# Tight Security of Double-Block Nonce-Based MACs

Wonseok Choi[1], Jooyoung Lee[2], and Yeongmin Lee[3]

[1] Purdue University, West Lafayette, IN, USA
wonseok@purdue.edu
[2] KAIST, Daejeon, Korea
hicalf@kaist.ac.kr
[3] DESILO Inc., Seoul, Korea
yeongmin.lee@desilo.ai

**Abstract.** In this paper, we study the security of MAC constructions among those classified by Chen *et al.* in ASIACRYPT '21. Precisely, $F_{B_2}^{\mathrm{EDM}}$ (or EWCDM as named by Cogliati and Seurin in CRYPTO '16), $F_{B_3}^{\mathrm{EDM}}$, $F_{B_2}^{\mathrm{SoP}}$, $F_{B_3}^{\mathrm{SoP}}$ (all as named by Chen *et al.*) are proved to be fully secure up to $2^n$ MAC queries in the nonce-respecting setting, improving the previous bound of $\frac{3n}{4}$-bit security. In particular, $F_{B_2}^{\mathrm{SoP}}$ and $F_{B_3}^{\mathrm{SoP}}$ enjoy graceful degradation as the number of queries with repeated nonces grows (when the underlying universal hash function satisfies a certain property called *multi-xor-collision resistance*). To do this, we develop a new tool, namely extended Mirror theory based on two independent permutations to a wide range of $\xi_{\max}$ including inequalities. Furthermore, we give a generic semi-black-box reduction from single-user security bound in the standard model to multi-user security bound in the ideal cipher model, yielding significantly better bounds than the naive hybrid argument. This reduction is applicable to all MAC construction we considered in this paper and even can be more generalized.
We also present matching attacks on $F_{B_4}^{\mathrm{EDM}}$ and $F_{B_5}^{\mathrm{EDM}}$ using $O(2^{3n/4})$ MAC queries and $O(1)$ verification query without using repeated nonces.

**Keywords:** message authentication code, beyond birthday bound security, Mirror theory

## 1 Introduction

Beyond Birthday Bound MACs. A message authentication code (MAC) is a fundamental symmetric primitive allowing two entities sharing a secret key to verify that a received message originates from one of the two parties and was not modified by an attacker. Most popular MAC constructions are based on block ciphers (e.g., CBC-MAC [2], PMAC [7], and OMAC [19]). At a high level, well-known block cipher-based MAC constructions such as CBC-MAC and PMAC follow the *UHF-then-PRF* design paradigm: a message is first mapped

onto a short string through a universal hash function (UHF) and then encrypted through a fixed-input-length PRF to obtain a short tag. This method is simple, deterministic and stateless, yet its security caps at the so-called birthday bound; any collision at the output of the UHF, which translates into a tag collision, is usually enough to break the security of the scheme. The birthday bound security might not be enough, in particular, when the MAC construction is instantiated with a block cipher such as PRESENT [8], LED [16], and GIFT [1] operating on small blocks. A small block length, such as 64 bits, of the underlying primitive can render it a practical attack target when used in modes with birthday-bound security, as was illustrated by the recent attacks on popular communication protocols such as TLS [6].

Nonce-based MACs. Authenticated encryption schemes use a nonce (a value that never repeats) to give diversity to encryption of messages. The tag generation can be modeled as a nonce-based MAC in this case. Nonce-based MACs might be designed by a deterministic MAC using the concatenation of a nonce and a message as an input, or the well-known Wegman-Carter (WC) [28,29] construction. Many studies have tried to tweak deterministic MACs to obtain BBB security. They share a similar structural design of doubling the internal state of the hash function [30,31,32,24]. Better security bounds can be obtained for Wegman-Carter style MACs [4,12,29,28]. The WC construction is based on a universal hash function $H$ and a pseudorandom function (PRF) $F$, that computes the corresponding tag as

$$T = H_{K_h}(M) \oplus F_K(N)$$

where $K$ is the key for $F$, $K_h$ is the key for $H$, and $N$ and $M$ denote a nonce and a message, respectively. It enjoys a powerful security bound when nonces are never repeated. Assuming $F_K$ is a uniformly random function, the adversary can make a forgery with probability at most $v\epsilon$, where $v$ is the number of verification queries and $\epsilon$ is the collision probability of $H$. By assuming $\epsilon$ is close to $\frac{1}{2^n}$, WC is secure up to $O(2^n)$ forgery attempts. This paradigm has been widely employed, e.g., in the Poly1305-AES [5] and GMAC [23] standards, and studied in depth [4].

Nonce Misuse Resistance. Despite the strong security advantages, the WC construction suffers from one major shortcoming: it is vulnerable to *nonce-misuse*. The construction might be seriously attacked if a nonce is repeated even once. For example, in the case of polynomial universal hashing, a repeated nonce can lead to the recovery of the hash key, which allows successful forgeries [17]. It might be challenging to maintain the uniqueness of a nonce in certain environments, for example, when a nonce is chosen from a set of low entropy or when the state of the MAC is reset due to some fault in its implementation. For this reason, there has been a considerable amount of research on constructing nonce-based MACs that provide security under nonce misuse.

### 1.1 Motivation

EWCDM [12] is based on an $n$-bit hash function $H$ and an $n$-bit block cipher $E$; it takes as input an $n$-bit nonce $N$ and a message $M$, and outputs the corresponding tag as follows.

$$\mathsf{EWCDM}[H, E](N, M) = E_{K_2}(H_{K_h}(M) \oplus E_{K_1}(N) \oplus N)$$

for hash key $K_h$ and block cipher keys $K_1$ and $K_2$. By using two block cipher calls, its security has been proved up to $O(2^{2n/3})$ MAC queries and $O(2^n)$ verification queries. As a variant of EWCDM, Datta *et al.* [14] proposed to replace the second block cipher call of EWCDM by block cipher decryption using the same key; for a nonce $N = N^* \,\|\, 0^{n/3}$ and a message $M$,

$$\mathsf{DWCDM}[H, E](N, M) = E_K^{-1}(H_{K_h}(M) \oplus E_K(N) \oplus N).$$

DWCDM is also secure up to $O(2^{2n/3})$ MAC queries and $O(2^n)$ verification queries.

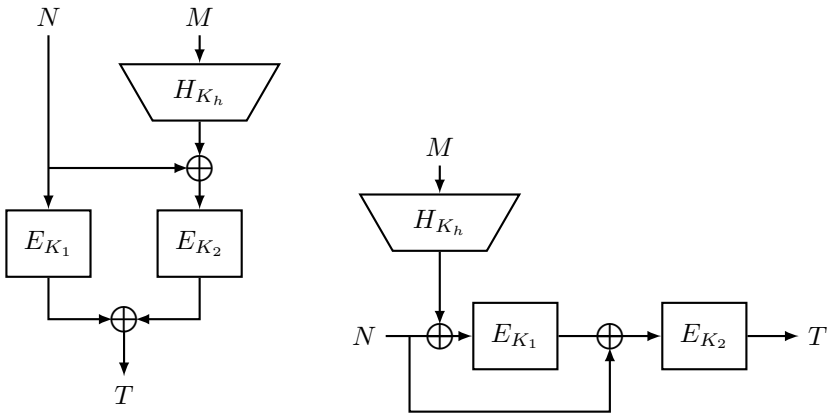
Notably, Mennink and Neves [21] proved $n$-bit PRF security of EWCDM, but their proof relied on unverifiable Mirror theory. Recently, Datta *et al.* [13] proved $\frac{3n}{4}$-bit MAC security of EWCDM and DWCDM using $\frac{3n}{4}$-bit nonces using verifiable Mirror theory. More precisely, the adversarial advantages against the PRF security of EWCDM and DWCDM are upper bounded by $O(q^{4/3}/2^n)$ and $O(q^{1/3}/2^{n/4})$, respectively, in the nonce-respecting setting, while both constructions are secure up to $O(2^n)$ verification queries.

Dutta *et al.* [15] formalized the faulty nonce model for MAC constructions, where a MAC query is considered *faulty* if it is queried with a repeated nonce. They introduced the nonce-based Enhanced Hash-then-Mask (nEHtM) construction and proved its security up to $O(2^{2n/3})$ MAC queries and $O(2^n)$ verification queries in a nonce-respecting setting. Moreover, nEHtM enjoys graceful security degradation when nonces are misused. For the number of faulty nonces $\mu$, their bound on the forging advantage includes $\mu q/2^n$ and $\mu v/2^n$ terms, where $q$ and $v$ denote the number of MAC queries and the number of verification queries, respectively. Subsequently, Choi *et al.* [10] improved this security bound to $\frac{3n}{4}$ bits when the number of faulty nonces is below $2^{3n/8}$, and also proved graceful security degradation for $\mu \leq 2^{n/2}$. Recently, Chen *et al.* [9] classified nonce-based double-block MAC constructions and analyzed their PRF security in the faulty nonce model. Some constructions have been shown to achieve $\frac{3n}{4}$-bit PRF security. However, the tightness of those constructions still remains open. This line of research raises the following fundamental question:

*"Is there a block cipher-based MAC construction using nonces that provides both full $n$-bit security and nonce misuse resistance?"*

### 1.2 Our Contribution

To affirmatively answer the question, we selected six candidates of double-block nonce-based MAC constructions from [9]; EWCDM (denoted as $F_{B_2}^{\mathrm{EDM}}$ in [9],




(a) $F_{B_2}^{\mathrm{SoP}}$ (b) $F_{B_4}^{\mathrm{EDM}}$

Fig. 1: MAC constructions $F_{B_2}^{\mathrm{SoP}}$ and $F_{B_4}^{\mathrm{EDM}}$ based on a universal hash function $H$ and a block cipher $E$.

while denoted EWCDM in this paper), $F_{B_3}^{\mathrm{EDM}}$, $F_{B_2}^{\mathrm{SoP}}$, $F_{B_3}^{\mathrm{SoP}}$, $F_{B_4}^{\mathrm{EDM}}$, and $F_{B_5}^{\mathrm{EDM}}$. For a nonce $N$ and a message $M$, $F_{B_2}^{\mathrm{SoP}}$ and $F_{B_4}^{\mathrm{EDM}}$ compute the corresponding tags as follows:

$$F_{B_2}^{\mathrm{SoP}}[H,E](N,M) = E_{K_1}(N) \oplus E_{K_2}(N \oplus H_{K_h}(M)),$$
$$F_{B_4}^{\mathrm{EDM}}[H,E](N,M) = E_{K_2}(E_{K_1}(N \oplus H_{K_h}(M)) \oplus N)$$

where $K_h$ is a hash key and $K_1$ and $K_2$ are block cipher keys (see Figure 1). We can also prove the security of the following constructions:

$$F_{B_3}^{\mathrm{EDM}}[H,E](N,M) = \mathsf{EWCDM}[H,E](N,M) \oplus H_{K_h}(M),$$
$$F_{B_3}^{\mathrm{SoP}}[H,E](N,M) = F_{B_2}^{\mathrm{SoP}}[H,E](N,M) \oplus H_{K_h}(M),$$
$$F_{B_5}^{\mathrm{EDM}}[H,E](N,M) = F_{B_4}^{\mathrm{EDM}}[H,E](N,M) \oplus H_{K_h}(M),$$

since adding $H_{K_h}(M)$ to the tag does not significantly affect their security proof.

Our contribution is summarized as follows:

1. We prove the tightness of the security bounds for 6 MAC schemes using two (independent) block cipher calls except $F_{B_2}^{\mathrm{EDMD}}$ from Chen *et al.* [9]. This result will be discussed in more detail in the next part of this section.
2. To prove their security, we generalize state-of-the-art Mirror theory for two independent permutations with equation and inequality systems. To obtain the result, we first prove the Mirror theory when the distinction condition between variables is relaxed. Then, we further formalize the extended Mirror theory by using a new approach: estimates the ratio between the number of solutions to a system of equations and those with the addition of inequalities.

3. We also prove multi-xor-collision probability of CBC-MAC is negligible: for any distinct $x_1, \ldots, x_k \in \{0,1\}^*$ and distinct $y_1, \ldots, y_k \in \{0,1\}^n$,

$$\Pr\left[K_h \leftarrow_{\$} \mathcal{K}_h : H_{K_h}(x_1) \oplus y_1 = \cdots = H_{K_h}(x_k) \oplus y_k\right] \leq \epsilon$$

   for a small $\epsilon$. This allow us to prove that $F^{\mathrm{SoP}}_{B_2}$ and $F^{\mathrm{EDM}}_{B_5}$ with the internal hash function instantiated with CBC-MAC achieves $n$-bit security.
4. We show multi-user security bounds for all the MAC schemes using a semi-black-box approach in the ideal cipher model. Multi-user security bounds in the standard model can be obtained by setting the number of ideal cipher queries to 0.

For the tightness of the security bounds, we have the following results (see also Table 1):

1. We prove $n$-bit MAC security of EWCDM and $F^{\mathrm{EDM}}_{B_3}$ in the nonce respecting setting. More precisely, EWCDM and $F^{\mathrm{EDM}}_{B_3}$ are secure up to $O(2^n)$ MAC queries and $O(2^n)$ verification queries. It is the first concrete proof of $n$-bit MAC security of EWCDM to the best of our knowledge.
2. We prove that $F^{\mathrm{SoP}}_{B_2}$ and $F^{\mathrm{SoP}}_{B_3}$ are secure up to $O(2^n)$ MAC queries and $O(2^n)$ verification queries in the nonce respecting setting. In addition, we show that $F^{\mathrm{SoP}}_{B_2}$ and $F^{\mathrm{SoP}}_{B_3}$ are secure up to $O(2^n/\mu)$ MAC queries and $O(2^n)$ verification queries when the adversary makes $\mu$ faulty queries. Compared to the previous analysis, it enjoys stronger provable security when $\mu \leq O(2^{n/4})$. However, for these constructions, the underlying hash function should have a multi-xor-collision resistance property. As a concrete example, we show that CBC-MAC [18] is multi-xor-collision resistant.
3. We present a matching universal forgery attack on $F^{\mathrm{EDM}}_{B_4}$ and $F^{\mathrm{EDM}}_{B_4}$ using $O(2^{3n/4})$ MAC queries and $O(1)$ verification query without using repeated nonces. Since $F^{\mathrm{EDM}}_{B_4}$ and $F^{\mathrm{EDM}}_{B_4}$ are provably secure up to $O(2^{3n/4})$ queries when $\mu < O(2^{n/2})$, they achieve tight $\frac{3n}{4}$-bit security within the range of $\mu$. The core idea of this attack is to find four query-answer pairs $(N_1, M_1, T_1)$, $(N_2, M_2, T_2)$, $(N_3, M_3, T_3)$, and $(N_4, M_4, T_4)$ satisfying the following conditions:

$$\begin{aligned}
&N_1 \oplus H_{K_h}(M_1) = N_2 \oplus H_{K_h}(M_2),\\
&T_2 = T_3,\\
&N_3 \oplus H_{K_h}(M_3) = N_4 \oplus H_{K_h}(M_4),\\
&T_1 = T_4,\\
&N_1 \oplus N_2 \oplus N_3 \oplus N_4 = \mathbf{0}.
\end{aligned}$$

   By repeating a nonce $O(2^{n/2})$ times, one can find such pairs with high probability. On the other hand, in the nonce-respecting setting, one can choose a well-structured set of nonces. From such pairs, a forgery is made with high probability.

Table 1: Security of MAC constructions where $\mu$ is the number of faulty nonces and $n$ is the block size. NR (resp. NM) denotes security in the nonce respecting (resp. misuse) setting. CR and MCR denote xor-collision resistance and multi-xor-collision resistance, respectively.

| MAC | NR | NM | Tightness | Hash assumption | References |
|---|---|---|---|---|---|
| WC | $2^n$ | 0 | tight | CR | [29] |
| EWCDM | $2^{3n/4}$ | $2^{n/2}$ | - | CR | [12,13] |
| $F_{B_3}^{\mathrm{EDM}}$ | $2^{3n/4}$ | $2^{n/2}$ | - | CR | [9] |
| $F_{B_2}^{\mathrm{SoP}}$ | $2^{3n/4}$ | $2^{3n/4}$ ($\mu \leq 2^{n/4}$) | - | CR | [9] |
| $F_{B_3}^{\mathrm{SoP}}$ | $2^{3n/4}$ | $2^{3n/4}$ ($\mu \leq 2^{n/4}$) | - | CR | [9] |
| $F_{B_4}^{\mathrm{EDM}}$ | $2^{3n/4}$ | $2^{3n/4}$ ($\mu < 2^{n/2}$) | **tight** | CR | [9], Section 6 |
| $F_{B_5}^{\mathrm{EDM}}$ | $2^{3n/4}$ | $2^{3n/4}$ ($\mu < 2^{n/2}$) | **tight** | CR | [9], Section 6 |
| EWCDM | $\mathbf{2^n}$ | $\mathbf{2^{n/2}}$ | **tight** | CR | Section 4 |
| $F_{B_3}^{\mathrm{EDM}}$ | $\mathbf{2^n}$ | $\mathbf{2^{n/2}}$ | **tight** | CR | Section 4 |
| $F_{B_2}^{\mathrm{SoP}}$ | $\mathbf{2^n}$ | $\mathbf{2^n/\mu}$ ($\mu \leq 2^{n/2}$) | **tight (NR)** | MCR | Section 5 |
| $F_{B_3}^{\mathrm{SoP}}$ | $\mathbf{2^n}$ | $\mathbf{2^n/\mu}$ ($\mu \leq 2^{n/2}$) | **tight (NR)** | MCR | Section 5 |

As a proof strategy, we first extend a two-permutation version of Mirror theory to a wider range of $\xi_{\max}$, and then give a generic extension of Mirror theory for equation systems and Mirror theory for equation and inequality systems.

The main tool of our security proof is Mirror theory, which systematically estimates the number of solutions to a system of equations of the form $X_i \oplus X_j = \lambda_{i,j}$ such that $X_1, \ldots, X_q$ are pairwise distinct. Recently, Cogliati *et al.* [11] presented the complete proof of Mirror theory for a wide range of $\xi_{\max}$, where $\xi_{\max}$ denotes the maximum component size when a system of equations is represented by a graph. However, we cannot directly apply their result to our problem; since our target constructions are based on two independent permutations, all variables are not necessarily pairwise distinct. To address this case, we divide the set of variables $\mathcal{V}$ into $\mathcal{V}_1$ and $\mathcal{V}_2$ where $\mathcal{V} = \mathcal{V}_1 \sqcup \mathcal{V}_2$. Then, we estimate the number of solutions to a system of equations such that only the variables in $\mathcal{V}_1$ (or $\mathcal{V}_2$) are pairwise distinct. By letting $\mathcal{V}_1 = \mathcal{V}$ and $\mathcal{V}_2 = \emptyset$, one can recover the Mirror theory for a single permutation. Even with $n$-bit Mirror theory for independent permutations, the security proof is not immediate. It is not trivial to prove MAC security (also called "unforgeability") from regular Mirror theory. We propose a generic method for deriving extended Mirror theory from a regular Mirror theory. With our modular approach, we can apply regular Mirror theory to the extended Mirror theory, which is much simpler than proving the extended Mirror theory directly.

When it comes to $F_{B_2}^{\mathrm{SoP}}$ and $F_{B_3}^{\mathrm{SoP}}$, the underlying hash function is required to satisfy the multi-xor-collision resistance property. We prove multi-xor-collision resistance of CBC-MAC which is one of ISO standards using the well-known

structure graph technique [3,20,27]. We believe other MACs of ISO/IEC 9797-1 can be proved similarly since they have the same iteration algorithm.

## 2 Preliminaries

NOTATION. Throughout this paper, we fix positive integers $n$ to denote the block size. We denote $0^n$ (i.e., $n$-bit string of all zeros) by $\mathbf{0}$. The set $\{0,1\}^n$ is sometimes regarded as a set of integers $\{0,1,\ldots,2^n-1\}$ by converting an $n$-bit string $a_{n-1}\ldots a_1 a_0 \in \{0,1\}^n$ to an integer $a_{n-1}2^{n-1}+\cdots+a_1 2+a_0$. We also identify $\{0,1\}^n$ with a finite field $\mathbf{GF}(2^n)$ with $2^n$ elements. For a positive integer $q$, we write $[q]=\{1,\ldots,q\}$.

Given a non-empty finite set $\mathcal{X}$, $x \leftarrow_{\$} \mathcal{X}$ denotes that $x$ is chosen uniformly at random from $\mathcal{X}$. $|\mathcal{X}|$ means the number of elements in $\mathcal{X}$. The set of all permutations of $\{0,1\}^n$ is simply denoted $\mathsf{Perm}(n)$. For some positive integer $m$, the set of all functions with domain $\{0,1\}^n$ and codomain $\{0,1\}^m$ is simply denoted by $\mathsf{Func}(n,m)$. For a keyed function $F:\mathcal{K}\times\mathcal{X}\to\mathcal{Y}$ with key space $\mathcal{K}$ and non-empty sets $\mathcal{X}$ and $\mathcal{Y}$, we will denote $F(K,\cdot)$ by $F_K(\cdot)$ for $K\in\mathcal{K}$. The set of all sequences that consist of $b$ pairwise distinct elements of $\mathcal{X}$ is denoted $\mathcal{X}^{*b}$. For integers $1\le b\le a$, we will write $(a)_b = a(a-1)\cdots(a-b+1)$ and $(a)_0=1$ by convention. If $|\mathcal{X}|=a$, then $(a)_b$ becomes the size of $\mathcal{X}^{*b}$.

When two sets $\mathcal{X}$ and $\mathcal{Y}$ are disjoint, their (disjoint) union is denoted $\mathcal{X}\sqcup\mathcal{Y}$.

HASH FUNCTION. Let $\mathcal{K}_h$ and $\mathcal{X}$ be two non-empty finite sets and $H:\mathcal{K}_h\times\mathcal{X}\to\{0,1\}^n$ be the hash function. Then,

1. $H$ is said to be an *$\epsilon$-almost xor universal* (AXU) hash function, if for any distinct $x,x'\in\mathcal{X}$ and $y\in\{0,1\}^n$,
$$\Pr\left[K_h \leftarrow_{\$} \mathcal{K}_h : H_{K_h}(x)\oplus H_{K_h}(x')=y\right]\le\epsilon.$$
2. $H$ is said to be an *$(k,\epsilon)$-almost xor universal* (AXU) hash function, if for any distinct $x_1,\ldots,x_k\in\mathcal{X}$ and distinct $y_1,\ldots,y_k\in\{0,1\}^n$,
$$\Pr\left[K_h \leftarrow_{\$} \mathcal{K}_h : H_{K_h}(x_1)\oplus y_1=\cdots=H_{K_h}(x_k)\oplus y_k\right]\le\epsilon.$$

BLOCK CIPHER. Let $E:\mathcal{K}\times\{0,1\}^n\to\{0,1\}^n$ be an $n$-bit block cipher with key space $\mathcal{K}$. We will consider an information-theoretic distinguisher $\mathcal{A}$ that makes oracle queries to $E$, and returns a single bit. The advantage of $\mathcal{A}$ in breaking the $\mathsf{prp}$ security of $E$ is defined as
$$\mathbf{Adv}^{\mathsf{prp}}_E(\mathcal{A}) = \left|\Pr\left[K\leftarrow_{\$}\mathcal{K}:\mathcal{A}^{\mathsf{E}_K}=1\right]-\Pr\left[\mathsf{P}\leftarrow_{\$}\mathsf{Perm}(n):\mathcal{A}^{\mathsf{P}}=1\right]\right|.$$
We define $\mathbf{Adv}^{\mathsf{prp}}_E(\mu,q,t)$ as the maximum of $\mathbf{Adv}^{\mathsf{prp}}_E(\mathcal{A})$ over all the distinguishers against $E$ making at most $q$ queries and running in time at most $t$. When considering information-theoretic security, we will drop the parameter $t$.

NONCE-BASED PSEUDORANDOM FUNCTION. Let $F:\mathcal{K}\times\mathcal{N}\times\{0,1\}^*\to\{0,1\}^n$ be a nonce-based keyed function with key space $\mathcal{K}$ and nonce space $\mathcal{N}$. We will

consider an information-theoretic distinguisher $\mathcal{A}$ that makes oracle queries to $F$, and returns a single bit. The advantage of $\mathcal{A}$ in breaking the $\mathsf{prf}$ security of $F$, i.e., in distinguishing $F_K$ where $K \leftarrow_{\$} \mathcal{K}$ from the random oracle $\mathsf{Rand}$, is defined as

$$\mathbf{Adv}_F^{\mathsf{prf}}(\mathcal{A}) = \left|\Pr\left[K \leftarrow_{\$} \mathcal{K} : \mathcal{A}^{F_K} = 1\right] - \Pr\left[\mathcal{A}^{\mathsf{Rand}} = 1\right]\right|.$$

We define $\mathbf{Adv}_F^{\mathsf{prf}}(\mu, q, t)$ as the maximum of $\mathbf{Adv}_F^{\mathsf{prf}}(\mathcal{A})$ over all the distinguishers against $F$ making at most $q$ queries, at most $\mu$ faulty queries and running in time at most $t$. We also denote $\mathbf{Adv}_F^{\mathsf{prf}}(q, t)$ for $\mathbf{Adv}_F^{\mathsf{prf}}(0, q, t)$. When we consider information theoretic security, we will drop the parameter $t$.

Nonce-based MACs. Given four non-empty sets $\mathcal{K}$, $\mathcal{N}$, $\mathcal{M}$, and $\mathcal{T}$, a nonce-based keyed function with key space $\mathcal{K}$, nonce space $\mathcal{N}$, message space $\mathcal{M}$ and tag space $\mathcal{T}$ is simply a function $F : \mathcal{K} \times \mathcal{N} \times \mathcal{M} \to \mathcal{T}$. Stated otherwise, it is a keyed function whose domain is a cartesian product $\mathcal{N} \times \mathcal{M}$. We denote $F_K(N, M)$ for $F(K, N, M)$.

For $K \in \mathcal{K}$, let $\mathsf{Auth}_K$ be the MAC oracle which takes as input a pair $(N, M) \in \mathcal{N} \times \mathcal{M}$ and returns $F_K(N, M)$, and let $\mathsf{Ver}_K$ be the verification oracle which takes as input a triple $(N, M, T) \in \mathcal{N} \times \mathcal{M} \times \mathcal{T}$ and returns 1 ("accept") if $F_K(N, M) = T$, and 0 ("reject") otherwise. We assume an adversary queries the two oracles $\mathsf{Auth}_K$ and $\mathsf{Ver}_K$ for a secret key $K \in \mathcal{K}$.

A $(\mu, q, v, t)$-adversary against the nonce-based MAC-security of $F$ is an adversary $\mathcal{A}$ with oracle access to oracles $\mathsf{Auth}_K$ and $\mathsf{Ver}_K$, making at most $q$ MAC queries to $\mathsf{Auth}$ oracle, at most $\mu$ faulty queries, at most $v$ verification queries to $\mathsf{Ver}$ oracle, and running in time at most $t$. We say that $\mathcal{A}$ forges if any of its queries to $\mathsf{Ver}_K$ returns 1. The advantage of $\mathcal{A}$ against the nonce-based MAC security of $F$ is defined as

$$\mathbf{Adv}_F^{\mathsf{mac}}(\mathcal{A}) = \Pr\left[K \leftarrow_{\$} \mathcal{K} : \mathcal{A}^{\mathsf{Auth}_K, \mathsf{Ver}_K} \text{forges}\right].$$

where the probability is also taken over the random coins of $\mathcal{A}$, if any. $\mathcal{A}$ is not allowed to ask a verification query $(N, M, T)$ to $\mathsf{Ver}_K$ if a previous query $(N, M)$ to $\mathsf{Auth}_K$ returned $T$. When $\mu = 0$, we say that $\mathcal{A}$ is nonce-respecting, otherwise, $\mathcal{A}$ is said nonce-misusing. However, the adversary is allowed to repeat nonces in its verification queries.

We define $\mathbf{Adv}_F^{\mathsf{mac}}(\mu, q, v, t)$ as the maximum of $\mathbf{Adv}_F^{\mathsf{mac}}(\mathcal{A})$ over all $(\mu, q, v, t)$-adversaries. We also define $\mathbf{Adv}_F^{\mathsf{mac}}(q, v, t)$ as the maximum of $\mathbf{Adv}_F^{\mathsf{mac}}(\mathcal{A})$ over all $(0, q, v, t)$-adversaries. When we consider information-theoretic security, we will drop the parameter $t$.

We obtain an upper bound for the forging advantage of $F$ in terms of distinguishing advantage, where the ideal world is comprised of a random oracle $\mathsf{Rand}$ and the reject oracle $\mathsf{Rej}$ that always returns 0 for any verification query. For any $(\mu, q, v, t)$-adversary $\mathcal{A}$, $\mathbf{Adv}_F^{\mathsf{mac}}(\mathcal{A})$ is upper bounded by

$$\max_{\mathcal{A}} \left|\Pr\left[K \leftarrow_{\$} \mathcal{K} : \mathcal{A}^{\mathsf{Auth}_K, \mathsf{Ver}_K} = 1\right] - \Pr\left[\mathcal{A}^{\mathsf{Rand}, \mathsf{Rej}} = 1\right]\right|.$$

### 2.1 Coefficient-H Technique

We will use Patarin's coefficient-H technique. The goal of this technique is to upper bound the adversarial distinguishing advantage between a real construction and its ideal counterpart. In the ideal and the real worlds, an information-theoretic adversary $\mathcal{A}$ is allowed to make $q$ queries to certain oracles (with the same oracle interfaces), denoted $\mathcal{S}_0$ and $\mathcal{S}_1$, respectively. The interaction between the adversary $\mathcal{A}$ and the oracle determines a "transcript" $\tau \in \Omega^q$; it contains all the information obtained by $\mathcal{A}$ during the interaction. We call a transcript $\tau$ *attainable* if the probability of obtaining $\tau$ in the ideal world is non-zero.

We partition the set of attainable transcripts $\Theta$ into a set of "good" transcripts $\Theta_{\mathsf{good}}$ such that the probabilities of obtaining some transcript $\tau \in \Theta_{\mathsf{good}}$ are close in the real world and the ideal world, and a set $\Theta_{\mathsf{bad}}$ of "bad" transcripts such that the probability of obtaining any $\tau \in \Theta_{\mathsf{bad}}$ is small in the ideal world. The coefficient-H technique is summarized in the following lemma.

**Lemma 1.** *Let $\Theta = \Theta_{\mathsf{good}} \sqcup \Theta_{\mathsf{bad}}$ be a partition of the set of attainable transcripts, where there exists a non-negative $\epsilon_1$ such that for any $\tau \in \Theta_{\mathsf{good}}$,*

$$\frac{\mathsf{p}^q_{\mathcal{S}_1}(\tau)}{\mathsf{p}^q_{\mathcal{S}_0}(\tau)} \geq 1 - \epsilon_1,$$

*and there exists $\epsilon_2$ such that $\sum_{\tau \in \Theta_{\mathsf{bad}}} \mathsf{p}^q_{\mathcal{S}_0}(\tau) \leq \epsilon_2$. Then,*

$$\sum_{\tau \in \Theta} \max\left\{0, \mathsf{p}^q_{\mathcal{S}_0}(\tau) - \mathsf{p}^q_{\mathcal{S}_1}(\tau)\right\} \leq \epsilon_1 + \epsilon_2.$$

*Proof.* We have

$$\begin{aligned}
\sum_{\tau \in \Theta} \max\left\{0, \mathsf{p}^q_{\mathcal{S}_0}(\tau) - \mathsf{p}^q_{\mathcal{S}_1}(\tau)\right\} &= \sum_{\substack{\tau \in \Theta \\ \mathsf{p}^q_{\mathcal{S}_0}(\tau) > \mathsf{p}^q_{\mathcal{S}_1}(\tau)}} \left(\mathsf{p}^q_{\mathcal{S}_0}(\tau) - \mathsf{p}^q_{\mathcal{S}_1}(\tau)\right) \\
&= \sum_{\substack{\tau \in \Theta \\ \mathsf{p}^q_{\mathcal{S}_0}(\tau) > \mathsf{p}^q_{\mathcal{S}_1}(\tau)}} \mathsf{p}^q_{\mathcal{S}_0}(\tau) \left(1 - \frac{\mathsf{p}^q_{\mathcal{S}_1}(\tau)}{\mathsf{p}^q_{\mathcal{S}_0}(\tau)}\right) \\
&\leq \sum_{\tau \in \Theta_{\mathsf{good}}} \mathsf{p}^q_{\mathcal{S}_0}(\tau)\epsilon_1 + \sum_{\tau \in \Theta_{\mathsf{bad}}} \mathsf{p}^q_{\mathcal{S}_0}(\tau) \\
&\leq \epsilon_1 + \epsilon_2.
\end{aligned}$$

□

## 3 Mirror Theory

Patarin's Mirror theory [25,26] has been a valuable tool for proving PRF security and MAC security. However, the original proof provided by Patarin is complex and hard to verify, containing several gaps. Recently, Cogliati *et al.* [11] presented the complete proof of Mirror theory for a wide range of $\xi_{\max}$. Nevertheless, there

are limitations when it comes to proving the security of our target MACs using the Mirror theory in [11]. This is because the Mirror theory focuses on a single permutation. To address this limitation, we refine the Mirror theory to cover constructions based on two independent permutations, allowing us to analyze the security of two permutation-based constructions. Additionally, we need to extend the Mirror theory to include inequalities for MAC security. This extended version is known as "Extended Mirror theory".

### 3.1 Extended Mirror Theory for Two Independent Permutations

The goal of this section is to compute a lower bound of the number of solutions to a certain type of system of equations and inequalities.

We consider a system of equations and inequalities $\gamma = (\gamma^{=}, \gamma^{\neq})$, which is divided into a system of equations $\gamma^{=}$ and a system of inequalities $\gamma^{\neq}$. A set of variables $\mathcal{V}$ is partitioned into $\mathcal{V}_1 \sqcup \mathcal{V}_2$. Intuitively, variables in $\mathcal{V}_1$ come from one permutation and ones in $\mathcal{V}_2$ are results of the other permutation. In this section, we assume that they are arbitrarily partitioned. So, the variables in $\mathcal{V}_1$ (or $\mathcal{V}_2$) should be distinct. We use the notion $X \sim Y$ to indicate that $X$ and $Y$ belong to the same subset. Additional constraints are imposed on $\gamma$ as follows: If $X \sim Y$, then $X \neq Y$.

Fix a positive integer $c$. For $1 \leq i \leq c$ and a positive integer $\xi_i > 1$, the system of equations as $\gamma^{=}$ is represented as:

$$\gamma^{=} : \begin{cases} X_{1,0} \oplus X_{1,1} = \lambda_{1,1}, \ldots, X_{1,0} \oplus X_{1,\xi_1-1} = \lambda_{1,\xi_1-1}, \\ \qquad\qquad \vdots \\ X_{c,0} \oplus X_{c,1} = \lambda_{c,1}, \ldots, X_{c,0} \oplus X_{c,\xi_c-1} = \lambda_{c,\xi_c-1} \end{cases}$$

where $\lambda_{\alpha,i} \in \{0,1\}^n$ for $1 \leq \alpha \leq c$ and $0 \leq i \leq \xi_\alpha - 1$. The set of variables on $\gamma^{=}$ is denoted as $\mathcal{V}^{=}$ and we define $\mathcal{V}_1^{=} =^{\text{def}} \mathcal{V}^{=} \cap \mathcal{V}_1$ and $\mathcal{V}_2^{=} =^{\text{def}} \mathcal{V}^{=} \cap \mathcal{V}_2$. We also define $\mathcal{V}^{\neq} =^{\text{def}} \mathcal{V} \setminus \mathcal{V}^{=}$, $\mathcal{V}_1^{\neq} =^{\text{def}} \mathcal{V}^{\neq} \cap \mathcal{V}_1$ and $\mathcal{V}_2^{\neq} =^{\text{def}} \mathcal{V}^{\neq} \cap \mathcal{V}_2$. The set of variables $\mathcal{V}^{=}$ consists of $c$ components, and for $i \in [c]$, the $i$-th component takes form of $\{X_{i,0}, \ldots, X_{i,\xi_i-1}\}$. The largest number of components is denoted as $\xi_{\max}$, where $\xi_{\max} = \max_{i \in [c]} \{\xi_i\}$.

We separately establish a system of inequalities with $\gamma^{=}$. For a non-negative integer $v$, we denote

$$\gamma^{\neq} : \begin{cases} X'_1 \oplus X'_2 \neq \lambda'_1, \\ X'_3 \oplus X'_4 \neq \lambda'_2, \\ \qquad\vdots \\ X'_{2v-1} \oplus X'_{2v} \neq \lambda'_v \end{cases}$$

where $\lambda'_i \in \{0,1\}^n$ for $1 \leq i \leq v$. It is assumed that, for some $i$, $X'_i$ can be identified as an element of $\mathcal{V}^{=}$ or another element of $\mathcal{V}^{\neq}$. This identification is publicly known and can be denoted as a relation $\sim_{\mathsf{eq}}$, i.e., $X'_i \sim_{\mathsf{eq}} X_{j,k} \Leftrightarrow X'_i = X_{j,k}$ and $X'_i \sim_{\mathsf{eq}} X'_j \Leftrightarrow X'_i = X'_j$.

In this section, we express the system of equations and inequalities with relation $\sim$ and $\sim_{\mathsf{eq}}$; denoted as $\Gamma =^{\text{def}} (\gamma^{=}, \gamma^{\neq}, \sim, \sim_{\mathsf{eq}})$. $h(\Gamma)$ denotes the number of solutions to $\gamma$ subject to the above constraints.

In this work, we focus on a system $\Gamma$ with non-degeneracy properties, as outlined below:

1. $\lambda_{\alpha,i} \neq 0$ for all $\alpha \in [c]$ and $i \in [\xi_\alpha - 1]$ such that $X_{\alpha,0} \sim X_{\alpha,i}$.
2. $\lambda_{\alpha,i} \neq \lambda_{\alpha,j}$ for all $\alpha \in [c]$ and distinct $i, j \in [\xi_\alpha - 1]$ such that $X_{\alpha,i} \sim X_{\alpha,j}$.
3. There is no $(\alpha, \beta, i, j)$ such that $\gamma^{=}$ contains $X_{\alpha,i} \oplus X_{\alpha,j} = \lambda'_\beta$ and $\gamma^{\neq}$ contains $X_{\alpha,i} \oplus X_{\alpha,j} \neq \lambda'_\beta$.

We refer to any system $\Gamma$ satisfying the above properties as a *nice* system. The following theorem provides a lower bound of $h(\Gamma)$ for a nice system $\Gamma$.

**Theorem 1.** *Let $(\Gamma)$ be a nice system over $\{0,1\}^n$ such that the number of equations is $q$ and the number of inequalities is $v$. Suppose the number of variables in the largest component of $\gamma^{=}$ is $\xi_{\max}$. If $\xi_{\max}^2 n + \xi_{\max} \leq 2^{n/2}$, $q\xi_{\max}^2 \leq \frac{2^n}{12}$ and $q + v \leq 2^{n-1}$, one has*

$$h(\Gamma) \geq \frac{(2^n - 2)_{|\mathcal{V}_1|}(2^n - 2)_{|\mathcal{V}_2|}}{2^{nq}} \left(1 - \frac{2v}{2^n}\right).$$

### 3.2 Mirror Theory with Equations

We first estimate the number of solutions for a system of equations. Let $\Gamma^{=}$ be a system of equations $\gamma^{=}$ with relation $\sim$ and $h(\Gamma^{=})$ be the number of solutions to $\Gamma^{=}$. We can prove the following theorem.

**Theorem 2.** *Let $\Gamma^{=}$ be a nice system over $\{0,1\}^n$ such that the number of equations is $q$. Suppose the number of variables in the largest component of $\Gamma^{=}$ is $\xi_{\max}$. If $\xi_{\max}^2 n + \xi_{\max} \leq 2^{n/2}$ and $q\xi_{\max}^2 \leq \frac{2^n}{12}$, one has*

$$h(\Gamma^{=}) \geq \frac{(2^n - 2)_{|\mathcal{V}_1^{=}|}(2^n - 2)_{|\mathcal{V}_2^{=}|}}{2^{nq}}.$$

The proof of Theorem 2 is rather complicated so we will defer the proof to the Supplementary Material.

### 3.3 Generalization of Extended Mirror Theory

Mirror theory is later generalized to *extended* Mirror theory [14,15], by including inequalities in the system. The extended Mirror theory systematically estimates the number of solutions to a system of equations and inequalities. On the other hand, the goal of this section is slightly different: we will estimate *the ratio* between two quantities:

1. The number of solutions to a system of equations.
2. The number of solutions to a system of equations and inequalities.

This approach separates the counting of inequalities from (equations-only) Mirror theory, eliminating the need for developing the Extended Mirror theory each time whenever there is an improvement of Mirror theory.

When a given system $\Gamma$ is nice, we can compute a lower bound on the ratio

$$\frac{h(\Gamma)}{h(\Gamma^{=})}$$

as follows.

**Lemma 2.** *Let $\Gamma$ be a nice system over $\{0,1\}^n$ such that the number of equations is $q$ and the number of inequalities is $v$. If $q+v \le 2^{n-1}$, one has*

$$\frac{h(\Gamma)}{h(\Gamma^{=})(2^n-|\mathcal{V}_1^{=}|)_{|\mathcal{V}_1^{\neq}|}(2^n-|\mathcal{V}_2^{=}|)_{|\mathcal{V}_2^{\neq}|}} \ge 1-\frac{2v}{2^n}.$$

*Proof (of Lemma 2).* Let $\Gamma_0 = \Gamma^{=}$ and $\Gamma_i = \Gamma_{i-1} \sqcup \{X'_{2i-1} \oplus X'_{2i} \neq \lambda'_i\}$ for $i \in [v]$. We additionally define $\Gamma'_i = \Gamma_{i-1} \sqcup \{X'_{2i-1} \oplus X'_{2i} = \lambda'_i\}$ for $i \in [v]$. Then, we have

$$h(\Gamma_{i+1}) = h(\Gamma_i) - h(\Gamma'_{i+1}). \tag{1}$$

If both $X'_{2i-1}$ and $X'_{2i}$ are in $\mathcal{V}^{=}$, then $\Gamma'_{i+1}$ contradicts, i.e., $h(\Gamma'_{i+1}) = 0$ since $\Gamma_{i+1}$ is nice. Thus, $h(\Gamma_{i+1}) = h(\Gamma_i)$.

Now, we suppose that $X'_{2i-1}$ or $X'_{2i}$ is not in $\mathcal{V}^{=}$. The number of possible assignments of distinct values outside $\mathcal{V}^{=}$ to the variables in $\mathcal{V}^{\neq}$ is $(2^n - |\mathcal{V}_1^{=}|)_{|\mathcal{V}_1^{\neq}|}(2^n-|\mathcal{V}_2^{=}|)_{|\mathcal{V}_2^{\neq}|}$. Among these assignments, it violates the inequality conditions when $X'_{2i-1} \oplus X'_{2i} = \lambda'_i$ for each $i \in [v]$. These assignments are at most

$$A \stackrel{\text{def}}{=} \max\left\{(2^n-|\mathcal{V}_1^{=}|)_{|\mathcal{V}_1^{\neq}|-1}(2^n-|\mathcal{V}_2^{=}|)_{|\mathcal{V}_2^{\neq}|}, (2^n-|\mathcal{V}_1^{=}|)_{|\mathcal{V}_1^{\neq}|}(2^n-|\mathcal{V}_2^{=}|)_{|\mathcal{V}_2^{\neq}|-1}\right\}.$$

Therefore, we have

$$\frac{h(\Gamma)}{h(\Gamma^{=})} \ge (2^n-|\mathcal{V}_1^{=}|)_{|\mathcal{V}_1^{\neq}|}(2^n-|\mathcal{V}_2^{=}|)_{|\mathcal{V}_2^{\neq}|} - vA$$

which means

$$\frac{h(\Gamma)}{h(\Gamma^{=})(2^n-|\mathcal{V}_1^{=}|)_{|\mathcal{V}_1^{\neq}|}(2^n-|\mathcal{V}_2^{=}|)_{|\mathcal{V}_2^{\neq}|}} \ge 1-\frac{2v}{2^n}.$$

It concludes the proof. □

By combining Theorem 2 and Lemma 2, Thorem 1 can be proved as

$$\begin{aligned} h(\Gamma) &\ge h(\Gamma^{=})(2^n-|\mathcal{V}_1^{=}|)_{|\mathcal{V}_1^{\neq}|}(2^n-|\mathcal{V}_2^{=}|)_{|\mathcal{V}_2^{\neq}|}\left(1-\frac{2v}{2^n}\right) \\ &\ge \frac{(2^n-2)_{|\mathcal{V}_1^{=}|}(2^n-2)_{|\mathcal{V}_2^{=}|}}{2^{nq}} \cdot (2^n-|\mathcal{V}_1^{=}|)_{|\mathcal{V}_1^{\neq}|}(2^n-|\mathcal{V}_2^{=}|)_{|\mathcal{V}_2^{\neq}|}\left(1-\frac{2v}{2^n}\right) \\ &\ge \frac{(2^n-2)_{|\mathcal{V}_1|}(2^n-2)_{|\mathcal{V}_2|}}{2^{nq}}\left(1-\frac{2v}{2^n}\right). \end{aligned}$$

## 4 Security of EWCDM and $F^{\mathrm{EDM}}_{B_3}$

In this section, we consider $\mathsf{EWCDM}[H,E]$ and $F^{\mathrm{EDM}}_{B_3}[H,E]$ based on an $n$-bit $\epsilon$-AXU hash function $H$ and an $n$-bit block cipher $E$. For given $n$-bit nonce $N$ and a message $M$, the user receives a tag as

$$\mathsf{EWCDM}[H,E](N,M) = E_{K_2}(H_{K_h}(M) \oplus E_{K_1}(N) \oplus N)$$

and

$$F^{\mathrm{EDM}}_{B_3}[H,E](N,M) = E_{K_2}(H_{K_h}(M) \oplus E_{K_1}(N) \oplus N) \oplus H_{K_h}(M)$$

by a hash key $K_h$ and block cipher keys $K_1$ and $K_2$. The goal of this section is to prove the security of $\mathsf{EWCDM}[H,E]$ and $F^{\mathrm{EDM}}_{B_3}[H,E]$. As a result, we have the following theorem.

**Theorem 3.** *Let $n \geq 30$, $\epsilon > 0$, $H : \mathcal{K}_h \times \{0,1\}^* \to \{0,1\}^n$ be an $\epsilon$-AXU hash function, and $E : \mathcal{K} \times \{0,1\}^n \to \{0,1\}^n$ be a block cipher. Let $q, v, t$ be nonnegative integers such that $q + v \leq 2^{n-1}$. Then, one has*

$$\mathbf{Adv}^{\mathsf{mac}}_{\mathsf{EWCDM}[H,E]}(q,v,t) \leq \frac{6q}{2^n} + \frac{q^2\epsilon}{2^n} + \frac{6v}{2^n} + v\epsilon + 2\mathbf{Adv}^{\mathsf{prp}}_E(q+v, t+t').$$

*where $t'$ is the time complexity necessary to compute $E$ for $q + v$ times.*

Since adding $H_{K_h}(M)$ to the tag does not make any significant difference, the MAC security of $F^{\mathrm{EDM}}_{B_3}$ follows immediately.

**Corollary 1.** *Let $n \geq 30$, $\epsilon > 0$, $H : \mathcal{K}_h \times \{0,1\}^* \to \{0,1\}^n$ be an $\epsilon$-AXU hash function, and $E : \mathcal{K} \times \{0,1\}^n \to \{0,1\}^n$ be a block cipher. Let $q, v, t$ be nonnegative integers such that $q + v \leq 2^{n-1}$. Then, one has*

$$\mathbf{Adv}^{\mathsf{mac}}_{F^{EDM}_{B_3}[H,E]}(q,v,t) \leq \frac{6q}{2^n} + \frac{q^2\epsilon}{2^n} + \frac{6v}{2^n} + v\epsilon + 2\mathbf{Adv}^{\mathsf{prp}}_E(q+v, t+t').$$

*where $t'$ is the time complexity necessary to compute $E$ for $q + v$ times.*

### 4.1 Proof of Theorem 3

We assume that the adversary is deterministic and never repeats a prior query. Assume further that the adversary never makes a redundant query. Up to the $\mathsf{prp}$-security of $E$, keyed block ciphers $E_{K_1}$ and $E_{K_2}$ can be replaced by truly random permutations $P_1$ and $P_2^{-1}$, respectively. The cost of this replacement is upper bounded by

$$2\mathbf{Adv}^{\mathsf{prp}}_E(q+v, t+t').$$

The resulting construction denotes $\mathsf{EWCDM}^*[H]$.

At the end of the interaction between an adversary and the oracle, additional information is freely given to an adversary, and a transcript is defined as a pair of query-answer pairs and additional information $K_h$. In the real world, $K_h$ is the hash key used in EWCDM. In the ideal world, $K_h$ is uniformly randomly chosen after the end of the interaction between an adversary and the oracle. Without loss of generality, we rearrange query indices so that verification queries come after MAC queries. Let $\Theta$ be the set of all attainable transcripts in the ideal world and $\tau = (\tau_m, \tau_v, K_h) \in \Theta$ be a transcript where $\tau_m$ and $\tau_v$ denote the list of MAC queries and the list of verification queries, i.e.,

$$\tau_m = \{(N_1, M_1, T_1), \ldots, (N_q, M_q, T_q)\},$$
$$\tau_v = \{(N_{q+1}, M_{q+1}, T_{q+1}, b_{q+1}), \ldots, (N_{q+v}, M_{q+v}, T_{q+v}, b_{q+v})\}.$$

From a transcript $\tau$, $\mathcal{A}$ can compute $X_i = H_{K_h}(M_i) \oplus N_i$ for $i \in [q+v]$ before outputting its decision bit.

This proof utilizes the extended Mirror theory stated in Theorem 1 and the coefficient-H technique stated in Lemma 1. The core of the security proof is to estimate the number of possible ways of fixing evaluations $P_1$ and $P_2$ in a way that

$$X_i = P_1(N_i) \oplus P_2(T_i)$$

for $i = 1, \ldots, q$ and

$$X_i \neq P_1(N_i) \oplus P_2(T_i)$$

for $i = q+1, \ldots, q+v$. We will identify $\mathcal{V}_1 = \{P_1(N_i)\}$ and $\mathcal{V}_2 = \{P_2(T_i)\}$ with as sets of variables. We also define $\mathcal{V} = \mathcal{V}_1 \sqcup \mathcal{V}_2$. Then we can construct the system of equations $\Gamma_\tau$ as defined in Section 3. To satisfy the conditions in Theorem 1, we must first define bad events on a transcript $\tau$, and then we can apply the extended Mirror theory to each transcript that the bad event does not happen.

*Defining and Bounding Bad Events.* A transcript $\tau = (\tau_m, \tau_v, K_h)$ is defined as *bad* if one of the following condition holds.

- $\mathsf{bad}_1 \Leftrightarrow$ there exists $(i_1, \ldots, i_n) \in [q]^{*n}$ such that $T_{i_1} = \cdots = T_{i_n}$.
- $\mathsf{bad}_2 \Leftrightarrow$ there exists $(i, j) \in [q]^{*2}$ such that $T_i = T_j$ and $X_i = X_j$.
- $\mathsf{bad}_3 \Leftrightarrow$ there exists $(i, j) \in [q] \times [q+1, q+v]$ such that $N_i = N_j, T_i = T_j,$ and $X_i = X_j$.

If a transcript $\tau$ is not bad, then it will be called a *good* transcript. The probability that the bad event occurs is obtained as follows:

- Since the tag is random in the ideal world, we have

$$\Pr[\mathsf{bad}_1] = \frac{\binom{q}{n}}{(2^n)^{n-1}} \leq \left(\frac{2q}{2^n}\right)^n \leq \frac{2q}{2^n}$$

since $q \le 2^{n-1}$ and

$$\Pr[\mathsf{bad}_2] \le \frac{q^2\epsilon}{2^n}.$$

– For each $j \in [q+1, q+v]$, there is at most one $i \in [q]$ such that $N_i = N_j$. For such pair $(i,j)$, one has $\Pr[X_i = X_j] \le \epsilon$. Therefore, we have

$$\Pr[\mathsf{bad}_3] \le v\epsilon.$$

Therefore, we have

$$\Pr[\mathsf{bad}] \le \Pr[\mathsf{bad}_1] + \Pr[\mathsf{bad}_2] + \Pr[\mathsf{bad}_3] \le \frac{2q}{2^n} + \frac{q^2\epsilon}{2^n} + v\epsilon. \tag{2}$$

*Good Transcript Analysis.* For a good transcript $\tau$ and its system $\Gamma_\tau$, by assuming nonces are not repeated, we observe that

– $\Gamma_\tau$ is nice by $\neg(\mathsf{bad}_2 \vee \mathsf{bad}_3)$;
– $\xi_{\max} \le n+1$ and $\xi_{\max}^2 n + \xi_{max} \le n(n+1)^2 + n + 1 \le 2^{n/2}$ since $n \ge 30$ by $\neg\mathsf{bad}_1$.

Henceforth, we can apply Theorem 1 and then we have

$$h(\Gamma_\tau) \ge \frac{(2^n-2)_{|\mathcal{V}_1|}(2^n-2)_{|\mathcal{V}_2|}}{2^{nq}}\left(1 - \frac{2v}{2^n}\right).$$

Furthermore, we see that

$$\mathsf{p}_{\mathcal{S}_0}^{q+v}(\tau) = \frac{1}{|\mathcal{K}_h|} \cdot \frac{1}{2^{nq}}$$

and

$$\mathsf{p}_{\mathcal{S}_1}^{q+v}(\tau) = \frac{1}{|\mathcal{K}_h|} \cdot \frac{h(\Gamma_\tau)}{(2^n)_{|\mathcal{V}_1|}(2^n)_{|\mathcal{V}_2|}}.$$

From the above, one has

$$\begin{aligned}
\frac{\mathsf{p}_{\mathcal{S}_1}^{q+v}(\tau)}{\mathsf{p}_{\mathcal{S}_0}^{q+v}(\tau)} &= \frac{h(\Gamma_\tau)2^{nq}}{(2^n)_{|\mathcal{V}_1|}(2^n)_{|\mathcal{V}_2|}} \\
&\ge \frac{(2^n-2)_{|\mathcal{V}_1|}(2^n-2)_{|\mathcal{V}_2|}}{(2^n)_{|\mathcal{V}_1|}(2^n)_{|\mathcal{V}_2|}}\left(1 - \frac{2v}{2^n}\right) \\
&= \frac{(2^n-|\mathcal{V}_1|)_2(2^n-|\mathcal{V}_2|)_2}{(2^n)_2(2^n)_2}\left(1 - \frac{2v}{2^n}\right) \\
&\ge \left(1 - \frac{q+v}{2^n}\right)^4\left(1 - \frac{2v}{2^n}\right) \\
&\ge 1 - \frac{4q}{2^n} - \frac{6v}{2^n}
\end{aligned} \tag{3}$$

since $|\mathcal{V}_1|, |\mathcal{V}_2| \le q+v$.

Plugging (2) and (3) to Lemma 1, we conclude that

$$\left\|\mathsf{p}_{\mathcal{S}_0}^{q+v}(\cdot) - \mathsf{p}_{\mathcal{S}_1}^{q+v}(\cdot)\right\| \le \frac{6q}{2^n} + \frac{q^2\epsilon}{2^n} + \frac{6v}{2^n} + v\epsilon.$$

## 5 Security of $F_{B_2}^{\mathrm{SoP}}$ and $F_{B_3}^{\mathrm{SoP}}$

In this section, we consider $F_{B_2}^{\mathrm{SoP}}[H,E]$ and $F_{B_3}^{\mathrm{SoP}}[H,E]$ based on an $n$-bit $(n,\epsilon_n)$-AXU hash function $H$ and an $n$-bit block cipher $E$. For given $n$-bit nonce $N$ and a message $M$, the user receives a tag as

$$E_{K_1}(N) \oplus E_{K_2}(H_{K_h}(M) \oplus N)$$

for $F_{B_2}^{\mathrm{SoP}}[H,E]$, and

$$E_{K_1}(N) \oplus E_{K_2}(H_{K_h}(M) \oplus N) \oplus H_{K_h}(M)$$

for $F_{B_3}^{\mathrm{SoP}}[H,E]$ by a hash key $K_h$ and block cipher keys $K_1$ and $K_2$. This section aims to prove the security of $F_{B_2}^{\mathrm{SoP}}[H,E]$ and $F_{B_3}^{\mathrm{SoP}}$. As a result, we have the following theorem and corollary.

**Theorem 4.** *Let $\epsilon > 0$ and $n \geq 32$. Let $H : \mathcal{K}_h \times \{0,1\}^* \to \{0,1\}^n$ be an $\epsilon$-AXU hash function and $(n,\epsilon_n)$-AXU hash function, and $E : \mathcal{K} \times \{0,1\}^n \to \{0,1\}^n$ be a block cipher. Let $\mu, q, v, t$ be nonnegative integers such that $n\mu \leq 2^{n/4}$, $12(\mu+n+2)^2 q \leq 2^n$ and $q+v \leq 2^{n-1}$. Then, one has*

$$\mathbf{Adv}^{\mathsf{mac}}_{F_{B_2}^{SoP}[H,E]}(\mu,q,v,t) \leq \binom{q}{n}\epsilon_n + 2\mu q\epsilon + \mu^2\epsilon + \frac{\mu^2}{2^n} + \frac{q^2\epsilon}{2^n} + \frac{4q}{2^n} + v\epsilon + \frac{6v}{2^n} + 2\mathbf{Adv}^{\mathsf{prp}}_E(q+v, t+t')$$

*where $t'$ is the time complexity necessary to compute $E$ for $q+v$ times.*

Since adding $H_{K_h}(M)$ to the tag does not make any significant difference, the MAC security of $F_{B_3}^{\mathrm{SoP}}$ follows immediately.

**Corollary 2.** *Let $\epsilon > 0$ and $n \geq 32$. Let $H : \mathcal{K}_h \times \{0,1\}^* \to \{0,1\}^n$ be an $\epsilon$-AXU hash function and $(n,\epsilon_n)$-AXU hash function, and $E : \mathcal{K} \times \{0,1\}^n \to \{0,1\}^n$ be a block cipher. Let $\mu, q, v, t$ be nonnegative integers such that $n\mu \leq 2^{n/4}$, $12(\mu+n+2)^2 q \leq 2^n$ and $q+v \leq 2^{n-1}$. Then, one has*

$$\mathbf{Adv}^{\mathsf{mac}}_{F_{B_3}^{SoP}[H,E]}(\mu,q,v,t) \leq \binom{q}{n}\epsilon_n + 2\mu q\epsilon + \mu^2\epsilon + \frac{\mu^2}{2^n} + \frac{q^2\epsilon}{2^n} + \frac{4q}{2^n} + v\epsilon + \frac{6v}{2^n} + 2\mathbf{Adv}^{\mathsf{prp}}_E(q+v, t+t')$$

*where $t'$ is the time complexity necessary to compute $E$ for $q+v$ times.*

At the last of this section, we prove CBC-MAC is a multi-xor-collision resistant hash function in Lemma 3. When the underlying hash function is instantiated with CBC-MAC, we have the following corollary.

**Corollary 3.** *Let $\epsilon > 0$ and $n \geq 32$. Let $E : \mathcal{K} \times \{0,1\}^n \to \{0,1\}^n$ be a block cipher. Let $\mu, q, v, t$ be nonnegative integers such that $n\mu \leq 2^{n/4}$, $12(\mu+n+2)^2 q \leq$*

*$2^n$ and $q+v \le 2^{n-1}$. Let $n(\ell+1) \le 2^{n-1}$ where $\ell$ be the maximum block length of MAC queries. Then, one has*

$$\mathbf{Adv}^{\mathsf{mac}}_{F^{SoP}_{B_2}[\mathsf{CBC\text{-}MAC},E]}(\mu,q,v,t) \le \frac{q(n\ell+1)^2}{2^n} + 2\mu q\epsilon + \mu^2\epsilon + \frac{\mu^2}{2^n} + \frac{q^2\epsilon}{2^n} + \frac{4q}{2^n} + v\epsilon + \frac{6v}{2^n} + 2\mathbf{Adv}^{\mathsf{prp}}_E(q+v,t+t')$$

*and*

$$\mathbf{Adv}^{\mathsf{mac}}_{F^{SoP}_{B_3}[\mathsf{CBC\text{-}MAC},E]}(\mu,q,v,t) \le \frac{q(n\ell+1)^2}{2^n} + 2\mu q\epsilon + \mu^2\epsilon + \frac{\mu^2}{2^n} + \frac{q^2\epsilon}{2^n} + \frac{4q}{2^n} + v\epsilon + \frac{6v}{2^n} + 2\mathbf{Adv}^{\mathsf{prp}}_E(q+v,t+t')$$

*where $t'$ is the time complexity necessary to compute $E$ for $q+v$ times.*

### 5.1 Proof of Theorem 4

Similarly to the proof of Theorem 3, we assume that the adversary is deterministic and never makes a redundant query. Up to the $\mathsf{prp}$-security of $E$, keyed block ciphers $E_{K_1}$ and $E_{K_2}$ can be replaced by truly random permutations $P_1$ and $P_2$, respectively. The cost of this replacement is upper bounded by

$$2\mathbf{Adv}^{\mathsf{prp}}_E(q+v,t+t').$$

The resulting construction denotes $F^{\mathrm{SoP}*}_{B_2}[H]$. At the end of the interaction, additional information $K_h$ is freely given to an adversary. Without loss of generality, we rearrange query indices so that verification queries come after MAC queries.

Let $\Theta$ be the set of all attainable transcripts in the ideal world and $\tau = (\tau_m, \tau_v, K_h) \in \Theta$ be a transcript where $\tau_m$ and $\tau_v$ denote the list of MAC queries and the list of verification queries, i.e.,

$$\tau_m = \{(N_1, M_1, T_1), \ldots, (N_q, M_q, T_q)\},$$
$$\tau_v = \{(N_{q+1}, M_{q+1}, T_{q+1}, b_{q+1}), \ldots, (N_{q+v}, M_{q+v}, T_{q+v}, b_{q+v})\}.$$

From a transcript $\tau$, $\mathcal{A}$ can compute $X_i = H_{K_h}(M_i) \oplus N_i$ for $i \in [q+v]$ before outputting its decision bit.

The core of the security proof is to estimate the number of possible ways of fixing evaluations $P_1$ and $P_2$ in a way that

$$T_i = P_1(N_i) \oplus P_2(X_i)$$

for $i = 1, \ldots, q$ and

$$T_i \neq P_1(N_i) \oplus P_2(X_i)$$

for $i = q+1, \ldots, q+v$. We will identify $\mathcal{V}_1 = \{P_1(N_i)\}$ and $\mathcal{V}_2 = \{P_2(X_i)\}$ with as sets of variables. We also define $\mathcal{V} = \mathcal{V}_1 \sqcup \mathcal{V}_2$. Then we can construct the system of equations $\Gamma_\tau$ as defined in Section 3. To satisfy the conditions in Theorem 1, we must first define bad events on a transcript $\tau$, and then we can apply the extended Mirror theory to each transcript that the bad event does not happen.

*Defining and Bounding Bad Events.* A transcript $\tau = (\tau_m, \tau_v, K_h)$ is defined as *bad* if one of the following condition holds.

- $\mathsf{bad}_1 \Leftrightarrow$ there exists $(i_1, \ldots, i_n) \in [q]^{*n}$ where $N_{i_1}, \ldots N_{i_n}$ are all distinct such that $X_{i_1} = \cdots = X_{i_n}$.
- $\mathsf{bad}_2 \Leftrightarrow$ there exists $(i, j) \in [q]^{*2}$ such that $N_i = N_j$ and $X_i = X_j$.
- $\mathsf{bad}_3 \Leftrightarrow$ there exists $(i, j) \in [q]^{*2}$ such that $N_i = N_j$ and $T_i = T_j$.
- $\mathsf{bad}_4 \Leftrightarrow$ there exists $(i, j) \in [q]^{*2}$ such that $X_i = X_j$ and $T_i = T_j$.
- $\mathsf{bad}_5 \Leftrightarrow$ there exists $(i, j, k) \in [q]^{*3}$ such that $N_i = N_j$ and $X_j = X_k$.
- $\mathsf{bad}_6 \Leftrightarrow$ there exists $(i, j) \in [q] \times [q+1, q+v]$ such that $N_i = N_j, X_i = X_j$ and $T_i = T_j$.

If a transcript $\tau$ is not bad, then it will be called a *good* transcript. Now, we upper bound the probability happens $\mathsf{bad}$ in the ideal world by the following:

1. Since $H$ is $(n, \epsilon_n)$-AXU hash function, we have
$$\Pr[\mathsf{bad}_1] \leq \binom{q}{n}\epsilon_n.$$
2. By symmetry, we can assume that $i < j$, which means that $N_j$ is a faulty nonce. For each MAC query using a faulty nonce, there are at most $\mu$ other queries using the same nonce. So, the number of pairs $(i, j)$ such that $i < j$ and $N_i = N_j$ is at most $\mu^2$. For each of such pair $(i, j)$, the probability that $X_i = X_j$ is $\epsilon$. Therefore, we have
$$\Pr[\mathsf{bad}_2] \leq \mu^2\epsilon.$$
Similarly, we can show that
$$\Pr[\mathsf{bad}_3] \leq \frac{\mu^2}{2^n}$$
and
$$\Pr[\mathsf{bad}_4] \leq \frac{q^2\epsilon}{2^n}$$
3. The number of indices $j$ such that $N_i = N_j$ is at most $2\mu$. So, the number of choices of $(j, k)$ is at most $2\mu q$. For each of such pairs, the probability that $X_j = X_k$ is at most $\epsilon$. Therefore, we have
$$\Pr[\mathsf{bad}_5] \leq 2\mu q\epsilon.$$
4. Suppose $\mathsf{bad}_3$ does not occur. When an adversary makes a verification query $(N_j, M_j, T_j)$, there is one MAC query $(N_i, M_i, T_i)$ such that $N_i = N_j$ and $T_i = T_j$. For each of such pairs, the probability that $X_i = X_j$ is at most $\epsilon$. Therefore, we have
$$\Pr[\mathsf{bad}_6 \mid \neg\mathsf{bad}_3] \leq v\epsilon.$$

To sum up, we have

$$\begin{aligned}\Pr[\mathsf{bad}] = {} & \Pr[\mathsf{bad}_1] + \Pr[\mathsf{bad}_2] + \Pr[\mathsf{bad}_3] + \Pr[\mathsf{bad}_4] + \Pr[\mathsf{bad}_5] + \Pr[\mathsf{bad}_6 \mid \neg\mathsf{bad}_3] \\ & \leq \binom{q}{n}\epsilon_n + 2\mu q\epsilon + \mu^2\epsilon + \frac{\mu^2}{2^n} + \frac{q^2\epsilon}{2^n} + v\epsilon. \qquad (4)\end{aligned}$$

*Good Transcript Analysis.* For a good transcript $\tau$ and its system of equations $\mathit{\Gamma}_\tau$, we observe that

- $\mathit{\Gamma}_\tau$ is nice by $\neg(\mathsf{bad}_2 \vee \mathsf{bad}_3 \vee \mathsf{bad}_4 \vee \mathsf{bad}_5 \vee \mathsf{bad}_6)$. Since $\neg(\mathsf{bad}_2 \vee \mathsf{bad}_5)$, for any component $\{X_{i,0}, \ldots, X_{i,\xi_i-1}\}$, $X_{i,0} \not\sim X_{i,j}$ for $1 \le j \le \xi_i - 1$, which means the first condition holds. The second and the third conditions are satisfied by $\neg(\mathsf{bad}_3 \vee \mathsf{bad}_4)$ and $\neg\mathsf{bad}_6$.
- By $\neg(\mathsf{bad}_1 \vee \mathsf{bad}_5)$, $\xi_{\max} \le \max\{\mu + 1, n + 1\}$. Therefore, we have

$$\xi_{\max}^2 n + \xi_{max} \le n(\mu + n + 2)^2 + \mu + n + 2 \le 2^{n/2}$$

  since $n \ge 32$ and $n\mu \le 2^{n/4}$. We also have $q\xi_{\max}^2 \le (\mu + n + 2)^2 q \le \frac{2^n}{12}$.

Henceforth, we can apply Theorem 1 and then we have

$$h(\mathit{\Gamma}_\tau) \ge \frac{(2^n - 2)_{|\mathcal{V}_1|}(2^n - 2)_{|\mathcal{V}_2|}}{2^{nq}} \left(1 - \frac{2v}{2^n}\right).$$

Furthermore, we see that

$$\mathsf{p}_{\mathcal{S}_0}^{q+v}(\tau) = \frac{1}{|\mathcal{K}_h|} \cdot \frac{1}{2^{nq}}$$

and

$$\mathsf{p}_{\mathcal{S}_1}^{q+v}(\tau) = \frac{1}{|\mathcal{K}_h|} \cdot \frac{h(\mathit{\Gamma}_\tau)}{(2^n)_{|\mathcal{V}_1|}(2^n)_{|\mathcal{V}_2|}}.$$

From the above, one has

$$\begin{aligned}
\frac{\mathsf{p}_{\mathcal{S}_1}^{q+v}(\tau)}{\mathsf{p}_{\mathcal{S}_0}^{q+v}(\tau)} &= \frac{h(\mathit{\Gamma}_\tau)2^{nq}}{(2^n)_{|\mathcal{V}_1|}(2^n)_{|\mathcal{V}_2|}} \\
&\ge \frac{(2^n - 2)_{|\mathcal{V}_1|}(2^n - 2)_{|\mathcal{V}_2|}}{(2^n)_{|\mathcal{V}_1|}(2^n)_{|\mathcal{V}_2|}} \left(1 - \frac{2v}{2^n}\right) \\
&= \frac{(2^n - |\mathcal{V}_1|)_2(2^n - |\mathcal{V}_2|)_2}{(2^n)_2(2^n)_2} \left(1 - \frac{2v}{2^n}\right) \\
&\ge \left(1 - \frac{q+v}{2^n}\right)^4 \left(1 - \frac{2v}{2^n}\right) \\
&\ge 1 - \frac{4q}{2^n} - \frac{6v}{2^n} \qquad (5)
\end{aligned}$$

since $|\mathcal{V}_1|, |\mathcal{V}_2| \le q + v$.

Plugging (4) and (5) to Lemma 1, we conclude that

$$\left\|\mathsf{p}_{\mathcal{S}_0}^{q+v}(\tau) - \mathsf{p}_{\mathcal{S}_1}^{q+v}(\tau)\right\| \le \binom{q}{n}\epsilon_n + 2\mu q\epsilon + \mu^2\epsilon + \frac{\mu^2}{2^n} + \frac{q^2\epsilon}{2^n} + \frac{4q}{2^n} + v\epsilon + \frac{6v}{2^n}.$$

### 5.2 Multi-xor-collision Probability of CBC-MAC

We state an example of a multi-xor-collision resistant hash function. We consider $\mathsf{CBC\text{-}MAC}[\pi]$ based on pseudorandom permutation $\pi$. For a permutation $\pi$ and a message $M = (M[1], \ldots, M[m]) \in (\{0,1\}^n)^m$ with $m$ blocks, the tag is given by

$$\mathsf{CBC\text{-}MAC}[\pi](M) = X[m]$$

where

$$X[i] = \pi(X[i-1] \oplus M[i])$$

for $i \in [m]$ and $X[0] = 0$. We will show that $\mathsf{CBC\text{-}MAC}$ is a $\left(n, \frac{2}{2^{(n-1)^2}}\right)$-AXU hash function.

We fix pairwise distinct $n$ messages $M_1, \ldots, M_n \in (\{0,1\}^n)^*$ and pairwise distinct $n$ strings $Y_1, \ldots, Y_n \in \{0,1\}^n$ throughout this section and let $m_i$ be the block length of $M_i$ and $\max_{i \in [n]} m_i = \ell$. For simplicity, we assume that the lengths of messages are multiple of $n$.

We define a $n$-multi-collision event

$$\mathsf{Coll}_\pi \Leftrightarrow \mathsf{CBC\text{-}MAC}[\pi](M_1) \oplus Y_1 = \cdots = \mathsf{CBC\text{-}MAC}[\pi](M_n) \oplus Y_n.$$

Equivalently, the collision event is regarded as

$$\mathsf{Coll}_\pi \Leftrightarrow \mathsf{CBC\text{-}MAC}[\pi](M_1 \,\|\, Y_1) = \cdots = \mathsf{CBC\text{-}MAC}[\pi](M_n \,\|\, Y_n).$$

We bound the probability of $\mathsf{Coll}_\pi$ by the following lemma:

**Lemma 3.** *With the above notations, suppose that $n(\ell+1) \le 2^{n-1}$. Then, we have*

$$\Pr\left[\pi \leftarrow_\$ \mathsf{Perm}(n) : \mathsf{Coll}_\pi\right] \le \frac{1}{(2^n - n(\ell+1))^{n-1}} + \left(\frac{(n\ell+1)^2}{2^n}\right)^n.$$

*Proof.* Let $\mathcal{M} = (M_1 \| Y_1, \ldots, M_n \| Y_n)$ and $m = \sum_{i=1}^n m_i + n$. We first represent a relation of internal outputs through the computation of $\mathsf{CBC\text{-}MAC}$ via the structure graph. The intermediate values will be defined as sequences over a two-dimensional index set. Each index is a pair where the first element of the pair corresponds to the message number and the second element is the block number of that message. We define the index set

$$\mathcal{I} = \{(r,i) \mid r \in [k], i \in [m_r]\}$$

and the dictionary order $\prec$ on it as follows: $(r,i) \prec (s,j)$ if $r < s$ or $r = s$ and $i < j$. We also consider the index set $\mathcal{I}_0 = \mathcal{I} \cup \{(r,0) \mid r \in [q]\}$ and the natural extension of the order $\prec$ on $\mathcal{I}_0$.

For any $\pi \in \mathsf{Perm}(n)$, we build the structure graph $G_\pi$, which is a directed graph $(V, E)$ as follows:

– For any $\pi \in \mathsf{Perm}(n)$, we denote the intermediate values for each message as

$$X_\pi[r,i] = \pi(X_\pi[r,i-1] \oplus M_r[i])$$

for $(r,i) \in \mathcal{I}$ and $X_\pi[r,0] = \mathbf{0}$ for $r \in [q]$.
– From this $X[r,i]$'s, we define the mapping $[\cdot]_\pi : \mathcal{I}_0 \to \mathcal{I}_0$ as $[(r,i)]_\pi = \min\{(s,j) \mid X_\pi[s,j] = X_\pi[r,i]\}$ where the minimum is determined through the dictionary order. Now the structure graph $G_\pi = (V,E)$ is given by

$$V = \{[(r,i)]_\pi \mid (r,i) \in \mathcal{I}_0\},$$
$$E = \{([(r,i-1)]_\pi, [(r,i)]_\pi; M_r[i]) \mid r \in [q], i \in [m_r]\}.$$

Note that $[(r,0)]_\pi = (1,0)$ for $r \in [n]$.

We define a binary function Iszero such that for a structure graph $G_\pi$, $\mathrm{Iszero}(G_\pi) = 1$ if the vertex $(1,0)$ has positive in-degree, otherwise it maps to 0. We say that $G_\pi$ has a collision in a vertex $z$ if there exist $u$ and $v$ such that $e_1 =^{\mathrm{def}} (u,z;L_u), e_2 =^{\mathrm{def}} (v,z;L_v) \in E$. Then, we must have $X[u] \oplus X[v] = L_u \oplus L_v$. For all collisions, the collection of those linear equations is denoted $\mathcal{L}$. Let $\mathrm{rank}(G_\pi)$ denote the rank of $\mathcal{L}$. We define the accident of a structure graph $G_\pi$ as $\mathsf{Acc}(G_\pi) =^{\mathrm{def}} \mathrm{rank}(G_\pi) + \mathrm{Iszero}(G_\pi)$.

$\mathsf{Coll}_\pi$ occurs if and only if $\mathsf{Acc}(G_\pi) \geq n-1$ since the last blocks of all messages are pairwise distinct. Moreover, at least $n-1$ accidents occur at a vertex $(1,m_1)$. Similarly to Proposition 2 in [20], we have

$$\Pr[\pi \leftarrow_\$ \mathsf{Perm}(n) : \mathsf{Coll}_\pi] \leq \frac{A}{(2^n-m)^{n-1}} + \left(\frac{m^2}{2^n}\right)^n$$

where $A$ is the number of all structure graphs with $n-1$ accidents and satisfying $\mathsf{Coll}_\pi$. It is easy to see that $A \leq 1$ since no collision can occur except the vertex $(1,m_1)$. Therefore, we have

$$\begin{aligned}\Pr[\pi \leftarrow_\$ \mathsf{Perm}(n) : \mathsf{Coll}_\pi] &\leq \frac{1}{(2^n-m)^{n-1}} + \left(\frac{m^2}{2^n}\right)^n \\ &\leq \frac{1}{(2^n-n(\ell+1))^{n-1}} + \left(\frac{(n\ell+1)^2}{2^n}\right)^n\end{aligned}$$

since $m \leq n(\ell+1)$. □

## 6 Matching Attack on $F^{\mathbf{EDM}}_{B_4}$ and $F^{\mathbf{EDM}}_{B_5}$

In this section, we present a universal forging attack on $F^{\mathrm{EDM}}_{B_4}$ and $F^{\mathrm{EDM}}_{B_5}$ with probability $\frac{1}{2}$ using $O(2^{3n/4})$ queries in the nonce-respecting setting. For given $n$-bit nonce $N$ and a message $M$, a tag is computed as

$$F^{\mathrm{EDM}}_{B_4}[H,E](N,M) = E_{K_2}(E_{K_1}(N \oplus H_{K_h}(M)) \oplus N)$$

and

$$F_{B_5}^{\mathrm{EDM}}[H,E](N,M) = F_{B_4}^{\mathrm{EDM}}[H,E](N,M) \oplus H_{K_h}(M)$$

where a hash key $K_h$ and block cipher keys $K_1$ and $K_2$ (see Figure 1). To ease the notation, we show an attack on $F_{B_4}^{\mathrm{EDM}}$ below, but the same idea is easily mounted to $F_{B_5}^{\mathrm{EDM}}$.

Let $M, M' \in \{0,1\}^n$ be distinct two messages. For a randomly selected hash key $K_h$, we assume that at least one bit of $H_{K_h}(M) \oplus H_{K_h}(M')$ is 1 with a high probability. Without loss of generality, we say

$$\Pr\left[K_h \leftarrow_{\$} \mathcal{K}_h : H_{K_h}(M) \oplus H_{K_h}(M') = 1 \,\|\, *\right] \approx \frac{1}{2}. \tag{6}$$

**Algorithm 1:** A universal forgery attack on $F_{B_4}^{\mathrm{EDM}}$ and $F_{B_5}^{\mathrm{EDM}}$

**Input:** A target message $M \in \{0,1\}^n$
**Output:** A set of forgeries $\mathcal{F}$

$\mathcal{F} \leftarrow \emptyset$
// First Phase
$M' \leftarrow_{\$} \{0,1\}^n \setminus \{M\}$
$\mathsf{Used} \leftarrow \emptyset$
**for** $i \leftarrow 0$ ***to*** $2^{3n/4} - 1$ **do**
  $N_i \leftarrow 0^{n/4} \,\|\, \langle i \rangle_{3n/4}$
  $N_i' \leftarrow 1 \,\|\, \langle i \rangle_{3n/4} \,\|\, 0^{n/4-1}$
  $T_i \leftarrow \mathcal{O}(N_i, M)$
  $T_i' \leftarrow \mathcal{O}(N_i', M')$
  $\mathsf{Used} \leftarrow \mathsf{Used} \cup \{N_i, N_i'\}$
$\mathcal{Y} \leftarrow \emptyset$
**if** $\exists (i,j,k,l)$ *such that* $(N_i \oplus N_j \oplus N_k' \oplus N_l' = \mathbf{0}) \wedge (T_i = T_j) \wedge (T_k' = T_l')$ **then**
  $\mathcal{Y} \leftarrow \mathcal{Y} \cup \{N_i \oplus N_k'\}$
**if** $\mathcal{Y} = \emptyset$ **then**
  **return** $\perp$
// Second Phase
**for** $i \leftarrow 0$ ***to*** $2^{n/2} - 1$ **do**
  $\overline{N}_i \leftarrow \{0,1\}^n \setminus \mathsf{Used}$
  $\overline{T}_i \leftarrow \mathcal{O}(\overline{N}_i, M')$
  **if** $\exists (i,j)$ *such that* $\overline{T}_i = \overline{T}_j$ **then**
    **for** $Y \in \mathcal{Y}$ **do**
      $T \leftarrow \mathcal{O}(\overline{N}_i \oplus Y, M)$
      $\mathcal{F} \leftarrow \mathcal{F} \cup \left\{\overline{N}_j \oplus Y, M, T\right\}$
    **return** $\mathcal{F}$
**return** $\perp$

In the following, we state that PolyHash [22] and CBC-MAC satisfy the above property. For input $M \in \{0,1\}^n$, $\mathrm{Poly}_{K_h} : \{0,1\}^n \to \{0,1\}^n$ is defined as

$$\mathrm{Poly}_{K_h}(M) = M \cdot K_h$$

and $\mathsf{CBC\text{-}MAC}[E_{K_h}](M) : \{0,1\}^n \to \{0,1\}^n$ is defined as

$$\mathsf{CBC\text{-}MAC}[E_{K_h}](M) = E_{K_h}(M).$$

Then, we have

$$\Pr\left[K_h \leftarrow_{\$} \mathcal{K}_h : (M \oplus M') \cdot K_h = 1 \parallel *\right] \approx \frac{1}{2}$$

and

$$\Pr\left[K_h \leftarrow_{\$} \mathcal{K}_h : E_{K_h}(M) \oplus E_{K_h}(M') = 1 \parallel *\right] \approx \frac{1}{2}.$$

Algorithm 1 describes an attack that outputs a valid forgery for a target message $M \in \{0,1\}^n$.

**Theorem 5.** *Let $\mathcal{A}^*$ be an adversary running Algorithm 1. Then,*

$$\mathbf{Adv}^{\mathsf{mac}}_{F^{EDM}_{B_4}}(\mathcal{A}^*) \approx \frac{1}{4}$$

*where the error is exponentially small.*

*Proof.* We argue that $\mathcal{A}^*$ can find at least one pair $(i,j,k,l)$ with a high probability. Suppose that $H_{K_h}(M) \oplus H_{K_h}(M') = N_i \oplus N'_k = N_j \oplus N'_l$. Then, it holds

$$\begin{aligned} T_i = T_j &\Leftrightarrow E_{K_1}(N_i \oplus H_{K_h}(M)) \oplus N_i = E_{K_1}(N_j \oplus H_{K_h}(M)) \oplus N_j \\ &\Leftrightarrow E_{K_1}(N'_k \oplus H_{K_h}(M')) \oplus N'_k = E_{K_1}(N'_l \oplus H_{K_h}(M')) \oplus N'_l \\ &\Leftrightarrow T'_k = T'_l \end{aligned}$$

For each quadruple $(i,j,k,l)$, the probability that $T_i = T_j$ and $T'_k = T'_l$ is $\frac{1}{2^n}$ if $H_{K_h}(M) \oplus H_{K_h}(M') = N_i \oplus N'_k = N_j \oplus N'_l$. Otherwise, the probability is $\frac{1}{2^{2n}}$.

For $2^{n-1} \le y \le 2^n - 1$, there are $q' = 2^{n/2+1}$ tuples of indices $(i,j)$ such that $N_i \oplus N'_j = \langle y \rangle_n$. If $H_{K_h}(M) \oplus H_{K_h}(M') = \langle y \rangle_n$ for some $y$, $\mathcal{A}^*$ can find a quadruple $(i,j,k,l)$ such that $N_i \oplus N'_k = N_j \oplus N'_l = \langle y \rangle_n$ with overwhelming probability since the expected number is $\frac{\binom{q'}{2}}{2^n} \ge 1$. So, the probability $\mathcal{Y}$ contains the real hash difference is, by (6),

$$\Pr\left[K_h \leftarrow_{\$} \mathcal{K}_h : H_{K_h}(M) \oplus H_{K_h}(M') = 1 \parallel *\right] \approx \frac{1}{2} \tag{7}$$

and the expected size of $\mathcal{Y}$ is

$$1 + (2^n - 1)\frac{\binom{q'}{2}}{2^{2n}} \le 5.$$

Once the hash difference is found, one can compute a forgery by finding a tag collision in the second phase, in which the probability is $\frac{\binom{2^{\frac{n}{2}}}{2}}{2^n} \approx \frac{1}{2}$. By combining with (7), the probability of successful forgery is approximately $\frac{1}{4}$ (with a significantly small error). The above attack holds when $q \leq 2^{3n/4+2}$ with a constant number of verification queries. □

## 7 Security Reduction to Multi-User Security

This section aims to provide a semi-black-box translation of single-user security in the standard model to multi-user security in the ideal cipher model. It is well known that, by naive hybrid argument, multi-user security bound can be obtained from single-user security bound by multiplying $u$, the number of users. However, several dedicated analysis indicates the gap between multi-user bound and single-user bound is much smaller. We reduced the overhead by a semi-black-box approach, even when switching the model between a single-user setting and a multi-user setting. We emphasize that multi-user security bound in the standard model can be easily obtained from that of the ideal cipher model by letting $p = 0$. Even more, when we consider the standard model, we don't have to be concerned about key-colliding bad events, i.e., ill-behaved events. Hence, we can recover the same bound as in the single-user setting, which is usually regarded as the optimal bound.

### 7.1 Multi-User Security Notion in the Ideal Cipher Model

For $(K_1, \ldots, K_u) \in \mathcal{K}^u$, let $(\mathsf{Auth}_{K_1}, \ldots, \mathsf{Auth}_{K_u})$ be MAC oracles implemented by $F$, built upon an ideal cipher, which takes as input a pair $(N, M) \in \mathcal{N} \times \mathcal{M}$ and returns $F_{K_i}(N, M)$ if a query is made to $i$-th oracle, and let $(\mathsf{Ver}_{K_1}, \ldots, \mathsf{Ver}_{K_u})$ be the verification oracle which takes as input a triple $(N, M, T) \in \mathcal{N} \times \mathcal{M} \times \mathcal{T}$ and returns 1 if $F_{K_i}(N, M) = T$, and 0 ("reject") otherwise for a given query to the $i$-th oracle. In the ideal cipher model, there is an additional ideal cipher oracles $\mathsf{IC}$ and $\mathsf{IC}^{-1}$ which takes $(K, M) \in \mathcal{K} \times \mathcal{M}$ (resp. $(K, C) \in \mathcal{K} \times \mathcal{C}$) and returns $C \in \mathcal{C}$ (resp. $M \in \mathcal{M}$).

A $(u, p, \mu, q, v, t)$-adversary against the nonce-based MAC-security of $F$ is an adversary $\mathcal{A}$ with oracle access to oracles $(\mathsf{Auth}_{K_1}, \ldots, \mathsf{Auth}_{K_u})$ and $(\mathsf{Ver}_{K_1}, \ldots, \mathsf{Ver}_{K_u})$, making at most $p$ ideal cipher queries to $\mathsf{IC}$ or $\mathsf{IC}^{-1}$ oracles, at most $q$ MAC queries to $\mathsf{Auth}$ oracle, at most $\mu$ faulty queries, at most $v$ verification queries to $\mathsf{Ver}$ oracle, and running in time at most $t$. We say that $\mathcal{A}$ forges if any of its queries to $\mathsf{Ver}_{K_i}$ returns 1 for any choice of $i$. The advantage of $\mathcal{A}$ against the nonce-based MAC security of $F$ is defined as

$$\mathbf{Adv}_F^{\mathsf{mu\text{-}mac}}(\mathcal{A}) = \Pr\left[(K_1, \ldots, K_u) \leftarrow_{\$} \mathcal{K}^u : \mathcal{A}^{(\mathsf{Auth}_{K_i}, \mathsf{Ver}_{K_i})_{i \in [u]}, \mathsf{IC}, \mathsf{IC}^{-1}} \text{forges}\right].$$

where the probability is also taken over the random coins of $\mathcal{A}$, if any. For any user $i$, the adversary is not allowed to ask a verification query $(N, M, T)$ to $\mathsf{Ver}_K$

if a previous query $(N, M)$ to $\mathsf{Auth}_K$ returned $T$. When $\mu = 0$, we say that $\mathcal{A}$ is nonce-respecting, otherwise, $\mathcal{A}$ is said nonce-misusing. $\mathcal{A}$ is allowed to repeat nonces in its verification queries.

### 7.2 Generic Transition to Multi-User Security

*Proof Setting.* As in the single-user proofs, we assume that the adversary is deterministic and never makes a redundant query. A block cipher $E$ is modeled as an ideal block cipher. The resulting construction is denoted as $F^*$. At the end of the game, hash keys $(K_{h,1}, \ldots, K_{h,u})$ as well as block cipher keys $((K_{1,1}, K_{2,1}), \ldots, (K_{1,u}, K_{2,u}))$ are freely given to an adversary $\mathcal{A}$, while they are generated uniformly randomly in the ideal world.

Let $\Theta$ be the set of all attainable transcripts in the ideal world and $\tau = ((\tau_{m,i}, \tau_{v,i}, K_{h,i}, K_{1,i}, K_{2,i})_{i\in[u]}, \tau_p) \in \Theta$ be a transcript where $\tau_{m,i}$, $\tau_{v,i}$, and $\tau_p$ denote the list of MAC queries to the $i$-th $\mathsf{Auth}$ oracle, the list of verification queries to the $i$-th $\mathsf{Ver}$ oracle, and the list of ideal cipher queries to the $\mathsf{IC}$ and $\mathsf{IC}^{-1}$ oracles, respectively. Let $\tau_p = ((K_{p,i}, M_i, C_i)_{i=1,\ldots,p})$.

We denote $\mu_i$, $q_i$, and $v_i$ as the number of faulty queries, the number of MAC queries, and the number of verification queries to the $i$-th oracles. We also assume a MAC construction $F$ uses a pair of secret keys $(K_h, K_1, K_2) \in \mathcal{K}_h \times \mathcal{K} \times \mathcal{K}$ where $\mathcal{K} = \{0,1\}^k$. When we consider a block-cipher-based hash as an underlying primitive as in $\mathsf{nEHtM}$, we also let $\mathcal{K}_h = \{0,1\}^k$.

*Defining and Bounding Ill-Behaved Events.* A transcript $\tau = ((\tau_{m,i}, \tau_{v,i}, K_{h,i})_{i\in[u]}, \tau_p)$ is defined as *ill-behaved* if one of the following condition holds.

- $\mathsf{ill}_1 \Leftrightarrow$ there exists $i \in [u]$ such that $K_{1,i} = K_{2,i}$.
- $\mathsf{ill}_2 \Leftrightarrow$ there exists $(i,j) \in [u]^{*2}$ such that $K_{1,i} = K_{1,j}$ or $K_{1,i} = K_{2,j}$ or $K_{2,i} = K_{2,j}$.
- $\mathsf{ill}_3 \Leftrightarrow$ there exists $(i,j) \in [u] \times [p]$ such that $K_{1,i} = K_{p,j}$ or $K_{2,i} = K_{p,j}$.
- $\mathsf{ill}_4 \Leftrightarrow$ there exists $i \in [u]$ such that $\tau_i = (\tau_{m,i}, \tau_{v,i}, K_{h,i})$ is bad.
- $\mathsf{aux}_1 \Leftrightarrow$ there exists $(i,j) \in [u]^{*2}$ such that $K_{h,i} = K_{h,j}$ or $K_{h,i} = K_{1,j}$ or $K_{h,i} = K_{2,j}$.
- $\mathsf{aux}_2 \Leftrightarrow$ there exists $(i,j) \in [u] \times [p]$ such that $K_{h,i} = K_{p,j}$.

Note that we only consider $\mathsf{aux}_1$ and $\mathsf{aux}_2$ when the underlying hash is block-cipher-based and $\mathcal{K}_h = \{0,1\}^k$. It does not need to be taken into account when we consider other hashes such as a polynomial hash.

If a transcript $\tau$ is not ill-behaved, then it will be called a *well-behaved* transcript. The probability that the ill-behaved event occurs is obtained as follows:

- Since all the keys are random in the ideal world, we have

$$\Pr[\mathsf{ill}_1] = \frac{u}{2^k},$$

$$\Pr[\mathsf{aux}_1] = \Pr[\mathsf{ill}_2] \le \frac{3\binom{u}{2}}{2^k} \le \frac{2u^2}{2^k},$$

and

$$\Pr[\mathsf{aux}_2] = \Pr[\mathsf{ill}_3] \leq \frac{up}{2^k}.$$

– Let $\mathsf{bad}[\mu_i, q_i, v_i]$ be the (upper-bound of) probability of the bad event happening for a given construction $F$ given a (single-user) $(\mu_i, q_i, v_i, t_i)$-adversary, which is defined and computed in the corresponding single-user proof of the construction $F$ in this paper. Then we have,

$$\Pr[\mathsf{ill}_4] \leq \sum_{i=1}^{u} \mathsf{bad}[\mu_i, q_i, v_i].$$

We note that $\mathsf{bad}$ is a polynomial of $\mu_i, q_i, v_i$ such that all terms in the polynomial have one variable of degree at least 1. For such a polynomial, we can deduce that

$$\sum_{i=1}^{u} \mathsf{bad}[\mu_i, q_i, v_i] \leq \mathsf{bad}[\mu, q, v].$$

For example, for $F = \mathsf{EWCDM}$, we have

$$\mathsf{bad}[\mu_i, q_i, v_i] = \frac{2q_i}{2^n} + \frac{{q_i}^2\epsilon}{2^n} + v_i\epsilon.$$

It follows that

$$\sum_{i=1}^{u} \mathsf{bad}[\mu_i, q_i, v_i] = \sum_{i=1}^{u} \left( \frac{2q_i}{2^n} + \frac{{q_i}^2\epsilon}{2^n} + v_i\epsilon \right) \leq \frac{2q}{2^n} + \frac{q^2\epsilon}{2^n} + v\epsilon = \mathsf{bad}[\mu, q, v].$$

Therefore, we have

$$\begin{aligned} \Pr[\mathsf{ill}] &\leq \Pr[\mathsf{ill}_1] + \Pr[\mathsf{ill}_2] + \Pr[\mathsf{ill}_3] + \Pr[\mathsf{ill}_4] + \Pr[\mathsf{aux}_1] + \Pr[\mathsf{aux}_2] \\ &\leq \frac{4u(u+p)+u}{2^k} + \mathsf{bad}[\mu, q, v]. \end{aligned} \tag{8}$$

*Well-Behaved Transcript Analysis.* For a well-behaved transcript $\tau$, it satisfies that $\tau_i = (\tau_{m,i}, \tau_{v,i}, K_{h,i})$ is good for all $i \in [u]$ since $\neg\mathsf{ill}_4$. Furthermore, by $\neg(\mathsf{ill}_1 \vee \mathsf{ill}_2 \vee \mathsf{ill}_3)$, there are no collide keys so $\tau_i$ are independent from $\tau_j$ for $j \neq i$. By $\neg\mathsf{ill}_4$, any primitive query does not affect construction queries. Hence the probability of obtaining $\tau_i$ is independent from $\tau_p$. Let

$$\frac{\mathsf{p}_{\mathcal{S}_1}^{q_i+v_i}(\tau_i)}{\mathsf{p}_{\mathcal{S}_0}^{q_i+v_i}(\tau_i)} \geq 1 - \mathsf{good}[\mu_i, q_i, v_i]$$

where $\mathsf{good}[\mu_i, q_i, v_i]$ is defined and computed in the corresponding single-user proof of the construction $F$ in this paper. We see that, as like $\mathsf{bad}[\mu_i, q_i, v_i]$,

$$\sum_{i=1}^{u} \mathsf{good}[\mu_i, q_i, v_i] \leq \mathsf{good}[\mu, q, v].$$

Finally, we have

$$\begin{aligned}\frac{\mathsf{p}_{\mathcal{S}_1}^{q+v}(\tau)}{\mathsf{p}_{\mathcal{S}_0}^{q+v}(\tau)} &= \frac{2^{2uk}\cdot \mathsf{p}_{\mathcal{S}_1}^{q+v}(\tau_p)}{2^{2uk}\cdot \mathsf{p}_{\mathcal{S}_0}^{q+v}(\tau_p)} \prod_{i=1}^{u} \frac{\mathsf{p}_{\mathcal{S}_1}^{q_i+v_i}(\tau_i)}{\mathsf{p}_{\mathcal{S}_0}^{q_i+v_i}(\tau_i)} \\ &\geq 1 - \sum_{i=1}^{u} \mathsf{good}[\mu_i, q_i, v_i] \\ &\geq 1 - \mathsf{good}[\mu, q, v]. \end{aligned} \tag{9}$$

By Lemma 1, it follows that

$$\mathbf{Adv}^{\mathsf{mac}}_{F^*[H]}(\mu, q, v) \leq \mathsf{good}[\mu, q, v] + \mathsf{bad}[\mu, q, v].$$

Plugging (8) and (9) to Lemma 1, we conclude that

$$\begin{aligned}\mathbf{Adv}^{\mathsf{mu\text{-}mac}}_{F^*}(u, \mu, q, v) &\leq \left\|\mathsf{p}_{\mathcal{S}_0}^{q+v}(\cdot) - \mathsf{p}_{\mathcal{S}_1}^{q+v}(\cdot)\right\| \\ &\leq \mathbf{Adv}^{\mathsf{mac}}_{F^*[H]}(\mu, q, v) + \frac{4u(u+p)+u}{2^k}.\end{aligned}$$

## References


1. Banik, S., Pandey, S.K., Peyrin, T., Sasaki, Y., Sim, S.M., Todo, Y.: GIFT: A Small Present. In: Fischer, W., Homma, N. (eds.) Cryptographic Hardware and Embedded Systems - CHES 2017. LNCS, vol. 10529, pp. 321–345. Springer (2017). https://doi.org/10.1007/978-3-319-66787-4_16
2. Bellare, M., Kilian, J., Rogaway, P.: The security of the cipher block chaining message authentication code. Journal of Computer and System Sciences **61**(3), 362–399 (2000)
3. Bellare, M., Pietrzak, K., Rogaway, P.: Improved security analyses for cbc macs. In: Advances in Cryptology - CRYPTO 2005: 25th Annual International Cryptology Conference, Santa Barbara, California, USA, August 14-18, 2005, Proceedings. Lecture Notes in Computer Science, vol. 3621, pp. 527–545. Springer (2005). https://doi.org/10.1007/11535218_32
4. Bernstein, D.J.: Stronger Security Bounds for Wegman-Carter-Shoup Authenticators. In: Cramer, R. (ed.) Advances in Cryptology - EUROCRYPT 2005. LNCS, vol. 3494, pp. 164–180. Springer (2005). https://doi.org/10.1007/11426639_10
5. Bernstein, D.J.: The Poly1305-AES message-authentication code. In: Gilbert, H., Handschuh, H. (eds.) Fast Software Encryption. LNCS, vol. 3557, pp. 32–49. Springer (2005). https://doi.org/10.1007/11502760_3
6. 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 CCS. pp. 456–467. ACM (2016). https://doi.org/10.1145/2976749.2978423
7. Black, J., Rogaway, P.: A Block-Cipher Mode of Operation for Parallelizable Message Authentication. In: Knudsen, L.R. (ed.) Advances in Cryptology - EUROCRYPT 2002. LNCS, vol. 2332, pp. 384–397. Springer (2002). https://doi.org/10.1007/3-540-46035-7_25, `https://iacr.org/archive/eurocrypt2002/23320380/pmac.pdf`

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.) Cryptographic Hardware and Embedded Systems - CHES 2007. LNCS, vol. 4727, pp. 450–466. Springer (2007). https://doi.org/10.1007/978-3-540-74735-2_31
9. Chen, Y.L., Mennink, B., Preneel, B.: Categorization of Faulty Nonce Misuse Resistant Message Authentication. In: Tibouchi, M., Wang, H. (eds.) Advances in Cryptology - ASIACRYPT 2021. LNCS, vol. 13092, pp. 520–550. Springer (2021). https://doi.org/10.1007/978-3-030-92078-4_18
10. 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.) Advances in Cryptology – ASIACRYPT 2020. LNCS, vol. 12491, pp. 697–723. Springer (2020). https://doi.org/10.1007/978-3-030-64837-4_23
11. Cogliati, B., Dutta, A., Nandi, M., Patarin, J., Saha, A.: Proof of Mirror Theory for a Wide Range of $\xi_{\max}$. In: Hazay, C., Stam, M. (eds.) Advances in Cryptology – EUROCRYPT 2023. LNCS, vol. 14007, pp. 470–501. Springer (2023). https://doi.org/10.1007/978-3-031-30634-1_16
12. Cogliati, B., Seurin, Y.: EWCDM: An Efficient, Beyond-Birthday Secure, Nonce-Misuse Resistant MAC. In: Robshaw, M., Katz, J. (eds.) Advances in Cryptology - CRYPTO 2016. LNCS, vol. 9814, pp. 121–149. Springer (2016). https://doi.org/10.1007/978-3-662-53018-4_5
13. Datta, N., Dutta, A., Dutta, K.: Improved Security Bound of (E/D)WCDM. IACR Transactions on Symmetric Cryptology **Issue 4**, 138–176 (2021). https://doi.org/10.46586/tosc.v2021.i4.138-176
14. 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.) Advances in Cryptology - CRYPTO 2018. LNCS, vol. 10991, pp. 631–661. Springer (2018). https://doi.org/10.1007/978-3-319-96884-1_21
15. Dutta, A., Nandi, M., Talnikar, S.: Beyond Birthday Bound Secure MAC in Faulty Nonce Model. In: Ishai, Y., Rijmen, V. (eds.) Advances in Cryptology - EUROCRYPT 2019. LNCS, vol. 11476, pp. 437–466. Springer (2019). https://doi.org/10.1007/978-3-030-17653-2_15
16. Guo, J., Peyrin, T., Poschmann, A., Robshaw, M.J.B.: The LED Block Cipher. In: Preneel, B., Takagi, T. (eds.) Cryptographic Hardware and Embedded Systems - CHES 2011. LNCS, vol. 6917, pp. 326–341. Springer (2011). https://doi.org/10.1007/978-3-642-23951-9_22
17. Handschuh, H., Preneel, B.: Key-recovery attacks on universal hash function based mac algorithms. In: Advances in Cryptology - CRYPTO 2008, 28th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 17-21, 2008. Lecture Notes in Computer Science, vol. 5157, pp. 144–161. Springer (2008). https://doi.org/10.1007/978-3-540-85174-5_9, `https://iacr.org/archive/crypto2008/51570145/51570145.pdf`
18. Information technology – Security techniques – Message Authentication Codes (MACs) – Part 1: Mechanisms using a block cipher. Standard, International Organization for Standardization (Mar 2011)
19. Iwata, T., Kurosawa, K.: OMAC: One-Key CBC MAC. In: Johansson, T. (ed.) Fast Software Encryption. LNCS, vol. 2887, pp. 129–153. Springer (2003). https://doi.org/10.1007/978-3-540-39887-5_11, `https://iacr.org/archive/fse2003/28870137/28870137.pdf`
20. Jha, A., Nandi, M.: Revisiting structure graphs: Applications to cbc-mac and emac. Journal of Mathematical Cryptology **10**(3-4), 157–180 (2016)

21. Mennink, B., Neves, S.: Encrypted Davies-Meyer and Its Dual: Towards Optimal Security Using Mirror Theory. In: Katz, J., Shacham, H. (eds.) Advances in Cryptology - CRYPTO 2017. LNCS, vol. 10403, pp. 556–583. Springer (2017). https://doi.org/10.1007/978-3-319-63697-9_19
22. Minematsu, K., Iwata, T.: Building blockcipher from tweakable blockcipher: Extending fse 2009 proposal. In: Cryptography and Coding: 13th IMA International Conference, IMACC 2011, Oxford, UK, December 12-15, 2011. Proceedings 13. pp. 391–412. Springer (2011)
23. Morris J. Dworkin: Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC. NIST Special Publication **800-38D** (Nov 28 2007)
24. Naito, Y.: Blockcipher-Based MACs: Beyond the Birthday Bound Without Message Length. In: ASIACRYPT (3). pp. 446–470. Springer (2017). https://doi.org/10.1007/978-3-319-70700-6_16
25. Patarin, J.: Introduction to Mirror Theory: Analysis of Systems of Linear Equalities and Linear Non Equalities for Cryptography. IACR Cryptology ePrint Archive, Report 2010/287 (2010), available at `https://eprint.iacr.org/2010/287`
26. Patarin, J.: Mirror Theory and Cryptography. IACR Cryptology ePrint Archive, Report 2016/702 (2016), available at `https://eprint.iacr.org/2016/702`
27. Pietrzak, K.: A tight bound for emac. In: Automata, Languages and Programming: 33rd International Colloquium, ICALP 2006, Venice, Italy, July 10-14, 2006, Proceedings, Part II 33. pp. 168–179. Springer (2006)
28. Shoup, V.: On Fast and Provably Secure Message Authentication Based on Universal Hashing. In: Koblitz, N. (ed.) Advances in Cryptology - CRYPTO '96. LNCS, vol. 1109, pp. 313–328. Springer (1996). https://doi.org/10.1007/3-540-68697-5_24
29. Wegman, M.N., Carter, J.L.: New hash functions and their use in authentication and set equality. Journal of Computer and System Sciences **22, Issue 3**, 265–279 (1981)
30. Yasuda, K.: The sum of CBC MACs is a secure PRF. In: Cryptographers' Track at the RSA Conference. pp. 366–381. Springer (2010)
31. Yasuda, K.: A New Variant of PMAC: Beyond the Birthday Bound. In: Advances in Cryptology - CRYPTO 2011 - 31st Annual Cryptology Conference. Lecture Notes in Computer Science, vol. 6841, p. 593. Springer (2011). https://doi.org/10.1007/978-3-642-22792-9_34, `https://www.iacr.org/archive/crypto2011/68410593/68410593.pdf`
32. Zhang, L., Wu, W., Sui, H., Wang, P.: 3kf9: Enhancing 3GPP-MAC beyond the Birthday Bound. In: ASIACRYPT. vol. 7658, pp. 296–312. Springer (2012). https://doi.org/10.1007/978-3-642-34961-4_19, `https://www.iacr.org/archive/asiacrypt2012/76580291/76580291.pdf`

# Supplementary Material

## A Proof of Theorem 2

### A.1 Set Representation

We start by establishing a fixed system $\Gamma$. Additionally, we define a new partition of $\mathcal{V}$ as $\mathcal{V} = C_1 \sqcup \cdots \sqcup C_c$, with each $C_i$ being a set of variables defined as $C_i = \{X_{i,0}, \ldots, X_{i,\xi_i - 1}\}$. Let $\mathcal{F} = \{C_1, \ldots, C_c\}$ represent a family of the sets $C_i$. In this context, we introduce a label function denoted as $\Lambda : \mathcal{V} \times \mathcal{V} \to \{0,1\}^n \cup \{\perp\}$ defined as follows: when both $X_{i,j}$ and $X_{i,k}$ are within the same set $C_i$, $\Lambda(X_{i,j}, X_{i,k})$ returns $\lambda_{i,j} \oplus \lambda_{i,k}$ by letting $\lambda_{i,0} = 0$. Otherwise, it returns $\perp$. In this section, we fix $\mathcal{F}$ and $\Lambda$.

Now, let us define terms related to a family of sets $\mathcal{G} = \{A_1, \ldots, A_a\}$, where $A_i$ is a subset of $\mathcal{V}$ and a label function $\mathcal{L}$:

- $\mathsf{N}(\mathcal{G})$ represents the total number of variables in $\mathcal{G}$, i.e., $\mathsf{N}(\mathcal{G}) = \sum_{1 \le i \le |\mathcal{G}|} |A_i|$.
- $\mathsf{N}_1(\mathcal{G})$ and $\mathsf{N}_2(\mathcal{G})$ denote the number of variables of $\mathcal{G}$ contained in $\mathcal{V}_1$ and $\mathcal{V}_2$, respectively. In other words,

$$\mathsf{N}_1(\mathcal{G}) = \sum_{1 \le i \le |\mathcal{G}|} |A_i \cap \mathcal{V}_1| \,,$$
$$\mathsf{N}_2(\mathcal{G}) = \sum_{1 \le i \le |\mathcal{G}|} |A_i \cap \mathcal{V}_2| \,.$$

- For a variable $v \in \mathcal{V}$,

$$\mathsf{N}_v(\mathcal{G}) = \begin{cases} \mathsf{N}_1(\mathcal{G}) \text{ if } v \in \mathcal{V}_1, \\ \mathsf{N}_2(\mathcal{G}) \text{ if } v \in \mathcal{V}_2. \end{cases}$$

- We denote $h(\mathcal{G}, \mathcal{L})$ as the number of assignments to $\mathcal{G}$ according to the label function $\mathcal{L}$ while all the variables in $\mathcal{V}_1$ (resp. $\mathcal{V}_2$) should take on different values. Specifically, $h(\mathcal{F}, \Lambda)$ is equivalent to $h(\Gamma)$.
- $\mathsf{M}(\mathcal{G})$ is the maximum number of components within the family, i.e., $\mathsf{M}(\mathcal{G}) = \max_{1 \le i \le |\mathcal{G}|} \{|A_i|\}$.

### A.2 Proof of Theorem 2

Let $\mathcal{G}$ be a sub-family of $\mathcal{F}$. For any set $S \in \mathcal{G}$, we claim that

$$h(\mathcal{G}, \Lambda) \ge 2^n h(\mathcal{G} \setminus \{S\}, \Lambda) \prod_{i=\mathsf{N}_1(\mathcal{G}\setminus\{S\})+1}^{\mathsf{N}_1(\mathcal{G})} \left(1 - \frac{i+1}{2^n}\right) \prod_{i=\mathsf{N}_2(\mathcal{G}\setminus\{S\})+1}^{\mathsf{N}_2(\mathcal{G})} \left(1 - \frac{i+1}{2^n}\right).$$

If $|S| = 1$, it means $S$ contains only one element, say $v$, i.e., $S = \{v\}$. The claim is obvious since

$$h(\mathcal{G}, \Lambda) = h(\mathcal{G} \setminus \{S\}, \Lambda) \times (2^n - \mathsf{N}_v(\mathcal{G}) + 1). \tag{10}$$

Next, suppose $|S| \geq 2$. We first consider the case that $\mathsf{N}(\mathcal{G}) \leq 2^{\frac{n}{2}}$. We have

$$h(\mathcal{G}, \Lambda) \geq h(\mathcal{G} \setminus \{S\}, \Lambda) \times (2^n - \mathsf{N}_1(S) \times \mathsf{N}_1(\mathcal{G} \setminus \{S\}) - \mathsf{N}_2(S) \times \mathsf{N}_2(\mathcal{G} \setminus \{S\})).$$

In order to prove the claim, it is enough to show that

$$1 - \frac{\mathsf{N}_1(S) \times \mathsf{N}_1(\mathcal{G} \setminus \{S\})}{2^n} - \frac{\mathsf{N}_2(S) \times \mathsf{N}_2(\mathcal{G} \setminus \{S\})}{2^n} \geq \prod_{i=\mathsf{N}_1(\mathcal{G}\setminus\{S\})+1}^{\mathsf{N}_1(\mathcal{G})} \left(1 - \frac{i+1}{2^n}\right) \prod_{i=\mathsf{N}_2(\mathcal{G}\setminus\{S\})+1}^{\mathsf{N}_2(\mathcal{G})} \left(1 - \frac{i+1}{2^n}\right). \tag{11}$$

The above inequality is represented by

$$1 - \frac{ar + bs}{2^n} \geq \left(1 - \frac{a+2}{2^n}\right) \ldots \left(1 - \frac{a+r+1}{2^n}\right) \left(1 - \frac{b+2}{2^n}\right) \left(1 - \frac{b+s+1}{2^n}\right).$$

This can be shown by induction on $r$ and $s$. For $r = 1$ and $s = 1$, the inequality holds since

$$\begin{aligned}\left(1 - \frac{a+2}{2^n}\right) \left(1 - \frac{b+2}{2^n}\right) &\leq 1 - \frac{a+b}{2^n} - \frac{4}{2^n} \left(1 - \frac{(a+2)(b+2)}{2^{n+2}}\right) \\ &\leq 1 - \frac{a+b}{2^n}.\end{aligned}$$

The last inequality holds since $a, b \leq 2^{\frac{n}{2}}$ and $n \geq 2$. If $r \geq s$ we obtain

$$\begin{aligned}&\left(1 - \frac{a(r-1) + bs}{2^n}\right) \left(1 - \frac{a+r+1}{2^n}\right) \\ &\qquad \leq 1 - \frac{ar + bs}{2^n} - \frac{r+1}{2^n} + \frac{(a(r-1) + bs)(a+r+1)}{2^{2n}} \\ &\qquad \leq 1 - \frac{ar + bs}{2^n} - \frac{r+1}{2^n} \left(1 - \frac{(a+b)(a+r+1)}{2^n}\right) \\ &\qquad \leq 1 - \frac{ar + bs}{2^n}\end{aligned}$$

since $a + b \leq 2^{n/2}$ and $a + r + 1 \leq 2^{n/2}$. If $r < s$, similarly, we have

$$\left(1 - \frac{ar + b(s-1)}{2^n}\right) \left(1 - \frac{b+s+1}{2^n}\right) \leq 1 - \frac{ar + bs}{2^n}.$$

By applying induction hypothesis for $r$ and $s$, the equation (11) holds.

For an element $v \in S \in \mathcal{G}$, we denote $\mathcal{G}_{-v}$ as a family of partitions deleting $v$, i.e., $\mathcal{G}_{-v} = (\mathcal{G} \setminus \{S\}) \cup \{S \setminus \{v\}\}$. We state the following lemma.

Given a set $S \in \mathcal{G}$, $v, w \in S$ and a label function $\mathcal{L}$, we define $\delta_{S,\mathcal{L}}(v, w)$ as the number of 2-subsets $\{a, b\}$ of $S$ such that $a \sim v$ and $b \sim w$ with $\mathcal{L}(a, b) = \mathcal{L}(v, w)$. We define

$$\delta_{\mathcal{G},\mathcal{L}}(v, w) \stackrel{\text{def}}{=} \sum_{S \in \mathcal{G}} \delta_{S,\mathcal{L}}(v, w), \quad \Delta_{\mathcal{G},\mathcal{L}} \stackrel{\text{def}}{=} \max_{S \in \mathcal{G}} \max_{(v,w) \in S^{*2}} \delta_{\mathcal{G},\mathcal{L}}(v, w).$$

Then, we estimate the lower bound of $h(\mathcal{G}, \Lambda)$.

**Lemma 4.** *Suppose the maximum $\Delta_{\mathcal{G},\Lambda}$ is attained for $v, v' \in S \in \mathcal{G}$. If $2^{\frac{n}{2}} \leq \mathsf{N}(\mathcal{G}) \leq \frac{2^n}{12\xi_{\max}^2}$, we have*

$$h(\mathcal{G}, \Lambda) \geq h(\mathcal{G}_{-v}, \Lambda) \left(1 - \frac{\mathsf{N}_v(\mathcal{G}) + 1}{2^n}\right)$$

When $2^{\frac{n}{2}} \leq \mathsf{N}(\mathcal{G}) \leq \frac{2^n}{12\xi_{\max}^2}$, the claim holds by Lemma 4. By iterating the inequality, we conclude that

$$\begin{aligned} h(\mathcal{F}, \Lambda) &\geq (2^n)^c \prod_{i=1}^{|\mathcal{V}_1|} \left(1 - \frac{i+1}{2^n}\right) \prod_{i=1}^{|\mathcal{V}_2|} \left(1 - \frac{i+1}{2^n}\right) \\ &\geq \frac{(2^n - 2)_{|\mathcal{V}_1|} (2^n - 2)_{|\mathcal{V}_2|}}{2^{nq}}. \end{aligned}$$

### A.3 Proof of Lemma 4

Let $\mathcal{G} = \{A_1, \ldots, A_a\}$ be a family of sets. For $v \in S \in \mathcal{G}$ and $w \in S' \in \mathcal{G}$, let $\mathcal{G}_{v=w}$ be made by combining $S$ and $S'$ and identifying $v$ and $w$. Formally,

$$\mathcal{G}_{v=w} = (\mathcal{G} \setminus \{S, S'\}) \cup \{S \cup S' \setminus \{w\}\}.$$

We also define a modified label function $\Lambda_{v=w}$ corresponding $\mathcal{G}_{v=w}$.

$$\Lambda_{v=w}(v', w') = \begin{cases} \Lambda(v, v') \oplus \Lambda(w, w') & \text{if } (v', w') \in S \times S', \\ \Lambda(v', w') & \text{otherwise.} \end{cases}$$

*Vertex-Deletion Equation.* Let

$$\mathcal{I}_{v,S} = \{(w, S') \mid w \in S' \in \mathcal{G} \setminus \{S\}, v \sim w, h(\mathcal{G}_{v=w}, \Lambda_{v=w}) > 0\}.$$

We claim the following equation.

$$h(\mathcal{G}, \Lambda) = h(\mathcal{G}_{-v}, \Lambda) - \sum_{(w,S') \in \mathcal{I}_{v,S}} h(\mathcal{G}_{v=w}, \Lambda_{v=w}). \tag{12}$$

The equation is derived directly from the fact that solutions to $(\mathcal{G}_{-v}, \Lambda)$ can be separated into two cases:

– Adding $v$ as a link to the set $S$ avoid any collision.
– There exists a collision. For every $(w, S') \in \mathcal{I}_{v,S}$, the number of solutions in this case is given by $h(\mathcal{G}_{v=w}, \Lambda_{v=w})$.

The number of solutions to $(\mathcal{G}, \Lambda)$ is equivalent to the number of solutions to $(\mathcal{G}_{-v}, \Lambda)$ within the first case.

The size of $\mathcal{I}_{v,S}$ is bounded as follows:

$$|\mathcal{I}_{v,S}| \leq \mathsf{N}_v(\mathcal{G}) - \Delta_{\mathcal{G},\Lambda}. \tag{13}$$

Consider any $S' \in \mathcal{G} \setminus \{S\}$. We choose $v' \in S$ in a way that maximizes $\delta_{\mathcal{G},\Lambda}(v, v')$. For two elements $w, w' \in S'$ such that $v \sim w$ and $v' \sim w'$, if $\Lambda(w, w') = \Lambda(v, v')$ then we have $(w, S') \notin \mathcal{I}_{v,S}$. Therefore, we have

$$\begin{aligned}|\mathcal{I}_{v,S}| = \sum_{S' \subset \mathcal{G} \setminus \{S\}} (\mathsf{N}_v(S') - \delta_{S',\Lambda}(v, v')) &= \mathsf{N}_v(\mathcal{G}) - \mathsf{N}_v(S) - \Delta_{\mathcal{G},\Lambda} + \delta_{S,\Lambda}(v, v') \\ &\leq \mathsf{N}_v(\mathcal{G}) - \Delta_{\mathcal{G},\Lambda}\end{aligned}$$

since $\mathsf{N}_v(S) \leq \delta_{S,\Lambda}(v, v')$.

*Recursive Inequality.* Now, we represent $h(\mathcal{G}_{v=w}, \Lambda_{v=w})$ in terms of $h(\mathcal{G}_{-v}, \Lambda)$. We denote $\mathcal{G}' = \mathcal{G} \setminus \{S\}$. Consider $\mathcal{E} = \mathcal{H} \cup \{T\}$ where $\mathcal{H}$ is a subset of $\mathcal{G}'$, $|\mathcal{E}| = \alpha$ and $\ell + 1 < |T| \leq \xi_{\max} + \ell + 1$. We also introduce a label function $\mathcal{L}$, an extension of $\Lambda$ satisfying the condition $h(\mathcal{E}, \mathcal{L}) > 0$.

For any subset $T \subset U$ of size $\ell + 1$, define $\mathcal{E}' =^{\text{def}} \mathcal{H} \cup \{U, T \setminus U\}$. We then define:

$$D(\alpha, \ell) = \max_{\mathcal{H},\mathcal{L},T,U} \left| \frac{1}{2^n} \cdot h(\mathcal{E}', \mathcal{L}) - h(\mathcal{E}, \mathcal{L}) \right|,$$

where the maximum is taken over all choices of $\mathcal{H} \in \mathcal{G}'$ of size $\alpha - 1$, a label function $\mathcal{L}$, a set $T$ with $|T| > \ell + 1$ such that $h(\mathcal{E}, \mathcal{L}) > 0$ and a subset $U \subset T$ of size $\ell + 1$. For all $\ell \leq 0$, we define $D(\alpha, \ell) = 0$.

Now, let $|\mathcal{G}'| = c$ and $\mathcal{H}' = \mathcal{H} \cup \{T \setminus U\}$. There are $c - \alpha + 1$ sets in $\mathcal{G}' \setminus \mathcal{H}$, which can be represented as:

$$\mathcal{G}' \setminus \mathcal{H} = \{B_1, \ldots, B_{c-\alpha+1}\}.$$

For $1 \leq i \leq c - \alpha + 1$, let $\mathcal{H}_i = \mathcal{H} \cup \{B_1, \ldots, B_i\}$ and $\mathcal{H}_0 = \mathcal{H}$. It is easy to see that

$$\frac{h(\mathcal{H}_i, \Lambda)}{h(\mathcal{H}_{i-1}, \Lambda)} \geq 2^n - c\xi_{\max}^2$$

for $1 \leq i \leq c - \alpha + 1$. Since $c\xi_{\max}^2 < 2^n$, the following inequality holds:

$$\frac{h(\mathcal{G}', \Lambda)}{h(\mathcal{H}, \Lambda)} \geq (2^n - c\xi_{\max}^2)^{c-\alpha+1} \tag{14}$$

Moreover, we have

$$h(\mathcal{H}', \mathcal{L}) \leq 2^n h(\mathcal{H}, \Lambda). \tag{15}$$

By combining (14) and (15), we obtain

$$\frac{h(\mathcal{G}', \Lambda)}{h(\mathcal{H}', \mathcal{L})} \geq \frac{(2^n - c\xi_{\max}^2)^{c-\alpha+1}}{2^n}. \tag{16}$$

By using these notations we can derive the recursive inequality.

**Lemma 5.** *The following holds*

$$D(\alpha, \ell) \leq D(\alpha, \ell - 1) + \xi_{\max} \sum_{i=1}^{c} D(\alpha - 1, \ell + \xi_i - 1) + \frac{2\xi_{\max}(\Delta_{\mathcal{G},\Lambda} + 1) \cdot h(\mathcal{G}, \Lambda)}{(2^n - c\xi_{\max}^2)^{c-\alpha+1}}.$$

The proof of Lemma 5 is deferred to Section B.

Let $a_{d,\ell} =^{\text{def}} \frac{\xi_{\max}^d}{4h(\mathcal{G}', \Lambda)} D(c - d, \ell)$. We have

$$a_{d,\ell} \leq a_{d,\ell-1} + \sum_{i=1}^{c} a_{d+1,\ell+\ell_i} + \frac{\Delta_{\mathcal{G},\Lambda} + 1}{2} \cdot \left( \frac{\xi_{\max}}{2^n - c\xi_{\max}^2} \right)^{d+1}$$

where $\ell_i = \xi_i - 1$. Note that

$$D(\alpha, \ell) = \max_{\mathcal{H},\mathcal{L},T,U} \left| \frac{1}{2^n} \cdot h(\mathcal{E}', \mathcal{L}) - h(\mathcal{E}, \mathcal{L}) \right| \leq \frac{2^{n+1} h(\mathcal{G}', \Lambda)}{(2^n - c\xi_{\max}^2)^{d+1}}.$$

since

$$h(\mathcal{E}', \mathcal{L}) \leq \frac{2^{2n} h(\mathcal{G}', \Lambda)}{(2^n - c\xi_{\max}^2)^{c-\alpha+1}},$$
$$h(\mathcal{E}, \mathcal{L}) \leq \frac{2^n h(\mathcal{G}', \Lambda)}{(2^n - c\xi_{\max}^2)^{c-\alpha+1}}.$$

Since

$$\frac{2^n}{2(2^n - c\xi_{\max}^2)} \leq 1,$$

we have

$$a_{d,\ell} \leq \left( \frac{\xi_{\max}}{2^n - c\xi_{\max}^2} \right)^d.$$

Note that $\frac{x}{1-x} \leq \frac{1}{4e}$ if $x \leq \frac{1}{12}$. So,

$$\frac{\xi_{\max}}{2^n - c\xi_{\max}^2} \leq \frac{1}{4e\xi_{\max} c}.$$

We state the recursive inequality lemma used to prove mirror theory [11].

**Lemma 6.** *Suppose $a_{d,\ell} \geq 0$ such that: (i) $a_{d,k} =^{\mathrm{def}} 0$ for all $k < 0$, and (ii) for all $0 \leq d \leq \xi n$ and $0 \leq \ell_i \leq \xi - 1$ for $i \in [q]$, we have*

$$\begin{aligned} a_{d,\ell} &\leq (4\xi eq)^{-d} \\ a_{d,\ell} &\leq a_{d,\ell-1} + \sum_{i=1}^{q} a_{d+1,\ell+\ell_i} + A \cdot (4\xi eq)^{-d} \end{aligned}$$

*for some $A > 0$. Then, for every $\ell \in [\xi - 2]$,*

$$a_{0,\ell} \leq \frac{4}{2^n} + 4A\xi.$$

Proof of this lemma can be found in [11].

By using Lemma 6, we have

$$a_{0,\ell} \leq \frac{4}{2^n} + \frac{2(\Delta_{\mathcal{G},\Lambda} + 1)\xi_{\max}^2}{2^n}.$$

Then, for $(w, S') \in \mathcal{I}_{v,S}$, we have

$$\begin{aligned} \left| \frac{1}{2^n} \cdot h(\mathcal{G}_{-v}, \Lambda) - h(\mathcal{G}_{v=w}, \Lambda_{v=w}) \right| &\leq D(c, |S| - 2) \\ &\leq 4h(\mathcal{G}', \Lambda) a_{0,|S|-2} \\ &\leq \frac{8h(\mathcal{G}', \Lambda)}{2^n}(2 + (\Delta_{\mathcal{G},\Lambda} + 1)\xi_{\max}^2). \end{aligned}$$

Note that

$$\begin{aligned} h(\mathcal{G}_{-v}, \Lambda) &\geq (2^n - \mathsf{N}_v(\mathcal{G})\xi_{\max})\, h(\mathcal{G}', \Lambda) \\ &\geq 2^n \left(1 - \frac{1}{12\xi_{\max}}\right) h(\mathcal{G}', \Lambda) \geq \frac{23 \cdot 2^n}{24} h(\mathcal{G}', \Lambda). \end{aligned}$$

Therefore,

$$\begin{aligned} h(\mathcal{G}_{v=w}, \Lambda_{v=w}) &\leq \frac{1}{2^n} \cdot h(\mathcal{G}_{-v}, \Lambda) + \frac{8h(\mathcal{G}', \Lambda)}{2^n}(2 + (\Delta_{\mathcal{G},\Lambda} + 1)\xi_{\max}^2) \\ &\leq \frac{1}{2^n} \left(1 + \frac{9((\Delta_{\mathcal{G},\Lambda} + 1)\xi_{\max}^2 + 2)}{2^n}\right) h(\mathcal{G}_{-v}, \Lambda) \\ &\leq \frac{1}{2^n} \left(1 + \frac{C(\Delta_{\mathcal{G},\Lambda} + 1)}{2^n}\right) h(\mathcal{G}_{-v}, \Lambda) \end{aligned}$$

where $C = 9(\xi_{\max}^2 + 2)$. Therefore, we have

$$\begin{aligned}
h(\mathcal{G}, \Lambda) &= h(\mathcal{G}_{-v}, \Lambda) - \sum_{(w,S') \in \mathcal{I}_{v,S}} h(\mathcal{G}_{v=w}, \Lambda_{v=w}) \\
&\geq h(\mathcal{G}_{-v}, \Lambda) - \sum_{(w,S') \in \mathcal{I}_{v,S}} \frac{1}{2^n} \left(1 + \frac{C(\Delta_{\mathcal{G},\Lambda} + 1)}{2^n}\right) h(\mathcal{G}_{-v}, \Lambda) \\
&\geq h(\mathcal{G}_{-v}, \Lambda) \left(1 - \frac{\mathsf{N}_v(\mathcal{G}) - \Delta_{\mathcal{G},\Lambda}}{2^n} \left(1 + \frac{C(\Delta_{\mathcal{G},\Lambda} + 1)}{2^n}\right)\right) \\
&= h(\mathcal{G}_{-v}, \Lambda) \left(1 - \frac{\mathsf{N}_v(\mathcal{G}) + 1}{2^n} + \frac{\Delta_{\mathcal{G},\Lambda} + 1}{2^n} \left(1 - \frac{C(\mathsf{N}_v(\mathcal{G}) - \Delta_{\mathcal{G},\Lambda})}{2^n}\right)\right) \\
&\geq h(\mathcal{G}_{-v}, \Lambda) \left(1 - \frac{\mathsf{N}_v(\mathcal{G}) + 1}{2^n}\right)
\end{aligned}$$

since $C \cdot \mathsf{N}_v(\mathcal{G}) \leq 2^n$. It concludes the proof.

## B Proof of Lemma 5

We fix $\mathcal{H} \in \mathcal{G}'$ where $|\mathcal{H}| = \alpha - 1$, a set $T$ with $\ell + 1 \leq |T| \leq \xi_{\max} + \ell + 1$ and a subset $U \in T$ with $|U| = \ell + 1$. Now we prove the inequality in two cases.

First, $|U| = 1$. Let $U = \{v\}$ and $\mathcal{H}' = \mathcal{H} \cup \{T \setminus U\}$. It is easy to see that $h(\mathcal{E}', \mathcal{L}) = (2^n - \mathsf{N}_v(\mathcal{H}')) \cdot h(\mathcal{H}', \mathcal{L})$. Note that $\mathcal{E}_{-v} = \mathcal{H}'$. By (12), we have

$$h(\mathcal{E}, \mathcal{L}) = h(\mathcal{H}', \mathcal{L}) - \sum_{(w,S') \in \mathcal{I}_{v,T}} h(\mathcal{E}_{v=w}, \mathcal{L}_{v=w}).$$

Note that $\mathcal{I}_{v,T} = \{(w, S') \mid w \in S' \in \mathcal{E} \setminus \{T\}, h(\mathcal{E}_{v=w}, \mathcal{L}_{v=w}) > 0\}$. For $w \in S' \in \mathcal{E} \setminus \{T\}$, $(w, S') \notin I_{v,T}$ if and only if there exists $v' \in T$ and $w' \in S'$ such that $\mathcal{L}(v, v') = \mathcal{L}(w, w')$. By (13), we have

$$\begin{aligned}
|\mathcal{I}_{v,T}| &\geq \sum_{S' \in \mathcal{E} \setminus \{T\}} \left(\mathsf{N}_v(S') - \sum_{v' \in T \setminus U} 2\delta_{S',\mathcal{L}}(\mathcal{L}(v, v'))\right) \\
&= \mathsf{N}_v(\mathcal{H}') - \mathsf{N}_v(T \setminus U) - \sum_{v' \in T \setminus U} 2\delta_{\mathcal{H},\mathcal{L}}(\mathcal{L}(v, v')) \\
&\geq \mathsf{N}_v(\mathcal{H}') - 2\xi_{\max}(\Delta_{\mathcal{G},\Lambda} + 1)
\end{aligned}$$

Hence,

$$\begin{aligned}
D(\alpha,0) &= \left|\frac{1}{2^n}\cdot h(\mathcal{E}',\mathcal{L}) - h(\mathcal{E},\mathcal{L})\right| \\
&= \left|\frac{\mathsf{N}_v(\mathcal{H}')}{2^n}\cdot h(\mathcal{H}',\mathcal{L}) - \sum_{(w,S')\in\mathcal{I}_{v,T}} h(\mathcal{E}_{v=w},\mathcal{L}_{v=w})\right| \\
&\le \sum_{(w,S')\in\mathcal{I}_{v,T}} \left|\frac{1}{2^n}\cdot h(\mathcal{H}',\mathcal{L}) - h(\mathcal{E}_{v=w},\mathcal{L}_{v=w})\right| + \frac{2\xi_{\max}(\Delta_{\mathcal{G},\Lambda}+1)\cdot h(\mathcal{H}',\mathcal{L})}{2^n} \\
&\le \xi_{\max}\cdot \sum_{S'\in\mathcal{E}\setminus\{T\}} D(\alpha-1,|S'|-1) + \frac{2\xi_{\max}(\Delta_{\mathcal{G},\Lambda}+1)\cdot h(\mathcal{H}',\mathcal{L})}{2^n} \\
&\le \xi_{\max}\cdot \sum_{S'\in\mathcal{E}\setminus\{T\}} D(\alpha-1,|S'|-1) + \frac{2\xi_{\max}(\Delta_{\mathcal{G},\Lambda}+1)\cdot h(\mathcal{G}',\Lambda)}{(2^n-c\xi_{\max}^2)^{c-\alpha+1}}
\end{aligned}$$

where the third inequality holds since $h(\mathcal{H}',\mathcal{L}) = h(\mathcal{H}',\mathcal{L}_{v=w})$ and the last inequality holds from (16).

Next, we consider $|U| \ge 2$. By (12), for $v \in U$,

$$\begin{aligned}
h(\mathcal{E},\mathcal{L}) &= h(\mathcal{E}_{-v},\mathcal{L}) - \sum_{(w,S')\in\mathcal{I}_{v,T}} h(\mathcal{E}_{v=w},\mathcal{L}_{v=w}) \\
h(\mathcal{E}',\mathcal{L}) &= h(\mathcal{E}'_{-v},\mathcal{L}) - \sum_{(w,S')\in\mathcal{I}_{v,U}} h(\mathcal{E}'_{v=w},\mathcal{L}_{v=w}).
\end{aligned}$$

Note that

$$\begin{aligned}
I &\stackrel{\text{def}}{=} \mathcal{I}_{v,T} = \{(w,S') \mid w\in S'\in\mathcal{H}, h(\mathcal{E}_{v=w},\mathcal{L}_{v=w})>0\}, \\
I' &\stackrel{\text{def}}{=} \mathcal{I}_{v,U} = \{(w,S') \mid w\in S'\in\mathcal{H}', h(\mathcal{E}'_{v=w},\mathcal{L}_{v=w})>0\}.
\end{aligned}$$

It is easy to see that $I \subset I'$. If $(w,S') \in I' \setminus I$, then one of the followings holds

- $S' = T \setminus U$ and $w \in S'$ such that $h(\mathcal{E}'_{v=w},\mathcal{L}_{v=w}) > 0$,
- $S' \in \mathcal{H}$ and $w \in S'$ such that $h(\mathcal{E}'_{v=w},\mathcal{L}_{v=w}) > 0$.

The first case is at most $|T \setminus U|$. The second case will happen if for some $v' \in U$ and $w' \in S'$, $\mathcal{L}(v,v') = \mathcal{L}(w,w')$. Thus

$$|I' \setminus I| \le |T \setminus U| + \sum_{v'\in U} 2\delta_{v,\mathcal{H},\mathcal{L}}(\mathcal{L}(v,v')) \le 2\xi_{\max}(\Delta_{\mathcal{G},\Lambda}+1).$$

By (13), we have

$$\begin{aligned}
&\left|\sum_{(w,S')\in I'}\frac{h(\mathcal{E}'_{v=w},\mathcal{L}_{v=w})}{2^n}-\sum_{(w,S')\in I}h(\mathcal{E}_{v=w},\mathcal{L}_{v=w})\right| \\
&\leq \sum_{(w,S')\in I}\left|\frac{h(\mathcal{E}'_{v=w},\mathcal{L}_{v=w})}{2^n}-h(\mathcal{E}_{v=w},\mathcal{L}_{v=w})\right|+\sum_{(w,S')\in I'\setminus I}\frac{h(\mathcal{E}'_{v=w},\mathcal{L}_{v=w})}{2^n} \\
&\leq \xi_{\max}\sum_{S'\in\mathcal{H}}D(\alpha-1,\ell+|S'|-1)+\sum_{(w,S')\in I'\setminus I}\frac{h(\mathcal{E}'_{v=w},\mathcal{L}_{v=w})}{2^n} \\
&\leq \xi_{\max}\sum_{S'\in\mathcal{H}}D(\alpha-1,\ell+|S'|-1)+\frac{2\xi_{\max}(\Delta_{\mathcal{G},\Lambda}+1)h(\mathcal{E}'_{v=w},\mathcal{L}_{v=w})}{2^n} \\
&\leq \xi_{\max}\sum_{S'\in\mathcal{H}}D(\alpha-1,\ell+|S'|-1)+\frac{2\xi_{\max}(\Delta_{\mathcal{G},\Lambda}+1)\cdot h(\mathcal{G}',\Lambda)}{(2^n-c\xi_{\max}^2)^{c-\alpha+1}}.
\end{aligned}$$

Therefore, we have

$$\begin{aligned}
D(\alpha,\ell) &= \left|\frac{h(\mathcal{E}',\mathcal{L})}{2^n}-h(\mathcal{E},\mathcal{L})\right| \\
&\leq \left|\frac{h(\mathcal{E}'_{-v},\mathcal{L})}{2^n}-h(\mathcal{E}_{-v},\mathcal{L})\right| \\
&\quad+\left|\sum_{(w,S')\in I'}\frac{h(\mathcal{E}'_{v=w},\mathcal{L}_{v=w})}{2^n}-\sum_{(w,S')\in I}h(\mathcal{E}_{v=w},\mathcal{L}_{v=w})\right| \\
&\leq D(\alpha,\ell-1) \\
&\quad+\xi_{\max}\sum_{S'\in\mathcal{H}}D(\alpha-1,\ell+|S'|-1)+\frac{2\xi_{\max}(\Delta_{\mathcal{G},\Lambda}+1)\cdot h(\mathcal{G}',\Lambda)}{(2^n-c\xi_{\max}^2)^{c-\alpha+1}}
\end{aligned}$$

as the last inequality is derived from

$$h(\mathcal{E}'_{v=w},\mathcal{L}_{v=w})\leq h(\mathcal{H}',\mathcal{L})\leq\frac{2^n h(\mathcal{G}',\Lambda)}{(2^n-c\xi_{\max}^2)^{c-\alpha+1}}$$

by (16).