Committing Wide Encryption Mode with Minimum Ciphertext Expansion

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

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

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

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

1 Introduction

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

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

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

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

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

4 Proof of Theorem 1

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

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

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

and $(K_{\mathsf{F}}^{\ddagger}, K_{\Pi}^{\ddagger}, A^{\ddagger}, M_2^{\ddagger}, \widetilde{C}_2^{\ddagger})$ such that $(K_{\mathsf{F}}^{\dagger}, K_{\Pi}^{\dagger}, A^{\dagger}) \neq (K_{\mathsf{F}}^{\ddagger}, K_{\Pi}^{\ddagger}, A^{\ddagger})$, $\mathbf{Adv}^{\mathsf{cmt\text{-}3}}_{\mathsf{FFF}}(\mathbf{A}) \leq \delta_{\mathsf{coll}} := \Pr\Big[\mathsf{Feistel}^3_{0^r}[\mathsf{F}](K_{\mathsf{F}}^{\dagger}, K_{\Pi}^{\dagger}, A^{\dagger}, M_2^{\dagger}, \widetilde{C}_2^{\dagger}) = \mathsf{Feistel}^3_{0^r}[\mathsf{F}](K_{\mathsf{F}}^{\ddagger}, K_{\Pi}^{\ddagger}, A^{\ddagger}, M_2^{\ddagger}, \widetilde{C}_2^{\ddagger})\Big]$, and the random-oracle list $\mathcal{T}_{\mathsf{F}}$ includes input-output tuples needed to perform $\mathsf{Feistel}^3_{0^r}[\mathsf{F}](K_{\mathsf{F}}^{\dagger}, K_{\Pi}^{\dagger}, A^{\dagger}, M_2^{\dagger}, \widetilde{C}_2^{\dagger})$ and $\mathsf{Feistel}^3_{0^r}[\mathsf{F}](K_{\mathsf{F}}^{\ddagger}, K_{\Pi}^{\ddagger}, A^{\ddagger}, M_2^{\ddagger}, \widetilde{C}_2^{\ddagger})$.

4.2 Collision Resistance of the Disjointed 3-round Feistel

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

Intuition. We use a $(\ell + r)$-multi-collision event in Z_2 values of r bits. The multi-collision probability is at most $\binom{p}{\ell+r}(1/2^r)^{\ell+r-1} \leq (\ell + r)p/2^r$. 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 $\mathsf{Feistel}^3_{0^r}$ occurs, there exists a pair of the $\ell + r$ inputs to F_3, the outputs C_2 must be equal, and the collision probability is at most $(\ell + r)^2/2^\ell$. Since the number of such multi-collision groups for C_3 is at most p, we have $\delta_{\mathsf{coll}} \leq (\ell+r)p/2^r + (\ell+r)^2p/2^\ell$. Note that the intuition does not consider query orders between F_2 and F_3 for the collision of $\mathsf{Feistel}^3_{0^r}$. The following evaluation derive a (slightly) better bound by taking into account the orders.

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

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

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

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

$D_2^{(\alpha_2)} \oplus Z_3^{(\alpha_{3,i})}$, and (3) $(K_{\mathsf{F}}^{(\alpha_2)}, K_{\Pi}^{(\alpha_2)}, A^{(\alpha_2)}) = (K_{\mathsf{F}}^{(\alpha_{3,i})}, K_{\Pi}^{(\alpha_{3,i})}, A^{(\alpha_{3,i})}) \neq (K_{\mathsf{F}}^{(\beta_{2,i})}, K_{\Pi}^{(\beta_{2,i})}, A^{(\beta_{2,i})}) = (K_{\mathsf{F}}^{(\beta_{3,i})}, K_{\Pi}^{(\beta_{3,i})}, A^{(\beta_{3,i})})$. (See Fig. 2-(right).)

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

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

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

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

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

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

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

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

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

Evaluating $\Pr[\mathsf{coll} \mid \neg\mathsf{mcoll}_2 \wedge \neg\mathsf{mcoll}_3 \wedge \neg\mathsf{mcoll}]$. Assume that mcoll_2, mcoll_3, and mcoll do not occur. We then consider the case that coll occurs just after the α-th query where $\alpha \in [p]$.

- Consider the sub-case with $\alpha \in \mathcal{Q}_2$. Fix $\alpha \in \mathcal{Q}_2$. Let $\alpha_2 := \alpha$. By $\neg\mathsf{mcoll}$, the number of pairs of indexes $(\alpha_{3,1}, \beta_{3,1}), (\alpha_{3,2}, \beta_{3,1}), \ldots \in (\mathcal{Q}_3^{(<\alpha_2)})^2$ such that the α_2-th output $Z_2^{(\alpha)}$ probabilistically connects with $D_1^{(\alpha_{3,i})}$ and yields a collision of $\mathsf{Feistel}_{0^r}^3$ is at most μ. See Fig. 2-(right) and the connection point is marked with (4). For each $\alpha_{3,i}$, we have $\Pr[D_1^{(\alpha_{3,i})} = Z_2^{(\alpha_2)}] \le \frac{1}{2^r}$. Hence, the probability that coll occurs in this case is at most $\frac{\mu p}{2^r}$.
- Consider the sub-case with $\alpha \in \mathcal{Q}_3$. Let $\mathcal{Q}_2^{\mathsf{new}} := \{\beta \in \mathcal{Q}_2 \mid \forall \beta_0 \in [\beta-1] \cap \mathcal{Q}_2 : Z_2^{(\beta)} \neq Z_2^{(\beta_0)}\}$ be the set of query indexes in $\mathcal{Q}_2$ such that the outputs are new. For $\beta \in \mathcal{Q}_2^{\mathsf{new}}$, let $\mathcal{Q}_2[\beta] = \{\ \beta_1 \in \mathcal{Q}_2 \mid Z_2^{(\beta_1)} = Z_2^{(\beta)}\}$ be multi-collision indexes with $Z_2^{(\beta)}$ and $\mu_\beta = |\mathcal{Q}_2[\beta]|$. Note that if coll occurs, then there exists $\beta \in \mathcal{Q}_2^{\mathsf{new}}$ such that $\mu_\beta \ge 2$, which is required to have a collision on the right part of $\mathsf{Feistel}_{0^r}^3$. Fix $\beta \in \mathcal{Q}_2^{\mathsf{new}}$ such that $\mu_\beta \ge 2$. Then, for each pair $(\beta_1, \beta_2) \in \mathcal{Q}_2[\beta]^2$ such that $\beta_1 \neq \beta_2$ and $(K_{\mathsf{F}}^{(\beta_1)}, K_{\Pi}^{(\beta_1)}, A^{(\beta_1)}) \neq (K_{\mathsf{F}}^{(\beta_2)}, K_{\Pi}^{(\beta_2)}, A^{(\beta_2)})$, we have $\Pr\Big[\mathsf{F}_3(K_{\mathsf{F}}^{(\beta_1)}, K_{\Pi}^{(\beta_1)}, A^{(\beta_1)}, Z_2^{(\beta_1)}) \oplus D_2^{(\beta_1)} = \mathsf{F}_3(K_{\mathsf{F}}^{(\beta_2)}, K_{\Pi}^{(\beta_2)}, A^{(\beta_2)}, Z_2^{(\beta_2)}) \oplus D_2^{(\beta_2)}\Big] \le \frac{1}{2^\ell}$, which is the bound of the collision probability at the left part. Hence, the probability that the collision of $\mathsf{Feistel}_{0^r}^3$ occurs due to $\mathcal{Q}_2[\beta]$ is at most $\binom{\mu_\beta}{2} \cdot \frac{1}{2^\ell} \le \frac{0.5\mu_\beta^2}{2^\ell}$. Note that $\mu_\beta \le \mu$ by $\neg\mathsf{mcoll}_2$ and $\sum_{\beta \in \mathcal{Q}_2^{\mathsf{new}}} \mu_\beta \le p$. Summing the bound for each $\beta \in \mathcal{Q}_2^{\mathsf{new}}$, the probability that coll occurs in this case is at most $\sum_{\beta \in \mathcal{Q}_2^{\mathsf{new}}} \frac{0.5\mu_\beta^2}{2^\ell} \le \mu \sum_{\beta \in \mathcal{Q}_2^{\mathsf{new}}} \frac{0.5\mu_\beta}{2^\ell} \le \frac{\mu p}{2^\ell}$.

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

5 Proof of Theorem 2

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

5.1 Notations

We define notations for this proof. Let q_e (resp. q_d) be the number of encryption (resp. decryption) queries, where $q = q_e + q_d$. For $\omega \in [u]$, let $\hat{q}_\omega$ be the number of queries to the ω-th user. For $\alpha \in [q]$, let $\mathsf{query}^{(\alpha)} \in \{\mathsf{enc}, \mathsf{dec}\}$ be the type of the α-th query: $\mathsf{query}^{(\alpha)} = \mathsf{enc}$ (resp. dec) if the query is an

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

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

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

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., there exists an adversary $\mathbf{A}_\mathsf{F}$ making at most $3q$ queries and having access to u users such that $\delta_1 \le \mathbf{Adv}^{\mathsf{mu\text{-}prf}}_{\mathsf{F}}(\mathbf{A}_\mathsf{F})$.

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 $\delta_2 \le \mathbf{Adv}^{\mathsf{mu\text{-}sprp}}_{\Pi}(\mathbf{A}_\Pi)$.

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

5.3 Bounding δ_3

We derive the bound of δ_3 by using the coefficient-H technique [26]. The following evaluation shows that $\delta_3 \le \frac{q_u q}{2^\ell} + \frac{q_d}{2^\tau}$.

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 $\mathcal{R} : [u] \times \{1, 3\} \times \mathcal{A} \times \{0,1\}^\tau \to \{0,1\}^\ell$ be a random function. The first element is a user index

and the second one is a round number. For $i \in \{1,3\}$, let $\mathcal{R}_i : [u] \times \mathcal{A} \times \{0,1\}^r \to \{0,1\}^\ell$ be the random function $\mathcal{R}$ with the round number i. For each $\alpha \in [q]$, the dummy values of the α-th query are defined as follows.

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

We then define a transcript τ which consists of

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

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

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

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

We can derive the bound of δ_3 by using the coefficient-H technique [26].

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

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

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

Good and Bad Transcripts and Bound of δ_3. We define bad events below.

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

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

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

5.4 Evaluation for Bad Transcript

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

Evaluating $\Pr[\mathsf{bad}_1^*]$. We first consider a pair $(\alpha, \beta) \in [q]^2$ such that $\alpha > \beta$, $\mathsf{user}^{(\alpha)} = \mathsf{user}^{(\beta)}$, and $\mathsf{query}^{(\alpha)} = \mathsf{enc}$, and evaluate the collision probability $\Pr[\widetilde{C}_2^{(\alpha)} = \widetilde{C}_2^{(\beta)}]$.

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

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

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

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

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

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

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

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

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

5.5 Evaluation for Good Transcript

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

Evaluating $\Pr[\mathsf{T}_4 = \tau]$. 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 $\Pr[\mathsf{T}_4 = \tau] = \left(\prod_{\alpha\in[q]} \frac{1}{2^{c_\alpha}}\right) \cdot \left(\frac{1}{2^\ell}\right)^{N_1+N_3}$.

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

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

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

6 Conclusion

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

References

1. Albertini, A., Duong, T., Gueron, S., Kölbl, S., Luykx, A., Schmieg, S.: How to abuse and fix authenticated encryption without key commitment. In: USENIX Security 2022. pp. 3291–3308 (2022)
2. Andreeva, E., Bogdanov, A., Luykx, A., Mennink, B., Mouha, N., Yasuda, K.: How to securely release unverified plaintext in authenticated encryption. In: ASIACRYPT 2014. LNCS, vol. 8873, pp. 105–125 (2014)
3. Bellare, M., Hoang, V.T.: Efficient schemes for committing authenticated encryption. In: EUROCRYPT 2022. vol. 13276, pp. 845–875 (2022)
4. Bellare, M., Hoang, V.T., Wu, C.: 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)
5. Bellare, M., Rogaway, P.: Encode-then-encipher encryption: How to exploit nonces or redundancy in plaintexts for efficient cryptography. In: ASIACRYPT 2000. pp. 317–330 (2000)
6. Bhaumik, R., List, E., Nandi, M.: ZCZ - achieving n-bit SPRP security with a minimal number of tweakable-block-cipher calls. In: ASIACRYPT 2018. pp. 336–366 (2018)
7. Băcuieți, N., Daemen, J., Hoffert, S., Assche, G.V., Keer, R.V.: Jammin' on the deck. In: ASIACRYPT 2022. pp. 555–584 (2022)
8. Chan, J., Rogaway, P.: On committing authenticated-encryption. In: ESORICS 2022. vol. 13555, pp. 275–294 (2022)
9. Chen, Y.L., Flórez-Gutiérrez, A., Inoue, A., Ito, R., Iwata, T., Minematsu, K., Mouha, N., Naito, Y., Sibleyras, F., Todo, Y.: Key committing security of AEZ and more. IACR Trans. Symmetric Cryptol. **2023**(4), 452–488 (2023)
10. Crowley, P., Biggers, E.: Adiantum: length-preserving encryption for entry-level processors. IACR Trans. Symmetric Cryptol. **2018**(4), 39–61 (2018)
11. Crowley, P., Huckleberry, N., Biggers, E.: Length-preserving encryption with HCTR2. IACR Cryptol. ePrint Arch. (2021), https://eprint.iacr.org/2021/1441

12. Dobraunig, C., Matusiewicz, K., Mennink, B., Tereschenko, A.: Efficient instances of docked double decker with AES. IACR Cryptol. ePrint Arch. p. 84 (2024), https://eprint.iacr.org/2024/084
13. Dodis, Y., Grubbs, P., Ristenpart, T., Woodage, J.: Fast message franking: From invisible salamanders to encryptment. In: CRYPTO 2018. vol. 10991, pp. 155–186. Springer (2018)
14. Dworkin, M.: NIST Special Publication 800-38A: Recommendation for block cipher modes of operation: Methods and techniques. https://csrc.nist.gov/pubs/sp/800/38/a/final (2001)
15. Farshim, P., Orlandi, C., Rosie, R.: Security of symmetric primitives under incorrect usage of keys. IACR Trans. Symmetric Cryptol. **2017**(1), 449–473 (2017)
16. Grubbs, P., Lu, J., Ristenpart, T.: Message franking via committing authenticated encryption. In: CRYPTO 2017. pp. 66–97 (2017)
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
18. Halevi, S., Rogaway, P.: A parallelizable enciphering mode. In: CT-RSA 2004. LNCS, vol. 2964, pp. 292–304 (2004)
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)
20. Len, J., Grubbs, P., Ristenpart, T.: Partitioning oracle attacks. In: USENIX Security 2021. pp. 195–212 (2021)
21. Menda, S., Len, J., Grubbs, P., Ristenpart, T.: Context discovery and commitment attacks - how to break CCM, EAX, SIV, and more. In: EUROCRYPT 2023. pp. 379–407. LNCS (2023)
22. Naito, Y., Sasaki, Y., Sugawara, T.: KIVR: committing authenticated encryption 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 Block Cipher Modes of Operation 2023. https://csrc.nist.gov/events/2023/third-workshop-on-block-cipher-modes-of-operation (2023)
24. 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)
25. Nir, Y., Langley, A.: ChaCha20 and Poly1305 for IETF protocols. RFC **8439**, 1–46 (2018)
26. Patarin, J.: The "Coefficients H" Technique. In: SAC 2008. vol. 5381, pp. 328–345. Springer (2008)
27. Shrimpton, T., Terashima, R.S.: A modular framework for building variable-input-length tweakable ciphers. In: ASIACRYPT 2013. pp. 405–423 (2013)

Appendix

A Figures

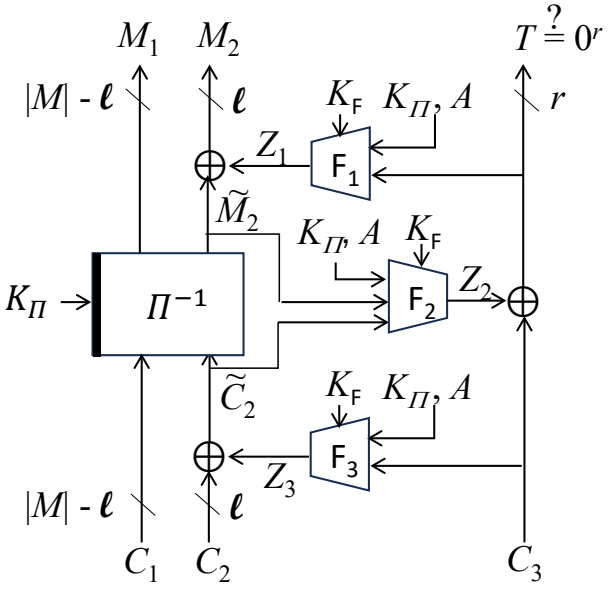

Fig. 3. FFF.Dec.

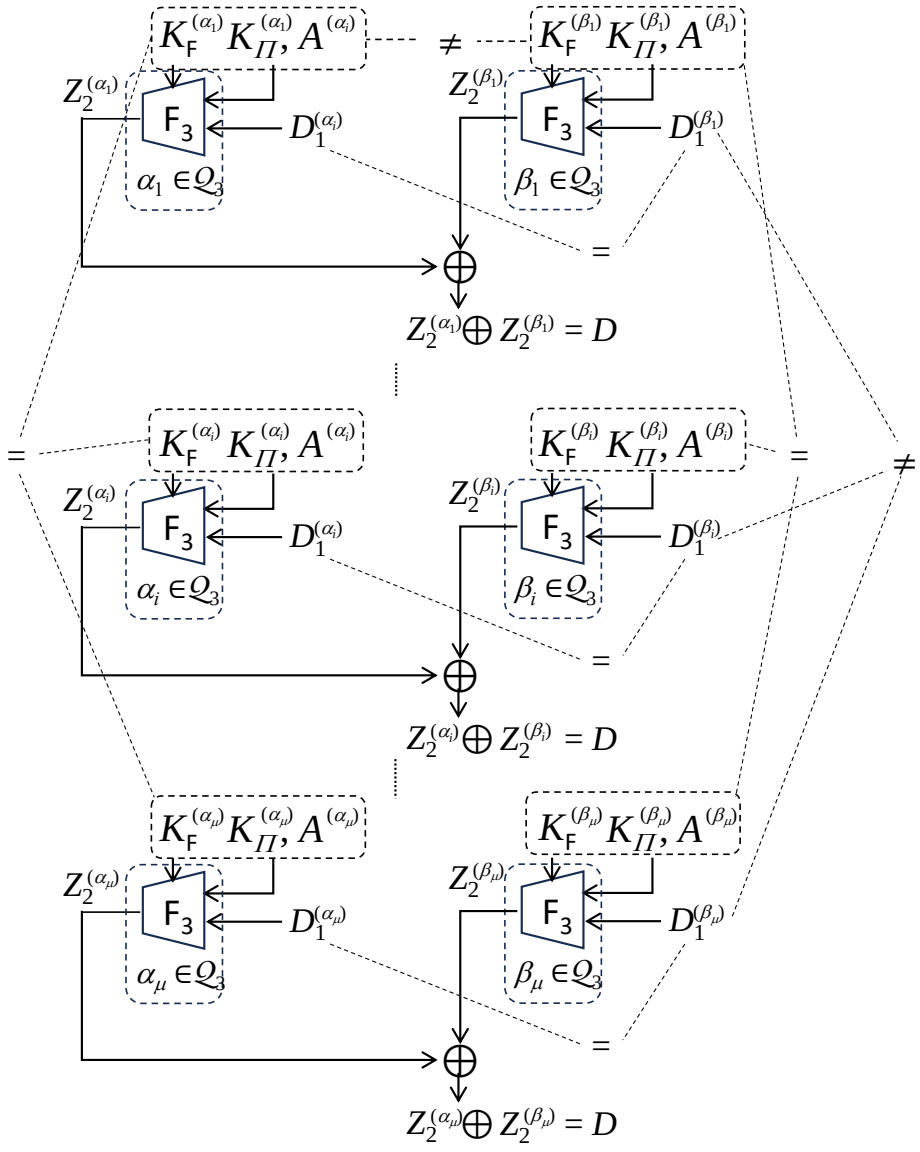

Fig. 4. The conditions on the event mcoll_3.

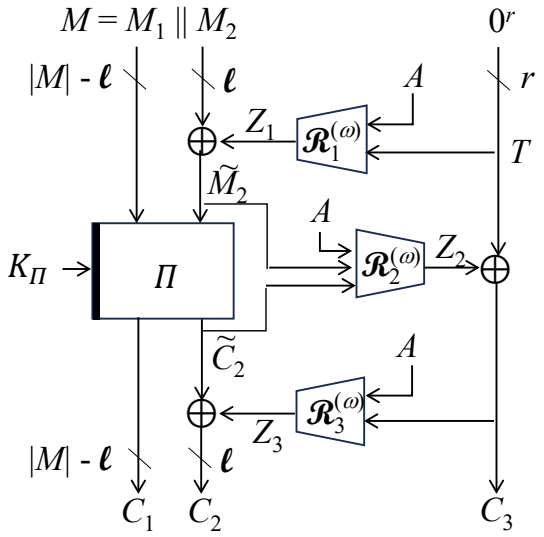

Fig. 5. The ω-th user's encryption in **G**2 of the proof of Theorem 2.

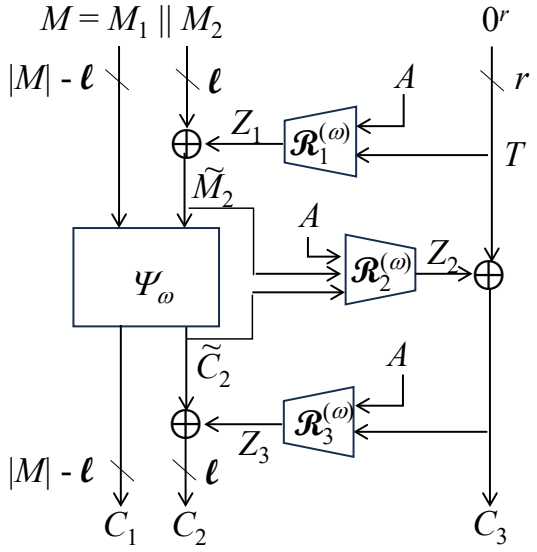

Fig. 6. The ω-th user's encryption in **G**3 of the proof of Theorem 2.