Committing Wide Encryption Mode with Minimum Ciphertext Expansion

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

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

Abstract. We propose a new wide encryption (WE) mode of operation that satisfies robust authenticated encryption (RAE) and committing security with minimum ciphertext expansion. WE is attracting much attention in the last few years, and its advantage includes RAE security that provides robustness against wide range of misuses, combined with the encode-then-encipher (EtE) construction. Unfortunately, WE-based EtE does not provide good committing security, and there is a recent constant-time CMT-4 attack (Chen et al., ToSC 2023(4)). Improving CMT-4 security requires considerable ciphertext expansion, and the state-of-the-art scheme expands the ciphertext by $s_{\mathsf{rae}} + 2s_{\mathsf{cmt}}$ bits from an original message to achieve s_{rae}-bit RAE and s_{cmt}-bit CMT-4 security. Our new WE mode FFF addresses the issue by achieving s_{rae}-bit RAE and s_{cmt}-bit CMT-4 security only with $\max\{s_{\mathsf{cmt}}, s_{\mathsf{rae}}\}$ bits of ciphertext expansion. Our design is based on the committing concealer proposed by Bellare et al., and its extension to WE (cf. tag-based AE) while satisfying RAE security is the main technical innovation.

Keywords: Wide encryption · Commitment · Robust authenticated encryption · Minimum ciphertext expansion · Mode of operation.

1 Introduction

Block cipher is an essential component of symmetric-key cryptography, which provides a pseudorandom permutation (PRP) of a fixed small length. If a PRP is secure for both forward and inverse queries, it is called a strong PRP (SPRP). Fixed-length PRP and SPRP are used with a mode of operation to handle variable-length input, but the resulting scheme is not necessarily a PRP or SPRP. For example, many common modes (ECB, CBC, OFB, CFB, and CTR [Dwo01]) are easily distinguishable from random functions, since changing a last message block only affects the last ciphertext block.

Wide encryption (WE) is a symmetric-key primitive that realizes an SPRP for a message of any length. Tweakable WE is a variant with an additional tweak input, with which an independent WE is instantiated with each tweak value. Hereafter, the term WE represents tweakable WE unless otherwise noted. Halevi and Rogaway formalized the security definition for WE, i.e. for tweakable, variable-length, and length-preserving SPRP [HR04]. Since then, researchers have proposed WE modes, including Shrimpton–Terashima [ST13], ZCZ [BLN18], and Băcuieți et al. [BDH+22], and concrete realizations such as AEZ [HKR15]. WE has practical applications, including full-disk encryption, and there are several proposals from the industry, including Adiantum [CB18] and HCTR2 [CHB21] by Google. Moreover, NIST has recently started standardizing

WEs [Nat23, Nat24], which stimulated even more WE proposals in the last few years, including the ones using double-decker and docked-double-decker [GDM22, DMMT24].

WE is an efficient building block for authenticated encryption with associated data (AE) that provide confidentiality and authenticity. More formally, an AE encryption $\mathsf{AE.Enc}$ takes a key K, associated data A, and a message M to generate a ciphertext $C = \mathsf{AE.Enc}(K, A, M)$. Throughout the paper, we assume that A includes a nonce N. The decryption $\mathsf{AE.Dec}$ takes the ciphertext C and the tuple (K, A) called the decryption context. It outputs the original message M with successful authentication; otherwise, it returns the invalid symbol **reject**. The encode-then-encipher (EtE) scheme proposed by Bellare and Rogaway [BR00] is a well-known way of constructing an AE from WE. WE-based EtE is particularly important because it realizes a robust AE (RAE) [HKR15]—a class of AEs that provides strong robustness against several misuses, including nonce reuse and the release of unverified plaintexts [ABL+14, HKR15].

WE-based EtE achieves s_{rae}-bit RAE security with ciphertext expansion by s_{rae} bits (up to the security bound of the WE). It first encodes s_{rae} bits of redundant data into an m-bit original message, e.g., by appending s_{rae} bits of zeros to the message, and encrypts the encoded message with the underlying WE to generate an $(m + s_{\mathsf{rae}})$-bit ciphertext. Upon decryption, EtE recovers an $(m + s_{\mathsf{rae}})$-bit encoded message, decodes the s_{rae}-bit redundancy, and checks it for authenticity. Meanwhile, WE's tweak input can be used to accept associated data A, including a nonce. AEZ [HKR15] is a well-known realization in this category.

Committing security is a relatively new security model with respect to AE [FOR17, GLR17]. The adversary is motivated to generate a ciphertext that is successfully decrypted with distinct decryption contexts. It is practically relevant because of the real-world attacks, including the multi-recipient integrity attack that delivers malicious content to a targeted user [GLR17, DGRW18, ADG+22] and the partitioning oracle attack that achieves efficient password brute-force attacks [LGR21]. The adversary in this model can know and choose a secret key, which significantly impacts the security analysis. This results in efficient attacks on common AE schemes, including GCM [GLR17, DGRW18], GCM-SIV [LGR21], CCM [MLGR23], and ChaCha20-Poly1305 [GLR17, NL18].

Bellare and Hoang [BH22] (and Chan and Rogaway independently [CR22]) generalized and formalized the committing security into CMT-1, CMT-3, and CMT-4 that consider the decryption contexts with $K \neq K'$, $(K, A) \neq (K', A')$, and $(K, A, M) \neq (K', A', M')$, respectively. CMT-1 covers committing security in the early days, also known as key commitment [FOR17, GLR17]. Meanwhile, CMT-3 and CMT-4 are equivalent, and they are strictly more secure than CMT-1.

Committing security of WE-based EtE is an emerging area of research. Grubbs et al. [GLR17] showed that EtE combined with an ideal WE satisfies a variant of key-committing security. Then, Chen et al. [CFI+23] pioneered cryptanalysis and security proof of concrete schemes, including AEZ, Adiantum-EtE, and HCTR2-EtE . Although WE-based EtE provides s_{cmt}-bit CMT-1 security with $2s_{\mathsf{cmt}}$ bits of ciphertext expansion, the security is clipped at $n/2$ wherein n is a block length of an underlying block cipher. With commonly used 128-bit block ciphers, i.e., $n = 128$, CMT-1 security saturates at 64 bits, which is insufficient for the minimum security level of 80 bits suggested by Chan and Rogaway [CR22]; the 80-bit security level is necessary because committing security is offline, where an adversary can efficiently make and verify guesses without any online query, in the same way as brute-force key recovery attack. The situation is even worse with CMT-4 security, and AEZ, Adiantum-EtE, and HCTR2-EtE are all broken in a constant time.

We can improve committing security of WE-based EtE beyond $n/2$ bits with the previous methods, at the cost of more ciphertext expansion, as summarized in Table 1. We assume a baseline WE-based EtE that satisfies s_{rae}-bit RAE security with s_{rae} bits of ciphertext expansion. We can use Fashim et al.'s method [FOR17] that adds an $2s_{\mathsf{cmt}}$-bit

Table 1: Ciphertext expansion in WE-based AEs for s_{rae}-bit RAE and s_{cmt}-bit CMT-1/CMT-4 security. The expansion is considered minimum when the target achieves the CMT-4 and RAE security with $\max\{s_{\mathsf{cmt}}, s_{\mathsf{rae}}\}$. The table assume $s_{\mathsf{cmt}} \geq s_{\mathsf{rae}}$, and $\max\{s_{\mathsf{cmt}}, s_{\mathsf{rae}}\} = s_{\mathsf{cmt}}$. The Primitive column shows assumptions of the underlying primitives for CMT-1/CMT-4 security: IC, CR hash, and RO represent an ideal cipher, a collision-resistant hash function, and a random oracle, respectively.

Scheme	Expansion size (bits)		Minimum?	Primitive	Ref.
	CMT-1	CMT-4			
WE + EtE†	$2s_{\mathsf{cmt}}$‡	—	No	IC	[BR00]
WE + EtE + $H(K)$	$s_{\mathsf{rae}} + 2s_{\mathsf{cmt}}$	—	No	CR Hash	[FOR17]
WE + EtE + $H(K, A)$	$s_{\mathsf{rae}} + 2s_{\mathsf{cmt}}$	$s_{\mathsf{rae}} + 2s_{\mathsf{cmt}}$	No	CR Hash	[FOR17, CR22]
FFF	s_{cmt}	s_{cmt}	Yes	RO	Ours

† AEZ, Adiantum-EtE, HCTR2-EtE, ‡The block size of the internal block cipher is $2s_{\mathsf{cmt}}$ bits.

hash digest of a key, denoted by $H(K)$, to the ciphertext. The resulting scheme achieves s_{cmt}-bit CMT-1 security, which can be larger than $n/2$ bits. By appending a $2s_{\mathsf{cmt}}$-bit hash digest of a key and associated data $H(K, A)$ instead [FOR17, CR22], we can achieve s_{cmt}-bit CMT-4 security.[1] However, as a drawback, the ciphertext expands by $s_{\mathsf{rae}} + 2s_{\mathsf{cmt}}$ bits from the original message. We also remark that there is no RAE security regarding the additional hash values $H(K)$ and $H(K, A)$, which is another issue that we address with the proposed method.

1.1 Design Goals

This paper improves the committing security of WE-based AEs. In particular, we propose a new method of building AE from the wide encryption that satisfies the following criteria.

- **RAE Security**: We focus on an RAE scheme with the security notion by Hoang et al. [HKR15] that provides strong robustness against several misuses.
- **CMT-4 Security**: We target CMT-4 security that is strictly more secure than CMT-1 and is unavailable with a simple EtE.
- **Minimum Ciphertext Expansion**: The design satisfies the minimum ciphertext expansion, which is $\max\{s_{\mathsf{cmt}}, s_{\mathsf{rae}}\}$ for an s_{rae}-bit RAE and s_{cmt}-bit CMT-4 security.

1.2 Our Approach

Obtaining CMT-4 security with the minimum ciphertext expansion is a major research challenge [BHW23, NSS24], and Bellare et al. [BHW23] already achieved the minimum ciphertext expansion for tag-based AEs, i.e., s_{cmt}-bit CMT-4 security with s_{cmt} bits of expansion. Fig. 1-(left) shows Bellare et al.'s construction wherein the committing concealer (CC) plays an important role. The construction splits a message into two parts, i.e., $M \to M_1 \| M_2$, and encrypts M_1 with an underlying tag-based AE to obtain a ciphertext

[1] Appending $H(K, A)$ is an extension of Farshim et al.'s method [FOR17] and is a variant of CTX [CR22] that appends $H(K, A, T)$ wherein T is a tag of an underlying tag-based AE.

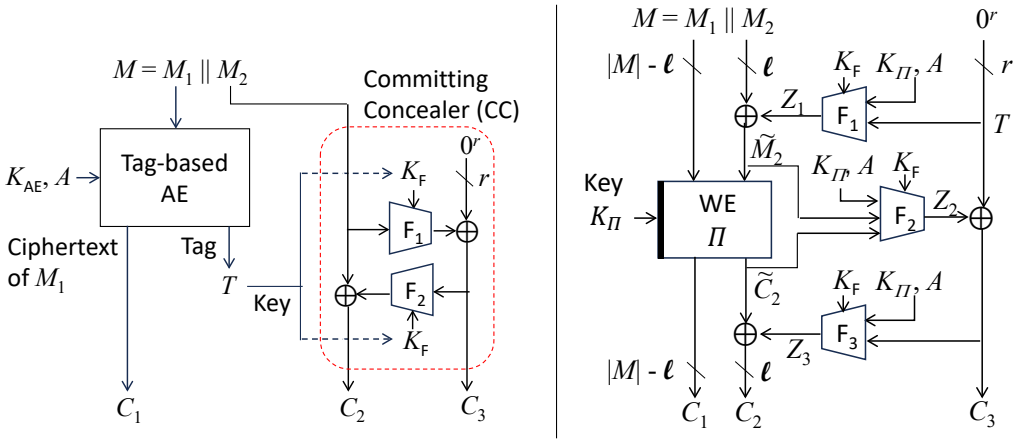

Figure 1: Existing Committing Mode: Tag-based AE with Committing Concealer (Left) and Our Committing Mode FFF: WE with 3-Round Feistel (Right).

C_1 and a tag T. Then, CC encrypts M_2 using the tag as its key and generates C_2 and C_3. $C_1||C_2||C_3$ is transmitted as a final ciphertext. In decryption, the scheme first decrypts C_1 by calling the tag-based AE to recover the message M_1 and the tag T. Then, it uses the tag to run the CC decryption to recover M_2. Authenticity is verified by checking 0^r in CC decryption. As a result, the size of $C_2||C_3$ contributes to the collision resistance for the committing security, while the ciphertext expansion is only $|C_3| = r$ bits thereby achieving minimum expansion.

We follow the above approach, but its application to WE and achieving RAE security are not straightforward. WE has no tag, and an attempt to use a fraction of WE's ciphertext as a CC's key does not work because, unlike the tag T, we cannot reproduce the fraction from the remaining part. Moreover, the scheme in Fig. 1-(left) does not provide RAE security; an adversary can efficiently distinguish the released unverified plaintexts from the ideal-world counterparts because (i) the decrypted M_1 is unaffected by $C_2||C_3$ and (ii) a difference in C_2 propagates directly to M_2.

1.3 Our Contributions

In this paper, we propose a new mode FFF that converts a WE into a RAE with provable committing security. The construction is depicted in Fig. 1-(right). It is parameterized by two variables, s_{rae} and s_{cmt}, which are target security levels as an RAE and as a CMT-4-secure AE, respectively. The size of the ciphertext expansion is minimal; the ciphertext size is only $\max\{s_{\mathsf{cmt}}, s_{\mathsf{rae}}\}$ bits larger than the message size.

In this construction, an input message M of size $|M|$ bits is divided into two parts $M \to M_1\|M_2$, where the sizes of M_1 and M_2 are $|M| - \ell$ bits and ℓ bits, respectively. The construction consists of WE Π for $|M|$-bit inputs and 3-round Feistel-like structure for processing $(\ell + r)$-bit input consisting of M_2 and r bits of zeros 0^r, where both the input and the output of Π are involved in the 3-round Feistel-like structure.

Inside the 3-round Feistel-like structure, three independent keyed hash functions $\mathsf{F}_1(K_\mathsf{F}, \cdot)$, $\mathsf{F}_2(K_\mathsf{F}, \cdot)$, and $\mathsf{F}_3(K_\mathsf{F}, \cdot)$, which serve as three random oracles for CMT-4 security or pseudorandom functions (PRFs) for RAE security, are computed.[2] All of them take a WE key K_Π and associated data A as input.[3] Besides, $\mathsf{F}_1(K_\mathsf{F}, \cdot)$ and $\mathsf{F}_3(K_\mathsf{F}, \cdot)$ take the

[2]By using domain separations, the three keyed hash functions can be realized from a single keyed hash function.

[3]By using iterated hash functions such as Merkle-Damgård or Sponge, one can share the state after processing K_Π and A within the three hashing processes.

r-bit state as the input and $\mathsf{F}_2(K_\mathsf{F},\cdot)$ take the last ℓ bits of the input and the output of Π as input. During the encryption, $\mathsf{F}_1(K_\mathsf{F},\cdot)$ is first computed and XORed with M_2, then Π is computed with a key K_Π to transform $M_1\|\widetilde{M_2}$ into $C_1\|\widetilde{C_2}$, where $\widetilde{M_2}$ and $\widetilde{C_2}$ are the last ℓ bits of the input and output of Π, respectively. At this stage, $|M|-\ell$ bits of the ciphertext C_1 can be output. After that, $\mathsf{F}_2(K_\mathsf{F},\cdot)$ and $\mathsf{F}_3(K_\mathsf{F},\cdot)$ are computed in turn, and ℓ bits and r bits of the ciphertext C_2 and C_3 are computed respectively as shown in Fig. 1. For decryption, first $\mathsf{F}_3(K_\mathsf{F},\cdot)$ is computed, and then the inverse of WE Π^{-1} is computed, followed by $\mathsf{F}_2(K_\mathsf{F},\cdot)$ and $\mathsf{F}_1(K_\mathsf{F},\cdot)$. The outputs Z_2 and Z_1 are respectively XORed with C_3 and $\widetilde{M_2}$ to compute T and M_2. The inputs are verified by checking if $T=0^r$. If so, $M_1\|M_2$ is a valid plaintext.

The design rational can be understood by intuitively understanding the security of this construction. To ensure RAE security, roughly speaking, any single-bit change in any of M_1, M_2, A must change all of C_1, C_2, C_3 randomly. The change of M_1, M_2 affects not only C_1, C_2 but C_3 through $\mathsf{F}_2(K_\mathsf{F},\cdot)$ that takes ℓ bits of the output from Π as input. The change of A will affect all the three rounds of the Feistel-like structure, which randomly changes C_1, C_2, C_3. Similarly, during the decryption, the change in C_1, C_2, C_3, A must change M_1,M_2, and T randomly. It is easy to see that any change in C_1, C_2, C_3, A will change the input to Π^{-1}, namely $C_1\|\widetilde{C_2}$, which randomly changes the output of Π^{-1}, namely $M_1\|\widetilde{M_2}$. With the similar analysis, any change in C_1, C_2, C_3, A will change Z_2 randomly, which changes T randomly.

For CMT-4, since CMT-4 and CMT-3 are equivalent, the goal of an adversary is to find a pair $((K_\Pi^\dagger, K_\mathsf{F}^\dagger, A^\dagger, M_1^\dagger, M_2^\dagger), (K_\Pi^\ddagger, K_\mathsf{F}^\ddagger, A^\ddagger, M_1^\ddagger, M_2^\ddagger))$ whose tuples of the first three values are distinct and the ciphertexts $C_1^\dagger\|C_2^\dagger\|C_3^\dagger$ and $C_1^\ddagger\|C_2^\ddagger\|C_3^\ddagger$ are the same. Then, the CMT-4 security is reduced to the collision resistance of the $C_2^\dagger\|C_3^\dagger$ part of the 3-round Feistel-like structure. The previous CC-construction [BHW23] in Fig. 1-(left) showed that this is possible even with 2-round Feistel network. With the similar approach, we can prove the collision resistance of our 3-round Feistel-like structure. In fact, only for proving CMT-4 security, 2 rounds are sufficient, but we need the additional round to make the construction a provably secure RAE.

Regarding the security bounds, FFF achieves about $\min\{r,\ell/2\}$-bit RAE security in the multi-user setting and about $\min\{r,\ell\}$-bit CMT-4-security. If $s_\mathsf{rae} \le s_\mathsf{cmt}/2$ (resp. $s_\mathsf{cmt}/2 < s_\mathsf{rae} \le s_\mathsf{cmt}$), then by choosing the parameters such that $\ell \ge r = s_\mathsf{cmt}$ (resp. $r = s_\mathsf{cmt}$ and $\ell = 2s_\mathsf{rae}$), the size of the ciphertext expansion of FFF is minimum regarding CMT-4 security. If $s_\mathsf{cmt} > s_\mathsf{rae}$, then by choosing the parameters such that $r = s_\mathsf{rae}$ and $\ell = 2s_\mathsf{rae}$, the size of the ciphertext expansion is minimum regarding RAE security.

Note that we require that the hash functions $\mathsf{F}_1(K_\mathsf{F},\cdot)$, $\mathsf{F}_2(K_\mathsf{F},\cdot)$, and $\mathsf{F}_3(K_\mathsf{F},\cdot)$ are keyed, and is a secure PRF. This is for proving RAE-security; RAE-security is usually proved under a secret key, and if the hash functions are keyless, key-dependent data may be passed to WE, yielding some attacks.

1.4 Related Works

Hash-then-Encrypt (HtE) [BH22] is another construction that converts a CMT-1-secure AE scheme into a CMT-4-secure one. HtE first generates a hash value $L = H(K, A)$ using a collision-resistant hash function H and uses L as a key for the underlying CMT-1-secure AE. We can achieve a CMT-4 security by combining HtE with WE and EtE, but the security is limited to $n/2$ bits, bottlenecked by WE-based EtE's CMT-1 security, as summarized in Table 1.

KIVR is another approach for improving CMT-4 security beyond the birthday bound regarding the tag in tag-based AEs [NSS24]. With $(r+t)$-bit ciphertext expansion for an r-bit plaintext redundancy and a t-bit tag, KIVR achieves $r/2$ or $(r+t)/2$ bits of CMT-4 security depending on the underlying tag-based AE.

2 Preliminaries

2.1 Notation

For integers $0 \leq i \leq j$, let $[i,j] := \{i, i+1, \ldots, j\}$ and $[j] := [1,j]$. Let ε be an empty string, $\emptyset$ an empty set, and $\{0,1\}^*$ be the set of all bit strings. For an integer $n \geq 0$, let $\{0,1\}^n$ be the set of all n-bit strings and $\{0,1\}^0 := \{\varepsilon\}$. 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 $0 \leq j, i$ 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. If $j \geq i$, then $\mathsf{msb}_j(X) = X$ and $\mathsf{lsb}_j(X) = X$. For a non-empty set $\mathcal{T}$, $T \xleftarrow{\$} \mathcal{T}$ means that an element is chosen uniformly at random from $\mathcal{T}$ and assigned to T. For two sets $\mathcal{T}$ and $\mathcal{T}'$, $\mathcal{T} \xleftarrow{\cup} \mathcal{T}'$ means $\mathcal{T} \leftarrow \mathcal{T} \cup \mathcal{T}'$. For integers $l_1, \ldots, l_j \geq 0$ and $X \in \{0,1\}^*$ such that $|X| = l_1 + \cdots + l_j$, $(X_1, \ldots, X_j) \xleftarrow{l_1,\ldots,l_j} X$ means parsing of X into j blocks such that $X = X_1\| \cdots \|X_j$ and $|X_i| = l_i$ for each $i \in [j]$.

2.2 Wide Encryption (WE)

A WE is a set of length-preserving permutations indexed by a key. Let $\mathcal{K}_{\mathsf{we}}$ and $\mathcal{M}_{\mathsf{we}}$ be the sets of keys and plaintexts. A WE $\Pi : \mathcal{K}_{\mathsf{we}} \times \mathcal{M}_{\mathsf{we}} \to \mathcal{M}_{\mathsf{we}}$ is such that for any key $K_\Pi \in \mathcal{K}_{\mathsf{we}}$ and distinct plaintexts $M, M' \in \mathcal{M}_{\mathsf{we}}$, $|M| = |\Pi(K_\Pi, M)|$ and $\Pi(K_\Pi, M) \neq \Pi(K_\Pi, M')$ must be satisfied. Let Π^{-1} be the inverse of Π. Π (resp. Π^{-1}) with a key K_Π is denoted by Π_{K_Π} (resp. $\Pi^{-1}_{K_\Pi}$). Let $\Pi^{\pm}_{K_\Pi} = (\Pi_{K_\Pi}, \Pi^{-1}_{K_\Pi})$. We call a WE with $\mathcal{K}_{\mathsf{we}} = \emptyset$ a "wide permutation (WP)". Let $\mathcal{WP}(\mathcal{M}_{\mathsf{we}})$ be the set of all WPs over $\mathcal{M}_{\mathsf{we}}$.

2.3 SPRP Security

For the RAE security of our mode, the underlying WE is assumed to be a secure multi-user-strong-pseudorandom-permutation (mu-SPRP). Let u be the number of users. In the mu-SPRP game, an adversary interacts with either the real-world oracles or the ideal-world oracles. The real-world oracles are $(\Pi_{K^{(1)}}, \Pi^{-1}_{K^{(1)}}, \ldots, \Pi_{K^{(u)}}, \Pi^{-1}_{K^{(u)}})$ where for each $i \in [u]$, $K^{(i)} \xleftarrow{\$} \mathcal{K}_{\mathsf{we}}$. The ideal-world oracles are ideal WPs $(\Psi_1, \Psi_1^{-1}, \ldots, \Psi_u, \Psi_u^{-1})$, where for each $\omega \in [u]$, $\Psi_\omega \xleftarrow{\$} \mathcal{WP}(\mathcal{M}_{\mathsf{we}})$. At the end of this game, $\mathbf{A}$ return a decision bit in $\{0,1\}$. Let $\mathbf{A}^{\mathcal{O}} \in \{0,1\}$ be an output of $\mathbf{A}$ with access to a set of oracles $\mathcal{O}$. Then, the mu-SPRP advantage function of $\mathbf{A}$ is defined as $\mathbf{Adv}^{\mathsf{mu\text{-}sprp}}_{\Pi}(\mathbf{A}) = \Pr\left[\mathbf{A}^{\Pi_{K^{(1)}}, \Pi^{-1}_{K^{(1)}}, \ldots, \Pi_{K^{(u)}}, \Pi^{-1}_{K^{(u)}}} = 1\right] - \Pr\left[\mathbf{A}^{\Psi_1, \Psi_1^{-1}, \ldots, \Psi_u, \Psi_u^{-1}} = 1\right]$.

2.4 Random Oracle

We prove the committing security of our mode in the random oracle model. For a positive integer n and a non-empty set $\mathcal{M}_{\mathsf{ro}}$, let $\mathsf{F} : \mathcal{M}_{\mathsf{ro}} \to \{0,1\}^n$ be an n-bit hash function. Let $\mathcal{F}(\mathcal{M}_{\mathsf{ro}}, \{0,1\}^n)$ be the set of all functions from $\mathcal{M}_{\mathsf{ro}}$ to $\{0,1\}^n$. In this model, a random oracle F is defined as $\mathsf{F} \xleftarrow{\$} \mathcal{F}(\mathcal{M}_{\mathsf{ro}}, \{0,1\}^n)$, and all parties have access to F by offline queries.

A random oracle F can be realized by lazy sampling. Let $\mathcal{T}_{\mathsf{F}}$ be a table that is initially empty and keeps query-response pairs of F. For a new query X to F, the response is defined as $Y \xleftarrow{\$} \{0,1\}^n$, and the pair (X,Y) is added to $\mathcal{T}_{\mathsf{F}}$: $\mathcal{T}_{\mathsf{F}} \xleftarrow{\cup} \{(X,Y)\}$. For a query stored in the table $\mathcal{T}_{\mathsf{F}}$, the same response is returned.

2.5 Pseudorandom Function (PRF)

We prove the RAE security of our mode with multi-user secure PRFs. For a positive integer n and non-empty sets $\mathcal{K}_{\mathsf{prf}}, \mathcal{M}_{\mathsf{prf}}$, let $\mathsf{F} : \mathcal{K}_{\mathsf{prf}} \times \mathcal{M}_{\mathsf{prf}} \to \{0,1\}^n$ be an n-bit keyed function, where $\mathcal{K}_{\mathsf{prf}}$ is the key space and $\mathcal{M}_{\mathsf{prf}}$ is the message space. The function with a key K is denoted by F_K. Let u be the number of users. Let $\mathcal{R}^{(1)}, \ldots, \mathcal{R}^{(u)}$ be u random functions where $\mathcal{R}_i \xleftarrow{\$} \mathcal{F}(\mathcal{M}_{\mathsf{prf}}, \{0,1\}^n)$ for each $i \in [u]$. Let $K^{(1)}, \ldots, K^{(u)}$ be u keys where $K^{(i)} \xleftarrow{\$} \mathcal{K}$ for each $i \in [u]$. Let $\mathbf{A}^{\mathcal{O}} \in \{0,1\}$ be an output of $\mathbf{A}$ with access to a set of oracles $\mathcal{O}$. The mu-PRF advantage function of an adversary $\mathbf{A}$ is defined as $\mathbf{Adv}^{\mathsf{mu\text{-}prf}}_{\mathsf{F}}(\mathbf{A}) := \Pr\left[\mathbf{A}^{\mathsf{F}_{K^{(1)}}, \ldots, \mathsf{F}_{K^{(u)}}} = 1\right] - \Pr\left[\mathbf{A}^{\mathcal{R}^{(1)}, \ldots, \mathcal{R}^{(u)}} = 1\right]$. In our RAE-security proof, $\mathbf{A}$ is a computationally-bounded adversary.

2.6 Authenticated Encryption (AE) with Decryption Leakage

Let AE be an AE scheme that is a pair of encryption and decryption algorithms $(\mathsf{AE.Enc}, \mathsf{AE.Dec})$. $\mathcal{K}$, $\mathcal{A}$, $\mathcal{M}$, $\mathcal{C}$ are the sets of keys, associated data (AD), plaintexts, and ciphertexts of AE, respectively. Note that if AE is a nonce-based (resp. tag-based) AE scheme, nonce (resp. a tag) is a part of AD (resp. a ciphertext). The encryption algorithm $\mathsf{AE.Enc} : \mathcal{K} \times \mathcal{A} \times \mathcal{M} \to \mathcal{C}$ takes a tuple (K, A, M), and returns, deterministically, a ciphertext C. The decryption algorithm $\mathsf{AE.Dec} : \mathcal{K} \times \mathcal{A} \times \mathcal{C} \to \{\mathbf{reject}\} \cup \mathcal{M}$ takes a tuple (K, A, C) and returns, deterministically, either the distinguished invalid symbol $\mathbf{reject} \notin \mathcal{M}$ or a plaintext $M \in \mathcal{M}$. We require that $\forall (K, A, M), (K', A', M') \in \mathcal{K} \times \mathcal{A} \times \mathcal{M}$ s.t. $|M| = |M'| : |\mathsf{AE.Enc}(K, A, M)| = |\mathsf{AE.Enc}(K', A', M')|$. We also require that $\forall K \in \mathcal{K}, A \in \mathcal{A}, M \in \mathcal{M} : \mathsf{AE.Dec}(K, A, \mathsf{AE.Enc}(K, A, M)) = M$.

2.7 Committing Security

We use the security notion, CMT-4, defined in [BH22]. Let $\mathsf{AE}[\mathsf{F}]$ be an AE scheme with an n-bit hash function $\mathsf{F} : \mathcal{M}_{\mathsf{ro}} \to \{0,1\}^n$ where $\mathcal{M}_{\mathsf{ro}}$ is a message space. Our proof assumes that F is a random oracle.

Bellare and Hoang [BH22] defines committing-security notions CMT-1 and CMT-3 as well as CMT-4. For $i \in \{1, 3, 4\}$, let WiC_i be a function for CMT-i security where on an input tuple (K, A, M), $\mathsf{WiC}_1(K, A, M) = K$, $\mathsf{WiC}_3(K, A, M) = (K, A)$, and $\mathsf{WiC}_4(K, A, M) = (K, A, M)$. In the CMT-i-security game, the goal of an adversary $\mathbf{A}$ is to return two distinct input tuples with respect to WiC_i on which the outputs of $\mathsf{AE.Enc}[\mathsf{F}]$ are the same. The CMT-i-security advantage of an adversary $\mathbf{A}$ for $i \in \{1, 3, 4\}$ is defined as $\mathbf{Adv}^{\mathsf{cmt}\text{-}i}_{\mathsf{AE}[\mathsf{F}]}(\mathbf{A}) := \Pr\left[(K^\dagger, A^\dagger, M^\dagger), (K^\ddagger, A^\ddagger, M^\ddagger) \leftarrow \mathbf{A}^{\mathsf{F}} \text{ s.t. } \mathsf{WiC}_i(K^\dagger, A^\dagger, M^\dagger) \neq \mathsf{WiC}_i(K^\ddagger, A^\ddagger, M^\ddagger) \wedge C^\ddagger = C^\ddagger\right]$. We assume that all input-output pairs of F required to calculate $C^\ddagger = \mathsf{AE.Enc}[\mathsf{F}](K^\dagger, A^\dagger, M^\dagger)$ and $C^\ddagger = \mathsf{AE.Enc}[\mathsf{F}](K^\ddagger, A^\ddagger, M^\ddagger)$ are defined by adversary's queries.

Bellare and Hoang [BH22] proved that CMT-4 and CMT-3 are equivalent.

Lemma 1. *For any* CMT-4 *adversary* $\mathbf{A}_4$ *making* p *queries, there exists a* CMT-3 *adversary* $\mathbf{A}_3$ *making* p *queries such that* $\mathbf{Adv}^{\mathsf{cmt}\text{-}4}(\mathbf{A}_4) \leq \mathbf{Adv}^{\mathsf{cmt}\text{-}3}(\mathbf{A}_3)$.

2.8 Robust-AE (RAE) Security

We use a slight variant of the RAE-security notion defined in [HKR15]. The variant notion $\mathsf{mu\text{-}RAE}$ is indistinguishabilty between AE and an ideal AE with decryption leakage in the multi-user setting. The ideal AE returns values that are randomly chosen with replacement where in the original notion, an ideal AE returns values that are randomly chosen without replacement.

In the $\mathsf{mu\text{-}RAE}$-security game, we consider the decryption function with leakage functionality, denoted by $\mathsf{AE.DecL}$. $\mathsf{AE.DecL}$ takes the same inputs as $\mathsf{AE.Dec}$, i.e., the input

Algorithm 1 FFF

Encryption $\mathsf{FFF.Enc}[\Pi_{K_\Pi}, \mathsf{F}_{K_\mathsf{F}}](A, M)$ where $|M| \geq \ell$

1: $(M_1, M_2) \xleftarrow{|M|-\ell,\ell} M$
2: $\widetilde{M_2} \leftarrow \mathsf{F}_1(K_\mathsf{F}, (K_\Pi, A, 0^r)) \oplus M_2$ ▷ 1st Round
3: $\widetilde{M} \leftarrow M_1 \| \widetilde{M_2}$; $\widetilde{C} \leftarrow \Pi(K_\Pi, \widetilde{M})$; $(C_1, \widetilde{C_2}) \xleftarrow{|\widetilde{C}|-\ell,\ell} \widetilde{C}$ ▷ Perform WE
4: $C_3 \leftarrow \mathsf{F}_2(K_\mathsf{F}, (K_\Pi, A, \widetilde{M_2}, \widetilde{C_2}))$ ▷ 2nd Round
5: $C_2 \leftarrow \mathsf{F}_3(K_\mathsf{F}, (K_\Pi, A, C_3)) \oplus \widetilde{C_2}$ ▷ 3nd Round
6: $C \leftarrow C_1 \| C_2 \| C_3$; **return** C

Decryption $\mathsf{FFF.Dec}[\Pi^{-1}_{K_\Pi}, \mathsf{F}_{K_\mathsf{F}}](A, C)$ where $|C| \geq \ell + r$

1: $(C_1, C_2, C_3) \xleftarrow{|C|-(\ell+r),\ell,r} C$
2: $\widetilde{C_2} \leftarrow \mathsf{F}_3(K_\mathsf{F}, (K_\Pi, A, C_3)) \oplus C_2$ ▷ 3nd Round
3: $\widetilde{C} \leftarrow C_1 \| \widetilde{C_2}$; $\widetilde{M} \leftarrow \Pi(K_\Pi, \widetilde{C})$; $(M_1, \widetilde{M_2}) \xleftarrow{|\widetilde{M}|-\ell,\ell} \widetilde{M}$ ▷ Perform WE
4: $T \leftarrow \mathsf{F}_2(K_\mathsf{F}, (K_\Pi, A, \widetilde{M_2}, \widetilde{C_2})) \oplus C_3$ ▷ 2nd Round
5: $M_2 \leftarrow \mathsf{F}_1(K_\mathsf{F}, (K_\Pi, A, T)) \oplus \widetilde{M_2}$
6: **if** $T = 0^r$ **then return** M; **else return reject end if**

space is $\mathcal{K} \times \mathcal{A} \times \mathcal{M}$, and returns leakage values as well as the result of the verification which is **accept** if the inputs are valid; **reject** otherwise. Our mode leaks a pair of an unverified plaintext and a value for authentication (See Section 3.1 for the leakage values). $\mathsf{AE.Enc}$ (resp. $\mathsf{AE.DecL}$) with a key K is denoted by $\mathsf{AE}_K.\mathsf{Enc}$ (resp. $\mathsf{AE}_K.\mathsf{DecL}$). Let $\mathsf{AEL}_K := (\mathsf{AE}_K.\mathsf{Enc}, \mathsf{AE}_K.\mathsf{DecL})$.

Let u be the number of users. In the mu-RAE-security game, an adversary $\mathbf{A}$ has access to either real-world oracles $(\mathsf{AEL}_{K^{(1)}}, \ldots, \mathsf{AEL}_{K^{(u)}})$ or ideal-world ones $((\$^{(1)}_{\mathsf{Enc}}, \$^{(1)}_{\mathsf{Dec}}), \ldots, (\$^{(u)}_{\mathsf{Enc}}, \$^{(u)}_{\mathsf{Dec}}))$. $K^{(1)}, \ldots, K^{(u)}$ are user's keys defined as $K^{(\omega)} \xleftarrow{\$} \mathcal{K}$ for each $\omega \in [u]$. $\$^{(\omega)}_{\mathsf{Enc}}$ is a random-bit encryption oracle of the ω-th user that takes a pair (A, M) of AD and a plaintext, and returns a random ciphertext defined as $C \xleftarrow{\$} \{0,1\}^{|\mathsf{AE.Enc}(K,A,M)|}$. $\$^{(\omega)}_{\mathsf{Dec}}$ is a random-bit decryption oracle that returns a pair $(\mathbf{reject}, V)$ where V is a random leak value defined as $V \xleftarrow{\$} \{0,1\}^{|\mathsf{AE.DecL}(K,A,M)|}$. At the end of this game, $\mathbf{A}$ return a decision bit in $\{0,1\}$. In this game, for a query-response tuple (A, M, C) of some user, $\mathbf{A}$ is forbidden to make the decryption query (A, C) to the same user. Let $\mathbf{A}^{\mathcal{O}} \in \{0,1\}$ be an output of $\mathbf{A}$ with access to a set of oracles $\mathcal{O}$. Then, the mu-RAE-security advantage function of $\mathbf{A}$ is defined as $\mathbf{Adv}^{\mathsf{mu\text{-}rae}}_{\mathsf{AE}}(\mathbf{A}) := \Pr\left[\mathbf{A}^{\mathsf{AEL}_{K^{(1)}},\ldots,\mathsf{AEL}_{K^{(\omega)}}} = 1\right] - \Pr\left[\mathbf{A}^{\$^{(1)}_{\mathsf{Enc}},\$^{(1)}_{\mathsf{Dec}},\ldots,\$^{(\omega)}_{\mathsf{Enc}},\$^{(\omega)}_{\mathsf{Dec}}} = 1\right]$.

3 FFF: Committing Wide Encryption Mode

We first define our mode FFF. We then show the CMT-4-security bound of FFF, followed by the mu-RAE-security bound of FFF.

3.1 Specifications of FFF

Our mode FFF has the 3-round Feistel-like structure with WE.

Let $\Pi : \mathcal{K}_{\mathsf{we}} \times \{0,1\}^* \to \{0,1\}^*$ be a WE, where $\mathcal{K}_{\mathsf{we}}$ is the key space. Let ℓ (resp. r) be a positive integer and the length of the left (resp. right) part of the 3-round Feistel-like structure. Let $\mathsf{F} : \mathcal{K}_{\mathsf{prf}} \times ([3] \times \mathcal{K}_{\mathsf{we}} \times \mathcal{A} \times \{0,1\}^* \times \{0,1\}^*) \to \{0,1\}^{\max\{\ell,r\}}$ be a function that is a hash function for CMT-4 security and that is a keyed function for mu-RAE security, where $\mathcal{K}_{\mathsf{prf}}$ is the key space. For $K_\mathsf{F} \in \mathcal{K}_{\mathsf{prf}}$, $K_\Pi \in \mathcal{K}_{\mathsf{we}}$, $A \in \mathcal{A}$,

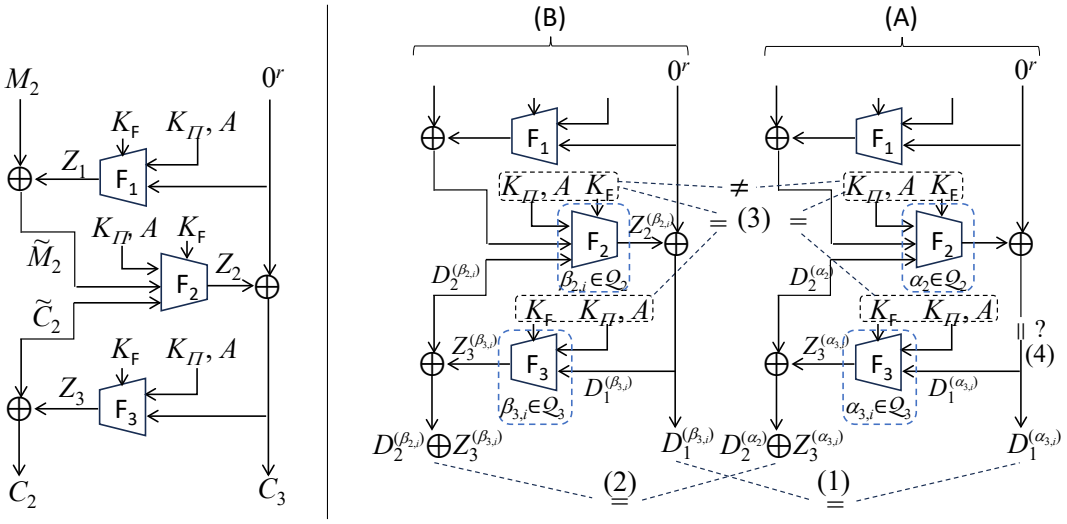

Figure 2: $\mathsf{Feistel}^3_{0^r}$ (left) and Multi-Collision Event mcoll (right)

$D_1 \in \{0,1\}^*$, and $D_2 \in \{0,1\}^*$, let $\mathsf{F}_1(K_\mathsf{F},(K_\Pi,A,D_1)) := \mathsf{msb}_\ell \circ \mathsf{F}(K_\mathsf{F},(1,K_\Pi,A,D_1,\varepsilon)$ be the 1st-round function of the 3-round Feistel-like structure, $\mathsf{F}_2(K_\mathsf{F},(K_\Pi,A,D_1,D_2) := \mathsf{msb}_r \circ \mathsf{F}(K_\mathsf{F},(2,K_\Pi,A,D_1,D_2))$ the 2nd-round function, and $\mathsf{F}_3(K_\mathsf{F},(K_\Pi,A,D_1)) := \mathsf{msb}_\ell \circ \mathsf{F}(K_\mathsf{F},(3,K_\Pi,A,D_1,\varepsilon))$ the 3rd-round function.

The specification of FFF is given in Algorithm 1. The encryption (resp. decryption) is depicted in Fig. 1-(right) (resp. Fig. 3 in Appendix A). $\mathsf{FFF.Enc}[\Pi_{K_\Pi},\mathsf{F}_{K_\mathsf{F}}]$ (resp. $\mathsf{FFF.Dec}[\Pi^{-1}_{K_\Pi},\mathsf{F}_{K_\mathsf{F}}]$) is the encryption (resp. decryption) function. We require that the lengths of plaintexts (resp. ciphertexts) are grater than or equal to ℓ (resp. $\ell+r$). We define the decryption function with leakage functionality $\mathsf{FFF.DecL}[\Pi^{-1}_{K_\Pi},\mathsf{F}_{K_\mathsf{F}}]$ as follows. For each inputs $((K_\Pi,K_\mathsf{F}),A,C)$, $\mathsf{FFF.DecL}[\Pi^{-1}_{K_\Pi},\mathsf{F}_{K_\mathsf{F}}]$ returns (M,T) as well as $\mathsf{vrf} \in \{\mathbf{accept},\mathbf{reject}\}$, where $\mathsf{vrf} = \mathsf{FFF.Dec}[\Pi^{-1}_{K_\Pi},\mathsf{F}_{K_\mathsf{F}}](A,C)$, and M and T are defined in the decryption procedure.

3.2 Security Bounds of FFF

3.2.1 CMT-4 Security

The following theorem shows the CMT-4-security bound of FFF in the random oracle model. The proof is given in Section 4.

Theorem 1. *Assume that* F *is a random oracle. For any* CMT-4 *computationally unbounded adversary* $\mathbf{A}$ *making at most* p *offline queries, we have* $\mathbf{Adv}^{\mathsf{cmt\text{-}4}}_{\mathit{FFF}}(\mathbf{A}) \le \frac{\frac{\ell+r}{\log_2(\ell+r)}\cdot p}{2^{\min\{r,\ell\}}} + \left(\frac{12(\ell+r)p}{2^{\min\{r,\ell\}}}\right)^{\frac{\ell+r}{\log_2(\ell+r)}}$.

The bound ensures that FFF is CMT-4-secure up to about $2^{\min\{r,\ell\}}$ offline queries and achieves about $\min\{r,\ell\}$-bit security.

3.2.2 Mu-RAE Security

The following theorem shows the mu-RAE-security bound of FFF. The proof is given in Section 5.

Theorem 2. *For any computationally bounded adversary* $\mathbf{A}$ *making at most* q *queries, making at most* q_u *queries to each user, having access to* u *users, and running in time at*

Algorithm 2 Disjointed 3-Round Feistel Structure with 0^r

Procedure $\mathsf{Feistel}^3_{0^r}[\mathsf{F}](K_\mathsf{F}, K_\Pi, A, M_2, \widetilde{C}_2)$
1: $\widetilde{M_2} \leftarrow \mathsf{F}_1(K_\mathsf{F}, K_\Pi, A, 0^r) \oplus M_2$ ▷ 1st Round
2: $C_3 \leftarrow \mathsf{F}_2(K_\mathsf{F}, K_\Pi, A, \widetilde{M_2}, \widetilde{C}_2)$ ▷ 2nd Round
3: $C_2 \leftarrow \mathsf{F}_3(K_\mathsf{F}, K_\Pi, A, C_3) \oplus \widetilde{C}_2$ ▷ 3nd Round
4: **return** $C_2 \| C_3$

most t, there exist an mu-SPRP *adversary* $\mathbf{A}_\Pi$ *and an* mu-PRF *adversary* $\mathbf{A}_\mathsf{F}$ *such that* $\mathbf{Adv}^{\mathsf{mu\text{-}rae}}_{\mathit{FFF}}(\mathbf{A}) \le \frac{q_u q}{2^\ell} + \frac{q_d}{2^r} + \mathbf{Adv}^{\mathsf{mu\text{-}sprp}}_{\Pi}(\mathbf{A}_\Pi) + \mathbf{Adv}^{\mathsf{mu\text{-}prf}}_{\mathsf{F}}(\mathbf{A}_\mathsf{F})$*, and* $\mathbf{A}_\Pi$ *and* $\mathbf{A}_{\mathsf{F}_1}$ *make at most q queries, have access to u users, and run in time $O(q + t)$.*

The bound ensures that FFF is mu-RAE secure up to $\min\{2^{\ell/2}, 2^r\}$ queries, assuming that the advantage functions of mu-SPRP and of mu-PRF are negligible compared with the other terms. Thus, FFF achieves $\min\{\ell/2, r\}$-bit mu-RAE security. If the number of queries to each user is limited, i.e., $q_\mathsf{u} \ll 2^{\ell/2}$, then FFF achieves beyond-birthday-bound security regarding the parameter ℓ.

4 Proof of Theorem 1

By Lemma 1, CMT-3 security and CMT-4 security are equivalent. Hence, we consider a CMT-3 adversary $\mathbf{A}$ against FFF[F] where F is a random oracle. Without loss of generality, assume that $\mathbf{A}$ is deterministic and makes no repeated query.

4.1 Decoupled 3-round Feistel-like Structure with 0^r

We consider the 3-round Feistel-like structure $\mathsf{Feistel}^3_{0^r}[\mathsf{F}]$ given in Algorithm 2 and Fig. 2-(left). In $\mathsf{Feistel}^3_{0^r}[\mathsf{F}]$, the right-part input is fixed to 0^r and the left part at the 2nd round is decoupled, i.e, $\mathsf{Feistel}^3_{0^r}[\mathsf{F}]$ is $\mathsf{FFF.Enc}[\Pi, \mathsf{F}]$ without Π. Hence, if the CMT-3 security of FFF is broken, i.e., $(K^\dagger_\Pi, K^\dagger_\mathsf{F}, A^\dagger) \neq (K^\ddagger_\Pi, K^\ddagger_\mathsf{F}, A^\ddagger)$ and $\mathsf{FFF.Enc}[\Pi_{K^\dagger_\Pi}, \mathsf{F}_{K^\dagger_\mathsf{F}}](A^\dagger, M^\dagger) = \mathsf{FFF.Enc}[\Pi_{K^\ddagger_\Pi}, \mathsf{F}_{K^\ddagger_\mathsf{F}}](A^\ddagger, M^\ddagger)$, then we have a collision of $\mathsf{Feistel}^3_{0^r}[\mathsf{F}]$, i.e., $\mathsf{Feistel}^3_{0^r}[\mathsf{F}](K^\dagger_\mathsf{F}, K^\dagger_\Pi, A^\dagger, M^\dagger_2, \widetilde{C}^\dagger_2) = \mathsf{Feistel}^3_{0^r}[\mathsf{F}](K^\ddagger_\mathsf{F}, K^\ddagger_\Pi, A^\ddagger, M^\ddagger_2, \widetilde{C}^\ddagger_2)$. Hence, by using the CMT-3 adversary $\mathbf{A}$, we can construct a collision-finding adversary $\mathbf{B}$ against $\mathsf{Feistel}^3_{0^r}[\mathsf{F}]$ making at most p queries to a random oracle F and outputting two tuples $(K^\dagger_\mathsf{F}, K^\dagger_\Pi, A^\dagger, M^\dagger_2, \widetilde{C}^\dagger_2)$ and $(K^\ddagger_\mathsf{F}, K^\ddagger_\Pi, A^\ddagger, M^\ddagger_2, \widetilde{C}^\ddagger_2)$ such that $(K^\dagger_\mathsf{F}, K^\dagger_\Pi, A^\dagger) \neq (K^\ddagger_\mathsf{F}, K^\ddagger_\Pi, A^\ddagger)$, $\mathbf{Adv}^{\mathsf{cmt\text{-}3}}_{\mathsf{FFF}}(\mathbf{A}) \le \delta_{\mathsf{coll}} := \Pr\Big[\mathsf{Feistel}^3_{0^r}[\mathsf{F}](K^\dagger_\mathsf{F}, K^\dagger_\Pi, A^\dagger, M^\dagger_2, \widetilde{C}^\dagger_2) = \mathsf{Feistel}^3_{0^r}[\mathsf{F}](K^\ddagger_\mathsf{F}, K^\ddagger_\Pi, A^\ddagger, M^\ddagger_2, \widetilde{C}^\ddagger_2)\Big]$, and the random-oracle list $\mathcal{T}_\mathsf{F}$ includes input-output tuples needed to perform $\mathsf{Feistel}^3_{0^r}[\mathsf{F}](K^\dagger_\mathsf{F}, K^\dagger_\Pi, A^\dagger, M^\dagger_2, \widetilde{C}^\dagger_2)$ and $\mathsf{Feistel}^3_{0^r}[\mathsf{F}](K^\ddagger_\mathsf{F}, K^\ddagger_\Pi, A^\ddagger, M^\ddagger_2, \widetilde{C}^\ddagger_2)$.

4.2 Collision Resistance of the Disjointed 3-round Feistel

We evaluate δ_{coll}, the probability that an adversary $\mathbf{B}$ making p queries finds a collision of $\mathsf{Feistel}^3_{0^r}$.

4.2.1 Intuition

We use a $(\ell + r)$-multi-collision event in Z_2 values of r bits. The multi-collision probability is at most $\binom{p}{\ell+r}(1/2^r)^{\ell+r-1} \le (\ell + r)p/2^r$. Assuming that the multi-collision does not occur, for each input to F_3 (including C_3), the number of inputs to F_2 whose outputs are equal to C_3 is at most $\ell + r$. Then, if a collision of $\mathsf{Feistel}^3_{0^r}$ occurs, there exists a pair of the $\ell + r$ inputs to F_3, the outputs C_2 must be equal, and the collision probability is at

most $(\ell+r)^2/2^\ell$. Since the number of such multi-collision groups for C_3 is at most p, we have $\delta_{\mathsf{coll}} \leq (\ell+r)p/2^r + (\ell+r)^2p/2^\ell$. Note that the intuition does not consider query orders between F_2 and F_3 for the collision of $\mathsf{Feistel}^3_{0^r}$. The following evaluation derive a (slightly) better bound by taking into account the orders.

4.2.2 Detail

For $\alpha \in [p]$, let $X^{(\alpha)} = (K_{\mathsf{F}}^{(\alpha)}, j^{(\alpha)}, K_{\Pi}^{(\alpha)}, A^{(\alpha)}, D_1^{(\alpha)}, D_2^{(\alpha)}) \in \mathcal{K}_{\mathsf{prf}} \times [3] \times \mathcal{K}_{\mathsf{we}} \times \mathcal{A} \times \{0,1\}^* \times \{0,1\}^*$ be the α-th query to F and $Z^{(\alpha)} = \mathsf{F}(X^{(\alpha)})$ the response. Let $Z^{(\alpha)}_{j^{(\alpha)}} := \mathsf{msb}_\ell(Z^{(\alpha)})$ if $j^{(\alpha)} \in \{1,3\}$ and $D^{(\alpha)}_{j^{(\alpha)}} = \varepsilon$; $Z_2^{(\alpha)} := \mathsf{msb}_r(Z^{(\alpha)})$ if $j^{(\alpha)} = 2$. Let $\mathcal{T}_{\mathsf{F}}^{(<\alpha)} := \{(X^{(\beta)}, Z_1^{(\beta)}) \mid \beta \in [\alpha-1]\}$. Let $\mathcal{L}^{(<\alpha)}_{\mathsf{Feistel}^3_{0^r}}$ be all input-output tuples of $\mathsf{Feistel}^3_{0^r}$ obtained from $\mathcal{T}_{\mathsf{F}}^{(<\alpha)}$, i.e., $\forall (I, C_{2,3}) \in \mathcal{L}^{(<\alpha)}_{\mathsf{Feistel}^3_{0^r}}$: the corresponding input-output tuples of F are defined in $\mathcal{T}_{\mathsf{F}}^{(<\alpha)}$, where $I = (K_{\mathsf{F}}, K_\Pi, A, M_2, \widetilde{C}_2)$ and $C_{2,3} = C_2 \| C_3$. For $i \in [3]$ and $\alpha \in [p]$, let $\mathcal{Q}_i^{(<\alpha)} := \{\beta \mid j^{(\beta)} = i \wedge \beta \in [\alpha-1]\}$ and $\mathcal{Q}_i := \mathcal{Q}_i^{(<p+1)}$. Let $\mu := \frac{\ell+r}{\log_2(\ell+r)}$.

We define four (muti-)collision events. coll is a collision event for $\mathsf{Feistel}^3_{0^r}$. For $i \in [2,3]$, mcoll_i is a μ-multi-collision event for F_i. mcoll is a μ-multi-collision event for the number of collision candidates in $\mathcal{L}_{\mathsf{Feistel}^3_{0^r}}$.

- coll: $\exists (I^\dagger, C^\dagger_{2,3}), (I^\ddagger, C^\ddagger_{2,3}) \in \mathcal{L}_{\mathsf{Feistel}^3_{0^r}}$ s.t. $I^\dagger \neq I^\ddagger$ and $C^\dagger_{2,3} = C^\ddagger_{2,3}$.
- mcoll_2: $\exists \alpha_1, \ldots, \alpha_\mu \in \mathcal{Q}_2$ s.t. $\alpha_1 < \ldots < \alpha_\mu$ and $Z_2^{(\alpha_1)} = \cdots = Z_2^{(\alpha_\mu)}$.
- mcoll_3: $\exists D \in \{0,1\}^\ell, \alpha_1, \ldots, \alpha_\mu, \beta_1, \ldots, \beta_\mu \in \mathcal{Q}_3$ s.t.
  - $D_1^{(\alpha_1)}, \ldots, D_1^{(\alpha_\mu)}$ are all distinct, $\forall i \in [\mu] : D_1^{(\alpha_i)} = D_1^{(\beta_i)}$, $(K_{\mathsf{F}}^{(\alpha_i)}, K_\Pi^{(\alpha_i)}, A^{(\alpha_i)}) = (K_{\mathsf{F}}^{(\alpha_1)}, K_\Pi^{(\alpha_1)}, A^{(\alpha_1)}) \neq (K_{\mathsf{F}}^{(\beta_1)}, K_\Pi^{(\beta_1)}, A^{(\beta_1)}) = (K_{\mathsf{F}}^{(\beta_i)}, K_\Pi^{(\beta_i)}, A^{(\beta_i)})$, and
  - $\forall i \in [\mu] : Z_3^{(\alpha_i)} \oplus Z_3^{(\beta_i)} = D$.

  (The structure of the event is depicted in Fig. 4 in Appendix A.)
- mcoll: $\exists \alpha_2 \in \mathcal{Q}_2, \beta_{2,1}, \ldots, \beta_{2,\mu} \in \mathcal{Q}_2^{(<\alpha_2)}$, $\alpha_{3,1}, \ldots, \alpha_{3,\mu}, \beta_{3,1}, \ldots, \beta_{3,\mu} \in \mathcal{Q}_3^{(<\alpha_2)}$ s.t. $\forall i \in [\mu]$: (1) $D_1^{(\alpha_{3,i})} = D_1^{(\beta_{3,i})} = Z_2^{(\beta_{2,i})}$, (2) $D_2^{(\beta_{2,i})} \oplus Z_3^{(\beta_{3,i})} = D_2^{(\alpha_2)} \oplus Z_3^{(\alpha_{3,i})}$, and (3) $(K_{\mathsf{F}}^{(\alpha_2)}, K_\Pi^{(\alpha_2)}, A^{(\alpha_2)}) = (K_{\mathsf{F}}^{(\alpha_{3,i})}, K_\Pi^{(\alpha_{3,i})}, A^{(\alpha_{3,i})}) \neq (K_{\mathsf{F}}^{(\beta_{2,i})}, K_\Pi^{(\beta_{2,i})}, A^{(\beta_{2,i})}) = (K_{\mathsf{F}}^{(\beta_{3,i})}, K_\Pi^{(\beta_{3,i})}, A^{(\beta_{3,i})})$. (See Fig. 2-(right).)

By using these events, we have $\delta_{\mathsf{coll}} = \Pr[\mathsf{coll}] \leq \Pr[\mathsf{coll} \mid \neg\mathsf{mcoll}_2 \wedge \neg\mathsf{mcoll}_3 \wedge \neg\mathsf{mcoll}] + \Pr[\mathsf{mcoll}_2] + \Pr[\mathsf{mcoll}_3] + \Pr[\mathsf{mcoll}]$. The bounds of these probabilities are given below, and we have $\delta_{\mathsf{coll}} \leq \frac{\mu p}{2^{\min\{r,\ell\}}} + 2^r \left(\frac{ep}{\mu 2^r}\right)^\mu + 2^\ell \cdot p \cdot (\frac{ep}{\mu 2^\ell})^\mu + p\left(\frac{3ep}{2^\ell}\right)^\mu \leq \frac{\frac{\ell+r}{\log_2(\ell+r)} \cdot p}{2^{\min\{r,\ell\}}} + \left(\frac{12(\ell+r)p}{2^{\min\{r,\ell\}}}\right)^{\frac{\ell+r}{\log_2(\ell+r)}}$, assuming $p \leq 2^{r-1}$.

4.2.3 Evaluating $\Pr[\mathsf{mcoll}_2]$

Fixing μ indexes $\alpha_1, \ldots, \alpha_\mu \in \mathcal{Q}_2$, we have $\Pr[Z_2^{(\alpha_1)} = \cdots = Z_2^{(\alpha_\mu)}] \leq \left(\frac{1}{2^r}\right)^{\mu-1}$. Summing the bound for each tuple of μ indexes and using Stirling's approximation ($x! \geq \left(\frac{x}{e}\right)^x$ for any x), we have $\Pr[\mathsf{mcoll}_2] \leq \binom{p}{\mu}\left(\frac{1}{2^r}\right)^{\mu-1} \leq 2^r\left(\frac{ep}{\mu 2^r}\right)^\mu$.

4.2.4 Evaluating $\mathbf{Pr}[\mathsf{mcoll}_3]$

Fix $D \in \{0,1\}^\ell, \alpha_1, \ldots, \alpha_\mu, \beta_1, \ldots, \beta_\mu \in \mathcal{Q}_3$ such that $\forall i \in [\mu] : D_1^{(\alpha_i)} = D_1^{(\beta_i)}$, and $(K_{\mathsf{F}}^{(\alpha_i)}, K_{\Pi}^{(\alpha_i)}, A^{(\alpha_i)}) = (K_{\mathsf{F}}^{(\alpha_1)}, K_{\Pi}^{(\alpha_1)}, A^{(\alpha_1)}) \neq (K_{\mathsf{F}}^{(\beta_1)}, K_{\Pi}^{(\beta_1)}, A^{(\beta_1)}) = (K_{\mathsf{F}}^{(\beta_i)}, K_{\Pi}^{(\beta_i)}, A^{(\beta_i)})$. We then have $\Pr[\forall i \in [\mu] : Z_3^{(\alpha_i)} \oplus Z_3^{(\beta_i)} = D] \leq (\frac{1}{2^\ell})^\mu$. The number of choices of $\alpha_1, \ldots, \alpha_\mu$ is at most $\binom{p}{\mu}$. The number of choices of β_1 is at most p. Fixing $(\alpha_1, \ldots, \alpha_\mu, \beta_1)$, $(\beta_2, \ldots, \beta_\mu)$ are uniquely fixed. Hence, we have $\Pr[\mathsf{mcoll}_3] \leq 2^\ell \cdot p \cdot \binom{p}{\mu} \cdot (\frac{1}{2^\ell})^\mu \leq 2^\ell \cdot p \cdot \binom{p}{\mu} \cdot (\frac{1}{2^\ell})^\mu \leq 2^\ell \cdot p \cdot (\frac{ep}{\mu 2^\ell})^\mu$, using Stirling's approximation.

4.2.5 Evaluating $\mathbf{Pr}[\mathsf{mcoll}]$

Fix $\alpha_2 \in \mathcal{Q}_2$ and $\gamma_1, \ldots, \gamma_\mu \in \mathcal{Q}_2^{(<\alpha_2)} \cup \mathcal{Q}_3^{(<\alpha_2)}$ where $\gamma_i = \max\{\alpha_{3,i}, \beta_{2,i}, \beta_{3,i}\}$. For $i \in [\mu]$, we consider the following cases.

Case 1. $\gamma_i = \alpha_{3,i}$, i.e., the γ_i query is the 3rd round of (A) in Fig. 2-(right).

Case 2. $\gamma_i = \beta_{2,i}$, i.e., the γ_i query is the 2nd round of (B) in Fig. 2-(right).

Case 3. $\gamma_i = \beta_{3,i}$, i.e., the γ_i query is the 3nd round of (B) in Fig. 2-(right).

We evaluate the probability that $\gamma_i = \alpha_{3,i}$ (Case 1) and the conditions (1),(2),(3) on mcoll are satisfied (See Fig. 2-(right)). Fixing the inputs $(K_{\mathsf{F}}^{(\gamma_i)}, K_{\Pi}^{(\gamma_i)}, A^{(\gamma_i)}, D_1^{(\gamma_i)}, D_2^{(\gamma_i)})$ to F_3, by $\neg\mathsf{mcoll}_2$, the number of candidates for $\beta_{2,i}$ (with the condition (1)) is at most μ. For each of the (at most) μ candidates, $\beta_{3,i}$ is uniquely fixed. Then, the probability that the condition (2) is satisfied is at most $\frac{\mu}{2^\ell}$.

We evaluate the probability that $\gamma_i = \beta_{2,i}$ (Case 2) and the conditions (1),(2),(3) are satisfied. Fixing the inputs $(K_{\mathsf{F}}^{(\gamma_i)}, K_{\Pi}^{(\gamma_i)}, A^{(\gamma_i)}, D_1^{(\gamma_i)}, D_2^{(\gamma_i)})$ to F_2, by $\neg\mathsf{mcoll}_3$, the number of candidates for the pair $(\alpha_{3,i}, \beta_{3,i})$ (with the condition (2)) is at most μ. Then, the probability that the condition (1) is satisfied is at most $\frac{\mu}{2^r}$.

We evaluate the probability that $\gamma_i = \beta_{3,i}$ (Case 3) and the conditions (1),(2),(3) are satisfied. Fixing the inputs $(K_{\mathsf{F}}^{(\gamma_i)}, K_{\Pi}^{(\gamma_i)}, A^{(\gamma_i)}, D_1^{(\gamma_i)}, D_2^{(\gamma_i)})$ to F_3, by $\neg\mathsf{mcoll}_2$, the number of candidates for $\beta_{2,i}$ is at most μ. For each of the μ candidates, with the condition (1), $\alpha_{3,i}$ is uniquely fixed. Then, the probability that the condition (2) is satisfied is at most $\frac{\mu}{2^\ell}$.

Fixing $\alpha_2 \in \mathcal{Q}_2$, the number of choices of $\gamma_1, \ldots, \gamma_\mu \in [\alpha_2 - 1]$ is at most $\binom{\alpha_2}{\mu}$. Hence, using the above bounds, we have $\Pr[\mathsf{mcoll}] \leq \sum_{\alpha_2 \in [p]} \binom{\alpha_2}{\mu} \cdot \left(\frac{3\mu}{2^\ell}\right)^\mu \leq \sum_{\alpha_2 \in [p]} \left(\frac{3e\alpha_2}{2^\ell}\right)^\mu \leq p\left(\frac{3ep}{2^\ell}\right)^\mu$.

4.2.6 Evaluating $\mathbf{Pr}[\mathsf{coll} \mid \neg\mathsf{mcoll}_2 \wedge \neg\mathsf{mcoll}_3 \wedge \neg\mathsf{mcoll}]$

Assume that mcoll_2, mcoll_3, and mcoll do not occur. We then consider the case that coll occurs just after the α-th query where $\alpha \in [p]$.

- Consider the sub-case with $\alpha \in \mathcal{Q}_2$. Fix $\alpha \in \mathcal{Q}_2$. Let $\alpha_2 := \alpha$. By $\neg\mathsf{mcoll}$, the number of pairs of indexes $(\alpha_{3,1}, \beta_{3,1}), (\alpha_{3,2}, \beta_{3,1}), \ldots \in (\mathcal{Q}_3^{(<\alpha_2)})^2$ such that the α_2-th output $Z_2^{(\alpha)}$ probabilistically connects with $D_1^{(\alpha_{3,i})}$ and yields a collision of $\mathsf{Feistel}_{0^r}^3$ is at most μ. See Fig. 2-(right) and the connection point is marked with (4). For each $\alpha_{3,i}$, we have $\Pr[D_1^{(\alpha_{3,i})} = Z_2^{(\alpha_2)}] \leq \frac{1}{2^r}$. Hence, the probability that coll occurs in this case is at most $\frac{\mu p}{2^r}$.
- Consider the sub-case with $\alpha \in \mathcal{Q}_3$. Let $\mathcal{Q}_2^{\mathsf{new}} := \{\beta \in \mathcal{Q}_2 \mid \forall \beta_0 \in [\beta - 1] \cap \mathcal{Q}_2 : Z_2^{(\beta)} \neq Z_2^{(\beta_0)}\}$ be the set of query indexes in $\mathcal{Q}_2$ such that the outputs are new. For $\beta \in \mathcal{Q}_2^{\mathsf{new}}$, let $\mathcal{Q}_2[\beta] = \{\ \beta_1 \in \mathcal{Q}_2 \mid Z_2^{(\beta_1)} = Z_2^{(\beta)}\}$ be multi-collision

indexes with $Z_2^{(\beta)}$ and $\mu_\beta = |\mathcal{Q}_2[\beta]|$. Note that if coll occurs, then there exists $\beta \in \mathcal{Q}_2^{\mathsf{new}}$ such that $\mu_\beta \geq 2$, which is required to have a collision on the right part of $\mathsf{Feistel}_{0^r}^3$. Fix $\beta \in \mathcal{Q}_2^{\mathsf{new}}$ such that $\mu_\beta \geq 2$. Then, for each pair $(\beta_1, \beta_2) \in \mathcal{Q}_2[\beta]^2$ such that $\beta_1 \neq \beta_2$ and $(K_{\mathsf{F}}^{(\beta_1)}, K_\Pi^{(\beta_1)}, A^{(\beta_1)}) \neq (K_{\mathsf{F}}^{(\beta_2)}, K_\Pi^{(\beta_2)}, A^{(\beta_2)})$, we have $\Pr\Big[\mathsf{F}_3(K_{\mathsf{F}}^{(\beta_1)}, K_\Pi^{(\beta_1)}, A^{(\beta_1)}, Z_2^{(\beta_1)}) \oplus D_2^{(\beta_1)} = \mathsf{F}_3(K_{\mathsf{F}}^{(\beta_2)}, K_\Pi^{(\beta_2)}, A^{(\beta_2)}, Z_2^{(\beta_2)}) \oplus D_2^{(\beta_2)}\Big] \leq \frac{1}{2^\ell}$, which is the bound of the collision probability at the left part. Hence, the probability that the collision of $\mathsf{Feistel}_{0^r}^3$ occurs due to $\mathcal{Q}_2[\beta]$ is at most $\binom{\mu_\beta}{2} \cdot \frac{1}{2^\ell} \leq \frac{0.5\mu_\beta^2}{2^\ell}$. Note that $\mu_\beta \leq \mu$ by $\neg\mathsf{mcoll}_2$ and $\sum_{\beta \in \mathcal{Q}_2^{\mathsf{new}}} \mu_\beta \leq p$. Summing the bound for each $\beta \in \mathcal{Q}_2^{\mathsf{new}}$, the probability that coll occurs in this case is at most $\sum_{\beta \in \mathcal{Q}_2^{\mathsf{new}}} \frac{0.5\mu_\beta^2}{2^\ell} \leq \mu \sum_{\beta \in \mathcal{Q}_2^{\mathsf{new}}} \frac{0.5\mu_\beta}{2^\ell} \leq \frac{\mu p}{2^\ell}$.

By using the bounds, we have $\Pr[\mathsf{coll} \mid \neg\mathsf{mcoll}_2 \wedge \neg\mathsf{mcoll}_3 \wedge \neg\mathsf{mcoll}] \leq \frac{\mu p}{2^{\min\{r,\ell\}}}$.

5 Proof of Theorem 2

Without loss of generality, assume that an adversary $\mathbf{A}$ is deterministic and makes no repeated query.

5.1 Notations

We define notations for this proof. Let q_e (resp. q_d) be the number of encryption (resp. decryption) queries, where $q = q_e + q_d$. For $\omega \in [u]$, let $\hat{q}_\omega$ be the number of queries to the ω-th user. For $\alpha \in [q]$, let $\mathsf{query}^{(\alpha)} \in \{\mathsf{enc}, \mathsf{dec}\}$ be the type of the α-th query: $\mathsf{query}^{(\alpha)} = \mathsf{enc}$ (resp. dec) if the query is an encryption (resp. decryption) one. Let $\mathsf{user}^{(\alpha)} \in [u]$ be the user number of the α-th query, i.e., if the α-th query is to the ω-th user, $\mathsf{user}^{(\alpha)} = \omega$. For $\alpha \in [q]$, values defined at the α-th query are denoted by using the superscript of (α). The stage that an adversary makes queries is called "query stage". The stage after the query stage is called "decision stage". For $\omega \in [u]$, let $\mathsf{FFF}[\Pi_{K_\Pi^{(\omega)}}^{\pm}, \mathsf{F}_{K_{\mathsf{F}}^{(\omega)}}] := (\mathsf{FFF.Enc}[\Pi_{K_\Pi^{(\omega)}}, \mathsf{F}_{K_{\mathsf{F}}^{(\omega)}}], \mathsf{FFF.DecL}[\Pi_{K_\Pi^{(\omega)}}^{-1}, \mathsf{F}_{K_{\mathsf{F}}^{(\omega)}}])$.

5.2 Deriving the Bound

We consider four games $\mathbf{G}1, \mathbf{G}2, \mathbf{G}3$, and $\mathbf{G}4$. For $i \in [4]$, let $\mathcal{O}_i$ be the set of oracles in the game $\mathbf{G}i$. The games are defined below.

- $\mathbf{G}1$ is the real-world and $\mathcal{O}_1 := (\mathsf{FFF}[\Pi_{K_\Pi^{(1)}}^{\pm}, \mathsf{F}_{K_{\mathsf{F}}^{(1)}}], \ldots, \mathsf{FFF}[\Pi_{K_\Pi^{(u)}}^{\pm}, \mathsf{F}_{K_{\mathsf{F}}^{(u)}}])$.
- $\mathbf{G}2$ is a variant of $\mathbf{G}1$ where the underlying functions $\mathsf{F}_{K_{\mathsf{F}}^{(1)}}, \ldots, \mathsf{F}_{K_{\mathsf{F}}^{(u)}}$ are replaced with random functions $\mathcal{R}^{(1)}, \ldots, \mathcal{R}^{(u)}$ and K_Π values are removed from inputs to the random functions. Then, $\mathcal{O}_2 := (\mathsf{FFF}[\Pi_{K_\Pi^{(1)}}^{\pm}, \mathcal{R}^{(1)}], \ldots, \mathsf{FFF}[\Pi_{K_\Pi^{(u)}}^{\pm}, \mathcal{R}^{(u)}])$. The ω-th user's encryption is depicted in Fig. 5 in Appendix A.
- $\mathbf{G}3$ is a variant of $\mathbf{G}_2$ where the underlying WE $\Pi_{K_\Pi^{(1)}}^{\pm}, \ldots, \Pi_{K_\Pi^{(u)}}^{\pm}$ are replaced with ideal WPs $\Psi_1^{\pm}, \ldots, \Psi_u^{\pm}$. Then, $\mathcal{O}_3 := (\mathsf{FFF}[\Psi_1^{\pm}, \mathcal{R}^{(1)}], \ldots, \mathsf{FFF}[\Psi_u^{\pm}, \mathcal{R}^{(u)}])$. The ω-th user's encryption is depicted in Fig. 6 in Appendix A.
- $\mathbf{G}4$ is the ideal world and $\mathcal{O}_4 := (\$_{\mathsf{Enc}}^{(1)}, \$_{\mathsf{Dec}}^{(1)}, \ldots, \$_{\mathsf{Enc}}^{(u)}, \$_{\mathsf{Dec}}^{(u)})$.

Using these games, we have $\mathbf{Adv}_{\mathsf{FFF}}^{\mathsf{mu\text{-}rae}}(\mathbf{A}) = \Pr[\mathbf{A}^{\mathcal{O}_1} = 1] - \Pr[\mathbf{A}^{\mathcal{O}_4} = 1]$
$= \sum_{i \in [3]} \underbrace{\big(\Pr[\mathbf{A}^{\mathcal{O}_i} = 1] - \Pr[\mathbf{A}^{\mathcal{O}_{i+1}} = 1]\big)}_{=:\delta_i}$.

From $\mathbf{G}1$ to $\mathbf{G}2$, the underlying functions in $\mathbf{G}1$ are replaced with random functions. Hence, δ_1 is bounded by the mu-PRF-security advantage function of F, i.e., there exists an adversary $\mathbf{A}_{\mathsf{F}}$ making at most $3q$ queries and having access to u users such that $\delta_1 \leq \mathbf{Adv}^{\mathsf{mu\text{-}prf}}_{\mathsf{F}}(\mathbf{A}_{\mathsf{F}})$.

From $\mathbf{G}2$ to $\mathbf{G}3$, WEs are replaced with ideal WPs. Hence, δ_2 is bounded by the mu-SPRP-security advantage function of Π, i.e., there exists an adversary $\mathbf{A}_{\Pi}$ making at most q queries and having access to u users such that $\delta_2 \leq \mathbf{Adv}^{\mathsf{mu\text{-}sprp}}_{\Pi}(\mathbf{A}_{\Pi})$.

The bound of the δ_3 is given in Section 5.3. By using the bounds of $\delta_1, \delta_2, \delta_3$, we have $\mathbf{Adv}^{\mathsf{mu\text{-}rae}}_{\mathsf{FFF}}(\mathbf{A}) \leq \frac{q_u q}{2^\ell} + \frac{q_d}{2^r} + \mathbf{Adv}^{\mathsf{mu\text{-}prf}}_{\mathsf{F}}(\mathbf{A}_{\mathsf{F}}) + \mathbf{Adv}^{\mathsf{mu\text{-}sprp}}_{\Pi}(\mathbf{A}_{\Pi})$.

5.3 Bounding δ_3

We derive the bound of δ_3 by using the coefficient-H technique [Pat08]. The following evaluation shows that $\delta_3 \leq \frac{q_u q}{2^\ell} + \frac{q_d}{2^r}$.

5.3.1 Adversary's View

We define dummy values of $\mathbf{G}4$ according to the structure of FFF. The dummy values are defined in the decision stage. Let $\mathcal{R} : [u] \times \{1,3\} \times \mathcal{A} \times \{0,1\}^r \to \{0,1\}^\ell$ be a random function. The first element is a user index and the second one is a round number. For $i \in \{1,3\}$, let $\mathcal{R}_i : [u] \times \mathcal{A} \times \{0,1\}^r \to \{0,1\}^\ell$ be the random function $\mathcal{R}$ with the round number i. For each $\alpha \in [q]$, the dummy values of the α-th query are defined as follows.

- $M_1^{(\alpha)}, M_2^{(\alpha)} \xleftarrow{|M|-\ell,\ell} M^{(\alpha)}$ and $C_1^{(\alpha)}, C_2^{(\alpha)}, C_3^{(\alpha)} \xleftarrow{|C|-\ell,\ell,r} C^{(\alpha)}$.
- If $\mathsf{query}^{(\alpha)} = \mathsf{enc}$, then $T^{(\alpha)} \leftarrow 0^r$.
- $Z_1^{(\alpha)} \xleftarrow{\$} \mathcal{R}_1(\mathsf{user}^{(\alpha)}, A^{(\alpha)}, T^{(\alpha)})$, $Z_2^{(\alpha)} \leftarrow T^{(\alpha)} \oplus C_3^{(\alpha)}$, and $Z_3^{(\alpha)} \leftarrow \mathcal{R}_3(\mathsf{user}^{(\alpha)}, A^{(\alpha)}, C_3^{(\alpha)})$.
- $\widetilde{M}_2^{(\alpha)} \leftarrow M_2^{(\alpha)} \oplus Z_1^{(\alpha)}$ and $\widetilde{C}_2^{(\alpha)} \leftarrow C_2^{(\alpha)} \oplus Z_3^{(\alpha)}$.

We then define a transcript τ which consists of

- $(\mathsf{query}^{(\alpha)}, \mathsf{user}^{(\alpha)}, M^{(\alpha)}, C^{(\alpha)}, T^{(\alpha)}, Z_1^{(\alpha)}, Z_2^{(\alpha)}, Z_3^{(\alpha)})$ for $\alpha \in [q]$,

where in $\mathbf{G}3$, if $\mathsf{query}^{(\alpha)} = \mathsf{enc}$, then $T^{(\alpha)} := 0^r$.

This proof reveals the transcript to the adversary $\mathbf{A}$ in the decision stage.

5.3.2 Coefficient-H Technique

Let T_3 be a transcript obtained by sampling in $\mathbf{G}3$, i.e., sampling of Π_ω and $\mathcal{R}_\omega$ for $\omega \in [u]$. Let T_4 be a transcript obtained by sampling in $\mathbf{G}4$, i.e., sampling of $\$_{\mathsf{Enc}}^{(\omega)}, \$_{\mathsf{Dec}}^{(\omega)}$, and $\mathcal{R}$ for $\omega \in [u]$. We call a transcript τ *valid* if $\Pr[\mathsf{T}_4 = \tau] > 0$. Let $\mathcal{T}$ be the set of all valid transcripts such that $\forall \tau \in \mathcal{T} : \Pr[\mathsf{T}_3 = \tau] \leq \Pr[\mathsf{T}_4 = \tau]$. Then, we have $\delta_3 \leq \mathsf{SD}(\mathsf{T}_3, \mathsf{T}_4) := \sum_{\tau \in \mathcal{T}} (\Pr[\mathsf{T}_3 = \tau] - \Pr[\mathsf{T}_4 = \tau])$.

We can derive the bound of δ_3 by using the coefficient-H technique [Pat08].

Lemma 2. *Let $\mathcal{T}_{\mathsf{good}}$ and $\mathcal{T}_{\mathsf{bad}}$ be good and bad transcripts into which $\mathcal{T}$ is partitioned. If $\forall \tau \in \mathcal{T}_{\mathsf{good}} : \frac{\Pr[\mathsf{T}_3 = \tau]}{\Pr[\mathsf{T}_4 = \tau]} \geq 1 - \varepsilon$ s.t. $0 \leq \varepsilon \leq 1$, then $\mathsf{SD}(\mathsf{T}_3, \mathsf{T}_4) \leq \Pr[\mathsf{T}_4 \in \mathcal{T}_{\mathsf{bad}}] + \varepsilon$.*

We thus (1) define good and bad transcripts; (2) upper-bound $\Pr[\mathsf{T}_4 \in \mathcal{T}_{\mathsf{bad}}]$; and (3) lower-bound $\frac{\Pr[\mathsf{T}_3 = \tau]}{\Pr[\mathsf{T}_4 = \tau]}$. Then, putting these bounds into the above lemma, we obtain the upper-bound of δ_3.

In the following, firstly good and bad transcripts are defined. Then, in Section 5.4, the upper-bound of $\Pr[\mathsf{T}_4 \in \mathcal{T}_{\mathsf{bad}}]$ is derived. In Section 5.5, the lower-bound of $\frac{\Pr[\mathsf{T}_3 = \tau]}{\Pr[\mathsf{T}_4 = \tau]}$. By using these bounds, we have $\delta_3 \leq \frac{q_u q}{2^\ell} + \frac{q_d}{2^r}$.

5.3.3 Good and Bad Transcripts and Bound of δ_3

We define bad events below.

- bad_1: $\exists \alpha, \beta \in [q]$ s.t. $\alpha > \beta$, $\mathsf{user}^{(\alpha)} = \mathsf{user}^{(\beta)}$, and
  - $\mathsf{query}^{(\alpha)} = \mathsf{enc} \wedge \widetilde{C}_2^{(\alpha)} = \widetilde{C}_2^{(\beta)}$ or
  - $\mathsf{query}^{(\alpha)} = \mathsf{dec} \wedge \widetilde{M}_2^{(\alpha)} = \widetilde{M}_2^{(\beta)}$.
- bad_2: $\exists \alpha, \beta \in [q]$ s.t. $\alpha > \beta$, $\mathsf{user}^{(\alpha)} = \mathsf{user}^{(\beta)}$, and
  - $\mathsf{query}^{(\alpha)} = \mathsf{enc} \wedge (A^{(\alpha)}, M_2^{(\alpha)}) \neq (A^{(\beta)}, M_2^{(\beta)}) \wedge \widetilde{M}_2^{(\alpha)} = \widetilde{M}_2^{(\beta)}$ or
  - $\mathsf{query}^{(\alpha)} = \mathsf{dec} \wedge (A^{(\alpha)}, C_2^{(\alpha)}, C_3^{(\alpha)}) \neq (A^{(\beta)}, C_2^{(\beta)}, C_3^{(\beta)}) \wedge \widetilde{C}_2^{(\alpha)} = \widetilde{C}_2^{(\beta)}$.
- bad_3: $\exists \alpha \in [q]$ s.t. $\mathsf{query}^{(\alpha)} = \mathsf{dec}$ and $T^{(\alpha)} = 0^r$.

Let $\mathsf{bad} = \mathsf{bad}_1 \vee \mathsf{bad}_2 \vee \mathsf{bad}_3$.

$\mathcal{T}_{\mathsf{bad}}$ is a set of transcripts that satisfy bad, and $\mathcal{T}_{\mathsf{good}} := \mathcal{T} \backslash \mathcal{T}_{\mathsf{bad}}$.

5.4 Evaluation for Bad Transcript

We derive the bound of $\Pr[\mathsf{T}_4 \in \mathcal{T}_{\mathsf{bad}}]$. For $i \in [3]$, let bad_i^* be an event that bad_i occurs before the other bad events occur. Then, we have $\Pr[\mathsf{T}_4 \in \mathcal{T}_{\mathsf{bad}}] \leq \Pr[\mathsf{bad}_1^*] + \Pr[\mathsf{bad}_2^*] + \Pr[\mathsf{bad}_3^*]$. The bounds of $\Pr[\mathsf{bad}_1^*]$, $\Pr[\mathsf{bad}_2^*]$, and $\Pr[\mathsf{bad}_3^*]$ are given below, and we have $\Pr[\mathsf{T}_4 \in \mathcal{T}_{\mathsf{bad}}] \leq \frac{q_u q}{2^\ell} + \frac{q_d}{2^r}$.

Evaluating $\Pr[\mathsf{bad}_1^*]$

We first consider a pair $(\alpha, \beta) \in [q]^2$ such that $\alpha > \beta$, $\mathsf{user}^{(\alpha)} = \mathsf{user}^{(\beta)}$, and $\mathsf{query}^{(\alpha)} = \mathsf{enc}$, and evaluate the collision probability $\Pr[\widetilde{C}_2^{(\alpha)} = \widetilde{C}_2^{(\beta)}]$.

- If the inputs to $\mathcal{R}_3$ are distinct, $(A^{(\alpha)}, C_3^{(\alpha)}) \neq (A^{(\beta)}, C_3^{(\beta)})$, then $\widetilde{C}_2^{(\alpha)}$ and $\widetilde{C}_2^{(\beta)}$ are independently defined and we have $\Pr[\widetilde{C}_2^{(\alpha)} = \widetilde{C}_2^{(\beta)}] \leq \frac{1}{2^\ell}$.
- If the inputs to $\mathcal{R}_3$ are the same, i.e., $Z_3^{(\alpha)} = Z_3^{(\beta)}$, then $C_2^{(\alpha)}$ is uniformly at random from $\{0,1\}^\ell$, thus we have $\Pr[\widetilde{C}_2^{(\alpha)} = \widetilde{C}_2^{(\beta)}] \leq \frac{1}{2^\ell}$.

Regarding a pair $(\alpha, \beta) \in [q]^2$ such that $\alpha > \beta$ and $\mathsf{query}^{(\alpha)} = \mathsf{dec}$, the evaluation is the same as that with $\mathsf{query}^{(\alpha)} = \mathsf{enc}$ due to the symmetric structure of FFF. We thus have $\Pr[\widetilde{M}_2^{(\alpha)} = \widetilde{M}_2^{(\beta)}] \leq \frac{1}{2^\ell}$.

By summing these bounds for each $(\alpha, \beta) \in [q]^2$ such that $\alpha > \beta$, we have $\Pr[\mathsf{bad}_1^*] \leq \sum_{\omega \in [u]} \binom{\hat{q}_\omega}{2} \cdot \frac{1}{2^\ell} \leq \sum_{\omega \in [u]} \frac{0.5 \hat{q}_\omega^2}{2^\ell} \leq \frac{0.5 q_u q}{2^\ell}$.

Bounding $\Pr[\mathsf{bad}_2^*]$

We first consider a pair $(\alpha, \beta) \in [q]^2$ such that $\alpha > \beta$, $\mathsf{user}^{(\alpha)} = \mathsf{user}^{(\beta)}$, $\mathsf{query}^{(\alpha)} = \mathsf{enc}$, and $(A^{(\alpha)}, M_2^{(\alpha)}) \neq (A^{(\beta)}, M_2^{(\beta)})$. We evaluate the collision probability $\Pr[\widetilde{M}_2^{(\alpha)} = \widetilde{M}_2^{(\beta)}] = \Pr[M_2^{(\alpha)} \oplus M_2^{(\beta)} = Z_1^{(\alpha)} \oplus Z_1^{(\beta)}]$.

- If $A^{(\alpha)} = A^{(\beta)} \wedge M_2^{(\alpha)} \neq M_2^{(\beta)}$, then $Z_1^{(\alpha)} = Z_1^{(\beta)}$, thus we have $\Pr[\widetilde{M}_2^{(\alpha)} = \widetilde{M}_2^{(\beta)}] = 0$.
- If $A^{(\alpha)} \neq A^{(\beta)}$, then $Z_1^{(\alpha)}$ and $Z_1^{(\beta)}$ are independently chosen. We thus have $\Pr[\widetilde{M}_2^{(\alpha)} = \widetilde{M}_2^{(\beta)}] \leq \frac{1}{2^\ell}$.

We next consider a pair $(\alpha, \beta) \in [q]^2$ such that $\alpha > \beta$, $\mathsf{user}^{(\alpha)} = \mathsf{user}^{(\beta)}$, $\mathsf{query}^{(\beta)} = \mathsf{dec}$, and $(A^{(\alpha)}, C_2^{(\alpha)}, C_3^{(\alpha)}) \neq (A^{(\beta)}, C_2^{(\beta)}, C_3^{(\beta)})$. We evaluate the collision probability $\Pr[\widetilde{C}_2^{(\alpha)} = \widetilde{C}_2^{(\beta)}] = \Pr[C_2^{(\alpha)} \oplus C_2^{(\beta)} = Z_3^{(\alpha)} \oplus Z_3^{(\beta)}]$.

- If $(A^{(\alpha)}, C_3^{(\alpha)}) = (A^{(\beta)}, C_3^{(\beta)}) \wedge C_2^{(\alpha)} \neq C_2^{(\beta)}$, then $Z_3^{(\alpha)} = Z_3^{(\beta)}$, thus we have $\Pr[\widetilde{C}_2^{(\alpha)} = \widetilde{C}_2^{(\beta)}] = 0$.
- If $(A^{(\alpha)}, C_3^{(\alpha)}) \neq (A^{(\beta)}, C_3^{(\beta)})$, then $Z_3^{(\alpha)}$ and $Z_3^{(\beta)}$ are independently chosen. We thus have $\Pr[\widetilde{C}_2^{(\alpha)} = \widetilde{C}_2^{(\beta)}] \leq \frac{1}{2^\ell}$.

By summing these bounds for each $(\alpha, \beta) \in [q]^2$ such that $\alpha > \beta$, we have $\Pr[\mathsf{bad}_2^*] \leq \sum_{\omega \in [u]} \binom{\hat{q}_\omega}{2} \cdot \frac{1}{2^\ell} \leq \sum_{\omega \in [u]} \frac{0.5 \hat{q}_\omega^2}{2^\ell} \leq \frac{0.5 q_u q}{2^\ell}$.

Bounding $\Pr[\mathsf{bad}_3^*]$

For each $\alpha \in [q]$ such that $\mathsf{query}^{(\alpha)} = \mathsf{dec}$, $T^{(\alpha)}$ is chosen uniformly at random from $\{0,1\}^n$. We thus have $\Pr[\mathsf{bad}_3^*] \leq \sum_{\alpha \in [q]} \Pr[T^{(\alpha)} = 0^r] \leq \frac{q_d}{2^r}$.

5.5 Evaluation for Good Transcript

Fix a good transcript τ. Values in τ are denoted by using the symbol "$*$", e.g., $M^{*(\alpha)}, C^{*(\alpha)}, Z_1^{*(\alpha)}$, etc. Let $\tau_{M,C,T} = \{M^{*(\alpha)}, C^{*(\alpha)}, T^{*(\alpha)} \mid \alpha \in [q]\}$, and $\tau_{Z_{1,3}} = \{Z_1^{*(\alpha)}, Z_3^{*(\alpha)} \mid \alpha \in [q]\}$. For a set $\mathcal{S}$ and $i \in [3,4]$, let $\mathsf{T}_i \vdash \mathcal{S}$ be an event that sampling of T_i results in elements in $\mathcal{S}$. For each $\alpha \in [q]$, let $c_\alpha := |C^{*(\alpha)}|$. Let N_1 (resp. N_3) be the number of distinct inputs to $\mathcal{R}_1$ (resp. $\mathcal{R}_3$) defined from τ, i.e., $N_1 = \left|\{(\mathsf{user}^{*(\alpha)}, A^{*(\alpha)}, T^{*(\alpha)}) \mid \alpha \in [q]\}\right|$ and $N_3 = \left|\{(\mathsf{user}^{*(\alpha)}, A^{*(\alpha)}, C_3^{*(\alpha)}) \mid \alpha \in [q]\}\right|$. Note that by $\neg\mathsf{bad}_1$ and $\neg\mathsf{bad}_2$, τ is defined such that all $\widetilde{M}_2$ values are distinct and $\widetilde{C}_2$ values are distinct, thus the number of distinct inputs to $\mathcal{R}_2$ is q.

5.5.1 Evaluating $\Pr[\mathsf{T}_4 = \tau]$

We evaluate the probabilities $\Pr[\mathsf{T}_4 \vdash \tau_{M,C,T}]$ and $\Pr[\mathsf{T}_4 \vdash \tau_{Z_{1,3}}]$, since $\Pr[\mathsf{T}_4 = \tau] = \Pr[\mathsf{T}_4 \vdash \tau_{M,C,T}] \cdot \Pr[\mathsf{T}_4 \vdash \tau_{Z_{1,3}}]$ and $Z_2^{(\alpha)} = T^{(\alpha)} \oplus C_3^{(\alpha)}$.

- Evaluating $\Pr[\mathsf{T}_4 \vdash \tau_{M,C,T}]$. For each $\alpha \in [q]$,
  - if $\mathsf{query}^{(\alpha)} = \mathsf{enc}$, then $C^{(\alpha)}$ is chosen uniformly at random from $\{0,1\}^{c_\alpha}$, we have $\Pr[\mathsf{T}_4 \vdash \{M^{*(\alpha)}, C^{*(\alpha)}\}] = \frac{1}{2^{c_\alpha}}$, and
  - if $\mathsf{query}^{(\alpha)} = \mathsf{dec}$, then $M^{(\alpha)}$ is chosen uniformly at random from $\{0,1\}^{c_\alpha - r}$ and $T^{(\alpha)}$ is chosen uniformly at random from $\{0,1\}^r$, we have $\Pr[\mathsf{T}_4 \vdash \{M^{*(\alpha)}, C^{*(\alpha)}\}] = \frac{1}{2^{c_\alpha}}$.

  By using the probabilities, we have $\Pr[\mathsf{T}_4 \vdash \tau_{M,C,T}] = \prod_{\alpha \in [q]} \frac{1}{2^{c_\alpha}}$.
- Evaluating $\Pr[\mathsf{T}_4 \vdash \tau_{Z_{1,3}}]$. For each new input to $\mathcal{R}$, the output is chosen uniformly at random from $\{0,1\}^\ell$, thus we have $\Pr[\mathsf{T}_4 \vdash \tau_{Z_{1,3}}] = \left(\frac{1}{2^\ell}\right)^{N_1+N_3}$.

By using the probabilities, we have $\Pr[\mathsf{T}_4 = \tau] = \left(\prod_{\alpha \in [q]} \frac{1}{2^{c_\alpha}}\right) \cdot \left(\frac{1}{2^\ell}\right)^{N_1+N_3}$.

5.5.2 Evaluating $\Pr[\mathsf{T}_3 = \tau]$

We evaluate the probabilities $\Pr\left[\mathsf{T}_3 \vdash \tau_{M,C,T}\right]$ and $\Pr\left[\mathsf{T}_3 \vdash \tau_{Z_{1,3}}\right]$.

- Evaluating $\Pr\left[\mathsf{T}_3 \vdash \tau_{Z_{1,3}}\right]$. For each new input to $\mathcal{R}$, the output is chosen uniformly at random from $\{0,1\}^\ell$, thus we have $\Pr\left[\mathsf{T}_4 \vdash \tau_{Z_{1,3}}\right] = \left(\frac{1}{2^\ell}\right)^{N_1+N_3}$.
- Evaluating $\Pr\left[\mathsf{T}_3 \vdash \tau_{M,C,T}\right]$. For each $\alpha \in [q]$, if $\mathsf{query}^{(\alpha)} = \mathsf{enc}$ (resp. $\mathsf{query}^{(\alpha)} = \mathsf{dec}$), then $\neg\mathsf{bad}_2$, the input to $\Psi_{\mathsf{user}^{(\alpha)}}$ (resp. $\Psi^{-1}_{\mathsf{user}^{(\alpha)}}$) is distinct from the previous inputs, thus chosen uniformly at random from $\{0,1\}^{c_\alpha} \setminus \{\widetilde{C}^{(\beta)} \mid \beta \in [\alpha-1] \wedge \mathsf{user}^{(\beta)} = \mathsf{user}^{(\alpha)}\}$ (resp. $\{0,1\}^{c_\alpha} \setminus \{\widetilde{C}^{(\beta)} \mid \beta \in [\alpha-1] \wedge \mathsf{user}^{(\beta)} = \mathsf{user}^{(\alpha)}\}$). By $\neg\mathsf{bad}_1$ and $\neg\mathsf{bad}_2$, the input to $\mathcal{R}_2$ at the α-th query is new, thus the output is chosen uniformly at random from $\{0,1\}^r$. We thus have $\Pr[\mathsf{T}_3 \vdash \{M^{(\alpha)}, C^{(\alpha)}, T^{(\alpha)}\}] \geq \frac{1}{2^{c_\alpha - r}} \cdot \frac{1}{2^r} = \frac{1}{2^{c_\alpha}}$. By using the bound, we have $\Pr\left[\mathsf{T}_3 \vdash \tau_{M,C,T}\right] \geq \prod_{\alpha\in[q]} \frac{1}{2^{c_\alpha}}$.

By using the probabilities, we have $\Pr[\mathsf{T}_3 = \tau] \geq \left(\prod_{\alpha\in[q]} \frac{1}{2^{c_\alpha}}\right) \cdot \left(\frac{1}{2^\ell}\right)^{N_1+N_3}$.

5.5.3 Lower-bound of $\frac{\mathbf{Pr}[\mathsf{T}_3=\tau]}{\mathbf{Pr}[\mathsf{T}_4=\tau]}$

By the above bounds, we have $\frac{\Pr[\mathsf{T}_3=\tau]}{\Pr[\mathsf{T}_4=\tau]} \geq 1$.

6 Conclusion

This paper proposed FFF, a new WE mode that achieves s_{rae}-bit RAE and s_{cmt}-bit CMT-4 security with a minimum ciphertext expansion, $\max\{s_{\mathsf{cmt}}, s_{\mathsf{rae}}\}$ bits from an original message. With $s_{\mathsf{cmt}} \geq s_{\mathsf{rae}}$, s_{cmt} bits of ciphertext expansion is sufficient to achieve s_{cmt}-bit RAE and CMT-4 security. To achieve RAE and CMT-4 security with minimum ciphertext expansion, our new mode comprises a 3-round Feistel-like structure, ensuring indistinguishability under the release of unverified plaintexts. Several important questions are open for future research. In particular, achieving the same level of security with two (cf. three) hash function calls is an important challenge regarding the efficiency. Unlike our design that treats an underlying WE as a blackbox, making more rigorous optimization beyond the WE's boundary, i.e., a dedicated design, is another research challenge.

References

[ABL+14] Elena Andreeva, Andrey Bogdanov, Atul Luykx, Bart Mennink, Nicky Mouha, and Kan Yasuda. How to securely release unverified plaintext in authenticated encryption. In *ASIACRYPT 2014*, volume 8873 of *LNCS*, pages 105–125, 2014.

[ADG+22] Ange Albertini, Thai Duong, Shay Gueron, Stefan Kölbl, Atul Luykx, and Sophie Schmieg. How to abuse and fix authenticated encryption without key commitment. In *USENIX Security 2022*, pages 3291–3308, 2022.

[BDH+22] Norica Băcuieți, Joan Daemen, Seth Hoffert, Gilles Van Assche, and Ronny Van Keer. Jammin' on the deck. In *ASIACRYPT 2022*, pages 555–584, 2022.

[BH22] Mihir Bellare and Viet Tung Hoang. Efficient schemes for committing authenticated encryption. In *EUROCRYPT 2022*, volume 13276, pages 845–875, 2022.

[BHW23] Mihir Bellare, Viet Tung Hoang, and Cong Wu. The landscape of committing authenticated encryption (presentation at NIST Workshop 2023). https://csrc.nist.gov/csrc/media/Presentations/2023/landscape-of-committing-authenticated-encryption/images-media/sess-2-hoang-bcm-workshop-2023.pdf, 2023.

[BLN18] Ritam Bhaumik, Eik List, and Mridul Nandi. ZCZ - achieving n-bit SPRP security with a minimal number of tweakable-block-cipher calls. In *ASIACRYPT 2018*, pages 336–366, 2018.

[BR00] Mihir Bellare and Phillip Rogaway. Encode-then-encipher encryption: How to exploit nonces or redundancy in plaintexts for efficient cryptography. In *ASIACRYPT 2000*, pages 317–330, 2000.

[CB18] Paul Crowley and Eric Biggers. Adiantum: length-preserving encryption for entry-level processors. *IACR Trans. Symmetric Cryptol.*, 2018(4):39–61, 2018.

[CFI+23] Yu Long Chen, Antonio Flórez-Gutiérrez, Akiko Inoue, Ryoma Ito, Tetsu Iwata, Kazuhiko Minematsu, Nicky Mouha, Yusuke Naito, Ferdinand Sibleyras, and Yosuke Todo. Key committing security of AEZ and more. *IACR Trans. Symmetric Cryptol.*, 2023(4):452–488, 2023.

[CHB21] Paul Crowley, Nathan Huckleberry, and Eric Biggers. Length-preserving encryption with HCTR2. *IACR Cryptol. ePrint Arch.*, 2021.

[CR22] John Chan and Phillip Rogaway. On committing authenticated-encryption. In *ESORICS 2022*, volume 13555, pages 275–294, 2022.

[DGRW18] Yevgeniy Dodis, Paul Grubbs, Thomas Ristenpart, and Joanne Woodage. Fast message franking: From invisible salamanders to encryptment. In *CRYPTO 2018*, volume 10991, pages 155–186. Springer, 2018.

[DMMT24] Christoph Dobraunig, Krystian Matusiewicz, Bart Mennink, and Alexander Tereschenko. Efficient instances of docked double decker with AES. *IACR Cryptol. ePrint Arch.*, page 84, 2024.

[Dwo01] Morris Dworkin. NIST Special Publication 800-38A: Recommendation for block cipher modes of operation: Methods and techniques. https://csrc.nist.gov/pubs/sp/800/38/a/final, 2001.

[FOR17] Pooya Farshim, Claudio Orlandi, and Razvan Rosie. Security of symmetric primitives under incorrect usage of keys. *IACR Trans. Symmetric Cryptol.*, 2017(1):449–473, 2017.

[GDM22] Aldo Gunsing, Joan Daemen, and Bart Mennink. Deck-based wide block cipher modes and an exposition of the blinded keyed hashing model. *IACR Cryptol. ePrint Arch.*, 2022.

[GLR17] Paul Grubbs, Jiahui Lu, and Thomas Ristenpart. Message franking via committing authenticated encryption. In *CRYPTO 2017*, pages 66–97, 2017.

[HKR15] Viet Tung Hoang, Ted Krovetz, and Phillip Rogaway. Robust authenticated-encryption AEZ and the problem that it solves. In *EUROCRYPT 2015*, volume 9056 of *LNCS*, pages 15–44, 2015.

[HR04] Shai Halevi and Phillip Rogaway. A parallelizable enciphering mode. In *CT-RSA 2004*, volume 2964 of *LNCS*, pages 292–304, 2004.

[LGR21] Julia Len, Paul Grubbs, and Thomas Ristenpart. Partitioning oracle attacks. In *USENIX Security 2021*, pages 195–212, 2021.

[MLGR23] Sanketh Menda, Julia Len, Paul Grubbs, and Thomas Ristenpart. Context discovery and commitment attacks - how to break CCM, EAX, SIV, and more. In *EUROCRYPT 2023*, LNCS, pages 379–407, 2023.

[Nat23] National Institute of Standards and Technology (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.

[Nat24] National Institute of Standards and Technology (NIST). NIST workshop on the requirements for an accordion cipher mode 2024. https://csrc.nist.gov/csrc/media/Events/2024/accordion-cipher-mode-workshop-2024/documents/WorkshopAnnouncement-CipherModes2024.pdf, 2024.

[NL18] Yoav Nir and Adam Langley. ChaCha20 and Poly1305 for IETF protocols. *RFC*, 8439:1–46, 2018.

[NSS24] Yusuke Naito, Yu Sasaki, and Takeshi Sugawara. KIVR: committing authenticated encryption using redundancy and application to GCM, CCM, and more. In *ACNS 2024*, volume 14583 of *LNCS*, pages 318–347, 2024.

[Pat08] Jacques Patarin. The "Coefficients H" Technique. In *SAC 2008*, volume 5381, pages 328–345. Springer, 2008.

[ST13] Thomas Shrimpton and R. Seth Terashima. A modular framework for building variable-input-length tweakable ciphers. In *ASIACRYPT 2013*, pages 405–423, 2013.

Appendix

A Figures

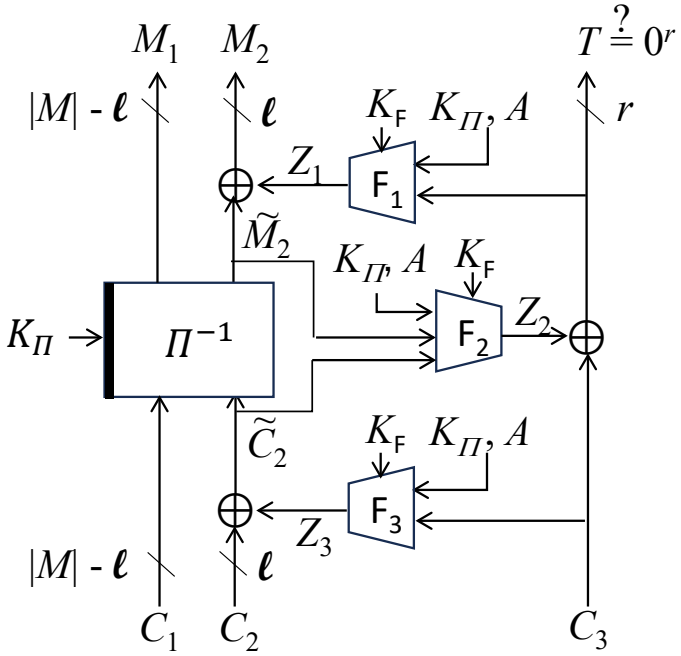

Figure 3: FFF.Dec.

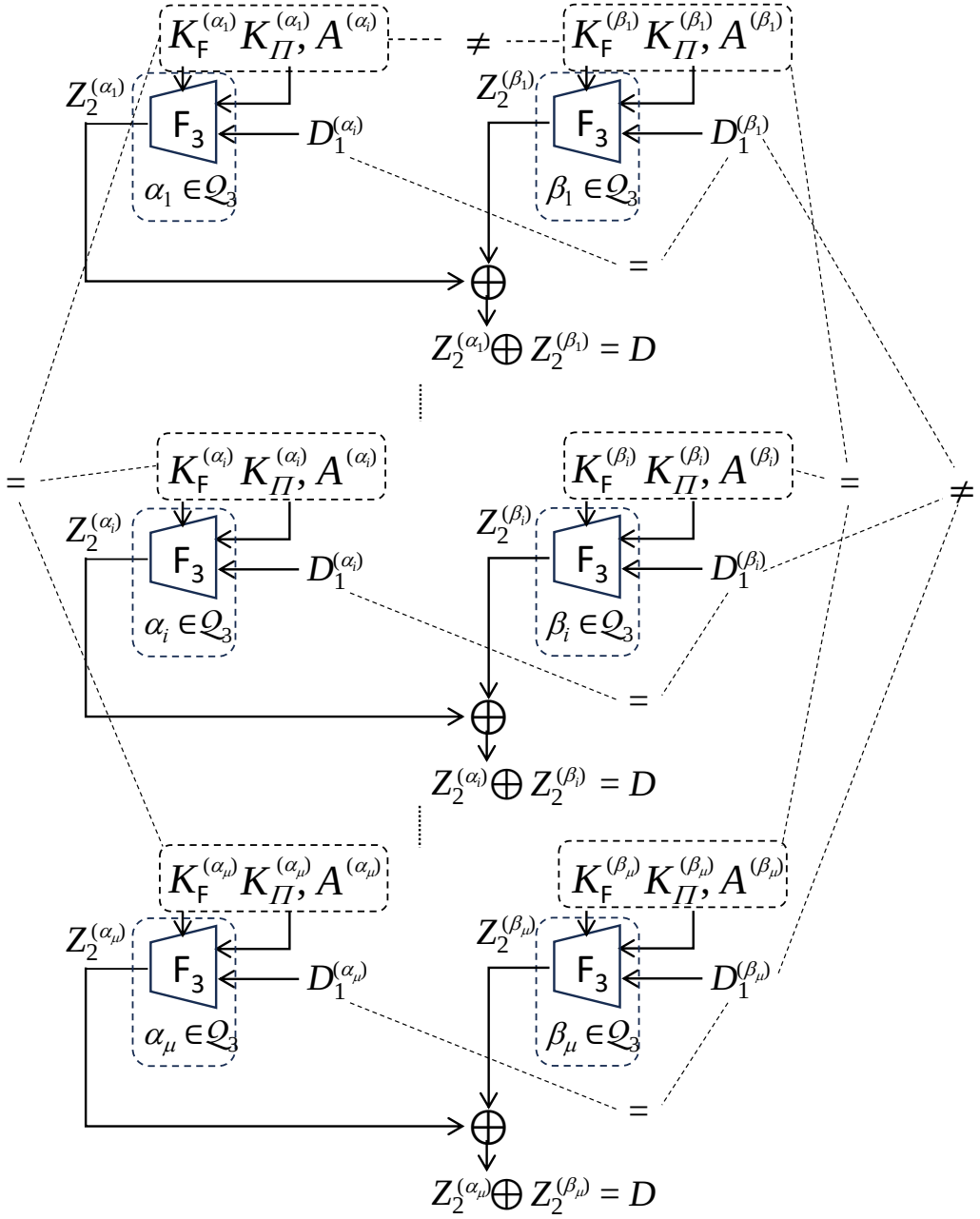

Figure 4: The conditions on the event mcoll_3.

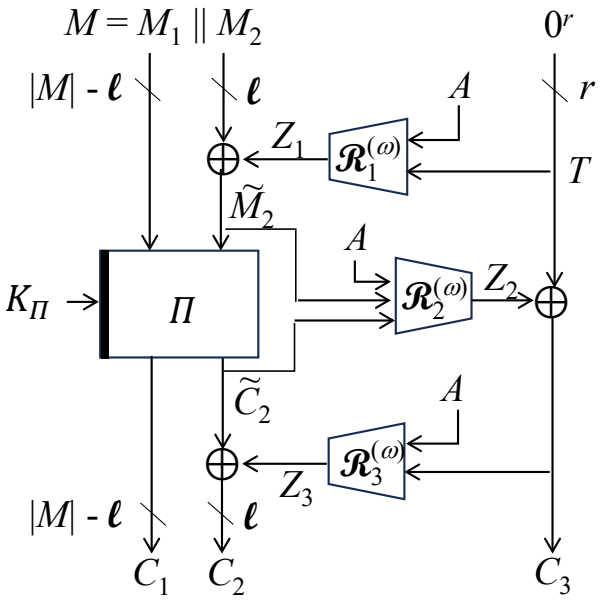

Figure 5: The ω-th user's encryption in **G**2 of the proof of Theorem 2.

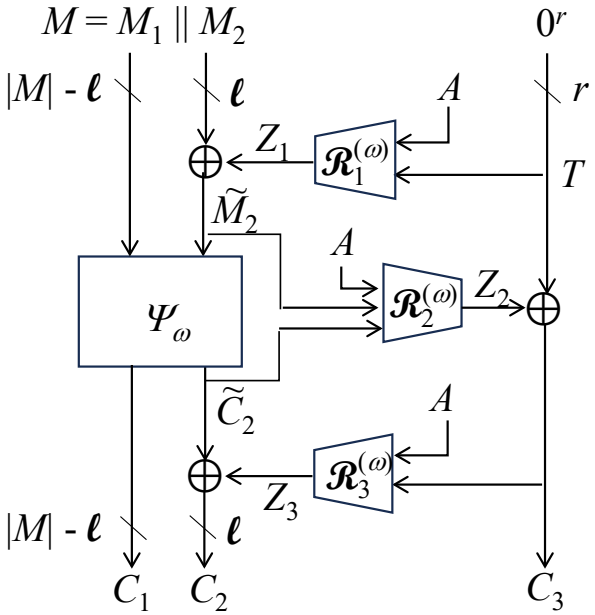

Figure 6: The ω-th user's encryption in **G**3 of the proof of Theorem 2.