Categorization of Faulty Nonce Misuse Resistant Message Authentication

Yu Long Chen[1], Bart Mennink[2], and Bart Preneel[1]

[1] imec-COSIC, KU Leuven, Belgium
yulong.chen, bart.preneel@kuleuven.be
[2] Digital Security Group, Radboud University, Nijmegen, The Netherlands
b.mennink@cs.ru.nl

Abstract. A growing number of lightweight block ciphers are proposed for environments such as the Internet of Things. An important contribution to the reduced implementation cost is a block length n of 64 or 96 bits rather than 128 bits. As a consequence, encryption modes and message authentication code (MAC) algorithms require security beyond the $2^{n/2}$ birthday bound. This paper provides an extensive treatment of MAC algorithms that offer beyond birthday bound PRF security for both nonce-respecting and nonce-misusing adversaries. We study constructions that use two block cipher calls, one universal hash function call and an arbitrary number of XOR operations. We start with the separate problem of generically identifying all possible secure n-to-n-bit pseudorandom functions (PRFs) based on two block cipher calls. The analysis shows that the existing constructions EDM, SoP, and EDMD are the only constructions of this kind that achieve beyond birthday bound security. Subsequently we deliver an exhaustive treatment of MAC algorithms, where the outcome of a universal hash function evaluation on the message may be entered at any point in the computation of the PRF. We conclude that there are a total amount of nine schemes that achieve beyond birthday bound security, and a tenth construction that cannot be proven using currently known proof techniques. For these former nine MAC algorithms, three constructions achieve optimal n-bit security in the nonce-respecting setting, but are completely insecure if the nonce is reused. The remaining six constructions have $3n/4$-bit security in the nonce-respecting setting, and only four out of these six constructions still achieve beyond the birthday bound security in the case of nonce misuse.

Keywords: PRF, beyond birthday bound security, faulty nonce model, EDM, SoP, EDMD

1 Introduction

Message authentication code (MAC) algorithms are one of the fundamental building blocks in cryptography. Given a message M, it allows a sender in possession of a secret key K to compute an authentication tag T, which can then be verified by the receiver provided that it is also in possession of the key. The tag should be hard to forge, i.e., without knowledge of the key, it should be computationally infeasible to compute the tag corresponding to any new message. In this work, we will focus on nonce-based MAC algorithms. These functions take as additional input a nonce N that is used to randomize the scheme.

1.1 Wegman-Carter

Undoubtedly one of the most influential nonce-based MAC algorithms to date is due to Wegman and Carter [44], which was built on earlier work by Gilbert, MacWilliams, and Sloane [19]. Their construction first processes the message with a universal hash function H using a secret hash key, and subsequently masks the output with a pseudorandom function (PRF) F evaluated on the nonce:

$$\mathrm{WC}_{K,K_h}(N,M) = F_K(N) \oplus H_{K_h}(M)\,.$$

The Wegman-Carter construction is proven to achieve n-bit security if H is an ϵ-almost XOR universal hash function with small ϵ ($\epsilon \approx 2^{-n}$), F is a PRF, and the nonce is never repeated [44].

One concern with WC is that dedicated PRFs are difficult to construct. The only exceptions are SURF [5], AES-PRF [31], and SipHash [1], which might ultimately considered to be permutation-based as well. Pseudorandom permutations (PRPs), on the other hand, are in abundance, but instantiating Wegman-Carter with a PRP instead of a PRF – the resulting function is known as Wegman-Carter-Shoup – only achieves close to birthday bound security [6, 28, 34, 43]. This bound may be on the edge of what is desired if the construction is instantiated with a lightweight block cipher [2,3,8,10,16,20,42] with small block size n. For example, it only takes approximately $2^{32} \cdot 64$ bits of data (35 GB) to break Wegman-Carter-Shoup with a 64-bit block cipher.

1.2 Nonce-Misuse Resistance

A second concern about the Wegman-Carter construction is its strict dependency on the nonce. Any repetition of a single nonce will break the Wegman-Carter(-Shoup) MAC [21, 24]: it would result in two tags $T = E_K(N) \oplus H_{K_h}(M)$ and $T' = E_K(N) \oplus H_{K_h}(M')$ for two different messages M, M' which might allow an attacker to deduce information about K_h.

In order to solve this nonce-misuse problem, Cogliati and Seurin introduced Encrypted Wegman-Carter with Davies-Meyer (EWCDM) [13]. EWCDM can be seen as a Wegman-Carter construction, with a Davies-Meyer construction as PRF, then followed by an encryption of the output. The security improvement in EWCDM lies in the “protection” of the outcome of this construction by an extra evaluation of a block cipher:

$$\mathrm{EWCDM}_{K_1,K_2,K_h}(N,M) = E_{K_2}(E_{K_1}(N) \oplus N \oplus H_{K_h}(M))\,.$$

Cogliati and Seurin [13] proved that this construction achieves $2n/3$-bit MAC security in the nonce-respecting scenario and $n/2$-bit MAC security in the nonce-misuse scenario. Mennink and Neves [30] proved almost n-bit PRF security of the mode in the nonce-respecting scenario. Later, a dual variant of EWCDM, called the Decrypted Wegman-Carter with Davies-Meyer (DWCDM), was introduced by Datta et al. [15]. Instead of making the second block cipher call using another independent key, DWCDM evaluates the block cipher in the inverse direction using the same key.

While these MAC algorithms provide security beyond the birthday barrier, most of them are only birthday bound secure if a nonce is reused. This might occur, for example, if a stateless device chooses nonces uniformly at random from a small set, if there is a faulty implementation of the cipher involved, or otherwise. For example, Böck et al. performed an internet-wide scan [7] and found 184 HTTPS servers that used a duplicate nonce for AES-GCM [29].

Dutta et al. [18] formalized the "faulty nonce model" for MAC algorithms. In the faulty nonce model, one considers a nonce-based MAC as usual, but labels a MAC query as "faulty" if it is performed for a repeated nonce. The authors furthermore introduced the nonce-based Enhanced Hash-then-Mask (nEHtM). At its base, nEHtM is a nonce-based variant of EHtM [32] where the random salt is replaced by a nonce and the PRF by a block cipher:

$$\mathrm{nEHtM}_{K,K_h}(N,M) = E_K(0 \parallel N) \oplus E_K(1 \parallel (N \oplus H_{K_h}(M)))\,.$$

Dutta et al. proved that nEHtM achieves $2n/3$-bit security when the number of faulty nonces is below $2^{n/3}$, and proved graceful security degradation of at least $n/2$-bit security in the faulty model. Choi et al. [12] improved the security bound to $3n/4$-bit when the number of faulty nonces is below $2^{3n/8}$, and also proved graceful security degradation. Graceful degradation here means that the actual security level is between $3n/4$ (resp., $2n/3$) and $n/2$, depending on the total number of faulty queries that an adversary makes.

1.3 Our Contribution

In this work, we perform a general treatment of the design of block cipher based MAC algorithms that achieve beyond birthday bound PRF security in the nonce-respecting model. We subsequently consider how these schemes behave in the faulty nonce model. We restrict our focus to MAC algorithms based on a single universal hash function call on the input, two block cipher calls, and an arbitrary amount of XOR operations to combine the inputs and outcomes of the cryptographic building blocks.

Before diving into MAC design, however, we make one step backwards. Hidden in EWCDM is an n-bit PRF construction called the Encrypted Davies-Meyer construction EDM:

$$\mathrm{EDM}_{K_1,K_2}(N) = E_{K_2}(E_{K_1}(N) \oplus N)\,. \qquad (1)$$

Although one cannot reduce security of EWCDM to that of EDM [13], the proofs share similarities [13, 30]. Likewise, nEHtM can be seen to hide the Sum of Permutation construction SoP [4]:

$$\mathrm{SoP}_{K_1,K_2}(N) = E_{K_1}(N) \oplus E_{K_2}(N)\,. \tag{2}$$

We can conclude that one might have little hope in designing a MAC algorithm with beyond the birthday bound PRF security if that particular construction with the universal hash function evaluation omitted is not a good PRF in the first place. Therefore, in Section 3, we start with performing a general analysis of n-to-n-bit PRF designs from two block cipher calls. We prove that, although there are 2^6 constructions of that type to consider, for *all but six of them*, an attack in the birthday bound or faster can be mounted. The six remaining schemes are, perhaps unsurprisingly, EDM of (1), SoP of (2), the Encrypted Davies-Meyer Dual construction EDMD [30]:

$$\mathrm{EDMD}_{K_1,K_2}(N) = E_{K_2}(E_{K_1}(N)) \oplus E_{K_1}(N)\,, \tag{3}$$

and the natural siblings of these three schemes that consist of XORing the input to the output.

Supported by these results, we go on to perform an exhaustive analysis of all MAC algorithms that can be constructed from two block cipher calls with a universal hash evaluation on the message. We prove that although there are 2^9 constructions of that type to consider, the quest leads to ten interesting MAC algorithms: five are based on EDM, three on SoP, and two on EDMD. The schemes are formalized in Section 4.

Out of these ten schemes, three of them are simply Wegman-Carter based on the PRFs EDM, SoP, and EDMD, respectively. These achieve n-bit security, but are completely insecure if the nonce is reused. The four remaining EDM-based schemes and two remaining SoP-based schemes achieve $3n/4$-bit security in the nonce-respecting scenario, and four out these six schemes still achieve beyond the birthday bound security in the case of nonce misuse. Note that there is always a safety margin that must be taken into account. This means that when we talk about $3n/4$-bit security, only $2^{3n/4-\delta}$ queries can be made, where δ is chosen such that the resulting advantage of the distinguisher remains negligible. Currently known proof techniques did not allow us to prove security of the final EDMD-based scheme, which was already mentioned (without proof) by Nandi [35]. We conjecture that this scheme has beyond birthday bound security against nonce-respecting adversaries. Our results are performed in the faulty nonce model of Dutta et al. [18] and are given in Section 4. These ten MAC algorithms are compared in terms of their security and efficiency in Table 1.

In Figure 1, we show the four constructions that still achieve beyond the birthday bound security in the case of nonce misuse: two are serial, while the other two are parallel. The two serial constructions are new, and the two parallel constructions based on SoP are variants of the nEHtM construction of Dutta et al. [18] that uses two independent keys. The parallel constructions still achieve

Table 1: Comparison of the ten MAC algorithms, where μ is the number of faulty nonces. Here, n is the block size and E_{K_1} refers to the first block cipher evaluation in the construction. EWCDM was shown to achieve n-bits security using an unverified version of the mirror theory.

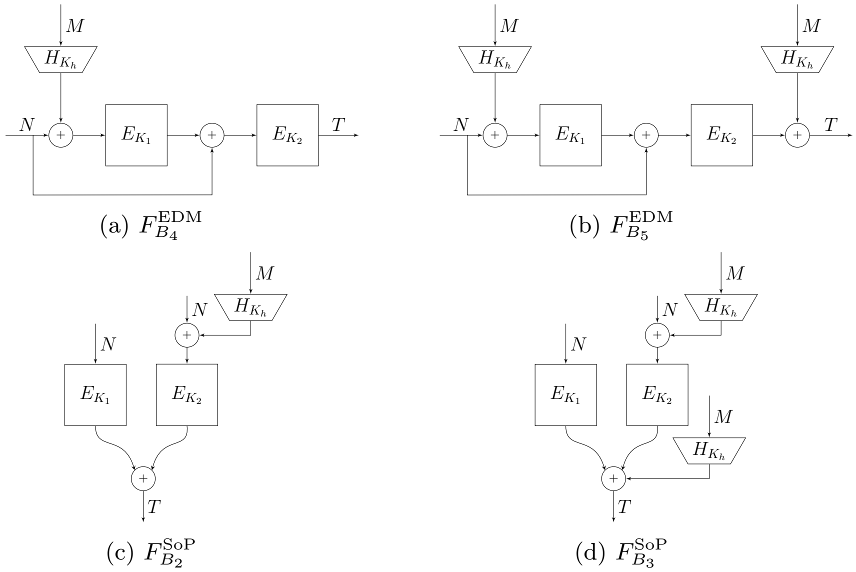
MAC	nonce-resp. security ($\log_2$)	nonce-misuse security ($\log_2$)	computing E_{K_1} without M	sequential/ parallel	security tightness	note
$F^{\text{EDM}}_{B_1}$	n	0	✓	S	tight	WC-with-EDM [44]
$F^{\text{SoP}}_{B_1}$	n	0	✓	P	tight	WC-with-SoP [44]
$F^{\text{EDMD}}_{B_1}$	n	0	✓	S	tight	WC-with-EDMD [44]
$F^{\text{EDM}}_{B_2}$	$3n/4$ (n)	$n/2$	✓	S	not (tight)	EWCDM [13], Thm. 2 ([30])
$F^{\text{EDM}}_{B_3}$	$3n/4$	$n/2$	✓	S	not	Thm. 2
$F^{\text{EDM}}_{B_4}$	$3n/4$	$3n/4$ ($\mu < 2^{n/2}$)	—	S	?	Thm. 3
$F^{\text{EDM}}_{B_5}$	$3n/4$	$3n/4$ ($\mu < 2^{n/2}$)	—	S	?	Thm. 3
$F^{\text{SoP}}_{B_2}$	$3n/4$	$3n/4$ ($\mu \leq 2^{n/4}$)	✓	P	?	Thm. 4
$F^{\text{SoP}}_{B_3}$	$3n/4$	$3n/4$ ($\mu \leq 2^{n/4}$)	✓	P	?	Thm. 4
$F^{\text{EDMD}}_{B_2}$	?	?	✓	S	—	—

$3n/4$ security with $\mu \leq 2^{n/4}$ faulty nonces. Surprisingly, for the two serial constructions, the security does not decrease as long as the number of faulty nonces is below $2^{n/2}$. While parallel modes inherently profit most from modern parallel architectures, the Comb scheduling technique introduced in [9] can solve this problem even for serial modes on the server side. Besides, the serial structure can be particularly suited for the design of efficient dedicated primitives [17,31], while this is not the case for parallel modes. Therefore, an interesting consequence of our results is the introduction of two new constructions $F^{\text{EDM}}_{B_4}$ and $F^{\text{EDM}}_{B_5}$, where the security of these constructions remains the same as long as the number of faulty nonces is below $2^{n/2}$.

The security proofs in this work are performed using Patarin's H-coefficient technique [11, 36, 38], and using the mirror theory by Kim et al. [26]. We believe that the security bounds of the two SoP-based MAC algorithms can be improved by improving the mirror theory. The main security analysis is given in Section 5.3, where we show the PRF security of these MAC algorithms, the analysis straightforwardly generalizes to MAC security.

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 $X \oplus Y$. We denote by $\{0,1\}^*$ the set of bit strings of arbitrary length. For a value Z, we denote by $z \leftarrow Z$ the assignment of Z to the variable z. For a finite set S, we denote by $s \overset{\$}{\leftarrow} S$ the uniformly random selection of s from S. For an algorithm $\mathcal{D}$ and two oracles $\mathcal{O}, \mathcal{P}$, we denote by $\mathcal{D}^{\mathcal{O}}$ the evaluation of $\mathcal{D}$ with oracle interaction to $\mathcal{O}$,



(a) $F^{\mathrm{EDM}}_{B_4}$

(b) $F^{\mathrm{EDM}}_{B_5}$

(c) $F^{\mathrm{SoP}}_{B_2}$

(d) $F^{\mathrm{SoP}}_{B_3}$

Fig. 1: Depiction of four MAC algorithms, where E is a block cipher and H a universal hash function.

and by $\Delta_{\mathcal{D}}\Big(\mathcal{O}\ ; \mathcal{P}\Big)$ the advantage of $\mathcal{D}$ in distinguishing $\mathcal{O}$ from an oracle $\mathcal{P}$. For a primitive P, we denote by $\mathcal{O}[P]$ the oracle $\mathcal{O}$ built on the primitive P. We denote by $[q]$ the shorthand notation for $\{1, \ldots, q\}$. For two disjoint sets P and Q, we denote their (disjoint) union as $P \sqcup Q$.

2.1 Block Ciphers

For $k, n \in \mathbb{N}$, a block cipher is a function $E\colon \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ such that for fixed key $K \in \{0,1\}^k$, $E_K(\cdot) = E(K, \cdot)$ is a permutation on $\{0,1\}^n$.

Denote by $\mathrm{Perm}(n)$ the set of all permutations on $\{0,1\}^n$. The prp-security of a block cipher E is measured by considering a distinguisher $\mathcal{D}$ that is given forward access to either E_K for secret key $K \xleftarrow{\$} \{0,1\}^k$, or a random permutation $\pi \xleftarrow{\$} \mathrm{Perm}(n)$, and its goal is to determine which oracle it is given access to:

$$\mathbf{Adv}^{\mathrm{prp}}_{E}(\mathcal{D}) = \left| \Pr\left[K \xleftarrow{\$} \{0,1\}^k \colon \mathcal{D}^{E_K} = 1\right] - \Pr\left[\pi \xleftarrow{\$} \mathrm{Perm}(n) \colon \mathcal{D}^{\pi} = 1\right] \right| .$$

Note that we only consider the prp-security of block ciphers instead of the sprp-security, where $\mathcal{D}$ would have access to the inverse of E_K as well. The reason for this is that the constructions that we analyze only evaluate the underlying block ciphers in forward direction.

2.2 Nonce-Based Pseudorandom Functions

For $k, n \in \mathbb{N}$, a nonce-based pseudorandom function is a function $F\colon \{0,1\}^k \times \{0,1\}^n \times \{0,1\}^* \to \{0,1\}^n$, that takes as input a key $K \in \{0,1\}^k$, a nonce $N \in \{0,1\}^n$, a message $M \in \{0,1\}^*$, and outputs a tag $T \in \{0,1\}^n$.

We define a perfectly random oracle $\mathsf{Rand}\colon \{0,1\}^n \times \{0,1\}^* \to \{0,1\}^n$ as a function that for each new input in $\{0,1\}^n \times \{0,1\}^*$ generates a random string of length n bits. The prf-security of a function F is measured by considering a distinguisher $\mathcal{D}$ that is given access to either F_K for secret key $K \xleftarrow{\$} \{0,1\}^k$, or the random oracle Rand:

$$\mathbf{Adv}_F^{\mathrm{prf}}(\mathcal{D}) = \left| \Pr\left[K \xleftarrow{\$} \{0,1\}^k \colon \mathcal{D}^{F_K} = 1\right] - \Pr\left[\mathcal{D}^{\mathsf{Rand}} = 1\right] \right| .$$

We call a query a faulty query if the distinguisher $\mathcal{D}$ has already queried its oracle with the same nonce. The distinguisher $\mathcal{D}$ is allowed to make at most μ faulty queries. We call $\mathcal{D}$ a nonce-respecting adversary if $\mu = 0$, and nonce-misusing if $\mu \geq 1$.

2.3 Universal Hash Functions

For $n \in \mathbb{N}$, an universal hash function is a function $H\colon \mathcal{K}_h \times \{0,1\}^* \to \{0,1\}^n$, such that for fixed key $K_h \in \mathcal{K}_h$, we have $H_{K_h}(\cdot) = H(K_h, \cdot)$. We call H an ϵ-almost XOR universal (ϵ-AXU) hash function [27] if for all distinct $M, M' \in \{0,1\}^*$ and all $C \in \{0,1\}^n$, we have

$$\Pr\left[K_h \xleftarrow{\$} \mathcal{K}_h \colon H_{K_h}(M) \oplus H_{K_h}(M') = C\right] \leq \epsilon .$$

Unfortunately, we cannot immediately use this probability bound to bound the occurrence of the following event:

$$H_{K_{h_1}}(M_i) = H_{K_{h_1}}(M_j) \wedge H_{K_{h_2}}(M_j) = H_{K_{h_2}}(M_k) \wedge H_{K_{h_1}}(M_k) = H_{K_{h_1}}(M_l) ,$$

for $K_{h_1}, K_{h_2} \xleftarrow{\$} \mathcal{K}_h$. We cannot claim that the probability of this event is ϵ^3 for any fixed distinct M_i, M_j, M_k, and M_l, since the first and the last event are not independent. We will use the following lemma in our security proofs.

Lemma 1 (alternating events lemma [12, 23]). *Let $q_i, q_j, q_k, q_l, q \in \mathbb{N}$ such that $q_i, q_j, q_k, q_l \leq q$. Let $X^q = (X_1, \ldots, X_q)$ be a q-tuple of random variables, and let $X^{q_i}, X^{q_j}, X^{q_k}, X^{q_l} \subseteq X^q$. For distinct $i \in [q_i], j \in [q_j]$, let $E_{i,j}$ be events associated with $X_i \in X^{q_i}$ and $X_j \in X^{q_j}$, possibly dependent, which all hold with probability at most ϵ. For distinct $i \in [q_i], j \in [q_j], k \in [q_k], l \in [q_l]$, let $F_{i,j,k,l}$ be events associated with $X_i \in X^{q_i}$, $X_j \in X^{q_j}$, $X_k \in X^{q_k}$, and $X_l \in X^{q_l}$ which all hold with probability at most ϵ'. Moreover, the collection of events $(F_{i,j,k,l})_{i,j,k,l}$ is independent with the collection of event $(E_{i,j})_{i,j}$. Then,*

$$\Pr[\exists i \in [q_i], j \in [q_j], k \in [q_k], l \in [q_l], E_{i,j} \wedge E_{k,l} \wedge F_{i,j,k,l}] \leq \sqrt{q_i q_j q_k q_l} \cdot \epsilon \cdot \sqrt{\epsilon'} .$$

Jha and Nandi [23] proved the alternating events lemma for $q_i, q_j, q_k, q_l = q$, the lemma can straightforwardly be generalized to different q_i, q_j, q_k, q_l, a similar proof for this is given in the bad transcripts analysis of the work by Choi et al. [12]. Note that Lemma 1 can be used to solve the above-mentioned example using the independent randomness of the hash keys K_{h_1} and K_{h_2}. For our constructions, we only have one hash key, hence we will use the randomly generated output tags as our second source of randomness.

2.4 Double Collision Attack

We will rely on the double collision attack by Nandi [35]. We recall the result of this attack in the following lemma.

Lemma 2 (double collision attack [35]). *For $k, n \in \mathbb{N}$, let $F1\colon \{0,1\}^k \times \{0,1\}^* \to \{0,1\}^n$ and $F2\colon \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ be non-injective functions. Consider $F3_{K_1,K_2} := F2_{K_2} \circ F1_{K_1}$. There is a non-negligible constant c such that for a distinguisher $\mathcal{D}$ making $(1/\sqrt{2}) \cdot 2^{n/2}$ queries, we have*

$$\mathbf{Adv}^{\mathrm{prf}}_{F3}(\mathcal{D}) \geq c\,.$$

3 Generalized Fixed-Input-Length PRF Construction

We present a synthetic categorization of all beyond birthday bound secure fixed-input-length PRFs from two block cipher calls and plain XOR operations.

Let $k, n \in \mathbb{N}$. Let $E\colon \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ be a block cipher. For a binary 3×3 matrix A of the form

$$A = \begin{pmatrix} a_{11} & 0 & 0 \\ a_{21} & a_{22} & 0 \\ a_{31} & a_{32} & a_{33} \end{pmatrix}, \tag{4}$$

our target PRF $F_A\colon \{0,1\}^{2k} \times \{0,1\}^n \to \{0,1\}^n$ defined by A is described in Algorithm 1 and given in Figure 2. Note that any fixed-input-length PRF $F\colon \{0,1\}^n \to \{0,1\}^n$ based on two block cipher calls can be represented by this generic construction, omitting all possible constructions that can be obtained by applying linear transformations to the variables. In total, we thus analyze 2^6 fixed-input-length PRFs. However for some A, the resulting PRF is clearly not secure beyond the birthday bound. In Section 3.1, we first eliminate trivially insecure matrices. Then, in Section 3.2 we reason about the remaining ones.

3.1 Trivial Matrices

We call a matrix "trivial" if it does not make proper use of one or both block cipher calls. More formally, matrix A is called "non-trivial" if it satisfies the following properties:

Algorithm 1 PRF F_A with A of (4)

```
Input: $(K_1, K_2) \in \{0,1\}^{2k}$, $N \in \{0,1\}^n$
Output: $T \in \{0,1\}^n$
$u \leftarrow a_{11} \cdot N$
$v \leftarrow E_{K_1}(u)$
$x \leftarrow a_{21} \cdot N \oplus a_{22} \cdot v$
$y \leftarrow E_{K_2}(x)$
$T \leftarrow a_{31} \cdot N \oplus a_{32} \cdot v \oplus a_{33} \cdot y$
return $T$
```

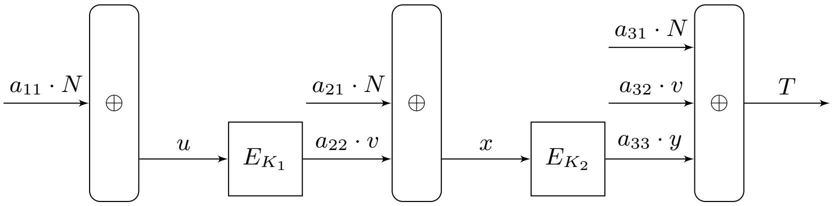


Fig. 2: PRF F_A based on two block ciphers E_{K_1} and E_{K_2}, and with A of (4).

(1) Each row of the matrix must contain at least one non-zero element. This requirement ensures that at least one input is XORed to each of the three XOR-operators. Note that the first two XOR-operations correspond respectively to the inputs of the two block ciphers. If no inputs are XORed to these XOR-operators, then the corresponding block cipher is independent of the inputs to the PRF. In this case, the resulting PRF can be broken in at most $2^{n/2}$ queries. The last XOR-operation corresponds to the output T, if no inputs are XORed to this XOR-operator, then the resulting PRF outputs a constant T for every query.

(2) Each column of the matrix must contain at least one non-zero element. This requirement ensures that each of the three inputs N, v, and y is used at least once.

We can derive the following four requirements from above properties:

$$a_{11} = 1\,, \qquad a_{33} = 1\,, \qquad a_{22} + a_{32} \geq 1\,, \qquad a_{21} + a_{22} \geq 1\,.$$

Notice that if $a_{11} = 0$, the block cipher E_{K_1} is not used in the computation; if $a_{33} = 0$, the block cipher E_{K_2} is not used in the output; if $a_{22} + a_{32} = 0$, the output of the block cipher E_{K_1} is not used in the output; and if $a_{21} + a_{22} = 0$, the block cipher E_{K_2} is not used in the computation. If one of the four requirements is not satisfied, then the resulting PRF can be broken in at most $2^{n/2}$ queries.

Thus, in the remainder, we focus on matrices A of the following form:

$$A = \begin{pmatrix} 1 & 0 & 0 \\ a_{21} & a_{22} & 0 \\ a_{31} & a_{32} & 1 \end{pmatrix}\,, \tag{5}$$

where $a_{21} + a_{22} \geq 1$ and $a_{22} + a_{32} \geq 1$ (ten schemes in total).

3.2 Generic Results for PRFs

Before we start with our generic analysis, we provide the following observation to simplify our analysis: XORing the input N to the output T does not influence the security of the PRF.

Proposition 1. *Let A be any non-trivial matrix of the form (5). Let*

$$A' := A \oplus \begin{pmatrix} 0\,0\,0 \\ 0\,0\,0 \\ 1\,0\,0 \end{pmatrix} .$$

For any distinguisher $\mathcal{D}$, there exists a distinguisher $\mathcal{D}'$ such that $\mathbf{Adv}^{\mathrm{prf}}_{F_A}(\mathcal{D}') \geq \mathbf{Adv}^{\mathrm{prf}}_{F_{A'}}(\mathcal{D})$ and $\mathbf{Adv}^{\mathrm{prf}}_{F_{A'}}(\mathcal{D}') \geq \mathbf{Adv}^{\mathrm{prf}}_{F_A}(\mathcal{D})$.

Proof. We only prove the part $\mathbf{Adv}^{\mathrm{prf}}_{F_{A'}}(\mathcal{D}') \geq \mathbf{Adv}^{\mathrm{prf}}_{F_A}(\mathcal{D})$, the part $\mathbf{Adv}^{\mathrm{prf}}_{F_A}(\mathcal{D}') \geq \mathbf{Adv}^{\mathrm{prf}}_{F_{A'}}(\mathcal{D})$ is proven in a similar way. Let $K_e = (K_1, K_2) \xleftarrow{\$} \{0,1\}^{2k}$, and note that $F_{A'}[E_{K_1}, E_{K_2}](N) = F_A[E_{K_1}, E_{K_2}](N) \oplus N$. For any distinguisher $\mathcal{D}$ whose goal is to distinguish the real world oracle $F_A[E_{K_1}, E_{K_2}]$ from the ideal world oracle $\varphi \xleftarrow{\$} \mathrm{Func}(n)$, we can build a distinguisher $\mathcal{D}'$ that has access to either $F_{A'}[E_{K_1}, E_{K_2}]$ or φ, and that simulates $\mathcal{D}$'s oracles. More precisely, for each query N made by $\mathcal{D}$, $\mathcal{D}'$ queries its oracle for N to retrieve a value T, and it returns $T \oplus N$ to $\mathcal{D}$. At the end, $\mathcal{D}'$ relays the decision bit output by $\mathcal{D}$. Distinguisher $\mathcal{D}'$ has at least the same success probability as $\mathcal{D}$, and this completes the proof. □

We are left with matrices A of the form

$$A = \begin{pmatrix} 1 & 0 & 0 \\ a_{21} & a_{22} & 0 \\ 0 & a_{32} & 1 \end{pmatrix} , \tag{6}$$

where $a_{21} + a_{22} \geq 1$ and $a_{22} + a_{32} \geq 1$. There are five options in total:

$$A_1 = \begin{pmatrix} 1\,0\,0 \\ 0\,1\,0 \\ 0\,0\,1 \end{pmatrix} , A_2 = \begin{pmatrix} 1\,0\,0 \\ 1\,1\,0 \\ 0\,0\,1 \end{pmatrix} , A_3 = \begin{pmatrix} 1\,0\,0 \\ 1\,0\,0 \\ 0\,1\,1 \end{pmatrix} , A_4 = \begin{pmatrix} 1\,0\,0 \\ 0\,1\,0 \\ 0\,1\,1 \end{pmatrix} , A_5 = \begin{pmatrix} 1\,0\,0 \\ 1\,1\,0 \\ 0\,1\,1 \end{pmatrix} . \tag{7}$$

Clearly, F_{A_1} is a cascade of two PRPs. This means that it does not have collisions and can be distinguished from a random function φ in around $2^{n/2}$ queries. Likewise, F_{A_5} is a composition of two PRFs. More specifically, F_{A_5} is equivalent to a cascade of two Davies-Meyer constructions (taking into account that $x = N \oplus v$ in the second Davies-Meyer construction), which is at most birthday bound secure due to Lemma 2. The remaining three functions for binary matrices A_2, A_3, A_4 are Encrypted Davies-Meyer [13], Sum of Permutation [4], and Encrypted Davies-Meyer Dual [30], respectively. All three constructions have been proven to achieve optimal n-bit security using Patarin's mirror theory [33,37,39,40], and the Sum of Permutation and the Encrypted Davies-Meyer Dual constructions have also been proven to achieve optimal n-bit security using the chi-squared method [14]. We thus arrive at the following results.

Proposition 2. *Let $k, n \in \mathbb{N}$. Let $E : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ be a block cipher. For $x = 1, 5$, consider F_{A_x} of Algorithm 1 that is defined by binary matrix A_x of (7).*

(i) There is a distinguisher $\mathcal{D}$ making $2^{n/2}$ queries such that

$$\mathbf{Adv}^{\mathrm{prf}}_{F_{A_1}}(\mathcal{D}) \geq 1 - \frac{1}{e}\,.$$

(ii) There is a non-negligible constant c such that for a distinguisher $\mathcal{D}$ making $(1/\sqrt{2}) \cdot 2^{n/2}$ queries, we have

$$\mathbf{Adv}^{\mathrm{prf}}_{F_{A_5}}(\mathcal{D}) \geq c\,.$$

Proof. For case (i), consider a distinguisher $\mathcal{D}$ that makes $2^{n/2}$ queries and operates as follows. For $i = 1, \ldots, 2^{n/2}$, it selects arbitrary $N^{(i)}$'s to obtain $T^{(i)}$'s. If all $T^{(i)}$'s are distinct, output 1. Otherwise, output 0. In the real world, F_{A_1} behaves as a PRP, and thus $\Pr\left[\mathcal{D}^{F_{A_1}} = 1\right] = 1$. For the ideal world, we have

$$\Pr\left[\mathcal{D}^{\varphi} = 1\right] = \Pr\left[\cap_{i,i'} T^{(i)} \neq T^{(i')}\right] \leq 1 - \left(1 - e^{-\binom{q}{2}\frac{1}{2^n}}\right) = e^{-\binom{q}{2}\frac{1}{2^n}}\,,$$

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

The proof of case (ii) follows from Lemma 2. □

Theorem 1. *Let $k, n \in \mathbb{N}$. Let $E : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ be a block cipher. For $x = 2, 3, 4$, consider F_{A_x} of Algorithm 1 that is defined by binary matrix A_x of (7).*

(i) Let ξ be any threshold, and for any distinguisher $\mathcal{D}$ making at most $q \leq 2^n/(67\xi^2)$ queries, we have

$$\mathbf{Adv}^{\mathrm{prf}}_{F_{A_2}}(\mathcal{D}) \leq \frac{q}{2^n} + \frac{\binom{q}{\xi+1}}{2^{n\xi}}\,.$$

(ii) For any distinguisher $\mathcal{D}$ making at most q queries, we have

$$\mathbf{Adv}^{\mathrm{prf}}_{F_{A_3}}(\mathcal{D}),\, \mathbf{Adv}^{\mathrm{prf}}_{F_{A_4}}(\mathcal{D}) \leq \frac{q}{2^n}\,.$$

Proof. We refer to Mennink and Neves [30] for the proofs of security of F_{A_2} and F_{A_4}, and to Dai et al. [14] for the proof of security of F_{A_3}. □

We conclude that EDM, SoP, and EDMD are the only three n-bit secure fixed-input-length PRFs that can be build using two block cipher calls and XOR operations (modulo the reduction of Proposition 1 that consists of feed-forwarding the input), and one should start from these fixed-input-length PRFs while building beyond birthday bound secure variable-input-length PRF algorithms.

Algorithm 2 Nonce-based PRF F_{A^*} with A^* of (8)

```
Input: $(K_1, K_2) \in \{0,1\}^{2k}$, $K_h \in \mathcal{K}_h$, $N \in \{0,1\}^n$, $M \in \{0,1\}^*$
Output: $T \in \{0,1\}^n$
$u \leftarrow a_{11} \cdot N \oplus b_1 \cdot H_{K_h}(M)$
$v \leftarrow E_{K_1}(u)$
$x \leftarrow a_{21} \cdot N \oplus a_{22} \cdot v \oplus b_2 \cdot H_{K_h}(M)$
$y \leftarrow E_{K_2}(x)$
$T \leftarrow a_{31} \cdot N \oplus a_{32} \cdot v \oplus a_{33} \cdot y \oplus b_3 \cdot H_{K_h}(M)$
return $T$
```

4 Generalized Nonce-Based PRF Construction

We consider how to generically construct a nonce-based PRF algorithm from two block cipher calls and one universal hash function call.

Let $k, n \in \mathbb{N}$. Let $E \colon \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ be a block cipher. For a binary 3×4 matrix A^* of the form

$$A^* = \begin{pmatrix} a_{11} & 0 & 0 & b_1 \\ a_{21} & a_{22} & 0 & b_2 \\ a_{31} & a_{32} & a_{33} & b_3 \end{pmatrix} , \tag{8}$$

our target nonce-based PRF $F_{A^*} \colon \{0,1\}^{2k} \times \mathcal{K}_h \times \{0,1\}^n \times \{0,1\}^* \to \{0,1\}^n$ defined by A^* is described in Algorithm 2 and given in Figure 3. Note that any nonce-based PRF $F \colon \{0,1\}^n \times \{0,1\}^* \to \{0,1\}^n$ based on two block cipher calls and one universal hash function call can be represented by this generic construction, omitting all possible constructions that can be obtained by applying linear transformations to the variables. In total, we thus analyze 2^9 nonce-based PRFs. However for some A^*, the resulting construction is clearly not secure beyond the birthday bound. In Section 4.1, we first eliminate trivially insecure matrices. Then, we reason about the remaining ones.

4.1 Generic Results for Nonce-Based PRF Algorithms

Note that the reasoning of Section 3.1 also applies here: the distinguisher can eliminate the effect of the universal hash function by keeping the message M constant. Therefore, intuitively, a nonce-based PRF can only be secure if its underlying fixed-input-length PRF is built on a non-trivial matrix. We therefore focus on nonce-based PRF algorithm built on fixed-input-length PRFs from equation (6).

Thus, in the remainder, we focus on matrices A^* of the following form:

$$A^* = \begin{pmatrix} 1 & 0 & 0 & b_1 \\ a_{21} & a_{22} & 0 & b_2 \\ 0 & a_{32} & 1 & b_3 \end{pmatrix} , \tag{9}$$

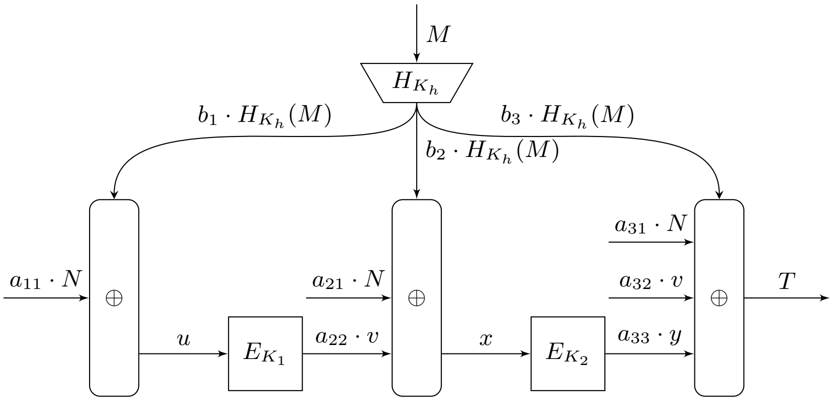


Fig. 3: Nonce-based PRF F_{A^*} based on two block ciphers E_{K_1}, E_{K_2}, and an universal hash function H_{K_h}, and with A^* of (8).

where $a_{21} + a_{22} \geq 1$, $a_{22} + a_{32} \geq 1$ and $b_1 + b_2 + b_3 \geq 1$. These options are:

$$\begin{aligned} A_1^* &= \begin{pmatrix} 1 & 0 & 0 & b_1 \\ 0 & 1 & 0 & b_2 \\ 0 & 0 & 1 & b_3 \end{pmatrix}, A_2^* = \begin{pmatrix} 1 & 0 & 0 & b_1 \\ 1 & 1 & 0 & b_2 \\ 0 & 0 & 1 & b_3 \end{pmatrix}, A_3^* = \begin{pmatrix} 1 & 0 & 0 & b_1 \\ 1 & 0 & 0 & b_2 \\ 0 & 1 & 1 & b_3 \end{pmatrix}, \\ A_4^* &= \begin{pmatrix} 1 & 0 & 0 & b_1 \\ 0 & 1 & 0 & b_2 \\ 0 & 1 & 1 & b_3 \end{pmatrix}, A_5^* = \begin{pmatrix} 1 & 0 & 0 & b_1 \\ 1 & 1 & 0 & b_2 \\ 0 & 1 & 1 & b_3 \end{pmatrix}. \end{aligned} \tag{10}$$

As in Section 3.2, nonce-based PRFs based on A_1^* cannot achieve beyond birthday bound security, as the distinguisher can make $2^{n/2}$ queries by keeping the message M constant and observe no collision in the tag. nonce-based PRFs based on A_5^* also cannot achieve beyond birthday bound security, as these constructions can be seen as a cascade of two PRFs, and hence can be broken in the birthday bound using Lemma 2.

In the following, we denote $F_{B_x}^{\text{EDM}}$, $F_{B_x}^{\text{SoP}}$, and $F_{B_x}^{\text{EDMD}}$ as the nonce-based PRFs based on matrices A_2^*, A_3^*, and A_4^*, respectively. For $x = 0, \ldots, 7$, we will consider all variants of B_x depending on the values of b_1, b_2, and b_3.

$$\begin{aligned} B_0 &= \begin{pmatrix} 0 & 0 & 0 \end{pmatrix}, & B_4 &= \begin{pmatrix} 1 & 0 & 0 \end{pmatrix}, \\ B_1 &= \begin{pmatrix} 0 & 0 & 1 \end{pmatrix}, & B_5 &= \begin{pmatrix} 1 & 0 & 1 \end{pmatrix}, \\ B_2 &= \begin{pmatrix} 0 & 1 & 0 \end{pmatrix}, & B_6 &= \begin{pmatrix} 1 & 1 & 0 \end{pmatrix}, \\ B_3 &= \begin{pmatrix} 0 & 1 & 1 \end{pmatrix}, & B_7 &= \begin{pmatrix} 1 & 1 & 1 \end{pmatrix}. \end{aligned} \tag{11}$$

4.2 Nonce-Based PRFs Based on A_2^* (Encrypted Davies-Meyer)

In this section, we consider nonce-based PRFs based on the Encrypted Davies-Meyer construction F^{EDM}. Let $k, n \in \mathbb{N}$, let $E\colon \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$

be a block cipher, and $H\colon \mathcal{K}_h \times \{0,1\}^* \to \{0,1\}^n$ be an ϵ-AXU hash function. Consider generic construction $F^{\mathrm{EDM}}_{B_x}\colon \{0,1\}^{2k} \times \mathcal{K}_h \times \{0,1\}^n \times \{0,1\}^* \to \{0,1\}^n$:

$$\begin{aligned} &F^{\mathrm{EDM}}_{B_x}[E_{K_1}, E_{K_2}, H_{K_h}](N, M) = \\ &\qquad E_{K_2}(E_{K_1}(N \oplus b_1 \cdot H_{K_h}(M)) \oplus N \oplus b_2 \cdot H_{K_h}(M)) \oplus b_3 \cdot H_{K_h}(M)\,, \end{aligned} \tag{12}$$

with $B_x \in \{B_0, B_1, \ldots, B_7\}$ of (11).

Here, $F^{\mathrm{EDM}}_{B_2}$ is the EWCDM construction of Cogliati and Seurin [13], which is shown to achieve $2n/3$-bit security against nonce-respecting adversaries. Using Patarin's mirror theory, Mennink and Neves [30] have shown that $F^{\mathrm{EDM}}_{B_2}$ also achieves n-bit security against nonce-respecting adversaries. The function $F^{\mathrm{EDM}}_{B_0}$ is trivially insecure and henceforth excluded. The function $F^{\mathrm{EDM}}_{B_1}$ is a Wegman-Carter construction with EDM as its underlying PRF, hence it is optimally n-bit secure against nonce-respecting adversaries, and totally broken when the nonce is reused. For the remaining six schemes, we show that four of these achieve beyond birthday bound security against nonce-respecting distinguisher. Moreover, two of these four constructions still provide the same amount of security in the faulty nonce model when the number of faulty nonces is below $2^{n/2}$, and the security drops to the birthday bound when $2^{n/2}$ faulty nonces are made. The security of the other two constructions drops to birthday bound once a single nonce is repeated.

Proposition 3. *Let $k, n \in \mathbb{N}$. Let $E : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ be a block cipher, and $H\colon \mathcal{K}_h \times \{0,1\}^* \to \{0,1\}^n$ be an ϵ-AXU hash function. Consider $F^{\mathrm{EDM}}_{B_x}$ of equation (12) for binary matrix $B_x \in \{B_6, B_7\}$ of (11). There is a nonce-respecting distinguisher $\mathcal{D}$ making $4 \cdot 2^{n/2}$ queries such that*

$$\mathbf{Adv}^{\mathrm{prf}}_{F^{\mathrm{EDM}}_{B_x}}(\mathcal{D}) \geq 1 - \frac{1}{2^n}\,.$$

Proof. The proof is given in the full version of the paper. □

Proposition 4. *Let $k, n \in \mathbb{N}$. Let $E : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ be a block cipher, and $H\colon \mathcal{K}_h \times \{0,1\}^* \to \{0,1\}^n$ be an ϵ-AXU hash function. Consider $F^{\mathrm{EDM}}_{B_x}$ of equation (12) for binary matrix $B_x \in \{B_2, B_3\}$ of (11). There is a distinguisher $\mathcal{D}$ making $2^{n/2} + 2$ queries with 2 faulty nonces such that*

$$\mathbf{Adv}^{\mathrm{prf}}_{F^{\mathrm{EDM}}_{B_x}}(\mathcal{D}) \geq 1 - \frac{1}{\sqrt{e}} - \frac{1}{2^n}\,.$$

Proof. The proof is given in the full version of the paper. □

Proposition 5. *Let $k, n \in \mathbb{N}$. Let $E : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ be a block cipher, and $H\colon \mathcal{K}_h \times \{0,1\}^* \to \{0,1\}^n$ be an ϵ-AXU hash function. Consider $F^{\mathrm{EDM}}_{B_x}$ of equation (12) for binary matrix $B_x \in \{B_4, B_5\}$ of (11). There is a distinguisher $\mathcal{D}$ making $2 \cdot 2^{n/2} + 4$ queries with $2^{n/2}$ faulty nonces such that*

$$\mathbf{Adv}^{\mathrm{prf}}_{F^{\mathrm{EDM}}_{B_x}}(\mathcal{D}) \geq 1 - \frac{1}{\sqrt{e}} - \frac{1}{2^n}\,.$$

Proof. The proof is given in the full version of the paper. □

Theorem 2. *Let $k, n \in \mathbb{N}$. Let $E : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ be a block cipher, and $H \colon \mathcal{K}_h \times \{0,1\}^* \to \{0,1\}^n$ be an ϵ-AXU hash function. Consider $F^{\mathrm{EDM}}_{B_x}$ of equation (12) for binary matrix $B_x \in \{B_2, B_3\}$ of (11). For any nonce-respecting distinguisher $\mathcal{D}$ making at most $q \le 2^{3n/4}$ queries, there exist distinguishers $\mathcal{D}'_1$ and $\mathcal{D}'_2$ with the same query complexity such that*

$$\begin{aligned}\mathbf{Adv}^{\mathrm{prf}}_{F^{\mathrm{EDM}}_{B_2}}(\mathcal{D}) \le \mathbf{Adv}^{\mathrm{prp}}_{E}(\mathcal{D}'_1) + \mathbf{Adv}^{\mathrm{prp}}_{E}(\mathcal{D}'_2) + \frac{q^2\epsilon}{2^n}\\ + \frac{19q^{\frac{4}{3}}}{2^n} + \frac{6q^{\frac{8}{3}}}{2^{2n}} + \frac{18q^{\frac{7}{3}}}{2^{2n}} + \frac{q^2}{2^{2n}} + \frac{8q^4}{3 \cdot 2^{3n}}\,,\\ \mathbf{Adv}^{\mathrm{prf}}_{F^{\mathrm{EDM}}_{B_3}}(\mathcal{D}) \le \mathbf{Adv}^{\mathrm{prp}}_{E}(\mathcal{D}'_1) + \mathbf{Adv}^{\mathrm{prp}}_{E}(\mathcal{D}'_2) + \frac{q^2\epsilon}{2^n} + q^{\frac{4}{3}}\epsilon\\ + \frac{18q^{\frac{4}{3}}}{2^n} + \frac{6q^{\frac{8}{3}}}{2^{2n}} + \frac{18q^{\frac{7}{3}}}{2^{2n}} + \frac{q^2}{2^{2n}} + \frac{8q^4}{3 \cdot 2^{3n}}\,.\end{aligned}$$

Proof. The proof is given in Section 5.3. □

Theorem 3. *Let $k, n \in \mathbb{N}$. Let $E : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ be a block cipher, and $H \colon \mathcal{K}_h \times \{0,1\}^* \to \{0,1\}^n$ be an ϵ-AXU hash function. Consider $F^{\mathrm{EDM}}_{B_x}$ of equation (12) for binary matrix $B_x \in \{B_4, B_5\}$ of (11). Let μ be a fixed parameter. For any distinguisher $\mathcal{D}$ making at most $q \le 2^{3n/4}$ queries, and at most μ faulty nonces, there exist distinguishers $\mathcal{D}'_1$ and $\mathcal{D}'_2$ with the same query complexity such that*

$$\begin{aligned}\mathbf{Adv}^{\mathrm{prf}}_{F^{\mathrm{EDM}}_{B_4}}(\mathcal{D}) \le \mathbf{Adv}^{\mathrm{prp}}_{E}(\mathcal{D}'_1) + \mathbf{Adv}^{\mathrm{prp}}_{E}(\mathcal{D}'_2) + \frac{\mu^2}{2^n} + \mu^2\epsilon + \frac{q^2\epsilon}{2^n} + \frac{q^2\epsilon}{2^{n/2}} + \frac{q^2\sqrt{\epsilon}}{2^n}\\ + q^{\frac{4}{3}}\epsilon + \frac{19q^{\frac{4}{3}}}{2^n} + \frac{6q^{\frac{8}{3}}}{2^{2n}} + \frac{18q^{\frac{7}{3}}}{2^{2n}} + \frac{q^2}{2^{2n}} + \frac{8q^4}{3 \cdot 2^{3n}}\,,\\ \mathbf{Adv}^{\mathrm{prf}}_{F^{\mathrm{EDM}}_{B_5}}(\mathcal{D}) \le \mathbf{Adv}^{\mathrm{prp}}_{E}(\mathcal{D}'_1) + \mathbf{Adv}^{\mathrm{prp}}_{E}(\mathcal{D}'_2) + 2\mu^2\epsilon + \frac{q^2\epsilon}{2^n} + \frac{q^2\epsilon}{2^{n/2}} + \frac{q^2\sqrt{\epsilon}}{2^n} + 2q^{\frac{4}{3}}\epsilon\\ + \frac{18q^{\frac{4}{3}}}{2^n} + \frac{6q^{\frac{8}{3}}}{2^{2n}} + \frac{18q^{\frac{7}{3}}}{2^{2n}} + \frac{q^2}{2^{2n}} + \frac{8q^4}{3 \cdot 2^{3n}}\,.\end{aligned}$$

Proof. The proof is given in Section 5.3. □

For Theorem 3, when μ is sufficiently smaller than $2^{n/2}$, $F^{\mathrm{EDM}}_{B_4}$ and $F^{\mathrm{EDM}}_{B_5}$ achieve $3n/4$-bit security. Note that this optimal bound holds under the assumption that ϵ is sufficiently small ($\epsilon \approx 2^{-n}$) and the block cipher E is sufficiently PRP secure, such that the other terms in the bound are dominating.

4.3 Nonce-Based PRFs Based on A_3^* (Sum of Permutations)

In this section, we consider nonce-based PRFs based on the Sum of Permutations construction F^{SoP}. Let $k, n \in \mathbb{N}$, let $E \colon \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ be a block cipher, and $H\colon \mathcal{K}_h \times \{0,1\}^* \to \{0,1\}^n$ be an ϵ-AXU hash function. Consider generic construction $F^{\mathrm{SoP}}_{B_x}\colon \{0,1\}^{2k} \times \mathcal{K}_h \times \{0,1\}^n \times \{0,1\}^* \to \{0,1\}^n$:

$$\begin{aligned} &F^{\mathrm{SoP}}_{B_x}[E_{K_1}, E_{K_2}, H_{K_h}](N, M) = \\ &\qquad E_{K_1}(N \oplus b_1 \cdot H_{K_h}(M)) \oplus E_{K_2}(N \oplus b_2 \cdot H_{K_h}(M)) \oplus b_3 \cdot H_{K_h}(M)\,, \end{aligned} \tag{13}$$

with $B_x \in \{B_0, B_1, \ldots, B_7\}$ of (11).

The function $F^{\mathrm{SoP}}_{B_4}$ is symmetric to $F^{\mathrm{SoP}}_{B_2}$, and $F^{\mathrm{SoP}}_{B_5}$ is symmetric to $F^{\mathrm{SoP}}_{B_3}$, and hence $F^{\mathrm{SoP}}_{B_4}$ and $F^{\mathrm{SoP}}_{B_5}$ can be omitted. The function $F^{\mathrm{SoP}}_{B_2}$ is the two keyed variant of the nEHtM construction of Dutta et al. [18]. Dutta et al. have shown that nEHtM based on a single key with domain separation achieves $2n/3$-bit security when $2^{n/3}$ faulty nonces are made, and its security degrades in a graceful manner when the number of faulty nonces go beyond $2^{n/3}$. Later, Choi et al. [12] have shown that single keyed nEHtM actually achieves $3n/4$-bit security when up to $2^{3n/8}$ faulty nonces are made, and its security also degrades in a graceful manner. Here, $F^{\mathrm{SoP}}_{B_2}$ is the nEHtM constructiuon based on two keys without domain separation. The function $F^{\mathrm{SoP}}_{B_0}$ is trivially insecure and henceforth excluded. The function $F^{\mathrm{SoP}}_{B_1}$ is a Wegman-Carter construction with SoP as its underlying PRF, hence it is optimally n-bit secure against nonce-respecting adversaries, and totally broken when the nonce is reused. For the remaining four schemes, we show that two of these schemes achieve beyond birthday bound security, even in the case of nonce reuse.

Proposition 6. *Let $k, n \in \mathbb{N}$. Let $E : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ be a block cipher, and $H\colon \mathcal{K}_h \times \{0,1\}^* \to \{0,1\}^n$ be an ϵ-AXU hash function. Consider $F^{\mathrm{SoP}}_{B_x}$ of equation (13) for binary matrix $B_x \in \{B_6, B_7\}$ of (11). There is a nonce-respecting distinguisher $\mathcal{D}$ that making $4 \cdot 2^{n/2}$ queries such that*

$$\mathbf{Adv}^{\mathrm{prf}}_{F^{\mathrm{SoP}}_{B_x}}(\mathcal{D}) \geq 1 - \frac{1}{2^n}\,.$$

Proof. The proof is given in the full version of the paper. □

Theorem 4. *Let $k, n \in \mathbb{N}$. Let $E : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ be a block cipher, and $H\colon \mathcal{K}_h \times \{0,1\}^* \to \{0,1\}^n$ be an ϵ-AXU hash function. Consider $F^{\mathrm{SoP}}_{B_x}$ of equation (13) for binary matrix $B_x \in \{B_2, B_3\}$ of (11). Let $\mu \leq q^{1/3}$. For any distinguisher $\mathcal{D}$ making at most $q \leq 2^{3n/4}$ queries, and at most μ faulty nonces, there exist distinguishers $\mathcal{D}'_1$ and $\mathcal{D}'_2$ with the same query complexity such that*

$$\begin{aligned} \mathbf{Adv}^{\mathrm{prf}}_{F^{\mathrm{SoP}}_{B_2}}(\mathcal{D}) \leq{}& \mathbf{Adv}^{\mathrm{prp}}_{E}(\mathcal{D}'_1) + \mathbf{Adv}^{\mathrm{prp}}_{E}(\mathcal{D}'_2) + \frac{\mu^2}{2^n} + \mu^2\epsilon + \frac{q^2\epsilon}{2^n} + 4\mu^2\epsilon + \frac{3\mu q^{3n/2}\epsilon}{2^{n/2}} \\ &+ q^{\frac{4}{3}}\epsilon + \frac{18q^{\frac{4}{3}}}{2^n} + \frac{6q^{\frac{8}{3}}}{2^{2n}} + \frac{18q^{\frac{7}{3}}}{2^{2n}} + \frac{q^2}{2^{2n}} + \frac{8q^4}{3 \cdot 2^{3n}}\,, \\ \mathbf{Adv}^{\mathrm{prf}}_{F^{\mathrm{SoP}}_{B_3}}(\mathcal{D}) \leq{}& \mathbf{Adv}^{\mathrm{prp}}_{E}(\mathcal{D}'_1) + \mathbf{Adv}^{\mathrm{prp}}_{E}(\mathcal{D}'_2) + 2\mu^2\epsilon + \frac{q^2\epsilon}{2^n} + 4\mu^2\epsilon + \frac{3\mu q^{3n/2}\epsilon}{2^{n/2}} + q^{\frac{4}{3}}\epsilon \\ &+ \frac{18q^{\frac{4}{3}}}{2^n} + \frac{6q^{\frac{8}{3}}}{2^{2n}} + \frac{18q^{\frac{7}{3}}}{2^{2n}} + \frac{q^2}{2^{2n}} + \frac{8q^4}{3 \cdot 2^{3n}}\,. \end{aligned}$$

Proof. The proof is given in Section 5.3. □

In that case $F^{\mathrm{SoP}}_{B_2}$ and $F^{\mathrm{SoP}}_{B_3}$ achieve $3n/4$-bit security with $\mu \leq 2^{n/4}$. Although both nEHtM based on a single key and based on two independent keys achieve $3n/4$-bit security, the number of faulty nonces μ that can be made for our nEHtM based on two keys is $2^{n/4}$ when $q = 2^{3n/4}$, which is less than $2^{3n/8}$ for the case of single keyed nEHtM. This follows from the comparison with the results in [12], which is due to the version of mirror theory we are using here, since the versions of mirror theory used by Dutta et al. [18] and Choi et al. [12] are for single permutation, and cannot be applied for our nEHtM based on two keys. Our result can be improved by improving the mirror theory for two permutations. These optimal bounds again hold under the assumption that ϵ is sufficiently small ($\epsilon \approx 2^{-n}$) and the block cipher E is sufficiently PRP secure, such that the other terms in the bound are dominating.

4.4 Nonce-Based PRFs Based on A^*_4 (Encrypted Davies-Meyer Dual)

In this section, we consider nonce-based PRFs based on the Encrypted Davies-Meyer Dual construction F^{EDMD}. Let $k, n \in \mathbb{N}$, let $E\colon \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ be a block cipher, and $H\colon \mathcal{K}_h \times \{0,1\}^* \to \{0,1\}^n$ be an ϵ-AXU hash function. Consider generic construction $F^{\mathrm{EDMD}}_{B_x}\colon \{0,1\}^{2k} \times \mathcal{K}_h \times \{0,1\}^n \times \{0,1\}^* \to \{0,1\}^n$:

$$F^{\mathrm{EDMD}}_{B_x}[E_{K_1}, E_{K_2}, H_{K_h}](N, M) =$$

$$E_{K_2}(E_{K_1}(N \oplus b_1 \cdot H_{K_h}(M)) \oplus b_2 \cdot H_{K_h}(M)) \oplus E_{K_1}(N \oplus b_1 \cdot H_{K_h}(M)) \oplus b_3 \cdot H_{K_h}(M)\,, \tag{14}$$

with $B_x \in \{B_0, B_1, \ldots, B_7\}$ of (11).

Again, the function $F^{\mathrm{EDMD}}_{B_0}$ is trivially insecure and henceforth excluded. The function $F^{\mathrm{EDMD}}_{B_1}$ is a Wegman-Carter construction with EDMD as its underlying PRF, hence it is optimally n-bit secure against nonce-respecting adversaries, and totally broken when the nonce is reused. For the remaining six schemes, we provide birthday bound attacks for five out these six schemes.

Proposition 7. *Let $k, n \in \mathbb{N}$. Let $E : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ be a block cipher, and $H\colon \mathcal{K}_h \times \{0,1\}^* \to \{0,1\}^n$ be an ϵ-AXU hash function. Consider $F^{\mathrm{EDMD}}_{B_x}$ of equation (14) for binary matrix $B_x \in \{B_3, B_4, B_5, B_6, B_7\}$ of (11). There is a non-negligible constant c such that for a distinguisher $\mathcal{D}$ making $(1/\sqrt{2}) \cdot 2^{n/2}$ queries, we have*

$$\mathbf{Adv}^{\mathrm{prf}}_{F^{\mathrm{EDMD}}_{B_x}}(\mathcal{D}) \geq c\,.$$

Proof. These constructions can be seen as the composition of two random functions. The proposition follows straightforwardly from Lemma 2. □

We conclude that only $F^{\mathrm{EDMD}}_{B_2}$ may achieve beyond birthday bound security. However, for all four constructions, the output of their second permutation E_{K_2} is XORed with its input, this makes it a non-trivial exercise to derive security beyond the birthday bound for these constructions.

5 Security Analysis

Our analysis is performed using the H-coefficients technique, recapped in Section 5.1, and Patarin's mirror theory, recapped in Section 5.2. The proof of Theorem 2 and 3 on EDM-based algorithms, and the proof of Theorem 4 on SoP-based algorithms, are given in Section 5.3.

5.1 H-coefficients Technique

We will use Patarin's H-coefficient technique [11,36,38] for our security proofs.

Consider two oracles $\mathcal{O}$ and $\mathcal{P}$, and a deterministic distinguisher $\mathcal{D}$ that has query access to either of these oracles. 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 define a transcript τ which summarizes all query-response tuples learned by $\mathcal{D}$ during its interaction with its oracle $\mathcal{O}$ or $\mathcal{P}$. We denote by $X_{\mathcal{O}}$ and $X_{\mathcal{P}}$ the probability distribution of transcripts when interacting with $\mathcal{O}$ and $\mathcal{P}$, respectively. 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 3 (H-coefficients technique [22]). *Consider a deterministic distinguisher $\mathcal{D}$. Define a partition $\mathcal{T} = \mathcal{T}_{\text{good}} \sqcup \mathcal{T}_{\text{bad}}$, 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. Assume that there exists ε_1 such that for all attainable $\tau \in \mathcal{T}_{\text{good}}$:*

$$\frac{\Pr[X_{\mathcal{O}} = \tau]}{\Pr[X_{\mathcal{P}} = \tau]} \geq 1 - \varepsilon_1 \,,$$

and that there exists ε_2 such that $\Pr[X_{\mathcal{P}} \in \mathcal{T}_{\text{bad}}] \leq \varepsilon_2$. Then, we have

$$\mathbf{Adv}(\mathcal{D}) \leq \varepsilon_1 + \varepsilon_2 \,.$$

5.2 Mirror Theory

Patarin's mirror theory [33,37,39,40] was popularized by Mennink and Neves [30] and used to prove the optimal n-bit security of EDM and EWCDM. However, in Patarin's original work, the proof is highly complex and too difficult to verify, and it contains several gaps. In recent years, many different versions of mirror theory were presented [12,15,18,23,26]. We follow the description of the mirror theory by Kim et al. [26].

Let $G = (\mathcal{V}, \mathcal{S})$ be a graph and let $\overline{PQ} \in \mathcal{S}$ be an edge for $P, Q \in \mathcal{V}$. If this edge is labeled with $\lambda \in \{0,1\}^n$, then it means an equation $P \oplus Q = \lambda$, while if it is labeled with the symbol $\neq$, then it means that P and Q are distinct (since P and Q are from two independent sets). We write $P \overset{\star}{-} Q$ when an edge $\overline{PQ}$ is labeled with $\star \in \{0,1\}^n \cup \{\neq\}$.

Let $G^{=}$ denote the graph obtained by deleting all $\neq$-labeled edges from G. For $\ell > 0$ and a trail

$$\mathcal{L} : P_0 \overset{\lambda_1}{-} P_1 \overset{\lambda_2}{-} \ldots \overset{\lambda_\ell}{-} P_\ell$$

in $G^{=}$, its label is defined as

$$\lambda(\mathcal{L}) = \lambda_1 \oplus \lambda_2 \oplus \ldots \oplus \lambda_\ell \,.$$

We decompose $G^{=}$ into its connected components:

$$G^{=} = \mathcal{C}_1 \sqcup \mathcal{C}_2 \sqcup \cdots \sqcup \mathcal{C}_\alpha \sqcup \mathcal{D}_1 \sqcup \mathcal{D}_2 \sqcup \cdots \sqcup \mathcal{D}_\beta$$

for some $\alpha, \beta \geq 0$, where $\mathcal{C}_i$ denotes a component of size greater than 2, and $\mathcal{D}_i$ denotes a component of size 2. We will also write $\mathcal{C} = \mathcal{C}_1 \sqcup \mathcal{C}_2 \sqcup \cdots \sqcup \mathcal{C}_\alpha$ and $\mathcal{D} = \mathcal{D}_1 \sqcup \mathcal{D}_2 \sqcup \cdots \sqcup \mathcal{D}_\beta$. We call the graph G a *nice graph* if G satisfies the following two restrictions.

Definition 1 (acyclic). *$G^{=}$ contains no cycle.*

Definition 2 (non-zero path label (NPL)). *$\lambda(\mathcal{L}) \neq 0$ for any trail $\mathcal{L}$ of even length ℓ in $G^{=}$.*

Acyclic means that there is no linear combination of the equations that is independent of the unknowns, and NPL means that there is no linear combination of the equations that implies equality of two distinct unknowns. Given a nice graph $G = (\mathcal{V}, \mathcal{S})$, where the vertex set $\mathcal{V}$ is partitioned into two disjoint parts $\mathcal{P}$ and $\mathcal{Q}$, a solution to G should satisfy all the λ-labeled equations in $G^{=}$, while all the variables in $\mathcal{P}$ (resp., $\mathcal{Q}$) should take different values.

Lemma 4 (mirror theorem [26]). *Let G be a nice graph, and let q and q_c denote the number of edges of $G^{=}$ and $\mathcal{C}$, respectively. If $q < \frac{2^n}{8}$, then the number of solutions to G, denoted $h(G)$, satisfies*

$$\frac{h(G)2^{nq}}{(2^n)_{|\mathcal{P}|}(2^n)_{|\mathcal{Q}|}} \geq 1 - \frac{9q_c^2}{8 \cdot 2^n} - \frac{3q_c q^2}{2 \cdot 2^{2n}} - \frac{q^2}{2^{2n}} - \frac{9q_c^2 q}{8 \cdot 2^{2n}} - \frac{8q^4}{3 \cdot 2^{3n}} .$$

5.3 Proof of Theorem 2, 3, and 4

Recall that we consider the constructions $F^{\text{EDM}}_{B_2}, F^{\text{EDM}}_{B_3}$ in Theorem 2 for any nonce-respecting distinguisher, the constructions $F^{\text{EDM}}_{B_4}, F^{\text{EDM}}_{B_5}$ in Theorem 3 for any distinguisher making at most μ faulty nonces, and $F^{\text{SoP}}_{B_2}, F^{\text{SoP}}_{B_3}$ in Theorem 4 for any distinguisher making at most μ faulty nonces. The first part of the analyses of the three theorems is very similar. Only in Section 5.3.5 we consider the three theorems (and thus six schemes) independently.

Let $K_e = (K_1, K_2) \xleftarrow{\$} \{0,1\}^{2k}$, and $K_h \xleftarrow{\$} \mathcal{K}_h$. For $\mathcal{F} \in \{\text{EDM}, \text{SoP}\}$, consider any distinguisher $\mathcal{D}$ that has access to either the real world oracle $F^{\mathcal{F}}_{B_x}[E_{K_1}, E_{K_2}, H_{K_h}]$, with $x = 2, \ldots, 5$ (resp., $x = 2, 3$) if $\mathcal{F} = \text{EDM}$ (resp.,

$\mathcal{F} = \mathrm{SoP}$), or the ideal world oracle Rand. We first consider the case $\mathcal{F} = \mathrm{EDM}$. Instead of replacing the block ciphers E_{K_1}, E_{K_2} by π_1, π_2, we replace them by π_1, π_2^{-1}. As π_1, π_2 are drawn independently, these two constructions are provably equally secure. However it is more convenient to reason about the latter one, as an evaluation of the latter case can be viewed as the XOR of two permutations in the middle of the function. Let $\pi_1, \pi_2^{-1} \xleftarrow{\$} \mathrm{Perm}(n)$. We have

$$\begin{aligned}
&\mathbf{Adv}^{\mathrm{prf}}_{F^{\mathrm{EDM}}_{B_x}}(\mathcal{D}) \\
&\le \varDelta_{\mathcal{D}}\Big(F^{\mathrm{EDM}}_{B_x}[E_{K_1}, E_{K_2}, H_{K_h}] \ ; \ \mathsf{Rand}\Big) \\
&\le \varDelta_{\mathcal{D}}\Big(F^{\mathrm{EDM}}_{B_x}[\pi_1, \pi_2^{-1}, H_{K_h}] \ ; \ \mathsf{Rand}\Big) + \varDelta_{\mathcal{D}'_1}\Big(E_{K_1} \ ; \ \pi_1\Big) + \varDelta_{\mathcal{D}'_2}\Big(E_{K_2} \ ; \ \pi_2^{-1}\Big) \\
&= \varDelta_{\mathcal{D}}\Big(F^{\mathrm{EDM}}_{B_x}[\pi_1, \pi_2^{-1}, H_{K_h}] \ ; \ \mathsf{Rand}\Big) + \mathbf{Adv}^{\mathrm{prp}}_{E}(\mathcal{D}'_1) + \mathbf{Adv}^{\mathrm{prp}}_{E}(\mathcal{D}'_2) \,, \qquad (15)
\end{aligned}$$

for some distinguishers $\mathcal{D}'_1$ and $\mathcal{D}'_2$ with the same complexity as $\mathcal{D}$. We focus on the remaining distance in (15). As of now, we drop $[\pi_1, \pi_2^{-1}, H_{K_h}]$ for readability, and assume $\mathcal{D}$ is computationally unbounded and deterministic. The case of $\mathcal{F} = \mathrm{SoP}$ is similar, but we replace the block ciphers E_{K_1}, E_{K_2} by π_1, π_2.

5.3.1 Transcripts.

$\mathcal{D}$ makes q queries to $\mathcal{O} \in \{F^{\mathcal{F}}_{B_x}, \mathsf{Rand}\}$, and these are summarized in a transcript

$$\tau_m = \{(N^{(1)}, M^{(1)}, T^{(1)}), \ldots, (N^{(q)}, M^{(q)}, T^{(q)})\} \,.$$

After $\mathcal{D}$'s interaction with the oracles, but before it outputs its decision, we disclose the hash key K_h to the distinguisher. In the real world, this is the key used in the hash function. In the ideal world, K_h is a dummy key that is drawn uniformly at random. The complete view is denoted $\tau = (\tau_m, K_h)$.

5.3.2 Attainable Index Mappings.

In the real world, each query $(N^{(i)}, M^{(i)}, T^{(i)}) \in \tau$ corresponds to an evaluation of the oracle $F^{\mathcal{F}}_{B_x}$. Note that each scheme consists of an evaluation of π_1 and an evaluation of π_2, these are of the form $X^{(i)} \mapsto \pi_1(X^{(i)})$ and $Y^{(i)} \mapsto \pi_2(Y^{(i)})$ such that $\pi_1(X^{(i)}) \oplus \pi_2(Y^{(i)}) = Z^{(i)}$. The values of $X^{(i)}, Y^{(i)}, Z^{(i)}$ are specific for the particular construction under analysis (recall that currently we consider six different constructions $F^{\mathrm{EDM}}_{B_2}, F^{\mathrm{EDM}}_{B_3}, F^{\mathrm{EDM}}_{B_4}, F^{\mathrm{EDM}}_{B_5}$ and $F^{\mathrm{SoP}}_{B_2}, F^{\mathrm{SoP}}_{B_3}$ at once), and can be deduced from τ. This will also become clear in Section 5.3.5, where the separate schemes are treated individually. The transcript τ defines q equations on the unknowns, and these q equations are the following:

$$\mathcal{E} = \begin{cases} \pi_1(X^{(1)}) \oplus \pi_2(Y^{(1)}) = Z^{(1)} \,, \\ \pi_1(X^{(2)}) \oplus \pi_2(Y^{(2)}) = Z^{(2)} \,, \\ \quad \vdots \\ \pi_1(X^{(q)}) \oplus \pi_2(Y^{(q)}) = Z^{(q)} \,. \end{cases}$$

In the above q equations, some of the unknowns may be equal to each other. We have that $\pi_1(X^{(i)}) \neq \pi_1(X^{(j)})$ if and only if $X^{(i)} \neq X^{(j)}$, and $\pi_2(Y^{(i)}) \neq \pi_2(Y^{(j)})$ if and only if $Y^{(i)} \neq Y^{(j)}$. No condition holds for $\pi_1(X^{(i)})$ versus $\pi_2(Y^{(i)})$, as these are defined by independent permutations. Thus, $\{\pi_1(X^{(i)})\}_{1\leq i\leq q}$ and $\{\pi_2(Y^{(i)})\}_{1\leq i\leq q}$ are identified with two sets of unknowns

$$\mathcal{P} = \{P_1, \ldots, P_{q_1}\},$$
$$\mathcal{Q} = \{Q_1, \ldots, Q_{q_2}\}.$$

with $q_1, q_2 \leq q$. Since $\mathcal{P}$ and $\mathcal{Q}$ are defined by independent permutations, we know that $\mathcal{P}$ and $\mathcal{Q}$ are independent. We connect P_j and $Q_{j'}$ with a $Z^{(i)}$-labeled edge if $\pi_1(X^{(i)}) = P_j$ and $\pi_2(Y^{(i)}) = Q_{j'}$ for some i. Any pair of vertices in the same set (either $\mathcal{P}$ or $\mathcal{Q}$) are connected by a $\neq$-labeled edge. In this way, we obtain the transcript graph of τ on $\mathcal{P} \sqcup \mathcal{Q}$, and we denote it by G_τ.

5.3.3 Bad Transcripts. Informally, bad events are the properties which would make the mirror theory inapplicable. One can only apply the mirror theory if the transcript graph G_τ is (1) acyclic, (2) satisfies the NPL condition, and (3) the number of edges in $\mathcal{C}$ (i.e., edges in the components of size greater than two) is not greater than $\overline{q}_c$, for some parameter $\overline{q}_c$ that will be defined later on. The first two conditions come from Definitions 1 and 2, the last one is the condition on the number of edges in $\mathcal{C}$ in Lemma 4. Stated differently, we need to say that τ is a bad transcript if the corresponding transcript graph G_τ either includes a circle or a path of even length with $\lambda(\mathcal{L}) = 0$, or the number of edges in $\mathcal{C}$ exceeds $\overline{q}_c$.

The first two are implied if either of the following two events is set.

(i) G_τ contains an alternating circle of length 2 or an alternating path of length 2 such that $\lambda(\mathcal{L}) = 0$,

(ii) G_τ contains an alternating path of length 4 starting at the X-shore, or it contains an alternating path of length 4 starting at the Y-shore such that $\lambda(\mathcal{L}) = 0$.

We remark that it appears a bit odd to require the side-condition for the second part of event (ii) only. However, it turns out that by releasing that condition for this second part, we would not be able to derive a strong security bound for constructions based on SoP (see Section 5.3.5 for more details). Fortunately, it turns out that we *can* add this side-condition without problems, as negation of above two conditions (i)-(ii) indeed imply (1) and (2). Together with the third condition,

(iii) the number of edges in $\mathcal{C}$ is greater than $\overline{q}_c$,

these form the three conditions which a good transcript graph should satisfy. In other words, we say that $\tau \in \mathcal{T}_{\text{bad}}$ if and only if one of the above conditions holds.

Below, we will describe these three sets of bad events in more detail, the bad events for all six schemes are defined separately in the full version of the paper.

Recalling that we denote by $X^{(i)}$ the i-th input to π_1, $Y^{(i)}$ the i-th input to π_2, and $Z^{(i)} = \pi_1(X^{(i)}) \oplus \pi_2(Y^{(i)})$.

(i) This event is covered by AP2 = AP2a ∨ AP2b ∨ AP2c, defined as follows:

$$\begin{aligned}
\text{AP2}a\colon & \exists \, \text{distinct} \, (i,j) \, \text{such that} \, X^{(i)} = X^{(j)} \, \wedge \, Y^{(i)} = Y^{(j)} \, , \\
\text{AP2}b\colon & \exists \, \text{distinct} \, (i,j) \, \text{such that} \, X^{(i)} = X^{(j)} \, \wedge \, Z^{(i)} = Z^{(j)} \, , \\
\text{AP2}c\colon & \exists \, \text{distinct} \, (i,j) \, \text{such that} \, Z^{(i)} = Z^{(j)} \, \wedge \, Y^{(i)} = Y^{(j)} \, .
\end{aligned}$$

(ii) This event is covered by AP4 = AP4a ∨ AP4b, defined as follows:

$$\begin{aligned}
\text{AP4}a\colon & \exists \, \text{distinct} \, (i,j,k,l) \, \text{such that} \, X^{(i)} = X^{(j)} \, \wedge \, Y^{(j)} = Y^{(k)} \, \wedge \, X^{(k)} = X^{(l)} \, , \\
\text{AP4}b\colon & \exists \, \text{distinct} \, (i,j,k,l) \, \text{such that} \, Y^{(i)} = Y^{(j)} \, \wedge \, X^{(j)} = X^{(k)} \, \wedge \, Y^{(k)} = Y^{(l)} \\
& \qquad\qquad (\wedge \, Z^{(i)} \oplus Z^{(j)} \oplus Z^{(k)} \oplus Z^{(l)} = 0) \, ,
\end{aligned}$$

where $Z^{(i)} \oplus Z^{(j)} \oplus Z^{(k)} \oplus Z^{(l)} = 0$ is the side condition of the event AP4b.

(iii) This event is covered by NC = NCa ∨ NCb, defined as follows:

$$\begin{aligned}
\text{NC}a\colon & |\{(i,j) \, \text{such that} \, i \neq j \wedge X^{(i)} = X^{(j)}\}| \geq \overline{q}_c/4 \, , \\
\text{NC}b\colon & |\{(i,j) \, \text{such that} \, i \neq j \wedge Y^{(i)} = Y^{(j)}\}| \geq \overline{q}_c/4 \, .
\end{aligned}$$

A distinct pair of "half-colliding" queries such that either $X^{(i)} = X^{(j)}$ or $Y^{(i)} = Y^{(j)}$ will add an edge to any component containing it, and make the size of the component greater than two; hence the number of edges in $\mathcal{C}$ cannot be twice as many as the number of half-collisions.

The probability that $\tau \in \mathcal{T}_{\text{bad}}$ happens, is given by

$$\Pr[\tau \in \mathcal{T}_{\text{bad}}] \leq \Pr[\text{AP2}] + \Pr[\text{AP4}] + \Pr[\text{NC}] \, , \tag{16}$$

where AP2 = AP2a∨AP2b∨AP2c, AP4 = AP4a∨AP4b, and NC = NCa∨NCb.

5.3.4 Ratio for Good Transcripts for $F^{\mathbf{EDM}}_{B_2}$, $F^{\mathbf{EDM}}_{B_3}$, $F^{\mathbf{EDM}}_{B_4}$, $F^{\mathbf{EDM}}_{B_5}$, and $F^{\mathbf{SoP}}_{B_2}$, $F^{\mathbf{SoP}}_{B_3}$.

Consider an attainable transcript $\tau \in \mathcal{T}_{\text{good}}$. We now lower bound $\Pr[X_{\mathcal{O}} = \tau]$ and compute $\Pr[X_{\mathcal{P}} = \tau]$ in order to obtain a lower bound for the ratio of these probabilities. We denote by $comp_{\mathcal{O}}(\tau)$ (resp., $comp_{\mathcal{P}}(\tau)$) the set of oracles in the real world (resp., the ideal world) that are compatible with τ. We first consider the ideal world $\mathcal{P}$, and obtain

$$\Pr[X_{\mathcal{P}} = \tau] = \Pr[\mathsf{Rand} \in comp_{\mathcal{P}}(\tau)] = \frac{1}{|\mathcal{K}_h|} \cdot \frac{1}{2^{nq}} \, .$$

For the real world oracle $\mathcal{O}$, the probability of obtaining τ is computed over the randomness of π_1 and π_2. Now, fix a parameter $\overline{q}_c$ (to be optimized later). For a transcript graph G_τ, let $G^{=}_\tau$ denote the graph obtained by deleting all $\neq$-labeled edges from G_τ. Then $G^{=}_\tau$ is a bipartite graph with q edges. By the fact that the considered transcript τ is good, the induced graph G_τ (i) is acyclic, (ii) satisfies the NPL condition, and (iii) the number of edges in $\mathcal{C}$ (i.e., edges in the components of size greater than two) is not greater than $\overline{q}_c$. By Theorem 4 and since $q_c \leq \overline{q}_c$, the number of possible ways of fixing $\pi_1(X^{(i)})$ and $\pi_2(Y^{(i)})$ is lower bounded by $\frac{(2^n)_{|\mathcal{P}|}(2^n)_{|\mathcal{Q}|}}{2^{nq}}(1-\varepsilon_1)$ where

$$\varepsilon_1 = \frac{9\overline{q}_c^2}{8 \cdot 2^n} + \frac{3\overline{q}_c q^2}{2 \cdot 2^{2n}} + \frac{q^2}{2^{2n}} + \frac{9\overline{q}_c^2 q}{8 \cdot 2^{2n}} + \frac{8q^4}{3 \cdot 2^{3n}} \,. \tag{17}$$

The probability that π_1 and π_2 realize each assignment is exactly $1/(2^n)_{|\mathcal{P}|}(2^n)_{|\mathcal{Q}|}$. We thus obtain

$$\frac{\Pr[X_\mathcal{O} = \tau]}{\Pr[X_\mathcal{P} = \tau]} \geq 1 - \varepsilon_1 \,.$$

5.3.5 Probability of Bad Transcripts for $F^{\mathrm{EDM}}_{B_2}$, $F^{\mathrm{EDM}}_{B_3}$, $F^{\mathrm{EDM}}_{B_4}$, $F^{\mathrm{EDM}}_{B_5}$, and $F^{\mathrm{SoP}}_{B_2}$, $F^{\mathrm{SoP}}_{B_3}$.

The exact values of X, Y, and Z are, respectively,

MAC	X	Y	Z
$F^{\mathrm{EDM}}_{B_2}$	N	T	$N \oplus H_{K_h}(M)$
$F^{\mathrm{EDM}}_{B_3}$	N	$T \oplus H_{K_h}(M)$	$N \oplus H_{K_h}(M)$
$F^{\mathrm{EDM}}_{B_4}$	$N \oplus H_{K_h}(M)$	T	N
$F^{\mathrm{EDM}}_{B_5}$	$N \oplus H_{K_h}(M)$	$T \oplus H_{K_h}(M)$	N
$F^{\mathrm{SoP}}_{B_2}$	N	$N \oplus H_{K_h}(M)$	T
$F^{\mathrm{SoP}}_{B_3}$	N	$N \oplus H_{K_h}(M)$	$T \oplus H_{K_h}(M)$

Let $\overline{q}_c \in \mathbb{N}$. We denote by $\mathcal{I}$ the set of all query indices i such that $N^{(i)} = N^{(j)}$ for some $j \neq i$. One can see that $|\mathcal{I}| \leq 2\mu$. Note that $|\mathcal{I}| = 0$ for $F^{\mathrm{EDM}}_{B_2}$ and $F^{\mathrm{EDM}}_{B_3}$. We define by $\mathrm{AP2}^{\mathcal{F}}[B_x]$ (resp., $\mathrm{AP4}^{\mathcal{F}}[B_x]$ and $\mathrm{NC}^{\mathcal{F}}[B_x]$) the bad event AP2 (resp., AP4 and NC) for $F^{\mathrm{EDM}}_{B_x}$ with $x = 2, \ldots, 5$, or $F^{\mathrm{SoP}}_{B_x}$ with $x = 2, 3$. Note that we treat $F^{\mathrm{EDM}}_{B_2}$ and $F^{\mathrm{EDM}}_{B_3}$ for nonce-respecting distinguisher only, hence the bad events AP2a, AP2b, AP4a, AP4b, and NCa do not appear for these two constructions. We consider the bad events for each of the six construction separately.

(i) An alternating circle of length 2 or an alternating path of length such that $\lambda(\mathcal{L}) = 0$.

- $F^{\mathrm{EDM}}_{B_4}$. We first consider the bad event AP2a. The probability that $N^{(i)} \oplus H_{K_h}(M^{(i)}) = N^{(j)} \oplus H_{K_h}(M^{(j)})$ happens for fixed i, j is ϵ, and the probability that $T^{(i)} = T^{(j)}$ happens for fixed i, j is $1/2^n$. Summed over all q possible i's, and all q possible j's, we have

$$\Pr\left[\mathrm{AP2}a^{\mathrm{EDM}}[B_4]\right] \leq \frac{q^2\epsilon}{2^n} \,. \tag{18}$$

We then consider the bad event AP2b. The probability that $N^{(i)} \oplus H_{K_h}(M^{(i)}) = N^{(j)} \oplus H_{K_h}(M^{(j)})$ happens for fixed i, j is ϵ. Assume that $i < j$, which means that $N^{(j)}$ is a faulty nonce. Then the number of pairs (i, j) such that $N^{(i)} = N^{(j)}$ is at most μ^2, and we have

$$\Pr\left[\mathrm{AP2}b^{\mathrm{EDM}}[B_4]\right] \leq \mu^2 \epsilon\,. \tag{19}$$

Bad event AP2c is similar to AP2b. However, the second event is $T^{(i)} = T^{(j)}$, which holds with probability $1/2^n$. Then the number of pairs (i, j) such that $N^{(i)} = N^{(j)}$ is at most μ^2, and we have

$$\Pr\left[\mathrm{AP2}c^{\mathrm{EDM}}[B_4]\right] \leq \frac{\mu^2}{2^n}\,. \tag{20}$$

– $F^{\mathrm{EDM}}_{B_5}$. We first consider the bad event AP2a. The probability that $N^{(i)} \oplus H_{K_h}(M^{(i)}) = N^{(j)} \oplus H_{K_h}(M^{(j)})$ and $T^{(i)} \oplus H_{K_h}(M^{(i)}) = T^{(j)} \oplus H_{K_h}(M^{(j)})$ happens for fixed i, j is $\epsilon/2^n$. Summed over all q possible i's, and all q possible j's, we have

$$\Pr\left[\mathrm{AP2}a^{\mathrm{EDM}}[B_5]\right] \leq \frac{q^2 \epsilon}{2^n}\,. \tag{21}$$

The bad event AP2b is already analyzed in (19). We then consider the bad event AP2c. The probability that $T^{(i)} \oplus H_{K_h}(M^{(i)}) = T^{(j)} \oplus H_{K_h}(M^{(j)})$ happens for fixed i, j is ϵ. Assume that $i < j$, which means that $N^{(j)}$ is a faulty nonce. Then the number of pairs (i, j) such that $N^{(i)} = N^{(j)}$ is at most μ^2, and we have

$$\Pr\left[\mathrm{AP2}c^{\mathrm{EDM}}[B_5]\right] \leq \mu^2 \epsilon\,. \tag{22}$$

– $F^{\mathrm{EDM}}_{B_2}$. Note that the X and Z values of $F^{\mathrm{EDM}}_{B_2}$ are the reverse of those of $F^{\mathrm{EDM}}_{B_4}$, and the Y value of the both constructions is the same. Hence the analysis is the same as that for $F^{\mathrm{EDM}}_{B_4}$ with $\mu = 0$ because we consider nonce-respecting dinstinguishers for $F^{\mathrm{EDM}}_{B_2}$.
– $F^{\mathrm{EDM}}_{B_3}$. Note that the X and Z values of $F^{\mathrm{EDM}}_{B_3}$ are the reverse of those of $F^{\mathrm{EDM}}_{B_5}$, and the Y value of the both constructions is the same. Hence the analysis is the same as that for $F^{\mathrm{EDM}}_{B_5}$ with $\mu = 0$ because we consider nonce-respecting dinstinguishers for $F^{\mathrm{EDM}}_{B_3}$.
– $F^{\mathrm{SoP}}_{B_2}$. Note that the X, Y, and Z values of $F^{\mathrm{SoP}}_{B_2}$ are a reshuffling of the X, Y, and Z values of $F^{\mathrm{EDM}}_{B_4}$. Hence we have that $\Pr\left[\mathrm{AP2}^{\mathrm{SoP}}[B_2]\right] = \Pr\left[\mathrm{AP2}^{\mathrm{EDM}}[B_4]\right]$.
– $F^{\mathrm{SoP}}_{B_3}$. Note that the X, Y, and Z values of $F^{\mathrm{SoP}}_{B_3}$ are a reshuffling of the X, Y, and Z values of $F^{\mathrm{EDM}}_{B_5}$. Hence we have that $\Pr\left[\mathrm{AP2}^{\mathrm{SoP}}[B_3]\right] = \Pr\left[\mathrm{AP2}^{\mathrm{EDM}}[B_5]\right]$.

We have obtained

$$\Pr\left[\mathrm{AP2}^{\mathrm{EDM}}[B_2]\right] \le \frac{q^2\epsilon}{2^n}\,, \tag{23}$$

$$\Pr\left[\mathrm{AP2}^{\mathrm{EDM}}[B_3]\right] \le \frac{q^2\epsilon}{2^n}\,. \tag{24}$$

$$\Pr\left[\mathrm{AP2}^{\mathrm{EDM}}[B_4]\right],\, \Pr\left[\mathrm{AP2}^{\mathrm{SoP}}[B_2]\right] \le \frac{\mu^2}{2^n} + \frac{q^2\epsilon}{2^n} + \mu^2\epsilon\,, \tag{25}$$

$$\Pr\left[\mathrm{AP2}^{\mathrm{EDM}}[B_5]\right],\, \Pr\left[\mathrm{AP2}^{\mathrm{SoP}}[B_3]\right] \le 2\mu^2\epsilon + \frac{q^2\epsilon}{2^n}\,. \tag{26}$$

(ii) An alternating path of length 4. We want to recall that since we treat $F^{\mathrm{EDM}}_{B_2}$ and $F^{\mathrm{EDM}}_{B_3}$ for nonce-respecting distinguisher only, alternating paths do not appear for these two constructions. Thus, we only have to consider $F^{\mathrm{EDM}}_{B_4}$, $F^{\mathrm{EDM}}_{B_5}$, $F^{\mathrm{SoP}}_{B_2}$, and $F^{\mathrm{SoP}}_{B_3}$.

– $F^{\mathrm{EDM}}_{B_4}$. We will use Lemma 1 to bound the event, with $q_i = q_j = q_k = q_l = q$. We first consider the bad event AP4a. We denote $E_{i,j} : N^{(i)} \oplus H_{K_h}(M^{(i)}) = N^{(j)} \oplus H_{K_h}(M^{(j)})$ (same for $E_{k,\ell}$), and $F_{i,j,k,\ell} : T^{(j)} = T^{(k)}$. The probability that $E_{i,j}$ happens for fixed i,j is ϵ (same for $E_{k,\ell}$), and the probability that $F_{i,j,k,\ell}$ happens for fixed j,k is $1/2^n$. Summed over all possible i,j,k,ℓ's, we have

$$\Pr\left[\mathrm{AP4}a^{\mathrm{EDM}}[B_4]\right] \le \frac{q^2\epsilon}{2^{n/2}}\,. \tag{27}$$

Next, we consider the bad event AP4b, again with $q_i = q_j = q_k = q_l = q$. We drop the side-condition $Z^{(i)} \oplus Z^{(j)} \oplus Z^{(k)} \oplus Z^{(l)} = 0$ for simplicity. We denote $E_{i,j} : T^{(i)} = T^{(j)}$ (same for $E_{k,\ell}$), and $F_{i,j,k,\ell} : N^{(j)} \oplus H_{K_h}(M^{(j)}) = N^{(k)} \oplus H_{K_h}(M^{(k)})$. The probability that $E_{i,j}$ happens for fixed i,j is $1/2^n$ (same for $E_{k,\ell}$), and the probability that $F_{i,j,k,\ell}$ happens for fixed j,k is ϵ. Summed over all possible i,j,k,ℓ's, we have

$$\Pr\left[\mathrm{AP4}b^{\mathrm{EDM}}[B_4]\right] \le \frac{q^2\sqrt{\epsilon}}{2^n}\,. \tag{28}$$

– $F^{\mathrm{EDM}}_{B_5}$. The analysis is identical to the one of $F^{\mathrm{EDM}}_{B_4}$. The only difference is that we have $Y = T \oplus H_{K_h}(M)$ instead of $Y = T$. However, we can still rely on the randomness of T.

– $F^{\mathrm{SoP}}_{B_2}$ and $F^{\mathrm{SoP}}_{B_3}$. Since the X and Y values are the same for these two constructions, we will consider these together. We first consider the bad event AP4a. The number of queries using any repeated nonce is at most 2μ. This means that the number of pairs (j,k) such that $N^{(j)} = N^{(i)}$ for some $i \ne j$ and $N^{(k)} = N^{(l)}$ for some $k \ne l$ is at most $4\mu^2$. The probability that $N^{(j)} \oplus H_{K_h}(M^{(j)}) = N^{(k)} \oplus H_{K_h}(M^{(k)})$ happens for fixed j,k is ϵ. Summed over all possible j,k's, we have

$$\Pr[\mathrm{AP4}a^{\mathrm{SoP}}[B_2]] \le 4\mu^2\epsilon\,. \tag{29}$$

Next, we consider the bad event AP4b. Note that since the only randomness we have is the universal hash key K_h, we will explicitly rely on the side event $Z^{(i)} \oplus Z^{(j)} \oplus Z^{(k)} \oplus Z^{(l)} = 0$. We will use Lemma 1 to bound this event. We first consider the case that $k > \max\{i, j, l\}$ and the k-th query sets AP4b. We denote $E_{i,j} : N^{(i)} \oplus H_{K_h}(M^{(i)}) = N^{(j)} \oplus H_{K_h}(M^{(j)})$ (same for $E_{k,l}$), and $F_{i,j,k,l} : T^{(i)} \oplus T^{(j)} \oplus T^{(k)} \oplus T^{(l)} = 0$. The probability that $E_{i,j}$ happens for fixed i, j is ϵ (same for $E_{k,l}$), and the probability that $F_{i,j,k,l}$ happens for fixed i, j, k, l is $1/2^n$. For each fixed k, and summed over q possible i's, q possible j's, and q possible l's, and since the k-th query makes an inner edge of the trail, it should be a faulty query (there are μ possible k's in total). Therefore this case happens with probability at most

$$\mu\sqrt{\frac{q^3}{2^n}}\epsilon\,.$$

Next, consider the case that $l > \max\{i, j, k\}$ and the l-th query makes AP4b. We denote $E_{i,j} : N^{(i)} \oplus H_{K_h}(M^{(i)}) = N^{(j)} \oplus H_{K_h}(M^{(j)})$ (same for $E_{k,\ell}$), and $F_{i,j,k,\ell} : T^{(i)} \oplus T^{(j)} \oplus T^{(k)} \oplus T^{(l)} = 0$. The probability that $E_{i,j}$ happens for fixed i, j is ϵ (same for $E_{k,\ell}$), and the probability that $F_{i,j,k,\ell}$ happens for fixed i, j, k, l is $1/2^n$. For each fixed l (there are q possible l's in total), and summed over q possible i's, 2μ possible j's, and 2μ possible k's, this case happens with probability

$$2q\sqrt{\frac{\mu^2 q}{2^n}}\epsilon\,.$$

By symmetry, all other cases (i.e., $i > \max\{j, k, l\}$ and $j > \max\{i, k, l\}$) are also covered, we have

$$\Pr[\mathrm{AP4}b^{\mathrm{SoP}}[B_2]] \le \mu\sqrt{\frac{q^3}{2^n}}\epsilon + 2q\sqrt{\frac{\mu^2 q}{2^n}}\epsilon = \frac{3\mu q^{3n/2}\epsilon}{2^{n/2}}\,. \tag{30}$$

We have obtained

$$\Pr\left[\mathrm{AP4}^{\mathrm{EDM}}[B_4]\right], \Pr\left[\mathrm{AP4}^{\mathrm{EDM}}[B_5]\right] \le \frac{q^2\epsilon}{2^{n/2}} + \frac{q^2\sqrt{\epsilon}}{2^n}\,, \tag{31}$$

$$\Pr\left[\mathrm{AP4}^{\mathrm{SoP}}[B_2]\right], \Pr\left[\mathrm{AP4}^{\mathrm{SoP}}[B_3]\right] \le 4\mu^2\epsilon + \frac{3\mu q^{3n/2}\epsilon}{2^{n/2}}\,. \tag{32}$$

(iii) The number of edges in $\mathcal{C}$ is greater than $\overline{q}_c$.

- $F_{B_4}^{\mathrm{EDM}}$. For NCa, $X = N \oplus H_{K_h}(M)$. Using Markov inequality, we have:

$$\Pr\left[\mathrm{NC}a^{\mathrm{EDM}}[B_4]\right] \le \frac{4q^2\epsilon}{\overline{q}_c}\,. \tag{33}$$

For NCb, $Y = T$. Using Markov inequality, we have:

$$\Pr\left[\mathrm{NC}b^{\mathrm{EDM}}[B_4]\right] \le \frac{4q^2}{\overline{q}_c \cdot 2^n}\,. \tag{34}$$

- $F^{\mathrm{EDM}}_{B_5}$. The bad event NCa is already analyzed in (33). For NCb, $Y = T \oplus H_{K_h}(M)$. Using Markov inequality, we have:

$$\Pr\left[\mathrm{NC}b^{\mathrm{EDM}}[B_5]\right] \le \frac{4q^2\epsilon}{\overline{q}_c}\,. \tag{35}$$

- $F^{\mathrm{EDM}}_{B_2}$. The analysis is the same as that for $F^{\mathrm{EDM}}_{B_4}$, except that NCa would not happen due to $X = N$ and $\mu = 0$.
- $F^{\mathrm{EDM}}_{B_3}$. The analysis is the same as that for $F^{\mathrm{EDM}}_{B_5}$, except that NCa would not happen due to $X = N$ and $\mu = 0$.
- $F^{\mathrm{SoP}}_{B_2}$. Assuming that $\overline{q}_c/4 \ge \mu^2$ ($\overline{q}_c$ will be chosen later on to satisfy this condition), NCa would not happen. The bad event NCb is already analyzed in (33).
- $F^{\mathrm{SoP}}_{B_3}$. Assuming that $\overline{q}_c/4 \ge \mu^2$ ($\overline{q}_c$ will be chosen later on to satisfy this condition), NCa would not happen. The bad event NCb is already analyzed in (33).

We have obtained

$$\Pr\left[\mathrm{NC}^{\mathrm{EDM}}[B_2]\right] \le \frac{4q^2}{\overline{q}_c \cdot 2^n}\,, \tag{36}$$

$$\Pr\left[\mathrm{NC}^{\mathrm{EDM}}[B_3]\right], \Pr\left[\mathrm{NC}^{\mathrm{SoP}}[B_2]\right], \Pr\left[\mathrm{NC}^{\mathrm{SoP}}[B_3]\right] \le \frac{4q^2\epsilon}{\overline{q}_c}\,, \tag{37}$$

$$\Pr\left[\mathrm{NC}^{\mathrm{EDM}}[B_4]\right] \le \frac{4q^2\epsilon}{\overline{q}_c} + \frac{4q^2}{\overline{q}_c \cdot 2^n}\,, \tag{38}$$

$$\Pr\left[\mathrm{NC}^{\mathrm{EDM}}[B_5]\right] \le \frac{8q^2\epsilon}{\overline{q}_c}\,, \tag{39}$$

Conclusion for bad events. Combining (23)-(26), (31)-(32), and (36)-(39) with (16), we obtain

$$\begin{aligned}
\Pr\left[\tau^{\mathrm{EDM}}[B_2] \in \mathcal{T}_{\mathrm{bad}}\right] &\le \frac{q^2\epsilon}{2^n} + \frac{4q^2}{\overline{q}_c \cdot 2^n}\,,\\
\Pr\left[\tau^{\mathrm{EDM}}[B_3] \in \mathcal{T}_{\mathrm{bad}}\right] &\le \frac{q^2\epsilon}{2^n} + \frac{4q^2\epsilon}{\overline{q}_c}\,,\\
\Pr\left[\tau^{\mathrm{EDM}}[B_4] \in \mathcal{T}_{\mathrm{bad}}\right] &\le \frac{\mu^2}{2^n} + \mu^2\epsilon + \frac{q^2\epsilon}{2^n} + \frac{q^2\epsilon}{2^{n/2}} + \frac{q^2\sqrt{\epsilon}}{2^n} + \frac{4q^2\epsilon}{\overline{q}_c} + \frac{4q^2}{\overline{q}_c \cdot 2^n}\,,\\
\Pr\left[\tau^{\mathrm{EDM}}[B_5] \in \mathcal{T}_{\mathrm{bad}}\right] &\le 2\mu^2\epsilon + \frac{q^2\epsilon}{2^n} + \frac{q^2\epsilon}{2^{n/2}} + \frac{q^2\sqrt{\epsilon}}{2^n} + \frac{8q^2\epsilon}{\overline{q}_c}\,,\\
\Pr\left[\tau^{\mathrm{SoP}}[B_2] \in \mathcal{T}_{\mathrm{bad}}\right] &\le \frac{\mu^2}{2^n} + \mu^2\epsilon + \frac{q^2\epsilon}{2^n} + 4\mu^2\epsilon + \frac{3\mu q^{3n/2}\epsilon}{2^{n/2}} + \frac{4q^2\epsilon}{\overline{q}_c}\,,\\
\Pr\left[\tau^{\mathrm{SoP}}[B_3] \in \mathcal{T}_{\mathrm{bad}}\right] &\le 2\mu^2\epsilon + \frac{q^2\epsilon}{2^n} + 4\mu^2\epsilon + \frac{3\mu q^{3n/2}\epsilon}{2^{n/2}} + \frac{4q^2\epsilon}{\overline{q}_c}\,.
\end{aligned}$$

5.3.6 Conclusion. We will discuss the restrictions on the number of faulty queries for $F^{\mathrm{EDM}}_{B_4}, F^{\mathrm{EDM}}_{B_5}$, and $F^{\mathrm{SoP}}_{B_2}, F^{\mathrm{SoP}}_{B_3}$. We have assumed that $\overline{q}_c/4 \geq \mu^2$ for $F^{\mathrm{SoP}}_{B_2}$ and $F^{\mathrm{SoP}}_{B_3}$. In order to obtain $3n/4$-bit security, we choose $\overline{q}_c = 4q^{\frac{2}{3}}$. Above terms that include $\overline{q}_c$ get simplified as follows:

$$\frac{4q^2\epsilon}{\overline{q}_c} = q^{\frac{4}{3}}\epsilon\,,$$
$$\frac{4q^2}{\overline{q}_c \cdot 2^n} = \frac{q^{\frac{4}{3}}}{2^n}\,.$$

Based on this condition, we have $\mu \leq q^{\frac{1}{3}}$ for $F^{\mathrm{SoP}}_{B_2}$ and $F^{\mathrm{SoP}}_{B_3}$, and there is no restriction on μ for $F^{\mathrm{EDM}}_{B_4}$ and $F^{\mathrm{EDM}}_{B_5}$. Using the H-coefficients Technique (Lemma 3) with

$$\varepsilon_1 = \frac{18q^{\frac{4}{3}}}{2^n} + \frac{6q^{\frac{8}{3}}}{2^{2n}} + \frac{18q^{\frac{7}{3}}}{2^{2n}} + \frac{q^2}{2^{2n}} + \frac{8q^4}{3 \cdot 2^{3n}}\,,$$

we obtain the results stated in Theorem 2, Theorem 3, and Theorem 4.

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). The authors would like to thank the anonymous reviewers for their comments and suggestions.

References

1. Aumasson, J., Bernstein, D.J.: SipHash: A Fast Short-Input PRF. In: Galbraith, S.D., Nandi, M. (eds.) INDOCRYPT 2012. LNCS, vol. 7668, pp. 489–508. Springer (2012)
2. 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)
3. 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)
4. 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)
5. Bernstein, D.J.: SURF: Simple Unpredictable Random Function (april 1997)
6. Bernstein, D.J.: Stronger Security Bounds for Wegman-Carter-Shoup Authenticators. In: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 164–180. Springer (2005)
7. Böck, H., Zauner, A., Devlin, S., Somorovsky, J., Jovanovic, P.: Nonce-Disrespecting Adversaries: Practical Forgery Attacks on GCM in TLS. In: Silvanovich, N., Traynor, P. (eds.) USENIX WOOT 16. USENIX Association (2016)

8. 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)
9. Bogdanov, A., Lauridsen, M.M., Tischhauser, E.: Comb to Pipeline: Fast Software Encryption Revisited. In: Leander, G. (ed.) Fast Software Encryption - 22nd International Workshop, FSE 2015, Istanbul, Turkey, March 8-11, 2015, Revised Selected Papers. Lecture Notes in Computer Science, vol. 9054, pp. 150–171. Springer (2015)
10. 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, X., Sako, K. (eds.) ASIACRYPT 2012. LNCS, vol. 7658, pp. 208–225. Springer (2012)
11. 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)
12. Choi, W., Lee, B., Lee, Y., Lee, J.: Improved Security Analysis for Nonce-Based Enhanced Hash-then-Mask MACs. In: Moriai, S., Wang, H. (eds.) ASIACRYPT 2020, Part I. LNCS, vol. 12491, pp. 697–723. Springer (2020)
13. Cogliati, B., Seurin, Y.: EWCDM: An Efficient, Beyond-Birthday Secure, Nonce-Misuse Resistant MAC. In: Robshaw and Katz [41], pp. 121–149
14. Dai, W., Hoang, V.T., Tessaro, S.: Information-Theoretic Indistinguishability via the Chi-Squared Method. In: Katz and Shacham [25], pp. 497–523
15. Datta, N., Dutta, A., Nandi, M., Yasuda, K.: Encrypt or Decrypt? To Make a Single-Key Beyond Birthday Secure Nonce-Based MAC. In: Shacham, H., Boldyreva, A. (eds.) CRYPTO 2018, Part I. LNCS, vol. 10991, pp. 631–661. Springer (2018)
16. 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)
17. Derbez, P., Iwata, T., Sun, L., Sun, S., Todo, Y., Wang, H., Wang, M.: Cryptanalysis of AES-PRF and Its Dual. IACR Trans. Symmetric Cryptol. 2018(2), 161–191 (2018)
18. Dutta, A., Nandi, M., Talnikar, S.: Beyond Birthday Bound Secure MAC in Faulty Nonce Model. In: Ishai, Y., Rijmen, V. (eds.) EUROCRYPT 2019, Part I. pp. 437–466 (2019)
19. Gilbert, E.N., MacWilliams, F.J., Sloan, N.J.A.: Codes Which Detect Deception. Bell System Technical Journal (1974)
20. 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)
21. Handschuh, H., Preneel, B.: Key-Recovery Attacks on Universal Hash Function Based MAC Algorithms. In: Wagner, D.A. (ed.) CRYPTO 2008. LNCS, vol. 5157, pp. 144–161. Springer (2008)
22. Hoang, V.T., Tessaro, S.: Key-Alternating Ciphers and Key-Length Extension: Exact Bounds and Multi-user Security. In: Robshaw and Katz [41], pp. 3–32
23. Jha, A., Nandi, M.: Tight Security of Cascaded LRW2. J. Cryptol. 33(3), 1272–1317 (2020)
24. Joux, A.: Authentication Failures in NIST Version of GCM. Comments submitted to NIST Modes of Operation Process (2006)

25. Katz, J., Shacham, H. (eds.): CRYPTO 2017, Part III, LNCS, vol. 10403. Springer (2017)
26. Kim, S., Lee, B., Lee, J.: Tight Security Bounds for Double-Block Hash-then-Sum MACs. In: Canteaut, A., Ishai, Y. (eds.) EUROCRYPT 2020, Part I. LNCS, vol. 12105, pp. 435–465. Springer (2020)
27. Krawczyk, H.: LFSR-based Hashing and Authentication. In: Desmedt, Y. (ed.) CRYPTO '94. LNCS, vol. 839, pp. 129–139. Springer (1994)
28. Luykx, A., Preneel, B.: Optimal Forgeries Against Polynomial-Based MACs and GCM. In: Nielsen, J.B., Rijmen, V. (eds.) EUROCRYPT 2018, Part I. LNCS, vol. 10820, pp. 445–467. Springer (2018)
29. McGrew, D.A., Viega, J.: The Security and Performance of the Galois/Counter Mode (GCM) of Operation. In: Canteaut, A., Viswanathan, K. (eds.) INDOCRYPT 2004. LNCS, vol. 3348, pp. 343–355. Springer (2004)
30. Mennink, B., Neves, S.: Encrypted Davies-Meyer and Its Dual: Towards Optimal Security Using Mirror Theory. In: Katz and Shacham [25], pp. 556–583
31. Mennink, B., Neves, S.: Optimal PRFs from Blockcipher Designs. IACR Trans. Symmetric Cryptol. 2017(3), 228–252 (2017)
32. Minematsu, K.: How to Thwart Birthday Attacks against MACs via Small Randomness. In: Hong, S., Iwata, T. (eds.) FSE 2010. LNCS, vol. 6147, pp. 230–249. Springer (2010)
33. Nachef, V., Patarin, J., Volte, E.: Feistel Ciphers - Security Proofs and Cryptanalysis. Springer (2017)
34. Nandi, M.: Bernstein Bound on WCS is Tight - Repairing Luykx-Preneel Optimal Forgeries. In: Shacham, H., Boldyreva, A. (eds.) CRYPTO 2018, Part II. LNCS, vol. 10992, pp. 213–238. Springer (2018)
35. Nandi, M.: Mind the Composition: Birthday Bound Attacks on EWCDMD and SoKAC21. In: Canteaut, A., Ishai, Y. (eds.) EUROCRYPT 2020, Part I. LNCS, vol. 12105, pp. 203–220. Springer (2020)
36. 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)
37. 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)
38. 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)
39. 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)
40. Patarin, J.: Mirror Theory and Cryptography. Cryptology ePrint Archive, Report 2016/702 (2016)
41. Robshaw, M., Katz, J. (eds.): CRYPTO 2016, Part I, LNCS, vol. 9814. Springer (2016)
42. Shibutani, K., Isobe, T., Hiwatari, H., Mitsuda, A., Akishita, T., Shirai, T.: Piccolo: An Ultra-Lightweight Blockcipher. In: Preneel, B., Takagi, T. (eds.) CHES 2011. LNCS, vol. 6917, pp. 342–357. Springer (2011)
43. 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 (1996)
44. Wegman, M.N., Carter, L.: New Hash Functions and Their Use in Authentication and Set Equality. J. Comput. Syst. Sci. 22(3), 265–279 (1981)