Article

Almost-Minimal-Round BBB-Secure Tweakable Key-Alternating Feistel Block Cipher

Ming Jiang and Lei Wang *

Department of Computer Science and Engineering, Shanghai Jiao Tong University, Shanghai 200240, China; trojan1019@sjtu.edu.cn
* Correspondence: wanglei_hb@sjtu.edu.cn

Abstract: This paper focuses on designing a tweakable block cipher via tweaking the Key-
Alternating Feistel (KAF for short) construction. Very recently Yan et al. published a tweakable KAF
construction. It provides a birthday-bound security with 4 rounds and Beyond-Birthday-Bound
(BBB for short) security with 10 rounds. Following their work, we further reduce the number
of rounds in order to improve the efficiency while preserving the same level of security bound.
More specifically, we rigorously prove that 6-round tweakable KAF cipher is BBB- secure. The main
technical contribution is presenting a more refined security proof framework, which makes significant
efforts to deal with several subtle and complicated sub-events. Note that Yan et al. showed that
4-round KAF provides exactly Birthday-Bound security by a concrete attack. Thus, 6 rounds are
(almost) minimal rounds to achieve BBB security for tweakable KAF construction.

Keywords: beyond-birthday-bound security; H-coefficient technique; key-alternating Feistel cipher;
provable security; tweakable block cipher

1. Introduction

A block cipher, also known as a pseudorandom permutation, which is a pair of algorithms
\((E, D)\). A block cipher has two important parameters: block length and key length. If the
block length is \(n\) bits and the key length is \(k\) bits, for a mathematical point of view, the block
cipher can be seen as a mapping
\[
\{0, 1\}^k \times \{0, 1\}^n \rightarrow \{0, 1\}^n.
\]

\(E\) represents a mapping that from the key space and the message space to the message space,
and \(D\) is the opposite direction of the mapping in \(E\). In addition, we call \(E\) is encryption, and
\(D\) is decryption. The schemes of block cipher are roughly separated into two main classes,
which are named Feistel networks and substitution—permutation networks (SPNs).

The tweakable block cipher is formalized by Liskov et al. [1]. It introduces to the block
cipher an extra public input parameter tweak. The tweak provides inherent variability
for building higher higher-level cryptographic schemes, namely modes of operation. So
far, the tweakable block cipher has got received wide applications. Examples include
Message Encryption, Message Authentication Code [1,2], and Authenticated Encryption
Mode [3–5], etc. Now designing secure tweakable block ciphers has become a very
important research topic. Cryptographers build tweakable block ciphers either from the
scratch [6–8], or based on existing cryptographic primitives such as block ciphers or per-
mutations [2,9–11]. Among these approaches, one is introducing the tweak to general
structures of classical block ciphers, namely the Feistel construction [12] and the Even—
Mansour construction [13]. We refer the interested readers to [9,14–18] for tweaking the
Even—Mansour construction.

This paper mainly focuses on tweaking the Feistel construction. Since invented by
Horst Feistel in 1973 [12], the Feistel construction has been a mainstream class of block
ciphers. More specifically, there are several Feistel construction variants, such as Luby—Rackoff [19], Generalized Feistel [20], Key-Alternating Feistel [21], etc. They have been adopted in dedicated block ciphers including international and national standards. In 2007, Goldenberg et al. published the first paper of incorporating tweak to the Feistel constructions [22]. In particular, they paid attention to the Luby—Rackoff ciphers, and XOR tweaks to the dataflow branches. We write such tweak injection as linear tweak injection in this paper. Goldenberg et al. found that 6 rounds and more are secure (against polynomial adversaries). Moreover, they showed that 10 rounds are secure against $2^n$ adversarial queries, that is i.e., fully secure with $n$ as the branch bit size of Luby—Rackoff structure. After that, Mitsuda and Iwata analyzed tweaking Generalized Feistel Structures with similar linear tweak injection [20]. They proved that $2d$ rounds are birthday-bound secure with $d$ as the number of branches of Generalized Feistel Structure. Very recently, Yan et al. published a result of tweaking the Key-Alternating Feistel (KAF) Cipher [23]. They introduced the tweak by mixing round keys, and proved that 4 rounds have a birthday-bound security and 10 rounds enable a beyond-birthday-bound security of roughly $2^{2n/3}$ adversarial queries with $n$ as the branch bit size. We will carry on the research of tweaking the KAF. (It is referred to as Feistel-2 in IACR Tikz Library).

The Feistel network [12] is a popular structure of block ciphers. In the $i$-th round of the Feistel cipher, the intermediate state of input $x_i = L \parallel R$ is updated by the round function $G_i$, i.e., $L \parallel R \rightarrow R \parallel L \oplus G_i(k_i, R)$. After tweaking the generalized Feistel ciphers by Mitsuda and Iwata [20], there is are only a few works about tweaking the Feistel cipher. The most mainstream research is tweaking KAF ciphers as Yan et al did recently [23]. They introduced the tweak by several round keys by using a universal hash function $H(\cdot)$, that is, $t_ki \leftarrow H_ki(t)$, where $k_i$ is the secret key, $t$ is the tweak. By tweaking KAF with the $i$-th round function, the input is updated through

$$m_L \parallel m_R \leftarrow m_R \parallel m_L \oplus F_i(H_ki(t) \oplus m_R),$$

where $F(\cdot)$ is the $i$th-round function. Yan et al. presented a 4-round minimized structure with two round keys and a single random function, proved that it achieves Birthday-Bound security. Meanwhile, they presented a 10-round tweakable KAF (TKAF for short) construction (depict in Figure 1) that can achieve BBB security. In this work, we aim to optimize Yan et al’s 10-round structure, and adopt other distinct construction of tweakable block ciphers. Then we give the proof that the new construction still meets the BBB security. We compared with Yan et al’s work [23] which lists in Table 1.

### Table 1. Comparison with related works.

| Key Size | Rounds | Number of Round Functions | Bound | Reference |
|----------|--------|---------------------------|-------|-----------|
| $10n$    | 10     | 10                        | $2n/3$| Yan et al. [23] |
| $6n$     | 6      | 6                         | $2n/3$| Guo et al. [24] (without tweak) |
| $6n$     | 6      | 6                         | $2n/3$| Section 3 (tweaked) |

#### 1.1. Our Contributions

In this paper, we present a 6-round TKAF cipher which meets the BBB security, with tweaking the additional outer four rounds based on based on Guo et al.’s 6-round KAF [24]. Unlike Yan et al.’s research, we adopt the approach of introducing tweak into the 6-round KAF directly. By utilizing Guo et al’s proof methodology, we introduce the tweak via using a universal hash function. We prove when the adversary makes distinct queries with different tweaks, due to the uniformity of the mentioned hash function, it still meets BBB security.
Figure 1. 10-round tweakable Key-Alternating Feistel cipher presented by Yan et al.

1.2. Structure of This Paper

Section 2 is the preliminaries of notations and definitions. Section 3 is the overview of proofs and core contribution. Section 4 is the proof of our conclusion. Section 5 is the future work.

2. Preliminaries

2.1. Notations and General Definitions

Let \( n \) denote a positive integer. Then \( \mathcal{N} = 2^n \) and \( \mathcal{N} = \{0, 1\}^n \). \( F(n) \) denotes the set of all functions mapping from \( \mathcal{N} \) to \( \mathcal{N} \). \( \mathcal{P}(2^n) \) denotes the set of all permutations in the range of \( \{0, 1\}^{2n} \). Let \( \theta(s) \) be a random variable relying on one another random variable \( s \). Then we denote by \( \mathbb{E}_{s \in \mathcal{S}}[\theta(s)] \) the expectation of \( \theta(s) \) taken over all \( s \in \mathcal{S} \). For \( X, Y \in \mathcal{N} \), denote \( X \parallel Y \) or simply \( XY \) as their concatenation.

2.1.1. Block Cipher

A block cipher is a family of permutations indexed by the secret key. It is denoted as \( E : K \times M \to C \), where \( K \) is the key space, \( M \) is the message space, and \( C \) is the ciphertext space. Hence for each \( K \in K \), \( E(K, \cdot) \) or simply \( E_K(\cdot) \) is a permutation from \( M \) to \( C \). In this paper, \( M = C = \{0, 1\}^{2n} \).

2.1.2. Tweakable Block Cipher

A tweakable block cipher is a family of permutations indexed by the secret key and the public tweak. It is denoted as \( E : K \times T \times M \to C \), where \( K \) is the key space, \( T \) is the tweak space, \( M \) is the message space, and \( C \) is the ciphertext space. Hence for each \( K \in K \) and each \( T \in T \), \( E(K, T, \cdot) \) or simply \( E_{K,T}(\cdot) \) is a permutation from \( M \) to \( C \). Similarly, \( M = C = \{0, 1\}^{2n} \). We denote \( \tilde{\Pi}(T, 2n) \) as the set of all tweakable permutations with \( M = C = \{0, 1\}^{2n} \).

2.1.3. Key-Alternating Feistel (KAF) Cipher

A KAF is a block cipher with \( M = C = \{0, 1\}^{2n} \). It has an iterative structure. The \( i \)-th round function has the form \( \Psi^i_k(L \parallel R) = (R \parallel L \oplus F_i(R \oplus k_i)) \), where \( L \) and \( R \) are the left half and the right half of the inputs respectively, \( k_i \) is the \( i \)-th secret round key, and \( F_i \) is
the $i$-th public round function. We denote the $r$-round KAF with $r$ public round functions $F = (F_1, \ldots, F_r)$ in $\mathcal{F}(n)$ and a round-key vector $k = (k_1, \ldots, k_r)$ by

$$KAF^F_k(L \parallel R) = \Psi^{F_r}_{k_r} \circ \cdots \circ \Psi^{F_1}_{k_1}(L \parallel R).$$

### 2.1.4 Uniform AXU Hash Functions

A set of hash functions is denoted as $H : K \times T \rightarrow N$. For each key $k \in K$, a keyed hash function $H_k(\cdot)$ maps the tweak space $T$ to $N$. $H$ is said to be uniform hash function if for any $t \in T$ and $y \in N$,

$$\Pr[k \leftarrow K : H_k(t) = y] = 2^{-n}.$$

Moreover, it is said to be $\epsilon$-almost XOR-universal ($\epsilon$-AXU) if for any $t, t' \in T$ with $t \neq t'$ and any $y \in N$,

$$\Pr[k \leftarrow K : H_k(t) \oplus H_k(t') = y] \leq \epsilon.$$

### 2.2 Security Definitions

A distinguisher $D$ can be thought as a fundamental attacker, and it can make queries to one (or more) “oracle” which can be the block ciphers or the random permutations. The advantage of a distinguisher $D$ in distinguishing two oracles $O$ and $Q$ can be defined as:

$$\text{Adv}(D) = \left| \Pr[D^O \rightarrow 1] - \Pr[D^Q \rightarrow 1] \right|.$$

We discuss this under the Random Permutation model. Firstly, we define two worlds—“the real world” and “the ideal world”. When the distinguisher $D$ interacts with the oracle $(O, F)$, the real world means $O$ is a tweakable block cipher $\tilde{E}(k, \cdot)$, $F = (F_1, \ldots, F_r)$ is a public random function or permutation of $\tilde{E}$, where $k$ is uniformly taken from $K$. In addition, in the ideal world, $O$ is a tweakable permutation $\tilde{\Pi}$ and $F = (F_1, \ldots, F_r)$ is a public random function or permutation of $\tilde{\Pi}$. We call $O$ construction oracle and $F$ inner component oracles. The security of a tweakable block cipher is measured by the advantage of the distinguisher $D$ that distinguishes the two worlds: $(\tilde{E}(k, \cdot), F)$ and $(\tilde{\Pi}, F)$ (depicted in Figure 2). We write

$$\text{Adv}(D) = \left| \Pr[D^{\tilde{E}(k, \cdot), F} \rightarrow 1] - \Pr[D^{\tilde{\Pi}, F} \rightarrow 1] \right|.$$

![Figure 2. A distinguisher $D$ distinguishes the real world and the ideal world.](image)

Theoretically, we only consider the information-theoretic distinguisher whose computation power is unlimited, i.e., it is determined, and only with limited information, that which means the number of access to the oracle is limited. We assume that the distinguishers do not make redundant queries. We also consider the distinguishers are under the...
chosen-ciphertext-attack (CCA) model, meanwhile they can choose tweaks, where they have the ability to query all the oracles either forward or backward.

We denote \( q_e \) as the quantity of queries to the construction oracle and \( q_f \) as the number of queries to each inner component oracle, then the definition of insecurity of the tweakable block cipher \( \tilde{E} \) is

\[
\text{Adv}_{\tilde{E}}(q_e, q_f) = \max_{D} \{ \text{Adv}(D) \}.
\]

H-Coefficient Technique

We utilize the H-coefficient technique \([25,26]\) to evaluate the upper bound of the advantage of the adversary mentioned above.

**Definition 1** (Transcript). A transcript \( \tau = (Q_E, Q_F) \) is the response-tuple when the distinguisher \( D \) interacts with its oracle, where \( Q_E \) contains the tuples of the form \((t, LR, ST) \in T \times \{0, 1\}^{2n} \times \{0, 1\}^{2n} \) which interacts with the construction oracle and \( Q_F \) contains the tuples \((x, y) \) which interacts with the inner component oracle.

By definition, we can see that \( D \) either makes the direct query \((t, LR) \) to the construction oracle with \( x \) to the inner component oracle, receiving answer \( ST \) and \( y \), or makes the inverse query \((t, ST) \) to the construction oracle with \( y \) to the inner component oracle, receiving answer \( LR \) and \( x \). Suppose that \( |Q_E| = q_e \), and there are \( m \) distinct tweaks in the \( Q_E \). We assume there exist \( q_i(1 \leq i \leq m) \) distinct queries for the \( i \)-th tweak, hence \( \sum_{i=1}^{m} q_i = q_e \). That means \( Q_E = \bigcup Q_E_i, 1 \leq i \leq m, \) where \( Q_E_i \) are the corresponding queries of the \( i \)-th tweak. Similarly, we have \( |Q_F| = q_f \) and \( Q_F = \bigcup Q_F_j, 1 \leq j \leq r \).

We note that all the transcripts of queries are directionless and disordered form, but according to our hypothesis that the distinguisher \( D \) is deterministic. Thus, there is a one-to-one mapping between this statement and the primitive transcript of the interaction of \( D \) with its oracles. Meanwhile, the output of \( D \) is a deterministic function of \( \tau \).

In addition, for the function \( F_j \) and its set of queries \( Q_{F_j} \), if for each \((x, y) \in Q_{F_j}, F_j(x) = y \), we say that \( F_j \) extends \( Q_{F_j} \), denoted by \( F_j \upharpoonright Q_{F_j} \). Similarly, for the permutation \( P^{(i)} \) and its transcript sets \( Q_{E_i} \), if for each \((t, LR, ST) \in Q_{E_i}, P^{(i)}(t, LR) = ST \), we say that \( P^{(i)} \) extends \( Q_{E_i} \), denoted by \( P^{(i)} \upharpoonright Q_{E_i} \). With the above definition of “extend”, we can define \( \text{KAF}^{(i)}_{(j)} \upharpoonright Q_{E_i} \). Finally, for \( Q_F = (Q_{F_1}, \ldots, Q_{F_j}) \) and \( F = (F_1, \ldots, F_j) \), if \( F_1 \upharpoonright Q_{F_1} \land \ldots \land F_j \upharpoonright Q_{F_j} \), then we have \( F \upharpoonright Q_F \).

We further define the probability that the interactions of the distinguisher \( D \) with the real world and the ideal world. In addition, we respectively denote them by \( \Pr_{re}(\tau) \) and \( \Pr_{id}(\tau) \), where \( \tau \) is a transcript of these interactions.

With these definitions, we give the core lemma of the H-coefficient technique, and the distinguishing advantage could be inferred by the ratio of \( \Pr_{re}(\tau) \) and \( \Pr_{id}(\tau) \).

**Lemma 1** (From [27]). Assume that there is a function \( \varphi(q_f, q_e) \) such that for every possible transcript \( \tau \) with \( q_e \) and \( q_f \) queries of the two types it holds

\[
|\Pr_{id}(\tau) - \Pr_{re}(\tau)| \leq \Pr_{id}(\tau) \cdot \varphi(q_f, q_e),
\]

then it holds

\[
\text{Adv}_{\text{KAF}}(q_f, q_e) \leq \varphi(q_f, q_e).
\]

According to [27], the upper bound of \( |\Pr_{id}(\tau) - \Pr_{re}(\tau)| \) is named “\( \varphi \)-point-wise proximity” of \( \tau \), which was raised by Hoang and Tessaro (HT) [27]. We let \( K = K_{\text{good}} \cup K_{\text{bad}} \), where \( K_{\text{good}} \) and \( K_{\text{bad}} \) are mutual exclusive subsets. Denote \( \Pr_{re}(\tau, k) \) as the probability that \( D \) interacts with the real world, where \( k \in K \), and \( \Pr_{id}(\tau, k) \) is that \( D \) interacts with the ideal world, where \( k \) is a “virtual” key uniformly selected from the key space \( K \). With the above definition, HT provided a lemma to establish point-wise proximity.
Lemma 2 (Lemma 1 of [27]). Fix a transcript τ with \( \Pr_{id}(\tau) > 0 \). Assume that: (i) \( \Pr[k \in K_{bad}] \leq \delta \), and (ii) there is a function \( g : K \rightarrow [0, \infty) \) such that for all \( k \in K_{good} \), it holds \( \frac{\Pr_{re}(\tau, k)}{\Pr_{id}(\tau)} \geq 1 - g(k) \). Then we have

\[
\Pr_{id}(\tau) - \Pr_{re}(\tau) \leq \Pr_{id}(\tau) \cdot (\delta + \mathbb{E}_{k \in K}[g(k)]).
\]

3. Overview

3.1. Beyond Birthday-Bound Security for Six Rounds

In the beginning, we need to guarantee that tweaking the KAF cipher does not break its construction, and the influence on efficiency of the scheme execution can not be very enormous. For study of the execution efficiency and security, Liskov et al. [1] thought the cost of changing tweaks should be less than that of changing keys. However, the study by Jean et al. [14] showed that the adversary can hardly obtain the key, but has the ability to control the good event.

In this paper, we use a nonlinear compound mode for tweaking the Feistel structure, instead of tweaking dependent or independent keys. As we known, the four rounds of KAF cipher do not meet BBB security [24]. Yan’s [23] work showed that tweaking 10 rounds KAF cipher can meet BBB security. Our work shows a method for tweaking the KAF cipher by the nonlinear pattern, and reduces the rounds of the scheme. For requirement of security, we consider to introduce the tweak with the round-key vectors by using a universal hash function.

Firstly, we use the suitable round-key vector which was defined by Guo [24]:

**Definition 2** (Suitable Round-Key Vector for 6 Rounds [24]). A round-key vector \( k = (k_1, k_2, k_3, k_4, k_5, k_6) \) is suitable if it satisfies the following conditions:

(i) \( k_1, k_2, k_3, k_4, k_5, k_6 \) are uniformly distributed in \( \{0, 1\}^n \);

(ii) for \( (i, j) \in \{(1, 2), (2, 3), (4, 5), (5, 6), (1, 6)\} \), \( k_i \) and \( k_j \) are independent.

Yan’s [23] work used the minimized 6-round KAF as a “core”, with additional four more rounds on the first and last sides of the “core”, meanwhile introducing the tweak into these four rounds. They gave a 10-round TKAF construction with BBB security. In our work, we aim to “tweak” the first and last two rounds of the “core”, and use a universal hash function to merge the tweak into round-key vectors.

Next, we denote this 6-round construction by

\[
\text{TKAF}^F_k(t, x) = \Psi_{k_6, t}^F \circ \Psi_{k_5, t}^F \circ \Psi_{k_4, t}^F \circ \Psi_{k_3, t}^F \circ \Psi_{k_2, t}^F \circ \Psi_{k_1, t}^F(x),
\]

where \( F = (F_1, F_2, F_3, F_4, F_5, F_6) \) are random functions, \( k = (k_1, k_2, k_3, k_4, k_5, k_6) \) are the corresponding round keys, \( t \in T \) is a tweak and \( x \in \{0, 1\}^{2n} \) is a message (depict in Figure 3).

Finally, we upper-bound the advantage of an adversary to attack this scheme. By utilizing the H-coefficient technique which is in Lemma 2, we firstly upper bound the bad key event \( \delta \), then upper-bound the expectation of the function \( g(k) \), which holds \( \frac{\Pr_{re}(\tau, k)}{\Pr_{id}(\tau, k)} \geq 1 - g(k) \). By Lemma 1, we could obtain the advantage. Thus, we have this theorem:

**Theorem 1.** For the 6-round tweakable KAF cipher with a suitable round-key vector as specified in Definition 2, it holds

\[
\text{Adv}_{\text{TKAF}}(q_f, q_t) \leq (7q_e^2 + 24q_t^2q_f + 20q_tq_f^2) \frac{1}{N^2} + (4q_e^2 + 4q_t^2q_f + 2q_tq_f^2 + 4q_t^2 + 6q_tq_f) \frac{\varepsilon}{N} + 4q_t^2q_f^2 + 4q_t^2q_e^2.
\]
3.2. Core Contribution

In our work, we analyze the influence of tweaking KAF ciphers on security. We tweak the outer four rounds of Guo et al’s 6-round KAF and the proof of BBB security is the major research work we have done.

4. Security Proof of Theorem 1

In the following subsections, we present the methodology to prove Theorem 1. We fix a transcript $\tau = (Q_E, Q_F)$ with $Q_F = (Q_{E_1}, Q_{F_2}, Q_{E_3}, Q_{F_4}, Q_{E_5}, Q_{F_6})$, where $|Q_E| = q_e$ and $|Q_F| = q_f$, $i = 1, \ldots, 6$. We divide the analysis of this claim into two parts: (i) define bad key vectors, then (ii) lower bound the probability $\Pr_{\tau}(\tau, k)$. We analyze these two parts respectively.

4.1. Bad Key Vectors and Probability

**Definition 3 (Bad Key Vectors for 6 rounds).** A suitable key vector $k \in K$ is bad, for a transcript $\tau = (Q_E, Q_F)$, if one of the follow conditions is met:

- **(A-1)** there exists $(t, LR, ST) \in Q_E$, $(x_1, y_1) \in Q_{E_1}$, $(x_6, y_6) \in Q_{F_6}$, such that $H_{k_1}(t) = R \oplus x_1$, $H_{k_6}(t) = S \oplus x_6$.
- **(A-2)** there exists $(t, LR, ST) \in Q_E$, $(x_1, y_1) \in Q_{E_1}$, $(x_2, y_2) \in Q_{F_2}$, such that $H_{k_1}(t) = R \oplus x_1$, $H_{k_2}(t) = L \oplus y_1 \oplus x_2$.
- **(A-3)** there exists $(t, LR, ST) \in Q_E$, $(x_5, y_5) \in Q_{E_5}$, $(x_6, y_6) \in Q_{F_6}$, such that $H_{k_5}(t) = S \oplus x_6$, $H_{k_6}(t) = T \oplus y_6 \oplus x_5$.

otherwise, $k$ is good. We denote $K_{\text{bad}}$ for the set of bad key vectors, and $K_{\text{good}}$ for the good key vectors.

In the beginning, we upper-bound the probability of the bad key vectors. Firstly, we analyze the above three conditions respectively, consider **(A-1)** first. Since we have the key $k_1$ and $k_6$ picked from the key space $K$ uniformly and randomly, for the properties of suitable, $k_1$ and $k_6$ are independent of each other (Definition 2). By the uniformity of $H$, $H_{k_1}$ and

![Figure 3. A tweakable Key-Alternating Feistel cipher with 6 rounds](image-url)
Symmetry 2021, 13, 649

$H_k$ are also independent. Thus, there are $N^2$ possible choices. For $(t, LR, ST) \in Q_E$, $(x_1, y_1) \in Q_{F_1}$ and $(x_6, y_6) \in Q_{F_6}$, we have at most $q \eta^2$ choices, as $|Q_E| = q_e, |\text{Dom} F_1| = |\text{Dom} F_6| = q_f$, where $\text{Dom} F$ is a set of $x$ that there exists $(x, y) \in Q_E$ such that $F(x) = y$, i.e., $\text{Dom} F \overset{\text{def}}{=} \{x \in \{0, 1\}^n : \exists (x, y) \in Q_E, F(x) = y\}$. Therefore, the probability of condition (A-1) is at most $\frac{q \eta^2}{N^2}$.

Similarly, by definition of suitable key vector (Definition 2), it also holds that $(k_1, k_2)$, $(k_5, k_6)$ are independent, and for the uniformity of $H$, we have $\Pr[(A-2)] = \Pr[(A-3)] \leq \frac{q \eta^2}{N^2}$.

To sum up, we can upper-bound the probability of the bad key vectors with

$$\Pr[k \overset{\text{random}}{\leftarrow} K : k \in K_{\text{bad}}] \leq \frac{3q \eta^2}{N^2}. \quad (2)$$

4.2. Analysis for Good Keys

In the following, we fix the round-key vectors $k \in K_{\text{good}}$, and aim to lower bound the probability $\Pr[F \overset{\text{random}}{\leftarrow} F_3^3 : \text{TKEF}^T_k \vdash Q_E \mid F \vdash Q_T]$. By the analytical method of Cogliati et al. [9, 15], we divide this proof process into two steps: (i) upper bounding the probability that a pair of functions $(F_1, F_6)$ satisfies “bad” conditions. By these means, the “good” conditions of the function-pair can transfer the transcripts of the distinguisher on 6 rounds to a special transcripts on 4 rounds, it can be said that we “peel off” the outer two rounds [24]; then (ii) assuming that $(F_1, F_6)$ is good, by bounding the inner 4 rounds, we will prove the claim of Theorem 1.

Peeling Off the Outer Two Rounds

We pick a pair of round functions $(F_1, F_6)$ such that $F_1 \vdash Q_{F_1}$ and $F_6 \vdash Q_{F_6}$. For each transcript $(t, LR, ST) \in Q_E$, denote $X \leftarrow L \oplus F_1(H_k(t) \oplus R)$ and $A \leftarrow T \oplus F_6(H_k(t) \oplus S)$. From this, we obtain $q_e$ transcripts with the form of $(t, RX, AS)$. For convenience, we denote a new set including all these introduced transcript tuples by $Q_E^x(F_1, F_6)$. For convenience, we define two subsets of $Q_E^x(F_1, F_6)$, the transcripts that collide at the positions of $X$ and $A$, respectively. Denote them by $TD(X)$ and $TD(A)$:

$$TD(X) = \{(t, RX, AS) : (t, RX, AS) \in Q_E^x(F_1, F_6), X \text{ is identical}\}$$

$$TD(A) = \{(t, RX, AS) : (t, RX, AS) \in Q_E^x(F_1, F_6), A \text{ is identical}\}$$

In order to characterize $\tau$, we define four key-dependent quantities:

$$n_{(1)}(k) \overset{\text{def}}{=} |\{(t, LR, ST), (x_1, y_1) \in Q_E \times Q_{F_1} : H_k(t) = R \oplus x_1\}|$$

$$n_{(6)}(k) \overset{\text{def}}{=} |\{(t, LR, ST), (x_6, y_6) \in Q_E \times Q_{F_6} : H_k(t) = S \oplus x_6\}|$$

$$n_{(2,3)}(k) \overset{\text{def}}{=} |\{(t, LR, ST), (x_2, y_2, x_3, y_3) \in Q_E \times Q_{F_2} \times Q_{F_3} : k_3 = R \oplus y_2 \oplus x_3\}|$$

$$n_{(4,5)}(k) \overset{\text{def}}{=} |\{(t, LR, ST), (x_4, y_4, x_5, y_5) \in Q_E \times Q_{F_4} \times Q_{F_5} : k_4 = S \oplus y_5 \oplus x_4\}|$$

Now we define the “bad event” on the pair $(F_1, F_6)$. If the corresponding set $Q_E^x(F_1, F_6)$ of the pair $(F_1, F_6)$ fulfills one of the following “collision” conditions, we say that the predicate is bad, denoted by $\text{Bad}(F_1, F_6)$:

- **(B-1)** there exists $(t, RX, AS) \in Q_E^x(F_1, F_6)$, $(x_2, y_2) \in Q_{F_2}$, $(x_5, y_5) \in Q_{F_5}$, such that $H_k(t) = X \oplus x_2, H_k(t) = A \oplus x_5$;
- **(B-2)** there exists $(t, RX, AS) \in Q_E^x(F_1, F_6)$, $(x_2, y_2) \in Q_{F_2}$, $(x_3, y_3) \in Q_{F_3}$, such that $H_k(t) = X \oplus x_2, k_3 = R \oplus y_2 \oplus x_3$;
- **(B-3)** there exists $(t, RX, AS) \in Q_E^x(F_1, F_6)$, $(x_4, y_4) \in Q_{F_4}$, $(x_5, y_5) \in Q_{F_5}$, such that $H_k(t) = A \oplus x_5, k_4 = S \oplus y_5 \oplus x_4$. 
• (B-4) there exist two distinct \((t, RX, AS), (t', R'X', A'S') \in \mathcal{Q}_x^*(F_1, F_6), (x_2, y_2) \in \mathcal{Q}_F^x\), such that \(X = X'\) and \(H_{k_2}(t) = X \oplus x_2\); or symmetrically two distinct \((t, RX, AS), (t', R'X', A'S') \in \mathcal{Q}_x^*(F_1, F_6), (x_5, y_5) \in \mathcal{Q}_F^x\), such that \(A = A'\) and \(H_{k_2}(t) = A \oplus x_5\);

• (B-5) there exist two distinct \((t, RX, AS), (t', R'X', A'S') \in \mathcal{Q}_x^*(F_1, F_6), (x_2, y_2) \in \mathcal{Q}_F^x\), such that \(A = A'\) and \(H_{k_2}(t) = X \oplus x_2\); or symmetrically two distinct \((t, RX, AS), (t', R'X', A'S') \in \mathcal{Q}_x^*(F_1, F_6), (x_5, y_5) \in \mathcal{Q}_F^x\), such that \(X = X'\) and \(H_{k_2}(t) = A \oplus x_5\).

If the predicate \(\text{Bad}(F_1, F_6)\) does not hold, then we can deem that \((F_1, F_6)\) is good.

Now we bound the probability of \(\text{Bad}(F_1, F_6)\).

Lemma 3. It holds

\[
\Pr[\text{Bad}(F_1, F_6) | F_1 \vdash Q_{F_1} \land F_6 \vdash Q_{F_6}]
\leq \frac{4q_2^2 q_f + q_4 q_f^2}{N^2} + \frac{q_f(n(1)(k) + n(6)(k))}{N}
+ \frac{n(2)(k) + n(4)(k)}{N} + \frac{4q_4^2 q_f^2 + q_f(n(1)(k) + n(6)(k))}{N}
\]

Proof. We prove the above 5 cases of \(\text{Bad}(F_1, F_6)\) on the condition of \(F_1 \vdash Q_{F_1} \land F_6 \vdash Q_{F_6}\):

(B-1) For arbitrary \((t, RX, AS) \in \mathcal{Q}_x^*(F_1, F_6)\), if there exists \((x_2, y_2) \in \mathcal{Q}_F^x\) and \((x_5, y_5) \in \mathcal{Q}_F^x\), such that \(H_{k_2}(t) = X \oplus x_2\) and \(H_{k_2}(t) = A \oplus x_5\). Then for the corresponding \((t, LR, ST) \in \mathcal{Q}_E\), we have \(L \oplus F_1(H_{k_2}(t) \oplus R) = H_{k_2}(t) \oplus x_2\) and \(T \oplus F_6(H_{k_2}(t) \oplus S) = H_{k_2}(t) \oplus x_5\). On account of the uniformity of \(H\), it must hold \(H_{k_2}(t) \oplus R \notin \text{Dom}F_1\) (if \(H_{k_2}(t) \oplus R \in \text{Dom}F_1\) and \(H_{k_2}(t) = X \oplus x_2\), then the condition (A-2) is fulfilled). Similarly, it must be \(H_{k_2}(t) \oplus S \notin \text{Dom}F_6\). Thus, on the condition of \(F_1 \vdash Q_{F_1} \land F_6 \vdash Q_{F_6}\), \(F_1(H_{k_2}(t) \oplus R) \land F_6(H_{k_2}(t) \oplus S)\) keep uniform. So, the probability of both \(L \oplus F_1(H_{k_2}(t) \oplus R) = H_{k_2}(t) \oplus x_2\) and \(T \oplus F_6(H_{k_2}(t) \oplus S) = H_{k_2}(t) \oplus x_5\) holding is at most \(\frac{1}{N^2}\). And in addition, the choices of all 3-tuples \((t, LR, ST), (x_2, y_2), (x_5, y_5)\) do not exceed \(q_4 q_f^2\). Therefore, we have \(\Pr[(B-1)] \leq \frac{q_4 q_f^2}{N^2}\).

(B-2) and (B-3) We consider (B-2) firstly.

There exists a 3-tuple \((t, LRX, AST), (x_2, y_2), (x_5, y_5)\), such that the number of \(k_3 = R \oplus y_2 \oplus x_5\) is \(n(2)(k)\), where \((t, LRX, AST)\) is a joint notation of \((t, LRX, AST)\) and its corresponding induced \(X\) and \(A\). Moreover, \(H_{k_2}(t) = X \oplus x_2\) means \(L \oplus F_1(H_{k_2}(t) \oplus R) = H_{k_2}(t) \oplus x_2\). When \(H_{k_2}(t) \oplus R \in \text{Dom}F_1\), then it cannot hold \(L \oplus \text{Img}F_1(H_{k_2}(t) \oplus R) = H_{k_2}(t) \oplus x_2\), otherwise (A-2) is fulfilled. Furthermore, when \(H_{k_2}(t) \oplus R \notin \text{Dom}F_1\), on the condition of \(F_1 \vdash Q_{F_1}\), then \(F_1(H_{k_2}(t) \oplus R)\) keeps uniform. Meanwhile \(H\) also keeps uniform, thus we have the probability of \(L \oplus F_1(H_{k_2}(t) \oplus R) = H_{k_2}(t) \oplus x_2\) is at most \(\frac{1}{N^2}\). Therefore, \(\Pr[(B-2)] \leq \frac{n(2)(k)}{N^2}\). The condition (B-3) is symmetric with (B-2), so with the similar analysis, we have \(\Pr[(B-3)] \leq \frac{n(4)(k)}{N^2}\).

(B-4) For the given pair of distinct merged transcripts \((t, LRX, AST)\) and \((t', L'R'X', A'S'T')\) together with \((x_2, y_2) \in \mathcal{Q}_F^x\), we discuss the cases in three conditions:

• Case 1: when \(t \neq t'\), if it holds \(H_{k_2}(t) \oplus R = H_{k_2}(t') \oplus R'\), i.e., for the \(e\)-ALIX property of \(H\) function, the probability of \(H_{k_2}(t) \oplus H_{k_2}(t') \oplus R = R \oplus R'\) is at most \(e\). If \(H_{k_2}(t) \oplus R \neq H_{k_2}(t') \oplus R'\), we note that \(H_{k_2}(t) \oplus R \notin \text{Dom}F_1, F_1(H_{k_2}(t') \oplus R') \notin \text{Dom}F_1\), otherwise (A-2) is fulfilled. Thus, on the condition of \(F_1 \vdash Q_{F_1}\), \(F_1(H_{k_2}(t) \oplus R)\) and \(F_1(H_{k_2}(t') \oplus R')\) are independent with each other, also keep uniformly random. Then it holds \(\Pr[F_1(H_{k_2}(t) \oplus R) = L \oplus L' \oplus F_1(H_{k_2}(t') \oplus R')] \leq e + (1 - e) \frac{1}{N} = e + \frac{1}{N} \epsilon\). Therefore, the probability of the collision at the position \(H_{k_2}(t) \oplus X\) and \(X = X'\) is at most \((e + \frac{1}{N} e) \leq e^2 + \frac{1}{N} \epsilon\).

• Case 2: if \(t = t'\) and \(R \neq R'\), for \(X = X'\), the probability of \(F_1(H_{k_2}(t) \oplus R) \oplus L = F_1(H_{k_2}(t') \oplus R') \oplus L'\) is at most \(\frac{1}{N^2}\). And in addition, for \(H_{k_2}(t) = X \oplus x_2\), the probability of \(H_{k_2}(t) = F_1(H_{k_2}(t) \oplus R) \oplus L \oplus x_2\) is at most \(\frac{1}{N^2}\). For the property of \(H\), we have the probability of the collision at the position \(X\) is at most \(\frac{1}{N^2}\).
**Case 3:** if \( t = t' \) and \( R = R' \) but \( L \neq L' \), it can not cannot be held that \( X = X' \) and \( H_{k_2}(t) = X \oplus x_2 \).

To sum up, the probability of “former” part of (B-4) can not cannot exceed \( \epsilon^2 + \frac{1}{N^2} \), and the analysis of “latter” part is similar to the former part. We consider all possible pairs of transcripts, the quantity of these pairs can not cannot exceed \( \frac{2q_f^2q_f}{N} \).

\[
Pr(B-4) \leq \frac{2q_f^2q_f}{N} + \frac{q_f^2q_f}{N}.
\]

(B-5) For the given transcripts \( (t, LRX, AST) \neq (t', L'R'X', A'S'T') \) and \( (x_2, y_2) \in Q_{F_2} \), due to the conditions on good key vector, it holds \( H_{k_1}(t) \oplus R \notin DomF_3 \). The same as (B-4), we consider the front part of this condition. According to the state of \( S \), we respectively discuss in three cases:

**Case 1:** it holds \( H_{k_6}(t) \oplus S \notin DomF_6 \), then for the distinct \( (t, LRX, AST) \) and \( (t', L'RX', A'S'T') \), they all have \( q_f \) choices.

- **If** \( t \neq t' \), if it holds \( H_{k_6}(t) \oplus S = H_{k_6}(t') \oplus S' \), then the probability of \( H_{k_6}(t) \oplus H_{k_6}(t') = S \oplus S' \) is at most \( \epsilon \);

- **If** \( t \neq t' \), if it holds \( H_{k_6}(t) \oplus S \neq H_{k_6}(t') \oplus S' \), then \( F_6(H_{k_6}(t) \oplus S) \) and \( F_6(H_{k_6}(t') \oplus S') \) are independent and uniformly random. Thus, on the condition of \( F_6 \nmid Q_{F_6} \), we have

\[
Pr[T \oplus F_6(H_{k_6}(t) \oplus S) = T' \oplus F_6(H_{k_6}(t') \oplus S')] \leq \epsilon + (1 - \epsilon) \frac{1}{N} \leq \epsilon + \frac{1}{N}.
\]

On the condition of \( F_1 \nmid Q_{F_1} \), \( F_1(H_{k_1}(t) \oplus R) \) is also uniform. Hence, similar with (B-4), we have

\[
Pr[H_{k_2}(t) \oplus X = H_{k_2}(t') \oplus X'] \leq \epsilon^2 + \frac{1}{N} \epsilon.
\]

- **If** \( t = t' \) but \( S \neq S' \), if \( A = A' \), then it holds

\[
Pr[F_6(H_{k_6}(t) \oplus S) \oplus T = F_6(H_{k_6}(t') \oplus S') \oplus T'] \leq \frac{1}{N},
\]

and for \( H_{k_2}(t) = X \oplus x_2 \), the probability of \( H_{k_2}(t) = F_1(H_{k_1}(t) \oplus R) \oplus L \oplus x_2 \) is at most \( \frac{1}{N} \);

- **If** \( t = t' \) and \( S = S' \) but \( T \neq T' \), it could not be held that \( A = A' \) or \( H_{k_2}(t) = X \oplus x_2 \).

Under the above cases, we have the probability of the collision at the position \( H_{k_2}(t) \oplus X \) and \( A = A' \) is at most \( \epsilon^2 + \frac{1}{N} \epsilon \). In addition, for \( H_{k_6}(t) \oplus S \notin DomF_6 \), the probability of (B-5)’s front part is at most \( \frac{2q_f^2q_f}{N} + \frac{q_f^2q_f}{N^2} \).

**Case 2:** For \( H_{k_6}(t) \oplus S \in DomF_6 \), the choices of \( (t, LRX, AST) \) are \( n_{6}(k) \). Similar with Case 1, we have \( Pr[L \oplus F_1(H_{k_1}(t) \oplus R) \oplus H_{k_2}(t) \in F_2] \leq \frac{q_f}{N} + q_f \epsilon \). Therefore, the probability of holding at least one such transcript \( (t, LRX, AST) \) is at most \( \frac{q_f^2n_{6}(k)}{N} + q_f n_{1}(k) \epsilon \).

To sum up the above two cases, the probability that the former part of (B-5) holding is at most \( q_f^2q_f \epsilon^2 + \frac{q_f^2n_{6}(k)}{N} + \frac{q_f^2q_f}{N^2} + q_f \epsilon n_{1}(k) + n_{6}(k) \). Similarly, the latter part of (B-5) is symmetric with the former part. Therefore, we have

\[
Pr(B-5) \leq 2q_f^2q_f \epsilon^2 + \frac{q_f \cdot (n_{1}(k) + n_{6}(k))}{N} + \frac{2q_f^2q_f}{N^2} + q_f \epsilon (n_{1}(k) + n_{6}(k)).
\]
We sum up all the five conditions, it holds
\[
\Pr[\text{Bad}(F_1, F_6)|F_1 \vdash Q_{f_1} \land F_6 \vdash Q_{f_6}] \\
\leq \frac{4q_f^2q_\epsilon + q_\epsilon q_f^2}{N^2} + \frac{q_f \cdot (n_{(1)}(k) + n_{(6)}(k))}{N} \\
+ \frac{n_{(2,3)}(k) + n_{(4,5)}(k)}{N} + \frac{4q_f^2q_\epsilon^2}{N^2} + q_\epsilon(q_{(1)}(k) + n_{(6)}(k)).
\]

Now we prove the Lemma 3. \(\square\)

4.3. Analysis of the Inner Four Rounds

In the following section, we analyze the inner four rounds of TKAF which depicts in Figure 4. We denote \(Q_E(F_1, F_6)\) the set of tuples in the form \((t, RX, AS)\), which is induced by peeling off outer two rounds. Similar with [24], we also write \(F^* = (F_2, F_3, F_4, F_5)\), further denote
\[
p(\tau, F_1, F_6) = \Pr[F^* \xrightarrow{\delta} (F(n))^4 : \text{TKAF}_k^F \vdash Q_E(F_1, F_6)|F_1 \vdash Q_{f_1}, i = 1, 2, 3, 4, 5, 6].
\]

Figure 4. Inner 4 rounds of the tweakable Key-Alternating Feistel cipher.

Lemma 4 (From [24]). Assume that there exists a function \(\varphi : (F(n))^2 \times K \rightarrow [0, \infty)\) such that for any good \((F_1, F_6)\), it holds
\[
p(\tau, F_1, F_6) \leq \frac{q_\epsilon^{-1} \prod_{i=0}^{q_\epsilon-1} \left( \frac{1}{N^2 - 1} \right)}{1 - \varphi(F_1, F_6, k)}. \tag{3}
\]

Then we have
\[
\frac{\Pr_{\text{re}}(\tau, k)}{\Pr_{\text{id}}(\tau, k)} \geq 1 - \Pr[\text{Bad}(F_1, F_6)|F_1 \vdash Q_{f_1}, F_6 \vdash Q_{f_6}] \\
- \mathbb{E}_{F_1, F_6}[\varphi(F_1, F_6, k)|F_1 \vdash Q_{f_1}, F_6 \vdash Q_{f_6}].
\]

Lemma 5. For any fixed good tuple \((F_1, F_6)\), there exists a function \(\varphi(F_1, F_6, k)\) of the function pair and the round-key vector \(k\) such that the inequality (3) mentioned in Lemma 4. Then,
\[
\mathbb{E}_{F_1, F_6, k}[\varphi(F_1, F_6, k)] \leq \frac{4q_f^2q_\epsilon^2 + 7q_f^3 + 20q_f^2q_\epsilon + 12q_\epsilon q_f^2}{N^2} \\
+ \frac{4q_f^2q_\epsilon + 4q_f^2q_\epsilon q_\epsilon + 4q_\epsilon^2 + 6q_\epsilon q_\epsilon}{N}. \tag{4}
\]
Proof. Due to the space constraints, the full proof must be deferred to Appendix A. In the following, we only present a proof sketch and the core conclusions. At the beginning of the proof, we define some notations and values in order to present the proof process.

We divide the transcripts in $Q^*_k(F_1, F_6)$ into four sets:

- $G_1 = \{ |\mathcal{ID}(X)| = |\mathcal{ID}(A)| = 1, \text{ and } H_k(t) \oplus X \notin \text{Dom}F_2 \lor H_{k_5}(t) \oplus X \notin \text{Dom}F_5 \};$
- $G_2 = \{ H_k(t) \oplus X \in \text{Dom}F_2 \};$
- $G_3 = \{ H_{k_5}(t) \oplus A \in \text{Dom}F_5 \};$
- $G_4 = \{ |\mathcal{ID}(X)| \geq 2 \lor |\mathcal{ID}(A)| \geq 2 \}.$

Then we denote $E_{G_1}, E_{G_2}, E_{G_3}$ and $E_{G_4}$ by the events that $\text{TKAF}^{F^{*}_{k(t)}}_{A_{G}^{1}(t)} \vdash G_1, G_2, G_3$ and $G_4$ respectively, and let $\beta_1 = |G_2|, \beta_2 = |G_3|, \beta_3 = |G_4|.$ We list $G_l = \{(t, RX, AS), \ldots, (t, R, X_i, A_i |G_i, A |G_i, S |G_i)\}$ with some arbitrary orders. Denote $E_{G_l}$ the event that $\text{TKAF}^{F^{*}_{k(t)}}$ extends the $i$-th tuple $(t, R, X_i, A_i S_i).$ We define four sets of “collision position”:

$$
\begin{align*}
\text{Ext}F_3^{(l)} & \overset{\text{def}}{=} \{ x_3 : \exists (t, R, X_i, A_i S_i) \in G_l, \ i \leq l, \text{s.t. } x_3 = k_3 \oplus R \oplus F_2(H_k(t) \oplus X_i) \}; \\
\text{Ext}F_3^{(l)} & \overset{\text{def}}{=} \{ x_3 : \exists (t, RX, AS) \in G_2, \text{s.t. } x_3 = k_3 \oplus R \oplus \text{Img}F_2(H_k(t) \oplus X) \}; \\
\text{Ext}F_4^{(l)} & \overset{\text{def}}{=} \{ x_4 : \exists (t, R, X_i, A_i S_i) \in G_l, \ i \leq l, \text{s.t. } x_4 = k_4 \oplus S_i \oplus F_5(H_{k_5}(t) \oplus A_i) \}; \\
\text{Ext}F_4^{(l)} & \overset{\text{def}}{=} \{ x_4 : \exists (t, RX, AS) \in G_3, \text{s.t. } x_4 = k_4 \oplus S \oplus \text{Img}F_5(H_{k_5}(t) \oplus A) \}.
\end{align*}
$$

For convenience, we denote two values $e_3^{(l)} = |\text{Ext}F_3^{(l)} \setminus \text{Dom}F_3|,$ and $e_4^{(l)} = |\text{Ext}F_4^{(l)} \setminus \text{Ext}F_3^{(l)}|,$ which are the quantities of choices in the sets. Finally, the function $\text{Num}_3^{(l)}(y_3)$ is the number of pre-images $y_3,$ which belongs to the set $\text{Dom}F_3 \cup \text{Ext}F_3^{(l)}.$ That is $\text{Num}_3^{(l)}(y_3) = |\{ x_3 \in \text{Dom}F_3 \cup \text{Ext}F_3^{(l)} : F_3(x_3) = y_3 \}|.$

Since we have these definitions mentioned above, we can lower bound

$$
p(\tau, F_1, F_6) = \Pr[E_{G_1} \land E_{G_2} \land E_{G_3} \land E_{G_4} | F \vdash Q_F].
$$

Analyzing these four sets in turn. First, we consider $\Pr[E_{G_1} | F \vdash Q_F].$ There are three cases for each transcript $(t, RX, AS) \in G_1$:

(i) The two intermediate values $Y$ and $Z$ derived from $F_2$ and $F_5$ will not collide with the values that have been queried in the past time. So, the probability of this case is at least

$$
\left(1 - \frac{q_f + e_3^{(l)} + |G_2F_3|}{N} \right) \left(1 - \frac{q_f + e_4^{(l)} + |G_3F_4|}{N} \right) \frac{1}{N^2}.
$$

(ii) The intermediate value $Y$ collides with some values of the past queries, but $Z$ is still “free”. So, the probability of this case is at least

$$
\left(\frac{q_f + e_3^{(l)}}{N} - \frac{\sum_{x_3 \in G_2F_3} \text{Num}_3^{(l)}(X_{l_3} \oplus k_3 \oplus x_3)}{N} \right) - \frac{q_f^2}{N^2} = \frac{1}{N^2}.
$$

(iii) This case is symmetrical to the second one, where $Z$ collides with some past values, but $Y$ is “free”. The probability is at least

$$
\left(\frac{q_f + e_4^{(l)}}{N} - \frac{\sum_{x_4 \in G_2F_3} \text{Num}_4^{(l)}(A_{l_4} \oplus k_3 \oplus x_3)}{N} \right) - \frac{(2q_f + q_e)(q_f + q_e)}{N^2} \frac{1}{N^2}.
$$
Summing over the above five cases, we have
\[
\mathbb{E}_k \left[ \Pr \left[ E_{G_1} | F \vdash Q_F \right] \right] \geq \left( 1 - \frac{q_e q_f^2}{N^2} - \frac{2q_e(2q_f + q_e)(q_f + q_e)}{N^2} \right) \frac{1}{N^2} - \frac{(q_f + 2q_e)(\beta_1 + \beta_2)}{N} \cdot \frac{1}{N^2[G_1]}.
\]

Then, we analyze \(E_{G_1^2}, E_{G_2}, \) and \(E_{G_3^2}\). The events \(E_{G_1^2}\) and \(E_{G_2}\) can be considered simultaneously. For the rest events, we need to upper-bound the corresponding "bad" events, then consider the efficiency of introducing tweak. Through this method, we can lower bound these three events. See Appendix A for more details about the proof.

For the proof, we have the results of the following three events:
\[
\Pr \left[ E_{G_2} \cap E_{G_3} | F \vdash Q_F \right] \geq \left( 1 - \Pr \left[ \text{Bad}_1(F_3) - \text{Bad}_2(F_4) \right] \right) \cdot \Pr \left[ E_{G_2} \cap E_{G_3} | -\text{Bad}_1(F_3) \cap -\text{Bad}_2(F_4) \right] \geq \left( 1 - \frac{(\beta_1 + \beta_2)(q_f + q_e)}{N} - \frac{(\beta_1 + \beta_2)\epsilon}{N^2} \right) \cdot \frac{1}{N^2[G_1]}.
\]

Finally, we sum up all four events, i.e.,
\[
p(\tau, F_1, F_6) = \Pr \left[ E_{G_1} \cap E_{G_2} \cap E_{G_3} \cap E_{G_4} | F \vdash G_F \right] \geq (1 - \theta_1)(1 - \theta_2)(1 - \theta_3) \frac{1}{N^2[G_1] + [G_2] + [G_3] + [G_4]} \geq (1 - (\theta_1 + \theta_2 + \theta_3)) \frac{1}{N^2q_e}.
\]

where \(\theta_1, \theta_2, \theta_3\) are (A1), (A2) and (A3) respectively, furthermore \(|G_1| + |G_2| + |G_3| + |G_4| = q_e\). We note that
\[
\frac{1}{N^2q_e} \sum_{i=0}^{q_e-1} \frac{1}{N^2 - i} \geq \left( 1 - \frac{q_e}{N^2} \right)^{q_e} \geq 1 - \frac{q_e^2}{N^2} \geq 1 - \frac{q_e^3}{N^2},
\]
then for (3), we have
\[
\mathbb{E}_k[\varphi(F_1, F_6, k)] \leq \left( \frac{3q_e + 2q_f}{N} \right) \frac{\beta_1 + \beta_2}{N^2} + \frac{2q_e(q_c + 2q_f)(q_c + q_f) + q_c^3}{N^2} + \frac{q_e q_f^2}{N^2} + (\beta_1 + \beta_2 + 2\beta_3)\epsilon.
\]

We know that \(\beta_1, \beta_2, \) and \(\beta_3\) depend on \((F_1, F_6)\). We consider them respectively, focusing on \(\beta_1\) firstly. For each \((t, RX, AS) \in Q_k^k(F_1, F_6)\), if \(H_{k_i}(t) \oplus R \in \text{Dom}F_1\), then it must be \(H_{k_i}(t) \oplus X \notin \text{Dom}F_2\) because of (A-2). Thus, on the condition of \(F_1 \vdash Q_{F_1}\), \(F_1(H_{k_i}(t) \oplus R)\) keeps uniform, then we have
\[
\Pr \left[ H_{k_i}(t) \oplus L \oplus F_1(H_{k_i}(t) \oplus R) \in \text{Dom}F_2 \right] \leq \frac{q_f}{N}.
\]
Therefore, \(\mathbb{E}_k[\beta_1] \leq \frac{\varphi d_f}{N}\). The analysis method of \(\beta_2\) is symmetric with \(\beta_1\), by the uniformity of \(F_6\), we have \(\mathbb{E}_k[\beta_2] \leq \frac{\varphi d_f}{N}\).
Thus, we have as claimed in (4).

Gathering all the above yields, we have

$$\Pr[X = X'] = \Pr[L \oplus F_1(H_k(t) \oplus R) = L' \oplus F_1(H_k(t') \oplus R')] \leq \varepsilon;$$

if \( t = t' \) and \( R = R' \), then it must be \( L \neq L' \), thus \( X = X' \) is impossible; if \( t = t' \) and \( L = L' \) but \( R \neq R' \), on account of \( H_k(t) \oplus R \notin \text{Dom}F_1 \), then \( F_1(H_k(t) \oplus R) \) keeps uniformly random conditioned on \( F_1 \upharpoonright Q_{F_1} \); therefore \( \Pr[X = X'] = \frac{1}{N} \). In addition, the choices of distinct pairs \((t, LR, ST)\) and \((t', LR', ST')\) are at most \( q_e^2 \). Thus, we have

$$\mathbb{E}_k[\{(t, LR, ST) : H_k(t) \oplus R \notin \text{Dom}F_1, \text{ and } \exists (t', LR', ST') \text{ s.t. } X = X'\}] \leq q_e^2 \varepsilon + q_e^2 (1 - \varepsilon) \leq q_e^2 \varepsilon + \frac{q_e^2}{N}.$$

For \( H_k(t) \oplus R \in \text{Dom}F_1 \), the number of the transcripts \((t, LR, ST)\) which meet the above conditions is \( n_{(1)}(k) \). We have

$$\mathbb{E}_k[\{(t, LR, ST) : \exists (t', LR', ST') \text{ s.t. } X = X'\}] \leq q_e^2 \varepsilon + n_{(1)}(k).$$

Symmetrically,

$$\mathbb{E}_k[\{(t, LR, ST) : \exists (t', LR', ST') \text{ s.t. } A = A'\}] \leq q_e^2 \varepsilon + n_{(6)}(k).$$

Thus, we have

$$\mathbb{E}_k[\beta_3] \leq \frac{2q_e^2}{N} + 2q_e^2 \varepsilon + n_{(1)}(k) + n_{(6)}(k).$$

Finally, \( H_k(t) \) and \( H_k(t) \) are uniform in \( 2^n \) possible choices,

$$\mathbb{E}_k[n_{(1)}(k)] = \mathbb{E}_k[n_{(6)}(k)] = \sum_{(t, LR, ST) \in Q_e} \sum_{(x_1, q_1) \in Q_{F_1}} \Pr[H_k(t) = R \oplus x_1] \leq \frac{q_e q_f}{N}.$$

Gathering all the above yields, we have

$$\mathbb{E}_{F_1, F_6, k}[\varphi(F_1, F_6, k)] \leq \frac{6q_e^2 q_f^2 + 4q_e q_f^2}{N^2} + \frac{4q_e^2 (q_e + q_f)^2}{N^2} + \frac{2q_e (q_e + 2q_f) (q_e + q_f) + q_e^3}{N^2} + \frac{q_e q_f^2}{N^2} + \frac{4q_e^2 (q_e + q_f) e}{N} + \frac{2 q_e q_f e}{N} + \frac{4 q_e (q_e + q_f) e}{N} + \frac{4 q_e^2 e^2}{N} + \frac{4 q_e^2 e^2}{N} + \frac{7 q_e^3 + 20 q_e^2 q_f + 12 q_e q_f^2}{N^2} + \frac{4 q_e^2 e + 4 q_e^2 q_f e + 4 q_e^2 e + 6 q_e q_f e}{N},$$

as claimed in (4). \( \Box \)
Now we have Lemma 2, Lemma 4, and (2), we obtain
\[
\frac{\Pr_{re}(\tau)}{\Pr_{id}(\tau)} \geq 1 - \left(\frac{3q_3q_4^2}{N^2}\right) + \mathbb{E}_k\left[\Pr\left[\text{Bad}(F_1, F_6) | F_1 \vdash Q_{f_1}, F_6 \vdash Q_{f_6}\right]\right] \\
+ \mathbb{E}_k\left[\mathbb{E}_{F_1, F_6}\left[\phi(F_1, F_6, k) | F_1 \vdash Q_{f_1}, F_6 \vdash Q_{f_6}\right]\right].
\]

For the expectation \(\mathbb{E}_k\left[\Pr\left[\text{Bad}(F_1, F_6) | F_1 \vdash Q_{f_1}, F_6 \vdash Q_{f_6}\right]\right]\), we note that \(k_3\) and \(k_4\) are uniformly picked from \(2^n\) possibilities, then
\[
\mathbb{E}_k\left[n_{(2,3)}(k)\right] = \mathbb{E}_k\left[n_{(4,5)}(k)\right] \leq \frac{q_3q_4^2}{N^2}.
\]

It has been shown that \(\mathbb{E}_k\left[n_{(1)}(k)\right] = \mathbb{E}_k\left[n_{(6)}(k)\right] \leq \frac{q_3q_4}{N^2}\). Then Lemma 3 yields
\[
\mathbb{E}_k\left[\Pr\left[\text{Bad}(F_1, F_6) | F_1 \vdash Q_{f_1}, F_6 \vdash Q_{f_6}\right]\right] \\
\leq \frac{4q_3^2q_4^2 + 5q_3q_4^2}{N^2} + \frac{2q_3q_4^2}{N} + 4q_3^2q_4^2\varepsilon^2.
\]

From all above, by Lemmas 1 and 2, we have proved the conclusion of Theorem 1.

5. Conclusions and Future Work

This paper presents a result of constructing a tweakable block cipher from the KAF construction. Our work is based on the study by Guo et al. [24], we introduce the tweak into their optimized 6-round scheme KAF in order to achieve the Beyond Birthday-Bound security. We utilize a universal hash function which is called \(\varepsilon\)-almost XOR-universal hash function, with tweak and round-key vector, we rebuild a new tweakable KAF scheme TKAF which meets the security of beyond birthday-bound. Finally, by using the H-coefficient technique [25], we prove the security requirement and obtain a better conclusion with fewer rounds. Our approach is to introduce the tweak into the first and last two rounds of Guo’s 6-round KAF structure, and utilize the universal hash function as the operation method. Can we introduce the tweak directly into the round function without using the universal hash function, and still meeting the beyond birthday-bound security? Or can we use another linear method to introduce a tweak? We leave these as future work.

Author Contributions: Conceptualization, M.J. and L.W.; methodology, M.J.; validation, M.J. and L.W.; formal analysis, M.J.; investigation, M.J.; writing—original draft preparation, M.J.; writing—review and editing, M.J. and L.W.; supervision, L.W.; project administration, L.W. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by National Key Research and Development Program of China No. 2018YFB0803400.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.
Appendix A. Proof of Lemma 5

Appendix A.1. \( \Pr [E_{G_f}|F \not\sqsubseteq Q_f] \)

Firstly, we consider the event \( E_{G_f} \), i.e., lower bounding \( \Pr [E_{G_f}|F \not\sqsubseteq Q_f] \). By the definition, there must be \( E_{G_f} = E_{G_{F^1}} \lor \ldots \lor E_{F^4} \). So, therefore, we consider to lower bounding the probability of \( E_{F^1} \) on the condition of \( E_{F^1} \lor \ldots \lor E_{F^4} \). We note that on the condition of \( E_{F^1} \lor \ldots \lor E_{F^4} \), for arbitrary \( x_3 \in \text{Ext}F_3^{(l)} \) and \( x_4 \in \text{Ext}F_4^{(l)} \), \( F_3(x_3) \) and \( F_4(x_4) \) will be considered to be “fixed”. For convenience, we denote \( x_2^{(l+1)} = H_{k_2}(t) \oplus X_{l+1} \) and \( x_5^{(l+1)} = H_{k_5}(t) \oplus A_{l+1} \); furthermore denote \( Y_{l+1} = R_{l+1} \oplus F_2(x_2^{(l+1)}) \) and \( Z_{l+1} = S_{l+1} \oplus F_5(x_5^{(l+1)}) \). Depending on the states of two intermediate values \( Y_{l+1} \) and \( Z_{l+1} \), we consider the event \( E_{F^1} \) in three cases:

- **Case 1-no collision**: \( Y_{l+1} \) and \( Z_{l+1} \) satisfy
  \[ k_3 \oplus Y_{l+1} \notin \text{Dom}F_3 \cup \text{Ext}F_3^{(l)} \cup G_2F_3 \]
  \[ k_4 \oplus Z_{l+1} \notin \text{Dom}F_4 \cup \text{Ext}F_4^{(l)} \cup G_3F_4 \]

  It holds \( F_3(k_3 \oplus Y_{l+1}) = X_{l+1} \oplus Z_{l+1} \) and \( F_4(k_4 \oplus Z_{l+1}) = Y_{l+1} \oplus A_{l+1} \);

- **Case 2-left collision**: \( Y_{l+1} \) satisfies \( k_3 \oplus Y_{l+1} \in \text{Dom}F_3 \cup \text{Ext}F_3^{(l)} \), but \( Z_{l+1} \) satisfies
  \[ k_4 \oplus Z_{l+1} \notin \text{Dom}F_4 \cup \text{Ext}F_4^{(l)} \cup G_3F_4 \]
  It holds \( F_4(k_4 \oplus Z_{l+1}) = Y_{l+1} \oplus A_{l+1} \) and \( F_3(k_3 \oplus Y_{l+1}) = X_{l+1} \oplus Y_{l+1} \).

- **Case 3-right collision**: \( Z_{l+1} \) satisfies \( k_4 \oplus Z_{l+1} \in \text{Dom}F_4 \cup \text{Ext}F_4^{(l)} \), but \( Y_{l+1} \) satisfies
  \[ k_3 \oplus Y_{l+1} \notin \text{Dom}F_3 \cup \text{Ext}F_3^{(l)} \cup G_2F_3 \]
  It holds \( F_2(x_2^{(l+1)}) = Y_{l+1} \oplus R_{l+1} \) and \( F_3(k_3 \oplus Y_{l+1}) = Z_{l+1} \oplus X_{l+1} \).

By these, accumulating all probabilities of above three cases, we have

\[ \Pr [E_{F^1}|E_{F^1} \lor \ldots \lor E_{F^4} \not\sqsubseteq Q_f] \]

Now we consider these three cases respectively.

Appendix A.1.1. Case 1

For \((t, R_{l+1}X_{l+1}A_{l+1}S_{l+1}) \in G_f\), by definition, we have \( x_2^{(l+1)} = H_{k_2}(t) \oplus X_{l+1} \notin \text{Dom}F_2 \). With tuples in \( \mathcal{Q}_E(F_1, F_6) \), \( X_{l+1} \) does not collide with other corresponding positions since \( |TD(X_{l+1})| = 1 \). Thus Thus, \( F_2(x_2^{(l+1)}) \) remains uniformly random on the condition of \( E_{F^1} \lor \ldots \lor E_{F^4} \). Moreover, \( \Pr [k_3 \oplus Y_{l+1} \in \text{Dom}F_3 \cup \text{Ext}F_3^{(l)} \cup G_2F_3] \leq q_f + q_3^{(l+1)} / N \). Symmetrically, we have \( \Pr [k_4 \oplus Z_{l+1} \in \text{Dom}F_4 \cup \text{Ext}F_4^{(l)} \cup G_3F_4] \leq q_f + q_4^{(l+1)} / N \). Then, the probability that these two equations \( F_3(k_3 \oplus Y_{l+1}) = X_{l+1} \oplus Z_{l+1} \) and \( F_4(k_4 \oplus Z_{l+1}) = Y_{l+1} \oplus A_{l+1} \) are simultaneously fulfilled is \( \frac{1}{N^2} \).

From above,

\[ \Pr [E_{F^1} \land \text{CASE 1}|E_{F^1} \land \ldots \land E_{F^4} \not\sqsubseteq Q_f] \geq \left( 1 - q_f + q_3^{(l+1)} / N \right) \left( 1 - q_f + q_4^{(l+1)} / N \right) \frac{1}{N^2} \]

Appendix A.1.2. Case 2

We consider the opposite case of CASE 2, and upper-bound the probability on this condition. Let \( p_{coll} \) be the probability of the contrary case. We have
\(p_{\text{coll}} = \Pr\left[ \exists x_3 \in \text{Dom}\, F_3 \cup \text{Ext}\, F_3^{(l)}, \exists x_4 \in \text{Dom}\, F_4 \cup \text{Ext}\, F_4^{(l)} \cup G_3 \, F_4 : \text{Coll}(x_3, x_4)|E_1 \land \ldots \land E_1 \land F \vdash Q_F, \right]\)

where \(\text{Coll}(x_3, x_4)\) stands for the collision event:

\[X_{i+1} \oplus y_3 = (k_4 \oplus x_4) \land R_{i+1} \oplus F_2(x_2^{(l+1)}) = k_3 \oplus x_3,\]

Then, we consider five subcases of the opposite Case 2 respectively, and upper-bound for each in turn.

- **Subcase 2.1:** \(x_3 \in \text{Dom}\, F_3 \cup \text{Ext}\, F_3^{(l)}, \text{ and } x_4 \in G_3 \, F_4\).
  
  For each \(x_4 \in G_3 \, F_4\), by definition, we have the number of \(x_3 \in \text{Dom}\, F_3 \cup \text{Ext}\, F_3^{(l)}\) which satisfies the collision \(X_{i+1} \oplus y_3 = k_4 \oplus x_4\) is \(\sum_{x_4 \in G_3 \, F_4} \text{Num}^{(l)}_3(X_{i+1} \oplus k_4 \oplus x_4)\). In addition, similar with Case 1, we can still deem \(F_2(x_2^{(l+1)})\) as uniformly random. Thus, it holds \(\Pr[F_2(x_2^{(l+1)}) = R_{i+1} \oplus k_3 \oplus x_3] \leq \frac{1}{N}\). Therefore, the upper bound of Subcase 2.1 is

\[
\sum_{x_3 \in \text{Dom}\, F_3 \cup \text{Ext}\, F_3^{(l)}} \Pr[\text{Coll}(x_3, x_4)|E_1 \land \ldots \land E_1 \land F \vdash Q_F] \leq \frac{\sum_{x_4 \in G_3 \, F_4} \text{Num}^{(l)}_3(X_{i+1} \oplus k_4 \oplus x_4)}{N}.
\]

- **Subcase 2.2:** \(x_3 \in \text{Dom}\, F_3\), and \(x_4 \in \text{Dom}\, F_4\). Define a key-dependent value:

\[
\text{Num}^{+}_{3,4}(k, X) \overset{\text{def}}{=} |\{(x_3, y_3), (x_4, y_4)\} \in Q_{F_3} \times Q_{F_4} : k_4 = X \oplus y_3 \oplus x_4\}|.
\]

Then we have the quantity of \((x_3, x_4)\) which satisfies the collision condition \(X_{i+1} \oplus y_3 = k_4 \oplus x_4\) is \(\text{Num}^{+}_{3,4}(k, X_{i+1})\). Same as Subcase 2.1,

\[
\Pr[F_2(x_2^{(l+1)}) = R_{i+1} \oplus k_3 \oplus x_3] \leq \frac{1}{N}.
\]

Thus, we have

\[
\sum_{x_3 \in \text{Dom}\, F_3 \atop x_4 \in \text{Dom}\, F_4} \Pr[\text{Coll}(x_3, x_4)|E_1 \land \ldots \land E_1 \land F \vdash Q_F] \leq \frac{\text{Num}^{+}_{3,4}(k, X_{i+1})}{N}.
\]

It can be seen, \(k_4\) is uniform in \(N\) values. So, the expectation of \(\text{Num}^{+}_{3,4}(k, X_{i+1})\) is at most \(\frac{q^2}{N}\). Thus Thus, the upper bound of the probability on the condition of Subcase 2.2 is at most \(\frac{q^2}{N^2}\).

- **Subcase 2.3:** \(x_3 \in \text{Dom}\, F_3\), and \(x_4 \in \text{Ext}\, F_4^{(l)} \setminus \text{Dom}\, F_4\). By definition, we write

\[
\sum_{x_3 \in \text{Dom}\, F_3 \atop x_4 \in \text{Ext}\, F_4^{(l)} \setminus \text{Dom}\, F_4} \Pr[\text{Coll}(x_3, x_4)|E_1 \land \ldots \land E_1 \land F \vdash Q_F] = \sum_{x_3 \in \text{Dom}\, F_3 \atop i = 1, \ldots , l} \text{sgn}(i) \cdot \Pr[\text{Coll}(x_3, x_4^{(i)})|E_1 \land \ldots \land E_1 \land F \vdash Q_F],
\]

where $x_4^{(i)} = k_4 \oplus Z_i$, and for $i$-th tuple $(t, R_i, X_i, A_i, S_i) \in G_4$, we have $Z_i = S_i \oplus F_5(H_k(t) \oplus A_i)$. In addition, $\text{sgn}(i) = 1$ if and only if $i$ is the smallest index that satisfies $x_4^{(i)} \in \text{ExtF}_4 \setminus \text{DomF}_4$, since $x_4^{(i)} \notin \text{ExtF}_4^{(i-1)}$.

First, we focus on $\text{Pr}\left[\text{Coll}(x_3, x_4^{(i)}) | E_i \wedge \ldots \wedge E_1 \wedge F \vdash Q_F\right]$. Considering the probability on the condition that $E_i$ fits into Case 1, 2 and 3. It can be seen that if $E_i$ fits into Case 3, then we have $x_4^{(i)} \in \text{DomF}_4$, it contradicts the Subcase 2.3. Let $y_3 = \text{ImgF}_3(x_3)$, write $Y_i = R_i \oplus F_2(H_k(t) \oplus X_i)$.

(i) $E_i$ fits into Case 1

We derive $Z_i$ from $Z_i = S_i \oplus F_5(H_k(t) \oplus A_i)$, and $F_5(x_3^{(i)})$ keeps uniform. Then we have

$$\text{Pr}\left[X_{i+1} \oplus y_3 = (k_4 \oplus x_4^{(i)})\right] = \text{Pr}[X_{i+1} \oplus y_3 = Z_i] = \text{Pr}\left[F_5(x_3^{(i)}) = X_{i+1} \oplus y_3 \oplus S_i\right] \leq \frac{1}{N}.$$

Furthermore, we have $\text{Pr}\left[F_2(x_2^{(i)}) = R_{i+1} \oplus k_3 \oplus x_3\right] \leq \frac{1}{N}$. Thus

$$\text{Pr}\left[\text{Coll}(x_3, x_4^{(i)}) | E_i \text{ fits into Case 1} \wedge E_1 \wedge \ldots \wedge E_1 \wedge F \vdash Q_F\right] \leq \frac{1}{N^2}.$$

(ii) $E_i$ fits into Case 2

Let $x_3^{(i)} = k_3 \oplus Y_i$, $y_3^{(i)} = F_3(x_3^{(i)})$. We have $X_{i+1} \oplus y_3 = Z_i = X_i \oplus y_3^{(i)}$. By definition, the number of choices for such $y_3^{(i)}$ is $\text{Num}_3^{(i)}(X_{i+1} \oplus y_3 \oplus X_i)$. Furthermore, for these choices of $y_3^{(i)}$, the probability of the following two collisions is at most $\frac{1}{N}$, i.e.,

$$R_i \oplus F_2(H_k(t) \oplus X_i) = k_3 \oplus x_3^{(i)} = R_{i+1} \oplus F_2(H_k(t) \oplus X_{i+1}) = k_3 \oplus x_3.$$

Thus

$$\text{Pr}\left[\text{Coll}(x_3, x_4^{(i)}) | E_i \text{ fits into Case 2} \wedge E_1 \wedge \ldots \wedge E_1 \wedge F \vdash Q_F\right] \leq \frac{\text{Num}_3^{(i)}(X_{i+1} \oplus y_3 \oplus X_i)}{N^2}.$$

From the above,

$$\sum_{x_3 \in \text{DomF}_3} \sum_{x_4 \in \text{ExtF}_4^{(i)} \setminus \text{DomF}_4} \text{Pr}[\text{Coll}(x_3, x_4) | E_1 \wedge \ldots \wedge E_1 \wedge F \vdash Q_F] \leq \sum_{x_3 \in \text{DomF}_3} \sum_{i=1, \ldots, l} \text{sgn}(i) \cdot \frac{\text{Num}_3^{(i)}(X_{i+1} \oplus y_3 \oplus X_i)}{N^2} \leq \sum_{x_3 \in \text{DomF}_3} q_f + e_3^{(i)} \frac{q_f + q_e}{N^2} \leq \frac{q_f q_f + q_e}{N^2}.$$
• **Subcase 2.4:** $x_3 \in \text{Ext} F_3^{(i)} \setminus \text{Dom} F_3$, and $x_4 \in \text{Dom} F_4$. By definition, we write

$$
\sum_{x_3 \in \text{Ext} F_3^{(i)} \setminus \text{Dom} F_3 \atop x_4 \in \text{Dom} F_4} \text{Pr}[\text{Coll}(x_3, x_4) | E_1 \wedge \ldots \wedge E_1 \wedge F \vdash q_F] 
= \sum_{i = 1, \ldots, l} \text{sgn}'(i) \cdot \text{Pr}[\text{Coll}(x_3^{(i)}, x_4) | E_1 \wedge \ldots \wedge E_1 \wedge F \vdash q_F],
$$

where $x_3^{(i)} = k_i \oplus Y_i$, and for $i$-th tuple $(t, R_i, X_i, A_i) \in G_4$, we have $Y_i = R_i \oplus F_2(H_{k_i}(t) \oplus X_i)$. In addition, $\text{sgn}'(i) = 1$ if and only if $i$ is the smallest index that satisfies $x_3^{(i)} \in \text{Ext} F_3^{(i)} \setminus \text{Dom} F_3$, since $x_3^{(i)} \notin \text{Ext} F_3^{(i-1)}$.

First, we focus on $\text{Pr}[\text{Coll}(x_3^{(i)}, x_4) | E_1 \wedge \ldots \wedge E_1 \wedge F \vdash q_F]$. Let $y_4 = \text{Img} F_4(x_4)$, write $Z_i = S_i \oplus F_5(H_{k_i}(t) \oplus A_i)$. That is $y_3^{(i)} = X_i \oplus Z_i$. Thus, the collision $X_{i+1} \oplus y_3^{(i)} = (k_4 \oplus x_4)$ can be seen as $X_{i+1} \oplus X_i = Z_i \oplus (k_4 \oplus x_4)$. Same as **Subcase 2.3**, we only need to consider two cases on $E_i$.

(i) $E_i$ fits into **Case 1**

We know that $Z_i = S_i \oplus F_5(H_{k_i}(t) \oplus A_i)$ and $F_5(H_{k_5}(t) \oplus A_i)$ keep uniform. Then it holds

$$
\text{Pr}[X_{i+1} \oplus X_i = Z_i \oplus (k_4 \oplus x_4)] = \text{Pr}[F_5(H_{k_5}(t) \oplus A_i) = S_i \oplus X_{i+1} \oplus X_i \oplus k_4 \oplus x_4] \leq \frac{1}{N}. 
$$

Then, we have $\text{Pr}[F_2(H_{k_2}(t) \oplus X_{i+1}) = R_{i+1} \oplus k_3 \oplus x_3^{(i)}] \leq \frac{1}{N}$. Thus

$$
\text{Pr}[\text{Coll}(x_3^{(i)}, x_4) | E_i \text{ fits into Case 1 } \wedge \ldots \wedge E_1 \wedge F \vdash q_F)] \leq \frac{1}{N^2}.
$$

(ii) $E_i$ fits into **Case 3**

Let $x_4^{(i)} = k_4 \oplus Z_i$. We have $X_{i+1} \oplus X_i = x_4^{(i)} \oplus x_4$ because of $X_{i+1} \oplus X_i = Z_i \oplus k_4 \oplus x_4$. We note that if $X_{i+1}$, $X_i$ and $x_4$ are “fixed”, then the possibility of choices of $x_4^{(i)}$ is at most 1. Therefore, if $Y_{i+1}$ collides with $x_3^{(i)}$, the following two collisions have to happen:

$$
S_i \oplus F_5(H_{k_5}(t) \oplus A_i) = k_4 \oplus x_4^{(i)}, R_i \oplus F_2(H_{k_2}(t) \oplus X_{i+1}) = k_3 \oplus x_3^{(i)}. 
$$

Thus

$$
\text{Pr}[\text{Coll}(x_3^{(i)}, x_4) | E_i \text{ fits into Case 3 } \wedge \ldots \wedge E_1 \wedge F \vdash q_F)] \leq \frac{1}{N^2}.
$$

According to **Subcase 2.3**, we have

$$
\sum_{x_3 \in \text{Ext} F_3^{(i)} \setminus \text{Dom} F_3 \atop x_4 \in \text{Dom} F_4} \text{Pr}[\text{Coll}(x_3, x_4) | E_1 \wedge \ldots \wedge E_1 \wedge F \vdash q_F] 
\leq \sum_{i = \ldots, l} \text{sgn}'(i) \cdot \frac{1}{N^2} \leq \frac{q_{\text{rel}}}{N^2} \leq \frac{q_{\text{rel}}}{N^2}.
$$
Subcase 2.5: $x_3 \in \text{Ext}_3 \backslash \text{Dom}_3$, and $x_4 \in \text{Ext}_4 \backslash \text{Dom}_4$. By definition, we write

$$
\sum_{x_3 \in \text{Ext}_3 \backslash \text{Dom}_3} \sum_{x_4 \in \text{Ext}_4 \backslash \text{Dom}_4} \text{Pr}[\text{Coll}(x_3, x_4)|E_1 \land \ldots \land E_1 \land F \vdash Q_F]
$$

where $x_3^{(i)} = k_3 \oplus Y_i$, and for $i$-th tuple $(t, R, X_i, A_i, S_i) \in \mathcal{G}_4$, we have $Y_i = R_i \oplus F_2(H_{k_2}(t) \oplus X_i)$. In addition, $\text{sgn}(i) = 1$ if and only if $i$ is the smallest index that satisfies $x_3^{(i)} \in \text{Ext}_3 \backslash \text{Dom}_3$, since $x_3^{(i)} \notin \text{Ext}_3^{(i-1)}$. In addition, $x_4^{(j)} = k_4 \oplus Z_j$, and for $j$-th tuple $(t, R, X_j, A_j, S_j) \in \mathcal{G}_4$, we have $Z_j = S_j \oplus F_3(H_{k_3}(t) \oplus A_j)$. In addition, $\text{sgn}'(j) = 1$ if and only if $j$ is the smallest index that satisfies $x_4^{(j)} \in \text{Ext}_4 \backslash \text{Dom}_4$, since $x_4^{(j)} \notin \text{Ext}_4^{(j-1)}$.

(i) When $j > i$, due to $X_{i+1} \oplus y_3^{(i)} = X_j \oplus y_3^{(i)}$, according to Subcase 2.3, the number of choices for such $y_3^{(i)}$ is $\text{Num}_3^{(i)}(X_{i+1} \oplus y_3^{(i)} \oplus X_j)$. Furthermore, for each $(x_3^{(i)}, x_4^{(j)})$, the upper bound of the probability is $\frac{\text{Num}_3^{(i)}(X_{i+1} \oplus y_3^{(i)} \oplus X_j)}{N^2}$.

(ii) When $i > j$, due to $X_{i+1} \oplus X_i = x_4^{(i)} \oplus x_4^{(j)}$, according to Subcase 2.4, the upper bound of the probability for each $(x_3^{(i)}, y_3^{(j)})$ is $\frac{1}{N^2}$.

To sum up,

$$
\sum_{x_3 \in \text{Ext}_3 \backslash \text{Dom}_3} \sum_{x_4 \in \text{Ext}_4 \backslash \text{Dom}_4} \text{Pr}[\text{Coll}(x_3, x_4)|E_1 \land \ldots \land E_1 \land F \vdash Q_F]
$$

$$
\leq \sum_{j=1}^{l} \sum_{i=1}^{l} \frac{\text{Num}_3^{(i)}(X_{i+1} \oplus y_3^{(i)} \oplus X_j)}{N^2}
$$

$$
\leq \sum_{j=1}^{l} \frac{q_f + e_3^{(j)}}{N^2} \leq \frac{q_f(q_f + q_e)}{N^2}.
$$

Summing over all five subcases: We have

$$
\mathbb{E}_k[\text{pcoll}] \leq \sum_{x_4 \in \mathcal{G}_4} \frac{\text{Num}_3^{(i)}(X_{i+1} \oplus k_4 \oplus x_4)}{N} + \frac{q_f^2}{N^2} + \frac{(q_f + q_e)(q_f + q_e)}{N^2}.
$$

The five cases above are opposite conditions to Case 2. Moreover, if it holds $(t, R_{i+1}X_{i+1}, A_{i+1}S_{i+1}) \in \mathcal{G}_4$, then we have (i) $x_3^{(i+1)} \notin \text{Dom}_3$ and $|\mathcal{ID}(A_{i+1})| = 1$, that implies the position of $x_3^{(i+1)}$ can be deemed as “new”.

For these arguments above, we have

$$
\mathbb{E}_4\left[\text{Pr}[E_{i+1} \land \text{CASE 2} | E_1 \land \ldots \land E_1 \land F \vdash Q_F]\right]
$$

$$
\geq \left(\frac{q_f + e_3^{(i)}}{N} - \sum_{x_4 \in \mathcal{G}_4} \frac{\text{Num}_3^{(i)}(X_{i+1} \oplus k_4 \oplus x_4)}{N} - \frac{q_f^2}{N^2} - \frac{(q_f + q_e)(q_f + q_e)}{N^2}\right) \cdot 1.
$$
Appendix A.1.3. Case 3

In this case, if it holds \( x_2^{(l+1)} \notin \text{Dom}.F_2 \) and \( x_3 = k_3 \oplus Y_{l+1} \notin \text{Dom}.F_3 \cup \text{Ext}.F_3^{(l)} \cup \text{G}_2.F_3 \), then we have

\[
\text{Pr}[\text{TKAF extends } (t, R_t X_{l+1}, A_{l+1} S_{l+1})] = \frac{\text{Pr}\left[F_2(x_2^{(l+1)}) = R_{l+1} \oplus Y_{l+1} \land F_3(x_3) = X_{l+1} \oplus Z_{l+1}\right]}{N_2} = \frac{1}{N_2}
\]

With the similar analysis of Case 2, we denote

\[
p_{\text{coll}} = \sum_{x_3 \in \text{Dom}.F_3 \cup \text{Ext}.F_3^{(l)} \cup \text{G}_2.F_3, x_4 \in \text{Dom}.F_4 \cup \text{Ext}.F_4^{(l)}} \text{Pr}(|\text{Coll}(x_3, x_4)| \land \ldots \land E_1 \land F \vdash Q_F |)
\]

Also, we consider five subcases in turn.

- **Subcase 3.1:** \( x_3 \in \text{G}_2.F_3, \) and \( x_4 \in \text{Dom}.F_4 \cup \text{Ext}.F_4^{(l)} \). On this condition, as the constraint \( A_{l+1} + y_4 = k_3 \oplus x_3 \), we have

\[
\sum_{x_3 \in \text{G}_2.F_3, x_4 \in \text{Dom}.F_4 \cup \text{Ext}.F_4^{(l)}} \text{Pr}(|\text{Coll}(x_3, x_4)| \land \ldots \land E_1 \land F \vdash Q_F) \leq \sum_{x_3 \in \text{G}_2.F_3} \frac{\text{Num}_4^{(l)}(A_{l+1} \oplus k_3 \oplus x_3)}{N}
\]

where \( \text{Num}_4^{(l)}(y_4) = |\{x_4 \in \text{Dom}.F_4 \cup \text{Ext}.F_4^{(l)} : F_4(x_4) = y_4\}| \).

- **Subcase 3.2:** \( x_3 \in \text{Dom}.F_3, \) and \( x_4 \in \text{Dom}.F_4 \). Define a key-dependent value:

\[
\text{Num}_{3,4}^{-1}(k, A) \overset{\text{def}}{=} \left|\left\{((x_3, y_3), (x_4, y_4)) \in Q_{F_3} \times Q_{F_4} : k_3 = A \oplus y_4 \oplus x_3\right\}\right|
\]

On account of the uniformity of \( k_3 \) in \( N \) choices, we have

\[
\begin{aligned}
\mathbb{E}_k\left[\sum_{x_3 \in \text{Dom}.F_3, x_4 \in \text{Dom}.F_4} \text{Pr}(|\text{Coll}(x_3, x_4)| \land \ldots \land E_1 \land F \vdash Q_F)\right] &\leq \mathbb{E}_k\left[\frac{\text{Num}_{3,4}^{-1}(k, A_{l+1})}{N}\right] \leq \frac{q_f^2}{N^2}.
\end{aligned}
\]

- **Subcase 3.3:** \( x_3 \in \text{Ext}.F_3^{(l)} \setminus \text{Dom}.F_3, \) and \( x_4 \in \text{Dom}.F_4 \). By definition, we write

\[
\sum_{x_3 \in \text{Ext}.F_3^{(l)} \setminus \text{Dom}.F_3, x_4 \in \text{Dom}.F_4} \text{Pr}(|\text{Coll}(x_3, x_4)| \land \ldots \land E_1 \land F \vdash Q_F) = \sum_{i = 1, \ldots, I} \text{sgn}'(i) \cdot \text{Pr}\left[\text{Coll}(x_3^{(i)}, x_4) | E_1 \land \ldots \land E_1 \land F \vdash Q_F\right],
\]

where \( x_3^{(i)} = k_3 \oplus Y_{i} \), and for \( i \)-th tuple \((t, R_t X_i, A_i S_i) \in G_4\), we have \( Y_i = R_i \oplus F_2(H_{k_3}(i) \oplus X_i) \). In addition, \( \text{sgn}'(i) = 1 \) if and only if \( i \) is the smallest index that satisfies \( x_3^{(i)} \in \text{Ext}.F_3^{(l)} \setminus \text{Dom}.F_3 \), since \( x_3^{(i)} \notin \text{Ext}.F_3^{(l-1)} \). Similar with Subcase 2.3,
(i) E_i fits into CASE 1
We have
\[ \Pr\left[ \text{Coll}(x_3^{(i)}, x_4) \mid E_i \text{ fits into CASE 1} \land E_1 \land \ldots \land E_k \land F \vdash Q_F \right] \leq \frac{1}{N^2}. \]

(ii) E_i fits into CASE 3
We have \( A_{l+1} \oplus y_4 = A_i \oplus y_4^{(i)} \). Therefore,
\[ \Pr\left[ \text{Coll}(x_3^{(i)}, x_4) \mid E_i \text{ fits into CASE 3} \land E_1 \land \ldots \land E_k \land F \vdash Q_F \right] \]
\[ \leq \frac{\text{Num}_{4}^{(i)} (A_{l+1} \oplus y_4 \oplus A_i)}{N^2}. \]

From above with the similar calculation, we have
\[ \sum_{x_3 \in \text{Ext}F_3} \Pr[\text{Coll}(x_3, x_4) \mid E_1 \land \ldots \land E_k \land F \vdash Q_F] \]
\[ \leq \sum_{x_4 \in \text{Dom}F_4} \sum_{i = 1}^{l} \text{sgn}(i) \cdot \frac{\text{Num}_{4}^{(i)} (A_{l+1} \oplus y_4 \oplus A_i)}{N^2} \leq \frac{q_f (q_f + q_e)}{N^2}. \]

- **Subcase 3.4:** \( x_3 \in \text{Dom}F_3, \) and \( x_4 \in \text{Ext}F_4 \setminus \text{Dom}F_4. \) By definition, we write
\[ \sum_{x_3 \in \text{Dom}F_3} \Pr[\text{Coll}(x_3, x_4) \mid E_1 \land \ldots \land E_k \land F \vdash Q_F] \]
\[ = \sum_{x_4 \in \text{Dom}F_4} \sum_{i = 1}^{l} \text{sgn}(i) \cdot \Pr[\text{Coll}(x_3, x_4^{(i)}) \mid E_1 \land \ldots \land E_k \land F \vdash Q_F], \]

It also holds \( \Pr[\text{Coll}(x_3, x_4^{(i)}) \mid E_i \text{ fits into CASE 1} \land E_1 \land \ldots \land E_k \land F \vdash Q_F] \leq \frac{1}{N^2}. \) When \( E_i \) fits into CASE 2, due to \( A_{l+1} \oplus A_i = x_3^{(i)} \oplus x_3 \), we have
\[ \Pr[\text{Coll}(x_3, x_4^{(i)}) \mid E_i \text{ fits into CASE 2} \land E_1 \land \ldots \land E_k \land F \vdash Q_F] = \frac{1}{N^2}. \]

Therefore,
\[ \sum_{x_3 \in \text{Dom}F_3} \Pr[\text{Coll}(x_3, x_4) \mid E_1 \land \ldots \land E_k \land F \vdash Q_F] \leq \frac{q_f}{N^2} \leq \frac{q_f q_e}{N^2}. \]
• **Subcase 3.5:** \( x_3 \in \text{Ext}\mathcal{F}_3 \setminus \text{Dom}\mathcal{F}_3 \), and \( x_4 \in \text{Ext}\mathcal{F}_4 \setminus \text{Dom}\mathcal{F}_4 \). Similar to Subcase 2.5, we have

\[
\sum_{x_3 \in \text{Ext}\mathcal{F}_3 \setminus \text{Dom}\mathcal{F}_3} \sum_{x_4 \in \text{Ext}\mathcal{F}_4 \setminus \text{Dom}\mathcal{F}_4} \Pr[\text{Coll}(x_3, x_4) | E_1 \land \ldots \land E_1 \land F \vdash Q_F] \\
\leq \sum_{j=1}^{l=1} \sum_{i=1}^{l} \frac{\text{Num}_4^{(l)} (A_{i+1} \oplus y_4 \oplus A_j)}{N^2} \\
\leq \sum_{j=1}^{l=1} \frac{q_f + q_e^{(l)}}{N^2} \leq q_e(q_f + q_e) \frac{N^2}{N^2}.
\]

• **Summing over all five subcases:** We have

\[
\mathbb{E}_k[\Pr[E_{l+1} \land \text{CASE 3}|E_1 \land \ldots \land E_1 \land F \vdash Q_F]] \\
\geq \left( \frac{q_f + e_4^{(l)}}{N} - \frac{\sum_{x_3 \in \text{Dom}\mathcal{F}_3} \text{Num}_4^{(l)} (A_{i+1} \oplus k_3 \oplus x_3)}{N} - \frac{(2q_f + q_e)(q_f + q_e)}{N^2} \right) \frac{1}{N^2}.
\]

Appendix A.1.4. Conclusions of \( E_{\bar{G}_1} \)

Summing over all the three cases:

\[
\mathbb{E}_k \left[ \Pr[E_{l+1} | E_1 \land \ldots \land E_1 \land F \vdash Q_F] \right] \\
\geq \left( 1 - \frac{q_f + e_3^{(l)} + |G_2 F_3|}{N} \right) \left( 1 - \frac{q_f + e_4^{(l)} + |G_2 F_4|}{N} \right) \\
+ \frac{2q_f + e_3^{(l)} + e_4^{(l)}}{N} - \frac{q_f^2}{N^2} - \frac{2(2q_f + q_e)(q_f + q_e)}{N^2} \\
- \frac{1}{N} \sum_{x_3 \in \text{Dom}\mathcal{F}_3} \text{Num}_3^{(l)} (X_{i+1} \oplus k_4 \oplus x_4) - \frac{1}{N} \sum_{x_3 \in \text{Dom}\mathcal{F}_4} \text{Num}_4^{(l)} (A_{i+1} \oplus k_3 \oplus x_3) \right) \frac{1}{N^2}.
\]

We denote

\[
B_l = \frac{1}{N} \left( \sum_{x_3 \in \text{Dom}\mathcal{F}_3} \text{Num}_3^{(l)} (X_{i+1} \oplus k_4 \oplus x_4) + \sum_{x_3 \in \text{Dom}\mathcal{F}_4} \text{Num}_4^{(l)} (A_{i+1} \oplus k_3 \oplus x_3) \right),
\]

|\( G_2 F_3 | \leq |G_2 | = \beta_1, |G_3 F_4 | \leq |G_3 | = \beta_2, \) and |\( G_1 | \leq q_e \). Then it holds

\[
\mathbb{E}_k \left[ \Pr[E_{\bar{G}_1} | F \vdash Q_F] \right] \\
\leq \prod_{l=0}^{|G_1| - 1} \left( 1 - \frac{q_f^2}{N^2} - \frac{2q_e(2q_f + q_e)(q_f + q_e)}{N^2} - \frac{|G_2 F_3 | + |G_3 F_4 |}{N} - B_l \right) \cdot \frac{1}{N^{2|G_1|}} \\
\geq \left( 1 - \frac{q_e q_f^2}{N^2} - \frac{2q_e(2q_f + q_e)(q_f + q_e)}{N^2} - \frac{q_e(q_f + q_e)}{N} - \sum_{l=0}^{q_e - 1} B_l \right) \cdot \frac{1}{N^{2|G_1|}}.
\]

Secondly, we consider \( \sum_{l=0}^{q_e - 1} B_l \). By definition, we have

\[
\sum_{y_3 \in \{0, 1\}^n} \text{Num}_3^{(l)} (y_3) = q_f + e_3^{(l)} \leq q_f + q_e \\
\sum_{y_4 \in \{0, 1\}^n} \text{Num}_4^{(l)} (y_4) = q_f + e_4^{(l)} \leq q_f + q_e.
\]
Thus
\[
\sum_{l=0}^{q_e-1} \sum_{x_4 \in G_2F_4} \text{Num}_3^{(l)}(X_{l+1} \oplus k_4 \oplus x_4) \leq \sum_{x_4 \in G_2F_4} (q_f + q_e) \leq (q_f + q_e)\beta_2.
\]

Similarly,
\[
\sum_{l=0}^{q_e-1} \sum_{x_3 \in G_2F_3} \text{Num}_4^{(l)}(A_{l+1} \oplus k_3 \oplus x_3) \leq (q_f + q_e)|G_2F_3| \leq (q_f + q_e)\beta_1.
\]

Finally, we have the upper bound
\[
E_k \left[ \Pr \left[ E_{G_1} | F \vdash \forall F \right] \right] \geq \left( 1 - \frac{q_eq_f^2}{N^2} - \frac{2q_e(2q_f + q_e)(q_f + q_e)}{N^2} \right) \frac{1}{N^2|G_1|}.
\] (A1)

Appendix A.2. Pr\[E_{G_2} \wedge E_{G_3} | E_{G_1} \wedge F \vdash G_F\]

Next, we analyze the event $E_{G_2} \wedge E_{G_3}$, we firstly focus on $E_{G_2}$. Define the “bad” event on this condition, we denote by Bad$_1(F_3)$: there exists $(t, RX, AS) \in G_2$, one of the following conditions is fulfilled:

(i) $x_3 = k_4 \oplus X \oplus F_3(x_3) \in \text{Dom}F_4$, where $x_3 = k_3 \oplus R \oplus \text{Img}F_2(H_{k_2}(t) \oplus X)$;

(ii) there exists $(t', R'X', A'S') \in G_2$, such that $X \oplus F_3(x_3) = X' \oplus F_3(x_3')$, where $x_3' = k_3 \oplus R' \oplus \text{Img}F_2(H_{k_2}(t') \oplus X')$;

(iii) there exists $(t'', R''X'', A''S'') \in G_1 \cup G_3$, such that $X \oplus F_3(x_3) = S'' \oplus F_5(H_{k_5}(t'') \oplus A'')$.

We note that for each $(t, RX, AS) \in G_2$, we have $x_3 \not\in \text{Dom}F_3$ (for the condition of $\neg\text{Bad}(F_1, F_6)$) and $x_3 \not\in \text{Ext}F_3^{G_1}$ (for the analysis of $E_{G_1}$). Then, on the condition of $E_{G_1} \wedge F_3 \vdash G_F$, the values of function $F_3(x_3)$ keep uniform. Thus, for $(t, RX, AS)$:

(i) the probability of condition (i) fulfilled is at most $\frac{q_e}{N}$;

(ii) for each $(t', R'X', A'S') \in G_2$, if the corresponding $x_3 \not= x_3'$, we have
\[
\Pr \left[ X \oplus F_3(x_3) = X' \oplus F_3(x_3') \right] \leq \frac{1}{N};
\]

If the two tuples are distinct, i.e., $(t, RX, AS) \not= (t', R'X', A'S')$: (a) $t \not= t'$, $X = X'$, and $x_3 = x_3'$, then $\Pr \left[ X \oplus F_3(x_3) = X' \oplus F_3(x_3') \right] \leq \varepsilon$; (b) if $t = t'$, $X \not= X'$, and $x_3 = x_3'$, then it must be $X \oplus F_3(x_3) \not= X' \oplus F_3(x_3')$.

(iii) for each $(t'', R''X'', A''S'') \in G_1 \cup G_3$, we have
\[
\Pr \left[ X \oplus F_3(x_3) = S'' \oplus F_5(H_{k_5}(t'') \oplus A'') \right] \leq \frac{1}{N}.
\]

Summing up the above, we have the probability of Bad$_1(F_3)$:
\[
\Pr \left[ \text{Bad}_1(F_3) | E_{G_1} \wedge F \vdash Q_F \right] \leq \frac{|G_2| \cdot (q_f + |G_1| + |G_2| + |G_3|)}{N} + |G_2| \cdot \varepsilon
\]
\[
\leq \frac{\beta_1(q_f + q_e)}{N} + \beta_1 \cdot \varepsilon.
\]

We can see that if Bad$_1(F_3)$ does not happen, there are $|G_2|$ values $Z_1, \ldots, Z_{|G_2|}$ in $G_2$ which are distinct (otherwise (ii) is fulfilled). In addition, $F_4(k_4 \oplus Z_1), \ldots, F_4(k_4 \oplus Z_{|G_2|})$ are all undetermined (otherwise (i) and (iii) are fulfilled).
Moreover, at the “right” part, there are also $|G_2|$ values $A_1, \ldots, A_{|G_2|}$, such that $F_5(H_{k_5}(t) \oplus A_1), \ldots, F_5(H_{k_5}(t) \oplus A_{|G_2|})$ are also undetermined.

Therefore, the event $E_{G_2}$ is equivalent to $F_4$ and $F_5$ satisfying $2|G_2|$ new equations, so the probability does not exceed $\frac{1}{N^{2|G_2|}}$.

Similar to the analysis of $E_{G_2}$, we consider the event $E_{G_3}$. Likewise, we define the bad event $\text{Bad}_2(F_4)$ that there exists $(t, RX, AS) \in G_3$, one of the following conditions is fulfilled:

(i) $x_3 = k_3 + A \oplus F_4(x_4) \in \text{Dom}F_3$, where $x_4 = k_4 + S \oplus \text{Img}F_5(H_{k_5}(t) \oplus A)$, the probability is at most $\frac{2^{k_5}}{N}$; 
(ii) there exists $(t', R'X', A'S') \in G_3$, such that $A \oplus F_4(x_4) = A' \oplus F_4(x'_4)$, where $x_4' = k_4 + S' \oplus \text{Img}F_5(H_{k_5}(t') \oplus A')$, and the probability is at most $\frac{|G_3|}{N} + \varepsilon$; 
(iii) there exists $(t', R'X', A'S'X') \in G_1 \cup G_2$, such that $A \oplus F_4(x_4) = R' \oplus F_2(H_{k_2}(t') \oplus X')$, and the probability is at most $\frac{|G_1| + |G_2|}{N}$.

Thus, we have the probability of $\text{Bad}_2(F_4)$:

\[
\Pr[\text{Bad}_2(F_4)|E_{G_1} \land F \not\subset Q_F] \leq \frac{|G_3| \cdot (q_f + |G_1| + |G_2| + |G_3|)}{N} + |G_3| \cdot \varepsilon 
\leq \frac{\beta_2(q_f + q_e)}{N} + \beta_2 \cdot \varepsilon.
\]

Same as $E_{G_2}$, the event $E_{G_3}$ is equivalent to $F_2$ and $F_3$ satisfying $2|G_3|$ new equations.

Therefore, on the condition of $E_{G_1} \land F \not\subset Q_F$, we have

\[
\Pr[E_{G_2} \land E_{G_3}|E_{G_1} \land F \not\subset Q_F] \geq (1 - \Pr[\text{Bad}_1(F_3)] - \Pr[\text{Bad}_2(F_4)]) \cdot \Pr[E_{G_2} \land E_{G_3} \not\subset \text{Bad}_1(F_3) \land \text{Bad}_2(F_4)] 
\geq \left(1 - \frac{(\beta_1 + \beta_2)(q_f + q_e)}{N} - (\beta_1 + \beta_2)\varepsilon\right) \cdot \frac{1}{N^{2(|G_2| + |G_3|)}} .
\]

**Appendix A.3.** $\Pr[E_{G_1}|E_{G_1} \land E_{G_2} \land E_{G_3} \land F \not\subset Q_F]$

Thirdly, we analyze the event $E_{G_4}$. By definition, for arbitrary $(t, RX, AS) \in G_4$, we denote $x_2 = H_{k_2}(t) \oplus X$ and $x_3 = H_{k_3}(t) \oplus A$ such that $x_2 \notin \text{Dom}F_2$ and $x_3 \notin \text{Dom}F_3$. Furthermore, on the condition of $E_{G_1} \land E_{G_2} \land E_{G_3}$, and the conditions of bad event $\text{Bad}(F_1, F_5)$, the two values of functions $F_2(x_2)$ and $F_3(x_3)$ must be uniform and undetermined.

We also define the bad event $\text{Bad}_3(F_2, F_3)$ that there exists $(t, RX, AS) \in G_4$, such that $x_2$ and $x_3$ fulfill one of the following conditions:

- **left part:** consider $F_2(x_2)$:
  (i) $x_3 = k_3 + R \oplus F_2(x_2) \in \text{Dom}F_3$, on account of the randomness of $F_2(x_2)$, for each $(t, RX, AS) \in G_4$, the probability of which is at most $\frac{q_r}{N}$; 
  (ii) there exists $(t', R'X', A'S') \in G_1 \cup G_2 \cup G_3$, such that $R \oplus F_2(x_2) = R' \oplus F_2(H_{k_2}(t') \oplus X')$. For distinct two tuples in $G_4$, (a) it might be $t \neq t'$, such that $Y$ collides with some “previously-ly determined” $Y'$, whose probability of which is $\varepsilon$; (b) if $t = t'$ but $X \neq X'$ (it can not cannot be $R = R'$), by the randomness of $F_2(x_2)$, for each $(t, RX, AS) \in G_4$, the upper bound of the probability is $\frac{|G_1| + |G_2| + |G_3|}{N} + \varepsilon \leq \frac{q_r}{N} + \varepsilon$.

- **right part:** consider $F_3(x_3)$, similar to the above:
  (i) $k_4 + S \oplus F_3(x_3) \in \text{Dom}F_3$, for each $(t, RX, AS) \in G_4$, the probability of which is at most $\frac{q_s}{N}$; 
  (ii) there exists another distinct $(t', R'X', A'S') \in G_1 \cup G_2 \cup G_3$, such that $S \oplus F_3(x_3) = S' \oplus F_3(H_{k_3}(t') \oplus A')$. For each $(t, RX, AS) \in G_4$, the upper bound of the probability is $\frac{|G_1| + |G_2| + |G_3|}{N} + \varepsilon \leq \frac{q_s}{N} + \varepsilon$. 


Thus, denote $|G_4| = \beta_3$, we have

$$\Pr[E_{G_4} | E_{G_1} \wedge E_{G_2} \wedge E_{G_3} \wedge F \vdash G_F] \geq \left(1 - \frac{\Pr[\text{Bad}_3(F_2, F_3)]}{N^{2k_4}}\right) \cdot \frac{1}{N^{2k_4}} \geq \left(1 - \frac{2\beta_3(q_f + q_e)}{N} - 2\beta_3^2\right) \cdot \frac{1}{N^{2k_4}} \quad (A3)$$

References

1. Liskov, M.; Rivest, R.L.; Wagner, D. Tweakable block ciphers. In Proceedings of the Annual International Cryptology Conference, Santa Barbara, CA, USA, 18–22 August 2002; Springer: Berlin/Heidelberg, Germany, 2002; pp. 31–46.

2. Landecker, W.; Shrimpton, T.; Terashima, R.S. Tweakable blockciphers with beyond birthday-bound security. In Proceedings of the Annual Cryptology Conference, Santa Barbara, CA, USA, 19–23 August 2012; Springer: Berlin/Heidelberg, Germany, 2012; pp. 14–30.

3. Andreeva, E.; Bogdanov, A.; Luykx, A.; Mennink, B.; Tischhauser, E.; Yasuda, K. Parallelizable and authenticated online ciphers. In Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security, Bangalore, India, 1–5 December 2013; Springer: Berlin/Heidelberg, Germany, 2013; pp. 424–443.

4. Rogaway, P. Efficient instantiations of tweakable blockciphers and refinements to modes OCB and PMAC. In Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security, Jeju Island, Korea, 5–9 December 2004; Springer: Berlin/Heidelberg, Germany, 2004; pp. 16–31.

5. Rogaway, P.; Bellare, M.; Black, J. OCB: A block-cipher mode of operation for efficient authenticated encryption. ACM Trans. Inf. Syst. Secur. (TISSEC) 2003, 6, 365–403. [CrossRef]

6. Crowley, P. Mercy: A fast large block cipher for disk sector encryption. In Proceedings of the International Workshop on Fast Software Encryption, New York, NY, USA, 10–12 April 2000; Springer: Berlin/Heidelberg, Germany, 2000; pp. 49–63.

7. Ferguson, N.; Lucks, S.; Schneier, B.; Whiting, D.; Bellare, M.; Kohno, T.; Callas, J.; Walker, J. The Skein hash function family. NIST (Round 3) 2010, 7, 3, submitted.

8. Schroeppe, R. Hasty pudding cipher specification. In Proceedings of the First AES Candidate Workshop, Ventura, CA, USA, 20–22 August 1998.

9. Cogliati, B.; Seurin, Y. Beyond-birthday-bound security for tweakable Even-Mansour ciphers with linear tweak and key mixing. In Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security, Auckland, New Zealand, 29 November–3 December 2015; Springer: Berlin/Heidelberg, Germany, 2015; pp. 134–158.

10. Mennink, B. XPX: Generalized tweakable even-mansour with improved security guarantees. In Proceedings of the Annual International Conference, Santa Barbara, CA, USA, 14–18 August 2016; Springer: Berlin/Heidelberg, Germany, 2016; pp. 64–94.

11. Naito, Y. Tweakable blockciphers for efficient authenticated encryptions with beyond the birthday-bound security. IACR Trans. Symmetric Cryptol. 2017, 1, 26. [CrossRef]

12. Feistel H. Cryptography and computer privacy. Sci. Am. 1973, 228, 15–23. [CrossRef]

13. Even, S.; Mansour, Y. A construction of a cipher from a single pseudorandom permutation. J. Cryptol. 1997, 10, 151–161. [CrossRef]

14. Jean, J.; Nikolić, I.; Peyrin, T. Tweaks and keys for block ciphers: The TWEAKEY framework. In Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security, Kaoshiung, Taiwan, 7–11 December 2014; Springer: Berlin/Heidelberg, Germany, 2014; pp. 274–288.

15. Cogliati, B.; Lampe, R.; Seurin, Y. Tweak even-mansour ciphers. In Proceedings of the Annual Cryptology Conference, Santa Barbara, CA, USA, 16–20 August 2015; Springer: Berlin/Heidelberg, Germany, 2015; pp. 189–208.

16. Cogliati, B.; Seurin, Y. On the provable security of the iterated Even-Mansour cipher against related-key and chosen-key attacks. In Proceedings of the Annual International Conference on the Theory and Applications of Cryptographic Techniques, Sofia, Bulgaria, 26–30 April 2015; Springer: Berlin/Heidelberg, Germany, 2015; pp. 584–613.

17. Farshim, P.; Procter, G. The related-key security of iterated Even—Mansour ciphers. In Proceedings of the International Workshop on Fast Software Encryption, Istanbul, Turkey, 8–11 March 2015; Springer: Berlin/Heidelberg, Germany, 2015; pp. 342–363.

18. Granger, R.; Jovanovic, P.; Mennink, B.; Neves, S. Improved masking for tweakable blockciphers with applications to authenticated encryption. In Proceedings of the Annual International Conference on the Theory and Applications of Cryptographic Techniques, Vienna, Austria, 8–12 May 2016; Springer: Berlin/Heidelberg, Germany, 2016; pp. 263–293.

19. Luby, M.; Rackoff, C. How to construct pseudorandom permutations from pseudorandom functions. SIAM J. Comput. 1988, 17, 373–386. [CrossRef]

20. Mitsuwa, A.; Iwata, T. Tweakable pseudorandom permutation from generalized feistel structure. In Proceedings of the International Conference on Provable Security, Shanghai, China, 30 October–1 November 2008; Springer: Berlin/Heidelberg, Germany, 2008; pp. 22–37.

21. Lampe, R.; Seurin, Y. Security analysis of key-alternating Feistel ciphers. In Proceedings of the International Workshop on Fast Software Encryption, London, UK, 3–5 March 2014; Springer: Berlin/Heidelberg, Germany, 2014; pp. 243–264.
22. Goldenberg, D.; Hohenberger, S.; Liskov, M.; Schwartz, E.C.; Seyalioglu, H. On tweaking luby-rackoff blockciphers. In Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security, Kuching, Malaysia, 2–6 December 2007; Springer: Berlin/Heidelberg, Germany, 2007; pp. 342–356.

23. Yan, H.; Wang, L.; Shen, Y.; Lai, X. Tweaking Key-Alternating Feistel Block Ciphers. In Proceedings of the International Conference on Applied Cryptography and Network Security, Rome, Italy, 9–22 October 2020; Springer: Cham, Switzerland, 2020; pp. 69–88.

24. Guo, C.; Wang, L. Revisiting key-alternating Feistel ciphers for shorter keys and multi-user security. In Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security, Brisbane, QLD, Australia, 2–6 December 2018; Springer: Cham, Switzerland, 2018; pp. 213–243.

25. Patarin J. The “coefficients H” technique. In Proceedings of the International Workshop on Selected Areas in Cryptography, Sackville, NB, Canada, 14–15 August 2008; Springer: Berlin/Heidelberg, Germany, 2008; pp. 328–345.

26. Chen, S.; Steinberger, J. Tight security bounds for key-alternating ciphers. In Proceedings of the Annual International Conference on the Theory and Applications of Cryptographic Techniques, Copenhagen, Denmark, 11–15 May 2014; Springer: Berlin/Heidelberg, Germany, 2014; pp. 327–350.

27. Hoang, V.T.; Tessaro, S. Key-alternating ciphers and key-length extension: Exact bounds and multi-user security. In Proceedings of the Annual International Cryptology Conference, Santa Barbara, CA, USA, 14–18 August 2016; Springer: Berlin/Heidelberg, Germany, 2016; pp. 3–32.