Quantum Attacks on PRFs Based on Public Random Permutations

Tingting Guo[1,2], Peng Wang[1,2(✉)], Lei Hu[1,2], and Dingfeng Ye[1,2]

[1] SKLOIS, Institute of Information Engineering, CAS
w.rocking@gmail.com,{guotingting, hulei, yedingfeng}@iie.ac.cn
[2] School of Cyber Security, University of Chinese Academy of Sciences

Abstract. We proposed three general frameworks $F1, F2$, and $F3$ for n-to-n-bit PRFs with one, two parallel, and two serial public permutation calls respectively, where every permutation is preceded and followed by any bitwise linear mappings. We analyze them in the $Q2$ model where attackers have quantum-query access to PRFs and permutations. Our results show $F1$ is not secure with $\mathcal{O}(n)$ quantum queries while its PRFs achieve $n/2$-bit security in the classical setting, and $F2, F3$ are not secure with $\mathcal{O}(2^{n/2}n)$ quantum queries while their PRFs, such as SoEM, PDMMAC, and pEDM, achieve $2n/3$-bit security in the classical setting. Besides, we attack three general instantiations XopEM, EDMEM, and EDMDEM of $F2, F3$, which derive from replacing the two PRPs in Xop, EDM, and EDMD with two independent EM constructions, and concrete PRF instantiations DS-SoEM, PDMMAC, and pEDM, SoKAC21 of $F2, F3$, with at most $\mathcal{O}(2^{n/2}n)$ quantum queries.

Keywords: PRF · Permutation · Quantum Attack

1 Introduction

Symmetric-key Schemes based on PRFs. A Message Authentication Code (MAC) is a symmetric-key primitive that ensures message integrity. For a popular nouce-based MAC, the Wegman-Carter (WC) scheme [35,9,33,5], it offers better security when replacing the underlying Pseudorandom Permutation (PRP) with Pseudorandom Function (PRF). For other cryptographic designs, such as encryption mode CTR [1] and authenticated encryption mode GCM [26], it also offers better security when replacing the underlying PRPs (block ciphers) with PRFs. Thus it is of great necessity to design pseudorandom functions (PRFs) even with fixed-input length. Unfortunately, dedicated fixed input length PRF designs are scarce. The well-known PRP/PRF switching lemma [22,4] suggests simply viewing the PRP as a PRF. However, it makes the cryptographic designs be limited to only birthday bound security, i.e., $n/2$-bit security (We say a design m-bit security if it is secure up to $\mathcal{O}(2^m)$ queries) assuming the size of the out of PRP is n bits. Thus, plenty of researchers make a great effort to transform PRPs to PRFs with high quality.

PRP-to-PRF Conversion Methods with BBB Security. Fortunately, there have existed four main PRP-to-PRF transformation methods in achieving security beyond the birthday bound: Trunc, Xop, EDM, and EDMD. Let block ciphers be modeled as PRPs. Trunc [21] truncates the output of an n-bit block cipher by $m < n$ bits, resulting $(m+n)/2$-bit security [2,18]. Let E_1, E_2 be two independent block ciphers. Xop, EDM, and EDMD based on E_1, E_2 all provide n-bit security [29,30,31,27]. Xop [3] is the XOR of PRPs for input M: $\text{XoP}_{E_1,E_2}(M) = E_1(M) \oplus E_2(M)$. Encrypted Davies-Meyer (EDM) [15] and Encrypted Davies-Meyer Dual (EDMD) [27] serial perform two block ciphers: $\text{EDM}_{E_1,E_2}(M) = E_2(E_1(M) \oplus M), \text{EDMD}_{E_1,E_2}(M) = E_2(E_1(M)) \oplus E_1(M)$. In fact, at ASIACRYPT 2021, Chen et al. [14] have proved XoP, EDM, and EDMD are the only constructions with Beyond-Birthday-Bound (BBB) security ($> n/2$-bit security) of all n-to-n-bit PRFs based on two block cipher calls.

Advantages of Permutation-Based Designs. It is well known that designing a block cipher is more complex than a keyless public permutation, as the former involves evaluating the underlying key scheduling algorithm. Besides, we do not need to store the round keys in public permutation-based designs. In addition, the theory of analyzing the security of any cryptographic design based on public permutations is full-fledged. Therefore, it has been an extraordinarily popular approach to design cryptographic schemes based on public permutations straightforwardly.

Even-Mansour Constructions. We can view PRPs as PRFs directly. One of the most famous public permutation-based PRPs is Even-Mansour (EM) construction [17]: $\text{EM}(M) = \pi(M \oplus K_1) \oplus K_2$, where π is a public random permutation and K_1, K_2 are two independent keys. Later, Bogdanov et al. [7] introduced a more general PRP KAC by iterating EM for multiple rounds. However, they both only provide birthday bound security with respect to the block size by PRP/PRF switching lemma.

***n*-to-*n*-Bit PRFs with One or Two Permutation Calls.** Researchers try to design public permutation-based n-to-n-bit PRFs that provide BBB security with one or two permutations calls. At CRYPTO 2019 Chen et al. [13] firstly delved into the methods of designing such PRFs. They presented the general design of a PRF with only one public permutation call and whose permutation is preceded and followed by any linear mappings consisting of bitwise exclusive-or and scalar multiplication (see Fig.1(a)). They showed such construction cannot be secure beyond the birthday bound for any linear mapping in the classical setting.

So they try to design PRFs with higher security by making two public permutations calls. In the same paper [13], they try to get such PRFs by instantiating generic BBB secure PRP-to-PRF conversion functions with EMs or their variants, i.e., replacing the two PRPs in Xop and EDMD with two independent EMs or their variants. They firstly proposed SoKAC by instantiating with the variants of EM for EDMD construction, which is similar to 2-round KAC [7], with two public permutations and two keys. They named it SoKAC1 if the two permutations are the same, which only provides birthday bound security [13]. And they named it SoKAC21 if the two keys are the same, which provides BBB security [13] but unfortunately attacked by Nandi [28] at EUROCRYPT 2020 with only birthday bound complexity. In addition to SoKAC, they also put forward SoEM by instantiating with EM for Xop construction. SoEM is based on two public permutations and two keys as well. They called it SoEM1 if the two permutations are the same and SoEM21 if the two keys are the same, which are both only birthday bound securities [13]. Delightfully, they proved that SoEM22, with two independent permutations and two independent keys, is secure up to $2n/3$ bits [13].

Following their design method, plentiful fantabulous PRFs have been put forward. Quickly, at CRYPTO 2020 Chakraborti et al. [12] introduced PDMMAC, which is based on only single public permutation and its reverse and only takes a single key, by instantiating with the EM appropriately for EDM construction. It also provides $2n/3$-bit security [12]. Next to PDMMAC, in 2020, Bhattacharjee et al. [6] designed DS-SoEM, which is based on only one public permutation and even doesn't need the inverse of the permutation like PDMMAC. It is a Xop construction instantiated with EM with two same public permutation calls and two independent keys and still maintains $2n/3$-bit security. Another preeminent PRF based on only one public permutation and two keys is pEDM, which is introduced by Dutta [16] in 2021. It is also an EDM construction instantiated with EMs with $2n/3$-bit security.

Previous Quantum Attacks. There have existed attacks for permutation-based PRFs in the $Q2$ model, which means attackers can make superposition queries to a quantum oracle of $U_F : |x, y\rangle \mapsto |x, y \oplus F(x)\rangle$, where F is the classic primitive. In 2012, Kuwakado et al. [24] firstly recover the keys of Even-Mansour cipher by applying Simon's algorithm with only $\mathcal{O}(n)$ quantum queries. And for PRFs based on two public permutation calls, recently in 2022 Shinagawa et al. [32] presented key recovery attacks against SoEM. They successfully attacked SoEM1 and SoEM21 with polynomial quantum queries by applying Simon's algorithm, and SoEM22 with $\mathcal{O}(2^{n/2}n)$ quantum queries by applying Grover-meet-Simon algorithm. For SoEM variants with linear key schedules, Zhang [36] showed they are also vulnerable to Simon's algorithm and Grover-meet-Simon algorithm.

Motivations. There are still plenty of PRFs based on permutations haven't been analyzed in the $Q2$ model, such as SoKAC, PDMMAC, DS-SoEM, pEDM, and so on. What about the security of such PRFs in the $Q2$ model? Is it possible to get an optimal PRF based on one or two permutations? How to propose general frameworks and analyze their securities?

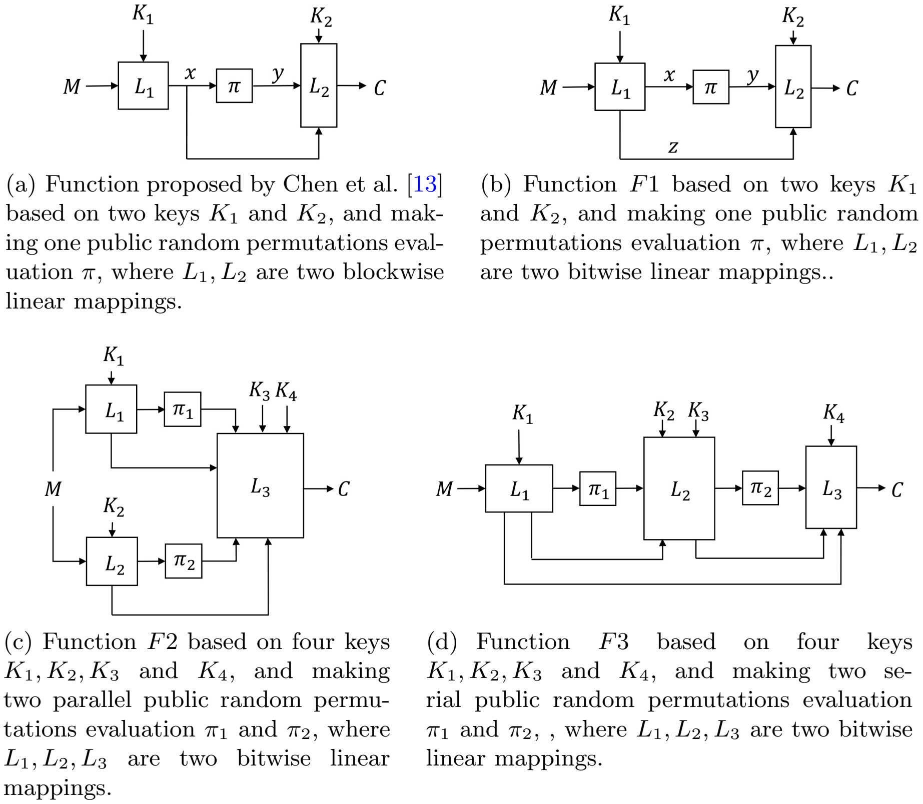
Our Contributions. We assume all permutations in all functions we analyzed are on n bits. And then the following functions are all n-to-n-bit functions except for DS-SoEM. We summarize our main results in Table 1.

1. The first contribution of work is to systematically tackle the security of a PRF with one random permutation call whose permutation is preceded and

followed by linear mappings from a generalized perspective in the $Q2$ model. The general function we considered (See Fig.1(b)) is more universal than Chen et al. [13] (See Fig.1(a)):

1) First, we popularize the value from the first linear mapping to the permutation (i.e. x) and the value from the first linear mapping to the second linear mapping (i.e. z) from same to be independent;
2) Second we extend blockwise linear mappings to bitwise linear mappings.

We name our generalized function as $F1$. We considering different types of linear mappings and prove that such construction is not secure with polynomial quantum queries in the $Q2$ model in spite of its birthday bound security [13] in the classical setting.



(a) Function proposed by Chen et al. [13] based on two keys K_1 and K_2, and making one public random permutations evaluation π, where L_1, L_2 are two blockwise linear mappings.

(b) Function $F1$ based on two keys K_1 and K_2, and making one public random permutations evaluation π, where L_1, L_2 are two bitwise linear mappings..

(c) Function $F2$ based on four keys K_1, K_2, K_3 and K_4, and making two parallel public random permutations evaluation π_1 and π_2, where L_1, L_2, L_3 are two bitwise linear mappings.

(d) Function $F3$ based on four keys K_1, K_2, K_3 and K_4, and making two serial public random permutations evaluation π_1 and π_2, , where L_1, L_2, L_3 are two bitwise linear mappings.

Fig. 1. Functions based on one or two public permutations calls.

2. The second contribution of work is to systematically tackle the the security of a PRF with two public random permutations calls and both permutations are preceded and followed by bitwise linear mappings from a generalized perspective. We show that all such PRFs can be divided into two kinds: one's two permutation calls are parallel and the other's are serial. We call the general design of the former as $F2$ as pictured in Fig.1(c) and the latter as $F3$ as pictured in Fig.1(d). We find that both two constructions cannot be

secure beyond $\mathcal{O}(2^{n/2}n)$ quantum queries in the $Q2$ model in spite of BBB security of their concrete instantiations in the classical setting [12,16,13].

3. Our third contribution is to present the quantum security of general and cencrete instantiations of $F2, F3$. We show the hierarchy of all PRFs based on two public permutations in Fig.2.

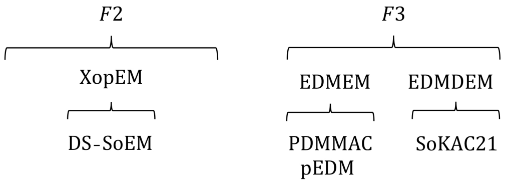


Fig. 2. The hierarchy of all PRFs based on two public permutations calls.

1) By replacing the two PRPs in Xop, EDM, and EDMD with two independent EMs respectively, we get three general instantiations of $F2, F3$: XopEM, EDMEM, and EDMDEM. We show they are not secure with at most $\mathcal{O}(2^{n/2}n)$ quantum queries in the $Q2$ model in spite of their concrete instantiations (PDMMAC, pEDM, and SoEM22) are secure up to $2n/3$ bits.
2) We show the security of concrete PRF designs instantiated with EM for Xop, EDM, and EDMD. Our results show $2n/3$-bit secure DS-SoEM, PDMMAC, pEDM in the classical break with at most $\mathcal{O}(2^{n/2}n)$ queries in the $Q2$ model. We also show SoKAC21 break with $\mathcal{O}(2^{n/3})$ queries in the $Q2$ model.

Table 1. Summary of the our main results. n is the size of permutation. b is a truncation parameter.

	Functions	The number of calls of public permutations	The number of public permutations	The number of keys	The query complexity of our quantum attack
Generic functions	$F1$	1	1	2	$\mathcal{O}(n)$
	$F2$	2	2	4	$\mathcal{O}(2^{n/2}n)$
	$F3$	2	2	4	$\mathcal{O}(2^{n/2}n)$
Instantiations with EM	EDMEM	2	2	4	$\mathcal{O}(2^{n/2}n)$
	EDMDEM	2	2	4	$\mathcal{O}(2^{n/2}n)$
	XopEM	2	2	4	$\mathcal{O}(2^{n/2}n)$
Special instantiations	DS-SoEM [6]	2	1	2	$\mathcal{O}(2^{(n-d)/2}(n-d))$
	PDMMAC [12]	2	1	1	$\mathcal{O}(2^{n/2})$
	pEDM [16]	2	1	2	$\mathcal{O}(2^{n/2}n)$
	SoKAC21 [13]	2	2	1	$\mathcal{O}(2^{n/3})$

2 Preliminaries

2.1 Notations

Let $\mathbb{N}$ be the set of positive integers. For $n \in \mathbb{N}$, let $\{0,1\}^n$ be the set of all n-bit binary strings. Let $\mathrm{Perm}(n)$ be the set of all permutations on n bits and

Func(m,n) be the set of all functions from m bits to n bits. Let $x \overset{\$}{\leftarrow} \mathcal{X}$ indicate choosing x from set $\mathcal{X}$ uniformly and random. Let $\pi \overset{\$}{\leftarrow}$ Perm(n) be a random permutation on n bits (i.e. $\pi \overset{\$}{\leftarrow}$Perm$(n)$). Let ρ be a random function from n bits to n bits (i.e. $\rho \overset{\$}{\leftarrow}$Func$(n,n)$). Let $\#\mathcal{X}$ be the number of the elements in set $\mathcal{X}$. Let O indicate the zero linear mappings which maps all values in $\{0,1\}^n$ to 0^n.

2.2 The Security of qPRF Based on Public Random Permutations

Let $\pi_1,\ldots,\pi_\ell$ be public random permutations. Let F be a keyed function that may depend on $\pi_1,\ldots,\pi_\ell$ and ρ be a random function that is independent of $\pi_1,\ldots,\pi_\ell$. Given the quantum oracle of $\pi_1^{\pm},\ldots,\pi_\ell^{\pm}$ and function F or ρ, where the superscript ± for π_i indicates the distinguisher has bi-directional access. The security of quantum pseudorandom function (qPRF) of F is defined by the minimum number of quantum queries of all distinguishers to distinguish $(F,\pi_1^{\pm},\ldots,\pi_\ell^{\pm})$ from $(\rho,\pi_1^{\pm},\ldots,\pi_\ell^{\pm})$.

2.3 Quantum Algorithms

1) Grover's Algorithm. Let $test : \{0,1\}^n \rightarrow \{0,1\}$ be a boolean function. Classically, we can find a u such that $test(u)=1$ with $\mathcal{O}(\frac{2^n}{\#\{u:test(u)=1\}})$ queries to $test(\cdot)$. However, in the $Q2$ model Grover's algorithm [19] can speed up the search by square root [10]. More generally, the $test$ function can't describe the target set so precisely. That is to say, $test(u)$ always outputs 1 for elements in the target set, but for elements not in the target set that $test(u)$ also output 1 with some probability. Luckily, Grover's algorithm can find an element in such a target set as well, which is shown in theorem 1.

Theorem 1. ([20,8]) *Let $\mathcal{U} \subseteq \{0,1\}^n$ and test : $\{0,1\}^n \rightarrow \{0,1\}$ be a boolean function who satisfies*

$$\begin{cases} \Pr[test(u)=1]=1, & u \in \mathcal{U}, \\ \Pr[test(u)=1] \leq p_1, & u \notin \mathcal{U}. \end{cases}$$

Then the Grover's algorithm with $\mathcal{O}(2^{n/2})$ quantum queries to test$(\cdot)$ using $\mathcal{O}(n+m)$ qubits can output a $u \in \mathcal{U}$ with probability almost 1 assuming $\#\mathcal{U} \leq 2, p_1 \leq \frac{1}{2^{2n}}$, sufficient large n and m-qubit quantum implementation of test$(\cdot)$.

2) Simon's algorithm. Let $f : \{0,1\}^n \rightarrow \{0,1\}^n$ be a boolean function. We call f as a *periodic function* if there is a unique $s \in \{0,1\}^n \backslash \{0^n\}$ such that $f(x) = f(x \oplus s)$ for all $x \in \{0,1\}^n$. Classically, we can find out the period of a periodic function by searching collisions with $\mathcal{O}(2^{n/2})$ queries. However, in the $Q2$ model Simon's algorithm [34] can reduce the queries rapidly to only polynomial times and find the period as well, which is shown in theorem 2.

Theorem 2. ([23]) *Let $f : \{0,1\}^n \to \{0,1\}^n$ be a periodic function with a period s and*

$$\varepsilon(f) := \max_{t \in \{0,1\}^n \backslash \{0^n, s\}} \Pr_x[f(x) = f(x \oplus t)].$$

Then Simon's algorithm with $\mathcal{O}(n)$ quantum queries to f using $\mathcal{O}(n)$ qubits can recover s with probability almost 1 assuming $\varepsilon(f) \leq 1/2$.

Remark 1. $\varepsilon(f)$ in theorem 2 quantifies the disturbance of other partial periods, i.e., $f(x) = f(x \oplus t)$ where $t \in \{0,1\}^n \backslash \{0^n, s\}$.

3) Grover-meet-Simon Algorithm. In 2017 Leander and May [25] combined Grover's algorithm with Simon's algorithm to recover the keys of FX construction. They named their technique as Grover-meet-Simon algorithm. Paper [8,20] considered the universal case. In short, this algorithm can find a u in a special set $\mathcal{U}$ by quering function $f(u,x)$, where $f(u,\cdot)$ is periodic function for $u \in \mathcal{U}$ but for other us it doesn't hold with some probability. The main idea of the algorithm is to search $u \in \mathcal{U}$ by Grover's algorithm and check whether or not $u \in \mathcal{U}$ by whether $f(u,\cdot)$ is periodic or not, which can be implemented by Simon's algorithm. The formalization is in theorem 3.

Theorem 3. ([20]) *Let set $\mathcal{U} \subseteq \{0,1\}^n$ and $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ be a function who satisfies*

$$\begin{cases} f(u,\cdot) \text{ is a period function with period } s_u, & u \in \mathcal{U}, \\ f(u,\cdot) \text{ is not a periodic function}, & u \notin \mathcal{U}. \end{cases}$$

Let $\mathcal{U}_s := \{(u, s_u) : u \in \mathcal{U}, s_u$ is the period of $f(u,\cdot)\}$, and

$$\varepsilon(f) := \max_{(u,t) \in \{0,1\}^m \times \{0,1\}^n \backslash (\mathcal{U}_s \cup \{0,1\}^m \times \{0^n\})} \Pr_x[f(u,x) = f(u, x \oplus t)].$$

Then Grover-meet-Simon algorithm with $\mathcal{O}(2^{n/2}n)$ quantum queries to f using $\mathcal{O}(n^2)$ qubits will output a tuple $(u, s_u) \in \mathcal{U}_s$ with probability almost 1 assuming $\varepsilon(f) \leq 7/8, \#\mathcal{U} \leq 2$ and sufficient large n.

Remark 2. $\varepsilon(f)$ in theorem 3 is to quantify the disturbance of $u \notin \mathcal{U}$ and other partial periods ts for $u \in \mathcal{U}$, i.e., $f(u,x) = f(u, x \oplus t)$ where $(u,t) \in \{0,1\}^m \times \{0,1\}^n \backslash (\mathcal{U}_s \cup \{0,1\}^m \times \{0^n\})$.

3 Attack on Function with One Permutation Call

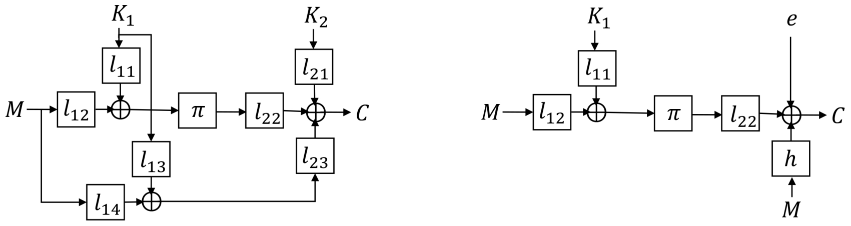
We will show that any function that makes only one public random permutation call and has linear pre- and post-processing functions of the permutation only is not secure with polynomial queries in the $Q2$ model. Let $M, C \in \{0,1\}^n$ and K_1, K_2 be two independent keys in $\{0,1\}^n$. Let π be a public random permutation, $L_1 : (\{0,1\}^n)^2 \to (\{0,1\}^n)^2$ and $L_2 : (\{0,1\}^n)^3 \to \{0,1\}^n$ be any two linear mappings. Then we let $F1 : \{0,1\}^{2n} \times \{0,1\}^n \to \{0,1\}^n$ be the general function using keys K_1, K_2 with input M and output C. And it makes one call to public random permutation π and has the pre- and post-linear mapping L_1, L_2. See $F1$ in Fig.1(b).

Theorem 4. *Let $n \in \mathbb{N}$, and consider the function $F1 : \{0,1\}^{2n} \times \{0,1\}^n \to \{0,1\}^n$ of Fig.1(b) based on a public random permutation π with block length of n bits and using two keys $K_1, K_2 \xleftarrow{\$} \{0,1\}^n$, for any linear mappings L_1, L_2. There exists a distinguisher $\mathcal{D}$ making at most $\mathcal{O}(n)$ construction queries and at most $\mathcal{O}(n)$ primitive queries to distinguish $F1$ from random oracle with probability almost 1.*

Proof. Firstly, we decompose $L_1 = (l_{11}, l_{12}, l_{13}, l_{14}), L_2 = (l_{21}, l_{22}, l_{23})$ such that $L_1(K_1, M) = (l_{11}(K_1) \oplus l_{12}(M), l_{13}(K_1) \oplus l_{14}(M))$, $L_2(K_2, y, z) = l_{21}(K_2) \oplus l_{22}(y) \oplus l_{23}(z)$, where every sub linear mapping l_{ij} maps $\{0,1\}^n \to \{0,1\}^n$. The function $F1$ after decomposition is in Fig.3(a). Then we can distinguish $(F1, \pi)$ from (ρ, π) by considering these sub mappings in three cases, which cover all scenarios. In the case 1), 2), and 3.1), we refer to the attack in [13] to distinguish $F1$ from random function just by $\mathcal{O}(1)$ classical queries. The subcase 3.2) is a bit more complicated. However, we can still attack it by constructing a periodic function and applying Simon's algorithm to recover the secret period of $F1$, which leads to distinguishing attack as well. Let e denote a value only related to keys. And $h(M)$ denotes a function which can been calculated by public functions or primitive queries with M. For simplicity, then we can write function $F1$ as:

$$F1(M) = l_{22}\pi(l_{12}(M) \oplus l_{11}(K_1)) \oplus h(M) \oplus e,$$

where here $e = l_{23}l_{13}(K_1)$ and $h(M) = l_{23}l_{14}(M)$. See Fig.3(b).



(a) The decomposition of function $F1$ by $L_1 = (l_{11}, l_{12}, l_{13}, l_{14})$ and $L_2 = (l_{21}, l_{22}, l_{23})$.

(b) The simple form of function $F1$ after decomposition.

Fig. 3. The decomposition of function $F1$.

Case 1) $\boldsymbol{l_{22} = O}$. When $l_{22} = O$, the output of the permutation π is not related to C. That is to say, $F1(M) = h(M) \oplus e$. We select arbitrary two different messages M and M' and query the construction oracle with them to get answers C and C'. If the function is $F1$, then $C' \oplus C = h(M) \oplus h(M')$. However, for random function it holds with negligible probability. So we distinguish them.

Case 2) $\boldsymbol{l_{11}(K_1) = 0^n}$. In this case, the input of the function π is independent of the key K_1. We select arbitrary two different messages M and M' and query the construction oracle with them to get answers C and C'. Then we distinguish $F1$ from random function by whether or not $C' \oplus C = l_{22}\pi(l_{12}(M)) \oplus l_{22}\pi(l_{12}(M')) \oplus h(M) \oplus h(M')$.

Case 3) $\boldsymbol{l_{22} \neq O, l_{11}(K_1) \neq 0^n}$.

Subcase 3.1) $\boldsymbol{l_{12}}$ is irreversible. Firstly, we find two different M and M' who satisfies $l_{12}(M) = l_{12}(M')$. Then we query the construction oracle with them to obtain C and C'. And we can distinguish $F1$ from random function by whether or not $C' \oplus C = h(M) \oplus h(M')$.

Subcase 3.2) $\boldsymbol{l_{12}}$ is reversible. We let

$$\begin{aligned} f(M) :=& F1(M) \oplus h(M) \oplus l_{22}\pi(l_{12}(M)) \\ =& l_{22}\pi(l_{12}(M) \oplus l_{11}(K_1)) \oplus l_{22}\pi(l_{12}(M)) \oplus e. \end{aligned}$$

Given the quantum oracle of $F1$ and π, we can get the quantum oracle of f referring to paper [23]. It is easily to obtain $f(M) = f(M \oplus l_{12}^{-1} l_{11}(K_1))$ for all M. That is to say, f is a periodic function with period $s := l_{12}^{-1}(l_{11}(K_1))$. If $\varepsilon(f) \leq 1/2$, then by theorem 2, Simon's algorithm can find the period with $\mathcal{O}(n)$ quantum queries to $F1$ and π using $\mathcal{O}(n)$ qubits. We put the proof of $\varepsilon(f) \leq 1/2$ in Appendix A. After recovering s, query the construction oracle with any $M, M \oplus s$ to get responds C, C' and query $l_{22}\pi(\cdot)$ with $l_{12}(M), l_{12}(M \oplus s)$ to get responses y, y'. Then $C' \oplus C = h(M) \oplus y \oplus h(M \oplus s) \oplus y'$. Instead, if the adversary is given quantum access to random function ρ and permutation π, it doesn't hold. Because Simon's algorithm will output a random value after querying random function. So we distinguish them. The method can be applied to EM construction. □

4 Pseudorandom Function with Two Permutation Calls

We will show that any pseudorandom function that makes two serial (see Fig.1(d)) or parallel (see Fig.1(c)) public permutation calls and every permutation has linear pre- and post-processing functions is not secure with $\mathcal{O}(2^{n/2}n)$ queries in the $Q2$ model by applying Grover-meet-Simon algorithm. In section 5, the method applies to EDM [15], EDMD [27] and Xop [3] constructions instantiated with EM construction [17], and concrete schemes DS-SoEM [6], PDMMAC [12] and pEDM [16].

4.1 Attack on Pseudorandom Function with Two Parallel Permutation Calls

Let $\pi_1, \pi_2 \in \mathrm{Perm}(n)$ and K_1, K_2, K_3, K_4 are four independent keys in $\{0,1\}^n$. Let $L_1 : (\{0,1\}^n)^2 \to (\{0,1\}^n)^2, L_2 : (\{0,1\}^n)^2 \to (\{0,1\}^n)^2, L_3 : (\{0,1\}^n)^6 \to \{0,1\}^n$ be any three linear mappings. Then let the general function $F2 : \{0,1\}^{4n} \times \{0,1\}^n \to \{0,1\}^n$ based on two parallel public permutation calls be defined as Fig.1(c).

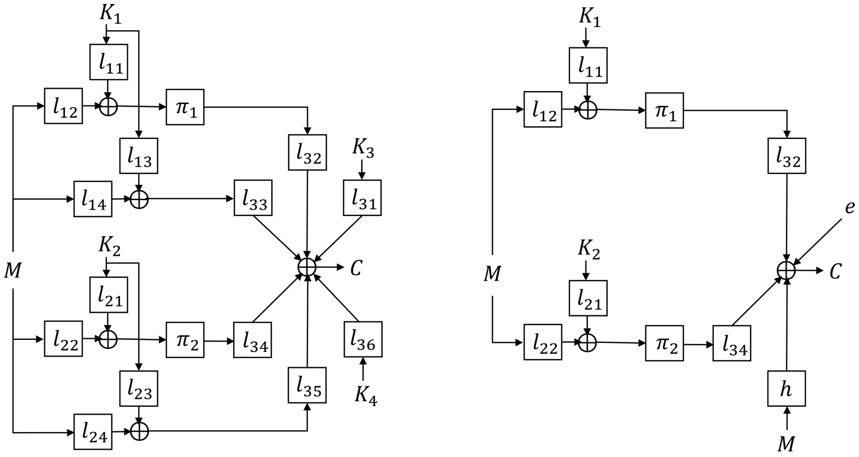
Theorem 5. *Let $n \in \mathbb{N}$, and consider the function $F2 : \{0,1\}^{4n} \times \{0,1\}^n \to \{0,1\}^n$ of Fig.1(c) based on public random permutations π_1 and π_2 with block length of n bits and using four keys $K_1, K_2, K_3, K_4 \overset{\$}{\leftarrow} \{0,1\}^n$, for any linear mapplings L_1, L_2, L_3. There exists a distinguisher $\mathcal{D}$ making at most $\mathcal{O}(2^{n/2}n)$*

construction queries and at most $\mathcal{O}(2^{n/2}n)$ primitive queries to distinguish $F2$ from random oracle with probability almost 1.

Proof. Firstly, we decompose L_1, L_2, L_3 into $L_1 = (l_{11}, l_{12}, l_{13}, l_{14})$, $L_2 = (l_{21}, l_{22}, l_{23}, l_{24})$, $L_3 = (l_{31}, l_{32}, l_{33}, l_{34}, l_{35}, l_{36})$ as in Fig.4(a), where every sub linear mapping $l_{ij} : \{0,1\}^n \to \{0,1\}^n$. Then we will attack the decomposition form of $F2$. We consider four cases as follows, which cover all scenarios. Let e denote a value only related to keys. And $h(M)$ denotes a function which can been calculated by public functions or primitive queries with M. For simplicity, then we can write

$$F2(M) = l_{32}\pi_1(l_{12}(M) \oplus l_{11}(K_1)) \oplus l_{34}\pi_2(l_{22}(M) \oplus l_{21}(K_2)) \oplus h(M) \oplus e,$$

where here $h(M) = l_{33}l_{14}(M) \oplus l_{35}l_{24}(M)$ and $e = l_{31}(K_1) \oplus l_{36}(K_4) \oplus l_{35}l_{23}(K_2) \oplus l_{33}l_{13}(K_1)$. See Fig.4(b).



(a) The decomposition of function $F2$ by $L_1 = (l_{11}, l_{12}, l_{13}, l_{14}), L_2 = (l_{21}, l_{22}, l_{23}, l_{24})$ and $L_3 = (l_{31}, l_{32}, l_{33}, l_{34}, l_{35}, l_{36})$.

(b) The simple form of function $F2$ after decomposition.

Fig. 4. The decomposition of function $F2$.

Case 1) $\boldsymbol{l_{32} = O}$ or $\boldsymbol{l_{34} = O}$. Take $l_{32} = O$ as an example. Now

$$F2(M) = l_{34}\pi_2(l_{22}(M) \oplus l_{21}(K_2)) \oplus h(M) \oplus e,$$

which degenerates into $F1$. By theorem 4 there exists a distinguisher making at most $\mathcal{O}(n)$ construction queries and at most $\mathcal{O}(n)$ primitive queries to distinguish it from random oracle.

Case 2) $\boldsymbol{l_{12} = O}$ or $\boldsymbol{l_{22} = O}$. Take $l_{12} = O$ as an example. Now

$$F2(M) = l_{34}\pi_2(l_{22}(M) \oplus l_{21}(K_2)) \oplus h(M) \oplus e \oplus l_{32}\pi_1(l_{11}(K_1)),$$

which degenerates into $F1$, too.

Case 3) $\boldsymbol{l_{11}(K_1) = 0^n}$ or $\boldsymbol{l_{21}(K_2) = 0^n}$. Take $l_{11}(K_1) = 0^n$ as an example. Now

$$F2(M) = l_{34}\pi_2(l_{22}(M) \oplus l_{21}(K_2)) \oplus h(M) \oplus l_{32}\pi_1(l_{12}(M)) \oplus e,$$

which degenerates into $F1$, too.

Case 4) $\boldsymbol{l_{32} \neq O, l_{12} \neq O, l_{34} \neq O, l_{22} \neq O, l_{11}(K_1) \neq 0^n, l_{21}(K_2) \neq 0^n}$.

Subcase 4.1) $\boldsymbol{l_{12}}$ is irreversible or $\boldsymbol{l_{22}}$ is irreversible. We take l_{12} is irreversible as an example.

If there are two different M and M' such that $l_{12}(M) = l_{12}(M')$ and $l_{22}(M) = l_{22}(M')$, we query the construction oracle with M and M' to obtain C and C'. Then we can distinguish $F2$ from random function by whether or not $C \oplus C' = h(M) \oplus h(M')$.

If there are no two different M and M' such that $l_{12}(M) = l_{12}(M')$ and $l_{22}(M) = l_{22}(M')$, no nonzero element of the kernel of linear mapping l_{22} (resp.l_{12}) belongs to the kernel of l_{12} (resp.l_{22}). Fix an arbitrary nonzero element a of the kernel of l_{12} and any M. Then $l_{12}(M) = l_{12}(M \oplus a)$ and $l_{22}(M) \oplus l_{22}(M \oplus a) = l_{22}(a)(\neq 0^n)$ hold. Assume the size of the kernel of l_{12} (resp. l_{22}) is r (resp. x), then linear mapping l_{12} (resp. l_{22}) has $2^n/r$ (resp. $2^n/x$) different images and every image of l_{12} (resp. l_{22}) has r (resp. x) pre-images. By there being no two different M and M' such that $l_{12}(M) = l_{12}(M')$ and $l_{22}(M) = l_{22}(M')$, we get every different pre-images corresponding to the same image of l_{12} (resp. l_{22}) correspond to different images of l_{22} (resp. l_{12}), which leads $r \leq 2^n/x$ (resp. $x \leq 2^n/r$). Thus $\max\{2^n/x, 2^n/r\} \geq 2^{n/2}$, which means the larger size of the images of l_{12}, l_{22} is at least $2^{n/2}$. Assume the image size of l_{22} is larger than l_{21}. Under this assumption there exist the following attack, or there exist another similar attack as well. Let

$$\begin{aligned} f(u) :=& F2(M) \oplus h(M) \oplus F2(M \oplus a) \oplus h(M \oplus a) \oplus \\ & l_{34}\pi_2(l_{22}(M) \oplus u) \oplus l_{34}\pi_2(l_{22}(M \oplus a) \oplus u). \\ =& l_{34}\pi_2(l_{22}(M) \oplus l_{21}(K_2)) \oplus l_{34}\pi_2(l_{22}(M \oplus a) \oplus l_{21}(K_2)) \oplus \\ & l_{34}\pi_2(l_{22}(M) \oplus u) \oplus l_{34}\pi_2(l_{22}(M \oplus a) \oplus u) \end{aligned}$$

Let $\mathcal{U} := \{l_{21}(K_2), l_{21}(K_2) \oplus l_{22}(a)\}$. It is easy to obtain when $u \in \mathcal{U}$, $f(u) = 0^n$ for all $M \in \{0,1\}^n$. So we try to search an $u \in \mathcal{U}$ by Grover's algorithm through defining a *test* function, which filters $u \in \mathcal{U}$ from all us by whether or not $f(u) = 0^n$. Firstly, fix $\mathcal{M} := \{M_1, M_2, \ldots, M_q\}$ which satisfies for any M_i that $l_{22}(M_i), l_{22}(M_i \oplus a) \notin \{l_{22}(M_j), l_{22}(M_j \oplus a) | M_j \in \mathcal{M} \backslash \{M_i\}\}$. Secondly, calculate $b_i := F2(M_i) \oplus h(M_i) \oplus F2(M_i \oplus a) \oplus h(M_i \oplus a)$ for $i = 1, \ldots, q$ through querying $F2$. Then let $test : \{0,1\}^n \to \{0,1\}$ be

$$test(u) = \begin{cases} 1, \text{if } b_i = l_{34}\pi_2(l_{22}(M_i) \oplus u) \oplus l_{34}\pi_2(l_{22}(M_i \oplus a) \oplus u) & i = 1, \ldots, q, \\ 0, \text{otherwise}. \end{cases}$$

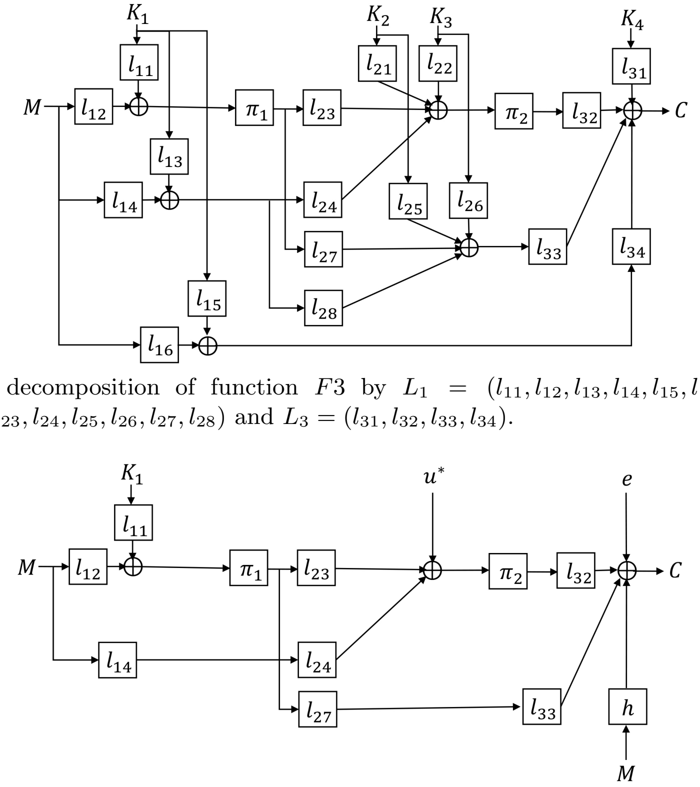
It is easy to obtain that $test(u) = 1$ for any $u \in \mathcal{U}$. If $\Pr[test(u) = 1] \leq \frac{1}{2^{2n}}$ holds for any $u \notin \mathcal{U}$, then we can recovery an $u \in \mathcal{U}$ by theorem 1. We prove $\Pr[test(u) = 1] \leq \frac{1}{2^{2n}}$ for any $u \notin \mathcal{U}$ when $q \geq 4n$ in Appendix B. After recovering a $u \in \mathcal{U}$, for a fixed $M \in \{0,1\}^n \backslash \mathcal{M}$ we check whether $F2(M) \oplus h(M) \oplus F2(M \oplus a) \oplus h(M \oplus a) \oplus l_{34}\pi_2(l_{22}(M) \oplus u) \oplus l_{34}\pi_2(l_{22}(M \oplus a) \oplus u) = 0^n$ or not by $\mathcal{O}(1)$ classical queries to $F2$ and π_2. It holds beyond doubt. However, if we replace the construction function from $F2$ to a random function, it happens with negligible probability. Thus we distinguish $F2$ from the random function.

Subcase 4.2) l_{12}, l_{22} are reversible. Because π_1 and π_2 are two independent random permutations, so $\pi_1 = \pi_2$ with negligible probability. We only consider $\pi_1 \neq \pi_2$. We let

$$\begin{aligned} f(u,M) :=& F3(M) \oplus h(M) \oplus l_{34}\pi_2(l_{22}(M) \oplus u) \oplus l_{32}\pi_1(l_{12}(M)) \\ =& l_{34}\pi_2(l_{22}(M) \oplus l_{21}(K_2)) \oplus l_{32}\pi_1(l_{12}(M) \oplus l_{11}(K_1)) \oplus \\ & l_{34}\pi_2(l_{22}(M) \oplus u) \oplus l_{32}\pi_1(l_{12}(M)) \oplus e. \end{aligned}$$

Let $\mathcal{U} := \{l_{21}(K_2), l_{22}l_{12}^{-1}l_{11}(K_1) \oplus l_{21}(K_2)\}$ and $s := l_{12}^{-1}l_{11}(K_1)$. It is easy to get when $u \in \mathcal{U}$, $f(u,M) = f(u, M \oplus s)$ holds for all M. Thus if $\varepsilon(f) \leq 7/8$, then by theorem 3 Grover-meet-Simon algorithm can recover an $u \in \mathcal{U}$ and s with $\mathcal{O}(2^{n/2}n)$ quantum queries to f. After that, we can distinguish $F2$ from random function. We put the proof of $\varepsilon(f) \leq 7/8$ in Appendix C. □

4.2 Attack on Pseudorandom Function with Two Serial Permutation Calls



(a) The decomposition of function $F3$ by $L_1 = (l_{11}, l_{12}, l_{13}, l_{14}, l_{15}, l_{16}), L_2 = (l_{21}, l_{22}, l_{23}, l_{24}, l_{25}, l_{26}, l_{27}, l_{28})$ and $L_3 = (l_{31}, l_{32}, l_{33}, l_{34})$.

(b) The simple form of function $F3$ after decomposition.

Fig. 5. The decomposition of function $F3$.

Let $\pi_1, \pi_2 \xleftarrow{\$} \mathrm{Perm}(n)$ and K_1, K_2, K_3, K_4 are four independent keys in $\{0,1\}^n$. Let $L_1 : (\{0,1\}^n)^2 \to (\{0,1\}^n)^3, L_2 : (\{0,1\}^n)^4 \to (\{0,1\}^n)^2, L_3 : (\{0,1\}^n)^4 \to$

$\{0,1\}^n$ be any three linear mappings. And let the general function $F3 : \{0,1\}^{4n} \times \{0,1\}^n \to \{0,1\}^n$ based on two serial public permutation calls be defined as in Fig.1(d). Similar to $F1$ and $F2$, we can decompose L_1, L_2, L_3 into $L_1 = (l_{11}, l_{12}, l_{13}, l_{14}, l_{15}, l_{16})$, $L_2 = (l_{21}, l_{22}, l_{23}, l_{24}, l_{25}, l_{26}, l_{27}, l_{28})$, $L_3 = (l_{31}, l_{32}, l_{33}, l_{34})$ as in Fig.5(a), where every sub linear mapping $l_{ij} : \{0,1\}^n \to \{0,1\}^n$. For whether general or concrete instantiations of $F3$ in section 5, l_{12} is identical mappling. Thus for $l_{12} \neq O$, we only consider l_{12} is reversible.

Theorem 6. *Let $n \in \mathbb{N}$, and consider the function $F3 : \{0,1\}^{4n} \times \{0,1\}^n \to \{0,1\}^n$ of Fig.1(d) based on two public random permutation π_1 and π_2 with block length of n bits and using four keys K_1, K_2, $K_3, K_4 \xleftarrow{\$} \{0,1\}^n$, for any linear mapplings L_1, L_2, L_3 where $l_{12} = O$ or reversible. There exists a distinguisher $\mathcal{D}$ making at most $\mathcal{O}(2^{n/2}n)$ construction queries and at most $\mathcal{O}(2^{n/2}n)$ primitive queries to distinguish $F3$ from random oracle with probability almost 1.*

Proof. For simplicity, we let $h(M) := l_{33}l_{28}l_{14}(M) \oplus l_{34}l_{16}(M), e := l_{33}(l_{28}l_{13}(K_1) \oplus l_{25}(K_2) \oplus l_{26}(K_3)) \oplus l_{31}(K_4) \oplus l_{34}l_{15}(K_1), u^* := l_{21}\,(K_2) \oplus l_{22}\,(K_3) \oplus l_{24}l_{13}(K_1)$. Then

$$\begin{aligned} F3(M) =& l_{32}\pi_2(l_{23}\pi_1(l_{12}(M) \oplus l_{11}(K_1)) \oplus l_{24}l_{14}(M) \oplus u^*) \oplus \\ & l_{33}l_{27}\pi_1(l_{12}(M) \oplus l_{11}(K_1)) \oplus h(M) \oplus e. \end{aligned}$$

See Fig.5(b). We will attack $F3$ by attacking four cases as follows.

Case 1) $\boldsymbol{l_{32} = O}$. In this case,

$$F3(M) = l_{33}l_{27}\pi_1(l_{12}(M) \oplus l_{11}(K_1)) \oplus h(M) \oplus e,$$

which degenerates into $F1$.

Case 2) $\boldsymbol{l_{12} = O}$. In this case,

$$F3(M) = l_{32}\pi_2(l_{23}\pi_1(l_{11}(K_1)) \oplus l_{24}l_{14}(M) \oplus u^*) \oplus h(M) \oplus e \oplus l_{33}l_{27}\pi_1(l_{11}(K_1)),$$

which degenerates into $F1$, too.

Case 3) $\boldsymbol{l_{23} = O}$. In this case,

$$F3(M) = l_{32}\pi_2(l_{24}l_{14}(M) \oplus u^*) \oplus l_{33}l_{27}\pi_1(l_{12}(M) \oplus l_{11}(K_1)) \oplus h(M) \oplus e,$$

which degenerates into $F2$.

Case 4) $\boldsymbol{l_{32} \neq O, l_{12} \neq O, l_{23} \neq O}$. In this case, l_{12} is reversible. Let $u^{**} := u^* \oplus l_{24}l_{14}l_{12}^{-1}l_{11}\,(K_1)\,, g(u,x) := l_{32}\pi_2\left(l_{23}\pi_1(x) \oplus l_{24}l_{14}l_{12}^{-1}(x) \oplus u\right) \oplus l_{33}l_{27}\pi_1(x)$. Then

$$F3(M) = g(u^{**}, l_{12}(M) \oplus l_{11}(K_1)) \oplus h(M) \oplus e.$$

Let

$$\begin{aligned} f(u,M) :=& F3(M) \oplus h(M) \oplus g(u, l_{12}(M)) \\ =& g(u^{**}, l_{12}(M) \oplus l_{11}(K_1)) \oplus g(u, l_{12}(M)) \oplus e. \end{aligned}$$

Then it is easy to get when $u = u^{**}, f(u^{**}, M) = f(u^{**}, M \oplus s)$ holds for all $M \in \{0,1\}^n$ where $s := l_{12}^{-1}l_{11}(K_1)$. Thus if $\varepsilon(f) \leq 7/8$, then by theorem 3 Grover-meet-Simon algorithm can recover an u^{**} and s with $\mathcal{O}(2^{n/2}n)$ quantum queries to f. We put the proof of $\varepsilon(f) \leq 7/8$ in Appendix D. After that, we can distinguish $F3$ from random function. □

5 Instantiation

In this section, we show the security of general and some concrete instantiations of $F2$ and $F3$. In the following, we always assume $K_1, K_2, K_3, K_4 \overset{\$}{\leftarrow} \{0,1\}^n$ and $\pi_1, \pi_2 \overset{\$}{\leftarrow} \mathrm{Perm}(n)$. For the reason that $K_i = 0^n$ happens with negligible probability, we assume $K_i \neq 0^n$ for $i = 1, 2, 3, 4$. And we only put the key recovery methods of concrete functions. After recovery the distinguishing attacks from random function are similar as $F2, F3$, so we omit them.

5.1 Xop construction instantiated with EM construction

We instantiate Xop construction by replacing two block ciphers with two EM constructions $\mathrm{EM}(x) = \pi_1(x \oplus K_1) \oplus K_2$ and $\mathrm{EM}(x) = \pi_2(x \oplus K_3) \oplus K_4$, and get

$$\mathrm{XopEM}(M) = \pi_1(M \oplus K_1) \oplus \pi_2(M \oplus K_2) \oplus K_3 \oplus K_4.$$

It is a general instantiation of $F2$. Thus we can recover K_1, K_2 by applying Grover-meet-Simon algorithm with $\mathcal{O}(2^{n/2}n)$ queries using $\mathcal{O}(n^2)$ qubits when considering function

$$f(u, M) = \mathrm{XopEM}(M) \oplus \pi_1(M) \oplus \pi_2(M \oplus u),$$

which has a period K_1 in its second component when $u = K_1 \oplus K_2$ or K_2.

DS-SoEM. For message $M \in \{0,1\}^{n-d}$, 'msb$_{n-d}$' means the truncation of key masks at the input to their $n - b$ most significant bits. Bhattarcharjee et al. [6] defined

$$\begin{aligned}\text{DS-SoEM}(M) =&\pi_1((M \oplus \mathrm{msb}_{n-d}(K_1))\|0^d)\oplus\\ &\pi_1((M \oplus \mathrm{msb}_{n-d}(K_2))\|1^d) \oplus K_1 \oplus K_2.\end{aligned}$$

It is a concrete variant of the instantiation of Xop. We can recover $\mathrm{msb}_{n-d}(K_1)$, $\mathrm{msb}_{n-d}(K_2)$ by applying Grover-meet-Simon algorithm with $\mathcal{O}(2^{\frac{n-d}{2}}(n-d))$ queries using $\mathcal{O}(n^2)$ qubits when considering function

$$f(u, M) = \text{DS-SoEM}(M) \oplus \pi_1(M\|0^d) \oplus \pi_1((M \oplus u)\|1^d),$$

which has a period $\mathrm{msb}_{n-d}(K_1)$ in its second component when $u = \mathrm{msb}_{n-d}(K_1 \oplus K_2)$ or $\mathrm{msb}_{n-d}(K_2)$.

5.2 EDM construction instantiated with EM construction

We can instantiate EDM construction with two EM construction and get

$$\mathrm{EDMEM}(M) = \pi_2(\pi_1(M \oplus K_1) \oplus M \oplus K_2 \oplus K_3) \oplus K_4.$$

It is a general instantiation of $F3$. We can recover $K_1, K_2 \oplus K_3$ by applying Grover-meet-Simon algorithm with $\mathcal{O}(2^{n/2}n)$ queries using $\mathcal{O}(n^2)$ qubits when considering function

$$f(u, M) = \mathrm{EDMEM}(M) \oplus \pi_2(\pi_1(M) \oplus M \oplus u),$$

which has a period K_1 in its second component when $u = K_1 \oplus K_2 \oplus K_3$.

PDMMAC. Chakraborti et al. [12] defined

$$\mathrm{PDMMAC}(M) = \pi_1^{-1}(\pi_1(M \oplus K_1) \oplus M \oplus K_1 \oplus 2K_1) \oplus 2K_1.$$

It is a concrete instantiation of EDM. Although we can apply Grover-meet-Simon algorithm to attack it with $\mathcal{O}(2^{n/2}n)$ queries using $\mathcal{O}(n^2)$ qubits as EDMEM. However, here it is easier to search K_1 straightforwardly by Grover's search, which costs $\mathcal{O}(2^{n/2})$ queries to π_1, π_1^{-1}, $\mathcal{O}(n)$ queries to PDMMAC and $\mathcal{O}(n)$ qubits.

pEDM. Dutta et al [16] defined

$$\mathrm{pEDM}(M) = \pi_1(\pi_1(M \oplus K_1) \oplus M \oplus K_1 \oplus K_2) \oplus K_1.$$

It is a concrete instantiation of EDM. We apply Grover-meet-Simon algorithm to attack it with $\mathcal{O}(2^{n/2}n)$ queries to pEDM and π using $\mathcal{O}(n^2)$ qubits when considering function

$$f(u, M) = \mathrm{pEDM}(M) \oplus \pi_1(\pi_1(M) \oplus M \oplus u),$$

which has a period K_1 in its second component when $u = K_2$.

5.3 EDMD construction instantiated with EM construction

We instantiate EDMD construction with EM construction and get

$$\mathrm{EDMDEM}(M) = \pi_2(\pi_1(M \oplus K_1) \oplus K_2 \oplus K_3) \oplus \pi_1(M \oplus K_1) \oplus K_2 \oplus K_4.$$

It is a general instantiation of $F3$. We can recover $K_1, K_2 \oplus K_3$ by applying Grover-meet-Simon algorithm with $\mathcal{O}(2^{n/2}n)$ queries using $\mathcal{O}(n^2)$ qubits when considering function

$$f(u, M) = \mathrm{EDMDEM}(M) \oplus \pi_2(\pi_1(M) \oplus u) \oplus \pi_1(M),$$

which has a period K_1 in its second component when $u = K_2 \oplus K_3$.

SoKAC21. SoKAC21 [13] is as follows:

$$\mathrm{SoKAC21}(M) = \pi_2(\pi_1(M \oplus K_1) \oplus K_1) \oplus \pi_1(M \oplus K_1) \oplus K_1.$$

It is a concrete instantiation of EDMD. It is well known that BHT algorithm [11] is a time-memory trade-off algorithm of Grover's algorithm. By applying this algorithm to speed up the birthday bound classical attack [28] by Nandi, we can distinguish it from random function with $\mathcal{O}(2^{n/3})$ quantum queries.

6 Conclusion

In this paper, we systematically analyze the security of PRFs based on one or two public random permutation calls with pre- and post-linear processes of each permutation in the $Q2$ model. Besides, we present the security of some popular instantiations: contain general instantiations (XopEM, EDMEM, EDMDEM)and concrete PRFs (DS-SoEM, PDMMAC, pEDM, SoKAC21). Notice that our attack for $F3$ in section 4.2 not include that case l_{12} irreversible. We find it is more complexity to find attack when l_{12} is irreversible for whatever other linear mapplings be. We leave it as an open problem. Generally, it is sufficient to consider $l_{12} = O$ or reversible with respect to existing instantiations.

The further question is if there is provable security in the $Q2$ model to show the tightness of the bound.

A Proof of $\varepsilon(f) \leq 1/2$ in Subcase 3.2) in Section 3

In fact, we can prove $\varepsilon(f)$ is at most $\frac{1}{2}$, i.e., for any $t \in \{0,1\}^n \backslash \{0^n, s\}$ that

$$\Pr_M \left[\begin{array}{c} l_{22}\pi(l_{12}(M) \oplus l_{11}(K_1)) \oplus l_{22}\pi(l_{12}(M)) \\ l_{22}\pi(l_{12}(M \oplus t) \oplus l_{11}(K_1)) \oplus l_{22}\pi(l_{12}(M \oplus t)) = 0^n \end{array} \right] \leq 1/2. \quad (1)$$

By $t \notin \{0^n, s\}$ we know the four inputs of $l_{22}\pi$, i.e., $l_{12}(M) \oplus l_{11}(K_1), l_{12}(M)$, $l_{12}(M \oplus t) \oplus l_{11}(K_1)$, and $l_{12}(M \oplus t)$, are different from each other. Then by the randomness of π, the four inputs of $l_{22}(\cdot)$ are four distinct random values in $\{0,1\}^n$. By $l_{22} \neq O$, we obtain the range of $l_{22}(\cdot)$ has at least two elements and the probability of $l_{22}(x) = y$ for any random $x \in \{0,1\}^n$ and y in the range is at most $\frac{1}{2}$. Thus the equation (1) happens with probability no more than $\frac{1}{2}$.

B Proof of $\Pr[test(u) = 1] \leq \frac{1}{2^{2n}}$ for Any $u \notin \mathcal{U}$ in Subcase 4.1) in Section 4.1

$$\begin{aligned} \text{Let } f_i(u) :=& F2(M_i) \oplus h(M_i) \oplus F2(M_i \oplus a) \oplus h(M_i \oplus a) \oplus l_{34}\pi_2(l_{22}(M_i) \oplus u) \oplus \\ & l_{34}\pi_2(l_{22}(M_i \oplus a) \oplus u) \\ =& l_{34}\pi_2(l_{22}(M_i) \oplus l_{21}(K_2)) \oplus l_{34}\pi_2(l_{22}(M_i \oplus a) \oplus l_{21}(K_2)) \oplus \\ & l_{34}\pi_2(l_{22}(M_i) \oplus u) \oplus l_{34}\pi_2(l_{22}(M_i \oplus a) \oplus u), \end{aligned}$$

and $y_i^1 := l_{22}(M_i) \oplus l_{21}(K_2), y_i^2 := l_{22}(M_i \oplus a) \oplus l_{21}(K_2), y_i^3 := l_{22}(M_i) \oplus u, y_i^4 := l_{22}(M_i \oplus a) \oplus u$, for $i = 1, 2, \ldots, q$. By $l_{22}(a) \neq 0^n, u \notin \mathcal{U}$ we get for any function f_i, the y_i^1, y_i^2, y_i^3, and y_i^4 are different from each other. To calculate the probability of these q equations $f_i(u) = 0^n$ where $u \notin \mathcal{U}$, we consider sampling about π_2. If y_i^1, y_i^2, y_i^3, and y_i^4, who are the inputs of π_2 in ith equation, all have appeared in the other $q-1$ equations, then we don't sample in the ith equation. By any M_i that $l_{22}(M_i), l_{22}(M_i \oplus a) \notin \{l_{22}(M_j), l_{22}(M_j \oplus a) : M_j \in \mathcal{M} \setminus \{M_i\}\}$, we get $y_i^1, y_i^2 \notin \{y_j^1, y_j^2 : j \in \{1, 2, \ldots, q\} \setminus \{i\}\}$. However, if $u = l_{22}(M_i) \oplus l_{22}(M_j) \oplus l_{21}(K_2)$ then $y_i^1 = y_j^3, y_i^2 = y_j^4, y_i^3 = y_j^1, y_i^4 = y_j^2$. Or if $u = l_{22}(M_i) \oplus l_{22}(M_j) \oplus l_{21}(K_2) \oplus l_{22}(a)$ then $y_i^1 = y_j^4, y_i^2 = y_j^3, y_i^3 = y_j^2, y_i^4 = y_j^1$. Therefore, even in the worst case we have to sample π_2 in at least $\lfloor \frac{q}{2} \rfloor$ equations among q. For every equation needing sample, by the randomness of π_2, it holds with probability at most $\frac{1}{2}$. Therefore, for any $u \notin \mathcal{U}$, we have $\Pr[test(u) = 1] \leq (\frac{1}{2})^{\lfloor \frac{q}{2} \rfloor}$. We have $\Pr[test(u) = 1] \leq 1/2^{2n}$ for $q \geq 4n$. We notice that this attack requires l_{22} with at least $4n$ different images. When $4n \leq 2^{n/2}$, that is to say, $n \geq 6$, it works.

C Proof of $\varepsilon(f) \leq 7/8$ in Subcase 4.2) in Section 4.1

Let $\mathcal{U}_t = \{0,1\}^n \times \{0,1\}^n \backslash (\{(l_{21}(K_2), s), (l_{22}l_{12}^{-1}l_{11}(K_1) \oplus l_{21}(K_2), s)\} \cup \{0,1\}^n \times \{0^n\})$. In this case, $\varepsilon(f) = \max\limits_{(u,t)\in\mathcal{U}_t} \Pr_M[f(u,M) = f(u, M \oplus t)]$. The function $f(u,M) = f(u, M \oplus t)$ equals

$$\begin{array}{l} l_{34}\pi_2(l_{22}(M) \oplus l_{21}(K_2)) \oplus l_{34}\pi_2(l_{22}(M) \oplus u) \oplus \\ l_{34}\pi_2(l_{22}(M \oplus t) \oplus l_{21}(K_2)) \oplus l_{34}\pi_2(l_{22}(M \oplus t) \oplus u) \oplus \\ l_{32}\pi_1(l_{12}(M) \oplus l_{11}(K_1)) \oplus l_{32}\pi_1(l_{12}(M)) \oplus \\ l_{32}\pi_1(l_{12}(M \oplus t) \oplus l_{11}(K_1)) \oplus l_{32}\pi_1(l_{12}(M \oplus t)) = 0^n \end{array} \tag{2}$$

1) $u \in \mathcal{U}, t \notin \{0^n, s\}$. By $l_{11}(K_1) \neq 0^n, t \notin \{0^n, s\}$ we get the four inputs of $l_{32}\pi_1$ in equation (2) are different. By the randomness of π_1 the equation (2) holds with probability at most 1/2.

2) $u \notin \mathcal{U}, t = s$. Now the equation (2) equals

$$l_{34}\pi_2(l_{22}(M) \oplus l_{21}(K_2)) \oplus l_{34}\pi_2(l_{22}(M) \oplus u) \oplus$$

$$l_{34}\pi_2(l_{22}(M \oplus l_{12}^{-1}l_{11}(K_1)) \oplus l_{21}(K_2)) \oplus l_{34}\pi_2(l_{22}(M \oplus l_{12}^{-1}l_{11}(K_1)) \oplus u) = 0^n$$

By $u \notin \mathcal{U}, l_{22}l_{12}^{-1}l_{11}(K_1) \neq 0^n$, we get the four inputs of $l_{34}\pi_2$ in equation (2) are different. By the randomness of π_2 the equation (2) holds with probability at most 1/2.

3) $u \notin \mathcal{U}, t \notin \{0^n, s\}$. We can prove the equation (2) holds with probability at most 1/2 the same as 1), so we omit it.

D Proof of $\varepsilon(f) \leq 7/8$ in Case 4) of Section 4.2

Let $\mathcal{U}_t = \{0,1\}^n \times \{0,1\}^n \backslash (\{(u^{**}, s)\} \cup \{0,1\}^n \times \{0^n\})$. In this case, $\varepsilon(f) = \max\limits_{(u,t)\in\mathcal{U}_t} \Pr_M[f(u,M) = f(u, M \oplus t)]$. we take $l_{33}l_{27} = l_{24}l_{14} = O$ as an example. The other cases when $l_{33}l_{27} \neq O, l_{24}l_{14} \neq O$ are similar. We divide $(u,t) \in \mathcal{U}_t$ into the following cases, which cover all sceneries.

1) $u = u^{**}, t \notin \{0^n, s\}$. Now the equation $f(u,M) = f(u, M \oplus t)$ equals

$$l_{32}\pi_2(y_1) \oplus l_{32}\pi_2(y_2) \oplus l_{32}\pi_2(y_3) \oplus l_{32}\pi_2(y_4) = 0^n, \tag{3}$$

wherec $y_1 = l_{23}\pi_1(l_{12}(M) \oplus l_{11}(K_1)) \oplus u^{**}, y_2 = l_{23}\pi_1(l_{12}(M)) \oplus u^{**}$, $y_3 = l_{23}\pi_1(l_{12}(M \oplus t) \oplus l_{11}(K_1)) \oplus u^{**}, y_4 = l_{23}\pi_1(l_{12}(M \oplus t)) \oplus u^{**}$. If $y_1 = y_2, y_3 = y_4$ or $y_1 = y_3, y_2 = y_4$ or $y_1 = y_4, y_2 = y_3$, then equation (3) holds. We observe that four inputs of $l_{23}\pi_1$ in y_1, y_2, y_3, and y_4 are distinct from each other by $l_{11}(K_1) \neq 0^n$ and $t \notin \{0^n, s\}$. So this case happens with probability at most 3/4 by the randomness of π_1. Otherwise, there is at least one $y_i (i \in \{1,2,3,4\})$ is different from the other three. In this case, by the randomness of π_2, the equation (3) holds with probability at most 1/2. So the equation (3) holds with a bound $3/4 + 1/4 \cdot 1/2 = 7/8$.

2) $u \neq u^{**}, t = s$. Now the equation $f(u,M) = f(u, M \oplus t)$ is equal to

$$l_{32}\pi_2(y_1) \oplus l_{32}\pi_2(y_2) \oplus l_{32}\pi_2(y_3) \oplus l_{32}\pi_2(l_{23}\pi_1(y_4) = 0^n, \tag{4}$$

where $y_1 = l_{23}\pi_1(l_{12}(M) \oplus l_{11}(K_1)) \oplus u^{**}, y_2 = l_{23}\pi_1(l_{12}(M)) \oplus u, y_3 = l_{23}\pi_1(l_{12}(M)) \oplus u^{**}, y_4 = l_{23}\pi_1(l_{12}(M) \oplus l_{11}(K_1)) \oplus u$. By $u \neq u^{**}$, we get $y_1 \neq y_4$. And we observe that $[y_1 = y_2 \Leftrightarrow y_3 = y_4]$ (resp. $[y_1 = y_3 \Leftrightarrow y_2 = y_4]$). So $y_1 = y_2$ and $y_1 = y_3$ don't hold simultaneously, or it leads to $y_1 = y_4$. If $y_1 = y_2$, the equation (4) holds. This case holds with probability at most $1/2$ by the randomness of π_1. Otherwise, if $y_1 \neq y_2$ and $y_1 = y_3$, the equation (4) holds as well. This case holds with probability at most $1/2 \cdot 1/2 = 1/4$ by the randomness of π_1. At last, if $y_1 \neq y_2$ and $y_1 \neq y_3$, then y_1, y_2, y_3, and y_4 are different from each other, the equation (4) holds with probability of $1/2 \cdot 1/2 \cdot 1/2 = 1/8$ by the randomness of π_2. So the equation (4) holds with a bound $7/8$.

3) $\boldsymbol{u \neq u^{**}, t \notin \{0^n, s\}}$. This case is similar to 1), so we omit it.

References

1. Bellare, M., Desai, A., Jokipii, E., Rogaway, P.: A concrete security treatment of symmetric encryption. In: FOCS '97. pp. 394–403. IEEE Computer Society (1997), https://doi.org/10.1109/SFCS.1997.646128 1
2. Bellare, M., Impagliazzo, R.: A tool for obtaining tighter security analyses of pseudorandom function based constructions, with applications to PRP to PRF conversion. IACR Cryptol. ePrint Arch. **1999**, 24 (1999), http://eprint.iacr.org/1999/024 2
3. Bellare, M., Krovetz, T., Rogaway, P.: Luby-rackoff backwards: Increasing security by making block ciphers non-invertible. In: EUROCRYPT '98. vol. 1403, pp. 266–280. Springer (1998), https://doi.org/10.1007/BFb0054132 2, 9
4. Bellare, M., Rogaway, P.: The security of triple encryption and a framework for code-based game-playing proofs. In: EUROCRYPT 2006. vol. 4004, pp. 409–426. Springer (2006), https://doi.org/10.1007/11761679_25 1
5. Bernstein, D.J.: Stronger security bounds for wegman-carter-shoup authenticators. In: EUROCRYPT 2005. vol. 3494, pp. 164–180. Springer (2005), https://doi.org/10.1007/11426639_10 1
6. Bhattacharjee, A., List, E., Nandi, M.: CENCPP - beyond-birthday-secure encryption from public permutations. IACR Cryptol. ePrint Arch. **2020**, 602 (2020), https://eprint.iacr.org/2020/602 3, 5, 9, 14
7. Bogdanov, A., Knudsen, L.R., Leander, G., Standaert, F., Steinberger, J.P., Tischhauser, E.: Key-alternating ciphers in a provable setting: Encryption using a small number of public permutations - (extended abstract). In: EUROCRYPT 2012. vol. 7237, pp. 45–62. Springer (2012), https://doi.org/10.1007/978-3-642-29011-4_5 2
8. Bonnetain, X.: Tight bounds for simon's algorithm. In: LATINCRYPT 2021. vol. 12912, pp. 3–23. Springer (2021), https://doi.org/10.1007/978-3-030-88238-9_1 6, 7
9. Brassard, G.: On computationally secure authentication tags requiring short secret shared keys. In: CRYPTO '82. pp. 79–86. Plenum Press, New York (1982), https://doi.org/10.1007/978-1-4757-0602-4_7 1
10. Brassard, G., Hoyer, P., Mosca, M., Tapp, A.: Quantum amplitude amplification and estimation. Contemporary Mathematics **305**, 53–74 (2002) 6
11. Brassard, G., Hoyer, P., Tapp, A.: Quantum algorithm for the collision problem. arXiv preprint quant-ph/9705002 (1997) 15

12. Chakraborti, A., Nandi, M., Talnikar, S., Yasuda, K.: On the composition of single-keyed tweakable even-mansour for achieving BBB security. IACR Trans. Symmetric Cryptol. **2020**(2), 1–39 (2020), https://doi.org/10.13154/tosc.v2020.i2.1-39 3, 5, 9, 15
13. Chen, Y.L., Lambooij, E., Mennink, B.: How to build pseudorandom functions from public random permutations. In: CRYPTO 2019. vol. 11692, pp. 266–293. Springer (2019), https://doi.org/10.1007/978-3-030-26948-7_10 2, 3, 4, 5, 8, 15
14. Chen, Y.L., Mennink, B., Preneel, B.: Categorization of faulty nonce misuse resistant message authentication. In: ASIACRYPT 2021. vol. 13092, pp. 520–550. Springer (2021), https://doi.org/10.1007/978-3-030-92078-4_18 2
15. Cogliati, B., Seurin, Y.: EWCDM: an efficient, beyond-birthday secure, nonce-misuse resistant MAC. In: CRYPTO 2016. vol. 9814, pp. 121–149. Springer (2016), https://doi.org/10.1007/978-3-662-53018-4_5 2, 9
16. Dutta, A., Nandi, M., Talnikar, S.: Permutation based EDM: an inverse free BBB secure PRF. IACR Trans. Symmetric Cryptol. **2021**(2), 31–70 (2021), https://doi.org/10.46586/tosc.v2021.i2.31-70 3, 5, 9, 15
17. Even, S., Mansour, Y.: A construction of a cipher from a single pseudorandom permutation. J. Cryptol. **10**(3), 151–162 (1997), https://doi.org/10.1007/s001459900025 2, 9
18. Gilboa, S., Gueron, S.: The advantage of truncated permutations. CoRR **abs/1610.02518** (2016), http://arxiv.org/abs/1610.02518 2
19. 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, 1996. pp. 212–219 (1996), https://doi.org/10.1145/237814.237866 6
20. Guo, T., Wang, P., Hu, L., Ye, D.: Attacks on beyond-birthday-bound macs in the quantum setting. In: PQCrypto 2021. vol. 12841, pp. 421–441. Springer (2021), https://doi.org/10.1007/978-3-030-81293-5_22 6, 7
21. Hall, C., Wagner, D.A., Kelsey, J., Schneier, B.: Building prfs from prps. In: CRYPTO '98. vol. 1462, pp. 370–389. Springer (1998), https://doi.org/10.1007/BFb0055742 2
22. Impagliazzo, R., Rudich, S.: Limits on the provable consequences of one-way permutations. In: CRYPTO '88. vol. 403, pp. 8–26. Springer (1988), https://doi.org/10.1007/0-387-34799-2_2 1
23. Kaplan, M., Leurent, G., Leverrier, A., Naya-Plasencia, M.: Breaking symmetric cryptosystems using quantum period finding. In: CRYPTO 2016. vol. 9815, pp. 207–237. Springer (2016), https://doi.org/10.1007/978-3-662-53008-5_8 7, 9
24. Kuwakado, H., Morii, M.: Security on the quantum-type even-mansour cipher. In: ISITA 2012. pp. 312–316. IEEE (2012), http://ieeexplore.ieee.org/document/6400943/ 3
25. Leander, G., May, A.: Grover meets simon - quantumly attacking the FX-construction. In: ASIACRYPT 2017. pp. 161–178 (2017), https://doi.org/10.1007/978-3-319-70697-9_6 7
26. McGrew, D.A., Viega, J.: The security and performance of the galois/counter mode (GCM) of operation. In: INDOCRYPT 2004. vol. 3348, pp. 343–355. Springer (2004), https://doi.org/10.1007/978-3-540-30556-9_27 1
27. Mennink, B., Neves, S.: Encrypted davies-meyer and its dual: Towards optimal security using mirror theory. In: CRYPTO 2017. vol. 10403, pp. 556–583. Springer (2017), https://doi.org/10.1007/978-3-319-63697-9_19 2, 9

28. Nandi, M.: Mind the composition: Birthday bound attacks on EWCDMD and sokac21. In: EUROCRYPT 2020. vol. 12105, pp. 203–220. Springer (2020), https://doi.org/10.1007/978-3-030-45721-1_8 3, 15
29. Patarin, J.: A proof of security in o(2n) for the xor of two random permutations. In: ICITS 2008. vol. 5155, pp. 232–248. Springer (2008), https://doi.org/10.1007/978-3-540-85093-9_22 2
30. Patarin, J.: Introduction to mirror theory: Analysis of systems of linear equalities and linear non equalities for cryptography. IACR Cryptol. ePrint Arch. **2010**, 287 (2010), http://eprint.iacr.org/2010/287 2
31. Patarin, J.: Generic attacks for the xor of k random permutations. In: ACNS 2013. vol. 7954, pp. 154–169. Springer (2013), https://doi.org/10.1007/978-3-642-38980-1_10 2
32. Shinagawa, K., Iwata, T.: Quantum attacks on sum of even-mansour pseudorandom functions. Inf. Process. Lett. **173**, 106172 (2022), https://doi.org/10.1016/j.ipl.2021.106172 3
33. Shoup, V.: On fast and provably secure message authentication based on universal hashing. In: CRYPTO '96. vol. 1109, pp. 313–328. Springer (1996), https://doi.org/10.1007/3-540-68697-5_24 1
34. Simon, D.R.: On the power of quantum computation. SIAM J. Comput. **26**(5), 1474–1483 (1997), https://doi.org/10.1137/S0097539796298637 6
35. Wegman, M.N., Carter, L.: New hash functions and their use in authentication and set equality. J. Comput. Syst. Sci. **22**(3), 265–279 (1981), https://doi.org/10.1016/0022-0000(81)90033-7 1
36. Zhang, P.: Quantum attacks on sum of even–mansour construction with linear key schedules. Entropy **24**(2), 153 (2022) 3