mathematics

MDPI

Article

GCM Variants with Robust Initialization Vectors

Ping Zhang

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

Abstract: The complexity and isomerization of communication networks have put forth new requirements for cryptographic schemes to ensure the operation of network security protocols. Robust cryptographic schemes have been gradually favored. The robust initialization vector (RIV) instead of the synthetic initialization vector (SIV) was first introduced to support strong security and robust authenticated encryption. This paper first introduces RIV to GCM-SIV1, proposes a robust variant, GCM-RIV1, and proves that it ensures birthday-bound subtle AE (SAE) security and nonce-misuse resistance. Then, to support beyond-birthday-bound (BBB) security with graceful degradation, we introduce another, stronger security variant, GCM-RIV2, and prove that it allows gracefully degrading BBB SAE security in the faulty nonce setting. Finally, the performance of GCM-RIV1 and GCM-RIV2 is discussed and compared.

Keywords: robust authenticated encryption; robust initialization vector; synthetic initialization vector; GCM; provable security; faulty nonce

MSC: 94A60; 68P25

1. Introduction

With the development of cloud-end convergence networks, the industrial Internet, and the Internet of Things, the security of critical infrastructure and protocols on the network has become more and more important. As a high-speed lightweight authenticated encryption (AE) scheme or protocol, Galois/Counter Mode (GCM) plays an important role in network security communication. GCM is a commonly used AE mode based on symmetric-key cryptography and included in the NIST and IETF standards, and it has been widely used in cloud computing, the Internet of Things, network communication protocols, and other fields [1–3]. For example, the well-known transport layer security protocol TLS1.2 uses AES-GCM [3]. However, with the complexity, diversity, and heterogeneity of communication networks, more robust and resilient cryptographic schemes have attracted people's attention.

Most AE schemes including GCM are nonce-based AE (nAE) schemes and they have proven security in the nonce-respecting setting (the nonce used in the encryption algorithm is distinct). In real life, however, the nonce is often reused. If the nonce is reused, the security of nonce-respecting AE (NRAE) schemes represented by GCM will be broken. To settle this problem, Rogaway and Shrimpton introduced the nonce-misuse-resistant AE (MRAE) notion and proposed the first MRAE construction, called the synthetic initialization vector (SIV) [4]. SIV is roughly as efficient as the general two-pass AE modes (such as CCM), but more resilient to nonce misuse [4]. A large number of MRAE designs followed, such as HBS [5], BTM [6], MR-OMD [7], GCM-SIV [8], AES-GCM-SIV [9], GCM-SIV1 [10], GCM-SIV2 [10], CCM-SIV [11], SAEF [12], and GIFT-COFB [13]. Later, Dutta et al. refined nonce misuse and introduced a faulty nonce notion to specify the degree of repeated nonce tolerance [14]. The faulty nonce notion covers nonce respecting and nonce misuse. For a μ-faulty nonce, if $\mu = 0$, it is expected to degenerate to nonce-respecting; if $\mu \geq 1$, it is nonce-misuse. At ASIACRYPT 2021, Choi et al. introduced the faulty nonce to AE,

check for updates

Citation: Zhang, P. GCM Variants with Robust Initialization Vectors. *Mathematics* **2023**, *11*, 4888. https://doi.org/10.3390/math11244888

Academic Editor: Antanas Cenys

Received: 15 November 2023
Revised: 27 November 2023
Accepted: 4 December 2023
Published: 6 December 2023

presented a parallelizable nonce-based AE mode SCM, and proved its security with graceful degradation in the faulty nonce security model [15].

In addition to nonce misuse or a faulty nonce, Andreeva et al. proposed a new security model, releasing unverified plaintext (RUP), on the traditional nAE security model, to adapt to a new or side-channel environment in which plaintext information is released before verification [16]. There exist many RUP-secure AE schemes, such as COLM [17], OCB-IC [18], ChaCha20-Poly1305 [19], LOCUS [20], LOTUS [20], GCM-RUP [21], and SAEB [22].

Besides this, Hoang et al. built a robust AE (RAE) notion to adapt to the ciphertext expansion and then constructed a well-optimized AEZ mode [23]. Later, Badertscher et al. investigated RAE and gave formal descriptions for two additional features of RAE [24]. Shrimpton et al. introduced a protected IV (PIV) framework and gave encode-then-encipher over PIV AE with associated data schemes [25]. Barwell et al. introduced a subtle AE (SAE) security notion using an extra "leakage" algorithm on the basis of the traditional AE security model [26]. The SAE security covers RUP and RAE and is able to leak some information about the invalid plaintext. At FSE 2016, Abed et al. extended the SIV framework by adopting an additional pseudorandom function, introduced a robust initialization vector (RIV) framework for robust authenticated encryption, and proved that RIV supports SAE security [27]. RIV fully inherits the security guarantees of SIV, but, unlike SIV and other MRAE schemes, RIV is also provably secure under RUP and RAE. The robustness mentioned here is a gradient concept. RAE is the most robust version and the traditional AE is the most basic version. Aiming at various possible attacks or complex environments, robust AE schemes are designed to meet the corresponding needs to maintain the confidentiality and integrity of data.

Contributions. In order to adapt to the more complex network environment, the goal of this paper is to put forward robust variants on the basis of GCM and incorporate as many characteristics of robustness into our design scheme as possible. To enhance the robustness of GCM-SIV1, we propose its robust variant, called GCM-RIV1, by introducing RIV instead of SIV, and prove that GCM-RIV1 guarantees birthday-bound SAE security of $n/2$-bit and nonce-misuse resistance if the underlying block cipher uses secure pseudorandom permutation (PRP) and the hash function is XOR-universal, where n is the block size. Then, to support beyond-birthday-bound (BBB) security with graceful degradation and a nonce fault, we introduce another variant, GCM-RIV2, and prove that it not only enjoys approximately $3n/4$-bit BBB SAE security but also supports graceful security degradation. Besides this, GCM-RIV1 and GCM-RIV2 are inverse-free, which reduces the cost of block cipher decryption. Moreover, both of them are parallel and robust against the leakage of invalid plaintext. Finally, we present a comparison between our schemes and previous related schemes, which is shown in Table 1.

Table 1. Comparison between our schemes and previous related schemes, where # represents the count, m represents the largest number of plaintext blocks, n is the block size, and NR (resp. NM, resp. NF) stands for the nonce-respecting setting (resp. the nonce-misuse setting, resp. the nonce-faulty setting).

Scheme	# Key	# Block Cipher	# Hash	Inverse Free	Reference
GCM	2	m	1	Yes	[1]
GCM-SIV1	2	$m+1$	1	Yes	[10]
GCM-SIV2	6	$2m+4$	2	Yes	[10]
GCM-RUP	4	$m+3$	2	No	[21]
GCM-RIV1	2	$m+2$	2	Yes	Section 4
GCM-RIV2	4	$2m+2$	2	Yes	Section 5

Table 1. *Cont.*

Scheme	NR Security	NM Security	NF Security	Security Model	Robust Level
GCM	$n/2$-bit	-	-	nAE	Low
GCM-SIV1	$n/2$-bit	$n/2$-bit	-	nAE	Medium
GCM-SIV2	$2n/3$-bit	$2n/3$-bit	-	nAE	Medium
GCM-RUP	$n/2$-bit	$n/2$-bit	-	RUP	High
GCM-RIV1	$n/2$-bit	$n/2$-bit	$n/2$-bit	SAE	Higher
GCM-RIV2	$3n/4$-bit	$3n/4$-bit	$3n/4$-bit [1]	SAE	Higher

[1] $3n/4$-bit gracefully degradable as parameter μ increases.

The rest of the article is arranged as follows. Section 2 presents some basic preliminaries and related security models. Section 3 shows the extended mirror theory. Sections 4 and 5 show our designs, GCM-RIV1 and GCM-RIV2, and derive their security proof, respectively. Finally, we conclude this paper in Section 6.

2. Preliminaries

Some symbols used in the paper are described in Table 2.

Table 2. Descriptions of symbols.

Symbol	Description	Symbol	Description
$\mathcal{K}$	the key space	$\mathcal{N}$	the nonce space
$\mathcal{H}$	the associated data space	$\mathcal{M}$	the plaintext space
$\mathcal{C}$	the ciphertext space	$\mathcal{T}$	the authentication tag space
$\oplus$	the bitwise XOR	$+$	the addition modulo 2^n
$\cdot$	the multiplication modulo 2^n	$\|\|$	the concatenation of strings
$\{0,1\}^*$	a set of all strings	$\{0,1\}^n$	a set of n-bit strings
$Perm(n)$	an n-bit permutation set	$\twoheadleftarrow$	uniform random sampling
$Func(m,n)$	a set of all functions from m-bit inputs to n-bit outputs	$\mathcal{A}^O = 1$	an adversary $\mathcal{A}$ outputs 1 after interacting with the oracle O
$Pr[E]$	the probability of an event E	$[r]$	a set $\{1,2,\ldots,r\}$
$\top$	a valid (success) symbol	$\perp$	a reject (failure) symbol
msb	the most significant bit	lsb	the least significant bit
$\|X\|$	the number of elements in set X	$(2^n)_q$	$2^n \cdot (2^n-1)\ldots(2^n-q+1)$

Block Cipher. A block cipher is an important part of symmetric-key cryptography and has been widely used in real life, such as standardized block ciphers SM4 and AES. Its mathematical model can be expressed as $E : \mathcal{K} \times \{0,1\}^n \to \{0,1\}^n$. We describe its pseudorandom permutation (PRP) security model as follows.

Definition 1 (PRP Advantage [27])**.** *Let $\mathcal{A}$ be an adversary that has access to an encryption oracle E. Then, the PRP advantage of $\mathcal{A}$ against E is defined as*

$$Adv_E^{PRP}(\mathcal{A}) = \mid Pr[K \twoheadleftarrow \mathcal{K} : \mathcal{A}^{E_K} = 1] - Pr[\pi \twoheadleftarrow Perm(n) : \mathcal{A}^{\pi} = 1] \mid .$$

Keyed Function. Let $F : \mathcal{K} \times \{0,1\}^m \to \{0,1\}^n$ be a keyed function. We describe its pseudorandom function (PRF) security model as follows.

Definition 2 (PRF Advantage [27])**.** *Let $\mathcal{A}$ be an adversary that has access to the function oracle F. Then, the PRF advantage of $\mathcal{A}$ against F is defined as*

$$Adv_F^{PRF}(\mathcal{A}) = \mid Pr[K \twoheadleftarrow \mathcal{K} : \mathcal{A}^{F_K} = 1] - Pr[\$ \twoheadleftarrow Func(m,n) : \mathcal{A}^{\$} = 1] \mid .$$

Nonce-Based Authenticated Encryption (nAE). An nAE with associated data scheme $\Pi = (\mathcal{E}, \mathcal{D})$ consists of an encryption algorithm $\mathcal{E} : \mathcal{K} \times \mathcal{N} \times \mathcal{H} \times \mathcal{M} \to \mathcal{C} \times \mathcal{T}$ and a

decryption algorithm $\mathcal{D} : \mathcal{K} \times \mathcal{N} \times \mathcal{H} \times \mathcal{C} \times \mathcal{T} \rightarrow \mathcal{M} \cup \{\perp\}$. The correctness means that $(C, T) = \mathcal{E}_K(N, A, M)$ if and only if (iff) $M = \mathcal{D}_K(N, A, C, T)$. For nAE schemes, the conventional security model includes IND-CPA and INT-CTXT, which are described as follows.

Definition 3 (IND-CPA Advantage [27]). *Let $\mathcal{A}$ be an adversary that has access to an encryption oracle $\mathcal{E}$. Then, the IND-CPA advantage of $\mathcal{A}$ against Π is defined as*

$$Adv_{\Pi}^{IND-CPA}(\mathcal{A}) = \mid Pr[K \twoheadleftarrow \mathcal{K} : \mathcal{A}^{\mathcal{E}_K} = 1] - Pr[\mathcal{A}^{\$} = 1] \mid$$

where $\$$ is the ideal version of $\mathcal{E}_K$.

Definition 4 (INT-CTXT Advantage [27]). *Let $\mathcal{A}$ be an adversary that has access to an encryption oracle $\mathcal{E}$ and a decryption oracle $\mathcal{D}$ but does not make repeated queries. Then, the INT-CTXT advantage of $\mathcal{A}$ against Π is defined as*

$$Adv_{\Pi}^{INT-CTXT}(\mathcal{A}) = Pr[K \twoheadleftarrow \mathcal{K} : \mathcal{A}^{\mathcal{E}_K, \mathcal{D}_K} \ forges]$$

where forge means that $\mathcal{D}_K$ returns anything other than $\perp$ for any query of $\mathcal{A}$.

Later, Rogaway and Shrimpton introduced the all-in-one AE security notion [4], which is described as follows.

Definition 5 (nAE Advantage [4,27]). *Let $\mathcal{A}$ be an adversary that has access to an encryption oracle $\mathcal{E}$ and a decryption oracle $\mathcal{D}$ but does not make repeated queries. Then, the nAE advantage of $\mathcal{A}$ against Π is defined as*

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

where $\$$ is the ideal version of $\mathcal{E}_K$ and $\perp$ is a reject function that always returns a reject symbol.

The all-in-one AE security covered IND-CPA and INT-CTXT; the decomposition of nAE security is described as follows.

Lemma 1 (Decomposition of nAE Security [26,27]). *Let $\mathcal{A}$ be an adversary that runs in time at most t and asks at most q queries of at most σ blocks to its respective oracles. Then, there exist computationally bounded IND-CPA and INT-CTXT adversaries $\mathcal{B}$ and $\mathcal{C}$, respectively, on Π such that*

$$Adv_{\Pi}^{nAE}(\mathcal{A}) \leq Adv_{\Pi}^{IND-CPA}(\mathcal{B}) + Adv_{\Pi}^{INT-CTXT}(\mathcal{C}),$$

where $\mathcal{B}$ and $\mathcal{C}$ each make at most q queries of at most σ blocks and run in time $O(t)$ each.

Subtle Authenticated Encryption (SAE). An SAE scheme $\Pi = (\mathcal{E}, \mathcal{D}, \Lambda)$ introduced by Barwell et al. [26] includes a new deterministic leakage algorithm $\Lambda : \mathcal{K} \times \mathcal{N} \times \mathcal{H} \times \mathcal{C} \times \mathcal{T} \rightarrow \{\top\} \cup \mathcal{L}$ in addition to the encryption and decryption algorithms $\mathcal{E}$ and $\mathcal{D}$ as above, where $\mathcal{L}$ is a non-empty leakage space.

Definition 6 (ERR-CCA Advantage [26,27]). *Let $\mathcal{A}$ be an adversary that has access to an encryption oracle $\mathcal{E}$, a decryption oracle $\mathcal{D}$, and a leakage oracle Λ but does not make repeated queries. Then, the ERR-CCA advantage of $\mathcal{A}$ against Π is defined as*

$$Adv_{\Pi}^{ERR-CCA}(\mathcal{A}) = \mid Pr[K \twoheadleftarrow \mathcal{K} : \mathcal{A}^{\mathcal{E}_K, \mathcal{D}_K, \Lambda_K} = 1] - Pr[K, K' \twoheadleftarrow \mathcal{K} : \mathcal{A}^{\mathcal{E}_K, \mathcal{D}_K, \Lambda_{K'}} = 1] \mid .$$

Definition 7 (SAE Advantage [26,27]). *Let $\mathcal{A}$ be an adversary that has access to an encryption oracle $\mathcal{E}$, a decryption oracle $\mathcal{D}$, and a leakage oracle Λ but does not make repeated queries. Then, the SAE advantage of $\mathcal{A}$ against Π is defined as*

$$Adv_{\Pi}^{SAE}(\mathcal{A}) = \mid Pr[K \twoheadleftarrow \mathcal{K} : \mathcal{A}^{\mathcal{E}_K, \mathcal{D}_K, \Lambda_K} = 1] - Pr[K' \twoheadleftarrow \mathcal{K} : \mathcal{A}^{\$, \perp, \Lambda_{K'}} = 1] \mid$$

where $\$$ is the ideal version of $\mathcal{E}_K$ and $\perp$ is a reject function that always returns a reject symbol.

Lemma 2 (Decomposition of SAE Security [26,27]). *Let $\mathcal{A}$ run in time at most t and ask at most q queries of at most σ blocks to its respective oracles. Then, there exist computationally bounded IND-CPA, INT-CTXT, and ERR-CCA adversaries $\mathcal{B}$, $\mathcal{C}$, and $\mathcal{D}$, respectively, on Π such that*

$$Adv_{\Pi}^{SAE}(\mathcal{A}) \leq Adv_{\Pi}^{IND-CPA}(\mathcal{B}) + Adv_{\Pi}^{INT-CTXT}(\mathcal{C}) + Adv_{\Pi}^{ERR-CCA}(\mathcal{D}),$$

where $\mathcal{B}$, $\mathcal{C}$, and $\mathcal{D}$ each make at most q queries of at most σ blocks and run in time $O(t)$ each.

AXU Hash Functions [27]. 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

$$Pr[L \twoheadleftarrow \mathcal{K}_H : H_L(x) \oplus H_L(x') = y] \leq \epsilon,$$

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

H-Coefficient Technique [28,29]. The H-coefficient technique introduced by Patarin is a very useful tool in the security proof of symmetric-key cryptography. Assume that $\mathcal{A}$ is a deterministic adversary whose goal is to distinguish the real scheme X from the ideal scheme Y. $\mathcal{A}$ interacts with X and Y and records a series of query–response pairs as a transcript τ. Let Γ be the set of all possible transcripts. Let X_{re} be the random variable interacting with X and Y_{id} be the random variable interacting with Y. Then, the H-coefficient lemma is presented as follows.

Lemma 3 (H-Coefficient Lemma [29]). *Let $\Gamma = \Gamma_{good} \cup \Gamma_{bad}$ and $\varepsilon, \delta \in [0,1]$. If $Pr[Y_{id} \in \Gamma_{bad}] \leq \varepsilon$ and for all $\tau \in \Gamma_{good}$, $Pr[X_{re} = \tau]/Pr[Y_{id} = \tau] \geq 1 - \delta$, then*

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

O extends τ. Given a transcript $\tau = \{(x_1, y_1), \ldots, (x_q, y_q)\}$ and an oracle O, if $O(x_i) = y_i$ for all $i \in [q]$, we consider that O extends τ, which is symbolized as $O \vdash \tau$.

3. Extended Mirror Theory

Let $\mathcal{E} = \mathcal{E}^{=} \cup \mathcal{E}^{\neq}$ be the following affine system of bi-variate equations and non-equations [30,31]:

$$\mathcal{E}^{=} \begin{cases} X_1 \oplus Y_1 = \lambda_1 \\ X_2 \oplus Y_2 = \lambda_2 \\ \cdots\cdots\cdots\cdots \\ X_q \oplus Y_q = \lambda_q \end{cases} \quad \mathcal{E}^{\neq} \begin{cases} X'_1 \oplus Y'_1 \neq \lambda'_1 \\ X'_2 \oplus Y'_2 \neq \lambda'_2 \\ \cdots\cdots\cdots\cdots \\ X'_{q_v} \oplus Y'_{q_v} \neq \lambda'_{q_v} \end{cases}$$

The affine system $\mathcal{E}$ can be described as an undirected weighted graph $G =< V, E, W >$ or bipartite graph $G =< V_1, V_2, E, W >$, where the vertex set $V = V_1 \cup V_2$, the edge set E, and the weighted function W are, respectively,

$$V_1 = \{X_1, \ldots, X_q, X'_1, \ldots, X'_{q_v}\}, V_2 = \{Y_1, \ldots, Y_q, Y'_1, \ldots, Y'_{q_v}\},$$
$$E = \{e = (X, Y)\} \cup \{e' = (X', Y')\},$$
$$W : E \to \{0,1\}^n.$$

Let $G^= =< V^=, E^=, W >$ be the subgraph of G induced by $\mathcal{E}^=$. We assume that $G^=$ is divided into α components with more than two vertexes and β components with only two vertexes, i.e., $G^= = C_1 \cup \ldots \cup C_\alpha \cup D_1 \cup \ldots \cup D_\beta$.

We say that graph G is good if it satisfies the following three conditions:

- $G^=$ must be acylic, i.e., $G^=$ has no graph cycles.
- $W(\mathcal{P}) \neq 0$ for all paths $\mathcal{P}$ in the graph $G^=$, where $W(\mathcal{P}) = \sum_{e \in \mathcal{P}} W(e)$.
- $W(\mathcal{C}) \neq 0$ for all cycles $\mathcal{C}$ with exactly one non-equation edge e' (the remaining edges are the equation edges) in the graph G, where $W(\mathcal{C}) = \sum_{e \in \mathcal{C}} W(e)$.

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

- $G^=$ must be acylic, i.e., $G^=$ has no graph cycles.
- $W(\mathcal{P}) \neq 0$ for all paths $\mathcal{P}$ with an even length in the graph $G^=$, where $W(\mathcal{P}) = \sum_{e \in \mathcal{P}} W(e)$.
- $W(\mathcal{C}) \neq 0$ for all cycles $\mathcal{C}$ with an even length containing exactly one non-equation edge e' (the remaining edges are the equation edges) in the graph G, where $W(\mathcal{C}) = \sum_{e \in \mathcal{C}} W(e)$.

Lemma 4 (Graph Description of Extended Mirror Theory [30]). *Let $G =< V, E, W >$ be a good undirected weighted graph induced by $\mathcal{E}$, and $|V| = r, |E| = q + q_v$. 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*

$$\frac{(2^n)_r}{2^{nq}}(1 - \frac{9q_c^2}{4 \cdot 2^n} - \frac{9q_c^2 q + 24q_c q^2 + 6q_c q + 40q^2}{2^{2n}} - \frac{16q^4}{2^{3n}} - \frac{7q_v}{2^n}).$$

Lemma 5 (Bipartite Graph Description of Extended Mirror Theory [30]). *Let $G =< V_1, V_2, E, W >$ be a good undirect weighted bipartite graph induced by $\mathcal{E}$, and $|V_1| = q', |V_2| = q'', q' + q'' = r, |E| = q + q_v$. 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*

$$\frac{(2^n)_{q'}(2^n)_{q''}}{2^{nq}}(1 - \frac{9q_c^2}{4 \cdot 2^n} - \frac{9q_c^2 q + 6q_c q^2 + 4q^2}{4 \cdot 2^{2n}} - \frac{8q^4}{3 \cdot 2^{3n}} - \frac{5q_v}{2^n}).$$

4. GCM-RIV1

We introduce RIV to GCM-SIV1, propose GCM-RIV1, and prove its sAE security. GCM-RIV1 inherits the full security guarantee from GCM-SIV1 and provides stronger security and robustness against the leakage of invalid plaintext.

4.1. Specific Description of GCM-RIV1

Let $H : \mathcal{K}_H \times \mathcal{N} \times \mathcal{H} \times \{0,1\}^* \to \{0,1\}^n$ be an ϵ AXU hash function, and $E : \mathcal{K}_E \times \{0,1\}^n \to \{0,1\}^n$ be a block cipher, where $\mathcal{K}_H$ is a hash key space, $\mathcal{N}$ is a nonce space, $\mathcal{H}$ is an associated data space, $\mathcal{K}_E$ is an encryption key space, and n is the block size.

According to the idea of RIV, firstly, a nonce $N \in \mathcal{N}$, an associated datum $A \in \mathcal{H}$, and a plaintext $M \in \{0,1\}^*$ can be processed by a function constructed by a hash function H with a hash key $L \in \mathcal{K}_H$ and a block cipher E with an encryption key $K \in \mathcal{K}_E$ to generate a robust initialization vector $V \in \{0,1\}^n$. Then, the initialization vector V and the plaintext

M are taken as inputs of the CounTeR (CTR) encryption algorithm with a block cipher E_K and return the ciphertext C. Again, the nonce N, the associated datum A, and the ciphertext C are processed by the function constructed by a hash function H with a hash key L and a block cipher E with an encryption key K and then it returns S. Finally, S is added to V to generate the authentication tag $T \in \{0,1\}^n$.

The overview of GCM-RIV1 is illustrated in Figure 1. The key generation, encryption, decryption, leakage, GHASH, and CTR algorithms are shown in Algorithms 1, 2, 3, 4, 5 and 6, respectively.

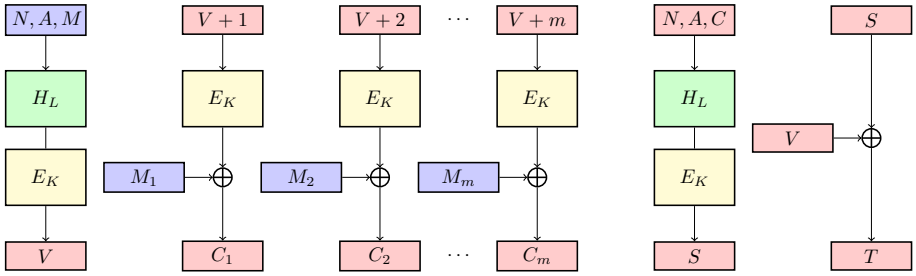

Figure 1. GCM-RIV1: GCM variant with robust initialization vector.

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

Input: a key parameter k
Output: two keys (L, K)
$(L, K) \xleftarrow{\$} \mathcal{K}_H \times \mathcal{K}_E$
return (L, K)

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

Input: two keys (L, K), a nonce N, an associated datum A, and a plaintext M
Output: a ciphertext C and a tag T
$I = H_L(N, A, M) = GHASH_L(A, M) \oplus N||[0]_{\frac{n}{4}}$
$V = E_K(I)$
$C = CTR_K(V, M)$
$J = H_L(N, A, C) = GHASH_L(A, C) \oplus N||[0]_{\frac{n}{4}}$
$S = E_K(J)$
$T = V \oplus S$
return (C, T)

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

Input: two keys (L, K), a nonce N, an associated datum A, a ciphertext C, and a tag T
Output: a plaintext M or $\perp$
$J = H_L(N, A, C) = GHASH_L(A, C) \oplus N||[0]_{\frac{n}{4}}$
$S = E_K(J)$
$V = T \oplus S$
$M = CTR_K(V, C)$
$I = H_L(N, A, M) = GHASH_L(A, M) \oplus N||[0]_{\frac{n}{4}}$
$V' = E_K(I)$
if $V' = V$, **return** M
else return $\perp$ (INVALID)
endif

Algorithm 4 The leakage algorithm: Λ

Input: two keys (L, K), a nonce N, an associated datum A, a ciphertext C, and a tag T
Output: a leaking invalid plaintext M or $\top$
$J = H_L(N, A, C) = GHASH_L(A, C) \oplus N||[0]_{\frac{n}{4}}$
$S = E_K(J)$
$V = T \oplus S$
$M = CTR_K(V, C)$
$I = H_L(N, A, M) = GHASH_L(A, M) \oplus N||[0]_{\frac{n}{4}}$
$V' = E_K(I)$
if $V' = V$, **return** $\top$
else return M
endif

Algorithm 5 GHASH algorithm: $GHASH_L(A, M)$

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

Algorithm 6 CTR algorithm: $CTR_K(V, M)$

Input: a key K, an initial vector V, and a plaintext M
Output: a ciphertext C
Partition M into $M_1 \| \ldots \| M_m$, $|M_i| = n, 1 \leq i \leq m-1, 0 < |M_m| \leq n$
for $i = 1$ **to** $m-1$ **do**
  $C_i \leftarrow E_K(V + i) \oplus M_i$
endfor
$C_m \leftarrow msb_{|M_m|}(E_K(V + m)) \oplus M_m$
return $C = C_1||C_2|| \ldots ||C_m$

4.2. Security of GCM-RIV1

We present the information-theoretic security proof of GCM-RIV1 under the assumption that the underlying block cipher is a secure pseudorandom permutation.

Theorem 1. *Let H be an ϵ-AXU hash function. Let $\mathcal{A}$ be an adversary against GCM-RIV1 that makes at most q queries with at most σ blocks in total. Then, there exists an adversary $\mathcal{B}$ against E that makes at most $7(2q + \sigma)$ queries, and one has*

$$Adv^{SAE}_{GCM-RIV1}(\mathcal{A}) \leq Adv^{PRP}_{E}(\mathcal{B}) + \frac{6(q+\sigma)^2 + 3q}{2^n} + 12q^2\epsilon.$$

Proof. The idea of the proof depends on the decomposition of the SAE security model. Thus, calculating the upper bound on $Adv^{SAE}_{GCM-RIV1}(\mathcal{A})$ is transformed into calculating the upper bounds of $Adv^{IND-CPA}_{GCM-RIV1}(\mathcal{A}_1)$, $Adv^{INT-CTXT}_{GCM-RIV1}(\mathcal{A}_2)$, and $Adv^{ERR-CCA}_{GCM-RIV1}(\mathcal{A}_3)$, where $\mathcal{A}_1, \mathcal{A}_2$ and $\mathcal{A}_3$ are IND-CPA, INT-CTXT, and ERR-CCA adversaries against GCM-RIV1, respectively, and each makes at most q queries of at most σ blocks.

First, we upper-bound $Adv^{IND-CPA}_{GCM-RIV1}(\mathcal{A}_1)$. In the IND-CPA security model, the adversary $\mathcal{A}_1$ makes q queries to the encryption oracle $\mathcal{E}_K$ (real scheme GCM-RIV1) or \$ (ideal version of GCM-RIV1). According to Definition 3, one has

$$Adv^{IND-CPA}_{GCM-RIV1}(\mathcal{A}_1) = \mid Pr[K \leftarrow \mathcal{K} : \mathcal{A}^{\mathcal{E}_K} = 1] - Pr[\mathcal{A}^{\$} = 1] \mid$$

We replace the block ciphers E_K in GCM-RIV1 with a random permutation π, which costs $Adv^{PRP}_{E}(\mathcal{B})$ for a PRP adversary $\mathcal{B}$ against E with at most $q + \sigma$ queries.

We assume that the adversary $\mathcal{A}_1$ makes q queries $(N^1, A^1, M^1), \ldots, (N^q, A^q, M^q)$ to the encryption oracle and it reruns $(C^1, T^1), \ldots, (C^q, T^q)$. We record all query–response pairs as a transcript $\tau = \{(N^1, A^1, M^1, C^1, T^1), \ldots, (N^q, A^q, M^q, C^q, T^q)\}$.

According to the H-coefficient lemma (Lemma 3), here, we first define a bad transcript and then state the probability of a bad transcript in the ideal world.

Definition 8. *A transcript τ is called bad if one of the following events holds:*

1. *Collisions occur between the outputs of the ϵ-AXU hash function H_L.*
   - *Bad1: $I^i = I^j$ $(V^i = V^j)$ for any $1 \le i \ne j \le q$.*
   - *Bad2: $J^i = J^j$ $(S^i = S^j)$ for any $1 \le i \ne j \le q$.*
   - *Bad3: $I^i = J^j$ $(V^i = S^j)$ for any $1 \le i, j \le q$.*
2. *Collisions occur between the inputs or outputs of π.*
   - *Bad4: $V^i + k = V^j + l$ for any $1 \le i, j \le q$, $1 \le k \le m^i$, $1 \le l \le m^j$, and $(i, k) \ne (j, l)$.*
   - *Bad5: $V^i + k = I^j$ for any $1 \le i, j \le q$, $1 \le k \le m^i$.*
   - *Bad6: $V^i + k = J^j$ for any $1 \le i, j \le q$, $1 \le k \le m^i$.*
3. *Collisions occur between the authentication tags.*
   - *Bad7: $T^i = T^j$ for any $1 \le i \ne j \le q$.*

Let Γ_{bad} be a set of all bad transcripts, Γ be a set of all transcripts, and $\Gamma = \Gamma_{bad} \cup \Gamma_{good}$. Let X_{re} be the random variable interacting with the real scheme GCM-RIV1$[\pi]$ and Y_{id} be the random variable interacting with the ideal version. We first upper-bound the probability $Pr[Y_{id} \in \Gamma_{bad}]$.

For the event Bad1, given any two distinct tuples of the nonce, the associated data, and the plaintext $(N^i, A^i, M^i) \ne (N^j, A^j, M^j)$, according to the properties of the ϵ-AXU hash function H, the probability of $I^i = I^j$ is

$$Pr[I^i = I^j] = Pr[H_L(N^i, A^i, M^i) = H_L(N^j, A^j, M^j)] \le \epsilon.$$

Therefore, for q queries, one has

$$Pr[Bad1] = \sum_{1 \le i \ne j \le q} Pr[I^i = I^j] \le q^2\epsilon/2.$$

Similarly, for the event Bad2, one has $Pr[Bad2] = \sum_{1 \le i \ne j \le q} Pr[J^i = J^j] \le q^2\epsilon/2$.

For the event Bad3, one has $Pr[Bad3] = \sum_{1 \le i,j \le q} Pr[I^i = J^j] \le q^2\epsilon$.

For the event Bad4, according to $\sigma = \sum_{1 \le i \le q} m^i = \sum_{1 \le j \le q} m^j$, one has

$$\begin{aligned} Pr[Bad4] &= \sum_{1 \le i \ne j \le q} \sum_{1 \le k \le m^i, 1 \le l \le m^j} Pr[V^i + k = V^j + l] + \sum_{1 \le i \le q} \sum_{1 \le k \ne l \le m^i} Pr[V^i + k = V^j + l] \\ &\le \sigma^2/2^n. \end{aligned}$$

For the event Bad5, according to the properties of the ϵ-AXU hash function H, the probability of $V^i + k = I^j$ is

$$Pr[V^i + k = I^j] = Pr[V^i + k = H_L(N^j, A^j, M^j)] \leq 1/2^n.$$

Therefore, for q queries, according to $\sigma = \sum_{1 \leq i \leq q} m^i$, one has

$$Pr[Bad5] = \sum_{1 \leq i,j \leq q} \sum_{1 \leq k \leq m^i} Pr[V^i + k = I^j] \leq q\sigma/2^n.$$

Similarly, for the event Bad6, $Pr[Bad6] = \sum_{1 \leq i,j \leq q} \sum_{1 \leq k \leq m^i} Pr[V^i + k = J^j] \leq q\sigma/2^n$.
For the event Bad7, one has $Pr[Bad7] = \sum_{1 \leq i \neq j \leq q} Pr[T^i = T^j] \leq q^2/2^{n+1}$.
To sum up, one has

$$Pr[Y_{id} \in \Gamma_{bad}] = \bigcup_{1 \leq i \leq 7} Pr[Badi] \leq \sum_{1 \leq i \leq 7} Pr[Badi] \leq \frac{(q+\sigma)^2}{2^n} + 2q^2\epsilon.$$

In the good transcript τ, we bound the ratio between $Pr[X_{re} = \tau]$ and $Pr[Y_{id} = \tau]$.
For the real scheme GCM-RIV1[π], one has

$$\begin{aligned} Pr[X_{re} = \tau] &= Pr[\pi \in Perm(n) : GCM - RIV1[\pi] \vdash \tau] \\ &= \frac{|\pi \in Perm(n) : GCM - RIV1[\pi] \vdash \tau|}{|Perm(n)|} \\ &= \frac{(2^n - (q+\sigma))!}{(2^n)!} = \frac{1}{(2^n)_{q+\sigma}} \geq \frac{1}{2^{(q+\sigma)n}}. \end{aligned}$$

For the ideal version \$, one has

$$Pr[Y_{id} = \tau] = Pr[\$ \in Func(|N| + |A| + |M|, (q+\sigma)n) : \$ \vdash \tau] = \frac{1}{2^{(q+\sigma)n}}.$$

Therefore, the ratio between $Pr[X_{re} = \tau]$ and $Pr[Y_{id} = \tau]$ is $\frac{Pr[X_{re}=\tau]}{Pr[Y_{id}=\tau]} \geq 1$.
Therefore, according to the H-coefficient technique, for a PRP adversary $\mathcal{B}$ against E with at most $q + \sigma$ queries, one has

$$Adv^{IND-CPA}_{GCM-RIV1}(\mathcal{A}_1) \leq Adv^{PRP}_{E}(\mathcal{B}) + \frac{(q+\sigma)^2}{2^n} + 2q^2\epsilon.$$

Then, we upper-bound $Adv^{INT-CTXT}_{GCM-RIV1}(\mathcal{A}_2)$. In the INT-CTXT security model, the adversary $\mathcal{A}_2$ has access to encryption and decryption oracles $\mathcal{E}_K$ and $\mathcal{D}_K$, with at most q queries of at most σ blocks each. According to Definition 4, one has

$$Adv^{INT-CTXT}_{GCM-RIV1}(\mathcal{A}) = Pr[K \twoheadleftarrow \mathcal{K} : \mathcal{A}^{\mathcal{E}_K, \mathcal{D}_K} \, forges].$$

The evaluation of $Adv^{INT-CTXT}_{GCM-RIV1}(\mathcal{A}_2)$ is similar to the above. Therefore, we briefly describe it here. In the decryption oracle, for every fresh tuple of the nonce, the associated data, and the plaintext, the ϵ-AXU hash function H generates an identical I or V with ϵ probability. Similarly, for every fresh tuple of the nonce, the associated data, and the ciphertext, the ϵ-AXU hash function H generates an identical J or S with ϵ probability. Therefore, the adversary makes q queries to bring at most approximately $q^2\epsilon$ collision probabilities. In addition, I may collide with J, which brings about $q^2\epsilon$ collision probabilities. For each fresh V, CTR will generate a random key-stream. According to the result of the CTR mode, it costs $Adv^{PRP}_{E}(\mathcal{B}) + \frac{\sigma^2}{2^n}$. Similarly, collisions may occur between the authentication tags, which cost $\frac{q^2}{2^{n+1}}$. Besides this, $V+1, V+2, \ldots$ may collide with I or J, which costs $\frac{2q\sigma}{2^n}$. For each new tuple of the nonce, the associated data, the ciphertext, and

the authentication tag, the probability that the decryption algorithm passes the verification is at most $q/2^n$. Therefore, for a PRP adversary $\mathcal{B}$ against E with at most $2(2q+\sigma)$ queries, one has

$$Adv^{INT-CTXT}_{GCM-RIV1}(\mathcal{A}_2) \leq Adv^{PRP}_{E}(\mathcal{B}) + \frac{(q+\sigma)^2+q}{2^n} + 2q^2\epsilon.$$

Finally, we upper-bound $Adv^{ERR-CCA}_{GCM-RIV1}(\mathcal{A}_3)$. In the ERR-CCA security model, the adversary $\mathcal{A}_3$ has access to encryption, decryption, and leakage oracles, with at most q queries of at most σ blocks each. According to Definition 6, one has

$$Adv^{ERR-CCA}_{GCM-RIV1}(\mathcal{A}) = \mid Pr[K \twoheadleftarrow \mathcal{K} : \mathcal{A}^{\mathcal{E}_K,\mathcal{D}_K,\Lambda_K} = 1] - Pr[K, K' \twoheadleftarrow \mathcal{K} : \mathcal{A}^{\mathcal{E}_K,\mathcal{D}_K,\Lambda_{K'}} = 1] \mid .$$

Similar to the cases above, the probability of bad events (collisions occur) in the encryption or decryption oracles is upper-bounded by $Adv^{PRP}_{E}(\mathcal{B}) + \frac{(q+\sigma)^2}{2^n} + 2q^2\epsilon$. In the leakage algorithm Λ, for two distinct dummy keys K, K', the probability of bad events (collisions occur) is also upper-bounded by $Adv^{PRP}_{E}(\mathcal{B}) + \frac{(q+\sigma)^2}{2^n} + 2q^2\epsilon$. Besides this, for each new tuple of the nonce, the associated data, the ciphertext, and the authentication tag, the probability that the leakage algorithm passes the verification is at most $q/2^n$. Therefore, for a PRP adversary $\mathcal{B}$ against E with at most $4(2q+\sigma)$ queries, one has

$$Adv^{ERR-CCA}_{GCM-RIV1}(\mathcal{A}_3) \leq Adv^{PRP}_{E}(\mathcal{B}) + \frac{4(q+\sigma)^2+2q}{2^n} + 8q^2\epsilon.$$

To summarize, according to Lemma 2, the SAE security of GCM-RIV1 is upper-bounded by

$$Adv^{SAE}_{GCM-RIV1}(\mathcal{A}) \leq Adv^{PRP}_{E}(\mathcal{B}) + \frac{6(q+\sigma)^2+3q}{2^n} + 12q^2\epsilon.$$

The security proof of Theorem 1 is finished. □

Theorem 1 shows that GCM-RIV1 enjoys birthday-bound SAE security with $n/2$-bit and nonce-misuse resistance if the underlying block cipher is a secure PRP and $\epsilon = 2^{-n}$.

5. GCM-RIV2

To support beyond-birthday-bound (BBB) security, we introduce the sum of permutation (SoP) construction to GCM-RIV1, propose GCM-RIV2, and prove its sAE security. GCM-RIV2 provides stronger BBB security and robustness against the leakage of invalid plaintext.

5.1. Specific Description of GCM-RIV2

Before describing the specific scheme, let us explain our design idea. In the beginning, we wished to construct it based on GCM-SIV2. GCM-SIV2 is a BBB-secure nonce-based AE scheme and it follows SIV. Similar to GCM-RIV1, we introduce RIV instead of SIV to GCM-SIV2 and invoke two extra hash functions to generate two initialization vectors. In the encryption algorithm of GCM-SIV2, two initialization vectors are taken as the inputs of the SoP-based CTR-like mode to generate the key-stream and then the result is XORed to the plaintext to generate the ciphertext. Meanwhile, two initialization vectors are taken as the inputs of an SoP construction to generate the authentication tag. However, we found that the design obtained in this way is very inefficient. To improve the efficiency while ensuring BBB security, we utilize an initialization vector and a nonce instead of two initialization vectors so that we can perform pre-calculations during the encryption and decryption. Let us name this new scheme GCM-RIV2. The encryption part of GCM-RIV2 is an SoP-based CTR-like mode that ensures BBB security. The authentication part of GCM-RIV2 is an XOR construction of two pseudorandom values, which ensures BBB security.

We specifically describe GCM-RIV2 as follows. Let $H : \mathcal{K}_H \times \mathcal{N} \times \mathcal{H} \times \{0,1\}^* \to \{0,1\}^n$ be an ϵ-AXU-hash function and $E : \mathcal{K}_E \times \{0,1\}^n \to \{0,1\}^n$ be a block cipher, where $\mathcal{K}_H$ is a hash key space, $\mathcal{N}$ is a nonce space, $\mathcal{H}$ is an associated data space, $\mathcal{K}_E$ is an encryption key space, and n is the block size.

According to the idea of RIV, firstly, a nonce $N \in \mathcal{N}$, an associated datum $A \in \mathcal{H}$, and a plaintext $M \in \{0,1\}^*$ can be processed by a function constructed by a hash function H with a hash key $L \in \mathcal{K}_H$ and a block cipher E with an encryption key $K \in \mathcal{K}_E$ to generate a robust initialization vector $V \in \{0,1\}^n$. Then, the initialization vector V, the nonce N, and the plaintext M are taken as inputs of the SoP-based CTR encryption algorithm with two block ciphers E_{K_1} and E_{K_2} and return the ciphertext C. Again, the nonce N, the associated datum A, and the ciphertext C are processed by the function constructed by a hash function H with a hash key L and a block cipher E with an encryption key K and then it returns S. Finally, S is added to V to generate the authentication tag $T \in \{0,1\}^n$.

The overview of GCM-RIV2 is illustrated in Figure 2.

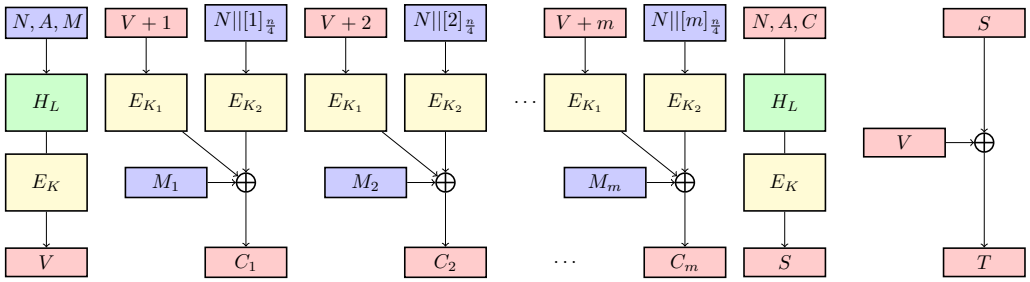

Figure 2. GCM-RIV2: beyond-birthday-bound secure GCM variant with robust initialization vector.

The key generation, encryption, decryption, leakage, and SoP-based CTR algorithms are shown in Algorithms 7, 8, 9, 10 and 11, respectively.

Algorithm 7 The key generation algorithm: $\mathcal{KG}$

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

Algorithm 8 The encryption algorithm: $\mathcal{E}$

Input: four keys (K, K_1, K_2, L), a nonce N, an associated datum A, and a plaintext M
Output: a ciphertext C and a tag T
$I = H_L(N, A, M) = GHASH_L(A, M) \oplus N||[0]_{\frac{n}{4}}$
$V = E_K(I)$
$C = SCTR_{K_1,K_2}(V, N, M)$
$J = H_L(N, A, C) = GHASH_L(A, C) \oplus N||[0]_{\frac{n}{4}}$
$S = E_K(J)$
$T = S \oplus V$
return (C, T)

Algorithm 9 The decryption algorithm: $\mathcal{D}$

Input: four keys (K, K_1, K_2, L), a nonce N, an associated datum A, a ciphertext C, and a tag T
Output: a plaintext M or $\perp$
$J = H_L(N, A, C) = GHASH_L(A, C) \oplus N||[0]_{\frac{n}{4}}$
$S = E_K(J)$
$V = S \oplus T$
$M = SCTR_{K_1,K_2}(V, N, C)$
$I = H_L(N, A, M) = GHASH_L(A, M) \oplus N||[0]_{\frac{n}{4}}$
$V' = E_K(I)$
if $V' = V$, **return** M
else return $\perp$ (INVALID)
endif

Algorithm 10 The leaking algorithm: Λ

Input: four keys (K, K_1, K_2, L), a nonce N, an associated datum A, a ciphertext C, and a tag T
Output: a leaking invalid plaintext M or $\top$
$J = H_L(N, A, C) = GHASH_L(A, C) \oplus N||[0]_{\frac{n}{4}}$
$S = E_K(J)$
$V = S \oplus T$
$M = SCTR_{K_1,K_2}(V, N, C)$
$I = H_L(N, A, M) = GHASH_L(A, M) \oplus N||[0]_{\frac{n}{4}}$
$V' = E_K(I)$
if $V' = V$, **return** $\top$
else return M
endif

Algorithm 11 SoP-based CTR algorithm: $SCTR_{K_1,K_2}(V, N, M)$

Input: two keys K_1, K_2, an initial vector V, a nonce N, and a plaintext M
Output: a ciphertext C
Partition M into $M_1 \| \ldots \| M_m$, $|M_i| = n, 1 \leq i \leq m-1, 0 < |M_m| \leq n$
for $i = 1$ **to** $m-1$ **do**
  $C_i \leftarrow E_{K_1}(V + i) \oplus E_{K_2}(N||[i]_{\frac{n}{4}}) \oplus M_i$
endfor
$C_m \leftarrow msb_{|M_m|}(E_{K_1}(V + m) \oplus E_{K_2}(N||[m]_{\frac{n}{4}})) \oplus M_m$
return $C = C_1||C_2||\ldots||C_m$

5.2. Security of GCM-RIV2

We present the information-theoretic security proof of GCM-RIV2 under the assumption that the underlying block cipher is a secure pseudorandom permutation.

Theorem 2. *Let H be an ϵ-AXU hash function. Let $\mathcal{A}$ be an adversary against GCM-RIV2 that makes at most q queries with at most σ blocks in total. Then, there exists an adversary $\mathcal{B}$ against E that makes at most $7(2q + 2\sigma)$ queries, and one has*

$$Adv^{SAE}_{GCM-RIV2}(\mathcal{A}) \leq Adv^{PRP}_{E}(\mathcal{B}) + +12q^{4/3}\epsilon + \frac{6\sigma^{4/3}}{2^{n+1}} + \frac{6q^{4/3}}{2^{n+1}} + \frac{12\sigma\mu^2}{2^n} + \frac{6\sigma^2}{2^{2n}} + 6q^2\epsilon^2 + \frac{12q^2\epsilon}{2^n} + \frac{4\sigma^2\mu^2}{2^{2n}} + \frac{8q^2\epsilon^2}{2^n} + \frac{486\sigma^{4/3} + 26\sigma + 1752q^{4/3} + 412q}{2^n}.$$

Proof. Similar to the security proof of Theorem 1, according to the decomposition of SAE security, calculating the upper bound on $Adv^{SAE}_{GCM-RIV2}(\mathcal{A})$ is transformed into calculating the upper bounds of $Adv^{IND-CPA}_{GCM-RIV2}(\mathcal{A}_1)$, $Adv^{INT-CTXT}_{GCM-RIV2}(\mathcal{A}_2)$, and $Adv^{ERR-CCA}_{GCM-RIV2}(\mathcal{A}_3)$, where

$\mathcal{A}_1, \mathcal{A}_2$ and $\mathcal{A}_3$ are IND-CPA, INT-CTXT, and ERR-CCA adversaries against GCM-RIV2, respectively, and each makes at most q queries of at most σ blocks.

First, we upper-bound $Adv^{IND-CPA}_{GCM-RIV2}(\mathcal{A}_1)$. In the IND-CPA security model, the adversary $\mathcal{A}_1$ makes q queries to the encryption oracle $\mathcal{E}$ (real scheme GCM-RIV2) or \$ (ideal version of GCM-RIV2).

We replace all block ciphers E_K, E_{K_1}, and E_{K_2} in GCM-RIV2 with random permutations π, π_1, and π_2, which costs $Adv^{PRP}_E(\mathcal{B})$ for a PRP adversary $\mathcal{B}$ against E with at most $2q + 2\sigma$ queries. Then, one has

$$Adv^{IND-CPA}_{GCM-RIV2}(\mathcal{A}_1) \leq Adv^{PRP}_E(\mathcal{B}) + Adv^{IND-CPA}_{GCM-RIV2[\pi,\pi_1,\pi_2]}(\mathcal{A}_1). \tag{1}$$

We assume that the adversary $\mathcal{A}_1$ makes q queries $(N^1, A^1, M^1), \ldots, (N^q, A^q, M^q)$ to the encryption oracle and it reruns $(C^1, T^1), \ldots, (C^q, T^q)$. We record all query–response pairs as a transcript $\tau = \{(N^1, A^1, M^1, C^1, T^1), \ldots, (N^q, A^q, M^q, C^q, T^q)\}$. Then, one has

$$V : \begin{cases} V^1 = \pi(H_L(N^1, A^1, M^1)) \\ \ldots\ldots\ldots\ldots\ldots \\ V^q = \pi(H_L(N^q, A^q, M^q)) \end{cases}$$

$$SCTR : \begin{cases} \pi_1(V^1 + 1) \oplus \pi_2(N^1||[1]_{\frac{n}{4}}) = M^1_1 \oplus C^1_1 \\ \ldots\ldots\ldots\ldots\ldots \\ \pi_1(V^1 + m^1) \oplus \pi_2(N^1||[m^1]_{\frac{n}{4}}) = M^1_{m^1} \oplus C^1_{m^1} \\ \pi_1(V^2 + 1) \oplus \pi_2(N^2||[1]_{\frac{n}{4}}) = M^2_1 \oplus C^2_1 \\ \ldots\ldots\ldots\ldots\ldots \\ \pi_1(V^2 + m^2) \oplus \pi_2(N^2||[m^2]_{\frac{n}{4}}) = M^2_{m^2} \oplus C^2_{m^2} \\ \ldots\ldots\ldots\ldots\ldots \\ \pi_1(V^q + 1) \oplus \pi_2(N^q||[1]_{\frac{n}{4}}) = M^q_1 \oplus C^q_1 \\ \ldots\ldots\ldots\ldots\ldots \\ \pi_1(V^q + m^q) \oplus \pi_2(N^q||[m^q]_{\frac{n}{4}}) = M^q_{m^q} \oplus C^q_{m^q} \end{cases}$$

$$S : \begin{cases} S^1 = \pi(H_L(N^1, A^1, C^1)) \\ \ldots\ldots\ldots\ldots\ldots \\ S^q = \pi(H_L(N^q, A^q, C^q)) \end{cases}$$

$$T : \begin{cases} S^1 \oplus V^1 = T^1 \\ S^2 \oplus V^2 = T^2 \\ \ldots\ldots\ldots\ldots\ldots \\ S^q \oplus V^q = T^q \end{cases}$$

According to the H-coefficient lemma (Lemma 3), here, we first define a bad transcript and then state the probability of a bad transcript in the ideal world and the ratio between the probability of good transcripts in the real world and the probability of good transcripts in the ideal world.

After observing, we found that the equations above correspond to two distinct mirror systems: the SCTR mirror system and the T mirror system. Let $X_{i,j} = \pi_1(V^i + j)$, $Y_{i,j} = \pi_2(N^i||[j]_{\frac{n}{4}})$, and $\lambda_{i,j} = M^i_j \oplus C^i_j$, where $i \in [q], j \in [m^i]$ and $\sigma = \sum_{i\in[q]} m^i$. Let $V_1^=$

be a set of vertices $\{X_{i,j}\}_{i\in[q],j\in[m^i]}$, $V_2^=$ be a set of vertices $\{Y_{i,j}\}_{i\in[q],j\in[m^i]}$, $E^=$ be a set of edges $\{(X_{i,j}, Y_{i,j})\}_{i\in[q],j\in[m^i]}$, and $W^= : E^= \rightarrow \{\lambda_{i,j}\}_{i\in[q],j\in[m^i]}$ be a weighted function. Then, the SCTR mirror system corresponds to a bipartite graph $G^=_{SCTR} =< V_1^=, V_2^=, E^=, W^= >$. Similarly, the T mirror system corresponds to a graph $G^=_T =< V_T^=, E_T^=, W_T^= >$, where $V_T^= = \{S^i, V^i\}_{i\in[q]}, E_T^= = \{(S^i, V^i)\}_{i\in[q]}$ and $W_T^= : E_T^= \rightarrow \{T^i\}_{i\in[q]}$.

In order to be able to use the extended mirror theory and H-coefficient technique, we need to define bad transcripts.

Definition 9. *A transcript τ is called bad if one of the following events holds:*

1. *The number of collisions from the outputs of the hash function H_L is larger than $q^{2/3}$.*
   - *Bad1: $|I^i = I^j| \geq q^{2/3}$ or $|V^i = V^j| \geq q^{2/3}$.*
   - *Bad2: $|J^i = J^j| \geq q^{2/3}$ or $|S^i = S^j| \geq q^{2/3}$.*
   - *Bad3: $|I^i = J^j| \geq q^{2/3}$ or $|V^i = S^j| \geq q^{2/3}$.*
2. *The number of collisions from the inputs of π_1 is larger than $\sigma^{2/3}$.*
   - *Bad4: $|V^i + k = V^j + l| \geq \sigma^{2/3}$.*
3. *The number of collisions from the inputs of π_2 is larger than $q^{2/3}$.*
   - *Bad5: $|N^i = N^j| \geq q^{2/3}$.*
4. *The number of collisions from the authentication tag is larger than $q^{2/3}$.*
   - *Bad6: $|T^i = T^j| \geq q^{2/3}$.*
5. *The constraints of the extended mirror theory include the constraints of the SCTR mirror system (Bad7–Bad9) and the constraints of the the T mirror system (Bad10–Bad15).*
   - *Bad7: There exist distinct $i, k \in [q]$ such that $X_{i,j} = X_{k,l}$ and $Y_{i,j} = Y_{k,l}$, where $j \in [m^i]$ and $l \in [m^k]$, i.e., $V^i + j = V^k + l$ and $N^i||[j]_{n/4} = N^k||[l]_{n/4}$ (it implies $j = l$).*
   - *Bad8: There exist distinct $i, k \in [q]$ such that $X_{i,j} = X_{k,l}$ and $\lambda_{i,j} = \lambda_{k,l}$, where $j \in [m^i]$ and $l \in [m^k]$, i.e., $V^i + j = V^k + l$ and $M^i_j \oplus C^i_j = M^k_l \oplus C^k_l$.*
   - *Bad9: There exist distinct $i, k \in [q]$ such that $Y_{i,j} = Y_{k,l}$ and $\lambda_{i,j} = \lambda_{k,l}$, where $j \in [m^i]$ and $l \in [m^k]$, i.e., $N^i||[j]_{n/4} = N^k||[l]_{n/4}$ (it implies $j = l$) and $M^i_j \oplus C^i_j = M^k_l \oplus C^k_l$.*
   - *Bad10: There exist distinct $i, j \in [q]$ such that $S^i = S^j$ and $V^i = V^j$, i.e., $H_L(N^i, A^i, C^i) = H_L(N^j, A^j, C^j)$ and $H_L(N^i, A^i, M^i) = H_L(N^j, A^j, M^j)$.*
   - *Bad11: There exist distinct $i, j \in [q]$ such that $S^i = S^j$ and $T^i = T^j$, i.e., $H_L(N^i, A^i, C^i) = H_L(N^j, A^j, C^j)$ and $T^i = T^j$.*
   - *Bad12: There exist distinct $i, j \in [q]$ such that $V^i = V^j$ and $T^i = T^j$, i.e., $H_L(N^i, A^i, M^i) = H_L(N^j, A^j, M^j)$ and $T^i = T^j$.*
   - *Bad13: There exist distinct $i, j \in [q]$ such that $S^i = V^j$ and $V^i = S^j$, i.e., $H_L(N^i, A^i, C^i) = H_L(N^j, A^j, M^j)$ and $H_L(N^i, A^i, M^i) = H_L(N^j, A^j, C^j)$.*
   - *Bad14: There exist distinct $i, j \in [q]$ such that $S^i = V^j$ and $T^i = T^j$, i.e., $H_L(N^i, A^i, C^i) = H_L(N^j, A^j, M^j)$ and $T^i = T^j$.*
   - *Bad15: There exist distinct $i, j \in [q]$ such that $V^i = S^j$ and $T^i = T^j$, i.e., $H_L(N^i, A^i, M^i) = H_L(N^j, A^j, C^j)$ and $T^i = T^j$.*

Let Γ_{bad} be a set of all bad transcripts, Γ be a set of all transcripts, and $\Gamma = \Gamma_{bad} \cup \Gamma_{good}$. Let X_{re} be the random variable interacting with the real scheme GCM-RIV2[π, π_1, π_2] and Y_{id} be the random variable interacting with the ideal version. We first upper-bound the probability $Pr[Y_{id} \in \Gamma_{bad}]$.

For Bad1, according to the properties of ϵ-AXU hash functions, the expectation of $|I^i = I^j|$ for all q queries is $E[|I^i = I^j|] = q(q-1)\epsilon/2$. Then, according to Markov's inequality, the probability that Bad1 occurs is

$$Pr[Bad1] = Pr[|I^i = I^j|] \geq q^{2/3}] \leq \frac{E[|I^i = I^j|]}{q^{2/3}} \leq q^{4/3}\epsilon/2.$$

Similarly, for Bad2, one has $Pr[Bad2] \leq q^{4/3}\epsilon/2$.

For Bad3, according to the properties of ϵ-AXU hash functions, the expectation of $|I^i = J^j|$ for all q queries is $E[|I^i = J^j|] = q^2\epsilon$. Then, according to Markov's inequality, the probability that Bad1 occurs is

$$Pr[Bad3] = Pr[|I^i = J^j|] \geq q^{2/3}] \leq \frac{E[|I^i = J^j|]}{q^{2/3}} \leq q^{4/3}\epsilon.$$

For Bad4, the probability that $V^i + k = V^j + l$ occurs for any i, j, k, l is 2^{-n}. Therefore, the expectation of $|V^i + k = V^j + l|$ for all σ blocks is $E[|V^i + k = V^j + l|] \leq \sigma^2/2^{n+1}$. Then, according to Markov's inequality, the probability that Bad4 occurs is

$$Pr[Bad4] = Pr[|V^i + k = V^j + l|] \geq \sigma^{2/3}] \leq \frac{E[|V^i + k = V^j + l|]}{\sigma^{2/3}} \leq \frac{\sigma^{4/3}}{2^{n+1}}.$$

For Bad5, we consider the nonce-faulty setting. Let N be a μ-faulty nonce and $\mu^2 < q^{2/3}$. Therefore, the probability that Bad5 occurs is 0.

For Bad6, the probability that $T^i = T^j$ occurs for any i, j is 2^{-n}. Therefore, the expectation of $|T^i = T^j|$ for all q blocks is $E[|T^i = T^j|] \leq q^2/2^{n+1}$. Then, according to Markov's inequality, the probability that Bad6 occurs is

$$Pr[Bad6] = Pr[|T^i = T^j|] \geq q^{2/3}] \leq \frac{E[|T^i = T^j|]}{q^{2/3}} \leq \frac{q^{4/3}}{2^{n+1}}.$$

For Bad7, the probability that $V^i + j = V^k + l$ occurs for any i, j, k, l is 2^{-n} and the number of pairs (i, k) such that $N^i = N^k$ is at most μ^2. Then, the probability that Bad7 occurs is

$$Pr[Bad7] = \sum_{i,j,k,l} Pr[X_{i,j} = X_{k,l}, Y_{i,j} = Y_{k,l}] = \sum_{i,j,k} Pr[V^i + j = V^k + j, N^i = N^k] \leq \sigma\mu^2/2^n.$$

Similarly, for Bad8, the probability that $M^i_j \oplus C^i_j = M^k_l \oplus C^k_l$ occurs for any i, j, k, l is 2^{-n}. Then, the probability that Bad7 occurs is

$$\begin{aligned} Pr[Bad8] &= \sum_{i,j,k,l} Pr[X_{i,j} = X_{k,l}, \lambda_{i,j} = \lambda_{k,l}] = \sum_{i,j,k,l} Pr[V^i + j = V^k + l, M^i_j \oplus C^i_j = M^k_l \oplus C^k_l] \\ &\leq \sigma^2/2^{2n}. \end{aligned}$$

For Bad9, one has

$$Pr[Bad9] = \sum_{i,j,k,l} Pr[Y_{i,j} = Y_{k,l}, \lambda_{i,j} = \lambda_{k,l}] = \sum_{i,j,k} Pr[N^i = N^k, M^i_j \oplus C^i_j = M^k_j \oplus C^k_j] \leq \sigma\mu^2/2^n.$$

For Bad10, the probability that $S^i = S^j$ and $V^i = V^j$ occur for any i, j is ϵ. Then, the probability that Bad10 occurs is

$$\begin{aligned} Pr[Bad10] &= \sum_{i,j} Pr[S^i = S^j, V^i = V^j] \\ &= \sum_{i,j} Pr[H_L(N^i, A^i, C^i) = H_L(N^j, A^j, C^j), H_L(N^i, A^i, M^i) = H_L(N^j, A^j, M^j)] \\ &\leq q^2\epsilon^2/2. \end{aligned}$$

For Bad11, one has

$$\begin{aligned} Pr[Bad11] &= \sum_{i,j} Pr[S^i = S^j, T^i = T^j] \\ &= \sum_{i,j} Pr[H_L(N^i, A^i, C^i) = H_L(N^j, A^j, C^j), T^i = T^j] \\ &\leq q^2\epsilon/2^{n+1}. \end{aligned}$$

For Bad12, one has

$$\begin{aligned} Pr[Bad12] &= \sum_{i,j} Pr[V^i = V^j, T^i = T^j] \\ &= \sum_{i,j} Pr[H_L(N^i, A^i, M^i) = H_L(N^j, A^j, M^j), T^i = T^j] \\ &\leq q^2\epsilon/2^{n+1}. \end{aligned}$$

For Bad13, the probability that $S^i = V^j$ and $V^i = S^j$ occur for any i, j is ϵ. Then, the probability that Bad13 occurs is

$$\begin{aligned} Pr[Bad13] &= \sum_{i,j} Pr[S^i = V^j, V^i = S^j] \\ &= \sum_{i,j} Pr[H_L(N^i, A^i, C^i) = H_L(N^j, A^j, M^j), H_L(N^i, A^i, M^i) = H_L(N^j, A^j, C^j)] \\ &\leq q^2\epsilon^2/2. \end{aligned}$$

For Bad14, one has

$$\begin{aligned} Pr[Bad14] &= \sum_{i,j} Pr[S^i = V^j, T^i = T^j] \\ &= \sum_{i,j} Pr[H_L(N^i, A^i, C^i) = H_L(N^j, A^j, M^j), T^i = T^j] \\ &\leq q^2\epsilon/2^{n+1}. \end{aligned}$$

For Bad15, one has

$$\begin{aligned} Pr[Bad15] &= \sum_{i,j} Pr[V^i = S^j, T^i = T^j] \\ &= \sum_{i,j} Pr[H_L(N^i, A^i, M^i) = H_L(N^j, A^j, C^j), T^i = T^j] \\ &\leq q^2\epsilon/2^{n+1}. \end{aligned}$$

To sum up, the probability of bad transcripts is

$$\begin{aligned} Pr[Y_{id} \in \Gamma_{bad}] &= \bigcup_{1\le i\le 15} Pr[Badi] \le \sum_{1\le i\le 15} Pr[Badi] \\ &\le 2q^{4/3}\epsilon + \frac{\sigma^{4/3}}{2^{n+1}} + \frac{q^{4/3}}{2^{n+1}} + \frac{2\sigma\mu^2}{2^n} + \frac{\sigma^2}{2^{2n}} + q^2\epsilon^2 + \frac{2q^2\epsilon}{2^n}. \end{aligned} \tag{2}$$

In the good transcript τ, we bound the ratio $\frac{Pr[X_{re}=\tau]}{Pr[Y_{id}=\tau]}$ between the real scheme GCM-RIV2$[\pi, \pi_1, \pi_2]$ and its ideal version.

First, we consider $Pr[X_{re} = \tau]$ for a good transcript τ in the real scheme GCM-RIV2$[\pi, \pi_1, \pi_2]$.

For the SCTR mirror system, as $|V^i + k = V^j + l| \le \sigma^{2/3}$, the number of edges in components with a size of more than 2 is $\sigma_c \le 4\sigma^{2/3}$. Therefore, according to Theorem 5, the number of solutions of $G^{=}_{SCTR}$ is at least

$$\frac{(2^n)_{|V_1^=|}(2^n)_{|V_2^=|}}{2^{n\sigma}}(1-\delta_1),$$

where $\delta_1 = \frac{9\sigma_c^2}{4\cdot 2^n} + \frac{9\sigma_c^2\sigma + 6\sigma_c\sigma^2 + 4\sigma^2}{4\cdot 2^{2n}} + \frac{8\sigma^4}{3\cdot 2^{3n}} \le \frac{36\sigma^{4/3}}{2^n} + \frac{36\sigma^{7/3} + 6\sigma^{8/3} + \sigma^2}{2^{2n}} + \frac{8\sigma^4}{3\cdot 2^{3n}} \le \frac{81\sigma^{4/3}+\sigma}{2^n}$.

Similarly, for the T mirror system, as $|S^i = S^j| \le q^{2/3}$ and $|V^i = V^j| \le q^{2/3}$, the number of edges in components with a size of more than 2 is $q_c \le 4q^{2/3}$. Therefore, according to Theorem 4, the number of solutions of $G^{=}_{T}$ is at least

$$\frac{(2^n)_{|V_T^=|}}{2^{nq}}(1-\delta_2),$$

where $\delta_2 = \frac{9q_c^2}{4\cdot 2^n} + \frac{9q_c^2 q + 24q_c q^2 + 6q_c q + 40q^2}{2^{2n}} + \frac{16q^4}{2^{3n}} \le \frac{36q^{4/3}}{2^n} + \frac{144q^{7/3} + 96q^{8/3} + 24q^{5/3} + 40q^2}{2^{2n}} + \frac{16q^4}{2^{3n}} \le \frac{292q^{4/3}+64q}{2^n}$.

Therefore, for a good graph, it must satisfy both $G^{=}_{SCTR}$ and $G^{=}_{T}$. It follows that the number of solutions of a good graph G is at least

$$\frac{(2^n)_{|V_1^=|}(2^n)_{|V_2^=|}}{2^{n\sigma}} \frac{(2^n)_{|V_T^=|}}{2^{nq}}(1-\delta_1)(1-\delta_2).$$

In the real scheme GCM-RIV2$[\pi, \pi_1, \pi_2]$, one has

$$\begin{aligned} Pr[X_{re} = \tau] &= Pr[\pi, \pi_1, \pi_2 \in Perm(n) : GCM - RIV2[\pi, \pi_1, \pi_2] \vdash \tau] \\ &= \frac{|\pi, \pi_1, \pi_2 \in Perm(n) : GCM - RIV2[\pi, \pi_1, \pi_2] \vdash \tau|}{|Perm(n)|^3} \\ &\ge \frac{\frac{(2^n)_{|V_1^=|}(2^n)_{|V_2^=|}}{2^{n\sigma}} \frac{(2^n)_{|V_T^=|}}{2^{nq}}(1-\delta_1)(1-\delta_2)(2^n - |V_1^=|)!(2^n - |V_2^=|)!(2^n - |V_T^=|)!}{(2^n!)^3} \\ &= \frac{1}{2^{n\sigma}} \frac{1}{2^{nq}}(1-\delta_1)(1-\delta_2). \end{aligned}$$

In the ideal version \$, one has

$$Pr[Y_{id} = \tau] = Pr[\$ \in Func(|N| + |A| + |M|, (q+\sigma)n) : \$ \vdash \tau] = \frac{1}{2^{(q+\sigma)n}}.$$

Therefore, the ratio between $Pr[X_{re} = \tau]$ and $Pr[Y_{id} = \tau]$ in the good transcript is

$$\frac{Pr[X_{re} = \tau]}{Pr[Y_{id} = \tau]} \ge (1-\delta_1)(1-\delta_2) \ge 1 - (\delta_1 + \delta_2) = 1 - \delta, \tag{3}$$

where $\delta = \delta_1 + \delta_2 \leq \frac{81\sigma^{4/3}+\sigma+292q^{4/3}+64q}{2^n}$.

According to the H-coefficient technique and Equations (1)–(3), for a PRP adversary $\mathcal{B}$ against E with at most $2q + 2\sigma$ queries, one has

$$Adv^{IND-CPA}_{GCM-RIV2}(\mathcal{A}_1) \leq Adv^{PRP}_{E}(\mathcal{B}) + 2q^{4/3}\epsilon + \frac{\sigma^{4/3}}{2^{n+1}} + \frac{q^{4/3}}{2^{n+1}} + \frac{2\sigma\mu^2}{2^n} + \frac{\sigma^2}{2^{2n}} + q^2\epsilon^2 + \frac{2q^2\epsilon}{2^n} + \frac{81\sigma^{4/3}+\sigma+292q^{4/3}+64q}{2^n}.$$

Then, we upper-bound $Adv^{INT-CTXT}_{GCM-RIV2}(\mathcal{A}_2)$. The evaluation process is similar to that of $Adv^{IND-CPA}_{GCM-RIV2}(\mathcal{A}_1)$ except that it also includes that of the extended mirror system with equations and non-equations under forgery attempts. In the INT-CTXT security model, the adversary can access the encryption and decryption oracles. We assume that the adversary $\mathcal{A}_2$ makes q forgery attempts $(N^{*1}, A^{*1}, C^{*1}, T^{*1}), \ldots, (N^{*q}, A^{*q}, C^{*q}, T^{*q})$ to the decryption oracle after q queries $(N^1, A^1, M^1), \ldots, (N^q, A^q, M^q)$ to the encryption oracle and does not make invalid queries. We record all query–response pairs as a transcript $\tau = \{(N^1, A^1, M^1, C^1, T^1), \ldots, (N^q, A^q, M^q, C^q, T^q), (N^{*1}, A^{*1}, M^{*1}, C^{*1}, T^{*1}), ..., (N^{*q}, A^{*q}, M^{*q}, C^{*q}, T^{*q})\}$. Unlike the mirror system in the IND-CPA security model, here, we consider an extended mirror system with equations and non-equations. The system with equations generated by the encryption oracle is the same as that of IND-CPA, so they are not listed. Let us simply list the system with equations and non-equations generated by the decryption oracle (forgery attempts) below.

$$S^* : \begin{cases} S^{*1} = \pi(H_L(N^{*1}, A^{*1}, C^{*1})) \\ \ldots\ldots\ldots\ldots\ldots \\ S^{*q} = \pi(H_L(N^{*q}, A^{*q}, C^{*q})) \end{cases}$$

$$V^* : \begin{cases} V^{*1} = \pi(H_L(N^{*1}, A^{*1}, M^{*1})) \\ \ldots\ldots\ldots\ldots\ldots \\ V^{*q} = \pi(H_L(N^{*q}, A^{*q}, M^{*q})) \end{cases}$$

$$SCTR^* : \begin{cases} \pi_1(V^{*1}+1) \oplus \pi_2(N^{*1}||[1]_{\frac{n}{4}}) \neq M^{*1}_1 \oplus C^{*1}_1 \\ \ldots\ldots\ldots\ldots\ldots \\ \pi_1(V^{*1}+m^{*1}) \oplus \pi_2(N^{*1}||[m^{*1}]_{\frac{n}{4}}) \neq M^{*1}_{m^{*1}} \oplus C^{*1}_{m^{*1}} \\ \pi_1(V^{*2}+1) \oplus \pi_2(N^{*2}||[1]_{\frac{n}{4}}) \neq M^{*2}_1 \oplus C^{*2}_1 \\ \ldots\ldots\ldots\ldots\ldots \\ \pi_1(V^{*2}+m^{*2}) \oplus \pi_2(N^{*2}||[m^{*2}]_{\frac{n}{4}}) \neq M^{*2}_{m^{*2}} \oplus C^{*2}_{m^{*2}} \\ \ldots\ldots\ldots\ldots\ldots \\ \pi_1(V^{*q}+1) \oplus \pi_2(N^{*q}||[1]_{\frac{n}{4}}) \neq M^{*q}_1 \oplus C^{*q}_1 \\ \ldots\ldots\ldots\ldots\ldots \\ \pi_1(V^{*q}+m^{*q}) \oplus \pi_2(N^{*q}||[m^{*q}]_{\frac{n}{4}}) \neq M^{*q}_{m^{*q}} \oplus C^{*q}_{m^{*q}} \end{cases}$$

$$T^* : \begin{cases} S^{*1} \oplus V^{*1} \neq T^{*1} \\ S^{*2} \oplus V^{*2} \neq T^{*2} \\ \ldots\ldots\ldots\ldots\ldots \\ S^{*q} \oplus V^{*q} \neq T^{*q} \end{cases}$$

According to the H-coefficient lemma (Lemma 3), here, we first define a bad transcript and then state the probability of a bad transcript in the ideal world and the ratio between

the probability of good transcripts in the real world and the probability of good transcripts in the ideal world.

After observing, we found that the system above corresponds to two distinct extended mirror systems: the SCTR with SCTR* system and the T with T* system. Let $X_{i,j} = \pi_1(V^i + j)$, $Y_{i,j} = \pi_2(N^i||[j]_{\frac{n}{4}})$, and $\lambda_{i,j} = M^i_j \oplus C^i_j$, where $i \in [q], j \in [m^i]$ and $\sigma = \sum_{i\in[q]} m^i$. Let $V_1^=$ be a set of vertices $\{X_{i,j}\}_{i\in[q],j\in[m^i]}$, $V_2^=$ be a set of vertices $\{Y_{i,j}\}_{i\in[q],j\in[m^i]}$, $E^=$ be a set of edges $\{(X_{i,j}, Y_{i,j})\}_{i\in[q],j\in[m^i]}$, and $W^= : E^= \to \{\lambda_{i,j}\}_{i\in[q],j\in[m^i]}$ be a weighted function. Then, the SCTR mirror system corresponds to a bipartite graph $G^=_{SCTR} =< V_1^=, V_2^=, E^=, W^= >$. Let $X^*_{i,j} = \pi_1(V^{*i} + j)$, $Y^*_{i,j} = \pi_2(N^{*i}||[j]_{\frac{n}{4}})$, and $\lambda^*_{i,j} = M_j{*i} \oplus C_j{*i}$, where $i \in [q], j \in [m^{*i}]$ and $\sigma = \sum_{i\in[q]} m^{*i}$. Let $V_1^{\neq}$ be a set of vertices $\{X^*_{i,j}\}_{i\in[q],j\in[m^{*i}]}$, $V_2^{\neq}$ be a set of vertices $\{Y^*_{i,j}\}_{i\in[q],j\in[m^{*i}]}$, $E^{\neq}$ be a set of edges $\{(X^*_{i,j}, Y^*_{i,j})\}_{i\in[q],j\in[m^{*i}]}$, and $W^{\neq} : E^{\neq} \to \{\lambda^*_{i,j}\}_{i\in[q],j\in[m^{*i}]}$ be a weighted function. Then, the SCTR with the SCTR* system corresponds to a bipartite graph $G_{SCTR} =< V_1, V_2, E, W >$, where $V_1 = V_1^= \cup V_1^{\neq}$, $V_2 = V_2^= \cup V_2^{\neq}$, $E = E^= \cup E^{\neq}$, and $W = W^= \cup W^{\neq}$.

Similarly, the T mirror system corresponds to a graph $G^=_T =< V^=_T, E^=_T, W^=_T >$, where $V^=_T = \{S^i, V^i\}_{i\in[q]}$, $E^=_T = \{(S^i, V^i)\}_{i\in[q]}$ and $W^=_T : E^=_T \to \{T^i\}_{i\in[q]}$. Then, the T with T* system corresponds to a graph $G_T =< V_T, E_T, W_T >$, where $V_T = V^=_T \cup V^{\neq}_T$, $E_T = E^=_T \cup E^{\neq}_T$, and $W_T = W^=_T \cup W^{\neq}_T$.

In order to be able to use the extended mirror theory and H-coefficient technique, we need to define bad transcripts.

Definition 10. *A transcript τ is called bad if one of the following events holds:*

1. *Bad1–Bad15 is the same as that of Definition 9.*
2. *Bad16: $V^{*i} + j = V^k + l$, $N^{*i}||[j]_{\frac{n}{4}} = N^k||[l]_{\frac{n}{4}}$, and $M^{*i}_j \oplus C^{*i}_j = M^{*k}_l \oplus C^{*k}_l$.*
3. *Bad17: $S^{*i} = S^j$, $V^{*i} = V^j$, and $T^{*i} = T^j$.*
4. *Bad18: $S^{*i} = V^j$, $V^{*i} = S^j$, and $T^{*i} = T^j$.*

Let Γ_{bad} be a set of all bad transcripts, Γ be a set of all transcripts, and $\Gamma = \Gamma_{bad} \cup \Gamma_{good}$. Let X_{re} be the random variable interacting with the real scheme GCM-RIV2$[\pi, \pi_1, \pi_2]$ and Y_{id} be the random variable interacting with the ideal version. We first upper-bound the probability $Pr[Y_{id} \in \Gamma_{bad}]$.

For Bad1–Bad15, Equation (2) has given

$$Pr[Bad1 - Bad15] \leq 2q^{4/3}\epsilon + \frac{\sigma^{4/3}}{2^{n+1}} + \frac{q^{4/3}}{2^{n+1}} + \frac{2\sigma\mu^2}{2^n} + \frac{\sigma^2}{2^{2n}} + q^2\epsilon^2 + \frac{2q^2\epsilon}{2^n}.$$

For Bad16, the probability that $V^{*i} + j = V^k + l$ or $M^{*i}_j \oplus C^{*i}_j = M^{*k}_l \oplus C^{*k}_l$ occurs for any i, j, k, l is 2^{-n} and the number of pairs (i, k) such that $N^{*i} = N^k$ is at most μ^2. Then, the probability of Bad16 is

$$\begin{aligned} Pr[Bad16] &= \sum_{i,j,k,l} Pr[V^{*i} + j = V^k + l, N^{*i}||[j]_{\frac{n}{4}} = N^k||[l]_{\frac{n}{4}}, M^{*i}_j \oplus C^{*i}_j = M^{*k}_l \oplus C^{*k}_l] \\ &= \sum_{i,j,k} Pr[V^{*i} + j = V^k + j, N^{*i} = N^k, M^{*i}_j \oplus C^{*i}_j = M^{*k}_j \oplus C^{*k}_j] \\ &\leq \frac{\sigma^2\mu^2}{2^{2n}}. \end{aligned}$$

For Bad17, the probability that $S^{*i} = S^j$ or $V^{*i} = V^j$ occurs for any i, j is at most ϵ and the probability that $T^{*i} = T^j$ occurs for any i, j is 2^{-n}. Then, the probability of Bad17 is

$$Pr[Bad17] = \sum_{i,j} Pr[S^{*i} = S^j, V^{*i} = V^j, T^{*i} = T^j] \leq \frac{q^2\epsilon^2}{2^n}.$$

For Bad18, the probability that $S^{*i} = V^j$ or $V^{*i} = S^j$ occurs for any i, j is at most ϵ and the probability that $T^{*i} = T^j$ occurs for any i, j is 2^{-n}. Then, the probability of Bad18 is

$$Pr[Bad18] = \sum_{i,j} Pr[S^{*i} = V^j, V^{*i} = S^j, T^{*i} = T^j] \leq \frac{q^2\epsilon^2}{2^n}.$$

To sum up, the probability of bad transcripts in the ideal world is

$$\begin{aligned} Pr[Y_{id} \in \Gamma_{bad}] &= \bigcup_{i\in[18]} Pr[Badi] \leq \sum_{i\in[18]} Pr[Badi] \\ &\leq 2q^{4/3}\epsilon + \frac{\sigma^{4/3}}{2^{n+1}} + \frac{q^{4/3}}{2^{n+1}} + \frac{2\sigma\mu^2}{2^n} + \frac{\sigma^2}{2^{2n}} + q^2\epsilon^2 + \frac{2q^2\epsilon}{2^n} + \frac{\sigma^2\mu^2}{2^{2n}} + \frac{2q^2\epsilon^2}{2^n}. \end{aligned} \tag{4}$$

In the good transcript τ, we bound the ratio $\frac{Pr[X_{re}=\tau]}{Pr[Y_{id}=\tau]}$ between the real scheme GCM-RIV2$[\pi, \pi_1, \pi_2]$ and its ideal version.

First, we consider $Pr[X_{re} = \tau]$ for a good transcript τ in the real scheme GCM-RIV2$[\pi, \pi_1, \pi_2]$.

For the SCTR with the SCTR* extended mirror system, as $|V^i + k = V^j + l| \leq \sigma^{2/3}$, the number of edges in components with a size of more than 2 is $\sigma_c \leq 4\sigma^{2/3}$. Therefore, according to Theorem 5, the number of solutions of G_{SCTR} is at least

$$\frac{(2^n)_{|V_1|}(2^n)_{|V_2|}}{2^{n\sigma}}(1-\delta_1),$$

where $\delta_1 = \frac{9\sigma_c^2}{4\cdot 2^n} + \frac{9\sigma_c^2\sigma+6\sigma_c\sigma^2+4\sigma^2}{4\cdot 2^{2n}} + \frac{8\sigma^4}{3\cdot 2^{3n}} + \frac{5\sigma}{2^n} \leq \frac{36\sigma^{4/3}}{2^n} + \frac{36\sigma^{7/3}+6\sigma^{8/3}+\sigma^2}{2^{2n}} + \frac{8\sigma^4}{3\cdot 2^{3n}} + \frac{5\sigma}{2^n} \leq \frac{81\sigma^{4/3}+6\sigma}{2^n}$.

Similarly, for the T with the T* extended mirror system, as $|S^i = S^j| \leq \sqrt{q}$ and $|V^i = V^j| \leq q^{2/3}$, the number of edges in components with a size of more than 2 is $q_c \leq 4q^{2/3}$. Therefore, according to Theorem 4, the number of solutions of G_T is at least

$$\frac{(2^n)_{|V_T|}}{2^{nq}}(1-\delta_2),$$

where $\delta_2 = \frac{9q_c^2}{4\cdot 2^n} + \frac{9q_c^2q+24q_cq^2+6q_cq+40q^2}{2^{2n}} + \frac{16q^4}{2^{3n}} + \frac{7q}{2^n} \leq \frac{36q^{4/3}}{2^n} + \frac{144q^{7/3}+96q^{8/3}+24q^{5/3}+40q^2}{2^{2n}} + \frac{16q^4}{2^{3n}} + \frac{7q}{2^n} \leq \frac{292q^{4/3}+71q}{2^n}$.

Therefore, for a good graph, it must satisfy both G_{SCTR} and G_T. It follows that the number of solutions of a good graph is at least

$$\frac{(2^n)_{|V_1|}(2^n)_{|V_2|}}{2^{n\sigma}} \frac{(2^n)_{|V_T|}}{2^{nq}}(1-\delta_1)(1-\delta_2).$$

In the real scheme GCM-RIV2$[\pi, \pi_1, \pi_2]$, one has

$$\begin{aligned} Pr[X_{re} = \tau] &= Pr[\pi, \pi_1, \pi_2 \in Perm(n) : GCM - RIV2[\pi, \pi_1, \pi_2] \vdash \tau] \\ &= \frac{|\pi, \pi_1, \pi_2 \in Perm(n) : GCM - RIV2[\pi, \pi_1, \pi_2] \vdash \tau|}{|Perm(n)|^3} \\ &\geq \frac{\frac{(2^n)_{|V_1|}(2^n)_{|V_2|}}{2^{n\sigma}} \frac{(2^n)_{|V_T|}}{2^{nq}} (1-\delta_1)(1-\delta_2)(2^n - |V_1|)!(2^n - |V_2|)!(2^n - |V_T|)!}{(2^n!)^3} \\ &= \frac{1}{2^{n\sigma}} \frac{1}{2^{nq}} (1-\delta_1)(1-\delta_2). \end{aligned}$$

In the ideal version \$, one has

$$Pr[Y_{id} = \tau] = Pr[\$ \in Func(|N| + |A| + |M|, (q+\sigma)n) : \$ \vdash \tau] = \frac{1}{2^{(q+\sigma)n}}.$$

Therefore, the ratio between $Pr[X_{re} = \tau]$ and $Pr[Y_{id} = \tau]$ in the good transcript is

$$\frac{Pr[X_{re} = \tau]}{Pr[Y_{id} = \tau]} \geq (1-\delta_1)(1-\delta_2) \geq 1 - (\delta_1 + \delta_2) = 1 - \delta, \tag{5}$$

where $\delta = \delta_1 + \delta_2 \leq \frac{81\sigma^{4/3} + 6\sigma + 292q^{4/3} + 71q}{2^n}$.

According to the H-coefficient technique and Equations (1), (4) and (5), for a PRP adversary $\mathcal{B}$ against E with at most $4q + 4\sigma$ queries, one has

$$\begin{aligned} Adv^{INT-CTXT}_{GCM-RIV2}(\mathcal{A}_1) \leq & Adv^{PRP}_E(\mathcal{B}) + 2q^{4/3}\epsilon + \frac{\sigma^{4/3}}{2^{n+1}} + \frac{q^{4/3}}{2^{n+1}} + \frac{2\sigma\mu^2}{2^n} + \frac{\sigma^2}{2^{2n}} + q^2\epsilon^2 + \frac{2q^2\epsilon}{2^n} \\ & + \frac{\sigma^2\mu^2}{2^{2n}} + \frac{2q^2\epsilon^2}{2^n} + \frac{81\sigma^{4/3} + 6\sigma + 292q^{4/3} + 71q}{2^n}. \end{aligned}$$

Finally, we upper-bound $Adv^{ERR-CCA}_{GCM-RIV1}(\mathcal{A}_3)$. In the ERR-CCA security model, the adversary $\mathcal{A}_3$ has access to the encryption, decryption, and leakage oracles, with at most q queries of at most σ blocks each. The security analysis in the encryption or decryption oracle is similar to that under the above security models, and the security analysis in the leakage oracle is similar to that of the decryption oracle with forgery attempts under the INT-CTXT. Besides this, we also need to consider an extended mirror system with equations and non-equations for distinct dummy keys in the leakage oracle. Therefore, for a PRP adversary $\mathcal{B}$ against E with at most $8q + 8\sigma$ queries, one has

$$\begin{aligned} Adv^{ERR-CCA}_{GCM-RIV2}(\mathcal{A}_3) \leq & Adv^{PRP}_E(\mathcal{B}) + 8q^{4/3}\epsilon + \frac{4\sigma^{4/3}}{2^{n+1}} + \frac{4q^{4/3}}{2^{n+1}} + \frac{8\sigma\mu^2}{2^n} + \frac{4\sigma^2}{2^{2n}} + 4q^2\epsilon^2 + \frac{8q^2\epsilon}{2^n} \\ & + \frac{3\sigma^2\mu^2}{2^{2n}} + \frac{6q^2\epsilon^2}{2^n} + \frac{324\sigma^{4/3} + 19\sigma + 1168q^{4/3} + 277q}{2^n}. \end{aligned}$$

To summarize, according to Lemma 2, the SAE security of GCM-RIV2 is upper-bounded by

$$\begin{aligned} Adv^{SAE}_{GCM-RIV2}(\mathcal{A}) \leq & Adv^{PRP}_E(\mathcal{B}) + 12q^{4/3}\epsilon + \frac{6\sigma^{4/3}}{2^{n+1}} + \frac{6q^{4/3}}{2^{n+1}} + \frac{12\sigma\mu^2}{2^n} + \frac{6\sigma^2}{2^{2n}} + 6q^2\epsilon^2 + \frac{12q^2\epsilon}{2^n} \\ & + \frac{4\sigma^2\mu^2}{2^{2n}} + \frac{8q^2\epsilon^2}{2^n} + \frac{486\sigma^{4/3} + 26\sigma + 1752q^{4/3} + 412q}{2^n}. \end{aligned}$$

The security proof of Theorem 2 is finished. □

Theorem 2 shows that GCM-RIV2 enjoys beyond-birthday-bound SAE security with $3n/4$-bit and its security bound decreases as parameter μ increases if the underlying block cipher is a secure PRP and $\epsilon = 2^{-n}$.

6. Discussion and Conclusions

GCM-RIV1 and GCM-RIV2 are robust authenticated encryption modes with an inverse-free nature. Both of them are based on the RIV framework, which extends the SIV construction by adopting an extra hash function with block cipher encryption and support nonce misuse. GCM-RIV1 is rate 1 (a plaintext block per each encryption), while GCM-RIV2 is rate 1/2 (a plaintext block per two encryptions). However, fortunately, the nonce-based encryption part of GCM-RIV2 can be precomputed, which means that the running speed of GCM-RIV2 is close to that of GCM-RIV1. Besides this, GCM-RIV1 and GCM-RIV2 are parallelizable. Therefore, overall, the performance of GCM-RIV1 and GCM-RIV2 is only slightly lower than that of GCM-SIV1.

From the perspective of the security, GCM-RIV1 and GCM-RIV2 support stronger security than GCM-SIV1. GCM-RIV1 guarantees birthday-bound SAE security of $n/2$-bit and supports robustness against the leakage of invalid plaintext. GCM-RIV2 enjoys beyond-birthday-bound SAE security with $3n/4$-bit graceful degradation and supports robustness against faulty nonces and the leakage of invalid plaintext. Table 1 shows the comparison between our schemes and previous related schemes.

Currently, GCM, GCM-SIV, and its related variants have been widely used in network security protocols. With the complexity, isomerization, and diversification of the network environment, GCM-RIV1 and GCM-RIV2, as robust AE modes, will be highly valued. GCM-RIV1 and GCM-RIV2 provide subtle AE security, nonce-faulty resistance, and birthday-bound security or even degradation-friendly beyond-birthday-bound security, meeting the requirements of the complex, isomerized, and diversified network environments for the robustness, elasticity, and reliable security of AE schemes. However, GCM-RIV1 and GCM-RIV2 need to be further optimized in terms of efficiency and security. GCM-RIV1 only ensures birthday-bound security, while GCM-RIV2 is rate 1/2. One potential future task is to further design more efficient and robust cryptographic schemes adapted to specific environments.

Funding: This research was funded by the National Natural Science Foundation of China (Grant Nos. 61902195, 62072207, and 62272238) and Guangdong Basic and Applied Basic Research Foundation (Grant No. 2022A1515140090).

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

Acknowledgments: I would like to express my sincere thanks to editors and the anonymous reviewers for their 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, Proceedings of the 5th International Conference on Cryptology in India, Chennai, India, 20–22 December 2004*; Canteaut, A., Viswanathan, K., Eds.; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2004; Volume 3348, pp. 343–355. [CrossRef]
2. Viega, J.; McGrew, D.A. The Use of Galois/Counter Mode (GCM) in IPsec Encapsulating Security Payload (ESP). *RFC* **2005**, *4106*, 1–11. [CrossRef]
3. Salowey, J.; Choudhury, A.; McGrew, D.A. AES Galois Counter Mode (GCM) Cipher Suites for TLS. *RFC* **2008**, *5288*, 1–8. [CrossRef]
4. Rogaway, P.; Shrimpton, T. A Provable-Security Treatment of the Key-Wrap Problem. In *Advances in Cryptology—EUROCRYPT 2006, Proceedings of the 25th Annual International Conference on the Theory and Applications of Cryptographic Techniques, St. Petersburg, Russia, 28 May–1 June 2006*; Vaudenay, S., Ed.; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2006; Volume 4004, pp. 373–390. [CrossRef]
5. Iwata, T.; Yasuda, K. HBS: A Single-Key Mode of Operation for Deterministic Authenticated Encryption. In *Fast Software Encryption, Proceedings of the 16th International Workshop, FSE 2009, Leuven, Belgium, 22–25 February 2009*; Dunkelman, O., Ed.; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2009; Volume 5665, pp. 394–415. [CrossRef]

6. Iwata, T.; Yasuda, K. BTM: A Single-Key, Inverse-Cipher-Free Mode for Deterministic Authenticated Encryption. In *Selected Areas in Cryptography, Proceedings of the 16th Annual International Workshop, SAC 2009, Calgary, AL, Canada, 13–14 August 2009*; Jacobson, M.J., Rijmen, V., Safavi-Naini, R., Eds.; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2009; Volume 5867, pp. 313–330. [CrossRef]
7. Reyhanitabar, R.; Vaudenay, S.; Vizár, D. Misuse-Resistant Variants of the OMD Authenticated Encryption Mode. In *Provable Security, Proceedings of the 8th International Conference, ProvSec 2014, Hong Kong, China, 9–10 October 2014*; Chow, S.S.M., Liu, J.K., Hui, L.C.K., Yiu, S., Eds.; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2014; Volume 8782, pp. 55–70. [CrossRef]
8. Gueron, S.; Lindell, Y. GCM-SIV: Full Nonce Misuse-Resistant Authenticated Encryption at Under One Cycle per Byte. In Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, Denver, CO, USA, 12–16 October 2015; Ray, I., Li, N., Kruegel, C., Eds.; ACM, Association for Computing Machinery: New York, NY, USA, 2015; pp. 109–119. [CrossRef]
9. Gueron, S.; Langley, A.; Lindell, Y. AES-GCM-SIV: Nonce Misuse-Resistant Authenticated Encryption. *RFC* **2019**, *8452*, 1–42. [CrossRef]
10. Iwata, T.; Minematsu, K. Stronger Security Variants of GCM-SIV. *IACR Trans. Symmetric Cryptol.* **2016**, *2016*, 134–157. [CrossRef]
11. Kresmer, P.; Zeh, A. CCM-SIV: Single-PRF Nonce-Misuse-Resistant Authenticated Encryption. *IACR Cryptol. ePrint Arch.* **2019**, *892*, 1–29.
12. Andreeva, E.; Bhati, A.S.; Vizár, D. Nonce-Misuse Security of the SAEF Authenticated Encryption Mode. In *Selected Areas in Cryptography, Proceedings of the SAC 2020—27th International Conference, Halifax, NS, Canada (Virtual Event), 21–23 October 2020*; Dunkelman, O., Jacobson, M.J., O'Flynn, C., Eds.; Lecture Notes in Computer Science; Springer: Cham, Switzerland, 2020; Volume 12804, pp. 512–534. [CrossRef]
13. Inoue, A.; Guo, C.; Minematsu, K. Nonce-misuse resilience of Romulus-N and GIFT-COFB. *IET Inf. Secur.* **2023**, *17*, 468–484. [CrossRef]
14. Dutta, A.; Nandi, M.; Talnikar, S. Beyond Birthday Bound Secure MAC in Faulty Nonce Model. In *Advances in Cryptology, Proceedings of the EUROCRYPT 2019—38th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Part I, Darmstadt, Germany, 19–23 May 2019*; Ishai, Y., Rijmen, V., Eds.; Lecture Notes in Computer Science; Springer: Cham, Switzerland, 2019; Volume 11476, pp. 437–466. [CrossRef]
15. Choi, W.; Lee, B.; Lee, J.; Lee, Y. Toward a Fully Secure Authenticated Encryption Scheme from a Pseudorandom Permutation. In *Advances in Cryptology, Proceedings of the ASIACRYPT 2021—27th International Conference on the Theory and Application of Cryptology and Information Security, Part III, Singapore, 6–10 December 2021*; Tibouchi, M., Wang, H., Eds.; Lecture Notes in Computer Science; Springer: Cham, Switzerland, 2021; Volume 13092, pp. 407–434. [CrossRef]
16. Andreeva, E.; Bogdanov, A.; Luykx, A.; Mennink, B.; Mouha, N.; Yasuda, K. How to Securely Release Unverified Plaintext in Authenticated Encryption. In *Advances in Cryptology, Proceedings of the ASIACRYPT 2014—20th International Conference on the Theory and Application of Cryptology and Information Security, Part I, Kaoshiung, Taiwan, 7–11 December 2014*; Sarkar, P., Iwata, T., Eds.; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2014; Volume 8873, pp. 105–125. [CrossRef]
17. Datta, N.; Luykx, A.; Mennink, B.; Nandi, M. Understanding RUP Integrity of COLM. *IACR Trans. Symmetric Cryptol.* **2017**, *2017*, 143–161. [CrossRef]
18. Zhang, P.; Wang, P.; Hu, H.; Cheng, C.; Kuai, W. INT-RUP Security of Checksum-Based Authenticated Encryption. In *Provable Security, Proceedings of the 11th International Conference, ProvSec 2017, Xi'an, China, 23–25 October 2017*; Okamoto, T., Yu, Y., Au, M.H., Li, Y., Eds.; Lecture Notes in Computer Science; Springer: Cham, Switzerland, 2017; Volume 10592, pp. 147–166. [CrossRef]
19. Imamura, K.; Minematsu, K.; Iwata, T. Integrity analysis of authenticated encryption based on stream ciphers. *Int. J. Inf. Sec.* **2018**, *17*, 493–511. [CrossRef]
20. Chakraborti, A.; Datta, N.; Jha, A.; Mancillas-López, C.; Nandi, M.; Sasaki, Y. INT-RUP Secure Lightweight Parallel AE Modes. *IACR Trans. Symmetric Cryptol.* **2019**, *2019*, 81–118. [CrossRef]
21. Ashur, T.; Dunkelman, O.; Luykx, A. Boosting Authenticated Encryption Robustness with Minimal Modifications. In *Advances in Cryptology, Proceedings of the CRYPTO 2017—37th Annual International Cryptology Conference, Part III, Santa Barbara, CA, USA, 20–24 August 2017*; Katz, J., Shacham, H., Eds.; Lecture Notes in Computer Science; Springer: Cham, Switzerland, 2017; Volume 10403, pp. 3–33. [CrossRef]
22. Datta, N.; Dutta, A.; Ghosh, S. INT-RUP Security of SAEB and TinyJAMBU. In *Progress in Cryptology, Proceedings of the INDOCRYPT 2022—23rd International Conference on Cryptology in India, Kolkata, India, 11–14 December 2022*; Isobe, T., Sarkar, S., Eds.; Lecture Notes in Computer Science; Springer: Cham, Switzerland, 2022; Volume 13774, pp. 146–170. [CrossRef]
23. Hoang, V.T.; Krovetz, T.; Rogaway, P. Robust Authenticated-Encryption AEZ and the Problem That It Solves. In *Advances in Cryptology, Proceedings of the EUROCRYPT 2015—34th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Part I, Sofia, Bulgaria, 26–30 April 2015*; Oswald, E., Fischlin, M., Eds.; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2015; Volume 9056, pp. 15–44. [CrossRef]
24. Badertscher, C.; Matt, C.; Maurer, U.; Rogaway, P.; Tackmann, B. Robust Authenticated Encryption and the Limits of Symmetric Cryptography. In *Cryptography and Coding, Proceedings of the 15th IMA International Conference, IMACC 2015, Oxford, UK, 15–17 December 2015*; Groth, J., Ed.; Lecture Notes in Computer Science; Springer: Cham, Switzerland, 2015; Volume 9496, pp. 112–129. [CrossRef]

25. Shrimpton, T.; Terashima, R.S. A Modular Framework for Building Variable-Input-Length Tweakable Ciphers. In *Advances in Cryptology, Proceedings of the ASIACRYPT 2013—19th International Conference on the Theory and Application of Cryptology and Information Security, Part I, Bengaluru, India, 1–5 December 2013*; Sako, K., Sarkar, P., Eds.; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2013; Volume 8269, pp. 405–423. [CrossRef]
26. Barwell, G.; Page, D.; Stam, M. Rogue Decryption Failures: Reconciling AE Robustness Notions. In *Cryptography and Coding, Proceedings of the 15th IMA International Conference, IMACC 2015, Oxford, UK, 15–17 December 2015*; Groth, J., Ed.; Lecture Notes in Computer Science; Springer: Cham, Switzerland, 2015; Volume 9496, pp. 94–111. [CrossRef]
27. Abed, F.; Forler, C.; List, E.; Lucks, S.; Wenzel, J. RIV for Robust Authenticated Encryption. In *Fast Software Encryption, Proceedings of the 23rd International Conference, FSE 2016, Bochum, Germany, 20–23 March 2016*; Peyrin, T., Ed.; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2016; Volume 9783, pp. 23–42. [CrossRef]
28. Patarin, J. The "Coefficients H" Technique. In *Selected Areas in Cryptography, Proceedings of the 15th International Workshop, SAC 2008, Sackville, NB, Canada, 14–15 August 2008*; Avanzi, R.M., Keliher, L., Sica, F., Eds.; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2008; Volume 5381, pp. 328–345. [CrossRef]
29. Hoang, V.T.; Tessaro, S. Key-Alternating Ciphers and Key-Length Extension: Exact Bounds and Multi-user Security. In *Advances in Cryptology, Proceedings of the CRYPTO 2016—36th Annual International Cryptology Conference, Santa Barbara, CA, USA, 14–18 August 2016*; Robshaw, M., Katz, J., Eds.; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2016; Volume 9814, pp. 3–32. [CrossRef]
30. Datta, N.; Dutta, A.; Dutta, K. Improved Security Bound of (E/D)WCDM. *IACR Trans. Symmetric Cryptol.* **2021**, *2021*, 138–176. [CrossRef]
31. Mennink, B.; Neves, S. Encrypted Davies-Meyer and Its Dual: Towards Optimal Security Using Mirror Theory. In *Advances in Cryptology, Proceedings of the CRYPTO 2017—37th Annual International Cryptology Conference, Part III, Santa Barbara, CA, USA, 20–24 August 2017*; Katz, J., Shacham, H., Eds.; Lecture Notes in Computer Science; Springer: Cham, Switzerland, 2017; Volume 10403, pp. 556–583. [CrossRef]