K_1,K_2}(M) = P_1(M \oplus K_1) \oplus K_1 \oplus P_2(M \oplus K_2) \oplus K_2.$$

3. Quantum Algorithms

This section presents brief descriptions of Simon's algorithm [3], Grover's algorithm [2], and the Grover-meet-Simon algorithm [13].

3.1. Simon's Algorithm

Simon's algorithm [3] is an algorithm that specializes in solving period finding problem efficiently. The period finding problem is called Simon's problem which is described as follows:

Period Finding Problem. Given a boolean function $f : \{0,1\}^n \to \{0,1\}^n$, assume that there exists $s \in \{0,1\}^n \setminus \{0^n\}$, for any $x \neq y \in \{0,1\}^n$, such that $f(x) = f(y) \Leftrightarrow x \oplus y = s$. The goal is to find the period s.

In the classical algorithm, people solve this problem by searching and finding collisions. The optimal time complexity is $O(2^{n/2})$. While, in the quantum algorithm, by Simon's algorithm, it can be solved in a polynomial time of n (i.e., $O(n)$ quantum query complexity and $O(n)$ qubits memory complexity). The details of Simon's algorithm are not introduced here. We just need to know that the period finding problem can be solved by Simon's algorithm with $O(n)$ quantum query complexity and $O(n)$ qubits memory complexity.

3.2. Grover's Algorithm

Grover's algorithm [2] is a quantum search algorithm that specializes in solving a search problem efficiently. The search problem is described as follows:

The Search Problem. Given a function $g : \{0,1\}^n \to \{0,1\}$, if $x \in \{0,1\}^n$ is a solution of the search problem, then $g(x) = 1$, otherwise $g(x) = 0$. The goal is to find the solution x.

In the classical algorithm, people solve this problem by searching this solution. The time complexity is $O(2^n)$. While, in the quantum algorithm, by Grover's algorithm, it can be solved in $O(2^{n/2})$ quantum query complexity and $O(n)$ qubits memory complexity. Grover's search algorithm improves search complexity exponentially. The details of Grover's algorithm are not introduced here.

3.3. Grover-Meet-Simon Algorithm

The Grover-meet-Simon algorithm [13] is a quantum asymmetric search of a period algorithm. It combined Grover's search algorithm with Simon's algorithm to recover keys. The asymmetric search of a period problem is described as follows:

Grover-meet-Simon Problem. Let m, n, l be three positive integers, $U \subseteq \{0,1\}^m$ be a finite set, and $f : \{0,1\}^m \times \{0,1\}^n \to \{0,1\}^l$ be a function which meets that 1) if $u \in U$, then $f(u,\cdot)$ is a period function with period s_u; 2) if $u \notin U$, then $f(u,\cdot)$ is an aperiodic function. The goal is to find the search-period pair (u, s_u).

The idea of settling the Grover-meet-Simon problem is to first search $u \in U$ by Grover's algorithm and then check whether $f(u,\cdot)$ is a period function or not by Simon's algorithm. If $f(u,\cdot)$ is a period function with period s_u, then (u, s_u) is what we need. Therefore, in the quantum algorithm, the Grover-meet-Simon problem can be solved in $O(n) \times O(2^{n/2}) = O(n \cdot 2^{n/2})$ quantum query complexity and $O(n) \times O(n) = O(n^2)$ qubits memory complexity. The details of the Grover-meet-Simon algorithm are not introduced here.

4. Quantum Attacks against SoEM with Linear Key Schedules

4.1. Quantum Attacks against SoEM21

Shinagawa and Iwata left it as an open problem for the analysis of the security of the following construction [27]:

$$C = SoEM21_K^{P_1,P_2}(M) = P_1(M \oplus K) \oplus K \oplus P_2(M \oplus 2 \cdot K) \oplus 2 \cdot K.$$

In particular, if $P_1 = P_2 = P$, then SoEM21 degrades to SoEM11, i.e.,

$$C = SoEM11_K^P(M) = P(M \oplus K) \oplus K \oplus P(M \oplus 2 \cdot K) \oplus 2 \cdot K.$$

For the above SoEM11 and SoEM21 constructions, we present quantum attacks in Theorems 1 and 2.

Theorem 1. *There exists a quantum key recovery attack against SoEM11 in $O(n)$ quantum query complexity and $O(n)$ qubits memory complexity.*

Proof. Our proof utilizes Simon's algorithm. By careful observation of SoEM11, we find that SoEM11 itself is a period function with period $3 \cdot K$. To be specific, let $f : \{0,1\}^n \to \{0,1\}^n$ be a function, which is defined as:

$$f(x) = SoEM11_K^P(x) = P(x \oplus K) \oplus P(x \oplus 2 \cdot K) \oplus 3 \cdot K.$$

It follows that,

$$\begin{aligned} f(x \oplus 3 \cdot K) &= P(x \oplus 3 \cdot K \oplus K) \oplus P(x \oplus 3 \cdot K \oplus 2 \cdot K) \oplus 3 \cdot K \\ &= P(x \oplus 2 \cdot K) \oplus P(x \oplus K) \oplus 3 \cdot K = f(x), \end{aligned}$$

where $K \oplus 2 \cdot K = 3 \cdot K$, $K \oplus 3 \cdot K = 2 \cdot K$, and $3 \cdot K \oplus 2 \cdot K = K$.

Therefore, f is a period function with period $3 \cdot K$. Then, $3 \cdot K$ can be derived in $O(n)$ quantum queries and $O(n)$ qubits memory complexity to f by Simon's algorithm. It follows that, $K = 3 \cdot K/3$ can be recovered. □

Theorem 2. *There exists a quantum key recovery attack against SoEM21 in $O(2^{n/2})$ quantum query complexity and $O(n)$ qubits memory complexity.*

Proof. Our proof utilizes Grover's algorithm. First, we construct a new function $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ as:

$$\begin{aligned} f(k,x) &= SoEM21_K^{P_1,P_2}(x) \oplus P_1(x) \oplus P_2(x \oplus k) \\ &= P_1(x \oplus K) \oplus K \oplus P_2(x \oplus 2 \cdot K) \oplus 2 \cdot K \oplus P_1(x) \oplus P_2(x \oplus k) \\ &= P_1(x \oplus K) \oplus P_1(x) \oplus P_2(x \oplus 2 \cdot K) \oplus P_2(x \oplus k) \oplus 3 \cdot K. \end{aligned}$$

By careful observation, we find that if $k = 3 \cdot K$, then $f(3 \cdot K, \cdot)$ is a period function with period K, as:

$$\begin{aligned} f(3 \cdot K, x \oplus K) =& P_1(x \oplus K \oplus K) \oplus P_1(x \oplus K) \\ & \oplus P_2(x \oplus K \oplus 2 \cdot K) \oplus P_2(x \oplus K \oplus 3 \cdot K) \oplus 3 \cdot K \\ =& P_1(x) \oplus P_1(x \oplus K) \oplus P_2(x \oplus 3 \cdot K) \oplus P_2(x \oplus 2 \cdot K) \oplus 3 \cdot K \\ =& f(3 \cdot K, x). \end{aligned}$$

Therefore, we first search $k = 3 \cdot K$ by Grover's algorithm and then verify whether $f(3 \cdot K, \cdot)$ is a period function with a period $K = 3 \cdot K/3$ or not. Therefore, K can be derived in a $O(2^{n/2})$ quantum queries to f and $O(n)$ qubits memory complexity by Grover's algorithm. □

4.2. Quantum Attacks against SoEM with Linear Key Schedules

We consider a generalized construction of SoEM21 with linear key schedules and rename it as SoEM21L, i.e.,

$$C = SoEM21L_K^{P_1,P_2}(M) = P_1(M \oplus a \cdot K) \oplus P_2(M \oplus b \cdot K) \oplus c \cdot K,$$

where a, b, c are three integers and $(a, b, c) \neq (0, 0, 0)$.

In particular, if $P_1 = P_2 = P$ and $a \neq b$, then SoEM21L degrades to SoEM11L, i.e.,

$$C = SoEM11L_K^P(M) = P(M \oplus a \cdot K) \oplus K \oplus P(M \oplus b \cdot K) \oplus c \cdot K.$$

For the above SoEM21L and SoEM11L constructions, we present quantum attacks in Theorems 3 and 4.

Theorem 3. *There exists a quantum key recovery attack against SoEM11L in $O(n)$ quantum query complexity and $O(n)$ qubits memory complexity.*

Proof. Our proof utilizes Simon's algorithm. By careful observation of SoEM11L, we find that SoEM11L itself is a period function with period $(a \oplus b) \cdot K$. To be specific, let $f : \{0,1\}^n \to \{0,1\}^n$ be a function, which is defined as:

$$f(x) = SoEM11L_K^P(x) = P(x \oplus a \cdot K) \oplus P(x \oplus b \cdot K) \oplus c \cdot K.$$

It follows that,

$$\begin{aligned} f(x \oplus (a \oplus b) \cdot K) &= P(x \oplus (a \oplus b) \cdot K \oplus a \cdot K) \oplus P(x \oplus (a \oplus b) \cdot b \oplus 2 \cdot K) \oplus c \cdot K \\ &= P(x \oplus b \cdot K) \oplus P(x \oplus a \cdot K) \oplus c \cdot K = f(x), \end{aligned}$$

where $a \cdot K \oplus b \cdot K = (a \oplus b) \cdot K$, $a \cdot K \oplus (a \oplus b) \cdot K = b \cdot K$, and $(a \oplus b) \cdot K \oplus b \cdot K = a \cdot K$.

Therefore, f is a period function with period $(a \oplus b) \cdot K$. Then, $(a \oplus b) \cdot K$ can be derived in polynomial time of n ($O(n)$ qubits and $O(n)$ quantum oracle queries to f) by Simon's algorithm. It follows that, $K = (a \oplus b) \cdot K / (a \oplus b)$ can be recovered. □

Theorem 4. *There exists a quantum key recovery attack against SoEM21L in $O(2^{n/2})$ quantum query complexity and $O(n)$ qubits memory complexity.*

Proof. Our proof utilizes Grover's algorithm. We construct a new function $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ as:

$$\begin{aligned} f(k, x) &= SoEM21L_K^{P_1,P_2}(x) \oplus P_1(x) \oplus P_2(x \oplus k) \\ &= P_1(x \oplus a \cdot K) \oplus P_2(x \oplus b \cdot K) \oplus P_1(x) \oplus P_2(x \oplus k) \oplus c \cdot K. \end{aligned}$$

By careful observation, we find that if $k = (a \oplus b) \cdot K$, then f is a period function with period $a \cdot K$, i.e.,

$$\begin{aligned} f((a \oplus b) \cdot K, x \oplus a \cdot K) =& P_1(x \oplus a \cdot K \oplus a \cdot K) \oplus P_2(x \oplus a \cdot K \oplus b \cdot K) \\ & \oplus P_1(x \oplus a \cdot K) \oplus P_2(x \oplus a \cdot K \oplus (a \oplus b) \cdot K) \oplus c \cdot K \\ =& P_1(x) \oplus P_2(x \oplus (a \oplus b) \cdot K) \\ & \oplus P_1(x \oplus a \cdot K) \oplus P_2(x \oplus b \cdot K) \oplus c \cdot K \\ =& f((a \oplus b) \cdot K, x). \end{aligned}$$

Therefore, for any SoEM21L, we first search $k = (a \oplus b) \cdot K$ by Grover's algorithm and then verify whether $f((a \oplus b) \cdot K, \cdot)$ is a period function with a period $a \cdot K$ or not. It follows that K can be derived in a $O(2^{n/2})$ quantum queries to f and $O(n)$ qubits memory complexity by Grover's algorithm. □

5. Generalizations and Attacks

Inspired by linear key schedules, this section considers natural generalizations of SoEM1, SoEM21, and SoEM22, and presents quantum key recovery attacks against these constructions.

5.1. Generalizations

We define SoEM1sL, SoEMs1L, and SoEMssL as natural generalizations of SoEM1, SoEM21, and SoEM22 with linear key schedules, respectively. The constructions of them are respectively shown as follows.

Let $s \geq 2$ and $(a_1, a_2, \cdots, a_s) \neq (0, 0, \cdots, 0)$ be integers. Let $P_1, \cdots, P_s$ be s public n-bit permutations, $K_1, \cdots, K_s$ be s n-bit keys, M be a plaintext, and C be a ciphertext, then SoEMssL (SoEM with s permutations and s linear keys) is defined as:

$$\begin{aligned} C &= SoEMssL^{P_1,\cdots,P_s}_{K_1,\cdots,K_s}(M) \\ &= P_1(M \oplus a_1 \cdot K_1) \oplus a_1 \cdot K_1 \oplus \cdots \oplus P_s(M \oplus a_s \cdot K_s) \oplus a_s \cdot K_s. \end{aligned}$$

If $P_1 = \cdots = P_s = P$, then SoEMssL will degrade to SoEM1sL which is defined as:

$$\begin{aligned} C &= SoEM1sL^{P}_{K_1,\cdots,K_s}(M) \\ &= P(M \oplus a_1 \cdot K_1) \oplus a_1 \cdot K_1 \oplus \cdots \oplus P(M \oplus a_s \cdot K_s) \oplus a_s \cdot K_s. \end{aligned}$$

If $K_1 = \cdots = K_s = K$, then SoEMssL will degrade to SoEMs1L, which is defined as:

$$\begin{aligned} C &= SoEMs1L^{P_1,\cdots,P_s}_{K}(M) \\ &= P_1(M \oplus a_1 \cdot K) \oplus \cdots \oplus P_s(M \oplus a_s \cdot K) \oplus a_{s+1} \cdot K, \end{aligned}$$

where a_{s+1} is an arbitrary integer.

If $P_1 = \cdots = P_s = P$, $K_1 = \cdots = K_s = K$, and $a_1 \neq a_2 \neq \cdots \neq a_s$, then SoEMssL will degrade to SoEM11L, which is defined as:

$$\begin{aligned} C &= SoEM11L^{P}_{K}(M) \\ &= P(M \oplus a_1 \cdot K) \oplus \cdots \oplus P(M \oplus a_s \cdot K) \oplus a_{s+1} \cdot K, \end{aligned}$$

where a_{s+1} is an arbitrary integer.

5.2. Quantum Key Recovery Attacks

Theorem 5. *There exists a quantum key recovery attack against SoEM1sL that obtains the secret key $K_1, \cdots, K_s$ in $O(n^2 + sn)$ qubits and $O(sn \cdot 2^{(s-1)n/2})$ quantum queries.*

Proof. Our attack is based on the Grover-meet-Simon algorithm and is similar with the attack against SoEMss [27]. We consider two functions $g : \{0,1\}^{(s-1)n} \times \{0,1\}^n \to \{0,1\}^n$ and $f : \{0,1\}^{(s-1)n} \times \{0,1\}^n \to \{0,1\}^n$, which are defined as follows.

$$\begin{aligned} g(k_2, \cdots, k_s, x) =& P(x) \oplus P(x \oplus a_2 \cdot k_2) \oplus \cdots \oplus P(x \oplus a_s \cdot k_s), \\ f(k_2, \cdots, k_s, x) =& SoEM1sL^{P}_{K_1,\cdots,K_s}(x) \oplus g(k_2, \cdots, k_s, x) \\ =& P(x \oplus a_1 \cdot K_1) \oplus a_1 \cdot K_1 \oplus \cdots \oplus P(x \oplus a_s \cdot K_s) \oplus a_s \cdot K_s \\ & \oplus P(x) \oplus P(x \oplus a_2 \cdot k_2) \oplus \cdots \oplus P(x \oplus a_s \cdot k_s). \end{aligned}$$

If $(k_2, \cdots, k_s) = (K_2, \cdots, K_s)$, then $f(K_2, \cdots, K_s, x) = P(x \oplus a_1 \cdot K_1) \oplus a_1 \cdot K_1 \oplus \cdots \oplus a_s \cdot K_s \oplus P(x)$ and $f(K_2, \cdots, K_s, x)$ is a period function with period $a_1 \cdot K_1$. Therefore, by Simon's algorithm, we can obtain the period $a_1 \cdot K_1$. It follows that we recover $K_1 = a_1 \cdot K_1 / a_1$.

Then we utilize Grover's algorithm to recover $K_2, \cdots, K_s$. Similar with FX construction and SoEM22, we utilize the Grover-meet-Simon algorithm to find the value of $(k_2, \cdots, k_s)$ that makes $f(k_2, \cdots, k_s, x)$ period. If we find a period function, then, at this point, $(k_2, \cdots, k_s)$ is the secret keys $(K_2, \cdots, K_s)$ that we need to recover and the period is $a_1 \cdot K_1$.

Therefore, for any SoEM1sL, we can construct two functions f and g. By the Grover-meet-Simon algorithm, $(K_1, K_2, \cdots, K_s)$ can be derived in $O(n^2 + sn)$ qubits and $O(sn \cdot 2^{(s-1)n/2})$ quantum oracle queries to f and g. □

Theorem 6. *There exists a quantum key recovery attack against SoEMs1L that obtains the secret key K in $O(n)$ qubits and $O(2^{n/2})$ quantum oracle queries.*

Proof. Our attack is based on Grover's algorithm and is a generalization of the quantum attack against SoEM21L. We consider a function $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$, which is defined as follows.

$$\begin{aligned} f(k,x) =& SoEMs1L_K^{P_1,\cdots,P_s}(x) \oplus P_1(x) \oplus P_2(x \oplus a_2 \cdot k) \oplus \cdots \oplus P_s(x \oplus a_s \cdot k) \\ =& P_1(x \oplus a_1 \cdot K) \oplus \cdots \oplus P_s(x \oplus a_s \cdot K) \oplus a_{s+1} \cdot K \\ & \oplus P_1(x) \oplus P_2(x \oplus a_2 \cdot k) \oplus \cdots \oplus P_s(x \oplus a_s \cdot k). \end{aligned}$$

By careful observation, we find that if $k = K$, then f is a period function with period $a_1 \cdot K$, i.e., $f(K, x \oplus a_1 \cdot K) = f(K, x)$.

Therefore, for any SoEMs1L, we first search $k = K$ by Grover's algorithm and then verify whether $f(K, \cdot)$ is a period function with a period $a_1 \cdot K$ or not. It follows that K can be derived in the $O(2^{n/2})$ quantum queries to f and $O(n)$ qubits memory complexity by Grover's algorithm. □

Theorem 7. *There exists a quantum key recovery attack against SoEMssL that recovers the secret key $K_1, \cdots, K_s$ in $O(n^2 + sn)$ qubits and $O(sn \cdot 2^{(s-1)n/2})$ quantum queries.*

Proof. Our attack is based on the Grover-meet-Simon algorithm and is similar with the attack against SoEMss [27]. We consider two functions $g : \{0,1\}^{(s-1)n} \times \{0,1\}^n \to \{0,1\}^n$ and $f : \{0,1\}^{(s-1)n} \times \{0,1\}^n \to \{0,1\}^n$, which are defined as follows:

$$\begin{aligned} g(k_2, \cdots, k_s, x) =& P_1(x) \oplus P_2(x \oplus a_2 \cdot k_2) \oplus \cdots \oplus P_s(x \oplus a_s \cdot k_s), \\ f(k_2, \cdots, k_s, x) =& SoEM1sL_{K_1,\cdots,K_s}^{P_1,\cdots,P_s}(x) \oplus g(K_2, \cdots, K_s, x) \\ =& P_1(x \oplus a_1 \cdot K_1) \oplus a_1 \cdot K_1 \oplus \cdots \oplus P_s(x \oplus a_s \cdot K_s) \oplus a_s \cdot K_s \\ & \oplus P_1(x) \oplus P_2(x \oplus a_2 \cdot k_2) \oplus \cdots \oplus P_s(x \oplus a_s \cdot k_s). \end{aligned}$$

If $(k_2, \cdots, k_s) = (K_2, \cdots, K_s)$, then $f(K_2, \cdots, K_s, x) = P_1(x \oplus a_1 \cdot K_1) \oplus a_1 \cdot K_1 \oplus \cdots \oplus a_s \cdot K_s \oplus P_1(x)$ and $f(K_2, \cdots, K_s, x)$ is a period function with period $a_1 \cdot K_1$. Therefore, by Simon's algorithm, we can obtain the period $a_1 \cdot K_1$. It follows that we recover $K_1 = a_1 \cdot K_1 / a_1$.

Then we utilize Grover's algorithm to recover $K_2, \cdots, K_s$. Similar with FX construction and SoEM22, we utilize the Grover-meet-Simon algorithm to find the value of $(k_2, \cdots, k_s)$ that makes $f(k_2, \cdots, k_s, x)$ period. If we find a period function, then $(k_2, \cdots, k_s)$ is the secret keys $(K_2, \cdots, K_s)$ and the period is $a_1 \cdot K_1$.

Therefore, for any SoEMssL, we can construct two functions f and g. By the Grover-meet-Simon algorithm, $(K_1, K_2, \cdots, K_s)$ can be derived in $O(n^2 + sn)$ qubits and $O(sn \cdot 2^{(s-1)n/2})$ quantum oracle queries to f and g. □

6. Conclusions and Future Works

Shinagawa and Iwata left two open problems in their paper and this paper settles one of them. For variants of SoEM, we set up a generalized construction with linear key schedules and found their quantum attacks. This paper also considered natural generalizations of SoEM with linear key schedules and presents quantum key recovery attacks. For non-linear variants, quantum attacks could recover the intermediate state, and then use some new techniques to recover the key. This paper focuses on the intuitive consequences of quantum attacks, so there is no discussion of non-linear variants. Therefore,

one of the future works is to discuss the quantum attacks for non-linear variants and to try make quantum attacks for other symmetric cryptographic schemes. Other future works is to settle another open problem.

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

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

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

Acknowledgments: We would like to express our sincere thanks to editors and the anonymous reviewers for their 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 Rev.* **1999**, *41*, 303–332. [CrossRef]
2. Grover, L.K. A fast quantum mechanical algorithm for database search. In *Annual ACM Symposium on the Theory of Computing*; Miller, G.L., Ed.; ACM: Berlin/Heidelberg, Germany, 2020; pp. 212–219.
3. Simon, D.R. On the power of quantum computation. *SIAM J. Comput.* **1997**, *26*, 1474–1483. [CrossRef]
4. 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, Austin, TX, USA, 13–18 June 2010; pp. 2682–2685.
5. Hosoyamada, A.; Aoki, K. On quantum related-key attacks on iterated Even–Mansour ciphers. *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.* **2019**, *102*, 27–34. [CrossRef]
6. Kuwakado, H.; Morii, M. Security on the quantum-type Even–Mansour cipher. In Proceedings of the International Symposium on Information Theory and Its Applications, Honolulu, HI, USA, 28–31 October 2012; pp. 312–316.
7. Cui, J.; Guo, J.; Ding, S. Applications of Simon's algorithm in quantum attacks on Feistel variants. *Quantum Inf. Process* **2021**, *20*, 117. [CrossRef]
8. Dong, X.; Dong, B.; Wang, X. Quantum attacks on some feistel block ciphers. *Des. Codes Cryptogr.* **2020**, *88*, 1179–1203. [CrossRef]
9. Dong, X.; Wang, X. Quantum key-recovery attack on Feistel structures. *Sci. China Inf. Sci.* **2018**, *61*, 102501. [CrossRef]
10. Ito, G.; Hosoyamada, A.; Matsumoto, R.; Sasaki, Y.; Iwata, T. Quantum chosen-ciphertext attacks against Feistel ciphers. In *Topics in Cryptology—CT-RSA 2019*; Matsui, M., Ed.; Springer: Berlin/Heidelberg, Germany, 2019; pp. 391–411.
11. Ni, B.; Ito, G.; Dong, X.; Iwata, T. Quantum attacks against type-1 generalized Feistel ciphers and applications to CAST-256. In *Progress in Cryptology—INDOCRYPT 2019*; Hao, F., Ruj, S., Gupta, S.S., Eds.; Springer: Berlin/Heidelberg, Germany, 2017; pp. 433–455.
12. Hosoyamada, A.; Iwata, T. 4-round Luby-Rackoff construction is a qPRP. In *Advances in Cryptology—ASIACRYPT 2019*; Galbraith, S.D., Moriai, S., Eds.; Springer: Berlin/Heidelberg, Germany, 2019; pp. 145–174.
13. Leander, G.; May, A. Grover meets Simon - quantumly attacking the FX-construction. In *Advances in Cryptology—ASIACRYPT 2017*; Takagi, T., Peyrin, T., Eds.; Springer: Berlin/Heidelberg, Germany, 2017; pp. 161–178.
14. Chen, Y.L.; Lambooij, E.; Mennink, B. How to build pseudorandom functions from public random permutations. In *Advances in Cryptology—CRYPTO 2019*; Boldyreva, A., Micciancio, D., Eds.; Springer: Berlin/Heidelberg, Germany, 2019; pp. 266–293.
15. Bonnetain, X.; Naya-Plasencia, M.; Schrottenloher, A. Quantum security analysis of AES. *IACR Trans. Symmetric Cryptol.* **2019**, *2*, 55–93. [CrossRef]
16. Hosoyamada, A.; Iwata, T. Provably quantum-secure tweakable block ciphers. *IACR Trans. Symmetric Cryptol.* **2021**, *1*, 337–377. [CrossRef]
17. Hosoyamada, A.; Sasaki, Y. Quantum collision attacks on reduced SHA-256 and SHA-512. In *Advances in Cryptology—CRYPTO 2021*; Malkin, T., Peikert, C., Eds.; Springer: Berlin/Heidelberg, Germany, 2021; pp. 616–646.
18. Kaplan, M.; Leurent, G.; Leverrier, A.; Naya-Plasencia, M. Breaking symmetric cryptosystems using quantum period finding. In *Advances in Cryptology—CRYPTO 2021*; Robshaw, M., Katz, J., Eds.; Springer: Berlin/Heidelberg, Germany, 2016; pp. 207–237.
19. Liu, H.; Yang, L. Quantum key recovery attack on SIMON32/64. *Cybersecurity* **2021**, *4*, 23. [CrossRef]
20. Ni, B.; Dong, X.; Jia, K.; You, Q. Quantum collision attacks on reduced Simpira v2. *IACR Trans. Symmetric Cryptol.* **2021**, *2*, 222–248. [CrossRef]
21. Chailloux, A.; Naya-Plasencia, M.; Schrottenloher, A. An efficient quantum collision search algorithm and implications on symmetric cryptography. In *Advances in Cryptology—ASIACRYPT 2017*; Takagi, T., Peyrin, T., Eds.; Springer: Berlin/Heidelberg, Germany, 2017; pp. 211–240.

22. 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 *Advances in Cryptology—ASIACRYPT 2020*; Moriai, S., Wang, H., Eds.; Springer: Berlin/Heidelberg, Germany, 2020; pp. 727–757.
23. Kumar Chauhan, A.; Kumar, A.; Kumar Sanadhya, S. Quantum free-start collision attacks on double block length hashing with round-reduced AES-256. *IACR Trans. Symmetric Cryptol.* **2021**, *1*, 316–336. [CrossRef]
24. Guo, T.; Wang, P.; Hu, L.; Ye, D. Attacks on beyond-birthday-bound MACs in the quantum setting. In *Post-Quantum Cryptography—PQCrypto 2021*; Cheon, J.H., Tillich, J.P., Eds.; Springer: Berlin/Heidelberg, Germany, 2021; pp. 421–441.
25. Bonnetain, X. Quantum key-recovery on full AEZ. In Proceedings of the International Conference on Selected Areas in Cryptography, Ottawa, ON, Canada, 16–18 August 2017; pp. 394–406.
26. 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]
27. Shinagawa, K.; Iwata, T. Quantum attacks on Sum of Even–Mansour pseudorandom functions. *Inf. Process. Lett.* **2022**, in press. [CrossRef]