How to Build Pseudorandom Functions From Public Random Permutations

Yu Long Chen[1], Eran Lambooij[2], and Bart Mennink[3]

[1] imec-COSIC, KU Leuven, Belgium
yulong.chen@kuleuven.be
[2] University of Haifa, Israel
eranlambooij@gmail.com
[3] Digital Security Group, Radboud University, Nijmegen, The Netherlands
b.mennink@cs.ru.nl

Abstract. Pseudorandom functions are traditionally built upon block ciphers, but with the trend of permutation based cryptography, it is a natural question to investigate the design of pseudorandom functions from random permutations. We present a generic study of how to build beyond birthday bound secure pseudorandom functions from public random permutations. We first show that a pseudorandom function based on a single permutation call cannot be secure beyond the $2^{n/2}$ birthday bound, where n is the state size of the function. We next consider the Sum of Even-Mansour (SoEM) construction, that instantiates the sum of permutations with the Even-Mansour construction. We prove that SoEM achieves tight $2n/3$-bit security if it is constructed from two independent permutations and two randomly drawn keys. We also demonstrate a birthday bound attack if either the permutations or the keys are identical. Finally, we present the Sum of Key Alternating Ciphers (SoKAC) construction, a translation of Encrypted Davies-Meyer Dual to a public permutation based setting, and show that SoKAC achieves tight $2n/3$-bit security even when a single key is used.

Keywords: RP-to-PRF, SoEM, SoKAC, beyond the birthday bound

1 Introduction

In the seminal work of Luby and Rackoff [44], a paradigm of constructing a pseudorandom permutation (PRP) from a pseudorandom function (PRF) was introduced. Their work, motivated by the DES block cipher, consists of an r-round Feistel construction involving independent invocations of a PRF. Soon people realized that they actually needed the opposite construction, i.e., constructing a PRF from a PRP. The reason for this is two-fold: (i) PRPs are easier to design than PRFs and (ii) many cryptographic schemes, such as counter mode, are better off if instantiated with a PRF.

The classical PRP-PRF switch [6, 8, 19, 37, 39], which consists of taking an n-bit block cipher E_K as a PRF, is only secure up to the birthday bound: an

attacker that can learn around $2^{n/2}$ evaluations of E_K can distinguish it from random. Although this bound is acceptable for large enough n, in light of the rise of lightweight block ciphers [3, 4, 16, 18, 30, 35, 38, 43, 59, 63] this bound is on the edge for certain applications. For example, for a 64-bit block cipher, breaking security requires approximately $2^{32} \cdot 64$ bits of data, which is approximately 35GB. Of a similar kind, Bhargavan and Leurent [13] performed practical attacks on TLS and OpenVPN when a 64-bit block cipher is used.

Various approaches of turning a PRP into a PRF with beyond birthday bound security have been introduced. Hall et al. [37] suggested truncation: $\mathrm{trunc}_m(E_K(M))$, an approach that was later proven to be secure up to around $2^{n-m/2}$ queries [5, 34]. Bellare et al. [7] proposed the sum of permutations (SoP),

$$E_{K_1}(M) \oplus E_{K_2}(M)\,, \tag{1}$$

a construction that is known to achieve $q/2^n$ security [5, 28, 45, 54]. Cogliati and Seurin [24] introduced the Encrypted Davies-Meyer (EDM) construction, $E_{K_2}(E_{K_1}(M) \oplus M)$, and proved that it is $2^{2n/3}$ secure. Mennink and Neves [47] improved the security to be 2^n using Patarin's mirror theory [50, 52, 54, 55]. They also introduced the dual: $E_{K_2}(E_{K_1}(M)) \oplus E_{K_1}(M)$, called Encrypted Davies-Mayer Dual (EDMD), and showed that its security is implied by that of the sum of permutations.

All constructions, however, are yet based on block ciphers. Even stronger, they only evaluate E_K in the forward direction. As block ciphers are designed to be efficient in both the forward and inverse direction, these are thus over-engineered primitives for this purpose. This is in contrast with the modern trend in cryptography, namely that of permutation based cryptography, where the underlying permutations are particularly developed to be fast in the forward direction, but not necessarily in the inverse direction. Examples of cryptographic permutations include Keccak [12], Gimli [9], and SPONGENT [15].

So what we really need is a PRF designed from public permutations, but the state of the art in this direction is scarce. To our knowledge, the only notable approach in this direction are the keyed sponge [1, 11, 49] and Farfalle [10], however these constructions have been developed with different incentives in mind. Most importantly, they are variable-length, and for small fixed length messages better solutions may be possible.

Acknowledgedly, the state size of a permutation is typically larger than the block size n of a message: whereas AES has a block size of 128 bits, making the naive birthday bound PRP-PRF switch on the edge, the SHA-3 permutation is of size 1600 bits, and a simple Even-Mansour [32] construction on top of it would give a PRP that behaves like a PRF up to an attack complexity of 2^{800}. However, this example permutation is on the extreme end: lightweight permutations such as SPONGENT [15] and PHOTON [36] go as low as 88 and 100 bits, respectively. For these types of permutations, birthday bound solutions are inadequate.

1.1 Towards Birthday Bound Security

Suppose we take the sum of permutations (1), and want to turn it into a PRF conversion function for a public random permutation. Recall that the sum of permutations is secure up to complexity 2^n as long as the underlying block ciphers are secure. A naive way of proceeding is to plug the Even-Mansour block cipher construction

$$EM_K(M) = \pi(M \oplus K) \oplus K\,,$$

where π is an n-bit permutation, into the sum of permutations. However, the Even-Mansour construction is known to be tightly $2^{n/2}$ birthday bound secure. A simple modular reasoning, in turn, leaves us with an unsatisfiable birthday bound security level.

One way to resolve this is by eschewing the Even-Mansour construction in favor of multiple-round Even-Mansour. For example, 2-round Even-Mansour is secure up to complexity around $2^{2n/3}$, and the generic composition of the sum of permutation with this construction guarantees security up to the same level as well. On the other hand, the scheme has become twice as expensive in the number of primitive evaluations: it is based on four permutation calls. Fortunately, the poor bound of the composition of the sum of permutations with Even-Mansour is not inherent to the scheme, but rather, it is due to a lossy composition. A dedicated analysis can render an improved bound.

1.2 Our Contribution

We tackle the problem of designing a PRF from a public random permutation from a generalized perspective. First, we consider the general design of a PRF based on one and only one public permutation that is preceded and followed by linear mappings, and demonstrate that such construction cannot be secure beyond the birthday bound. The proof consists of considering different types of linear mappings, and deriving attacks in the birthday bound (or faster) for all variants. The result is given in Section 3.

Our second and main contribution centers around the sum of permutations instantiated with Even-Mansour, a construction which we dub SoEM: (Sum of Even Mansour). It is based on two permutations π_1, π_2, and it either takes two keys K_1, K_2 (one before and after each permutation) or it takes a single key K (added before each permutation, and to the final sum). We derive the following results in Section 4:

(i) If $\pi_1 = \pi_2$, so if both Even-Mansour constructions are instantiated using the same permutation, SoEM can be broken in complexity around $2^{n/2}$;
(ii) If π_1 and π_2 are independent, and the construction takes a single key K, SoEM can again be broken in complexity around $2^{n/2}$;
(iii) If π_1 and π_2 are independent, and so are K_1 and K_2, the resulting construction is tightly secure up to complexity $2^{2n/3}$.

The proof of (iii) is performed in the ideal permutation model, using Patarin's H-coefficient technique [21, 51, 53]. It resembles ideas of the first iteration in Patarin's mirror theory [54], but difficulties appear in the fact that the permutations π_1, π_2 can be queried by the distinguisher.

The result sparks curiosity on whether $2n/3$-security is also achievable by a construction based on a single key. We answer this question positively by introducing SoKAC (Sum of Key Alternating Ciphers) in Section 5. SoKAC reminds of EDMD instantiated with Even-Mansour, barring subtle differences, but it can likewise be seen as adding a 1-round Key Alternating Cipher (KAC) [17] to a 2-round one. By putting the first permutation equal in both KACs, the construction makes in total two permutation calls per evaluation. Whereas the scheme is only birthday bound secure if the permutations are identical, i.e. if $\pi_1 = \pi_2$, for the case of independent permutations the construction achieves $2n/3$-security even though it only relies on a single n-bit key. The proof is based on the sum-capture lemma [2, 20, 25, 48, 60].

1.3 Our Contribution in Bigger Perspective

Conversion from public or secret permutations to public or secret functions and vice versa is a fundamental problem in symmetric key cryptography, and our work fills the last remaining notable gap in the picture.

We already discussed the issue of PRF-to-PRP conversion: Luby and Rackoff [44] described the Feistel network, a method still used to design block ciphers. Reversely, PRP-to-PRF conversion was covered by SoP [7], EDM [24], and EDMD [47].

One can consider similar techniques for conversion between public random permutations (RPs) and public random functions (RFs). In this setting, the functions are keyless, and one assumes ideality of the underlying primitives in order to prove security in the indifferentiability framework [46]. The Feistel construction has seen notable indifferentiability analysis [26, 27, 29], and so has the sum of permutation construction [14, 23, 48].

Note that there is little incentive to investigate conversion from PRP/PRF to RP/RF. The Even-Mansour construction [32] transforms an RP to a PRP; it has been generalized in [17, 21, 31, 41, 61]. Gentry and Ramzan [33] proposed the idea of combining the Feistel construction and the Even-Mansour cipher, which was later named the Key alternating Feistel cipher by Lampe and Seurin [42]. Given that RPs are easier to design than RFs, the conversion between RF-to-PRF is not so meaningful.

This leaves the problem of RP-to-PRF conversion, i.e. the problem considered in this work. The full picture of example conversion techniques is given in Figure 1.

2 Preliminaries

For $n \in \mathbb{N}$, we denote by $\{0,1\}^n$ the set of bit strings of length n. For two bit strings $X, Y \in \{0,1\}^n$, we denote their bitwise addition as $X \oplus Y$. For a

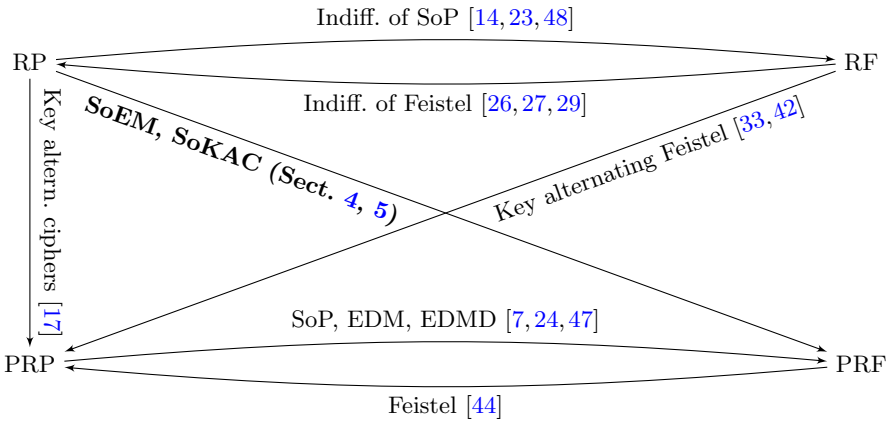

Fig. 1: Conversion among PRP, PRF, RP, and RF. The given example constructions are not exhaustive.

value Z, we denote by $A \leftarrow Z$ the assignment of Z to the variable A. For a finite set $\mathcal{S}$, we denote by $S \xleftarrow{\$} \mathcal{S}$ the uniformly random selection of S from $\mathcal{S}$. We denote by $\mathrm{Func}(n)$ the set of all functions on $\{0,1\}^n$ and by $\mathrm{Perm}(n)$ the set of all permutations on $\{0,1\}^n$. We denote by $\langle t \rangle_n$ the encoding of a value $t \in \{0, \ldots, 2^n - 1\}$ as an n-bit string.

For $k, n, r \in \mathbb{N}$, let $F\colon \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ be a function that is based on r n-bit permutations $\pi_1, \ldots, \pi_r$. We will consider pseudorandom function security of F, where we assume that $\pi_1, \ldots, \pi_r \xleftarrow{\$} \mathrm{Perm}(n)$, and where the distinguisher $\mathcal{D}$ is given access to either $(F_K^{\pi_1,\ldots,\pi_r}, \pi_1^{\pm}, \ldots, \pi_r^{\pm})$ for secret key $K \xleftarrow{\$} \{0,1\}^k$ or $(\varphi, \pi_1^{\pm}, \ldots, \pi_r^{\pm})$ for $\varphi \xleftarrow{\$} \mathrm{Func}(n)$, where the superscript $\pm$ for the π_i's indicates that the distinguisher has bi-directional access. Its goal is to determine which oracle it is given access to:

$$\mathbf{Adv}_F^{\mathrm{prf}}(\mathcal{D}) = \left| \Pr\left[\mathcal{D}^{F_K^{\pi_1,\ldots,\pi_r},\pi_1^{\pm},\ldots,\pi_r^{\pm}} = 1\right] - \Pr\left[\mathcal{D}^{\varphi,\pi_1^{\pm},\ldots,\pi_r^{\pm}} = 1\right] \right|, \qquad (2)$$

for $K \xleftarrow{\$} \{0,1\}^k$, $\pi_1, \ldots, \pi_r \xleftarrow{\$} \mathrm{Perm}(n)$, and $\varphi \xleftarrow{\$} \mathrm{Func}(n)$.

In the remainder of this work, we will focus on keys of size n or $2n$ bits.

3 Pseudorandom Functions With One Permutation Call

We will show that any pseudorandom function F that makes only one permutation call and has linear pre- and post-processing functions cannot achieve security beyond the birthday bound. Let $n \in \mathbb{N}$, and let $\pi \in \mathrm{Perm}(n)$. Let $L_1\colon \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ and $L_2\colon \{0,1\}^n \times \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ be any two linear mappings (that only consist of modular addition and scalar multiplication). Let $F1\colon \{0,1\}^{2n} \times \{0,1\}^n \to \{0,1\}^n$ be the function of Figure 2.

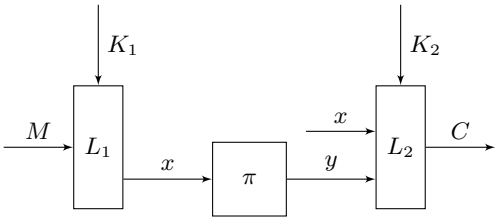

Fig. 2: Function $F1$ based on two keys K_1 and K_2, and making one public random permutations evaluation.

We will show that for independent K_1, K_2, there exists a distinguisher that can distinguish any such function from random using at most $3 \cdot 2^{n/2}$ construction queries and at most $3 \cdot 2^{n/2}$ primitive queries. Note that modular addition of the input M to the output C does not influence the security of $F1$, as the distinguisher knows the exact value of M.

Proposition 1. *Let $n \in \mathbb{N}$, and consider the function $F1\colon \{0,1\}^{2n} \times \{0,1\}^n \to \{0,1\}^n$ of Figure 2 based on permutation $\pi \xleftarrow{\$} \mathrm{Perm}(n)$ and two keys $K_1, K_2 \xleftarrow{\$} \{0,1\}^n$, for any linear L_1, L_2. There exists a distinguisher $\mathcal{D}$ making at most $3 \cdot 2^{n/2}$ construction queries and at most $3 \cdot 2^{n/2}$ primitive queries such that*

$$\mathbf{Adv}^{\mathrm{prf}}_{F1}(\mathcal{D}) \geq 1 - \frac{1}{e}\,. \tag{3}$$

Proof. As the mixing functions L_1, L_2 are linear, we can represent these as

$$\begin{aligned} L_1 &= \begin{pmatrix} l_{11} & l_{12} \end{pmatrix} \\ L_2 &= \begin{pmatrix} l_{21} & l_{22} & l_{23} \end{pmatrix}, \end{aligned}$$

where L_1, L_2 are evaluated on (K_1, M) and (K_2, x, y), respectively.

The distinguisher's advantage satisfies

$$\mathbf{Adv}^{\mathrm{prf}}_{F1}(\mathcal{D}) = \left| \Pr\left[\mathcal{D}^{F1^{\pi},\pi^{\pm}} = 1\right] - \Pr\left[\mathcal{D}^{\varphi,\pi^{\pm}} = 1\right] \right|.$$

Subcase $l_{12} = 0 \vee l_{23} = 0$. In this case, the input to or the output of the permutation π is not related to M or C. When $l_{12} = 0$, the distinguisher selects arbitrary M, M' to obtain C, C'. If the event $C = C'$ happens, then output 1; otherwise, output 0. This gives a distinguisher in two construction queries with a success probability of $1 - 1/2^n$. Similar for $l_{23} = 0$.

Subcase $l_{11} = 0 \vee l_{21} = 0$. In this case, the input to or the output of the permutation π is independent of the keys. When $l_{11} = 0$, the distinguisher selects

arbitrary x, x' to obtain y, y'. Then, it puts $M = l_{12}^{-1}x$ and $M' = l_{12}^{-1}x'$ to obtain C and C'. If the event A happens, then output 1; otherwise, output 0:

$$A = \begin{cases} C \oplus C' = l_{23}y \oplus l_{23}y' & \text{if } l_{22} = 0\,, \\ C \oplus C' = l_{23}y \oplus l_{23}y' \oplus l_{22}x \oplus l_{22}x' & \text{if } l_{22} \neq 0\,. \end{cases}$$

This gives a distinguisher in two construction and two primitive queries with a success probability of $1 - 1/2^n$. Similar for $l_{21} = 0$.

Subcase $l_{22} = 0$. In this case, the construction is a generalization of the Even-Mansour cipher. We will construct a distinguisher $\mathcal{D}$ distinguishing the real world oracle $(F1^\pi, \pi)$ from the ideal world oracle (φ, π) with significant probability. $\mathcal{D}$ makes $2^{n/2}$ construction queries and no primitive queries and operates as follows. For $j = 1, \ldots, 2^{n/2}$, the distinguisher selects arbitrary $M^{(j)}$'s to obtain $C^{(j)}$. If we have $C^{(\bar{j})} \neq C^{(\bar{j}')}$ for all query indices $\bar{j} \neq \bar{j}'$, then output 1; otherwise, output 0.

In the real world, $F1$ behaves as a PRP, and thus $\Pr\left[\mathcal{D}^{F1^\pi, \pi^\pm} = 1\right] = 1$. For the ideal world, we have

$$\Pr\left[\mathcal{D}^{\varphi, \pi^\pm} = 1\right] = \Pr\left[\cap_{j,j'}\, C^{(j)} \neq C^{(j')}\right] \leq 1 - \left(1 - e^{-\binom{q}{2}\frac{1}{2^n}}\right) = e^{-\binom{q}{2}\frac{1}{2^n}}\,,$$

where $q = 2^{n/2}$.

Subcase $l_{11}, l_{12}, l_{21}, l_{22}, l_{23} \neq 0$. This is the most general subcase. We will construct a distinguisher $\mathcal{D}$ distinguishing the real world oracle $(F1^\pi, \pi)$ from the ideal world oracle (φ, π) with significant probability. The distinguisher $\mathcal{D}$ returns 1 if it guesses that it is interacting with the real world oracle and returns 0 otherwise. $\mathcal{D}$ makes $3 \cdot 2^{n/2}$ construction queries, and $3 \cdot 2^{n/2}$ primitive queries to π in total and operates as follows.

(i) For $j = 1, \ldots, 2^{n/2}$, query $M^{(j)} = l_{12}^{-1}(\langle j \rangle_{n/2} \parallel 0^{n/2})$ to obtain $C^{(j)}$, query $M^{*(j)} = l_{12}^{-1}(\langle j \rangle_{n/2} \parallel 0^{n/2-1}1)$ to obtain $C^{*(j)}$, and $M^{**(j)} = l_{12}^{-1}(\langle j \rangle_{n/2} \parallel 0^{n/2-2}10)$ to obtain $C^{**(j)}$;

(ii) For $i = 1, \ldots, 2^{n/2}$, query $x^{(i)} = 0^{n/2} \parallel \langle i \rangle_{n/2}$ to obtain $y^{(i)}$. Define $(x^{*(i)}, y^{*(i)})$ and $(x^{**(i)}, y^{**(i)})$ as the tuples that satisfy $x^{*(i)} = x^{(i)} \oplus 0^{n-1}1$ and $x^{**(i)} = x^{(i)} \oplus 0^{n-2}10$, respectively;

(iii) If there are two query indices $\bar{j}, \bar{i}$ such that $C^{(\bar{j})} \oplus C^{*(\bar{j})} = l_{22}(x^{(\bar{i})} \oplus x^{*(\bar{i})}) \oplus l_{23}(y^{(\bar{i})} \oplus y^{*(\bar{i})})$ and $C^{(\bar{j})} \oplus C^{**(\bar{j})} = l_{22}(x^{(\bar{i})} \oplus x^{**(\bar{i})}) \oplus l_{23}(y^{(\bar{i})} \oplus y^{**(\bar{i})})$, then output 1; otherwise, output 0.

In the real world, there is exactly one $(\bar{j}, \bar{i})$ such that $l_{11}^{-1}(l_{12}M^{(\bar{j})} \oplus x^{(\bar{i})}) = K_1$, leading to

$$C^{(\bar{j})} = l_{22}x^{(\bar{i})} \oplus l_{23}y^{(\bar{i})} \oplus l_{21}K_2\,.$$

In addition, also $l_{11}^{-1}(l_{12}M^{*(\bar{j})} \oplus x^{*(\bar{i})}) = K_1$ and $l_{11}^{-1}(l_{12}M^{**(\bar{j})} \oplus x^{**(\bar{i})}) = K_1$, leading to

$$C^{*(\bar{j})} = l_{22}x^{*(\bar{i})} \oplus l_{23}y^{*(\bar{i})} \oplus l_{21}K_2\,,$$
$$C^{**(\bar{j})} = l_{22}x^{**(\bar{i})} \oplus l_{23}y^{**(\bar{i})} \oplus l_{21}K_2\,.$$

The equations imply that

$$A_{\bar{j},\bar{i}}\colon C^{(\bar{j})} \oplus C^{*(\bar{j})} = l_{22}(x^{(\bar{i})} \oplus x^{*(\bar{i})}) \oplus l_{23}(y^{(\bar{i})} \oplus y^{*(\bar{i})})\,,$$
$$B_{\bar{j},\bar{i}}\colon C^{(\bar{j})} \oplus C^{**(\bar{j})} = l_{22}(x^{(\bar{i})} \oplus x^{**(\bar{i})}) \oplus l_{23}(y^{(\bar{i})} \oplus y^{**(\bar{i})})\,,$$

and thus that $\Pr\left[\mathcal{D}^{F1^{\pi},\pi^{\pm}} = 1\right] = 1$.

For the ideal world, we have

$$\Pr\left[\mathcal{D}^{\varphi,\pi^{\pm}} = 1\right] = \Pr\left[\cup_{j,i}\, A_{j,i} \wedge B_{j,i}\right] \leq \frac{qp}{2^{2n}}\,,$$

where $q = p = 2^{n/2}$. □

4 Sum of Even-Mansour

We consider the *Sum of Even-Mansour* construction, called SoEM, that combines the sum of permutations of Bellare et al. [7] with the Even-Mansour cipher [32]. Let $n \in \mathbb{N}$, and let $\pi_1, \pi_2 \in \mathrm{Perm}(n)$. One can consider a generic construction SoEM$\colon \{0,1\}^{2n} \times \{0,1\}^n \to \{0,1\}^n$ as

$$\mathrm{SoEM}(K_1, K_2, M) = \pi_1(M \oplus K_1) \oplus K_1 \oplus \pi_2(M \oplus K_2) \oplus K_2\,. \tag{4}$$

See also Figure 3. We will consider the construction for three variants: SoEM1 for the case where π_1 and π_2 are identical in Section 4.1, SoEM21 for the case where π_1, π_2 are independent but K_1 and K_2 are identical (so the key space is n bits) in Section 4.2, and SoEM22 for the case where π_1, π_2 are independent and K_1, K_2 are independent in Section 4.3. Note that for SoEM21, we will have to make a slight adjustment, because by simply putting $K_1 = K_2$ in above equation, the addition of the keys at the end of the permutation calls will cancel out. We will detail this in Section 4.2.

4.1 One Permutation

We show that SoEM1, where $\pi_1 = \pi_2$ (but no a priori restriction on K_1, K_2 is imposed) cannot achieve security beyond the birthday bound.

Proposition 2. *Let $n \in \mathbb{N}$, and consider* SoEM1$\colon \{0,1\}^{2n} \times \{0,1\}^n \to \{0,1\}^n$ *based on permutation $\pi \xleftarrow{\$} \mathrm{Perm}(n)$ and two keys $K_1, K_2 \xleftarrow{\$} \{0,1\}^n$. There exists a distinguisher $\mathcal{D}$ making $4 \cdot 2^{n/2}$ construction queries such that*

$$\mathbf{Adv}^{\mathrm{prf}}_{\mathrm{SoEM1}}(\mathcal{D}) \geq 1 - \frac{1}{2^n}\,. \tag{5}$$

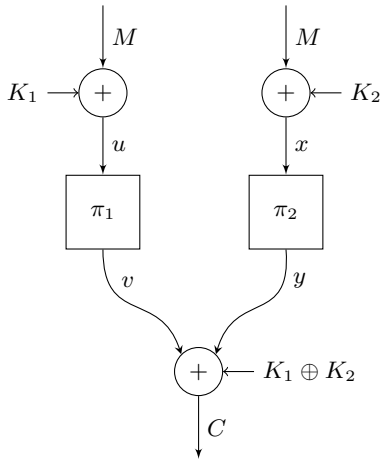

Fig. 3: Encryption of SoEM based on two keys K_1 and K_2, and with π_1 and π_2 two public random permutations.

Proof. We will construct a distinguisher $\mathcal{D}$ distinguishing the real world oracle $(\text{SoEM1}^{\pi}, \pi^{\pm})$ from the ideal world oracle $(\varphi, \pi^{\pm})$ with significant probability. The distinguisher $\mathcal{D}$ returns 1 if it guesses that it is interacting with the real world oracle and returns 0 otherwise. $\mathcal{D}$ makes $4 \cdot 2^{n/2}$ construction queries and no primitive queries and operates as follows.

(i) For $j = 1, \ldots, 2^{n/2}$, query $M^{(j)} = \langle j \rangle_{n/2} \parallel 0^{n/2}$ to obtain $C^{(j)}$, and query $M^{*(j)} = M^{(j)} \oplus 0^{n-1}1$ to obtain $C^{*(j)}$;
(ii) For $j' = 1, \ldots, 2^{n/2}$, query $M^{(j')} = 0^{n/2} \parallel \langle j' \rangle_{n/2}$ to obtain $C^{(j')}$. Define $(M^{*(j')}, C^{*(j')})$ as the tuple that satisfies $M^{*(j')} = M^{(j')} \oplus 0^{n-1}1$;
(iii) If there are two query indices $\bar{j}, \bar{j}'$ such that $C^{(\bar{j})} = C^{(\bar{j}')}$ and $C^{*(\bar{j})} = C^{*(\bar{j}')}$, then output 1; otherwise, output 0.

The distinguisher's advantage satisfies

$$\mathbf{Adv}^{\text{prf}}_{\text{SoEM1}}(\mathcal{D}) = \left| \Pr\left[\mathcal{D}^{\text{SoEM1}^{\pi}_{K_1,K_2},\pi^{\pm}} = 1\right] - \Pr\left[\mathcal{D}^{\varphi,\pi^{\pm}} = 1\right] \right| .$$

In the real world, there is exactly one $(\bar{j}, \bar{j}')$ such that $M^{(\bar{j})} \oplus M^{(\bar{j}')} = K_1 \oplus K_2$, leading to $C^{(\bar{j})} = C^{(\bar{j}')}$ in the real world. In addition, also $M^{*(\bar{j})} \oplus M^{*(\bar{j}')} = K_1 \oplus K_2$, and $C^{*(\bar{j})} = C^{*(\bar{j}')}$ as well. Thus, $\Pr\left[\mathcal{D}^{\text{SoEM1}^{\pi}_{K_1,K_2},\pi^{\pm}} = 1\right] = 1$.

For the ideal world, we have

$$\Pr\left[\mathcal{D}^{\varphi,\pi^{\pm}} = 1\right] = \Pr\left[\cup_{j,j'} C^{(j)} = C^{(j')} \wedge C^{*(j)} = C^{*(j')}\right] \leq \frac{q^2}{2^{2n}} ,$$

where $q = 2^{n/2}$. □

Note that the cost of step (i) in the attack can be reduced by only querying $M^{*(j)}$ for $j = \bar{j}$, but this would complicate the simple description of the distinguisher.

4.2 Two Permutations, One Key

Let $n \in \mathbb{N}$. Let $\pi_1, \pi_2 : \{0,1\}^n \to \{0,1\}^n$ be two independent random permutations. We define SoEM construction based on π_1, π_2 and using a single key K as follows:

$$\text{SoEM21}^{\pi_1,\pi_2}(K, M) = \pi_1(M \oplus K) \oplus \pi_2(M \oplus K) \oplus K\,, \tag{6}$$

and we show that SoEM21 cannot achieve beyond the birthday bound security.

Proposition 3. *Let $n \in \mathbb{N}$, and consider* SoEM21$\colon \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ *based on two permutations $\pi_1, \pi_2 \xleftarrow{\$} \text{Perm}(n)$ and one key $K \xleftarrow{\$} \{0,1\}^n$. There exists a distinguisher $\mathcal{D}$ making $3 \cdot 2^{n/2}$ construction queries, $3 \cdot 2^{n/2}$ primitive queries to π_1, and $3 \cdot 2^{n/2}$ primitive queries to π_2 such that*

$$\mathbf{Adv}^{\text{prf}}_{\text{SoEM21}}(\mathcal{D}) \geq 1 - \frac{1}{2^n}\,. \tag{7}$$

Proof. We will construct a distinguisher $\mathcal{D}$ distinguishing the real world oracle $(\text{SoEM21}_K^{\pi_1,\pi_2}, \pi_1^{\pm}, \pi_2^{\pm})$ from the ideal world oracle $(\varphi, \pi_1^{\pm}, \pi_2^{\pm})$ with significant probability. The distinguisher $\mathcal{D}$ returns 1 if it guesses that it is interacting with the real world oracle and returns 0 otherwise. $\mathcal{D}$ makes $3 \cdot 2^{n/2}$ construction queries, $3 \cdot 2^{n/2}$ primitive queries to π_1, and $3 \cdot 2^{n/2}$ primitive query to π_2 in total and operates as follows.

(i) For $j = 1, \ldots, 2^{n/2}$, query $M^{(j)} = \langle j \rangle_{n/2} \parallel 0^{n/2}$ to obtain $C^{(j)}$, query $M^{*(j)} = \langle j \rangle_{n/2} \parallel 0^{n/2-1}1$ to obtain $C^{*(j)}$, and query $M^{**(j)} = \langle j \rangle_{n/2} \parallel 0^{n/2-2}10$ to obtain $C^{**(j)}$;

(ii) For $i = 1, \ldots, 2^{n/2}$, query $x^{(i)} = 0^{n/2} \parallel \langle i \rangle_{n/2}$ to π_1 and π_2 to obtain $y_1^{(i)}$ and $y_2^{(i)}$. Define $(x^{*(i)}, y_1^{*(i)})$ and $(x^{**(i)}, y_1^{**(i)})$ as the tuples that satisfy $x^{*(i)} = x^{(i)} \oplus 0^{n-1}1$ and $x^{**(i)} = x^{(i)} \oplus 0^{n-2}10$, respectively, and similarly for the queries to π_2;

(iii) If there are two query indices $\bar{j}, \bar{i}$ such that $C^{(\bar{j})} \oplus C^{*(\bar{j})} = y_1^{(\bar{i})} \oplus y_1^{*(\bar{i})} \oplus y_2^{(\bar{i})} \oplus y_2^{*(\bar{i})}$ and $C^{(\bar{j})} \oplus C^{**(\bar{j})} = y_1^{(\bar{i})} \oplus y_1^{**(\bar{i})} \oplus y_2^{(\bar{i})} \oplus y_2^{**(\bar{i})}$, then output 1; otherwise, output 0.

The distinguisher's advantage satisfies

$$\mathbf{Adv}^{\text{prf}}_{\text{SoEM21}}(\mathcal{D}) = \left| \Pr\left[\mathcal{D}^{\text{SoEM21}^{\pi_1,\pi_2},\pi_1^{\pm},\pi_2^{\pm}} = 1\right] - \Pr\left[\mathcal{D}^{\varphi,\pi_1^{\pm},\pi_2^{\pm}} = 1\right] \right|.$$

In the real world, there is exactly one $(\bar{j}, \bar{i})$ such that $M^{(\bar{j})} \oplus x^{(\bar{i})} = K$, leading to

$$C^{(\bar{j})} = y_1^{(\bar{i})} \oplus y_2^{(\bar{i})} \oplus K\,.$$

In addition, also $M^{*(\bar{j})} \oplus x^{*(\bar{i})} = K$ and $M^{**(\bar{j})} \oplus x^{**(\bar{i})} = K$, leading to

$$C^{*(\bar{j})} = y_1^{*(\bar{i})} \oplus y_2^{*(\bar{i})} \oplus K\,,$$
$$C^{**(\bar{j})} = y_1^{**(\bar{i})} \oplus y_2^{**(\bar{i})} \oplus K\,.$$

The equations imply that

$$A_{\bar{j},\bar{i}}\colon C^{(\bar{j})} \oplus C^{*(\bar{j})} = y_1^{(\bar{i})} \oplus y_1^{*(\bar{i})} \oplus y_2^{(\bar{i})} \oplus y_2^{*(\bar{i})}\,,$$
$$B_{\bar{j},\bar{i}}\colon C^{(\bar{j})} \oplus C^{**(\bar{j})} = y_1^{(\bar{i})} \oplus y_1^{**(\bar{i})} \oplus y_2^{(\bar{i})} \oplus y_2^{**(\bar{i})}\,,$$

and thus that $\Pr\left[\mathcal{D}^{\mathrm{SoEM21}^{\pi_1,\pi_2},\pi_1^{\pm},\pi_2^{\pm}} = 1\right] = 1$.

For the ideal world, we have

$$\Pr\left[\mathcal{D}^{\varphi,\pi_1^{\pm},\pi_2^{\pm}} = 1\right] = \Pr\left[\cup_{j,i}\, A_{j,i} \wedge B_{j,i}\right] \le \frac{qp}{2^{2n}}\,,$$

where $q = p = 2^{n/2}$. □

4.3 Two Permutations, Two Keys

We prove that SoEM22 for independent π_1, π_2 and independent K_1, K_2 is secure up to attack complexity $2^{2n/3}$. We also demonstrate an attack matching this bound.

Theorem 1. *Let $n \in \mathbb{N}$, and consider* SoEM22$\colon \{0,1\}^{2n} \times \{0,1\}^n \to \{0,1\}^n$ *based on two permutations $\pi_1, \pi_2 \xleftarrow{\$} \mathrm{Perm}(n)$ and two keys $K_1, K_2 \xleftarrow{\$} \{0,1\}^n$. For any distinguisher $\mathcal{D}$ making at most q construction queries, at most p primitive queries to $\pi_1^{\pm}$ and p primitive queries to $\pi_2^{\pm}$, we have*

$$\mathbf{Adv}^{\mathrm{prf}}_{\mathrm{SoEM22}}(\mathcal{D}) \le \frac{q(p+q)^2}{2^{2n}} + \frac{3qp^2}{2^{2n}}\,. \tag{8}$$

The proof is given in Section 6.3.

Proposition 4. *Let $n \in \mathbb{N}$, and consider* SoEM22$\colon \{0,1\}^{2n} \times \{0,1\}^n \to \{0,1\}^n$ *based on two permutations $\pi_1, \pi_2 \xleftarrow{\$} \mathrm{Perm}(n)$ and two keys $K_1, K_2 \xleftarrow{\$} \{0,1\}^n$. There exists a distinguisher $\mathcal{D}$ making $4 \cdot 2^{2n/3}$ construction queries, and $4 \cdot 2^{2n/3}$ primitive queries to π_1 and $4 \cdot 2^{2n/3}$ primitive queries to π_2 such that*

$$\mathbf{Adv}^{\mathrm{prf}}_{\mathrm{SoEM22}}(\mathcal{D}) \ge 1 - \frac{1}{e} - \frac{1}{2^n}\,. \tag{9}$$

Proof. We will construct a distinguisher $\mathcal{D}$ distinguishing the real world oracle $(\mathrm{SoEM22}^{\pi_1,\pi_2}_{K_1,K_2}, \pi_1^{\pm}, \pi_2^{\pm})$ from the ideal world oracle $(\varphi, \pi_1^{\pm}, \pi_2^{\pm})$ with significant probability. The distinguisher $\mathcal{D}$ returns 1 if it guesses that it is interacting with the real world oracle and returns 0 otherwise. $\mathcal{D}$ makes $4 \cdot 2^{2n/3}$ construction queries, $4 \cdot 2^{2n/3}$ primitive queries to π_1, and $4 \cdot 2^{2n/3}$ primitive query to π_2 in total and operates as follows.

(i) For $j = 1, \ldots, 2^{2n/3}$, query $M^{(j)} = \langle j \rangle_{2n/3} \parallel 0^{n/3}$ to obtain $C^{(j)}$, query $M^{*(j)} = \langle j \rangle_{2n/3} \parallel 0^{n/3-1}1$ to obtain $C^{*(j)}$, query $M^{**(j)} = \langle j \rangle_{2n/3} \parallel 0^{n/3-2}10$ to obtain $C^{**(j)}$, and query $M^{***(j)} = \langle j \rangle_{2n/3} \parallel 0^{n/3-2}11$ to obtain $C^{***(j)}$;

(ii) For $i = 1, \ldots, 2^{2n/3}$, query $u^{(i)} = 0^{n/3} \parallel \langle i \rangle_{2n/3}$ to π_1 to obtain $v^{(i)}$. Define $(u^{*(i)}, v^{*(i)})$, $(u^{**(i)}, v^{**(i)})$, and $(u^{***(i)}, v^{***(i)})$ as the tuples that satisfy $u^{*(i)} = u^{(i)} \oplus 0^{n-1}1$, $u^{**(i)} = u^{(i)} \oplus 0^{n-2}10$, and $u^{***(i)} = u^{(i)} \oplus 0^{n-2}11$, respectively;

(iii) For $i' = 1, \ldots, 2^{2n/3}$, query $x^{(i')}$ at random to obtain $y^{(i')}$, query $x^{*(i')} = x^{(i')} \oplus 0^{n-1}1$ to obtain $y^{*(i')}$, query $x^{**(i')} = x^{(\bar{i}')} \oplus 0^{n-2}10$ to obtain $y^{**(i')}$, and query $x^{***(i')} = x^{(\bar{i}')} \oplus 0^{n-2}11$ to obtain $y^{***(i')}$;

(iv) If there are three query indices $\bar{j}, \bar{i}, \bar{i}'$ such that $C^{(\bar{j})} \oplus C^{*(\bar{j})} = v^{(\bar{i})} \oplus v^{*(\bar{i})} \oplus y^{(\bar{i}')} \oplus y^{*(\bar{i}')}$, $C^{(\bar{j})} \oplus C^{**(\bar{j})} = v^{(\bar{i})} \oplus v^{**(\bar{i})} \oplus y^{(\bar{i}')} \oplus y^{**(\bar{i}')}$ and $C^{(\bar{j})} \oplus C^{***(\bar{j})} = v^{(\bar{i})} \oplus v^{***(\bar{i})} \oplus y^{(\bar{i}')} \oplus y^{***(\bar{i}')}$, then output 1; otherwise, output 0.

The distinguisher's advantage satisfies

$$\mathbf{Adv}^{\mathrm{prf}}_{\mathrm{SoEM22}}(\mathcal{D}) = \left| \Pr\left[\mathcal{D}^{\mathrm{SoEM22}^{\pi_1,\pi_2},\pi_1^{\pm},\pi_2^{\pm}} = 1\right] - \Pr\left[\mathcal{D}^{\varphi,\pi_1^{\pm},\pi_2^{\pm}} = 1\right] \right| .$$

Put $q = p = 2^{2n/3}$. First consider the real world. Define $I_{K_1} = \{(j,i) \colon M^{(j)} \oplus u^{(i)} = K_1\}$, and note that $|I_{K_1}| = 2^{n/3}$. We denote by $E_{j,i'}$ the event that $M^{(j)} \oplus x^{(i')} = K_2$, for fixed j, i' where $(j,\cdot) \in I_{K_1}$. For each j, i', we have $\Pr[E_{j,i'}] = 1/2^n$, and we obtain from the union bound:

$$\Pr\left[\cup_{j,i'} E_{j,i'}\right] \leq \frac{2^{n/3}p}{2^n} . \tag{10}$$

For the lower bound, we denote by D_j the event that a fixed j with $(j,\cdot) \in I_{K_1}$ satisfies $M^{(j)} \oplus x^{(i')} \neq K_2$ for all i'. Note that the D_j's are mutually independent for different j, and the probability of any D_j is

$$\Pr[D_j] = \frac{2^n - p}{2^n} = 1 - \frac{p}{2^n} .$$

The probability of $M^{(j)} \oplus x^{(i')} \neq K_2$ for all j, i' can now be computed as

$$1 - \Pr\left[\cup_{j,i'} E_{j,i'}\right] = \prod_{j=1}^{2^{n/3}} \Pr[D_j] = \prod_{j=1}^{2^{n/3}} \left(1 - \frac{p}{2^n}\right) .$$

As $p/2^n \leq 1$, we can use the inequality $1 - x \leq e^{-x}$ for each term of above expression, and find an upper bound

$$\prod_{j=1}^{2^{n/3}} e^{-\frac{p}{2^n}} = e^{-\frac{2^{n/3}p}{2^n}} .$$

Putting all this together we get the lower bound

$$\Pr\left[\cup_{j,i'} E_{j,i'}\right] \geq 1 - e^{-\frac{2^{n/3}p}{2^n}} . \tag{11}$$

Note that if there exist $(\bar{j}, \bar{i}) \in I_{K_1}$ and $\bar{i}'$ such that $M^{(\bar{j})} \oplus x^{(\bar{i}')} = K_2$, we also have that

$$C^{(\bar{j})} \oplus v^{(\bar{i})} \oplus y^{(\bar{i}')} = K_1 \oplus K_2 \,. \tag{12}$$

We in addition have that $(M^{(\bar{j})} \oplus \Delta) \oplus (u^{(\bar{i})} \oplus \Delta) = K_1$ and that $(M^{(\bar{j})} \oplus \Delta) \oplus (x^{(\bar{i}')} \oplus \Delta) = K_2$ for any $\Delta \in \{0,1\}^n$. Due to our definition of $M^{**(\bar{j})}$, $M^{***(\bar{j})}$, $u^{**(\bar{j})}$, $u^{***(\bar{j})}$, $x^{**(\bar{j})}$, and $x^{***(\bar{j})}$,, we thus obtain that also

$$\begin{aligned} C^{*(\bar{j})} \oplus v^{*(\bar{i})} \oplus y^{*(\bar{i}')} &= K_1 \oplus K_2 \,, \\ C^{**(\bar{j})} \oplus v^{**(\bar{i})} \oplus y^{**(\bar{i}')} &= K_1 \oplus K_2 \,, \\ C^{***(\bar{j})} \oplus v^{***(\bar{i})} \oplus y^{***(\bar{i}')} &= K_1 \oplus K_2 \,. \end{aligned}$$

Combining these three equations with (12), we can conclude that under the premise that (12) holds, the following three events

$$\begin{aligned} A_{\bar{j},\bar{i},\bar{i}'} &: C^{(\bar{j})} \oplus C^{*(\bar{j})} = v^{(\bar{i})} \oplus v_1^{*(\bar{i})} \oplus y^{(\bar{i}')} \oplus y^{*(\bar{i}')} \,, \\ B_{\bar{j},\bar{i},\bar{i}'} &: C^{(\bar{j})} \oplus C^{**(\bar{j})} = v^{(\bar{i})} \oplus v^{**(\bar{i})} \oplus y^{(\bar{i}')} \oplus y^{**(\bar{i}')} \,, \\ C_{\bar{j},\bar{i},\bar{i}'} &: C^{(\bar{j})} \oplus C^{***(\bar{j})} = v^{(\bar{i})} \oplus v^{***(\bar{i})} \oplus y^{(\bar{i}')} \oplus y^{***(\bar{i}')} \,, \end{aligned}$$

are satisfied in the real world. Therefore, for the real world, we can conclude the following:

$$\begin{aligned} &\Pr\left[\mathcal{D}^{\mathrm{SoEM22}^{\pi_1,\pi_2},\pi_1^{\pm},\pi_2^{\pm}} = 1\right] \\ &= \Pr\left[\cup_{j,i'} E_{j,i'}\right] + \Pr\left[\cup_{j,i,i'} A_{j,i,i'} \wedge B_{j,i,i'} \wedge C_{j,i,i'} \mid \cap_{j,i'} \neg E_{j,i'}\right] \cdot \Pr\left[\cap_{j,i'} \neg E_{j,i'}\right] \,. \end{aligned}$$

From (10) and (11), we obtain

$$\begin{aligned} \Pr\left[\mathcal{D}^{\mathrm{SoEM22}^{\pi_1,\pi_2},\pi_1^{\pm},\pi_2^{\pm}} = 1\right] &\geq 1 - e^{-\frac{2^{n/3}p}{2^n}} + \frac{qp^2}{2^{3n}}\left(1 - \frac{2^{n/3}p}{2^n}\right) \\ &= 1 - e^{-\frac{2^{n/3}p}{2^n}} \,, \end{aligned}$$

where $p = 2^{2n/3}$.

For the ideal world, we have

$$\Pr\left[\mathcal{D}^{\varphi,\pi_1^{\pm},\pi_2^{\pm}} = 1\right] = \Pr\left[\cup_{j,i,i'} A_{j,i,i'} \wedge B_{j,i,i'} \wedge C_{j,i,i'}\right] \leq \frac{qp^2}{2^{3n}} \,,$$

where $q = p = 2^{2n/3}$. □

5 Sum of Key Alternating Ciphers

Inspired by the result on SoEM22, we consider a sequential evaluation, which we call the *Sum of Key Alternating Ciphers* (SoKAC). It reminds of the EDMD

construction of Mennink and Neves [47] instantiated with Even-Mansour, but it is not quite the same. Let $n \in \mathbb{N}$, and let $\pi_1, \pi_2 \in \mathrm{Perm}(n)$. We define the generic construction SoKAC: $\{0,1\}^{2n} \times \{0,1\}^n \to \{0,1\}^n$ as

$$\mathrm{SoKAC}(K_1, K_2, M) = \pi_2(\pi_1(M \oplus K_1) \oplus K_2) \oplus K_1 \oplus \pi_1(M \oplus K_1) \oplus K_2\,, \quad (13)$$

See also Figure 4. We will consider the construction for two variants: SoKAC1 for the case where $\pi_1 = \pi_2$ are identical in Section 5.1, and SoKAC21 for the case where π_1, π_2 are independent but $K_1 = K_2$ are identical (so the key space is n bits) in Section 5.2. As before, for SoKAC21, we will have to make a slight adjustment, because by simply putting $K_1 = K_2$ in above equation, the addition of the keys at the end of the permutation calls will cancel out. We will detail this in Section 5.2.

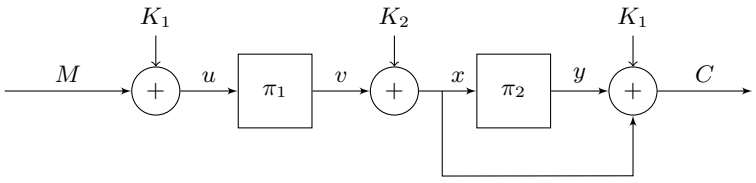

Fig. 4: Encryption of SoKAC based on two keys K_1 and K_2, and with π_1 and π_2 two public random permutations.

5.1 One Permutation

We show that SoKAC1, where $\pi_1 = \pi_2$ (but no a priori restriction on K_1, K_2 is imposed), cannot achieve security beyond the birthday bound.

Proposition 5. *Let $n \in \mathbb{N}$, and consider* $\mathrm{SoKAC1} : \{0,1\}^{2n} \times \{0,1\}^n \to \{0,1\}^n$ *based on permutation $\pi \xleftarrow{\$} \mathrm{Perm}(n)$ and two keys $K_1, K_2 \xleftarrow{\$} \{0,1\}^n$. There exists a distinguisher $\mathcal{D}$ making $3 \cdot 2^{n/2}$ construction queries such that*

$$\mathbf{Adv}^{\mathrm{prf}}_{\mathrm{SoKAC1}}(\mathcal{D}) \geq 1 - \frac{1}{2^n}\,. \quad (14)$$

Proof. The attack is identical to that of SoEM1 of Proposition 2, and henceforth omitted. □

5.2 Two Permutations, One Key

Let $n \in \mathbb{N}$. Let $\pi_1, \pi_2 : \{0,1\}^n \to \{0,1\}^n$ be two independent random permutations. We define SoKAC construction based on π_1, π_2 and using a single key K as follows:

$$\mathrm{SoKAC21}^{\pi_1,\pi_2}(K, M) = \pi_2(\pi_1(M \oplus K) \oplus K) \oplus \pi_1(M \oplus K) \oplus K\,, \quad (15)$$

and we show that SoKAC21 is secure up to attack complexity $2^{2n/3}$. We also demonstrate an attack matching this bound.

Theorem 2. *Let $n \in \mathbb{N}$, and consider* SoKAC21$\colon \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ *based on two permutations $\pi_1, \pi_2 \xleftarrow{\$} \mathrm{Perm}(n)$ and one key $K \xleftarrow{\$} \{0,1\}^n$. For any distinguisher $\mathcal{D}$ making at most q construction queries, at most p primitive queries to $\pi_1^{\pm}$ and p primitive queries to $\pi_2^{\pm}$, we have*

$$\mathbf{Adv}^{\mathrm{prf}}_{\mathrm{SoKAC21}}(\mathcal{D}) \leq \frac{q(p+q)^2}{2^{2n}} + \frac{2}{2^n} + \frac{qp^2}{2^{2n}} + \frac{2p^2\sqrt{qp}}{2^{2n}} + \frac{3\sqrt{nqp^2}}{2^n} + \frac{4\sqrt{qp^2}}{2^n}\,. \tag{16}$$

The proof is given in Section 6.4.

Proposition 6. *Let $n \in \mathbb{N}$, and consider* SoKAC21$\colon \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ *based on two permutations $\pi_1, \pi_2 \xleftarrow{\$} \mathrm{Perm}(n)$ and one key $K \xleftarrow{\$} \{0,1\}^n$. There exists a distinguisher $\mathcal{D}$ making $4 \cdot 2^{2n/3}$ construction queries, and $4 \cdot 2^{2n/3}$ primitive queries to π_1 and $4 \cdot 2^{2n/3}$ primitive queries to π_2 such that*

$$\mathbf{Adv}^{\mathrm{prf}}_{\mathrm{SoKAC21}}(\mathcal{D}) \geq 1 - \frac{1}{e} - \frac{1}{2^n}\,. \tag{17}$$

Proof. The attack is identical to that of SoEM22 of Proposition 4, and henceforth omitted. □

6 Security Proofs

The security proofs of SoEM22 and SoKAC21 are given in Sections 6.3 and 6.4. The proofs are performed using Patarin's H-coefficient technique, which we will recap in Section 6.1. The proof of SoKAC21 relies on the sum-capture lemma, which we revisit in Section 6.2. The analysis for good transcripts resembles ideas of the first iteration in Patarin's mirror theory, but difficulties appear in the fact that the distinguisher can make direct queries to the permutations π_1 and π_2.

6.1 Patarin's H-Coefficient Technique

In this work, we use the H-coefficient technique by Patarin [51, 53], but we will follow the modernization of Chen and Steinberger [21].

Let $\pi_1, \pi_2, \ldots, \pi_r \xleftarrow{\$} \mathrm{Perm}(n)$, and $\varphi \xleftarrow{\$} \mathrm{Func}(n)$. Let $K \xleftarrow{\$} \{0,1\}^k$, and $F\colon \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ be a pseudorandom function based on public random permutations $\pi_1, \pi_2, \ldots, \pi_r$. We consider a deterministic distinguisher $\mathcal{D}$ that has query access to either the real world oracle $\mathcal{O} = (F_K^{\pi_1,\ldots,\pi_r}, \pi_1^{\pm}, , \ldots, \pi_r^{\pm})$ or the ideal world oracle $\mathcal{P} = (\varphi, \pi_1^{\pm}, \ldots, \pi_r^{\pm})$. The distinguisher's goal is to distinguish both worlds and we denote by

$$\mathbf{Adv}(\mathcal{D}) = \left|\Pr\left[\mathcal{D}^{\mathcal{O}} = 1\right] - \Pr\left[\mathcal{D}^{\mathcal{P}} = 1\right]\right|$$

its advantage. We summarize all query-response tuples learned by $\mathcal{D}$ during its interaction with its oracle $\mathcal{O}$ or $\mathcal{P}$ in a transcript τ. We denote by $X_{\mathcal{O}}$ (resp. $X_{\mathcal{P}}$) the probability distribution of transcripts when interacting with $\mathcal{O}$ (resp. $\mathcal{P}$). We call a transcript $\tau \in \mathcal{T}$ attainable if $Pr[X_{\mathcal{P}} = \tau] > 0$, or in other words if the transcript τ can be obtained from an interaction with $\mathcal{P}$.

Lemma 1 (H-coefficient Technique). *Consider a deterministic distinguisher $\mathcal{D}$. Define a partition $\mathcal{T} = \mathcal{T}_{\text{good}} \cup \mathcal{T}_{\text{bad}}$, where $\mathcal{T}_{\text{good}}$ is the subset of $\mathcal{T}$ which contains all the "good" transcripts and $\mathcal{T}_{\text{bad}}$ is the subset with all the "bad" transcripts. Let $0 \leq \epsilon \leq 1$ be such that for all $\tau \in \mathcal{T}_{\text{good}}$:*

$$\frac{Pr(X_{\mathcal{O}} = \tau)}{Pr(X_{\mathcal{P}} = \tau)} \geq 1 - \epsilon\,. \tag{18}$$

Then, we have $\mathbf{Adv}(\mathcal{D}) \leq \epsilon + \Pr[X_{\mathcal{P}} \in \mathcal{T}_{\text{bad}}]$.

6.2 Sum-Capture Lemma

We use the sum-capture lemma [20, 25, 48], which is built upon the work of Babai [2] and Steinberger [60]. Such results typically state that for a random subset Z of $\{0,1\}^n$ of size p, the quantity

$$\mu(Z, A, B) = |\{(z, a, b) \in Z \times A \times B \colon z = a \oplus b\}|$$

is at most around $p \cdot |A| \cdot |B| / 2^n$ for any possible choice of A and B, except with negligible probability. In our setting, Z will consist of query-response tuples from a permutation, i.e., Z consists of values $u^{(i)} \oplus v^{(i)}$ where $\{(u^{(1)}, v^{(1)}), \ldots, (u^{(p)}, v^{(p)})\}$ is a permutation transcript. We will appeal to the sum-capture theorem by Chen et al. [20].

Lemma 2 (Sum-Capture Lemma). *Let $n, p \in \mathbb{N}$ such that $9n \leq p \leq 2^{n-1}$. Let $\pi \xleftarrow{\$} \text{Perm}(n)$, let $\{(u^{(1)}, v^{(1)}), \ldots, (u^{(p)}, v^{(p)})\}$ be p tuples of π, and let $Z = \{(u^{(1)} \oplus v^{(1)}), \ldots, (u^{(p)} \oplus v^{(p)})\}$. For any two subsets $A, B \subseteq \{0,1\}^n$, we have*

$$\Pr\left[\mu(Z, A, B) \geq \frac{p\,|A|\,|B|}{2^n} + \frac{2p^2\sqrt{|A|\,|B|}}{2^n} + 3\sqrt{np\,|A|\,|B|}\right] \leq \frac{2}{2^n}\,.$$

6.3 Proof of Theorem 1 on SoEM22

Let $K = (K_1, K_2) \xleftarrow{\$} \{0,1\}^{2n}$, $\pi_1, \pi_2 \xleftarrow{\$} \text{Perm}(n)$, and $\varphi \xleftarrow{\$} \text{Func}(n)$. Consider any distinguisher $\mathcal{D}$ that has access to three oracles: $(\text{SoEM22}_K^{\pi_1,\pi_2}, \pi_1^{\pm}, \pi_2^{\pm})$ in the real world or $(\varphi, \pi_1^{\pm}, \pi_2^{\pm})$ in the ideal world. We assume $\mathcal{D}$ is computational unbounded and deterministic. The distinguisher makes q construction queries to $\mathcal{O}_0 \in \{\text{SoEM22}_K^{\pi_1,\pi_2}, \varphi\}$, and these are summarized in a transcript of the form $\tau_0 = \{(M^{(1)}, C^{(1)}), \ldots, (M^{(q)}, C^{(q)})\}$. It also makes p primitive queries to $\mathcal{O}_1 = \pi_1^{\pm}$ and p primitive queries to $\mathcal{O}_2 = \pi_2^{\pm}$, and like before, these are respectively summarized in transcripts $\tau_1 = \{(u^{(1)}, v^{(1)}), \ldots, (u^{(p)}, v^{(p)})\}$ and

$\tau_2 = \{(x^{(1)}, y^{(1)}), \ldots, (x^{(p)}, y^{(p)})\}$. We assume that τ_0, τ_1, and τ_2 do not contain duplicate elements. After $\mathcal{D}$'s interaction with the oracles, but before it outputs its decision, we disclose the keys K_1, K_2 to the distinguisher. In real world, these are the keys used in the construction. In the ideal world K_1, K_2 are dummy keys that are drawn uniformly at random. The complete view is denoted $\tau = (\tau_0, \tau_1, \tau_2, K_1, K_2)$.

Bad Events. We say that $\tau \in \mathcal{T}_{\text{bad}}$ if and only if there exists a construction query $(M^{(j)}, C^{(j)}) \in \tau_0$ and primitive queries $(u^{(i)}, v^{(i)}) \in \tau_1$ and $(x^{(i')}, y^{(i')}) \in \tau_2$ such that one of the following conditions holds:

$$\text{bad}_1 \colon M^{(j)} \oplus u^{(i)} = K_1 \wedge M^{(j)} \oplus x^{(i')} = K_2 \,, \tag{19}$$

$$\text{bad}_2 \colon M^{(j)} \oplus u^{(i)} = K_1 \wedge C^{(j)} \oplus v^{(i)} \oplus y^{(i')} = K_1 \oplus K_2 \,, \tag{20}$$

$$\text{bad}_3 \colon M^{(j)} \oplus x^{(i')} = K_2 \wedge C^{(j)} \oplus v^{(i)} \oplus y^{(i')} = K_1 \oplus K_2 \,. \tag{21}$$

Note that any attainable transcript τ for which $\tau \notin \mathcal{T}_{\text{bad}}$, implies that τ is a good transcript.

We give an informal explanation of the definition of the bad event. In the real world, every construction query j induces *exactly one* evaluation $(u^{(j)}, v^{(j)})$ of the underlying public permutation π_1, and *exactly one* evaluation $(x^{(j)}, y^{(j)})$ of the underlying public permutation π_2. These two queries naturally satisfy

$$\begin{aligned} M^{(j)} \oplus u^{(j)} &= K_1 \,, \\ M^{(j)} \oplus x^{(j)} &= K_2 \,, \\ C^{(j)} \oplus v^{(j)} \oplus y^{(j)} &= K_1 \oplus K_2 \,. \end{aligned}$$

Clearly, $u^{(j)}$ and $x^{(j)}$ are fixed by $M^{(j)}$, K_1, and K_2, but there is "freedom" in the value $v^{(j)} \oplus y^{(j)}$. If it happens to be that the distinguisher queried $u^{(j)}$, i.e., that $(u^{(j)}, v^{(j)}) \in \tau_1$, it consequently fixes the tuple $(x^{(j)}, y^{(j)})$ for π_2. However, in the ideal world, there is no such dependency. This means that if the adversary had queried $u^{(j)} = M^{(j)} \oplus K_1$ to π_1 and $x^{(j)} = M^{(j)} \oplus K_2$ to π_2, with high probability the third equation would not hold. An identical reasoning applies for the case where the distinguisher happened to have set any other two out of three equations.

$\mathbf{Pr}[X_{\mathcal{P}} \in \mathcal{T}_{\text{bad}}]$. We want to bound the probability that an ideal world transcript τ satisfies either of (19)-(21). Therefore, the probability that $\tau \in \mathcal{T}_{\text{bad}}$ is given by

$$\Pr[\tau \in \mathcal{T}_{\text{bad}}] \leq \Pr[\text{bad}_1] + \Pr[\text{bad}_2] + \Pr[\text{bad}_3] \,.$$

We consider the first bad event bad_1. For any possible construction query $(M^{(j)}, C^{(j)}) \in \tau_0$, any possible π_1 primitive query $(u^{(i)}, v^{(i)})$, and any possible π_2 primitive query $(x^{(i')}, y^{(i')})$, the only randomness in the first equation is K_1 and the only randomness in the second equation is K_2. This means that the probabilities that

each of the equation holds in bad_1 are independent of each other. By the fact that the keys $K = (K_1, K_2) \xleftarrow{\$} \{0,1\}^{2n}$ are dummy keys generated independently of τ_0, τ_1 and τ_2, the probability that bad_1 holds for fixed j, i, i' is $1/2^{2n}$. Summed over all q possible construction queries, p possible π_1 primitive queries, and p possible π_2 primitive queries, we have

$$\Pr[\mathrm{bad}_1] \leq \frac{qp^2}{2^{2n}}\,.$$

For the second bad event bad_2, note that we can replace K_1 in the second equation by $M^{(j)} \oplus u^{(i)}$. Hereby, the only randomness in the first equation is K_1 and the only randomness in the second equation is K_2. The probabilities that each of the equation holds in bad_2 are independent of each other. Again, summing over all the construction and the primitive queries, we have

$$\Pr[\mathrm{bad}_2] \leq \frac{qp^2}{2^{2n}}\,.$$

The same reasoning applies for bad_3. Summing the three probabilities, we get

$$\Pr[\tau \in \mathcal{T}_{\mathrm{bad}}] \leq \frac{3qp^2}{2^{2n}}\,. \tag{22}$$

$\Pr[X_{\mathcal{O}} = \tau] / \Pr[X_{\mathcal{P}} = \tau]$. Consider an attainable transcript $\tau \in \mathcal{T}_{\mathrm{good}}$. To compute $\Pr[X_{\mathcal{O}} = \tau]$ and $\Pr[X_{\mathcal{P}} = \tau]$, it suffices to compute the probability of oracles that could result in view τ. Denote by $all_{\mathcal{O}}$ the set of all oracles in the real world, and by $comp_{\mathcal{O}}(\tau)$ the fraction of them compatible with τ, we see that $\Pr[X_{\mathcal{O}} = \tau] = |comp_{\mathcal{O}}(\tau)| \,/\, |all_{\mathcal{O}}|$. Similarly we have $all_{\mathcal{P}}$ and $comp_{\mathcal{P}}(\tau)$ for the ideal world. We obtain

$$\frac{\Pr[X_{\mathcal{O}} = \tau]}{\Pr[X_{\mathcal{P}} = \tau]} = \frac{|comp_{\mathcal{O}}(\tau)| \cdot |all_{\mathcal{P}}|}{|all_{\mathcal{O}}| \cdot |comp_{\mathcal{P}}(\tau)|}\,. \tag{23}$$

For the real world $\mathcal{O}$, we have $|all_{\mathcal{O}}| = 2^{2n} \cdot (2^n!)^2$, which is equal to the number of possible keys $K = (K_1, K_2)$ times the number of possible public random permutations π_1 and π_2. Similarly, for the ideal world $\mathcal{P}$, we have $|all_{\mathcal{P}}| = 2^{2n} \cdot 2^{n2^n} (2^n!)^2$. The first term corresponds to the number of randomly drawn keys, the second term is the number of possible random functions $\varphi \in \mathrm{Func}(n)$, and the last term the number of possible public random permutations π_1 and π_2. For the computation of the number of oracles compatible with τ in the ideal world, we see that there are $2^{n(2^n - q)}$ random functions $\varphi \in \mathrm{Func}(n)$ compliant with τ_0, $(2^n - p)!$ public random permutations π_1 compliant with τ_1, and $(2^n - p)!$ public random permutations π_2 compliant with τ_2. We find

$$|comp_{\mathcal{P}}(\tau)| = 2^{n(2^n - q)} \cdot (2^n - p)!^2\,.$$

From (23), we have

$$\frac{\Pr[X_{\mathcal{O}} = \tau]}{\Pr[X_{\mathcal{P}} = \tau]} = \frac{|comp_{\mathcal{O}}(\tau)| \cdot 2^{2n} 2^{n2^n} (2^n!)^2}{2^{2n}(2^n!)^2 \cdot (2^{n(2^n - q)})(2^n - p)!^2} = \frac{|comp_{\mathcal{O}}(\tau)| \cdot 2^{nq}}{(2^n - p)!^2}\,. \tag{24}$$

What remains is the computation of the number of oracles compatible with τ in the real world. As defined by the bad events, a transcript τ is bad if we get both the same input or output to π_1, and the same input or output to π_2. This means that for any $\tau \in \mathcal{T}_{\text{good}}$, a construction query collides with at most one query in $\tau_1 \cup \tau_2$. We conclude this fact in the following claim:

Claim. For $\tau \in \mathcal{T}_{\text{good}}$, any construction query $(M^{(j)}, C^{(j)}) \in \tau_0$ collides with at most one primitive query $(u^{(i)}, v^{(i)}) \in \tau_1$ and at most one primitive query $(x^{(i')}, y^{(i')}) \in \tau_2$, but never with both a τ_1 and τ_2 query.

We will use this claim to re-group the transcripts τ_0, τ_1, and τ_2 into three new transcripts τ_0^{new}, τ_1^{new}, and τ_2^{new}. We initially define $\tau_0^{\text{new}} = \tau_0$, $\tau_1^{\text{new}} = \tau_1$ and $\tau_2^{\text{new}} = \tau_2$. The trick will be to consider each individual construction query $(M^{(j)}, C^{(j)})$, and to operate as follows:

- if $M^{(j)} \oplus K_1 = u^{(i)}$ for some i, then remove $(M^{(j)}, C^{(j)})$ from τ_0^{new}, and add $(x, y) = (M^{(j)} \oplus K_2, C^{(j)} \oplus v^{(i)} \oplus K_1 \oplus K_2)$ to τ_2^{new};
- if $M^{(j)} \oplus K_2 = x^{(i')}$ for some i', then remove $(M^{(j)}, C^{(j)})$ from τ_0^{new}, and add $(u, v) = (M^{(j)} \oplus K_1, C^{(j)} \oplus y^{(i')} \oplus K_1 \oplus K_2)$ to τ_1^{new}.

Note that any good transcript will have to meet $\neg\text{bad}_1 \wedge \neg\text{bad}_2 \wedge \neg\text{bad}_3$. We know that if a construction query $(M^{(j)}, C^{(j)})$ collides with $(u^{(i)}, v^{(i)}) \in \tau_1$, then $M^{(j)} \oplus K_2$ cannot be a valid $x^{(i')}$ value because of $\neg\text{bad}_1$, and $C^{(j)} \oplus v^{(i)} \oplus K_1 \oplus K_2$ cannot be a valid $y^{(i')}$ value because of $\neg\text{bad}_2$, for any $(x^{(i')}, y^{(i')}) \in \tau_2$. Similarly for τ_1^{new}. This way, we will end up with soundly defined τ_1^{new} and τ_2^{new} for π_1 and π_2, and a set of construction queries τ_0^{new} that does not collide with any tuple in τ_1^{new} or τ_2^{new}. Let $s_2, s_1 \leq p$ be the number of construction queries that collides with $(u^{(i)}, v^{(i)}) \in \tau_1$ resp. $(x^{(i')}, y^{(i')}) \in \tau_2$. The number of elements in the new transcripts τ_1^{new} and τ_2^{new} are equal to $p + s_2$ resp. $p + s_1$, and the number of construction queries that remains in τ_0^{new} is equal to $q' = q - s_1 - s_2$.

The two sets of transcripts, τ_1^{new} and τ_2^{new}, define *exactly* $p + s_2$ input-output tuples for π_1 and *exactly* $p + s_1$ input-output tuples for π_2. What remains is the counting of the number of permutations π_1, π_2 that satisfy these $p + s_2$ resp. $p + s_1$ tuples, and that could give the remaining transcript τ_0^{new}.

For a given transcript τ_0^{new} of q' elements, our goal is to count the number of n-bit permutations $\pi_1 \colon \mathcal{D}_1 \to \mathcal{R}_1$ with $|\mathcal{D}_1| = |\mathcal{R}_1| = 2^n - p - s_2$, and the number of n-bit permutations $\pi_2 \colon \mathcal{D}_2 \to \mathcal{R}_2$ with $|\mathcal{D}_2| = |\mathcal{R}_2| = 2^n - p - s_1$. We define $V_{\text{out}} = \{0,1\}^n \backslash \mathcal{R}_1$ as the set of range values of π_1 that are not permitted (basically these are the v values from $\tau_1^{\text{new}}, \tau_2^{\text{new}}$) and similarly for Y_{out}.

For $\alpha = 0, \ldots, q' - 1$, define $\lambda_{\alpha+1}$ as the number of solutions

$$\{v^{(1)}, \ldots, v^{(\alpha+1)}; y^{(1)}, \ldots, y^{(\alpha+1)}\}$$

that satisfy:

(1) $\{v^{(1)}, \ldots, v^{(\alpha)}; y^{(1)}, \ldots, y^{(\alpha)}\}$ satisfy λ_α;
(2) $v^{(\alpha+1)} \oplus y^{(\alpha+1)} = C^{(\alpha+1)} \oplus K_1 \oplus K_2$;
(3) $v^{(\alpha+1)} \notin \{v^{(1)}, \ldots, v^{(\alpha)}\} \cup V_{\text{out}}$;

(4) $y^{(\alpha+1)} \notin \{y^{(1)}, \ldots, y^{(\alpha)}\} \cup Y_{\text{out}}$.

Our goal is to derive a recursive formula for $\lambda_{\alpha+1}$ that depends on λ_α, such that a lower bound can be found for the expression $\lambda_{\alpha+1}/\lambda_\alpha$. Note that, by definition,

$$|comp_{\mathcal{O}}(\tau)| = \lambda_{q'}(2^n - p - s_2 - q')!(2^n - p - s_1 - q')! \,. \tag{25}$$

Processing from (24), we obtain

$$\frac{\Pr[X_{\mathcal{O}} = \tau]}{\Pr[X_{\mathcal{P}} = \tau]} = \frac{\lambda_{q'}(2^n - p - s_2 - q')!(2^n - p - s_1 - q')! \cdot 2^{nq}}{(2^n - p)!^2} \,. \tag{26}$$

We will derive a lower bound for $\lambda_{\alpha+1}/\lambda_\alpha$. Define by $B_{(1,2)}$ the set of solutions that only comply with (1) and (2), with no side condition from (3) and (4). Define by $B_{(3:i)}$ the set of solutions that comply with (1) and (2) of above, and satisfy $\neg(3:i)$ for $i = 1, \ldots, \alpha + |V_{\text{out}}|$. It means that any solution in this case satisfies (1) and (2), and $v^{(\alpha+1)} \in \{v^{(1)}, \ldots, v^{(\alpha)}\} \cup V_{\text{out}}$ (nothing is said about $y^{(\alpha+1)}$ except for property (2)). Similarly for $B(4:i)$. By the principle of inclusion-exclusion, we obtain

$$\begin{aligned}
\lambda_{\alpha+1} &= \left|B_{(1,2)}\right| - \left|\bigcup_{i=1}^{\alpha+|V_{\text{out}}|} B_{(3:i)} \cup \bigcup_{i=1}^{\alpha+|Y_{\text{out}}|} B_{(4:i')}\right| \\
&\geq \left|B_{(1,2)}\right| - \sum_{i=1}^{\alpha+|V_{\text{out}}|} \left|B_{(3:i)}\right| - \sum_{i=1}^{\alpha+|Y_{\text{out}}|} \left|B_{(4:i)}\right| + \sum_{i'=1}^{\alpha+|Y_{\text{out}}|} \sum_{i=1}^{\alpha+|V_{\text{out}}|} \left|B_{(3:i)} \cap B_{(4:i')}\right| \\
&\geq 2^n \cdot \lambda_\alpha - \sum_{i=1}^{\alpha+|V_{\text{out}}|} \lambda_\alpha - \sum_{i=1}^{\alpha+|Y_{\text{out}}|} \lambda_\alpha + \sum_{i'=1}^{\alpha+|Y_{\text{out}}|} \sum_{i=1}^{\alpha+|V_{\text{out}}|} \left|B_{(3:i)} \cap B_{(4:i')}\right| \,.
\end{aligned}$$

By the fact that

$$\sum_{i'=1}^{\alpha+|Y_{\text{out}}|} \sum_{i=1}^{\alpha+|V_{\text{out}}|} \left|B_{(3:i)} \cap B_{(4:i')}\right| \geq 0 \,,$$

we get

$$\lambda_{\alpha+1} \geq 2^n \lambda_\alpha - (\alpha + p + s_2)\lambda_\alpha - (\alpha + p + s_1)\lambda_\alpha \,.$$

Thus, we have obtained

$$\frac{\lambda_{\alpha+1}}{\lambda_\alpha} \geq 2^n - 2\alpha - 2p - s_1 - s_2 \,, \tag{27}$$

with $\lambda_0 = 1$.

Processing from (26), we obtain

$$\begin{aligned}
(26) = \prod_{i=1}^{s_1-1} \frac{2^n}{(2^n - p - i)} \cdot \prod_{i=1}^{s_2-1} \frac{2^n}{(2^n - p - i)} \\
\cdot \prod_{i=0}^{q'-1} \frac{\lambda_{i+1}}{\lambda_i} \cdot \frac{2^n}{(2^n - p - s_2 - i)(2^n - p - s_1 - i)} \,.
\end{aligned} \tag{28}$$

Using that $p, s_1, s_2 \leq 2^n$, and combining (27) with (28), we obtain

$$\begin{aligned}
(28) &\geq \prod_{i=0}^{q'-1} \frac{\lambda_{i+1}}{\lambda_i} \cdot \frac{2^n}{(2^n-p-s_2-i)(2^n-p-s_1-i)} \\
&\geq \prod_{i=0}^{q'-1} \frac{(2^n-2i-2p-s_1-s_2)2^n}{(2^n-p-s_2-i)(2^n-p-s_1-i)} \\
&= \prod_{i=0}^{q'-1} \left(1 - \frac{(p+s_2+p)(p+s_1+p)}{(2^n-p-s_2-p)(2^n-p-s_1-p)}\right) \\
&\geq \prod_{i=0}^{q'-1} \left(1 - \frac{(p+s_2+q')(p+s_1+q')}{(2^n-p-s_2-q')(2^n-p-s_1-q')}\right) \\
&\geq \prod_{i=0}^{q'-1} \left(1 - \frac{(p+s_2+q')(p+s_1+q')}{2^{2n}}\right) \\
&= \left(1 - \frac{(p+s_2+q')(p+s_1+q')}{2^{2n}}\right)^{q'} \\
&\geq 1 - \frac{q'(p+s_2+q')(p+s_1+q')}{2^{2n}} \\
&\geq 1 - \frac{q(p+q)^2}{2^{2n}} \,. \qquad (29)
\end{aligned}$$

where we use that $(1-x)^y \geq 1-xy$ and $q' + s_1 + s_2 = q$. We conclude from (28) and (29) that

$$\frac{\Pr[X_{\mathcal{O}} = \tau]}{\Pr[X_{\mathcal{P}} = \tau]} \geq 1 - \frac{q(p+q)^2}{2^{2n}} =: 1 - \epsilon \,.$$

Conclusion. Using Patarin's H-Coefficient technique (Lemma 1), we obtain

$$\mathbf{Adv}^{\mathrm{prf}}_{\mathrm{SoEM22}}(\mathcal{D}) \leq \frac{q(p+q)^2}{2^{2n}} + \frac{3qp^2}{2^{2n}} \,.$$

6.4 Proof of Theorem 2 on SoKAC21

The proof is similar to the one of Theorem 1 (Section 6.3). Let $K \xleftarrow{\$} \{0,1\}^n$, $\pi_1, \pi_2 \xleftarrow{\$} \mathrm{Perm}(n)$, and $\varphi \xleftarrow{\$} \mathrm{Func}(n)$. Consider any distinguisher $\mathcal{D}$ that has access to three oracles: $(\mathrm{SoKAC21}_K^{\pi_1,\pi_2}, \pi_1^{\pm}, \pi_2^{\pm})$ in the real world or $(\varphi, \pi_1^{\pm}, \pi_2^{\pm})$ in the ideal world. We assume $\mathcal{D}$ is computational unbounded and deterministic. The distinguisher makes q construction queries to $\mathcal{O}_0 \in \{\mathrm{SoKAC21}_K^{\pi_1,\pi_2}, \varphi\}$, and these are summarized in a transcript of the form $\tau_0 = \{(M^{(1)}, C^{(1)}), \ldots, (M^{(q)}, C^{(q)})\}$. It also makes p primitive queries to $\mathcal{O}_1 = \pi_1^{\pm}$ and p primitive queries to $\mathcal{O}_2 = \pi_2^{\pm}$, and like before, these are respectively summarized in transcripts $\tau_1 =$

$\{(u^{(1)}, v^{(1)}), \ldots, (u^{(p)}, v^{(p)})\}$ and $\tau_2 = \{(x^{(1)}, y^{(1)}), \ldots, (x^{(p)}, y^{(p)})\}$. We assume that τ_0, τ_1, and τ_2 do not contain duplicate elements. After $\mathcal{D}$'s interaction with the oracles, but before it outputs its decision, we disclose the key K to the distinguisher. In real world, this is the key used in the construction. In the ideal world K is a dummy key that is drawn uniformly at random. The complete view is denoted $\tau = (\tau_0, \tau_1, \tau_2, K)$.

Bad Events. We say that $\tau \in \mathcal{T}_{\text{bad}}$ if and only if there exists a construction query $(M^{(j)}, C^{(j)}) \in \tau_0$ and primitive queries $(u^{(i)}, v^{(i)}) \in \tau_1$ and $(x^{(i')}, y^{(i')}) \in \tau_2$ such that one of the following conditions holds:

$$\text{bad}_1 \colon K = M^{(j)} \oplus u^{(i)} = v^{(i)} \oplus x^{(i')}\,, \tag{30}$$

$$\text{bad}_2 \colon K = M^{(j)} \oplus u^{(i)} = C^{(j)} \oplus v^{(i)} \oplus y^{(i')}\,, \tag{31}$$

$$\text{bad}_3 \colon K = v^{(i)} \oplus x^{(i')} = C^{(j)} \oplus v^{(i)} \oplus y^{(i')}\,. \tag{32}$$

Note that any attainable transcript τ for which $\tau \notin \mathcal{T}_{\text{bad}}$, implies that τ is a good transcript.

The bad events (30-32) match those of SoEM22, (19-21), with the difference that one single key K is used instead of two different keys K_1, K_2. Indeed, in SoKAC21$_K^{\pi_1,\pi_2}$, every construction query j induces *exactly one* evaluation $(u^{(j)}, v^{(j)})$ of the underlying public permutation π_1, and *exactly one* evaluation $(x^{(j)}, y^{(j)})$ of the underlying public permutation π_2, and these two queries satisfy

$$\begin{aligned} M^{(j)} \oplus u^{(j)} &= K\,, \\ v^{(j)} \oplus x^{(j)} &= K\,, \\ C^{(j)} \oplus v^{(j)} \oplus y^{(j)} &= K\,. \end{aligned}$$

As before, $(M^{(j)}, C^{(j)})$ and K fix the value $u^{(j)}$, but there is "freedom" in the values $v^{(j)} \oplus x^{(j)}$ and $v^{(j)} \oplus y^{(j)}$. As before, if it happens to be that the distinguisher queried $u^{(j)}$, this would fix the tuple $(x^{(j)}, y^{(j)})$ for π_2. If the distinguisher also happened to have queried this one, in the real world it would match but in the ideal world it would mismatch with high probability.

$\mathbf{Pr}[\boldsymbol{X_{\mathcal{P}}} \in \boldsymbol{\mathcal{T}_{\text{bad}}}]$. We want to bound the probability that an ideal world transcript τ satisfies either of (30)-(32). Therefore, the probability that $\tau \in \mathcal{T}_{\text{bad}}$ is given by

$$\Pr[\tau \in \mathcal{T}_{\text{bad}}] \le \Pr[\text{bad}_1] + \Pr[\text{bad}_2] + \Pr[\text{bad}_3]\,.$$

We denote

$$\begin{aligned} \Omega_1 &= \left| \left\{ (j,i,i') \;\middle|\; u^{(i)} \oplus v^{(i)} = M^{(j)} \oplus x^{(i')} \right\} \right|\,, \\ \Omega_2 &= \left| \left\{ (j,i,i') \;\middle|\; M^{(j)} \oplus C^{(j)} = u^{(i)} \oplus v^{(i)} \oplus y^{(i')} \right\} \right|\,, \\ \Omega_3 &= \left| \left\{ (j,i,i') \;\middle|\; C^{(j)} = x^{(i')} \oplus y^{(i')} \right\} \right|\,. \end{aligned}$$

Clearly, as $K \xleftarrow{\$} \{0,1\}^n$, for any $i \in \{1,2,3\}$ and $A_i \in \mathbb{N}$, we have

$$\Pr[\mathrm{bad}_i] \le \Pr[\Omega_i \ge A_i] + \frac{A_i}{2^n}\,.$$

For $i = 1$, we will use the sum-capture lemma of Section 6.2. Define

$$\begin{aligned} Z &= \{u^{(i)} \oplus v^{(i)} \colon (u^{(i)}, v^{(i)}) \in \tau_1\}\,, \\ A &= \{M^{(j)} \colon (M^{(j)}, C^{(j)}) \in \tau_0\}\,, \\ B &= \{x^{(i')} \colon (x^{(i')}, y^{(i')}) \in \tau_2\}\,. \end{aligned}$$

Then, by Lemma 2 with $\Omega_1 = \mu(Z, A, B)$,

$$\Pr\left[\mu(Z,A,B) \ge \frac{qp^2}{2^n} + \frac{2p^2\sqrt{qp}}{2^n} + 3\sqrt{nqp^2}\right] \le \frac{2}{2^n}\,.$$

We thus set $A_1 = \frac{qp^2}{2^n} + \frac{2p^2\sqrt{qp}}{2^n} + 3\sqrt{nqp^2}$ and obtain

$$\Pr[\mathrm{bad}_1] \le \frac{2}{2^n} + \frac{qp^2}{2^{2n}} + \frac{2p^2\sqrt{qp}}{2^{2n}} + \frac{3\sqrt{nqp^2}}{2^n}\,.$$

For $i = 2$, the equation in Ω_2 involves two random values ($C^{(j)}$ and $u^{(i)} \oplus v^{(i)}$), and we resort to a simple Markov bound:

$$\Pr[\Omega_2 \ge A_2] \le \frac{qp^2}{2^n A_2}\,,$$

and obtain by setting $A_2 = \sqrt{qp^2}$:

$$\Pr[\mathrm{bad}_2] \le \frac{2\sqrt{qp^2}}{2^n}\,.$$

For $i = 3$, $\Omega_3 \ge A_3$ means that

$$\Omega_3' = \left|\left\{(j,i') \;\middle|\; C^{(j)} = x^{(i')} \oplus y^{(i')}\right\}\right| \ge A_3/p\,.$$

By a simple Markov bound,

$$\Pr[\Omega_3' \ge A_3/p] \le \frac{qp^2}{2^n A_3}\,,$$

and we obtain by setting $A_3 = \sqrt{qp^2}$:

$$\Pr[\mathrm{bad}_3] \le \frac{2\sqrt{qp^2}}{2^n}\,.$$

Summing the three probabilities, we get

$$\Pr[\tau \in \mathcal{T}_{\mathrm{bad}}] \le \frac{2}{2^n} + \frac{qp^2}{2^{2n}} + \frac{2p^2\sqrt{qp}}{2^{2n}} + \frac{3\sqrt{nqp^2}}{2^n} + \frac{4\sqrt{qp^2}}{2^n}\,. \tag{33}$$

$\mathbf{Pr}[\boldsymbol{X_{\mathcal{O}}} = \boldsymbol{\tau}] / \mathbf{Pr}[\boldsymbol{X_{\mathcal{P}}} = \boldsymbol{\tau}]$. The analysis of good transcripts of Theorem 1 (Section 6.3) carries over verbatim with the difference that we generate the transcripts τ_0^{new}, τ_1^{new} and τ_2^{new} in the following way. Consider each individual construction query $(M^{(j)}, C^{(j)})$, if $M^{(j)} \oplus K = u^{(i)}$ for some i, then remove $(M^{(j)}, C^{(j)})$ from τ_0^{new} and add $(x, y) = (v^{(i)} \oplus K, C^{(j)} \oplus v^{(i)} \oplus K)$ to τ_2^{new}. We know that if a construction query $(M^{(j)}, C^{(j)})$ collides with $(u^{(i)}, v^{(i)}) \in \tau_1$, then $v^{(i)} \oplus K$ cannot be a valid $x^{(i')}$ value because of $\neg\text{bad}_1$, and $C^{(j)} \oplus v^{(i)} \oplus K$ cannot be a valid $y^{(i')}$ value because of $\neg\text{bad}_2$, for any $(x^{(i')}, y^{(i')}) \in \tau_2$. Similarly for τ_1^{new}.

Conclusion. Using Patarin's H-Coefficient technique (Lemma 1), we obtain

$$\mathbf{Adv}^{\text{prf}}_{\text{SoKAC21}}(\mathcal{D}) \leq \frac{q(p+q)^2}{2^{2n}} + \frac{2}{2^n} + \frac{qp^2}{2^{2n}} + \frac{2p^2\sqrt{qp}}{2^{2n}} + \frac{3\sqrt{nqp^2}}{2^n} + \frac{4\sqrt{qp^2}}{2^n}\,.$$

Acknowledgments. This work was supported in part by the Research Council KU Leuven: GOA TENSE (C16/15/058). Yu Long Chen is supported by a Ph.D. Fellowship from the Research Foundation - Flanders (FWO). Bart Mennink is supported by a postdoctoral fellowship from the Netherlands Organisation for Scientific Research (NWO) under Veni grant 016.Veni.173.017. The authors would like to thank the anonymous reviewers of CRYPTO 2019 for their comments and suggestions.

References

1. Andreeva, E., Daemen, J., Mennink, B., Van Assche, G.: Security of Keyed Sponge Constructions Using a Modular Proof Approach. In: Leander, G. (ed.) FSE 2015. LNCS, vol. 9054, pp. 364–384. Springer (2015)
2. Babai, L.: The Fourier Transform and Equations over Finite Abelian Groups (Lecture Notes, version 1.3) (2002), http://people.cs.uchicago.edu/~laci/reu02/fourier.pdf
3. Beaulieu, R., Shors, D., Smith, J., Treatman-Clark, S., Weeks, B., Wingers, L.: The SIMON and SPECK Families of Lightweight Block Ciphers. Cryptology ePrint Archive, Report 2013/404 (2013)
4. Beierle, C., Jean, J., Kölbl, S., Leander, G., Moradi, A., Peyrin, T., Sasaki, Y., Sasdrich, P., Sim, S.M.: The SKINNY Family of Block Ciphers and Its Low-Latency Variant MANTIS. In: Robshaw, M., Katz, J. (eds.) CRYPTO 2016, Part II. LNCS, vol. 9815, pp. 123–153. Springer (2016)
5. Bellare, M., Impagliazzo, R.: A tool for obtaining tighter security analyses of pseudorandom function based constructions, with applications to PRP to PRF conversion. Cryptology ePrint Archive, Report 1999/024 (1999)
6. Bellare, M., Kilian, J., Rogaway, P.: The Security of Cipher Block Chaining. In: Desmedt, Y. (ed.) CRYPTO '94. LNCS, vol. 839, pp. 341–358. Springer (1994)
7. Bellare, M., Krovetz, T., Rogaway, P.: Luby-Rackoff Backwards: Increasing Security by Making Block Ciphers Non-invertible. In: Nyberg, K. (ed.) EUROCRYPT '98. LNCS, vol. 1403, pp. 266–280. Springer (1998)

8. Bellare, M., Rogaway, P.: The Security of Triple Encryption and a Framework for Code-Based Game-Playing Proofs. In: Vaudenay, S. (ed.) EUROCRYPT 2006. LNCS, vol. 4004, pp. 409–426. Springer (2006)
9. Bernstein, D.J., Kölbl, S., Lucks, S., Massolino, P.M.C., Mendel, F., Nawaz, K., Schneider, T., Schwabe, P., Standaert, F., Todo, Y., Viguier, B.: Gimli : A Cross-Platform Permutation. In: Fischer, W., Homma, N. (eds.) CHES 2017. LNCS, vol. 10529, pp. 299–320. Springer (2017)
10. Bertoni, G., Daemen, J., Hoffert, S., Peeters, M., Van Assche, G., Van Keer, R.: Farfalle: parallel permutation-based cryptography. IACR Trans. Symmetric Cryptol. 2017(4), 1–38 (2017)
11. Bertoni, G., Daemen, J., Peeters, M., Van Assche, G.: On the Security of the Keyed Sponge Construction. Symmetric Key Encryption Workshop (February 2011)
12. Bertoni, G., Daemen, J., Peeters, M., Van Assche, G.: The keccak sha-3 submission. Submission to NIST (Round 3) 6(7), 16 (2011)
13. Bhargavan, K., Leurent, G.: On the Practical (In-)Security of 64-bit Block Ciphers: Collision Attacks on HTTP over TLS and OpenVPN. In: Weippl, E.R., Katzenbeisser, S., Kruegel, C., Myers, A.C., Halevi, S. (eds.) ACM SIGSAC. pp. 456–467. ACM (2016)
14. Bhattacharya, S., Nandi, M.: Full Indifferentiable Security of the Xor of Two or More Random Permutations Using the chi^2 Method. In: Nielsen, J.B., Rijmen, V. (eds.) EUROCRYPT 2018, Part I. LNCS, vol. 10820, pp. 387–412. Springer (2018)
15. Bogdanov, A., Knezevic, M., Leander, G., Toz, D., Varici, K., Verbauwhede, I.: spongent: A Lightweight Hash Function. In: Preneel and Takagi [57], pp. 312–325
16. Bogdanov, A., Knudsen, L.R., Leander, G., Paar, C., Poschmann, A., Robshaw, M.J.B., Seurin, Y., Vikkelsoe, C.: PRESENT: An Ultra-Lightweight Block Cipher. In: Paillier, P., Verbauwhede, I. (eds.) CHES 2007. LNCS, vol. 4727, pp. 450–466. Springer (2007)
17. 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: Pointcheval and Johansson [56], pp. 45–62
18. Borghoff, J., Canteaut, A., Güneysu, T., Kavun, E.B., Knezevic, M., Knudsen, L.R., Leander, G., Nikov, V., Paar, C., Rechberger, C., Rombouts, P., Thomsen, S.S., Yalçin, T.: PRINCE - A Low-Latency Block Cipher for Pervasive Computing Applications - Extended Abstract. In: Wang and Sako [62], pp. 208–225
19. Chang, D., Nandi, M.: A Short Proof of the PRP/PRF Switching Lemma. Cryptology ePrint Archive, Report 2008/078 (2008)
20. Chen, S., Lampe, R., Lee, J., Seurin, Y., Steinberger, J.P.: Minimizing the Two-Round Even-Mansour Cipher. In: Garay, J.A., Gennaro, R. (eds.) CRYPTO 2014, Part I. LNCS, vol. 8616, pp. 39–56. Springer (2014)
21. 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 (2014)
22. Cid, C., Rechberger, C. (eds.): FSE 2014, LNCS, vol. 8540. Springer (2015)
23. Cogliati, B., Lampe, R., Patarin, J.: The Indistinguishability of the XOR of k Permutations. In: Cid and Rechberger [22], pp. 285–302
24. Cogliati, B., Seurin, Y.: EWCDM: An Efficient, Beyond-Birthday Secure, Nonce-Misuse Resistant MAC. In: Robshaw and Katz [58], pp. 121–149
25. Cogliati, B., Seurin, Y.: Analysis of the single-permutation encrypted Davies-Meyer construction. Des. Codes Cryptography 86(12), 2703–2723 (2018)

26. Coron, J., Holenstein, T., Künzler, R., Patarin, J., Seurin, Y., Tessaro, S.: How to Build an Ideal Cipher: The Indifferentiability of the Feistel Construction. J. Cryptology 29(1), 61–114 (2016)
27. Dachman-Soled, D., Katz, J., Thiruvengadam, A.: 10-Round Feistel is Indifferentiable from an Ideal Cipher. In: Fischlin, M., Coron, J. (eds.) EUROCRYPT 2016, Part II. LNCS, vol. 9666, pp. 649–678. Springer (2016)
28. Dai, W., Hoang, V.T., Tessaro, S.: Information-Theoretic Indistinguishability via the Chi-Squared Method. In: Katz and Shacham [40], pp. 497–523
29. Dai, Y., Steinberger, J.P.: Indifferentiability of 8-Round Feistel Networks. In: Robshaw and Katz [58], pp. 95–120
30. De Cannière, C., Dunkelman, O., Knezevic, M.: KATAN and KTANTAN - A Family of Small and Efficient Hardware-Oriented Block Ciphers. In: Clavier, C., Gaj, K. (eds.) CHES 2009. LNCS, vol. 5747, pp. 272–288. Springer (2009)
31. Dunkelman, O., Keller, N., Shamir, A.: Minimalism in Cryptography: The Even-Mansour Scheme Revisited. In: Pointcheval and Johansson [56], pp. 336–354
32. Even, S., Mansour, Y.: A Construction of a Cipher From a Single Pseudorandom Permutation. In: Imai, H., Rivest, R.L., Matsumoto, T. (eds.) ASIACRYPT '91. LNCS, vol. 739, pp. 210–224. Springer (1991)
33. Gentry, C., Ramzan, Z.: Eliminating Random Permutation Oracles in the Even-Mansour Cipher. In: Lee, P.J. (ed.) ASIACRYPT 2004. LNCS, vol. 3329, pp. 32–47. Springer (2004)
34. Gilboa, S., Gueron, S.: The Advantage of Truncated Permutations. CoRR abs/1610.02518 (2016)
35. Gong, Z., Nikova, S., Law, Y.W.: KLEIN: A New Family of Lightweight Block Ciphers. In: Juels, A., Paar, C. (eds.) RFIDSec 2011. LNCS, vol. 7055, pp. 1–18. Springer (2011)
36. Guo, J., Peyrin, T., Poschmann, A.: The PHOTON Family of Lightweight Hash Functions. In: Rogaway, P. (ed.) CRYPTO 2011. LNCS, vol. 6841, pp. 222–239. Springer (2011)
37. Hall, C., Wagner, D., Kelsey, J., Schneier, B.: Building PRFs from PRPs. In: Krawczyk, H. (ed.) CRYPTO '98. LNCS, vol. 1462, pp. 370–389. Springer (1998)
38. Hong, D., Sung, J., Hong, S., Lim, J., Lee, S., Koo, B., Lee, C., Chang, D., Lee, J., Jeong, K., Kim, H., Kim, J., Chee, S.: HIGHT: A New Block Cipher Suitable for Low-Resource Device. In: Goubin, L., Matsui, M. (eds.) CHES 2006. LNCS, vol. 4249, pp. 46–59. Springer (2006)
39. Impagliazzo, R., Rudich, S.: Limits on the Provable Consequences of One-way Permutations. In: Goldwasser, S. (ed.) CRYPTO '88. LNCS, vol. 403, pp. 8–26. Springer (1988)
40. Katz, J., Shacham, H. (eds.): CRYPTO 2017, Part III, LNCS, vol. 10403. Springer (2017)
41. Lampe, R., Patarin, J., Seurin, Y.: An Asymptotically Tight Security Analysis of the Iterated Even-Mansour Cipher. In: Wang and Sako [62], pp. 278–295
42. Lampe, R., Seurin, Y.: Security Analysis of Key-Alternating Feistel Ciphers. In: Cid and Rechberger [22], pp. 243–264
43. Lim, C.H., Korkishko, T.: mCrypton - A Lightweight Block Cipher for Security of Low-Cost RFID tags and sensors. In: Song, J., Kwon, T., Yung, M. (eds.) WISA 2005. LNCS, vol. 3786, pp. 243–258. Springer (2005)
44. Luby, M., Rackoff, C.: How to Construct Pseudorandom Permutations from Pseudorandom Functions. SIAM J. Comput. 17(2), 373–386 (1988)
45. Lucks, S.: The Sum of PRPs Is a Secure PRF. In: Preneel, B. (ed.) EUROCRYPT 2000. LNCS, vol. 1807, pp. 470–484. Springer (2000)

46. Maurer, U.M., Renner, R., Holenstein, C.: Indifferentiability, Impossibility Results on Reductions, and Applications to the Random Oracle Methodology. In: Naor, M. (ed.) TCC 2004. vol. 2951, pp. 21–39. Springer (2004)
47. Mennink, B., Neves, S.: Encrypted Davies-Meyer and Its Dual: Towards Optimal Security Using Mirror Theory. In: Katz and Shacham [40], pp. 556–583
48. Mennink, B., Preneel, B.: On the XOR of Multiple Random Permutations. In: Malkin, T., Kolesnikov, V., Lewko, A.B., Polychronakis, M. (eds.) ACNS 2015. LNCS, vol. 9092, pp. 619–634. Springer (2015)
49. Mennink, B., Reyhanitabar, R., Vizár, D.: Security of Full-State Keyed Sponge and Duplex: Applications to Authenticated Encryption. In: Iwata, T., Cheon, J.H. (eds.) ASIACRYPT 2015, Part II. LNCS, vol. 9453, pp. 465–489. Springer (2015)
50. Nachef, V., Patarin, J., Volte, E.: Feistel Ciphers - Security Proofs and Cryptanalysis. Springer (2017)
51. Patarin, J.: Étude des Générateurs de Permutations Basés sur le Schéma du D.E.S. Ph.D. thesis, Université Paris 6, Paris, France (Nov 1991)
52. Patarin, J.: On Linear Systems of Equations with Distinct Variables and Small Block Size. In: Won, D., Kim, S. (eds.) ICISC 2005. LNCS, vol. 3935, pp. 299–321. Springer (2005)
53. Patarin, J.: The "Coefficients H" Technique. In: Avanzi, R.M., Keliher, L., Sica, F. (eds.) SAC 2008. LNCS, vol. 5381, pp. 328–345. Springer (2008)
54. Patarin, J.: Introduction to Mirror Theory: Analysis of Systems of Linear Equalities and Linear Non Equalities for Cryptography. Cryptology ePrint Archive, Report 2010/287 (2010)
55. Patarin, J.: Mirror Theory and Cryptography. Cryptology ePrint Archive, Report 2016/702 (2016)
56. Pointcheval, D., Johansson, T. (eds.): EUROCRYPT 2012, LNCS, vol. 7237. Springer (2012)
57. Preneel, B., Takagi, T. (eds.): CHES 2011, LNCS, vol. 6917. Springer (2011)
58. Robshaw, M., Katz, J. (eds.): CRYPTO 2016, Part I, LNCS, vol. 9814. Springer (2016)
59. Shibutani, K., Isobe, T., Hiwatari, H., Mitsuda, A., Akishita, T., Shirai, T.: Piccolo: An Ultra-Lightweight Blockcipher. In: Preneel and Takagi [57], pp. 342–357
60. Steinberger, J.: The Sum-Capture Problem for Abelian Groups (2014), http://arxiv.org/abs/1309.5582
61. Steinberger, J.P.: Improved Security Bounds for Key-Alternating Ciphers via Hellinger Distance. Cryptology ePrint Archive, Report 2012/481 (2012)
62. Wang, X., Sako, K. (eds.): ASIACRYPT 2012, LNCS, vol. 7658. Springer (2012)
63. Wu, W., Zhang, L.: LBlock: A Lightweight Block Cipher. In: Lopez, J., Tsudik, G. (eds.) ACNS 2011. LNCS, vol. 6715, pp. 327–344 (2011)