Tweaking Key-Alternating Feistel Block Ciphers

Hailun Yan[1,2], Lei Wang[2,4(✉)], Yaobin Shen[2], and Xuejia Lai[2,3,4(✉)]

[1] École Polytechnique Fédérale de Lausanne (EPFL), Lausanne, Switzerland
hailun.yan@epfl.ch
[2] Shanghai Jiao Tong University, Shanghai, China
{wanglei_hb,yb_shen,laix}@sjtu.edu.cn
[3] State Key Laboratory of Cryptology, P. O. Box 5159, Beijing 100878, China
[4] Westone Cryptologic Research Center, Beijing 100070, China

Abstract. Tweakable block cipher as a cryptographic primitive has found wide applications in disk encryption, authenticated encryption mode and message authentication code, etc. One popular approach of designing tweakable block ciphers is to tweak the generic constructions of classic block ciphers. This paper focuses on how to build a secure tweakable block cipher from the Key-Alternating Feistel (KAF) structure, a dedicated Feistel structure with round functions of the form $F_i(k_i \oplus x_i)$, where k_i is the secret round key and F_i is a public random function in the i-th round. We start from the simplest KAF structures that have been published so far, and then incorporate the tweaks to the round key XOR operations by (almost) universal hash functions. Moreover, we limit the number of rounds with the tweak injections for the efficiency concerns of changing the tweak value. Our results are two-fold, depending on the provable security bound: For the birthday-bound security, we present a 4-round minimal construction with two independent round keys, a single round function and two universal hash functions; For the beyond-birthday-bound security, we present a 10-round construction secure up to $O(\min\{2^{2n/3}, \sqrt[4]{2^{2n}\epsilon^{-1}}\})$ adversarial queries, where n is the output size of the round function and ϵ is the upper bound of the collision probability of the universal hash functions. Our security proofs exploit the hybrid argument combined with the H-coefficient technique.

Keywords: Tweakable block cipher · Key-Alternating Feistel cipher · Provable security · H-coefficient technique

1 Introduction

Tweakable block ciphers are formalized by Liskov et al. [28], which generalize the standard block cipher by introducing an auxiliary input called *tweak*. As a more natural primitive for building modes of operation, tweakable block cipher has found wide applications in encryption schemes [2,10,19,31,40,43], authenticated encryption modes [1,28,37,38], message authentication codes [26,28],

M. Conti et al. (Eds.): ACNS 2020, LNCS 12146, pp. 69–88, 2020.
https://doi.org/10.1007/978-3-030-57808-4_4

online ciphers [1,39] and disk encryption [20,21]. A tweakable block cipher can be designed from scratch [8,14,41], or from conventional block ciphers by using it as a black-box [3,24,26,27,29,30,34,37,42]. Another approach is incorporating the additional parameter *tweak* directly into generic constructions of conventional block ciphers [5–7,12,16,17,23,32], which is the case we considered in this paper.

There are two popular block cipher constructions. One is the Even-Mansour construction based on round permutations [11] and the other is the Feistel construction based on round functions [13]. For tweaking Even-Mansour constructions, a series of papers have been published [5–7,12,17,23]. However, there has been little progress toward tweaking Feistel constructions, since the work of Goldenberg et al. on ASIACRYPT 2007 tweaking Luby-Rackoff ciphers [16], and the work of Mitsuda and Iwata on ProvSec 2008 tweaking generalized Feistel ciphers [32]. We follow this research line but turn to a new direction, namely tweaking the so-called Key-Alternating Feistel ciphers.

The Luby-Rackoff Scheme vs. Key-Alternating Feistel Ciphers. The Feistel network [13] is an important structure for designing block ciphers. In a Feistel cipher, the intermediate state $x = x_L||x_R$ in the i-th round is updated by the round function G_i according to $x_L||x_R \rightarrow x_R||x_L \oplus G_i(k_i, x_R)$. When the round functions G_i are uniformly random and independent (or generated from a pesudo-random generator), the model is called Luby-Rackoff (LR) construction. The LR construction might be the most popular model for Feistel ciphers so far, however, it falls short of showing how to concretely design the keyed round functions. The model named Key-Alternating Feistel (KAF) [25] provides the idea to instantiate the round function in the form of $G_i(k_i, x_i) = F_i(x_i \oplus k_i)$, where F_i is *keyless* and *public*.

Security analysis of the KAF model is of great significance. From practical points of views, many Feistel block ciphers in reality, such as DES, GOST, Camellia variant without FL/FL^{-1} functions, LBlock and TWINE (the last two adopt generalized Feistel), employ keyless round functions and xor each round key before applying the corresponding round function. On the theoretical side, there is a non-negligible gap between the Luby-Rackoff and KAF models. More specifically, KAF is based on public round functions, which enables the adversary to query the round functions directly. Thus, a security proof for the Luby-Rackoff model cannot be extended to the KAF model. For example, 6-round Luby-Rackoff is proven optimal security against 2^n adversarial queries [33]. On the other hand, there exists a generic distinguishing attack against t-round KAF with a complexity of $2^{\frac{(t-2)n}{t-1}}$ queries [18]. In Table 1, we summarize some known security results of KAF constructions.

Our Contributions. This paper takes several steps towards constructing secure tweakable block ciphers from the Key-Alternating Feistel structure. We focus on a general construction of tweaking KAF with the i-th round as below

$$tk_i \leftarrow H_i(k_i, t), \qquad x_L\|x_R \leftarrow x_R\|x_L \oplus F_i(x_R \oplus tk_i),$$

Table 1. Existing provable results on KAF.

#Rounds	Key size	#Round functions	Security bound	Model	References
3	n	1	$n/2$	CPA	[44]
4	$4n$	2	$n/2$	CCA	[15]
4	n	1	$n/2$	CCA	[18]
6	$2n$	6	$2n/3$	CCA	[18]
12	$12n$	12	$2n/3$	CCA	[25]
$6t$	$6tn$	$6tn$	$tn/(t+1)$	CCA	[25]

where k_i is the secret key, t is the tweak, $H_i(\cdot)$ is an universal hash function and $F_i(\cdot)$ is a public random function. We refer the readers to Sect. 3 for detailed discussions about the rationale of this generic construction. Moreover, instead of the general KAF structure, we base our design on the simplified KAF structures recently published by Guo and Wang [18], which enables to reduce the number of independent round key k_i's and the number of random functions F_i's. In the end, we obtain the following results.

- For the birthday bound security, we present a 4-round minimized structure depicted in Fig. 1, that uses two round keys (k_1, k_2) and a single random function $F(\cdot)$.
- For the beyond-birthday security, we present a 10-round structure depicted in Fig. 2, which pre- and post-add two rounds to the minimized 6-round KAF in [18]. The injection of tweaks is limited to the first and the last two rounds.

2 Preliminaries

2.1 Notation and General Definitions

Fix an integer $n \geq 1$. Denote $N = 2^n$ and denote by $(N)_q$ the product $\prod_{i=0}^{q-1}(N-i)$. Further denote $\mathsf{F}(n)$ the set of all functions of domain $\{0,1\}^n$ and range $\{0,1\}^n$. For $X, Y \in \{0,1\}^n$, denote their concatenation by $X||Y$ or simply XY.

Tweakable Block Ciphers. A conventional block cipher E is a permutation that takes two inputs - a *key* and a *message* (or *plaintext*) - and outputs the corresponding *ciphertext*, while a tweakable block cipher $\widetilde{E}$ introduces the third input called *tweak*. Formally, a tweakable block cipher is denoted as a mapping $\widetilde{E} : \mathcal{K} \times \mathcal{T} \times \mathcal{M} \to \mathcal{M}$, where $\mathcal{K}$ is the key space, $\mathcal{T}$ is the tweak space and $\mathcal{M}$ is the message space. In the following, we denote by $\mathsf{TP}(\mathcal{T}, 2n)$ the set of all tweakable permutations with tweak space $\mathcal{T}$ and message space $\{0,1\}^{2n}$.

Key-Alternating Feistel Ciphers. Given a function F in $\mathsf{F}(n)$ and an n-bit key k, the one-round Key-Alternating Feistel permutation is a permutation defined on $\{0,1\}^{2n}$, which is defined as:

$$\Psi_k^F(L||R) = (R||L \oplus F(R \oplus k)),$$

where L and R are respectively the left and right n-bit halves of the input.

Let $r \geq 1$ and let $F_1, F_2, \ldots, F_r$ be r public functions in $\mathsf{F}(n)$. An r-round Key-Alternating Feistel (KAF for short) cipher associated with the round functions $F_1, \ldots, F_r$, denoted $\Psi^{F_1,\ldots,F_r}$, is a function that maps a key $(k_1, k_2, \ldots, k_r) \in (\{0,1\}^n)^r$ and a message $x \in \{0,1\}^{2n}$ to the ciphertext defined as:

$$\Psi^{F_1,\ldots,F_r}((k_1, k_2, \ldots, k_r), x) = \Psi_{k_r}^{F_r} \circ \ldots \circ \Psi_{k_2}^{F_2} \circ \Psi_{k_1}^{F_1}(x).$$

Uniform AXU Hash Functions. Let $\mathcal{H} = (H_k)_{k \in \mathcal{K}}$ be a set of hash functions from some set $\mathcal{T}$ to $\{0,1\}^n$ indexed by a set of keys $\mathcal{K}$. $\mathcal{H}$ is said to be *uniform* if for any $t \in \mathcal{T}$ and $y \in \{0,1\}^n$,

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

$\mathcal{H}$ is said ϵ-*almost XOR-universal* (ϵ-AXU) if for all distinct $t_1, t_2 \in \mathcal{T}$ and all $y \in \{0,1\}^n$,

$$\Pr\left[k \xleftarrow{\$} \mathcal{K} : H_k(t_1) \oplus H_k(t_2) = y\right] \leq \epsilon.$$

Particularly, $\mathcal{H}$ is XOR-universal if $\epsilon = 2^{-n}$, simply denoted by XU.

2.2 Security Definitions

A *distinguisher* $\mathcal{D}$ is an algorithm which is given query access to one (or more) oracle of being either $\mathcal{O}$ and $\mathcal{Q}$, and outputs one bit. The advantage of a distinguisher $\mathcal{D}$ in distinguishing these two primitives $\mathcal{O}$ and $\mathcal{Q}$ is defined as

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

In the Random Permutation model, the security of a tweakable block cipher is defined by upper bounding the advantage of distinguisher $\mathcal{D}$ in the following scenario. $\mathcal{D}$ interacts with the oracles $(\mathcal{O}, \boldsymbol{F})$, which is either the so-called *real world* or the so-called *ideal word*. In the real world, $\mathcal{O}$ is the tweakable block cipher $\widetilde{E}(k, \cdot)$, $\boldsymbol{F} = (F_1, F_2 \ldots, F_r)$ is a tuple of public random functions/permutations used as the underlying components of $\widetilde{E}$, and k is drawn uniformly at random from the key space. In the ideal world, $\mathcal{O}$ is a uniformly random tweakable permutation $\widetilde{\Pi}$ and $\boldsymbol{F}$ is a tuple of public random functions/permutations independent from $\widetilde{\Pi}$. We will refer to $\mathcal{O}$ as the *construction oracle* and to $F_1, F_2 \ldots, F_r$ the *inner component oracles*. The goal of $\mathcal{D}$ is to distinguish these two worlds: $(\widetilde{E}(k, \cdot), \boldsymbol{F})$ and $(\widetilde{\Pi}, \boldsymbol{F})$. The advantage of $\mathcal{D}$ is defined as

$$\mathbf{Adv}(\mathcal{D}) = |\Pr\left[\mathcal{D}^{\widetilde{E}(k,\cdot),\boldsymbol{F}} \to 1\right] - \Pr\left[\mathcal{D}^{\widetilde{\Pi},\boldsymbol{F}} \to 1\right]|,$$

where the probability is taken over the random choice of k, $\boldsymbol{F}$ and $\widetilde{\Pi}$. In the following, we consider information-theoretic distinguishers that are computationally unbounded (thereby deterministic) but with limited information (the number of queries to its oracles), assuming that they never make redundant queries. Moreover, we consider distinguishers in the chosen-ciphertext attack (CCA) model with an additional ability to choose tweaks, where they can make adaptive *bidirectional* queries to all the oracles. (This will be made more clear later.)

For non-negative integers q_e, q_f, we define the insecurity of the tweakable block cipher $\widetilde{E}$ as

$$\mathbf{Adv}_{\widetilde{E}}(q_e, q_f) = max_{\mathcal{D}}\{\mathbf{Adv}(\mathcal{D})\},$$

where the maximum is taken over all distinguishers making exactly q_e queries to the construction oracle and exactly q_f queries to *each* inner component oracle.

2.3 H-Coefficient Technique

In the following, we recall Patarin's H-coefficient technique [4,35], which will be used in our security proof to evaluate the upper bound of the advantage of an adversary.

View. A view $v = (\mathcal{Q}_E, \mathcal{Q}_{\mathbf{F}})$ is the query-response tuples that $\mathcal{D}$ receives when interacting with its oracles. $\mathcal{Q}_E$ contains all triples $(t, LR, ST) \in \mathcal{T} \times \{0,1\}^{2n} \times \{0,1\}^{2n}$ such that $\mathcal{D}$ either made the direct query (t, LR) to the construction oracle and received answer ST, or made the inverse query (t, ST) and received answer LR. Suppose that $|\mathcal{Q}_E| = q_e$, there are m distinct tweaks appearing in $\mathcal{Q}_E$, and there exist q_i distinct queries for the i-th tweak $(1 \le i \le m)$, so that $\sum_{i=1}^{m} q_i = q_e$. We denote the queries corresponding to the same tweak by

$$\mathcal{Q}_{E_i} = \{(t_i, L_i^1 R_i^1, S_i^1 T_i^1), (t_i, L_i^2 R_i^2, S_i^2 T_i^2), \ldots, (t_i, L_i^{q_i} R_i^{q_i}, S_i^{q_i} T_i^{q_i})\},$$

then $\mathcal{Q}_E = \bigcup \mathcal{Q}_{E_i}$, $1 \le i \le m$. $\mathcal{Q}_{\boldsymbol{F}}$ contains query-response pairs when $\mathcal{D}$ interacts with all the inner functions $\boldsymbol{F} = (F_1, F_2, \ldots, F_r)$. We denote by $\mathcal{Q}_{F_j}$ all pairs $(u, v) \in \{0,1\}^n \times \{0,1\}^n$ such that $\mathcal{D}$ either made the direct query u to random function F_j and received answer v, or made the inverse query v and received answer u. That is,

$$\mathcal{Q}_{F_j} = \{(u_j^1, v_j^1), (u_j^2, v_j^2), \ldots, (u_j^{q_f}, v_j^{q_f})\},$$

where $|\mathcal{Q}_{F_j}| = q_f$. Then $\mathcal{Q}_{\boldsymbol{F}} = \bigcup \mathcal{Q}_{F_j}$, for $1 \le j \le r$.

Note that queries are recorded in a directionless and unordered fashion, but by our assumption that the distinguisher is deterministic, there is a one-to-one mapping between this representation and the raw transcript of the interaction of $\mathcal{D}$ with its oracles.

In all the following, we denote $X_{re}(v)$ resp. $X_{id}(v)$ the probability distribution of the view when $\mathcal{D}$ interacts with the real world, resp. the ideal world,

producing view v. We use the same notation to denote a random variable distributed according to each distribution. We say that a view v is *attainable* (with respect to some fixed distinguisher $\mathcal{D}$) if the probability to obtain this view in the ideal world is non-zero, i.e., $\Pr[X_{id} = v] > 0$. We denote $\mathcal{V}$ the set of all the attainable views, that is $\mathcal{V} = \{v \mid \Pr[X_{id} = v] > 0\}$.

Core Lemma. The main lemma of the H-coefficient technique is as follows. Please refer to [4] for the proof.

Lemma 1. *Fix a distinguisher $\mathcal{D}$. Let $\mathcal{V} = \mathcal{V}_{good} \cup \mathcal{V}_{bad}$ be a partition of the set of attainable views. Assume that there exists $\alpha \geq 0$ such that for any $v \in \mathcal{V}_{good}$, one has*

$$1 - \frac{\Pr[X_{re} = v]}{\Pr[X_{id} = v]} \leq \alpha,$$

and there exists $\beta \geq 0$ such that

$$\Pr[X_{id} \in \mathcal{V}_{bad}] \leq \beta.$$

Then one concludes that the advantage of $\mathcal{D}$ is upper bounded as

$$\mathbf{Adv}(\mathcal{D}) \leq \alpha + \beta.$$

In [22], Hoang and Tessaro (HT) established the so-called "point-wise proximity", which in a sense corresponds to applying the H-coefficient method without bad views. When partitioning the key set $\mathcal{K} = \mathcal{K}_{good} \cup \mathcal{K}_{bad}$ with two disjoint subsets $\mathcal{K}_{good}$ and $\mathcal{K}_{bad}$, HT provided a general lemma for establishing point-wise proximity.

Lemma 2. *Fix a distinguisher $\mathcal{D}$ with an attainable view v. Assume that: there exists $\alpha \geq 0$ such that for any $k \in \mathcal{K}_{good}$, one has*

$$1 - \frac{\Pr[X_{re} = v, k]}{\Pr[X_{id} = v, k]} \leq \alpha,$$

and there exists $\beta \geq 0$ such that

$$\Pr[k \in \mathcal{K}_{bad}] \leq \beta.$$

Then we have $1 - \frac{\Pr[X_{re}=v]}{\Pr[X_{id}=v]} \leq \alpha + \beta$, namely

$$\mathbf{Adv}(\mathcal{D}) \leq \alpha + \beta.$$

Here, $\Pr[X_{re} = v, k]$ is the probability $\mathcal{D}$ interacting with the real world with $k \in \mathcal{K}$ sampled as the key. While in the ideal world, we simply draw dummy keys $k \xleftarrow{\$} \mathcal{K}$ independently from the answers of the oracle. Then $\Pr[X_{id} = v, k]$ is defined as $\Pr[X_{id} = v] \cdot \Pr\left[k \xleftarrow{\$} \mathcal{K}\right]$.

Additional Notation. Given a tweakable permutation $\widetilde{\Pi}$ and a view $\widetilde{Q}$ of tweakable permutation queries, we say that $\widetilde{\Pi}$ extends $\widetilde{Q}$ if $\widetilde{\Pi}(t,x) = y$ for all $(t,x,y) \in \widetilde{Q}$, denoted by $\widetilde{\Pi} \vdash \widetilde{Q}$. Note that for a view $\widetilde{Q}$ of a tweakable random permutation, with m distinct tweaks and q_i queries corresponding to the i-th tweak, we have

$$\Pr\left[\widetilde{\Pi} \xleftarrow{\$} \mathsf{TP}(\mathcal{T}, 2n) : \widetilde{\Pi} \vdash \widetilde{Q}\right] = \prod_{i=1}^{m} \frac{1}{(N^2)_{q_i}}. \tag{1}$$

Similarly, given a function F and a view Q_F of function queries, we say that F *extends* Q_F if $F(u) = v$ for all $(u,v) \in Q_F$, denoted by $F \vdash Q_F$. For any $u \in \{0,1\}^n$, if there exists a corresponding record (u,v) in Q_F, then we write $u \in Dom\mathcal{F}$ (and $u \notin Dom\mathcal{F}$ otherwise). For a function view Q_F of size q_f, we have that

$$\Pr\left[F \xleftarrow{\$} \mathsf{F}(n) : F \vdash Q_F\right] = \frac{1}{N^{q_f}}. \tag{2}$$

3 Approach Overview

Firstly, we focus on a targeted construction of tweaking the Key-Alternating Feistel, which replaces the round keys k_i of KAF by tweak-dependent keys denoted as tk_i and generated from the round key k_i and the tweak t. In this paper, we treat the tweak and the key comparably. From the efficiency concerns, Liskov et al. [28] suggested that changing the tweak should be less costly than changing the key. However, from the security concerns, it is indeed counter-intuitive as pointed out by Jean et al. [23], because the adversary has full control over the tweak. We follow the latter argument. Moreover, it makes the target construction as neat, simple and clean as the KAF.

Secondly, it is always interesting and important to achieve the same security level, but with less resources such as the number of secret keys and the number of public round functions. We find that recently Guo and Wang published in [18] minimized 4-round and 6-round KAF structures that achieve birthday-bound and beyond-birthday-bound security, respectively. Thus, we build tweaked KAFs from their minimized KAF structures, which in turn enables to reduce the number of secret keys and the number of round functions.

Finally, we limit the number of rounds where the tweak is injected to generate tweak-dependent round keys. This improves the efficiency of changing the tweak, because the tweak is updated much more frequently than the key.

4 Birthday-Bound Security for Four Rounds

In this section, we give a 4-round minimal tweakable Key-Alternating Feistel construction (refer to Fig. 1), which is proved secure up to birthday-bound adversarial queries. Additionally, we prove that this 4-round construction is round-optimal, by showing a simple chosen-ciphertext attack on 3 rounds.

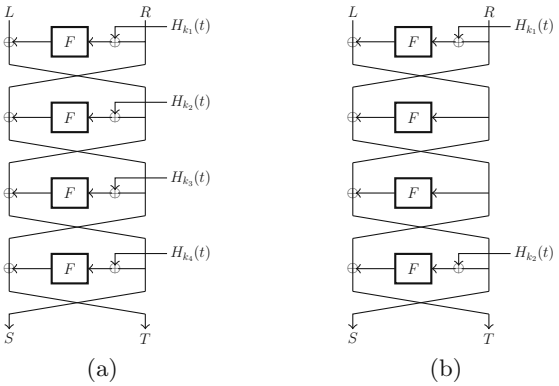

Fig. 1. (a) A general 4-round TKAFSF. (b) The "minimized" TKAFSF.

Fix integers $n, r \geq 1$. Let $\mathcal{T}$ and $\mathcal{K}$ be two sets, and $\mathcal{H} = (H_k)_{k \in \mathcal{K}}$ be an AXU family of hash functions from $\mathcal{T}$ to $\{0,1\}^n$ indexed by $\mathcal{K}$. We consider tweakable KAF with all the round functions *identical* and denote it by TKAFSF. Actually, we started from a general TKAFSF construction (refer to Fig. 1(a)) that maps a key $\boldsymbol{k} = (k_1, k_2, k_3, k_4)$, a tweak $t \in \mathcal{T}$ and a message $x \in \{0,1\}^{2n}$ to the ciphertext:

$$\mathsf{TKAFSF}(x) = \Psi^F_{k_4,t} \circ \Psi^F_{k_3,t} \circ \Psi^F_{k_2,t} \circ \Psi^F_{k_1,t}(x),$$

where $\Psi^F_{k_i,t}$ is a permutation on $\{0,1\}^{2n}$ defined as $\Psi^F_{k_i,t}(x) = \Psi^F_{H_{k_i}(t)}(x)$. We found that both k_2 and k_3 are "redundant" for the birthday-bound security, thereby deducing a "minimal" 4-round construction with only two keys (refer to Fig. 1(b)):

$$\mathsf{TKAFSF}(x) = \Psi^F_{k_2,t} \circ \Psi^F \circ \Psi^F \circ \Psi^F_{k_1,t}(x).$$

Security Analysis for 4-Round TKAFSF. In the following, we go directly to the security proof of the 4-round minimal TKAFSF. The main result is shown in Theorem 1.

Theorem 1. *For the 4-round idealized* TKAFSF *construction as depicted in Fig. 1(b) with two independent random round keys k_1, k_2, it holds*

$$\mathbf{Adv}_{\mathsf{TKAFSF}}(q_e, q_f) \leq \frac{9q_e^2 + 4q_e q_f}{N} + 2q_e^2\epsilon.$$

Definition and Probability of Bad Keys. We first define bad keys and upper bound their probability in the ideal world.

Definition 1 (Bad Key Vector for 4 Rounds). *With respect to a view (Q_E, Q_F), we say a key vector $k = (k_1, k_2)$ is bad if one of the following conditions is fulfilled:*

- *(B-1) there exists $(t, LR, ST) \in Q_E$ such that either $H_{k_1}(t) \oplus R \in Dom\mathcal{F}$ or $H_{k_2}(t) \oplus S \in Dom\mathcal{F}$;*

– *(B-2) there exists two (not necessarily distinct)* $(t, LR, ST), (t', L'R', S'T') \in Q_E$ *such that* $H_{k_1}(t) \oplus R = H_{k_2}(t') \oplus S'$.

Otherwise we say that the key vector k *is good. We denote* $\mathcal{K}_{good}$*, resp.* $\mathcal{K}_{bad}$ *the set of good, resp. bad key vectors.*

Lemma 3.

$$\Pr\left[k \xleftarrow{\$} \mathcal{K} : k \in \mathcal{K}_{bad}\right] \leq \frac{2q_e q_f + q_e^2}{N}.$$

Proof. The probability that a key vector fulfills (B-1) is at most $\frac{2q_e q_f}{N}$. More specifically, for each of the q_e query-response records $(t, LR, ST) \in Q_E$, recall that the key $k = (k_1, k_2)$ is drawn at random from the key space independently from the queries, and $|Dom\mathcal{F}| = q_f$, it fulfills (B-1) with probability at most $\frac{2q_f}{N}$ by the uniformity of $\mathcal{H}$.

Moreover, the probability that it fulfills (B-2) is at most $\frac{q_e^2}{N}$: For each of the q_e^2 pairs of records (t, LR, ST) $(t', L'R', S'T')$, it fulfills (B-2) with probability at most $\frac{1}{N}$. □

Analysis of Good Keys. We then show that, for any good key, the probability to obtain a view in the real world and the ideal world are sufficiently close.

Lemma 4. *For any key vector* $k \in \mathcal{K}_{good}$*, one has*

$$1 - \frac{\Pr[X_{re} = v, k]}{\Pr[X_{id} = v, k]} \leq \frac{8q_e^2}{N} + \frac{2q_e q_f}{N} + 2q_e^2\epsilon.$$

Proof. In the ideal world, the probability to get any attainable transcript v is

$$\Pr[X_{id} = v] = \Pr\left[k \xleftarrow{\$} \mathcal{K}, \widetilde{\Pi} \xleftarrow{\$} \mathsf{TP}(\mathcal{T}, 2n), F \xleftarrow{\$} \mathsf{F}(n) : \widetilde{\Pi} \vdash Q_E \wedge F \vdash \mathcal{Q}_F\right],$$

combined with Eq. (1) and (2), we have

$$\Pr[X_{id} = v, k] = \frac{1}{|\mathcal{K}|^2} \cdot \frac{1}{N^{q_f}} \cdot \prod_{i=1}^{m} \frac{1}{(N^2)_{q_i}}.$$

Similarly, in the real world, we have

$$\Pr[X_{re} = v, k] = \frac{1}{|\mathcal{K}|^2} \cdot \frac{1}{N^{q_f}} \cdot \Pr\left[k \xleftarrow{\$} \mathcal{K}, F \xleftarrow{\$} \mathsf{F}(n) : \mathsf{TKAFSF} \vdash Q_E \mid F \vdash \mathcal{Q}_F\right].$$

Then, in order to give the lower bound of the ratio

$$\frac{\Pr[X_{re} = v, k]}{\Pr[X_{id} = v, k]} = \Pr\left[k \xleftarrow{\$} \mathcal{K}, F \xleftarrow{\$} \mathsf{F}(n) : \mathsf{TKAFSF} \vdash Q_E \mid F \vdash \mathcal{Q}_F\right] \cdot \prod_{i=1}^{m} (N^2)_{q_i},$$

we only need to focus on the lower bound of the probability

$$\Pr\left[k \xleftarrow{\$} \mathcal{K}, F \xleftarrow{\$} \mathsf{F}(n) : \mathsf{TKAFSF} \vdash Q_E \mid F \vdash \mathcal{Q}_F\right]. \tag{3}$$

For this, we follow a clean "predicate" approach from [9]. In the following, we will define a "bad" predicate $\mathsf{E}(F)$ corresponding to the round function F such that if E does not hold (with probability that can be lower bounded, will be shown in Eq. 4), then the event $\mathsf{TKAFSF} \vdash Q_E$ conditioned on $F \vdash Q_F$ is equivalent to $2q_e$ new and distinct equations on the random round function F (will be shown in Eq. 5).

Given (Q_E, Q_F), given $F \xleftarrow{\$} \mathsf{F}(n)$ with $F \vdash Q_F$, we say that a predicate $\mathsf{E}(F)$ holds, if one of the following conditions is fulfilled:

- (C-1) there exists $(t, LR, ST) \in Q_E$, such that $F(R \oplus H_{k_1}(t)) \oplus L \in U_1 \cup U_4 \cup Dom\mathcal{F}$ or $F(S \oplus H_{k_2}(t)) \oplus T \in U_1 \cup U_4 \cup Dom\mathcal{F}$,
- (C-2) there exists $(t, LR, ST) \neq (t', L'R', S'T') \in Q_E$, such that $F(R \oplus H_{k_1}(t)) \oplus L = F(R' \oplus H_{k_1}(t')) \oplus L'$ or $F(S \oplus H_{k_2}(t)) \oplus T = F(S' \oplus H_{k_2}(t')) \oplus T'$,
- (C-3) there exists $(t, LR, ST), (t', L'R', S'T') \in Q_E$, such that $F(R \oplus H_{k_1}(t)) \oplus L = F(S' \oplus H_{k_2}(t')) \oplus T'$,

where

$$U_1 := \{u_1 \in \{0,1\}^n \mid (t, LR, ST) \in Q_E \text{ for } R = u_1 \oplus H_{k_1}(t) \text{ and some } t, L, S, T\},$$
$$U_4 := \{u_4 \in \{0,1\}^n \mid (t, LR, ST) \in Q_E \text{ for } S = u_4 \oplus H_{k_2}(t) \text{ and some } t, L, R, T\}.$$

Clearly, $|U_1|, |U_4| \leq q_e$. We consider the above three conditions respectively. For (C-1), since $k = (k_1, k_2)$ is good, the value $F(R \oplus H_{k_1}(t))$ and $F(S \oplus H_{k_2}(t))$ remain uniformly distributed, then

$$\Pr\left[\text{(C-1)} \mid F \vdash Q_F\right] \leq 2 \cdot q_e \cdot (2q_e + q_f) \cdot \frac{1}{N} = \frac{4q_e^2 + 2q_e q_f}{N}.$$

For (C-3), there exists two (not necessarily distinct) records (t, LR, ST) and $(t', L'R', S'T')$ in Q_E such that $F(R \oplus H_{k_1}(t)) \oplus L = F(S' \oplus H_{k_2}(t')) \oplus T'$. The two function values $F(R \oplus H_{k_1}(t))$ and $F(S' \oplus H_{k_2}(t'))$ are independent by $\neg$(B-2). Therefore,

$$\Pr\left[\text{(C-3)} \mid F \vdash Q_F\right] \leq \frac{q_e^2}{N}$$

by virtue of the uniformity of F. For (C-2), The analysis is a little bit complicated. Given two distinct records (t, LR, ST) and $(t', L'R', S'T')$, we first consider the "collision" $F(R \oplus H_{k_1}(t)) \oplus L = F(R' \oplus H_{k_1}(t')) \oplus L'$ in three cases.

- If $t \neq t'$, the probability that $R \oplus H_{k_1}(t) = R' \oplus H_{k_1}(t')$ is the probability that $H_{k_1}(t) \oplus H_{k_1}(t') = R \oplus R'$ which is at most ϵ by the ϵ-AXU property of $\mathcal{H}$. Conditioned on $R \oplus H_{k_1}(t) \neq R' \oplus H_{k_1}(t')$, the two function values $F(R \oplus H_{k_1}(t))$ and $F(R' \oplus H_{k_1}(t'))$ are independent and remains uniformly random, the probability to hit a collision is thereby at most $\frac{1}{N}$. To sum up, the probability that we hit a collision in $F(R \oplus H_{k_1}(t)) \oplus L$ is at most $\epsilon \cdot 1 + (1 - \epsilon) \cdot \frac{1}{N} \leq \epsilon + \frac{1}{N}$.
- If $t = t'$ but $R \neq R'$, then the probability to hit a collision is the probability that $F_1(R \oplus H_{K_1}(t)) = F_1(R' \oplus H_{K_1}(t)) \oplus L \oplus L'$ which is at most $\frac{1}{N}$.
- If $t = t'$, $R = R'$ but $L \neq L'$, then the collision can never happen.

In either case, the probability that $F(R \oplus H_{k_1}(t)) \oplus L = F(R' \oplus H_{k_1}(t')) \oplus L'$ is bounded by $\epsilon + \frac{1}{N}$. The analysis is similar for the "collision" $F(S \oplus H_{k_2}(t)) \oplus T = F(S' \oplus H_{k_2}(t')) \oplus T'$. By summing over all possible pairs, we have

$$\Pr\left[\text{(C-2)} \mid F \vdash Q_F\right] \leq 2q_e^2\epsilon + \frac{2q_e^2}{N}.$$

Finally, we have that

$$\Pr\left[\mathsf{E}(F) \mid F \vdash Q_F\right] \leq \frac{7q_e^2}{N} + \frac{2q_e q_f}{N} + 2q_e^2\epsilon. \tag{4}$$

When the predicate $\mathsf{E}(F)$ does not hold, the probability that TKAFSF extends Q_E conditioned on $F \vdash Q_F$ is relatively easy to analyze. For a given F, for each record $(t, LR, ST) \in Q_E$, denote

$$u_2 = F(R \oplus H_{k_1}(t)) \oplus L \text{ and } u_3 = F(S \oplus H_{k_2}(t)) \oplus T.$$

For q_e records $(t^{(i)}, L^{(i)}R^{(i)}, S^{(i)}T^{(i)})$ (by using an arbitrary order) in Q_E, we can get a sequence of u_2 resp. u_3,

$$\{u_2^{(1)}, u_2^{(2)}, \ldots, u_2^{(q_e)}\},\ \textit{resp.}\ \{u_3^{(1)}, u_3^{(2)}, \ldots, u_3^{(q_e)}\}.$$

We "peel off" the outer two rounds. Then the event $\mathsf{TKAFSF}(k, t^{(i)}, L^{(i)}R^{(i)}) = (S^{(i)}T^{(i)})$ is equivalent to the event that

$$F(u_2^{(i)}) = R \oplus u_3^{(i)} \text{ and } F(u_3^{(i)}) = S \oplus u_2^{(i)}.$$

Note that the $2q_e$ values in $\{u_2^{(1)}, u_2^{(q_e)}, \ldots, u_2^{(q_e)}\}$ and $\{u_3^{(1)}, u_3^{(2)}, \ldots, u_3^{(2)}\}$ are *new* and *distinct* conditioned on $\neg\mathsf{E}$. (Distinct: if $\exists u_2^{(i)} = u_2^{(j)}$ or $u_3^{(i)} = u_3^{(j)}$ then condition (C-2) is fulfilled; if $\exists u_2^{(i)} = u_3^{(j)}$ then condition (C-3) is fulfilled. New: the $2q_e$ images of F remain fully undetermined and thus uniformly random, otherwise condition (C-1) if fulfilled.) Therefore, for each of the q_e records (t, LR, ST), we have that

$$\Pr\left[F(u_2) = R \oplus u_3 \wedge F(u_3) = S \oplus u_2\right] = \frac{1}{N^2},$$

thereby having

$$\Pr\left[k \xleftarrow{\$} \mathcal{K}, F \xleftarrow{\$} \mathsf{F}(n) : \mathsf{TKAFSF} \vdash Q_E \mid F \vdash \mathcal{Q}_F \wedge \neg\mathsf{E}(F)\right] = \frac{1}{N^{2q_e}}. \tag{5}$$

Now that we can lower bound the probability in 3 by the law of total probability, which is $\frac{1}{N^{2q_e}} \cdot (1 - \frac{7q_e^2}{N} - \frac{2q_e q_f}{N} - 2q_e^2\epsilon)$. Finally, we can get the result in

Lemma 4:

$$\begin{aligned}\frac{\Pr[X_{re}=v,k]}{\Pr[X_{id}=v,k]} &\geq \frac{1}{N^{2q_e}}\cdot(1-\frac{7q_e^2}{N}-\frac{2q_eq_f}{N}-2q_e^2\epsilon)\cdot\prod_{i=1}^{m}(N^2)_{q_i}\\ &\geq (1-\frac{7q_e^2}{N}-\frac{2q_eq_f}{N}-2q_e^2\epsilon)\cdot\frac{(N^2)_{q_e}}{N^{2q_e}}\\ &\geq (1-\frac{7q_e^2}{N}-\frac{2q_eq_f}{N}-2q_e^2\epsilon)\cdot(1-\frac{q_e^2}{N^2})\\ &\geq 1-\frac{7q_e^2}{N}-\frac{2q_eq_f}{N}-2q_e^2\epsilon-\frac{q_e^2}{N^2}\\ &\geq 1-\frac{8q_e^2}{N}-\frac{2q_eq_f}{N}-2q_e^2\epsilon.\end{aligned}$$

□

Gathering Lemma 3, Lemma 4 and Lemma 2, we finally draw the conclusion in Theorem 1.

CCA for Three Rounds with $q_e = 3$. For completeness, we show a simple chosen-ciphertext attack on 3-round tweakable KAF construction with round permutations $\Psi_{k_i,t}^{F_i}(i=1,2,3)$, which indicates that the above 4-round construction is round-optimal. The attack is almost the same with that on classical Feistel ciphers [36]. Consider the following CCA-distinguisher $\mathcal{D}$:

1. $\mathcal{D}$ chooses $t \in \mathcal{T}$, $L, L', R \in \{0,1\}^n$ with $L \neq L'$, and queries $[S,T] \triangleq \mathcal{O}([t,L,R])$ and $[S',T'] \triangleq \mathcal{O}([t,L',R])$.
2. $\mathcal{D}$ asks for the value $[L'',R''] \triangleq \mathcal{O}^{-1}(t,[S',T'\oplus L\oplus L'])$.
3. $\mathcal{D}$ checks if $R''=S'\oplus S\oplus R$: if it holds, $\mathcal{D}$ outputs 1; otherwise outputs 0.

If $\mathcal{O}$ is a tweakable permutation randomly chosen, the probability that $\mathcal{D}$ outputs 1 is $1/N$, while it always holds for Construction I that $\mathcal{D}$ outputs 1, as $R''=S'\oplus F_2(\underbrace{F_3(S'\oplus H_{k_3}(t))\oplus T'\oplus L\oplus L'}_{F_(R\oplus H_{k_1}(t))\oplus L}\oplus H_{k_2}(t))$.
$\underbrace{\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad}_{S\oplus R}$

5 Beyond-Birthday-Bound Security for Ten Rounds

In this section, we consider constructing tweakable Key-Alternating Feistel cipher with beyond-birthday-bound (BBB) security. We build a tweaked KAF from Guo-Wang's minimized KAF structure [18], leading to a 10-round BBB-secure construction.

Recall that Guo and Wang [18] published at ASIACRYPT 2018 a minimized 6-round KAF structure which achieves BBB security.

Definition 2 (Suitable Round Key Vectors for 6-Round KAF [18]). *A round key vector $k=(k_1,k_2,\ldots,k_6)$ for 6-round Key-Alternating Feistel is suitable if it satisfies the following conditions:*

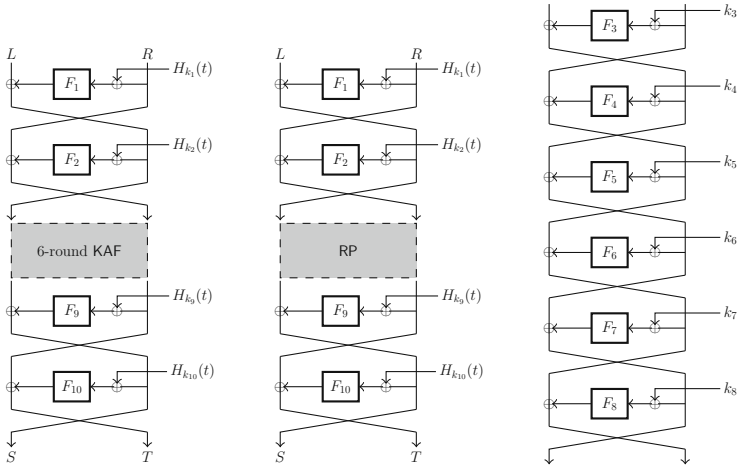

Fig. 2. (a) 10-Round TKAF. (b) 10-round Hybrid. (c) 6-round KAF.

(i) $k_1, k_2, \ldots, k_6$ *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.*

Lemma 5 (Guo-Wang [18]). *For the 6-round idealized Key-Alternating Feistel cipher* KAF *with a suitable round key vector as specified in Definition 2, it holds*

$$\mathbf{Adv}_{\mathsf{KAF}}(q_e, q_f) \leq \frac{7q_e^3 + 21q_eq_f^2 + 4q_e^2q_f}{N^2}.$$

Thus, by using their 6-round KAF as a "core", with tweaks incorporated in the first and the last two rounds, we give a 10-round construction, denoted by TKAF, (refer to Fig. 2). Formally speaking, TKAF corresponding to random functions $\boldsymbol{F} = (F_1, F_2, \ldots, F_{10})$ maps a key $k = (k_1, k_2, \ldots, k_{10})$, a tweak $t \in \mathcal{T}$ and a message $x \in \{0,1\}^{2n}$ to the ciphertext defined as:

$$\mathsf{TKAF}_k^{\boldsymbol{F}}(t,x) = \Psi_{k_{10},t}^{F_{10}} \circ \Psi_{k_9,t}^{F_9} \circ \Psi_{k_8}^{F_8} \circ \Psi_{k_7}^{F_7} \circ \ldots \circ \Psi_{k_4}^{F_4} \circ \Psi_{k_3}^{F_3} \circ \Psi_{k_2,t}^{F_2} \circ \Psi_{k_1,t}^{F_1}(x).$$

Theorem 2. *For the 10-round idealized* TKAF *construction as depicted in Fig. 2(a) with suitable key vectors, it holds*

$$\mathbf{Adv}_{\mathsf{TKAF}}(q_e, q_f) \leq \frac{23q_eq_f^2 + q_e^2(7q_e + 4q_f + 2)}{N^2} + \frac{4q_e^2q_f^2}{N^3} + \frac{4q_e^2q_f^2\epsilon}{N^2}.$$

To prove the BBB security for 10-round TKAF, we use the hybrid technique combine with the H-coefficient technique. Denote by G_1 the 10-round TKAF construction (Fig. 2(a)), by G_2 the refinement of TKAF with the intermediate 6 rounds replaced by a random permutation (RP) (Fig. 2(b)), by G_3 a tweakable

random permutation. We consider the advantage $\mathbf{Adv}_{G_1,G_3}(\mathcal{D})$ of a distinguisher $\mathcal{D}$ to distinguish G_1 and G_3 by the following triangle inequality:

$$\mathbf{Adv}_{G_1,G_3}(\mathcal{D}) \leq \mathbf{Adv}_{G_1,G_2}(\mathcal{D}) + \mathbf{Adv}_{G_2,G_3}(\mathcal{D}).$$

The indistinguishability between G_1 and G_2 can be trivially reduced to the indistinguishability between KAF and a random permutation. For any distinguisher $\mathcal{D}$ which distinguish between G_1 and G_2, we can easily construct a distinguisher $\mathcal{D}'$ which distinguish between the 6-round KAF and a random permutation Π, thus upper bounding $\mathbf{Adv}_{G_1,G_2}(\mathcal{D})$ by $\mathbf{Adv}_{\mathsf{KAF}}(\mathcal{D}')$. In the following, we will upper bound the advantage of a distinguisher $\mathcal{D}$ to distinguish G_2 and G_3, by using the H-coefficient technique.

Lemma 6. *For any distinguisher $\mathcal{D}$ making exactly q_e queries to the construction oracle and exactly q_f queries to each inner component oracle,*

$$\mathbf{Adv}_{G_2,G_3}(\mathcal{D}) \leq \frac{2q_e q_f^2}{N^2} + \frac{4q_e^2 q_f^2}{N^3} + \frac{4q_e^2 q_f^2 \epsilon}{N^2} + \frac{2q_e^2}{N^2}.$$

Definition and Probability of Bad Views. We first define bad views and upper bound their probability in the ideal world. For convenience, we denote

$$\begin{aligned}
&A = L \oplus F_1(R \oplus H_{k_1}(t)),\\
&B = R \oplus F_2(A \oplus H_{k_2}(t)) = R \oplus F_2(L \oplus F_1(R \oplus H_{k_1}(t)) \oplus H_{k_2}(t)),\\
&D = T \oplus F_{10}(S \oplus H_{k_{10}}(t)),\\
&C = S \oplus F_9(D \oplus H_{k_9}(t)) = S \oplus F_9(T \oplus F_{10}(S \oplus H_{k_{10}}(t)) \oplus H_{k_9}(t)).
\end{aligned}$$

Definition 3. *For the two worlds G_2 and G_3, we say that an attainable view $v = (Q_E, Q_{\boldsymbol{F}})$ is bad if one of the following conditions is fulfilled:*

- *(D-1) there exists two distinct records (t, LR, ST), $(t', L'R', S'T') \in Q_E$, such that $AB = A'B'$.*
- *(D-2) there exists two distinct records (t, LR, ST), $(t', L'R', S'T') \in Q_E$, such that $CD = C'D'$.*

Lemma 7.

$$\Pr\left[X_{id} \in \mathcal{V}_{bad}\right] \leq \frac{2q_e q_f^2}{N^2} + \frac{4q_e^2 q_f^2}{N^3} + \frac{4q_e^2 q_f^2 \epsilon}{N^2} + \frac{2q_e^2}{N^2}.$$

Proof. To upper bound the probability of bad views in the ideal world, we first define an event E':

- (E-1) there exists $(t, LR, ST) \in Q_E$, $(x_1, y_1) \in Q_{F_1}$, $(x_2, y_2) \in Q_{F_2}$ such that $H_{k_1}(t) \oplus R = x_1$ and $H_{k_2}(t) \oplus L \oplus y_1 = x_2$;
- (E-2) there exists $(t, LR, ST) \in Q_E$, $(x_9, y_9) \in Q_{F_9}$, $(x_{10}, y_{10}) \in Q_{F_{10}}$ such that $H_{k_{10}}(t) \oplus S = x_{10}$ and $H_{k_9}(t) \oplus T \oplus y_{10} = x_9$.

By the uniformity of $\mathcal{H}$, $\Pr[\text{(E-1)}] = \Pr[\text{(E-2)}] \leq \frac{q_e q_f^2}{N^2}$, thus we have that

$$\Pr[\mathsf{E}'] \leq \frac{2q_e q_f^2}{N^2}. \tag{6}$$

We then consider the probability to get a bad view under the condition that the event E' does not happen. Note that we only need to consider the case where $t \neq t'$, since the transformation is a permutation when $t = t'$ and it is impossible to hit a collision in AB or CD for distinct inputs. We analyze condition (D-1) and condition (D-2) respectively. Conditioned on $\neg\mathsf{E}'$, the probability to fulfil condition (D-1) is

$$\begin{aligned}\Pr[\text{(D-1)} \mid \neg\mathsf{E}'] &= \Pr[A = A' \wedge B = B' \mid \neg\mathsf{E}'] \\ &= \Pr[A = A' \mid \neg\mathsf{E}'] \cdot \Pr[B = B' \mid A = A', \neg\mathsf{E}'],\end{aligned}$$

where the event $A = A'$ is equivalent to

$$F_1(H_{k_1}(t) \oplus R) \oplus L = F_1(H_{k_1}(t') \oplus R') \oplus L', \tag{7}$$

and the event $B = B'$ conditioned on $A = A'$ is equivalent to

$$F_2(H_{k_2}(t) \oplus A) \oplus R = F_2(H_{k_2}(t') \oplus A) \oplus R'. \tag{8}$$

Given a pair $(t, LR, ST) \neq (t', L'R', S'T') \in Q_E$, we consider them in three cases.

Case (i) $H_{k_1}(t) \oplus R \notin Dom\mathcal{F}_1$ *and* $H_{k_2}(t) \oplus A \notin Dom\mathcal{F}_2$. The probability that $H_{k_1}(t) \oplus R = H_{k_1}(t') \oplus R$ is the probability that $H_{k_1}(t) \oplus H_{k_1}(t') = 0$, which is at most ϵ by the ϵ-AXU property of $\mathcal{H}$. Conditioned on $H_{k_1}(t) \oplus R \neq H_{k_1}(t') \oplus R$, the probability that Eq. (7) holds is $\frac{1}{N}$ by the uniformity of F_1. To sum up, $\Pr[A = A' \mid case(i), \neg\mathsf{E}']$ is at most $\epsilon + \frac{1}{N}$. Similarly, $\Pr[B = B' \mid A = A', case(i), \neg\mathsf{E}'] \leq \epsilon + \frac{1}{N}$. Then we have

$$\Pr[A = A' \wedge B = B' \mid case(i), \neg\mathsf{E}'] \leq \epsilon^2 + \frac{1}{N^2} + \frac{2\epsilon}{N}.$$

Case (ii) $H_{k_1}(t) \oplus R \notin Dom\mathcal{F}_1$, $H_{k_2}(t) \oplus A, H_{k_2}(t') \oplus A \in Dom\mathcal{F}_2$. The probability that case (ii) happens is bound by $\frac{q_f}{N} \cdot \frac{q_f}{N} = \frac{q_f^2}{N^2}$. In this case, we upper bound $\Pr[A = A' \wedge B = B' \mid case(ii), \neg\mathsf{E}']$ by $\Pr[A = A' \mid case(ii), \neg\mathsf{E}']$, which is at most $\epsilon + \frac{1}{N}$ (the analysis is similar with that in case (i)). Then we have

$$\Pr[A = A' \wedge B = B', case(ii) \mid \neg\mathsf{E}'] \leq \frac{q_f^2}{N^2} \cdot (\epsilon + \frac{1}{N}).$$

Case (iii) $H_{k_1}(t) \oplus R, H_{k_1}(t') \oplus R' \in Dom\mathcal{F}_1$. Then $H_{k_2}(t) \oplus A \notin Dom\mathcal{F}_2$ otherwise it fulfils condition (E-1). Similarly with case (ii), we have

$$\Pr[A = A' \wedge B = B', case(iii) \mid \neg\mathsf{E}'] \leq \frac{q_f^2}{N^2} \cdot (\epsilon + \frac{1}{N}).$$

Summing over all $\frac{q_e(q_e-1)}{2}$ possible pairs and all the three cases, we get

$$\Pr\left[A = A' \wedge B = B' \mid \neg \mathsf{E}'\right] \leq \frac{2q_e^2 q_f^2}{N^3} + \frac{2q_e^2 q_f^2 \epsilon}{N^2} + \frac{q_e^2}{N^2}.$$

The analysis of condition (D-2) is totally parallel to condition (D-1), where

$$\Pr\left[C = C' \wedge D = D' \mid \neg \mathsf{E}'\right] \leq \frac{2q_e^2 q_f^2}{N^3} + \frac{2q_e^2 q_f^2 \epsilon}{N^2} + \frac{q_e^2}{N^2}.$$

Then, we have

$$\Pr\left[X_{id} \in \mathcal{V}_{bad} \mid \neg \mathsf{E}'\right] \leq \frac{4q_e^2 q_f^2}{N^3} + \frac{4q_e^2 q_f^2 \epsilon}{N^2} + \frac{2q_e^2}{N^2}. \tag{9}$$

Finally, combined with Eq. 6 and Eq. 9, we upper bound the probability of had views in the ideal world by

$$\Pr\left[X_{id} \in \mathcal{V}_{bad}\right] \leq \Pr\left[\mathsf{E}'\right] + \Pr\left[X_{id} \in \mathcal{V}_{bad} \mid \neg \mathsf{E}'\right] \leq \frac{2q_e q_f^2}{N^2} + \frac{4q_e^2 q_f^2}{N^3} + \frac{4q_e^2 q_f^2 \epsilon}{N^2} + \frac{2q_e^2}{N^2}.$$

□

Analysis of Good Views. The condition of good views is easy to analyze.

Lemma 8. *For any good view v,*

$$\frac{\Pr\left[X_{re} = v\right]}{\Pr\left[X_{id} = v\right]} \geq 1.$$

Proof. Let v be a good view. For q_e records (t, LR, ST) in the view Q_E, the corresponding q_e values of AB as well as CD are distinct. Then, the event $G_2 \vdash Q_E$ is equivalent to the event that the random permutation Π extends the view $\{(A_i B_i, C_i D_i),\ i = 1, \ldots, q_e\}$. That is

$$\Pr\left[G_2 \vdash Q_E \mid \boldsymbol{F} \vdash \mathcal{Q}_{\boldsymbol{F}}\right] = \frac{1}{(N^2)_{q_e}}.$$

Then we have,

$$\begin{aligned}
\frac{\Pr\left[X_{re} = v\right]}{\Pr\left[X_{id} = v\right]} &= \frac{\Pr\left[k \xleftarrow{\$} \mathcal{K}, \widetilde{\Pi} \xleftarrow{\$} \mathsf{TP}(\mathcal{T}, 2n), \boldsymbol{F} \xleftarrow{\$} (\mathsf{F}(n))^{10} : \widetilde{\Pi} \vdash Q_E \wedge \boldsymbol{F} \vdash \mathcal{Q}_{\boldsymbol{F}}\right]}{\Pr\left[k \xleftarrow{\$} \mathcal{K}, \boldsymbol{F} \xleftarrow{\$} (\mathsf{F}(n))^{10} : \mathsf{TKAF} \vdash Q_E \wedge \boldsymbol{F} \vdash \mathcal{Q}_{\boldsymbol{F}}\right]} \\
&= \frac{\Pr\left[G_2 \vdash Q_E \mid \boldsymbol{F} \vdash \mathcal{Q}_{\boldsymbol{F}}\right]}{\prod_{i=1}^{m} \frac{1}{(N^2)_{q_i}}} \\
&\geq \frac{1}{(N^2)_{q_e}} \Big/ \prod_{i=1}^{m} \frac{1}{(N^2)_{q_i}} \geq 1.
\end{aligned}$$

□

Gathering this with Lemma 7 and Lemma 1 yiels Lemma 6. Combined with the upper bound of $\mathbf{Adv}_{G_1, G_2}(\mathcal{D})$, we finally prove Theorem 2.

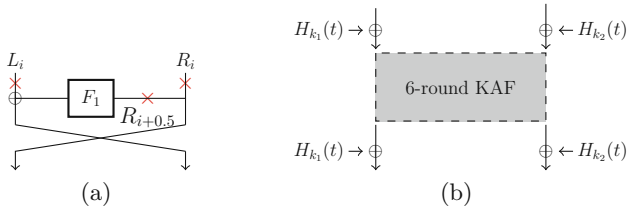

Fig. 3. (a) Possible Locations to Include Tweaks. (b) 6-Round TKAF.

6 Conclusion and Open Discussions

In this paper, we make some attempts to tweak Key-Alternating Feistel structures with provable security. We provide a 4-round scheme TKAFSF with birthday-bound security and a 10-round scheme TKAF with beyond-birthday-bound security. For the birthday-bound security, our proof is based on establishing the so-called point-wise proximity. We get positive results of theoretically minimal and round-optimal construction, with round functions of the form $F(H_k(t) \oplus x)$. For the beyond-birthday-bound security, our proof exploits the hybrid argument. The 6-round KAF given by Guo and Wang is used as a core in our construction, which can be replaced by a truly random permutation up to $2^{2n/3}$ queries. Finally we obtain an LRW-like construction and prove its security by using the H-coefficient technique. Intuitively, the TKAF scheme can be improved (in terms of number of rounds) if given a dedicated analysis, rather than an modular approach. We leave the round-optimal TKAF construction with beyond-birthday-bound security as future work.

Open Discussions. Differently from our target construction, Goldenberg et al. [16] utilize three types of locations (refer to Fig. 3(a)) in the dataflow to incorporate tweaks, the left and right halves of the input dataflow in each round and the dataflow before applying the corresponding round function, which are respectively denoted by $\mathcal{L}_i$, $\mathcal{R}_i$ and $\mathcal{R}_{i+0.5}$.

In our 4-round TKAFSF and 10-round TKAF constructions, we only consider incorporating tweaks at $\mathcal{R}_{i+0.5}$ locations to keep them in the general KAF structure. However, when considering all these three types of locations, there must be more possibilities for tweakable KAF ciphers with beyond-birthday-bound security. A straightforward way to build a BBB-secure TKAF with only 6 rounds is XORing tweak-dependent keys to the input and output of Guo-Wang's 6-round KAF, which is depicted in Fig. 3(b). Formally, such 6-round TKAF corresponding to random functions $\boldsymbol{F} = (F_1, F_2, \ldots, F_6)$ maps a key $k = (k_1, k_2, \ldots, k_8)$, a tweak $t \in \mathcal{T}$ and a message $L||R \in \{0,1\}^{2n}$ to the ciphertext defined as:

$$\mathsf{TKAF}_k^{\boldsymbol{F}}(t, LR) = \Psi_{k_8,t}^{F_6} \circ \ldots \circ \Psi_{k_4}^{F_2} \circ \Psi_{k_3}^{F_1}(L \oplus H_{k_2}(t)||R \oplus H_{k_1}(t)) \oplus (H_{k_1}(t)||H_{k_2}(t)).$$

Via a hybrid argument, the security of LRW2 [28] and the security of KAF [18] yields that this construction ensures security up to $2^{2n/3}$ adversarial queries.

Acknowledgments. We thank the reviewers for their helpful comments. This work is supported by the National Natural Science Foundation of China (61972248, 61702331, U1536101, 61602302, 61472250, 61672347), 13th five-year National Development Fund of Cryptography (MMJJ20170105, MMJJ20170114), National Key Research and Development Program of China (No. 2018YFB0803400, No. 2019YFB2101601), Natural Science Foundation of Shanghai (16ZR1416400), Shanghai Excellent Academic Leader Funds (16XD1401300), China Postdoctoral Science Foundation (2017M621471) and Science and Technology on Communication Security Laboratory.

References

1. Andreeva, E., Bogdanov, A., Luykx, A., Mennink, B., Tischhauser, E., Yasuda, K.: Parallelizable and authenticated online ciphers. In: Sako, K., Sarkar, P. (eds.) ASIACRYPT 2013. LNCS, vol. 8269, pp. 424–443. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-42033-7_22
2. Chakraborty, D., Sarkar, P.: HCH: a new tweakable enciphering scheme using the hash-encrypt-hash approach. In: Barua, R., Lange, T. (eds.) INDOCRYPT 2006. LNCS, vol. 4329, pp. 287–302. Springer, Heidelberg (2006). https://doi.org/10.1007/11941378_21
3. Chakraborty, D., Sarkar, P.: A general construction of tweakable block ciphers and different modes of operations. IEEE Trans. Inf. Theory **54**(5), 1991–2006 (2008)
4. Chen, S., Steinberger, J.: Tight security bounds for key-alternating ciphers. In: Nguyen, P.Q., Oswald, E. (eds.) EUROCRYPT 2014. LNCS, vol. 8441, pp. 327–350. Springer, Heidelberg (2014). https://doi.org/10.1007/978-3-642-55220-5_19
5. Cogliati, B., Lampe, R., Seurin, Y.: Tweaking even-mansour ciphers. In: Gennaro, R., Robshaw, M. (eds.) CRYPTO 2015. LNCS, vol. 9215, pp. 189–208. Springer, Heidelberg (2015). https://doi.org/10.1007/978-3-662-47989-6_9
6. Cogliati, B., Seurin, Y.: Beyond-birthday-bound security for tweakable even-mansour ciphers with linear tweak and key mixing. In: Iwata, T., Cheon, J.H. (eds.) ASIACRYPT 2015. LNCS, vol. 9453, pp. 134–158. Springer, Heidelberg (2015). https://doi.org/10.1007/978-3-662-48800-3_6
7. Cogliati, B., Seurin, Y.: On the provable security of the iterated even-mansour cipher against related-key and chosen-key attacks. In: Oswald, E., Fischlin, M. (eds.) EUROCRYPT 2015. LNCS, vol. 9056, pp. 584–613. Springer, Heidelberg (2015). https://doi.org/10.1007/978-3-662-46800-5_23
8. Crowley, P.: Mercy: a fast large block cipher for disk sector encryption. In: Goos, G., Hartmanis, J., van Leeuwen, J., Schneier, B. (eds.) FSE 2000. LNCS, vol. 1978, pp. 49–63. Springer, Heidelberg (2001). https://doi.org/10.1007/3-540-44706-7_4
9. Dodis, Y., Katz, J., Steinberger, J.P., Thiruvengadam, A., Zhang, Z.: Provable security of substitution-permutation networks. IACR Cryptology ePrint Archive 2017, 16 (2017)
10. Dworkin, M.J.: Recommendation for block cipher modes of operation: the XTS-AES mode for confidentiality on storage devices. Technical report (2010)
11. Even, S., Mansour, Y.: A construction of a cipher from a single pseudorandom permutation. In: Imai, H., Rivest, R.L., Matsumoto, T. (eds.) ASIACRYPT 1991. LNCS, vol. 739, pp. 210–224. Springer, Heidelberg (1993). https://doi.org/10.1007/3-540-57332-1_17
12. Farshim, P., Procter, G.: The related-key security of iterated even–mansour ciphers. In: Leander, G. (ed.) FSE 2015. LNCS, vol. 9054, pp. 342–363. Springer, Heidelberg (2015). https://doi.org/10.1007/978-3-662-48116-5_17

13. Feistel, H.: Cryptography and computer privacy. Sci. Am. **228**(5), 15–23 (1973)
14. Ferguson, N., et al.: The skein hash function family. Submission to NIST (round 3) **7**(7.5), 3 (2010)
15. Gentry, C., Ramzan, Z.: Eliminating random permutation oracles in the even-mansour cipher. In: Lee, P.J. (ed.) ASIACRYPT 2004. LNCS, vol. 3329, pp. 32–47. Springer, Heidelberg (2004). https://doi.org/10.1007/978-3-540-30539-2_3
16. Goldenberg, D., Hohenberger, S., Liskov, M., Schwartz, E.C., Seyalioglu, H.: On tweaking luby-rackoff blockciphers. In: Kurosawa, K. (ed.) ASIACRYPT 2007. LNCS, vol. 4833, pp. 342–356. Springer, Heidelberg (2007). https://doi.org/10.1007/978-3-540-76900-2_21
17. Granger, R., Jovanovic, P., Mennink, B., Neves, S.: Improved masking for tweakable blockciphers with applications to authenticated encryption. In: Fischlin, M., Coron, J.-S. (eds.) EUROCRYPT 2016. LNCS, vol. 9665, pp. 263–293. Springer, Heidelberg (2016). https://doi.org/10.1007/978-3-662-49890-3_11
18. Guo, C., Wang, L.: Revisiting key-alternating feistel ciphers for shorter keys and multi-user security. In: Peyrin, T., Galbraith, S. (eds.) ASIACRYPT 2018. LNCS, vol. 11272, pp. 213–243. Springer, Cham (2018). https://doi.org/10.1007/978-3-030-03326-2_8
19. Halevi, S.: EME*: extending EME to handle arbitrary-length messages with associated data. In: Canteaut, A., Viswanathan, K. (eds.) INDOCRYPT 2004. LNCS, vol. 3348, pp. 315–327. Springer, Heidelberg (2004). https://doi.org/10.1007/978-3-540-30556-9_25
20. Halevi, S., Rogaway, P.: A tweakable enciphering mode. In: Boneh, D. (ed.) CRYPTO 2003. LNCS, vol. 2729, pp. 482–499. Springer, Heidelberg (2003). https://doi.org/10.1007/978-3-540-45146-4_28
21. Halevi, S., Rogaway, P.: A parallelizable enciphering mode. In: Okamoto, T. (ed.) CT-RSA 2004. LNCS, vol. 2964, pp. 292–304. Springer, Heidelberg (2004). https://doi.org/10.1007/978-3-540-24660-2_23
22. Hoang, V.T., Tessaro, S.: Key-alternating ciphers and key-length extension: exact bounds and multi-user security. In: Robshaw, M., Katz, J. (eds.) CRYPTO 2016. LNCS, vol. 9814, pp. 3–32. Springer, Heidelberg (2016). https://doi.org/10.1007/978-3-662-53018-4_1
23. Jean, J., Nikolić, I., Peyrin, T.: Tweaks and keys for block ciphers: the `TWEAKEY` framework. In: Sarkar, P., Iwata, T. (eds.) ASIACRYPT 2014. LNCS, vol. 8874, pp. 274–288. Springer, Heidelberg (2014). https://doi.org/10.1007/978-3-662-45608-8_15
24. Lampe, R., Seurin, Y.: Tweakable blockciphers with asymptotically optimal security. In: Moriai, S. (ed.) FSE 2013. LNCS, vol. 8424, pp. 133–151. Springer, Heidelberg (2014). https://doi.org/10.1007/978-3-662-43933-3_8
25. Lampe, R., Seurin, Y.: Security analysis of key-alternating feistel ciphers. In: Cid, C., Rechberger, C. (eds.) FSE 2014. LNCS, vol. 8540, pp. 243–264. Springer, Heidelberg (2015). https://doi.org/10.1007/978-3-662-46706-0_13
26. Landecker, W., Shrimpton, T., Terashima, R.S.: Tweakable blockciphers with beyond birthday-bound security. In: Safavi-Naini, R., Canetti, R. (eds.) CRYPTO 2012. LNCS, vol. 7417, pp. 14–30. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-32009-5_2
27. Lee, B.H., Lee, J.: Tweakable block ciphers secure beyond the birthday bound in the ideal cipher model. In: Peyrin, T., Galbraith, S. (eds.) ASIACRYPT 2018. LNCS, vol. 11272, pp. 305–335. Springer, Cham (2018). https://doi.org/10.1007/978-3-030-03326-2_11

28. Liskov, M., Rivest, R.L., Wagner, D.: Tweakable block ciphers. In: Yung, M. (ed.) CRYPTO 2002. LNCS, vol. 2442, pp. 31–46. Springer, Heidelberg (2002). https://doi.org/10.1007/3-540-45708-9_3
29. Mennink, B.: XPX: generalized tweakable even-mansour with improved security guarantees. In: Robshaw, M., Katz, J. (eds.) CRYPTO 2016. LNCS, vol. 9814, pp. 64–94. Springer, Heidelberg (2016). https://doi.org/10.1007/978-3-662-53018-4_3
30. Minematsu, K.: Improved security analysis of XEX and LRW modes. In: Biham, E., Youssef, A.M. (eds.) SAC 2006. LNCS, vol. 4356, pp. 96–113. Springer, Heidelberg (2007). https://doi.org/10.1007/978-3-540-74462-7_8
31. Minematsu, K., Matsushima, T.: Tweakable enciphering schemes from hash-sum-expansion. In: Srinathan, K., Rangan, C.P., Yung, M. (eds.) INDOCRYPT 2007. LNCS, vol. 4859, pp. 252–267. Springer, Heidelberg (2007). https://doi.org/10.1007/978-3-540-77026-8_19
32. Mitsuda, A., Iwata, T.: Tweakable pseudorandom permutation from generalized feistel structure. In: Baek, J., Bao, F., Chen, K., Lai, X. (eds.) ProvSec 2008. LNCS, vol. 5324, pp. 22–37. Springer, Heidelberg (2008). https://doi.org/10.1007/978-3-540-88733-1_2
33. Nachef, V., Patarin, J., Volte, E.: Feistel Ciphers - Security Proofs and Cryptanalysis. Springer, Heidelberg (2017). https://doi.org/10.1007/978-3-319-49530-9
34. Naito, Y.: Tweakable blockciphers for efficient authenticated encryptions with beyond the birthday-bound security. IACR Transactions on Symmetric Cryptology **2017**(2), 1–26 (2017)
35. Patarin, J.: The "Coefficients H" technique. In: Avanzi, R.M., Keliher, L., Sica, F. (eds.) SAC 2008. LNCS, vol. 5381, pp. 328–345. Springer, Heidelberg (2009). https://doi.org/10.1007/978-3-642-04159-4_21
36. Patarin, J.: Generic attacks on feistel schemes. IACR Cryptology ePrint Archive 2008, 36 (2008). http://eprint.iacr.org/2008/036
37. Rogaway, P.: Efficient instantiations of tweakable blockciphers and refinements to modes OCB and PMAC. In: Lee, P.J. (ed.) ASIACRYPT 2004. LNCS, vol. 3329, pp. 16–31. Springer, Heidelberg (2004). https://doi.org/10.1007/978-3-540-30539-2_2
38. Rogaway, P., Bellare, M., Black, J.: OCB: a block-cipher mode of operation for efficient authenticated encryption. ACM Trans. Inf. Syst. Secur. **6**(3), 365–403 (2003)
39. Rogaway, P., Zhang, H.: Online ciphers from tweakable blockciphers. In: Kiayias, A. (ed.) CT-RSA 2011. LNCS, vol. 6558, pp. 237–249. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-19074-2_16
40. Sarkar, P.: Efficient tweakable enciphering schemes from (block-wise) universal hash functions. IEEE Trans. Inf. Theory **55**(10), 4749–4760 (2009)
41. Schroeppel, R., Orman, H.: The hasty pudding cipher. AES candidate submitted to NIST, p. M1 (1998)
42. Wang, L., Guo, J., Zhang, G., Zhao, J., Gu, D.: How to build fully secure tweakable blockciphers from classical blockciphers. In: Cheon, J.H., Takagi, T. (eds.) ASIACRYPT 2016. LNCS, vol. 10031, pp. 455–483. Springer, Heidelberg (2016). https://doi.org/10.1007/978-3-662-53887-6_17
43. Wang, P., Feng, D., Wu, W.: HCTR: a variable-input-length enciphering mode. In: Feng, D., Lin, D., Yung, M. (eds.) CISC 2005. LNCS, vol. 3822, pp. 175–188. Springer, Heidelberg (2005). https://doi.org/10.1007/11599548_15
44. Yaobin, S., Hailun, Y., Lei, W., Xuejia, L.: Secure key-alternating feistel ciphers without key schedule. Cryptology ePrint Archive, Report 2020/288 (2020). https://eprint.iacr.org