KIVR: Committing Authenticated Encryption Using Redundancy and Application to GCM, CCM, and More

Yusuke Naito[1(✉)], Yu Sasaki[2,3], and Takeshi Sugawara[4]

[1] Mitsubishi Electric Corporation, Kanagawa, Japan
Naito.Yusuke@ce.MitsubishiElectric.co.jp
[2] NTT Social Informatics Laboratories, Tokyo, Japan
yusk.sasaki@ntt.com
[3] Associate of National Institute of Standards and Technology, Gaithersburg, USA
[4] The University of Electro-Communications, Tokyo, Japan
sugawara@uec.ac.jp

Abstract. Constructing a committing authenticated encryption (AE) satisfying the **CMT**-4 security notion is an ongoing research challenge. We propose a new mode KIVR, a black-box conversion for adding the **CMT**-4 security to existing AEs. KIVR is a generalization of the Hash-then-Enc (HtE) [Bellare and Hoang, EUROCRYPT 2022] and uses a collision-resistant hash function to generate an initial value (or nonce) and a mask for redundant bits, in addition to a temporary key. We obtain a general bound $r/2 + \mathsf{tag\text{-}col}$ with r-bit redundancy for a large class of CTR-based AEs, where tag-col is the security against tag-collision attacks. Unlike HtE, the security of KIVR linearly increases with r, achieving beyond-birthday-bound security. With a t-bit tag, tag-col lies $0 \leq \mathsf{tag\text{-}col} \leq t/2$ depending on the target AE. We set $\mathsf{tag\text{-}col} = 0$ for GCM, GCM-SIV, and CCM, and the corresponding bound $r/2$ is tight for GCM and GCM-SIV. With CTR-HMAC, $\mathsf{tag\text{-}col} = t/2$, and the bound $(r+t)/2$ is tight.

Keywords: Key Commitment · Context Commitment · Authenticated Encryption · Security Proof · CTR · GCM · GCM-SIV · CCM · HMAC

1 Introduction

Authenticated encryption with associated data (AE) schemes that achieve confidentiality and authenticity are essential components in symmetric-key cryptography. The security of AE is well-studied, and the schemes usually come with security proofs based on a formal security notion. However, AE schemes are sometimes misused in a way beyond their promise, resulting in security problems. Committing security of AEs falls in this category and has been actively studied in the last few years [1,5,6,9,11,15,16,21,22].

Farshim et al. initiated the theoretical study of key commitment in 2017 [15], followed by the real-world attacks, including the multi-recipient integrity attack that delivers malicious content to a targeted user [1,11,16] and the

C. Pöpper and L. Batina (Eds.): ACNS 2024, LNCS 14583, pp. 318–347, 2024.
https://doi.org/10.1007/978-3-031-54770-6_13

partitioning oracle attack that achieves efficient password brute-force attacks [21]. The absence of the commitment to a secret key is the root cause of these problems. An AE encryption Π_{Enc} receives a secret key K, nonce N, associated data A, and plaintext M and generates a ciphertext $\Pi_{\mathsf{Enc}}(K, N, A, M)$. Without key-committing security, an adversary can efficiently find a ciphertext decrypted with multiple keys, i.e., $\Pi_{\mathsf{Enc}}(K, N, A, M) = \Pi_{\mathsf{Enc}}(K', N', A', M')$ with $K \neq K'$. Unfortunately, the previous AE security notions do not support key commitment, and there are $O(1)$ attacks on GCM [11,16], GCM-SIV [21], CCM [22], and ChaCha20-Poly1305 [16].

In the meantime, standardization bodies are starting to support committing security in AEs. For example, the recent RFC draft on usage limits on AEs considers key-committing security [19]. Similarly, the recent NIST workshop for updating the federal standard of block-cipher modes noted explicitly that key commitment is an additional security feature [25].

Context commitment is the generalization considering a stronger adversary. Bellare and Hoang [6] (and Chan and Rogaway independently [9]) proposed the security notions for context commitment. The security notions **CMT**-1, **CMT**-3, and **CMT**-4 consider $K \neq K'$, $(K, N, A) \neq (K', N', A')$, and $(K, N, A, M) \neq (K', N', A', M')$, respectively [6]. **CMT**-1 is the previous key-committing security. **CMT**-3 and **CMT**-4 are equivalent, and they are strictly more secure than **CMT**-1, covering a broader range of misuses.

As discussed above, ensuring and building AEs with committing security is an ongoing research challenge [1,11,16,21]. Before introducing the details about the concrete methods, we summarize the desired properties regarding this challenge, which are also our goals in this paper.

1. We want a conversion for adding the committing security to the standard AEs. In particular, we target a class of the AE schemes based on CTR [12], referred to as CTRAE, that includes GCM [14], GCM-SIV [17,18], and CCM [13]. We also target CTR-HMAC, the CTR combined with HMAC [24] comprising particular hash functions, such as SHA-256.
2. The schemes should satisfy the context-committing security, i.e., **CMT**-4.
3. A black-box conversion that respects the interface of the existing AEs is preferred for maintaining compatibility with the specifications of the standardized AE schemes and the hardware already deployed in the field.
4. The bit-security level for committing security is ideally the key size k, or at least greater than $\frac{k}{2}$, i.e., the beyond-birthday-bound (BBB) security regarding the key size. That is necessary to achieve an offline security level comparable with the standard AE-security, which is basically k bits.

1.1 Research Challenges

Here, we explain that the previous works [1,11,15,16,21] cannot achieve the above desired properties perfectly.

There is a line of works for designing a dedicated scheme with committing security [11,15], but they are not blackbox. In particular, Farshim et al. proposed to use a collision-resistant pseudo-random function (PRF) [15].

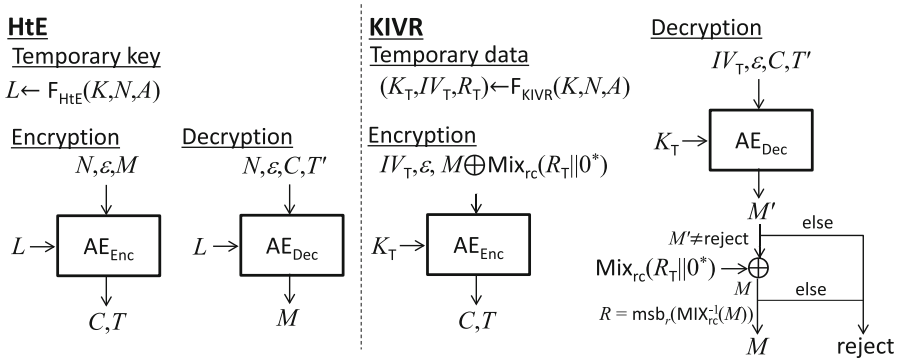

Fig. 1. HtE [6] (left) and KIVR (right). The function $\mathsf{F}_{\mathsf{KIVR}}$ generates a tuple of temporary key, IV, and redundant data. $\mathsf{Mix}_{\mathsf{rc}}$ is a function representing the positions of redundant bits.

The padding fix [1] prepends zero bits at the beginning of the message and enhances security by checking whether the prepended zero bits are successfully recovered in decryption. This method provides excellent compatibility because the changes to the original AE scheme are limited to messages. However, the security of the padding fix is proved for GCM only and is limited to CMT-1.

CTX [9] converts arbitrary AEs to **CMT**-4 secure ones. After computing a ciphertext C and tag T' using an underlying AE, it generates a new tag $T = H(K, N, A, T')$ by using a collision resistant (CR) hash function H. Unfortunately, CTX's compatibility with existing AEs is limited. In decryption, CTX should first regenerate T' and then $T = H(K, N, A, T')$ for comparison. Here, T' is an unverified tag within the original AE and is unavailable when the interface of the original AEAD is strict, e.g., in cryptographic APIs in a hardware security module or when there is a security policy regarding the release of unverified plaintexts [2]. NC4, a CTX-based scheme with reduced ciphertext expansion [7], has the same limitation.

HtE [6] shown in Fig. 1-(left) converts a **CMT**-1-secure AE to a **CMT**-4-secure one [6]. It generates a temporary key $L \leftarrow \mathsf{F}_{\mathsf{HtE}}(K, N, A)$ using a CR hash function $\mathsf{F}_{\mathsf{HtE}}$, and then L is used as the key of an underlying AE. Although HtE requires an additional CR hash function, it only changes the original AE's key values, thus maintaining high compatibility. The security of HtE combined with a non-**CMT**-1-secure AE, e.g., GCM, GCM-SIV, or CCM, is not guaranteed and is unknown. In particular, the security of HtE with GCM/CCM is limited by $\frac{k}{2}$, i.e., the birthday bound of the key. This is because the encryption results will also collide if two temporary keys collide. $\frac{k}{2}$ bits of security is too short for common cases, e.g., $k = n$ in AES-GCM, and can be even smaller considering concrete AEs.

In summary, designing a method to convert CTRAEs to achieve BBB security for **CMT**-4 in a black-box manner is a meaningful research challenge.[1]

1.2 Contributions

We propose a new black-box conversion KIVR that achieves BBB and **CMT**-4 security. The security bound is proved for CTRAE, including GCM, GCM-SIV, CCM, and CTR-HMAC.

The considerable difficulty is that the **CMT**-4 security of CTRAE is limited by $\frac{t}{2}$ bits due to a birthday attack on a tag, wherein the tag length t is often $t \leq k$. We approach the problem by adding redundancy to plaintexts, a natural extension of the padding fix [1]. Let M_{origin} be an original plaintext and R redundancy. We then define a plaintext with redundancy as $M = \mathsf{Mix}_{\mathsf{rc}}(R \| M_{\mathsf{origin}})$ wherein $\mathsf{Mix}_{\mathsf{rc}}$ is a function for defining the positions of each bit (or byte) of redundancy. The CMT security notion is naturally extended considering this plaintext with redundancy. We can increase the security by adding redundancy to messages. Besides adding extra redundancy, we can optionally exploit the redundancy already present in the message, such as constant strings or magic numbers found in popular file formats [20,28].[2]

The receiver who decrypts the message can check the decrypted message for redundancy, which potentially improves the context-committing security. However, such an improvement turns out to be non-trivial. The previous $O(1)$ attacks still break GCM, GCM-SIV, and CCM, even with redundancy (see Table 1). Similarly, the security of CTR-HMAC with redundancy is limited to $\frac{t}{2}$ due to a birthday attack on a tag. Combining HtE with redundancy is a viable option, but its security is upper-bounded by a simple attack using a collision either in redundancy or a key.

New Mode. KIVR shown in Fig. 1-(right) is a generalization of HtE. In HtE, a temporary key L is generated by $\mathsf{F}_{\mathsf{HtE}}(K, N, A)$. In contrast, KIVR generates a tuple of temporary values $(K_{\mathsf{T}}, IV_{\mathsf{T}}, R_{\mathsf{T}})$ using $\mathsf{F}_{\mathsf{KIVR}}(K, N, A)$, preventing the output size of the hash function $\mathsf{F}_{\mathsf{KIVR}}$ from becoming a security bottleneck. In encryption, we get a masked message $M \oplus \mathsf{Mix}_{\mathsf{rc}}(R_{\mathsf{T}} \| 0^*)$: a modified message wherein the redundant bits are masked with R_{T}. Finally, the original AE encrypts the masked message along with K_{T}, IV_{T}, and empty associated data. Decryption is naturally defined, but we additionally check if the redundancy R is correctly recovered.

We give a general bound for the **CMT**-4 security of KIVR with CTRAE that covers a large class of practical AEs, i.e., CTR combined with any MAC.

[1] An alternative approach for **CMT**-4 security is designing an indifferentiable AE scheme [4]. It can be used as an ideal AE scheme, where an adversary is allowed to select AE's keys, and is **CMT**-4-secure. An indifferentiable AE claims the security beyond the committing security notions, and thus its design is harder than that of a **CMT**-4-secure AE scheme.

[2] PNG and XML files have 64 and 192 bits of redundancy, respectively [20,28].

Table 1. AE schemes with black-box conversions for **CMT**-4 security using r-bit redundancy. k and t are the key and tag lengths, respectively.

Conversion	AE	CMT-4 Security	Ref.
Naive	GCM, GCM-SIV, CCM	0	[16,21,22]
Naive	CTR-HMAC	$\frac{t}{2}$	[15]
HtE [6]	GCM, GCM-SIV, CCM	$\min\{\frac{r}{2}, \frac{k}{2}\}$	—†
KIVR	GCM, GCM-SIV, CCM	$\frac{r}{2}$	Cor. 1
KIVR	CTR-HMAC	$\frac{r+t}{2}$	Cor. 2

†The security determined by a collision either in redundancy or a key.

Table 2. Attacks on KIVR-based AE schemes.

Conversion	AE	Complexity	Security	Ref.
KIVR	GCM, GCM-SIV	$\frac{r}{2}$	**CMT**-1	Theorem 2
KIVR	CCM	—	—	—
KIVR	CTR-HMAC	$\frac{r+t}{2}$	**CMT**-1	Theorem 3

The obtained **CMT**-4 security bound is $\frac{r}{2} + \mathsf{tag\text{-}col}$, where tag-col is the security against tag-collision attacks by changing any of (K, N, A).[3] In other words, KIVR's security linearly increases with r, unlike HtE upper-bounded by $\frac{k}{2}$. We ensure that KIVR causes no adverse side effects by proving that the conventional AE security after applying KIVR reduces to the multi-user (mu) security of the original AE.

Evaluation with Representative AEAD Instantiations. The term tag-col lies $0 \leq \mathsf{tag\text{-}col} \leq \frac{t}{2}$ depending on the target AE, as summarized in Table 1. We set $\mathsf{tag\text{-}col} = 0$ for GCM and GCM-SIV and obtain $\frac{r}{2}$ as a corresponding bound. This bound is tight because the attacker achieves full control over GHASH, and tag-col of GMAC is 0. Analyzing tag-col with CCM is more complicated, and we conservatively set $\mathsf{tag\text{-}col} = 0$ considering the worst case. The corresponding bound is $\frac{r}{2}$, and its tightness is unclear. In the case of CTR-HMAC, on the other hand, $\mathsf{tag\text{-}col} = \frac{t}{2}$, and the bound is $\frac{r+t}{2}$. It achieves $\mathsf{tag\text{-}col} = \frac{t}{2}$ because of the collision-resistant property of HMAC. This bound is proven tight. Table 2 summarizes the attacks. Since **CMT**-1 is weaker than **CMT**-4, a **CMT**-1-security bound can be better than a **CMT**-4-security bound. However, in the case of the KIVR-based AE schemes with GCM, GCM-SIV, and CTR-HMAC, the matching attacks break the **CMT**-1 security, and there is no room for further improving the **CMT**-1-security bounds. Meanwhile, finding an attack for KIVR with CCM remains open, and a better **CMT**-1-security bound is still possible.

[3] Specifically, the bound given in Theorem 1 is $O(\frac{\mu}{2^r})$ plus the advantage of finding μ-collisions for tags. By choosing the parameter μ so that these terms are balanced according to the structure of the tagging function, we have the security $\frac{r}{2} + \mathsf{tag\text{-}col}$.

With $r = 256$, KIVR combined with GCM, GCM-SIV, and CCM achieves 128-bit security. KIVR combined with CTR-HMAC, on the other hand, achieves $(\frac{r}{2} + 64)$-bit security with a 128-bit tag. In this case, KIVR achieves 128-bit **CMT**-4 security with $r = 128$.

Comparison with the Padding Fix. KIVR achieves higher security and supports a wider range of AEs compared with the padding fix. Specifically, KIVR enables **CMT**-4 with CTRAE, including GCM, GCM-SIV, CCM, and CTR-HMAC, in contrast with the padding fix that enables **CMT**-1 with GCM only. KIVR achieves those with a reasonable overhead and is still a one-pass scheme with a one-pass underling AE. The main overhead is processing K and N in the hash function $\mathsf{F}_{\mathsf{KIVR}}$, approximately two more blocks considering the lengths of K and N. There is no (or minor) overhead for processing AD in $\mathsf{F}_{\mathsf{KIVR}}$ because instead we can skip AD processing in the underlying AE.

1.3 Organization

We begin by giving basic definitions in Sect. 2. Then, we formally define a plaintext with redundancy and an extended CMT security considering redundancy in Sect. 3. We introduce the KIVR conversion in Sect. 4. Section 5 gives KIVR's general security bound with CTRAE, followed by the proof in Sect. 6. Section 7 discusses the security and its tightness of KIVR combined with GCM, GCM-SIV, and CCM. Similarly, Sect. 8 shows the tight security bound of KIVR with CTR-HMAC. Section 9 is a conclusion.

2 Preliminaries

Notation. For integers $0 \le i \le j$, let $[i, j] := \{i, i+1, \ldots, j\}$ and $[j] := [1, j]$. If $i > j$ then $[i, j] := \emptyset$. Let ε be an empty string, $\emptyset$ an empty set, and $\{0,1\}^*$ be the set of all bit strings. For an integer $n \ge 0$, let $\{0,1\}^n$ be the set of all n-bit strings, $\{0,1\}^0 := \{\varepsilon\}$, $\{0,1\}^{\le n} := \{X \in \{0,1\}^* \mid |X| \le n\}$, and $\{0,1\}^{n*} := \{X \in \{0,1\}^* \mid |X| \bmod n = 0\}$. Let 0^i be the bit string of i-bit zeros. For $X \in \{0,1\}^j$, let $|X| := j$. The concatenation of two bit strings X and Y is written as $X\|Y$ or XY when no confusion is possible. For integers $i \ge 0$ and $0 \le X \le 2^i - 1$, let $\mathsf{str}_i(X)$ be the i-bit representation of X. For integers $0 \le j \le i$ and $X \in \{0,1\}^i$, let $\mathsf{msb}_j(X)$ (resp. $\mathsf{lsb}_j(X)$) be the most (resp. least) significant j bits of X. For an integer $1 \le n$ and $X \in \{0,1\}^*$, let $\mathsf{zp}_n(X) := X\|0^{\lceil |X|/n \rceil \cdot n - |X|}$ be a zero-padding function such that the length of the padded value becomes a multiple of n. For a non-empty set $\mathcal{T}$, $T \xleftarrow{\$} \mathcal{T}$ means that an element is chosen uniformly at random from $\mathcal{T}$ and assigned to T. For two sets $\mathcal{T}$ and $\mathcal{T}'$, $\mathcal{T} \xleftarrow{\cup} \mathcal{T}'$ means $\mathcal{T} \leftarrow \mathcal{T} \cup \mathcal{T}'$. For an integer $l \ge 0$ and $X \in \{0,1\}^*$, $(X_1, \ldots, X_\ell) \xleftarrow{l} X$ means parsing of X into fixed-length l-bit strings, where if $X \ne \varepsilon$ then $X = X_1\| \cdots \|X_\ell$, $|X_i| = l$ for $i \in [\ell - 1]$, and $0 < |X_\ell| \le l$; if $X = \varepsilon$ then $\ell = 1$ and $X_1 = \varepsilon$.

For μ pairs with four values $\mathcal{S}[i] = \{(K'_i, N'_i, A'_i, D'_i), (K''_i, N''_i, A''_i, D''_i)\}$ $(i \in [\mu])$, Boolean function $\mathsf{diff}_{\mathsf{KNA}}$ with the input $\mathcal{S} := (\mathcal{S}[1], \ldots, \mathcal{S}[\mu])$ is defined as

- $\mathsf{diff}_{\mathsf{KNA}}(\mathcal{S}) = 1$ if $\Big(\forall i \in [\mu] : (K'_i, N'_i, A'_i) \neq (K''_i, N''_i, A''_i)\Big)$ and $\Big(\forall i \in [\mu], j \in [i-1] : \{(K'_i, N'_i, A'_i), (K''_i, N''_i, A''_i)\} \neq \{(K'_j, N'_j, A'_j), (K''_j, N''_j, A''_j)\}\Big)$;
- $\mathsf{diff}_{\mathsf{KNA}}(\mathcal{S}) = 0$ otherwise.

Block Cipher (BC). A BC is a set of permutations indexed by a key. For positive integers κ and n, let $E : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ be an encryption of a BC with k-bit keys and n-bit blocks that is used in CTR and BC-based MACs such as GMAC, GMAC^+, and CBC. Let $E^{-1} : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ be its decryption. For positive integers b and v, let $F : \{0,1\}^b \times \{0,1\}^v \to \{0,1\}^v$ be an encryption of a BC with b-bit keys and v-bit blocks that is used in Merkle-Damgård hash function.

Ideal Cipher (IC). Let $\mathcal{BC}(k,n)$ be a set of all encryptions of BCs with k-bit keys and n-bit blocks. An IC is an ideal BC and defined as $E \xleftarrow{\$} \mathcal{BC}$. An IC E can be implemented by lazy sampling. Let $\mathcal{T}_E$ be a table that is initially empty and keeps query-response tuples of E and E^{-1}. Let $\mathcal{T}_{E,2}[W] := \{Y \mid (W,X,Y) \in \mathcal{T}_E\}$ and $\mathcal{T}_{E,1}[W] := \{X \mid (W,X,Y) \in \mathcal{T}_E\}$ be tables that respectively keep ciphertext and plaintext blocks defined in $\mathcal{T}_E$ such that the key elements are W. For a new forward query (W,X) to E (resp. inverse query (W,Y) to E^{-1}), the response is defined as $Y \xleftarrow{\$} \{0,1\}^n \backslash \mathcal{T}_{E,2}[W]$ (resp. $X \xleftarrow{\$} \{0,1\}^n \backslash \mathcal{T}_{E,1}[W]$), and $\mathcal{T}_E \xleftarrow{\cup} \{(W,X,Y)\}$. For a query stored in the table $\mathcal{T}_E$, the same response is returned.

Hash Function. Let $\mathcal{M} \subseteq \{0,1\}^*$ and h be a positive integer. Let $H[\Psi] : \mathcal{M} \to \{0,1\}^h$ be a hash function with a primitive Ψ that on an input message in $\mathcal{M}$ returns an h-bit hash value. In this paper, we assume that Ψ is ideal, and use the following security notions for hash function.

μ-Collision Resistance. $H[\Psi]$ is μ-collision resistance if it is hard to find μ pairs of distinct messages such that for each pair the hash values are the same. The μ-collision-resistant advantage function of $\mathbf{A}$ with access to an ideal primitive Ψ against $H[\Psi]$ is defined as

$$\mathbf{Adv}^{\mathsf{colls}}_{H,\mu}(\mathbf{A}) := \Pr\Big[((M^{(1)}, M'^{(1)}), \ldots, (M^{(\mu)}, M'^{(\mu)})) \leftarrow \mathbf{A}^{\Psi} \text{ s.t. } \Big(\forall i \in [\mu] : H[\Psi](M^{(i)}) = H[\Psi](M'^{(i)}) \wedge M^{(i)} \neq M'^{(i)}\Big) \wedge \Big(\forall i, j \text{ s.t. } i \neq j : \{M^{(i)}, M'^{(i)}\} \neq \{M^{(j)}, M'^{(j)}\}\Big)\Big] .$$

The notion with $\mu = 1$ is the standard notion for collision resistance. Let $\mathbf{Adv}^{\mathsf{coll}}_H(\mathbf{A}) := \mathbf{Adv}^{\mathsf{colls}}_{H,1}(\mathbf{A})$ be a collision-resistant advantage function of $\mathbf{A}$.

Random Oracle (RO). An RO is an ideal hash function from $\mathcal{M}$ to $\{0,1\}^h$. An RO can be realized by lazy sampling. Let $\mathcal{T}_{\mathsf{RO}}$ be a table that is initially empty and keeps query-response pairs of RO. For a new query X to RO, the response is defined as $Y \xleftarrow{\$} \{0,1\}^h$, and the query-response pair (X,Y) is added to $\mathcal{T}_{\mathsf{RO}}$: $\mathcal{T}_{\mathsf{RO}} \xleftarrow{\cup} \{(X,Y)\}$. For a query stored in the table $\mathcal{T}_{\mathsf{RO}}$, the same response is returned.

Authenticated Encryption (AE). Let $\Pi[\Psi]$ be a (tag-based) AE scheme using a primitive (or set of primitives) Ψ. $\Pi[\Psi]$ is a pair of encryption and decryption algorithms $(\Pi_{\mathsf{Enc}}[\Psi], \Pi_{\mathsf{Dec}}[\Psi])$. $\mathcal{K}$, $\mathcal{N}$, $\mathcal{M}$, $\mathcal{C}$, $\mathcal{A}$, and $\mathcal{T}$ are the sets of keys, nonces, plaintexts, ciphertexts, associated data (AD), and tags, respectively. Let ν and t be respectively nonce and tag sizes, i.e., $\mathcal{N} = \{0,1\}^\nu$ and $\mathcal{T} = \{0,1\}^t$. The encryption algorithm $\Pi_{\mathsf{Enc}}[\Psi] : \mathcal{N} \times \mathcal{A} \times \mathcal{M} \to \mathcal{C} \times \mathcal{T}$ takes a tuple (N, A, M), and returns, deterministically, a pair (C, T). The decryption algorithm $\Pi_{\mathsf{Dec}}[\Psi] : \mathcal{N} \times \mathcal{A} \times \mathcal{C} \times \mathcal{T} \to \{\mathbf{reject}\} \cup \mathcal{M}$ takes a tuple (N, A, C, T') and returns, deterministically, either the distinguished invalid symbol $\mathbf{reject} \notin \mathcal{M}$ or a plaintext $M \in \mathcal{M}$. We require that $\forall (K,N,A,M),(K',N',A',M') \in \mathcal{K} \times \mathcal{N} \times \mathcal{A} \times \mathcal{M}$ s.t. $|M| = |M'| : |\Pi_{\mathsf{Enc}}[\Psi](K,N,A,M)| = |\Pi_{\mathsf{Enc}}[\Psi](K',N',A',M')|$. We also require that $\forall K \in \mathcal{K}, N \in \mathcal{N}, A \in \mathcal{A}, M \in \mathcal{M} : \Pi_{\mathsf{Dec}}[\Psi](K,N,A,\Pi_{\mathsf{Enc}}[\Psi](K,N,A,M)) = M$.

3 Committing Security with Plaintext Redundancy

In this section, we define notions for committing security with plaintext redundancy. The notions are defined by extending the original notions [6] such that plaintext redundancy is incorporated.

3.1 Plaintext with Redundancy

We formalize a plaintext with redundancy that extends the idea of zero padding in the padding fix [1]. A plaintext consists of redundancy R and original message M_{origin}. Let r be the length of redundancy. A plaintext with redundancy is defined as $M = \mathsf{Mix}_{\mathsf{rc}}(R \| M_{\mathsf{origin}})$ wherein $\mathsf{Mix}_{\mathsf{rc}}$ is a function for defining the positions of each bit (or byte) of redundancy in a plaintext. If $R = 0^r$ and $\mathsf{Mix}_{\mathsf{rc}}$ is an identity function, then the plaintexts are equal to those of the padding fix. The generalization covers not only the padding fix but also other padding schemes and plaintexts with inherent redundancy discussed later.

In this paper, we assume that $\mathsf{Mix}_{\mathsf{rc}}$ is length-preserving (i.e., $|R \| M_{\mathsf{origin}}| = |\mathsf{Mix}_{\mathsf{rc}}(R \| M_{\mathsf{origin}})|$), linear, invertible, and bijective. Then, redundancy in a plaintext M can be obtained by $\mathsf{msb}_r \circ \mathsf{Mix}_{\mathsf{rc}}^{-1}(M)$. We call $\mathsf{Mix}_{\mathsf{rc}}$ "(ω, n)-mixing function" if the number of n-bit blocks with redundant bits is at most ω. Specifically, let $\mathsf{Mix}_{\mathsf{rc}}(R \| M_{\mathsf{origin}}) := M_1 \| M_2 \| \cdots \| M_m$ such that $|M_i| = n$ $(i \in [m-1])$ and $|M_m| \leq n$. Then, for any original message M_{origin}, and distinct r-bit redundant values R' and R^*, there exist ω distinct indexes $i_1, \ldots, i_\omega \in [m]$ such that $(M'_{i_1}, \ldots, M'_{i_\omega}) \neq (M^*_{i_1}, \ldots, M^*_{i_\omega})$ and $\forall j \in [m] \backslash \{i_1, \ldots, i_\omega\} : M'_j = M^*_j$. For example, if $\mathsf{Mix}_{\mathsf{rc}}(R \| M_{\mathsf{origin}}) = R \| M_{\mathsf{origin}}$, then $\omega = \lceil \frac{r}{n} \rceil$.

The above definition covers a case where the original message has inherent redundancy, such as constant strings in popular file formats. For example, PNG and XML files have 64 and 192 bits of magic numbers, respectively [20,28]. Such inherent redundancy that a receiver knows in advance can be counted as a part of the redundancy R, thus reducing the number of extra redundant bits.

3.2 Definitions for Committing Security with Redundancy

For $i \in \{1,3,4\}$, let WiC_i be a function that on input tuple (K,N,A,M) of a key, a nonce, AD, and a plaintext (with redundancy), returns the first i elements to which a ciphertext is committed: $\mathsf{WiC}_1(K,N,A,M) = K$, $\mathsf{WiC}_3(K,N,A,M) = (K,N,A)$, and $\mathsf{WiC}_4(K,N,A,M) = (K,N,A,M)$.

Let $\Pi[\Psi]$ be an AE scheme with an ideal primitive(s) Ψ. In the **CMT**-i-security game where $i \in \{1,3,4\}$, the goal of an adversary $\mathbf{A}$ with access to Ψ is to return two tuples of a key, a nonce, AD, and a plaintext on which the outputs of $\Pi_{\mathsf{Enc}}[\Psi]$ are the same. Since we consider plaintexts with redundancy, the game is defined so that the plaintexts in the $\mathbf{A}$'s output tuples contain redundancy. For $i \in \{1,3,4\}$, redundancy R, and a mixing function $\mathsf{Mix}_{\mathsf{rc}}$, the **CMT**-$i$-security advantage of an adversary $\mathbf{A}$ is defined as

$$\begin{aligned}\mathbf{Adv}^{\mathsf{cmt}\text{-}i}_{\Pi,\mathsf{Mix}_{\mathsf{rc}},R}(\mathbf{A}) := \Pr\Big[&(K^\dagger,N^\dagger,A^\dagger,M^\dagger),(K^\ddagger,N^\ddagger,A^\ddagger,M^\ddagger) \leftarrow \mathbf{A}^{\Psi} \text{ s.t.} \\ &\Big(\mathsf{WiC}_i(K^\dagger,N^\dagger,A^\dagger,M^\dagger) \neq \mathsf{WiC}_i(K^\ddagger,N^\ddagger,A^\ddagger,M^\ddagger)\Big) \\ &\wedge \Big(\Pi_{\mathsf{Enc}}[\Psi](K^\dagger,N^\dagger,A^\dagger,M^\dagger) = \Pi_{\mathsf{Enc}}[\Psi](K^\ddagger,N^\ddagger,A^\ddagger,M^\ddagger)\Big) \\ &\wedge \Big(\mathsf{msb}_r \circ \mathsf{Mix}_{\mathsf{rc}}^{-1}(M^\dagger) = \mathsf{msb}_r \circ \mathsf{Mix}_{\mathsf{rc}}^{-1}(M^\ddagger) = R\Big)\Big].\end{aligned}$$

$\Pi[\Psi]$ is **CMT**-i secure if for any R, $\mathsf{Mix}_{\mathsf{rc}}$, and $\mathbf{A}$, the advantage function is upper-bounded by a negligible probability. In other words, $\Pi[\Psi]$ is not **CMT**-i secure if there exist R, $\mathsf{Mix}_{\mathsf{rc}}$, and $\mathbf{A}$ such that the **CMT**-i security of $\Pi[\Psi]$ is lower-bounded by a non-negligible probability. Note that **CMT**-3 and **CMT**-4 security are equivalent [6]. In this paper, we consider computationally unbounded adversaries.

4 KIVR Transform

In this section, we present KIVR, a generalization of HtE that enhances the committing security by using plaintext redundancy.

4.1 Specification of KIVR

KIVR, on an input tuple of a key, a nonce, and AD, generates a temporary key, a temporary nonce, and a mask value that are defined by using a hash function $\mathsf{F}_{\mathsf{KIVR}}$. The mask value is applied to redundancy in a plaintext. $\mathsf{F}_{\mathsf{KIVR}}$ should be

Algorithm 1. KIVR Transform

Encryption $\mathsf{KIVR}[\Pi_{\mathsf{Enc}}][\mathsf{Mix}_{\mathsf{rc}}, R, \Psi, \Psi_{\mathsf{KIVR}}](K, N, A, M)$
1: $(K_{\mathsf{T}}, IV_{\mathsf{T}}, R_{\mathsf{T}}) \leftarrow \mathsf{F}_{\mathsf{KIVR}}[\Psi_{\mathsf{KIVR}}](K, N, A)$
2: $(C, T) \leftarrow \Pi_{\mathsf{Enc}}[\Psi](K_{\mathsf{T}}, IV_{\mathsf{T}}, \varepsilon, M \oplus \mathsf{Mix}_{\mathsf{rc}}(R_{\mathsf{T}} \| 0^{|M|-r_{\mathsf{T}}}))$; **return** (C, T)

Decryption $\mathsf{KIVR}[\Pi_{\mathsf{Dec}}][\mathsf{Mix}_{\mathsf{rc}}, R, \Psi, \Psi_{\mathsf{KIVR}}](K, N, A, C, T')$
1: $(K_{\mathsf{T}}, IV_{\mathsf{T}}, R_{\mathsf{T}}) \leftarrow \mathsf{F}_{\mathsf{KIVR}}[\Psi_{\mathsf{KIVR}}](K, N, A)$
2: $M' \leftarrow \Pi_{\mathsf{Dec}}[\Psi](K_{\mathsf{T}}, IV_{\mathsf{T}}, \varepsilon, C, T')$ **if** $M' =$ **reject then return reject end if**
3: $M \leftarrow M' \oplus \mathsf{Mix}_{\mathsf{rc}}(R_{\mathsf{T}} \| 0^{|M|-r_{\mathsf{T}}})$
4: **if** $R = \mathsf{msb}_r \circ \mathsf{Mix}_{\mathsf{rc}}^{-1}(M)$ **then return** M **else return reject end if**

collision resistant for **CMT**-4 security and be pseudorandom-function secure for **mu-AE** security.

The specification of $\mathsf{KIVR}[\Pi]$ (KIVR with an AE scheme Π) is given in Algorithm 1 and Fig. 1. Let Ψ (resp. Ψ_{KIVR}) be the underlying primitive(s) of Π (resp. $\mathsf{F}_{\mathsf{KIVR}}$). Let R be redundancy, $r = |R|$, and $\mathsf{Mix}_{\mathsf{rc}}$ a mixing function. Let r_{T} be the length of the mask value defined by $\mathsf{F}_{\mathsf{KIVR}}$ such that $r_{\mathsf{T}} \leq r$. Let $\mathsf{F}_{\mathsf{KIVR}} : \mathcal{K} \times \mathcal{N} \times \mathcal{A} \to \mathcal{K} \times \mathcal{N} \times \{0,1\}^{r_{\mathsf{T}}}$ be a function of KIVR that on an input tuple (K, N, A) of a key, a nonce, and AD, derives a tuple $(K_{\mathsf{T}}, IV_{\mathsf{T}}, R_{\mathsf{T}})$ of a temporary key, an IV, and a mask value.[4]

4.2 Security of KIVR

Regarding the **mu-AE** security of AE schemes $\mathsf{KIVR}[\Pi]$, assuming that $\mathsf{F}_{\mathsf{KIVR}}$ is a pseudorandom function secure in the mu-setting, for each tuple of a key, a nonce, and AD, the temporary key is chosen uniformly at random from $\mathcal{K}$. Hence, the **mu-AE** security of $\mathsf{KIVR}[\Pi]$ is reduced to the **mu-AE** security of the underlying AE scheme Π. The detail is given in Supplementary material C.

Regarding committing security, in Sects. 5, 7, and 8, we show that KIVR enhances the committing security of CTR-based AE schemes by the length of redundancy r. In Sect. 5, we define CTRAE, which is a CTR-based AE scheme with a general tagging function and covers GCM, GCM-SIV, CCM, and CTR-HMAC (CTR-based AE with HMAC). We show a general bound of the **CMT**-4 security of CTRAE. In Sect. 7, we derive **CMT**-4-bounds of KIVR[GCM], KIVR[GCM-SIV], and KIVR[CCM] by using the general bound of CTRAE. In Sect. 8, we similarly derive a **CMT**-4-bound of KIVR[CTR-HMAC].

5 Committing Security of KIVR with CTR-Based AE

In this section, we first define CTRAE, a CTR-based AE scheme with a generalized tagging function. We then show a **CMT**-4-security bound of KIVR[CTRAE].

[4] We exemplify the structure of the masked plaintext $M \oplus \mathsf{Mix}_{\mathsf{rc}}(R_{\mathsf{T}} \| 0^{|M|-r_{\mathsf{T}}})$ by using the padding fix. In the padding fix, $R_{\mathsf{T}} = 0^r$ and $\mathsf{Mix}_{\mathsf{rc}}$ is an identity function. Then, the masked plaintext is $(0^r \| M_{\mathsf{origin}}) \oplus (R_{\mathsf{T}} \| 0^{|M|-r_{\mathsf{T}}}) = (R_{\mathsf{T}} \| 0^{r-r_{\mathsf{T}}}) \| M_{\mathsf{origin}}$.

Algorithm 2. Counter Mode

Encryption/Decryption $\mathsf{CTR}[E](K_{\mathsf{bc}}, IV, D)$

1: **for** $i = 1, \ldots, \lceil |D|/n \rceil$ **do** $KS_i \leftarrow E(K_{\mathsf{bc}}, \mathsf{add}(IV, i))$ **end for**
2: $KS \leftarrow \mathsf{msb}_{|D|}(KS_1 \| \cdots \| KS_{\lceil |D|/n \rceil})$; $D' \leftarrow D \oplus KS$; **return** D'

Algorithm 3. CTR-based AE CTRAE

Encryption $\mathsf{CTRAE}_{\mathsf{Enc}}[E, \Psi_{\mathsf{tag}}]((K_{\mathsf{bc}}, K_{\mathsf{tag}}), N, A, M)$

1: $T \leftarrow \mathsf{TagGen}[\Psi_{\mathsf{tag}}](K_{\mathsf{tag}}, N, A, M)$; $C \leftarrow \mathsf{CTR}[E](K_{\mathsf{bc}}, \mathsf{GetIV}(N, T), M)$
2: **return** (C, T)

Decryption $\mathsf{CTRAE}_{\mathsf{Dec}}[E, \Psi_{\mathsf{tag}}]((K_{\mathsf{bc}}, K_{\mathsf{tag}}), N, A, C, T')$

1: $M \leftarrow \mathsf{CTR}[E](K_{\mathsf{bc}}, \mathsf{GetIV}(N, T'), C)$; $T \leftarrow \mathsf{TagGen}[\Psi_{\mathsf{tag}}](K_{\mathsf{tag}}, N, A, M)$
2: **if** $T = T'$ **then return** M; **else return reject end if**

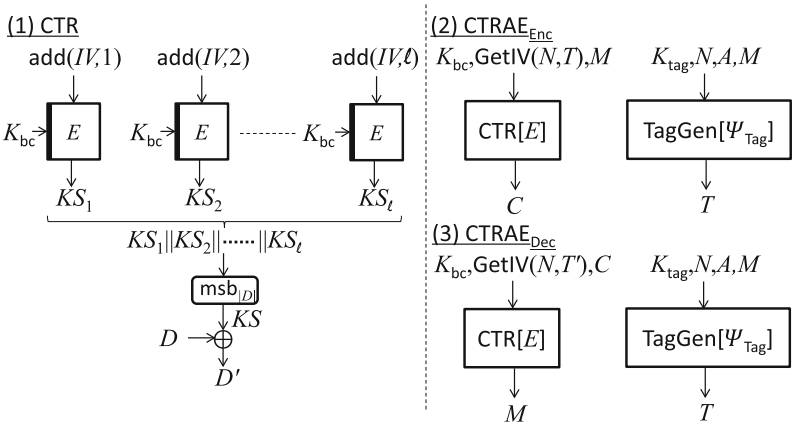

Fig. 2. (1) CTR Mode where $\ell = \lceil |D|/n \rceil$ and (D, D') is a pair of plaintext and ciphertext or of ciphertext and plaintext; (2) $\mathsf{CTRAE}_{\mathsf{Enc}}$; (3) $\mathsf{CTRAE}_{\mathsf{Dec}}$.

5.1 Specification of CTR-Based AE

Counter Mode. The specification of the counter mode CTR is given in Algorithm 2 and Fig. 2(1), where E is the underlying BC. Let c be the counter size such that $c \leq n$. Let $\mathcal{D} \subset \{0,1\}^*$ be the plaintext/ciphertext space. $\{0,1\}^k$ is the key space. $\mathsf{CTR}[E] : \{0,1\}^k \times \{0,1\}^n \times \mathcal{D} \rightarrow \mathcal{D}$ takes a tuple of a key K_{bc}, an initial value IV, and a plaintext/ciphertext D, and returns its ciphertext/plaintext D' such that $|D| = |D'|$. If D is a plaintext (resp. ciphertext), then D' is the ciphertext (resp. plaintext). KS is a key stream with which a ciphertext (resp. plaintext) is defined by XORing a plaintext (resp. ciphertext). $\mathsf{add} : \{0,1\}^n \times [0, 2^c - 1] \rightarrow \{0,1\}^n$ is a function that on an input pair of an IV and a counter, returns an input block of E. Regarding add, we consider the following two types of functions. The type-1 is used in the standard CTR (used in GCM, CCM, and CTR-HMAC) and the type-2 is used in GCM-SIV.

– The type-1 function is defined as $\mathsf{add}(IV, i) := (\mathsf{msb}_\nu(IV))\|(\mathsf{lsb}_c(IV) + i + 1 \bmod 2^c)$, where $n = \nu + c$, for the counter addition $\mathsf{lsb}_c(IV)$ is considered as an integer, and the added value is regarded as a c-bit string.
– The type-2 function is defined as $\mathsf{add}(IV, i) := (1\|(\mathsf{msb}_{n-c-1}(IV))\|(\mathsf{lsb}_c(IV) + i \bmod 2^c))$, where $\mathsf{lsb}_c(IV)$ is considered as an integer and the added value is regarded as a c-bit string.

CTRAE. We define CTRAE, a CTR-based AE scheme with primitives E and Ψ_{tag}. CTRAE is a generalization of GCM, GCM-SIV, CCM, and CTR-HMAC. The specification of $\mathsf{CTRAE}[E, \Psi_{\mathsf{tag}}]$ is given in Algorithm 3 and Fig. 2. Let $\mathcal{K}_{\mathsf{tag}}$ be the key space of the tagging function. Hence, $\mathcal{K} := \{0,1\}^k \times \mathcal{K}_{\mathsf{tag}}$ is the key space of CTRAE. Let $\mathsf{TagGen}[\Psi_{\mathsf{tag}}]$ be the tagging function with the primitive Ψ_{tag} that on an input tuple of a key K_{tag}, a nonce N, and a plaintext M, returns a t-bit tag. Note that although the tagging functions of GCM, CCM, and CTR-HMAC take a ciphertext instead of a plaintext, $\mathsf{TagGen}[\Psi_{\mathsf{tag}}]$ covers these functions by incorporating the procedure of CTR into the tagging functions. Let GetIV be a function that on an input tuple of a nonce and a tag, returns an IV of CTR. The function of GCM, CCM, and CTR-HMAC is defined as $\mathsf{GetIV}(N, T) := \mathsf{zp}_n(N)$. The function of GCM-SIV is defined as $\mathsf{GetIV}(N, T) := T$.

Let $\mathsf{KIVR}[\mathsf{CTRAE}_{\mathsf{Enc}}]$ and $\mathsf{KIVR}[\mathsf{TagGen}]$ be the encryption and tagging functions of $\mathsf{KIVR}[\mathsf{CTRAE}]$, respectively. Let $\mathsf{F}_{\mathsf{K}_{\mathsf{bc}}IVR}$ be a function that returns a tuple of a temporary key of CTR, an IV, and a mask value, i.e., $\mathsf{F}_{\mathsf{K}_{\mathsf{bc}}IVR}[\Psi_{\mathsf{KIVR}}](K, N, A) := (K_{\mathsf{bcT}}, IV_{\mathsf{T}}, R_{\mathsf{T}})$.

5.2 CMT-4-Security of KIVR[CTRAE]

Let $\Pi^* := \mathsf{KIVR}[\mathsf{CTRAE}]$, $\Pi^*_{\mathsf{Enc}} := \mathsf{KIVR}[\mathsf{CTRAE}_{\mathsf{Enc}}]$ and $\Pi^*_{\mathsf{TGen}} := \mathsf{KIVR}[\mathsf{TagGen}]$. The following theorem shows an upper-bound of the **CMT**-4-security of Π^*.

Theorem 1. *For any redundancy R, (ω, n)-mixing function $\mathsf{Mix}_{\mathsf{rc}}$, and* **CMT**-4 *adversary* $\mathbf{A}$ *making p_{ic} queries to E or E^{-1}, p_{tag} queries to Ψ_{tag}, and p_{kivr} queries to Ψ_{KIVR}, there exist adversaries $\mathbf{A}_1$ and $\mathbf{A}_2$ such that $\mathbf{Adv}^{\mathsf{cmt\text{-}4}}_{\Pi^*,\mathsf{Mix}_{\mathsf{rc}},R}(\mathbf{A}) \le \frac{2^\omega \cdot (\mu-1)}{2^r} + \mathbf{Adv}^{\mathsf{colls}}_{\Pi^*_{\mathsf{TGen}},\mu}(\mathbf{A}_1) + \mathbf{Adv}^{\mathsf{coll}}_{\mathsf{F}_{\mathsf{K}_{\mathsf{bc}}IVR}}(\mathbf{A}_2)$, for the $\mathbf{A}_1$'s output $\mathcal{S}_1$, $\mathsf{diff}_{\mathsf{KNA}}(\mathcal{S}_1) = 1$, and for each $i \in [2]$, $\mathbf{A}_i$ makes p_{ic} queries to E or E^{-1}, p_{tag} queries to Ψ_{tag}, and p_{kivr} queries to Ψ_{KIVR}.*

Note that $\mathbf{Adv}^{\mathsf{colls}}_{\Pi^*_{\mathsf{TGen}},\mu}(\mathbf{A}_1)$ is the μ-collision advantage of Π^*_{TGen} with the condition of $\mathsf{diff}_{\mathsf{KNA}}$, i.e., for each pair of $\mathbf{A}_1$, the tuples of a key, a nonce, and AD are distinct. Although the parameter r_{T} does not appear in the bound, the last term depends on the parameter. The proof is given in Sect. 6.

6 Proof of Theorem 1

Since **CMT**-3-security and **CMT**-4-security are equivalent [6], we evaluate the **CMT**-3-security advantage of $\mathbf{A}$ for Π^*.

6.1 Tools

Full-Block Query. To ensure the randomnesses of the outputs of an IC E or E^{-1}, we use the technique given in [3].

- For a key element W of an IC, after $\mathbf{A}$ makes 2^{n-1} queries with W to E or E^{-1}, we permit an adversary $\mathbf{A}$ to obtain the remaining input-output tuples of E with W, i.e., $\mathbf{A}$ obtains all input-output tuples with W. We call the additional queries "full-block queries."

The full-block queries ensure that the outputs of E or E^{-1} are chosen uniformly at random from 2^{n-1} elements in $\{0,1\}^n$.[5] Specifically, fixing Y^*, for a full-block query (W, X), the probability that the output Y is equal to Y^* is $\frac{(2^{n-1}-1)!}{(2^{n-1})!} = \frac{1}{2^{n-1}}$. Without loss of generality, full-block queries are forward ones.

Property of CTR with Redundancy. The following lemma shows that a collision of CTR with redundancy implies that the sum of the key streams meets the sum of redundancy. The lemma is used in our proofs.

Lemma 1. *Let* $\mathsf{Mix}_{\mathsf{rc}}$ *be a* (ω, n)*-mixing linear function. Let* R' *and* R'' *be* r*-bit (masked) redundancy. Let* (K', IV', M') *and* (K'', IV'', M'') *be tuples of a key, an IV, and a plaintext with redundancy such that* $(K', IV') \neq (K'', IV'')$, $|M'| = |M''|$, $\mathsf{msb}_r \circ \mathsf{Mix}_{\mathsf{rc}}^{-1}(M') = R'$*, and* $\mathsf{msb}_r \circ \mathsf{Mix}_{\mathsf{rc}}^{-1}(M'') = R''$*. For* $\square \in \{\prime, \prime\prime\}$*, let* $C^{\square} := \mathsf{CTR}[E](K^{\square}, IV^{\square}, M^{\square})$ *and* $KS^{\square}$ *the key stream. Then, we have*

$$C' = C'' \Rightarrow \mathsf{msb}_r \circ \mathsf{Mix}_{\mathsf{rc}}^{-1}(KS' \oplus KS'') = R' \oplus R''.$$

Proof (Lemma 1). The relation in the lemma is obtained as follows.

$$\begin{aligned} C' = C'' &\Rightarrow KS' \oplus KS'' = M' \oplus M'' \\ &\Rightarrow \mathsf{msb}_r \circ \mathsf{Mix}_{\mathsf{rc}}^{-1}(KS' \oplus KS'') = \mathsf{msb}_r \circ \mathsf{Mix}_{\mathsf{rc}}^{-1}(M' \oplus M'') \\ &\Rightarrow \mathsf{msb}_r \circ \mathsf{Mix}_{\mathsf{rc}}^{-1}(KS' \oplus KS'') = R' \oplus R''. \end{aligned}$$

6.2 Symbol Definitions

Let $\mathcal{I}_{\mathsf{KIVR}}$ be the set of all possible input tuples of $\mathsf{F}_{\mathsf{KIVR}}[\Psi_{\mathsf{KIVR}}]$ derived from query-response tuples of Ψ_{KIVR}. Let $\mathcal{I}_{\mathsf{TGen}}$ be the set of all possible input tuples of Π^*_{TGen} derived from query-response tuples of Ψ_{tag} and Ψ_{KIVR}. Let $(K^{\dagger}, N^{\dagger}, A^{\dagger}, M^{\dagger})$, $(K^{\ddagger}, N^{\ddagger}, A^{\ddagger}, M^{\ddagger})$ be $\mathbf{A}$'s outputs. For an input tuple $(K^{\square}, N^{\square}, A^{\square}, M^{\square})$ of a key, a nonce, AD and a plaintext with redundancy,

- $(C^{\square}, T^{\square}) := \Pi^*_{\mathsf{Enc}}[\mathsf{Mix}_{\mathsf{rc}}, R, E, \Psi_{\mathsf{tag}}, \Psi_{\mathsf{KIVR}}](K^{\square}, N^{\square}, A^{\square}, M^{\square})$,
- $(K^{\square}_{\mathsf{bcT}}, IV^{\square}_{\mathsf{T}}, R^{\square}_{\mathsf{T}}) := \mathsf{F}_{\mathsf{K_{bc}}IVR}(K^{\square}, N^{\square}, A^{\square})$, and
- $KS^{\square}$ is the key stream of $\mathsf{CTR}[E](K^{\square}_{\mathsf{T}}, IV^{\square}_{\mathsf{T}}, M^{\square})$.

In the following proof, the symbol $\square$ is replaced with $(i), \prime, \prime\prime, \dagger$, and $\ddagger$ where i is an integer.

[5] In [3], the additional queries are called super queries.

6.3 Deriving the CMT-4-Security Bound

We derive the upper-bound of $\mathbf{Adv}^{\mathsf{cmt\text{-}3}}_{\Pi^*}(\mathbf{A}) = \Pr[(C^\dagger, T^\dagger) = (C^\ddagger, T^\ddagger)]$ by using the following collision event for $\mathsf{F}_{\mathsf{K}_{\mathsf{bc}}IVR}$.

– coll: $\exists X, X' \in \mathcal{I}_{\mathsf{KIVR}}$ s.t. $X \neq X' \wedge \mathsf{F}_{\mathsf{K}_{\mathsf{bc}}IVR}(X) = \mathsf{F}_{\mathsf{K}_{\mathsf{bc}}IVR}(X')$.

Using the events, we have

$$\mathbf{Adv}^{\mathsf{cmt\text{-}3}}_{\Pi^*,\mathsf{Mix}_{\mathsf{rc}},R}(\mathbf{A}) \leq \Pr[\mathsf{coll}] + \Pr[(C^\dagger, T^\dagger) = (C^\ddagger, T^\ddagger) \wedge \neg\mathsf{coll}] \ .$$

The event coll implies that there exists an adversary $\mathbf{A}_2$ finding a collision of $\mathsf{F}_{\mathsf{K}_{\mathsf{bc}}IVR}$, i.e., $\Pr[\mathsf{coll}] \leq \mathbf{Adv}^{\mathsf{coll}}_{\mathsf{F}_{\mathsf{K}_{\mathsf{bc}}IVR}}(\mathbf{A}_2)$. The bound of $\Pr[(C^\dagger, T^\dagger) = (C^\ddagger, T^\ddagger) \wedge \neg\mathsf{coll}]$ is given in Eq. (1). These bounds provide the bound in Theorem 1.

6.4 Bounding $\Pr[(C^\dagger, T^\dagger) = (C^\ddagger, T^\ddagger) \wedge \neg\mathsf{coll}]$

We define the following event that considers μ-collisions of Π^*_{TGen} such that for each of the μ-collision, the input tuples of a key, a nonce, and AD are distinct.

$$\begin{aligned}
&\mathsf{colls} \Leftrightarrow \\
&\exists \mathcal{S} := \left\{ \left\{ (K'^{(i)}, N'^{(i)}, A'^{(i)}, C'^{(i)}), (K''^{(i)}, N''^{(i)}, A''^{(i)}, C''^{(i)}) \right\} \in (\mathcal{I}_{\mathsf{TGen}})^2 : i \in [\mu] \right\} \\
&\text{s.t.} \left(\forall i \in [\mu] : \Pi^*_{\mathsf{TGen}}(K'^{(i)}, N'^{(i)}, A'^{(i)}, C'^{(i)}) = \Pi^*_{\mathsf{TGen}}(K''^{(i)}, N''^{(i)}, A''^{(i)}, C''^{(i)}) \right) \\
&\quad \wedge (\mathsf{diff}_{\mathsf{KNA}}(\mathcal{S}) = 1).
\end{aligned}$$

Using the event, we have

$$\begin{aligned}
&\Pr[(C^\dagger, T^\dagger) = (C^\ddagger, T^\ddagger) \wedge \neg\mathsf{coll}] \\
&\leq \Pr[\mathsf{colls}] + \Pr[(C^\dagger, T^\dagger) = (C^\ddagger, T^\ddagger) \mid \neg(\mathsf{coll} \vee \mathsf{colls})].
\end{aligned}$$

These bounds are given below. Using the bounds, we have

$$\Pr[(C^\dagger, T^\dagger) = (C^\ddagger, T^\ddagger) \wedge \neg\mathsf{coll}] \leq 2^\omega \cdot \frac{\mu - 1}{2^r} + \mathbf{Adv}^{\mathsf{colls}}_{\Pi^*_{\mathsf{TGen}},\mu}(\mathbf{A}_1) \ . \tag{1}$$

Bounding $\Pr[\mathsf{colls}]$. The event colls implies that there exists an adversary $\mathbf{A}_1$ finding μ-collisions of Π^*_{TGen} with the condition of $\mathsf{diff}_{\mathsf{KNA}}$. We thus have

$$\Pr[\mathsf{colls}] \leq \mathbf{Adv}^{\mathsf{colls}}_{\Pi^*_{\mathsf{TGen}},\mu}(\mathbf{A}_1) \ .$$

Bounding $\Pr[(C^\dagger, T^\dagger) = (C^\ddagger, T^\ddagger) \mid \neg(\mathsf{coll} \vee \mathsf{colls})]$. Regarding the ciphertext collision, by Lemma 1, we have

$$\begin{aligned}
C^\dagger = C^\ddagger &\Rightarrow \mathsf{msb}_r \circ \mathsf{Mix}^{-1}_{\mathsf{rc}}\left(KS^\dagger \oplus KS^\ddagger\right) = (R \oplus \mathsf{zp}_r(R^\dagger_{\mathsf{T}})) \oplus (R \oplus \mathsf{zp}_r(R^\ddagger_{\mathsf{T}})) \\
&\Rightarrow \mathsf{msb}_r \circ \mathsf{Mix}^{-1}_{\mathsf{rc}}\left(KS^\dagger \oplus KS^\ddagger\right) = \mathsf{zp}_r(R^\dagger_{\mathsf{T}} \oplus R^\ddagger_{\mathsf{T}})
\end{aligned}$$

where $KS^\dagger$ and $KS^\ddagger$ are respectively determined from $(K^\dagger, N^\dagger, A^\dagger)$ and $(K^\ddagger, N^\ddagger, A^\ddagger)$. By $\neg\mathsf{colls}$, there are at most $\mu - 1$ pairs with a key, a nonce, and AD with which tag collision occurs. Fix distinct tuples $(K', N', A'), (K'', N'', A'') \in \mathcal{I}_{\mathsf{KIVR}}$ and assume that coll does not occur. We then consider the following two cases.

Algorithm 4. GHASH

GHASH $\mathsf{GHASH}(L, A, D)$
1: $X_1, \ldots, X_l \xleftarrow{n} \mathsf{zp}_n(A) \| \mathsf{zp}_n(D) \| \mathsf{str}_{n/2}(|A|) \| \mathsf{str}_{n/2}(|D|)$
2: $Y \leftarrow X_1 \bullet L^l \oplus X_2 \bullet L^{l-1} \oplus \cdots X_l \bullet L$; **return** Y

– If $(K'_{\mathsf{bcT}}, IV'_{\mathsf{T}}) = (K''_{\mathsf{bcT}}, IV''_{\mathsf{T}})$, then since $KS' = KS''$, we have $C^\dagger = C^\ddagger \Rightarrow R^\dagger_{\mathsf{T}} = R^\ddagger_{\mathsf{T}}$. Hence, a collision of $\mathsf{F}_{\mathsf{K}_{\mathsf{bc}} IVR}$ occurs, which contradicts the condition $\neg\mathsf{coll}$. We thus have $\Pr[C' = C''] = 0$.
– If $(K'_{\mathsf{bcT}}, IV'_{\mathsf{T}}) \neq (K''_{\mathsf{bcT}}, IV''_{\mathsf{T}})$, then in the processes of CTR, the IC's input-output tuples are defined by E or E^{-1}. Due to full-block queries, for $Z \in \{0,1\}^n$ and $j \in \{0,1\}^c$,

$$\Pr[E(K'_{\mathsf{bcT}}, \mathsf{add}(IV'_{\mathsf{T}}, j) = Z] \leq \frac{2}{2^n}, \quad \Pr[E^{-1}(K'_{\mathsf{bcT}}, Z) = \mathsf{add}(IV'_{\mathsf{T}}, j)] \leq \frac{2}{2^n},$$
$$\Pr[E(K''_{\mathsf{bcT}}, \mathsf{add}(IV''_{\mathsf{T}}, j) = Z] \leq \frac{2}{2^n}, \quad \Pr[E^{-1}(K''_{\mathsf{bcT}}, Z) = \mathsf{add}(IV''_{\mathsf{T}}, j)] \leq \frac{2}{2^n} \ .$$

As there are ω blocks that depend on redundant data, we have

$$\Pr[C' = C''] \leq 2^{\omega n - r} \cdot \left(\frac{2}{2^n}\right)^\omega = \frac{2^\omega}{2^r} \ .$$

By $\neg\mathsf{colls}$, the number of collisions of Π^*_{TGen} is at most $\mu - 1$. In order to have the collision $(C^\dagger, T^\dagger) = (C^\ddagger, T^\ddagger)$, one of the (at most) $\mu - 1$ pairs of key stream must satisfy the relation $\mathsf{msb}_r \circ \mathsf{Mix}_{\mathsf{rc}}^{-1}\left(KS^\dagger \oplus KS^\ddagger\right) = \mathsf{zp}_r(R^\dagger_{\mathsf{T}} \oplus R^\ddagger_{\mathsf{T}})$. The probability that the relation is satisfied is at most $(\mu - 1) \cdot \frac{2^\omega}{2^r}$, and we have

$$\Pr[(C^\dagger, T^\dagger) = (C^\ddagger, T^\ddagger) \mid \neg(\mathsf{coll} \vee \mathsf{colls})] \leq 2^\omega \cdot \frac{\mu - 1}{2^r} \ .$$

7 Committing Security of KIVR with GCM, GCM-SIV, and CCM

In this section, we derive the **CMT**-4-bounds of KIVR with the CTR-based AE schemes GCM, GCM-SIV, and CCM by using the bound in Theorem 1.

7.1 Specifications of GCM, GCM-SIV, and CCM

GHASH. GHASH used in GCM and GCM-SIV is a polynomial hash function defined in Algorithm 4. GHASH takes an n-bit hash key L, AD A, and a plaintext/ciphertext D, and returns an n-bit hash value Y. GHASH is the hash function used in GCM and GCM-SIV. Let $\mathbb{F}$ be a finite field of 2^n elements. We can interpret a string in $\{0,1\}^n$ as an element in $\mathbb{F}$, and the addition in $\mathbb{F}$ is the same as $\oplus$ in $\{0,1\}^n$. Let $\bullet$ be the finite-field multiplication in $\mathbb{F}$.

Algorithm 5. Tag Generation of GCM

Tag Generation $\mathsf{GMAC}[E]((K_{\mathsf{bc}}, L), N, A, C)$
1: $H \leftarrow \mathsf{GHASH}(L, A, C)$; $X \leftarrow N \| 0^{c-1}1$; $T \leftarrow \mathsf{msb}_t(H \oplus E(K_{\mathsf{bc}}, X))$; **return** T

Algorithm 6. Tag Generation GMAC^+

Tag Generation $\Pi_{\mathsf{TGen}}[E]((K_{\mathsf{bc}}, L), N, A, M)$
1: $H \leftarrow \mathsf{GHASH}(L, A, M)$; $X \leftarrow 0 \| \mathsf{lsb}_{n-1}(H) \oplus (0^c \| N)$; $T \leftarrow E(K_{\mathsf{bc}}, X)$; **return** T

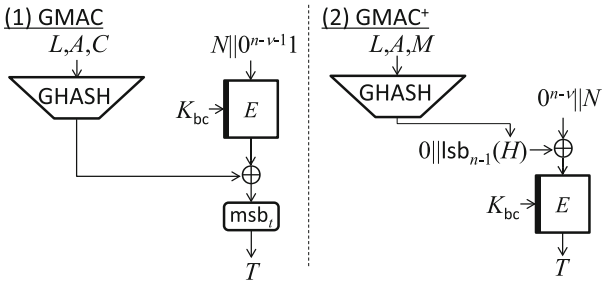

Fig. 3. Tagging functions GMAC (1) and of GMAC^+ (2).

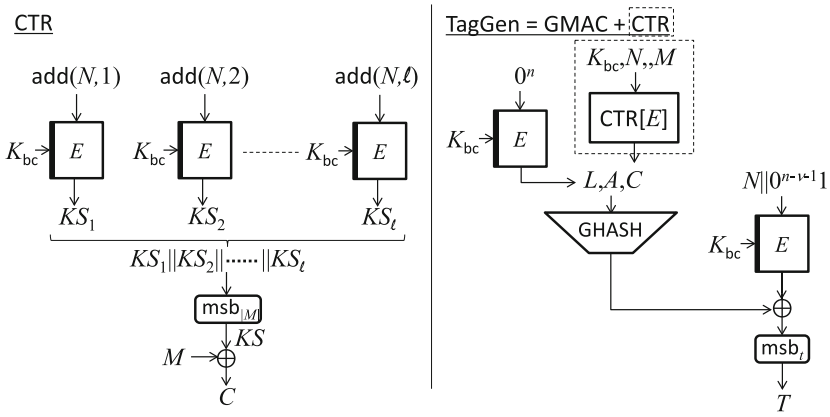

Fig. 4. Encryption of GCM. GCM is a special case of CTRAE: By introducing the redundant procedure in the dot line, GCM meets the interface of CTRAE.

GCM. GCM is a single-key CTRAE scheme with the tagging function GMAC. Hence, the key of the tag generation function is equal to that of CTR (i.e., $K_{\mathsf{tag}} = K_{\mathsf{bc}}$ and $\mathcal{K}_{\mathsf{tag}} = \{0,1\}^k$). The specification of GMAC is given in Algorithm 5 and Fig. 3(1). The hash key of GMAC is defined as $L \leftarrow E(K, 0^n)$. The encryptions of GCM and of KIVR[GCM] are respectively given in Figs. 4 and 5.

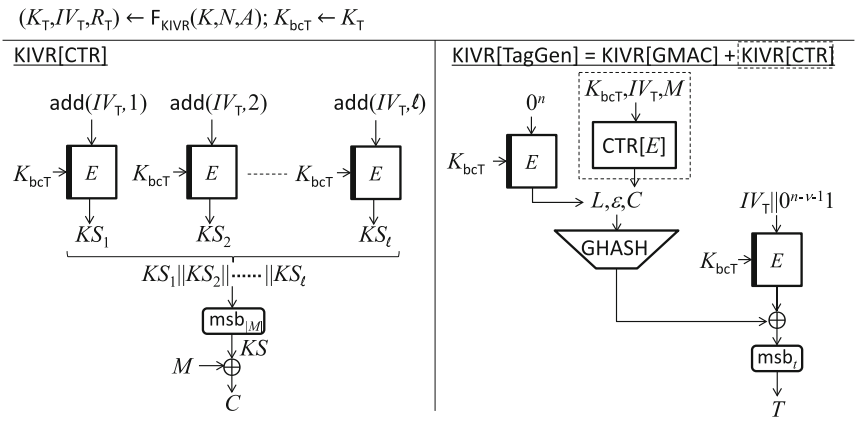

Fig. 5. Encryption of KIVR[GCM]. GCM is a special case of CTRAE: by introducing the redundant procedure in the dot line, GCM meets the interface of CTRAE.

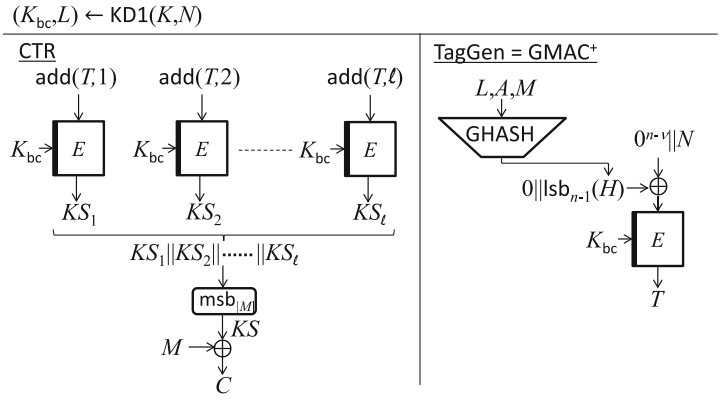

Fig. 6. Encryption of GCM-SIV.

GCM-SIV. GCM-SIV [8] is CTRAE with the tagging function GMAC$^+$ and the key derivation KD1. The specification of GMAC$^+$ is given in Algorithm 6 and Fig. 3(2). (K_{bc}, L) is a pair of (temporary) keys of GMAC$^+[E]$, where K_{bc} is equal to the key of CTR. GMAC$^+[E] : \{0,1\}^k \times \{0,1\}^n \times \mathcal{A} \times \mathcal{M} \rightarrow \{0,1\}^n$ takes an input tuple $(K_{\mathsf{bc}}, L, N, A, M)$ and returns an n-bit tag T. Note that (K_{bc}, L) is derived by using KD1. KD1 is a concatenation of truncated BCs where each BC call takes input tuple of a key, a nonce, and a counter. For the sake of simplifying the proof, when considering KIVR with GCM-SIV, KD1 is incorporated into $\mathsf{F}_{\mathsf{KIVR}}$. The encryptions of GCM-SIV and of KIVR[GCM-SIV] are respectively given in Figs. 6 and 7.

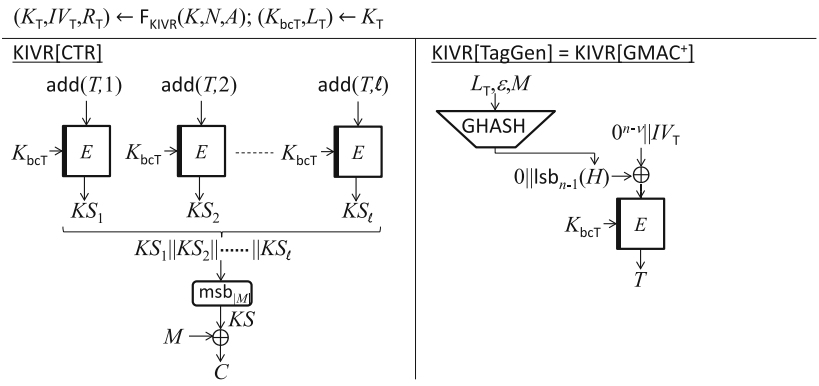

Fig. 7. Encryption of KIVR[GCM-SIV]. KD1 is incorporated into $\mathsf{F}_{\mathsf{KIVR}}$.

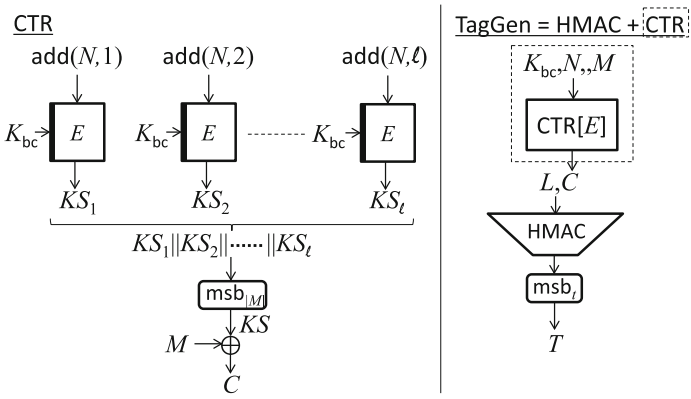

Fig. 8. Encryption of CTR-HMAC. CTR-HMAC is a special case of CTRAE: by introducing the redundant procedure in the dot line, the interface of CTR-HMAC meets the interface of CTRAE.

CCM. CCM is a single-key CTRAE with the CBC MAC as the tagging function. Hence, the key of the tagging function is equal to that of CTR (i.e., $K_{\mathsf{tag}} = K_{\mathsf{bc}}$ and $\mathcal{K}_{\mathsf{tag}} = \{0,1\}^k$). The encryption of CCM, the CBC MAC, and the encryption of KIVR[CCM] are respectively given in Figs. 10, 11, and 12.

7.2 CMT-4-Security of KIVR[GCM], KIVR[GCM-SIV], and KIVR[CCM]

We derive the **CMT**-4-security bounds of KIVR[GCM], KIVR[GCM-SIV], and KIVR[CCM] by using the bound in Theorem 1. For the sake of simplicity, we assume that $\mathsf{F}_{\mathsf{KIVR}}$ is a RO. Then, p_{kivr} is the number of queries to the RO, and we have $\mathbf{Adv}^{\mathsf{coll}}_{\mathsf{F}_{\mathsf{K_{bc}}}IVR}(\mathbf{A}_2) \leq \frac{0.5p^2_{\mathsf{kivr}}}{2^{k+\nu+r_T}}$ by the birthdaty analysis. We define the parameter as $\mu := 0.5p^2_{\mathsf{kivr}} + 1$. Then, the size of $\mathcal{S}_1$ which is $\mathbf{A}_1$'s output with

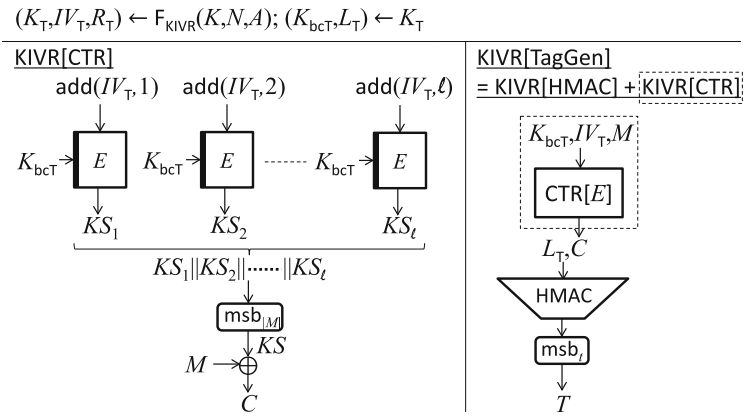

Fig. 9. Encryption of KIVR[CTR-HMAC]. CTR-HMAC is a special case of CTRAE: by introducing the redundant procedure in the dot line, the interface of CTR-HMAC meets the interface of CTRAE.

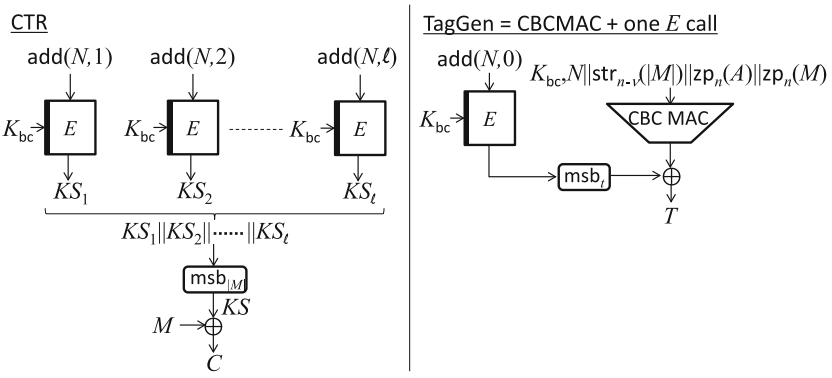

Fig. 10. Encryption of CCM.

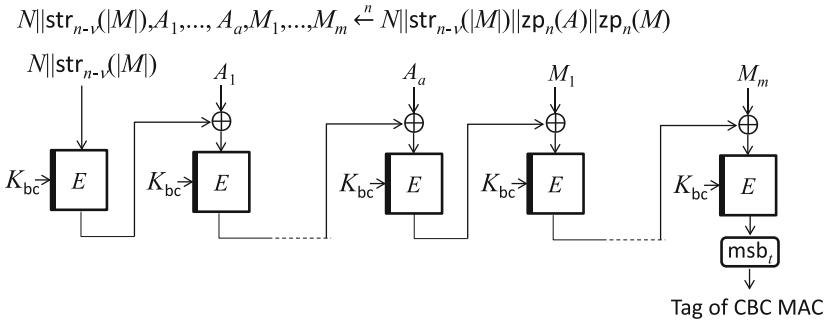

Fig. 11. CBC MAC.

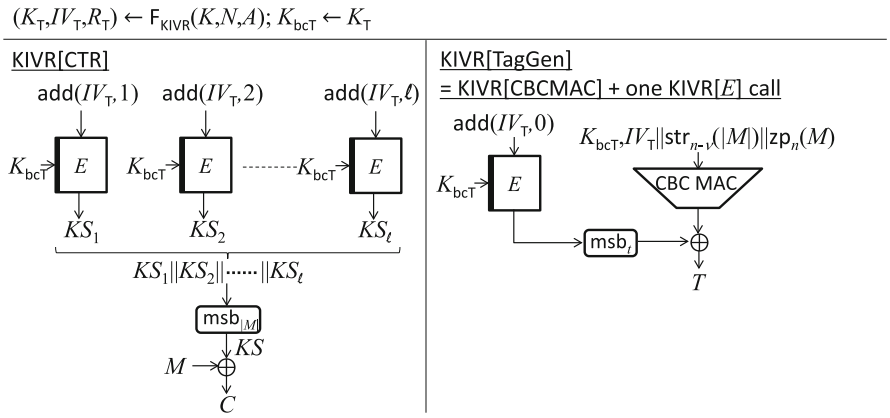

Fig. 12. Encryption of KIVR[CCM].

the condition $\mathsf{diff}_{\mathsf{KNA}}(\mathcal{S}_1) = 1$ is upper-bounded by $\binom{p_{\mathsf{kivr}}}{2} = 0.5p_{\mathsf{kivr}}(p_{\mathsf{kivr}} - 1)$, and we have $\mathbf{Adv}^{\mathsf{colls}}_{\Pi^*_{\mathsf{TGen}},\mu}(\mathbf{A}_1) = 0$. Hence, we obtain the following bounds.

Corollary 1. *Let* $\Pi^* \in \{KIVR[\mathsf{GCM}], KIVR[\mathsf{GCM\text{-}SIV}], KIVR[\mathsf{CCM}]\}$. *Assume that* F_{KIVR} *is a RO. For any redundancy* R, (ω, n)*-mixing function* $\mathsf{Mix}_{\mathsf{rc}}$, *and* **CMT**-4 *adversary* $\mathbf{A}$ *making* p_{ic} *queries to an IC, and* p_{kivr} *queries to a RO, there exists an adversary* $\mathbf{A}_2$ *such that* $\mathbf{Adv}^{\mathsf{cmt\text{-}4}}_{\Pi^*,\mathsf{Mix}_{\mathsf{rc}},R}(\mathbf{A}) \leq \frac{2^{\omega-1} \cdot p_{\mathsf{ic}}^2}{2^r} + \frac{0.5p_{\mathsf{kivr}}^2}{2^{k+\nu+r_{\mathsf{T}}}}$ *and* $\mathbf{A}_2$ *makes* p_{ic} *queries to an IC and* p_{kivr} *queries to a RO.*

We assume that the term $\frac{0.5p_{\mathsf{kivr}}^2}{2^{k+\nu+r_{\mathsf{T}}}}$ is negligible, which can be ensured by choosing the parameter r_{T} such that $r \leq \kappa + \nu + r_{\mathsf{T}}$. Then, the above bound shows that KIVR[GCM], KIVR[GCM-SIV], and KIVR[CCM] achieve $\frac{r}{2}$-bit **CMT**-4-security.

7.3 Tightness of the CMT-4-Security of KIVR[GCM] and KIVR[GCM-SIV]

We show attacks whose probabilities are the same as Corollary 1, ensuring that the tightness of the bounds of KIVR[GCM] and of KIVR[GCM-SIV] in Corollary 1. The attacks are extensions of the **CMT**-1-attack given in [1] that makes use of the linearity of GHASH.

Theorem 2. *Let* $\Pi^* \in \{KIVR[\mathsf{GCM}], KIVR[\mathsf{GCM\text{-}SIV}]\}$. *Assume that* F_{KIVR} *is a RO. There exist redundancy* R, *a* (ω, n)*-mixing function* $\mathsf{Mix}_{\mathsf{rc}}$, *and an adversary* $\mathbf{A}$ *making* p *queries to an IC or a RO such that* $\mathbf{Adv}^{\mathsf{cmt\text{-}1}}_{\Pi^*,\mathsf{Mix}_{\mathsf{rc}},R}(\mathbf{A}) = O\left(\max\left\{\frac{p^2}{2^r}, \frac{p^2}{2^{k+\nu+r_{\mathsf{T}}}}\right\}\right)$.

Proof of Theorem 2 for KIVR[GCM]. Fix redundancy $R \in \{0,1\}^r$. We consider the following mixing function: $\mathsf{Mix}_{\mathsf{rc}}(R \| M_{\mathsf{origin}}) = R \| M_{\mathsf{origin}}$ for each core data M_{origin}. We then define two adversaries $\mathbf{A}_1$ and $\mathbf{A}_2$ that offer the first and second terms, respectively.

Algorithm 7. Adversary $\mathbf{A}_1$ Breaking the **CMT**-1-Security of KIVR[GCM]

1: $p_1 \leftarrow \lceil \frac{p}{\omega+2} \rceil - 4$
2: Choose p_1 distinct keys $K^{(1)}, \ldots, K^{(p_1)} \in \{0,1\}^k$
3: Choose a pair $(N, A) \in \mathcal{N} \times \mathcal{A}$ of a nonce and AD
4: **for** $i = 1, \ldots, p_1$ **do**
5: $\quad (K_{\mathsf{T}}^{(i)}, IV_{\mathsf{T}}^{(i)}, R_{\mathsf{T}}^{(i)}) \leftarrow \mathsf{F}_{\mathsf{KIVR}}(K^{(i)}, N, A)$; $KS^{(i)} \leftarrow \varepsilon$
6: $\quad$ **for** $j = 1, \ldots, \omega + 1$ **do** $KS^{(i)} \leftarrow KS^{(i)} \| E(K_{\mathsf{T}}^{(i)}, \mathsf{add}(IV_{\mathsf{T}}^{(i)}, j))$ **end for**
7: **end for**
8: **if** $\exists \alpha, \beta \in [p_1]$ s.t.
$\quad \alpha \neq \beta \wedge \mathsf{msb}_r(KS^{(\alpha)} \oplus KS^{(\beta)}) = \mathsf{zp}_r(R_{\mathsf{T}}^{(\alpha)} \oplus R_{\mathsf{T}}^{(\beta)})$ **then**
9: $\quad Z^{(\alpha)} \leftarrow E(K_{\mathsf{T}}^{(\alpha)}, IV_{\mathsf{T}}^{(\alpha)} \| 0^{n-\nu-1}1)$; $Z^{(\beta)} \leftarrow E(K_{\mathsf{T}}^{(\beta)}, IV_{\mathsf{T}}^{(\beta)} \| 0^{n-\nu-1}1)$
10: $\quad L^{(\alpha)} \leftarrow E(K_{\mathsf{T}}^{(\alpha)}, 0^n)$; $L^{(\beta)} \leftarrow E(K_{\mathsf{T}}^{(\beta)}, 0^n)$
11: $\quad$ Find C s.t. $|C| = n(\omega+1)$, $\mathsf{msb}_r(C) = R \oplus KS^{(\alpha)} \oplus \mathsf{zp}_r(R_{\mathsf{T}}^{(\alpha)})$,
$\quad\quad$ and $\mathsf{GHASH}(L^{(\alpha)}, \varepsilon, C) \oplus \mathsf{GHASH}(L^{(\beta)}, \varepsilon, C) = Z^{(\alpha)} \oplus Z^{(\beta)}$
12: $\quad M^{(\alpha)} \leftarrow C \oplus KS^{(\alpha)} \oplus \mathsf{zp}_{|C|}(R_{\mathsf{T}}^{(\alpha)})$; $M^{(\beta)} \leftarrow C \oplus KS^{(\beta)} \oplus \mathsf{zp}_{|C|}(R_{\mathsf{T}}^{(\beta)})$
13: $\quad$ **return** $((K^{(\alpha)}, N, A, M^{(\alpha)}), (K^{(\beta)}, N, A, M^{(\beta)}))$
14: **end if**
15: **return** $((K^{(1)}, N, A, KS^{(1)}), (K^{(2)}, N, A, KS^{(2)}))$

Adversary $\mathbf{A}_1$. $\mathbf{A}_1$ breaking the **CMT**-1-security of KIVR[GCM] is defined in Algorithm 7. $\mathbf{A}_1$ returns tuples $((K^{(\alpha)}, N^{(\alpha)}, A^{(\alpha)}, M^{(\alpha)}), (K^{(\beta)}, N^{(\beta)}, A^{(\beta)}, M^{(\beta)}))$ of a key, a nonce, AD, and a plaintext with redundancy such that $(N^{(\alpha)}, A^{(\alpha)}) = (N^{(\beta)}, A^{(\beta)})$, $K^{(\alpha)} \neq K^{(\beta)}$, and $M^{(\alpha)} \neq M^{(\beta)}$. We explain the algorithm below.

- Steps 2 and 3 define p_1 tuples of a key, a nonce, and AD, where the keys are all distinct. Using the tuples, Steps 4–7 calculate key streams.
- Step 8 searches a pair (α, β) with the relation $\mathsf{msb}_r \circ \mathsf{Mix}_{\mathsf{rc}}^{-1}\left(KS^{(\alpha)} \oplus KS^{(\beta)}\right) = \mathsf{zp}_r\left(R_{\mathsf{T}}^{(\alpha)} \oplus R_{\mathsf{T}}^{(\beta)}\right)$ that is the sufficient condition to obtain a ciphertext collision from Lemma 1. For each pair (α, β), $KS^{(\alpha)}$ and $KS^{(\beta)}$ are (almost) r-bit random values, and thus the probability that the relation is satisfied is $O(\frac{1}{2^r})$. Summing the bound for each pair, we have the bound $O\left(\frac{p^2}{2^r}\right)$ of the probability that the relation is satisfied.
- If such a pair is found, then we can find the collision $(C^{(\alpha)}, T^{(\alpha)}) = (C^{(\beta)}, T^{(\alpha)})$ by using the freeness of plaintext blocks. In Step 11, by using the linearity of GHASH, a ciphertext C that yields a tag collision is found by solving the equation $\mathsf{GHASH}(L^{(\alpha)}, \varepsilon, C) \oplus \mathsf{GHASH}(L^{(\beta)}, \varepsilon, C) = Z^{(\alpha)} \oplus Z^{(\beta)}$. In Step 12, we have plaintexts $M^{(\alpha)}$ and $M^{(\beta)}$ with the redundancy R that yield the collision.

Hence, the probability that $\mathbf{A}_1$ breaks the **CMT**-1-security of KIVR[GCM] is at least $O\left(\frac{p^2}{2^r}\right)$.

Adversary $\mathbf{A}_2$. $\mathbf{A}_2$ breaks the **CMT**-1-security of KIVR[GCM] by using a collision of $\mathsf{F}_{\mathsf{K}_{\mathsf{bc}}IVR}$. If $\mathsf{F}_{\mathsf{K}_{\mathsf{bc}}IVR}(K^{(\alpha)}, N^{(\alpha)}, A^{(\alpha)}) = \mathsf{F}_{\mathsf{K}_{\mathsf{bc}}IVR}(K^{(\beta)}, N^{(\beta)}, A^{(\beta)})$ such

Algorithm 8. MD Hash Function with DM Compression Function

Hash Function $\mathsf{MD}^{\mathsf{DM}^F}(D)$

1: $D_1, \ldots, D_d \xleftarrow{b} \mathsf{sfpad}(D)$; $S \leftarrow IS$; **for** $i = 1, \ldots, d$ **do** $S \leftarrow \mathsf{DM}^F(S, D_i)$ **end for**
2: **return** S

Algorithm 9. Tag Generation HMAC

Tag Generation $\mathsf{HMAC}[\mathsf{MD}^{\mathsf{DM}^F}](L, D)$

1: $S \leftarrow \mathsf{MD}^{\mathsf{DM}^F}(\mathsf{ipad} \oplus \mathsf{ozp}_b(L) \| D)$; $T \leftarrow \mathsf{lsb}_t\left(\mathsf{MD}^{\mathsf{DM}^F}(\mathsf{opad} \oplus \mathsf{ozp}_b(L) \| S)\right)$
2: **return** T

that $K^{(\alpha)} \neq K^{(\beta)}$ and $(N^{(\alpha)}, A^{(\alpha)}) = (N^{(\beta)}, A^{(\beta)})$, then by choosing the same plaintexts $M^{(\alpha)} = M^{(\beta)}$ with the redundancy R, we obtain the output collision $(C^{(\alpha)}, T^{(\alpha)}) = (C^{(\beta)}, T^{(\beta)})$. By the birthday analysis, we have the bound of the collision probability $O\left(\frac{p^2}{2^{k+\nu+r_{\mathrm{T}}}}\right)$. □

Outline of Proof for KIVR[GCM-SIV]. The proof is the same as that of Theorem 2. The first bound is obtained by an attack that finds a pair of input to CTR such that the key streams satisfy the condition in Lemma 1 (i.e., a ciphertext collision occurs). Note that the tag collision is found with the probability 1 by using the linearity of GHASH. The second bound is obtained by an attack that makes use of a collision of $\mathsf{F}_{\mathsf{K}_{\mathsf{bc}}IVR}$. □

7.4 On the Tightness of CMT-4-Security of KIVR[CCM]

Since the CBC MAC does not have the linearity as GMAC, the attack of the adversary $\mathbf{A}_1$ in the proof of Theorem 2 does not work, and there is a possibility that the bound $\frac{2^{\omega-1} \cdot p_{\mathrm{ic}}^2}{2^r}$ is improved. Proving the tightness for the **CMT**-4-Security of KIVR[CCM] is an open problem.

8 Committing Security of KIVR with CTR-HMAC

By using the bound in Theorem 1, we derive the **CMT**-4-bound of KIVR with the CTR-based AE scheme with HMAC with the Merkle-Damgård (MD) hash function. Since SHA-2 family has the MD structure, the bound supports the widely used MAC HMAC-SHA-256.

8.1 Specification of CTR-HMAC

CTR-HMAC is CTRAE that uses HMAC as the underlying MAC. HMAC is a hash-function-based MAC and we consider the Merkle-Damgård (MD) hash function with the Davies-Meyer (DM) compression function as the underlying hash function which is employed in the SHA-2 family.

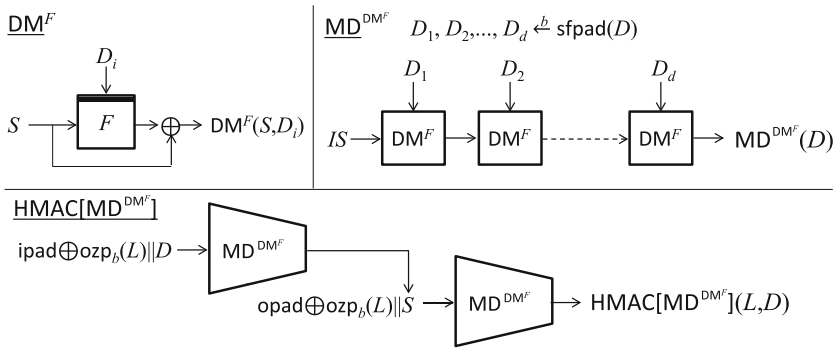

Fig. 13. DM, MD, and HMAC.

Let $F : \{0,1\}^v \times \{0,1\}^b \to \{0,1\}^v$ be the underlying primitive (or block cipher) of DM with v-bit blocks and b-bit key elements. Then, DM with F is defined as $\mathsf{DM}^F(S, D_i) = S \oplus F(S, D_i)$.

$\mathsf{MD}^{\mathsf{DM}^F}$ is a hash function that iterates DM^F. Let IS be a v-bit constant and initial value of $\mathsf{MD}^{\mathsf{DM}^F}$. Let $\mathsf{sfpad} : \{0,1\}^* \to \{0,1\}^{b*}$ be a suffix-free padding function such that for any distinct inputs D and D', $\mathsf{sfpad}(D)$ is not a prefix of $\mathsf{sfpad}(D')$.[6] MD with DM^F is defined in Algorithm 8.

Let L be the HMAC's key such that $|L| \leq b$. Let ipad and opad be distinct b-bit constants that are used to define the inner key $\mathsf{zp}_b(L) \oplus \mathsf{ipad}$ and the outer key $\mathsf{zp}_b(L) \oplus \mathsf{opad}$. HMAC processes the underlying hash function twice. The first hash call takes the inner key and the input D. The second hash call takes the outer key and the output of the first hash call. The output of the second hash call (with truncation) is a tag of HMAC. HMAC is defined in Algorithm 9.

DM, MD, and HMAC are given in Fig. 13, and the encryptions of CTR-HMAC and of KIVR[CTR-HMAC] are respectively given in Figs. 8 and 9. Note that CTR-HMAC with AES-128 and SHA-256 is a widely used AE scheme and does not support AD inputs. By using KIVR, one can convert the AE scheme so that the AD inputs are supported.

8.2 CMT-4-Security Bound of KIVR[CTR-HMAC]

Regarding the collision resistance of HMAC, Damgård [10] and Merkle [26] showed that an iterated structure of a compression function preserves its collision resistance of the underlying function. Hence, the collision resistance of HMAC is reduced to the collision resistance of $\mathsf{MD}^{\mathsf{DM}^F}$ that is further reduced to the collision resistance of DM^F. We use the collision bound in the IC model proven by Stam [27]: for any adversary $\mathbf{A}'$ making p_{tag} queries

[6] SHA-2 uses the following suffix-free padding function: for an input D, a one-zero value 10^i is appended to D, followed by the 64-bit encoding of $|D|$ so that the total length is a multiple of b and i is minimum.

to F or F^{-1}, $\mathbf{Adv}^{\mathsf{coll}}_{\mathsf{HMAC}}(\mathbf{A}') \leq \frac{p_{\mathsf{tag}}(p_{\mathsf{tag}}+1)}{2^t}$. By using Markov's inequality, $\mathbf{Adv}^{\mathsf{colls}}_{\mathsf{KIVR[HMAC]},\mu}(\mathbf{A}_1) \leq \frac{p_{\mathsf{tag}}(p_{\mathsf{tag}}+1)}{\mu 2^t}$. Then, we choose μ such that $\frac{2^\omega \cdot (\mu-1)}{2^r} \simeq \frac{p_{\mathsf{tag}}(p_{\mathsf{tag}}+1)}{\mu 2^t}$, i.e., $\mu = \frac{(p_{\mathsf{tag}}(p_{\mathsf{tag}}+1))^{1/2}}{2^{\frac{t-r+\omega}{2}}}$. Putting the bound into Theorem 1, we obtain the following corollary.

Corollary 2. *For any redundancy R, (ω, n)-mixing function $\mathsf{Mix}_{\mathsf{rc}}$, and* **CMT**-4 *adversary* $\mathbf{A}$ *making p_{ic} queries to E or E^{-1}, p_{tag} queries to F or F^{-1}, and p_{kivr} queries to Ψ_{KIVR}, there exists an adversary $\mathbf{A}_2$ such that $\mathbf{Adv}^{\mathsf{cmt\text{-}4}}_{KIVR[\mathsf{CTR\text{-}HMAC}],\mathsf{Mix}_{\mathsf{rc}},R}(\mathbf{A}) \leq \left(\frac{2^{\omega+2} \cdot p_{\mathsf{tag}}(p_{\mathsf{tag}}+1)}{2^{r+t}}\right)^{\frac{1}{2}} + \mathbf{Adv}^{\mathsf{coll}}_{\mathsf{F}_{\mathsf{K}_{\mathsf{bc}}} IVR}(\mathbf{A}_2)$ and $\mathbf{A}_2$ makes p_{ic} queries to E or E^{-1}, p_{tag} queries to F or F^{-1}, and p_{kivr} queries to Ψ_{KIVR}.*

We assume that the term $\mathbf{Adv}^{\mathsf{coll}}_{\mathsf{F}_{\mathsf{K}_{\mathsf{bc}}} IVR}(\mathbf{A}_2)$ is negligible, which can be ensured by using a secure hash function. Then, the above bound shows that KIVR[CTR-HMAC] achieves $\frac{r+t}{2}$-bit **CMT**-4-security. $2^{\omega+2}$ is a small constant.

8.3 Tightness of the CMT-4-Security of KIVR[CTR-HMAC]

We show attacks on KIVR[CTR-HMAC] whose bound matches the one in Corollary 1, thereby ensuring the tightness of the bound. In this proof, we assume that HMAC is a random oracle that is an ideal hash function.

Theorem 3. *Let $\delta_{\mathsf{coll}}(p)$ be the lower-bound of the probability that a collision of $\mathsf{F}_{\mathsf{K}_{\mathsf{bc}}} IVR$ is found with p queries to Ψ_{KIVR} such that the input keys are distinct and the other inputs are the same. Assume that* HMAC *is a random oracle* RO*. There exist redundancy R, a (ω, n)-mixing function $\mathsf{Mix}_{\mathsf{rc}}$, and an adversary breaking the* **CMT**-1*-security of Π^* making p queries to E, E^{-1},* RO*, or Ψ_{KIVR} such that $\mathbf{Adv}^{\mathsf{cmt\text{-}1}}_{KIVR[\mathsf{CTR\text{-}HMAC}],\mathsf{Mix}_{\mathsf{rc}},R}(\mathbf{A}) = O\left(\max\{\frac{p^2}{2^{r+t}}, \delta_{\mathsf{coll}}(p)\}\right)$.*

Proof (Outline). The first bound is obtained by an attack that finds two input tuples of KIVR[CTR-HMAC] such that the key streams satisfy the condition in Lemma 1 (i.e., a ciphertext collision occurs) and a collision of the tags occurs. By the birthday analysis, we obtain the first bound. The second bound is obtained by an attack that makes use of a collision of $\mathsf{F}_{\mathsf{K}_{\mathsf{bc}}} IVR$. The formal proof is given in Appendix E. □

9 Conclusion

We propose the KIVR conversion for enabling the BBB and CMT-4 security by exploiting redundancy. KIVR uses a collision-resistant hash function to convert a tuple of a key, a nonce, and associated data into a temporary key, an initial value (or nonce), and a masking value applied to redundant data used by an underlying AE. We give a general bound for the **CMT**-4 security of KIVR with CTRAE, CTR combined with any MAC, covering a large class of practical AEs.

The bound is $\frac{r}{2} + \mathsf{tag\text{-}col}$ bits wherein r is the number of redundant bits and $\mathsf{tag\text{-}col}$ is the tag-collision security of the underlying AE. We set $\mathsf{tag\text{-}col} = 0$ for GCM, GCM-SIV, and CCM, and the corresponding bound becomes $\frac{r}{2}$, which is tight for GCM and GCM-SIV. Meanwhile, KIVR with CTR-HMAC achieves a better tight bound, $\frac{r+t}{2}$ bits, with a t-bit tag. There are interesting open research questions. In particular, analyzing/salvaging the other popular AEs, including ChaCha20-Poly1305 [23], for committing security is open for future research.

Acknowledgement. We thank Dong Hoon Chang, an associate of National Institute of Standards and Technology, for helpful comments on the formalization of the redundant plaintext. We also thank anonymous reviewers for constructive feedback.

A Multi-user Security for AE

Multi-user-AE (**mu-AE**) security is the indistinguishability between the real and ideal worlds. Let $\Pi = (\Pi_{\mathsf{Enc}}, \Pi_{\mathsf{Dec}})$ be an AE scheme that has encryption and decryption algorithms. Let u be the number of users. In the **mu-AE**-security game, an adversary $\mathbf{A}$ has access to either real-world oracles $(\Pi_{K_1}, \ldots, \Pi_{K_u})$ or ideal-world ones $((\$_1, \perp), \ldots, (\$_u, \perp))$. $K_1, \ldots, K_u$ are user's keys defined as $K_i \xleftarrow{\$} \mathcal{K}$ where $i \in [u]$. $\$_\xi$ is a random-bit oracle of the ξ-th user that takes an input tuple (N, A, M) of nonce, AD, and plaintext, and returns a pair of random ciphertext and tag defined as $(C, T) \xleftarrow{\$} \{0,1\}^{|\Pi_{\mathsf{Enc}}[E](K,N,A,M)|}$. $\perp$ is a reject oracle that returns **reject** for each query. At the end of this game, $\mathbf{A}$ return a decision bit in $\{0,1\}$. If the underlying primitive is ideal, then $\mathbf{A}$ has access to the ideal primitive. Let $\mathbf{A}^{\mathcal{O}} \in \{0,1\}$ be an output of $\mathbf{A}$ with access to a set of oracles $\mathcal{O}$. Then, the **mu-AE**-security advantage function of $\mathbf{A}$ is defined as $\mathbf{Adv}^{\mathbf{mu\text{-}ae}}_{\Pi}(\mathbf{A}) := \Pr\left[\mathbf{A}^{\Pi_{K_1},\ldots,\Pi_{K_u}} = 1\right] - \Pr\left[\mathbf{A}^{(\$_1,\perp),\ldots,(\$_u,\perp)} = 1\right]$. We consider nonce-respecting adversaries where for each user, all nonces in queries to the encryption oracle are distinct. In this game, making a trivial query (ξ, N, A, C, T') to the decryption oracle is forbidden, which was received by some previous query to the encryption one.

B Multi-user PRF Security

The **mu-AE** security of KIVR-based schemes relies on multi-user pseudo-random-function (mu-PRF) security. Let $\mathsf{F}_K : \mathcal{M} \to \{0,1\}^s$ be a keyed function with a key $K \in \mathcal{K}_{\mathsf{F}}$ where $\mathcal{M} \subseteq \{0,1\}^*$ is the input space, s is the output length, and $\mathcal{K}_{\mathsf{F}}$ is the key space. Let u be the number of users. Let Func be the set of all functions from $\mathcal{M}$ to $\{0,1\}^s$. In the mu-PRF-security game, an adversary $\mathbf{A}$ has access to either real-world oracles $(\mathsf{F}_{K_1}, \ldots, \mathsf{F}_{K_u})$ or ideal-world ones $(\mathcal{R}_1, \ldots, \mathcal{R}_u)$, where K_i is the i-th user's key defined as $K_i \xleftarrow{\$} \{0,1\}^{\mathcal{K}}$ and $\mathcal{R}_i$ is a random function of the i-th user defined as $\mathcal{R}_i \xleftarrow{\$} \mathsf{Func}$. At the end of this game, $\mathbf{A}$ return a decision bit. Let $\mathbf{A}^{\mathcal{O}_1,\ldots,\mathcal{O}_u}$ be an output of $\mathbf{A}$ with access to oracles $(\mathcal{O}_1, \ldots, \mathcal{O}_u)$. Then, the mu-PRF-security advantage function of $\mathbf{A}$ is defined as $\mathbf{Adv}^{\mathsf{mu\text{-}prf}}_{\mathsf{F}}(\mathbf{A}) := \Pr\left[\mathbf{A}^{\mathsf{F}_{K_1},\ldots,\mathsf{F}_{K_u}} = 1\right] - \Pr\left[\mathbf{A}^{\mathcal{R}_1,\ldots,\mathcal{R}_u} = 1\right]$.

C mu-AE Security of AE Schemes with KIVR

The following theorem shows that the **mu-AE** security of an AE scheme Π with KIVR is reduced to the **mu-AE**-security of the underlying AE scheme Π and the mu-PRF security of $\mathsf{F}_{\mathsf{KIVR}}$. Note that in the theorem, $\mathsf{F}_{\mathsf{KIVR}}$ is a keyed function.

Theorem 4. *Let Π be an AE scheme. Let R be redundancy and $\mathsf{Mix}_{\mathsf{rc}}$ a (ω, n)-mixing function. For any* **mu-AE** *adversary* $\mathbf{A}$ *against KIVR$[\Pi]$ making at most q queries and running in time T, there exists an* **mu-AE** *adversary $\mathbf{A}_1$ against Π and a* mu-PRF *adversary $\mathbf{A}_2$ against $\mathsf{F}_{\mathsf{KIVR}}$ such that $\mathbf{Adv}^{\mathbf{mu\text{-}ae}}_{\mathsf{KIVR}[\Pi]}(\mathbf{A}) \leq \mathbf{Adv}^{\mathbf{mu\text{-}ae}}_{\Pi}(\mathbf{A}_1) + \mathbf{Adv}^{\mathsf{mu\text{-}prf}}_{\mathsf{F}_{\mathsf{KIVR}}}(\mathbf{A}_2)$, where $\mathbf{A}$ makes at most q construction queries and runs in time T, and $\mathbf{A}_1$ and $\mathbf{A}_2$ respectively make at most q construction queries and runs in time $T + O(q)$.*

Proof. Firstly, the keyed functions $\mathsf{F}_{\mathsf{KIVR}}(K_1, \cdot, \cdot), \ldots, \mathsf{F}_{\mathsf{KIVR}}(K_u, \cdot, \cdot)$ are replaced with random functions $\mathcal{R}_1, \ldots, \mathcal{R}_u$. Then, the mu-PRF-advantage function of $\mathbf{A}_2$ is introduced in the **mu-AE**-security bound.

We next consider the **mu-AE**-security of KIVR$[\Pi]$ where $\mathsf{F}_{\mathsf{KIVR}}$ is a random function $\mathcal{R}_i$. By random functions, for each of tuples of a key, nonce, and AD, the temporary key is chosen uniformly at random from $\mathcal{K}$, the **mu-AE**-security of KIVR$[\Pi]$ is reduced to the **mu-AE**-security of Π, i.e., for any adversary breaking the **mu-AE**-security of KIVR$[\Pi]$, there exists an adversary $\mathbf{A}_1$ breaking the **mu-AE**-security of Π.

Hence, we have $\mathbf{Adv}^{\mathbf{mu\text{-}ae}}_{\mathsf{KIVR}[\Pi]}(\mathbf{A}) \leq \mathbf{Adv}^{\mathbf{mu\text{-}ae}}_{\Pi}(\mathbf{A}_1) + \mathbf{Adv}^{\mathsf{mu\text{-}prf}}_{\mathsf{F}_{\mathsf{KIVR}}}(\mathbf{A}_2)$. □

D Proof of Theorem 2 for KIVR[GCM-SIV]

Fix redundancy $R \in \{0,1\}^r$. We consider the mixing function: $\mathsf{Mix}_{\mathsf{rc}}(R \| M_{\mathsf{origin}}) = R \| M_{\mathsf{origin}}$ for each core data M_{origin}. We then define two adversaries $\mathbf{A}_1$ and $\mathbf{A}_2$ that offer the terms $\frac{p^2}{2^r}$ and $\frac{p^2}{2^{k+\nu+r_{\mathsf{T}}}}$, respectively.

Adversary $\mathbf{A}_1$. $\mathbf{A}_1$ breaking the **CMT**-1-security of KIVR[GCM-SIV] is given in Algorithm 10. $\mathbf{A}_1$ returns a pair $((K^{(\alpha)}, N, A, M^{(\alpha)}), (K^{(\beta)}, N, A, M^{(\beta)}))$ such that $K^{(\alpha)} \neq K^{(\beta)}$. We explain the algorithm below.

- Steps 2 and 3 define p_1 tuples of a key, a nonce, and AD, where the keys are all distinct. In Steps 4-7, $\mathbf{A}$ calculates key streams for the input tuples.
- Step 8 searches a pair (α, β) with the following conditions: $\mathsf{msb}_1(X^{(\alpha)}) = \mathsf{msb}_1(X^{(\beta)}) = 0$ and $\mathsf{msb}_r\left(KS^{(\alpha)} \oplus KS^{(\beta)}\right) = \mathsf{zp}_r(R^{(\alpha)}_{\mathsf{T}} \oplus R^{(\beta)}_{\mathsf{T}})$. The second condition is a sufficient one to obtain a ciphertext collision due to Lemma 1. For each pair (α, β), $KS^{(\alpha)}$ and $KS^{(\beta)}$ are (almost) r-bit random values, and thus the probability that the relation is satisfied is $O(\frac{1}{2^r})$. Summing the bound for each pair, we have the bound $O\left(\frac{p^2}{2^r}\right)$ of the probability that the relation is satisfied.

Algorithm 10. Adversary $\mathbf{A}$ Breaking the **CMT**-1-Security of KIVR[GCM-SIV]

1: $\omega \leftarrow \lceil \frac{r}{n} \rceil$; $p_1 \leftarrow \lceil \frac{p}{\omega+4} \rceil$
2: Choose p_1 distinct keys $K^{(1)}, \ldots, K^{(p_1)} \in \mathcal{K}$
3: Choose a pair $(N, A) \in \mathcal{N} \times \mathcal{A}$ of nonce and AD and a tag $T \in \{0,1\}^n$
4: **for** $i = 1, \ldots, p_1$ **do**
5: $\quad((K^{(i)}_{\mathsf{bcT}}, L^{(i)}_{\mathsf{T}}), IV^{(i)}_{\mathsf{T}}, R^{(i)}_{\mathsf{T}}) \leftarrow \mathsf{F}_{\mathsf{KIVR}}(K^{(i)}, N, A)$; $X^{(i)} \leftarrow E^{-1}(K^{(i)}_{\mathsf{bcT}}, T)$
6: $\quad$**for** $j = 1, \ldots, \omega+2$ **do** $KS^{(i)} \leftarrow KS^{(i)} \| E(K^{(i)}_{\mathsf{bcT}}, \mathsf{add}(T, j))$ **end for**
7: **end for**
8: **if** $\exists \alpha, \beta \in [p_1]$ s.t. $\alpha \neq \beta \wedge \mathsf{msb}_1(X^{(\alpha)}) = \mathsf{msb}_1(X^{(\beta)}) = 0 \wedge$
$\qquad\qquad \mathsf{msb}_r\left(KS^{(\alpha)} \oplus KS^{(\beta)}\right) = \mathsf{zp}_r(R^{(\alpha)}_{\mathsf{T}} \oplus R^{(\beta)}_{\mathsf{T}})$ **then**
9: $\quad H^{(\alpha)} \leftarrow X^{(\alpha)} \oplus 0^{n-\nu} \| IV^{(\alpha)}_{\mathsf{T}}$; $H^{(\beta)} \leftarrow X^{(\beta)} \oplus 0^{n-\nu} \| IV^{(\beta)}_{\mathsf{T}}$
10: $\quad$Find $\omega+2$ block plaintexts $M^{(\alpha)}, M^{(\beta)}$ s.t.
$\qquad \mathsf{msb}_r(M^{(\alpha)}) = \mathsf{msb}_r(M^{(\beta)}) = R$,
$\qquad C^{(\alpha)} = C^{(\beta)}$,
$\qquad \mathsf{lsb}_{n-1}(\mathsf{GHASH}(L^{(\alpha)}_{\mathsf{T}}, \varepsilon, M^{(\alpha)})) = \mathsf{lsb}_{n-1}(H^{(\alpha)})$, and
$\qquad \mathsf{lsb}_{n-1}(\mathsf{GHASH}(L^{(\beta)}_{\mathsf{T}}, \varepsilon, M^{(\beta)})) = \mathsf{lsb}_{n-1}(H^{(\beta)})$
11: $\quad$**return** $((K^{(\alpha)}, N, A, M^{(\alpha)}), (K^{(\beta)}, N, A, M^{(\beta)}))$
12: **end if**
13: **return** $((K^{(1)}, N, A, 0), (K^{(2)}, N, A, 0))$

– If such pair is found, then $\mathbf{A}$ can find a pair $((K^{(\alpha)}, N, A, M^{(\alpha)}), (K^{(\beta)}, N, A, M^{(\beta)}))$ such that $(C^{(\alpha)}, T^{(\alpha)}) = (C^{(\beta)}, T^{(\beta)})$ by solving the equations: $\mathsf{msb}_r(M^{(\alpha)}) = \mathsf{msb}_r(M^{(\beta)}) = R$, $C^{(\alpha)} = C^{(\beta)}$ ($\Leftrightarrow M^{(\alpha)} \oplus M^{(\beta)} = KS^{(\alpha)} \oplus KS^{(\beta)}$), $\mathsf{GHASH}(L^{(\alpha)}, \varepsilon, M^{(\alpha)}) = H^{(\alpha)}$, and $\mathsf{GHASH}(L^{(\beta)}, \varepsilon, M^{(\beta)}) = H^{(\beta)}$. Since Step 8 ensures that the ciphertext collision occurs, this step searches the pair that yields the tag collision. In the equations, there are $2(\omega+2)$ plaintext blocks and there are $\omega+4$ equations for the blocks. Fixing the 2ω message blocks with redundancy such that $\mathsf{msb}_{\omega n}(C^{(\alpha)}) = \mathsf{msb}_{\omega n}(C^{(\beta)})$, the remaining 4 message blocks are uniquely determined from the equations $\mathsf{lsb}_{2n}(C^{(\alpha)}) = \mathsf{lsb}_{2n}(C^{(\beta)})$, $\mathsf{lsb}_{n-1}(\mathsf{GHASH}(L^{(\alpha)}_{\mathsf{T}}, A^{(\alpha)}, M^{(\alpha)})) = \mathsf{lsb}_{n-1}(H^{(\alpha)})$, and $\mathsf{lsb}_{n-1}(\mathsf{GHASH}(L^{(\beta)}_{\mathsf{T}}, A^{(\beta)}, M^{(\beta)})) = \mathsf{lsb}_{n-1}(H^{(\beta)})$. Then, we have a pair with the output collision.

Hence, the probability that $\mathbf{A}$ win the **CMT**-1 game is $O\left(\frac{p^2}{2^r}\right)$.

Adversary $\mathbf{A}_2$. The second adversary $\mathbf{A}_2$ that breaks the **CMT**-1-security of KIVR[GCM-SIV] by using a collision of $\mathsf{F}_{\mathsf{K}_{\mathsf{bc}}IVR}$. If $\mathsf{F}_{\mathsf{K}_{\mathsf{bc}}IVR}(K^{(\alpha)}, N^{(\alpha)}, A^{(\alpha)}) = \mathsf{F}_{\mathsf{K}_{\mathsf{bc}}IVR}(K^{(\beta)}, N^{(\beta)}, A^{(\beta)})$ such that $K^{(\alpha)} \neq K^{(\beta)}$ and $(N^{(\alpha)}, A^{(\alpha)}) = (N^{(\beta)}, A^{(\beta)})$, then by choosing the same plaintexts $M^{(\alpha)}$ and $M^{(\beta)}$ such that $\mathsf{msb}_r(M^{(\alpha)}) = \mathsf{msb}_r(M^{(\beta)}) = R$ and the tag collision occurs, we obtain the output collision $(C^{(\alpha)}, T^{(\alpha)}) = (C^{(\beta)}, T^{(\beta)})$. The collision probability is $O\left(\frac{p^2}{2^{k+\nu+r_{\mathsf{T}}}}\right)$. Note that the plaintexts with the tag collision can be found by the same procedure as $\mathbf{A}_1$ that finds ciphertexts with the tag collision by making use of the linearity of GHASH. □

Algorithm 11. Adversary $\mathbf{A}_1$ Breaking the **CMT**-1-Security of KIVR[CTR-HMAC]

1: $p_1 \leftarrow 0.5\lceil \frac{p}{\omega+1} \rceil$
2: Choose p_1 distinct keys $K^{(1)}, \ldots, K^{(p_1)} \in \{0,1\}^k$
3: Choose a pair $(N, A) \in \mathcal{N} \times \mathcal{A}$ of a nonce and AD
4: **for** $i = 1, \ldots, p_1$ **do**
5: $\quad (K_{\mathsf{T}}^{(i)}, IV_{\mathsf{T}}^{(i)}, R_{\mathsf{T}}^{(i)}) \leftarrow \mathsf{F}_{\mathsf{KIVR}}(K^{(i)}, N, A)$; $KS^{(i)} \leftarrow \varepsilon$
6: $\quad$ **for** $j = 1, \ldots, \omega + 1$ **do** $KS^{(i)} \leftarrow KS^{(i)} \| E(K_{\mathsf{T}}^{(i)}, \mathsf{add}(IV_{\mathsf{T}}^{(i)}, j))$ **end for**
7: **end for**
8: **for** each $(\alpha, \beta) \in [p_1]^2$ s.t. $\alpha \neq \beta \wedge \mathsf{msb}_r(KS^{(\alpha)} \oplus KS^{(\beta)}) = \mathsf{zp}_r(R_{\mathsf{T}}^{(\alpha)} \oplus R_{\mathsf{T}}^{(\beta)})$ **do**
9: $\quad M^{(\alpha)} \leftarrow R \| \mathsf{lsb}_{(\omega+1)n-r}(KS^{(\alpha)} \oplus \mathsf{zp}_{(\omega+1)n}(R_{\mathsf{T}}^{(\alpha)}))$
10: $\quad M^{(\beta)} \leftarrow R \| \mathsf{lsb}_{(\omega+1)n-r}(KS^{(\beta)} \oplus \mathsf{zp}_{(\omega+1)n}(R_{\mathsf{T}}^{(\beta)}))$
11: $\quad C \leftarrow M^{(\alpha)} \oplus (KS^{(\alpha)} \oplus \mathsf{zp}_{(\omega+1)n}(R_{\mathsf{T}}^{(\alpha)}))$
12: $\quad T^{(\alpha)} \leftarrow \mathsf{RO}(K_{\mathsf{tagT}}^{(\alpha)}, IV_{\mathsf{T}}^{(\alpha)}, C)$; $T^{\beta} \leftarrow \mathsf{RO}(K_{\mathsf{tagT}}^{(\beta)}, IV_{\mathsf{T}}^{(\beta)}, C)$
13: $\quad$ **if** $T^{\alpha} = T^{\beta}$ **then return** $((K^{(\alpha)}, N, A, M^{(\alpha)}), (K^{(\beta)}, N, A, M^{(\beta)}))$ **end if**
14: **end for**
15: **return** $((K^{(1)}, N, A, KS^{(1)}), (K^{(2)}, N, A, KS^{(2)}))$

E Proof of Theorem 3

In this proof, we assume that HMAC is a random oracle RO which is an ideal hash function. Let $R \in \{0,1\}^r$ be redundancy. We consider the following mixing function: $\mathsf{Mix}_{\mathsf{rc}}(R \| M_{\mathsf{origin}}) = R \| M_{\mathsf{origin}}$ for each core data M_{origin}. We then define two adversaries $\mathbf{A}_1$ and $\mathbf{A}_2$ that offer the terms $\frac{p^2}{2^{r+t}}$ and $\delta_{\mathsf{coll}}(p)$, respectively.

Adversary $\mathbf{A}_1$. The adversary $\mathbf{A}_1$ breaking the **CMT**-1-security of KIVR[CTR-HMAC] is defined in Algorithm 11. The adversary returns a pair $((K^{(\alpha)}, N^{(\alpha)}, A^{(\alpha)}, M^{(\alpha)}) (K^{(\beta)}, N^{(\beta)}, A^{(\beta)}, M^{(\beta)}))$ such that $(N^{(\alpha)}, A^{(\alpha)}) = (N^{(\beta)}, A^{(\beta)})$, $K^{(\alpha)} \neq K^{(\beta)}$, and $M^{(\alpha)} \neq M^{(\beta)}$. We explain the algorithm below.

- Steps 2 and 3 define p_1 tuples of a key, a nonce, and AD, where the keys are all distinct. Steps 4-7 calculates the key streams of these input tuples.
- Step 8 searches a pair (α, β) with the following relations: $\mathsf{msb}_1(X^{(\alpha)}) = \mathsf{msb}_1(X^{(\beta)}) = 0$ and $\mathsf{msb}_r\left(KS^{(\alpha)} \oplus KS^{(\beta)}\right) = \mathsf{zp}_r(R_{\mathsf{T}}^{(\alpha)} \oplus R_{\mathsf{T}}^{(\beta)})$, which is the sufficient condition to obtain a ciphertext collision from Lemma 1. For each pair (α, β), $KS^{(\alpha)}$ and $KS^{(\beta)}$ are (almost) r-bit random values, and thus the probability that the relation is satisfied is $O(\frac{1}{2^r})$.
- For such pair, Steps 10 and 11 calculate a pair of plaintexts $(M^{(\alpha)}, M^{(\beta)})$ that yield the same ciphertext C, and Step 12 calculates the tags. Step 13 checks the equality of the tags. If the tag collision occurs, $\mathbf{A}_1$ breaks the **CMT**-1-security of CTR-HMAC. The probability that the tag collision occurs is at most $\frac{1}{2^t}$.

– Summing the bound $\frac{1}{2^r} \cdot \frac{1}{2^t}$ for each pair (α, β), we have the bound $O\left(\frac{p^2}{2^{r+t}}\right)$.

Hence, the probability that $\mathbf{A}_1$ breaks the **CMT**-1-security of KIVR[GCM] is at least $O\left(\frac{p^2}{2^{r+t}}\right)$.

Adversary $\mathbf{A}_2$. The second adversary $\mathbf{A}_2$ that breaks the **CMT**-1-security of KIVR[CTR-HMAC] by using a collision of $\mathsf{F}_{\mathsf{KIVR}}$. If the collision is found: $\mathsf{F}_{\mathsf{KIVR}}(K^{(\alpha)}, N^{(\alpha)}, A^{(\alpha)}) = \mathsf{F}_{\mathsf{KIVR}}(K^{(\beta)}, N^{(\beta)}, A^{(\beta)})$ such that $K^{(\alpha)} \neq K^{(\beta)}$ and $(N^{(\alpha)}, A^{(\alpha)}) = (N^{(\beta)}, A^{(\beta)})$, then by choosing the same plaintexts $M^{(\alpha)} = M^{(\beta)}$, we obtain the output collision $(C^{(\alpha)}, T^{(\alpha)}) = (C^{(\beta)}, T^{(\beta)})$. The collision probability is $\delta_{\mathsf{coll}}(p)$. □

References

1. Albertini, A., Duong, T., Gueron, S., Kölbl, S., Luykx, A., Schmieg, S.: How to abuse and fix authenticated encryption without key commitment. In: USENIX Security 2022, pp. 3291–3308 (2022)
2. Andreeva, E., Bogdanov, A., Luykx, A., Mennink, B., Mouha, N., Yasuda, K.: How to securely release unverified plaintext in authenticated encryption. In: Sarkar, P., Iwata, T. (eds.) ASIACRYPT 2014. LNCS, vol. 8873, pp. 105–125. Springer, Heidelberg (2014). https://doi.org/10.1007/978-3-662-45611-8_6
3. Armknecht, F., Fleischmann, E., Krause, M., Lee, J., Stam, M., Steinberger, J.: The preimage security of double-block-length compression functions. In: Lee, D.H., Wang, X. (eds.) ASIACRYPT 2011. LNCS, vol. 7073, pp. 233–251. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-25385-0_13
4. Barbosa, M., Farshim, P.: Indifferentiable authenticated encryption. In: Shacham, H., Boldyreva, A. (eds.) CRYPTO 2018. LNCS, vol. 10991, pp. 187–220. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-96884-1_7
5. Bellare, M., et al.: Ask your cryptographer if context-committing AEAD is right for you. In: Real World Crypto Symposium (RWC), vol. 2023 (2023)
6. Bellare, M., Hoang, V.T.: Efficient schemes for committing authenticated encryption. In: EUROCRYPT 2022, vol. 13276, pp. 845–875 (2022). https://doi.org/10.1007/978-3-031-07085-3_29
7. Bellare, M., Hoang, V.T., Wu, C.: The landscape of committing authenticated encryption. https://csrc.nist.gov/Presentations/2023/landscape-of-committing-authenticated-encryption (2023), the Third NIST Workshop on Block Cipher Modes of Operation
8. Bose, P., Hoang, V.T., Tessaro, S.: Revisiting AES-GCM-SIV: multi-user security, faster key derivation, and better bounds. In: Nielsen, J.B., Rijmen, V. (eds.) EUROCRYPT 2018. LNCS, vol. 10820, pp. 468–499. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-78381-9_18
9. Chan, J., Rogaway, P.: On committing authenticated-encryption. In: ESORICS 2022, vol. 13555, pp. 275–294 (2022)
10. Damgård, I.B.: A design principle for hash functions. In: Brassard, G. (ed.) CRYPTO 1989. LNCS, vol. 435, pp. 416–427. Springer, New York (1990). https://doi.org/10.1007/0-387-34805-0_39
11. Dodis, Y., Grubbs, P., Ristenpart, T., Woodage, J.: Fast message franking: from invisible salamanders to encryptment. In: Shacham, H., Boldyreva, A. (eds.) CRYPTO 2018. LNCS, vol. 10991, pp. 155–186. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-96884-1_6

12. Dworkin, M.: NIST Special Publication 800–38A: Recommendation for block cipher modes of operation: Methods and techniques (2001). https://csrc.nist.gov/pubs/sp/800/38/a/final
13. Dworkin, M.: NIST Special Publication 800–38C: Recommendation for block cipher modes of operation: the CCM mode for authentication and confidentiality (2007). https://csrc.nist.gov/pubs/sp/800/38/c/upd1/final
14. Dworkin, M.: NIST Special Publication 800–38D: Recommendation for block cipher modes of operation: Galois/counter mode (GCM) and GMAC (2007). https://csrc.nist.gov/pubs/sp/800/38/d/final
15. Farshim, P., Orlandi, C., Rosie, R.: Security of symmetric primitives under incorrect usage of keys. IACR Trans. Symmetric Cryptol. **2017**(1), 449–473 (2017)
16. Grubbs, P., Lu, J., Ristenpart, T.: Message Franking via Committing Authenticated Encryption. In: Katz, J., Shacham, H. (eds.) CRYPTO 2017. LNCS, vol. 10403, pp. 66–97. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-63697-9_3
17. Gueron, S., Langley, A., Lindell, Y.: AES-GCM-SIV: nonce misuse-resistant authenticated encryption. RFC **8452**, 1–42 (2019)
18. Gueron, S., Lindell, Y.: GCM-SIV: full nonce misuse-resistant authenticated encryption at under one cycle per byte. In: CCS 2015. pp. 109–119. ACM (2015)
19. Günther, F., Thomson, M., Wood, C.A.: Usage limits on AEAD algorithms (2023). https://www.ietf.org/archive/id/draft-irtf-cfrg-aead-limits-06.txt
20. Kessler, G.C.: GCK's file signatures table (2023). https://www.garykessler.net/library/file_sigs.html, (Accessed 19 Oct 2023)
21. Len, J., Grubbs, P., Ristenpart, T.: Partitioning oracle attacks. In: USENIX Security 2021, pp. 195–212 (2021)
22. Menda, S., Len, J., Grubbs, P., Ristenpart, T.: Context discovery and commitment attacks - how to break CCM, EAX, SIV, and more. In: EUROCRYPT 2023. LNCS, pp. 379–407 (2023). https://doi.org/10.1007/978-3-031-30634-1_13
23. Nir, Y., Langley, A.: ChaCha20 and Poly1305 for IETF protocols. RFC **8439**, 1–46 (2018)
24. NIST: FIPS 198–1: The keyed-hash message authentication code (HMAC) (2008). https://csrc.nist.gov/pubs/fips/198-1/final
25. NIST: The third NIST workshop on block cipher modes of operation 2023 (2023). https://csrc.nist.gov/Events/2023/third-workshop-on-block-cipher-modes-of-operation (Acessed 20 Oct 2023)
26. Merkle, R.C.: One way hash functions and DES. In: Brassard, G. (ed.) CRYPTO 1989. LNCS, vol. 435, pp. 428–446. Springer, New York (1990). https://doi.org/10.1007/0-387-34805-0_40
27. Stam, M.: Blockcipher-based hashing revisited. In: Dunkelman, O. (ed.) FSE 2009. LNCS, vol. 5665, pp. 67–83. Springer, Heidelberg (2009). https://doi.org/10.1007/978-3-642-03317-9_5
28. Wikipedia: List of file signatures (2023). https://en.wikipedia.org/wiki/List_of_file_signatures, (Accessed 19 Oct 2023)