**Noname manuscript No.**
(will be inserted by the editor)

# Superposition Attacks on Pseudorandom Schemes based on Two or Less Permutations

**Shaoxuan Zhang · Chun Guo · Qingju Wang**

Received: date / Accepted: date

**Abstract** We study quantum superposition attacks against permutation-based pseudorandom cryptographic schemes.

We first extend Kuwakado and Morii's attack against the Even-Mansour cipher (ISITA 2012), and exhibit key recovery attacks against a large class of pseudorandom schemes based on a single call to an $n$-bit permutation, with polynomial $O(n)$ quantum steps. We also show how to overcome restrictions on available quantum data in certain relevant settings.

We then consider $\mathsf{TPPR}$ schemes, namely, Two Permutation-based PseudoRandom cryptographic schemes. Using the improved Grover-meet-Simon method of Bonnetain et al. (ASIACRYPT 2019), we show that the keys of a wide class of $\mathsf{TPPR}$ schemes can be recovered with $O(n)$ superposition queries and $O(n2^{n/2})$ quantum steps. We also exhibit sub-classes of "degenerated" $\mathsf{TPPR}$ schemes that lack certain internal operations, and exhibit more efficient key recovery attacks using either the Simon's algorithm or Chailloux et al.'s algorithm for collision searching (ASIACRYPT 2017).

Further using the all-subkeys-recovery idea of Isobe and Shibutani (SAC 2012), our results give rise to key recovery attacks against several recently

Shaoxuan Zhang
School of Cyber Science and Technology, Shandong University
Key Laboratory of Cryptologic Technology and Information Security, Ministry of Education, Shandong University
E-mail: shaoxuanzhang@mail.sdu.edu.cn

Chun Guo
School of Cyber Science and Technology, Shandong University
Key Laboratory of Cryptologic Technology and Information Security, Ministry of Education, Shandong University
State Key Laboratory of Information Security (Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093)
E-mail: chun.guo@sdu.edu.cn

Qingju Wang
SnT, University of Luxembourg
E-mail: qjuwang@gmail.com

proposed permutation-based PRFs, as well as the 2-round Even-Mansour ciphers with generic key schedule functions (Chen et al., JoC 2018) and their tweakable variants (Cogliati et al., CRYPTO 2015). From a constructive perspective, our results establish new quantum Q2 security upper bounds for two permutation-based pseudorandom schemes as well as sound design choices.

**Keywords** Quantum attacks · permutation-based cryptography · tweakable blockcipher · PRF

**Mathematics Subject Classification (2000)** 94A60 · 68P25

## 1 Introduction

### 1.1 Permutation-Based Cryptography

A remarkable trend in cryptography is the development of constructions built upon *(public) keyless cryptographic permutations*. It seems to originate from omitting key expansions in blockciphers [7,60], in order to increase efficiency and to remove a number of attack vectors leveraging correlations between distinct keys. Subsequent goal of constructing "richer" cryptographic objects from such permutations would be addressed by provable security. In all, permutation-based cryptography appears to ease security evaluations, and this has motivated a huge number of designs and constructions to be proposed. In fact, during the NIST hash function competition [58], 3 among the 5 finalists utilized permutations including the final winner KECCAK; during the NIST lightweight competition [56], 6 among the 10 finalists utilized permutations.

Complicated objects from permutation-based cryptography include (tweakable) pseudorandom permutations [32,8,22,23,33,37,51,28] and functions [20,16,31,21], (authenticated) encryption schemes [56,29,5,17], MACs [53,30,16], and (keyless) hash functions [60,52,4,58]. Such designs have been informally divided into the sponge-based approach [4] and the "full domain" approach [20,30]. Roughly speaking, sponge-based designs invoke the permutation with the concatenation of a secret key/state with an input-dependent value, whereas "full domain" designs invoke the permutation with $\varphi(k,x)$ for $\varphi$ being (close to) a keyed permutation, and this is crucial for better concrete security. Moreover, to increase efficiency, most designs choose linear transformations for the keyed function $\varphi$.[1] This paper focuses on the latter.

It has been shown that pseudorandom schemes using a single call to an $n$-bit permutation achieve at most $n/2$ bit security due to birthday collisions, even if they employ the "full domain" approach [20]. This is insufficient for lightweight permutations such as KECCAK-$f$[200] [58], SPONGENT [39], and PHOTON [39], and as a result, the approach of using two permutations has appeared as the best trade-off between efficiency and security, and have been adopted in a number of recent designs elaborated as follows.

[1] Though, there is no formal definition.

Constructing (tweakable) pseudorandom permutations from public permutations was initiated by Even and Mansour [32], who proposed a scheme $\mathsf{EM}^P_{k_1,k_2}(x) = k_2 \oplus P(k_1 \oplus x)$ that whitens a public $n$-bit permutation $P$ with two secret keys $k_1$ and $k_2$. Now known as the Even-Mansour construction, the scheme was proved secure up to $n/2$ queries, which is then proved tight [24]. To break the $n/2$ bit security barrier, the scheme was later generalized to the Iterated Even-Mansour construction [8,19]. In fact, this was also the first $\mathsf{TPPR}$ scheme. With 2 rounds and $3n$-bit keys [8], provable security increases to $2n/3$ bits which is tight in the information theoretic sense. Conditions on the keys were then relaxed to using 2 keys or a single $n$-bit key with appropriate key derivation functions [18]. Further subsequent work investigated adding tweaks to the iterated Even-Mansour via the almost universal hash functions and pinpointed 2-round tweakable Even-Mansour ciphers as the minimal permutation-based tweakable blockcipher with $2n/3$-bit security [22,28]. The aforementioned advances in provable security also attracted numerous cryptanalytic efforts [27,55,25,49].

For PRFs, Chen et al. proposed two PRFs $\mathsf{SoEM}$ and $\mathsf{SoKAC21}$, both using two permutation calls that achieve beyond-birthday $2n/3$ bit security [20]. Unfortunately, the sequential construction $\mathsf{SoKAC21}$ turned out flawed [54], and it was Chakraborti et al. [16] to bridge the gap of sequential PRF, and later Dutta et al. [31] to make the PRF inverse-free, at the expense of using a longer key. The parallel PRF $\mathsf{SoEM}$ remains secure and has inspired Dutta and Nandi to design a nonce-based MAC scheme $\mathsf{nEHtM}_p$ [29] and Bhattacharjee et al. designing $\mathsf{CENCPP}^*$ [5], a permutation-based variant of the blockcipher mode $\mathsf{CENC}$ [41].

In all, the above has established two permutation-based pseudorandom ($\mathsf{TPPR}$) schemes as a rising class of objects, and relevant research appears to keep evolving. In the classical setting, it seems $2n/3$ bit security has been accepted as a general *upper bound* on the security of $\mathsf{TPPR}$ schemes, and designs typically tried to achieve this goal.

### 1.2 Quantum Superposition Attacks

Advances in quantum algorithms and computing devices have posed serious threats to common cryptographic schemes. Regarding public-key cryptography, the seminal work of Shor [64] enables factoring and computing discrete logs in polynomial quantum steps. This has triggered the NIST Post-Quantum Cryptography Standardization Process [57].

Regarding symmetric cryptography, it was believed that the main impact is due to Grover's algorithm [34] accelerating brute force search. Concretely, any cryptosystem with $\kappa$-bit secret keys admits a key recovery attack in $O(2^{\kappa/2})$ quantum steps. However, non-trivial symmetric constructions may hide periodic information and lend themselves to surprisingly efficient attacks based on Simon's quantum algorithm. Let $\mathsf{O}_k : \mathcal{X} \rightarrow \mathcal{Y}$ be the classical function describing the (keyed) oracle of the targeted scheme. When such a scheme is implemented in a quantum computer, then the adversary can issue a quantum superposition $\sum_{x,y} \alpha_{x,y} |x\rangle|y\rangle$ as a query and obtain $|x\rangle|y\rangle \mapsto |x\rangle|\mathsf{O}_k(x) \oplus y\rangle$ as the response, where $x$ and $y$ are arbitrary $n$-bit strings and $|x\rangle$, $|y\rangle$ are the corresponding $n$-qubit states expressed in the computational basis. Such a superposition query may extract some information about $\mathsf{O}_k(x)$ for all $x \in \mathcal{X}$. Such attacks are called *superposition attacks*, and the security model is sometimes referred to as *quantum Q2 model*.[2] With such superposition queries, Simon's algorithm is able to compute the hidden period, which corresponds to the secret key for a number of symmetric schemes. This line of research was initiated by Kuwakado and Morii [46], who showed that the 3-round Feistel networks, which are well-known to be CPA secure in the classical setting, can be fully broken by superposition CPA attacks. Subsequent works relaxed the conditions for Simon algorithm and exhibited applications to popular MACs and authenticated encryption modes [61,44].

Perhaps more importantly for us, Kuwakado and Morii [47] showed that the Even-Mansour construction can be broken in polynomial time in the quantum CPA-setting. The main idea of [47] was to consider the function $f(x) := \mathsf{EM}^{P}_{k_1,k_2}(x) \oplus P(x)$. As this function fulfills $f(x) = f(x \oplus k_1)$ for all $x$, an application of Simon's algorithm [13,67] immediately yields the unknown period $k_1$ of $f$ in $O(n)$ quantum steps. This already showed that the classical approach to key-length extension via adding whitening keys may not be effective in the Q2 model. Indeed, Leander and May [48] proposed an approach embedding Simon's test in a Grover search, and used this to break the FX key-length extension scheme $\mathsf{FX}^{\mathsf{E}}_{k_0,k_1,k_2}(x) = k_2 \oplus \mathsf{E}(k_0, k_1 \oplus x)$, which may be viewed as a Even-Mansour variant built upon a blockcipher $\mathsf{E} : \{0,1\}^{\kappa} \times \{0,1\}^{n} \to \{0,1\}^{n}$. This idea is referred to as *Grover-meet-Simon* in subsequent works. Later, Bonnetain et al. [11] improved Grover-meet-Simon process using a careful reorganization of the online and offline quantum queries, and this reduces the quantum data complexity to polynomial.

On the constructive side, security definitions and Q2 secure PRFs, PRPs, MACs, signatures, and encryption schemes have been proposed [68,38,9,10,3,6]. Alagic and Russell proposed to counter Simon's algorithm-based attacks via replacing the common $\oplus$ operations by modular additions [2], though the gain was later shown to be limited [12].

### 1.3 Our Results

Pseudorandom schemes are central building blocks for various cryptosystems and are thus fundamental for post-quantum cryptography. As mentioned by Kuwakado and Morii [47] and later re-stressed by Leander and May [48, Sect. 4], an important open question is the quantum Q2 security of the iterated Even-Mansour with 2 and more rounds. In fact, this constitutes the initial

[2] On the other hand, in the *Q1 model*, attackers have an access to a quantum computer to perform any offline computation, while they are only allowed to make online queries in a classical manner.

motivation of our work. In addition, the state-of-the-art indicates a more severe influence on schemes using whitening keys, which is particularly relevant to permutation-based cryptography. By these and by the popularity of permutations, we seek for characterization of cryptographic schemes using 2 (or less) permutation calls in the face of superposition attacks.

We first extend the idea of Kuwakado and Morii [47] and show that the general design of Chen et al. [20] built on one public permutation preceded and followed by linear mappings can be broken by Simon's algorithm. Formally, $\mathsf{F1P}^{P}_{k_1,k_2}(x) = a_{21}k_2 \oplus a_{22}x \oplus a_{23}P(a_{11}k_1 \oplus a_{12}x)$, where $P$ is an $n$-bit permutation and multiplications are on the finite field $\mathbb{F}_2^n$. These include a number of popular classically secure schemes including the Even-Mansour construction [32], the (1-round) tweakable Even-Mansour construction [22], and some permutation-based PRFs [36,35,21].

The PRFs [36,21] are typically used in MPC settings, and such protocols enforce strong restrictions on the form of queries to the PRF oracle. In detail, the scheme in [35] varies the permutation $P$ after every PRF query, while the scheme in [21] changes the key after every PRF query. As a consequence, the number of allowed superposition queries for every single instance or key is limited to 1. In this respect, we further show that such query restrictions can be overcome and the Simon-based attack remains applicable even with such severely restricted superposition queries.

Our main result is on *Two Permutation-based PseudoRandom (*TPPR*) schemes*. In detail, we consider schemes parameterized by eight field elements $a_{00}, a_{01}, a_{10}, a_{11}, a_{12}, a_{20}, a_{21}, a_{23} \in \mathbb{F}_2^n$ and defined as

$$\begin{aligned}\mathsf{F2P}^{P_1,P_2}_{\mathsf{A},\mathbf{k}}(x) = {} & P_2\big(a_{12}P_1(a_{01}x \oplus a_{00}k_1) \oplus a_{11}x \oplus a_{10}k_2\big) \\ & \oplus a_{22}P_1(a_{01}x \oplus a_{00}k_1) \oplus a_{21}x \oplus a_{20}k_3, \end{aligned} \quad (1)$$

where $P_1$ and $P_2$ are two (independent) $n$-bit permutations, and $\mathbf{k} = (k_0, k_1, k_2) \in (\{0,1\}^n)^3$ are three (independent) $n$-bit keys. We characterize its superposition attacks as follows.

(i) We first identify a class of TPPR schemes that are "degenerated", in the sense that they are easily broken by Simon algorithm and provide no Q2 security at all.

(ii) We then identify two classes of TPPR schemes that are "partially degenerated". Both of them could be viewed as cascading a single permutation-based keyed function and a variant of the (keyless) Davies-Meyer construction, and we thereby refer to them as *Cascaded constructions with unkeyed Davies-Meyer (*CUDM*)*. In detail, they are defined as

$$\begin{aligned}\mathsf{CUDM1}^{P_1,P_2}_{k_1}(x) &= P_2(a_{12}P_1(a_{01}x \oplus a_{00}k_1) \oplus a_{11}x) \oplus a_{22}P_1(a_{01}x \oplus a_{00}k_1), \\ & \qquad a_{00}, a_{01}, a_{11}, a_{12}, a_{22} \neq 0, \\ \mathsf{CUDM2}^{P_1,P_2}_{k_2,k_3}(x) &= P_2(a_{12}P_1(a_{01}x) \oplus a_{11}x \oplus a_{10}k_2) \oplus a_{20}k_3, \\ & \qquad a_{01}, a_{10}, a_{11}, a_{12}, a_{20} \neq 0.\end{aligned}$$

The single permutation-based keyed function, on its own, is clearly vulnerable to Simon's algorithm. The interesting observation is that in both cases, the additional Davies-Meyer construction eliminates algebraic properties and prevents polynomial attacks. To understand their Q2 security, we leverage collisions in their computations and develop key recovery attacks using the quantum collision searching algorithm of Brassard et al. [14]. For both classes, our attacks $O(n)$ qubits, $O(2^{2n/5})$ quantum steps, and $O(2^{n/5})$ classical memory, and remain faster than the naïve Grover key search.

(iii) Finally, for the remaining "non-degenerated" TPPR schemes, we are able to mount key recovery attacks using the Grover-meet-Simon approach, i.e., by guessing a part of the keys to reach periodicity on the remaining components.

Combining our attack with the all-subkeys-recovery idea of Isobe and Shibutani [40], we exhibit key recovery attacks against the PEDM PRF of [31], the SoKAC1 PRF of [20,16], as well as the 2-round Even-Mansour ciphers with any key schedule functions and with tweaks. For the 2-round Even-Mansour, as long as the master key length $\kappa$ has $\kappa \gg n+2\log_2 n$, our attack complexity $O(n2^{n/2})$ is better than $O(2^{\kappa/2})$ of the naïve Grover key search and $O(2^{2n/3})$ of the quantum meet-in-the-middle attack (for all-subkeys-recovery) of Kaplan [43]. We also improve the superposition attack of Shinagawa and Iwata against the SoEM PRF [62] thanks to the use of Alg-PolyQ2 of [11].

*Interpretation.* Admittedly, superposition attacks and the Q2 model are over generous to the attacker, and recent works [11] have turned to improve attacks in the Q1 model (in which accelerations are limited to offline quantum computations). Though, we view our results as establishing new Q2 security upper bounds on a wide class of pseudorandom schemes and unveiling potential design choices, which is fundamental since they may be key building blocks of various other quantum cryptographic protocols. In particular,

(i) Since TPPRS cannot enjoy more than $n/2$ bit security in the Q2 model, TPPRS with $n$-bit keys (and $2n/3$-bit classical security) is preferable;

(ii) Once carefully designed, additional keyless "rounds" may help eliminate algebraic properties and prevent relevant attacks, despite that they don't increase key-length.

### 1.4 Other Related Work

Quantum Q1 security has been proved for the FX construction and the (1-round) Even-Mansour cipher [42,1]. This line on Q1 security is largely orthogonal to our work.

Finally, quantum versions of well-known cryptanalytic methods have been developed [45,44], including differential, linear, and slide attacks.

## 2 Preliminaries

For an integer $n \in \mathbb{N}$, we denote by $\{0,1\}^n$ the set of bit strings of length $n$. For two bit strings $x, y$, we denote by $x\|y$ their concatenation and by $x \oplus y$ their bitwise XOR. When $x$ and $y$ are viewed as bit vectors, we denote by $\langle x, y\rangle$ the inner product of $x$ and $y$. If $\mathcal{X}$ is a set, by $x \overset{\$}{\leftarrow} \mathcal{X}$ we denote the uniformly random sampling of an element from $\mathcal{X}$. By $P_i$ we denote a random permutation operating on $n$ bits. For a matrix $\mathsf{A}$, by $a_{i,j}$ we denote its coefficient at the $i^{th}$ row and $j^{th}$ column. By $a_{i,*}$ we denote the $i^{th}$ row of $\mathsf{A}$, and by $a_{*,j}$ its $j^{th}$ column. Given an $n$-bit string $x$ and $a \le n$, denote by $\mathsf{left}_a(x)$ (resp., $\mathsf{right}_a(x)$) the $a$ leftmost (resp., rightmost) bits of $x$.

### 2.1 Quantum algorithms

In this section, we briefly recall the quantum algorithms that will be used in this paper, namely, Simon's algorithm [66] for extracting periodic information of functions, Grover's algorithm [34] for exhaustive searching, and their combination Grover-meet-Simon algorithm of Leander and May [48].

#### *2.1.1 Simon's algorithm for extracting periodic information*

Consider a Boolean function $f : \{0,1\}^n \to \{0,1\}^n$ with the promise that there exists $s \in \{0,1\}^n$ (which is unknown) such that for any $(x, x') \in \{0,1\}^n$, $f(x) = f(x')$ if and only if $x \oplus x' \in \{0^n, s\}$. The goal is to recover $s$. Classical solutions to this problem consume $\Theta(2^{n/2})$ computations. Whereas Simon's algorithm solves its with quantum complexity $O(n)$. To see how it works, recall that the Hadamard transform $H^{\otimes n}$ applied on an $n$-qubit state $|x\rangle$ for some $x \in \{0,1\}^n$ gives $H^{\otimes n}|x\rangle = \frac{1}{\sqrt{2^n}} \sum_{y\in\{0,1\}^n} (-1)^{\langle x,y\rangle}|y\rangle$. With this, below we present a description of [44].

1. Initializes a $2n$-qubit state $|0\rangle|0\rangle$, and then applies the Hadamard transform $H^{\otimes n}$ to the first register to obtain the uniform quantum superposition
$$\frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle|0\rangle. \tag{2}$$
2. Issues a quantum query to the function $f$ and maps Eq. (2) to the state
$$\frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle|f(x)\rangle$$
3. Measures the second register in the computational basis to yield a value $f(z)$ and collapse the first register to
$$\frac{1}{\sqrt{2}}\big(|z\rangle + |z \oplus s\rangle\big)$$

4. Applies the Hadamard transform $H^{\otimes n}$ again to the first register and yields
$$\frac{1}{\sqrt{2}}\frac{1}{\sqrt{2^n}}\sum_{y\in\{0,1\}^n}(-1)^{\langle y,z\rangle}\big(1+(-1)^{\langle y,s\rangle}\big)|y\rangle$$
5. The vectors $y$ such that $\langle y,s\rangle=1$ have amplitude 0. Therefore, measuring the state in the computational basis yields a random vector $y$ such that $\langle y,s\rangle=0$.

Repeating these steps $O(n)$ times yield $n-1$ independent vectors orthogonal to $s$ with high probability, and thus $s$ can be recovered by solving linear equations. However, as discussed by Santoli and Schaffner [61] and Kaplan et al. [44], functions defined upon cryptographic primitives are seldom "perfectly periodic", and random collisions of the form $f(x)=f(x')$, $x\oplus x'\neq s$, may interfere. To rescue, Kaplan et al. [44] showed that Simon's promise can be weakened to allow for the aforementioned "false positives" $f(x)=f(x')$, at the expense of slightly more repetitions. Formally, for $f:\{0,1\}^n\to\{0,1\}^n$ such that $f(x\oplus s)=f(x)$ for all $x$, define
$$\varepsilon(f,s):=\max_{t\in\{0,1\}^n\setminus\{0,s\}}\Pr_x\big[f(x)=f(x\oplus t)\big]. \tag{3}$$
If $\varepsilon(f,s)\leq p_0<1$, then Simon's algorithm returns $s$ with $cn$ queries, with probability at least $1-\big(2\big(\frac{1+p_0}{2}\big)^c\big)^n$.

Leander and May [48] introduced the assumption adopted by many [26] that $f(x)$ behaves like a random periodic function, and argued its practical relevance. Precise bounds on $\varepsilon(f,s)$ are certainly preferable. In our work, the precise probabilities of such collisions are related to the differential and second order differential properties of random permutations. The former has been characterized by O'Connor [59], while the latter appears unfortunately missing. We thereby follow the random periodic function assumption of Leander and May [48] for our complexity analysis, i.e., we also assume that all the periodic functions used in our attacks behave as random periodic functions. Under this assumption, Leander and May showed that any function value $f(x)$ has only two preimages with probability at least $\frac{1}{2}$. Moreover, they show that $\lambda=2(n+\sqrt{n})$ repetitions of the Simon's algorithm are sufficient to compute $s$.

### *2.1.2 Grover's algorithm for exhaustive searching*

In general, the searching problem is as follows. Given a set $X$ (the "search space") and let $g:\{0,1\}^n\to\{0,1\}$ be a function such that $g(x)=1$ if and only if $x\in X$. Find a value $x\in X$. Classical solutions have to resort to $O(\frac{2^n}{|X|})$ queries. Given a quantum oracle of $g$, Grover's algorithm [34] can solve the problem by using $O(\frac{2^{n/2}}{\sqrt{|X|}})$ quantum queries.

### *2.1.3 Grover-meet-Simon*

For most cryptographic cracking problems, Simon's algorithm does not immediately yield solutions. Though, a class of cracking problems is such that once we fix a part of the guess, the problem instance can be translated into another problem instance that fulfills Simon's approximate promise. Bonnetain et al. [11] formalized such problems as *Asymmetric Search of a Period*, which is presented below.

*Problem 1 (Asymmetric Search of a Period).* Let $F : \{0,1\}^\kappa \times \{0,1\}^n \to \{0,1\}^\ell$ and $g : \{0,1\}^n \to \{0,1\}^\ell$ be two functions such that $F$ is a family of functions indexed by $\{0,1\}^\kappa$. Assume that we are given quantum oracle access to $F$, and classical or quantum oracle access to $g$. (In the Q1 setting, $g$ will be a classical oracle. In the Q2 setting, $g$ will be a quantum oracle.)

Assume that there exists exactly one $i \in \{0,1\}^\kappa$ such that $F(i,\cdot) \oplus g$ has a hidden period, i.e., $\forall x \in \{0,1\}^n$, $F(i_0, x) \oplus g(x) = F(i_0, x \oplus s) \oplus g(x \oplus s)$for some $s$. Furthermore, assume that

$$\max_{\substack{i \in \{0,1\}^\kappa \setminus \{i_0\} \\ t \in \{0,1\}^n \setminus \{0^n\}}} \Pr_{x \xleftarrow{\$} \{0,1\}^n} \big[F(i, x \oplus t) \oplus g(x \oplus t) = F(i,x) \oplus g(x)\big] \leq \frac{1}{2}. \qquad (4)$$

Then find $i_0$ and $s$. As remarked in prior works, Eq. (4) is a reasonable assumption for "sufficiently strong" cryptographic functions.

Problem 1 abstracts the key recovery of a number of cryptosystems, which in particular includes the aforementioned FX construction $\mathsf{FX}^{\mathsf{E}}_{k_0,k_1,k_2}(x) = k_2 \oplus \mathsf{E}(k_0, k_1 \oplus x)$ for a blockcipher $\mathsf{E} : \{0,1\}^\kappa \times \{0,1\}^n \to \{0,1\}^n$, as well as our general $\mathsf{TPPR}$ scheme (this enables our attack). More clearly, $\mathsf{FX}^{\mathsf{E}}_{k_0,k_1,k_2}$ collapses to the 1-round Even-Mansour scheme when $k_0$ is fixed to a guess, and this appeared to motivate Leander and May [48] proposing the *Grover-meet-Simon* algorithm and recovering the keys of $\mathsf{FX}^{\mathsf{E}}_{k_0,k_1,k_2}(x)$ in $O(n2^{\kappa/2})$ quantum steps. As mentioned in the Introduction, Bonnetain et al. [11] subsequently improved Grover-meet-Simon process and developed $\mathsf{Alg\text{-}PolyQ2}$ (see Algorithm 1 below). The central idea is to carefully reuse $O(cn)$ superposition states in all Grover iterations, such that the states are used for testing without being measured. By this, the number of superposition queries to the quantum oracle $|g\rangle$ is reduced to $O(cn)$ compared with $O(n2^{\kappa/2})$ in [48].

For concreteness, we fix a constant $c \simeq \kappa/(n \log_2(4/3))$. Then the offline Simon's algorithm finds $i_0$ with a probability in $\Theta(1)$ by making $O(n)$ quantum queries to $g$ and $O(n2^{\kappa/2})$ quantum queries to $F$. The offline computation (the procedures excluding the ones to prepare the state $|\psi_g\rangle$) of Algorithm 1 is done in time $O((n^3 + nT_F)2^{\kappa/2})$, where $T_F$ is the time required to evaluate $F$ once.

## 3 Breaking Schemes with One Permutation Call

In this section, we show that all "full-domain" pseudorandom schemes that make only one permutation call and have linear pre-and post-processing func-

**Algorithm 1** Bonnetain et al.'s algorithm $\mathsf{Alg\text{-}PolyQ2}$ [11]

```
Start in the all-zero state.
Using $cn$ queries to $|g\rangle$ to create the state[3]
    $$|\psi_g\rangle = \bigotimes^{cn} \left( \sum_{x \in \{0,1\}^n} |x\rangle |g(x)\rangle \right)$$
    The circuit now contains $|\psi_g\rangle$, the "g-database", and additional registers on which we can perform Grover search. Notice that $|\psi_g\rangle$ contains $cn$ independent (and disentangled) registers.
Create the uniform superposition over indices $i \in \{0,1\}^\kappa$:
    $$|\psi_g\rangle \otimes \sum_{i \in \{0,1\}^\kappa} |i\rangle$$
Apply Grover iterations. The testing oracle is a unitary operator **test** (see Algorithm 2 below) that takes in input a register for $|i\rangle$ and the "g-database", and tests in superposition whether $F(i,\cdot) \oplus g$ has a hidden period. If this is the case, it returns $|b \oplus 1\rangle$ on input $|b\rangle$. Otherwise it returns $|b\rangle$. (Algorithm 2 gives the details for **test** in the case that $i$ is fixed.)
After $O(2^{\kappa/2})$ Grover iterations, measure the index $i$.
If the hidden shift is also wanted, apply a single instance of Simon's algorithm (or re-use the database and perform a slightly extended computation of **test** to retrieve the result).
```

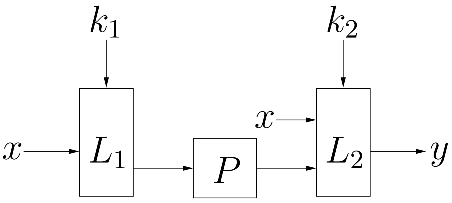

Fig. 1: Function $\mathsf{F1P}^P_{k_1,k_2}$ based on two keys $k_1$ and $k_2$ and a single call to a public random permutation.

tions can be fully broken in the Q2 model. To formally define our target, let $P$ be an $n$-bit permutation, and let $L_1 : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ and $L_2 : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ be any two linear mappings (that only consist of modular addition and scalar multiplication). Further, write

$$L_1 = (a_{11}, a_{12}), \qquad L_2 = (a_{21}, a_{22}, a_{23}),$$

where $a_{11}, a_{12}, a_{21}, a_{22}, a_{23} \in \mathbb{F}_2^n$.

[3] This state be created by an exponential number of classical queries to $g$ as well [11]. As we only consider superposition attacks, we will focus on the variant relying on $|g\rangle$.

**Algorithm 2** The procedure **test** that checks if a function $F(i,\cdot)\oplus g$ as a period against the "g-database", without any new query to $g$.

```
We start with the g-database
    $$|\psi_g\rangle = \bigotimes^{cn}\left(\sum_{x\in\{0,1\}^n}|x\rangle|g(x)\rangle\right).$$
Using $cn$ superposition queries to $F$, build the state:
    $$\left|\psi_{F(i,\cdot)\oplus g}\right\rangle = \bigotimes^{cn}\left(\sum_{x\in\{0,1\}^n}|x\rangle\big|g(x)\oplus F(i,x)\big\rangle\right).$$
    We will now perform, in a reversible way, the exact computations of Simon's algorithm
    to find if $g\oplus F(i,\cdot)$ has a hidden period or not (in which case $F(i,\cdot)$ and $g$ have a hidden
    shift).
Apply $(H^{\otimes n}\otimes I_m)^{cn}\otimes I_1$ to $|\psi_{F(i,\cdot)\oplus g}\rangle\otimes|b\rangle$, to obtain
    $$\left(\sum_{u_1,x_1\in\{0,1\}^n}(-1)^{u_1\cdot x_1}\big|u_1\big\rangle\big|F(i,x_1)\oplus g(x_1)\big\rangle\right)\otimes\cdots$$
    $$\otimes\left(\sum_{u_{cn}\cdot x_{cn}\in\{0,1\}^n}(-1)^{u_{cn},x_{cn}}\big|u_{cn}\big\rangle\big|F(i,x_{cn})\oplus g(x_{cn})\big\rangle\right)\otimes|b\rangle$$
Compute $d := \dim(\mathrm{Span}(u_1,\ldots,u_{cn}))$, set $r := 0$ if $d = n$ and $r := 1$ if $d < n$, and add
    $r$ to $b$. Then uncompute $d$ and $r$, and obtain
    $$\sum_{\substack{u_1,\ldots,u_{cn}\\x_1,\ldots,x_{cn}}}(-1)^{u_1\cdot x_1}\big|u_1\big\rangle\big|F(i,x_1)\oplus g(x_1)\big\rangle\otimes\cdots$$
    $$\cdots\otimes(-1)^{u_{cn}\cdot x_{cn}}\big|u_{cn}\big\rangle\big|F(i,x_{cn})\oplus g(x_{cn})\big\rangle\otimes\big|b\oplus r\big\rangle$$
Uncompute $(H^{\otimes n}\otimes I_m)^{cn}\otimes I_1$.
Using $cn$ new superposition queries to $F$, revert $|\psi_{F(i,\cdot)\oplus g}\rangle$ to $|\psi_g\rangle$. There are two cases:
    – If $g\oplus F(i,\cdot)$ has a hidden period, then $r = 1$ always holds. Hence, in the output
      register, we always write 1.
    – If $g\oplus F(i,\cdot)$ does not have a hidden period, then with high probability, $r = 0$. Hence,
      in the output register, we write 0.
```

Let $\mathsf{F1P}^P_{k_1,k_2}:\{0,1\}^{2n}\times\{0,1\}^n\to\{0,1\}^n$ be the function of Fig. 1, i.e.,

$$\begin{aligned}\mathsf{F1P}^P_{k_1,k_2}(x) &= L_2\Big(k_2,x,P\big(L_1(k_1,x)\big)\Big)\\ &= a_{21}k_2\oplus a_{22}x\oplus a_{23}P(a_{11}k_1\oplus a_{12}x),\end{aligned}\tag{5}$$

where multiplications are over the finite field $\mathbb{F}_2^n$. Even if $k_1$ and $k_2$ are independent, the keys can be recovered by Simon's algorithm. To this end, we distinguish two subcases.

*Case 1: $a_{11} = 0$ or $a_{12} = 0$.* In this case, the input to the permutation is independent of either the keys or $x$. As shown by Chen et al. [20], there exist distinguishing attacks even in the classical setting. Here we put forward (obvious) key recovery attacks.

When $a_{11}=0$, given a single pair $(x,y)$ of input/output, it holds

$$a_{21}k_2 \oplus a_{22}x \oplus a_{23}P(a_{12}x).$$

Thus, $a_{21}k_2 = a_{22}x \oplus a_{23}P(a_{12}x)$, and $k_2$ can be recovered by $k_2 = a_{21}^{-1}\big(a_{22}x \oplus a_{23}P(a_{12}x)\big)$.

On the other hand, when $a_{12}=0$, given a single pair $(x,y)$ of input/output, it holds

$$a_{21}k_2 \oplus a_{22}x \oplus a_{23}P(a_{11}k_1),$$

and we have $a_{21}k_2 \oplus a_{23}P(a_{11}k_1) = a_{22}x$. While we cannot further recover the keys, the $n$-bit secret $a_{21}k_2 \oplus a_{23}P(a_{11}k_1)$ already enables free evaluations of $\mathsf{F1P}^{P}_{k_1,k_2}(x)$ for any $x$.

*Case 2: $a_{11} \neq 0$, $a_{12} \neq 0$.* In this case, consider the function $f : \{0,1\}^n \to \{0,1\}^n$ defined as

$$\begin{aligned} f(x) &:= \mathsf{F1P}^{P}_{k_1,k_2}(x) \oplus a_{23}P(a_{12}x) \oplus a_{22}x \\ &= a_{21}k_2 \oplus a_{23}P(a_{11}k_1 \oplus a_{12}x) \oplus a_{23}P(a_{12}x). \end{aligned} \tag{6}$$

It can be seen that $f(x)$ is periodic with period $a_{12}^{-1}a_{11}k_1$, since

$$\begin{aligned} f(x \oplus a_{12}^{-1}a_{11}k_1) &= a_{21}k_2 \oplus a_{23}P(a_{11}k_1 \oplus a_{12}x \oplus a_{11}k_1) \oplus a_{23}P(a_{12}x \oplus a_{11}k_1) \\ &= f(x). \end{aligned}$$

Moreover, as discussed in Sect. 2.1.1, under the assumption that $f$ is a random periodic function, then the key $a_{12}^{-1}a_{11}k_1$ can be recovered after applying Simon's algorithm with $2(n+\sqrt{n})$ repetitions.

## 3.1 Extensions to settings with extreme data limit

Simon's algorithm requires $O(n)$ queries to the keyed oracle. A number of cryptosystems vary the keyed oracle for every query, and it is thus natural to ask if this prevents Simon's attack. Below we show that in two such relevant settings, the attack remains applicable.

### *3.1.1 Extension I: varied permutation*

For the (non-trivial) case $a_{11} \neq 0$, $a_{12} \neq 0$, the Simon-based attack remains applicable even if the permutation varies for every online query. Formally, consider $\widetilde{\mathsf{F1P}} : \{0,1\}^{2n} \times \mathcal{I} \times \{0,1\}^n \to \{0,1\}^n$, which is a variant of $\mathsf{F1P}^{P}_{k_1,k_2}$ defined upon $|\mathcal{I}|$ permutations $P_1, ..., P_{|\mathcal{I}|}$:

$$\widetilde{\mathsf{F1P}}^{P_1,\ldots,P_{|\mathcal{I}|}}_{k_1,k_2}(i,x) = a_{21}k_2 \oplus a_{22}x \oplus a_{23}P_i(a_{11}k_1 \oplus a_{12}x). \tag{7}$$

Moreover, queries to $|\widetilde{\mathsf{F1P}}_{k_1,k_2}^{P_1,\ldots,P_{|\mathcal{I}|}}\rangle$ are restricted with respect to $i$. In detail, the $i$-th adversarial query to $|\widetilde{\mathsf{F1P}}_{k_1,k_2}^{P_1,\ldots,P_{|\mathcal{I}|}}\rangle$ is a quantum superposition $\sum_{x\in\{0,1\}^n,y\in\{0,1\}^n}\alpha_{x,y}|x\rangle|y\rangle$, and the corresponding response is the superposition $\sum_{x\in\{0,1\}^n,y\in\{0,1\}^n}\alpha_{x,y}|x\rangle|y\oplus\widetilde{\mathsf{F1P}}_{k_1,k_2}^{P_1,\ldots,P_{|\mathcal{I}|}}(i,x)\oplus y\rangle$. Namely, all the function values in the superposition are computed using the same index $i$.

Even with such query restrictions, Simon's algorithm remains applicable. In detail, consider the function $f:\mathcal{I}\times\{0,1\}^n\to\{0,1\}^n$ defined as

$$\begin{aligned} f(i,x) &:= \widetilde{\mathsf{F1P}}_{k_1,k_2}^{P_1,\ldots,P_{|\mathcal{I}|}}(i,x)\oplus a_{23}P_i(a_{12}x)\oplus a_{22}x \\ &= a_{21}k_2\oplus a_{23}P_i(a_{11}k_1\oplus a_{12}x)\oplus a_{23}P_i(a_{12}x). \end{aligned} \tag{8}$$

Then for all $i\in\mathcal{I}$, the function $f(i,\cdot)$ is periodic with period $a_{12}^{-1}a_{11}k_1$. We thus runs the Simon's algorithm except that we query $f(i,\cdot)$ with the uniform superposition during the $i$-th iteration. This fulfills the query restriction, while the vectors produced in all the iterations are orthogonal to the same secret period $a_{12}^{-1}a_{11}k_1$. It thus remains easy to recover $a_{12}^{-1}a_{11}k_1$ after $O(n)$ iterations.

This setting with restricted queries is relevant to some recent proposals. For example, Guo et al. [35] introduced an AES-based "tweakable correlation robust hash function" for MPC protocols. In detail, let $\mathsf{E}:\{0,1\}^n\times\{0,1\}^n\to\{0,1\}^n$ be a blockcipher with $n$-bit blocks and $n$-bit keys (e.g., the AES-128 with $n=128$). Then, the function is defined as $\mathsf{H}^{\mathsf{E}}(i,x):=\mathsf{E}(i,\sigma(x))\oplus\sigma(x)$, where $\sigma:\{0,1\}^n\to\{0,1\}^n$ is a fixed linear orthomorphism. The security of $\mathsf{H}^{\mathsf{E}}(i,x)$ is proved as follows. Given a random secret key $k$,

$$\begin{aligned} &\mathsf{H}^{\mathsf{E}}(i_1,x_1\oplus k):=\mathsf{E}(i_1,\sigma(x_1)\oplus\sigma(k))\oplus\sigma(x_1)\oplus\sigma(k), \\ &..., \\ &\mathsf{H}^{\mathsf{E}}(i_\ell,x_\ell\oplus k):=\mathsf{E}(i_\ell,\sigma(x_\ell)\oplus\sigma(k))\oplus\sigma(x_\ell)\oplus\sigma(k) \end{aligned}$$

are $\ell$ independent pseudorandom strings as long as $i_1,...,i_\ell$ *are distinct and fixed by the protocol*. It is easy to see that this construction and its security model are exactly captured by our extended attack.

### *3.1.2 Extension II: varied key*

For the (non-trivial) case $a_{11}\neq0$, $a_{12}\neq0$, the Simon-based attack remains applicable even if the key varies (in a public manner) for every online query. Formally, consider an oracle $\widetilde{\mathsf{F1PRK}}_{k_1,k_2}^{P}$, which replies its $i$-th superposition query $\sum_{x\in\{0,1\}^n,y\in\{0,1\}^n}\alpha_{x,y}|x\rangle|y\rangle$ with the superposition of oracle responses $\sum_{x\in\{0,1\}^n,y\in\{0,1\}^n}\alpha_{x,y}|x\rangle|y\oplus\mathsf{F1P}_{c_{i,1}k_1,c_{i,2}k_2}^{P}(i,x)\oplus y\rangle$, where $c_{i,1},c_{i,2}\in\mathbb{F}_2^n\backslash\{0\}$. Namely, $\widetilde{\mathsf{F1PRK}}_{k_1,k_2}^{P}$ offers a related-key oracle of $\mathsf{F1P}_{k_1,k_2}^{P}$, whereas the online data complexity is limited to 1 for every related-key. While related-key increases adversarial power, the severely limited data complexity seems to prohibit using Simon's algorithm.

However, in this setting, Simon's algorithm remains applicable. In detail, consider the function $f : \mathcal{I} \times \{0,1\}^n \to \{0,1\}^n$ defined as

$$\begin{aligned} f(i,x) &:= \mathsf{F1P}^{P}_{c_{i,1}k_1,c_{i,2}k_2}(i,x) \oplus a_{23}P_i(a_{12}x) \oplus a_{22}x \\ &= a_{21}c_{i,2}k_2 \oplus a_{23}P_i(a_{11}c_{i,1}k_1 \oplus a_{12}x) \oplus a_{23}P_i(a_{12}x). \end{aligned} \tag{9}$$

Then for all $i \in \mathcal{I}$, the function $f(i,\cdot)$ is periodic with period $a_{12}^{-1}a_{11}c_{i,1}k_1$. The Simon's algorithm thus runs just as before, except that the $i$-th iteration produces a vector $s_i$ orthogonal to the corresponding period $a_{12}^{-1}a_{11}c_{i,1}k_1$. By this, after $O(n)$ iterations, if we view the obtained vectors $s_1, ..., s_\ell$ as column vectors, then we have a system of equations

$$\begin{matrix} \langle s_1, a_{12}^{-1}a_{11}c_{1,1}k_1\rangle = 0, \\ \langle s_2, a_{12}^{-1}a_{11}c_{2,1}k_1\rangle = 0, \\ \cdots \\ \langle s_\ell, a_{12}^{-1}a_{11}c_{\ell,1}k_1\rangle = 0 \end{matrix} \quad \Longrightarrow \quad \begin{matrix} \langle c_{1,1}^{-1}a_{11}^{-1}a_{12}s_1, k_1\rangle = 0, \\ \langle c_{2,1}^{-1}a_{11}^{-1}a_{12}s_2, k_1\rangle = 0, \\ \cdots \\ \langle c_{\ell,1}^{-1}a_{11}^{-1}a_{12}s_\ell, k_1\rangle = 0 \end{matrix}$$

It thus remains feasible to recover $k_1$ by solving equations.

This setting may appear in modes of operations using the 1-round tweakable Even-Mansour ciphers [22,51]. As a concrete example, the tweakable correlation robust hash function of Chen and Tessaro [21] defines $\mathsf{H}(i,x) := P(tx) \oplus tx$ mapping an index and an $n$-bit input to an $n$-bit output using the multiplication over $\mathbb{F}_2^n$, and ensures security that $\mathsf{H}(i_1, x \oplus k), ..., \mathsf{H}(i_\ell, x \oplus k)$ are $\ell$ independent pseudorandom functions. It is easy to see $\mathsf{H}(i_j, x \oplus k) = P(i_jk \oplus i_jx) \oplus i_jk \oplus i_jx$, which exactly fits into our above discussion.

## 4 Schemes with Two Permutations and Attacks

In this section, we first formally define our model for two-permutation-based pseudorandom (TPPR) schemes. Formally, let $P_1, P_2$ be two $n$-bit permutations. For a $3 \times 3$ matrix $\mathsf{A}$ of the form

$$\mathsf{A} = \begin{pmatrix} a_{00} & a_{01} & 0 \\ a_{10} & a_{11} & a_{12} \\ a_{20} & a_{21} & a_{22} \end{pmatrix}, \tag{10}$$

with $a_{ij} \in \mathbb{F}_2^n$. The keyed function $\mathsf{F2P}^{P_1,P_2}_{\mathsf{A},\mathbf{k}} : \{0,1\}^{3n} \times \{0,1\}^n \to \{0,1\}^n$ is defined as

$$\begin{aligned} \mathsf{F2P}^{P_1,P_2}_{\mathsf{A},\mathbf{k}}(x) = z, \text{ where } & y_1 \leftarrow P_1(a_{00}k_1 \oplus a_{01}x), \\ & y_2 \leftarrow P_2(a_{10}k_2 \oplus a_{11}x \oplus a_{12}y_1), \\ & z \leftarrow a_{20}k_3 \oplus a_{21}x \oplus a_{22}y_1 \oplus y_2. \end{aligned} \tag{11}$$

where multiplications are on the finite field $\mathbb{F}_2^n$. The function $\mathsf{F2P}^{P_1,P_2}_{\mathsf{A},\mathbf{k}}$ is depicted in Fig. 2. This in particular includes the 2-round Even-Mansour, the

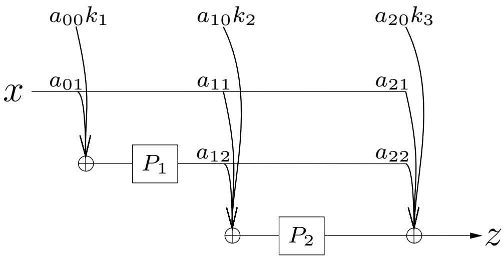

Fig. 2: The two permutation-based keyed function $\mathsf{F}_{\mathsf{A},\mathbf{k}}$ of Eq. (11).

SoEM PRF, the SoKAC1 PRF, and the PEDM PRF: we refer to Sect. 4.3.1 and 4.3.2 for detailed elaboration.

An initial observation is that the final operation of XORing $a_{21}x$ has no influence on key recovery security since $a_{21}$ is public, and we can always define

$$\begin{aligned}\mathsf{F2P}_{\mathsf{A},\mathbf{k}}^{P_1,P_2\,\prime}(x) &:= \mathsf{F2P}_{\mathsf{A},\mathbf{k}}^{P_1,P_2}(x) \oplus a_{21}x \\ &= P_2\big(a_{12}P_1(a_{01}x \oplus a_{00}k_1) \oplus a_{11}x \oplus a_{10}k_2\big) \\ &\qquad\qquad\qquad \oplus a_{22}P_1(a_{01}x \oplus a_{00}k_1) \oplus a_{20}k_3\end{aligned}$$

as the target of the attack. We thereby simply take $a_{21} = 0$ in our attacks.

## 4.1 Fully Degenerated Cases and Attacks using Simon's Algorithm

In this section, we identify "fully degenerated" TPPR schemes, i.e., those provide no Q2 security at all due to Simon's algorithm. To simplify the language, we define $Bo(a_{ij}) = 0$ if $a_{ij} = 0$, and $Bo(a_{ij}) = 1$ otherwise. Furthermore, if $a_{ij} = 0$ then we write $a_{ij}^{-1} = 0$.

### *4.1.1 Case 1: $Bo(a_{01}) = 0$*

Then the $P_1$ invocation does not depend on $x$ at all, and the construction becomes

$$\mathsf{F2P}_{\mathsf{A},\mathbf{k}}^{P_1,P_2}(x) = P_2(a_{12}P_1(a_{00}k_1) \oplus a_{11}x \oplus a_{10}k_2) \oplus a_{22}P_1(a_{00}k_1) \oplus a_{20}k_3.$$

Let $k_2' = a_{12}P_1(a_{00}k_1) \oplus a_{10}k_2$, $k_3' = a_{22}P_1(a_{00}k_1) \oplus a_{20}k_3$. Then the scheme becomes $\mathsf{F2P}_{\mathsf{A},\mathbf{k}}^{P_1,P_2}(x) = P_2(k_2' \oplus a_{11}x) \oplus k_3'$, and the attacks presented in Sect. 3 applies.

### *4.1.2 Case 2: Other Degenerated Cases*

1. when $(\overline{Bo(a_{10})} + \overline{Bo(a_{11})})\overline{Bo(a_{12})}\;\overline{Bo(a_{22})} = 1$, the construction provides no security even in the classical setting. In detail, when $\overline{Bo(a_{12})} = \overline{Bo(a_{22})} = 1$, the scheme becomes $\mathsf{F2P}_{\mathsf{A},\mathbf{k}}^{P_1,P_2}(x) = P_2(a_{11}x \oplus a_{10}k_2) \oplus a_{20}k_3$.

- when $\overline{Bo(a_{10})} = 1$, the scheme becomes $\mathsf{F2P}^{P_1,P_2}_{\mathsf{A},\mathbf{k}}(x) = P_2(a_{11}x) \oplus a_{20}k_3$, we can recover $k_3$ by $a_{20}^{-1}(\mathsf{F2P}^{P_1,P_2}_{\mathsf{A},\mathbf{k}}(x) \oplus P_2(a_{11}x)) = k_3$;
- when $\overline{Bo(a_{11})} = 1$, the scheme $\mathsf{F2P}^{P_1,P_2}_{\mathsf{A},\mathbf{k}}(x) = P_2(a_{10}k_2) \oplus a_{20}k_3$ is a constant, which is also trivially insecure.

2. when $\overline{Bo(a_{10})}(\overline{Bo(a_{12})}Bo(a_{22}) + \overline{Bo(a_{11})}Bo(a_{12})) + Bo(a_{10})\overline{Bo(a_{12})}(Bo(a_{11}) \oplus Bo(a_{22})) = 1$, the scheme again collapses to the EM construction. In detail,
   - when $Bo(a_{10}) = \overline{Bo(a_{12})} = 1$, the scheme becomes $\mathsf{F2P}^{P_1,P_2}_{\mathsf{A},\mathbf{k}}(x) = P_2(a_{11}x \oplus a_{10}k_2) \oplus a_{22}P_1(a_{01}x \oplus a_{00}k_1) \oplus a_{20}k_3$, we can see if $\overline{Bo(a_{11})} = 1$, the scheme $\mathsf{F2P}^{P_1,P_2}_{\mathsf{A},\mathbf{k}}(x) = P_2(a_{10}k_2) \oplus a_{22}P_1(a_{01}x \oplus a_{00}k_1) \oplus a_{20}k_3$ degenerate to the Even-Mansour scheme. And we can recover $P_2(a_{10}k_2) \oplus a_{20}k_3$ if $Bo(a_{00}) = 0$. If $\overline{Bo(a_{22})} = 1$, the scheme $\mathsf{F2P}^{P_1,P_2}_{\mathsf{A},\mathbf{k}}(x) = P_2(a_{11}x \oplus a_{10}k_2) \oplus a_{20}k_3$ degenerate to the Even-Mansour scheme. But if $\overline{Bo(a_{11})} = \overline{Bo(a_{22})} = 1$, the scheme $\mathsf{F2P}^{P_1,P_2}_{\mathsf{A},\mathbf{k}}(x) = P_2(a_{10}k_2) \oplus a_{20}k_3$ is a constant;
   - when $\overline{Bo(a_{10})} = \overline{Bo(a_{00})} = 1$, the scheme becomes $\mathsf{F2P}^{P_1,P_2}_{\mathsf{A},\mathbf{k}}(x) = P_2(a_{12}P_1(a_{01}x) \oplus a_{11}x) \oplus a_{22}P_1(a_{01}x) \oplus a_{20}k_3$. It is trivially insecure. When $\overline{Bo(a_{10})} = Bo(a_{00}) = 1$, the scheme becomes $\mathsf{F2P}^{P_1,P_2}_{\mathsf{A},\mathbf{k}}(x) = P_2(a_{12}P_1(a_{01}x \oplus a_{00}k_1) \oplus a_{11}x) \oplus a_{22}P_1(a_{01}x \oplus a_{00}k_1) \oplus a_{20}k_3$. Further:
     - when $\overline{Bo(a_{11})} = Bo(a_{12}) = 1$, the scheme becomes a keyless function $h$ whitened by two keys, i.e., $\mathsf{F2P}^{P_1,P_2}_{\mathsf{A},\mathbf{k}}(x) = h(x \oplus a_{01}^{-1}a_{00}k_1) \oplus a_{20}k_3$, where $h(u) = P_2(a_{12}P_1(u)) \oplus a_{22}P_1(u)$. Then the function $f' = \mathsf{F2P}^{P_1,P_2}_{\mathsf{A},\mathbf{k}}(x) \oplus h(x)$ has period $a_{01}^{-1}a_{00}k_1$ which just resembles the 1-round Even-Mansour cipher, and the scheme is thus breakable by using Simon's algorithm;
     - when $\overline{Bo(a_{12})} = Bo(a_{22}) = 1$, the scheme $\mathsf{F2P}^{P_1,P_2}_{\mathsf{A},\mathbf{k}}(x) = P_2(a_{11}x) \oplus a_{22}P_1(a_{01}x \oplus a_{00}k_1) \oplus a_{20}k_3$, and $f' = \mathsf{F2P}^{P_1,P_2}_{\mathsf{A},\mathbf{k}}(x) \oplus P_2(a_{11}x) \oplus a_{22}P_1(a_{01}x)$ has period $a_{01}^{-1}a_{00}k_1$ and can be broken by using Simon's algorithm.
3. when $\overline{Bo(a_{00})}(\overline{Bo(a_{12})} \oplus \overline{Bo(a_{11})}) = 1$, the scheme again collapses to the EM construction. In detail, when $\overline{Bo(a_{00})} = 1$, the input to $P_1$ is not secret, the scheme becomes $\mathsf{F2P}^{P_1,P_2}_{\mathsf{A},\mathbf{k}}(x) = P_2(a_{12}P_1(a_{01}x) \oplus a_{11}x \oplus a_{10}k_2) \oplus a_{20}k_3$.
   - when $\overline{Bo(a_{12})} = Bo(a_{11}) = 1$, the corresponding scheme $\mathsf{F2P}^{P_1,P_2}_{\mathsf{A},\mathbf{k}}(x) = P_2(a_{11}x \oplus a_{10}k_2) \oplus a_{20}k_3$ degenerate to the Even-Mansour scheme;
   - when $\overline{Bo(a_{11})} = Bo(a_{12}) = 1$, the corresponding scheme $\mathsf{F2P}^{P_1,P_2}_{\mathsf{A},\mathbf{k}}(x) = P_2(a_{12}P_1(a_{01}x) \oplus a_{10}k_2) \oplus a_{20}k_3$ degenerate to the Even-Mansour again.

The remaining cases appear secure against Simon's algorithm and will be addressed in the subsequent sections.

### 4.2 Cascaded Constructions with unkeyed Davies-Meyer

In this section, we identify the "partially degenerated" cascaded constructions with unkeyed Davies-Meyer ($\mathsf{CUDM}$). Such constructions could be viewed as

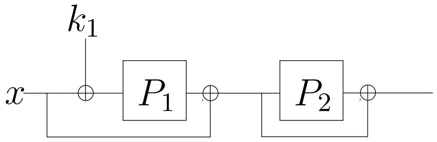

Fig. 3: Simplest variant of the function $\mathsf{CUDM1}_{k_1}^{P_1,P_2}$.

cascading a single permutation-based keyed "round function" and a variant of the (keyless) Davies-Meyer construction. The permutation invocation in the Davies-Meyer is somewhat "wasted" due to the non-secrecy. Though, no periodicity can be exhibited. Our discussion further distinguishes between two subcases in Sect. 4.2.1 and Sect. 4.2.2 respectively.

### *4.2.1 Subcase 1: Keyed round comes first*

By "keyed round comes first", it means the function is defined as

$$\mathsf{CUDM1}_{k_1}^{P_1,P_2}(x) := P_2(a_{12}P_1(a_{01}x \oplus a_{00}k_1) \oplus a_{11}x) \oplus a_{22}P_1(a_{01}x \oplus a_{00}k_1),$$

where $Bo(a_{00}), Bo(a_{01}), Bo(a_{11}), Bo(a_{12}), Bo(a_{22}) \neq 0$. The simplest variant has all the constants equal 1, and is depicted in Fig. 3.

**Algorithm 3** A (non-unique) claw-finding algorithm based on [15, Algorithm 4].

The input are two functions $h : \{0,1\}^n \to \{0,1\}^n$ and $g : \{0,1\}^n \to \{0,1\}^n$ to which we have quantum oracle access.[4] The output is a claw $(x, u)$ such that $h(x) = g(u)$. The parameters $r$ and $t$ are fixed and will be optimized later. For $r \in [1, ..., n]$, let $S_r^h := \big\{(x, h(x)) : \mathsf{left}_r\big(h(x)\big) = 0^r\big\}$ and $S_r^g := \big\{(x, g(x)) : \mathsf{left}_r\big(g(x)\big) = 0^r\big\}$. The algorithm works as follows.

1. Define a helper function $f_{S_r^g}(x) := 1$ if $x \in S_r^g$ and $f_{S_r^g}(x) := 1$ otherwise. Run Grover's search algorithm on $f_{S_r^g}$ for $2^{t-r}$ times to construct a list $L$ of $2^{t-r}$ elements from $S_r^g$. Let $f_L^h(x) := 1$ if $\exists(u, g(u)) \in L$ such that $h(x) = g(u)$ and $f_L^h(x) := 0$ otherwise.
2. Apply a quantum amplification algorithm where
   - The setup is the construction of $|\phi_r\rangle := \frac{1}{\sqrt{|S_r^h|}} \sum_{x \in S_r^h} |x, h(x)\rangle$.
   - The projector is a quantum oracle query to $O_{f_L^h}$ meaning that

$$O_{f_L^h}\big(|x, h(x)\rangle\ |b\rangle\big) = |x, h(x)\rangle\ \big|b \oplus f_L^h(x)\big\rangle.$$

The above quantum amplification algorithm is essentially a Grover search algorithm for $f_L^h$ but on input space $S_r^h$. The algorithm will output an element $(x, h(x))$ such that $f_L^h(x) = 1$, which means that $\exists(u, g(u)) \in L$, $h(x) = g(u)$. This gives rise to a claw.

[4] As argued in [15], when the input length of $h$, resp. $g$, is larger than the output length $n$, one can insert a pad to turn them into functions on $\{0,1\}^n$.

For simplicity, define $\mathrm{DMx}^{P_2}(u) := P_2(a_{22}a_{12}^{-1}u) \oplus a_{22}a_{12}^{-1}u$. Then we have $\mathsf{CUDM1}_{k_1}^{P_1,P_2}{}_{k}(x) \oplus a_{22}a_{12}^{-1}a_{11}x = \mathrm{DMx}^{P_2}\big(P_1(a_{01}x \oplus a_{00}k) \oplus a_{11}x\big)$. We defer discussion on obstacles on seeking for periodicity to the end of this subsection. For our attack, we seek for $x, u \in \{0,1\}^n$ such that $\mathsf{CUDM1}_{k_1}^{P_1,P_2}{}_{k}(x) \oplus a_{22}a_{12}^{-1}a_{11}x = \mathrm{DMx}^{P_2}(u)$. Once such a pair is found, it might indicate $P_1(a_{01}x \oplus a_{00}k) \oplus a_{11}x = u$, and $k_1$ is recovered by $k_1 = a_{00}^{-1}\big(P_1^{-1}(a_{11}x \oplus u) \oplus a_{01}x\big)$. This type of collision was also used in [54], though in the classical setting. In our quantum setting, it indicates the possibility of faster attacks using the quantum collision algorithm of Brassard et al. [14].

However, Chailloux et al. [15] argued that the use of $O(2^{n/3})$ qubits and $O(2^{n/3})$ quantum steps in [14] may be less convincing, and developed a quantum algorithm using $O(n)$ qubits, $O(2^{2n/5})$ quantum steps, and $O(2^{n/5})$ classical memory. Chailloux et al.'s algorithm [15, Algorithm 4] aims at finding collisions $h(x) = h(x')$ on a single function, whereas we are seeking for claws $h(x) = g(u)$ in this subsection. As we believe (non-unique) claw-finding in such specific settings is commonly used in symmetric cryptography, we adapt Algorithm 4 of Chailloux et al. and provide a dedicated claw-finding algorithm in Algorithm 3.

Running Algorithm 3 with $h(x) = \mathsf{CUDM1}_{k_1}^{P_1,P_2}(x) \oplus a_{22}a_{12}^{-1}a_{11}x$ and $g(u) = \mathrm{DMx}^{P_2}(u)$ yields a random $x$ such that there exists $(u, g(u)) \in L$ with $h(x) = g(u)$. The attacker then outputs $k_1 = a_{00}^{-1}\big(P_1^{-1}(a_{11}x \oplus u) \oplus a_{01}x\big)$ as the key. The complexities are the same as Chailloux et al., i.e., $O(n)$ qubits, $O(2^{2n/5})$ quantum steps, and $O(2^{n/5})$ classical memory. This remains faster than the naïve Grover key search (which needs $O(2^{n/2})$ quantum steps).

Regarding success probability, let $\mathcal{X} \subseteq \{0,1\}^n$ be the set such that $\forall x \in \mathcal{X}$, there exists $(u, g(u)) \in L$ with $h(x) = g(u)$. Then Algorithm 3 returns a random $x$ from $\mathcal{X}$. By constructions, for every $(u, g(u)) \in L$, a "clawed" $x \in \{0,1\}^n$ with $h(x) = g(u)$ may fall into two cases:

- **Right claw**: it holds $P_1(a_{01}x \oplus a_{00}k) \oplus a_{11}x = u$. The number of such collision is at least 1 for every $u$.
- **False positive**: $P_1(a_{01}x \oplus a_{00}k) \oplus a_{11}x = u' \neq u$, though $\mathrm{DMx}^{P_2}(u) = \mathrm{DMx}^{P_2}(u')$. Since the probability to have $\mathrm{DMx}^{P_2}(u) = \mathrm{DMx}^{P_2}(u')$ is $1/(2^n - 1)$, the expected number of such false positives for a single $u$ is $(2^n - 1)/(2^n - 1) = 1$.

By the above, the size of $\mathcal{X}$ is expected to be $2|L|$, and the number of right clawed $x$ in $\mathcal{X}$ is at least $|L|$. Therefore, with probability $1/2$, the value $x$ in the resulted claw $(x, u)$ does have $P_1(a_{01}x \oplus a_{00}k) \oplus a_{11}x = u$, and the subsequently recovered key $k_1$ is correct. Namely, the expected success probability of the above attack is $1/2$.

*Further discussion.* Such schemes are clearly unpreferable since the keyless "second round" does not increase security in the classical setting. In addition, symmetric cryptographic schemes typically have the key addition that goes "ahead of" the feeding forward. Though, the interesting observation is that the keyless "second round" as well as the abnormal key addition seem to protect the scheme against Simon attacks. To this end, consider the variant in Fig. 3 for simplicity:

- Without the keyless "second round" computation $P_2(u) \oplus u$, the scheme further collapses to a single permutation-based function, and attacks in Sect. 3 becomes feasible;
- Consider the variant $\mathsf{CUDM1}'^{P_1,P_2}_{k_1}(x) := P_2(P_1(x \oplus k_1) \oplus x \oplus k_1) \oplus P_1(x \oplus k_1)$, in which the input whitening key "runs ahead" of the feeding forward of $x$. This variant is a special case of whitened functions $h(x \oplus k_1)$ for $h$ a keyless function $h(u) = P_2(P_1(u) \oplus u) \oplus P_1(u)$, and Simon-based attacks become feasible again. The abnormal key addition, to some extent, renders the "inner" cryptographic function key-dependent, and this prohibits the approach of [47].

### *4.2.2 Davies-Meyer comes first*

When $Bo(a_{00}) = 0$ and further $Bo(a_{12})Bo(a_{11}) \neq 0$, let $k_2' = a_{10}k_2$, $k_3' = a_{20}k_3$. Then the input to $P_1$ is not secret, and the scheme becomes $\mathsf{CUDM}$ with "Davies-Meyer coming first". In detail, the function is defined as

$$\mathsf{CUDM2}^{P_1,P_2}_{k_2,k_3}(x) := P_2\big(a_{12}P_1(a_{01}x) \oplus a_{11}x \oplus k_2'\big) \oplus k_3'.$$

Let $u = P_1(a_{01}x) \oplus a_{12}^{-1}a_{11}x$, then we have $\mathsf{CUDM2}^{P_1,P_2}_{k_2,k_3}(x) = \mathsf{EMx}^{P_2}_{k_2',k_3'}(u) := P_2(a_{12}u \oplus k_2') \oplus k_3'$. While $\mathsf{EMx}^{P_2}_{k_2',k_3'}$ is a variant of the Even-Mansour cipher with known periodic properties for Simon's algorithm, the "first round" keyless function $x \mapsto P_1(a_{01}x) \oplus a_{12}^{-1}a_{11}x$ effectively destroys the periodic properties. In detail, to apply Simon's algorithm to $\mathsf{EMx}^{P_2}_{k_2',k_3'}$, it is required to construct the superposition $\sum_{u\in\{0,1\}^n} |u\rangle\big|\mathsf{EMx}^{P_2}_{k_2',k_3'}(u) \oplus P_2(u)\big\rangle$. One may attempt to make a superposition query to $|P_1\rangle$ and turn $\sum_{x\in\{0,1\}^n} |x\rangle|0\rangle|\mathsf{CUDM2}^{P_1,P_2}_{k_2,k_3}(x)\rangle$ into $\sum_{x\in\{0,1\}^n} |x\rangle|P_1(a_{01}x) \oplus a_{12}^{-1}a_{11}x\rangle|\mathsf{CUDM2}^{P_1,P_2}_{k_2,k_3}(x)\rangle$. However, the subtlety is that, when $a_{11}, a_{12} \neq 0$, the "first round" transformation $x \mapsto P_1(a_{01}x) \oplus a_{12}^{-1}a_{11}x$ is unlikely injective. Consequently, the second quantum register of the superposition $\sum_{x\in\{0,1\}^n} |x\rangle|P_1(a_{01}x) \oplus a_{12}^{-1}a_{11}x\rangle|\mathsf{CUDM2}^{P_1,P_2}_{k_2,k_3}(x)\rangle$ does not spam over $\{0,1\}^n$. It is thus infeasible to expect both $a_{12}P_1(a_{01}x) \oplus a_{11}x$ and $a_{12}P_1(a_{01}x) \oplus a_{11}x \oplus k_2'$ are in the second quantum register of the superposition $\sum_{x\in\{0,1\}^n} |x\rangle|P_1(a_{01}x) \oplus a_{12}^{-1}a_{11}x\rangle|\mathsf{CUDM2}^{P_1,P_2}_{k_2,k_3}(x)\rangle$. This also means Bonnetain et al.'s offline Simon's attack against the Even-Mansour [11, Sect. 5.1] is inapplicable either: their attack still crucially relies on the hidden periodicity, which, as discussed, was broken by the keyless "first round".

On the other hand, the idea of Kuwakado and Morii's attack [47] remains exploitable. Concretely, note that the periodic property of the "second round"

$$u = u' \oplus a_{12}^{-1}k_2 \Leftrightarrow P_2(a_{12}u \oplus k_2') \oplus k_3' \oplus P_2(u) = P_2(a_{12}u' \oplus k_2') \oplus k_3' \oplus P_2(u')$$

can be naturally extended to

$$\begin{aligned}
&a_{12}P_1(a_{01}x) \oplus a_{11}x = a_{12}P_1(a_{01}x') \oplus a_{11}x' \oplus k_2' \\
\Rightarrow\ &\mathsf{CUDM2}_{k_2,k_3}^{P_1,P_2}(x) \oplus P_2(a_{12}P_1(a_{01}x) \oplus a_{11}x) \\
&= \mathsf{CUDM2}_{k_2,k_3}^{P_1,P_2}(x') \oplus P_2(a_{12}P_1(a_{01}x') \oplus a_{11}x'). \qquad (12)
\end{aligned}$$

With this in mind, define

$$h(x) := \mathsf{CUDM2}_{k_2,k_3}^{P_1,P_2}(x) \oplus P_2(a_{12}P_1(a_{01}x) \oplus a_{11}x). \qquad (13)$$

Then, once we observe $h(x) = h(x')$, it might hold $a_{12}P_1(a_{01}x) \oplus a_{11}x = a_{12}P_1(a_{01}x') \oplus a_{11}x' \oplus k_2'$, in which case $k_2'$ could be recovered by $k_2' = a_{12}P_1(a_{01}x) \oplus a_{11}x \oplus a_{12}P_1(a_{01}x') \oplus a_{11}x'$. This inspires using quantum collision searching algorithm [15, Algorithm 4], which is essentially Algorithm 3 with $g = h$. In this case, a detailed investigation indicates that Algorithm 3 returns a random $x$ such that there exists $(x', h(x')) \in L$ with $h(x') = h(x)$. By constructions, for every $(x', h(x'))) \in L$, a collided $x \in \{0,1\}^n$ with $h(x) = h(x')$ may fall into three cases:

- **Right collision**: it holds $a_{12}P_1(a_{01}x) \oplus a_{11}x = a_{12}P_1(a_{01}x') \oplus a_{11}x' \oplus k_2'$, though $x \neq x'$. For every $(x', h(x')) \in L$, the number of such collision is expected to be $\approx 1$.
- **False positive I**: $a_{12}P_1(a_{01}x) \oplus a_{11}x = a_{12}P_1(a_{01}x') \oplus a_{11}x'$. For every $(x', h(x')) \in L$, the number of such collision is expected to be $\approx 1$.
- **False positive II**: $a_{12}P_1(a_{01}x) \oplus a_{11}x \neq a_{12}P_1(a_{01}x') \oplus a_{11}x' \oplus k_2'$ and $a_{12}P_1(a_{01}x) \oplus a_{11}x \neq a_{12}P_1(a_{01}x') \oplus a_{11}x'$, though $h(x) = h(x')$. The expected number of such false positives for a every $(x', h(x')) \in L$ is also close to 1.
- **False positive III**: $x = x'$. For every $(x', h(x')) \in L$, the number of such collision is 1.

Therefore, with probability $\approx 1/4$, the value $x$ in the resulted collision $(x, x')$ does have $a_{12}P_1(a_{01}x) \oplus a_{11}x = a_{12}P_1(a_{01}x') \oplus a_{11}x' \oplus k_2'$, and the subsequently recovered key $k_2'$ is correct. Namely, after a single application of Algorithm 3, the expected success probability is $\approx 1/4$. Note that the first and third types of false positives are easily detected, and an attacker could thus repeat the above iteration to increase the success probability.

We remark that, for $\mathsf{CUDM2}_{k_2,k_3}^{P_1,P_2}$, the interesting observation is that the keyless "first round" seems to protect the scheme against Simon's algorithm.

### 4.3 The Non-degenerated Case and Its Grover-meet-Simon Attack

When (and only when) $Bo(a_{10})Bo(a_{12}) + Bo(a_{10})Bo(a_{22})Bo(a_{11}) = 1$, the best key recovery attack we found is based on the Grover-meet-Simon algorithm. We call such cases non-degenerated, and elaborate our attack and concrete applications in this subsection.

In detail, we define $g(k,u) = P_2(a_{12}P_1(a_{01}u) \oplus a_{11}u \oplus k) \oplus a_{22}P_1(a_{01}u)$, $\mathsf{F2P}_{\mathsf{A},\mathbf{k}}^{P_1,P_2} = P_2(a_{12}P_1(a_{01}x \oplus a_{00}k_1) \oplus a_{11}x \oplus a_{10}k_2) \oplus a_{22}P_1(a_{01}x \oplus a_{00}k_1) \oplus a_{20}k_3$, and further

$$\begin{aligned} f'(x) =& \mathsf{F2P}_{\mathsf{A},\mathbf{k}}^{P_1,P_2}(x) \oplus \mathsf{F2P}_{\mathsf{A},\mathbf{k}}^{P_1,P_2}(x \oplus 1) \\ g'(k,x) =& g(k,x) \oplus g(k,x \oplus 1) \end{aligned}$$

Then

$$f'(x) \oplus g'(k',x) = f'(x \oplus a_{01}^{-1}a_{00}k_1) \oplus g'(k', x \oplus a_{01}^{-1}a_{00}k_1)$$

holds with $k' = a_{10}k_2 \oplus a_{11}a_{01}^{-1}a_{00}k_1$, i.e., $f'(x) \oplus g'(k',x)$ has a period $a_{01}^{-1}a_{00}k_1$. Thus the problem of recovering $\mathbf{k}$ fulfills the conditions of Problem 1 (Sect. 2.1.3), and we can apply Algorithm 1. Formally, the attack procedure is as follows.

*Attack Description*

1. Run Algorithm 1 for the above $f'$ and $g'$ to recover $k'$.
2. Apply Simon's algorithm to $f'(x) \oplus g'(k',x)$ to recover $k_1$.
3. Compute the two involved secret keys $a_{10}k_2 = k' \oplus a_{11}a_{01}^{-1}a_{00}k_1$ and $a_{20}k_3 = \mathsf{F2P}_{\mathsf{A},\mathbf{k}}^{P_1,P_2}(0^n) \oplus P_2(a_{12}P_1(a_{00}k_1) \oplus a_{10}k_2) \oplus a_{22}P_1(a_{00}k_1)$.

To ensure that the first step recovers $k'$ successfully, the condition Eq. (4) should be satisfied. For $i \neq k'$, the involved noisy collision event $f'(x) \oplus g'(i,x) = f'(x') \oplus g'(i,x')$ translates into

$$\begin{aligned} & P_2(a_{12}P_1(a_{01}x \oplus a_{00}k_1) \oplus a_{11}x \oplus a_{10}k_2) \\ & \quad \oplus a_{22}P_1(a_{01}x \oplus a_{00}k_1) \oplus a_{20}k_3 \\ \oplus & P_2(a_{12}P_1(a_{01}(x \oplus 1) \oplus a_{00}k_1) \oplus a_{11}(x \oplus 1) \oplus a_{10}k_2) \\ & \quad \oplus a_{22}P_1(a_{01}(x \oplus 1) \oplus a_{00}k_1) \oplus a_{20}k_3 \\ \oplus & P_2(a_{12}P_1(a_{01}x) \oplus a_{11}x \oplus i) \\ & \quad \oplus a_{22}P_1(a_{01}x) \\ \oplus & P_2(a_{12}P_1(a_{01}(x \oplus 1)) \oplus a_{11}(x \oplus 1) \oplus i) \\ & \quad \oplus a_{22}P_1(a_{01}(x \oplus 1)) \\ = & P_2(a_{12}P_1(a_{01}x' \oplus a_{00}k_1) \oplus a_{11}x' \oplus a_{10}k_2) \\ & \quad \oplus a_{22}P_1(a_{01}x' \oplus a_{00}k_1) \oplus a_{20}k_3 \\ \oplus & P_2(a_{12}P_1(a_{01}(x' \oplus 1) \oplus a_{00}k_1) \oplus a_{11}(x' \oplus 1) \oplus a_{10}k_2) \\ & \quad \oplus a_{22}P_1(a_{01}(x' \oplus 1) \oplus a_{00}k_1) \oplus a_{20}k_3 \\ \oplus & P_2(a_{12}P_1(a_{01}x') \oplus a_{11}x' \oplus i) \\ & \quad \oplus a_{22}P_1(a_{01}x') \\ \oplus & P_2(a_{12}P_1(a_{01}(x' \oplus 1)) \oplus a_{11}(x' \oplus 1) \oplus i) \\ & \quad \oplus a_{22}P_1(a_{01}(x' \oplus 1)). \end{aligned}$$

On the other hand, to ensure that the second step recovers $k_1$ successfully, the condition Eq. (3) should be satisfied. For $i = k'$, the involved collision event is $f'(x) \oplus g'(k', x) = f'(x \oplus t) \oplus g'(k', x \oplus t)$, $t \neq a_{01}^{-1} a_{00} k_1$. This condition translates into

$$\begin{aligned}
&P_2(a_{12}P_1(a_{01}x \oplus a_{00}k_1) \oplus a_{11}x \oplus a_{10}k_2)\\
&\quad \oplus a_{22}P_1(a_{01}x \oplus a_{00}k_1) \oplus a_{20}k_3\\
&\oplus P_2(a_{12}P_1(a_{01}(x \oplus 1) \oplus a_{00}k_1) \oplus a_{11}(x \oplus 1) \oplus a_{10}k_2)\\
&\quad \oplus a_{22}P_1(a_{01}(x \oplus 1) \oplus a_{00}k_1) \oplus a_{20}k_3\\
&\oplus P_2(a_{12}P_1(a_{01}x) \oplus a_{11}x \oplus k')\\
&\quad \oplus a_{22}P_1(a_{01}x)\\
&\oplus P_2(a_{12}P_1(a_{01}(x \oplus 1)) \oplus a_{11}(x \oplus 1) \oplus k')\\
&\quad \oplus a_{22}P_1(a_{01}(x \oplus 1))\\
&= P_2(a_{12}P_1(a_{01}(x \oplus t) \oplus a_{00}k_1) \oplus a_{11}(x \oplus t) \oplus a_{10}k_2)\\
&\quad \oplus a_{22}P_1(a_{01}(x \oplus t) \oplus a_{00}k_1) \oplus a_{20}k_3\\
&\oplus P_2(a_{12}P_1(a_{01}(x \oplus t \oplus 1) \oplus a_{00}k_1) \oplus a_{11}(x \oplus t \oplus 1) \oplus a_{10}k_2)\\
&\quad \oplus a_{22}P_1(a_{01}(x \oplus t \oplus 1) \oplus a_{00}k_1) \oplus a_{20}k_3\\
&\oplus P_2(a_{12}P_1(a_{01}(x \oplus t)) \oplus a_{11}(x \oplus t) \oplus k')\\
&\quad \oplus a_{22}P_1(a_{01}(x \oplus t))\\
&\oplus P_2(a_{12}P_1(a_{01}(x \oplus t \oplus 1)) \oplus a_{11}(x \oplus t \oplus 1) \oplus k')\\
&\quad \oplus a_{22}P_1(a_{01}(x \oplus t \oplus 1)).
\end{aligned}$$

Both of the above two equations are related to third order differential properties of $P_2$. While we found no explicit upper bound in the literature, the bound $\frac{1}{2}$ is likely fulfilled when $P_2$ is a random permutation. In all, we can assume that $f'(x) \oplus g'(k', x)$ is far from periodic for all $i \neq k'$, and that the condition Eq. (4) in Problem 1 is fulfilled. By this and by the discussion in 2.1.3 and [11, Proposition 2], our attack recovers the keys of $\mathsf{F2P}_{\mathsf{A},\mathbf{k}}^{P_1,P_2}(x)$ with overwhelming probability by making $O(n)$ quantum queries to the (keyed) online oracle $|\mathsf{F2P}_{\mathsf{A},\mathbf{k}}^{P_1,P_2}(x) \oplus \mathsf{F2P}_{\mathsf{A},\mathbf{k}}^{P_1,P_2}(x \oplus 1)\rangle$ and performing $O(n2^{n/2})$ quantum steps as well as $O(n^3 2^{n/2})$ classical computations. Note that when the keys $k_1, k_2, k_3$ are *not* independent, the attack remains effective: it just runs as if the keys are independent.

### *4.3.1 Straightforward applications*

In this section, we discuss (straightforward) applications of our attack to recent permutation-based PRFs. First, the SoEM PRF introduce by Chen et al. [20] is defined as

$$\mathsf{SoEM}_{\nu_1,\nu_2}^{P_1,P_2}(x) = P_2(x \oplus \nu_2) \oplus P_1(x \oplus \nu_1) \oplus \nu_1 \oplus \nu_2,$$

where $\nu_1, \nu_2 \in \{0,1\}^n$ are two independent keys. This corresponds to $a_{00} = a_{01} = a_{10} = a_{11} = a_{20} = a_{22} = 1$, $a_{12} = a_{21} = 0$, and $(k_1, k_2, k_3) =$

$(\nu_1, \nu_2, \nu_1 \oplus \nu_2)$. The application of our attack in Sect. 4.3 is straightforward (recall that our attack remains effective against correlated keys $k_1, k_2, k_3$). The complexity of our attack is $O(cn)$ superposition queries to $\left|\mathsf{SoEM}^{P_1,P_2}_{\nu_1,\nu_2}\right\rangle$ and $O(n2^{n/2})$ quantum steps. Superposition attacks against $\mathsf{SoEM}$ have been exhibited in [63], which are applications of the original Grover-meet-Simon algorithm of [48] and consume $O(n2^{n/2})$ superposition queries to $\left|\mathsf{SoEM}^{P_1,P_2}_{\nu_1,\nu_2}\right\rangle$ and quantum steps. Thanks to our use of Bonnetain et al. [11], our attack has a much smaller quantum data complexity.

The construction $\mathsf{SoEM}$ is parallel. Chen et al. [20] also proposed a sequential PRF

$$\mathsf{SoKAC21}^{P_1,P_2}_{\nu}(x) = \nu \oplus P_2\big(\nu \oplus P_1(\nu \oplus x)\big) \oplus P_1(\nu \oplus x),$$

and proved security up to $2^{2n/3}$ queries. As mentioned in the Introduction, this result turned out flawed [54], and Chakraborti et al. [16] proposed a two key variant

$$\mathsf{SoKAC1}^{P}_{\nu_1,\nu_2}(x) = \nu_1 \oplus \nu_2 \oplus P\big(\nu_2 \oplus P(\nu_1 \oplus x)\big) \oplus P(\nu_1 \oplus x)$$

and bridge the gap. Later Dutta et al. [31] proposed an inverse-free PRF $\mathsf{PEDM}$ using two $n$-bit keys $k_1, k_2$, which is defined as

$$\mathsf{PEDM}^{P}_{\nu_1,\nu_2}(x) = \nu_1 \oplus P\big(\nu_1 \oplus x \oplus \nu_2 \oplus P(\nu_1 \oplus x)\big).$$

It is easy to see $\mathsf{SoKAC1}^{P}_{\nu_1,\nu_2}$ corresponds to $a_{00} = a_{01} = a_{10} = a_{12} = a_{20} = a_{22} = 1$, $a_{11} = a_{21} = 0$, and $(k_1, k_2, k_3) = (\nu_1, \nu_2, \nu_1 \oplus \nu_2)$. On the other hand, $\mathsf{PEDM}^{P}_{\nu_1,\nu_2}$ corresponds to $a_{00} = a_{01} = a_{10} = a_{11} = a_{12} = a_{20} = 1$, $a_{21} = a_{22} = 0$, and $(k_1, k_2, k_3) = (\nu_1, \nu_1 \oplus \nu_2, \nu_1)$. The applications of our attack in Sect. 4.3 to $\mathsf{SoKAC1}^{P}_{\nu_1,\nu_2}$ and $\mathsf{PEDM}^{P}_{\nu_1,\nu_2}$ are thus straightforward, and the costs are $O(cn)$ quantum data and $O(n2^{n/2})$ quantum steps as before.

### *4.3.2 Application to 2-round (tweakable) Even-Mansour ciphers*

The 2-round Even-Mansour cipher using three independent round keys first appears in [8] and is defined as

$$\mathsf{EM2IK}^{P_1,P_2}_{k_0,k_1,k_2}(x) := k_2 \oplus P_2\big(k_1 \oplus P_1(k_0 \oplus x)\big). \tag{14}$$

This corresponds to $a_{00} = a_{01} = a_{10} = a_{12} = a_{20} = 1$ and $a_{11} = a_{21} = a_{22} = 0$, and the application of our attack in Sect. 4.3 is straightforward. The complexity of our attack is $O(cn)$ data and $O(n2^{n/2})$ quantum steps.

The naïve Grover key search consumes $O(2^{3n/2})$ quantum steps. If we apply the idea of Kaplan [43] to the classical meet-in-the-middle attack on $\mathsf{EM2IK}^{P_1,P_2}_{k_0,k_1,k_2}$, we obtain a quantum meet-in-the-middle attack on $\mathsf{EM2IK}^{P_1,P_2}_{k_0,k_1,k_2}$ with $O(2^{2n/3})$ quantum steps. Though, both are more expensive than our attack.

The construction $\mathsf{EM2IK}^{P_1,P_2}_{k_0,k_1,k_2}$ is generalized to many variants with correlated round keys [19,18], i.e., the keys $k_0, k_1, k_2$ are derived from a single master key $K \in \{0,1\}^\kappa$ using a key schedule function $(k_0, k_1, k_2) \leftarrow \gamma(K)$. We denote such variant by $\mathsf{EM2}^{P_1,P_2}_{K,\gamma}$. Though, using the idea of all-subkeys-recovery of Isobe and Shibutani [40], we can simply assume that the cipher $\mathsf{EM2}$ is using independent round keys $k_0, k_1, k_2$, and directly recover these round keys instead of the master key $K$. Therefore, our attack in Sect. 4.3 remains applicable to $\mathsf{EM2}^{P_1,P_2}_{K,\gamma}$. As long as $\kappa \gg n+2\log_2 n$, our attack complexity $O(n2^{n/2})$ is better than $O(2^{\kappa/2})$ of the naïve Grover key search.

Cogliati et al. [22] introduce the 2-round tweakable Even-Mansour cipher, which is defined as

$$\mathsf{TEM2}^{P_1,P_2}_{h_1,h_2}(t,x) := h_2(t) \oplus P_2\Big(h_2(t) \oplus h_1(t) \oplus P_1\big(h_1(t) \oplus x\big)\Big), \tag{15}$$

where the keys $h_1$ and $h_2$ are two (secret) universal hash functions. Cogliati et al. proved that this construction is a secure tweakable blockcipher up to beyond birthday $2^{2n/3}$ adversarial queries. Subsequently Dutta [28] proved that a simplified variant of $\mathsf{TEM2}^{P_1,P_2}_{h_1,h_2}(t,x)$ with $P_1 = P_2$ remains secure up to $2^{2n/3}$ queries.

While the attack spectrum of tweakable blockciphers is much wider than a standard PRF/PRP, here we simply focus on (the most devastating) key recovery attack. To this end, note that once we fix the tweak $t$, the scheme $\mathsf{TEM2}^{P_1,P_2}_{h_1,h_2}(t,\cdot)$ collapses to the aforementioned $\mathsf{EM2IK}^{P_1,P_2}_{k_0,k_1,k_2}$ with $k_0 = h_1(t)$, $k_1 = h_2(t) \oplus h_1(t)$, and $k_2 = h_2(t)$. Therefore, once allowed to make $O(cn)$ superposition queries *with the same tweak* $t$, the two corresponding secrets $h_1(t)$ and $h_2(t)$ can be recovered after $O(n2^{n/2})$ quantum steps. Then, the secret keys $h_1$ and $h_2$ are typically computable. For example, the multiplication-based hash introduce by Shoup [65] is defend as

$$h(t_1\|...\|t_\ell) := \sum_{j=1}^{\ell} s^j t_j,$$

where $s \in \mathbb{F}_2^n$ is the key of the hash, and multiplications are on the field $\mathbb{F}_2^n$. It is clearly easy to recover $s$ via solving the equation $h_i(t_1\|...\|t_\ell) = \sum_{j=1}^{\ell} s_i^j t_j$.

## 5 Conclusion

We study superposition attacks against pseudorandom schemes built upon $n$-bit keyless permutations. Using Simon's algorithm, we exhibit key recovery attacks against all "full-domain" pseudorandom schemes built upon a single permutation, with polynomial $O(n)$ quantum complexities. Using the recently proposed improved Grover-meet-Simon algorithm, we exhibit key recovery attacks against all "full-domain" pseudorandom schemes built upon two permutations, with $O(n)$ quantum data and $O(n2^{n/2})$ quantum computations. We also identify certain weak designs and exhibit faster attacks using either Simon's algorithm or quantum collision searching. Our attacks are applicable to a number of popular permutation-based schemes.

In the classical setting, the $t$-round iterated Even-Mansour cipher ensures security up to at most $2^{\frac{tn}{t+1}}$ queries. By this, it seems natural to conjecture a superposition attacker (with unlimited quantum steps) could break $t$ permutation-based schemes within $n2^{\frac{(t-1)n}{t}}$ permutation queries, which somehow matches the "Reciprocal Plus 1 Rule" of Liu and Zhandry [50]. However, the straightforward application of Grover-meet-Simon does not work since the number of to-be-guessed key bits quickly exceeds $2n$.

## References

1. Alagic, G., Bai, C., Katz, J., Majenz, C.: Post-quantum security of the even-mansour cipher. Cryptology ePrint Archive, Report 2021/1601 (2021), https://ia.cr/2021/1601
2. Alagic, G., Russell, A.: Quantum-secure symmetric-key cryptography based on hidden shifts. In: Coron, J., Nielsen, J.B. (eds.) EUROCRYPT 2017, Part III. LNCS, vol. 10212, pp. 65–93. Springer, Heidelberg (Apr / May 2017)
3. Anand, M.V., Targhi, E.E., Tabia, G.N., Unruh, D.: Post-quantum security of the CBC, CFB, OFB, CTR, and XTS modes of operation. In: Takagi, T. (ed.) Post-Quantum Cryptography - 7th International Workshop, PQCrypto 2016. pp. 44–63. Springer, Heidelberg (2016)
4. Bertoni, G., Daemen, J., Peeters, M., Van Assche, G.: On the indifferentiability of the sponge construction. In: Smart, N.P. (ed.) EUROCRYPT 2008. LNCS, vol. 4965, pp. 181–197. Springer, Heidelberg (Apr 2008)
5. Bhattacharjee, A., Dutta, A., List, E., Nandi, M.: CENCPP* - beyond-birthday-secure encryption from public permutations. Cryptology ePrint Archive, Report 2020/602 (2020), https://eprint.iacr.org/2020/602
6. Bhaumik, R., Bonnetain, X., Chailloux, A., Leurent, G., Naya-Plasencia, M., Schrottenloher, A., Seurin, Y.: QCB: efficient quantum-secure authenticated encryption. In: Tibouchi, M., Wang, H. (eds.) Advances in Cryptology - ASIACRYPT 2021 - 27th International Conference on the Theory and Application of Cryptology and Information Security, Singapore, December 6-10, 2021, Proceedings, Part I. Lecture Notes in Computer Science, vol. 13090, pp. 668–698. Springer (2021), https://doi.org/10.1007/978-3-030-92062-3_23
7. Black, J., Cochran, M., Shrimpton, T.: On the impossibility of highly-efficient blockcipher-based hash functions. In: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 526–541. Springer, Heidelberg (May 2005)
8. Bogdanov, A., Knudsen, L.R., Leander, G., Standaert, F.X., Steinberger, J.P., Tischhauser, E.: Key-alternating ciphers in a provable setting: Encryption using a small number of public permutations - (extended abstract). In: Pointcheval, D., Johansson, T. (eds.) EUROCRYPT 2012. LNCS, vol. 7237, pp. 45–62. Springer, Heidelberg (Apr 2012)
9. Boneh, D., Zhandry, M.: Quantum-secure message authentication codes. In: Johansson, T., Nguyen, P.Q. (eds.) EUROCRYPT 2013. LNCS, vol. 7881, pp. 592–608. Springer, Heidelberg (May 2013)
10. Boneh, D., Zhandry, M.: Secure signatures and chosen ciphertext security in a quantum computing world. In: Canetti, R., Garay, J.A. (eds.) CRYPTO 2013, Part II. LNCS, vol. 8043, pp. 361–379. Springer, Heidelberg (Aug 2013)
11. Bonnetain, X., Hosoyamada, A., Naya-Plasencia, M., Sasaki, Y., Schrottenloher, A.: Quantum attacks without superposition queries: The offline Simon's algorithm. In: Galbraith, S.D., Moriai, S. (eds.) ASIACRYPT 2019, Part I. LNCS, vol. 11921, pp. 552–583. Springer, Heidelberg (Dec 2019)

12. Bonnetain, X., Naya-Plasencia, M.: Hidden shift quantum cryptanalysis and implications. In: Peyrin, T., Galbraith, S. (eds.) ASIACRYPT 2018, Part I. LNCS, vol. 11272, pp. 560–592. Springer, Heidelberg (Dec 2018)
13. Brassard, G., Høyer, P.: An exact quantum polynomial-time algorithm for simon's problem. In: Fifth Israel Symposium on Theory of Computing and Systems, ISTCS 1997, Ramat-Gan, Israel, June 17-19, 1997, Proceedings. pp. 12–23. IEEE Computer Society (1997), https://doi.org/10.1109/ISTCS.1997.595153
14. Brassard, G., Høyer, P., Tapp, A.: Quantum cryptanalysis of hash and claw-free functions. In: LATIN '98: Theoretical Informatics, Third Latin American Symposium, Campinas, Brazil, April, 20-24, 1998, Proceedings. pp. 163–169 (1998), https://doi.org/10.1007/BFb0054319
15. Chailloux, A., Naya-Plasencia, M., Schrottenloher, A.: An efficient quantum collision search algorithm and implications on symmetric cryptography. In: Takagi, T., Peyrin, T. (eds.) ASIACRYPT 2017, Part II. LNCS, vol. 10625, pp. 211–240. Springer, Heidelberg (Dec 2017)
16. Chakraborti, A., Nandi, M., Talnikar, S., Yasuda, K.: On the composition of single-keyed tweakable Even-Mansour for achieving BBB security. IACR Trans. Symm. Cryptol. 2020(2), 1–39 (2020)
17. Chakraborty, D., Dutta, A., Kundu, S.: Designing tweakable enciphering schemes using public permutations. Cryptology ePrint Archive, Report 2021/128 (2021), https://ia.cr/2021/128
18. Chen, S., Lampe, R., Lee, J., Seurin, Y., Steinberger, J.P.: Minimizing the two-round Even-Mansour cipher. Journal of Cryptology 31(4), 1064–1119 (Oct 2018)
19. Chen, S., Steinberger, J.P.: Tight security bounds for key-alternating ciphers. In: Nguyen, P.Q., Oswald, E. (eds.) EUROCRYPT 2014. LNCS, vol. 8441, pp. 327–350. Springer, Heidelberg (May 2014)
20. Chen, Y.L., Lambooij, E., Mennink, B.: How to build pseudorandom functions from public random permutations. In: Boldyreva, A., Micciancio, D. (eds.) CRYPTO 2019, Part I. LNCS, vol. 11692, pp. 266–293. Springer, Heidelberg (Aug 2019)
21. Chen, Y.L., Tessaro, S.: Better security-efficiency trade-offs in permutation-based two-party computation. In: Advances in Cryptology - ASIACRYPT 2021 - 27th International Conference on the Theory and Application of Cryptology and Information Security, Singapore, December 6-10, 2021, Proceedings, Part II. pp. 275–304 (2021), https://doi.org/10.1007/978-3-030-92075-3_10
22. Cogliati, B., Lampe, R., Seurin, Y.: Tweaking Even-Mansour ciphers. In: Gennaro, R., Robshaw, M.J.B. (eds.) CRYPTO 2015, Part I. LNCS, vol. 9215, pp. 189–208. Springer, Heidelberg (Aug 2015)
23. Cogliati, B., Seurin, Y.: Beyond-birthday-bound security for tweakable Even-Mansour ciphers with linear tweak and key mixing. In: Iwata, T., Cheon, J.H. (eds.) ASIACRYPT 2015, Part II. LNCS, vol. 9453, pp. 134–158. Springer, Heidelberg (Nov / Dec 2015)
24. Daemen, J.: Limitations of the Even-Mansour construction (rump session). In: Imai, H., Rivest, R.L., Matsumoto, T. (eds.) ASIACRYPT'91. LNCS, vol. 739, pp. 495–498. Springer, Heidelberg (Nov 1993)
25. Dinur, I., Dunkelman, O., Keller, N., Shamir, A.: Key recovery attacks on 3-round Even-Mansour, 8-step LED-128, and full AES2. In: Sako, K., Sarkar, P. (eds.) ASIACRYPT 2013, Part I. LNCS, vol. 8269, pp. 337–356. Springer, Heidelberg (Dec 2013)
26. Dong, X., Dong, B., Wang, X.: Quantum attacks on some feistel block ciphers. Des. Codes Cryptogr. 88(6), 1179–1203 (2020), https://doi.org/10.1007/s10623-020-00741-y
27. Dunkelman, O., Keller, N., Shamir, A.: Slidex attacks on the Even-Mansour encryption scheme. Journal of Cryptology 28(1), 1–28 (Jan 2015)
28. Dutta, A.: Minimizing the two-round tweakable Even-Mansour cipher. In: ASIACRYPT 2020, Part I. pp. 601–629. LNCS, Springer, Heidelberg (Dec 2020)
29. Dutta, A., Nandi, M.: BBB secure nonce based MAC using public permutations. Cryptology ePrint Archive, Report 2020/509 (2020), https://eprint.iacr.org/2020/509
30. Dutta, A., Nandi, M.: BBB secure nonce based MAC using public permutations. In: AFRICACRYPT 20. pp. 172–191. LNCS, Springer, Heidelberg (2020)

31. Dutta, A., Nandi, M., Talnikar, S.: Permutation based edm: An inverse free bbb secure prf. IACR Transactions on Symmetric Cryptology 2021(2), 31–70 (Jun 2021), https://tosc.iacr.org/index.php/ToSC/article/view/8905
32. Even, S., Mansour, Y.: A construction of a cipher from a single pseudorandom permutation. Journal of Cryptology 10(3), 151–162 (Jun 1997)
33. Granger, R., Jovanovic, P., Mennink, B., Neves, S.: Improved masking for tweakable blockciphers with applications to authenticated encryption. In: Fischlin, M., Coron, J.S. (eds.) EUROCRYPT 2016, Part I. LNCS, vol. 9665, pp. 263–293. Springer, Heidelberg (May 2016)
34. Grover, L.K.: A fast quantum mechanical algorithm for database search. In: 28th ACM STOC. pp. 212–219. ACM Press (May 1996)
35. Guo, C., Katz, J., Wang, X., Weng, C., Yu, Y.: Better concrete security for half-gates garbling (in the multi-instance setting). In: Shacham, H., Boldyreva, A. (eds.) CRYPTO 2020, Part II. pp. 793–822. LNCS, Springer, Heidelberg (Aug 2020)
36. Guo, C., Katz, J., Wang, X., Yu, Y.: Efficient and secure multiparty computation from fixed-key block ciphers. In: 2020 IEEE Symposium on Security and Privacy. pp. 825–841. IEEE Computer Society Press (2020)
37. Hoang, V.T., Tessaro, S.: Key-alternating ciphers and key-length extension: Exact bounds and multi-user security. In: Robshaw, M., Katz, J. (eds.) CRYPTO 2016, Part I. LNCS, vol. 9814, pp. 3–32. Springer, Heidelberg (Aug 2016)
38. Hosoyamada, A., Iwata, T.: 4-round Luby-Rackoff construction is a qPRP. In: Galbraith, S.D., Moriai, S. (eds.) ASIACRYPT 2019, Part I. LNCS, vol. 11921, pp. 145–174. Springer, Heidelberg (Dec 2019)
39. ISO: Iso/iec 29192-5:2016, information technology – security techniques – 727 lightweight cryptography – part 5: Hash-functions (2016), https://www.iso.org/standard/67173.html
40. Isobe, T., Shibutani, K.: All subkeys recovery attack on block ciphers: Extending meet-in-the-middle approach. In: Knudsen, L.R., Wu, H. (eds.) SAC 2012. LNCS, vol. 7707, pp. 202–221. Springer, Heidelberg (Aug 2013)
41. Iwata, T.: New blockcipher modes of operation with beyond the birthday bound security. In: Robshaw, M.J.B. (ed.) FSE 2006. LNCS, vol. 4047, pp. 310–327. Springer, Heidelberg (Mar 2006)
42. Jaeger, J., Song, F., Tessaro, S.: Quantum Key-Length Extension. In: Theory of Cryptography - 19th International Conference, TCC 2021, Raleigh, NC, USA, November 8-11, 2021, Proceedings, Part I. pp. 209–239 (2021), https://doi.org/10.1007/978-3-030-90459-3_8
43. Kaplan, M.: Quantum attacks against iterated block ciphers. CoRR abs/1410.1434 (2014), http://arxiv.org/abs/1410.1434
44. Kaplan, M., Leurent, G., Leverrier, A., Naya-Plasencia, M.: Breaking symmetric cryptosystems using quantum period finding. In: Robshaw, M., Katz, J. (eds.) CRYPTO 2016, Part II. LNCS, vol. 9815, pp. 207–237. Springer, Heidelberg (Aug 2016)
45. Kaplan, M., Leurent, G., Leverrier, A., Naya-Plasencia, M.: Quantum differential and linear cryptanalysis. IACR Trans. Symm. Cryptol. 2016(1), 71–94 (2016), https://tosc.iacr.org/index.php/ToSC/article/view/536
46. Kuwakado, H., Morii, M.: Quantum distinguisher between the 3-round feistel cipher and the random permutation. In: IEEE International Symposium on Information Theory, ISIT 2010, June 13-18, 2010, Austin, Texas, USA, Proceedings. pp. 2682–2685 (2010), https://doi.org/10.1109/ISIT.2010.5513654
47. Kuwakado, H., Morii, M.: Security on the quantum-type even-mansour cipher. In: Proceedings of the International Symposium on Information Theory and its Applications, ISITA 2012, Honolulu, HI, USA, October 28-31, 2012. pp. 312–316 (2012), https://ieeexplore.ieee.org/document/6400943/
48. Leander, G., May, A.: Grover meets simon - quantumly attacking the FX-construction. In: Takagi, T., Peyrin, T. (eds.) ASIACRYPT 2017, Part II. LNCS, vol. 10625, pp. 161–178. Springer, Heidelberg (Dec 2017)
49. Leurent, G., Sibleyras, F.: Low-memory attacks against two-round even-mansour using the 3-XOR problem. In: Boldyreva, A., Micciancio, D. (eds.) CRYPTO 2019, Part II. LNCS, vol. 11693, pp. 210–235. Springer, Heidelberg (Aug 2019)

50. Liu, Q., Zhandry, M.: On finding quantum multi-collisions. In: Ishai, Y., Rijmen, V. (eds.) EUROCRYPT 2019, Part III. LNCS, vol. 11478, pp. 189–218. Springer, Heidelberg (May 2019)
51. Mennink, B.: XPX: Generalized tweakable Even-Mansour with improved security guarantees. In: Robshaw, M., Katz, J. (eds.) CRYPTO 2016, Part I. LNCS, vol. 9814, pp. 64–94. Springer, Heidelberg (Aug 2016)
52. Mennink, B., Preneel, B.: Hash functions based on three permutations: A generic security analysis. In: Safavi-Naini, R., Canetti, R. (eds.) CRYPTO 2012. LNCS, vol. 7417, pp. 330–347. Springer, Heidelberg (Aug 2012)
53. Mouha, N., Mennink, B., Van Herrewege, A., Watanabe, D., Preneel, B., Verbauwhede, I.: Chaskey: An efficient MAC algorithm for 32-bit microcontrollers. In: Joux, A., Youssef, A.M. (eds.) SAC 2014. LNCS, vol. 8781, pp. 306–323. Springer, Heidelberg (Aug 2014)
54. Nandi, M.: Mind the composition: Birthday bound attacks on EWCDMD and SoKAC21. In: Rijmen, V., Ishai, Y. (eds.) EUROCRYPT 2020, Part I. pp. 203–220. LNCS, Springer, Heidelberg (May 2020)
55. Nikolic, I., Wang, L., Wu, S.: Cryptanalysis of round-reduced LED. In: Moriai, S. (ed.) FSE 2013. LNCS, vol. 8424, pp. 112–129. Springer, Heidelberg (Mar 2014)
56. NIST: Nist lightweight cryptography. https://csrc.nist.gov/Projects/ Lightweight-Cryptography.
57. NIST: Nist post-quantum cryptography standardization process. https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization.
58. NIST: Nist sha-3 project. https://csrc.nist.gov/projects/hash-functions/ sha-3-project.
59. O'Connor, L.: On the distribution of characteristics in bijective mappings. Journal of Cryptology 8(2), 67–86 (Mar 1995)
60. Rogaway, P., Steinberger, J.P.: Security/efficiency tradeoffs for permutation-based hashing. In: Smart, N.P. (ed.) EUROCRYPT 2008. LNCS, vol. 4965, pp. 220–236. Springer, Heidelberg (Apr 2008)
61. Santoli, T., Schaffner, C.: Using simon's algorithm to attack symmetric-key cryptographic primitives. Quantum Inf. Comput. 17(1&2), 65–78 (2017), https://doi.org/10.26421/QIC17.1-2-4
62. Shinagawa, K., Iwata, T.: Quantum attacks on sum of even-mansour pseudorandom functions. Information Processing Letters 173, 106172 (2022), https://www.sciencedirect.com/science/article/pii/S0020019021000879
63. 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
64. Shor, P.W.: Algorithms for quantum computation: Discrete logarithms and factoring. In: 35th FOCS. pp. 124–134. IEEE Computer Society Press (Nov 1994)
65. Shoup, V.: On fast and provably secure message authentication based on universal hashing. In: Koblitz, N. (ed.) CRYPTO'96. LNCS, vol. 1109, pp. 313–328. Springer, Heidelberg (Aug 1996)
66. Simon, D.R.: On the power of quantum computation. In: 35th FOCS. pp. 116–123. IEEE Computer Society Press (Nov 1994)
67. Simon, D.R.: On the power of quantum computation. SIAM journal on computing 26(5), 1474–1483 (1997)
68. Zhandry, M.: How to construct quantum random functions. In: 53rd FOCS. pp. 679–687. IEEE Computer Society Press (Oct 2012)