Information Processing Letters 173 (2022) 106172

Contents lists available at ScienceDirect

Information Processing Letters

www.elsevier.com/locate/ipl

Quantum attacks on Sum of Even-Mansour pseudorandom functions

Kazuo Shinagawa, Tetsu Iwata *

Nagoya University, Furo-cho, Chikusa-ku, Nagoya, 464-8603, Japan

ARTICLE INFO

Article history:
Received 24 March 2021
Received in revised form 25 June 2021
Accepted 17 July 2021
Available online 29 July 2021
Communicated by Ranko Lazic

Keywords:
Cryptography
Pseudorandom function
Sum of Even-Mansour
Simon's algorithm
Grover's algorithm

ABSTRACT

At CRYPTO 2019, constructions of a pseudorandom function from public random permutations were presented. We consider one of the constructions called Sum of Even-Mansour (SoEM), and present quantum attacks against the construction. Our attacks are based on two quantum algorithms, Simon's algorithm and Grover's algorithm, and derive the secret key. We also present quantum attacks against natural variants of SoEM.

1. Introduction

At CRYPTO 2019, Chen, Lambooij, and Mennink presented constructions of a pseudorandom function (PRF) from public cryptographic permutations [1]. One of constructions is called Sum of Even-Mansour (SoEM), as it is formed by the XOR of two instances of Even-Mansour cipher [2]. The most general construction of SoEM uses two independent permutations and two independent secret keys, and there are variants by changing the number of permutations and/or keys. The designers presented provable security results on each variant in the classical setting [1].

In the quantum setting, it is well known that classical public key cryptosystems like RSA and ElGamal are insecure against quantum attacks [3]. For symmetric key cryptosystems, Kuwakado and Morii [4,5] showed polynomial-time quantum attacks against 3-round Feistel cipher and Even-Mansour cipher. These attacks use a quantum algorithm called Simon's algorithm [6] that can efficiently find a secret period in a periodic function. These constructions are provably secure in the classical setting, and hence these results demonstrate the possibility that quantum attacks can have a significant impact on the security of symmetric key cryptosystems. Indeed, Kaplan et al. [7] presented quantum attacks against various message authentication codes and authenticated encryption schemes by using Simon's algorithm. Leander and May [8] combined Simon's and Grover's quantum algorithms [9] for the key recovery attack against FX-construction [10] in the quantum setting. See e.g., [11–17] for a series of non-exhaustive quantum attacks and provable security results of symmetric key cryptosystems.

Our contributions. Given that there is an efficient quantum key recovery attack against Even-Mansour cipher, it is natural to ask if we have quantum attacks against the Sum of Even-Mansour pseudorandom function, which is the focus of this paper. First, we show quantum key recovery attacks against three constructions of SoEM, called

* Corresponding author.
E-mail addresses: shinagawa.kazuo@b.mbox.nagoya-u.ac.jp (K. Shinagawa), tetsu.iwata@nagoya-u.jp (T. Iwata).

https://doi.org/10.1016/j.ipl.2021.106172

Table 1
The complexity of the attacks against SoEM. Here, n is the block length and $s \geq 2$ is a parameter. The row "Classical provable security" shows the provable security bound, listing the lower bounds of query complexity required in classical attacks. The cells of SoEMs1 and SoEMss are left blank as provable security bounds are not known. The row "Grover's algorithm" shows the quantum query complexity if we directly use Grover's algorithm [9] to recover the secret key. The row "Quantum complexity" shows the quantum query complexity of our attacks.

Scheme (key length)	SoEM1 ($2n$)	SoEM21 (n)	SoEM22 ($2n$)	SoEMs1 (n)	SoEMss (sn)
Classical provable security [1]	$O(2^{n/2})$	$O(2^{n/2})$	$O(2^{2n/3})$	–	–
Grover's algorithm [9]	$O(2^n)$	$O(2^{n/2})$	$O(2^n)$	$O(2^{n/2})$	$O(2^{sn/2})$
Quantum complexity [this article]	$O(n)$	$O(n)$	$O(n \cdot 2^{n/2})$	$O(n)$	$O(sn \cdot 2^{(s-1)n/2})$

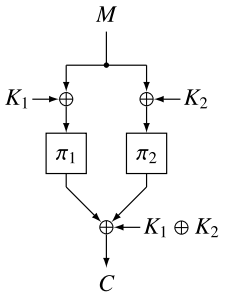

Fig. 1. SoEM.

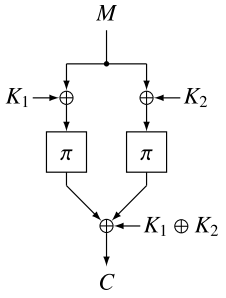

Fig. 2. SoEM1.

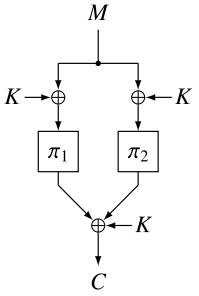

Fig. 3. SoEM21.

SoEM1, SoEM21, and SoEM22, presented in [1]. These constructions use at most two independent permutations and/or secret keys. We next consider natural generalizations of SoEM, which we call SoEMs1 and SoEMss, to have more than two permutations and/or keys, and demonstrate that similar attacks are possible. Here, $s \geq 2$ is a parameter. A summary of our results is presented in Table 1, showing the provable security bounds in the classical setting [1], quantum complexity if we directly use Grover's algorithm [9], and our results. We remark that quantum security of SoEM is not claimed in [1] and the results of this article do not contradict any of the security claims by the designers.

2. Preliminaries

Notation. For $n \in \mathbb{N} = \{1, 2, \ldots\}$, let $\{0,1\}^n$ be the set of all n-bit strings. We write $\mathrm{Perm}(n)$ for the set of all permutations over $\{0,1\}^n$. For two bit strings X and Y of the same length, let $X \oplus Y$ be their bit-wise XOR.

Specifications of SoEM. Let $n \in \mathbb{N}$, $\pi_1, \pi_2 \in \mathrm{Perm}(n)$, and $K_1, K_2 \in \{0,1\}^n$. The generic construction of SoEM : $\{0,1\}^{2n} \times \{0,1\}^n \to \{0,1\}^n$ is defined as

$$\mathrm{SoEM}^{\pi_1,\pi_2}_{K_1,K_2}(M) = \pi_1(M \oplus K_1) \oplus K_1 \oplus \pi_2(M \oplus K_2) \oplus K_2 \,. \tag{1}$$

See Fig. 1.

There are several variants of SoEM, by changing the number of underlying permutations and/or keys [1]. We call the scheme SoEM1 when $\pi_1 = \pi_2$ but K_1, K_2 are independent. When π_1 and π_2 are independent but $K_1 = K_2$, we call the scheme SoEM21, and when π_1, π_2 are independent and K_1, K_2 are independent, then we call the scheme SoEM22. We note that, if we simply put $K_1 = K_2$ in Eq. (1) to construct SoEM21, the keys XORed into the outputs of π_1, π_2 are cancelled, and the actual specification makes a slight adjustment to remedy this.

The construction of SoEM1 : $\{0,1\}^{2n} \times \{0,1\}^n \to \{0,1\}^n$ based on one permutation $\pi \in \mathrm{Perm}(n)$ and two keys $K_1, K_2 \in \{0,1\}^n$ is defined as

$$\mathrm{SoEM1}^{\pi}_{K_1,K_2}(M) = \pi(M \oplus K_1) \oplus K_1 \oplus \pi(M \oplus K_2) \oplus K_2 \,,$$

which is illustrated in Fig. 2. The construction of SoEM21 : $\{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ based on two permutations $\pi_1, \pi_2 \in \mathrm{Perm}(n)$ and one key $K \in \{0,1\}^n$ is defined as

$$\mathrm{SoEM21}^{\pi_1,\pi_2}_{K}(M) = \pi_1(M \oplus K) \oplus \pi_2(M \oplus K) \oplus K \,.$$

See Fig. 3. Finally, the construction of SoEM22 : $\{0,1\}^{2n} \times \{0,1\}^n \to \{0,1\}^n$ based on two permutations $\pi_1, \pi_2 \in \mathrm{Perm}(n)$ and two keys $K_1, K_2 \in \{0,1\}^n$ is defined as

$$\mathrm{SoEM22}^{\pi_1,\pi_2}_{K_1,K_2}(M) = \pi_1(M \oplus K_1) \oplus K_1 \oplus \pi_2(M \oplus K_2) \oplus K_2 \,.$$

See Fig. 4 (which is the same as SoEM in Fig. 1).

3. Quantum algorithms

In this section, we describe two quantum algorithms that we use in our attacks: Simon's algorithm [6] and

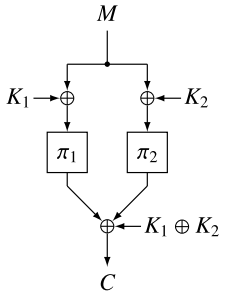

Fig. 4. SoEM22.

Grover's algorithm [9]. We use Simon's algorithm against SoEM1 and SoEM21, and use combination of Simon's and Grover's algorithms against SoEM22.

3.1. Simon's algorithm

Simon's algorithm [6] can solve the following period finding problem efficiently.

Problem 1. Suppose that a function $f : \{0,1\}^n \to \{0,1\}^n$ has a period $s \in \{0,1\}^n \backslash \{0^n\}$ such that for any distinct $x, x' \in \{0,1\}^n$, it holds that $f(x) = f(x') \Leftrightarrow x' = x \oplus s$. Find the value of s.

While $O(2^{n/2})$ queries are required to solve this problem in the classical setting, this problem can be solved with $O(n)$ queries and $O(n)$ qubits in the quantum setting by using Simon's algorithm. The algorithm uses f as a quantum oracle. We do not present the detailed steps of Simon's algorithm (see, e.g., [6,7]), and we use this as a black-box to solve Problem 1.

3.2. Grover's algorithm

Grover's algorithm [9] is an algorithm for database search to efficiently solve the following problem.

Problem 2. Let $g : \{0,1\}^n \to \{0,1\}$ be a function such that $g(x) = 1$ holds for some $x = x_0$, while $g(x) = 0$ holds for all $x \neq x_0$. Find the value of x_0.

In the classical setting, $O(2^n)$ queries are needed to solve the problem. However, given a quantum oracle of g, Grover's algorithm can solve Problem 2 by using $O(2^{n/2})$ quantum queries.

Leander and May [8] presented a quantum attack against FX-construction [10]. The attack combines Simon's and Grover's algorithms, and in what follows, we outline their attack.

FX-construction is a method to expand the key length of a block cipher. For an n-bit block cipher $E : \{0,1\}^m \times \{0,1\}^n \to \{0,1\}^n$ of key length m, FX-construction is defined as

$$\mathrm{FX}_{K_0,K_1,K_2}(M) = E_{K_0}(M \oplus K_1) \oplus K_2\,, \tag{2}$$

where $K_0 \in \{0,1\}^m$, $K_1, K_2 \in \{0,1\}^n$ are secret keys, and $M \in \{0,1\}^n$ is a plaintext. See Fig. 5.

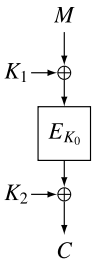

Fig. 5. FX-construction.

In Leander and May's attack, they considered a function g defined as the XOR of Eq. (2) and the block cipher E, where its key is treated as a part of the input variable k, i.e., g is defined as $g(k,x) = \mathrm{Enc}(x) \oplus E_k(x)$, where $\mathrm{Enc}(x) = \mathrm{FX}_{K_0,K_1,K_2}(x)$ is an encryption oracle given to the adversary. It is easy to see that g is a periodic function when $k = K_0$ with a period K_1. To see this, when $k = K_0$, we have

$$\begin{aligned} g(K_0,x) &= \mathrm{Enc}(x) \oplus E_{K_0}(x) \\ &= E_{K_0}(x \oplus K_1) \oplus K_2 \oplus E_{K_0}(x) \\ &= g(K_0, x \oplus K_1)\,. \end{aligned}$$

From the assumption that $E_k(\cdot)$ behaves as a random function for any fixed $k \in \{0,1\}^m$, g does not have a period with high probability when $k \neq K_0$. We apply Grover's algorithm on k and examine if $g(k,\cdot)$ is periodic by using Simon's algorithm. The value of k when a period is obtained is K_0. The running time of this attack is roughly $O(2^{m/2})$ in Grover's algorithm and polynomial in Simon's algorithm. Overall, the attack works with $O((m+n)\cdot 2^{m/2})$ quantum queries and $O(n^2+m)$ qubits [8, Theorem 2].

Our attack against SoEM22 presented in Section 4.3 follows this attack. Given oracle access to $\mathrm{SoEM22}^{\pi_1,\pi_2}_{K_1,K_2}(\cdot)$, we define a function $g(k,x)$ that has a period in its second argument when $k = K_2$. Then we apply Grover's algorithm to derive K_2, while we use Simon's algorithm to detect a period, which is K_1.

4. Quantum attacks against SoEM

In this section, we present our quantum attacks against SoEM1, SoEM21, and SoEM22.

4.1. Quantum attack against SoEM1

Theorem 1. *There exists a quantum attack against* SoEM1 *that recovers the secret keys K_1 and K_2 with $O(n)$ qubits and $O(n)$ quantum queries.*

Proof. The attack is in two steps. We first recover $K' = K_1 \oplus K_2$, and then we recover K_1 (or K_2). We first observe that $\mathrm{SoEM1}^{\pi}_{K_1,K_2}(\cdot)$ itself is a periodic function. Specifically, let $f : \{0,1\}^n \to \{0,1\}^n$ be a function defined as

$$\begin{aligned} f(x) &= \mathrm{SoEM1}^{\pi}_{K_1,K_2}(x) \\ &= \pi(x \oplus K_1) \oplus K_1 \oplus \pi(x \oplus K_2) \oplus K_2\,. \end{aligned}$$

Then, f is a periodic function with period $K' = K_1 \oplus K_2$, since

$$\begin{aligned} f(x \oplus K') &= \pi(x \oplus (K_1 \oplus K_2) \oplus K_1) \oplus K_1 \\ &\quad \oplus \pi(x \oplus (K_1 \oplus K_2) \oplus K_2) \oplus K_2 \\ &= f(x). \end{aligned}$$

Therefore, by applying Simon's algorithm on f, $K' = K_1 \oplus K_2$ can be derived by using $O(n)$ qubits and $O(n)$ quantum oracle queries.

We next derive the values of K_1 and K_2 by using Simon's algorithm once more. With the knowledge of K', we define a function $f' : \{0,1\}^n \to \{0,1\}^n$ by using $f(x) = \mathrm{SoEM1}^{\pi}_{K_1,K_2}(x)$ and the public permutation $\pi \in \mathrm{Perm}(n)$ as

$$\begin{aligned} f'(x) &= f(x) \oplus \pi(x) \oplus \pi(x \oplus K') \\ &= \pi(x \oplus K_1) \oplus K_1 \oplus \pi(x \oplus K_2) \oplus K_2 \oplus \pi(x) \\ &\quad \oplus \pi(x \oplus K'). \end{aligned}$$

We see that f' is a periodic function with period K_1, since

$$\begin{aligned} f'(x \oplus K_1) &= \pi((x \oplus K_1) \oplus K_1) \\ &\quad \oplus K_1 \oplus \pi((x \oplus K_1) \oplus K_2) \oplus K_2 \\ &\quad \oplus \pi(x \oplus K_1) \oplus \pi((x \oplus K_1) \oplus K') \\ &= f'(x). \end{aligned}$$

We also see that $f'(x)$ has K_2 and K' as its periods.

In this case, the condition of Simon's algorithm: $f'(x) = f'(x') \Leftrightarrow x' = x \oplus s$ is not satisfied. When f' has independent periods $s_1, \ldots, s_\ell$, Simon's algorithm outputs y which is orthogonal to all $s_1, \ldots, s_\ell$, and one can compute the vector space that those s_i's span [18,12]. Consequently, K_1 and K_2 can be derived by using Simon's algorithm, and overall, the attack works with $O(n)$ qubits and $O(n)$ quantum queries. □

We remark that $f'(x)$ above can be seen as

$$f'(x) = \mathrm{SoEM1}^{\pi}_{K_1,K_2}(x) \oplus \mathrm{SoEM1}^{\pi}_{0^n,K'}(x) \oplus K',$$

where the last two terms can be computed offline with the knowledge of K'.

4.2. Quantum attack against SoEM21

Theorem 2. *There exists a quantum attack against* SoEM21 *that recovers the secret key K with $O(n)$ qubits and $O(n)$ quantum queries.*

Proof. In this case, we define a function $f : \{0,1\}^n \to \{0,1\}^n$ as

$$\begin{aligned} f(x) &= \mathrm{SoEM21}^{\pi_1,\pi_2}_{K}(x) \oplus \pi_1(x) \oplus \pi_2(x) \\ &= \pi_1(x \oplus K) \oplus \pi_2(x \oplus K) \oplus K \oplus \pi_1(x) \oplus \pi_2(x), \end{aligned}$$

where $\mathrm{SoEM21}^{\pi_1,\pi_2}_{K}(x)$ is the oracle given to the adversary, and $\pi_1, \pi_2 \in \mathrm{Perm}(n)$ are public permutations used therein. We see that this f has a period K, since

$$\begin{aligned} f(x \oplus K) &= \pi_1(x \oplus K \oplus K) \oplus \pi_2(x \oplus K \oplus K) \oplus K \\ &\quad \oplus \pi_1(x \oplus K) \oplus \pi_2(x \oplus K) \\ &= f(x). \end{aligned}$$

Therefore, K can be derived with $O(n)$ qubits and in polynomial time quantum oracle queries to f. □

4.3. Quantum attack against SoEM22

Let $g' : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ be a function $g'(k,x) = \pi_1(x) \oplus \pi_2(x \oplus k)$. In our attack against SoEM22, we define a function g with variables x and k as the XOR of $\mathrm{SoEM22}^{\pi_1,\pi_2}_{K_1,K_2}(x)$ and $g'(k,x)$, namely,

$$\begin{aligned} g(k,x) &= \mathrm{SoEM22}^{\pi_1,\pi_2}_{K_1,K_2}(x) \oplus g'(k,x) \\ &= \pi_1(x \oplus K_1) \oplus K_1 \oplus \pi_2(x \oplus K_2) \oplus K_2 \\ &\quad \oplus \pi_1(x) \oplus \pi_2(x \oplus k). \end{aligned} \tag{3}$$

When the variable k is identical to K_2, g is simplified to

$$g(K_2,x) = \pi_1(x \oplus K_1) \oplus K_1 \oplus K_2 \oplus \pi_1(x),$$

which is a periodic function with a period K_1. Following the analysis of FX-construction, we assume that $g'(k,\cdot)$ behaves as a random function for any $k \in \{0,1\}^n$, and is not a periodic function with high probability when $k \neq K_2$.

Then, we apply Grover's algorithm to g on k. Inside Grover's algorithm, Simon's algorithm is operated to examine which value of k makes $g(k,\cdot)$ periodic. The value of k when a period is obtained through Simon's algorithm is the secret key K_2 of SoEM22, and the period gives the value of K_1.

From the same analysis as in [8, Theorem 2], we obtain the following theorem.

Theorem 3. *For any fixed $k \in \{0,1\}^n$, assume that $g'(k,\cdot)$ behaves as a random function $\{0,1\}^n \to \{0,1\}^n$. Given quantum oracle access to $\mathrm{SoEM22}^{\pi_1,\pi_2}_{K_1,K_2}(\cdot)$ and $g'(\cdot,\cdot)$, there exists a quantum attack against* SoEM22 *that recovers K_1 and K_2 by using $O(n^2)$ qubits and $O(n \cdot 2^{n/2})$ queries.*

We remark that, if $K_1 = 0^n$, $g(K_2,x)$ becomes constant $K_1 \oplus K_2$. The assumption of the randomness of g' is used to check if $g(K_2,x)$ is a constant function in the case $K_1 = 0^n$. When $K_1 \neq 0^n$, there is a test to check if k is K_2. The assumption is also used to show that the false positive probability[1] of the test is sufficiently small.

5. Generalizations and attacks

In this section, we consider natural generalizations of SoEM21 and SoEM22, and present quantum attacks against these constructions.

[1] The probability that the test incorrectly outputs $k = K_2$ even though $k \neq K_2$.

5.1. Generalizations

We define SoEMs1 as a natural generalization of SoEM21 that uses s permutations $\pi_1, \ldots, \pi_s \in \mathrm{Perm}(n)$, where $s \geq 2$, and one key $K \in \{0,1\}^n$. This is defined as

$$\mathrm{SoEM}s1_K^{\pi_1,\ldots,\pi_s}(M) = \pi_1(M \oplus K) \oplus \cdots \oplus \pi_s(M \oplus K) \oplus K\,.$$

We also define SoEMss as a natural generalization of SoEM22 that uses s permutations $\pi_1, \ldots, \pi_s \in \mathrm{Perm}(n)$ and s keys $K_1, \ldots, K_s \in \{0,1\}^n$, where $s \geq 2$. This is defined as

$$\begin{aligned}&\mathrm{SoEM}ss_{K_1,\ldots,K_s}^{\pi_1,\ldots,\pi_s}(M)\\ &= \pi_1(M \oplus K_1) \oplus K_1 \oplus \cdots \oplus \pi_s(M \oplus K_s) \oplus K_s\,.\end{aligned}$$

5.2. Quantum attacks

The attack against SoEMs1 is similar to the attack against SoEM21 in Theorem 2. We define a function f as

$$\begin{aligned}f(x) &= \mathrm{SoEM}s1_K^{\pi_1,\ldots,\pi_s}(x) \oplus \pi_1(x) \oplus \cdots \oplus \pi_s(x)\\ &= \pi_1(x \oplus K) \oplus \cdots \oplus \pi_s(x \oplus K) \oplus K\\ &\quad \oplus \pi_1(x) \oplus \cdots \oplus \pi_s(x)\,.\end{aligned}$$

It is easy to see that f is a periodic function with period K. Therefore, by applying Simon's algorithm on f, K can be derived in polynomial time quantum oracle queries and $O(n)$ qubits. We have the following corollary.

Corollary 1. *There exists a quantum attack against* SoEMs1 *that recovers K with $O(n)$ qubits and $O(n)$ quantum queries.*

Our attack against SoEMss is similar to the attack against SoEM22 in Theorem 3, and we consider the following functions $g' : \{0,1\}^{(s-1)n} \times \{0,1\}^n \to \{0,1\}^n$ and $g : \{0,1\}^{(s-1)n} \times \{0,1\}^n \to \{0,1\}^n$:

$$\begin{cases} g'(k_2, \ldots, k_s, x) = \pi_1(x) \oplus \pi_2(x \oplus k_2) \oplus \cdots \\ \qquad \oplus \pi_s(x \oplus k_s)\,, \\ g(k_2, \ldots, k_s, x) = \mathrm{SoEM}ss_{K_1,\ldots,K_s}^{\pi_1,\ldots,\pi_s}(x) \oplus g'(k_2, \ldots, k_s, x) \\ \quad = \pi_1(x \oplus K_1) \oplus K_1 \oplus \cdots \oplus \pi_s(x \oplus K_s) \oplus K_s \\ \qquad \oplus \pi_1(x) \oplus \pi_2(x \oplus k_2) \oplus \cdots \oplus \pi_s(x \oplus k_s)\,. \end{cases}$$

Since $g(K_2, \ldots, K_s, x) = \pi_1(x \oplus K_1) \oplus K_1 \oplus \cdots \oplus K_s \oplus \pi_1(x)$, we see that $g(k_2, \ldots, k_s, \cdot)$ has a period K_1 in its last argument when $(k_2, \ldots, k_s) = (K_2, \ldots, K_s)$.

Then, we apply Grover's algorithm to g on $k_2, \ldots, k_s$. As in the attacks against FX-construction and SoEM22, we use Simon's algorithm inside Grover's algorithm to examine which value of $k_2, \ldots, k_s$ makes $g(k_2, \ldots, k_s, \cdot)$ periodic. The value of $(k_2, \ldots, k_s)$ when a period is obtained is the correct keys $(K_2, \ldots, K_s)$, and the period gives the value of K_1.

We have the following corollary.

Corollary 2. *For any fixed $k_2, \ldots, k_s \in \{0,1\}^n$, assume that g' behaves as a random function $\{0,1\}^n \to \{0,1\}^n$. Given quantum oracle access to* $\mathrm{SoEM}ss_{K_1,\ldots,K_s}^{\pi_1,\ldots,\pi_s}(\cdot)$ *and $g'(\cdot, \ldots, \cdot)$, there exists a quantum attack against* SoEMss *that recovers $K_1, \ldots, K_s$ by using $O(n^2 + sn)$ qubits and $O(sn \cdot 2^{(s-1)n/2})$ queries.*

As in the remark below Theorem 3, the assumption of the randomness of g' is used to check if $g(K_2, \ldots, K_s, x)$ is a constant function in the case $K_1 = 0^n$, and this is also used to show that the false positive probability[2] of the test in the case $K_1 \neq 0^n$ is sufficiently small.

6. Conclusions

In this article, we presented quantum key recovery attacks against the SoEM1, SoEM21, and SoEM22 pseudorandom functions. The attacks against SoEM1 and SoEM21 work with polynomial-time quantum queries and make use of Simon's algorithm. The complexity of the attack against SoEM22 is $O(n \cdot 2^{n/2})$, and it uses Simon's algorithm and Grover's algorithm. We also presented quantum attacks against SoEMs1 and SoEMss, which are natural generalizations of SoEM21 and SoEM22.

Open problems. As in Table 1, the classical security of SoEMs1 and SoEMss is not known. It is in fact easy to see that SoEMss is at least as secure as SoEM22, and we expect that SoEMs1 is as secure as SoEM21. However, a detailed analysis is left open and we do not know if they have a stronger provable security bound.

A number of variants of SoEM can be considered, and for some of them, quantum attacks are not obvious. For instance, we find that a variant of SoEM21 defined as

$$\begin{aligned}\mathrm{SoEM21}_K^{\pi_1,\pi_2}(M) = \pi_1(M \oplus K) \oplus K \oplus \pi_2(M \oplus 2 \cdot K)\\ \oplus 2 \cdot K\end{aligned}$$

prevents the straightforward period finding attack of Theorem 2, where $2 \cdot K$ is a "doubling of K" in a finite field, and it would be interesting to see the security of such constructions.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgements

This work was supported in part by JSPS KAKENHI Grant Number JP20K11675.

References

[1] Y.L. Chen, E. Lambooij, B. Mennink, How to build pseudorandom functions from public random permutations, in: A. Boldyreva, D. Micciancio (Eds.), Advances in Cryptology - CRYPTO 2019 - 39th Annual

[2] In this case, the probability that the test incorrectly outputs $(k_2, \ldots, k_s) = (K_2, \ldots, K_s)$ even though $(k_2, \ldots, k_s) \neq (K_2, \ldots, K_s)$.

International Cryptology Conference, Proceedings, Part I, Santa Barbara, CA, USA, August 18–22, 2019, in: Lecture Notes in Computer Science, vol. 11692, Springer, 2019, pp. 266–293.

[2] S. Even, Y. Mansour, A construction of a cipher from a single pseudorandom permutation, in: H. Imai, R.L. Rivest, T. Matsumoto (Eds.), Advances in Cryptology - ASIACRYPT '91, International Conference on the Theory and Applications of Cryptology, Proceedings, Fujiyoshida, Japan, November 11–14, 1991, in: Lecture Notes in Computer Science, vol. 739, Springer, 1991, pp. 210–224.

[3] P.W. Shor, Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer, SIAM Rev. 41 (2) (1999) 303–332, https://doi.org/10.1137/S0036144598347011.

[4] H. Kuwakado, M. Morii, Quantum distinguisher between the 3-round Feistel cipher and the random permutation, in: IEEE International Symposium on Information Theory, Proceedings, ISIT 2010, Austin, Texas, USA, June 13–18, 2010, IEEE, 2010, pp. 2682–2685.

[5] H. Kuwakado, M. Morii, Security on the quantum-type Even-Mansour cipher, in: Proceedings of the International Symposium on Information Theory and Its Applications, ISITA 2012, Honolulu, HI, USA, October 28–31, 2012, IEEE, 2012, pp. 312–316, http://ieeexplore.ieee.org/document/6400943/.

[6] D.R. Simon, On the power of quantum computation, SIAM J. Comput. 26 (5) (1997) 1474–1483, https://doi.org/10.1137/S0097539796298637.

[7] M. Kaplan, G. Leurent, A. Leverrier, M. Naya-Plasencia, Breaking symmetric cryptosystems using quantum period finding, in: M. Robshaw, J. Katz (Eds.), Advances in Cryptology - CRYPTO 2016 - 36th Annual International Cryptology Conference, Proceedings, Part II, Santa Barbara, CA, USA, August 14–18, 2016, in: Lecture Notes in Computer Science, vol. 9815, Springer, 2016, pp. 207–237.

[8] G. Leander, A. May, Grover meets Simon - quantumly attacking the FX-construction, in: T. Takagi, T. Peyrin (Eds.), Advances in Cryptology - ASIACRYPT 2017 - 23rd International Conference on the Theory and Applications of Cryptology and Information Security, Proceedings, Part II, Hong Kong, China, December 3–7, 2017, in: Lecture Notes in Computer Science, vol. 10625, Springer, 2017, pp. 161–178.

[9] L.K. Grover, A fast quantum mechanical algorithm for database search, in: G.L. Miller (Ed.), Proceedings of the Twenty-Eighth Annual ACM Symposium on the Theory of Computing, Philadelphia, Pennsylvania, USA, May 22–24, 1996, ACM, 1996, pp. 212–219.

[10] J. Kilian, P. Rogaway, How to protect DES against exhaustive key search (an analysis of DESX), J. Cryptol. 14 (1) (2001) 17–35, https://doi.org/10.1007/s001450010015.

[11] G. Ito, A. Hosoyamada, R. Matsumoto, Y. Sasaki, T. Iwata, Quantum chosen-ciphertext attacks against Feistel ciphers, in: M. Matsui (Ed.), Topics in Cryptology - CT-RSA 2019 - The Cryptographers' Track at the RSA Conference 2019, Proceedings, San Francisco, CA, USA, March 4–8, 2019, in: Lecture Notes in Computer Science, vol. 11405, Springer, 2019, pp. 391–411.

[12] X. Bonnetain, Quantum key-recovery on full AEZ, in: C. Adams, J. Camenisch (Eds.), Selected Areas in Cryptography - SAC 2017 - 24th International Conference, Ottawa, ON, Canada, August 16–18, 2017, in: Lecture Notes in Computer Science, vol. 10719, Springer, 2017, pp. 394–406, Revised Selected Papers.

[13] B. Ni, G. Ito, X. Dong, T. Iwata, Quantum attacks against type-1 generalized Feistel ciphers and applications to CAST-256, in: F. Hao, S. Ruj, S.S. Gupta (Eds.), Progress in Cryptology - INDOCRYPT 2019 - 20th International Conference on Cryptology in India, Proceedings, Hyderabad, India, December 15–18, 2019, in: Lecture Notes in Computer Science, vol. 11898, Springer, 2019, pp. 433–455.

[14] A. Chailloux, M. Naya-Plasencia, A. Schrottenloher, An efficient quantum collision search algorithm and implications on symmetric cryptography, in: T. Takagi, T. Peyrin (Eds.), Advances in Cryptology – ASIACRYPT 2017, Springer International Publishing, Cham, 2017, pp. 211–240.

[15] A. Hosoyamada, T. Iwata, 4-round Luby-Rackoff construction is a qPRP, in: S.D. Galbraith, S. Moriai (Eds.), Advances in Cryptology - ASIACRYPT 2019 - 25th International Conference on the Theory and Application of Cryptology and Information Security, Proceedings, Part I, Kobe, Japan, December 8–12, 2019, in: Lecture Notes in Computer Science, vol. 11921, Springer, 2019, pp. 145–174.

[16] X. Bonnetain, M. Naya-Plasencia, A. Schrottenloher, Quantum security analysis of AES, IACR Trans. Symmetric Cryptol. 2019 (2) (2019) 55–93, https://doi.org/10.13154/tosc.v2019.i2.55-93.

[17] A. Hosoyamada, T. Iwata, Provably quantum-secure tweakable block ciphers, IACR Trans. Symmetric Cryptol. 2021 (1) (2021) 337–377, https://doi.org/10.46586/tosc.v2021.i1.337-377.

[18] L. Yang, H. Li, Investigating the linear structure of Boolean functions based on Simon's period-finding quantum algorithm, CoRR, arXiv:1306.2008, 2013.