Security Proof of mixFeed

Bishwajit Chakraborty and Mridul Nandi

Indian Statistical Institute, Kolkata

Abstract. mixFeed is a round 1 candidate in NIST LwC competition. It is important in the sense that it uses a state size as small as the block size of the underlying block cipher primitive. In this paper we define a new AEAD mode called mF which can viewed as a generalization of mixFeed. We give a security bound on mF and then comparing it with mixFeed we finally give a security bound of mixFeed. We conclude that mixFeed in secure within the NIST prescribed Data complexity of 2^{50} bytes and time complexity of 2^{112}.

1 Introduction

In recent years lightweight cryptography has been immensely popular in the sense that the modern computing is switching from desktop computers to small devices. due to the resource restrain in these small devices, lightweight schemes must be used to provide security . In this respect, to increase the research interest of the scientific community, NIST has initiated a Light Weight Cryptography competition. mixFeed [1] is a round one candidate in the NIST-LwC competition. In comparison to other submissions mixFeed has the major advantage that it is the only submission that has a state size as small as the block size of the underlying cipher along with other advantages like it uses minimal number of xor counts, it is inverse free and uses dynamic nonce dependent key.

Our Contribution

1. In **Section 2** we define a new mode of light weight AEAD called mF, which can be viewed as a more generalized version of mixFeed.
2. In **Section 3** we define different security notions of mF and in **Section 4-5** we give the complete security proof of mF. The **Main Results** being For any adversary running in time t and making atmost q many encryption and decryption(in case of forgery) query with total of at most σ many blocks,

   Theorem 1.

$$\mathbf{Adv}^{priv}_{\mathsf{mF}}(q,\sigma,t) \leq \frac{t+\sigma}{2^n} + \frac{\sigma^2}{2^{n+1}} + \frac{2\mu t}{2^n} + \frac{\binom{\sigma}{\mu+1}}{(2^n)^\mu} + \sigma\left(1+\frac{\mu^2}{2^n}\right)\left(\frac{\sigma}{2^{\frac{n}{2}}}\right)^{\mu-1}.$$

   Theorem 2.

$$\mathbf{Adv}^{forge}_{\mathsf{mF}}(q,\sigma,t) \leq \frac{\sigma}{2^{\frac{n}{2}}} + \frac{t+\sigma}{2^n} + \frac{3\sigma^2}{2^{n+1}} + \frac{2\mu t}{2^n} + \frac{\binom{\sigma}{\mu+1}}{(2^n)^\mu} + \sigma\left(1+\frac{\mu^2}{2^n}\right)\left(\frac{\sigma}{2^{\frac{n}{2}}}\right)^{\mu-1}$$

where n is the state size and μ is the number of multi collisions allowed in the input of the tweakable blockcipher(explained later in details).For all calculation purposes take $\mu \geq 5$.

Note that According to NIST requirement $\sigma \leq 2^{46}$ and $t \leq 2^{112}$. Following $\mathsf{mixFeed}$ we take $n = 128$ and $\mu = 5$. Then We have $\sigma\left(1 + \frac{\mu^2}{2^n}\right)\left(\frac{\sigma}{2^{\frac{n}{2}}}\right)^{\mu-1} < \frac{1}{2^{25}}$. And Hence the dominating term is $\frac{2\mu t}{2^n} < \frac{1}{2^{12}}$ in both Theorem 1 and Theorem 2. Hence we conclude that mF is well secured within the complexity bounds specification of NIST.

3. Finally in **Section 6** we compare the design difference between mF and $\mathsf{mixFeed}$ and as a consequence give the security proof of $\mathsf{mixFeed}$. We show that the difference in adversarial advantage is much less than that of the overall dominating term and hence following the security argument of mF we conclude that $\mathsf{mixFeed}$ is well secured within the complexity bounds specified by NIST.

2 The mF Mode of AEAD

Let $\tilde{E}$ be an n-bit tweakable block cipher[2] with tweak space $\{0,1\}^{n-8} \times [L]$ where L is a reasonably large positive integer. We define an encoding method to encode a triple (N, A, M) of bit strings where $N \in \{0,1\}^{n-8}$. Let us assume that both A and M are not empty. Let $\bar{N} = \begin{cases} 0^7 1 \| N \text{ if } |A| = 0 \\ 0^8 \| N \text{ otherwise.} \end{cases}$. We encode associate data by a prefix-free function $\mathsf{Fmt}_1(A, |M| =_? 0) = \bar{A} = (A_1, \ldots, A_a) \in (\{0,1\}^n)^a$ (for some positive integer a) and message by possibly another prefix-free function $\mathsf{Fmt}_2(M) = \bar{M} = (M_1, \ldots, M_m) \in (\{0,1\}^n)^m$ (for some nonnegative m). For empty message M, we encode to empty bit string (i.e. m is zero). We now define the mF mode encryption scheme as shown in figure :

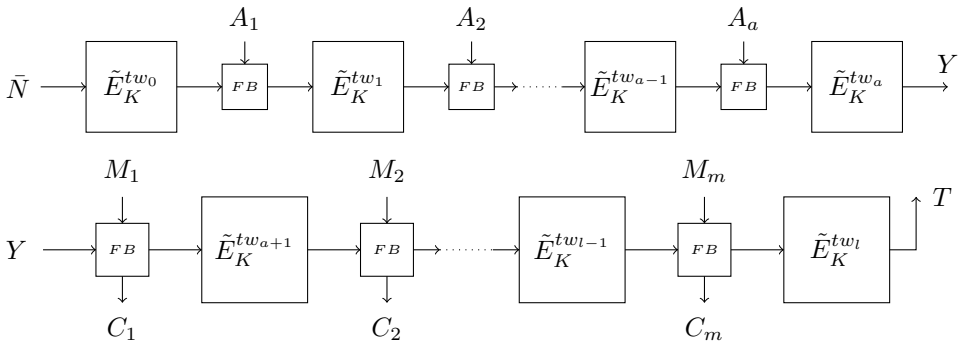
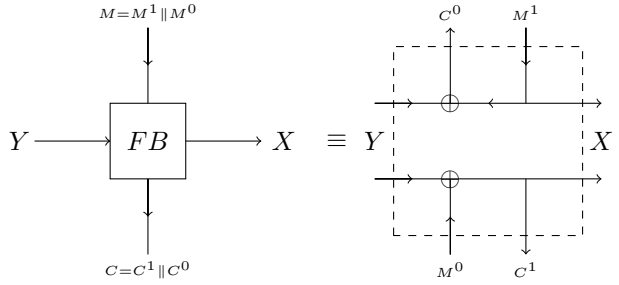


Fig. 1: mF mode of AEAD with tweakable block cipher $\tilde{E}$. Here the i-th block tweak $tw_i := (N, i)$. The Feedback function FB is presented in the diagram below.



3 Security Definitions

Here we define the Different security notions of mF and the tweakable block cipher $\tilde{E}$.

3.1 Security Definitions of mF

Let $\mathcal{E}nc_K, \mathcal{D}ec_K$ respectively denote the encryption and decryption algorithms of mF with key K.

Privacy Given an adversary $\mathscr{A}$ we define the privacy advantage of $\mathscr{A}$ against mF as $\mathbf{Adv}^{priv}_{\mathsf{mF}}(\mathscr{A}) = |\Pr\left[\mathscr{A}^{\mathcal{E}nc_K} = 1\right] - \Pr\left[\mathscr{A}^{\$} = 1\right]|$, where \$ returns a random output string of same length as $\mathcal{E}nc_K$. The *privacy advantage* of mF is defined as

$$\mathbf{Adv}^{priv}_{\mathsf{mF}}(q, \sigma, t) = \max_{\mathscr{A}} \mathbf{Adv}^{priv}_{\mathsf{mF}}(\mathscr{A})$$

where the maximum is taken over all the nonce respecting adversaries $\mathscr{A}$ running in time t and making at most q many encryption queries with total number of blocks in all the queries being σ.

Forgery We say that a nonce respecting oracle adversary $\mathscr{A}^{\mathcal{E}nc_K,\mathcal{D}ec_K}$ forges mF if $\mathscr{A}$ is able to make a fresh query (N,A,C,T) to $\mathcal{D}_K$ such that $\mathcal{D}_K(N,A,C,T) \neq \perp$. By fresh query we mean that the adversary does not make any previous query (N,A,M) to $\mathcal{E}nc_K$ such that $\mathcal{E}nc_K(N,A,M) = (C,T)$. We say a decryption query valid if $\mathcal{D}_K(N,A,C,T) \neq \perp$. The *forging advantage* of an adversary $\mathscr{A}$ is written as

$$\mathbf{Adv}^{forge}_{\mathsf{mF}}(\mathscr{A}) = \Pr\left[\mathscr{A}^{\mathcal{E}nc_K,\mathcal{D}ec_K} \text{ forges}\right]$$

and we write

$$\mathbf{Adv}^{forge}_{\mathsf{mF}}(q,\sigma,t) = \max_{\mathscr{A}} \mathbf{Adv}^{forge}_{\mathsf{mF}}(\mathscr{A})$$

where the maximum is taken over all adversary $\mathscr{A}$ running in time t, making at most q_e many nonce respecting encryption queries with maximum σ_e many blocks and making at most q_d many decryption queries with maximum σ_d many blocks. Define $q = q_e + q_d$, $\sigma = \sigma_e + \sigma_d$. Note that the decryption queries are not necessarily nonce respecting i.e. nonce can be repeated in the decryption queries and an encryption query and a decryption query can use the same nonce. However, all nonces used in encryption queries are distinct.

3.2 Security Definitions of Tweakable block cipher

TPRP-security Let $\tilde{E}$ be an n-bit tweakable block cipher with tweak space $\mathcal{T}$. The *TPRP-advantage* of $\tilde{E}$ against an oracle adversary $\mathscr{A}$ is defined as $\mathbf{Adv}^{TPRP}_{\tilde{E}}(\mathscr{A}) = |\Pr\left[\mathscr{A}^{\tilde{E}_K} = 1\right] - \Pr\left[\mathscr{A}^{\tilde{\Pi}} = 1\right]|$ where $\tilde{\Pi}$ is chosen uniformly from the set of all functions $\tilde{\pi} : \mathcal{T} \times \{0,1\}^n \to \{0,1\}^n$ where for every $tw \in \mathcal{T}$, $\tilde{\pi}(tw,\cdot)$ is a permutation on $\{0,1\}^n$. We call $\tilde{\Pi}$ a tweakable random permutation. We write,

$$\mathbf{Adv}^{TPRP}_{\tilde{E}}(q,t) = \max_{\mathscr{A}} \mathbf{Adv}^{TPRP}_{\tilde{E}}(\mathscr{A})$$

where maximum is taken over all adversaries $\mathscr{A}$ running in time t making q many tweak-input queries of the form (tw,X). We define μ-$TPRP$ advantage of $\tilde{E}$ to be

$$\mathbf{Adv}^{\mu\text{-}TPRP}_{\tilde{E}}(q,t) = \max_{\mathscr{A}} \mathbf{Adv}^{TPRP}_{\tilde{E}}(\mathscr{A})$$

where the maximum is taken over all the adversaries $\mathscr{A}$ as defined above with the additional restriction that it is μ-respecting i.e. the number of queries by $\mathscr{A}$ with same input X is at most μ. When the tweakable block cipher is instantiated in the ideal cipher model, the time parameter t denotes the number of ideal cipher calls.

Multi-Commitment Prediction Let $\tilde{E}$ be a tweakable block cipher. Let $\mathscr{A}$ be an adversary with oracle access to $\tilde{E}$, i.e. it can make queries of the form (tw,X) to $\tilde{E}$ to receive $\tilde{E}_K(tw,X)$. Given Such an adversary $\mathscr{A}$ consider the following game between $\mathscr{A}$ and $\tilde{E}$

PHASE 1 : $\mathscr{A}$ makes queries of the form (tw,X) and receives $Y = \tilde{E}_K(tw,X)$.

PHASE 2 : After all the queries of PHASE 1 is done,

(a) For some $k \leq \lambda$, adversary makes k many commitments of the form (tw_i, x_i, y_i) where $x_i, y_i \in \{0,1\}^{\frac{n}{2}}$.

(b) $\mathscr{A}$ makes at most λ many queries to produce at most λ many prediction tuples of the form $(tw_j, X_j)_{j\in[1,\lambda]}$ such that (tw_j, X_j) are fresh i.e. $\forall j, (tw_j, X_j)$ has never been queried before predicting it.

We say that any adversary $\mathscr{A}$ wins the λ-*multi-commitment-prediction* game if for some prediction tuple (tw^j, X^j) there exist a commitment tuple (tw_i, x_i, y_i) such that

$$tw_i = tw_j; x_i = \lceil X_j \rceil_{\frac{n}{2}}; \lfloor \tilde{E}_K(tw_j, X_j) \rfloor_{\frac{n}{2}} = y_i.$$

The λ-*multi-commitment-predicting* advantage of an adversary $\mathscr{A}$ is defined as

$$\mathbf{Adv}^{\lambda\text{-mcp}}_{\tilde{E}}(\mathscr{A}) = \Pr\left[\mathscr{A}^{\tilde{E}} \text{wins the } \lambda\text{-}\textit{multi-commitment-prediction} \text{ game}\right]$$

and we write,

$$\mathbf{Adv}^{\lambda\text{-mcp}}_{\tilde{E}}(q,t) = \max_{\mathscr{A}} \mathbf{Adv}^{\lambda\text{-mcp}}_{\tilde{E}}(\mathscr{A})$$

where maximum is taken over all adversaries $\mathscr{A}$ running in time t making at most q many queries.

We define (μ, λ)-mcp advantage of $\mathscr{A}$ to be

$$\mathbf{Adv}^{(\mu,\lambda)\text{-mcp}}_{\tilde{E}}(q,t) = \max_{\mathscr{A}} \mathbf{Adv}^{\lambda\text{-mcp}}_{\tilde{E}}(\mathscr{A})$$

where the maximum is taken over all adversaries as defined above with the additional restriction that they make μ-respecting queries in PHASE 1 of the game.

In the ideal cipher model the (λ, μ)-multi commitment prediction security is defined in the same way as above with an additional restriction that the adversary doesn't make any primitive calls to E in PHASE 2.

Multi-Collision Let $\tilde{E}$ be a tweakable block cipher. Define an oracle $\mathcal{O}_{\tilde{E}}$ which takes a query input of the form (tw, X, C) and returns $X' = C \oplus 0^{\frac{n}{2}} \| \lfloor Y \rfloor_{\frac{n}{2}}$ where $Y = \tilde{E}_K(tw, X)$.We say that an adversary $\mathscr{A}$ with oracle access to $\mathcal{O}$ produces a μ-multicollision if it can produce μ many trascripts of the form $(tw_i, X_i, C_i, X'_i)_{i\in[1,\mu]}$ such that $X'_i = X'_j$ for all $i, j \in [1, \mu]$. The μ-*multicollision*-advantage of the adversary $\mathscr{A}$ is defined as

$$\mathbf{Adv}^{\mu\text{-mcoll}}_{\tilde{E}}(\mathscr{A}) = \Pr\left[\mathscr{A}^{\mathcal{O}_{\tilde{E}}} \text{ produces } \mu\text{-multicollision}\right]$$

and we write

$$\mathbf{Adv}^{\mu\text{-mcoll}}_{\tilde{E}}(q) = \max_{\mathscr{A}} \mathbf{Adv}^{\mu\text{-mcoll}}_{\tilde{E}}(\mathscr{A})$$

where maximum is taken over all adversaries $\mathscr{A}$ making at most q many queries.

4 Security Proof of mF

Here we give upper bounds on the *privacy advantage* and *forging advantage* of mF against any adversary $\mathscr{B}$.

4.1 Privacy

Let $\mathscr{B}$ be any adversary which successfully breaks the privacy security of mF. We construct a μ-respecting adversary $\mathscr{A}$ which uses $\mathscr{B}$ to break the μ-$TPRP$ security of $\tilde{E}$.

Let $\mathcal{CH}$ be a μ-$TPRP$ challenger. $\mathscr{A}$ acts as a privacy challenger for $\mathscr{B}$ as follows:

1. $\mathcal{CH}$ randomly chooses a bit $b \in \{0,1\}$. if $b = 1$, $\mathcal{CH}$ computes using $\tilde{E}$. Otherwise $\mathcal{CH}$ chooses a random function $P : T \times \{0,1\}^n \to \{0,1\}^n$ such that for all $tw_i \in T$, $P(tw_i, \star)$ are independent random permutations from $\{0,1\}^n \to \{0,1\}^n$ and computes using P.

2. on receiving encryption queries from $\mathscr{B}$, of the form (N, A, M),

   (a) $\mathscr{A}$ computes $\mathsf{Fmt}(N, A, M) = (\bar{N}, (A_1, \ldots, A_a), (M_1, \ldots, M_m))$.

   (b) For all $0 \leq j \leq l$, $\mathscr{A}$ defines $tw_j = (N, j)$.

   (c) If number of previous queries to $\mathcal{CH}$ of the form $(\star, \bar{N})$ is less than μ then $\mathscr{A}$ queries $(tw_0, \bar{N})$ to $\mathcal{CH}$ to receive Y_0.Else it aborts.

   (d) For all $1 \leq j \leq a$,
      i. $\mathscr{A}$ computes $X_j = \lceil A_j \oplus Y_{j-1} \rceil_{\frac{n}{2}} \| \lfloor A_j \rfloor_{\frac{n}{2}}$.

      ii. If number of previous queries to $\mathcal{CH}$ of the form $(\star, X_j)$ is less than μ then it queries (tw_j, X_j) to $\mathcal{CH}$ to receive Y_j. Else it aborts.

   (e) For $1 \leq j \leq m$,
      i. $\mathscr{A}$ computes $C_j = M_j \oplus Y_{a+j-1}$ and $X_{a+j} = \lceil C_j \rceil_{\frac{n}{2}} \| \lfloor C_j \oplus Y_{a+j-1} \rfloor_{\frac{n}{2}}$.

      ii. If number of previous queries to $\mathcal{CH}$ of the form $(\star, X_{a+j})$ is less than μ then it queries (tw_{a+j}, X_{a+j}) to $\mathcal{CH}$ to receive Y_{a+j}. Else it aborts.

   (f) Finally if $\mathscr{A}$ doesn't abort in any of the previous steps, then it defines $C := C_m \| \cdots \| C_1$ and $T := Y_{a+m}$ and sends (C, T) to $\mathscr{B}$.

3. If $\mathscr{B}$ produces the distinguishing bit b' then $\mathscr{A}$ also produces the same distinguishing bit b'.

Theorem 3. *For any privacy breaking adversary $\mathscr{B}$ of mF any μ-$TPRP$ adversary $\mathscr{A}$ of $\tilde{E}$ and any $\mu+1$-multicollision adversary $\mathscr{C}$ of $\tilde{E}$, we have*

$$\mathbf{Adv}^{priv}_{\mathsf{mF}}(\mathscr{B}) \leq \mathbf{Adv}^{\mu\text{-}TPRP}_{\tilde{E}}(\mathscr{A}) + \mathbf{Adv}^{\mu+1\text{-mcoll}}_{P}(\mathscr{C}).$$

Proof. See Appendix.

4.2 Forgery

Let $\mathscr{B}$ be any forging adversary of mF. Suppose $\mathscr{B}$ makes q_d many forging attempts with σ_d many encryption blocks. We construct a $(\mu-1,\sigma_d)$-mcp adversary $\mathscr{A}$ which uses $\mathscr{B}$ to win the $(\mu-1,\sigma_d)$-multi-commitment-prediction game of $\tilde{E}$.

Let $\mathcal{CH}$ be a $(\mu-1,\lambda)$-mcp challenger. $\mathscr{A}$ acts as a forgery challenger for $\mathscr{B}$ as follows:

Phase 1:

1. Whenever $\mathscr{B}$ sends an encryption query of the form $(N^i, A^i, M^i)_{i\in\mathcal{E}}$,
   (a) $\mathscr{A}$ responds to the query by computing (C^i, T^i) by making the required $\tilde{E}_K$ queries to $\mathcal{CH}$.
   (b) In the previous step, $\mathscr{A}$ always follows the restriction that no more than $\mu-1$ queries to $\tilde{E}$ have the same input. Else it aborts.
2. For each $j \in [1, q_d]$, on receiving decryption queries of the form $(N^{*j}, A^{*j}, C^{*j}, T^{*j})$ from $\mathscr{B}$, $\mathscr{A}$ responds it with $\perp$, and does the following:
   (a) $\mathscr{A}$ checks if $\mathscr{B}$ has previously made any encryption query (N^i, A^i, M^i) and received output of the form (C^i, T^i) such that $T^i = T^{*j}$ and does the following:
      i. if there doesn't exist any encryption query (N^i, A^i, M^i) from $\mathscr{B}$ such that $T^i = T^{*j}$, then $\mathscr{A}$ sets $p_j = 0$.
      ii. Else if $\exists (N^i, A^i, M^i)$ such that $T^i = T^{*j}$ but $N^i \neq N^{*j}$ or $a_i + m_i \neq a^*_j + m^*_j$ or $\lceil C^i_{m_i} \rceil_{\frac{n}{2}} \neq \lceil C^{*j}_{m^*_j} \rceil_{\frac{n}{2}}$, then $\mathscr{A}$ sets $p_j = 0$.
      iii. Else if $p'_j \in \mathbb{N}$ be such that $C^{*j}_{m^*_j - k} = C^i_{m_i - k}, \forall k \in [0, p'_j)$ and $C^{*j}_{m^*_j - p'_j} \neq C^i_{m_i - p'_j}$ but $\lceil C^{*j}_{m^*_j - p'_j} \rceil_{\frac{n}{2}} = \lceil C^i_{m_i - p'_j} \rceil_{\frac{n}{2}}$ then define $p_j = p'_j + 1$.
      iv. Else let $p'_j \in \mathbb{N}$ be such that $C^{*j}_{m^*_j - k} = C^i_{m_i - k}, \forall k \in [0, p_j)$ and $\lceil C^{*j}_{m^*_j - p'_j} \rceil_{\frac{n}{2}} \neq \lceil C^i_{m_i - p'_j} \rceil_{\frac{n}{2}}$ then define $p_j = p'_j$.

(b) $\mathscr{A}$ computes Y_k^{*j} for all $k \in [0, a_j^* + m_j^* - p_j - 1]$ with the help of $\mathcal{CH}$ following the restriction that no more than $\mu - 1$ queries to $\tilde{E}$ have the same input. In that case $\mathscr{A}$ aborts.

(c) Note that, if there exist a common prefix between (N^i, A^i, C^i) and (N^{*j}, A^{*j}, C^{*j}) then $\mathscr{A}$ already have computed upto the common prefix length during encryption query and thus need not send any new encryption query to $\mathcal{CH}$ for computation up to that point.

Phase 2:

1. For each $j \in [1, q_d]$,and for each $k \in [1, p_j]$ $\mathscr{A}$ defines $\Delta_k^j = \lfloor C^{*j}_{m_j^*-k} \rfloor_{\frac{n}{2}} \oplus \lfloor C^i_{m_i-k} \rfloor_{\frac{n}{2}}$.

2. For each $j \in [1, q_d]$,and for each $k \in [0, p_j]$ $\mathscr{A}$ makes commitments of the form $(tw_k^{*j}, x_k^{*j}, y_k^{*j})$ where,

$$tw_k^{*j} = (N^{*j}, a_j^* + m_j^* - k); x_k^{*j} = \lceil C^{*j}_{m_j^*-k} \rceil_{\frac{n}{2}}$$

$$y_k^{*j} = \begin{cases} \lfloor T^{*j} \rfloor_{\frac{n}{2}} \text{ if } k = 0 \\ \lfloor C^i_{m_i-k+1} \oplus M^i_{m_i-k+1} \rfloor_{\frac{n}{2}} \oplus \Delta_k^j \text{ if } k \neq 0 \text{ and } N^i = N^{*j}. \end{cases}$$

3. For each $j \in [1, q_d]$, $\mathscr{A}$ proceeds as follows:
   (a) Note that, $\mathscr{A}$ knows $Y^{*j}_{a_j^*+m_j^*-p_j-1}$ from Phase 1.

   (b) for $k = p_j$ to 0,
      i. $\mathscr{A}$ knows the value of $Y^{*j}_{a_j^*+m_j^*-k-1}$.

      ii. $\mathscr{A}$ then sets $X^{*j}_{a_j^*+m_j^*-k} = (0^{\frac{n}{2}} \| \lfloor Y^{*j}_{a_j^*+m_j^*-k-1} \rfloor_{\frac{n}{2}}) \oplus C^{*j}_{m_j^*-k}$.

      iii. It sets $(tw_k^{*j}, X^{*j}_{a_j^*+m_j^*-k}, y_k^{*j})$ as a prediction tuple, where tw_k^{*j}, y_k^{*j} are as defined above.

      iv. finally it queries $(tw_k^{*j}, X^{*j}_{a_j^*+m_j^*-k})$ to $\mathcal{CH}$ and receives $Y^{*j}_{a_j^*+m_j^*-k}$.

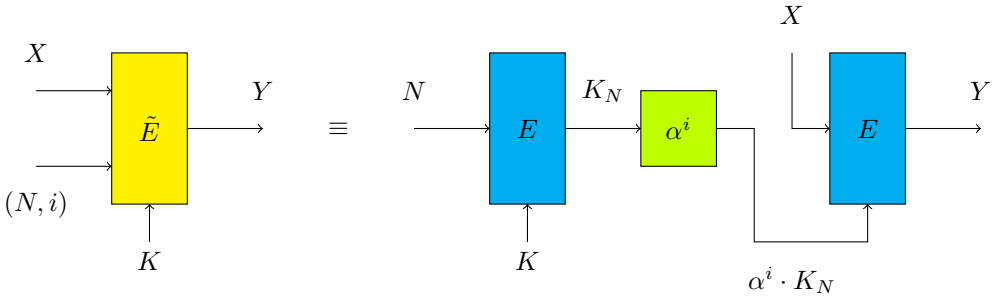
Theorem 4. *For any forging adversary $\mathscr{B}$ of mF making q_e many encryption queries with σ_e many encryption query blocks, q_d many decryption queries with σ_d many decryption query blocks , any $(\mu - 1, \sigma_d)$-mcp adversary $\mathscr{A}$ of $\tilde{E}$, and any $\mu + 1$-multicollision adversary $\mathscr{C}$ of $\tilde{E}$, we have*

$$\mathbf{Adv}^{forge}_{\mathsf{mF}}(\mathscr{B}) \leq \mathbf{Adv}^{(\mu-1,\sigma_d)\text{-}mcp}_{\tilde{E}}(\mathscr{A}) + \mathbf{Adv}^{(\mu+1)\text{-}\mathsf{mcoll}}_{\tilde{E}}(\mathscr{C}).$$

Proof. See Appendix.

5 Bounding security of $\tilde{E}$

Here we bound the advantages of an adversary playing in different security games as defined in **Section 3.2**. The tweakable block cipher $\tilde{E}$ can be best understood from the following diagram.



5.1 Bounding μ-TPRP Security

For a detailed discussion see Appendix. The main result is,

Theorem 5.

$$\mathbf{Adv}^{\mu\text{-}TPRP}_{\tilde{E}}(d,t,\mu) \leq \frac{t+d}{2^n} + \frac{d^2}{2^{n+1}} + \frac{2\mu t}{2^n} + \frac{\binom{d}{\mu+1}}{(2^n)^\mu}.$$

5.2 Bounding (μ,λ)-*mcp* Security

For a detailed discussion see Appendix. The main result is,

Theorem 6.

$$\mathbf{Adv}^{(\mu,\lambda)\text{-}\mathsf{mcp}}_{\tilde{E}}(d,t) \leq \frac{\lambda}{2^{\frac{n}{2}}} + \frac{t+d}{2^n} + \frac{d^2}{2^{n+1}} + \frac{2\mu t}{2^n} + \frac{\binom{d}{\mu+1}}{(2^n)^\mu} + \frac{\lambda d}{2^{n+1}} + \frac{\lambda t}{2^{\frac{3n}{2}}}.$$

5.3 Bounding μ-multi collision

For a detailed discussion see Appendix. The main results are

Theorem 7.

$$\mathbf{Adv}^{\mu\text{-}\mathsf{mcoll}}_{\tilde{E}}(d) \leq d\left(1+\frac{\mu^2}{2^n}\right)\left(\frac{d}{2^{\frac{n}{2}}}\right)^{\mu-1} + \frac{d^2}{2^{n+1}}$$

.

Theorem 8.

$$\mathbf{Adv}_P^{\mu\text{-mcoll}}(d) \leq d\left(1 + \frac{\mu^2}{2^n}\right)\left(\frac{d}{2^{\frac{n}{2}}}\right)^{\mu-1}$$

.

Theorem 1 can be derived from Theorem 3, Theorem 5 and Theorem 8.

Theorem 2 can be derived from Theorem 4 , Theorem 6 and Theorem 7.

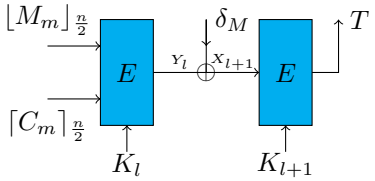
6 Security Proof of mixFeed

6.1 Comparision of mixFeed and mF

In this section we compare the mixFeed construction with our more general mF construction. There are two major differences.

First notice that for mF the properties of $\mathsf{Fmt}_1, \mathsf{Fmt}_2$ are required to prevent length extension or length reduction type attacks. In case of mixFeed this kind of attacks are prevented by using an extra call to the block cipher. Hence we can consider mixFeed to be a variation of mF with no Fmt_1 and Fmt_2 property and two extra block cipher calls.

Now the last associated data/message block processing of mixfeed can be best understood from the diagram bellow. since both are essentially same with different δ values as described in [1] we only draw the diagram for last message block.



Observe that since no value is leaked during this last block processing hence there is no adversarial advantage of the adversary in the sense of privacy.

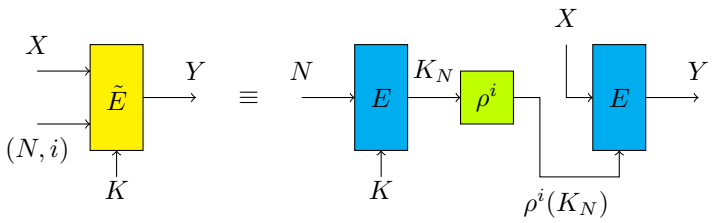
In case of forgery, the only difference comes from the absence of the properties of the Fmt_1 and Fmt_2 functions.

Consider the following events due to the difference in the last block processing.

BAD1 : For i-th encryption query and j-th decryption query we have $(x^{*j}_{l^*_j+1}, K^{*j}_{l^*_j+1}) \neq (x^i_{l_i+1}, K^i_{l_i+1})$ but $T^i = T^{*j}$.

BAD2 : For i-th encryption query and j-th decryption query we have $(x^{*j}_{l^*_j+1}, K^{*j}_{l^*_j+1}) = (x^i_{l_i+1}, K^i_{l_i+1})$.

The second difference between mF and mixFeed comes through the tweakable block cipher representations. The tweakable block cipher representation corresponding to mixFeed can be best understood from the diagram bellow.



The tweable block cipher in mixFeed. Here ρ is the 11-th round key function in AES[3] key scheduling algorithm. ρ^i denotes i-many consecutive applications of ρ.

The difference of security in mixFeed and mF comes from the periodicity of α multiplication and the ρ function. In mF, since α is a primitive element of degree n, the periodicity of multiplication by α is $2^n - 1$ which is very large and hence doesn't create any problem. In case of mixFeed the periodicity of ρ depends on the input and is not a constant value i.e. it may vary for different keys.
Note that, this difference in periodicity only effects the probability of occurrence of the event
BAD3 : For some $i_1 \neq i_2 \in \mathcal{E}$ we have $(N^{i_1}, j^{i_1}) \neq (N^{i_2}, j^{i_2})$ but $K^{i_1} = K^{i_2}$.
Rest of the analysis for mF can be applied for mixFeed as it is.

To bound BAD3 in case of mixFeed we make the following assumption on ρ.

Assumption 1 *For any $K \in \{0,1\}^n$ chosen uniformly at random, probability that K has a period at most l is at most $\frac{l}{2^{\frac{n}{2}}}$.*

Note that our assumption is weak in the sense that for an ideal permutation the above probability is at most $\frac{l}{2^n}$. Recently Mustafa Khairallah has observed that there are at least $2^{33.77}$ keys with a period of $2^{30.08}$ in the AES Key scheduling algorithm. Note that the probability that one of these keys are used is $\frac{2^{33.77}}{2^{128}} = 2^{-94.23}$. Whereas by our assumption the probability is at most $\frac{2^{30.08}}{2^{64}} = 2^{-33.92}$. So, we conclude that his observation does not violate our assumption.

Define $\text{BAD} = \cup_{i=1}^{3} \text{BAD}i$. Then given the above assumption we have,

Lemma 1.

$$\Pr[\text{BAD}] \leq \frac{3\sigma^2}{2^{n+1}} + \frac{\sigma}{2^{\frac{n}{2}}}.$$

Proof. For a detailed proof see Appendix F

Plugging in Lemma 1 properly in Theorems 5,6,7 we have from Theorem 3, Theorem 5 and Theorem 8

Theorem 9.

$$\mathbf{Adv}^{priv}_{\mathit{mixFeed}}(q,\sigma,t) \leq \frac{t+\sigma}{2^n} + \frac{\sigma^2}{2^{n+1}} + \frac{\sigma}{2^{\frac{n}{2}}} + \frac{2\mu t}{2^n} + \frac{\binom{\sigma}{\mu+1}}{(2^n)^\mu} + \sigma\left(1+\frac{\mu^2}{2^n}\right)\left(\frac{\sigma}{2^{\frac{n}{2}}}\right)^{\mu-1}.$$

And From Theorem 4, Theorem 6 and Theorem 7

Theorem 10.

$$\mathbf{Adv}^{forge}_{\mathit{mixFeed}}(q,\sigma,t) \leq \frac{3\sigma}{2^{\frac{n}{2}}} + \frac{t+\sigma}{2^n} + \frac{5\sigma^2}{2^{n+1}} + \frac{2\mu t}{2^n} + \frac{\binom{\sigma}{\mu+1}}{(2^n)^\mu} + \sigma\left(1+\frac{\mu^2}{2^n}\right)\left(\frac{\sigma}{2^{\frac{n}{2}}}\right)^{\mu-1}.$$

Now comparing Theorem 1 and 9 we have,

$$\mathbf{Adv}^{priv}_{\mathsf{mixFeed}}(q,\sigma,t) \leq \mathbf{Adv}^{priv}_{\mathsf{mF}}(q,\sigma,t) + \frac{\sigma}{2^{\frac{n}{2}}} + \frac{2\sigma^2}{2^{n+1}}.$$

Now as discussed in the introduction, with NIST specified complexity bounds the dominating term in the advantage of mF is bounded by $\frac{1}{2^{12}}$ and $\frac{\sigma}{2^{\frac{n}{2}}} \leq \frac{1}{2^{18}}$. Hence if $\mathbf{Adv}^{priv}_{\mathsf{mF}}(q,\sigma,t)$ is of order $\frac{1}{2^{12}}$ then so is $\mathbf{Adv}^{priv}_{\mathsf{mixFeed}}(q,\sigma,t)$.

From Theorem 2 and 10 similar argument follows for the forgery security of mixFeed and mF.

Acknowledgement

We thank Mustafa Khairallah, for doing analysis on mixFeed and informing us about his observations on the periodicity of AES key scheduling algorithm.

References

1. Bishwajit Chakraborty and Mridul Nandi. mixfeed. NIST LwC Competition Round 1 Candidate, 2019. `https://csrc.nist.gov/CSRC/media/Projects/Lightweight-Cryptography/documents/round-1/spec-doc/mixFeed-spec.pdf`.
2. Moses Liskov, Ronald L Rivest, and David Wagner. Tweakable block ciphers. In *Annual International Cryptology Conference*, pages 31–46. Springer, 2002.
3. NIST-FIPS Standard. Announcing the advanced encryption standard (aes). *Federal Information Processing Standards Publication*, 197(1-51):3–3, 2001.

A Proof of Theorem 3

Proof. Suppose $\mathcal{CH}$ output the bit $b \in \{0,1\}$. If $b = 1$ then $\mathcal{CH}^b(tw, X) = P(tw, X)$ and if $b = 0$ then $\mathcal{CH}^b(tw, X) = \tilde{E}_K(tw, X)$. We define the event $(\mathcal{CH} \to b) \cap (\mathscr{A}\text{Aborts})$ as $\mathscr{A}^b$ Aborts.

Note that at any stage of the game between $\mathscr{A}$ and $\mathscr{B}$, if while computing the encryption query responses for $\mathscr{B}$, $\mathscr{A}$ needs to make a new query of the form $(tw^{i_{\mu+1}}_{j_{\mu+1}}, X^{i_{\mu+1}}_{j_{\mu+1}})$ and it has already queried μ many queries of the form $(tw^{i_1}_{j_1}, X^{i_1}_{j_1}), \ldots, (tw^{i_\mu}_{j_\mu}, X^{i_\mu}_{j_\mu})$ to $\mathcal{CH}$ such that $X^{i_l}_{j_l} = X^{i_k}_{j_k}$ for all $l, k \in [1, \mu+1]$ then $\mathscr{A}$ aborts.

Let $D^{i_l}_{j_l} = \begin{cases} A^{i_l}_{j_l} \text{ if } j_l \leq a_i \\ C^{i_l}_{j_l - a_i} \text{otherwise.} \end{cases}$

In this case, adversary $\mathscr{C}$ can produce $\mu+1$ many tuples of the form $(tw^{i_l}_{j_l-1}, X^{i_l}_{j_l-1}, D^{i_l}_{j_l}, X^{i_l}_{j_l})$ such that $0^{\frac{n}{2}} \| \lfloor Y^{i_l}_{j_l-1} \rfloor_{\frac{n}{2}} \oplus D^{i_l}_{j_l} = X^{i_l}_{j_l}$ where $\mathcal{CH}^b(tw^{i_l}_{j_l-1}, Xi_{l\,j_l-1}) = Y^{i_l}_{j_l-1}$ for all $l \in [1, \mu+1]$. Thus $\mathscr{C}$ wins the $\mu+1$-multicollision game.

Hence we have

$$\begin{aligned} \Pr\left[\mathscr{A}^b \text{ Aborts}\right] &\leq \Pr\left[\mathscr{C}\text{produces } \mu+1\text{-multicollisions in the } \mathcal{CH}^b \text{ game}\right] \\ &= \mathbf{Adv}^{\mu+1\text{-mcoll}}_{\mathcal{CH}^b}(\mathscr{C}) \end{aligned}$$

Now suppose the adversary $\mathscr{A}$ never aborts i.e never had to violate the $\mu+1$-multicollision restriction.

Notice that $\mathscr{A}$ playing the above game, perfectly simulates as a *privacy challenger* for $\mathscr{B}$. Suppose the $TPRP$- challenger $\mathcal{CH}$ randomly chooses a bit $b = 1$. Then all the $\mathcal{CH}$ queries are responded through P. Suppose $\mathscr{B}$ makes a query of the form (N, A, M). Then it is clear from the game that $\forall 0 \leq j \leq a+m$, tw_j are distinct and hence we have Y_j are independent and uniformly random outputs from $P(tw_j, \star)$. Then since M is known we have $C_j = Y_{a+j-1} \oplus M_j$ are uniformly random and $T = Y_{a+m}$ is uniformly random. Hence the (C, T) response from $\mathscr{A}$ is uniformly random. Hence $\mathscr{A}$ acts as a *privacy* challenger which responds to the encryption queries uniformly randomly and we have,

$$\Pr\left[\mathscr{B}^{\$} = 1 \cap \mathscr{A} \text{ doesn't Abort}\right] \leq \Pr\left[\mathscr{A}^P = 1\right].$$

Similarly if $b = 0$. Then $\mathcal{CH}$ responds to the queries of $\mathscr{A}$ correctly with respect to $\tilde{E}$ and thus the (C, T) response from $\mathscr{A}$ to a (N, A, M) query by $\mathscr{B}$ is correctly computed with respect to $\tilde{E}$. Hence $\mathscr{A}$ acts as a *privacy* challenger which responds to the encryption queries correctly with respect to $\tilde{E}$ an we have

$$\Pr\left[\mathscr{B}^{\mathcal{E}nc} = 1 \cap \mathscr{A} \text{ doesn't Abort}\right] \leq \Pr\left[\mathscr{A}^{\tilde{E}} = 1\right]$$

Now without loss of generality assume $\Pr\left[\mathscr{B}^{\$}=1\right] \geq \Pr\left[\mathscr{B}^{\mathcal{E}nc}=1\right]$ else we consider the adversary $\mathscr{B}^C$ which is compliment of $\mathscr{B}$ in the sense that it follows the same security game as $\mathscr{B}$ with the difference that whenever $\mathscr{B}$ outputs guessing bit b, $\mathscr{B}^C$ outputs guessing bit $\bar{b}$.

Then we have,

$$\begin{aligned}
\Pr\left[\mathscr{B}^{\$}=1\right]-\Pr\left[\mathscr{B}^{\mathcal{E}nc}=1\right] &\leq \Pr\left[\mathscr{B}^{\$}=1\cap \mathscr{A} \text{ doesn't Abort}\right] \\
&\quad +\Pr\left[\mathscr{B}^{\$}=1\cap \mathscr{A}\text{Aborts}\right] \\
&\quad -\Pr\left[\mathscr{B}^{\mathcal{E}nc}=1\cap \mathscr{A} \text{ doesn't Abort}\right] \\
&\quad -\Pr\left[\mathscr{B}^{\mathcal{E}nc}=1\cap \mathscr{A}\text{Aborts}\right] \\
&\leq \Pr\left[\mathscr{A}^{P}=1\right]-\Pr\left[\mathscr{A}^{\tilde{E}}=1\right] \\
&\quad +\Pr\left[\mathscr{A}^{P}=1\cap \mathscr{A}\text{Aborts}\right] \\
&\leq \Pr\left[\mathscr{A}^{P}=1\right]-\Pr\left[\mathscr{A}^{\tilde{E}}=1\right] \\
&\quad +\Pr\left[\mathscr{A}^{1} \text{ Aborts}\right]
\end{aligned}$$

Hence, we have,

$$\begin{aligned}
\left|\Pr\left[\mathscr{B}^{\$}=1\right]-\Pr\left[\mathscr{B}^{\mathcal{E}nc}=1\right]\right| &\leq \left|\Pr\left[\mathscr{A}^{P}=1\right]-\Pr\left[\mathscr{A}^{\tilde{E}}=1\right]\right| \\
&\quad +\mathbf{Adv}_{P}^{\mu+1\text{-mcoll}}(\mathscr{C})
\end{aligned}$$

B Proof of Theorem 4

Claim. Suppose $\mathscr{A}$ never Aborts. If $(N^{*i}, A^{*i}, C^{*i}, T^{*i})$ is a valid forgery,for some $i \in [1, q_d]$ then for some $k \in [0, p_i]$ we have $(tw_k^{*i}, 0^{\frac{n}{2}} \| \lfloor Y^*_{a_i^*+m_i^*-k-1} \rfloor_{\frac{n}{2}} \oplus C^*_{m_i^*-k})$ is a successful prediction query tuple.

Proof. (Claim B) Let$(N^{*j}, A^{*j}, C^{*j}, T^{*j})$ is a valid forgery. If there doesn't exist any encryption query (N^i, A^i, M^i) from $\mathscr{B}$ such that $T^i = T^{*j}$ or $\exists (N^i, A^i, M^i)$ such that $T^i = T^{*j}$ but $N^i \neq N^{*j}$ or $m_j^* \neq m_i$ or $\lceil C^i_{m_i} \rceil_{\frac{n}{2}} \neq \lceil C^{*j}_{m_j^*} \rceil_{\frac{n}{2}}$, then we have $p_j = 0$.

In the commitment phase the adversary $\mathscr{A}$ commits $(tw_0^{*j}, x_0^{*j}, y_0^{*j})$ as defined above.

Now we have if any of the above condition is satisfied then $(tw_0^{*j}, X_{a_j^*+m_j^*}^{*j})$ is fresh i.e. $(tw_0^{*j}, X_{a_j^*+m_j^*}^{*j})$ has never been queried before by $\mathscr{A}$ to $\mathcal{CH}$, and $\tilde{E}_K(tw^{*j}, X_{a_j^*+m_j^*}^{*j}) = T^{*j}$. Hence we see that $(tw_0^{*j}, X_{a_j^*+m_j^*}^{*j}, \lfloor T^{*j} \rfloor_{\frac{n}{2}})$ is a valid prediction with respect to the commitment $(tw_0^{*j}, x_0^{*j}, y_0^{*j})$.

Now let $(N^{*j}, A^{*j}, C^{*j}, T^{*j})$ is a valid forgery. and let $p_j \neq 0$ is as defined before. Hence there exist a $i \in [1, q_e]$ such that $N^{*j} = N^i, a_j^* + m_j^* = a_i + m_i = l_j$(say).

First let $p_j' \in \mathbb{N}$ be such that $C_{m_j^*-k}^{*j} = C_{m_i-k}^i, \forall k \in [0, p_j')$ and $C_{m_j^*-p_j'}^{*j} \neq C_{m_i-p_j'}^i$ but $\lceil C_{m_j^*-p_j'}^{*j} \rceil_{\frac{n}{2}} = \lceil C_{m_i-p_j'}^i \rceil_{\frac{n}{2}}$. In this case $p_j = p_j' + 1$. We have by suffix property $Y_{l_j-p_j}^{*j} = Y_{l_j-p_j}^i \oplus \Delta_{m_j^*-p_j+1}^j$. and $\Delta_{m_j^*-p_j+1}^j \neq 0$. Since $tw_{p_j}^{*j} = tw_{p_j}^i$ we must have $X_{l_j-p_j}^{*j} \neq X_{l_j-p_j}^i$. And hence $(tw_{p_j}^{*j}, X_{l_j-p_j}^{*j}, y_{p_j}^{*j})$ is fresh.

Now let $p_j' \in \mathbb{N}$ be such that $C_{m_j^*-k}^{*j} = C_{m_i-k}^i, \forall k \in [0, p_j)$ and $\lceil C_{m_j^*-p_j'}^{*j} \rceil_{\frac{n}{2}} \neq \lceil C_{m_i-p_j'}^i \rceil_{\frac{n}{2}}$. Then we have $p_j = p_j'$ and by the suffix property we must have $\lfloor Y_{l_j-p_j-1}^{*j} \rfloor_{\frac{n}{2}} = \lfloor Y_{l_j-p_j-1}^i \rfloor_{\frac{n}{2}}$. Since $\lceil C_{m_j^*-p_j}^{*j} \rceil_{\frac{n}{2}} \neq \lceil C_{m_i-p_j}^i \rceil_{\frac{n}{2}}$ we have, $X_{l_j-p_j}^{*j} \neq X_{l_j-p_j}^i$ and hence $(tw_{p_j}^{*j}, X_{l_j-p_j}^{*j}, y_{p_j}^{*j})$ is fresh where $tw^{*j} = (N^{*j}, l_j - p_j)$.

In the commitment phase the adversary commits $(tw_k^{*j}, x_k^{*j}, y_k^{*j})$ for all $k \in [0, p_j]$.

Hence if $(tw_{p_j}^{*j}, X_{l_j-p_j}^{*j}, y_{p_j}^{*j})$ is a valid prediction with respect to $(tw_{p_j}^{*j}, x_{p_j}^{*j}, y_{p_j}^{*j})$ we are done.

If not then we have $\lfloor Y_{l_j-p_j}^{*j} \rfloor_{\frac{n}{2}} \neq \lfloor Y_{l_j-p_j}^i \rfloor_{\frac{n}{2}} \oplus \Delta_{m_j^*-p_j+1}^j$. Hence $X_{l_j-p_j+1}^{*j} \neq X_{l_j-p_j+1}^i$ as $C_{m_j^*-p_j+1}^{*j} \oplus C_{m_i-p_i+1}^i = 0^{\frac{n}{2}} \| \Delta_{m_j^*-p_j+1}^j$.

For $k = p_j - 1 to 1$, we have if $(tw_k^{*j}, X_{l_j-k}^{*j}, y_k^{*j})$ is a valid prediction with respect to the commitment $(tw_k^{*k}, x_k^{*j}, y_k^{*j})$ then we are done. Otherwise, we have $\lfloor Y_{l_j-k}^{*j} \rfloor_{\frac{n}{2}} \neq \lfloor Y_{l_j-k}^i \rfloor_{\frac{n}{2}}$. Hence $X_{l_j-k+1}^{*j} \neq X_{l_j-k+1}^i$ as $C_{m_j^*-k+1}^{*j} = C_{m_i-k+1}^i$ and $tw_{k-1}^{*j} = (N^{*j}, l_j - k + 1)$. Hence $(tw_{k-1}^{*j}, X_{l_j-k+1}^{*j})$ is fresh.

Finally if $k = 0$ and we have $\lfloor Y_{l_j-1}^{*j} \rfloor_{\frac{n}{2}} \neq \lfloor Y_{l_j-1}^i \rfloor_{\frac{n}{2}}$ then $X_{l_j}^{*j} \neq X_{l_j}^i$ as $C_{m_j^*}^{*j} = C_{m_i}^i$ and $tw_0^{*j} = (N^{*j}, l_j)$. Hence $(tw_0^{*j}, X_{l_j}^{*j})$ is fresh. Now since $(N^{*j}, A^{*j}, C^{*j}, T^{*j})$ is a valid forgery we must have $\tilde{E}_K(tw_0^{*j}, X_{l_j}^{*j}) = T^{*j}$. Hence $(tw_0^{*j}, X_{l_j}^{*j}, \lfloor T^{*j} \rfloor_{\frac{n}{2}})$ is a valid prediction with respect to $(tw_0^{*j}, x_0^{*j}, y_0^{*j})$.

Proof. Theorem 4. For all encryption query of the form (N^i, A^i, M^i), $\mathscr{A}$ can correctly simulate $\mathcal{E}nc_K$ as it has access to $\tilde{E}_K$.

Suppose while computing the encryption query responses for $\mathscr{B}$, $\mathscr{A}$ needs to make a new query of the form $(tw^{i_\mu}_{j_\mu}, X^{i_\mu}_{j_\mu})$ and it has already queried $\mu-1$ many queries of the form $(tw^{i_1}_{j_1}, X^{i_1}_{j_1}), \ldots, (tw^{i_\mu}_{j_\mu}, X^{i_\mu}_{j_\mu})$ to $\mathcal{CH}$ such that $X^{i_l}_{j_l} = X^{i_k}_{j_k}$ for all $l, k \in [1, \mu]$ then $\mathscr{A}$ aborts.

Let $D^i_j = \begin{cases} A^i_j \text{ if } j \leq a_i \\ C^i_{j-a_i} \text{otherwise.} \end{cases}$

Note that in this case, adversary $\mathscr{C}$ can produce μ many tuples of the form $(tw^{i_l}_{j_l-1}, X^{i_l}_{j_l-1}, D^{i_l}_{j_l}, X^{i_l}_{j_l})$ such that $0^{\frac{n}{2}} \| \lfloor Y^{i_l}_{j_l-1} \rfloor_{\frac{n}{2}} \oplus D^{i_l}_{j_l} = X^{i_l}_{j_l}$ where $\tilde{E}_K(tw^{i_l}_{j_l-1}, Xi_{l\,j_l-1}) = Y^{i_l}_{j_l-1}$ for all $l \in [1, \mu]$.
Let p'_j be the maximum length of the common prefix between a the decryption query $(N^{*j}, A^{*j}, C^{*j}, T^{*j})$ and any encryption response (N^i, A^i, C^i, T^i). Since the value of $Y^{*j}_{p'_j}$ is know from the encryption transcript, $\mathcal{C}$ can set $D^{*j}_{p'_j+1}$ in such a way that $X^{*j}_{p_j+1} = X^{i_\mu}_{j_\mu}$. Then $(tw^{i_l}_{j_l-1}, X^{i_l}_{j_l-1}, D^{i_l}_{j_l}, X^{i_l}_{j_l})_{l\in[1,\mu]}$ and $(tw^{*j}_{p'_j}, X^{*j}_{p'_j}, D^{*j}_{p_j+1}, X^{*j}_{p_j+1})$ produces $\mu+1$- multicollision tuple. Thus $\mathscr{C}$ wins the multicollision game.

Hence $\Pr[\mathscr{A} \text{ Aborts}] \leq \Pr[\mathscr{C} \text{ produces } \mu+1\text{-}multicollision]$.

Note that, $p_i < m^*_i$ for all i-th decryption query. Hence $\mathscr{A}$ makes at most $\sum_i p_i \leq \sum_i m_i \leq \sigma_d$ many commitments and makes at most σ_d many queries in Phase 2 to produce at most σ_d many prediction tuples.

Hence by the claim B we have,

$\Pr[\mathscr{A} \text{ wins } (\mu-1, \sigma_d)\text{-mcp game}]$

$$\geq \Pr[\mathscr{B} \text{ Forges } i\text{-th query for some } i \in [1, q_d] | \mathscr{A} \text{ doesn't Abort}]$$

$$\begin{aligned}\Pr[\mathscr{B} \text{ Forges}] &\leq \Pr[\mathscr{B} \text{ Forges } i\text{-th query for some } i \in [1, q_d] | \mathscr{A} \text{ doesn't Abort}] \\ &\quad + \Pr[\mathscr{A} \text{ Aborts}] \\ &\leq \Pr[\mathscr{A} \text{ wins } (\mu, \sigma_d)\text{-mcp game}] + \mathbf{Adv}^{\mu+1\text{-mcoll}}_{\tilde{E}}(\mathscr{C}) \\ &= \mathbf{Adv}^{(\mu-1,\sigma_d)\text{-}mcp}_{\tilde{E}}(\mathscr{A}) + + \mathbf{Adv}^{\mu+1\text{-mcoll}}_{\tilde{E}}(\mathscr{C}).\end{aligned}$$

C Bounding μ-TPRP Security

Here we try to bound the μ-$TPRP$-security of the tweakable block cipher $\tilde{E}$. Let $\mathscr{A}$ be any μ-respecting adversary playing the μ-$TPRP$ game and makes at most t many primitive queries and d many online queries.
We assume that the adversary doesn't make repetitive or redundant queries.

C.1 The Ideal world and Analysis of Bad events

Let $\mathcal{P}$ and $\mathcal{E}$ denote the index set of primitive queries and encryption queries respectively.

In ideal world the oracle chooses random functions $P : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ and $Q : T \times \{0,1\}^n \to \{0,1\}^n$ such that for all $K \in \{0,1\}^n$ we have $P(K,\star)$ is a random permutation and for all $tw \in T$ we have $Q(tw,\star)$ is a random permutation.

Primitive Query: In the Ideal world for the i-th primitive query of the form (K^i, X^i) it computes $Y^i = P(K^i, X^i)$ and sends it as a response.

Define $\omega_t = (K^i, X^i, Y^i)_{i\in\mathcal{P}}$ to be the primitive transcript.

Online Query: On receiving the i-th input query of the form $((N^i, j^i), X^i)$ it computes $Y^i = Q((N^i, j^i), X^i)$ and sends it as the response.

Offline Computation : Oracle Chooses $K \in \{0,1\}^n$ uniformly at random. It then chooses a permutation $\Pi : \{0,1\}^n \to \{0,1\}^n$ uniformly at random from the set of all permutations over $\{0,1\}^n$. It then defines $K_{N^i} := \Pi(N^i)$ and $K^i = \alpha^{j^i} \cdot K_{N^i}$.

Define $\omega_d = (K, ((N^i, j^i), X^i, Y^i, K^i)_{i\in\mathcal{E}},)$ to be the online transcript.
Define $\omega = (\omega_t, \omega_d)$ be the transcript for the adversary in the ideal world.
Bad Events Consider the following events due to ω,

BAD1: For some $i \in \mathcal{E} \cup \mathcal{P}$ we have $K^i = K$.

BAD2: For some $i_1 \neq i_2 \in \mathcal{E}$ we have $(N^{i_1}, j^{i_1}) \neq (N^{i_2}, j^{i_2})$ but $K^{i_1} = K^{i_2}$.

BAD3: For some $i \in \mathcal{E}$ and $i' \in \mathcal{P}$ we have $(K^i, X^i) = (K^{i'}, X^{i'})$.

BAD4: $\exists i_1, \ldots i_{\mu+1} \in \mathcal{E}$ s.t. $Y^{i_k} = Y^{i_l} \quad \forall k, l \in [1, \mu+1]$.

BAD5: For some $i \in \mathcal{E}$ and $i' \in \mathcal{P}$ we have $(K^i, Y^i) = (K^{i'}, Y^{i'})$.

Definition 1.

$$\text{BAD} = \cup_{i=1}^{5} \text{BAD}i.$$

Lemma 2.

$$\Pr[\text{BAD}] \leq \frac{t+d}{2^n} + \frac{d^2}{2^{n+1}} + \frac{2\mu t}{2^n} + \frac{\binom{d}{\mu+1}}{(2^n)^\mu}.$$

Proof. Here we try to bound the distinct bad events defined above.

Bounding BAD1: Fix $i \in \mathcal{P} \cup \mathcal{E}$, since K is chosen uniformly at random we have probabilty that $K^i = K$ is at most $\frac{1}{2^n}$. similar Varying over all i,

$$\Pr[\text{BAD1}] \leq \frac{d+t}{2^n}$$

.

Bounding BAD2: This event can be divided into the following cases.

Case 1: $(N^{i_1} \neq N^{i_2})$ In this case since Π is a random permutation, $K_{N^{i_1}} \neq K_{N^{i_2}}$ are distinct and independent. Hence probability that $K^{i_1} = K^{i_2}$ is atmost $\frac{1}{2^n}$. Varying over all $i_1, i_2 \in \mathcal{E}$ we have,

$$\Pr[\text{Case 1}] \leq \frac{d^2}{2^{n+1}}.$$

Case 2: $(N^{i_1} = N^{i_2}; j^{i_1} \neq j^{i_2})$ In this case we have $K_{N^{i_1}} = K_{N^{i_2}}$. Now since α is a primitive polynomial hence we have $K^{i_1} \neq K^{i_2}$.

Hence

$$\Pr[\text{BAD2}] \leq \frac{d^2}{2^{n+1}}.$$

Bounding BAD3: For a given $i' \in \mathcal{P}$, let the adversary makes the primitive query $(K^{i'}, X^{i'})$. Then there can be at most μ-many encryption query of the form $((N^{i_k}, j^{i_k}), X^{i'})_{k\in[1,\mu], i_k \in \mathcal{E}}$ and hence at most μ-many $(K^{i_k}, X^{i'})_{k\in[1,\mu], i_k\in\mathcal{E}}$ tuples. now since K^{i_k} are chosen uniformly at random during encryption query we have for a given $i_k \in \mathcal{E}$, probability that $K^{i_k} = K^{i'}$ is at most $\frac{1}{2^n}$. Hence for a given $i' \in \mathcal{P}$ probability that $\exists i \in \mathcal{E}$ s.t. $(K^i, X^i) = (K^{i'}, X^{i'})$ is at most $\frac{\mu}{2^n}$. Varying over all i', we have

$$\Pr[\text{BAD3}] \leq \frac{\mu t}{2^n}.$$

Bounding BAD4: Since for each $i \in \mathcal{E}$, Y^i is chosen uniformly at random. given $i_1, \ldots, i_{\mu+1} \in \mathcal{E}$ probability that $Y^{i_j} = Y^{i_j}$ for all $j \in [1, \mu+1]$ is at most $\frac{1}{(2^n)^\mu}$. Hence varying over all choices of $i_1, \ldots, i_{\mu+1}$ we have

$$\Pr\left[\text{BAD4}\right] \leq \frac{\binom{d}{\mu+1}}{(2^n)^\mu}.$$

BOUNDING BAD5$|\overline{\text{BAD4}}$: For a given $i' \in \mathcal{P}$, let the adversary's primitive transcript be $(K^{i'}, \star, Y^{i'})$. Then there can be at most μ-many encryption transcript of the form $((N^{i_k}, j^{i_k}), \star, Y^{i'})_{k\in[1,\mu], i_k\in\mathcal{E}}$ and hence at most μ-many $(K^{i_k}, Y^{i'})_{k\in[1,\mu], i_k\in\mathcal{E}}$ tuples. now since K^{i_k} are chosen uniformly at random during encryption query we have for a given $i_k \in \mathcal{E}$, probability that $K^{i_k} = K^{i'}$ is at most $\frac{1}{2^n}$. Hence for a given $i' \in \mathcal{P}$ probability that $\exists i \in \mathcal{E}$ s.t. $(K^i, Y^i) = (K^{i'}, Y^{i'})$ is atmost $\frac{\mu}{2^n}$. Varying over all i', we have

$$\Pr\left[\text{BAD5}|\overline{\text{BAD4}}\right] \leq \frac{\mu t}{2^n}.$$

Adding all the probabilities we get the Lemma.

C.2 Real World and Good transcript analysis

The real world has oracle E_K. All the primitive queries and the encryption queries are responded based on the responses of E_K.

By good transcript we mean any transcript which is not bad. Now consider a good transcript $\omega = (\omega_t, \omega_d)$. Let Θ_0 and Θ_1 be the transcript random variable obtained in the ideal world and real world respectively.

Then we have $\Pr\left[\Theta_0 = \omega\right] = \prod_{t_i} \frac{1}{(2^n)_{t_i}} \times \frac{1}{2^n} \times \frac{1}{(2^n)_d} \times \frac{1}{(2^n)_d}$.

Where t_i denotes the number of primitive Queries with the key $K'_i \in \{0,1\}^\kappa$. i.e $\sum_i t_i = t$.

Now note that in the real world the primitive queries and online queries are permutation compatible.

Hence we have $\Pr\left[\Theta_1 = \omega\right] = \prod_{k_i} \frac{1}{(2^n)_{k_i}} \times \frac{1}{2^n} \times \frac{1}{(2^n)_d}$. Where $k_i = d_i + t_i$ such that t_i denotes the number of primitive queries with key K_i and d_i denotes the number of encryption queries of the form (N^l, j^l, X) such that $K^l = K_i$. Note that $\sum_i k_i = d + t$.

Hence

$$\frac{\Pr[\Theta_1]}{\Pr[\Theta_0]} = \frac{\prod_{t_i}(2^n)_{t_i} \times 2^n \times (2^n)_d \times (2^n)_d}{\prod_{k_i}(2^n)_{k_i} \times 2^n \times (2^n)_d}$$
$$= \frac{\prod_{i}(2^n)_{t_i} \times (2^n)_d}{\prod_{i}(2^n)_{t_i+d_i}}$$
$$= \frac{(2^n)_d}{\prod_{i}(2^n - t_i)_{d_i}} > 1.$$

Hence by H-coefficient technique we have, Theorem 5.

D Bounding (μ, λ)-*mcp* Security

Here we try to bound the advantage of a μ-respecting adversary $\mathscr{A}$ making t-many primitive queries and d-many online queries playing the (μ, λ)-multi commitment prediction game with a challenger $\mathcal{CH}$.

We assume that the adversary doesn't make repetitive or redundant queries. Primitive Queries: Whenever $\mathscr{A}$ makes a primitive query of the form (K^i, X^i) for some $i \in \mathcal{P}$ the $\mathcal{CH}$ responds with $Y_i = E_{K^i}(X^i)$.Let $\omega_t = (K^i, X^i, Y^i)_{i\in\mathcal{P}}$ be the primitive transcript of the adversary $\mathscr{A}$.

Online Queries: Whenever $\mathscr{A}$ makes an online query of the form $((N^i, j^i), X^i)$ for some $i \in \mathcal{E}$, $\mathcal{CH}$ checks that the query is μ-respecting. If not, then it aborts. Else, $\mathcal{CH}$ computes $K_{N^i} = E_K(N^i)$, $K^i = \alpha^{j^i} \cdot K_{N^i}$ and finally outputs $Y^i = E_{K^i}(X)$ as response.

Let $\omega_d = ((N^i, j^i), K^i, X^i, Y^i)_{i\in\mathcal{E}}$ be the online transcript of the adversary.

Define $\omega = (\omega_t, \omega_d)$ as the transcript of $\mathscr{A}$.

Bad Events

Consider the following events depending on the transcript ω of the adversary $\mathscr{A}$.

Bad Events due to primitive and encryption query.

BAD1: For some $i \in \mathcal{E} \cup \mathcal{P}$ we have $K^i = K$.

BAD2: For some $i_1 \neq i_2 \in \mathcal{E}$ we have $(N^{i_1}, j^{i_1}) \neq (N^{i_2}, j^{i_2})$ but $K^{i_1} = K^{i_2}$.

BAD3: For some $i \in \mathcal{E}$ and $i' \in \mathcal{P}$ we have $(K^i, X^i) = (K^{i'}, X^{i'})$.

BAD4: $\exists i_1, \ldots i_{\mu+1} \in \mathcal{E}$ s.t. $Y^{i_k} = Y^{i_l} \quad \forall k, l \in [1, \mu+1]$.

BAD5: For some $i \in \mathcal{E}$ and $i' \in \mathcal{P}$ we have $(K^i, Y^i) = (K^{i'}, Y^{i'})$.

Bad event due to multi-commitment prediction game.
BAD 6 : For some $i \in [1, \lambda]$ and $k \in \mathcal{E}$, we have a commitment $((N^i, j^i), x^i, y^i)$ is such that, $(N^i, j^i) \neq (N^k, j^k)$ but $K^i = K^k$ where $K^i = \alpha^{j^i} \cdot E_K(N^i)$.

BAD7: For some $i \in [1, \lambda]$ and $k \in \mathcal{P}$, we have a commitment $((N^i, j^i), x^i, y^i)$ is such that, $(K^i, x^i) = (K^k, \lfloor X^k \rfloor_{\frac{n}{2}})$ where $K^i = \alpha^{j^i} \cdot E_K(N^i)$.

Definition 2.

$$\text{BAD} = \cup_{i=1}^{7} \text{BAD}i.$$

Lemma 3.

$$\Pr[\text{BAD}] \leq \frac{t+d}{2^n} + \frac{d^2}{2^{n+1}} + \frac{2\mu t}{2^n} + \frac{\binom{d}{\mu+1}}{(2^n)^\mu} + \frac{\lambda d}{2^{n+1}} + \frac{\lambda t}{2^{\frac{3n}{2}}}.$$

Proof. Here we try to bound the distinct bad events defined above.

Bounds of events BAD1 to BAD5 has been found while bounding μ-TPRP security of $\tilde{E}$.

Bounding BAD6: This event can be divided into the following cases.

Case 1: $(N^i \neq N^k)$ In this case $K_{N^i} \neq K_{N^k}$ are distinct. Hence probability that $K^i = K^k$ is at most $\frac{1}{2^n}$. Varying over all $i \in \mathcal{E}$ and $j \in [1, \lambda]$ we have,

$$\Pr[\text{Case 1}] \leq \frac{\lambda d}{2^{n+1}}.$$

Case 2: $(N^i = N^k; j^i \neq j^k)$ In this case we have $K_{N^i} = K_{N^j}$. Now since α is a primitive polynomial hence we have $K^i \neq K^k$.

Hence

$$\Pr[\text{BAD6}] \leq \frac{\lambda d}{2^{n+1}}.$$

Bounding BAD7: Fix $i \in [1, \lambda]$ and $k \in \mathcal{P}$. Since K_{N^i} is distributed uniformly at random, and there is no primitive query after commitment, we have probability that $(K^i, x^i) = (K^k, \lfloor X^k \rfloor_{\frac{n}{2}})$ is at most $\frac{1}{2^{\frac{3n}{2}}}$. varying over all i, k we have,

$$\Pr\left[\text{BAD7}\right] \leq \frac{\lambda t}{2^{\frac{3n}{2}}}.$$

Adding all the probabilities we get the Lemma.

Good Transcript Analysis

By good transcript we mean any transcript which is not bad. Now consider a good transcript $\omega = (\omega_t, \omega_d)$.

Then we have $(tw^i, X^i)_{i\in[1,\lambda]}$ is fresh. Hence for a fix i, probability that $\lfloor \tilde{E}(tw^i, X^i)\rfloor_{\frac{n}{2}} = y_i$ is bounded by at most $\frac{1}{2^{\frac{n}{2}}}$. Hence varying over all $i \in [1, \lambda]$ we have,

$$\Pr\left[\mathscr{A}^{\tilde{E}} \text{wins the } (\lambda,\mu)\text{-}mcp \text{ game }\right] \leq \frac{\lambda}{2^{\frac{n}{2}}}.$$

Combining the results we have Theorem 6.

E Bounding μ-multi collision

E.1 Bounding μ-multi collision for $\tilde{E}$

We model E as a random permutation. We assume that the adversary doesn't make repetitive or redundant queries.

$\mathcal{O}$ QUERIES: Whenever $\mathscr{A}$ makes an online query of the form $((N^i, j^i), X^i, C^i)$ for some $i \in \mathcal{E}$, $\mathcal{O}$ computes $K_{N^i} = E_K(N^i)$, $K^i = \alpha^{j^i} \cdot K_{N^i}$ and finally outputs$z^i = \lfloor Y^i \oplus C^i\rfloor_{\frac{n}{2}}$ as response where $Y^i = E_{K^i}(X^i)$.

Let $\omega_d = ((N^i, j^i), K^i, X^i, z^i)_{i\in\mathcal{E}}$ be the online transcript of the adversary.

We have the μ- multi collision occurs if $\exists i_1, \ldots, i_\mu \in [1, d]$ such that $z^{i_k} = z^{i_l}$ for all $k, l \in [1, \mu]$.

Consider the following event

BAD: For some $i_k \neq i_l \in [1, d]$ we have $tw^{i_k} \neq tw^{i_l}$ but $K^{i_k} = K^{i_l}$. As shown earlier, probability of this can be bounded by $\frac{d^2}{2^{n+1}}$.

Now suppose $\forall k, l \in [1, d]$ we have BAD doesn't occur. Then Note that the probability of μ-multi collision is highest when the tweak is same for all the queries.

In that case for a given $x \in \{0,1\}^{\frac{n}{2}}$, and fixed $\exists i_1, \ldots, i_\mu \in [1, d]$ number of possible tuples of $((Y^i, C^i)$ such that $z^i = \lfloor Y^{i_k} \oplus C^{i_k}\rfloor_{\frac{n}{2}} = x$ is bounded by $2^{\frac{n\mu}{2}}$. Varying over all $x \in \{0,1\}^{\frac{n}{2}}$ and for all combination of $i_1, \ldots, i_\mu \in [1, d]$ we have number of ways i which μ-multi collision occurs is at most $\binom{d}{\mu} 2^{\frac{(\mu+1)n}{2}}$.

Hence we have

$$\Pr\left[\mu\text{-mcoll}|\overline{\text{BAD}}\right] \leq \frac{\binom{d}{\mu}2^{\frac{(\mu+1)n}{2}}}{(2^n)_\mu} \leq d\left(1+\frac{\mu^2}{2^n}\right)\left(\frac{d}{2^{\frac{n}{2}}}\right)^{\mu-1}.$$

Combining the results of this section we have Theorem 7.

E.2 Bounding μ-multi collision for P

Let $P : T \times \{0,1\}^n \to \{0,1\}^n$ be a random function such that we have $P(tw, \star)$ is a random permutation for all $tw \in T$.

We assume that the adversary doesn't make repetitive or redundant queries.

$\mathcal{O}$ Queries: Whenever $\mathscr{A}$ makes an online query of the form $((N^i, j^i), X^i, C^i)$ for some $i \in \mathcal{E}$, $\mathcal{O}$ computes $z^i = \lfloor Y^i \oplus C^i \rfloor_{\frac{n}{2}}$ as response where $Y^i = P(tw^i, X^i)$.

Let $\omega_d = ((N^i, j^i), X^i, z^i)_{i\in\mathcal{E}}$ be the online transcript of the adversary.

We have the μ- multi collision occurs if $\exists i_1, \ldots, i_\mu \in [1, d]$ such that $z^{i_k} = z^{i_l}$ for all $k, l \in [1, \mu]$.

Note that the probability of μ-multi collision is highest when the tweak is same for all the queries.

In that case for a given $x \in \{0,1\}^{\frac{n}{2}}$, and fixed $\exists i_1, \ldots, i_\mu \in [1, d]$ number of possible tuples of (Y^i, C^i) such that $z^i = \lfloor Y^{i_k} \oplus C^{i_k} \rfloor_{\frac{n}{2}} = x$ is bounded by $2^{\frac{n\mu}{2}}$. Varying over all $x \in \{0,1\}^{\frac{n}{2}}$ and for all combination of $i_1, \ldots, i_\mu \in [1, d]$ we have number of ways i which μ-multi collision occurs is at most $\binom{d}{\mu}2^{\frac{(\mu+1)n}{2}}$.

Hence we have

$$\Pr\left[\mu\text{-mcoll}\right] \leq \frac{\binom{d}{\mu}2^{\frac{(\mu+1)n}{2}}}{(2^n)_\mu} \leq d\left(1+\frac{\mu^2}{2^n}\right)\left(\frac{d}{2^{\frac{n}{2}}}\right)^{\mu-1}.$$

Combining the results of this section we have Theorem 8.

F Bounding BAD for mixFeed

Bounding BAD1 : Note that since we model E as an ideal keyed permutation and the total number of encryption and decryption queries are bounded by σ we have,

$$\Pr[\text{BAD1}] \leq \frac{\sigma^2}{2^{n+1}}.$$

Bounding BAD2 : We postpone the probability bound of $K^i_{l_i+1} = K^{*j}_{l^*_j+1}$ to BAD3 . Suppose BAD3 occurs. if $(N^i, A^i, M^i) \neq (N^{*j}, A^{*j}, M^{*j})$ Then Let k be the smallest positive integer such that $D^i_k \neq D^{*j}_k$ where for any (N, A, M) we define $D_k = \begin{cases} \bar{N} \text{ if } k = 0 \\ A_k \text{ if } k \leq a \\ M_{k-l} \text{ if } k > a. \end{cases}$ Then we must have $X^i_{k+1} \neq X^{*j}_{k+1}$. And hence Y^i_{k+1}, Y^{*j}_{k+1} are independent. Consequently $Y^i_{l_i}$ and $Y^{*j}_{l^*_j}$ are independent. Now the event BAD2|BAD3 can be divided into two subcases.
Case 1: $\delta^i_{M^i} = \delta^{*j}_{M^{*j}}$. In this case we must have $Y^i_{k+1} = Y^{*j}_{k+1}$. Hence,

$$\Pr[\text{Case 1}] \leq \frac{\sigma^2}{2^{n+1}}.$$

Case 2: $\delta^i_{M^i} \neq \delta^{*j}_{M^{*j}}$. In this case we must have $Y^i_{k+1} \oplus \delta^i_{M^i} = Y^{*j}_{k+1} \oplus \delta^{*j}_{M^{*j}}$. Hence,

$$\Pr[\text{Case 2}] \leq \frac{\sigma^2}{2^{n+1}}.$$

Since this cases are mutually exclusive and exhaustive we have,

$$\Pr[\text{BAD2}|\text{BAD3}] \leq \frac{\sigma^2}{2^{n+1}}.$$

Bounding BAD3: Note that this event already occur as BAD2 in the analysis of μ-$TPRP$(Appendix C.1) and (μ, λ)-mcp (Appendix D) security and as BAD in the analysis of μ-multicollision security of $\tilde{E}$(Appendix E.1) for mF and is bounded by $\frac{d^2}{2^{n+1}}$.

In case of mixFeed, under Assumption 1 this event can be divided into the following cases.

Case 1: $(N^{i_1} \neq N^{i_2})$ In this case we have $K_{N^{i_1}} \neq K_{N^{i_2}}$ and Hence probability that $K^{i_1} = K^{i_2}$ is atmost $\frac{1}{2^n}$. Varying over all $i_1, i_2 \in \mathcal{E}$ we have,

$$\Pr[\text{Case 1}] \leq \frac{d^2}{2^{n+1}}.$$

Case 2: $(N^{i_1} = N^{i_2} = N^i(\text{say}); j^{i_1} \neq j^{i_2})$ In this case we have $K_{N^{i_1}} = K_{N^{i_2}}$. This event occurs if and only if, $r_i \mid (j^{i_1} - j^{i_2})$ where r_i is the periodicity of K_{N^i}.

Note that queries of this form arise due to the encryption query of $\mathscr{B}$ with nonce N^i.

Let l_i denote the number of blocks in the encryption query of $\mathscr{B}$ with nonce N^i. Then for all i_i, i_2 such that $N^{i_1} = N^{i_2} = N^i$, we have $|j^{i_1} - j^{i_2}| \leq l_i$.

Hence we have $r_i \leq l_i$ and by our assumption probability that this event holds is at most $\frac{l_i}{2^{\frac{n}{2}}}$.

Now varying over all possible i and from the observation that $\sum_i l_i \leq d$ we have,

$$\Pr\left[\textsc{Case } 2\right] \leq \sum_i \frac{l_i}{2^{\frac{n}{2}}} \leq \frac{d}{2^{\frac{n}{2}}}.$$

Since the above two cases are mutually exclusive we have,

$$\Pr\left[\text{BAD3}\right] \leq \frac{d^2}{2^{n+1}} + \frac{d}{2^{\frac{n}{2}}}.$$

Hence combining the bounds for all the events we have Lemma 1.