Commuting Wide Encryption Mode with Minimum Ciphertext Expansion

Yusuke Naito¹, Yu Sasaki²,³, and Takeshi Sugawara⁴

¹ Mitsubishi Electric Corporation, Kanagawa, Japan, Naito.Yusuke@ce.MitsubishiElectric.co.jp
² NTT Social Informatics Laboratories, Tokyo, Japan, yus.k.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_{rae} + 2s_{cont} bits from an original message to achieve s_{rae}-bit RAE and s_{cont}-bit CMT-4 security. Our new WE mode FFF addresses the issue by achieving s_{rae}-bit RAE and s_{cont}-bit CMT-4 security only with max{s_{cont}, s_{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 [14]) are easily distinguishable from random functions, since changing a last message block only affects the last ciphertext block.

Wide encryption (WE) is a mode of operation 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 [18]. Since then, researchers have proposed concrete modes, including AEZ [19], Shrimpton–Terashima [27], ZCZ [6], and Bäcucci et al. [7]. WE has practical applications, including full-disc encryption, and there are several proposals from the industry, including Adiantum [10] and HCTR2 [11] by Google. Moreover, NIST has recently started standardizing WEs [23, 24], which stimulated even more WE proposals in the last few years, including the ones using double-decker and docked-double-decker [17, 12].

WE is an efficient building block for authenticated encryption with associated data (AE) that provide confidentiality and authenticity. More formally, an AE encryption $\text{AE.Enc}$ takes a key $K$, associated data $A$, and a message $M$ to generate a ciphertext $C = \text{AE.Enc}(K, A, M)$. Throughout the paper, we assume that $A$ includes a nonce $N$. The decryption $\text{AE.Dec}$ 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 $\text{reject}$. The encode-then-encipher (EtE) scheme proposed by Bellare and Rogaway [5] is a well-known way of constructing an AE from WE. WE-based EtE is particularly important because it realizes a robust AE (RAE) [19]—a class of AEs that provides strong robustness against several misuses, including nonce reuse and the release of unverified plaintexts [2, 19].

WE-based EtE achieves $s_{\text{rae}}$-bit RAE security with ciphertext expansion by $s_{\text{rae}}$ bits (up to the security bound of the WE). It first encodes $s_{\text{rae}}$ bits of redundant data into an $m$-bit original message, e.g., by appending $s_{\text{rae}}$ bits of zeros to the message, and encrypts the encoded message with the underlying WE to generate an $(m + s_{\text{rae}})$-bit ciphertext. Upon decryption, EtE recovers an $(m + s_{\text{rae}})$-bit encoded message, decodes the $s_{\text{rae}}$-bit redundancy, and checks it for authenticity. Meanwhile, WE’s tweak input can be used to accept associated data $A$, including a nonce. AEZ [19] is a well-known realization in this category.

Committing security is a relatively new security model with respect to AE [15, 16]. 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 [16, 13, 1] and the partitioning oracle attack that achieves efficient password brute-force attacks [20]. 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 [16, 13], GCM-SIV [20], CCM [21], and ChaCha20-Poly1305 [16, 25].

Bellare and Hoang [3] (and Chan and Rogaway independently [8]) 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 [15, 16]. 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. [16] showed that EtE combined with an ideal WE satisfies a vari-
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{$s_{cmt}$, $s_{rae}$}. The table assume $s_{cmt} \geq s_{rae}$, and max{$s_{cmt}$, $s_{rae}$} = $s_{cmt}$. 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.

<table>
<thead>
<tr>
<th>Scheme</th>
<th>Expansion size (bits)</th>
<th>Minimum?</th>
<th>Primitive</th>
<th>Ref.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CMT-1</td>
<td>CMT-4</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>WE + EtE$^\dagger$</td>
<td>$2s_{cmt}^\dagger$</td>
<td>No</td>
<td>IC</td>
<td>[5]</td>
</tr>
<tr>
<td>WE + EtE + $H(K)$</td>
<td>$s_{rae} + 2s_{cmt}$</td>
<td>No</td>
<td>CR Hash</td>
<td>[15]</td>
</tr>
<tr>
<td>WE + EtE + $H(K, A)$</td>
<td>$s_{rae} + 2s_{cmt}$, $s_{rae} + 2s_{cmt}$</td>
<td>No</td>
<td>CR Hash</td>
<td>[15, 8]</td>
</tr>
<tr>
<td>FFF</td>
<td>$s_{cmt}$, $s_{cmt}$</td>
<td>Yes</td>
<td>RO</td>
<td>Ours</td>
</tr>
</tbody>
</table>

$^\dagger$ AEZ, Adiantum-EtE, HCTR2-EtE, $^\ddagger$The block size of the internal block cipher is $2s_{cmt}$ bits.

Ant of key-committing security. Then, Chen et al. [9] 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 $2s_{cmt}$ 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 [8]; 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 [15] that adds an $2s_{cmt}$-bit 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 $2s_{cmt}$-bit hash digest of a key and associated data $H(K, A)$ instead [15, 8], we can achieve $s_{cmt}$-bit CMT-4 security. However, as a drawback, the ciphertext expands by $s_{rae} + 2s_{cmt}$ bits from the original message. We also remark that there is no RAE security regarding the additional hash

$^5$ Appending $H(K, A)$ is an extension of Fasim et al.’s method [15] and is a variant of CTX [8] that appends $H(K, A, T)$ wherein $T$ is a tag of an underlying tag-based AE.
values $H(K)$ and $H(K, A)$, which is another issue that we address with the proposed method.

**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. [19] 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 $\max\{s_{\text{cmt}}, s_{\text{rae}}\}$ for an $s_{\text{rae}}$-bit RAE and $s_{\text{cmt}}$-bit CMT-4 security.

**Our Approach.** Obtaining CMT-4 security with the minimum ciphertext expansion is a major research challenge [4, 22], and Bellare et al. [4] already achieved the minimum ciphertext expansion for tag-based AEs, i.e., $s_{\text{cmt}}$-bit CMT-4 security with $s_{\text{cmt}}$ 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., $M \rightarrow M_1 \parallel M_2$, 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 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 $M_2$.

**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, $s_{\text{rae}}$ and $s_{\text{cmt}}$, 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 $\max\{s_{\text{cmt}}, s_{\text{rae}}\}$ bits larger than the message size.

In this construction, an input message $M$ of size $|M|$ bits is divided into two parts $M \rightarrow M_1 \parallel M_2$, where the sizes of $M_1$ and $M_2$ are $|M| - \ell$ bits and
\( \ell \) bits, respectively. The construction consists of WE \( \Pi \) 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 \( \Pi \) are involved in the 3-round Feistel-like structure.

Inside the 3-round Feistel-like structure, three independent keyed hash functions \( F_1(K_F, \cdot), F_2(K_F, \cdot), \) and \( F_3(K_F, \cdot) \), which serve as three random oracles for CMT-4 security or pseudorandom functions (PRFs) for RAE security, are computed.\(^6\) All of them take a WE key \( K_\Pi \) and associated data \( A \) as input.\(^7\) Besides, \( F_1(K_F, \cdot) \) and \( F_3(K_F, \cdot) \) take the \( r \)-bit state as the input and \( F_2(K_F, \cdot) \) take the last \( \ell \) bits of the input and the output of \( \Pi \) as input. During the encryption, \( F_1(K_F, \cdot) \) is first computed and XORed with \( M_2 \), then \( \Pi \) is computed with a key \( K_\Pi \) to transform \( M_1 \| M_2 \) into \( C_1 \| C_2 \), where \( C_2 \) and \( \bar{C}_2 \) are the last \( \ell \) bits of the input and output of \( \Pi \), respectively. At this stage, \(|M| - \ell \) bits of the ciphertext \( C_1 \) can be output. After that, \( F_2(K_F, \cdot) \) and \( F_3(K_F, \cdot) \) are computed in turn, and \( \ell \) bits and \( r \) bits of the ciphertext \( C_2 \) and \( \bar{C}_3 \) are computed respectively as shown in Fig. 1. For decryption, first \( F_3(K_F, \cdot) \) is computed, and then the inverse of WE \( \Pi^{-1} \) is computed, followed by \( F_2(K_F, \cdot) \) and \( F_1(K_F, \cdot) \). The outputs \( Z_2 \) and \( Z_4 \) are respectively XORed with \( C_3 \) and \( M_2 \) 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 rationale 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 \( F_2(K_F, \cdot) \) that takes \( \ell \) bits of the output from \( \Pi \) as input. The change of \( A \) will affect all the three rounds of

\(^6\) By using domain separations, the three keyed hash functions can be realized from a single keyed hash function.

\(^7\) By using iterated hash functions such as Merkle-Damgård or Sponge, one can share the state after processing \( K_\Pi \) and \( A \) within the three hashing processes.
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 $H^{-1}$, namely $C_1||C_2$, which randomly changes the output of $H^{-1}$, namely $M_1||M_2$. 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 $((K'_H, K'_E, A', M'_1, M'_2), (K'_H, K'_E, A', M'_1, M'_2))$ 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 $C'_1||C'_3$ part of the 3-round Feistel-like structure. The previous CC-construction [4] 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 $s_{rae} \leq s_{cmt}/2$ (resp. $s_{cmt}/2 < s_{rae} \leq s_{cmt}$), then by choosing the parameters such that $\ell \geq r = s_{cmt}$ (resp. $r = s_{cmt}$ and $\ell = 2s_{rae}$), the size of the ciphertext expansion of FFF is minimum regarding CMT-4 security. If $s_{cmt} > s_{rae}$, then by choosing the parameters such that $r = s_{rae}$ and $\ell = 2s_{rae}$, the size of the ciphertext expansion is minimum regarding RAE security.

Note that we require that the hash functions $F_1(K_E, \cdot), F_2(K_E, \cdot), \text{ and } F_3(K_E, \cdot)$ 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.

**Related Works.** Hash-then-Encrypt (HtE) [3] 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 [22]. 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

**Notation.** For integers $0 \leq i \leq j$, let $[i,j] := \{i, i+1, \ldots, j\}$ and $[j] := [1,j]$. Let $\varepsilon$ 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 $X \in \{0,1\}^I$, let
functions indexed \( \Pi \) let where sumed \( Π \) be the most (resp. least) significant \( j \) bits of \( X \). If \( j ≥ i \), then \( \text{msb}_j(X) = X \) and \( \text{lsb}_j(X) = X \). For a non-empty set \( T \), \( T ⇆ T \) means that an element is chosen uniformly at random from \( T \) and assigned to \( T \). For two sets \( T \) and \( T' \), \( T ⇆ T' \) means \( T \leftarrow T \cup T' \). For integers \( l_1, \ldots, l_j ≥ 0 \) and \( X ∈ \{0,1\}^* \) such that \( |X| = l_1 + \cdots + l_j \), \( (X_1, \ldots, X_j) \overset\$\leftarrow l_1+\cdots+l_j \) \( X \) means parsing of \( X \) into \( j \) blocks such that \( X = X_1|| \cdots ||X_j \) and \( |X_i| = l_i \) for each \( i ∈ [j] \).

Wide Encryption (WE). A WE is a set of length-preserving permutations indexed by a key. Let \( \mathcal{K}_{\text{we}} \) and \( \mathcal{M}_{\text{we}} \) be the sets of keys and plaintexts. A WE \( \Pi : \mathcal{K}_{\text{we}} × \mathcal{M}_{\text{we}} \rightarrow \mathcal{M}_{\text{we}} \) is such that for any key \( K \in \mathcal{K}_{\text{we}} \) and distinct plaintexts \( M, M' ∈ \mathcal{M}_{\text{we}}, |M| = |(K, M)| \) and \( \Pi(K, M) ≠ \Pi(K, M') \) must be satisfied. Let \( \Pi^{-1} \) be the inverse of \( \Pi \). \( \Pi \) (resp. \( \Pi^{-1} \)) with a key \( K \) is denoted by \( \Pi_K \) (resp. \( \Pi^{-1}_K \)). \( \Pi_{K_{(i)}} \) is \( \Pi_{K_{(i)}}, \Pi_{K_{(j)}}^{-1} \). We call a WE with \( \mathcal{K}_{\text{we}} = \emptyset \) a "wide permutation (WP)". Let \( \text{WP}(\mathcal{M}_{\text{we}}) \) be the set of all WPs over \( \mathcal{M}_{\text{we}} \).

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 \( n \) 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 \( (\Pi_{K_{(i)}}, \Pi_{K_{(j)}}, \Pi_{K_{(i)}}^{-1}, \Pi_{K_{(j)}}^{-1}) \) for each \( i ∈ [u] \), \( K \) is \( \mathcal{K}_{\text{we}} \). The ideal-world oracles are ideal WPs \( (\psi_1, \psi_1^{-1}, \ldots, \psi_u, \psi_u^{-1}) \), where for each \( \omega ∈ [u] \), \( \psi_\omega \overset\$\leftarrow \text{WP}(\mathcal{M}_{\text{we}}) \). At the end of this game, \( A \) return a decision bit in \( \{0,1\} \). Let \( A^{O} ∈ \{0,1\} \) be an output of \( A \) with access to a set of oracles \( O \). Then, the mu-SPRP advantage function of \( A \) is defined as \( \text{Adv}_{\Pi}^{\text{mu-SPRP}}(A) = \text{Pr} \left[ A^{H_{K_{(i)}}H_{K_{(j)}}^{-1}H_{K_{(i)}}^{-1}H_{K_{(j)}}^{-1}} = 1 \right] - \text{Pr} \left[ A^{\psi_1, \psi_1^{-1}, \ldots, \psi_u, \psi_u^{-1}} = 1 \right] \).

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 \( \mathcal{M}_r \), let \( F : \mathcal{M}_r \rightarrow \{0,1\}^n \) be an \( n \)-bit hash function. Let \( \mathcal{F}(\mathcal{M}_r, \{0,1\}^n) \) be the set of all functions from \( \mathcal{M}_r \) to \( \{0,1\}^n \). In this model, a random oracle \( F \) is defined as \( F \leftarrow \mathcal{F}(\mathcal{M}_r, \{0,1\}^n) \), and all parties have access to \( F \) by offline queries.

A random oracle \( F \) can be realized by lazy sampling. Let \( \mathcal{T}_F \) 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 \( Y \leftarrow \{0,1\}^n \), and the pair \( (X, Y) \) is added to \( \mathcal{T}_F \): \( \mathcal{T}_F \leftarrow \{ (X, Y) \} \). For a query stored in the table \( \mathcal{T}_F \), the same response is returned.

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 \( \mathcal{K}_{\text{prf}}, \mathcal{M}_{\text{prf}} \), let \( F : \mathcal{K}_{\text{prf}} × \mathcal{M}_{\text{prf}} \rightarrow \{0,1\}^n \) be an \( n \)-bit keyed function, where \( \mathcal{K}_{\text{prf}} \) is the key space and \( \mathcal{M}_{\text{prf}} \) is the message space. The function with a key \( K \) is denoted by \( F_K \). Let \( u \) be the number of users. Let \( \mathcal{R}^{(1)}(\ldots, \mathcal{R}^{(u)}(u) \) be \( u \) random functions where \( \mathcal{R}_i \leftarrow \mathcal{F}(\mathcal{M}_{\text{prf}}, \{0,1\}^n) \) for each \( i ∈ [u] \). Let \( K^{(1)}(\ldots, K^{(u)} \) be \( u \) keys.
where \( K^{(i)} \in \mathcal{K} \) for each \( i \in [u] \). Let \( A^O \in \{0, 1\} \) be an output of \( A \) with access to a set of oracles \( \mathcal{O} \). The mu-PRF advantage function of an adversary \( A \) is defined as 
\[
\text{Adv}_{F_{\text{mu-prf}}}^A(A) := \Pr[A_{F_{K^{(1)}}, \ldots, F_{K^{(n)}}} = 1] - \Pr[A_{\mathcal{R}^{(1)}, \ldots, \mathcal{R}^{(n)}} = 1].
\]

In our RAE-security proof, \( A \) is a computationally-bounded adversary.

**Authenticated Encryption (AE) with Decryption Leakage.** Let \( \text{AE} \) be an AE scheme that is a pair of encryption and decryption algorithms \((\text{AE.Enc}, \text{AE.Dec})\). \( K, \ A, \ M, \ C \) are the sets of keys, associated data (AD), plaintexts, and ciphertexts of \( \text{AE} \), respectively. Note that if \( \text{AE} \) is a nonce-based (resp. tag-based) AE scheme, nonce (resp. a tag) is a part of AD (resp. a ciphertext). The encryption algorithm \( \text{AE.Enc} : \mathcal{K} \times \mathcal{A} \times \mathcal{M} \rightarrow \mathcal{C} \) takes a tuple \((K, A, M)\), and returns, deterministically, a ciphertext \( C \). The decryption algorithm \( \text{AE.Dec} : \mathcal{K} \times \mathcal{A} \times \mathcal{C} \rightarrow \{\text{reject}\} \cup \mathcal{M} \) takes a tuple \((K, A, C)\) and returns, deterministically, either the distinguished invalid symbol \( \text{reject} \notin \mathcal{M} \) 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. \( |M| = |M'| \) : \( |\text{AE.Enc}(K, A, M)| = |\text{AE.Enc}(K', A', M')| \). We also require that \( \forall K \in \mathcal{K}, A \in \mathcal{A}, M \in \mathcal{M} : \text{AE.Dec}(K, A, \text{AE.Enc}(K, A, M)) = M \).

Committing Security. We use the security notion, CMT-4, defined in [3]. Let \( \text{AE}[F] \) be an AE scheme with an \( n \)-bit hash function \( F : \mathcal{M}_0 \rightarrow \{0, 1\}^n \) where \( \mathcal{M}_0 \) is a message space. Our proof assumes that \( F \) is a random oracle.

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

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

**Lemma 1.** For any CMT-4 adversary \( A_4 \) making \( p \) queries, there exists a CMT-3 adversary \( A_3 \) making \( p \) queries such that \( \text{Adv}_{\text{CMT-}4}^{\text{CMT-}4}(A_4) \leq \text{Adv}_{\text{CMT-}3}^{\text{CMT-}3}(A_3) \).

Robust-AE Security. We use a slight variant of the RAE-security notion defined in [19]. The variant notion mu-RAE is indistinguishability between \( \text{AE} \) and an ideal \( \text{AE} \) with decryption leakage in the multi-user setting. The ideal \( \text{AE} \) returns values that are randomly chosen with replacement where in the original notion, an ideal \( \text{AE} \) returns values that are randomly chosen without replacement.

In the mu-RAE-security game, we consider the decryption function with leakage functionality, denoted by \( \text{AE.DecL} \). \( \text{AE.DecL} \) takes the same inputs as \( \text{AE.Dec} \), 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 \text{accept} if the inputs are valid; \text{reject} otherwise. Our mode leaks a pair of an unverified plaintext and a value for authentication.
Algorithm 1 FFF

Encryption $\text{FFFF.Enc}[\Pi_{K_H}, F_{K_F}](A, M)$ where $|M| \geq \ell$
1: $(M_1, M_2) \leftarrow \Pi_{[\ell, \ell]} \ M$
2: $\widehat{M} \leftarrow F_1(K_F, (K_H, A, 0^r)) \oplus M_2$ \quad $\triangleright$ 1st Round
3: $\widehat{C} \leftarrow \Pi(K_H, \widehat{M}); (C_1, C_2) \leftarrow \Pi_{[\ell, \ell]} \ C$ \quad $\triangleright$ Perform WE
4: $C_3 \leftarrow F_2(K_F, (K_H, A, \widehat{M}, C_2))$ \quad $\triangleright$ 2nd Round
5: $C_2 \leftarrow F_3(K_F, (K_H, A, C_3)) \oplus C_2$ \quad $\triangleright$ 3rd Round
6: $C \leftarrow C_1 \parallel C_2 \parallel C_3$; return $C$

Decryption $\text{FFFF.Dec}[\Pi_{K_H}^{-1}, F_{K_F}](A, C)$ where $|C| \geq \ell + r$
1: $(C_1, C_2, C_3) \leftarrow \Pi_{[\ell + r, \ell + r]} \ C$
2: $C_2 \leftarrow F_3(K_F, (K_H, A, C_3)) \oplus C_2$ \quad $\triangleright$ 3rd Round
3: $\widehat{C} \leftarrow C_1 \parallel C_2; \quad \widehat{M} \leftarrow \Pi(K_H, \widehat{C}); (M_1, M_2) \leftarrow \Pi_{[\ell, \ell]} \ M$ \quad $\triangleright$ Perform WE
4: $T \leftarrow F_2(K_F, (K_H, A, \widehat{M}, C_2)) \oplus C_3$ \quad $\triangleright$ 2nd Round
5: $M_2 \leftarrow F_1(K_F, (K_H, A, T)) \oplus \widehat{M}$
6: if $T = 0^r$ then return $\hat{M}$; else return reject end if

(See Section 3.1 for the leakage values). $\text{AE.Enc}$ (resp. $\text{AE.DecL}$) with a key $K$ is denoted by $\text{AE}_{K} \cdot \text{Enc}$ (resp. $\text{AE}_{K} \cdot \text{DecL}$). Let $\text{AE}_{K} := (\text{AE}_{K} \cdot \text{Enc}, \text{AE}_{K} \cdot \text{DecL})$.

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

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 $II : K_{we} \times \{0,1\}^* \to \{0,1\}^*$ be a WE, where $K_{we}$ is the key space. Let $\ell$ (resp. $r$) be a positive integer and the length of the left (resp. right) part of the 3-round Feistel-like structure. Let $F : K_{prf} \times ([3] \times K_{we} \times A \times \{0,1\}^* \times \{0,1\}^*) \to \{0,1\}^{\max(\ell,r)}$ be a function that is a hash function for CMT-4 security and that is a keyed function for mu-RAE security, where $K_{prf}$ is the key space. For $K_{prf}, K_{II} \in K_{we}$, $A \in A$, $D_1 \in \{0,1\}^*$, and $D_2 \in \{0,1\}^*$, let $F_3(K_{prf}, (K_{II}, A, D_1)) := msb_2 \circ F(K_{prf}, (1, K_{II}, A, D_1, \varepsilon))$ be the 1st-round function of the 3-round Feistel-like structure, $F_3(K_{prf}, (K_{II}, A, D_1, D_2)) := msb_2 \circ F(K_{prf}, (2, K_{II}, A, D_1, D_2))$ the 2nd-round function, and $F_3(K_{prf}, (K_{II}, A, D_1)) := msb_2 \circ F(K_{prf}, (3, K_{II}, A, D_1, \varepsilon))$ 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). $\text{FFF.Enc}[II_{K_{II}}, F_{K_{prf}}]$ (resp. $\text{FFF.Dec}[II_{K_{II}}^{-1}, F_{K_{prf}}]$) is the encryption (resp. decryption) function. We require that the lengths of plaintexts (resp. ciphertexts) are greater than or equal to $\ell$ (resp. $\ell + r$). We define the decryption function with leakage functionality $\text{FFF.DecL}[II_{K_{II}}^{-1}, F_{K_{prf}}]$ as follows. For each inputs $((K_{II}, K_{prf}), A, C)$, $\text{FFF.DecL}[II_{K_{II}}^{-1}, F_{K_{prf}}]$ returns $(M, T)$ as well as $\text{vrf} \in \{\text{accept}, \text{reject}\}$, where $\text{vrf} = \text{FFF.Dec}[II_{K_{II}}^{-1}, F_{K_{prf}}](A, C)$, and $M$ and $T$ are defined in the decryption procedure.

### 3.2 Security Bounds of FFF

#### 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 $A$ making at most $p$ offline queries, we have $\text{Adv}_{\text{FFF}}^{\text{cmt-4}}(A) \leq \frac{\ell + r}{2^{\ell + r + \lambda}} + \left(\frac{12(\ell + r)p}{2^{\ell + r + \lambda}}\right)^{1.5}$. 

![Fig. 2. Feistel\(\text{]_\text{CMT}}\) (left) and Multi-Collision Event mcoll (right)](image-url)
Algorithm 2 Disjointed 3-Round Feistel Structure with 0°

Procedure $\text{Feistel}_3^0[F](K_F, K_H, A, M_2, \tilde{C}_2)$

1: $\tilde{M}_2 \leftarrow F_1(K_F, K_H, A, 0°) \oplus M_2$  \> 1st Round
2: $C_3 \leftarrow F_2(K_F, K_H, A, M_2, \tilde{C}_2)$  \> 2nd Round
3: $C_2 \leftarrow F_3(K_F, K_H, A, C_3) \oplus \tilde{C}_2$  \> 3rd Round
4: return $C_2 \parallel C_3$

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.

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 $A$ 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 $A_H$ and an mu-PRF adversary $A_F$ such that $\text{Adv}_{FFF}^{\text{mu-rae}}(A) \leq q_u + \frac{q_u}{2^{\ell}} + \text{Adv}_H^{\text{mu-sprp}}(A_H) + \text{Adv}_F^{\text{mu-prf}}(A_F)$, and $A_H$ and $A_H$ 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 $\min\{2^\ell/2, 2^\ell\}$ 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., $q_u \ll 2^{\ell/2}$, then $FFF$ achieves beyond-birthday-bound security regarding the parameter $\ell$.

4 Proof of Theorem 1

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

4.1 Decoupled 3-round Feistel-like Structure with 0°

We consider the 3-round Feistel-like structure $\text{Feistel}_3[F]$ given in Algorithm 2 and Fig. 2-(left). In $\text{Feistel}_3[F]$, the right-part input is fixed to 0° and the left part at the 2nd round is decoupled, i.e., $\text{Feistel}_3[F]$ is $FFF.\text{Enc}[II, F]$ without $II$. Hence, if the CMT-3 security of $FFF$ is broken, i.e., $(K^{1}_H, K^{1}_F, A^1) \neq (K^{1}_H, K^{1}_F, A^1)$ and $FFF.\text{Enc}[II, K^{1}_H, F, K^{1}_F](A^1, M^1) = FFFF.\text{Enc}[II, K^{1}_H, F, K^{1}_F](A^1, M^1)$, then we have a collision of $\text{Feistel}_3[F]$, i.e., $\text{Feistel}_3[F](K^{1}_F, K^{1}_H, A^1, M^1_2, C^1_2) = \text{Feistel}_3[F](K^{1}_F, K^{1}_H, A^1, M^1_2, C^1_2)$. Hence, by using the CMT-3 adversary $A$, we can construct a collision-finding adversary $B$ against $\text{Feistel}_3[F]$ making at most $p$ queries to a random oracle $F$ and outputting two tuples $(K^{1}_F, K^{1}_H, A^1, M^1_2, C^1_2)$
and \( (K_F^1, K_T^1, A^1, M^1_2, \overline{C}_2^1) \) such that \( (K_F^1, K_T^1, A^1) \neq (K_F^3, K_T^3, A^3) \), 
\[
\delta_{\text{coll}} := \Pr \left[ \text{Feistel}^3_{\text{prf}}[F](K_F^1, K_T^1, A^1, M^1_2, \overline{C}_2^1) = \text{Feistel}^3_{\text{prf}}[F](K_F^3, K_T^3, A^3, M^3_2, \overline{C}_2^3) \right],
\]
and the random-oracle list \( \mathcal{F} \) includes input-output tuples needed to perform 
\[
\text{Feistel}^3_{\text{prf}}[F](K_F^1, K_T^1, A^1, M^1_2, \overline{C}_2^1) \text{ and } \text{Feistel}^3_{\text{prf}}[F](K_F^3, K_T^3, A^3, M^3_2, \overline{C}_2^3).
\]

### 4.2 Collision Resistance of the Disjointed 3-round Feistel

We evaluate \( \delta_{\text{coll}} \), the probability that an adversary \( B \) making \( p \) queries finds a collision of \( \text{Feistel}^3_{\text{prf}} \).

**Intuition.** We use a \((\ell + r)\)-multi-collision event in \( Z_2 \) values of \( r \) bits. The multi-collision probability is at most \((1/2^r)^{(\ell + r - 1)} \leq (\ell + r)p/2^r \). 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 \( \text{Feistel}^3_{\text{prf}} \) occurs, there exists a pair of the \( \ell + r \) inputs to \( F_2 \), 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 
\[
\delta_{\text{coll}} \leq \frac{(\ell + r)p/2^r + (\ell + r)^2p/2^\ell}{p}.
\]
Note that the intuition does not consider query orders between \( F_2 \) and \( F_3 \) for the collision of \( \text{Feistel}^3_{\text{prf}} \). The following evaluation derives a (slightly) better bound by taking into account the orders.

**Detail.** For \( \alpha \in [p] \), let \( X^{(\alpha)} = (K_F^{(\alpha)}, j^{(\alpha)}, K_T^{(\alpha)}, A^{(\alpha)}, D_1^{(\alpha)}, D_2^{(\alpha)}) \in \mathcal{K}_\text{prf} \times [3] \times K_{\text{we}} \times A \times \{0, 1\}^* \) be the \( \alpha \)-th query to \( F \) and \( Z^{(\alpha)} = F(X^{(\alpha)}) \) the response. Let \( X^{(\alpha)} = \text{msbr}(Z^{(\alpha)}) \) if \( j^{(\alpha)} \in \{1, 3\} \) and \( D_2^{(\alpha)} = \varepsilon, Z_2^{(\alpha)} := \text{msbr}(Z^{(\alpha)}) \) if \( j^{(\alpha)} = 2 \). Let \( \mathcal{T}^{(\alpha)} := \{(X^{(\beta)}, Z_2^{(\beta)}) \mid \beta \in [\alpha - 1]\} \). Let \( \mathcal{L}^{(\alpha)} \) be all input-output tuples of \( \text{Feistel}^3_{\text{prf}} \) obtained from \( \mathcal{T}^{(\alpha)} \), i.e., \( \forall (I, C_{2,3}) \in \mathcal{L}^{(\alpha)} \) : the corresponding input-output tuples of \( F \) are defined in \( \mathcal{T}^{(\alpha)} \), where \( I = (K_F, K_T, A, M_2, \overline{C}_2) \) and \( C_{2,3} = C_2 || C_3 \). For \( i \in [3] \) and \( \alpha \in [p] \), let \( Q_i^{(\alpha)} := \{ \beta \mid j^{(\beta)} = i \wedge \beta \in [\alpha - 1]\} \) and \( Q_i := Q_i^{(\alpha + 1)} \). Let \( \mu := \frac{\ell + p}{\log(\ell + p)} \).

We define four (multi-)collision events. \( \text{coll} \) is a collision event for \( \text{Feistel}^3_{\text{prf}} \). For \( i \in [2, 3] \), \( \text{mcoll}_i \) is a \( \mu \)-multi-collision event for \( F_i \). \( \text{mcoll} \) is a \( \mu \)-multi-collision event for the number of collision candidates in \( \mathcal{L}^{(\alpha)} \).

- \( \text{coll} \): \( \exists (I^1, C_{2,3}^1), (I^1, C_{2,3}^2) \in \mathcal{L}^{(\alpha)} \), s.t. \( I^1 \neq I^2 \) and \( C_{2,3}^1 = C_{2,3}^2 \).
- \( \text{mcoll}_1 \): \( \exists \alpha_1, \ldots, \alpha_\mu \in Q_2 \) s.t. \( \alpha_1 < \ldots < \alpha_\mu \) and \( Z_2^{(\alpha_1)} = \ldots = Z_2^{(\alpha_\mu)} \).
- \( \text{mcoll}_2 \): \( \exists D \in \{0, 1\}^\ell, \alpha_1, \ldots, \alpha_\mu, \beta_1, \ldots, \beta_\mu \in Q_3 \) s.t.
  - \( D_1^{(\alpha_1)}, \ldots, D_1^{(\alpha_\mu)} \) are all distinct, \( \forall i \in [\mu] : D_1^{(\alpha_i)} = D_1^{(\beta_i)}, (K_F^{(\alpha_i)}, K_T^{(\alpha_i)}, A^{(\alpha_i)}), (K_F^{(\beta_i)}, K_T^{(\beta_i)}, A^{(\beta_i)}) \neq (K_F^{(\alpha)}, K_T^{(\alpha)}, A^{(\alpha)}), (K_F^{(\beta)}, K_T^{(\beta)}, A^{(\beta)}), \) and
  - \( \forall i \in [\mu] : Z_3^{(\alpha_i)} \oplus Z_3^{(\beta_i)} = D \).
- \( \text{mcoll}_3 \): \( \exists D_2 \in Q_3, \beta_1, \ldots, \beta_\mu \in Q_2^{(\alpha_2)} \) s.t. \( \forall i \in [\mu] : (1) D_2^{(\alpha_i)} = D_2^{(\beta_i)} = Z_2^{(\beta_i)} \), (2) \( D_2^{(\beta_i)} \oplus Z_3^{(\beta_i)} = \).
By using these events, we have $\delta_{\text{coll}} = \Pr[\text{coll}] \leq \Pr[\text{coll} \mid \neg \text{mcoll}_1 \land \neg \text{mcoll}_2 \land 
abla \neg \text{mcoll}_3] + \Pr[\text{mcoll}].$ The bounds of these probabilities are given below, and we have $\delta_{\text{coll}} \leq \frac{\mu p \cdot 2^r}{2^{2m(n+1)}} + 2^r \left( \frac{cp}{2^r} \right)^{\mu} + 2^r \cdot p \cdot \left( \frac{cp}{2^r} \right)^{\mu} \leq \frac{\mu p \cdot 2^r}{2^{2m(n+1)}} \cdot \left( \frac{2^r}{2^r} \right)^{\mu}$, assuming $p \leq 2^{r-1}$.

**Evaluating $\Pr[\text{mcoll}_2].$** Fixing $\mu$ indexes $\alpha_1, \ldots, \alpha_\mu \in Q_2$, we have $\Pr[Z_2^{(\alpha_1)} = \ldots = Z_2^{(\alpha_\mu)}] \leq \left( \frac{1}{2^r} \right)^{\mu-1}$. Summing the bound for each tuple of $\mu$ indexes and using Stirling’s approximation ($x ! \geq \left( \frac{e}{x} \right)^x$, for any $x$), we have $\Pr[\text{mcoll}_2] \leq \left( \frac{1}{2^r} \right)^{\mu-1} \leq 2^r \cdot \left( \frac{cp}{2^r} \right)^{\mu}$.

**Evaluating $\Pr[\text{mcoll}_3].$** Fix $D \in \{0, 1\}^\ell$, $\alpha_1, \ldots, \alpha_\mu, \beta_1, \ldots, \beta_\nu \in Q_3$ such that $\forall i \in [\mu] : D_i^{(\alpha_i)} = D_i^{(\beta_i)}$, and $(K_F^{(\alpha_1)}, K_H^{(\alpha_1)}, A^{(\alpha_1)}) = (K_F^{(\alpha_i)}, K_H^{(\alpha_i)}, A^{(\alpha_i)}) \neq (K_F^{(\beta_1)}, K_H^{(\beta_1)}, A^{(\beta_1)}).$ We then have $\Pr[\forall i \in [\mu] : Z_3^{(\alpha_i)} = Z_3^{(\beta_i)}] = D] \leq \left( \frac{1}{2^r} \right)^{\mu}$. The number of choices of $\alpha_1, \ldots, \alpha_\mu$ is at most $\binom{\mu}{\mu}$. The number of choices of $\beta_1$ is at most $\mu$. Fixing $(\alpha_1, \ldots, \alpha_\mu, \beta_1), (\beta_2, \ldots, \beta_\nu)$ are uniquely fixed. Hence, we have $\Pr[\text{mcoll}_3] \leq 2^\ell \cdot p \cdot \left( \frac{1}{2^r} \right)^{\mu} \leq 2^\ell \cdot p \cdot \left( \frac{cp}{2^r} \right)^{\mu} \leq 2^r \cdot \left( \frac{cp}{2^r} \right)^{\mu}$, using Stirling’s approximation.

**Evaluating $\Pr[\text{mcoll}].$** Fix $\alpha_2 \in Q_2$ and $\gamma_1, \ldots, \gamma_\mu \in Q_2^{(\leq \alpha_2)} \cup Q_3^{(\leq \alpha_2)}$ 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 $\gamma_i$ query is the 3rd round of (A) in Fig. 2-(right).

**Case 2.** $\gamma_i = \beta_2, i$, i.e., the $\gamma_i$ query is the 2nd round of (B) in Fig. 2-(right).

**Case 3.** $\gamma_i = \beta_3, i$, i.e., the $\gamma_i$ query is the 3rd 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 $(K_F^{(\gamma_1)}, K_H^{(\gamma_1)}, A^{(\gamma_1)}, D_2^{(\gamma_1)})$ to $F_3$, by $\neg \text{mcoll}_2$, the number of candidates for $\beta_2, i$ (with the condition (1)) is at most $\mu$. For each of the (at most) $\mu$ candidates, $\beta_3, i$ is uniquely fixed. Then, the probability that the condition (2) is satisfied is at most $\frac{\mu}{2^r}$.

We evaluate the probability that $\gamma_i = \beta_2, i$ (Case 2) and the conditions (1),(2),(3) are satisfied. Fixing the inputs $(K_F^{(\gamma_1)}, K_H^{(\gamma_1)}, A^{(\gamma_1)}, D_2^{(\gamma_1)})$ to $F_2$, by $\neg \text{mcoll}_3$, the number of candidates for the pair $(\alpha_3, i, \beta_3, i)$ (with the condition (2)) is at most $\mu$. 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 $(K_F^{(\gamma_1)}, K_H^{(\gamma_1)}, A^{(\gamma_1)}, D_2^{(\gamma_1)})$ to $F_3$, by $\neg \text{mcoll}_2$, the number of candidates for $\beta_2, i$ is at most $\mu$. For each of the $\mu$ candidates, with the condition (1), $\alpha_3, i$ is uniquely fixed. Then, the probability that the condition (2) is satisfied is at most $\frac{\mu}{2^r}$. 
Fixing $\alpha_2 \in \mathbb{Q}_2$, 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 $\Pr[\text{mcoll}] \leq \sum_{\alpha_2 \in [\mu]} \binom{\alpha_2}{\mu} \cdot \left(\frac{3\mu}{2^\mu}\right)^\mu \leq \sum_{\alpha_2 \in [\mu]} \left(\frac{3\alpha_2}{2^\mu}\right)^\mu \leq \left(\frac{3\mu}{2^\mu}\right)^\mu$.

**Evaluating $\Pr[\text{coll} | \neg\text{mcoll}_2 \land \neg\text{mcoll}_3 \land \neg\text{mcoll}]$.** Assume that $\text{mcoll}_2, \text{mcoll}_3,$ and $\text{mcoll}$ do not occur. We then consider the case that $\text{coll}$ occurs just after the $\alpha$-th query where $\alpha \in [\mu]$.

- Consider the sub-case with $\alpha \in \mathbb{Q}_2$. Fix $\alpha \in \mathbb{Q}_2$. Let $\alpha_2 := \alpha$. By $\neg\text{mcoll}$, the number of pairs of indexes $(\alpha_3,1, \beta_3,1), (\alpha_3,2, \beta_3,1), \ldots \in (\mathbb{Q}_2^{<\alpha_2})^2$ such that the $\alpha_2$-th output $Z_2^{(\alpha)}$ probabilistically connects with $D_1^{(\alpha_3,1)}$ and yields a collision of $\text{Feistel}_3$, is at most $\mu$. See Fig. 2-(right) and the connection point is marked with (4). For each $\alpha_3,1$, we have $\Pr[D_1^{(\alpha_3,1)} = Z_2^{(\alpha_2)}] \leq \frac{1}{\mu}$. Hence, the probability that $\text{coll}$ occurs in this case is at most $\frac{\mu p}{2^\mu}$.

- Consider the sub-case with $\alpha \in \mathbb{Q}_3$. Let $\mathbb{Q}_2^{\text{new}} := \{ \beta \in \mathbb{Q}_2 | \forall \beta_0 \in [\beta - 1] \cap \mathbb{Q}_2 : Z_2^{(\beta)} \neq Z_2^{(\beta_0)} \}$ be the set of query indexes in $\mathbb{Q}_2$ such that the outputs are new. For $\beta \in \mathbb{Q}_2^{\text{new}}$, let $\mathbb{Q}_2[\beta] = \{ \beta_1 \in \mathbb{Q}_2 | Z_2^{(\beta_1)} = Z_2^{(\beta)} \}$ be multi-collision indexes with $Z_2^{(\beta)}$ and $\mu_\beta = |\mathbb{Q}_2[\beta]|$. Note that if $\text{coll}$ occurs, then there exists $\beta \in \mathbb{Q}_2^{\text{new}}$ such that $\mu_\beta \geq 2$, which is required to have a collision on the right part of $\text{Feistel}_3$. Fix $\beta \in \mathbb{Q}_2^{\text{new}}$ such that $\mu_\beta \geq 2$. Then, for each pair $(\beta_1, \beta_2) \in \mathbb{Q}_2[\beta]^2$ such that $\beta_1 \neq \beta_2$ and $(K_F^{(\beta_1)}, K_H^{(\beta_1)}, A^{(\beta_1)}) \neq (K_F^{(\beta_2)}, K_H^{(\beta_2)}, A^{(\beta_2)})$, we have $\Pr[B_3(K_F^{(\beta_1)}, K_H^{(\beta_1)}, A^{(\beta_1)}, Z_2^{(\beta_1)}) + D_2^{(\beta_1)} = B_3(K_F^{(\beta_2)}, K_H^{(\beta_2)}, A^{(\beta_2)}, Z_2^{(\beta_2)}) \neq D_2^{(\beta_2)}] \leq \frac{1}{\mu}$, which is the bound of the collision probability at the left part. Hence, the probability that the collision of $\text{Feistel}_3$ occurs due to $\mathbb{Q}_2[\beta]$ is at most $\left(\frac{\mu_\beta}{2}\right) \cdot \frac{1}{\mu} \leq \frac{0.5\mu_\beta}{2^\mu}$. Note that $\mu_\beta \leq \mu$ by $\neg\text{mcoll}_2$ and $\sum_{\beta \in \mathbb{Q}_2^{\text{new}}} \mu_\beta \leq \mu$. Summing the bound for each $\beta \in \mathbb{Q}_2^{\text{new}}$, the probability that $\text{coll}$ occurs in this case is at most $\sum_{\beta \in \mathbb{Q}_2^{\text{new}}} \frac{0.5\mu_\beta}{2^\mu} \leq \mu \sum_{\beta \in \mathbb{Q}_2^{\text{new}}} \frac{0.5\mu_\beta}{2^\mu} \leq \frac{\mu p}{2^\mu}$.

By using the bounds, we have $\Pr[\text{coll} | \neg\text{mcoll}_2 \land \neg\text{mcoll}_3 \land \neg\text{mcoll}] \leq \frac{\mu p}{2^\mu \cdot 1.17}$.

### 5 Proof of Theorem 2

Without loss of generality, assume that an adversary $A$ 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 $\omega$-th user. For $\alpha \in [q]$, let $\text{query}^{(\alpha)} \in \{\text{enc}, \text{dec}\}$ be the type of the $\alpha$-th query: $\text{query}^{(\alpha)} = \text{enc}$ (resp. $\text{dec}$) if the query is an
encryption (resp. decryption) one. Let user\(^{(\alpha)}\) be the user number of the \(\alpha\)-th query, i.e., if the \(\alpha\)-th query is to the \(\omega\)-th user, user\(^{(\alpha)}\) = \(\omega\). For \(\alpha \in [q]\), values defined at the \(\alpha\)-th query are denoted using the superscript of \((\alpha)\). 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 
\[
\text{FFF}[\Pi_{K_H^\omega}^\pm, F_{K_F^\omega}] := \text{FFF. Enc}[\Pi_{K_H^\omega}, F_{K_F^\omega}], \text{FFF. DecL}[\Pi_{K_H^\omega}^\pm, F_{K_F^\omega}]).
\]

5.2 Deriving the Bound

We consider four games G1, G2, G3, and G4. For \(i \in [4]\), let \(\mathcal{O}_i\) be the set of oracles in the game \(\mathcal{G}_i\). The games are defined below.

- G1 is the real-world and \(\mathcal{O}_1 := (\text{FFF}[\Pi_{K_B^\omega}^\pm, F_{K_F^\omega}], \ldots, \text{FFF}[\Pi_{K_H^\omega}^\pm, F_{K_F^\omega}]).\)
- G2 is a variant of G1 where the underlying functions \(F_{K_B^\omega}, \ldots, F_{K_H^\omega}\) are replaced with random functions \(R^{(1)}, \ldots, R^{(u)}\) and \(K_H^\omega\) values are removed from inputs to the random functions. Then, \(\mathcal{O}_2 := (\text{FFF}[\Pi_{K_B^\omega}^\pm, R^{(1)}], \ldots, \text{FFF}[\Pi_{K_H^\omega}^\pm, R^{(u)}]).\)
- G3 is a variant of G2 where the underlying WE \(\Pi_{K_B^\omega}^\pm, \ldots, \Pi_{K_H^\omega}^\pm\) are replaced with ideal WPs \(\psi_1^\pm, \ldots, \psi_u^\pm\). Then, \(\mathcal{O}_3 := (\text{FFF}[\psi_1^\pm, R^{(1)}], \ldots, \text{FFF}[\psi_u^\pm, R^{(u)}]).\)
- G4 is the ideal world and \(\mathcal{O}_4 := (\text{FFF}[\mathcal{S}_{\text{Enc}}, \mathcal{S}_{\text{Dec}}^{(1)}], \ldots, \text{FFF}[\mathcal{S}_{\text{Enc}}, \mathcal{S}_{\text{Dec}}^{(u)}]).\)

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

From G1 to G2, the underlying functions in G1 are replaced with random functions. Hence, \(\delta_1\) is bounded by the \(\mu\)-PRF-security advantage function of F, i.e., there exists an adversary \(\mathcal{A}_F\) making at most 3q queries and having access to \(u\) users such that \(\delta_1 \leq \text{Adv}^\mu_{\text{prf}}(\mathcal{A}_F).\)

From G2 to G3, WEs are replaced with ideal WPs. Hence, \(\delta_2\) is bounded by the \(\mu\)-SPRP-security advantage function of \(\Pi\), i.e., there exists an adversary \(\mathcal{A}_\Pi\) making at most q queries and having access to \(u\) users such that \(\delta_2 \leq \text{Adv}^\mu_{\text{sprp}}(\mathcal{A}_\Pi).\)

The bound of the \(\delta_3\) is given in Section 5.3. By using the bounds of \(\delta_1, \delta_2, \delta_3\), we have
\[
\text{Adv}_{\text{FFF}}\text{-rae}(\mathcal{A}) \leq \frac{\delta_1}{2^f} + \frac{\delta_2}{2^f} + \text{Adv}^\mu_{\text{prf}}(\mathcal{A}_F) + \text{Adv}^\mu_{\text{sprp}}(\mathcal{A}_\Pi).
\]

5.3 Bounding \(\delta_3\)

We derive the bound of \(\delta_3\) by using the coefficient-H technique [26]. The following evaluation shows that \(\delta_3 \leq \frac{\delta_1}{2^f} + \frac{\delta_2}{2^f} + \frac{\delta_3}{2^f} + \ldots + \frac{\delta_{\ell}}{2^f}.\)

Adversary’s View. We define dummy values of G4 according to the structure of FFF. The dummy values are defined in the decision stage. Let \(R : [u] \times \{1, 3\} \times \mathcal{A} \times \{0, 1\}^* \to \{0, 1\}^\ell\) 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 $\mathcal{R}_i : [u] \times \mathcal{A} \times \{0, 1\}^\tau \rightarrow \{0, 1\}^\ell$ be the random function $\mathcal{R}$ with the round number $i$. For each $\alpha \in [q]$, the dummy values of the $\alpha$-th query are defined as follows.

- $M^{(\alpha)}_1, M^{(\alpha)}_2 \leftarrow \{M\}^{1-\ell, \ell, \ell}_\alpha M^{(\alpha)}$ and $C^{(\alpha)}_1, C^{(\alpha)}_2, C^{(\alpha)}_3 \leftarrow \{C\}^{1-\ell, \ell, \ell}\alpha C^{(\alpha)}$.
- If $\text{query}^{(\alpha)} = \text{enc}$, then $T^{(\alpha)} \leftarrow 0^\tau$.
- $Z^{(\alpha)}_2 \leftarrow \mathcal{R}_1(\text{user}^{(\alpha)}, A^{(\alpha)}, T^{(\alpha)}), Z^{(\alpha)}_3 \leftarrow T^{(\alpha)} \oplus C^{(\alpha)}_3$, and $Z^{(\alpha)}_3 \leftarrow \mathcal{R}_3(\text{user}^{(\alpha)}, A^{(\alpha)}, C^{(\alpha)}_3)$.
- $M^{(\alpha)}_2 \leftarrow M^{(\alpha)}_2 \oplus Z^{(\alpha)}_1$ and $C^{(\alpha)}_2 \leftarrow C^{(\alpha)}_2 \oplus Z^{(\alpha)}_3$.

We then define a transcript $\tau$ which consists of

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

where in G3, if $\text{query}^{(\alpha)} = \text{enc}$, then $T^{(\alpha)} := 0^\tau$.

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

**Coefficient-H Technique.** Let $T_3$ be a transcript obtained by sampling in G3, i.e., sampling of $P_{\omega}$ and $\mathcal{R}_\omega$ for $\omega \in [u]$. Let $T_4$ be a transcript obtained by sampling in G4, i.e., sampling of $S_{\text{enc}}^{(\omega)}$, $S_{\text{dec}}^{(\omega)}$, and $\mathcal{R}$ for $\omega \in [u]$. We call a transcript $\tau$ valid if $\Pr[T_4 = \tau] > 0$. Let $T$ be the set of all valid transcripts such that $\forall \tau \in T : \Pr[T_3 = \tau] \leq \Pr[T_4 = \tau]$. Then, we have $\delta_3 \leq \text{SD}(T_3, T_4) := \sum_{\tau \in T} (\Pr[T_3 = \tau] - \Pr[T_4 = \tau])$.

We can derive the bound of $\delta_3$ by using the coefficient-H technique [26].

**Lemma 2.** Let $T_{\text{good}}$ and $T_{\text{bad}}$ be good and bad transcripts into which $T$ is partitioned. If $\forall \tau \in T_{\text{good}} : \frac{\Pr[T_3 = \tau]}{\Pr[T_4 = \tau]} \geq 1 - \varepsilon$ s.t. $0 \leq \varepsilon \leq 1$, then $\text{SD}(T_3, T_4) \leq \Pr[T_4 \in T_{\text{bad}}] + \varepsilon$.

We thus (1) define good and bad transcripts; (2) upper-bound $\Pr[T_4 \in T_{\text{bad}}]$; and (3) lower-bound $\frac{\Pr[T_3 = \tau]}{\Pr[T_4 = \tau]}$. Then, putting these bounds into the above lemma, we obtain the upper-bound of $\delta_3$.

In the following, firstly good and bad transcripts are defined. Then, in Section 5.4, the upper-bound of $\Pr[T_4 \in T_{\text{bad}}]$ is derived. In Section 5.5, the lower-bound of $\frac{\Pr[T_3 = \tau]}{\Pr[T_4 = \tau]}$. By using these bounds, we have $\delta_3 \leq \frac{\delta_0}{2^\omega} + \frac{\delta_2}{2^\omega}$.

**Good and Bad Transcripts and Bound of $\delta_3$.** We define bad events below.

- **bad$_1$**: $\exists \alpha, \beta \in [q]$ s.t. $\alpha > \beta$, $\text{user}^{(\alpha)} = \text{user}^{(\beta)}$, and
  - $\text{query}^{(\alpha)} = \text{enc} \land \bar{C}^{(\alpha)}_2 = \bar{C}^{(\beta)}_2$ or
  - $\text{query}^{(\alpha)} = \text{dec} \land \bar{M}^{(\alpha)}_2 = \bar{M}^{(\beta)}_2$.
- **bad$_2$**: $\exists \alpha, \beta \in [q]$ s.t. $\alpha > \beta$, $\text{user}^{(\alpha)} = \text{user}^{(\beta)}$, and
  - $\text{query}^{(\alpha)} = \text{enc} \land (A^{(\alpha)}, M^{(\alpha)}_2) \neq (A^{(\beta)}, M^{(\beta)}_2) \land \bar{M}^{(\alpha)}_2 = \bar{M}^{(\beta)}_2$ or
  - $\text{query}^{(\alpha)} = \text{dec} \land (A^{(\alpha)}, C^{(\alpha)}_2, C^{(\alpha)}_3) \neq (A^{(\beta)}, C^{(\beta)}_2, C^{(\beta)}_3) \land \bar{C}^{(\alpha)}_2 = \bar{C}^{(\beta)}_2$.
- **bad$_3$**: $\exists \alpha \in [q]$ s.t. $\text{query}^{(\alpha)} = \text{dec}$ and $T^{(\alpha)} = 0^\tau$.

Let $\text{bad} = \text{bad}_1 \lor \text{bad}_2 \lor \text{bad}_3$.

$T_{\text{bad}}$ is a set of transcripts that satisfy bad, and $T_{\text{good}} := T \setminus T_{\text{bad}}$.  

5.4 Evaluation for Bad Transcript

We derive the bound of $\Pr[T_4 \in T_{\text{bad}}]$. For $i \in [3]$, let $\text{bad}_i^*$ be an event that $\text{bad}_i^*$ occurs before the other bad events occur. Then, we have $\Pr[T_4 \in T_{\text{bad}}] \leq \Pr[\text{bad}_1^*] + \Pr[\text{bad}_2^*] + \Pr[\text{bad}_3^*]$. The bounds of $\Pr[\text{bad}_1^*]$, $\Pr[\text{bad}_2^*]$, and $\Pr[\text{bad}_3^*]$ are given below, and we have $\Pr[T_4 \in T_{\text{bad}}] \leq \frac{5q^2}{2^7} + \frac{5q^2}{2^3}$.

Evaluating $\Pr[\text{bad}_1^*]$. We first consider a pair $(\alpha, \beta) \in [q]^2$ such that $\alpha > \beta$, $\text{user}^{(\alpha)} = \text{user}^{(\beta)}$, and $\text{query}^{(\alpha)} = \text{enc}$, and evaluate the collision probability $\Pr[C_2^{(\alpha)} = C_2^{(\beta)}]$.

- If the inputs to $R_3$ are distinct, $(A^{(\alpha)}, C_3^{(\alpha)}) \neq (A^{(\beta)}, C_3^{(\beta)})$, then $C_2^{(\alpha)}$ and $C_2^{(\beta)}$ are independently defined and we have $\Pr[C_2^{(\alpha)} = C_2^{(\beta)}] \leq \frac{1}{2^7}$.
- If the inputs to $R_3$ are the same, i.e., $Z_3^{(\alpha)} = Z_3^{(\beta)}$, then $C_2^{(\alpha)}$ is uniformly at random from $\{0, 1\}^t$, thus we have $\Pr[C_2^{(\alpha)} = C_2^{(\beta)}] \leq \frac{1}{2^t}$.

Regarding a pair $(\alpha, \beta) \in [q]^2$ such that $\alpha > \beta$ and $\text{query}^{(\alpha)} = \text{dec}$, the evaluation is the same as that with $\text{query}^{(\alpha)} = \text{enc}$ due to the symmetric structure of $F$. We thus have $\Pr[M_2^{(\alpha)} = M_2^{(\beta)}] \leq \frac{1}{2^7}$.

By summing these bounds for each $(\alpha, \beta) \in [q]^2$ such that $\alpha > \beta$, we have $\Pr[\text{bad}_1^*] \leq \frac{5q^2}{2^7} + \frac{5q^2}{2^3}$.

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

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

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

- If $(A^{(\alpha)}, C_3^{(\alpha)}) = (A^{(\beta)}, C_3^{(\beta)})$, $C_2^{(\alpha)} \neq C_2^{(\beta)}$, then $Z_3^{(\alpha)} = Z_3^{(\beta)}$, thus we have $\Pr[C_2^{(\alpha)} = C_2^{(\beta)}] = 0$.
- If $A^{(\alpha)} = A^{(\beta)}$, $C_3^{(\alpha)} \neq C_3^{(\beta)}$, then $Z_3^{(\alpha)}$ and $Z_3^{(\beta)}$ are independently chosen.

We thus have $\Pr[C_2^{(\alpha)} = C_2^{(\beta)}] \leq \frac{1}{2^t}$.

By summing these bounds for each $(\alpha, \beta) \in [q]^2$ such that $\alpha > \beta$, we have $\Pr[\text{bad}_2^*] \leq \frac{5q^2}{2^7} + \frac{5q^2}{2^3}$.

Bounding $\Pr[\text{bad}_3^*]$. For each $\alpha \in [q]$ such that $\text{query}^{(\alpha)} = \text{dec}$, $T^{(\alpha)}$ is chosen uniformly at random from $\{0, 1\}^n$. We thus have $\Pr[\text{bad}_3^*] \leq \sum_{\alpha \in [q]} \Pr[T^{(\alpha)} = 0^*] \leq \frac{5q}{2^t}$. 


5.5 Evaluation for Good Transcript

Fix a good transcript $\tau$. Values in $\tau$ are denoted by using the symbol “$*$”, e.g., $M^{\ast}(\alpha), C^{\ast}(\alpha), Z_1^{\ast}(\alpha)$, etc. Let $\tau_{M,C,T} = \{ M^{\ast}(\alpha), C^{\ast}(\alpha), T^{\ast}(\alpha) \mid \alpha \in [q] \}$, and $\tau_{Z,3} = \{ Z_1^{\ast}(\alpha), Z_3^{\ast}(\alpha) \mid \alpha \in [q] \}$. For a set $S$ and $i \in [3,4]$, let $T_i \vdash S$ be an event that sampling of $T_i$ results in elements in $S$. For each $\alpha \in [q]$, let $c_\alpha := |C^{\ast}(\alpha)|$. Let $N_1$ (resp. $N_3$) be the number of distinct inputs to $R_1$ (resp. $R_3$) defined from $\tau$, i.e., $N_1 = \{ (\text{user}^{\ast}(\alpha), A^{\ast}(\alpha), T^{\ast}(\alpha)) \mid \alpha \in [q] \}$ and $N_3 = \{ (\text{user}^{\ast}(\alpha), A^{\ast}(\alpha), C^{\ast}(\alpha)) \mid \alpha \in [q] \}$. Note that by $\neg \text{bad}_1$ and $\neg \text{bad}_2$, $\tau$ is defined such that all $M_2$ values are distinct and $C_2$ values are distinct, thus the number of distinct inputs to $R_2$ is $q$.

**Evaluating $\Pr[T_4 = \tau]$.** We evaluate the probabilities $\Pr[T_4 \vdash \tau_{M,C,T}]$ and $\Pr[T_4 \vdash \tau_{Z,3}]$, since $\Pr[T_4 = \tau] = \Pr[T_4 \vdash \tau_{M,C,T}] \cdot \Pr[T_4 \vdash \tau_{Z,3}]$ and $Z_2^{\ast}(\alpha) = T^{\ast}(\alpha) \oplus C_3^{\ast}(\alpha)$.

Evaluating $\Pr[T_4 \vdash \tau_{M,C,T}]$. For each $\alpha \in [q]$.

- If $\text{query}(\alpha) = \text{enc}$, then $C^{\ast}(\alpha)$ is chosen uniformly at random from $\{0,1\}^{c_\alpha}$, we have $\Pr[T_4 \vdash \{ M^{\ast}(\alpha), C^{\ast}(\alpha) \}] = \frac{1}{2^{c_\alpha}}$, and
- If $\text{query}(\alpha) = \text{dec}$, then $M^{\ast}(\alpha)$ is chosen uniformly at random from $\{0,1\}^{c_\alpha-r}$ and $T^{\ast}(\alpha)$ is chosen uniformly at random from $\{0,1\}^r$, we have $\Pr[T_4 \vdash \{ M^{\ast}(\alpha), C^{\ast}(\alpha) \}] = \frac{1}{2^{c_\alpha}}$. By using the probabilities, we have $\Pr[T_4 \vdash \tau_{M,C,T}] = \prod_{\alpha \in [q]} \frac{1}{2^{c_\alpha}}$.

Evaluating $\Pr[T_4 \vdash \tau_{Z,3}]$. For each new input to $R$, the output is chosen uniformly at random from $\{0,1\}^4$, thus we have $\Pr[T_4 \vdash \tau_{Z,3}] = \left( \frac{1}{2} \right)^{N_1 + N_3}$.

By using the probabilities, we have $\Pr[T_4 = \tau] = \left( \prod_{\alpha \in [q]} \frac{1}{2^{c_\alpha}} \right) \cdot \left( \frac{1}{2} \right)^{N_1 + N_3}$.

**Evaluating $\Pr[T_3 = \tau]$.** We evaluate the probabilities $\Pr[T_3 \vdash \tau_{M,C,T}]$ and $\Pr[T_3 \vdash \tau_{Z,3}]$.

Evaluating $\Pr[T_3 \vdash \tau_{Z,3}]$. For each new input to $R$, the output is chosen uniformly at random from $\{0,1\}^4$, thus we have $\Pr[T_3 \vdash \tau_{Z,3}] = \left( \frac{1}{2} \right)^{N_1 + N_3}$.

Evaluating $\Pr[T_3 \vdash \tau_{M,C,T}]$. For each $\alpha \in [q]$, if $\text{query}(\alpha) = \text{enc}$ (resp. $\text{query}(\alpha) = \text{dec}$), then $\neg \text{bad}_2$, the input to $\Psi_{\text{user}(\alpha)}$ (resp. $\Psi^{-1}_{\text{user}(\alpha)}$) is distinct from the previous inputs, thus chosen uniformly at random from $\{0,1\}^{c_\alpha} \setminus \{ C^{\ast}(\beta) \mid \beta \in [\alpha-1] \land \text{user}(\beta) = \text{user}(\alpha) \}$ (resp. $\{0,1\}^{c_\alpha} \setminus \{ C^{\ast}(\beta) \mid \beta \in [\alpha-1] \land \text{user}(\beta) = \text{user}(\alpha) \}$). By $\neg \text{bad}_1$ and $\neg \text{bad}_2$, the input to $R_2$ at the $\alpha$-th query is new, thus the output is chosen uniformly at random from $\{0,1\}^r$. We thus have $\Pr[T_3 \vdash \{ M^{\ast}(\alpha), C^{\ast}(\alpha), T^{\ast}(\alpha) \}] \geq \frac{1}{2^{c_\alpha-r}} \cdot \frac{1}{2^r} = \frac{1}{2^{c_\alpha}}$. By using the bound, we have $\Pr[T_3 \vdash \tau_{M,C,T}] \geq \prod_{\alpha \in [q]} \frac{1}{2^{c_\alpha}}$.

By using the probabilities, we have $\Pr[T_3 = \tau] \geq \left( \prod_{\alpha \in [q]} \frac{1}{2^{c_\alpha}} \right) \cdot \left( \frac{1}{2} \right)^{N_1 + N_3}$.

**Lower-bound of $\frac{\Pr[T_3 = \tau]}{\Pr[T_4 = \tau]}$.** By the above bounds, we have $\frac{\Pr[T_3 = \tau]}{\Pr[T_4 = \tau]} \geq 1$. 

$\Pr[T_3 = \tau]$ and $\Pr[T_4 = \tau]$
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, $\max\{s_{cmt}, s_{rae}\}$ bits from an original message. With $s_{cmt} \geq s_{rae}$, $s_{cmt}$ 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

12. Dobrâuńig, C., Matusiewicz, K., Mennink, B., Tereschenko, A.: Efficient instances of 
docked double decker with AES. IACR Trans. Cryptol. ePrint. Arch. p. 84 (2024), 
https://eprint.iacr.org/2024/084
Springer (2018)
 modes of operation: Methods and techniques. https://csrc.nist.gov/pubs/sp/800/38/a 
final (2001)
15. Farshim, P., Orlandi, C., Rosie, R.: Security of symmetric primitives under incorrect 
17. Gunsing, A., Daemen, J., Mennink, B.: Deck-based wide block cipher modes and 
an exposition of the blinded keyed hashing model. IACR Cryptol. ePrint Arch. 
(2022), https://eprint.iacr.org/2022/247
19. Hoang, V.T., Krovetz, T., Rogaway, P.: Robust authenticated-encryption AEZ and 
the problem that it solves. In: EUROCRYPT 2015. LNCS, vol. 9056, pp. 15–44 
(2015)
379–407. LNCS (2023)
using redundancy and application to GCM, CCM, and more. In: ACNS 2024. 
LNCS, vol. 14583, pp. 318–347 (2024)
23. National Institute of Standards and Technology (NIST): The Third NIST Workshop on 
(2023)
24. National Institute of Standards and Technology (NIST): NIST workshop on the requirements 
WorkshopAnnouncement-CipherModes2024.pdf (2024)
(2018)
Springer (2008)
27. Shrimpton, T., Terashima, R.S.: A modular framework for building variable-input-
Appendix

A Figures

Fig. 3. FFF.Dec.
Fig. 4. The conditions on the event mcoll3.
Fig. 5. The $\omega$-th user’s encryption in $G2$ of the proof of Theorem 2.

Fig. 6. The $\omega$-th user’s encryption in $G3$ of the proof of Theorem 2.