entropy

MDPI

Article

GCM-SIV1.5: Optimal Tradeoff between GCM-SIV1 and GCM-SIV2

Ping Zhang

School of Computer Science, Nanjing University of Posts and Telecommunications, Nanjing 210023, China; zhgp@njupt.edu.cn

Abstract: GCM-SIV2 is a nonce-based beyond-birthday-bound (BBB)-secure authenticated encryption (AE) mode introduced by Iwata and Minematsu at FSE 2017. However, it is built by combining two instances of GCM-SIV1 and needs eight keys, which increases the costs of hardware and software implementation. This paper aims to reduce these costs by optimizing components (such as key materials, hash calls, and block cipher calls) and proposes an optimal tradeoff between GCM-SIV1 and GCM-SIV2 called GCM-SIV1.5. Moreover, we introduce the faulty nonce setting to AE and prove the BBB security of GCM-SIV1.5 with graceful security degradation in the faulty nonce setting by mirror theory. Finally, we discuss advantages of GCM-SIV1.5.

Keywords: nonce-based authenticated encryption; GCM-SIV1; GCM-SIV2; beyond-birthday-bound security; faulty nonce setting; mirror theory

1. Introduction

The Galois Counter Mode (GCM) of operation introduced by McGrew and Viega is a very famous authenticated encryption (AE) mode [1]. Due to its friendly hardware implementation, superior software performance, no patent, and provable security, it has been widely used in high-speed network application environments. For example, GCM with the Advanced Encryption Standard (AES) has been used in IETF Transport Layer Security protocol TLS 1.3. Now, GCM has been included in the recommendations of NIST, ISO/IEC, IEEE, and IETF. As GCM is widely deployed, the CAESAR competition takes it as the baseline algorithm, which further promotes the research of GCM. There exist a large number of research results related to GCM [1–16].

GCM is a nonce-based AE mode. It takes a nonce as an extra input and requires that the nonce used in the encryption oracle is distinct (nonce-respecting setting). If the nonce length is restricted to 96 bits, GCM is provably birthday-bound secure up to approximately $2^{n/2}$ adversarial queries in the nonce-respecting setting [3,5], where n is the block-size of the underlying block cipher.

However, the nonce-respecting assumption does not fit the actual situation. The nonce is often misused in real life, bringing serious security threats. Joux found that, if the nonce is misused, then the hash key of GCM can be leaked and the leaked hash key can be utilized to achieve a universal forgery attack [2]. To settle the nonce misuse problem of GCM at little cost, Gueron and Lindell introduced a nonce-misuse-resistant AE (NMAE or MRAE) scheme GCM-SIV at CCS 2015 [11]. GCM-SIV covers GCM components and follows the SIV approach by Rogaway and Shrimpton [17]. In fact, as the syntax and the security model of NMAE became formalized, more and more NMAE schemes were proposed, such as [11–23]. GCM-SIV is just the first NMAE scheme that introduces SIV into GCM. GCM-SIV is proven secure even if the nonce is repeated. In 2016, Iwata and Minematsu pointed out that there exists a trivial distinguishing attack with approximately $2^{(n-k)/2}$ adversarial queries in GCM-SIV, where k is the bits of keys, and then presented an improved variant of GCM-SIV, called GCM-SIV1, which is proven secure up to $2^{n/2}$

Citation: Zhang, P. GCM-SIV1.5: Optimal Tradeoff between GCM-SIV1 and GCM-SIV2. *Entropy* **2023**, *25*, 107. https://doi.org/10.3390/e25010107

Academic Editor: Raúl Alcaraz

Received: 17 September 2022
Revised: 26 November 2022
Accepted: 30 December 2022
Published: 4 January 2023

(birthday bound) adversarial queries in the nonce misuse setting [12]. Furthermore, they considered a stronger security bound, and then proposed beyond-birthday-bound (BBB)-secure GCM-SIVr schemes that combine $r \geq 2$ instances of GCM-SIV1. BBB indicates that cryptographic schemes can resist beyond $O(2^{n/2})$ adversarial queries. The BBB-secure AE schemes are very rich, such as CHM [24], GCM-SIVr [12], SCT [20], ZAE [21], and PFBw [25]. GCM-SIVr is proven BBB-secure against $O(2^{\frac{rn}{r+1}})$ adversarial queries in the nonce misuse setting. Later, an updated variant of GCM-SIV called AES-GCM-SIV was proposed by Gueron et al., and AES-GCM-SIV was eventually accepted as a recommended standardization of IETF Crypto Forum Research Group [13,15]. Iwata and Seurin also made some important contributions to the promotion of standardization. They pointed out the problems in the earlier version, corrected them, and gave some suggestions for improving the key derivation function [14]. These problems and suggestions are accepted to further improve AES-GCM-SIV [15]. Unlike GCM-SIV, AES-GCM-SIV utilizes a key derivation function to generate the hash key and the encryption key, utilizes POLYVAL instead of GHASH, and invokes the full authentication tag as an initial counter. At Eurocrypt 2018, Bose et al. further considered the multi-user security, faster key derivation, and better bounds of AES-GCM-SIV [16].

Although there exists a large amount of research literature on the nonce misuse setting, the number of nonce misuse is often described vaguely. An effective measure of nonce misuse is the maximum number of its multi-collisions. To specify the level of nonce misuse, Dutta et al. introduced a quantitative index of nonce misuse for message authentication code (MAC) algorithms called the number of faulty nonces [23]. In the faulty nonce setting, a query is called as a faulty query if the nonce in this query is the same as the nonce in the previous queries, i.e., the nonce is re-used. The symbol μ is usually used to indicate the number of faulty nonces. Therefore, the faulty nonce setting covers nonce-respecting and nonce misuse settings. For an adversary that makes, at most, μ faulty queries, (1) if $\mu = 0$, then the adversary is called a nonce-respecting adversary; (2) if $\mu \geq 1$, then the adversary is called a nonce-misusing adversary. Dutta et al. presented a nonce-based MAC scheme, nEHtM, that ensures BBB security with graceful degradation in the faulty nonce setting [23]. Furthermore, they introduced an nEHtM-based AE scheme, CWC+, whose privacy is optimally secure in the nonce-respecting setting and whose authenticity is BBB-secure with graceful degradation in the faulty nonce setting. To ensure the faulty nonce misuse resistance of privacy and authenticity, Choi et al. introduced the first fully faulty nonce-misuse-resistant AE scheme SCM [22]. It utilizes a hash key and three encryption keys. From the perspective of the security, SCM ensures close-to optimal n-bit security in the nonce-respecting setting and supports graceful BBB security degradation (not only for privacy but also for authenticity) in the faulty nonce setting. In recent years, the research about the faulty nonce-misuse-resistant schemes mainly focuses on MACs [26,27]. This paper aims to introduce the faulty nonce setting to GCM-SIVr, and presents an improved AE scheme that ensures full BBB security with graceful degradation in the faulty nonce setting and utilizes as few keys as possible.

Our Contribution. We focus on the optimization of GCM-SIVr in the faulty nonce setting, and propose an optimal tradeoff between GCM-SIV1 and GCM-SIV2 called GCM-SIV1.5, which ensures full BBB security with graceful degradation in the faulty nonce setting. Specifically, our contribution includes:

1. From the point of view of the design, we introduce a BBB-secure sum of permutation (SoP) construction to encryption and authentication parts of GCM-SIV1.5, which makes GCM-SIV1.5 BBB secure. GCM-SIV1.5 follows "MAC-then-Encrypt" (MtE). The authentication part of GCM-SIV1.5 utilizes the construction F_{B2}^{SoP} proposed by Chen et al. [27] to ensure BBB security, and the encryption part of GCM-SIV1.5 is generated by SoP-based counter mode with an initial vector and a nonce CTR^{SoP} to provide BBB security. Moreover, to minimize costs of key management and implementation on software and hardware, and to maximize the running speed, GCM-SIV1.5 just utilizes two block cipher keys and a hash key, invokes a hash function and twice

plaintext blocks, and generates an authentication tag. More importantly, all encryption operations involving the nonce can be carried out offline, which saves half of the online computing resources.

2. From the point of view of the security, we prove that GCM-SIV1.5 enjoys BBB security with graceful degradation in the nonce faulty setting by using mirror theory, alternating events lemma, and the H-coefficient technique. Assuming that the underlying block cipher is a secure pseudorandom permutation (PRP) and the hash function is XOR-universal, then GCM-SIV1.5 is proven secure up to approximately $3n/4$-bit query complexity and approximately n-bit forgery attempts for μ-nonce faulty adversaries with $\mu \leq 2^{n/4}$. In the real world, if the underlying block cipher is instantiated with AES-128, then GCM-SIV1.5 achieves, at most, approximately 96-bit security for μ-nonce faulty adversaries with $\mu \leq 2^{32}$.

In order to better demonstrate the superiority of our design, we give a fair and thorough comparison between GCM-SIV1.5 and existing typical blockcipher-based AE schemes from the following aspects: the depended assumption (PRP means pseudorandom permutation, PRF means pseudorandom function, TPRP means tweakable PRP, and ICM means ideal cipher model), the number of the encryption keys (#Encryption keys), the number of the hash keys (#Hash keys), the number of the underlying primitive (block cipher) calls (#Primitive calls), the number of the hash calls (#Hash calls), the sizes of the authentication tag and nonce, security bound under the nonce-respecting scenario (NR security), security bound under the nonce misuse scenario (NM security), and graceful degradation. The details are shown in Table 1. Compared with GCM-SIV, GCM-SIV1, GCM-SIV2, and GCM-SIVr, GCM-SIV1.5 utilizes fewer keys, fewer blockcipher and hash calls, and shorter sizes, provides a better security bound, and supports graceful security degradation. Therefore, GCM-SIV1.5 reduces the costs of key management and communication throughput, increases the running speed, and ensures a graceful security. Compared with CWC+, GCM-SIV1.5 provides a better security bound and supports fully faulty nonce misuse resistance and graceful security degradation for both privacy and authenticity. Compared with SCM, GCM-SIV1.5 saves an encryption key, supports offline operations involving the nonce's encryption, and saves half of the online computing resources. In a word, our design has an excellent comprehensive performance.

Table 1. Comparison between GCM-SIV1.5 and existing typical nonce-based AE schemes, where PRP means pseudorandom permutation, PRF means pseudorandom function, TPRP means tweakable PRP, ICM means ideal cipher model, # means counting, m is blocks of the plaintext, a is blocks of associated data, and n is the block-size of the underlying primitive.

	Assumption	**#Encryption Keys**	**#Hash Keys**	**#Primitive Calls**	**#Hash Calls**
GCM [5]	PRP	1	1	$m+1$	1
ELmD [19]	PRP	1	0	$a+2m+2$	0
OCB3 [28]	PRP	1	1 [1]	$a+m+2$	1 [2]
ΘCB3 [28]	TPRP	1	1 [1]	$a+m+1$	1 [2]
mGCM [29]	PRP	1	1	$m+1$	1
GCM-SIV [11]	PRF	2	1	$m+1$	1
AES-GCM-SIV [15]	ICM	1 [3]	1 [4]	$m+1$	1
GCM-SIV1 [12]	PRP	2	1	$m+1$	1
GCM-SIV2 [12]	PRP	6	2	$2m+4$	2
GCM-SIVr [12]	PRP	r^2+r	r	$rm+r^2$	r
CWC+ [23]	PRP	1	1 [5]	$m+3$	1
SCM [22]	PRP	3	1	$m+5$	1
GCM-SIV1.5	PRP	2	1	$2m+2$	1

Table 1. *Cont.*

	Tag Size	Nonce Size	NR Security	NM Security	Graceful Degradation
GCM [5]	$\leq n$	$3n/4$	$O(2^{n/2})$	-	×
ELmD [19]	n	n	$O(2^{n/2})$	$O(2^{n/2})$	×
OCB3 [28]	$\leq n$	$\leq n$	$O(2^{n/2})$	-	×
ΘCB3 [28]	$\leq n$	$\leq n$	$O(2^{n})$	-	×
mGCM [29]	n	n	$O(2^{n})$	-	×
GCM-SIV [11]	n	n	$O(2^{n/2})$	$O(2^{n/2})$	×
AES-GCM-SIV [15]	n	$3n/4$	$O(2^{3n/4})$	$O(2^{n/2}) \sim O(2^{3n/4})$	✓
GCM-SIV1 [12]	n	n	$O(2^{n/2})$	$O(2^{n/2})$	×
GCM-SIV2 [12]	$2n$	n	$O(2^{2n/3})$	$O(2^{2n/3})$	×
GCM-SIVr [12]	rn	n	$O(2^{rn/r+1})$	$O(2^{rn/r+1})$	×
CWC+ [23]	$\leq n$	$3n/4$	$O(2^{2n/3})$	$O(2^{n/2}) \sim O(2^{2n/3})$ [6]	✓
SCM [22]	n	$n-2$	$O(2^{n})$	$O(2^{n/2}) \sim O(2^{n})$	✓
GCM-SIV1.5	n	$3n/4$	$O(2^{3n/4})$	$O(2^{n/2}) \sim O(2^{3n/4})$	✓

[1] The hash key is the encryption key. [2] The hash function is achieved by invoking a underlying primitives. [3] The encryption key is generated by invoking a key derivation function. [4] The hash key is generated by invoking a key derivation function. [5] The hash key is generated by the encryption key. [6] This security bound is just that of authenticity. The privacy of CWC+ is insecure in the nonce misuse setting.

The rest of this paper is organized as follows. Section 2 presents some preliminaries. Section 3 introduces mirror theory and its graph description. Section 4 shows the decomposition of nAE security. Section 5 described GCM-SIVr. Section 6 proposes our construction, GCM-SIV1.5. Section 7 derives the security proof. Section 8 concludes this paper.

2. Preliminaries

Notations. Some notations are described in Table 2.

Table 2. Descriptions of notations.

Notations	Descriptions
$\oplus$	the bitwise exclusive or (XOR)
$+$	addition modulo 2^n
$\cdot$	the multiplication over the finite field
$\|\|$	the concatenation of strings
$\{0,1\}^*$	a set of all strings (including an empty string)
$\{0,1\}^n$	a set of all strings whose bit-length is n
$Perm(n)$	a set of all permutations whose workspace is n
$Func(m,n)$	a set of all functions from m-bit inputs to n-bit outputs
$K \twoheadleftarrow \mathcal{K}$	the key K randomly sampled from the key space $\mathcal{K}$
$\mathcal{A}^O = 1$	an event where an adversary $\mathcal{A}$ outputs 1 after interacting with the oracle O
$[i]_m$	an m-bit binary representation of an integer i
$[r]$	a set of consecutive integers $\{1,2,\cdots,r\}$
$\|X\|$	the number of elements in the set X
$(2^n)_q$	$2^n \cdot (2^n-1)\cdots(2^n-q+1)$

Nonce-Based Authenticated Encryption (nAE). A nonce-based authenticated encryption (nAE) with associated data scheme $\Pi = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ consists of an encryption algorithm $\mathcal{E}$ and a decryption algorithm $\mathcal{D}$, where $\mathcal{K}$ is a non-empty set of keys. Let $K \in \mathcal{K}$. The encryption algorithm $\mathcal{E}$ takes a key K, a nonce N, associated data A, and a message M as the input and outputs a ciphertext and an authentication tag $(C,T) = \mathcal{E}_K(N,A,M)$. The decryption algorithm $\mathcal{D}$ takes a key K, a nonce N, associated data A, a ciphertext C, and an authentication tag T as the input and outputs a message or a reject symbol $M/\perp = \mathcal{D}_K(N,A,C,T)$. Here, $\mathcal{D}_K(N,A,\mathcal{E}_K(N,A,M)) = M$.

An nAE adversary $\mathcal{A}$ has access to encryption and decryption oracles $(\mathcal{E}_K, \mathcal{D}_K)$ or random and reject oracles $(\$, \perp)$, whose goal is to distinguish them. The random oracle

$\$$ takes (N, A, M) as the input and always outputs random strings $(C, T) \twoheadleftarrow \{0,1\}^{|M|+|T|}$. The reject oracle $\perp$ takes (N, A, C, T) as the input and always outputs a reject symbol $\perp$. The nAE advantage of $\mathcal{A}$ against Π is defined as

$$Adv_{\Pi}^{nAE}(\mathcal{A}) = |Pr[K \twoheadleftarrow \mathcal{K} : \mathcal{A}^{\mathcal{E}_K, \mathcal{D}_K} = 1] - Pr[\mathcal{A}^{\$,\perp} = 1]|.$$

We assume that $\mathcal{A}$ makes q encryption queries $(N^1, A^1, M^1), \cdots, (N^q, A^q, M^q)$ to $\mathcal{E}_K$ and returns $(C^1, T^1), \cdots, (C^q, T^q)$, and then makes q_v forgery attempts $(N'^1, A'^1, C'^1, T'^1), \cdots, (N'^{q_v}, A'^{q_v}, C'^{q_v}, T'^{q_v})$ to $\mathcal{D}_K$. For a nonce-based AE scheme, we call an AE query a faulty query if $\mathcal{A}$ has already queried its oracle with the same nonce, and assume that $\mathcal{A}$ can be allowed to make, at most, μ faulty queries. Then, $\mu = 0$ ($N^1, \cdots, N^q$ are distinct) corresponds to the nonce-respecting setting and $\mu \geq 1$ (there exists at least one collision in $N^1, \cdots, N^q$) corresponds to the nonce misuse setting.

Nonce-Based Encryption (nE). A nonce-based encryption (nE) scheme $\mathbf{E} = (\mathcal{K}_{\mathbf{E}}, \mathbf{E}-\mathcal{E}, \mathbf{E}-\mathcal{D})$ consists of an encryption algorithm $\mathbf{E}-\mathcal{E}$ and a decryption algorithm $\mathbf{E}-\mathcal{D}$. The encryption algorithm $\mathbf{E}-\mathcal{E}$ takes a key $K_{\mathbf{E}}$, a nonce N, associated data A, and a message M as the input and outputs a ciphertext $C = \mathbf{E}-\mathcal{E}_{K_{\mathbf{E}}}(N, A, M)$. The decryption algorithm $\mathbf{E}-\mathcal{D}$ takes a key $K_{\mathbf{E}}$, a nonce N, associated data A, and a ciphertext C as the input and outputs a message $M = \mathbf{E}-\mathcal{D}_{K_{\mathbf{E}}}(N, A, C)$. Here, $\mathbf{E}-\mathcal{D}_{K_{\mathbf{E}}}(N, A, \mathbf{E}-\mathcal{E}_{K_{\mathbf{E}}}(N, A, M)) = M$.

An nE adversary $\mathcal{A}$ has access to encryption oracle $\mathbf{E}-\mathcal{E}_{K_{\mathbf{E}}}$ or a random oracle $\$$, whose goal is to distinguish them. The random oracle $\$$ takes (N, A, M) as the input and always outputs random strings $C \twoheadleftarrow \{0,1\}^{|C|}$. We define the nE-advantage of $\mathcal{A}$ as

$$Adv_{\mathbf{E}}^{nE}(\mathcal{A}) = |Pr[K_{\mathbf{E}} \twoheadleftarrow \mathcal{K}_{\mathbf{E}} : \mathcal{A}^{\mathbf{E}-\mathcal{E}_{K_{\mathbf{E}}}} = 1] - Pr[\mathcal{A}^{\$} = 1]|.$$

Pseudo-Random Function (PRF). Let $F : \mathcal{K}_F \times \{0,1\}^m \to \{0,1\}^n$ be a keyed function, where $\mathcal{K}_F$ is a non-empty set of keys. It takes $K \in \mathcal{K}_F$ and $X \in \{0,1\}^m$ as the input, and returns $Y = F_K(X) \in \{0,1\}^n$. Let $R \twoheadleftarrow Func(m, n)$.

A PRF adversary $\mathcal{A}$ has access to encryption oracle F_K or a random oracle R, whose goal is to distinguish them. The PRF advantage of an adversary $\mathcal{A}$ is defined as

$$Adv_{F}^{prf}(\mathcal{A}) = |Pr[K \twoheadleftarrow \mathcal{K}_F : \mathcal{A}^{F_K} = 1] - Pr[\mathcal{A}^{R} = 1]|.$$

Pseudo-Random Permutation (PRP). Let $E : \mathcal{K}_E \times \{0,1\}^n \to \{0,1\}^n$ be a block cipher, where $\mathcal{K}_E$ is a non-empty set of keys. It takes a key $K \in \mathcal{K}_E$ and a plaintext block $M \in \{0,1\}^n$ as the input, and returns a ciphertext block $C = E_K(M)$. For each key $K \in \mathcal{K}_E$, the function $E_K : \{0,1\}^n \to \{0,1\}^n$ is a permutation, i.e., $E_K \in Perm(n)$. Let $P \twoheadleftarrow Perm(n)$.

A PRP adversary $\mathcal{A}$ has access to encryption oracle E_K or a random permutation oracle P, whose goal is to distinguish them. The PRP advantage of an adversary $\mathcal{A}$ is defined as

$$Adv_{E}^{prp}(\mathcal{A}) = |Pr[K \twoheadleftarrow \mathcal{K}_E : \mathcal{A}^{E_K} = 1] - Pr[\mathcal{A}^{P} = 1]|.$$

AXU Hash Functions [22,26,27,30]. Let $H : \mathcal{K}_H \times \{0,1\}^* \to \{0,1\}^n$ be a hash function, where $\mathcal{K}_H$ is a non-empty hash key space. Let L be a hash key randomly drawn from $\mathcal{K}_H$. If, for any distinct $x, x' \in \{0,1\}^*$ and $y \in \{0,1\}^n$, it holds that

$$Pr[H_L(x) \oplus H_L(x') = y] \leq \epsilon,$$

then H is called ϵ almost XOR universal (ϵ-AXU). If $\epsilon = 2^{-n}$, H is called an XOR universal (XU) hash function.

Alternating Events Lemma [26,27,30]. For bounding the probability of an alternating event, such as

$$H_L(x_i) = H_L(x_j) \wedge H_{L'}(x_j) = H_{L'}(x_k) \wedge H_L(x_k) = H_L(x_l),$$

the alternating events lemma is a vital technique in the security proofs.

Lemma 1 (Alternating Events Lemma [26,27,30]). *Let q_i, q_j, q_k, q_l, q such that $q_i, q_j, q_k, q_l \leq q$. Let $X^q = (X_1, \cdots, X_q)$ be a q-tuple of random variables, and let $X^{q_i}, X^{q_j}, X^{q_k}, X^{q_l} \subseteq X^q$. For distinct $i \in [q_i], j \in [q_j]$, let $E_{i,j}$ be events associated with $X_i \in X^{q_i}$ and $X_j \in X^{q_j}$, possibly dependent, which all hold with a probability of, at most, ϵ. For distinct $i \in [q_i], j \in [q_j]$, $k \in [q_k], l \in [q_l]$, let $F_{i,j,k,l}$ be events associated with $X_i \in X^{q_i}, X_j \in X^{q_j}, X_k \in X^{q_k}$ and $X_l \in X^{q_l}$, which all hold with a probability of, at most, ϵ'. Moreover, the collection of events $(F_{i,j,k,l})_{i,j,k,l}$ is independent with the collection of event $(E_{i,j})_{i,j}$. Then, there exist $i \in [q_i], j \in [q_j], k \in [q_k], l \in [q_l]$ such that*

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

H-coefficient Technique [31]. Patarin's H-coefficient technique is one of the very useful approaches to upper bound the distinguishing advantage of a cryptographic scheme. Given a real system X and an ideal system Y, let $\mathcal{A}$ be a deterministic adversary whose goal is distinguish X from Y. $\mathcal{A}$ interacts with X and Y and a series of query–response pairs are recorded as a transcript τ. Let $\mathcal{T}$ be the set of all possible transcripts. Let X_{re} be the random variable interacting with the real system X and Y_{id} be the random variable interacting with the ideal system Y. Then, the H-coefficient lemma is presented as follows.

Lemma 2 (H-coefficient Lemma). *Let $\mathcal{T} = \mathcal{T}_{good} \cup \mathcal{T}_{bad}$ and $\varepsilon, \delta \in [0, 1]$. If $Pr[Y_{id} \in \mathcal{T}_{bad}] \leq \varepsilon$ and for all $\tau \in \mathcal{T}_{good}$, $Pr[X_{re} = \tau]/Pr[Y_{id} = \tau] \geq 1 - \delta$, then*

$$|Pr[\mathcal{A}^X = 1] - Pr[\mathcal{A}^Y = 1]| \leq \varepsilon + \delta.$$

If an adversary makes q queries to an oracle O and obtains a transcript $\tau = \{(x_1, y_1), \cdots, (x_q, y_q)\}$, then we say that the oracle O extends the transcript τ and write it as $O \vdash \tau$, i.e., if $O(x_i) = y_i$ for all $i \in [q]$, then $O \vdash \tau$.

3. Mirror Theory

Patarin's mirror theory is a vital tool for bounding the number of solutions of affine systems of multivariate equations or non-equations, which can be applied in the security proofs of BBB-secure cryptographic schemes [27,32–35]. Here, we consider an affine system of bi-variate equations.

Let $G =< V_1, V_2, E, W >$ be a bipartite graph satisfying the following affine system of bi-variate equations $\mathcal{E}$:

$$\begin{cases} X_1 \oplus Y_1 = \lambda_1 \\ X_2 \oplus Y_2 = \lambda_2 \\ \cdots\cdots\cdots\cdots \\ X_q \oplus Y_q = \lambda_q \end{cases}$$

where $X_i \neq Y_j \in \{0,1\}^n$ for any i and j, and let the vertex sets V_1, V_2, the edge set E, and the weighted (labeled) function W be

$$\begin{aligned} &V_1 = \{X_1, , \cdots, X_q\}, V_2 = \{Y_1, \cdots, Y_q\}, \\ &E = \{e_i = (X_i, Y_i), i \in [q]\}, \\ &W : E \to \{0,1\}^n \setminus \{0^n\}, \text{ and } W(e_i) = \lambda_i, i \in [q]. \end{aligned}$$

We assume that G can be divided into α components with more than two vertexes and β components with just two vertexes, i.e., $G = C_1 \cup \cdots \cup C_\alpha \cup D_1 \cup \cdots \cup D_\beta$.

For a bipartite graph G, we say that G is good if it satisfies the following conditions:

- Acylic. G must contain no cycle.
- Non-zero path label (NPL). $W(\mathcal{P}) \neq 0$ for all paths $\mathcal{P}$ with an even length in the graph G, where $W(\mathcal{P}) = \sum_{e \in \mathcal{P}} W(e)$.

Lemma 3 (Bipartite Graph Description of Mirror Theory [27,35])**.** *Let $G =< V_1, V_2, E, W >$ be a good bipartite graph induced by $\mathcal{E}$, and $|V_1| = q' \leq q, |V_2| = q'' \leq q, |E| = q$. Let q_c be the total edges of components with more than two vertexes. Then, the number of solutions to $\mathcal{E}$ that are chosen from $\{0,1\}^n$ is at least*

$$\frac{(2^n)_{q'}(2^n)_{q''}}{2^{nq}}(1-\delta),$$

where

$$\delta = \frac{9q_c^2}{8 \cdot 2^n} + \frac{9q_c^2 q + 12q_c q^2 + 8q^2}{8 \cdot 2^{2n}} + \frac{8q^4}{3 \cdot 2^{3n}}.$$

4. Decomposition of nAE Security

Namprempre et al. explored the generic composition of nAE and revealed the decomposition of nAE (security) from IV-based or nonce-based encryption and an MAC [36]. Now, let us focus on N3 type nAE schemes.

An N3 type nAE scheme $\Pi = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ consists of a PRF $\mathbf{F}$ and an nE scheme $\mathbf{E}$, where $\mathcal{K}$ is the key space, $\mathcal{E}$ is the encryption algorithm, and $\mathcal{D}$ is the decryption algorithm. Given $K = (K_{\mathbf{F}}, K_{\mathbf{E}}) \xleftarrow{\$} \mathcal{K} = \mathcal{K}_{\mathbf{F}} \times \mathcal{K}_{\mathbf{E}}$, $\mathcal{E}$ takes (N, A, M) as the input and returns $(C, T) = \mathcal{E}_K(N, A, M)$. To be specific, first let $T = \mathbf{F}_{K_{\mathbf{F}}}(N, A, M)$, and then $C = \mathbf{E} - \mathcal{E}_{K_{\mathbf{E}}}(N, T, M)$. $\mathcal{D}$ takes (N, A, C, T) as the input and returns $M/\perp = \mathcal{D}_K(N, A, C, T)$. To be specific, first let $M = \mathbf{E} - \mathcal{D}_{K_{\mathbf{E}}}(N, T, C)$ and $T' = \mathbf{F}_{K_{\mathbf{F}}}(N, A, M)$, and then return M if $T = T'$ and $\perp$ otherwise.

Type N3 nAE is secure if its tag generation function is a PRF and if the nE scheme is secure [36]. We assume that an adversary $\mathcal{A}$ makes, at most, q encryption queries and q_v forgery attempts; then, the security of Π is shown in the following lemma.

Lemma 4 (Decomposition of nAE Security [36])**.** *Let $\boldsymbol{F} : \mathcal{K}_{\boldsymbol{F}} \times \mathcal{N} \times \mathcal{H} \times \mathcal{M} \to \mathcal{T}$ be a tag generation function and $\boldsymbol{E} : \mathcal{K}_{\boldsymbol{E}} \times \mathcal{N} \times \mathcal{T} \times \mathcal{M} \to \mathcal{C}$ be an nE scheme, where $\mathcal{T} = \{0,1\}^\tau$. Let $\Pi = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ be an N3 type nAE scheme constructed by $\boldsymbol{F}$ and $\boldsymbol{E}$. Let $\mathcal{A}$ be an nAE-adversary. Then, there are two adversaries, $\mathcal{B}$ and $\mathcal{C}$, such that*

$$Adv_{\Pi}^{nAE}(\mathcal{A}) \leq Adv_{\boldsymbol{F}}^{prf}(\mathcal{B}) + Adv_{\boldsymbol{E}}^{nE}(\mathcal{C}) + \frac{q_v}{2^\tau}.$$

The above lemma shows that the security proofs of nAE schemes are reduced to the security proofs of the PRF and the nE scheme.

5. GCM-SIVr

Let us first review the specification of GCM-SIVr [12], where $r \geq 1$ is an integer. It utilizes a block cipher $E : \mathcal{K}_E \times \{0,1\}^n \to \{0,1\}^n$ and a hash function $H : \mathcal{K}_H \times \{0,1\}^* \to \{0,1\}^n$. The encryption algorithm $\mathcal{E}$ of GCM-SIVr takes a key $K = (L_1, \cdots, L_r, K'_1, \cdots, K'_{r^2}, K_1, \cdots, K_r) \in (\mathcal{K}_H)^r \times (\mathcal{K}_E)^{r^2+r}$, a nonce N, associated data A, and a plaintext M as the input, and returns a ciphertext C and an authentication tag $T = T_1 || \cdots || T_r$, i.e., $(C, T_1 || \cdots || T_r) = \mathcal{E}_K(N, A, M)$. The decryption algorithm $\mathcal{D}$ of GCM-SIVr takes K, N, A, C, and T as the input, and returns $M/\perp = \mathcal{D}_K(N, A, C, T)$. The details are shown in Algorithms 1–5. GCM-SIV1 and GCM-SIV2 are degraded versions of GCM-SIVr when $r = 1$ and 2.

Algorithm 1 The key generation algorithm: $\mathcal{KG}$

Input: a key parameter k
Output: a key $K = (L_1, \cdots, L_r, K'_1, \cdots, K'_{r^2}, K_1, \cdots, K_r)$
$(L_1, \cdots, L_r, K'_1, \cdots, K'_{r^2}, K_1, \cdots, K_r) \xleftarrow{\$} (\mathcal{K}_H)^r \times (\mathcal{K}_E)^{r^2+r}$
return $K = (L_1, \cdots, L_r, K'_1, \cdots, K'_{r^2}, K_1, \cdots, K_r)$

Algorithm 2 The encryption algorithm: $\mathcal{E}$

Input: a key K, a nonce N, associated data A, and a plaintext M
Output: a ciphertext C and a tag T
Partition M into $M_1 \| \cdots \| M_m$, $|M_i| = n, 1 \le i \le m-1, 0 < |M_m| \le n$
for $i = 1$ **to** r **do**
  $V_i = H_{L_i}(N, A, M) = GHASH_{L_i}(A, M) \oplus N$
  $T_i = 0^n$
endfor
for $i = 1$ **to** r **do**
  for $j = 1$ **to** r **do**
    $T_i = T_i \oplus E_{K'_{i+r(j-1)}}(V_j)$
  endfor
endfor
for $i = 1$ **to** r **do**
  $S_i = CTR_{K_i}(T_i, m)$
  $M = M \oplus msb_{|M|}(S_i)$
endfor
$C \leftarrow M$
$T = T_1 || \cdots || T_r$
return (C, T)

Algorithm 3 The decryption algorithm: $\mathcal{D}$

Input: a key K, a nonce N, associated data A, a ciphertext C, and a tag T
Output: a plaintext M or $\perp$
Partition C into $C_1 \| C_2 \| \cdots \| C_m$, $|C_i| = n, 1 \le i \le m-1, 0 < |C_m| \le n$
for $i = 1$ **to** r **do**
  $S_i = CTR_{K_i}(T_i, m)$
  $C = C \oplus msb_{|C|}(S_i)$
endfor
$M \leftarrow C$
for $i = 1$ **to** r **do**
  $V_i = H_{L_i}(N, A, M) = GHASH_{L_i}(A, M) \oplus N$
  $T_i = 0^n$
endfor
for $i = 1$ **to** r **do**
  for $j = 1$ **to** r **do**
    $T_i = T_i \oplus E_{K'_{i+r(j-1)}}(V_j)$
  endfor
endfor
$T' = T_1 || \cdots || T_r$
if $T' = T$, **return** M
else return $\perp$ (INVALID)
endif

Algorithm 4 GHASH algorithm: $GHASH_L(A, M)$

Input: a key L, associated data A, and a plaintext M
Output: a hash value h
$A^+ \leftarrow A||0^{n-|A| \bmod n}$, $M^+ \leftarrow M||0^{n-|M| \bmod n}$
$X \leftarrow A^+||M^+||[|A|]_{n/2}||[|M|]_{n/2}$
$X_1\| \cdots \|X_x \leftarrow X, |X_i| = n, 1 \leq i \leq x$
$h \leftarrow 0$
for $i = 1$ **to** x **do**
  $h \leftarrow (h \oplus X_i) \cdot L$
endfor
return h

Algorithm 5 CTR algorithm: $CTR_K(T, m)$

Input: a key K, an initial vector T, and the number of plaintext blocks m
Output: a key stream S
$S_1 = E_K(T)$
for $i = 2$ **to** m **do**
  $S_i \leftarrow E_K(T + i - 1)$
endfor
return $S = S_1|| \cdots ||S_m$

6. GCM-SIV1.5

6.1. Specific Description of GCM-SIV1.5

Both GCM-SIV1 and GCM-SIV2 are nonce-based authenticated encryption with associated data modes by combining a PRF and an ivE scheme. GCM-SIV1 enjoys birthday-bound security up to almost $2^{n/2}$ adversarial queries by using an n-bit authentication tag. GCM-SIV2 utilizes two instances of GCM-SIV1 to achieve beyond-birthday-bound (BBB) security by increasing the number of keys, authentication tags, and block ciphers. However, these methods greatly affect the implementation cost and operation efficiency of cryptographic algorithms. In real life, cryptographic algorithms that provide BBB security, as low as possible hardware and software implementation costs, and high enough operational efficiencies are much more desirable.

Given an ϵ-AXU-hash function $H : \mathcal{K}_H \times \mathcal{N} \times \mathcal{H} \times \mathcal{M} \rightarrow \{0,1\}^n$ and a block cipher $E : \mathcal{K}_E \times \{0,1\}^n \rightarrow \{0,1\}^n$, where $\mathcal{K}_H$ and $\mathcal{K}_E$ are two non-empty sets of keys, and n is the block-size, we construct a new two-pass parallelizable nAE mode, GCM-SIV1.5. GCM-SIV1.5 is an optimal tradeoff between GCM-SIV1 and GCM-SIV2 for supporting BBB security with graceful degradation, as low as possible hardware and software implementation costs, and high enough operational efficiencies in nonce-faulty settings. We introduce a sum of permutation (SoP) construction to encryption and authentication parts of GCM-SIV1.5, which makes GCM-SIV1.5 BBB-secure. The authentication part of GCM-SIV1.5 is generated by $F_{B_2}^{SoP}$, which ensures BBB security. The encryption part of GCM-SIV1.5 is generated by CTR^{SoP} with an initial vector and a nonce, which ensures BBB security.

The overview of GCM-SIV1.5 is illustrated in Figure 1.

GCM-SIV1.5 consists of a key generation algorithm $\mathcal{KG}$, an encryption algorithm $\mathcal{E}$, and a decryption algorithm $\mathcal{D}$. The key generation algorithm $\mathcal{KG}$ takes a key parameter k as the input and returns a key $K = (K_1, K_2, L)$ (two encryption keys K_1, K_2 and a hash key L) from an entropy pool of a set of keys $\mathcal{K} = (\mathcal{K}_E, \mathcal{K}_E, \mathcal{K}_H) = \{0,1\}^k$. The encryption algorithm $\mathcal{E}$ takes a key $K = (K_1, K_2, L)$, a nonce N, associated data A, and a plaintext M as the input, invokes the tag generation algorithm $F_{B_2}^{SoP}$ and CTR with the SoP algorithm CTR^{SoP}, and outputs the corresponding ciphertext and authentication tag $(C, T) = \mathcal{E}_K(N, A, M)$. The decryption algorithm $\mathcal{D}$ takes a key $K = (K_1, K_2, L)$, a nonce N, associated data A, a ciphertext C, and an authentication tag T as the input, invokes the tag generation algorithm $F_{B_2}^{SoP}$ and CTR with the SoP algorithm CTR^{SoP}, and outputs the corresponding plaintext M or a reject symbol $\perp$, i.e., $M/\perp = \mathcal{D}_K(N, A, C, T)$. The key generation, encryption, and

decryption algorithms are described in Algorithms 6–8. The tag generation algorithm $F_{B_2}^{SoP}$ and CTR with the SoP algorithm CTR^{SoP} are described in Algorithms 9 and 10.

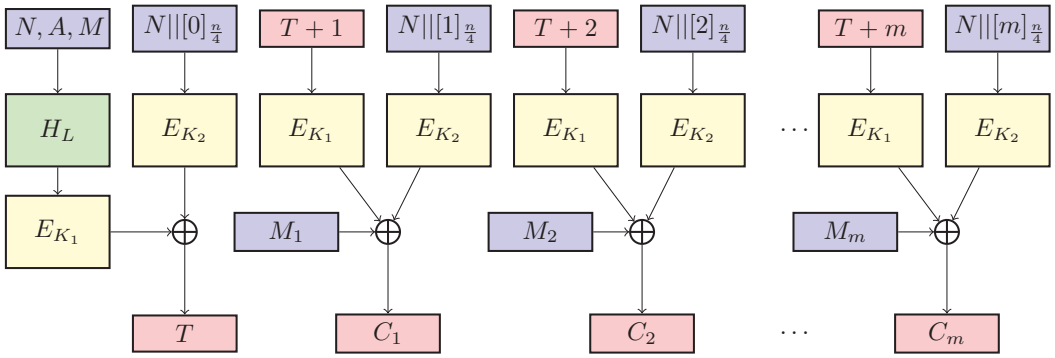

Figure 1. GCM-SIV1.5: An optimal tradeoff between GCM-SIV1 and GCM-SIV2.

Algorithm 6 The key generation algorithm: $\mathcal{KG}$

Input: a key parameter k
Output: a key $K = (K_1, K_2, L)$
$(K_1, K_2, L) \xleftarrow{\$} \mathcal{K} = (\mathcal{K}_E, \mathcal{K}_E, \mathcal{K}_H)$
return $K = (K_1, K_2, L)$

Algorithm 7 The encryption algorithm: $\mathcal{E}$

Input: a key $K = (K_1, K_2, L)$, a nonce N, associated data A, and a plaintext M
Output: a ciphertext C and a tag T
Partition M into $M_1 \| \cdots \| M_m$, $|M_i| = n, 1 \leq i \leq m-1, 0 < |M_m| \leq n$
$T = F_{B_2}^{SoP}(K, N, A, M)$
$S = CTR_{K_1,K_2}^{SoP}(N, T, m)$
$C = M \oplus msb_{|M|}(S)$
return (C, T)

Algorithm 8 The decryption algorithm: $\mathcal{D}$

Input: a key $K = (K_1, K_2, L)$, a nonce N, associated data A, a ciphertext C, and a tag T
Output: a plaintext M or $\perp$
Partition C into $C_1 \| C_2 \| \cdots \| C_m$, $|C_i| = n, 1 \leq i \leq m-1, 0 < |C_m| \leq n$
$S = CTR_{K_1,K_2}^{SoP}(N, T, m)$
$M = C \oplus msb_{|C|}(S)$
$T' = F_{B_2}^{SoP}(K, N, A, M)$
if $T' = T$, **return** M
else return $\perp$ (INVALID)
endif

Algorithm 9 The tag generation algorithm: $F_{B_2}^{SoP}(K, N, A, M)$

Input: a key $K = (K_1, K_2, L)$, a nonce N, associated data A, and a plaintext M
Output: a tag T
$V = H_L(N, A, M) = GHASH_L(A, M) \oplus N||[0]_{\frac{n}{4}}$
$T = E_{K_1}(V) \oplus E_{K_2}(N||[0]_{\frac{n}{4}})$
return T

Algorithm 10 CTR with SoP algorithm: $CTR^{SoP}_{K_1,K_2}(N,T,m)$

Input: a key $K=(K_1,K_2)$, a nonce N, an initial vector T, and the number of plaintext blocks m
Output: a key stream S
for $1 \le i \le m$
$S_i = E_{K_1}(T+i) \oplus E_{K_2}(N||[i]_{\frac{n}{4}})$
endfor
return $S = S_1||\cdots||S_m$

6.2. Security of GCM-SIV1.5

We present the information-theoretic security of GCM-SIV1.5 under the assumption that the underlying block cipher is a secure pseudorandom permutation.

GCM-SIV1.5 is an N3 type nAE scheme (and it can also be seen as an A7 type nAE scheme); therefore, it can be decomposed into a PRF **F** and an nE scheme **E**, where $\mathbf{F}: \mathcal{K}_\mathbf{F} \times \mathcal{N} \times \mathcal{H} \times \mathcal{M} \to \mathcal{T}$, $\mathbf{E}: \mathcal{K}_\mathbf{E} \times \mathcal{N} \times \mathcal{T} \times \mathcal{M} \to \mathcal{C}$, $\mathcal{K}_\mathbf{F} = \mathcal{K}_H \times \mathcal{K}_E \times \mathcal{K}_E = \mathcal{K}$, and $\mathcal{K}_\mathbf{E} = \mathcal{K}_E \times \mathcal{K}_E$.

F takes a key $K_\mathbf{F} = (L, K_1, K_2) \in \mathcal{K}_\mathbf{F}$, a nonce $N \in \mathcal{N}$, associated data $A \in \mathcal{H}$, and a message $M \in \mathcal{M}$ as the input and returns an authentication tag $T = \mathbf{F}(K_\mathbf{F}, N, A, M) = F^{SoP}_{B_2}(K, N, A, M)$. **E** takes the key $K_\mathbf{E} = (K_1, K_2) \in \mathcal{K}_\mathbf{E}$, the nonce $N \in \mathcal{N}$, the authentication tag $T \in \mathcal{T}$, and the message $M \in \mathcal{M}$ as the input, computes a key-stream $S = CTR^{SoP}_{K_\mathbf{E}}(N,T,m)$, and then encrypts M to return the corresponding ciphertext $C = \mathbf{E}(K_\mathbf{E}, N, T, M) = M \oplus msb_{|M|}(S)$.

According to Lemma 4, the nAE security of GCM-SIV1.5 can be decomposed into the PRF security of **F** and the nE security of **E**. Therefore, we have the following lemmas.

Lemma 5. *Let $\mathcal{A}$ be an μ-fault adversary and H_L be ϵ-AXU. Let $\mu \le q^{\frac{1}{3}}$. If $\mathcal{A}$ makes at most $q \le 2^{3n/4}$ queries, then there exist adversaries $\mathcal{A}_1$ and $\mathcal{A}_2$ with the same query complexity against the block cipher E such that*

$$\begin{aligned} Adv^{prf}_{\mathbf{F}}(\mathcal{A}) \le & Adv^{prp}_{E}(\mathcal{A}_1) + Adv^{prp}_{E}(\mathcal{A}_2) + \frac{\mu^2}{2^n} + \mu^2\epsilon + \frac{q^2\epsilon}{2^n} \\ & + 4\mu^2\epsilon + \frac{3\mu q^{3/2}\epsilon}{2^{n/2}} + q^{4/3}\epsilon + \frac{18q^{4/3}}{2^n} + \frac{6q^{8/3}}{2^{2n}} \\ & + \frac{18q^{7/3}}{2^{2n}} + \frac{q^2}{2^{2n}} + \frac{8q^4}{3\cdot 2^{3n}}. \end{aligned}$$

Lemma 6. *Let $\mathcal{A}$ be an μ-fault adversary that makes at most $q \le 2^{3n/4}$ queries and generates at most σ blocks, and let $\mu \le q^{\frac{1}{3}}$ and m be the maximum block of the plaintext; then, there exist adversaries $\mathcal{A}_1$ and $\mathcal{A}_2$ with the same query complexity against the block cipher E such that*

$$\begin{aligned} Adv^{nE}_{\mathbf{E}}(\mathcal{A}) \le & Adv^{prp}_{E}(\mathcal{A}_1) + Adv^{prp}_{E}(\mathcal{A}_2) + \frac{6m\mu^2}{2^n} \\ & + \frac{\sigma^2}{2^{2n}} + \frac{3\mu\sigma}{2^n}\sqrt{\frac{\sigma}{2^n}} + \frac{19\sigma^{\frac{4}{3}}}{2^n} + \frac{6\sigma^{\frac{8}{3}}}{2^{2n}} + \frac{18\sigma^{\frac{7}{3}}}{2^{2n}} \\ & + \frac{\sigma^2}{2^{2n}} + \frac{8\sigma^4}{3\cdot 2^{3n}}. \end{aligned}$$

The security proof of Lemma 5 is the same as that of Theorem 4 in the study by Chen et al. [27]. The security proof of Lemma 6 is shown in Section 7.

By combining Lemmas 4–6, we present the security of GCM-SIV1.5 as follows.

Theorem 1. *Let $\mathcal{A}$ be an μ-fault adversary and H_L be ϵ-AXU. Let $\mu \le q^{\frac{1}{3}}$ and m be the maximum block of the plaintext. If $\mathcal{A}$ makes at most $q \le 2^{3n/4}$ queries and generates at most σ blocks,*

then there exist adversaries $\mathcal{A}_1$ and $\mathcal{A}_2$ with the same query complexity against the block cipher E such that

$$\begin{aligned} Adv^{nAE}_{GCM-SIV1.5}(\mathcal{A}) \leq & Adv^{prp}_{E}(\mathcal{A}_1) + Adv^{prp}_{E}(\mathcal{A}_2) + \frac{10m\mu^2}{2^n} \\ & + \frac{3q\mu\epsilon}{2^n} + \frac{q^2\epsilon}{2^n} + 5\mu^2\epsilon + q^{\frac{4}{3}}\epsilon \\ & + \frac{(3\mu+2)\sigma}{2^n} + \frac{46\sigma^{\frac{4}{3}}}{2^n} + \frac{q_v}{2^n}. \end{aligned}$$

Theorem 1 shows that, if the underlying block cipher E is a secure PRP and $\epsilon = 2^{-n}$, GCM-SIV1.5 offers BBB nAE security up to approximately $\frac{3n}{4}$-bit query complexity and approximately n-bit forgery attempts for μ-nonce faulty adversaries with $\mu \leq 2^{\frac{n}{4}}$.

7. Proofs of Lemma 6

The proof is similar to that of Theorem 4 in Chen et al. [27]. Let $K_1, K_2 \twoheadleftarrow \mathcal{K}_E$. The adversary $\mathcal{A}$ makes q encryption queries $(N^1, T^1, m^1), \cdots, (N^q, T^q, m^q)$ to the real world $\mathbf{E}$ or the ideal world R (R is an ideal version of $\mathbf{E}$ and always random strings) and returns $S^1, S^2, \cdots, S^q$, and then encrypts plaintexts $M^1, \cdots, M^q$ to obtain ciphertexts $C^1 = M^1 \oplus msb_{|M^1|}(S^1), \cdots, C^q = M^q \oplus msb_{|M^q|}(S^q)$. First, we replace E_{K_1} and E_{K_2} with two independent random permutations P_1 and P_2, and the replacements cost us $Adv^{prp}_{E}(\mathcal{A}_1) + Adv^{prp}_{E}(\mathcal{A}_2)$, where $\mathcal{A}_1$ and $\mathcal{A}_2$ are PRP adversaries against the underlying block cipher. Then, we consider $Adv^{nE}_{\mathbf{E}[P_1,P_2]}(\mathcal{A})$. Let $\tau = \{(N^1, T^1, m^1, S^1), \cdots, (N^q, T^q, m^q, S^q)\}$. Let X_{re} be the random variable interacting with the real world $X = \mathbf{E}[P_1, P_2]$ and Y_{id} be the random variable interacting with the ideal world $Y = R$.

For the real world, the transcript with q queries corresponds to the following mirror system of bi-variate equations:

$$\mathcal{E}^{=} \begin{cases} P_1(T^1+1) \oplus P_2(N^1||[1]_{\frac{n}{4}}) = S^1_1 \\ P_1(T^1+2) \oplus P_2(N^1||[2]_{\frac{n}{4}}) = S^1_2 \\ \cdots\cdots\cdots\cdots \\ P_1(T^1+m^1) \oplus P_2(N^1||[m^1]_{\frac{n}{4}}) = S^1_{m^1} \\ \cdots\cdots\cdots\cdots \\ P_1(T^q+1) \oplus P_2(N^q||[1]_{\frac{n}{4}}) = S^q_1 \\ P_1(T^q+2) \oplus P_2(N^q||[2]_{\frac{n}{4}}) = S^q_2 \\ \cdots\cdots\cdots\cdots \\ P_1(T^q+m^q) \oplus P_2(N^q||[m^q]_{\frac{n}{4}}) = S^q_{m^q} \end{cases}$$

As P_1, P_2 are two independent random permutations, let $X_{i,j} = P_1(T^i + j)$, $Y_{i,j} = P_2(N^i||[j]_{\frac{n}{4}})$, and $\lambda_{i,j} = S^i_j$, where $j \in [m^i], i \in [q]$. Let $\sigma = \sum_{i=1}^{q} m^i$.

Let V_1 be the set of vertices $X_{1,1}, \cdots, X_{q,m^q}$, V_2 be the set of vertices $Y_{1,1}, \cdots, Y_{q,m^q}$, $E = \{e_{i,j} = (X_{i,j}, Y_{i,j}), j \in [m^i], i \in [q]\}$, and $W : E \to \{0,1\}^n$. The above mirror system $\{X_{i,j} \oplus Y_{i,j} = \lambda_{i,j}, j \in [m^i], i \in [q]\}$ with a transcript τ can be described as an undirected weighted bipartite graph $G^\tau =< V_1, V_2, E, W >$. As T is random, there exist collisions in $X_{i,j} = P_1(T^i + j)$ for any $j \in [m^i], i \in [q]$. Let m be the maximum block of the plaintext. According to the fact that the nonce is μ-fault, V_2 is $\mu \cdot m$-fault.

In order to utilize the mirror theory, we first define a bad transcript.

Definition 1 (Bad Transcript). *A transcript τ is called bad if one of the following events occurs:*

- *G^τ covers a circle of length 2 or a path of length 2 such that the weight of this path is zero.*

- ***B1****: There exist distinct $i,k \in [q]$ such that $X_{i,j} = X_{k,l}$ and $Y_{i,j} = Y_{k,l}$, where $j \in [m^i], l \in [m^k]$, i.e., $T^i + j = T^k + l$ and $N^i||[j]_{\frac{n}{4}} = N^k||[l]_{\frac{n}{4}}$ (it implies $j = l$).*
- ***B2****: There exist distinct $i,k \in [q]$ such that $X_{i,j} = X_{k,l}$ and $\lambda_{i,j} \oplus \lambda_{k,l} = 0$, where $j \in [m^i], l \in [m^k]$, i.e., $T^i + j = T^k + l$ and $S^i_j \oplus S^k_l = 0$.*
- ***B3****: There exist distinct $i,k \in [q]$ such that $Y_{i,j} = Y_{k,l}$ and $\lambda_{i,j} \oplus \lambda_{k,l} = 0$, where $j \in [m^i], l \in [m^k]$, i.e., $N^i||[j]_{\frac{n}{4}} = N^k||[l]_{\frac{n}{4}}$ (it implies $j = l$) and $S^i_j \oplus S^k_l = 0$.*

- *G^τ covers a path of length 4 starting at the Y-shore, or a path of length 4 starting at the X-shore such that the weight of this path is zero (this condition satisfies the fact that G^τ covers a circle of length 4 or a path of length 4 such that the weight of this path is zero).*
  - ***B4****: There exist distinct $i,k,w,y \in [q]$ such that $Y_{i,j} = Y_{k,l}$, $X_{k,l} = X_{w,x}$, and $Y_{w,x} = Y_{y,z}$, i.e., $N^i||[j]_{\frac{n}{4}} = N^k||[l]_{\frac{n}{4}}$, $T^k + l = T^w + x$, and $N^w||[x]_{\frac{n}{4}} = N^y||[z]_{\frac{n}{4}}$ (it implies $j = l, x = z$).*
  - ***B5****: There exist distinct $i,k,w,y \in [q]$ such that $X_{i,j} = X_{k,l}$, $Y_{k,l} = Y_{w,x}$, $X_{w,x} = X_{y,z}$, and $\lambda_{i,j} \oplus \lambda_{k,l} \oplus \lambda_{w,x} \oplus \lambda_{y,z} = 0$, i.e., $T^i + j = T^k + l$, $N^k||[l]_{\frac{n}{4}} = N^w||[x]_{\frac{n}{4}}$, $T^w + x = T^y + z$, and $\lambda_{i,j} \oplus \lambda_{k,l} \oplus \lambda_{w,x} \oplus \lambda_{y,z} = 0$ (it implies $l = x$).*
- *The number of edges in components with a size of more than 2 is $q_c \geq \widetilde{q}_c$. Each vertex in the components is associated with two edges in the average case. Let us assume that it may be evenly amortized to the two vertex sets of the bipartite graph.*
  - ***B6****: $|\{(i,k)|i \neq k, j \in [m^i], l \in [m^k], X_{i,j} = X_{k,l}\}| \geq \widetilde{q}_c/4$, i.e, $|\{(i,k)|i \neq k, j \in [m^i], l \in [m^k], T^i + j = T^k + l\}| \geq \widetilde{q}_c/4$.*
  - ***B7****: $|\{(i,k)|i \neq k, j \in [m^i], l \in [m^k], Y_{i,j} = Y_{k,l}| \geq \widetilde{q}_c/4$, i.e, $|\{(i,k)|i \neq k, N^i = N^k\}| \geq \widetilde{q}_c/4$.*

Let Γ_{bad} be bad transcripts, Γ be all attainable transcripts, and $\Gamma_{good} = \Gamma \backslash \Gamma_{bad}$.

Next, we upper bound the probability of bad transcripts in the ideal world $Pr[Y_{id} \in \Gamma_{bad}]$.

For **B1**, the probability that $T^i + j = T^k + l$ occurs for any fixed i,j,k,l is 2^{-n}, and the number of pairs (i,k) such that $N^i||[j]_{\frac{n}{4}} = N^k||[l]_{\frac{n}{4}}$ is at most μ^2, where $j \in [m^i], l \in [m^k]$; then, we have

$$\begin{aligned} Pr[\mathbf{B1}] &= Pr[X_{i,j} = X_{k,l}, Y_{i,j} = Y_{k,l}] \\ &= Pr[T^i + j = T^k + l, N^i||[j]_{\frac{n}{4}} = N^k||[l]_{\frac{n}{4}}] \\ &\leq \frac{m\mu^2}{2^n}. \end{aligned}$$

For **B2**, the probability that $T^i + j = T^k + l$ occurs for any fixed i,j,k,l is 2^{-n}, and the probability that $S^i_j \oplus S^k_l = 0$ occurs for any fixed i,j,k,l is 2^{-n}; then, we have

$$\begin{aligned} Pr[\mathbf{B2}] &= Pr[X_{i,j} = X_{k,l}, \lambda_{i,j} \oplus \lambda_{k,l} = 0] \\ &= Pr[T^i + j = T^k + l, S^i_j \oplus S^k_l = 0] \\ &\leq \frac{\sigma^2}{2^{2n}}. \end{aligned}$$

For **B3**, the probability that $S^i_j \oplus S^k_l = 0$ occurs for any fixed i,j,k,l is 2^{-n}, and the number of pairs (i,k) such that $N^i||[j]_{\frac{n}{4}} = N^k||[l]_{\frac{n}{4}}$ is at most μ^2, where $j \in [m^i], l \in [m^k]$; then, we have

$$\begin{aligned} Pr[\mathbf{B3}] &= Pr[Y_{i,j} = Y_{k,l}, \lambda_{i,j} \oplus \lambda_{k,l} = 0] \\ &= Pr[N^i||[j]_{\frac{n}{4}} = N^k||[l]_{\frac{n}{4}}, S^i_j \oplus S^k_l = 0] \\ &\leq \frac{m\mu^2}{2^n}. \end{aligned}$$

For **B4**, the probability that $T^k + l = T^w + x$ occurs for any fixed k, l, w, x is 2^{-n} and the number of pairs (i, k, w, y) such that $N^i||[j]_{\frac{n}{4}} = N^k||[l]_{\frac{n}{4}}$ and $N^w||[x]_{\frac{n}{4}} = N^y||[z]_{\frac{n}{4}}$ for any fixed $i \neq k, w \neq y$ is at most $4\mu^2$ (as the number of queries using any repeated nonce is at most 2μ); then, we have

$$\begin{aligned} Pr[\mathbf{B4}] =& Pr[Y_{i,j} = Y_{k,l}, X_{k,l} = X_{w,x}, Y_{w,x} = Y_{y,z}] \\ \leq& \frac{4m\mu^2}{2^n}. \end{aligned}$$

For **B5**, let $F_{i,j,k,l,w,x,y,z} : \lambda_{i,j} \oplus \lambda_{k,l} \oplus \lambda_{w,x} \oplus \lambda_{y,z} = 0$, the probability that $E_{i,j,k,l} : T^i + j = T^k + l$ occurs for any fixed i, j, k, l be 2^{-n} (the same for $E_{w,x,y,z} : T^w + x = T^y + z$), and the probability that $F_{i,j,k,l,w,x,y,z}$ occurs for any fixed i, j, k, l, w, x, y, z be 2^{-n}. According to alternating event lemma and $\sigma = mq$, we have

$$\begin{aligned} Pr[\mathbf{B5}] =& Pr[E_{i,j,k,l}, Y_{k,l} = Y_{w,x}, E_{w,x,y,z}, F_{i,j,k,l,w,x,y,z}] \\ \leq& \frac{3\mu\sigma}{2^n}\sqrt{\frac{\sigma}{2^n}}. \end{aligned}$$

For **B6**, according to Markov's inequality, the probability of **B6** is upper bounded by

$$\begin{aligned} Pr[\mathbf{B6}] &= Pr[|\{(i,k)|i \neq k, j \in [m^i], l \in [m^k], X_{i,j} = X_{k,l}\}| \geq \widetilde{q}_c/4] \\ &\leq \frac{\mathbb{E}[|\{(i,k)|i \neq k, j \in [m^i], l \in [m^k], X_{i,j} = X_{k,l}\}| \geq \widetilde{q}_c/4]}{\widetilde{q}_c/4} \\ &\leq \frac{\frac{\sigma^2}{2^n}}{\widetilde{q}_c/4} \leq \frac{4\sigma^2}{\widetilde{q}_c \cdot 2^n}. \end{aligned}$$

In order to obtain $\frac{3n}{4}$-bit security, we choose $\widetilde{q}_c = 4\sigma^{\frac{2}{3}}$. Then,

$$Pr[\mathbf{B6}] \leq \frac{4\sigma^2}{\widetilde{q}_c \cdot 2^n} = \frac{\sigma^{\frac{4}{3}}}{2^n}.$$

For **B7**, as $\mu^2 < q^{\frac{2}{3}} \leq \sigma^{\frac{2}{3}} = \widetilde{q}_c/4$, the probability of **B7** being upper bounded by

$$\begin{aligned} Pr[\mathbf{B7}] &= Pr[|\{(i,k)|i \neq k, j \in [m^i], l \in [m^k], Y_{i,j} = Y_{k,l}| \geq \widetilde{q}_c/4] \\ &= Pr[\mu^2 \geq \widetilde{q}_c/4] = 0. \end{aligned}$$

To summarize, the probability of bad transcripts is

$$\begin{aligned} Pr[Y_{id} \in \Gamma_{bad}] &= Pr[\bigcup_{i=1}^{7} \mathbf{Bi}] \\ &\leq \frac{6m\mu^2}{2^n} + \frac{\sigma^2}{2^{2n}} + \frac{3\mu\sigma}{2^n}\sqrt{\frac{\sigma}{2^n}} + \frac{\sigma^{\frac{4}{3}}}{2^n}. \end{aligned}$$

Then, we consider the ratio $\frac{Pr[X=\tau]}{Pr[Y=\tau]}$ between the real world X and the ideal world Y in the good transcript. In the good transcript, G^τ meets (1) acyclic, (2) NPL, and (3)

$q_c \leq \widetilde{q}_c = 4\sigma^{\frac{2}{3}}$. Let $q' = |V_1|$ and $q'' = |V_2|$; according to the mirror theory, the number of solutions is at least $\frac{(2^n)_{q'}(2^n)_{q''}}{2^{n\sigma}}(1-\delta)$, where

$$\begin{aligned}\delta =& \frac{9\widetilde{q}_c^2}{8\cdot 2^n} + \frac{9\widetilde{q}_c^2\sigma + 12\widetilde{q}_c\sigma^2 + 8\sigma^2}{8\cdot 2^{2n}} + \frac{8\sigma^4}{3\cdot 2^{3n}} \\ =& \frac{18\sigma^{\frac{4}{3}}}{2^n} + \frac{18\sigma^{\frac{7}{3}} + 6\sigma^{\frac{8}{3}} + \sigma^2}{2^{2n}} + \frac{8\sigma^4}{3\cdot 2^{3n}}.\end{aligned}$$

In the real world X, we have

$$\begin{aligned}Pr[X=\tau] &= Pr[P_1, P_2 \in Perm(n) : \mathbf{E}[P_1, P_2] \vdash \tau] \\ &= \frac{|P_1, P_2 \in Perm(n) : \mathbf{E}[P_1, P_2] \vdash \tau|}{|Perm(n)|^2} \\ &\geq \frac{\frac{(2^n)_{q'}(2^n)_{q''}}{2^{n\sigma}}(1-\delta)(2^n-q')!(2^n-q'')!}{(2^n!)^2} \\ &= \frac{1}{2^{n\sigma}}(1-\delta).\end{aligned}$$

In the ideal world Y, we have

$$Pr[Y=\tau] = Pr[R \in Func(2n,*) : R \vdash \tau] = \frac{1}{2^{n\sigma}}.$$

Therefore, the ratio between $Pr[X=\tau]$ and $Pr[Y=\tau]$ is

$$\frac{Pr[X=\tau]}{Pr[Y=\tau]} \geq 1-\delta.$$

According to the H-coefficient technique, we have

$$\begin{aligned}Adv_{\mathbf{E}}^{nE}(\mathcal{A}) \leq & Adv_E^{prp}(\mathcal{A}_1) + Adv_E^{prp}(\mathcal{A}_2) + \frac{6m\mu^2}{2^n} \\ &+ \frac{\sigma^2}{2^{2n}} + \frac{3\mu\sigma}{2^n}\sqrt{\frac{\sigma}{2^n}} + \frac{19\sigma^{\frac{4}{3}}}{2^n} + \frac{6\sigma^{\frac{8}{3}}}{2^{2n}} + \frac{18\sigma^{\frac{7}{3}}}{2^{2n}} \\ &+ \frac{\sigma^2}{2^{2n}} + \frac{8\sigma^4}{3\cdot 2^{3n}}.\end{aligned}$$

So far, we have completed the proof of Lemma 6.

8. Discussions and Conclusions

GCM-SIV1.5 is one of the favored generic nAE constructions described in [36], which combines a PRF **F** and an nE or ivE scheme **E**. Here, the PRF **F** is a BBB-secure F_{B2}^{SoP} scheme and the nE scheme **E** is a BBB-secure CTR^{SoP} scheme.

GCM-SIV1.5 offers an optimal tradeoff to GCM-SIV1 and GCM-SIV2 for supporting BBB security, as low as possible implementation costs, and high enough operational efficiencies. From the perspective of the security strength, if the underlying block cipher E is a secure PRP and $\epsilon = 2^{-n}$, GCM-SIV1.5 offers approximately $3n/4$-bit nAE security for μ-fault nonce-misusing adversaries and supports graceful security degradation, which is better than those of GCM-SIV1 and GCM-SIV2. From the perspective of implementation costs, compared with GCM-SIV2 and GCM-SIVr, GCM-SIV1.5 utilizes fewer keys (just two block cipher keys and a hash key) and lower storage and communication costs or throughput (just n-bit authentication tag). From the perspective of operational efficiencies, GCM-SIV1.5 utilizes just a hash function call and two plaintext blocks calls. More importantly, all encryption operations involving the nonce can be carried out offline, which saves half of the online computing resources. To sum up, our design achieves the optimal

tradeoff to GCM-SIV and GCM-SIVr from the security strength, implementation costs, and software performance aspects.

In order to further demonstrate the superiority of our design, Table 1 shows a fair and thorough comparison between GCM-SIV1.5 and other similar schemes. Compared with CWC+, GCM-SIV1.5 provides a better security bound and supports fully faulty nonce misuse resistance, but the number of the encryption keys and the number of the block cipher calls are slightly inferior. Compared with SCM, GCM-SIV1.5 saves an encryption key, supports offline operations involving the nonce's encryption, and saves half of the online computing resources, but other aspects, such as the number of block cipher calls, nonce size, and security bound, are slightly inferior. Besides that, SCM utilizes the finite field multiplication operations in the encryption part, although these multiplication operations can be quickly calculated using the double point technique. However, our design just utilizes some XOR and finite field addition operations.

GCM-SIV1.5 utilizes three keys. A natural future direction is to reduce the number of keys and to obtain a single-key BBB-secure variant. Besides that, GCM-SIV1.5 utilizes two plaintext blocks calls. Another future direction is to decrease the invocations of block ciphers and to improve the operational efficiencies. Our security is based on the condition that $\mu \leq 2^{n/4}$. We leave considering the case of $\mu > 2^{n/4}$ as an open problem.

Funding: This research was supported by National Key Research and Development Program of China (Grant No.: 2019YFB2101704), National Natural Science Foundation of China (Grant Nos.: 61902195, 62272238, 61902194, 62072207, and 62102196), NUPTSF (Grant No.: NY219131), and Henan Key Laboratory of Network Cryptography Technology (Grant No. LNCT2020-A05).

Informed Consent Statement: Not applicable.

Data Availability Statement: The data used to support the findings of the study are available within the article.

Acknowledgments: We would like to express our sincere thanks to editors and the anonymous reviewers for the valuable comments and suggestions.

Conflicts of Interest: The author declares no conflict of interest.

References

1. McGrew, D.A.; Viega, J. The security and performance of the Galois/Counter Mode (GCM) of operation. In *Progress in Cryptology— INDOCRYPT 2004*; Canteaut, A., Viswanathan, K., Eds.; Springer: Berlin/Heidelberg, Germany, 2004; pp. 343–355.
2. Joux, A. Authentication Failures in NIST Version of GCM. Public Comments to NIST. Available online: https://csrc.nist.gov/csrc/media/projects/block-cipher-techniques/documents/bcm/joux_comments.pdf (accessed on 17 September 2022).
3. Iwata, T.; Ohashi, K.; Minematsu, K. Breaking and repairing GCM security proofs. In *Advances in Cryptology—CRYPTO 2012*; Safavi-Naini, R., Canetti, R., Eds.; Springer: Berlin/Heidelberg, Germany, 2012; pp. 31–49.
4. Aoki, K.; Yasuda, K. The security and performance of GCM when short multiplications are used instead. In *Advances in Cryptology—Inscrypt 2012*; Kutylowski, M., Yung, M., Eds.; Springer: Berlin/Heidelberg, Germany, 2012; pp. 225–245.
5. Niwa, Y.; Ohashi, K.; Minematsu, K.; Iwata, T. GCM security bounds reconsidered. In *Advances in Cryptology—FSE 2015*; Leander, G., Ed.; Springer: Berlin/Heidelberg, Germany, 2015; pp. 385–407.
6. Bellare, M.; Tackmann, B. The multi-user security of authenticated encryption: AES-GCM in TLS 1.3. In *Advances in Cryptology—CRYPTO 2016*; Robshaw, M., Katz, J., Eds.; Springer: Berlin/Heidelberg, Germany, 2016; pp. 247–276.
7. Ashur, T.; Dunkelman, O.; Luykx, A. Boosting authenticated encryption robustness with minimal modifications. In *Advances in Cryptology—CRYPTO 2017*; Katz, J., Shacham, H., Eds.; Springer: Berlin/Heidelberg, Germany, 2017; pp. 3–33.
8. Zhang, P.; Hu, H.; Yuan, Q. Close to optimally secure variants of GCM. *Secur. Commun. Netw.* **2018**, *2018*, 9715947:1–9715947:12. [CrossRef]
9. Hoang, V.T.; Tessaro, S.; Thiruvengadam, A. The multi-user security of GCM, revisited: Tight bounds for nonce randomization. In Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security—CCS 2018, Toronto, ON, Canada, 15–19 October 2018; Association for Computing Machinery: New York, NY, USA, 2018; pp. 1429–1440.
10. Sovyn, Y.; Khoma, V.; Podpora, M. Comparison of three CPU-core families for IoT applications in terms of security and performance of AES-GCM. *IEEE Internet Things J.* **2020**, *7*, 339–348. [CrossRef]
11. Gueron, S.; Lindell, Y. GCM-SIV: Full nonce misuse-resistant authenticated encryption at under one cycle per byte. In Proceedings of the 2015 ACM SIGSAC Conference on Computer and Communications Security—CCS 2015, Denver, CO, USA, 12–16 October 2015; Association for Computing Machinery: New York, NY, USA, 2015; pp. 109–119.

12. Iwata, T.; Minematsu, K. Stronger security variants of GCM-SIV. *IACR Trans. Symmetric Cryptol.* **2016**, *2016*, 134–157. [CrossRef]
13. Gueron, S.; Langley, A.; Lindell, Y. *AES-GCM-SIV: Nonce Misuse-Resistant Authenticated Encryption*; RFC 8452; Crypto Forum Research Group: Stamford, CT, USA, 2019; pp. 1–42.
14. Iwata, T.; Seurin, Y. Reconsidering the security bound of AES-GCM-SIV. *IACR Trans. Symmetric Cryptol.* **2017**, *2017*, 240–267. [CrossRef]
15. Gueron, S.; Lindell, Y. Better bounds for block cipher modes of operation via nonce-based key derivation. In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security—CCS 2017, Dallas, TX, USA, 30 October–3 November 2017; Association for Computing Machinery: New York, NY, USA, 2017; pp. 1019–1036.
16. Bose, P.; Hoang, V.T.; Tessaro, S. Revisiting AES-GCM-SIV: Multi-user security, faster key derivation, and better bounds. In *Advances in Cryptology—EUROCRYPT 2018*; Nielsen, J.B., Rijmen, V., Eds.; Springer: Berlin/Heidelberg, Germany, 2018; pp. 468–499.
17. Rogaway, P.; Shrimpton, T. A provable-security treatment of the key-wrap problem. In *Advances in Cryptology—EUROCRYPT 2006*; Vaudenay, S., Ed.; Springer: Berlin/Heidelberg, Germany, 2006; pp. 373–390.
18. Andreeva, E.; Bogdanov, A.; Luykx, A.; Mennink, B.; Tischhauser, E.; Yasuda, K. Parallelizable and authenticated online ciphers. In *Advances in Cryptology—ASIACRYPT 2013*; Sako, K., Sarkar, P., Eds.; Springer: Berlin/Heidelberg, Germany, 2013; pp. 424–443.
19. Bossuet, L.; Datta, N.; Mancillas-Lopez, C.; Nandi, M. ELmD: A pipelineable authenticated encryption and its hardware implementation. *IEEE Trans. Comput.* **2016**, *65*, 3318–3331. [CrossRef]
20. Peyrin, T.; Seurin, Y. Counter-in-Tweak: Authenticated encryption modes for tweakable block ciphers. In *Advances in Cryptology—CRYPTO 2016*; Robshaw, M., Katz, J., Eds.; Springer: Berlin/Heidelberg, Germany, 2016; pp. 33–63.
21. Iwata, T.; Minematsu, K.; Peyrin, T.; Seurin, Y. ZMAC: A fast tweakable block cipher mode for highly secure message authentication. In *Advances in Cryptology—CRYPTO 2017*; Katz, J., Shacham, H., Eds.; Springer: Berlin/Heidelberg, Germany, 2017; pp. 34–65.
22. Choi, W.; Lee, B.; Lee, J.; Lee, Y. Toward a fully secure authenticated encryption scheme from a pseudorandom permutation. In *Advances in Cryptology—ASIACRYPT 2021*; Tibouchi, M., Wang, H., Eds.; Springer: Berlin/Heidelberg, Germany, 2021; pp. 407–434.
23. Dutta, A.; Nandi, M.; Talnikar, S. Beyond birthday bound secure MAC in faulty nonce model. In *Advances in Cryptology—EUROCRYPT 2019*; Ishai, Y., Rijmen, V., Eds.; Springer: Berlin/Heidelberg, Germany, 2019; pp. 437–466.
24. Iwata, T. New blockcipher modes of operation with beyond the birthday bound security. In *Advances in Cryptology—FSE 2006*; Robshaw, M., Ed.; Springer: Berlin/Heidelberg, Germany, 2006; pp. 310–327.
25. Naito, Y.; Sasaki, Y.; Sugawara, T. Lightweight authenticated encryption mode suitable for threshold implementation. In *Advances in Cryptology—EUROCRYPT 2020*; Canteaut, A., Ishai, Y., Eds.; Springer: Berlin/Heidelberg, Germany, 2020; pp. 705–735.
26. Choi, W.; Lee, B.; Lee, Y.; Lee, J. Improved security analysis for nonce-based enhanced hash-then-mask MACs. In *Advances in Cryptology—ASIACRYPT 2020*; Moriai, S., Wang, H., Eds.; Springer: Berlin/Heidelberg, Germany, 2020; pp. 697–723.
27. Chen, Y.L.; Mennink, B.; Preneel, B. Categorization of faulty nonce misuse resistant message authentication. In *Advances in Cryptology—ASIACRYPT 2021*; Tibouchi, M., Wang, H., Eds.; Springer: Berlin/Heidelberg, Germany, 2021; pp. 520–550.
28. Krovetz, T.; Rogaway, P. The software performance of authenticated encryption modes. In *Advances in Cryptology—FSE 2011*; Joux, A., Ed.; Springer: Berlin/Heidelberg, Germany, 2011; pp. 306–327.
29. Bhattacharya, S.; Nandi, M. Revisiting variable output length XOR pseudorandom function. *IACR Trans. Symmetric Cryptol.* **2018**, *2018*, 314–335. [CrossRef]
30. Jha, A.; Nandi, M. Tight security of cascaded LRW2. *J. Cryptol.* **2020**, *33*, 1272–1317. [CrossRef]
31. Patarin, J. The "coefficients H" technique. In *Selected Areas in Cryptography—SAC 2008*; Avanzi, R.M., Keliher, L., Sica, F., Eds.; Springer: Berlin/Heidelberg, Germany, 2008; pp. 328–345.
32. Patarin, J. Mirror theory and cryptography. *Appl. Algebra Eng. Commun. Comput.* **2017**, *28*, 321–338. [CrossRef]
33. Nachef, V.; Patarin, J.; Volte, E. Introduction to mirror theory. In *Feistel Ciphers*; Springer: Berlin/Heidelberg, Germany, 2017; pp. 203–221.
34. Patarin, J. Introduction to Mirror Theory: Analysis of Systems of Linear Equalities and Linear Non Equalities for Cryptography. Available online: http://eprint.iacr.org/2010/287 (accessed on 17 September 2022).
35. Kim, S.; Lee, B.; Lee, J. Tight security bounds for double-block hash-then-sum MACs. In *Advances in Cryptology—EUROCRYPT 2020*; Canteaut, A., Ishai, Y., Eds.; Springer: Berlin/Heidelberg, Germany, 2020; pp. 435–465.
36. Namprempre, C.; Rogaway, P.; Shrimpton, T. Reconsidering generic composition. In *Advances in Cryptology—EUROCRYPT 2014*; Nguyen, P.Q., Oswald, E., Eds.; Springer: Berlin/Heidelberg, Germany, 2014; pp. 257–274.