KIVR: Context-Committing Authenticated Encryption Using Plaintext Redundancy and Application to GCM and Variants

Yusuke Naito[1], Yu Sasaki[2], and Takeshi Sugawara[3]

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

Abstract. Committing security of authenticated encryption (AE) is an emerging area of research motivated by real-world attacks. In particular, constructing AEs satisfying CMT-4, a security notion considering an adversary who generates multiple inputs for encryption that result in the same ciphertext, is an ongoing research challenge. In this paper, we propose a new mode KIVR, which transforms existing AEs to have CMT-4 security without increasing the ciphertext size by exploiting plaintext redundancy found in practical use cases. KIVR uses a collision-resistant hash to convert a tuple of key, 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. Unlike the conventional HtE and CTX conversions limited by the birthday bounds of the key and tag sizes, the security of KIVR linearly increases with the number of redundant bits r and can achieve the beyond-birthday-bound (BBB) security. Combined with GCM, KIVR's security becomes $\frac{r}{2}$ bits. In practical use cases with a sufficiently large r, KIVR salvages GCM for BBB security while preserving the ciphertext size and respecting GCM's interface. Furthermore, if we can use modified AEs, KIVR combined with CAU-SIV-C1 (a variant of GCM-SIV for committing security) achieves $\frac{r}{2} + 64$ bits, enabling higher security with fewer redundant bits.

Keywords: Key Commitment, Context Commitment, Modes of Operation, Authenticated Encryption, Security Proof

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, 3, 4, 6, 7, 9, 10, 16, 17].

Farshim et al. initiated the theoretical study in 2017 [9], followed by the real-world attacks, including the multi-recipient integrity attack that delivers malicious content to a targeted user [10, 7, 1] and the partitioning oracle attack that achieves efficient password brute-force attacks [16]. Missing 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 conventional AE security notions do not support key commitment, and there are $O(1)$ attacks on GCM [10, 7], GCM-SIV [16], CCM [8, 17], and ChaCha20-Poly1305 [18, 10].

Addressing the issue, researchers are studying AE schemes with committing security [10, 7, 1, 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 [13]. Similarly, NIST is organizing a workshop for updating the federal standard of block-cipher modes, wherein key commitment is explicitly noted as an additional security feature [19].

Although key commitment was originally on finding distinct keys K and K' that decrypt the same ciphertext while using the same N and A, some applications should also consider a stronger attacker who can modify any of (K, N, A, M) [3]. The generalization is called *context commitment*, and Bellare and Hoang defined the security notions in 2022, including CMT-1 and CMT-4 [4]. The security game is about finding a ciphertext $\Pi_{\mathsf{Enc}}(K, N, A, M) = \Pi_{\mathsf{Enc}}(K', N', A', M')$, and CMT-1 refers to the conventional key-committing security with $K \neq K'$. Meanwhile, CMT-4 refers to the security with $(K, N, A, M) \neq (K', N', A', M')$ [4]. An AE scheme with CMT-4 guarantees more robust security than CMT-1 and prevents misuse in broader use cases. Consequently, constructing an AEs with CMT-4 security is an ongoing research challenge [4, 6, 17].

While it is possible to design a dedicated scheme with committing security [7], many studies aim at extending conventional AEs for committing security, including HtE [4] and CTX [6] for CMT-4 security. Fig. 1-(left) shows HtE that converts a CMT-1-secure AE to CMT-4-secure one. It generates a temporary key $L \leftarrow H(K, N, A)$ using a collision-resistant (CR) hash function H, then L is used as the key of an underlying AE. Combined with the generic conversions for realizing CMT-1 security (UtC and RtC), any AE can be transformed into a CMT-4-secure one [4]. Since UtC and RtC require ciphertext overhead as a drawback, the same authors also proposed the efficient CMT-1 variants of GCM and GCM-SIV [12, 11], namely CAU-C1 and CAU-SIV-C1. CAU-C1 (resp. CAU-SIV-C1) adds the feed-forward to BC computed in the tag generation of GCM (resp. GCM-SIV), and changes the XOR position of GMAC from the output of BC to the input. On the other hand, CTX 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 by $T \leftarrow H(K, N, A, T')$. The verification is done with T.

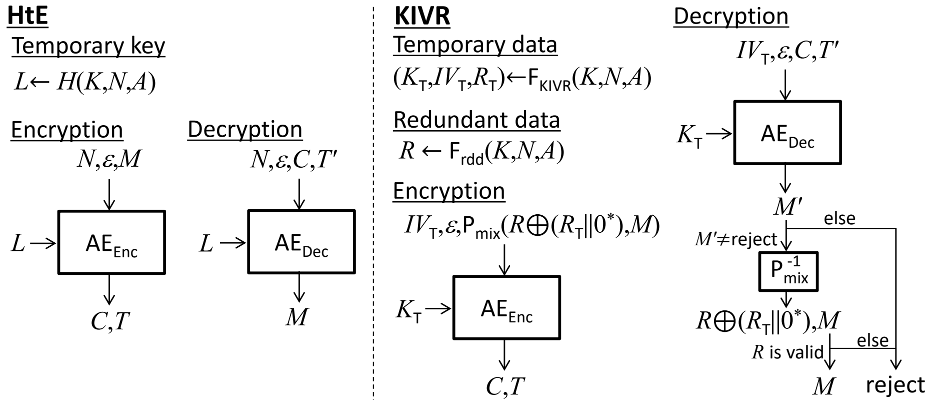
HtE
Temporary key
$L \leftarrow H(K,N,A)$
Encryption
$N,\mathcal{E},M$
L
$\mathsf{AE}_{\mathsf{Enc}}$
C,T
Decryption
$N,\mathcal{E},C,T'$
L
$\mathsf{AE}_{\mathsf{Dec}}$
M
KIVR
Temporary data
$(K_{\mathsf{T}},IV_{\mathsf{T}},R_{\mathsf{T}}) \leftarrow \mathsf{F}_{\mathsf{KIVR}}(K,N,A)$
Redundant data
$R \leftarrow \mathsf{F}_{\mathsf{rdd}}(K,N,A)$
Encryption
$IV_{\mathsf{T}},\mathcal{E},\mathsf{P}_{\mathsf{mix}}(R \oplus (R_{\mathsf{T}} \| 0^*),M)$
K_{T}
$\mathsf{AE}_{\mathsf{Enc}}$
C,T
Decryption
$IV_{\mathsf{T}},\mathcal{E},C,T'$
K_{T}
$\mathsf{AE}_{\mathsf{Dec}}$
M'
$M' \neq$reject
else
$\mathsf{P}_{\mathsf{mix}}^{-1}$
$R \oplus (R_{\mathsf{T}} \| 0^*),M$
R is valid
else
M
reject

Fig. 1. HtE [4] (left) and KIVR (right). The function $\mathsf{F}_{\mathsf{KIVR}}$ generates a tuple of temporary key, IV, and redundant data. The function $\mathsf{F}_{\mathsf{rdd}}$ generates redundant data. The function $\mathsf{P}_{\mathsf{mix}}$ generates a plaintext with redundancy from masked redundant data and a plaintext without redundancy.

1.1 Research Goal, Approach, and Challenges

Research Goal. We aim to construct CMT-4 secure AEs by using standardized AEs as a base. The target AEs are two CTR-based AE schemes CTRAE and CTRSIV. CTRAE is an Enc-then-MAC AE scheme (including GCM and CAU-C1, Section 3.2), and CTRSIV is an AE scheme following the SIV paradigm [20] (including GCM-SIV and CAU-SIV-C1, Section 3.3). By following the previous works [1], the ciphertext size should be preserved to maintain compatibility with the hardware, databases, and communication protocols already designed and deployed in the field. Commitment security is determined by an offline attack because the attacker can choose keys. The generic off-line attack is a brute-force search for the key, and its security is k bits. Hence, the bit-security level for committing security must be k-bits, or at least greater than $\frac{k}{2}$, i.e., the BBB of the key size.

Our Approach. The considerable difficulty is, as we will show later in Proposition 1, the CMT-4 security of CTRAE and CTRSIV is limited by $\frac{t}{2}$ bits with a t-bit tag and often $t \leq k$. We approach the problem by exploiting redundancy in plaintexts. It is a natural extension of Albertini et al.'s approach of achieving CMT-1 security by padding a message with zeroes [1], which inevitably increases the ciphertext size. We can increase the security without increasing the ciphertext size by exploiting plaintext redundancy already present in file formats [15, 21]. For example, PNG and XML files have 8 and 24 bytes of redundancy, respectively. Similar magic numbers are present in the practical network protocols. In HTTP, for example, it starts with `"HTTP/1.1"`, which can be used as an 8-byte redundancy. HTTP2 has an even longer 24-byte magic number, `"PRI *`

Table 1. Comparison of CMT-4 security for modes with r-bit redundancy.

Conversion	AE	CMT-4 Security	Prop.
CTX [6] + Redundancy	CTRAE	$\frac{t}{2}$	Prop. 3
HtE [4] + Redundancy	CTRAE, CTRSIV	$\frac{\kappa}{2}$	Prop. 4
KIVR + Redundancy	CTRAE	$\max\{\frac{r}{2}, \mathsf{tag\text{-}col}\}$	Thm. 1
KIVR + Redundancy	CTRSIV	$\frac{r}{2} + \mathsf{tag\text{-}col}$	Thm. 4

tag-col is the security against tag-collision attacks by changing any of K, N, A.

`HTTP/2.0\r\n\r\nSM\r\n\r\n"`. The recipient who decrypts the message can check the decrypted message for these known values.

Challenges. Unfortunately, as we will show with the attack in Section 4, simply adding plaintext redundancy (Albertini et al.'s approach) is insufficient for CMT-4 security, and CR hash is somehow necessary. To make matters more complicated, our analyses (Proposition 3 and 4) shows that the effect of CR hash does not simply add up with plaintext redundancy; Table 1 summarizes CMT-4 security of CTX and HtE with r-bit redundancy. CMT-4 security of CTX is independent of r and limited by $\frac{t}{2}$ (as shown in Proposition 3), with which BBB security is unachievable. In contrast, HtE's security is limited by $\frac{\kappa}{2}$ wherein κ is the AE's key length. This is too short for common cases, e.g., $\kappa = n$ in AES-GCM, and can be even smaller considering concrete AEs, as we will see in Table 2. In summary, a method to achieve BBB security for CMT-4 without increasing the ciphertext size is a meaningful research challenge. However, only $\frac{t}{2}$-bit or $\frac{\kappa}{2}$-bit security can be obtained with the conventional methods even with redundancy in plaintext if the ciphertext size is not increased.

1.2 Contributions

New Mode. We propose a KIVR mode, a generalization of HtE. In HtE, a temporary key L was generated by $H(K, N, A)$. In KIVR, instead of the temporary key, a tuple of temporary values $(K_\mathsf{T}, IV_\mathsf{T}, R_\mathsf{T})$ is generated by $H(K, N, A)$ with sufficiently large outputs so that the output size of H avoids becoming a bottleneck of the security bound. A diagram of encryption/decryption in KIVR is depicted in Fig. 1-(right). For encryption, to generally handle redundancy in plaintexts, we first perform the function F_rdd that extracts the redundant bits R from (K, N, A). R is then masked by R_T, and the function P_mix is performed to derive the plaintext that is a mixture of R and M. Finally, the original AE is computed by using K_T, IV_T, and an empty string as a key, a nonce, and an associated data, respectively. Decryption is naturally defined with the exception that we additionally check whether or not the valid R is correctly recovered. Note

Table 2. CMT-4 security of the instantiations with r-bit redundancy.

Conversion	**AE**	**CMT-4 Security w/ $k = 128$**	**Ref.**
CTX [6] + Redundancy	GCM, CAU-C1	64	Prop. 3†
HtE [4]+ Redundancy	GCM	$\min\{\frac{r}{2}, 64\}$	Prop. 5†
HtE [4]+ Redundancy	CAU-C1	64	Prop. 6†
HtE [4]+ Redundancy	GCM-SIV	$\min\{\frac{r}{2}, 64\}$	Prop. 7†
HtE [4]+ Redundancy	CAU-SIV-C1	64	Prop. 8†
KIVR + Redundancy	GCM	$\frac{r}{2}$	Cor. 2‡
KIVR + Redundancy	CAU-C1	$\max\{\frac{r}{2}, 64\}$	Cor. 3‡
KIVR + Redundancy	GCM-SIV	$\frac{r}{2}$	Cor. 5‡
KIVR + Redundancy	CAU-SIV-C1	$\frac{r}{2} + 64$	Cor. 6‡

†The security determined by an attack, ‡the security determined by a proof.

that security is dependent on the size of R_T instead of R. If R is sufficiently long, e.g., 1000 bits, and the desired bit-security is much lower, e.g., 128 bits, then R_T can be shorter than R, i.e., does not need to mask all the bits in R, which saves the computational cost of H and broadens primitive choices.

The actual CMT-4 security that can be proved depends on an underlying AE. When the underlying AE is CTRAE, we prove that the CMT-4 security bound is $\max\{\frac{r}{2}, \mathsf{tag\text{-}col}\}$, where tag-col is the security against tag-collision attacks by changing any of K, N, A. Also, when AE is CTRSIV, we prove that the CMT-4 security bound improves to $\frac{r}{2} + \mathsf{tag\text{-}col}$. Given that commitment is a setting where the adversary chooses the key, it is natural that security bound for the commitment is independent of the key size. In fact, even if an adversary is allowed to perform an exhaustive search of 2^k keys and 2^n plaintexts for a block cipher, it is difficult to break the committing security. KIVR's security bound is simple; consisting only of the redundancy size and tag-col, and thus is natural for committing security.

It is also necessary to ensure that the converted scheme by KIVR does not negatively affect the security as an ordinary AE. We prove that the AE security after applying KIVR is reduced to the multi-user security of the original AE.

Salvaging GCM, GCM-SIV, and Their Variants. Table 2 summarizes KIVR's CMT-4 security with r-bit redundancy instantiated with GCM, CAU-C1, GCM-SIV, and CAU-SIV-C1 for $k = 128$, e.g., AES-128. In all the combinations, KIVR's security increases linearly with r. This is in contrast to CTX and HtE which are limited by 64 bits, i.e., the birthday bound of either the tag or key sizes. KIVR with GCM is suitable when AES-GCM's interface should be strictly respected, e.g., in a hardware security module. For XML and HTTP2 with $r = 192$, KIVR with GCM achieves 96-bit security. With a moderate amount of r, on the other hand, the combination of KIVR and CAU-SIV-C1 is the best choice because it achieves $(\frac{r}{2} + 64)$-bit security, enjoying the benefits from both CR hash and redundancy. Applying this method for PNG and HTTP with $r = 64$ enables 96-bit CMT-4 security. In this case, AES and GHASH accelerators/instructions are reusable for realizing CAU-SIV-C1.

1.3 Organization

We begin by preliminaries in Section 2. We define CTRAE and CTRSIV in Section 3. Section 4 recalls HtE and CTX, and their limitations with plaintext redundancy. We introduce the KIVR conversion in Section 5. Sections 6 and 7 give security proofs of KIVR combined with CTRAE and CTRSIV. We further analyze HtE with plaintext redundancy in Section 8. Section 9 is a conclusion.

2 Preliminaries

Notation. For integers $0 \le i \le j$, let $[i,j] := \{i, i+1, \ldots, j\}$, $(j] := [0,j]$, 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, $\{0,1\}^0 := \{\varepsilon\}$, and $\{0,1\}^{\le n} := \cup_{i \in (n]} \{0,1\}^i$. 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 integers $0 \le i, j$ and $X \in \{0,1\}^i$, let $\mathsf{zp}_j(X) := X \| 0^{\lceil i/j \rceil \cdot j - i}$ be a zero-padding function such that the lengths of padded values become multiples of j. 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 that $\mathcal{T} \leftarrow \mathcal{T} \cup \mathcal{T}'$. 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 $X_1 = \varepsilon$.

Block Cipher (BC). The bit-lengths of block and key of BC are denoted by n and k, respectively. A BC is a set of n-bit permutations indexed by a k-bit key. An encryption of BC is denoted by $E : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$, and its decryption is denoted by $E^{-1} : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$. Let $\mathcal{BC}$ be the set of all encryptions of k-bit key and n-bit block BCs.

Ideal Cipher (IC). An IC is an ideal BC and defined as $E \xleftarrow{\$} \mathcal{BC}$. An IC E can be implemented by lazy sampling. Let $\mathcal{T}_{\mathsf{IC}}$ be a table that is initially empty and keeps query-response tuples of E and E^{-1}. Let $\mathcal{T}_{\mathsf{IC},2}[W] := \{Y \mid (W, X, Y) \in \mathcal{T}_{\mathsf{IC}}\}$

and $\mathcal{T}_{\mathsf{IC},1}[W] := \{X \mid (W,X,Y) \in \mathcal{T}_{\mathsf{IC}}\}$ be tables that respectively keep ciphertext and plaintext blocks defined in $\mathcal{T}_{\mathsf{IC}}$ 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 $Y \xleftarrow{\$} \{0,1\}^n \backslash \mathcal{T}_{\mathsf{IC},2}[W]$ (resp. $X \xleftarrow{\$} \{0,1\}^n \backslash \mathcal{T}_{\mathsf{IC},1}[W]$), and the query-response tuple (W,X,Y) is added to $\mathcal{T}_{\mathsf{IC}}$: $\mathcal{T}_{\mathsf{IC}} \xleftarrow{\cup} \{(W,X,Y)\}$. For a query stored in the table $\mathcal{T}_{\mathsf{IC}}$, the same response is returned.

Hash Function. Let $\mathcal{M} \subseteq \{0,1\}^*$ and h be a positive integer. Let $H[\Psi] : \mathcal{M} \rightarrow \{0,1\}^h$ 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 use the following security notions for hash function, where Ψ is ideal.
υ-Collision Resistance. $H[\Psi]$ is υ-collision resistant if it is hard to find υ pairs of distinct messages such that for each pair the hash values are the same. The υ-collision-resistant advantage function of $\mathbf{A}$ with access to an ideal primitive Ψ against $H[\Psi]$ is defined as

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

If $\upsilon = 1$ then, the notion is for the standard 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. Let $\mathcal{H}$ be the set of all hash functions from $\mathcal{M}$ to $\{0,1\}^h$. An RO is defined as $\mathcal{R} \xleftarrow{\$} \mathcal{H}$. 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 $\mathcal{R}$. Let $\mathcal{T}_{\mathsf{RO},2} := \{Y \mid (X,Y) \in \mathcal{T}_{\mathsf{RO}}\}$ be a table that keeps outputs defined in $\mathcal{T}_{\mathsf{RO}}$. For a new query X to $\mathcal{R}$, 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 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 $\Pi_{\mathsf{Enc}}[\Psi] : \mathcal{N} \times \mathcal{A} \times \mathcal{M} \rightarrow \mathcal{C} \times \mathcal{T}$ takes a tuple (N,A,M), and returns, deterministically, a pair (C,T). The decryption algorithm $\Pi_{\mathsf{Dec}}[\Psi] : \mathcal{N} \times \mathcal{A} \times \mathcal{C} \times \mathcal{T} \rightarrow \{\mathbf{reject}\} \cup \mathcal{M}$ 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 for any $(K,N,A,M), (K',N',A',M') \in \mathcal{K} \times \mathcal{N} \times \mathcal{A} \times \mathcal{M}$, $|\Pi_{\mathsf{Enc}}[\Psi](K,N,A,M)| = |\Pi_{\mathsf{Enc}}[\Psi](K',N',A',M')|$ is satisfied if $|M| = |M'|$. We also require that for any $K \in \mathcal{K}$, $N \in \mathcal{N}$, $A \in \mathcal{A}$, and $M \in \mathcal{M}$, $\Pi_{\mathsf{Dec}}[\Psi](K,N,A,\Pi_{\mathsf{Enc}}[\Psi](K,N,A,M)) = M$.

Committing Security [4]. We use functions WiC_i ($i \in \{1,3,4\}$) that on input tuple (K, N, A, M) of key, nonce, AD, and plaintext, 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 key, nonce, AD, and plaintext on which the outputs of $\Pi_{\mathsf{Enc}}[\Psi]$ are the same. The **CMT-i**-security advantage of an adversary $\mathbf{A}$ for $i \in \{1,3,4\}$ is defined as

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

In this paper, we consider computationally unbounded adversaries.

Tool for Security Proofs in the IC Model. Our proofs of committing security of AE schemes are given in the IC model. In the proofs, to ensure the randomnesses of the outputs of an IC E or E^{-1}, we use the technique given in [2].

Definition 1 (Full-block queries). *In a security game in the IC model, 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. The additional queries, which we call full-block queries, ensure that the outputs of E or E^{-1} are chosen uniformly at random from 2^{n-1} elements in $\{0,1\}^n$.*[4] *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.*

3 Specifications of GCM and Its Variants

We show the specifications of GCM and its variants, the AE schemes with the counter (CTR) mode. Firstly, we show the specification of CTR that is the encryption algorithms of GCM and its variants. Secondly, we show the specification of CTRAE, which is an Enc-then-MAC AE with CTR. Thirdly, we show the specifications of GCM and its variants, which are the special cases of CTRAE. Fourthly, we show the specification of CTRSIV, which follows the SIV paradigm [20] and uses CTR. Finally, we show the specifications of GCM-SIV and its variant, which are the special cases of CTRSIV.

[4] In [2], the additional queries are called super queries.

Algorithm 1 Counter Mode

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

Algorithm 2 CTR-based AE

```
Encryption $\mathsf{CTRAE}_{\mathsf{Enc}}[E, \Psi_{\mathsf{tag}}]((K_{\mathsf{bc}}, K_{\mathsf{tag}}), N, A, M)$
$C \leftarrow \mathsf{CTR}[E](K_{\mathsf{bc}}, \mathsf{zp}_n(N), M)$; $T \leftarrow \mathsf{CTRAE}_{\mathsf{TGen}}[\Psi_{\mathsf{tag}}](K_{\mathsf{tag}}, N, A, C)$
return $(C, T)$

Decryption $\mathsf{CTRAE}_{\mathsf{Dec}}[E, \Psi_{\mathsf{tag}}]((K_{\mathsf{bc}}, K_{\mathsf{tag}}), N, A, C, T')$
$M \leftarrow \mathsf{CTR}[E](K_{\mathsf{bc}}, \mathsf{zp}_n(N), C)$; $T \leftarrow \mathsf{CTRAE}_{\mathsf{TGen}}[\Psi_{\mathsf{tag}}](K_{\mathsf{tag}}, N, A, C)$
if $T = T'$ then return $M$; else return reject end if
```

Algorithm 3 CTR-based SIV

```
Encryption $\mathsf{CTRSIV}_{\mathsf{Enc}}[E, \Psi_{\mathsf{tag}}, \Psi_{\mathsf{kdf}}](K, N, A, M)$
$(K_{\mathsf{bc}}, K_{\mathsf{tag}}) \leftarrow \mathsf{KD}_{\mathsf{siv}}[\Psi_{\mathsf{kdf}}](K, N)$
$T \leftarrow \mathsf{CTRSIV}_{\mathsf{TGen}}[\Psi_{\mathsf{tag}}](K_{\mathsf{tag}}, N, A, M)$; $C \leftarrow \mathsf{CTR}[E](K_{\mathsf{bc}}, T, M)$; return $(C, T)$

Decryption $\mathsf{CTRSIV}_{\mathsf{Dec}}[E, \Psi_2, \Psi_{\mathsf{kdf}}](K, N, A, C, T')$
$(K_{\mathsf{bc}}, K_{\mathsf{tag}}) \leftarrow \mathsf{KD}_{\mathsf{siv}}[\Psi_{\mathsf{kdf}}](K, N)$
$M \leftarrow \mathsf{CTR}[E](K_{\mathsf{bc}}, T', C)$; $T \leftarrow \mathsf{CTRSIV}_{\mathsf{TGen}}[\Psi_{\mathsf{tag}}](K_{\mathsf{tag}}, N, A, M)$
if $T' = T$ then return $M$; else return reject end if
```

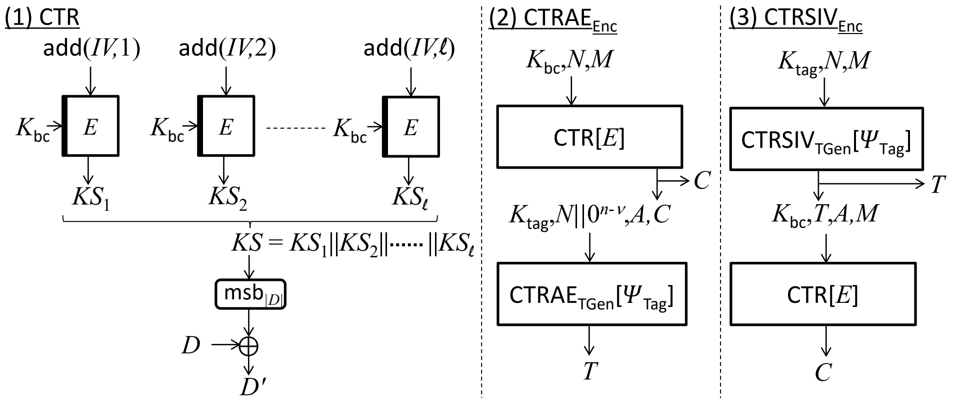

Fig. 2. (1) CTR Mode where $\ell = \lceil |D|/n \rceil$ and (D, D') is a pair of plaintext and ciphertext or of ciphertext and plaintext; (2) $\mathsf{CTRAE}_{\mathsf{Enc}}$; (3) $\mathsf{CTRSIV}_{\mathsf{Enc}}$ where a pair of temporary keys are defined as $(K_{\mathsf{bc}}, K_{\mathsf{tag}}) \leftarrow \mathsf{KD}_{\mathsf{siv}}[\Psi_{\mathsf{kdf}}](K, N)$.

3.1 Counter Mode

The specification of the counter mode CTR is given in Algorithm 1 and Fig. 2(1), where E is the underlying BC. Let c be the counter size such that $c \leq n$.

Algorithm 4 Tag Generation of $\mathit{\Pi} \in \{\mathsf{CAU}, \mathsf{CAU\text{-}C1}\}$

```
Tag Generation $\mathit{\Pi}_{\mathsf{TGen}}[E]((K_{\mathsf{bc}}, L), N, A, C)$
    $H \leftarrow \mathsf{Hash}(L, A, C)$; $X \leftarrow N \| 0^{c-1}1$
    if $\mathit{\Pi} = \mathsf{CAU}$ then $T \leftarrow \mathsf{msb}_t(H \oplus E(K_{\mathsf{bc}}, X))$; return $T$ end if
    if $\mathit{\Pi} = \mathsf{CAU\text{-}C1}$ then $X \leftarrow X \oplus H$; $T \leftarrow \mathsf{msb}_t(X \oplus E(K_{\mathsf{bc}}, X))$; return $T$ end if
```

Algorithm 5 GHASH

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

Algorithm 6 Tag Generation $\mathit{\Pi}_{\mathsf{TGen}} \in \{\mathsf{GMAC}^+, \mathsf{GMAC2}\}$

```
Tag Generation $\mathit{\Pi}_{\mathsf{TGen}}[E]((K_{\mathsf{bc}}, L), N, A, M)$
    $X \leftarrow 0 \| \mathsf{lsb}_{n-1}(H) \oplus (0^c \| N)$; $T \leftarrow E(K_{\mathsf{bc}}, X)$
    if $\mathit{\Pi} = \mathsf{CAU\text{-}SIV\text{-}C1}$ then $T \leftarrow T \oplus X$ end if
    return $T$
```

Let $\mathcal{D} \subset \{0,1\}^*$ be the plaintext/ciphertext space. $\{0,1\}^k$ is the key space. $\mathsf{CTR}[E] : \{0,1\}^k \times \{0,1\}^n \times \mathcal{D} \to \mathcal{D}$ takes a tuple of key K_{bc}, initial value IV, and data D, and returns encrypted/decrypted data D'. If D is a plaintext (resp. ciphertext), then D' is the ciphertext (resp. plaintext). $KS_1 \| \cdots \| KS_{\lceil |D|/n \rceil}$ is a key stream with which a ciphertext (resp. plaintext) is defined by XORing a plaintext (resp. ciphertext). $\mathsf{add} : \{0,1\}^n \times (2^c - 1] \to \{0,1\}^n$ is a function that on the input pair of IV and counter, returns an input block of E. add is defined for each AE scheme.

3.2 CTR-based AE

CTRAE. $\mathsf{CTRAE}[E, \mathit{\Psi}_{\mathsf{tag}}]$ is a tag-based AE scheme with CTR and the underlying primitives E and $\mathit{\Psi}_{\mathsf{tag}}$. The specification of $\mathsf{CTRAE}[E, \mathit{\Psi}_{\mathsf{tag}}]$ is given in Algorithm 2 and Fig. 2(2). Let $\mathcal{K}_{\mathsf{tag}}$ be the key space of the tag-generation function. Hence, $\mathcal{K} := \{0,1\}^k \times \mathcal{K}_{\mathsf{tag}}$ is the key space of CTRAE. The encryption/decryption function is the counter mode $\mathsf{CTR}[E]$. $\mathsf{CTRAE}_{\mathsf{TGen}}[\mathit{\Psi}_{\mathsf{tag}}] : \mathcal{K}_{\mathsf{tag}} \times \mathcal{N} \times \mathcal{A} \times \mathcal{C} \to \{0,1\}^t$ is a tag-generation function with a primitive $\mathit{\Psi}_{\mathsf{tag}}$. The parameters ν and c are such that $n = \nu + c$. The function add is defined as $\mathsf{add}(IV, i) := (\mathsf{msb}_\nu(IV)) \| (\mathsf{lsb}_c(IV) + i + 1 \bmod 2^c)$ where in the evaluation $\mathsf{lsb}_c(IV)$ is considered as an integer, and the result of the evaluation is regarded as a c-bit string.

CAU (Generalization of GCM). GCM (resp. its generalization CAU) is a single-key CTRAE scheme with the tag-generation function GMAC (resp. $\mathsf{CAU}_{\mathsf{TGen}}$). 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 $\mathsf{CAU}_{\mathsf{TGen}}$ is given in Algorithm 4 and Fig. 3(1)(2). Hash is a universal hash function with a key L, and the

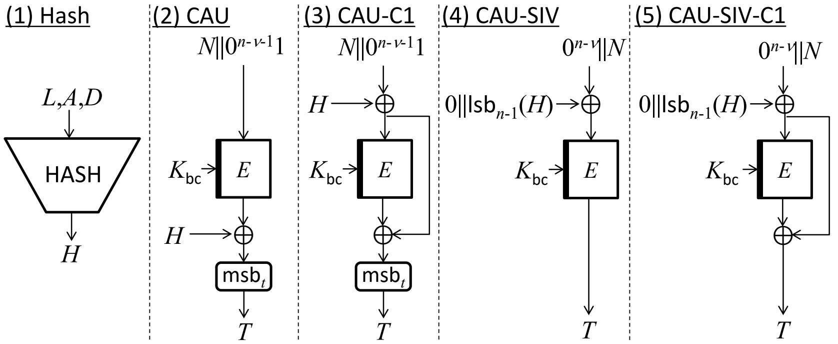

Fig. 3. Tag-generation functions of CAU (1)(2), of CAU-C1 (1)(3), of CAU-SIV (1)(4), and of CAU-SIV-C1 (1)(5). The hash key of CAU and CAU-C1 is defined as $L \leftarrow E(K, 0^n)$. D is a ciphertext (resp. plaintext) in CAU and CAU-C1 (resp. CAU-SIV and CAU-SIV-C1).

hash key is defined as $L \leftarrow E(K, 0^n)$. GMAC is $\mathsf{CAU}_{\mathsf{TGen}}$ with the hash function GHASH defined in Algorithm 5. GHASH uses field multiplications. 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 $\mathbb{F}$.

The multi-user AE (mu-AE) security of CAU (and GCM) was proven in the IC model [14]. On the other hand, several works e.g. [1, 10, 1, 16] show that GCM is not **CMT**-1 secure, i.e., there exists an adversary that breaks the **CMT**-1-security of GCM.

CAU-C1. CAU-C1 [4], a variant of CAU, is a single-key CTRAE scheme with the tag-generation function $\mathsf{CAU\text{-}C1}_{\mathsf{TGen}}$. Hence, $K_{\mathsf{tag}} = K_{\mathsf{bc}}$ and $\mathcal{K}_{\mathsf{tag}} = \{0,1\}^k$. $\mathsf{CAU\text{-}C1}_{\mathsf{TGen}}$ uses the Davies-Meyer (DM) mode instead of the plain BC encryption, and the hash value H is taken before the DM call. The specification of $\mathsf{CAU\text{-}C1}_{\mathsf{TGen}}$ is given in Algorithm 6 and Fig. 3(1)(3). Hash is a universal hash function with a key L, and the key is defined as $L \leftarrow E(K, 0^n)$. We call CAU-C1 with the hash function GHASH "GCM-C1".

In [4], the mu-AE-security of CAU-C1 was proven under the assumption that the underlying BCs are pseudorandom functions, and it was proven that CAU-C1 is **CMT**-1 secure as long as DM is collision resistant.

3.3 CTR-based SIV

CTRSIV. $\mathsf{CTRSIV}[E, \Psi_{\mathsf{tag}}, \Psi_{\mathsf{kdf}}]$, a tag-based AE scheme with $\mathsf{CTR}[E]$, is defined by following the GCM-SIV design [12, 11], and thus uses a nonce-based key derivation function (KDF). The specification of $\mathsf{CTRSIV}[E, \Psi_{\mathsf{tag}}, \Psi_{\mathsf{kdf}}]$ is given in Algorithm 3 and Fig. 2(3). Let $\mathcal{K}_{\mathsf{tag}}$ be the key space of the tag-generation function. $\mathsf{CTRSIV}_{\mathsf{TGen}}[\Psi_{\mathsf{tag}}] : \mathcal{K}_{\mathsf{tag}} \times \mathcal{N} \times \mathcal{A} \times \mathcal{M} \rightarrow \{0,1\}^n$ is the tag-generation function. The tag size is n, i.e., $t = n$. $\mathsf{KD}_{\mathsf{siv}}[\Psi_{\mathsf{kdf}}] : \mathcal{K} \times \{0,1\}^{\nu} \rightarrow \{0,1\}^k \times \mathcal{K}_{\mathsf{tag}}$ is the nonce-based KDF that on an input tuple (K, N) of an original key and nonce, returns a pair of temporary keys $(K_{\mathsf{bc}}, K_{\mathsf{tag}})$. K_{bc} (resp. K_{tag}) is a temporary key of CTR (resp. $\mathsf{CTRSIV}_{\mathsf{TGen}}$). The function add of $\mathsf{CAU\text{-}SIV}$ is defined as $\mathsf{add}(IV, i) := (1\|(\mathsf{msb}_{n-c-1}(IV))\|(\mathsf{lsb}_c(IV) + i \bmod 2^c))$, where in the evaluation $\mathsf{lsb}_c(IV)$ is considered as an integer, and the result of the evaluation is regarded as a c-bit string.

CAU-SIV (a Generalization of GCM-SIV). $\mathsf{CAU\text{-}SIV}[E]$ [5] is CTRSIV with the tag-generation function $\mathsf{GMAC}^+[E]$ and the KDF $\mathsf{KD1}[E]$. The specification is given in Algorithm 6 and Fig. 3(1)(4). (K_{bc}, L) is a pair of (temporary) keys of $\mathsf{GMAC}^+[E]$, where K_{bc} is equal to the key of CTR. $\mathsf{GMAC}^+[E] : \{0,1\}^k \times \{0,1\}^n \times \mathcal{A} \times \mathcal{M} \rightarrow \{0,1\}^n$ takes an input tuple $(K_{\mathsf{bc}}, L, N, A, M)$ and returns an n-bit tag T. $\mathsf{Hash} : \{0,1\}^n \times \mathcal{A} \times \mathcal{M} \rightarrow \{0,1\}^n$ is a universal hash function that on input tuple (L, A, M), returns a hash value H. The key derivation $\mathsf{KD1}[E]$ is a concatenation of truncated BC calls where each BC call takes input tuple of key, nonce, and counter.

The $\mathsf{mu\text{-}AE}$-security of $\mathsf{CAU\text{-}SIV}$ was proven in the IC model. On the other hand, as the attacks on GCM [1, 10, 1, 16], $\mathsf{GCM\text{-}SIV}$ is not **CMT**-1 secure.

CAU-SIV-C1. $\mathsf{CAU\text{-}SIV\text{-}C1}$ [4], a variant of $\mathsf{CAU\text{-}SIV}$, is CTRSIV with the tag-generation function $\mathsf{GMAC2}[E]$ and the KDF $\mathsf{KD1}[E]$. The specification of $\mathsf{GMAC2}$ is given in Algorithm 6 and Fig. 3(1)(5). $\mathsf{GMAC2}$ uses the DM mode instead of the plain BC's encryption, and the hash value H is taken before the DM call. We call $\mathsf{CAU\text{-}SIV\text{-}C1}$ with the hash function GHASH "$\mathsf{GCM\text{-}SIV\text{-}C1}$".

In [4], the $\mathsf{mu\text{-}AE}$-security of $\mathsf{CAU\text{-}SIV\text{-}C1}$ was proven under the assumptions that the underlying BCs are pseudorandom permutations and the key derivation functions are pseudorandom functions. In [4], it was proven that $\mathsf{CAU\text{-}SIV\text{-}C1}$ is **CMT**-1 secure as long as DM and $\mathsf{KD1}$ are collision resistance.

4 Plaintext Redundancy and Limitations of Committing AE

In this section, we define functions for plaintext redundancies and then show limitations of the existing conversions HtE and CTX with plaintext redundancies.

4.1 Limitations for Committing Security of CTRAE and CTRSIV

The following proposition shows that even when the tag-generation functions are ROs, the **CMT**-1 (resp. **CMT**-3) security of CTRAE (resp. CTRSIV) is broken by $O(2^{t/2})$ computations when there is no plaintext redundancy.

Proposition 1. *Let $\Pi \in \{\mathsf{CTRAE}, \mathsf{CTRSIV}\}$. Assume that E is an encryption of IC and the tag-generation function Π_{TGen} is an RO. Then, there exists an adversary $\mathbf{A}$ such that the number of queries to E, E^{-1}, or Π_{TGen} is p and $\mathbf{Adv}_{\Pi}^{\mathsf{cmt}\text{-}i}(\mathbf{A}) = O\left(\frac{p^2}{2^t}\right)$ where $i = 1$ if $\Pi = \mathsf{CTRAE}$; $i = 3$ if $\Pi = \mathsf{CTRSIV}$.*

Algorithm 7 **CMT**-1 Adversary **A** against CTRAE

```
Choose $p-2$ distinct keys of $\mathsf{CTR}$ $K_{\mathsf{bc}}^{(1)}, \ldots, K_{\mathsf{bc}}^{(p-2)} \in \{0,1\}^k$, $p-2$ distinct keys of $\mathsf{CTRAE}_{\mathsf{TGen}}$ $K_{\mathsf{tag}}^{(1)}, \ldots, K_{\mathsf{tag}}^{(p-2)} \in \mathcal{K}_{\mathsf{tag}}$, $(N, A) \in \{0,1\}^\nu \times \mathcal{A}$, and $C \leftarrow 0^n$
for $i = 1, \ldots, p-2$ do $T^{(i)} \leftarrow \mathsf{CTRAE}_{\mathsf{TGen}}(K_{\mathsf{tag}}^{(i)}, N, A, C)$ end for
if $\exists \alpha, \beta \in [p-2]$ s.t. $\alpha \neq \beta \wedge T^{(\alpha)} = T^{(\beta)}$ then
    $M^{(\alpha)} \leftarrow \mathsf{CTR}[E](K_{\mathsf{bc}}^{(\alpha)}, N \| 0^{n-\nu}, C)$; $M^{(\beta)} \leftarrow \mathsf{CTR}[E](K_{\mathsf{bc}}^{(\beta)}, N \| 0^{n-\nu}, C)$
    return $(((K_{\mathsf{bc}}^{(\alpha)}, K_{\mathsf{tag}}^{(\alpha)}), N, A, M^{(\alpha)}), ((K_{\mathsf{bc}}^{(\beta)}, K_{\mathsf{tag}}^{(\beta)}), N, A, M^{(\beta)}))$
end if
return $(((K_{\mathsf{bc}}^{(1)}, K_{\mathsf{tag}}^{(1)}), N, A, 0), ((K_{\mathsf{bc}}^{(2)}, K_{\mathsf{tag}}^{(2)}), N, A, 1))$
```

Algorithm 8 **CMT**-3 Adversary **A** against CTRSIV

```
Choose $p$ distinct AD $A^{(1)}, \ldots, A^{(p)} \in \mathcal{A}$ and $(K, N, M) \in \mathcal{K} \times \{0,1\}^\nu \times \mathcal{M}$
$(K_{\mathsf{bc}}, K_{\mathsf{tag}}) \leftarrow \mathsf{KD}_{\mathsf{siv}}[\Psi_{\mathsf{kdf}}](K, N)$
for $i = 1, \ldots, p$ do $T^{(i)} \leftarrow \mathsf{CTRSIV}_{\mathsf{TGen}}(K_{\mathsf{tag}}, N, A^{(i)}, M)$ end for
if $\exists \alpha, \beta \in [p]$ s.t. $\alpha \neq \beta \wedge T^{(\alpha)} = T^{(\beta)}$ then
    return $((K, N, A^{(\alpha)}, M), (K, N, A^{(\beta)}, M))$ end if
return $((K, N, A^{(1)}, M), (K, N, A^{(2)}, M))$
```

Proof. An adversary **A** breaking the **CMT**-1-security of CTRAE is defined in Algorithm 7. **A** fixes a nonce, AD, and a ciphertext, and varies keys. By the birthday analysis, the probability that a tag collision occurs is $O(p^2/2^t)$. Hence, the adversary breaks the **CMT**-1-security of CTRAE with the probability $O(p^2/2^t)$.

An adversary **A** breaking the **CMT**-3-security of CTRSIV is defined in Algorithm 8. The adversary fixes a tuple of key, nonce, and ciphertext, and varies AD values. By the birthday analysis, the probability that a tag collision occurs is $O(p^2/2^t)$. Since AD is not an input to CTR, the ciphertexts in the adversary's output are the same, and the adversary breaks the **CMT**-3-security of CTRSIV with the probability $O(p^2/2^t)$. □

4.2 Plaintext Redundancy

In order to overcome the birthday-bound limitation regarding the tag size in Proposition 1, we use plaintext redundancy, which adversaries cannot control. To handle plaintext redundancy in our proofs, we define the functions that capture the properties of plaintext redundancy.

Definition 2 (Plaintext Redundancy). *Let r be the length of redundant data. Let $\mathsf{F}_{\mathit{rdd}} : \mathcal{K} \times \mathcal{N} \times \mathcal{A} \to \{0,1\}^r$ be a redundant-data-derivation (RDD) function that derives an r-bit redundant data from an input tuple of key, nonce, and AD. Let $\mathsf{P}_{\mathit{mix}} : \{0,1\}^r \times \mathcal{M} \to \mathcal{M}$ is a mixing function that on input tuple (R, M) of r-bit redundant data and plaintext, returns a plaintext with the redundant data M^* such that $|M^*| = |M| + r$. $\mathsf{P}_{\mathit{mix}}$ is a (ω, n)-mixing linear function if the function is linear and bijection, and the number of n-bit blocks with redundant bits is at most ω, i.e., for any plaintext M and r-bit redundant* *data R, the number of n-bit blocks of $\mathsf{P}_{mix}(R, M)$ depending on R is at most ω.*[5] *For an AE, encryption,* CTR*, or a tag-generation scheme Π let $\Pi^{\mathsf{P}_{mix}, \mathsf{F}_{rdd}}$ be Π with the redundant functions F_{rdd} and P_{mix}.*

The above definition captures plaintext redundancy found in the real-world applications. As described in the introduction, practical file formats (e.g., PNG and XML) and network protocols (e.g., HTTP and HTTP2) have known constant strings, or magic numbers, to distinguish a particular format or protocol from others [15, 21]. We can use them as plaintext redundancy to increase the committing security without increasing the ciphertext size. In these cases, the RDD function is a constant map $\mathsf{F}_{\mathsf{rdd}} : (K, N, A) \mapsto \mathsf{const}$ and $\mathsf{P}_{\mathsf{mix}}$ is simple string concatenation. $\mathsf{F}_{\mathsf{rdd}}$ and $\mathsf{P}_{\mathsf{mix}}$ cover even wider range of redundancy, including non-consecutive constant values and the ones depend on associated data and other parameters.

Property of CTR with Plaintext Redundancy. The following lemma shows that a collision of CTR with plaintext redundancy implies that the sum of the key streams meets the sum of the plaintext redundancies.

Lemma 1. *Let P_{mix} be a (ω, n)-mixing linear function. Let (K', IV', M', R') and (K'', IV'', M'', R'') be tuples of key, IV, plaintext, and r-bit redundant data such that $(K', IV') \neq (K'', IV'')$ and $|M'| = |M''|$. For $\square \in \{\prime, \prime\prime\}$, let $C^{\square} := \mathsf{CTR}[E](K^{\square}, IV^{\square}, \mathsf{P}_{mix}(R^{\square} \| M^{\square}))$ and $KS^{\square}$ the key stream defined in the process of* CTR*. Then, we have*

$$C' = C'' \Rightarrow \mathsf{msb}_r \left(\mathsf{P}_{mix}^{-1} \left(\mathsf{msb}_{|C'|} \left(KS' \oplus KS'' \right) \right) \right) = R' \oplus R''.$$

The property is used to derive a probability of a collision of ciphertexts in our committing security proofs. Intuitively, KS' and KS'' are (almost) r-bit random values and the probability of the ciphertext collision is $O(1/2^r)$.

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

$$\begin{aligned} C' = C'' &\Rightarrow \mathsf{msb}_{|C'|} \left(KS' \oplus KS'' \right) = \mathsf{P}_{\mathsf{mix}}(R' \| M') \oplus \mathsf{P}_{\mathsf{mix}}(R'' \| M'') \\ &\Rightarrow \mathsf{msb}_{|C'|} \left(KS' \oplus KS'' \right) = \mathsf{P}_{\mathsf{mix}} \left((R' \oplus R'') \, \| \, (M' \oplus M'') \right) \\ &\Rightarrow \mathsf{msb}_r \left(\mathsf{P}_{\mathsf{mix}}^{-1} \left(\mathsf{msb}_{|C'|} \left(KS' \oplus KS'' \right) \right) \right) = R' \oplus R''. \end{aligned}$$

4.3 Committing Insecurity of GCM and Its Variants with Plaintext Redundancy

The following proposition shows that plaintext redundancy does not improve the committing security of GCM, $\mathsf{GCM\text{-}SIV}$, $\mathsf{GCM\text{-}C1}$, and $\mathsf{GCM\text{-}SIV\text{-}C1}$.

[5] When $(X_1, \ldots, X_\ell) \xleftarrow{n} \mathsf{P}_{\mathsf{mix}}(R, M)$, the number of blocks in $(X_1, \ldots, X_\ell)$ that depend on R is at most ω.

Algorithm 9 $\mathsf{CTX}[\mathsf{CTRAE}]$

```
Encryption $\mathsf{CTX}[\mathsf{CTRAE}_{\mathsf{Enc}}[E,\Psi]]((K_{\mathsf{bc}},K_{\mathsf{tag}}),N,A,M)$
  $C \leftarrow \mathsf{CTR}[E](K_{\mathsf{bc}},N,M)$; $T^{\dagger} \leftarrow \mathsf{CTRAE}_{\mathsf{TGen}}[\Psi_{\mathsf{tag}}](K_{\mathsf{tag}},N,A,C)$
  $T \leftarrow \mathsf{F}_{\mathsf{CTX}}(K,N,A,T^{\dagger})$; return $(C,T)$

Decryption $\mathsf{CTX}[\mathsf{CTRAE}_{\mathsf{Dec}}[E,\Psi]]((K_{\mathsf{bc}},K_{\mathsf{tag}}),N,A,C,T')$
  $M \leftarrow \mathsf{CTR}[E](K_{\mathsf{bc}},N,C)$; $T^{\dagger} \leftarrow \mathsf{CTRAE}_{\mathsf{TGen}}[\Psi_{\mathsf{tag}}](K_{\mathsf{tag}},N,A,C)$
  $T \leftarrow \mathsf{F}_{\mathsf{CTX}}(K,N,A,T^{\dagger})$; if $T = T'$ then return $M$; else return $\perp$ end if
```

Proposition 2. *For each of* $\Pi \in \{\mathsf{GCM},\mathsf{GCM\text{-}SIV},\mathsf{GCM\text{-}C1},\mathsf{GCM\text{-}SIV\text{-}C1}\}$*, there exists a RDD function* $\mathsf{F}_{\mathit{rdd}}$*, a* (ω,n)*-mixing function* $\mathsf{P}_{\mathit{mix}}$*, and an adversary* $\mathbf{A}$ *making* $(\omega+1)$ *queries to an IC such that* $\mathbf{Adv}^{\mathsf{cmt\text{-}3}}_{\Pi^{\mathsf{F}_{\mathit{rdd}},\mathsf{P}_{\mathit{mix}}}}(\mathbf{A}) = 1$.

Proof (Outline). We consider the RDD function $\mathsf{F}_{\mathsf{rdd}}$ that is independent of AD, i.e., $\forall(K,N) \in \mathcal{K} \times \mathcal{N}, (A^{\dagger},A^{\ddagger}) \in \mathcal{A}^2 : \mathsf{F}_{\mathsf{rdd}}(K,N,A^{\dagger}) = \mathsf{F}_{\mathsf{rdd}}(K,N,A^{\ddagger})$. For $\mathsf{CTRAE}_{\mathsf{TGen}}$ (resp. $\mathsf{CTRSIV}_{\mathsf{TGen}}$), if a collision of the tag-generation function $\mathsf{CTRAE}_{\mathsf{TGen}}$ (resp. $\mathsf{CTRSIV}_{\mathsf{TGen}}$) is found such that the AD values are distinct, the tuples of key, nonce, and ciphertext (resp. plaintext) are the same, and the plaintext redundancy is included, then the **CMT**-3 security of CTRAE (resp. CTRSIV) is broken, since CTR does not take AD. When using GHASH as an underlying hash function, the linearity of GHASH offers a tag collision with a constant complexity, breaking the **CMT**-3 security of CTRAE and CTRSIV, i.e., GCM, GCM-SIV, GCM-C1, and GCM-SIV-C1. The formal proof is given in Supporting Material C. □

4.4 CTX and Its Limitation with Plaintext Redundancy

CTX [6] converts AE schemes, except for SIV-based ones, to **CMT**-4-secure AE schemes by adding a hash function $\mathsf{F}_{\mathsf{CTX}} : \mathcal{K} \times \{0,1\}^{\nu} \times \mathcal{A} \times \{0,1\}^{t} \rightarrow \{0,1\}^{t'}$ that on an input tuple (K,N,A,T') of a key, nonce, AD, and tag (of the underlying AE), generates a t'-bit tag. CTX ensures that the AE schemes with CTX are **CMT**-4 secure as long as $\mathsf{F}_{\mathsf{CTX}}$ is collision resistant. The specification of CTRAE with CTX is given in Algorithm 9.

However, the following proposition shows that plaintext redundancy does not enhance the **CMT**-3 security of CTRAE with CTX.

Proposition 3. *Let* $\Pi^* := \mathit{CTX}[\mathsf{CTRAE}^{\mathsf{F}_{\mathit{rdd}},\mathsf{P}_{\mathit{mix}}}]$*. Assume that the tag-generation function* $\mathsf{CTRAE}_{\mathsf{TGen}}[\Psi_{\mathsf{tag}}]$ *is an RO. Then, there exists a RDD function* $\mathsf{F}_{\mathit{rdd}}$*, a mixing function* $\mathsf{P}_{\mathit{mix}}$*, and an adversary* $\mathbf{A}$ *breaking the* **CMT**-3*-security of* Π^* *such that the number of queries to an RO is* p *and* $\mathbf{Adv}^{\mathsf{cmt\text{-}3}}_{\Pi^*}(\mathbf{A}) = O\left(\frac{p^2}{2^{t'}}\right)$.

Proof (Outline). The attack finds a collision by the birthday attack on the hash function $\mathsf{F}_{\mathsf{CTX}}$ with distinct AD, breaking the **CMT**-3 security of CTRAE with CTX and with plaintext redundancy as CTR is independent of AD. By the birthday analysis, the collision probability is $O\left(\frac{p^2}{2^{t'}}\right)$. The formal proof is given in Supporting Material D. □

Algorithm 10 HtE

```
Encryption $\mathsf{HtE}[\mathit{\Pi}_{\mathsf{Enc}}](K, N, A, M)$
 1: $L \leftarrow \mathsf{F}_{\mathsf{HtE}}(K, N, A)$; $(C, T) \leftarrow \mathit{\Pi}_{\mathsf{Enc}}(L, N, \varepsilon, M)$; return $(C, T)$

Decryption $\mathsf{HtE}[\mathit{\Pi}].\mathsf{Dec}(K, N, A, C, T')$
 1: $L \leftarrow \mathsf{F}_{\mathsf{HtE}}(K, N, A)$; $M \leftarrow \mathit{\Pi}_{\mathsf{Dec}}(L, N, \varepsilon, C, T')$; return $M$
```

4.5 HtE and Its Limitation with Plaintext Redundancy

HtE [4] converts a **CMT**-1-secure AE to a **CMT**-4-secure one by adding a key-derivation function $\mathsf{F}_{\mathsf{HtE}}$ that on an input tuple of a key, nonce, and AD, returns a temporary key of the underlying AE. Let κ be the key length of the underlying AE. In this conversion, there is a security loss by the birthday bound for the output length of $\mathsf{F}_{\mathsf{HtE}}$. The specification of HtE is given in Algorithm 10.

The following proposition shows that HtE does not enhance the committing security of any AE scheme with a plaintext redundancy when κ is small, e.g., $\kappa = n$.

Proposition 4. *Assume that $\mathsf{F}_{\mathsf{HtE}}$ is an RO. For any AE scheme $\mathit{\Pi}$, RDD function $\mathsf{F}_{\mathsf{rdd}}$, and mixing function $\mathsf{P}_{\mathsf{mix}}$, there exists an adversary $\mathbf{A}$ on $\mathsf{HtE}[\mathit{\Pi}^{\mathsf{F}_{\mathsf{rdd}}, \mathsf{P}_{\mathsf{mix}}}]$ making p queries to $\mathsf{F}_{\mathsf{HtE}}$ such that $\mathbf{Adv}^{\mathsf{cmt\text{-}3}}_{\mathsf{HtE}[\mathit{\Pi}^{\mathsf{F}_{\mathsf{rdd}}, \mathsf{P}_{\mathsf{mix}}}]}(\mathbf{A}) = O\left(\frac{p^2}{2^\kappa}\right)$.*

Proof (Outline). The attack uses the property that a collision of $\mathsf{F}_{\mathsf{HtE}}$ yields a collision of an AE scheme with HtE. The formal proof is given in Supporting Material E. □

5 KIVR Transform

The previous section shows that plaintext redundancy do not enhance the committing security of AE schemes with CTX or HtE. In this section, we present KIVR, a generalization of HtE that enhances the committing security by using plaintext redundancy. KIVR, on an input tuple of a key, nonce, and AD, generates a temporary key, a temporary nonce, and a mask value are generated by using a hash function $\mathsf{F}_{\mathsf{KIVR}}$. The mask value is applied to redundant data.

5.1 Specification of KIVR

The specification of KIVR with an AE scheme $\mathit{\Pi}$, an RDD function $\mathsf{F}_{\mathsf{rdd}}$, and a mixing function $\mathsf{P}_{\mathsf{mix}}$ is given in Algorithm 11 and Fig. 1. Let $\mathit{\Psi}$ (resp. $\mathit{\Psi}_{\mathsf{KIVR}}$) be the underlying primitive of $\mathit{\Pi}$ (resp. $\mathsf{F}_{\mathsf{KIVR}}$). Let r_{T} be the length of the mask values defined by $\mathsf{F}_{\mathsf{KIVR}}$. Let $\mathsf{F}_{\mathsf{KIVR}} : \mathcal{K} \times \mathcal{N} \times \mathcal{A} \rightarrow \mathcal{K} \times \{0,1\}^\nu \times \{0,1\}^{r_{\mathsf{T}}}$ be a function of KIVR that on an input tuple (K, N, A) of a key, nonce, and AD, derives a tuple $(K_{\mathsf{T}}, IV_{\mathsf{T}}, R_{\mathsf{T}})$ of a temporary key, an IV (or nonce), and a mask value. For CTRAE and CTRSIV, let $K_{\mathsf{T}} := (K_{\mathsf{bcT}}, K_{\mathsf{tagT}})$. K_{bcT} is the temporary key of CTR, and K_{tagT} is the temporary key of the tag-generation function.

Hereafter, we use the following notations.

Algorithm 11 KIVR Transform

```
Encryption $\mathsf{KIVR}[\Pi_{\mathsf{Enc}}^{\mathsf{F}_{\mathsf{rdd}},\mathsf{P}_{\mathsf{mix}}}][\Psi,\Psi_{\mathsf{KIVR}}](K,N,A,M)$
    $R \leftarrow \mathsf{F}_{\mathsf{rdd}}(K,N,A)$; $(K_{\mathsf{T}},IV_{\mathsf{T}},R_{\mathsf{T}}) \leftarrow \mathsf{F}_{\mathsf{KIVR}}[\Psi_{\mathsf{KIVR}}](K,N,A)$; $R \leftarrow R \oplus (R_{\mathsf{T}} \| 0^{r-r_{\mathsf{T}}})$
    $(C,T) \leftarrow \Pi_{\mathsf{Enc}}[\Psi](K_{\mathsf{T}},IV_{\mathsf{T}},\varepsilon,\mathsf{P}_{\mathsf{mix}}(R\|M))$; return $(C,T)$

Decryption $\mathsf{KIVR}[\Pi_{\mathsf{Dec}}^{\mathsf{F}_{\mathsf{rdd}},\mathsf{P}_{\mathsf{mix}}}][\Psi,\Psi_{\mathsf{KIVR}}](K,N,A,C,T')$
    $(K_{\mathsf{T}},IV_{\mathsf{T}},R_{\mathsf{T}}) \leftarrow \mathsf{F}_{\mathsf{KIVR}}[\Psi_{\mathsf{KIVR}}](K,N,A)$; $R \leftarrow \mathsf{F}_{\mathsf{rdd}}(K,N,A)$; $R \leftarrow R \oplus (R_{\mathsf{T}} \| 0^{r-r_{\mathsf{T}}})$
    $M' \leftarrow \Pi_{\mathsf{Dec}}[\Psi](K_{\mathsf{T}},IV_{\mathsf{T}},\varepsilon,C,T')$ if $M^* =$ reject then return reject end if
    $M'' \leftarrow \mathsf{P}_{\mathsf{mix}}^{-1}(M')$; $M \leftarrow \mathsf{lsb}_{|M''|-r}(M'')$;
    if $R = \mathsf{lsb}_r(M'')$ then return $M$ else return reject end if
```

- Let $\mathsf{KIVR}[\Pi_{\mathsf{TGen}}^{\mathsf{F}_{\mathsf{rdd}},\mathsf{P}_{\mathsf{mix}}}]$ be the tag-generation function of $\mathsf{KIVR}[\Pi^{\mathsf{F}_{\mathsf{rdd}},\mathsf{P}_{\mathsf{mix}}}]$, i.e., Π_{TGen} with $\mathsf{F}_{\mathsf{KIVR}}$, $\mathsf{F}_{\mathsf{rdd}}$, and $\mathsf{P}_{\mathsf{mix}}$, where Π_{TGen} is the tag-generation function of Π.
- Let $\mathsf{F}_{\mathsf{K_{bc}IVR}}$ be a function such that $\mathsf{F}_{\mathsf{K_{bc}IVR}}[\Psi_{\mathsf{KIVR}}](K,N,A) := (K_{\mathsf{bcT}},IV_{\mathsf{T}},R_{\mathsf{T}})$, i.e., $\mathsf{F}_{\mathsf{K_{bc}IVR}}$ returns a tuple of a temporary key used in $\mathsf{CTR}[E]$, IV, and mask value.
- Let $\mathsf{F}_{\mathsf{K_{bc}R}}$ be a function such that $\mathsf{F}_{\mathsf{K_{bc}R}}[\Psi_{\mathsf{KIVR}}](K,N,A) := (K_{\mathsf{bcT}},R_{\mathsf{T}})$, i.e., $\mathsf{F}_{\mathsf{K_{bc}R}}$ returns a tuple of a temporary key used in $\mathsf{CTR}[E]$ and mask value.
- Let $\mathsf{F}_{\mathsf{K_{bc}}}$ be a function such that $\mathsf{F}_{\mathsf{K_{bc}}}[\Psi_{\mathsf{KIVR}}](K,N,A) := K_{\mathsf{bcT}}$, i.e., $\mathsf{F}_{\mathsf{K_{bc}}}$ returns a temporary key used in $\mathsf{CTR}[E]$.
- Let F_{R} be a function such that $\mathsf{F}_{\mathsf{R}}[\Psi_{\mathsf{KIVR}}](K,N,A) := R_{\mathsf{T}}$, i.e., F_{R} returns a mask value.
- Let $\mathsf{F}_{\mathsf{K_{bc}R}}^{\oplus \mathsf{F}_{\mathsf{rdd}}}$ be a function such that $\mathsf{F}_{\mathsf{K_{bc}R}}^{\oplus \mathsf{F}_{\mathsf{rdd}}}[\Psi_{\mathsf{KIVR}}](K,N,A) := (K_{\mathsf{bcT}},R_{\mathsf{T}} \oplus \mathsf{msb}_{r_{\mathsf{T}}}(\mathsf{F}_{\mathsf{rdd}}(K,N,A)))$.
- For $\mathcal{S} := (\{K^{(i)},N^{(i)},A^{(i)},D^{(i)}),(K^{[i]},N^{[i]},A^{[i]},D^{[i]}\})_{i \in \upsilon}$, υ pairs of tuples of a key, a nonce, an AD value, and data, Boolean functions $\mathsf{diff}_{\mathsf{K}}$ and $\mathsf{diff}_{\mathsf{KNA}}$ are defined as follows. Let $\mathcal{S}[i] := \{(K^{(i)},N^{(i)},A^{(i)},D^{(i)}),(K^{[i]},N^{[i]},A^{[i]},D^{[i]})\}$, where $K_{\mathsf{bc}}^{(i)}$ (resp. $K_{\mathsf{bc}}^{[i]}$) is a part of $K^{(i)}$ (resp. $K^{[i]}$).
    - $\mathsf{diff}_{\mathsf{KNA}}(\mathcal{S}) = 1$ if $\forall i \in [\upsilon] : (K^{(i)},N^{(i)},A^{(i)}) \neq (K^{[i]},N^{[i]},A^{[i]})$
      and $\forall i \in [\upsilon], j \in [i-1] : \mathcal{S}[i] \neq \mathcal{S}[j]$;
      $\mathsf{diff}_{\mathsf{KNA}}(\mathcal{S}) = 0$ otherwise.
    - $\mathsf{diff}_{\mathsf{K}}(\mathcal{S}) = 1$ if $\forall i \in [\upsilon] : K_{\mathsf{bc}}^{(i)} \neq K_{\mathsf{bc}}^{[i]}$
      and $\forall i \in [\upsilon], j \in [i-1] : \{K_{\mathsf{bc}}^{(i)},K_{\mathsf{bc}}^{[i]}\} \neq \{K_{\mathsf{bc}}^{(j)},K_{\mathsf{bc}}^{[j]}\}$;
      $\mathsf{diff}_{\mathsf{K}}(\mathcal{S}) = 0$ otherwise.

5.2 Security of KIVR

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

Regarding committing security, in Sections 6 and 7, we show that KIVR with plaintext redundancy enhances the committing security of GCM and its variants. The security bounds for CTRAE and the special cases GCM, CAU, and $\mathsf{CAU\text{-}C1}$ are given in Section 6. The security bounds for CTRSIV and the special cases $\mathsf{GCM\text{-}SIV}$, $\mathsf{CAU\text{-}SIV}$, and $\mathsf{CAU\text{-}SIV\text{-}C1}$ are given in Section 7.

6 Committing Security of $\mathsf{KIVR}[\mathsf{CTRAE}]$ with Plaintext Redundancy

Let $\mathsf{F}_{\mathsf{rdd}}$ be an RDD function and $\mathsf{P}_{\mathsf{mix}}$ be a (ω, n)-mixing linear function. Let $\ell_{\mathsf{kivr}} := k + \nu + r_{\mathsf{T}}$.

In this section, we first derive the **CMT**-4-security bound of $\mathsf{KIVR}[\mathsf{CTRAE}^{\mathsf{F}_{\mathsf{rdd}},\mathsf{P}_{\mathsf{mix}}}]$ where the tag-generation function $\mathsf{CTRAE}_{\mathsf{TGen}}$ is a black-box. We then apply the **CMT**-4-security bound to $\mathsf{KIVR}[\mathsf{GCM}^{\mathsf{F}_{\mathsf{rdd}},\mathsf{P}_{\mathsf{mix}}}]$ and $\mathsf{KIVR}[\mathsf{CAU\text{-}C1}^{\mathsf{F}_{\mathsf{rdd}},\mathsf{P}_{\mathsf{mix}}}]$. We assume that the underlying primitives E, Ψ_{tag}, and Ψ_{KIVR} are ideal.

6.1 CMT-4-Security of $\mathsf{KIVR}[\mathsf{CTRAE}^{\mathsf{F}_{\mathsf{rdd}},\mathsf{P}_{\mathsf{mix}}}]$

Main Theorem. The following theorem shows an upper-bound of the **CMT**-4-security of $\mathsf{KIVR}[\mathsf{CTRAE}^{\mathsf{F}_{\mathsf{rdd}},\mathsf{P}_{\mathsf{mix}}}]$.

Theorem 1. *Let* $\Pi^* := \mathit{KIVR}[\mathsf{CTRAE}^{\mathsf{F}_{\mathit{rdd}},\mathsf{P}_{\mathit{mix}}}]$ *and* $\Pi^*_{\mathsf{TGen}} := \mathit{KIVR}[\mathsf{CTRAE}^{\mathsf{F}_{\mathit{rdd}},\mathsf{P}_{\mathit{mix}}}_{\mathsf{TGen}}]$. *For any* **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 exists adversaries* $\mathbf{A}_1$, $\mathbf{A}_2$, *and* $\mathbf{A}_3$ *such that*

$$\mathbf{Adv}^{\mathsf{cmt\text{-}4}}_{\Pi^*}(\mathbf{A}) \le \frac{2^{\omega} \cdot (\upsilon - 1)}{2^r} + \mathbf{Adv}^{\mathsf{colls}}_{\Pi^*_{\mathsf{TGen}},\upsilon}(\mathbf{A}_1) + \mathbf{Adv}^{\mathsf{coll}}_{F_{\mathsf{K}_{\mathsf{bc}}\mathsf{IVR}}}(\mathbf{A}_2) + \mathbf{Adv}^{\mathsf{coll}}_{F^{\oplus \mathsf{F}_{\mathit{rdd}}}_{\mathsf{K}_{\mathsf{bc}}\mathsf{IVR}}}(\mathbf{A}_3)$$

and for the $\mathbf{A}_1$*'s output* $\mathcal{S}_1$, $\mathsf{diff}_{\mathsf{KNA}}(\mathcal{S}_1) = 1$. *For each* $i \in [3]$, $\mathbf{A}_i$ *makes* p_{ic} *queries to* E *or* E^{-1}, p_{tag} *queries to* Ψ_{tag}, *and* p_{kivr} *queries to* Ψ_{KIVR}.

The proof is given in Section 6.4.

Study of Theorem 1. We study the above bound by using ideal functions, that is, $\mathsf{F}_{\mathsf{KIVR}}$ and $\mathsf{CTRAE}_{\mathsf{TGen}}$ are ROs. By the birthday analysis, the collision probability of $\mathsf{CTRAE}_{\mathsf{TGen}}$ is at most $\frac{0.5p_{\mathsf{tag}}^2}{2^t}$, $\mathbf{Adv}^{\mathsf{coll}}_{\mathsf{F}_{\mathsf{K}_{\mathsf{bc}}\mathsf{IVR}}}(\mathbf{A}_2) \le \frac{0.5p_{\mathsf{kivr}}^2}{2^{\ell_{\mathsf{kivr}}}}$, and $\mathbf{Adv}^{\mathsf{coll}}_{\mathsf{F}^{\oplus \mathsf{F}_{\mathsf{rdd}}}_{\mathsf{K}_{\mathsf{bc}}\mathsf{IVR}}}(\mathbf{A}_3) \le \frac{0.5p_{\mathsf{kivr}}^2}{2^{\ell_{\mathsf{kivr}}}}$. By Markov's inequality, we have $\mathbf{Adv}^{\mathsf{colls}}_{\Pi^*_{\mathsf{TGen}},\upsilon}(\mathbf{A}_1) \le \frac{0.5p_{\mathsf{tag}}^2}{\upsilon 2^t}$. Then, we choose υ such that $\frac{2^{\omega}\cdot(\upsilon-1)}{2^r} \simeq \frac{0.5p_{\mathsf{tag}}^2}{\upsilon 2^t}$, i.e., $\upsilon = \frac{p_{\mathsf{tag}}}{2^{\frac{t-r+\omega}{2}}}$, providing the following corollary.

Corollary 1. *Let* $\Pi^* := \mathit{KIVR}[\mathsf{CTRAE}^{\mathsf{F}_{\mathit{rdd}},\mathsf{P}_{\mathit{mix}}}]$ *and* $\Pi^*_{\mathsf{TGen}} := \mathit{KIVR}[\mathsf{CTRAE}^{\mathsf{F}_{\mathit{rdd}},\mathsf{P}_{\mathit{mix}}}_{\mathsf{TGen}}]$. *Assume that* F_{KIVR} *and* $\mathsf{CTRAE}_{\mathsf{TGen}}$ *are ROs. For any* **CMT**-4 *adversary making* p_{ic} *queries to* E *or* E^{-1}, p_{tag} *queries to* $\mathsf{CTRAE}_{\mathsf{TGen}}$, *and* p_{kivr} *queries to* F_{KIVR}, $\mathbf{Adv}^{\mathsf{cmt\text{-}4}}_{\Pi^*}(\mathbf{A}) \le \left(\frac{3\cdot 2^{\omega}\cdot p_{\mathsf{tag}}^2}{2^{r+t}}\right)^{\frac{1}{2}} + \frac{p_{\mathsf{kivr}}^2}{2^{\ell_{\mathsf{kivr}}}}$.

The above bound shows that if 2^{ω} is a constant and $\ell_{\mathsf{kivr}} \geq r + t$, then Π^* is **CMT**-4-secure up to $O(2^{\frac{r+t}{2}})$ query complexity.

6.2 Application to $\mathsf{KIVR}[\mathsf{CAU}^{\mathsf{F_{rdd}},\mathsf{P_{mix}}}]$

Let $\Pi^* := \mathsf{KIVR}[\mathsf{CAU}^{\mathsf{P_{mix}},\mathsf{F_{rdd}}}]$ and $\Pi^*_{\mathsf{TGen}} := \mathsf{KIVR}[\mathsf{CAU}^{\mathsf{F_{rdd}},\mathsf{P_{mix}}}_{\mathsf{TGen}}]$. We first derive the **CMT**-4-security bound of Π^* by using the bound in Theorem 1. Then, we show that the bound is tight.

Upper-Bound. The following bound is obtained by choosing $\upsilon = 0.5p^2_{\mathsf{ic}} + 1$, as $\mathbf{Adv}^{\mathsf{colls}}_{\Pi^*_{\mathsf{TGen}},\upsilon}(\mathbf{A}_1) = 0$.

Corollary 2. *For any* **CMT**-4 *adversary* $\mathbf{A}$ *making* p_{ic} *queries to* E *or* E^{-1}*, and* p_{tag} *queries to* Ψ_{tag}*, there exist adversaries* $\mathbf{A}_2$ *and* $\mathbf{A}_3$ *such that* $\mathbf{Adv}^{\mathsf{cmt\text{-}4}}_{\Pi^*}(\mathbf{A}) \leq \frac{2^{\omega-1}\cdot p^2_{\mathsf{ic}}}{2^r} + \mathbf{Adv}^{\mathsf{coll}}_{F_{\mathsf{K_{bc}IVR}}}(\mathbf{A}_2) + \mathbf{Adv}^{\mathsf{coll}}_{F_{\mathsf{K_{bc}IVR}}^{\oplus \mathsf{F}_{rdd}}}(\mathbf{A}_3)$*, and for* $i \in [2,3]$*,* $\mathbf{A}_i$ *makes* p_{ic} *queries to* E *or* E^{-1}*,* p_{tag} *queries to* Ψ_{tag}*, and* p_{kivr} *queries to* Ψ_{KIVR}*.*

Assume that $t \leq n \leq k$, $\mathsf{F_{KIVR}}$ is an RO and $2^{\omega-1}$ is a small constant. Then, we have $\mathbf{Adv}^{\mathsf{coll}}_{\mathsf{F_{K_{bc}IVR}}}(\mathbf{A}_2) \leq \frac{0.5p^2_{\mathsf{kivr}}}{2^{\ell_{\mathsf{kivr}}}}$ and $\mathbf{Adv}^{\mathsf{coll}}_{\mathsf{F}_{\mathsf{K_{bc}IVR}}^{\oplus \mathsf{F_{rdd}}}}(\mathbf{A}_3) \leq \frac{0.5p^2_{\mathsf{tag}}}{2^{\ell_{\mathsf{kivr}}}}$. Hence, Π^* is **CMT**-4 secure up to $O(\min\{2^{\frac{r}{2}}, 2^{\frac{\ell_{\mathsf{kivr}}}{2}}\})$ query complexity. Assuming $r \geq k + \nu$ and using $\mathsf{F_{KIVR}}$ such that $\ell_{\mathsf{kivr}} \geq r$, the term $2^{\frac{r}{2}}$ becomes dominant.

Tightness. We show that the above bound is tight if the underlying AE scheme is GCM and the underlying function $\mathsf{F_{KIVR}}$ is an RO. The following theorem shows that the **CMT**-1 security of $\mathsf{KIVR}[\mathsf{GCM}^{\mathsf{F_{rdd}},\mathsf{P_{mix}}}]$ is broken with $O(\min\{2^{\frac{r}{2}}, 2^{\frac{k+\nu}{2}}\})$ query complexity, which matches the above bound.

Theorem 2. *Let* $\mathsf{CAU} := \mathsf{GCM}$*, i.e., the hash function of* Π^* *is* GHASH*. Assume that* $\mathsf{F}_{\mathit{KIVR}}$ *is an RO. Then, there exists a RDD function* $\mathsf{F}_{\mathit{rdd}}$*, a* (ω, n)*-mixing linear function* $\mathsf{P}_{\mathit{mix}}$*, and an adversary* $\mathbf{A}$ *making* p *queries to an IC or an RO such that* $\mathbf{Adv}^{\mathsf{cmt\text{-}1}}_{\Pi^*}(\mathbf{A}) = O\left(\min\left\{\frac{p^2}{2^r}, \frac{p^2}{2^{\ell_{\mathsf{kivr}}}}\right\}\right)$.

Proof (Outline). The first bound is obtained by an attack that finds a pair of input tuples of a key, nonce, and AD to CTR such that the key streams satisfy the condition in Lemma 1. Using the pair, one can find plaintexts with a ciphertext collision. 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 using a collision of $\mathsf{F_{KIVR}}$. The formal proof is given in Supporting Material G. □

6.3 Application to $\mathsf{KIVR}[\mathsf{CAU\text{-}C1}^{\mathsf{F_{rdd}},\mathsf{P_{mix}}}]$

Let $\Pi^* := \mathsf{KIVR}[\mathsf{CAU\text{-}C1}^{\mathsf{F_{rdd}},\mathsf{P_{mix}}}]$ and $\Pi^*_{\mathsf{TGen}} := \mathsf{KIVR}[\mathsf{CAU\text{-}C1}^{\mathsf{F_{rdd}},\mathsf{P_{mix}}}_{\mathsf{TGen}}]$. We first derive the **CMT**-4-security bound of Π^* by using the bound in Theorem 1. Then, we show that the bound is tight.

Upper-Bound. We first show an upper-bound of the υ-collision advantage $\mathbf{Adv}^{\mathsf{colls}}_{\Pi^*_{\mathsf{TGen}},\upsilon}(\mathbf{A}_1)$ with $\upsilon = 1$, which is the bound of the probability of finding a collision of Π^*_{TGen} with the condition $\mathsf{diff}_{\mathsf{KNA}}$.

Lemma 2. *Let $\mathcal{S}_1$ be an $\mathbf{A}_1$'s output with pairs of the tuples of a key, a nonce, AD, and a plaintext. For any adversary $\mathbf{A}_1$ making p_{ic} queries to E or E^{-1} and p_{kivr} queries to Ψ_{KIVR} such that $\mathsf{diff}_{\mathsf{KNA}}(\mathcal{S}_1) = 1$, there exists an adversary $\mathbf{A}_{1,1}$ finding a collision of $\mathsf{F}_{\mathsf{K_{bc}}}$ such that $\mathbf{Adv}^{\mathsf{colls}}_{\Pi^*_{\mathsf{TGen}},1}(\mathbf{A}_1) \leq \frac{p_{\mathsf{ic}}^2}{2^t} + \mathbf{Adv}^{\mathsf{coll}}_{\mathsf{F}_{\mathsf{K_{bc}}}}(\mathbf{A}_{1,1})$, and $\mathbf{A}_{1,1}$ makes queries to p_{ic} queries to E or E^{-1}, and p_{kivr} queries to Ψ_{KIVR}.*

Proof. The condition of $\mathsf{diff}_{\mathsf{KNA}}$ ensures that the collision probability is reduced to that of finding a collision of DM (the finalization function of Π^*_{TGen}). Assuming that no collision on $\mathsf{F}_{\mathsf{K_{bc}}}$ occurs which offers the term $\mathbf{Adv}^{\mathsf{coll}}_{\mathsf{F}_{\mathsf{K_{bc}}}}(\mathbf{A}_{1,1})$, inputs to DM are all distinct, and thus by the birthday analysis, the collision probability is at most $\binom{p_{\mathsf{ic}}}{2}\frac{2}{2^t} \leq \frac{p_{\mathsf{ic}}^2}{2^t}$. □

If $\upsilon = 0.5p_{\mathsf{ic}}^2 + 1$, then we have $\mathbf{Adv}^{\mathsf{colls}}_{\Pi^*_{\mathsf{TGen}},\upsilon}(\mathbf{A}_1) = 0$. Hence, putting the parameters $\upsilon = 0.5p_{\mathsf{ic}}^2 + 1, \upsilon = 1$ and the above bound into the one in Theorem 1, we obtain the following bound of the **CMT**-4-security of Π^*.

Corollary 3. *For any **CMT**-4 adversary $\mathbf{A}$ making p_{ic} queries to E or E^{-1}, and p_{kivr} queries to Ψ_{KIVR}, there exist adversaries $\mathbf{A}_{1,1}$, $\mathbf{A}_2$, and $\mathbf{A}_3$ such that*

$$\mathbf{Adv}^{\mathsf{cmt\text{-}4}}_{\Pi^*}(\mathbf{A}) \leq \min\left\{\frac{2^{\omega-1}\cdot p_{\mathsf{ic}}^2}{2^r},\ \frac{p_{\mathsf{ic}}^2}{2^t} + \mathbf{Adv}^{\mathsf{coll}}_{F_{\mathsf{K_{bc}}}}(\mathbf{A}_{1,1})\right\} + \mathbf{Adv}^{\mathsf{coll}}_{F_{\mathsf{K_{bc}IVR}}}(\mathbf{A}_2) + \mathbf{Adv}^{\mathsf{coll}}_{F_{\mathsf{K_{bc}IVR}}^{\oplus \mathsf{F}_{\boldsymbol{rdd}}}}(\mathbf{A}_3)$$

and $\mathbf{A}_{1,1}$, $\mathbf{A}_2$, and $\mathbf{A}_3$ respectively make queries to p_{ic} queries to E or E^{-1} and p_{kivr} queries to Ψ_{KIVR}.

Assume that $t \leq n \leq k$, $\mathsf{F}_{\mathsf{KIVR}}$ is an RO, and $2^{\omega-1}$ is a constant. Then, we have $\mathbf{Adv}^{\mathsf{coll}}_{\mathsf{F}_{\mathsf{K_{bc}}}}(\mathbf{A}_{1,1}) \leq \frac{p^2}{2^k}$, $\mathbf{Adv}^{\mathsf{coll}}_{\mathsf{F}_{\mathsf{K_{bc}IVR}}}(\mathbf{A}_2) \leq \frac{p^2}{2^{\ell_{\mathsf{kivr}}}}$, and $\mathbf{Adv}^{\mathsf{coll}}_{\mathsf{F}_{\mathsf{K_{bc}IVR}}^{\oplus \mathsf{F}_{\mathsf{rdd}}}}(\mathbf{A}_3) \leq \frac{p^2}{2^{\ell_{\mathsf{kivr}}}}$. Thus, Π^* is **CMT**-4 secure up to $O\left(\min\left\{\max\left\{2^{\frac{r}{2}}, 2^{\frac{t}{2}}\right\}, 2^{\frac{\ell_{\mathsf{kivr}}}{2}}\right\}\right)$ query complexity. Choosing r_{T} such that $\ell_{\mathsf{kivr}} \geq r$, the terms $\max\left\{2^{\frac{r}{2}}, 2^{\frac{t}{2}}\right\}$ become dominant.

Tightness. We show that the above bound is tight if the underlying function $\mathsf{F}_{\mathsf{KIVR}}$ is an RO and the hash function is GHASH, i.e., the underlying AE scheme is $\mathsf{GCM\text{-}C1}$. The following theorem shows that the **CMT**-1 security of Π^* with GHASH is broken with $O\left(\max\left\{2^{\frac{r}{2}}, 2^{\frac{t}{2}}\right\}\right)$ query complexity, which matches the above bound.

Theorem 3. *Assume that the hash function of Π^* is GHASH, F_{KIVR} is an RO, and ω is a constant. Then, there exists an RDD function $\mathsf{F}_{\mathit{rdd}}$, a (ω, n)-mixing linear function $\mathsf{P}_{\mathit{mix}}$, and an adversary $\mathbf{A}'$ making p queries to an IC or an RO such that $\mathbf{Adv}^{\mathsf{cmt\text{-}1}}_{\Pi^*}(\mathbf{A}') = O\left(\min\left\{\frac{p^2}{2^r}, 1\right\}\cdot\frac{p^2}{2^t}\right)$.*

Proof (Outline). The adversary first finds a pair of inputs to $\mathsf{CTR}[E]$ such that the key streams satisfy the condition in Lemma 1 (i.e., a ciphertext collision occurs). By the birthday analysis, the probability that the pair is found is $O\left(\frac{p^2}{2^r}\right)$. By the pairs of temporary key and IV that yield a ciphertext collision, the key elements of DM that is the finalization function of Π^*_{TGen} are fixed. Then, by using the linearity of GHASH and ciphertext blocks that are independent of the plaintext redundancy, one can choose any n-bit input block to DM. By the birthday attack, a collision of DM is found with the probability $O\left(\frac{p^2}{2^t}\right)$. Hence, we obtain the lower-bounds in the theorem. The formal proof is given in Supporting Material H. □

6.4 Proof of Theorem 1

We first use the following notations.

- $\Pi^*_{\mathsf{Enc}} := \mathsf{KIVR}[\mathsf{CTRAE}_{\mathsf{Enc}}^{\mathsf{F}_{\mathbf{rdd}},\mathsf{P}_{\mathbf{mix}}}]$
- For an input tuple $(K^\square, N^\square, A^\square, M^\square)$,

  $(C^\square, T^\square) := \Pi^*_{\mathsf{Enc}}[E, \Psi_{\mathsf{tag}}, \Psi_{\mathsf{KIVR}}](K^\square, N^\square, A^\square, M^\square),\ M^{\square *} := \mathsf{P}_{\mathsf{mix}}(R^\square, M^\square),$

  $R^\square := \mathsf{F}_{\mathsf{rdd}}(K^\square, N^\square, A^\square), \quad (K^\square_{\mathsf{bcT}}, IV^\square_{\mathsf{T}}, R^\square_{\mathsf{T}}) := \mathsf{F}_{\mathsf{K_{bc}IVR}}(K^\square, N^\square, A^\square),$

  $KS^\square$ is the key stream of $\mathsf{CTR}[E](K^\square_{\mathsf{T}}, IV^\square_{\mathsf{T}}, M^\square)$.

  In the following proof, the symbol □ is replaced with $(i), \prime, \prime\prime, \dagger$, and $\ddagger$ where i is an integer.
- $\mathcal{I}_{\mathsf{KIVR}}$: the set of all possible input tuples of $\mathsf{F}_{\mathsf{KIVR}}[\Psi_{\mathsf{KIVR}}]$ derived from query-response tuples of Ψ_{KIVR}.
- $\mathcal{I}_{\mathsf{TGen}}$: the set of all possible input tuples of Π^*_{TGen} derived from query-response tuples of Ψ_{tag} and Ψ_{KIVR}.
- $(K^\dagger, N^\dagger, A^\dagger, M^\dagger)$, $(K^\ddagger, N^\ddagger, A^\ddagger, M^\ddagger)$: $\mathbf{A}$'s outputs.

In this proof, we evaluate the **CMT**-3-security advantage of $\mathbf{A}$ for Π^*: $\mathbf{Adv}^{\mathsf{cmt\text{-}3}}_{\Pi^*}(\mathbf{A}) = \Pr[(C^\dagger, T^\dagger) = (C^\ddagger, T^\ddagger)]$, as **CMT**-3-security and **CMT**-4-security are equivalent [4].

We next define the following collision event for $\mathsf{F}_{\mathsf{KIVR}}$:

- coll_2: $\exists X, X' \in \mathcal{I}_{\mathsf{KIVR}}$ s.t. $X \neq X' \wedge \mathsf{F}_{\mathsf{K_{bc}IVR}}(X) = \mathsf{F}_{\mathsf{K_{bc}IVR}}(X')$.
- coll_3: $\exists X, X' \in \mathcal{I}_{\mathsf{KIVR}}$ s.t. $X \neq X' \wedge \mathsf{F}^{\oplus \mathsf{F}_{\mathbf{rdd}}}_{\mathsf{K_{bc}IVR}}(X) = \mathsf{F}^{\oplus \mathsf{F}_{\mathbf{rdd}}}_{\mathsf{K_{bc}IVR}}(X')$.

Let $\mathsf{coll} := \mathsf{coll}_2 \vee \mathsf{coll}_3$. Using the events, we have

$$\mathbf{Adv}^{\mathsf{cmt\text{-}3}}_{\Pi^*}(\mathbf{A}) \leq \Pr[\mathsf{coll}_2] + \Pr[\mathsf{coll}_3] + \Pr[(C^\dagger, T^\dagger) = (C^\ddagger, T^\ddagger) \wedge \neg\mathsf{coll}] \ .$$

These bounds are given in Eqs. (1) and (2), providing the bound in Theorem 1.

Bounds of Pr[coll_2] and of Pr[coll_3]. The event coll_2 (resp. coll_3) implies that there exists an adversary $\mathbf{A}_2$ (resp. $\mathbf{A}_3$) finding a collision of $\mathsf{F}_{\mathsf{K_{bc}IVR}}$ (resp. $\mathsf{F}^{\oplus \mathsf{F}_{\mathbf{rdd}}}_{\mathsf{K_{bc}IVR}}$). We thus have

$$\Pr[\mathsf{coll}_1] \leq \mathbf{Adv}^{\mathsf{coll}}_{\mathsf{F}_{\mathsf{K_{bc}IVR}}}(\mathbf{A}_2) \text{ and } \Pr[\mathsf{coll}_2] \leq \mathbf{Adv}^{\mathsf{coll}}_{\mathsf{F}^{\oplus \mathsf{F}_{\mathbf{rdd}}}_{\mathsf{K_{bc}IVR}}}(\mathbf{A}_3) \ . \qquad (1)$$

Bound of $\Pr[(C^\dagger, T^\dagger) = (C^\ddagger, T^\ddagger) \wedge \neg\mathsf{coll}]$. We evaluate the probability $\Pr[(C^\dagger, T^\dagger) = (C^\ddagger, T^\ddagger) \wedge \neg\mathsf{coll}]$. We consider the following event.[6]

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

Using the event, we have

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

Regarding $\Pr[\mathsf{colls}]$, colls implies that there exists an adversary $\mathbf{A}_1$ finding υ-collisions of Π^*_{TGen} with the condition of $\mathsf{diff}_{\mathsf{KNA}}$. We thus have $\Pr[\mathsf{colls}] \le \mathbf{Adv}^{\mathsf{colls}}_{\Pi^*_{\mathsf{TGen}},\upsilon}(\mathbf{A}_1)$.

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

$$C^\dagger = C^\ddagger \Rightarrow \mathsf{msb}_r\left(\mathsf{P}^{-1}_{\mathsf{mix}}\left(KS^\dagger \oplus KS^\ddagger\right)\right) = (R^\dagger \oplus \mathsf{zp}_r(R^\dagger_{\mathsf{T}})) \oplus (R^\ddagger \oplus \mathsf{zp}_r(R^\ddagger_{\mathsf{T}})),$$

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 $\upsilon - 1$ pairs of tuple of key, nonce, and AD with which tag collisions occur. 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.

- If $(K'_{\mathsf{bcT}}, IV'_{\mathsf{T}}) = (K''_{\mathsf{bcT}}, IV''_{\mathsf{T}})$, then $KS' = KS''$ but $R' \oplus R'_{\mathsf{T}} \neq R'' \oplus R''_{\mathsf{T}}$. Hence, we have

  $$\begin{aligned}&\Pr[C' = C''] \\ &\le \Pr\left[\mathsf{msb}_r\left(\mathsf{P}^{-1}_{\mathsf{mix}}\left(KS' \oplus KS''\right)\right) = (R' \oplus \mathsf{zp}_r(R'_{\mathsf{T}})) \oplus (R'' \oplus \mathsf{zp}_r(R''_{\mathsf{T}}))\right] = 0 \ .\end{aligned}$$

- 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 $j \in \{0,1\}^c$,

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

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

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

[6] The event implies that υ-collisions of Π^*_{TGen} occur such that for each of the υ-collision input pairs, the tuples of key, nonce, and AD are distinct, and any of the υ pairs is distinct from the other pairs.

As the number of key streams is at most p_{ic}, the probability that for some of the $(\upsilon{-}1)$ pairs, the key streams KS' and KS'' satisfy the relation $\mathsf{msb}_r\left(\mathsf{P}_{\mathsf{mix}}^{-1}\left(KS' \oplus KS''\right)\right) = (R' \oplus \mathsf{zp}_r(R'_{\mathsf{T}})) \oplus (R'' \oplus \mathsf{zp}_r(R''_{\mathsf{T}}))$ is at most $(\upsilon - 1) \cdot \frac{2^\omega}{2^r}$, i.e.,

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

Using these bounds, we have

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

7 Committing Security of $\mathsf{KIVR}[\mathsf{CTRSIV}]$ with Plaintext Redundancy

Let $\mathsf{F}_{\mathsf{rdd}}$ be an RDD function and $\mathsf{P}_{\mathsf{mix}}$ be a (ω, n)-mixing linear function. Let $\ell_{\mathsf{kivr}} := k + n + r_{\mathsf{T}}$.

We first derive the **CMT**-4-security bound of $\mathsf{KIVR}[\mathsf{CTRSIV}^{\mathsf{F}_{\mathsf{rdd}},\mathsf{P}_{\mathsf{mix}}}]$ where the tag-generation function $\mathsf{CTRSIV}_{\mathsf{TGen}}$ is a black-box. We then apply the **CMT**-4-security bound to $\mathsf{KIVR}[\mathsf{CAU\text{-}SIV}^{\mathsf{F}_{\mathsf{rdd}},\mathsf{P}_{\mathsf{mix}}}]$ and (a variant of) $\mathsf{KIVR}[\mathsf{CAU\text{-}SIV\text{-}C1}^{\mathsf{F}_{\mathsf{rdd}},\mathsf{P}_{\mathsf{mix}}}]$. We assume that the underlying primitives E, Ψ_{tag}, and Ψ_{KIVR} are ideal.

7.1 CMT-4-Security of $\mathsf{KIVR}[\mathsf{CTRSIV}^{\mathsf{F}_{\mathsf{rdd}},\mathsf{P}_{\mathsf{mix}}}]$

Main Theorem. Let $\Pi^* := \mathsf{KIVR}[\mathsf{CTRSIV}^{\mathsf{F}_{\mathsf{rdd}},\mathsf{P}_{\mathsf{mix}}}]$ and $\Pi^*_{\mathsf{TGen}} := \mathsf{KIVR}[\mathsf{CTRSIV}^{\mathsf{F}_{\mathsf{rdd}},\mathsf{P}_{\mathsf{mix}}}_{\mathsf{TGen}}]$. The following theorem shows an upper-bound of the **CMT**-4-security of Π^*.

Theorem 4. *For any $\mathsf{F}_{\mathit{rdd}}, \mathsf{P}_{\mathit{mix}}$, 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 exists adversaries $\mathbf{A}_1$, $\mathbf{A}_2$, and $\mathbf{A}_3$ such that*

$$\begin{aligned}\mathbf{Adv}^{\mathsf{cmt}\text{-}4}_{\Pi^*}(\mathbf{A}) \leq \frac{2^\omega \cdot (\upsilon - 1)}{2^r} &+ \mathbf{Adv}^{\mathsf{colls}}_{\Pi^*_{\mathsf{TGen}},\upsilon}(\mathbf{A}_1) \\ &+ \mathbf{Adv}^{\mathsf{coll}}_{F_{\mathsf{K}_{\mathsf{bc}}\mathsf{R}}^{\oplus \mathsf{F}_{\mathit{rdd}}}}(\mathbf{A}_2) + \mathbf{Adv}^{\mathsf{coll}}_{F_{\mathsf{K}_{\mathsf{bc}}\mathsf{R}}}(\mathbf{A}_3) \ ,\end{aligned}$$

the $\mathbf{A}_1$'s output $\mathcal{S}_1$ is such that $\mathsf{diff}_{\mathsf{K}}(\mathcal{S}_1) = 1$, and for each $i \in [3]$, $\mathbf{A}_i$ makes p_{ic} queries to E or E^{-1}, p_{tag} queries to Ψ_{tag}, and p_{kivr} queries to Ψ_{KIVR}.

The proof is given in Section 7.4.

Study of Theorem 4. We study the above bound by using ideal functions, that is, $\mathsf{F}_{\mathsf{KIVR}}$ and $\mathsf{CTRAE}_{\mathsf{TGen}}$ are ROs. By the birthday analysis, we have $\mathbf{Adv}^{\mathsf{coll}}_{\mathsf{F}_{\mathsf{K}_{\mathsf{bc}}\mathsf{R}}^{\oplus \mathsf{F}_{\mathsf{rdd}}}}(\mathbf{A}_2) \leq \frac{0.5p^2_{\mathsf{kivr}}}{2^{k+r_{\mathsf{T}}}}$ and $\mathbf{Adv}^{\mathsf{coll}}_{\mathsf{F}_{\mathsf{K}_{\mathsf{bc}}\mathsf{R}}}(\mathbf{A}_3) \leq \frac{0.5p^2_{\mathsf{kivr}}}{2^{k+r_{\mathsf{T}}}}$. The probability that a collision of Π^* occurs is at most $\frac{0.5p^2_{\mathsf{tag}}}{2^n}$, and by using Markov's inequality, we have $\mathbf{Adv}^{\mathsf{colls}}_{\Pi_{\mathsf{TGen}},\upsilon}(\mathbf{A}_1) \leq \frac{0.5p^2_{\mathsf{tag}}}{\upsilon 2^n}$. Then we choose υ such that $\frac{2^\omega \cdot (\upsilon - 1)}{2^r} \simeq \frac{0.5p^2_{\mathsf{tag}}}{\upsilon 2^n}$, i.e., $\upsilon = \frac{p_{\mathsf{tag}}}{2^{\frac{n-r+\omega}{2}}}$, providing the following corollary.

Corollary 4. *Let* $\mathsf{F}_{\mathit{rdd}}$ *be a RDD function and* $\mathsf{P}_{\mathit{mix}}$ *a* (ω, n)*-mixing linear function. Assume that* $\mathsf{CTRSIV}_{\mathsf{TGen}}$ *and* F_{KIVR} *are ROs. For any* **CMT**-4 *adversary making* p_{ic} *queries to* E *or* E^{-1}*,* p_{tag} *queries to* $\mathsf{CTRAE}_{\mathsf{TGen}}$*, and* p_{kivr} *queries to* F_{KIVR}*,* $\mathbf{Adv}^{\mathsf{cmt}\text{-}4}_{\Pi^*]}(\mathbf{A}) \leq \left(\frac{3 \cdot 2^{\omega} \cdot p_{\mathsf{tag}}^2}{2^{r+n}}\right)^{\frac{1}{2}} + \frac{p_{\mathsf{kivr}}^2}{2^{k+r_{\mathsf{T}}}}$.

The above bound shows that if 2^{ω} is a constant, then $\mathsf{KIVR}[\mathsf{CTRSIV}^{\mathsf{F}_{\mathsf{rdd}}, \mathsf{P}_{\mathsf{mix}}}]$ is **CMT**-4-secure up to $O(\min\{2^{\frac{r+n}{2}}, 2^{\frac{k+r_{\mathsf{T}}}{2}}\})$ query complexity. Choosing the parameter r_{T} such that $k + r_{\mathsf{T}} \geq r + n$, $\mathsf{KIVR}[\mathsf{CTRSIV}^{\mathsf{F}_{\mathsf{rdd}}, \mathsf{P}_{\mathsf{mix}}}]$ is **CMT**-4-secure up to $O(2^{\frac{r+n}{2}})$ query complexity.

7.2 Application to $\mathsf{KIVR}[\mathsf{GCM\text{-}SIV}^{\mathsf{F}_{\mathsf{rdd}}, \mathsf{P}_{\mathsf{mix}}}]$

Let $\Pi^* := \mathsf{KIVR}[\mathsf{GCM\text{-}SIV}^{\mathsf{F}_{\mathsf{rdd}}, \mathsf{P}_{\mathsf{mix}}}]$. We first derive the **CMT**-4-security bound of Π^* by using the bound in Theorem 4. Then, we show that the bound is tight.

Upper-Bound. When the number of queries to an IC is p_{ic}, the number of pairs in $\mathbf{A}_1$'s outputs is at most $\binom{p_{\mathsf{ic}}}{2} \leq \frac{0.5 p_{\mathsf{ic}}^2}{2}$. Choosing $\upsilon := \frac{0.5 p_{\mathsf{ic}}^2}{2} + 1$, we have $\mathbf{Adv}^{\mathsf{colls}}_{\Pi_{\mathsf{TGen}}, \upsilon}(\mathbf{A}_1) = 0$. We then obtain the following corollary.

Corollary 5. *For any* **CMT**-4 *adversary making* p_{ic} *queries to* E *or* E^{-1}*, and* p_{kivr} *queries to* Ψ_{KIVR}*, there exists adversaries* $\mathbf{A}_2$ *and* $\mathbf{A}_3$ *such that* $\mathbf{Adv}^{\mathsf{cmt}\text{-}4}_{\Pi^*}(\mathbf{A}) \leq \frac{2^{\omega-1} \cdot p_{\mathsf{ic}}^2}{2^r} + \mathbf{Adv}^{\mathsf{coll}}_{F^{\oplus \mathsf{F}_{\mathit{rdd}}}_{\mathsf{K}_{\mathsf{bc}}\mathsf{R}}}(\mathbf{A}_2) + \mathbf{Adv}^{\mathsf{coll}}_{F_{\mathsf{K}_{\mathsf{bc}}\mathsf{IVR}}}(\mathbf{A}_3)$*, and* $\mathbf{A}_2$ *and* $\mathbf{A}_3$ *respectively make* p_{ic} *queries to* E *or* E^{-1}*,* p_{tag} *queries to* Ψ_{tag}*, and* p_{kivr} *queries to* Ψ_{KIVR}.

Assume that $\mathsf{F}_{\mathsf{KIVR}}$ is an RO and 2^{ω} is a constant. Then, by the birthday analysis, we have $\mathbf{Adv}^{\mathsf{coll}}_{\mathsf{F}^{\oplus \mathsf{F}_{\mathsf{rdd}}}_{\mathsf{K}_{\mathsf{bc}}\mathsf{R}}}(\mathbf{A}_2) \leq \frac{0.5 p_{\mathsf{kivr}}^2}{2^{k+r_{\mathsf{T}}}}$ and $\mathbf{Adv}^{\mathsf{coll}}_{\mathsf{F}_{\mathsf{K}_{\mathsf{bc}}\mathsf{R}}}(\mathbf{A}_3) \leq \frac{0.5 p_{\mathsf{kivr}}^2}{2^{k+r_{\mathsf{T}}}}$. Hence, Π^* is **CMT**-4 secure up to $O(2^{\min\{\frac{r}{2}, \frac{k+r_{\mathsf{T}}}{2}\}})$ query complexity. Choosing the parameter r_{T} such that $r \leq r_{\mathsf{T}} + k$, the bound becomes $O(2^{\frac{r}{2}})$.

Tightness. We show that the above bound is tight, assuming the underlying hash function of Π^* is GHASH and $\mathsf{F}_{\mathsf{KIVR}}$ is an RO. The following theorem shows that the **CMT**-1 security of $\mathsf{KIVR}[\mathsf{GCM\text{-}SIV}^{\mathsf{F}_{\mathsf{rdd}}, \mathsf{P}_{\mathsf{mix}}}]$ is broken with $O(2^{\frac{r}{2}})$ query complexity, which matches the above bound with $r \leq r_{\mathsf{T}} + k$. Note that showing the tightness for $r < n/2$ is an open problem.

Theorem 5. *Let the underlying hash function of* Π^* *is* GHASH*. Assume that* E *is an IC and* F_{KIVR} *is a random oracle. There exists* $\mathsf{F}_{\mathit{rdd}}$*,* $\mathsf{P}_{\mathit{mix}}$*, and an adversary breaking the* **CMT**-1*-security of* Π^* *making* p *queries to* E*,* E^{-1}*,* Ψ_{tag}*, or* F_{KIVR} *such that* $\mathbf{Adv}^{\mathsf{cmt}\text{-}1}_{\Pi^*}(\mathbf{A}) = O\left(\frac{p^2}{2^r}\right)$.

Proof (Outline). The proof is the same as that of Theorem 2. The 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 formal proof is given in Supporting Material I. □

7.3 Application to (Variant of) $\mathsf{KIVR}[\mathsf{CAU\text{-}C1}^{\mathsf{F_{rdd}},\mathsf{P_{mix}}}]$

We apply the bound in Theorem 4 to a variant of GCM-SIV. In CAU-SIV-C1, a temporary key is derived by a key derivation function KD1 taking a pair of key and nonce. Combining CAU-SIV-C1 with KIVR, the temporary key is derived by two function calls $\mathsf{KD1} \circ \mathsf{F_{KIVR}}$, but one of which is redundant. Hence, we consider CAU-SIV-C1 without KD1, which we call CAU-SIV-DM. The key of CAU-SIV-DM is a pair (K_{bc}, L) of BC and hash keys and is directly input to CTR and GMAC2. In $\mathsf{KIVR}[\mathsf{CAU\text{-}SIV\text{-}DM}^{\mathsf{F_{rdd}},\mathsf{P_{mix}}}]$, $\mathsf{F_{KIVR}}$ returns a tuple $((K_{\mathsf{bcT}}, L_{\mathsf{T}}), IV_{\mathsf{T}}, R_{\mathsf{T}})$, and the pair of BC and hash keys $(K_{\mathsf{bcT}}, L_{\mathsf{T}})$ is used instead of (K_{bc}, L).

Let $\Pi^* := \mathsf{KIVR}[\mathsf{CAU\text{-}SIV\text{-}DM}^{\mathsf{F_{rdd}},\mathsf{P_{mix}}}]$. The following corollary shows the **CMT**-4-security bound of Π^* obtained from Theorem 4. Regarding the term $\mathbf{Adv}^{\mathsf{colls}}_{\Pi^*_{\mathsf{TGen}},\upsilon}(\mathbf{A}_1)$ where $\Pi^*_{\mathsf{TGen}} = \mathsf{KIVR}[\mathsf{GMAC2}]$, by the condition of $\mathsf{diff_K}$, the term is upper-bounded by the υ-collision probability of DM in the IC model. The collision probability of DM is at most $\binom{p_{\mathsf{ic}}^2}{2^n}\frac{2}{2^n} \le \frac{p_{\mathsf{ic}}^2}{2^n}$. By Markov's inequality, we have $\mathbf{Adv}^{\mathsf{colls}}_{\mathsf{GMAC2},\upsilon}(\mathbf{A}_1) \le \frac{p_{\mathsf{ic}}^2}{\upsilon 2^n}$. Choosing $\upsilon = \frac{p_{\mathsf{ic}}}{2^{\frac{n-r+\omega}{2}}}$, we obtain the following corollary.

Corollary 6. *Assume that $\mathsf{F_{KIVR}}$ is an RO. Let $\Pi^* := \mathsf{KIVR}[\mathsf{CAU\text{-}SIV\text{-}DM}^{\mathsf{F_{rdd}},\mathsf{P_{mix}}}]$. For any* **CMT**-4 *adversary making p_{ic} queries to E or E^{-1}, and p_{kivr} queries to $\mathsf{F_{KIVR}}$, we have $\mathbf{Adv}^{\mathsf{cmt\text{-}4}}_{\Pi^*}(\mathbf{A}) \le \left(2^{\omega+2} \cdot \frac{p_{\mathsf{ic}}^2}{2^{r+n}}\right)^{\frac{1}{2}} + \mathbf{Adv}^{\mathsf{coll}}_{\mathsf{F_{K_{bc}R}} \oplus \mathsf{F_{rdd}}}(\mathbf{A}_2) + \mathbf{Adv}^{\mathsf{coll}}_{\mathsf{F_{K_{bc}IVR}}}(\mathbf{A}_3)$, and $\mathbf{A}_2$ and $\mathbf{A}_3$ respectively make p_{ic} queries to E or E^{-1}, p_{tag} queries to Ψ_{tag}, and p_{kivr} queries to Ψ_{KIVR}.*

Assume that $\mathsf{F_{KIVR}}$ is an RO and 2^ω is a constant. By the birthday analysis, we have $\mathbf{Adv}^{\mathsf{coll}}_{\mathsf{F_{K_{bc}R}} \oplus \mathsf{F_{rdd}}}(\mathbf{A}_2) \le \frac{0.5p_{\mathsf{kivr}}^2}{2^{k+r_{\mathsf{T}}}}$ and $\mathbf{Adv}^{\mathsf{coll}}_{\mathsf{F_{K_{bc}IVR}}}(\mathbf{A}_3) \le \frac{0.5p_{\mathsf{kivr}}^2}{2^{k+r_{\mathsf{T}}}}$. The above bound shows that Π^* is **CMT**-4-secure up to $O(2^{\min\{\frac{r+n}{2},\frac{r_{\mathsf{T}}+k}{2}\}})$ query complexity. Choosing the parameter r_{T} such that $r+n \le r_{\mathsf{T}}+k$, the bound becomes $O(2^{\frac{r+n}{2}})$.

7.4 Proof of Theorem 4

In this proof, we use the following notations.

- $\Pi^*_{\mathsf{Enc}} := \mathsf{KIVR}[\mathsf{CTRSIV}^{\mathsf{F_{rdd}},\mathsf{P_{mix}}}_{\mathsf{Enc}}]$
- For an input tuple $(K^\square, N^\square, A^\square, M^\square)$,
  - $(C^\square, T^\square) := \Pi^*_{\mathsf{Enc}}[E, \Psi_{\mathsf{tag}}, \Psi_{\mathsf{KIVR}}](K^\square, N^\square, A^\square, M^\square)$,
  - $R^\square := \mathsf{F_{rdd}}(K^\square, N^\square, A^\square)$,
  - $(K^\square_{\mathsf{bcT}}, IV^\square_{\mathsf{T}}, R^\square_{\mathsf{T}}) := \mathsf{F_{K_{bc}IVR}}(K^\square, N^\square, A^\square)$,
  - $M^\square_{\mathsf{T}} := \mathsf{P_{mix}}(\mathsf{zp}_r(R^\square) \oplus R^\square_{\mathsf{T}}, M^\square)$, and
  - $KS^\square$ is the key stream of $\mathsf{CTR}[E](K^\square_{\mathsf{bcT}}, T^\square, M^\square_{\mathsf{T}})$.

  In the following proof, the symbol $\square$ is replaced with $(i), [i], \prime, \prime\prime, \dagger$, and $\ddagger$.
- $\mathcal{I}_{\mathsf{KIVR}}$: the set of all possible input tuples of $\mathsf{F_{KIVR}}[\Psi_{\mathsf{KIVR}}]$ derived from query-response tuples of Ψ_{KIVR}.
- $\mathcal{I}_{\mathsf{TGen}}$: the set of all possible input tuple to Π^*_{TGen} derived from query-response tuples of Ψ_{tag} and Ψ_{KIVR}.

- $(K^\dagger, N^\dagger, A^\dagger, M^\dagger)$, $(K^\ddagger, N^\ddagger, A^\ddagger, M^\ddagger)$: $\mathbf{A}$'s outputs.

In this proof, we evaluate the following probability for the **CMT**-3-security of $\mathit{\Pi}$, as **CMT**-3-security and **CMT**-4-security are equivalent.

$$\mathbf{Adv}^{\mathsf{cmt\text{-}3}}_{\mathit{\Pi}^*}(\mathbf{A}) = \Pr[(C^\dagger, T^\dagger) = (C^\ddagger, T^\ddagger) \text{ s.t. } (K^\dagger, N^\dagger, A^\dagger) \neq (K^\ddagger, N^\ddagger, A^\ddagger)] \ .$$

We next define the following collision event:

- coll_1: $\exists X', X'' \in \mathcal{I}_{\mathsf{KIVR}}$ s.t. $X' \neq X''$ and $\mathsf{F}_{\mathsf{K}_{\mathsf{bc}}\mathsf{R}}(X') = \mathsf{F}_{\mathsf{K}_{\mathsf{bc}}\mathsf{R}}(X'')$.
- coll_2: $\exists X', X'' \in \mathcal{I}_{\mathsf{KIVR}}$ s.t. $X' \neq X''$ and $\mathsf{F}^{\oplus \mathsf{F}_{\mathsf{rdd}}}_{\mathsf{K}_{\mathsf{bc}}\mathsf{R}}(X') = \mathsf{F}^{\oplus \mathsf{F}_{\mathsf{rdd}}}_{\mathsf{K}_{\mathsf{bc}}\mathsf{R}}(X'')$.
- tcolls: $\exists \mathcal{S}_{\mathsf{TGen}} = \big\{\{(K^{(i)}, N^{(i)}, A^{(i)}, M^{(i)}), (K'^{(i)}, N^{[i]}, A^{[i]}, M^{[i]})\} \in (\mathcal{I}_{\mathsf{TGen}})^2 \mid i \in [\upsilon]\big\}$ s.t. $\mathsf{diff}_{\mathsf{K}}(\mathcal{S}_{\mathsf{TGen}}) = 1$ and $\forall i \in [\upsilon] : T^{(i)} = T^{[i]}$.

$\mathsf{bad} := \mathsf{coll}_1 \vee \mathsf{coll}_2 \vee \mathsf{tcolls}$. Using these events, we have

$$\mathbf{Adv}^{\mathsf{cmt\text{-}3}}_{\mathit{\Pi}^*}(\mathbf{A}) \leq \Pr[\mathsf{coll}_1] + \Pr[\mathsf{coll}_2] + \Pr[\mathsf{tcolls}] + \Pr[(C^\dagger, T^\dagger) = (C^\ddagger, T^\ddagger) \wedge \neg\mathsf{bad}] \ .$$

These bounds are given in Eqs. (3), (4), and (5), offering the bound in Theorem 4.

Bounds of Pr[coll_1] and Pr[coll_2]. The event coll_1 (resp. coll_2) implies that there exists an adversary $\mathbf{A}_3$ (resp. $\mathbf{A}_2$) finding a collision of $\mathsf{F}_{\mathsf{K}_{\mathsf{bc}}\mathsf{R}}$ (resp. $\mathsf{F}^{\oplus \mathsf{F}_{\mathsf{rdd}}}_{\mathsf{K}_{\mathsf{bc}}\mathsf{R}}$). We thus have

$$\Pr[\mathsf{coll}_1] \leq \mathbf{Adv}^{\mathsf{coll}}_{\mathsf{F}_{\mathsf{K}_{\mathsf{bc}}\mathsf{R}}}(\mathbf{A}_3) \text{ and } \Pr[\mathsf{coll}_1] \leq \mathbf{Adv}^{\mathsf{coll}}_{\mathsf{F}^{\oplus \mathsf{F}_{\mathsf{rdd}}}_{\mathsf{K}_{\mathsf{bc}}\mathsf{R}}}(\mathbf{A}_2) \ . \tag{3}$$

Bounds of Pr[tcolls]. The event tcolls implies that there exists an adversary $\mathbf{A}_1$ finding υ-collisions of $\mathit{\Pi}^*_{\mathsf{TGen}}$ such that the $\mathbf{A}_1$'s output satisfies the condition of $\mathsf{diff}_{\mathsf{K}}$. We thus have

$$\Pr[\mathsf{tcolls}] \leq \mathbf{Adv}^{\mathsf{colls}}_{\mathit{\Pi}^*_{\mathsf{TGen}},\upsilon}(\mathbf{A}_1) \ . \tag{4}$$

Bound of Pr[$(C^\dagger, T^\dagger) = (C^\ddagger, T^\ddagger) \wedge \neg\mathsf{bad}$]. We first define the following two sub-sets $\mathcal{Q}^{(1)}_{\mathsf{KIVR}} \subseteq (\mathcal{I}_{\mathsf{KIVR}})^2$ and $\mathcal{Q}^{(2)}_{\mathsf{KIVR}} \subseteq (\mathcal{I}_{\mathsf{KIVR}})^2$.

$$\begin{aligned}\mathcal{Q}^{(1)}_{\mathsf{TGen}} := \{\{(K', N', A'), (K'', N'', A'')\} \mid T' = T'' \wedge K'_{\mathsf{bcT}} \neq K''_{\mathsf{bcT}} \wedge \\ \{(K', N', A', M'), (K'', N'', A'', M'')\} \in (\mathcal{I}_{\mathsf{TGen}})^2\}. \\ \mathcal{Q}^{(2)}_{\mathsf{TGen}} := \{\{(K', N', A'), (K'', N'', A'')\} \mid T' = T'' \wedge K'_{\mathsf{bcT}} = K''_{\mathsf{bcT}} \wedge \\ \{(K', N', A', M'), (K'', N'', A'', M'')\} \in (\mathcal{I}_{\mathsf{TGen}})^2\}.\end{aligned}$$

By Lemma 1,

$$C^\dagger = C^\ddagger \Rightarrow \mathsf{Cond}^{\dagger\ddagger} := \Big(\mathsf{msb}_r\left(\mathsf{P}^{-1}_{\mathsf{mix}}\left(KS^\dagger \oplus KS^\ddagger\right)\right) = \mathsf{zp}_r(R^\dagger_{\mathsf{T}} \oplus R^\ddagger_{\mathsf{T}}) \oplus R^\dagger \oplus R^\ddagger\Big) \ .$$

Using these sets and the relation, we have

$$\begin{aligned}
&\Pr[(C^{\dagger}, T^{\dagger}) = (C^{\ddagger}, T^{\ddagger}) \wedge \neg\mathsf{bad}] \\
&\leq \Pr[\mathsf{Cond}^{\dagger\ddagger} \wedge T^{\dagger} = T^{\ddagger} \wedge \neg\mathsf{bad}] \\
&= \Pr[\mathsf{Cond}^{\dagger\ddagger} \wedge (\{(K^{\dagger}, N^{\dagger}, A^{\dagger}), (K^{\ddagger}, N^{\ddagger}, A^{\ddagger})\} \in \mathcal{Q}^{(1)}_{\mathsf{TGen}} \cup \mathcal{Q}^{(2)}_{\mathsf{TGen}}) \wedge \neg\mathsf{bad}] \\
&= \underbrace{\Pr[\mathsf{Cond}^{\dagger\ddagger} \wedge \{(K^{\dagger}, N^{\dagger}, A^{\dagger}), (K^{\ddagger}, N^{\ddagger}, A^{\ddagger})\} \in \mathcal{Q}^{(1)}_{\mathsf{TGen}} \wedge \neg\mathsf{bad}]}_{=:\delta_1} \\
&\quad + \underbrace{\Pr[\mathsf{Cond}^{\dagger\ddagger} \wedge \{(K^{\dagger}, N^{\dagger}, A^{\dagger}), (K^{\ddagger}, N^{\ddagger}, A^{\ddagger})\} \in \mathcal{Q}^{(2)}_{\mathsf{TGen}} \wedge \neg\mathsf{bad}]}_{=:\delta_2} \ .
\end{aligned}$$

The bounds of δ_1 and δ_2 are given in the following.

- Bound of δ_1. For each pair $((K', N', A'), (K'', N'', A'')) \in \mathcal{Q}^{(1)}_{\mathsf{TGen}}$, as $K'_{\mathsf{bcT}} \neq K''_{\mathsf{bcT}}$, KS' and KS'' are independently defined. 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 $j \in \{0,1\}^c$,

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

  By using the bounds, we have

  $$\begin{aligned}
  &\Pr\left[\mathsf{msb}_r\left(\mathsf{P}^{-1}_{\mathsf{mix}}(KS' \oplus KS'')\right) = \mathsf{zp}_r(R'_{\mathsf{T}} \oplus R''_{\mathsf{T}}) \oplus R' \oplus R''\right] \\
  &\leq 2^{\omega n - r} \cdot \left(\frac{2}{2^n}\right)^{\omega} = \frac{2^{\omega}}{2^r} \ .
  \end{aligned}$$

  By $\neg\mathsf{tcolls}$, $|\mathcal{Q}^{(1)}_{\mathsf{KIVR}}| \leq \upsilon - 1$ is satisfied. We thus have $\delta_1 \leq 2^{\omega} \cdot \frac{\upsilon-1}{2^r}$.
- Bound of δ_2. For each pair $\{(K', N', A'), (K'', N'', A'')\} \in \mathcal{Q}^{(2)}_{\mathsf{KIVR}}$, if $KS' = KS''$, then we have $C' = C'' \Rightarrow \mathsf{zp}_r(R'_{\mathsf{T}} \oplus R''_{\mathsf{T}}) \oplus R' \oplus R'' = 0^n$. Hence, we have $\Pr[K'_{\mathsf{bcT}} = K''_{\mathsf{bcT}} \wedge \mathsf{zp}_r(R'_{\mathsf{T}} \oplus R''_{\mathsf{T}}) \oplus R' \oplus R'' = 0^n \mid \neg\mathsf{bad}]$. By $\neg\mathsf{coll}_2$, we have $\delta_2 = 0$.

Using these bounds, we have

$$\Pr[(C^{\dagger}, T^{\dagger}) = (C^{\ddagger}, T^{\ddagger}) \wedge \neg\mathsf{bad}] \leq 2^{\omega} \cdot \frac{\upsilon - 1}{2^r} \ . \qquad (5)$$

8 Further Limitations of HtE with Plaintext Redundancy

In this section, we show that there exist functions $\mathsf{F}_{\mathsf{rdd}}$ and $\mathsf{P}_{\mathsf{mix}}$ with which the **CMT**-1 security of HtE with GCM or its variants is broken.

8.1 Functions for Plaintext Redundancy

We consider the following functions: $\forall(K, N, A, M) \in \mathcal{K} \times \mathcal{N} \times \mathcal{A} \times \mathcal{M}$:

$$\mathsf{F}_{\mathsf{rdd}}(K, N, A) = 0^r \text{ and } \mathsf{P}_{\mathsf{mix}}(0^r \| M) = 0^r \| M. \tag{6}$$

Let $((K^\dagger, N^\dagger, A^\dagger), (K^\ddagger, N^\ddagger, A^\ddagger))$ be a pair of the tuples of a key, nonce, and AD. Let $(KS^\dagger, KS^\ddagger)$ be a pair of key streams of $\mathsf{HtE}[\mathsf{CTR}^{\mathsf{F}_{\mathsf{rdd}}, \mathsf{P}_{\mathsf{mix}}}]$ obtained from the pair. If the key streams $KS^\dagger$ and $KS^\ddagger$ satisfy the following relation:

$$\mathsf{msb}_r\left(KS^\dagger \oplus KS^\ddagger\right) = 0^r, \tag{7}$$

then by choosing plaintexts $M^\dagger$ and $M^\ddagger$ such that $\mathsf{msb}_r(M^\dagger) = \mathsf{msb}_r(M^\ddagger) = 0^r$ and $\mathsf{lsb}_{|M^\dagger|-r}(M^\dagger \oplus KS^\dagger) = \mathsf{msb}_{|M^\dagger|-r}(M^\ddagger \oplus KS^\ddagger)$, we obtain the ciphertext collision $C^\dagger = C^\ddagger$. The following attack uses the property.

8.2 Lower-Bound for $\mathsf{HtE}[\mathsf{GCM}^{\mathsf{F}_{\mathsf{rdd}}, \mathsf{P}_{\mathsf{mix}}}]$

Let $\Pi^* := \mathsf{HtE}[\mathsf{GCM}^{\mathsf{F}_{\mathsf{rdd}}, \mathsf{P}_{\mathsf{mix}}}]$ and $\Pi^*_{\mathsf{TGen}} := \mathsf{HtE}[\mathsf{GMAC}^{\mathsf{F}_{\mathsf{rdd}}, \mathsf{P}_{\mathsf{mix}}}]$. The following proposition shows that the **CMT**-1-security of Π^* is broken by $O\left(2^{\min\{r,k\}/2}\right)$ query complexity.

Proposition 5. *Assume that E is an IC and $\mathsf{F}_{\mathsf{HtE}}$ is an RO. For $\mathsf{F}_{\mathsf{rdd}}$ and $\mathsf{P}_{\mathsf{mix}}$ defined in Eq. (6), there exists an adversary $\mathbf{A}$ making p queries to E, E^{-1}, or $\mathsf{F}_{\mathsf{HtE}}$ such that $\mathbf{Adv}^{\mathsf{cmt}\text{-}1}_{\Pi^*}(\mathbf{A}) = O\left(\max\left\{\frac{p^2}{2^r}, \frac{p^2}{2^k}\right\}\right)$.*

Proof. The first attack is to find a collision of $\mathsf{F}_{\mathsf{HtE}}$ with distinct keys. By the birthday analysis, the collision probability is $O\left(\frac{p^2}{2^k}\right)$. Using the collision, one can break the **CMT**-1 security of $\mathsf{HtE}[\mathsf{GCM}^{\mathsf{F}_{\mathsf{rdd}}, \mathsf{P}_{\mathsf{mix}}}]$. Assume that no collision occurs for $\mathsf{F}_{\mathsf{HtE}}$.

The second attack is the same as the attack in Theorem 2. The attack first finds key streams with the relation in Eq. (7). For a pair of nonce and AD (N, A), if a pair $((K^\dagger, N, A), (K^\ddagger, N, A))$ of the tuples of a key, nonce, and AD such that the relation in Eq. (7) and $K^\dagger \neq K^\ddagger$ are satisfied is found, then one can obtain a collision of ciphertexts. By the birthday attack on the r-bit parts of the key streams, the relation in Eq. (7) is satisfied with the probability $O\left(\frac{p^2}{2^r}\right)$. Then, by using the linearity of GHASH and the invertibility of the finalization function of GMAC, $\mathbf{A}$ can find a ciphertext C that offers a tag collision with $((K^\dagger, N, A), (K^\ddagger, N, A))$. Then, by choosing $M^\dagger := C \oplus KS^\dagger$ and $M^\ddagger := C \oplus KS^\ddagger$, $\mathbf{A}$ can find a pair of tuples $((K^\dagger, N, A, M^\dagger), (K^\ddagger, N, A, M^\ddagger))$ that breaks the **CMT**-1 security of Π^*. Hence, the probability that the **CMT**-1 security of Π^* is broken is $O\left(\frac{p^2}{2^r}\right)$. □

8.3 Lower-Bound for $\mathsf{HtE}[\mathsf{CAU\text{-}C1}^{\mathsf{F_{rdd}},\mathsf{P_{mix}}}]$

We consider $\mathsf{HtE}[\mathsf{CAU\text{-}C1}^{\mathsf{F_{rdd}},\mathsf{P_{mix}}}]$ with GHASH, i.e., $\mathsf{HtE}[\mathsf{GCM\text{-}C1}^{\mathsf{F_{rdd}},\mathsf{P_{mix}}}]$. Let $\Pi^* := \mathsf{HtE}[\mathsf{GCM\text{-}C1}^{\mathsf{F_{rdd}},\mathsf{P_{mix}}}]$ and $\Pi^*_{\mathsf{TGen}} := \mathsf{HtE}[\mathsf{CAU\text{-}C1}^{\mathsf{F_{rdd}},\mathsf{P_{mix}}}_{\mathsf{TGen}}]$ with GHASH. The following proposition shows that the **CMT**-1-security of Π^* is broken by $O\left(2^{\min\{\max\{r,t\},k\}/2}\right)$ query complexity.

Proposition 6. *Assume that E is an encryption of IC and $\mathsf{F_{HtE}}$ is an RO. For F_{rdd} and P_{mix} defined in Eq. (6), there exists an adversary $\mathbf{A}$ making p queries to E, E^{-1}, or $\mathsf{F_{HtE}}$ such that $\mathbf{Adv}^{\mathsf{cmt\text{-}1}}_{\Pi^*}(\mathbf{A}) = O\left(\max\left\{\min\left\{\frac{p^2}{2^r}, 1\right\} \cdot \frac{p^2}{2^t}, \frac{p^2}{2^k}\right\}\right)$.*

Proof. The bound can be obtained by combining the proofs of Proposition 5 and of Theorem 3. The difference from Proposition 5 is non-invertibility of the finalization function of GMAC^+, i.e., DM. As the proof of Theorem 3, due to DM, the probability of finding a tag collision is improved to $O\left(\frac{p^2}{2^t}\right)$. Hence, by multiplying $\min\left\{\frac{p^2}{2^r}, 1\right\}$ by $\frac{p^2}{2^t}$, the collision probability of DM, we obtain the above bound. □

8.4 Lower-Bound for $\mathsf{HtE}[\mathsf{CAU\text{-}SIV}^{\mathsf{F_{rdd}},\mathsf{P_{mix}}}]$

We consider $\mathsf{HtE}[\mathsf{CAU\text{-}SIV}^{\mathsf{F_{rdd}},\mathsf{P_{mix}}}]$ with the hash function GHASH, i.e., $\mathsf{HtE}[\mathsf{GCM\text{-}SIV}^{\mathsf{F_{rdd}},\mathsf{P_{mix}}}]$. Let $\Pi^* := \mathsf{HtE}[\mathsf{GCM\text{-}SIV}^{\mathsf{F_{rdd}},\mathsf{P_{mix}}}]$. The following proposition shows that the **CMT**-1-security of Π^* is broken by $O\left(2^{\max\{r,k\}/2}\right)$ query complexity.

Proposition 7. *Assume that E is an IC and $\mathsf{F_{HtE}}$ is a RO. For F_{rdd} and P_{mix} defined in Eq. (6), there exists an adversary $\mathbf{A}$ making p queries to E, E^{-1}, or $\mathsf{F_{HtE}}$ such that $\mathbf{Adv}^{\mathsf{cmt\text{-}1}}_{\Pi^*}(\mathbf{A}) = O\left(\max\left\{\frac{p^2}{2^r}, \frac{p^2}{2^k}\right\}\right)$.*

Proof. The term $\frac{p^2}{2^k}$ is obtained by a birthday attack on $\mathsf{F_{HtE}}$, since the collision yields a collision of pairs of ciphertext and tag.

The term $\frac{p^2}{2^r}$ is obtained by a birthday attack of finding a pair of key streams with the relation in Eq. (7), which yield a collision of ciphertexts. As the proof of Theorem 5, by using the linearity of GHASH and the invertibility of the finalization function of GMAC, a tag collision is found with the probability 1. □

8.5 Lower-Bound for $\mathsf{HtE}[\mathsf{CAU\text{-}SIV\text{-}C1}^{\mathsf{F_{rdd}},\mathsf{P_{mix}}}]$

We consider $\mathsf{HtE}[\mathsf{CAU\text{-}SIV\text{-}C1}^{\mathsf{F_{rdd}},\mathsf{P_{mix}}}]$ with GHASH, i.e., $\mathsf{HtE}[\mathsf{GCM\text{-}SIV\text{-}C1}^{\mathsf{F_{rdd}},\mathsf{P_{mix}}}]$. Let $\Pi^* := \mathsf{HtE}[\mathsf{GCM\text{-}SIV\text{-}C1}^{\mathsf{F_{rdd}},\mathsf{P_{mix}}}]$. The following proposition shows that the **CMT**-1-security of Π^* is broken by $O\left(2^{\min\{r+n,k\}/2}\right)$ query complexity.

Proposition 8. *Assume that E is an IC and $\mathsf{F_{HtE}}$ is an RO. For F_{rdd} and P_{mix} defined in Eq. (6), there exists an adversary $\mathbf{A}$ making p queries to E, E^{-1}, or $\mathsf{F_{HtE}}$ such that $\mathbf{Adv}^{\mathsf{cmt\text{-}1}}_{\Pi^*}(\mathbf{A}) = O\left(\min\left\{\frac{p^2}{2^{r+n}}, \frac{p^2}{2^k}\right\}\right)$.*

Proof. The term $\frac{p^2}{2^k}$ comes from a collision of $\mathsf{F}_{\mathsf{HtE}}$. The term $\frac{p^2}{2^{r+n}}$ is obtained by the probability of finding pairs of tag and key stream such that the tag collision occurs and the key streams satisfy the relation in Eq. (7). By the birthday analysis, we obtain the term $\frac{p^2}{2^{r+n}}$. □

9 Conclusion

We proposed the KIVR conversion that constructs context-committing AEs satisfying CMT-4 security from CTRAE (resp. CTRSIV), including GCM (resp. GCM-SIV). KIVR achieves BBB security without increasing the ciphertext size by exploiting plaintext redundancy in practical use cases. KIVR uses a collision-resistant hash to convert a tuple of key, 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. KIVR combined with CTRAE (resp. CTRSIV) achieves $\max\{\frac{r}{2}, \mathsf{tag\text{-}col}\}$ (resp. $\frac{r}{2} + \mathsf{tag\text{-}col}$) bits of security wherein r is the number of redundant bits and tag-col is the tag-collision security of the underlying AE. With sufficiently large r, KIVR achieves higher security than the conventional conversions (HtE and CTX) limited by the birthday bounds of the tag and key sizes. There are interesting open research questions. In particular, analyzing/salvaging other popular AEs, including CCM [8] and ChaCha20-Poly1305 [18] for committing security is open for future research.

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. Armknecht, F., Fleischmann, E., Krause, M., Lee, J., Stam, M., Steinberger, J.P.: The preimage security of double-block-length compression functions. In: ASIACRYPT 2011. vol. 7073, pp. 233–251. Springer (2011)
3. Bellare, M., Chan, J., Grubbs, P., Hoang, V.T., Menda, S., Len, J., Ristenpart, T., Rogaway, P.: Ask your cryptographer if context-committing AEAD is right for you. In: Real World Crypto Symposium (RWC) 2023 (2023)
4. Bellare, M., Hoang, V.T.: Efficient schemes for committing authenticated encryption. In: EUROCRYPT 2022. vol. 13276, pp. 845–875 (2022)
5. Bose, P., Hoang, V.T., Tessaro, S.: Revisiting AES-GCM-SIV: multi-user security, faster key derivation, and better bounds. In: EUROCRYPT 2018. vol. 10820, pp. 468–499 (2018)
6. Chan, J., Rogaway, P.: On committing authenticated-encryption. In: ESORICS 2022. vol. 13555, pp. 275–294 (2022)
7. Dodis, Y., Grubbs, P., Ristenpart, T., Woodage, J.: Fast message franking: From invisible salamanders to encryptment. In: CRYPTO 2018. vol. 10991, pp. 155–186. Springer (2018)
8. Dworkin, M.: NIST Special Publication 800-38C: Recommendation for block cipher modes of operation: the CCM mode for authentication and confidentiality. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38c.pdf (2007)

9. Farshim, P., Orlandi, C., Rosie, R.: Security of symmetric primitives under incorrect usage of keys. IACR Trans. Symmetric Cryptol. **2017**(1), 449–473 (2017)
10. Grubbs, P., Lu, J., Ristenpart, T.: Message franking via committing authenticated encryption. In: CRYPTO 2017. pp. 66–97 (2017)
11. Gueron, S., Langley, A., Lindell, Y.: AES-GCM-SIV: nonce misuse-resistant authenticated encryption. RFC **8452**, 1–42 (2019)
12. 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)
13. Günther, F., Thomson, M., Wood, C.A.: Usage limits on AEAD algorithms. https://www.ietf.org/archive/id/draft-irtf-cfrg-aead-limits-06.txt (2023)
14. Hoang, V.T., Tessaro, S., Thiruvengadam, A.: The multi-user security of gcm, revisited: Tight bounds for nonce randomization. In: CCS 2018. pp. 1429–1440. ACM (2018)
15. Kessler, G.C.: GCK's file signatures table (2023), https://www.garykessler.net/library/file_sigs.html, Accessed: 2021-09-05
16. Len, J., Grubbs, P., Ristenpart, T.: Partitioning oracle attacks. In: USENIX Security 2021. pp. 195–212 (2021)
17. Menda, S., Len, J., Grubbs, P., Ristenpart, T.: Context discovery and commitment attacks: How to break CCM, EAX, SIV, and more. Cryptology ePrint Archive, Paper 2023/526 (2023), https://eprint.iacr.org/2023/526
18. Nir, Y., Langley, A.: Chacha20 and poly1305 for IETF protocols. RFC **8439**, 1–46 (2018)
19. NIST: The third NIST workshop on block cipher modes of operation 2023. https://csrc.nist.gov/Events/2023/third-workshop-on-block-cipher-modes-of-operation (2023), accessed: 2023-05-25
20. Rogaway, P., Shrimpton, T.: A Provable-Security Treatment of the Key-Wrap Problem. In: Vaudenay, S. (ed.) EUROCRYPT 2006. LNCS, vol. 4004, pp. 373–390. Springer (2006)
21. Wikipedia: List of file signatures (2023), https://en.wikipedia.org/wiki/List_of_file_signatures, Accessed: 2021-09-05

Supplementary Material

A Multi-User Security for AE

Multi-user-AE ($\mathsf{mu\text{-}AE}$) 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 $\mathsf{mu\text{-}AE}$-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 $\mathsf{mu\text{-}AE}$-security advantage function of $\mathbf{A}$ is defined as

$$\mathbf{Adv}^{\mathsf{mu\text{-}ae}}_{\Pi}(\mathbf{A}) := \Pr\left[\mathbf{A}^{\Pi_{K_1}, \ldots, \Pi_{K_u}} = 1\right] - \Pr\left[\mathbf{A}^{(\$_1, \perp), \ldots, (\$_u, \perp)} = 1\right] .$$

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 $\mathsf{mu\text{-}AE}$ security of KIVR-based schemes relies on multi-user pseudo-random-function ($\mathsf{mu\text{-}PRF}$) 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 $\mathsf{mu\text{-}PRF}$-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 $\mathsf{mu\text{-}PRF}$-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 Proof of Proposition 2

Let $\mathsf{P}_{\mathsf{mix}}$ be any mixing function. Let $\mathsf{F}_{\mathsf{rdd}}$ be an RDD function that is independent of AD, i.e., $\forall (K, N) \in \mathcal{K} \times \mathcal{N}, (A^\dagger, A^\ddagger) \in \mathcal{A}^2 : \mathsf{F}_{\mathsf{rdd}}(K, N, A^\dagger) =$

Algorithm 12 **CMT**-3 Adversary **A** on $\mathsf{GCM}, \mathsf{GCM\text{-}C1}$ with Plaintext Redundancy

```
Choose a pair $(K_{\mathsf{bc}}, N) \in \{0,1\}^k \times \{0,1\}^n \times \{0,1\}^\nu$ of BC's key and nonce
Choose AD $A^\dagger \in \{0,1\}^{2n}$ and a plaintext $M \in \{0,1\}$
$R \leftarrow \mathsf{F}_{\mathsf{rdd}}(K_{\mathsf{bc}}, N, A^\dagger)$; $M^* \leftarrow \mathsf{P}_{\mathsf{mix}}(R\|M)$; $C \leftarrow \mathsf{CTR}[E](K_{\mathsf{bc}}, M^*)$; $L \leftarrow E(K_{\mathsf{bc}}, 0^n)$
Derive AD $A^\ddagger \in \{0,1\}^{2n}$
        such that $A^\dagger \neq A^\ddagger$ and $\mathsf{GHASH}(L, A^\dagger, C) = \mathsf{GHASH}(L, A^\ddagger, C)$
**return** $((K_{\mathsf{bc}}, N, A^\dagger, M), (K_{\mathsf{bc}}, N, A^\ddagger, M))$
```

Algorithm 13 **CMT**-3 Adversary **A** on $\mathsf{GCM\text{-}SIV}, \mathsf{GCM\text{-}SIV\text{-}C1}$ with Plaintext Redundancy

```
Choose a tuple $(K_{\mathsf{bc}}, L, N) \in \{0,1\}^k \times \{0,1\}^n \times \{0,1\}^\nu$ of BC's key, hash key, and
    nonce, AD $A^\dagger \in \{0,1\}^{2n}$, and a plaintext $M \in \{0,1\}$
$R \leftarrow \mathsf{F}_{\mathsf{rdd}}(K, N, A^\dagger)$; $M^* \leftarrow \mathsf{P}_{\mathsf{mix}}(R\|M)$
Derive AD $A^\ddagger \in \{0,1\}^{2n}$
        such that $A^\dagger \neq A^\ddagger$ and $\mathsf{GHASH}(L, A^\dagger, M^*) = \mathsf{GHASH}(L, A^\ddagger, M^*)$
**return** $((K, N, A^\dagger, M), (K, N, A^\ddagger, M))$
```

$\mathsf{F}_{\mathsf{rdd}}(K, N, A^\ddagger)$. We define adversaries breaking the **CMT**-3 security of GCM and $\mathsf{GCM\text{-}C1}$ in Algorithm 12 and of $\mathsf{GCM\text{-}SIV}$ and $\mathsf{GCM\text{-}SIV\text{-}C1}$ in Algorithm 13. By the linearity of GHASH, AD $A^\ddagger$ that offers a collision of GHASH is found by solving the equation $\mathsf{GHASH}(L, A^\dagger, D) = \mathsf{GHASH}(L, A^\ddagger, D)$ where $D = C$ for GCM and $\mathsf{GCM\text{-}C1}$; $D = M^*$ for $\mathsf{GCM\text{-}SIV}$ and $\mathsf{GCM\text{-}SIV\text{-}C1}$. In GHASH, let

$$X_1^\dagger, X_2^\dagger, X_3, \ldots, X_l \xleftarrow{n} \mathsf{zp}(A^\dagger)\|\mathsf{zp}(D)\|\mathsf{str}_{n/2}(|A^\dagger|)\|\mathsf{str}_{n/2}(|D|) \text{ and}$$
$$X_1^\ddagger, X_2^\ddagger, X_3, \ldots, X_l \xleftarrow{n} \mathsf{zp}(A^\ddagger)\|\mathsf{zp}(D)\|\mathsf{str}_{n/2}(|A^\ddagger|)\|\mathsf{str}_{n/2}(|D|),$$

where $A^\dagger = X_1^\dagger \| X_2^\dagger$ and $A^\ddagger = X_1^\ddagger \| X_2^\ddagger$. Then,

$$\begin{aligned} &\mathsf{GHASH}(L, A^\dagger, D) = \mathsf{GHASH}(L, A^\ddagger, D) \\ &\Leftrightarrow X_1^\dagger \bullet L^l \oplus X_2^\dagger \bullet L^{l-1} = X_1^\ddagger \bullet L^l \oplus X_2^\ddagger \bullet L^{l-1} \end{aligned}$$

Hence, one can choose $A^\dagger$ and $A^\ddagger$ such that $A^\dagger \neq A^\ddagger$ and the above equation is satisfied. Using the collision of GHASH, we obtain tag collisions.

D Proof of Proposition 3

Let $\mathsf{P}_{\mathsf{mix}}$ be any mixing function. Let $\mathsf{F}_{\mathsf{rdd}}$ be an RDD function that is independent of AD, i.e., $\forall (K, N) \in \mathcal{K} \times \mathcal{N}, (A^\dagger, A^\ddagger) \in \mathcal{A}^2 : \mathsf{F}_{\mathsf{rdd}}(K, N, A^\dagger) = \mathsf{F}_{\mathsf{rdd}}(K, N, A^\ddagger)$. The attack is a simple collision attack on the tag-generation function of $\mathsf{CTX}[\mathsf{CTRAE}]$. The attack uses the property that the encryption $\mathsf{CTR}[E]$ is independent of AD. An adversary **A** is defined in Algorithm 14. By the birthday analysis on the tag-generation function, the adversary breaks the **CMT**-3-security of Π^* with the probability $O\left(\frac{p^2}{2^{t'}}\right)$.

Algorithm 14 CMT-3 Adversary **A** on $\mathsf{CTX}[\mathsf{CTRAE}]$

```
Choose a tuple $(K, N) \in \mathcal{K} \times \mathcal{N}$ of key and nonce
Choose $\frac{p-\omega-1}{2}$ distinct AD $A^{(1)}, \ldots, A^{(\frac{p-\omega-1}{2})} \in \mathcal{A}$
$R \leftarrow \mathsf{F}_{\mathsf{rdd}}(K, N, A^{(1)})$; $C \leftarrow \mathsf{CTR}[E](K, N, \mathsf{P}_{\mathsf{mix}}(R, 0))$        ▷ The plaintext is 0
for $i = 1, \ldots, \frac{p-\omega-1}{2}$ do
    $T^{\dagger(i)} \leftarrow \Pi_{\mathsf{TGen}}[\Psi_{\mathsf{tag}}](K, N, A^{(i)}, C)$; $T^{(i)} \leftarrow \mathsf{F}_{\mathsf{CTX}}(K, N, A^{(i)}, T^{\dagger(i)})$ end for
if $\exists \alpha, \beta \in [\frac{p-\omega-1}{2}]$ s.t. $\alpha \neq \beta \wedge T^{(\alpha)} = T^{(\beta)}$ then
    return $((K, N, A^{(\alpha)}, 0), (K, N, A^{(\beta)}, 0))$ end if
return $((K, N, 0, M), (K, N, 1, M))$
```

Algorithm 15 CMT-3 Adversary **A** on HtE-based AE

```
Choose $p$ distinct AD $A^{(1)}, \ldots, A^{(p)} \in \mathcal{A}$
Choose a tuple $(K, N, M) \in \mathcal{K} \times \{0,1\}^{\nu} \times \mathcal{M}$ of key, nonce, and plaintext
for $i = 1, \ldots, p$ do $L^{(i)} \leftarrow \mathsf{F}_{\mathsf{HtE}}(K, N, A^{(i)})$ end for
if $\exists \alpha, \beta \in [p]$ s.t. $\alpha \neq \beta \wedge L^{(\alpha)} = L^{(\beta)}$ then
    return $((K, N, A^{(\alpha)}, M), (K, N, A^{(\beta)}, M))$ end if
return $((K, N, 0, M), (K, N, 1, M))$
```

E Proof of Proposition 4

The attack is a simple collision attack on the key-derivation function $\mathsf{F}_{\mathsf{HtE}}$ that searches a collision with p distinct AD values. An adversary **A** is defined in Algorithm 15. By the birthday analysis, the adversary breaks the **CMT**-3-security of $\mathsf{HtE}[\Pi^{\mathsf{F}_{\mathsf{rdd}}, \mathsf{P}_{\mathsf{mix}}}]$ with the probability $O\left(\frac{p^2}{2^{\kappa}}\right)$.

F mu-AE Security of AE Schemes with KIVR

The definition of mu-AE, multi-user security of AE, is given in Supporting Material A.

F.1 mu-AE Security of AE 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 6. *Let Π be an AE scheme. Let $\mathsf{F}_{\mathit{rdd}}$ be an RDD function and $\mathsf{P}_{\mathit{mix}}$ a (ω, n)-mixing linear function. For any* mu-AE *adversary* **A** *against* $\mathit{KIVR}[\Pi^{\mathsf{F}_{\mathit{rdd}}, \mathsf{P}_{\mathit{mix}}}]$ *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* $\mathsf{F}_{\mathit{KIVR}}$ *such that*

$$\mathbf{Adv}^{\mathsf{mu\text{-}ae}}_{\mathit{KIVR}[\Pi]}(\mathbf{A}) \le \mathbf{Adv}^{\mathsf{mu\text{-}ae}}_{\Pi}(\mathbf{A}_1) + \mathbf{Adv}^{\mathsf{mu\text{-}prf}}_{\mathsf{F}_{\mathit{KIVR}}}(\mathbf{A}_2)\ ,$$

where **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 $T + O(q)$.*

Algorithm 16 Adversary $\mathbf{A}_1$ Breaking the **CMT**-1-Security of $\mathsf{KIVR}[\mathsf{GCM}^{\mathsf{F}_{\mathsf{rdd}},\mathsf{P}_{\mathsf{mix}}}]$

```
$p_1 \leftarrow \lceil \frac{p}{\omega+1} \rceil - 4$
Choose $p_1$ distinct keys $K^{(1)}, \ldots, K^{(p_1)} \in \{0,1\}^k$
Choose pair $(N, A) \in \mathcal{N}_{\mathsf{KIVR}} \times \mathcal{A}_{\mathsf{KIVR}}$ of nonce and AD
for $i = 1, \ldots, p_1$ do
    $R^{(i)} \leftarrow \mathsf{F}_{\mathsf{rdd}}(K^{(i)}, N, A)$; $(K_{\mathsf{T}}^{(i)}, IV_{\mathsf{T}}^{(i)}, R_{\mathsf{T}}^{(i)}) \leftarrow \mathsf{F}_{\mathsf{KIVR}}(K^{(i)}, N, A)$; $KS^{(i)} \leftarrow \varepsilon$
    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
end for
if $\exists \alpha, \beta \in [\lceil \frac{p_{\mathsf{ic}}}{\omega+1} \rceil - 4]$ s.t.
        $\alpha \neq \beta \wedge \mathsf{msb}_r(KS^{(\alpha)} \oplus KS^{(\beta)}) = R^{(\alpha)} \oplus \mathsf{zp}_r(R_{\mathsf{T}}^{(\alpha)}) \oplus R^{(\beta)} \oplus \mathsf{zp}_r(R_{\mathsf{T}}^{(\beta)})$ then
    $Z^{(\alpha)} \leftarrow E(K_{\mathsf{T}}^{(\alpha)}, IV_{\mathsf{T}}^{(\alpha)} \| 0^{n-\nu-1}1))$; $Z^{(\beta)} \leftarrow E(K_{\mathsf{T}}^{(\beta)}, IV_{\mathsf{T}}^{(\beta)} \| 0^{n-\nu-1}1)$
    $L^{(\alpha)} \leftarrow E(K_{\mathsf{T}}^{(\alpha)}, 0^n)$; $L^{(\beta)} \leftarrow E(K_{\mathsf{T}}^{(\beta)}, 0^n)$
    Find $C$ s.t. $|C| = n(\omega + 1)$
            and $\mathsf{GHASH}(L^{(\alpha)}, \varepsilon, C) \oplus \mathsf{GHASH}(L^{(\beta)}, \varepsilon, C) = Z^{(\alpha)} \oplus Z^{(\beta)}$
    $M^{(\alpha)} \leftarrow C \oplus KS^{(\alpha)}$; $M^{(\beta)} \leftarrow C \oplus KS^{(\beta)}$
    return $((K^{(\alpha)}, N, A, M^{(\alpha)}), (K^{(\beta)}, N, A, M^{(\beta)}))$
end if
return $((K^{(1)}, N, A, KS^{(1)}), (K^{(2)}, N, A, KS^{(2)}))$
```

F.2 Proof of Theorem 6

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 $\mathsf{KIVR}[\Pi^{\mathsf{F}_{\mathsf{rdd}},\mathsf{P}_{\mathsf{mix}}}]$ 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 $\mathsf{KIVR}[\Pi^{\mathsf{F}_{\mathsf{rdd}},\mathsf{P}_{\mathsf{mix}}}]$ is reduced to the mu-AE-security of $\Pi^{\mathsf{F}_{\mathsf{rdd}},\mathsf{P}_{\mathsf{mix}}}$, i.e., for any adversary breaking the mu-AE-security of $\mathsf{KIVR}[\Pi^{\mathsf{F}_{\mathsf{rdd}},\mathsf{P}_{\mathsf{mix}}}]$, there exists an adversary $\mathbf{A}_1$ breaking the mu-AE-security of $\Pi^{\mathsf{F}_{\mathsf{rdd}},\mathsf{P}_{\mathsf{mix}}}$.

By the above evaluations, we have

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

G Proof of Theorem 2 (CMT-1 Attack on $\mathsf{KIVR}[\mathsf{GCM}^{\mathsf{F}_{\mathsf{rdd}},\mathsf{P}_{\mathsf{mix}}}]$)

We consider any RDD function $\mathsf{P}_{\mathsf{mix}}$ and the following (ω, n)-mixing linear function $\mathsf{F}_{\mathsf{rdd}}$: $\forall R \in \{0,1\}^r, M \in \mathcal{M} : \mathsf{F}_{\mathsf{rdd}}(R, M) = R \| M$. Then, we have $\omega = \lceil \frac{r}{n} \rceil$. In this proof, we define two adversaries $\mathbf{A}_1$ and $\mathbf{A}_2$, and the term $\frac{p^2}{2^r}$ (resp. $\frac{p^2}{2^{\ell_{\mathsf{kivr}}}}$) comes from the first (resp. second) adversary $\mathbf{A}_1$ (resp. $\mathbf{A}_2$).

Adversary $\mathbf{A_1}$. The adversary $\mathbf{A}_1$ is defined in Algorithm 16. The goal of the adversary is to break the **CMT**-1-security of $\mathsf{KIVR}[\mathsf{GCM}^{\mathsf{F_{rdd}},\mathsf{P_{mix}}}]$. The adversary returns pairs $((K^{(\alpha)}, N^{(\alpha)}, A^{(\alpha)}, M^{(\alpha)}), (K^{(\beta)}, N^{(\beta)}, A^{(\beta)}, M^{(\beta)}))$ of tuples of key, nonce, AD, and plaintext such that $(N^{(\alpha)}, A^{(\alpha)}) = (N^{(\beta)}, A^{(\beta)})$, $K^{(\alpha)} \neq K^{(\beta)}$, and $M^{(\alpha)} \neq M^{(\beta)}$.

In the steps 4-7, $\mathbf{A}_1$ calculates key streams where pairs of nonce and AD are the same and the keys are distinct. Then, in the step 8, $\mathbf{A}_1$ searches a pair (α, β) with the following relation.

$$\mathsf{msb}_r\left(\mathsf{P}_{\mathsf{mix}}^{-1}\left(KS^{(\alpha)} \oplus KS^{(\beta)}\right)\right) = R^{(\alpha)} \oplus \mathsf{zp}_r(R_{\mathsf{T}}^{(\alpha)}) \oplus R^{(\beta)} \oplus \mathsf{zp}_r(R_{\mathsf{T}}^{(\beta)}).$$

By the birthday analysis, the probability that the relation is satisfied is $O\left(\frac{p^2}{2^r}\right)$. If such pair is found, then one can find the ciphertext collision $C^{(\alpha)} = C^{(\beta)}$ by using the freeness of plaintext blocks that are independent of the key streams. In the steps 8-14, $\mathbf{A}_1$ calculates a pair of plaintexts $(M^{(\alpha)}, M^{(\beta)})$ such that $(C^{(\alpha)}, T^{(\alpha)}) = (C^{(\beta)}, T^{(\beta)})$. As the proof of Proposition 2, using the linearity of GHASH, a ciphertext C that yields a tag collision is found by solving the equation $\mathsf{GHASH}(L^{(\alpha)}, \varepsilon, C) \oplus \mathsf{GHASH}(L^{(\beta)}, \varepsilon, C) = Z^{(\alpha)} \oplus Z^{(\beta)}$. The step 11 calculates the ciphertext.

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

Adversary $\mathbf{A_2}$. The second adversary $\mathbf{A}_2$ that breaks the **CMT**-1-security of $\mathsf{KIVR}[\mathsf{GCM}^{\mathsf{F_{rdd}},\mathsf{P_{mix}}}]$ by using a collision of $\mathsf{F_{KIVR}}$. By the birthday analysis, the collision probability is $O\left(\frac{p^2}{2^{\ell_{\mathsf{kivr}}}}\right)$). If the collision is found: $\mathsf{F_{KIVR}}(K^{(\alpha)}, N^{(\alpha)}, A^{(\alpha)}) = \mathsf{F_{KIVR}}(K^{(\beta)}, N^{(\beta)}, A^{(\beta)})$ 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 $(C^{(\alpha)}, T^{(\alpha)}) = (C^{(\beta)}, T^{(\beta)})$.

H Proof of Theorem 3 (CMT-1 Attack on $\mathsf{KIVR}[\mathsf{GCM\text{-}C1}^{\mathsf{F_{rdd}},\mathsf{P_{mix}}}]$)

We consider any RDD function $\mathsf{P_{mix}}$ and the following (ω, n)-mixing linear function $\mathsf{F_{rdd}}$: For each $R \in \{0,1\}^r$ and $M \in \mathcal{M}$, $\mathsf{P_{mix}}(R, M) := R \| M$. Then, we have $\omega = \lceil \frac{r}{n} \rceil$.

We define an adversary $\mathbf{A}$ in Algorithm 17. The goal of the adversary is to break the **CMT**-1-security of $\mathsf{KIVR}[\mathsf{GCM\text{-}C1}^{\mathsf{F_{rdd}},\mathsf{P_{mix}}}]$. The adversary returns pairs $((K^{(\alpha)}, N, A, M^{(\alpha)}), (K^{(\beta)}, N, A, M^{(\beta)}))$ of tuples of a key, a nonce, AD, and a plaintext such that $K^{(\alpha)} \neq K^{(\beta)}$.

In the steps 4-7, $\mathbf{A}$ calculates key streams where pairs of nonce and AD are the same and the keys are distinct. In the step 8, $\mathbf{A}$ searches a pair (α, β) with the following relation.

$$\mathsf{msb}_r\left(KS^{(\alpha)} \oplus KS^{(\beta)}\right) = R^{(\alpha)} \oplus \mathsf{zp}_r(R_{\mathsf{T}}^{(\alpha)}) \oplus R^{(\beta)} \oplus \mathsf{zp}_r(R_{\mathsf{T}}^{(\beta)}).$$

Algorithm 17 Adversary **A** Breaking the **CMT**-1-Security of $\mathsf{KIVR}[\mathsf{GCM\text{-}C1}^{\mathsf{F_{rdd}},\mathsf{P_{mix}}}]$

```
1: $p_1 \leftarrow \min\{2^n, \lceil \frac{p}{3} \rceil\}$; $p_2 \leftarrow \lceil \frac{p}{\omega+3} \rceil - 2p_1 - 4$
2: Choose $p_2$ distinct keys $K^{(1)}, \ldots, K^{(p_2)} \in \mathcal{K}_{\mathsf{KIVR}}$
3: Choose pair $(N, A) \in \mathcal{N}_{\mathsf{KIVR}} \times \mathcal{A}_{\mathsf{KIVR}}$ of nonce and AD
4: for $i = 1, \ldots, p_2$ do
5:     $R^{(i)} \leftarrow \mathsf{F_{rdd}}(K^{(i)}, N, A)$; $(K_{\mathsf{T}}^{(i)}, IV_{\mathsf{T}}^{(i)}, R_{\mathsf{T}}^{(i)}) \leftarrow \mathsf{F_{KIVR}}(K^{(i)}, N, A)$; $KS^{(i)} \leftarrow \varepsilon$
6:     for $j = 1, \ldots, \omega + 2$ 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 $\exists \alpha, \beta \in [p_2]$ s.t. $\alpha \neq \beta \wedge \mathsf{msb}_r(KS^{(\alpha)} \oplus KS^{(\beta)}) = R^{(\alpha)} \oplus \mathsf{zp}_r(R_{\mathsf{T}}^{(\alpha)}) \oplus R^{(\beta)} \oplus \mathsf{zp}_r(R_{\mathsf{T}}^{(\beta)})$ then
9:     for $i = 1, \ldots, p_1$ do
10:        $T^{(\alpha,i)} \leftarrow E(K_{\mathsf{T}}^{(\alpha)}, \mathsf{str}_n(i-1)) \oplus \mathsf{str}_n(i-1)$
11:        $T^{(\beta,i)} \leftarrow E(K_{\mathsf{T}}^{(\beta)}, \mathsf{str}_n(i-1)) \oplus \mathsf{str}_n(i-1)$
12:    end for
13:    if $\exists i_\alpha, i_\beta \in [p_1]$ s.t. $T^{(\alpha,i_\alpha)} = T^{(\beta,i_\beta)}$ then
14:        $Z^{(\alpha)} \leftarrow E(K_{\mathsf{T}}^{(\alpha)}, IV_{\mathsf{T}}^{(\alpha)} \| 0^{n-\nu-1}1))$; $Z^{(\beta)} \leftarrow E(K_{\mathsf{T}}^{(\beta)}, IV_{\mathsf{T}}^{(\beta)} \| 0^{n-\nu-1}1)$
15:        $L^{(\alpha)} \leftarrow E(K_{\mathsf{T}}^{(\alpha)}, 0^n)$; $L^{(\beta)} \leftarrow E(K_{\mathsf{T}}^{(\beta)}, 0^n)$
16:        Find $C$ s.t. $|C| = n(\omega + 2)$, $\mathsf{GHASH}(L^{(\alpha)}, \varepsilon, C) \oplus Z^{(\alpha)} = \mathsf{str}_n(i_\alpha - 1)$,
                   and $\mathsf{GHASH}(L^{(\beta)}, \varepsilon, C) \oplus Z^{(\beta)} = \mathsf{str}_n(i_\beta - 1)$
17:        $M^{(\alpha)} \leftarrow C \oplus \mathsf{msb}_{|C|}(KS^{(\alpha)})$; $M^{(\beta)} \leftarrow C \oplus \mathsf{msb}_{|C|}(KS^{(\beta)})$
18:        return $((K^{(\alpha)}, N, A, M^{(\alpha)}), (K^{(\beta)}, N, A, M^{(\beta)}))$
19:    end if
20: end if
21: return $((K^{(1)}, N, A, 0), (K^{(2)}, N, A, 1))$
```

By the birthday analysis, the probability that the relation is satisfied is $O\left(\frac{p^2}{2^r}\right)$. If such pair is found, then one can find the ciphertext collision $C^{(\alpha)} = C^{(\beta)}$ by using the freeness of plaintext blocks that are independent of the key streams. In the steps 9-12, **A** calculates DM's outputs $T^{(\alpha,i)}$ and $T^{(\beta,i)}$ whose input pairs are respectively $(K_{\mathsf{T}}^{(\alpha)}, \mathsf{str}_n(i-1))$ and $(K_{\mathsf{T}}^{(\beta)}, \mathsf{str}_n(i-1))$ which are candidates of tags. In the step 13, **A** searches a pair $((\alpha, i_\alpha), (\beta, i_\beta))$ such that a collision of DM, $T^{(\alpha,i_\alpha)} = T^{(\beta,i_\beta)}$, occurs. By the birthday analysis, the collision probability is $O\left(\frac{p^2}{2^t}\right)$. If such pair is found, then as the proof of Proposition 2, using the linearity of GHASH, a ciphertext C that offers the tag collision is found by solving the equations $\mathsf{GHASH}(L^{(\alpha)}, \varepsilon, C) \oplus Z^{(\alpha)} = \mathsf{str}_n(i_\alpha - 1)$ and $\mathsf{GHASH}(L^{(\beta)}, \varepsilon, C) \oplus Z^{(\beta)} = \mathsf{str}_n(i_\beta - 1)$. The step 16 calculates the ciphertext.

Hence, we have $\mathbf{Adv}_{\Pi^*}^{\mathsf{cmt\text{-}1}}(\mathbf{A}) = O\left(\min\left\{\frac{p^2}{2^r},\ 1\right\} \cdot \frac{p^2}{2^t}\right)$.

I Proof of Theorem 5

We consider any RDD function $\mathsf{P_{mix}}$ and the following (ω, n)-mixing linear function $\mathsf{F_{rdd}}$: For each $R \in \{0,1\}^r$ and $M \in \mathcal{M}$, $\mathsf{P_{mix}}(R, M) := R \| M$. Then, we

Algorithm 18 Adversary $\mathbf{A}$ Breaking the **CMT**-1-Security of $\mathsf{KIVR}[\mathsf{GCM\text{-}SIV}^{\mathsf{F_{rdd}},\mathsf{P_{mix}}}]$

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

have $\omega = \lceil \frac{r}{n} \rceil$. For the sake of simplicity, we assume that $\mathsf{KD1}$ is included in $\mathsf{F_{KIVR}}$.

We define an adversary $\mathbf{A}$ in Algorithm 18. The goal of the adversary is to break the **CMT**-1-security of $\mathsf{KIVR}[\mathsf{GCM\text{-}SIV}^{\mathsf{F_{rdd}},\mathsf{P_{mix}}}]$. The adversary returns a pair $((K^{(\alpha)}, N, A, M^{(\alpha)}), (K^{(\beta)}, N, A, M^{(\beta)}))$ of tuple of key, nonce, AD, and plaintext such that $K^{(\alpha)} \neq K^{(\beta)}$.

In the steps 4-8, $\mathbf{A}$ calculates key streams where pairs of nonce and AD are the same and the keys are distinct. In the step 9, $\mathbf{A}$ searches a pair (α, β) with the following relation.

$$\mathsf{msb}_1(X^{(\alpha)}) = \mathsf{msb}_1(X^{(\beta)}) = 0 \text{ and}$$
$$\mathsf{msb}_r\left(KS^{(\alpha)} \oplus KS^{(\beta)}\right) = R^{(\alpha)} \oplus \mathsf{zp}_r(R_{\mathsf{T}}^{(\alpha)}) \oplus R^{(\beta)} \oplus \mathsf{zp}_r(R_{\mathsf{T}}^{(\beta)}).$$

If such pair is found, then $\mathbf{A}$ can find the 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 $C^{(\alpha)} = C^{(\beta)}$ ($\Leftrightarrow M^{(\alpha)} \oplus M^{(\beta)} = KS^{(\alpha)} \oplus KS^{(\beta)}$), $\mathsf{GHASH}(L^{(\alpha)}, A^{(\alpha)}, M^{(\alpha)}) = H^{(\alpha)}$, and $\mathsf{GHASH}(L^{(\beta)}, A^{(\beta)}, M^{(\beta)}) = H^{(\beta)}$. In the equations, there are $2(\omega + 2)$ plaintext blocks and there are $\omega + 4$ equations in block. Fixing the 2ω message blocks with redundant data blocks such that $\mathsf{msb}_{\omega n}(C^{(\alpha)}) = \mathsf{msb}_{\omega n}(C^{(\beta)})$ is satisfied, the remaining 4 message blocks are uniquely determined from $\mathsf{lsb}_{2n}(C^{(\alpha)}) = \mathsf{lsb}_{2n}(C^{(\beta)})$, $\mathsf{lsb}_{n-1}(\mathsf{GHASH}(L_{\mathsf{T}}^{(\alpha)}, A^{(\alpha)}, M^{(\alpha)})) = \mathsf{lsb}_{n-1}(H^{(\alpha)})$, and $\mathsf{lsb}_{n-1}(\mathsf{GHASH}(L_{\mathsf{T}}^{(\beta)}, A^{(\beta)}, M^{(\beta)})) = \mathsf{lsb}_{n-1}(H^{(\beta)})$. Hence, the probability that $\mathbf{A}$ win the **CMT**-1 game is $O\left(\frac{p^2}{2^r}\right)$.