IACR Transactions on Symmetric Cryptology
ISSN 2519-173X, Vol. 2025, No. 1, pp. 44–69. DOI:10.46586/tosc.v2025.i1.44-69

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), Gaithersburg, USA
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. In response to the recent call for proposal by NIST, WE and its tweakable variant, TWE, are attracting much attention in the last few years. Combined with the encode-then-encipher (EtE) construction, TWE offers an RAE that provides robustness against wide range of misuses. The list of desired properties for WE-based authenticated encryption in the NIST standardization includes committing security that considers an attacker who generates ciphertexts that can be decrypted with different decryption contexts, but TWE-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

Wide encryption (WE) is a symmetric-key primitive that realizes a strong pseudorandom permutation (SPRP) for a message of any length. Tweakable WE (TWE) is a variant with an additional tweak input, with which an independent WE is instantiated for each tweak value. Halevi and Rogaway formalized the security definition for TWE, i.e. for tweakable, variable-length, and length-preserving SPRP [HR04]. Since then, researchers have proposed WE and TWE modes, including Shrimpton–Terashima [ST13], ZCZ [BLN18], and Băcuieți et al. [BDH+22], and concrete realizations such as AEZ [HKR15]. TWE has practical applications, such as 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 TWEs [Nat23, Nat24], which stimulated even more proposals in the last few years, including the ones using double-decker and docked-double-decker [GDM22, DMMT24].

Received: 2024-09-01 Revised: 2024-11-22 Accepted: 2025-01-23 Published: 2025-03-07

TWE 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 (resp. an IV) if AE is a nonce-based (resp. IV-based) scheme. 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 TWE. TWE-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].

TWE-based EtE achieves s_{rae}-bit RAE security by appending s_{rae} bits of zeros to an m-bit message, and encrypts the encoded message with TWE to generate an $(m + s_{\mathsf{rae}})$-bit ciphertext, thus requires ciphertext expansion by s_{rae} bits. Upon decryption, EtE recovers an $(m + s_{\mathsf{rae}})$-bit encoded message, decodes the s_{rae}-bit redundancy, and checks it for authenticity. TWE's tweak input can be used to accept A. AEZ [HKR15] is a well-known realization in this category.

Key-committing security is a relatively new security model [FOR17, GLR17] for AE. This model considers an adversary not covered in RAE who generates a ciphertext that can be decrypted with multiple keys. It is relevant to 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 choose a secret key, which changes the attack setting to key-less and significantly impacts the security analysis. This causes practical attacks on most of internationally standardized AE schemes, including GCM [GLR17, DGRW18], GCM-SIV [LGR21], CCM [MLGR23], and ChaCha20-Poly1305 [GLR17, NL18]. Note that Farshim et al. [FOR17] showed that if the increase of the ciphertext size is accepted, s_{cmt}-bit key-committing security can be achieved by appending or prepending an $2s_{\mathsf{cmt}}$-bit hash digest of a key, denoted by $H(K)$, to the ciphertext.

Bellare and Hoang [BH22] (and Chan and Rogaway independently [CR22]) generalized key-committing security to context-committing security that considers the decryption context beyond the keys. They introduced the new security notion called 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 the original key-committing security [FOR17, GLR17]. Meanwhile, CMT-3 and CMT-4 are equivalent, and they are strictly more secure than CMT-1. In these models, an adversary can efficiently carry out the attack without making any online query, in the same way as certain brute-force attacks, and Chan and Rogaway [CR22] suggested that more than 80-bit security is necessary. They also pointed out that s_{cmt}-bit CMT-4 security can be achieved by extending Farshim et al.'s method so that $2s_{\mathsf{cmt}}$ bits of $H(K, A)$ are added to the ciphertext instead of $H(K)$.

Committing security of TWE is an emerging area of research as it is explicitly stated as a desirable property in the NIST call for standardization [CDD+24]. Committing security of TWE-based EtE has been rigorously studied. Grubbs et al. [GLR17] showed that EtE combined with an ideal WE satisfies a variant of CMT-1 security. Then, Chen et al. [CFI+23] pioneered cryptanalysis and security proof of concrete schemes, including AEZ, Adiantum-EtE, and HCTR2-EtE, proving that TWE-based EtE provides s_{cmt}-bit CMT-1 security with $2s_{\mathsf{cmt}}$ bits of ciphertext expansion, as summarized in Table 1. However, this security is clipped at $n/2$ or $z/2$ wherein n is a block length of an underlying block cipher and z is the number of padded zeros. With commonly used 128-bit block ciphers, i.e., $n = 128$, CMT-1 security is clipped at 64 bits, which is insufficient for the 80-bit security [CR22].

Table 1: Comparison of AEAD schemes achieving the minimum ciphertext expansion or both s_{rae}-bit RAE and s_{cmt}-bit CMT-1/CMT-4 security. The expansion is considered minimum when the target achieves the CMT 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 and RO represent an ideal cipher and a random oracle, respectively.

Scheme	Expansion bits	AE	CMT	Minimum?	Primitive	Ref.
TWE + EtE†	$2s_{\mathsf{cmt}}{}^\ddagger$	RAE	CMT-1	No	IC	[BR00, CFI+23]
Tag AE + CC	s_{cmt}	non-RAE	CMT-4	Yes	RO	[BHW23]
FFF	s_{cmt}	RAE	CMT-4	Yes	RO	Ours

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

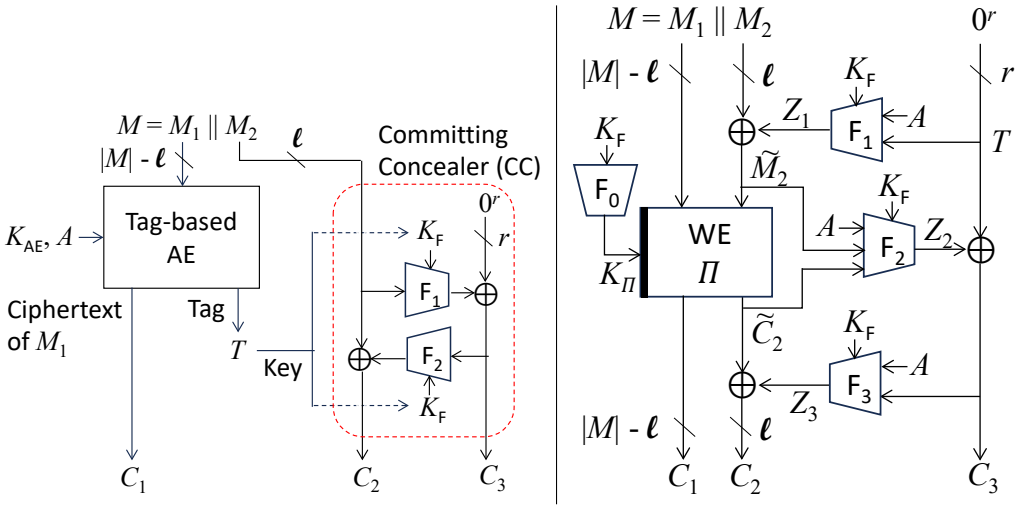

Figure 1: Existing committing mode: tag-based AE with committing concealer (left) and our committing mode FFF: WE with 3-Round Feistel (right).

The situation is even worse with CMT-4 security, and AEZ, Adiantum-EtE, and HCTR2-EtE are all broken in constant time regardless of the size of the ciphertext expansion. We can improve committing security of TWE-based EtE beyond $n/2$ bits by adding $H(K)$ or $H(K, A)$ to the ciphertext, but this causes a larger ciphertext expansion.

Obtaining CMT-4 security with minimal ciphertext expansion is a major research challenge [BHW23, NSS24]. If RAE-security is not required, 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)[1] 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 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

[1] CC is renamed to Hash-then-Mask in [BH24].

the collision resistance for the committing security, while the ciphertext expansion is only $|C_3| = r$ bits thereby achieving minimum expansion.

To achieve RAE security, CC cannot be directly applied to TWE. TWE has no tag, and an attempt to use a fraction of TWE'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.

1.1 Design Goals

This paper improves the committing security of TWE-based AEs. In particular, we propose a new method of building an AE scheme satisfying the following criteria from a WE, or a TWE with a fixed tweak.

- **RAE Security**: We focus on an AE scheme achieving RAE security that provides strong robustness against several misuses. We aim at s_{rae} bits of RAE security.
- CMT-4 **Security**: We target CMT-4 security that is strictly more secure than CMT-1 and is unavailable with a simple EtE. We aim at s_{cmt} bits of CMT-4 security.
- **Minimum Ciphertext Expansion**: The design satisfies the minimum ciphertext expansion, which is $\max\{s_{\mathsf{cmt}}, s_{\mathsf{rae}}\}$.

1.2 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 minimum; the ciphertext size is only $\max\{s_{\mathsf{cmt}}, s_{\mathsf{rae}}\}$ bits larger than the message size. The primitive is WE (cf. TWE) because AD is processed separately, not inside the tweak of TWE. The proposed mode also supports TWE by using a fixed constant for its tweak. Note that FFF's overhead is negligible for a long message and a short AD because the additional costs are independent of 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 a WE scheme Π for $|M|$-bit inputs and a 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. Note that, as later explained, the parameters ℓ and r are chosen depending on the required security levels s_{rae} and s_{cmt}. The expansion size only depends on r and is irrelevant to ℓ.

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.[2,3] All of them take a WE key K_Π and associated data A as inputs.[4] 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]A CMT-4 adversary can choose K_Π but the standard security assumption for WE does not support collision resistance. To ensure CMT-4 security, the WE's key K_Π is input to the three hash functions as well as the WE. The independent keys K_Π and K_{F} are required for the SPRP assumption on the WE and the PRF one on the keyed hash function in the proof of the RAE security.

[4]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 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 rationale for the design is explained by the target security. To ensure RAE security, broadly speaking, any single-bit modification in M_1, M_2, or A must result in a random alteration of all components C_1, C_2, and C_3. 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 a 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 $((K'_\Pi, A', M'_1, M'_2), (K^*_\Pi, A^*, M^*_1, M^*_2))$ whose tuples of the first three values are distinct and the ciphertexts $C'_1 \| C'_2 \| C'_3$ and $C^*_1 \| C^*_2 \| C^*_3$ are the same. Then, the CMT-4 security is reduced to the collision resistance of the $C^*_2 \| C^*_3$ part of the last 2-round of the 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 2-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, i.e., $\ell = \max\{2s_{\mathsf{rae}}, s_{\mathsf{cmt}}\}$, $r = \max\{s_{\mathsf{rae}}, s_{\mathsf{cmt}}\}$. If $s_{\mathsf{rae}} \leq s_{\mathsf{cmt}}/2$, then by choosing the parameters such that $r = \ell = s_{\mathsf{cmt}}$, the size of the ciphertext expansion of FFF, i.e. the size of r, is minimum regarding CMT-4 security. If $s_{\mathsf{cmt}}/2 < s_{\mathsf{rae}} \leq s_{\mathsf{cmt}}$, then by choosing the parameters such that $r = s_{\mathsf{cmt}}$ 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. As examples, we show parameters $(s_{\mathsf{cmt}}, s_{\mathsf{rae}})$ for the following three cases. For the case (1) $(s_{\mathsf{cmt}}, s_{\mathsf{rae}}) = (128, 64)$, the parameters must be $r \geq 128$ and $\ell \geq 128$. For the case (2) $(s_{\mathsf{cmt}}, s_{\mathsf{rae}}) = (128, 128)$, the parameters must be $r \geq 128$ and $\ell \geq 256$. For the case (3) $(s_{\mathsf{cmt}}, s_{\mathsf{rae}}) = (80, 128)$, the parameters must be $r \geq 128$ and $\ell \geq 256$.

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. Lastly, as a specific failure example, let us consider the case that the 3-round Feistel-like structure of FFF having some interaction with WE is replaced with a mere 3-round Feistel network that is independent from WE. Proving security of such a construction is impossible because 3-round Feistel network with secret random functions can be broken with three queries by CCA-adversaries. Moreover, calling a 3-round Feistel network independently of WE like the previous committing concealer makes it RAE-insecure as explained before, though 2-round Feistel network could be sufficient only for committing security.

1.3 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 CMT-4 security by combining HtE with TWE 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 $0 \le i \le j$, let $[i, j] \coloneqq \{i, i+1, \ldots, j\}$ and $[j] \coloneqq [1, j]$. Let ε be the empty string, $\emptyset$ the empty set, and $\{0,1\}^*$ the set of all bit strings. For an integer $n \ge 0$, let $\{0,1\}^n$ be the set of all n-bit strings and $\{0,1\}^0 \coloneqq \{\varepsilon\}$. For an integer $n \ge 0$, let $\{0,1\}^{\ge n}$ be the set of all strings of lengths $\ge n$. Let 0^i be the bit string of i-bit zeros. For $X \in \{0,1\}^j$, let $|X| \coloneqq j$. The concatenation of two bit strings X and Y is written as $X\|Y$ or XY when no confusion is possible. For integers $0 \le j, i$ 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 $j \ge i$, 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 $l_1, \ldots, l_j \ge 0$ 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. For an integer $k_{\mathsf{we}} \ge 0$, let $\{0,1\}^{k_{\mathsf{we}}}$ and $\mathcal{M}_{\mathsf{we}}$ be the sets of keys and plaintexts. A WE $\Pi : \{0,1\}^{k_{\mathsf{we}}} \times \mathcal{M}_{\mathsf{we}} \to \mathcal{M}_{\mathsf{we}}$ is such that for any key $K_\Pi \in \{0,1\}^{k_{\mathsf{we}}}$ and distinct plaintexts $M, M' \in \mathcal{M}_{\mathsf{we}}$, $|M| = |\Pi(K_\Pi, M)|$ and $\Pi(K_\Pi, M) \ne \Pi(K_\Pi, M')$ 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 $k_{\mathsf{we}} = 0$ 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 $i \in [u]$, $K^{(i)} \xleftarrow{\$} \{0,1\}^{k_{\mathsf{we}}}$.
- 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, $\mathbf{A}$ returns a decision bit in $\{0,1\}$. Let $\mathbf{A}^{\mathcal{O}} \in \{0,1\}$ be the 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

$$\mathbf{Adv}_{\Pi}^{\text{mu-sprp}}(\mathbf{A}) = \Pr\left[\mathbf{A}^{\Pi_{K^{(1)}},\Pi^{-1}_{K^{(1)}},\ldots,\Pi_{K^{(u)}},\Pi^{-1}_{K^{(u)}}} = 1\right] - \Pr\left[\mathbf{A}^{\Psi_1,\Psi_1^{-1},\ldots,\Psi_u,\Psi_u^{-1}} = 1\right].$$

2.4 Random Oracle

For the committing security of our mode, the underlying hash function is assumed to be a random oracle. 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 Collision Resistance

In the committing security proof, the committing security is reduced to the collision resistance of the last two rounds of our mode. For a positive integer l and a non-empty set $\mathcal{M} \subseteq \{0,1\}^*$, let $\mathsf{H}[\mathsf{F}] : \mathcal{M} \to \{0,1\}^l$ be an l-bit hash function with a random oracle $\mathsf{F} : \mathcal{M} \to \{0,1\}^s$. $\mathsf{H}[\mathsf{F}]$ is collision resistance if it is hard to find two distinct inputs that hash to the same output. The collision advantage of an adversary $\mathbf{A}$ is defined as

$$\mathbf{Adv}_{\mathsf{H}[\mathsf{F}]}^{\text{coll}}(\mathbf{A}) \coloneqq \Pr\left[\mathsf{H}[\mathsf{F}](M') = \mathsf{H}[\mathsf{F}](M^*) : (M', M^*) \leftarrow \mathbf{A}^{\mathsf{F}}\right] ,$$

where $(M', M^*) \leftarrow \mathbf{A}^{\mathsf{F}}$ means that $\mathbf{A}$ first interacts with F and then returns the pair (M', M^*). We assume that the input-output pairs of F that are defined in the computation of $\mathsf{H}[\mathsf{F}](M')$ and $\mathsf{H}[\mathsf{F}](M^*)$ are defined by adversary's queries, since all the pairs are necessary to check the collision. Our committing-security proofs assume that $\mathbf{A}$ is a computationally unbounded adversary.

2.6 Pseudorandom Function (PRF)

For the RAE security of our mode, the underlying keyed hash functions are assumed to be 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 the 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

$$\mathbf{Adv}_{\mathsf{F}}^{\text{mu-prf}}(\mathbf{A}) \coloneqq \Pr\left[\mathbf{A}^{\mathsf{F}_{K^{(1)}},\ldots,\mathsf{F}_{K^{(u)}}} = 1\right] - \Pr\left[\mathbf{A}^{\mathcal{R}^{(1)},\ldots,\mathcal{R}^{(u)}} = 1\right] .$$

In our RAE-security proof, $\mathbf{A}$ is a computationally-bounded adversary.

2.7 Authenticated Encryption (AE)

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. 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 $\forall K \in \mathcal{K}, A \in \mathcal{A}, M \in \mathcal{M} : \mathsf{AE.Dec}(K, A, \mathsf{AE.Enc}(K, A, M)) = M$.

2.8 Committing Security

For the notion of committing security, we use 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.

[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 $\mathbf{A}$ is defined as

$$\mathbf{Adv}^{\mathsf{cmt}\text{-}i}_{\mathsf{AE}[\mathsf{F}]}(\mathbf{A}) \coloneqq \Pr\Big[(K', A', M'), (K^*, A^*, M^*) \leftarrow \mathbf{A}^{\mathsf{F}} \text{ s.t.} \\ \mathsf{WiC}_i(K', A', M') \neq \mathsf{WiC}_i(K^*, A^*, M^*) \wedge C' = C^*\Big] \ .$$

We assume that all input-output pairs of ideal primitives, including F, required to calculate $C^* = \mathsf{AE.Enc}[\mathsf{F}](K', A', M')$ and $C^* = \mathsf{AE.Enc}[\mathsf{F}](K^*, A^*, M^*)$ 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*

$$\mathbf{Adv}^{\mathsf{cmt}\text{-}4}_{\mathsf{AE}[\mathsf{F}]}(\mathbf{A}_4) \leq \mathbf{Adv}^{\mathsf{cmt}\text{-}3}_{\mathsf{AE}[\mathsf{F}]}(\mathbf{A}_3) \ .$$

2.9 Robust-AE (RAE) Security

We use a slight variant of the notion of RAE security defined in [HKR15]. The variant notion mu-RAE is indistinguishability between AE and an ideal AE with decryption leakage in the multi-user setting.[5]

In the mu-RAE-security game, we consider the decryption function with leakage functionality, denoted by AE.DecL. AE.DecL takes the same inputs as AE.Dec, i.e., the input 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). AE.Enc (resp. AE.DecL) with a key K is denoted by $\mathsf{AE}_K.\mathsf{Enc}$ (resp. $\mathsf{AE}_K.\mathsf{DecL}$). Let $\mathsf{AEL}_K := (\mathsf{AE}_K.\mathsf{Enc}, \mathsf{AE}_K.\mathsf{DecL})$.

In the mu-RAE-security game with u users, an adversary $\mathbf{A}$ has access to either real-world oracles $(\mathsf{AEL}_{K^{(1)}}, \ldots, \mathsf{AEL}_{K^{(u)}})$ or ideal-world ones $((\$^{(1)}_{\mathsf{Enc}}, \$^{(1)}_{\mathsf{Dec}}), \ldots, (\$^{(u)}_{\mathsf{Enc}}, \$^{(u)}_{\mathsf{Dec}}))$. For each $\omega \in [u]$, $K^{(\omega)}$ is a ω-th user's key defined as $K^{(\omega)} \xleftarrow{\$} \mathcal{K}$. $\$^{(\omega)}_{\mathsf{Enc}}$ is a random-bit oracle of the ω-th user that takes a pair (A, M) of AD and a plaintext, and returns a random ciphertext

[5] Our ideal AE returns values that are randomly chosen with replacement where in the original notion given in [HKR15], the ideal AE returns values that are randomly chosen without replacement.

Algorithm 1 FFF

Encryption $\mathsf{FFF.Enc}[\Pi_{\mathsf{F}_0(K_\mathsf{F})}, \mathsf{F}_{K_\mathsf{F}}](A, M)$ where $|M| \geq \ell$

1: $(M_1, M_2) \xleftarrow{|M|-\ell,\ell} M$
2: $\widetilde{M_2} \leftarrow \mathsf{F}_1(K_\mathsf{F}, (A, 0^r)) \oplus M_2$ ▷ 1st Round
3: $\widetilde{M} \leftarrow M_1 \| \widetilde{M_2}$; $\widetilde{C} \leftarrow \Pi_{\mathsf{F}_0(K_\mathsf{F})}(\widetilde{M})$; $(C_1, \widetilde{C_2}) \xleftarrow{|\widetilde{C}|-\ell,\ell} \widetilde{C}$ ▷ Perform WE
4: $C_3 \leftarrow \mathsf{F}_2(K_\mathsf{F}, (A, \widetilde{M_2}, \widetilde{C_2}))$ ▷ 2nd Round
5: $C_2 \leftarrow \mathsf{F}_3(K_\mathsf{F}, (A, C_3)) \oplus \widetilde{C_2}$ ▷ 3rd Round
6: $C \leftarrow C_1 \| C_2 \| C_3$; **return** C

Decryption $\mathsf{FFF.Dec}[\Pi^{-1}_{\mathsf{F}_0(K_\mathsf{F})} \mathsf{F}_{K_\mathsf{F}}](A, C)$ where $|C| \geq \ell + r$

1: $(C_1, C_2, C_3) \xleftarrow{|C|-(\ell+r),\ell,r} C$
2: $\widetilde{C_2} \leftarrow \mathsf{F}_3(K_\mathsf{F}, (A, C_3)) \oplus C_2$ ▷ 3rd Round
3: $\widetilde{C} \leftarrow C_1 \| \widetilde{C_2}$; $\widetilde{M} \leftarrow \Pi_{\mathsf{F}_0(K_\mathsf{F})}(\widetilde{C})$; $(M_1, \widetilde{M_2}) \xleftarrow{|\widetilde{M}|-\ell,\ell} \widetilde{M}$ ▷ Perform WE
4: $T \leftarrow \mathsf{F}_2(K_\mathsf{F}, (A, \widetilde{M_2}, \widetilde{C_2})) \oplus C_3$ ▷ 2nd Round
5: $M_2 \leftarrow \mathsf{F}_1(K_\mathsf{F}, (A, T)) \oplus \widetilde{M_2}$
6: **if** $T = 0^r$ **then** $M \leftarrow M_1 \| M_2$; **return** M; **else return reject end if**

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, $\mathbf{A}$ returns 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 $\mathcal{O}$. The mu-RAE-security advantage function of $\mathbf{A}$ is defined as

$$\mathbf{Adv}^{\mathsf{mu\text{-}rae}}_{\mathsf{AE}}(\mathbf{A}) := \Pr\left[\mathbf{A}^{\mathsf{AEL}_{K^{(1)}},\ldots,\mathsf{AEL}_{K^{(u)}}} = 1\right] - \Pr\left[\mathbf{A}^{\$^{(1)}_{\mathsf{Enc}},\$^{(1)}_{\mathsf{Dec}},\ldots,\$^{(u)}_{\mathsf{Enc}},\$^{(u)}_{\mathsf{Dec}}} = 1\right] \ ..$$

3 FFF: Committing Wide Encryption Mode

We first define our mode FFF that has a 3-round Feistel-like structure with WE. We then show the CMT-4-security bound of FFF, followed by the mu-RAE-security bound.

3.1 Specifications of FFF

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 $\Pi : \{0,1\}^{k_\mathsf{we}} \times \{0,1\}^{\geq \ell} \to \{0,1\}^{\geq \ell}$ be a WE, where k_we is the key length and $\{0,1\}^{k_\mathsf{we}}$ is the key space.[6] Let $\mathsf{F} : \mathcal{K}_\mathsf{prf} \times ([0,3] \times \mathcal{A} \times \{0,1\}^* \times \{0,1\}^*) \to \{0,1\}^{\max\{k_\mathsf{we}, \ell, r\}}$ 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 $K_\mathsf{F} \in \mathcal{K}_\mathsf{prf}$, $A \in \mathcal{A}$, $D_1 \in \{0,1\}^*$, and $D_2 \in \{0,1\}^*$, let $\mathsf{F}_0(K_\mathsf{F}) := \mathsf{msb}_{k_\mathsf{we}} \circ \mathsf{F}(K_\mathsf{F}, (0, \varepsilon, \varepsilon, \varepsilon)$ be a key-derivation function that generates a key of the WE, $\mathsf{F}_1(K_\mathsf{F}, (A, D_1)) := \mathsf{msb}_\ell \circ \mathsf{F}(K_\mathsf{F}, (1, A, D_1, \varepsilon)$ the 1st-round function of the 3-round Feistel-like structure, $\mathsf{F}_2(K_\mathsf{F}, (A, D_1, D_2) := \mathsf{msb}_r \circ \mathsf{F}(K_\mathsf{F}, (2, A, D_1, D_2))$ the 2nd-round function, and $\mathsf{F}_3(K_\mathsf{F}, (A, D_1)) := \mathsf{msb}_\ell \circ \mathsf{F}(K_\mathsf{F}, (3, A, D_1, \varepsilon))$ 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. 2-(left)). $\mathsf{FFF.Enc}[\Pi_{\mathsf{F}_0(K_\mathsf{F})}, \mathsf{F}_{K_\mathsf{F}}]$ (resp. $\mathsf{FFF.Dec}[\Pi^{-1}_{\mathsf{F}_0(K_\mathsf{F})}, \mathsf{F}_{K_\mathsf{F}}]$) is the encryption (resp. decryption) function. We require that

[6] Note that when using a TWE, the tweak is fixed to some constant string such as the empty string.

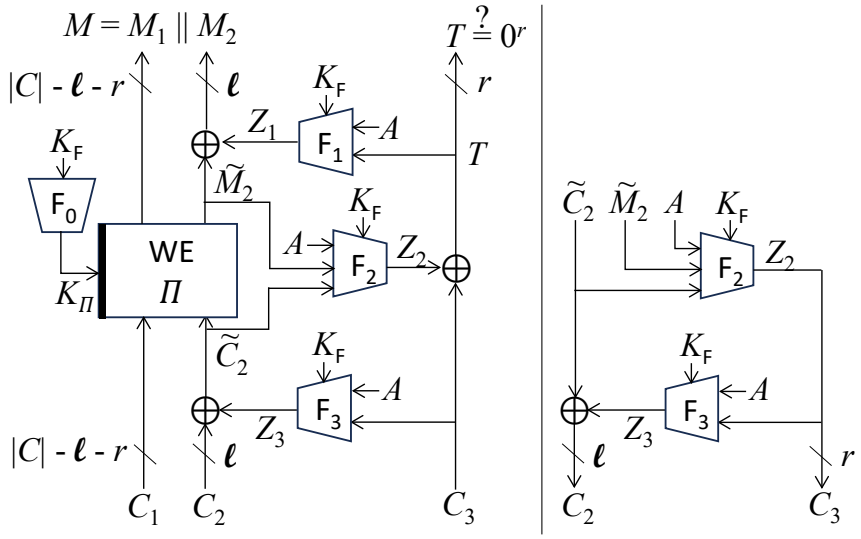

Figure 2: FFF.Dec (left) and FF (right)

the lengths of plaintexts (resp. ciphertexts) are greater than or equal to ℓ (resp. $\ell + r$). We define the decryption function with leakage functionality $\mathsf{FFF.DecL}[\Pi^{-1}_{\mathsf{F}_0(K_\mathsf{F})}, \mathsf{F}_{K_\mathsf{F}}]$ as follows. For each input tuple (K_F, A, C), $\mathsf{FFF.DecL}[\Pi^{-1}_{\mathsf{F}_0(K_\mathsf{F})}, \mathsf{F}_{K_\mathsf{F}}]$ returns (M, T) as well as $\mathsf{vrf} \in \{\mathbf{accept}, \mathbf{reject}\}$, where $\mathsf{vrf} = \mathsf{FFF.Dec}[\Pi^{-1}_{\mathsf{F}_0(K_\mathsf{F})}, \mathsf{F}_{K_\mathsf{F}}](A, C)$, 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*

$$\mathbf{Adv}^{\mathsf{cmt\text{-}4}}_{\mathsf{FFF}}(\mathbf{A}) \leq \frac{\ell + r}{\log_2(\ell + r)} \cdot \frac{p}{2^{\min\{r,\ell\}}} + \left(24(\ell + r) \cdot \frac{p}{2^{\min\{r,\ell\}}}\right)^{\frac{\ell+r}{\log_2(\ell+r)}} .$$

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 most* t*, there exist an* mu-SPRP *adversary* $\mathbf{A}_\Pi$ *and an* mu-PRF *adversary* $\mathbf{A}_\mathsf{F}$ *such that*

$$\mathbf{Adv}^{\mathsf{mu\text{-}rae}}_{\mathsf{FFF}}(\mathbf{A}) \leq \frac{q_u q}{2^\ell} + \frac{q_d}{2^r} + \mathbf{Adv}^{\mathsf{mu\text{-}sprp}}_{\Pi}(\mathbf{A}_\Pi) + \mathbf{Adv}^{\mathsf{mu\text{-}prf}}_{\mathsf{F}}(\mathbf{A}_\mathsf{F}) ,$$

and $\mathbf{A}_\Pi$ *and* $\mathbf{A}_{\mathsf{F}_1}$ *make at most* q *queries, have access to* u *users, and run in time* $O(q + t)$.

Algorithm 2 FF

Procedure $\mathsf{FF}[\mathsf{F}](K_{\mathsf{F}}, A, \widetilde{M}_2, \widetilde{C}_2)$
1: $C_3 \leftarrow \mathsf{F}_2(K_{\mathsf{F}}, A, \widetilde{M}_2, \widetilde{C}_2)$; $C_2 \leftarrow \mathsf{F}_3(K_{\mathsf{F}}, A, C_3) \oplus \widetilde{C}_2$; **return** $C_2 \| C_3$

The bound ensures that FFF is mu-RAE secure for up to $\min\{2^{\ell/2}, 2^r\}$ queries, assuming that the advantage functions of the mu-SPRP security of Π and of the mu-PRF security of F are respectively negligible compared with the other terms. Then, 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 where F is a random oracle. Without loss of generality, assume that $\mathbf{A}$ is deterministic and makes no repeated query.

4.1 Reducing the CMT-3 Security to the Collision Resistance of FF

We first introduce FF, which is a special case of SIV [RS06]. The specification of FF is given in Algorithm 2 and Fig. 2-(right). FF is equal to FFF without Π and the first-round function F_1, and the following lemma shows that the CMT-3 security of FFF can be reduced to the collision resistance of FF with a condition for inputs. Note that all inputs are public in these games.

Lemma 2. *For any* CMT-3 *adversary* $\mathbf{A}$ *making at most* p *offline queries, there exists a collision-finding adversary* $\mathbf{B}$ *such that*

$$\mathbf{Adv}^{\mathsf{cmt\text{-}3}}_{\mathsf{FFF}}(\mathbf{A}) \leq \mathbf{Adv}^{\mathsf{coll}}_{\mathsf{FF}}(\mathbf{B}) \ ,$$

$\mathbf{B}$ *makes* p *offline queries and the pairs of AD and key in* $\mathbf{B}$*'s output are distinct, i.e.,* $(K'_{\mathsf{F}}, A') \neq (K^*_{\mathsf{F}}, A^*)$.

We evaluate the collision resistance of FF with the condition $(K'_{\mathsf{F}}, A') \neq (K^*_{\mathsf{F}}, A^*)$ in Section 4.2.

Proof of Lemma 2

Let Π be a WE scheme of FFF with ideal primitive(s) $P_1, \ldots, P_i$. In the CMT-3-security game, an output of FFF can be computed by offline computations, and its output can be derived from the public procedure and making queries to the ideal primitives. We can ignore an ideal primitive if it is not used by Π. The random oracles for $\mathbf{A}$ and $\mathbf{B}$ are distinguished and denoted as $\mathsf{F}^{\mathbf{a}}$ and $\mathsf{F}^{\mathbf{b}}$, respectively.

For a CMT-3 adversary $\mathbf{A}$ targeting FFF with access to $\mathsf{F}^{\mathbf{a}}$, we construct a collision-finding adversary $\mathbf{B}$ targeting FF with access to $\mathsf{F}^{\mathbf{b}}$. The adversary $\mathbf{B}$ simulates $\mathbf{A}$'s environment in the following procedure that involves the random oracle $\mathsf{F}^{\mathbf{a}}$ and the ideal primitives $P_1, \ldots, P_i$ simulated by $\mathbf{B}$.

1. For each query $(K, (i, A, D_1, D_2)) \in \mathcal{K}_{\mathsf{prf}} \times ([0,3] \times \mathcal{A} \times \{0,1\}^* \times \{0,1\}^*)$ to $\mathsf{F}^{\mathbf{a}}$ made by the adversary $\mathbf{A}$, the adversary $\mathbf{B}$
   (a) makes the same query $(K, (i, A, D_1, D_2))$ to $\mathbf{B}$'s random oracle $\mathsf{F}^{\mathbf{b}}$,
   (b) receives the response $Z = \mathsf{F}^{\mathbf{b}}(K, (i, A, D_1, D_2))$ from $\mathsf{F}^{\mathbf{b}}$, and

(c) returns Z to the adversary $\mathbf{A}$ as the output of $\mathsf{F}^{\mathbf{a}}(K,(i,A,D_1,D_2))$.

2. If Π uses ideal primitives $P_1,\ldots,P_i$, then for each query X to P_j ($j\in[i]$) made by the adversary $\mathbf{A}$, the adversary $\mathbf{B}$

   (a) defines the output $Y=P_j(X)$, appropriately,[7] and

   (b) returns Y to the adversary $\mathbf{A}$.

3. The adversary $\mathbf{A}$ outputs $(K'_{\mathsf{F}},A',M'),(K^*_{\mathsf{F}},A^*,M^*)$ in their CMT-3-security game.

4. The adversary $\mathbf{B}$

   - calculates the ciphertexts $C'_1\|C'_2\|C'_3=\mathsf{FFF.Enc}[\Pi_{\mathsf{F}^{\mathbf{b}}_0(K'_{\mathsf{F}})},\mathsf{F}^{\mathbf{b}}_{K'_{\mathsf{F}}}](A',M')$ and $C^*_1\|C^*_2\|C^*_3=\mathsf{FFF.Enc}[\Pi_{\mathsf{F}^{\mathbf{b}}_0(K^*_{\mathsf{F}})},\mathsf{F}^{\mathbf{b}}_{K^*_{\mathsf{F}}}](A^*,M^*)$,[8]
   - finds the internal values $Z'_1=\mathsf{F}^{\mathbf{b}}_1(K'_{\mathsf{F}},(A',0^r))$, $Z^*_1=\mathsf{F}^{\mathbf{b}}_1(K^*_{\mathsf{F}},(A^*,0^r))$, $Z'_3=\mathsf{F}^{\mathbf{b}}_1(K'_{\mathsf{F}},(A',C'_3))$, and $Z^*_3=\mathsf{F}^{\mathbf{b}}_1(K^*_{\mathsf{F}},(A^*,C^*_3))$ from the query-response history of $\mathbf{A}$, and
   - calculates $\widetilde{M}'_2=Z'_1\oplus M'_2$, $\widetilde{M}^*_2=Z^*_1\oplus M^*_2$, $\widetilde{C}'_2=Z'_3\oplus C'_2$, and $\widetilde{C}^*_2=Z^*_3\oplus C^*_2$.

5. The adversary $\mathbf{B}$ returns $(K'_{\mathsf{F}},A',\widetilde{M}'_2,\widetilde{C}'_2)$ and $(K^*_{\mathsf{F}},A^*,\widetilde{M}^*_2,\widetilde{C}^*_2)$.

Since the outputs of $\mathsf{F}^{\mathbf{a}}$ are defined by using $\mathsf{F}^{\mathbf{b}}$, and $\mathsf{FF}[\mathsf{F}^{\mathbf{b}}]$ is equal to FFF without Π and the first-round function $\mathsf{F}^{\mathbf{a}}_1$, if $\mathbf{A}$ breaks the CMT-3-security of FFF with $\mathsf{F}^{\mathbf{a}}$, i.e., $C'_1\|C'_2\|C'_3=C^*_1\|C^*_2\|C^*_3\wedge(K'_{\mathsf{F}},A')\neq(K^*_{\mathsf{F}},A^*)$, then the above adversary $\mathbf{B}$ breaks the collision resistance of FF such that $(K'_{\mathsf{F}},A')\neq(K^*_{\mathsf{F}},A^*)$, i.e., $(K'_{\mathsf{F}},A')\neq(K^*_{\mathsf{F}},A^*)$ and $C'_2\|C'_3=\mathsf{FF}[\mathsf{F}^{\mathbf{b}}](K'_{\mathsf{F}},A',\widetilde{M}'_2,\widetilde{C}'_2)=\mathsf{FF}[\mathsf{F}^{\mathbf{b}}](K^*_{\mathsf{F}},A^*,\widetilde{M}^*_2,\widetilde{C}^*_2)=C^*_2\|C^*_3$.

□[proof of Lemma 2]

4.2 Collision Resistance of FF with $(K'_{\mathsf{F}},A')\neq(K^*_{\mathsf{F}},A^*)$

We evaluate the collision resistance of $\mathsf{FF}[\mathsf{F}]$ with the condition $(K'_{\mathsf{F}},A')\neq(K^*_{\mathsf{F}},A^*)$ for an adversary $\mathbf{B}$ making p offline queries to the random oracle F. The goal of $\mathbf{B}$ is to find a collision of $\mathsf{FF}[\mathsf{F}]$ such that $(K'_{\mathsf{F}},A')\neq(K^*_{\mathsf{F}},A^*)$, i.e., for $\mathbf{B}$'s output $I'=(K'_{\mathsf{F}},A',\widetilde{M}'_2,\widetilde{C}'_2)$ and $I^*=(K^*_{\mathsf{F}},A^*,\widetilde{M}^*_2,\widetilde{C}^*_2)$, $C'_2\|C'_3=C^*_2\|C^*_3$ and $(K'_{\mathsf{F}},A')\neq(K^*_{\mathsf{F}},A^*)$ hold. Let coll be the collision event. The formal definition is given later. Fig. 3 depicts the structure of the collision event. The collision event requires four input-output tuples of F labeled with (A2),(A3),(B2),(B3) in Fig. 3. Z'_2 and Z'_3 are respectively outputs of F_2 and F_3 for I'. Z^*_2 and Z^*_3 are respectively outputs of F_2 and F_3 for I^*. Without loss of generality, we assume that one of the "$*$"-outputs (labeled with (A2), (A3)) is defined after the other three outputs. We call the output "latest output."

4.2.1 Intuition

We consider the following two cases for Z^*_2 and Z^*_3.

- Case 1: Z^*_3 is the latest output.
- Case 2: Z^*_2 is the latest output.

[7] The random primitives can be simulated by lazy sampling.

[8] Note that from the definition of CMT-3 in Section 2.8, $\mathbf{A}$ must make queries to $P_1,\ldots,P_i$, and $\mathsf{F}^{\mathbf{a}}$ for calculating the outputs $C'_1\|C'_2\|C'_3=\mathsf{FFF.Enc}[\Pi_{\mathsf{F}^{\mathbf{b}}_0(K'_{\mathsf{F}})},\mathsf{F}^{\mathbf{b}}_{K'_{\mathsf{F}}}](A',M')$ and $C^*_1\|C^*_2\|C^*_3=\mathsf{FFF.Enc}[\Pi_{\mathsf{F}^{\mathbf{b}}_0(K^*_{\mathsf{F}})},\mathsf{F}^{\mathbf{b}}_{K^*_{\mathsf{F}}}](A^*,M^*)$. The other non-ideal procedures of FFF are public. Hence, $\mathbf{B}$ can calculate $C'_1\|C'_2\|C'_3$ and $C^*_1\|C^*_2\|C^*_3$ using the query-response history of $\mathbf{A}$ and the procedures of FFF.

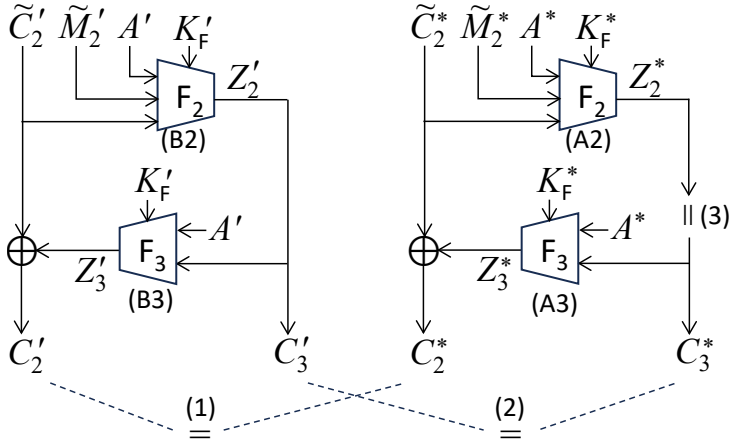

Figure 3: Bad event coll where $(K_{\mathsf{F}}', A') \neq (K_{\mathsf{F}}^*, A^*)$ and Eqs. (1), (2), (3) hold. Z_2^* or Z_3^* is defined after the other three outputs.

We evaluate the probability for the event coll with Case 1 by using an $(\ell + r)$-multi-collision event in Z_2 values of r bits. For each of the $\ell+r$ outputs of F_2, the probability that the $\ell + r$ outputs are the same is at most $\left(\frac{1}{2^r}\right)^{\ell+r-1}$. Hence, the multi-collision probability is at most $\binom{p}{\ell+r}\left(\frac{1}{2^r}\right)^{\ell+r-1} \leq \frac{(\ell+r)p}{2^r}$. 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 $\ell + r$. If a collision of FF occurs, then by Eq. (2) in Fig. 3, the outputs at (A2) and (B2) must be in the same multi-collision group. Fixing an input-output tuple at (B2), an input-output tuple at (B3) is uniquely fixed. Hence, for each input to F_3 with (A3), there are $(\ell + r)^2$ tuples for (A2), (B2), (B3) such that Eqs. (2), (3) holds and the collision probability for Eq. (1) is at most $\frac{(\ell+r)^2}{2^\ell}$ by the randomness of Z_3^*. Since the number of such multi-collision groups is at most p, the probability for coll with Case 1 is at most $\frac{(\ell+r)p}{2^r} + \frac{(\ell+r)^2 p}{2^\ell}$.

Regarding the event coll with Case 2, we use a multi-collision event for Z_3. Unlike Z_2, an output of Z_3 is XORed with $\widetilde{C}_2$ in FF, and the multi-collision event is defined so that the XOR operation is taken into account. With the multi-collision event, we can have the same bound as Case 1.

The detail evaluation is given in the following section. We define two multi-collision events mcoll_2 and mcoll_3. mcoll_2 is the multi-collision event for F_2 used in the above evaluation for Case 1. Note, however, that mcoll_2 is not particular for Case 1 and can be used for Case 2. mcoll_3 is the multi-collision event for Case 2. The following evaluation derives a (slightly) better bound than $O\left(\frac{(\ell+r)p}{2^r} + \frac{(\ell+r)^2 p}{2^\ell}\right)$.

4.2.2 Notations

We define notations used in this proof.

- For $\alpha \in [p]$, let $X^{(\alpha)} := (K_{\mathsf{F}}^{(\alpha)}, (j^{(\alpha)}, A^{(\alpha)}, D_1^{(\alpha)}, D_2^{(\alpha)})) \in \mathcal{K}_{\mathsf{prf}} \times [3] \times \mathcal{A} \times \{0,1\}^* \times \{0,1\}^*$ be the α-th offline query to F and $Z^{(\alpha)} := \mathsf{F}(X^{(\alpha)})$ the response.
- Let $Z_{j^{(\alpha)}}^{(\alpha)} := \mathsf{msb}_r(Z^{(\alpha)})$ if $j^{(\alpha)} = 2$; $Z_{j^{(\alpha)}}^{(\alpha)} := \mathsf{msb}_\ell(Z^{(\alpha)})$ if $j^{(\alpha)} = 3$.
- Let $\mathcal{T}_{\mathsf{F}}^{(<\alpha)} := \{(X^{(\beta)}, Z^{(\beta)}) \mid \beta \in [\alpha - 1]\}$ be the offline query-response pairs before the α-th offline query.

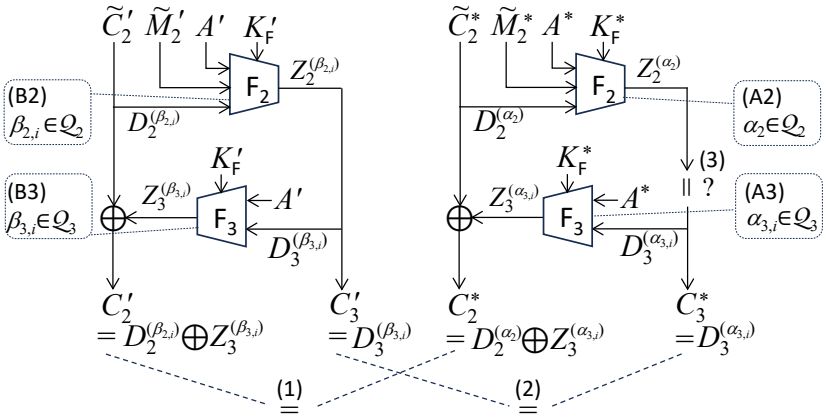

Figure 4: The multi-collision event mcoll_3.

- Let $\mathcal{L}_{\mathsf{FF}}$ be input-output tuples of FF obtained from $\mathcal{T}_{\mathsf{F}}$, i.e., $\forall(I, C_{2,3}) \in \mathcal{L}_{\mathsf{FF}}$: the two input-output tuples of F, which are used in the evaluation of $C_{2,3} = \mathsf{FF}[\mathsf{F}](I)$, are defined in $\mathcal{T}_{\mathsf{F}}$, where $I = (K_{\mathsf{F}}, (A, \widetilde{M}_2, \widetilde{C}_2))$ and $C_{2,3} = C_2 \| C_3$.
- For $i \in \{2, 3\}$ and $\alpha \in [p]$, let $\mathcal{Q}_i^{(<\alpha)} \coloneqq \{\beta \mid j^{(\beta)} = i \wedge \beta \in [\alpha - 1]\}$ and $\mathcal{Q}_i \coloneqq \mathcal{Q}_i^{(<p+1)}$.
- Let $\mu \coloneqq \frac{\ell + r}{\log_2(\ell + r)}$ be a threshold for multi-collisions.

4.2.3 Evaluation of $\mathbf{Pr}[\mathsf{coll}]$

The goal of the adversary $\mathbf{B}$ is to find a collision of FF. The collision event is defined as

- coll: $\exists(I', C'_{2,3}), (I^*, C^*_{2,3}) \in \mathcal{L}_{\mathsf{FF}}$ s.t. $(K'_{\mathsf{F}}, A') \neq (K^*_{\mathsf{F}}, A^*)$ and $C'_{2,3} = C^*_{2,3}$.

As discussed at Section 4.2.1, the bad event coll is divided into the two cases: Case 1: Z_3^* is the latest output; Case 2: Z_2^* is the latest output. For each case, we evaluate $\Pr[\mathsf{coll}]$ with multi-collision events mcoll_2 and mcoll_3.

Multi-Collision Event for Case 1 and Case 2. As discussed at Section 4.2.1, we use the following multi-collision event of F_2 for the evaluations of coll with Case 1 and Case 2.

- mcoll_2: $\exists \alpha_1, \ldots, \alpha_\mu \in \mathcal{Q}_2$ s.t. $\alpha_1 < \ldots < \alpha_\mu$ and $Z_2^{(\alpha_1)} = \cdots = Z_2^{(\alpha_\mu)}$.

This event is used in the evaluation for Case 1 in Section 4.2.1, wherein we show an intuition of the evaluation for Case 1 under the assumption that this event does not occur. Although Case 1 and Case 2 are disjoint, mcoll_2 focuses on outputs of Z_2 and is not particular for Case 1. We again stress that mcoll_2 can be used for Case 2 as well as Case 1.

Multi-Collision Event for Case 2. We define a multi-collision event for the evaluation of coll with Case 2. The event mcoll_3 considers the number of quadruplets $(\alpha_2, \beta_{2,i}, \alpha_{3,i}, \beta_{3,i})$ for input-output tuples of F with the structure in Fig. 3 such that Eqs. (1), (2) hold but Eq. (3) is not considered. $\alpha_2, \alpha_{3,i}, \beta_{2,i}$, and $\beta_{3,i}$ are respectively query indexes for (A2), (A3), (B2), and (B3). Note that the indexes for α_2 are the same for each $i \in [\mu]$. Fig. 4 is the revised version of Fig. 3 with the indexes. Assuming that mcoll_3 does not occur, for each α_2, the number of such quadruplets can be bounded by μ, and the probability that Eq. (3) holds is bounded by $\frac{\mu}{2^r}$.

- mcoll_3: $\exists \alpha_2 \in \mathcal{Q}_2, \beta_{2,1}, \ldots, \beta_{2,\mu} \in \mathcal{Q}_2^{(<\alpha_2)}$, $\alpha_{3,1}, \ldots, \alpha_{3,\mu}, \beta_{3,1}, \ldots, \beta_{3,\mu} \in \mathcal{Q}_3^{(<\alpha_2)}$ s.t. $\forall i \in [\mu]$: the quadruplet $(\alpha_2, \alpha_{3,i}, \beta_{2,i}, \beta_{3,i})$ satisfies

  (1) $D_2^{(\beta_{2,i})} \oplus Z_3^{(\beta_{3,i})} = D_2^{(\alpha_2)} \oplus Z_3^{(\alpha_{3,i})}$,

  (2) $D_3^{(\alpha_{3,i})} = D_3^{(\beta_{3,i})} = Z_2^{(\beta_{2,i})}$, and

  (4) $(K_{\mathsf{F}}^{(\alpha_2)}, A^{(\alpha_2)}) = (K_{\mathsf{F}}^{(\alpha_{3,i})}, A^{(\alpha_{3,i})}) \neq (K_{\mathsf{F}}^{(\beta_{2,i})}, A^{(\beta_{2,i})}) = (K_{\mathsf{F}}^{(\beta_{3,i})}, A^{(\beta_{3,i})})$.

  Note that the conditions (1), (2) correspond with Eqs. (1), (2) in Fig. 4, and the condition (4) comes from the condition on the output of $\mathbf{B}$.

Note that mcoll_2 and mcoll_3 are not disjoint, since mcoll_2 focuses on outputs of Z_2.

Evaluation of $\Pr[\mathsf{coll}]$ with Multi-Collision Events By using these events, we have

$$\mathbf{Adv}_{\mathsf{FF}}^{\mathsf{coll}}(\mathbf{B}) = \Pr[\mathsf{coll}] \leq \Pr[\mathsf{coll} \mid \neg\mathsf{mcoll}_2 \wedge \neg\mathsf{mcoll}_3] + \Pr[\mathsf{mcoll}_2] + \Pr[\mathsf{mcoll}_3 \wedge \neg\mathsf{mcoll}_2].$$

The bounds of the probabilities are given in Sections 4.2.4, 4.2.5, and 4.2.6, providing

$$\begin{aligned}\Pr[\mathsf{coll}] &\leq \frac{\mu p}{2^{\min\{r,\ell\}}} + 2^r \cdot \left(\frac{ep}{\mu 2^r}\right)^{\mu} + 2^{\ell} \cdot p \cdot \left(\frac{ep}{\mu 2^{\ell}}\right)^{\mu} + 2^{\ell} \cdot p \cdot \left(\frac{3ep}{2^{\ell}}\right)^{\mu} \\ &\leq \frac{\frac{\ell+r}{\log_2(\ell+r)} \cdot p}{2^{\min\{r,\ell\}}} + \left(\frac{24(\ell+r)p}{2^{\min\{r,\ell\}}}\right)^{\frac{\ell+r}{\log_2(\ell+r)}} ,\end{aligned}$$

assuming $p \leq 2^{r-1}$.

4.2.4 Evaluation of $\Pr[\mathsf{coll} \mid \neg\mathsf{mcoll}_2 \wedge \neg\mathsf{mcoll}_3]$

Assume that mcoll_2 and mcoll_3 do not occur.

We first consider the sub-case that coll with Case 2 occurs at the α_2-th query, i.e., $\alpha_2 \in \mathcal{Q}_2$ (α_2 in Fig. 4). By $\neg\mathsf{mcoll}_3$, the number of triplets of indexes $(\alpha_{3,1}, \beta_{2,1}, \beta_{3,1})$, $(\alpha_{3,2}, \beta_{2,2}, \beta_{3,2})$, $\ldots \in \mathcal{Q}_3^{(<\alpha_2)} \times \mathcal{Q}_2^{(<\alpha_2)} \times \mathcal{Q}_3^{(<\alpha_2)}$ such that the α_2-th output $Z_2^{(\alpha)}$ probabilistically connects with $D_3^{(\alpha_{3,i})}$ and yields a collision of FF is at most μ. See Fig. 4 and the connection point is Eq. (3). For each triplet, we have $\Pr[D_3^{(\alpha_{3,i})} = Z_2^{(\alpha_2)}] \leq \frac{1}{2^r}$. Hence, the probability that coll occurs in this case is at most $\frac{\mu p}{2^r}$.

We next consider the sub-case that coll with Case 1 occurs. Let $\mathcal{Q}_2^{\mathsf{new}} := \{\beta \in \mathcal{Q}_2 \mid \forall \beta_0 \in \mathcal{Q}_2^{(<\beta)} : Z_2^{(\beta)} \neq Z_2^{(\beta_0)}\}$ 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 $\mu_\beta := |\mathcal{Q}_2[\beta]|$. 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 FF (Eq. (2) in Fig. 3). Fix $\beta \in \mathcal{Q}_2^{\mathsf{new}}$ such that $\mu_\beta \geq 2$. For each pair $(\beta_2', \beta_2^*) \in \mathcal{Q}_2[\beta] \times \mathcal{Q}_2[\beta]$ such that $\beta_2' \neq \beta_2^*$ and $(K_{\mathsf{F}}^{(\beta_2')}, A^{(\beta_2')}) \neq (K_{\mathsf{F}}^{(\beta_2^*)}, A^{(\beta_2^*)})$ (the pair is (A2) and (B2) in Fig. 3), we have $\Pr\left[\mathsf{F}_3(K_{\mathsf{F}}^{(\beta_2')}, (A^{(\beta_2')}, Z_2^{(\beta_2')})) \oplus D_2^{(\beta_2')} = \mathsf{F}_3(K_{\mathsf{F}}^{(\beta_2^*)}, (A^{(\beta_2^*)}, Z_2^{(\beta_2^*)})) \oplus D_2^{(\beta_2^*)}\right] \leq \frac{1}{2^\ell}$, which is the bound of the collision probability at the left part (Eq. (1) in Fig. 3). Hence, the probability that the collision of FF 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

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

4.2.5 Evaluation of $\mathbf{Pr}[\mathsf{mcoll}_2]$

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

$$\Pr[\mathsf{mcoll}_2] \leq \binom{p}{\mu}\left(\frac{1}{2^r}\right)^{\mu-1} \leq 2^r\left(\frac{ep}{\mu 2^r}\right)^{\mu} .$$

4.2.6 Evaluation of $\mathbf{Pr}[\mathsf{mcoll}_3 \wedge \neg\mathsf{mcoll}_2]$

We evaluate the probability $\Pr[\mathsf{mcoll}_3 \wedge \neg\mathsf{mcoll}_2]$ with the following additional event. The additional event is introduced to handle the number of pairs $(\alpha_{3,j}, \beta_{3,j})$ with the condition (1) of mcoll_3 (Eq. (1) in Fig. 4), ensuring that the number of pairs for (A3) and (B3) satisfying Eq.(1) is at most μ. Fig. 5 shows the relation between mcoll_3 and mcoll'_3.

- mcoll'_3: $\exists D \in \{0,1\}^\ell, \alpha_1, \ldots, \alpha_\mu, \beta_1, \ldots, \beta_\mu \in \mathcal{Q}_3$ s.t.
  - (5) $D_3^{(\alpha_1)}, \ldots, D_3^{(\alpha_\mu)}$ are all distinct, $\forall i \in [\mu] : D_3^{(\alpha_i)} = D_3^{(\beta_i)}$, $(K_{\mathsf{F}}^{(\alpha_i)}, A^{(\alpha_i)}) \neq (K_{\mathsf{F}}^{(\beta_1)}, A^{(\beta_1)}) = (K_{\mathsf{F}}^{(\beta_i)}, A^{(\beta_i)})$, and
  - (6) $\forall i \in [\mu] : Z_3^{(\alpha_i)} \oplus Z_3^{(\beta_i)} = D$.

With mcoll'_3, we have

$$\Pr[\mathsf{mcoll}_3 \wedge \neg\mathsf{mcoll}_2] \leq \Pr[\mathsf{mcoll}_3 \mid \neg\mathsf{mcoll}_2 \wedge \neg\mathsf{mcoll}'_3] + \Pr[\mathsf{mcoll}'_3] .$$

We evaluate these probabilities below.

Evaluation of $\mathbf{Pr}[\mathsf{mcoll}_3 \mid \neg\mathsf{mcoll}_2 \wedge \neg\mathsf{mcoll}'_3]$. Assume that mcoll_2, and mcoll'_3 do not occur. Fix $\alpha_2 \in \mathcal{Q}_2$, thus the input tuple $(K_{\mathsf{F}}^{(\alpha_2)}, (A^{(\alpha_2)}, D_1^{(\alpha_2)}, D_2^{(\alpha_2)}))$ to F_2 is fixed. Also fix $\beta_{2,1}, \ldots, \beta_{2,\mu} \in \mathcal{Q}_2^{(<\alpha_2)}$, $\alpha_{3,1}, \ldots, \alpha_{3,\mu}, \beta_{3,1}, \ldots, \beta_{3,\mu} \in \mathcal{Q}_3^{(<\alpha_2)}$ that are query indexes in mcoll_3 (and of (B2), (B3), and (A3) in Fig. 4). For $i \in [\mu]$, let $\gamma_i = \max\{\alpha_{3,i}, \beta_{2,i}, \beta_{3,i}\}$, i.e., $\gamma_1, \ldots, \gamma_\mu \in \mathcal{Q}_2^{(<\alpha_2)} \cup \mathcal{Q}_3^{(<\alpha_2)}$ are the maximum number of query numbers at the 3rd round with (A3), the 2nd round with (B2), or the 3rd round with (B3) in Fig. 4. Since $\gamma_i = \max\{\alpha_{3,i}, \beta_{2,i}, \beta_{3,i}\}$, we consider all possible cases for γ_i.

Case 1. $\gamma_i = \alpha_{3,i}$, i.e., the γ_i query is at the 3rd round with (A3) in Fig. 4.

Case 2. $\gamma_i = \beta_{2,i}$, i.e., the γ_i query is at the 2nd round with (B2) in Fig. 4.

Case 3. $\gamma_i = \beta_{3,i}$, i.e., the γ_i query is at the 3nd round with (B3) in Fig. 4.

We evaluate the probability that $\gamma_i = \alpha_{3,i}$ (Case 1) and the conditions (1), (2) on mcoll_3 hold. For the input tuple $(K_{\mathsf{F}}^{(\gamma_i)}, (A^{(\gamma_i)}, D_3^{(\gamma_i)}))$ to F_3, by $\neg\mathsf{mcoll}_2$ and the condition (2), the number of candidates for $\beta_{2,i}$ (at (B2)) is at most μ. For each of the (at most) μ candidates, $\beta_{3,i}$ is uniquely fixed. Then, by the randomness of the output $Z_3^{(\gamma_i)}$, the probability that the condition (1) holds is at most $\frac{\mu}{2^\ell}$.

We evaluate the probability that $\gamma_i = \beta_{2,i}$ (Case 2) and the conditions (1), (2) hold. By $\neg\mathsf{mcoll}'_3$, the number of candidate pairs $(\alpha_{3,i}, \beta_{3,i})$ (at (A3), (B3)) is at most μ. Then, by the randomness of the output $Z_2^{(\gamma_i)}$, the probability that for some quadruplet $(\alpha_2, \beta_{2,i}, \alpha_{3,i}, \beta_{3,i})$, the condition (1) holds is at most $\frac{\mu}{2^r}$.

We evaluate the probability that $\gamma_i = \beta_{3,i}$ (Case 3) and the conditions (1), (2) hold. Fixing the input tuple $(K_{\mathsf{F}}^{(\gamma_i)}, (A^{(\gamma_i)}, D_1^{(\gamma_i)}, D_2^{(\gamma_i)}))$ to F_3, by $\neg\mathsf{mcoll}_2$, the number of

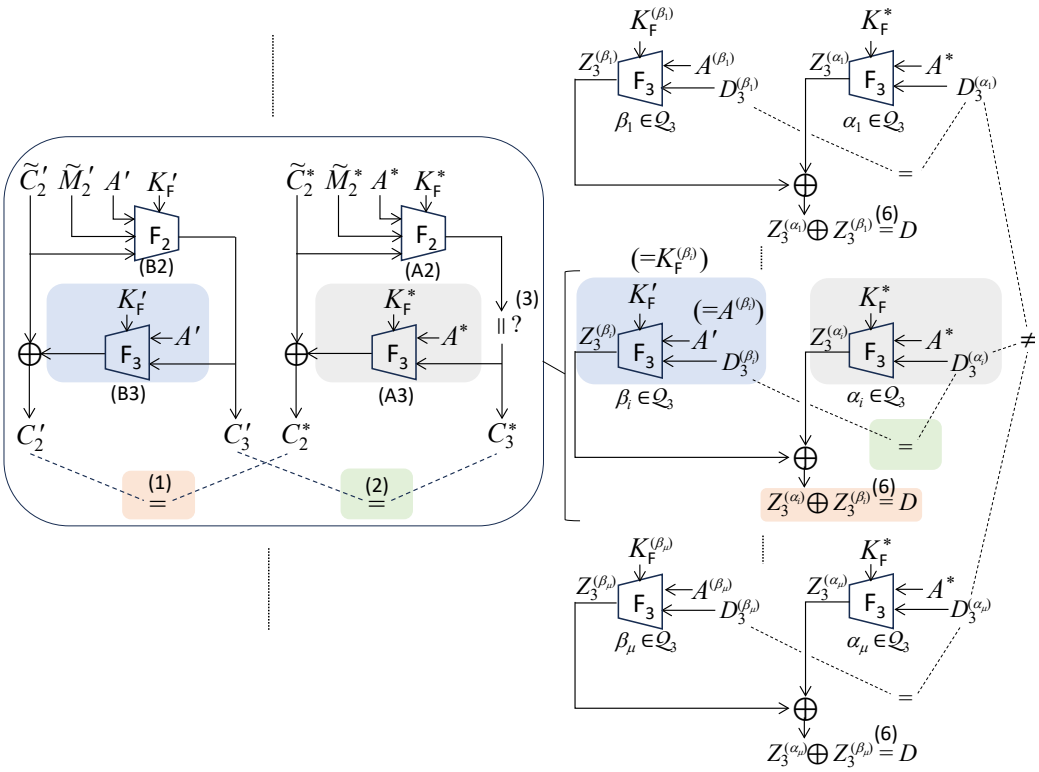

Figure 5: The multi-collision event mcoll'_3.

candidates for $\beta_{2,i}$ (at (B2)) is at most μ. For each of the μ candidates, with the condition (1), $\alpha_{3,i}$ (at (B3)) is uniquely fixed. Then, by the randomness of the output $Z_3^{(\gamma_i)}$, the probability that the condition (2) holds is at most $\frac{\mu}{2^\ell}$.

For each $\alpha_2 \in \mathcal{Q}_2$, the number of choices of $\gamma_1, \ldots, \gamma_\mu \in [\alpha_2 - 1]$ is at most $\binom{\alpha_2}{\mu}$. The input tuple of the α_2-th query is uniquely fixed when the input-output tuples of the three query indexes $\beta_{2,1}, \alpha_{3,1}, \beta_{3,1}$ are fixed such that the conditions of mcoll_3 hold. By using the above bounds and Stirling's approximation, we have

$$\begin{aligned}\Pr[\mathsf{mcoll}_3 \mid \neg\mathsf{mcoll}_2 \wedge \neg\mathsf{mcoll}'_3] &\le \sum_{\alpha_2 \in [p]} \binom{\alpha_2}{\mu} \cdot \left(\frac{3\mu}{2^\ell}\right)^{\mu-1} \\ &\le \sum_{\alpha_2 \in [p]} 2^\ell \cdot \left(\frac{3e\alpha_2}{2^\ell}\right)^{\mu} \le 2^\ell \cdot p \cdot \left(\frac{3ep}{2^\ell}\right)^{\mu} .\end{aligned}$$

Evaluation of $\Pr[\mathsf{mcoll}'_3]$. 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 $(K_{\mathsf{F}}^{(\alpha_i)}, A^{(\alpha_i)}) \neq (K_{\mathsf{F}}^{(\beta_1)}, A^{(\beta_1)}) = (K_{\mathsf{F}}^{(\beta_i)}, A^{(\beta_i)})$. We then have $\Pr[\forall i \in [\mu] : Z_3^{(\alpha_i)} \oplus Z_3^{(\beta_i)} = D] \le (\frac{1}{2^\ell})^\mu$. 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. By using Stirling's approximation, we have

$$\Pr[\mathsf{mcoll}'_3] \le 2^\ell \cdot p \cdot \binom{p}{\mu} \cdot \left(\frac{1}{2^\ell}\right)^{\mu} \le 2^\ell \cdot p \cdot \binom{p}{\mu} \cdot \left(\frac{1}{2^\ell}\right)^{\mu} \le 2^\ell \cdot p \cdot \left(\frac{ep}{\mu 2^\ell}\right)^{\mu} .$$

Bound of $\mathbf{Pr}[\mathsf{mcoll}_3 \wedge \neg\mathsf{mcoll}_2]$. We have

$$\Pr[\mathsf{mcoll}_3 \wedge \neg\mathsf{mcoll}_2] \leq 2^\ell \cdot p \cdot \left(\frac{3ep}{2^\ell}\right)^\mu + 2^\ell \cdot p \cdot \left(\frac{ep}{\mu 2^\ell}\right)^\mu .$$

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 used in 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, then $\mathsf{user}^{(\alpha)} = \omega$.
- For $\alpha \in [q]$, values defined at the α-th query are denoted by using the superscript (α).
- The stage that an adversary makes queries at is called "query stage". The stage after the query stage is called "decision stage".
- For $\omega \in [u]$, let $\mathsf{FFF}[\Pi^{\pm}_{\mathsf{F}_0(K_{\mathsf{F}}^{(\omega)})}, \mathsf{F}_{K_{\mathsf{F}}^{(\omega)}}] := (\mathsf{FFF.Enc}[\Pi_{\mathsf{F}_0(K_{\mathsf{F}}^{(\omega)})}, \mathsf{F}_{K_{\mathsf{F}}^{(\omega)}}], \mathsf{FFF.DecL}[\Pi^{-1}_{\mathsf{F}_0(K_{\mathsf{F}}^{(\omega)})}, \mathsf{F}_{K_{\mathsf{F}}^{(\omega)}}])$.

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. The set of oracles in $\mathbf{G}1$ is defined as

$$\mathcal{O}_1 := (\mathsf{FFF}[\Pi^{\pm}_{\mathsf{F}_0(K_{\mathsf{F}}^{(1)})}, \mathsf{F}_{K_{\mathsf{F}}^{(1)}}], \ldots, \mathsf{FFF}[\Pi^{\pm}_{\mathsf{F}_0(K_{\mathsf{F}}^{(u)})}, \mathsf{F}_{K_{\mathsf{F}}^{(u)}}]).$$

- $\mathbf{G}2$ 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 $\mathcal{R}^{(1)}, \ldots, \mathcal{R}^{(u)}$ whose interfaces are respectively the same as those of $\mathsf{F}_{K_{\mathsf{F}}^{(1)}}, \ldots, \mathsf{F}_{K_{\mathsf{F}}^{(u)}}$. The set of oracles in $\mathbf{G}2$ is defined as

$$\mathcal{O}_2 := (\mathsf{FFF}[\Pi^{\pm}_{K_\Pi^{(1)}}, \mathcal{R}^{(1)}], \ldots, \mathsf{FFF}[\Pi^{\pm}_{K_\Pi^{(u)}}, \mathcal{R}^{(u)}]),$$

  where $\forall \omega \in [u] : K_\Pi^{(\omega)} := \mathsf{msb}_{k_{\mathsf{we}}} \circ \mathcal{R}^{(\omega)}(0, \varepsilon, \varepsilon, \varepsilon)$.
- $\mathbf{G}3$ is a variant of $\mathbf{G}2$ where the underlying WE $\Pi^{\pm}_{K_\Pi^{(1)}}, \ldots, \Pi^{\pm}_{K_\Pi^{(u)}}$ are replaced with ideal WPs $\Psi_1^{\pm}, \ldots, \Psi_u^{\pm}$. The set of oracles in $\mathbf{G}3$ is defined as

$$\mathcal{O}_3 := (\mathsf{FFF}[\Psi_1^{\pm}, \mathcal{R}^{(1)}], \ldots, \mathsf{FFF}[\Psi_u^{\pm}, \mathcal{R}^{(u)}]).$$

- $\mathbf{G}4$ is the ideal world. The set of oracles in $\mathbf{G}4$ is defined as

$$\mathcal{O}_4 \coloneqq (\$^{(1)}_{\mathsf{Enc}}, \$^{(1)}_{\mathsf{Dec}}, \ldots, \$^{(u)}_{\mathsf{Enc}}, \$^{(u)}_{\mathsf{Dec}}).$$

Using these games, we have

$$\begin{aligned}\mathbf{Adv}^{\mathsf{mu\text{-}rae}}_{\mathsf{FFF}}(\mathbf{A}) &= \Pr[\mathbf{A}^{\mathcal{O}_1} = 1] - \Pr[\mathbf{A}^{\mathcal{O}_4} = 1] \\ &= \sum_{i\in[3]} \underbrace{\left(\Pr[\mathbf{A}^{\mathcal{O}_i} = 1] - \Pr[\mathbf{A}^{\mathcal{O}_{i+1}} = 1]\right)}_{=:\delta_i} \ .\end{aligned}$$

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 $\mathsf{mu\text{-}PRF}$-security advantage function of F, i.e., for an adversary $\mathbf{A}$, 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 $\mathsf{mu\text{-}SPRP}$-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 $\delta_1, \delta_2, \delta_3$,$\delta_4$, we have

$$\mathbf{Adv}^{\mathsf{mu\text{-}rae}}_{\mathsf{FFF}}(\mathbf{A}) \leq \frac{q_{\mathsf{u}}q}{2^{\ell}} + \frac{q_d}{2^r} + \mathbf{Adv}^{\mathsf{mu\text{-}prf}}_{\mathsf{F}}(\mathbf{A}_{\mathsf{F}}) + \mathbf{Adv}^{\mathsf{mu\text{-}sprp}}_{\Pi}(\mathbf{A}_{\Pi}) \ .$$

5.3 Bounding δ_3

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

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.

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

We then define a transcript τ which consists of

- $(\mathsf{query}^{(\alpha)}, \mathsf{user}^{(\alpha)}, M^{(\alpha)}, C^{(\alpha)}, T^{(\alpha)}, Z^{(\alpha)}_1, Z^{(\alpha)}_2, Z^{(\alpha)}_3)$ for $\alpha \in [q]$,

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

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

$$\delta_3 \leq \mathsf{SD}(\mathsf{T}_3, \mathsf{T}_4) \coloneqq \sum_{\tau \in \mathcal{T}} (\Pr[\mathsf{T}_3 = \tau] - \Pr[\mathsf{T}_4 = \tau]) \ .$$

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

Lemma 3. *Let $\mathcal{T}_{\mathsf{good}}$ and $\mathcal{T}_{\mathsf{bad}}$ be good and bad transcripts into which $\mathcal{T}$ is partitioned. If*

$$\forall \tau \in \mathcal{T}_{\mathsf{good}} : \frac{\Pr[\mathsf{T}_3 = \tau]}{\Pr[\mathsf{T}_4 = \tau]} \geq 1 - \varepsilon \ \textit{s.t.} \ 0 \leq \varepsilon \leq 1,$$

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

$$\delta_3 \leq \frac{q_{\mathsf{u}} q}{2^\ell} + \frac{q_d}{2^r} \ .$$

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. We then 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 in Sections 5.4.1-5.4.3, and we have

$$\Pr[\mathsf{T}_4 \in \mathcal{T}_{\mathsf{bad}}] \leq \frac{q_{\mathsf{u}} q}{2^\ell} + \frac{q_d}{2^r} \ .$$

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

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
$$\Pr[\mathsf{bad}_1^*] \leq \sum_{\omega \in [u]} \binom{\hat{q}_\omega}{2} \cdot \frac{1}{2^\ell} \leq \sum_{\omega \in [u]} \frac{0.5\hat{q}_\omega^2}{2^\ell} \leq \frac{0.5 q_{\mathsf{u}} q}{2^\ell} \ .$$

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

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 $\Pr[\widetilde{M}_2^{(\alpha)} = \widetilde{M}_2^{(\beta)}]$ which is equal to $\Pr[M_2^{(\alpha)} \oplus M_2^{(\beta)} = Z_1^{(\alpha)} \oplus Z_1^{(\beta)}]$.

- 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 $\Pr[\widetilde{C}_2^{(\alpha)} = \widetilde{C}_2^{(\beta)}]$ which is equal to $\Pr[C_2^{(\alpha)} \oplus C_2^{(\beta)} = Z_3^{(\alpha)} \oplus Z_3^{(\beta)}]$.

- 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
$$\Pr[\mathsf{bad}_2^*] \leq \sum_{\omega \in [u]} \binom{\hat{q}_\omega}{2} \cdot \frac{1}{2^\ell} \leq \sum_{\omega \in [u]} \frac{0.5\hat{q}_\omega^2}{2^\ell} \leq \frac{0.5 q_{\mathsf{u}} q}{2^\ell} \ .$$

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

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 $c_\alpha \coloneqq |C^{*(\alpha)}|$. 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., $N_1 \coloneqq \left|\{(\mathsf{user}^{*(\alpha)}, A^{*(\alpha)}, T^{*(\alpha)}) \mid \alpha \in [q]\}\right|$ and $N_3 \coloneqq \left|\{(\mathsf{user}^{*(\alpha)}, A^{*(\alpha)}, C_3^{*(\alpha)}) \mid \alpha \in [q]\}\right|$. 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 $\mathbf{Pr}[\mathsf{T}_4 = \tau]$

We evaluate the probabilities $\Pr[\mathsf{T}_4 \vdash \tau_{M,C,T}]$ and $\Pr\left[\mathsf{T}_4 \vdash \tau_{Z_{1,3}}\right]$, since $\Pr[\mathsf{T}_4 = \tau] = \Pr[\mathsf{T}_4 \vdash \tau_{M,C,T}] \cdot \Pr\left[\mathsf{T}_4 \vdash \tau_{Z_{1,3}}\right]$ 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 $\Pr\left[\mathsf{T}_4 \vdash \tau_{Z_{1,3}}\right]$. For each new input to $\mathcal{R}$, the output is chosen uniformly at random from $\{0,1\}^\ell$, thus we have
  $$\Pr\left[\mathsf{T}_4 \vdash \tau_{Z_{1,3}}\right] = \left(\frac{1}{2^\ell}\right)^{N_1+N_3} \ .$$

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

We evaluate the probabilities $\Pr[\mathsf{T}_3 \vdash \tau_{M,C,T}]$ 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

$$\Pr\left[\mathsf{T}_3 \vdash \tau_{Z_{1,3}}\right] = \left(\frac{1}{2^\ell}\right)^{N_1+N_3} .$$

- Evaluating $\Pr[\mathsf{T}_3 \vdash \tau_{M,C,T}]$. 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 the output is chosen uniformly at random from $\{0,1\}^{c_\alpha - r} \backslash \{\widetilde{C}^{(\beta)} \mid \beta \in [\alpha-1] \wedge \mathsf{user}^{(\beta)} = \mathsf{user}^{(\alpha)} \wedge |\widetilde{C}^{(\beta)}| = c_\alpha - r\}$ (resp. $\{0,1\}^{c_\alpha - r} \backslash \{\widetilde{M}^{(\beta)} \mid \beta \in [\alpha-1] \wedge \mathsf{user}^{(\beta)} = \mathsf{user}^{(\alpha)} \wedge |\widetilde{M}^{(\beta)}| = c_\alpha - r\}$). 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

$$\Pr[\mathsf{T}_3 \vdash \tau_{M,C,T}] \geq \prod_{\alpha \in [q]} \frac{1}{2^{c_\alpha}} .$$

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 of 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 (resp. 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 optimizations beyond the WE's boundary, i.e., a dedicated design, is another research challenge.

Acknowledgments

We thank the anonymous reviewers of SCN 2024, ToSC 2024 Issue 4, and ToSC 2025 Issue 1, and the shepherd for their valuable comments.

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.

[BH24] Mihir Bellare and Viet Tung Hoang. Succinctly-committing authenticated encryption. In *CRYPTO 2024*, volume 14923 of *LNCS*, pages 305–339, 2024.

[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.

[CDD+24] Yu Long Chen, Michael Davidson, Morris Dworkin, Jinkeon Kang, John Kelsey, Yu Sasaki, Meltem Sönmez Turan, Donghoon Chang, Nicky Mouha, and Alyssa Thompson. Proposal of requirements for an accordion mode. https://csrc.nist.gov/files/pubs/other/2024/04/10/proposal-of-requirements-for-an-accordion-mode-dis/iprd/docs/proposal-of-requirements-for-an-accordion-mode-discussion-draft.pdf, 2024.

[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.

[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.

[RS06] Phillip Rogaway and Thomas Shrimpton. A Provable-Security Treatment of the Key-Wrap Problem. In Serge Vaudenay, editor, *EUROCRYPT 2006*, volume 4004 of *LNCS*, pages 373–390. Springer, 2006.

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