# Revisiting Key-alternating Feistel Ciphers for Shorter Keys and Multi-user Security[⋆]

Chun Guo[1] and Lei Wang[2,3⋆⋆]

[1] ICTEAM/ELEN/Crypto Group, Université Catholique de Louvain, Belgium
[2] Shanghai Jiao Tong University, Shanghai, China
[3] Westone Cryptologic Research Center, Beijing, China
chun.guo.sc@gmail.com,wanglei_hb@sjtu.edu.cn

**Abstract.** Key-Alternating Feistel (KAF) ciphers, a.k.a. Feistel-2 models, refer to Feistel networks 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. This model roughly captures the structures of many famous Feistel ciphers, and the most prominent instance is DES.

Existing provable security results on KAF assumed independent round-keys and round functions (ASIACRYPT 2004 & FSE 2014). In this paper, we investigate how to achieve security under simpler and more realistic assumptions: with round-keys derived from a short main-key, and hopefully with identical round functions.

For birthday-type security, we consider 4-round KAF, investigate the minimal conditions on the way to derive the four round-keys, and prove that when such adequately derived keys and the same round function are used, the 4-round KAF is secure up to $2^{n/2}$ queries.

For beyond-birthday security, we focus on 6-round KAF. We prove that when the adjacent round-keys are independent, and independent round-functions are used, the 6 round KAF is secure up to $2^{2n/3}$ queries. To our knowledge, this is the first beyond-birthday security result for KAF without assuming completely independent round-keys.

Our results hold in the multi-user setting as well, constituting the first non-trivial multi-user provable security results on Feistel ciphers. We finally demonstrate applications of our results on designing key-schedules and instantiating keyed sponge constructions.

**Keywords:** blockcipher, provable security, multi-user security, key-alternating cipher, Feistel cipher, key-schedule design, keyed sponge

## 1 Introduction

**Overview.** We extend provable security of models of practical Feistel ciphers along multi-axes. First, we (significantly) reduce the key-sizes needed for super pseudorandom security. Second, we provide the first non-trivial multi-user

[⋆] The full version is available [28].

[⋆⋆] Corresponding author.

provable results. We also exhibit applications of our results: on designing key-schedules for practical Feistel ciphers, and on instantiating keyed sponges.

**Background.** Practical iterative blockcipher (BC) designs roughly fall into two classes (with some rare exceptions such as IDEA), namely *Feistel ciphers and their generalizations*, and *substitution-permutation networks* (SPNs). In a Feistel cipher, in the $i$-th round, the intermediate state $x = x_L \| x_R$ is updated according to $x_L \| x_R \mapsto x_R \| x_L \oplus G_i(k_i, x_R)$, where $G_i$ is called the $i$-th round function. On the other hand, their counterpart SPNs could be further abstracted as the *iterated Even-Mansour* ($\mathsf{IEM}$) *ciphers*, or *key-alternating ciphers*, which consist of alternatively applying round-key additions and keyless round permutations, i.e. $\mathsf{IEM}^{P_1,\ldots,P_t}_{k_0,k_1,\ldots,k_t}(M) = k_t \oplus P_t(\ldots(k_1 \oplus P_1(k_0 \oplus M)))$.

The traditional security notion for BCs is *pseudorandomness*: for any adversary with reasonable resources (e.g. polynomial complexity), the BC with *a random and secret key* should be indistinguishable from a truly random permutation. Proving such security for concrete BCs such as AES seems out of the reach of current techniques. Yet, by idealizing the underlying round functions, security could be proved. Following this line, both idealized Feistel [38,36] and $\mathsf{IEM}$ [22,11] have been proposed and analyzed.

To obtain a $2n$-bit BC, the $\mathsf{IEM}$ model requires $2n$-bit permutations. Whereas following the Feistel approach, several $n$-to-$n$-bit functions suffice. Moreover, these functions need *not* to be *invertible* (this might be the reason why Feistel ciphers were extremely popular before 1990s). In all, Feistel ciphers could be built upon primitives with smaller domain and less structural properties, which is particularly appealing from a theoretical point of view. From the security point of view, without any additional hardness assumption other than the idealness of round functions, provable security is limited by the domain-size of the round functions [49]. Therefore, $\mathsf{IEM}$ benefits from the use of larger primitives: with $t$ independent $2n$-bit random permutations and $2tn$ key bits, $t$-round $\mathsf{IEM}$ is provably secure up to $2^{\frac{2tn}{t+1}}$ adversarial queries [15] which approaches $2^{2n}$ for large $t$. In contrast, Feistel models can only be secure against at most $2^n$ queries [49], which is far less than its domain-size $2^{2n}$. This upper bound is very unsatisfying. Despite this limitation as well as the gap between the idealized model and the rather weak round functions in practice, this provable approach supplies insights into the BC structures, excludes generic attacks, and may help refine designs. Due to these, this approach is valuable and has received a lot of attention.

**The Luby-Rackoff ($\mathsf{LR}$) Scheme,** in reference to the seminal work of Luby and Rackoff [38], might be the most popular model for Feistel ciphers so far. In this model, the round functions $G_i(k_i, x_R)$ are *pseudorandom functions* (PRFs). Via a standard hybrid argument, this is transposed to the Feistel networks formed by uniformly random and *Secret* round functions $SG_i(x_R)$. Following [38], a long series of work established either better security (maybe using a larger number of rounds)—with [40,49,31,3,44] to name a few,—or reduced complexity for security [52,47,45,46].

**Key-Alternating Feistel Ciphers.** Works along the line of Luby and Rackoff are very generic and could cover all possible forms of round functions. On the opposite side, the $\mathsf{LR}$ model falls short of showing how to concretely design *keyed* primitives (BCs) from (conceptually) simpler *keyless* primitives—it just "defers" the task to designing *keyed* round functions $G_i(k_i, x_R)$, which is, however, not known to be simpler than designing the BCs themselves.

In reality, general purpose Feistel ciphers usually employ length-preserving keyless round functions, and xor each round-key before applying the corresponding round function. Examples include DES, GOST, Camellia variant without $FL/FL^{-1}$ functions [9], MIBS [34], and two recent designs LBlock [57] and Twine [55] (they are multi-line generalizations of Feistel). This idea corresponds to Feistel networks with round functions instantiated in the probably simplest form of $G_i(k_i, x_i) = F_i(k_i \oplus x_i)$, where $F_i$ is *keyless and public*; and at the $i$-th round, the intermediate state is updated according to

$$x_L \| x_R \to x_R \| x_L \oplus F_i(k_i \oplus x_R).$$

This model was named *Key-Alternating Feistel* ($\mathsf{KAF}$) by Lampe and Seurin [36], and is also known as *Feistel-2* schemes according to IACR Tikz library. It has been extensively studied by the cryptanalytic community [9,33,29], and frequently became the instructive example for new attacks [10,2].

The gap between $\mathsf{LR}$ and $\mathsf{KAF}$ ciphers is non-negligible. For example, with less than $2^{2n}$ complexity, the best known generic key recovery attacks break 4-round $\mathsf{LR}$ [33] which is in sharp contrast with 6-round $\mathsf{KAF}$ [29]. Moreover, 6- or even 5-round $\mathsf{LR}$ model is already sufficient for optimal information theoretic security against $2^n$ queries [44, chapter 17]. However, for $\mathsf{KAF}$ we exhibit a generic *distinguishing attack* against $t$ rounds using $O(\frac{(t-2)n}{t-1})$ queries, which means $O(n)$ number of rounds are necessary for optimal security. These indicate the $\mathsf{LR}$ model misses some important structural properties in practical Feistel ciphers, and $\mathsf{KAF}$ is likely to be a better model for the reality.

By the above, theoretical analysis of the $\mathsf{KAF}$ model is of significance. In this respect, one would assume the (keyless) round functions $F_i$ as *public* random functions that can be queried by the adversary in a black-box way, and try to establish indistinguishability for the worlds $(\mathsf{KAF}_k, F_1, \ldots, F_t)$ and $(P, F_1, \ldots, F_t)$ in the random oracle model, i.e. the cipher $\mathsf{KAF}$ with a secret random key $k$ is indistinguishable from a random permutation $P$ even if given the access of the $t$ random round functions $F_1, \ldots, F_t$. This is very similar to the setting introduced for $\mathsf{IEM}$ [11]. In this vein, we are only aware of two works. First, an early work of Gentry and Ramzan (GR) [24] proved a birthday-type security for a 4-round keyless Feistel scheme with pre- and post-whitening keys, which can be translated into a 4-round $\mathsf{KAF}$ variant. Then, a recent work of Lampe and Seurin (LS) [36] proved beyond-birthday security up to $2^{\frac{tn}{t+1}}$ adversarial queries for $6t$-round $\mathsf{KAF}$, assuming the round functions and round-keys are *both completely independent* [36].[4]

**Our Problem.** The secret-key analyzes of $\mathsf{KAF}$ of GR [24] and LS [36] mentioned before leave two remarkable gaps. The first gap lies between the models

[4] A more recent work of Gilboa et al. [25] analyzed a variant of 2-round $\mathsf{IEM}$, which corresponds to a $\mathsf{KAF}$ variant *with whitening keys*. We'll elaborate later.

and ciphers in practice. In detail, both LS and GR assumed completely Independent Round-Keys (INDRK). In contrast, BCs in practice utilize identical round functions as well as round-keys derived from a short main-key (thus highly correlated rather than completely independent). Security arguments with correlated round-keys are desired to bridge this gap.

On the theoretical side, arguments with correlated round-keys reduce the amount of key required by secure cryptosystems, and sometimes lead to minimal designs [21,14]. Therefore, such arguments are of great importance from both practical and theoretical points of view, and while the INDRK assumption is common in seminal theoretical results, e.g. LR [38], IEM [11], and models for SPNs [41], subsequent works usually tried to remove it. For example, Patarin et al. analyzed the possibility of designing secure LR variants using a single random function (which is equivalent to pseudorandom function with a single round-key) [47,52,48,45,46]; Chen et al. analyzed 2-round IEM with **correlated** round-keys and even *identical* permutations [14]; and Dodis et al. proved results for SPN models with correlated round-keys [20].

Regarding the round complexity for beyond-birthday security, there is one more gap. While optimal security up to $2^n$ queries *cannot* be achieved by a small constant number of rounds of KAF (as discussed before), the optimal security of 6-round LR motivates ones to expect that the **6**-round KAF is at least beyond-birthday secure. However, LS only proved (beyond-birthday) security against $2n/3$ queries for **12**-round KAF, which is twice as the expected rounds.

**Contribution I: Security with Correlated Round-Keys.** We narrow the above gaps, and make the first step towards minimizing sufficient conditions for the provable security of KAF models. The results consist of two parts depending on the security goal.

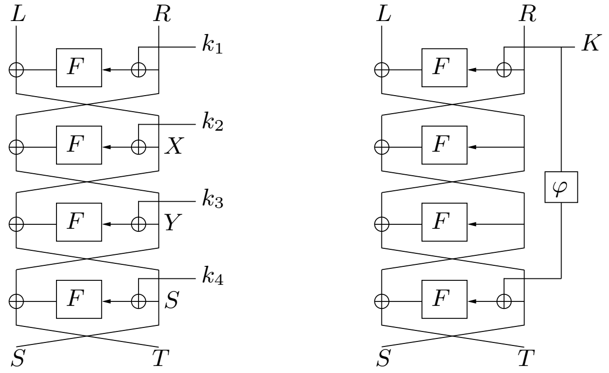

**Fig. 1.** (Left) The general 4-round KAFSF cipher in question. $F$ is a *public* random function. (Right) the "minimal" KAFSF scheme with birthday-type provable security. $\varphi$ is a fixed orthomorphism of $\mathbb{F}_2^n$.

Birthday-Type Security: Minimal Solution with 4 Rounds. In this regime, we consider the $\mathsf{KAF}$ ciphers with all the **round functions identical**, as depicted in Fig. 1 (left), and denote it $\mathsf{KAFSF}$ to make a clear distinction. For such variants, if the round-keys are also identical, then for $S\|T = \mathsf{KAFSF}(L\|R)$ it always holds $\mathsf{KAFSF}^{-1}(T\|S) = R\|L$, which means it can be distinguished by 2 queries (more severely, this allows ruining the secrecy of the plaintext in the CPA setting). Consequently, there have to be some non-trivial correlations between the round-keys. To unveil this, we investigate the minimal conditions on the round-keys that suffice for security. We prove that for the four $n$-bit round keys $(k_1, k_2, k_3, k_4)$, as long as $k_1$, $k_4$, and $k_1 \oplus k_4$ are all uniform (a quite mild requirement), the 4-round $\mathsf{KAFSF}$ is secure up to $2^{n/2}$ queries. The bound is tight, since any 4-round Feistel can be distinguished by $2^{n/2}$ queries [45].

This general result on the round-keys allows us to derive them from a short main-key in various ways. For the best efficiency, one could drop $k_2$ and $k_3$, and set $k_1 \leftarrow K$ and $k_4 \leftarrow \varphi(K)$, where $\varphi$ is an orthomorphism of $\mathbb{F}_2^n$, cf. Fig. 1 (right).[5] This yields a super pseudorandom $\mathsf{KAF}$ cipher from a single random function and an $n$-bit main-key. This construction is theoretically "minimal" in the sense that removing *any* of the components ruins security: removing $\varphi$ brings the severe weakness $\mathsf{KAFSF}(L\|R) = S\|T \Leftrightarrow \mathsf{KAFSF}^{-1}(T\|S) = R\|L$ back, while removing any call to $F$ brings us back to a 3-round Feistel network, which is not super pseudorandom. While it appears crazy to completely drop $k_2$ and $k_3$, this actually matches an early theoretical result of Ramzan and Reyzin [50], which will be discussed later. However, we stress our "minimal" scheme is of mainly theoretical interest. Most importantly, we are **not** advocating following **it** to design general purpose Feistel ciphers.

Birthday-type security is now usually deemed as quite weak. For example, general purpose Feistel BCs usually take $2n = 128$, for which a birthday-bound merely ensures 32-bit security. Though, we believe it's of significance to deepen the understanding of birthday-type security, shape existing results, and derive theoretically minimal constructions.

Beyond-Birthday Security: Improved Results with 6 Rounds. For $\mathsf{KAF}$ built upon **independent** round functions, see Fig. 2 (left), we prove security up to $2^{2n/3}$ adversarial queries as long as the six round-keys $(k_1, k_2, k_3, k_4, k_5, k_6)$ are uniform and *adjacent round-keys are independent*. It seems such a sequence of round-keys can be easily derived from a $2n$-bit main-key $K\|K'$ via the "word-aligned", feedback-shift-register-based key-schedules that are widely adopted. As far as we know, this is the first beyond-birthday result on $\mathsf{KAF}$ without INDRK assumption.

More generally, when $k_1$, $k_3$, and $k_5$ are uniform in $2^n$ values, while $k_2$, $k_4$, and $k_6$ are uniform in only $2^{n-r}$ values, security is up to $2^{(2n-r)/3}$ queries. While such round-keys appear quite artificial, it's valuable for two reasons: first, it appears

[5] A permutation $\varphi$ of $\mathbb{F}_2^n$ is an orthomorphism if $K \mapsto K \oplus \varphi(K)$ is also a permutation. The Feistel-like linear transformation $\varphi(K_L\|K_R) = K_L \oplus K_R\|K_L$ is a very efficient instance. Orthomorphisms have found many cryptographic applications, particularly in minimizing $\mathsf{LR}$ [52] and $\mathsf{IEM}$ models [14].

the first step towards modeling key-schedules of the form $\{0,1\}^{cn} \to \{0,1\}^{tn}$ for non-integers $c$; second, it cinches interesting implications on "partial-key" Even-Mansour and keyed sponges, which will be discussed latter.

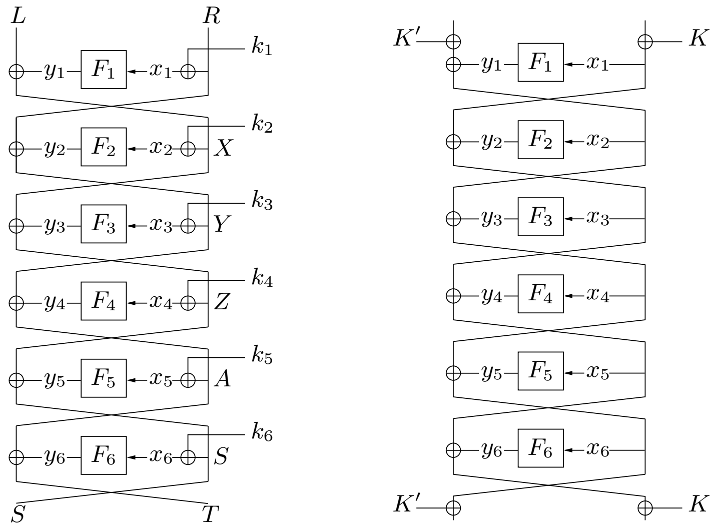

**Fig. 2.** (Left) The 6-round KAF ciphers with notations used in this paper. $F_1, \ldots, F_6$ are six independent public random functions. (Right) The single-key Even-Mansour cipher based on a 6-round keyless Feistel permutation $\mathsf{LR}_6$.

**Application: A Concret Proposal for KAF Key-Schedules.** Although our results turn heuristic once instantiated [13], we believe they shed some light on how to design key-schedules for practical Feistel ciphers, which appear quite non-trivial. In particular, key-schedules of KAF ciphers need not to be overly strong nor "one-way", and actually key-schedules with some simple combinatorial properties could be a good starting point (a similar conclusion has been made for the IEM ciphers [14]).

To further illustrate, based on our results and some additional intuitions, we propose to consider key-schedules that produce *pair-wise independent round-keys*[6] in KAF ciphers. We further demonstrate examples of such key-schedules. However, we stress that these proposals only serve as *starting points for further research*, and should *not* be used without deeper investigations.

**Multi-User (MU) Setting.** The discussed super pseudorandomness model is now termed as *single-user* (SU) setting. It has been noticed that in practice, cryptosystems are typically deployed en masse and attackers are often satisfied

[6] This should be distinguished from complete independence. For example, given the main-key $K \| K'$, the round-keys $K, K', K \oplus K'$ are pair-wise independent, but they aren't completely independent. In fact, appealing to pair-wise independence instead of complete independence is an approach to derandomization [37].

with compromising some users among many, which can be substantially easier [8]. In fact, massively parallel attacks on many keys at once have been considered as the most promising way to break AES-128 [6]. These motivated the *multi-user* (MU) security notion [5] and a lot of follow up works—please see [12] and the references therein. For BCs, this could even affect higher-level systems: frequently rekeying is sometimes used in BC-based modes in order to achieve better security bounds [26] or leakage resilience [54], and the security of such modes inherently relies on the MU security of the underlying BCs.

According to Mouha and Luykx [42], the MU security of BCs was formalized as $m > 1$ instances of BCs with $m$ independent user-keys being indistinguishable from $m$ *independent random permutations*. This could be related to the SU security: with $m$ independent keys, a generic reduction shows the MU security is $\log m$ bits less than the SU security (Jager et al. showed that this is unavoidable for generic reductions [35]). This is quantitatively weaker. Yet, interestingly, dedicated analyzes could usually establish MU bounds that are quantitatively the *same* as SU bounds [42,56,32].

**Contribution II: MU Security of KAF.** As mentioned, the MU security may be quantitatively weaker than the MU security. Yet, our positive results are proved via establishing the so-called *point-wise proximity* of Hoang and Tessaro [32], and our bounds satisfy their "super-additiveness" requirement. Therefore, by their general transition, these establish MU security against $2^{n/2}$ queries at 4 rounds and against $2^{(2n-r)/3}$ queries at 6 rounds. To our knowledge, these constitute the first non-trivial MU provable results on Feistel ciphers.

We remark that it's not as trivial as it appears to ensure "super-additiveness" during the analysis. For example, this requires to get rid of terms of the form $f(q_f)$ or $f(q_f) \cdot \sqrt{q_e}$. In particular, our proof follows a "two-step" approach used by Cogliati et al. for analyzing tweakable Even-Mansour [16,17], yet neither of the bounds given in these works fulfills this requirement. To resolve this, we eschew many concrete approaches used in [16,17] (in particular, the use of Markov inequality), and extensively use the expectation method from [32] instead, to derive more "smooth" bounds.

As a final remark, Hoang and Tessaro proved that the SU and MU security bounds of IEM with INDRK are quantitatively the same [32]. While our results appear to indicate the same conclusion, we don't expect this to be true for KAF in general. A deeper investigation is left for future.

**Implications.** As multi-user secure BCs, our provable KAF constructions could be plugged into many BC-based (secret-key) modes to reduce the size of (ideal) primitives in use, or to drop the requirement on the invertibility of the underlying ideal primitives. The latter is particularly attractive in the multi-party computation setting, in which invertibility could be quite expensive [51]. In addition, depending on the concrete parameters, in some cases, e.g. truncated CBC [23], this even does not result in a security loss.

Less obviously, our general results on 6-round KAF imply that it's secure to alternatively use an $n$-bit key $K$ and another $(n-r)$-bit key $K'$ at each round. With such an alternating key-schedule, the 6-round KAF collapses to a 1-round

$\mathsf{IEM}$ with key $0^r\|K'\|K$ and the permutation instantiated by a 6-round keyless Feistel permutation $\mathsf{LR}_6$, as in Fig. 2 (right). Therefore, this shows *instantiating the permutation $\pi$ in the 1-round "Partial-Key" Even-Mansour*

$$\mathsf{PKEM}^{\pi}_{0^r\|K'\|K}(M) = (0^r\|K'\|K) \oplus \pi((0^r\|K'\|K) \oplus M) \tag{1}$$

*by a 6-round keyless Feistel permutation $\mathsf{LR}_6$ preserves security, and for $r > n/2$ the security is beyond-birthday with respect to the domain-size of the underlying ideal primitives.* This extends the birthday-type result of GR [24] (two more Feistel rounds for beyond-birthday security).

This results in even more interesting implications. Sponge functions are versatile cryptographic primitives [7]. Keyed sponges can be used for encryption and message authentication. Many variants of lightweight keyed sponges can be rewritten as a construction built upon the aforementioned $\mathsf{PKEM}^{\pi}_{0^r\|K'\|K}$ cipher, and the sponge is secure as long as $\mathsf{PKEM}^{\pi}_{0^r\|K'\|K}$ is secure (maybe in the MU setting) [43,1,23]. Thus by the above implication, such keyed sponges could rely on $\mathsf{PKEM}^{\mathsf{LR}_6}_{0^r\|K'\|K}$ instead of $\mathsf{PKEM}^{\pi}_{0^r\|K'\|K}$. With the keys canceled, we obtain a sponge built upon $\mathsf{LR}_6$. Therefore, our results indicate: *the random permutation underlying many keyed sponge variants could be securely instantiated with a 6-round keyless Feistel permutation $\mathsf{LR}_6$.* For concrete security results please see Section 7.

We stress that these results *cannot* be derived from existing provable results on $\mathsf{IEM}$/keyed sponges and keyless Feistel via general transitions. The most relevant results are the correlation intractability [39] and CP-indifferentiability [53] positive results on $\mathsf{LR}_6$. But they are quantitatively weak: $q^4/2^n$ for correlation intractability of $\mathsf{LR}_6$ [39], and $q^6/2^n$ for CP-indifferentiability of $\mathsf{LR}_{\mathbf{5}}$ [53].

**Table 1.** Comparison to existing provable results on $\mathsf{KAF}$. We stress that our results include more general ones that allow deriving the round-keys in flexible ways. And rows 4 and 5 are the *theoretically best possible* ones derived from the general ones.

| Key size | Rounds | Num. of rand. func. | SU bound | MU bound | Reference |
|---|---|---|---|---|---|
| $4n$ | 4 | 2 | $n/2$ | missed | GR [24] |
| $12n$ | 12 | 12 | $2n/3$ | missed | LS [36] |
| $6tn$ | $6t$ | $6t$ | $tn/(t+1)$ | missed | LS [36] |
| $\boldsymbol{n}$ | **4** | **1** | $n/2$ | $\boldsymbol{n/2}$ | Section 4 |
| $\boldsymbol{2n}$ | **6** | **6** | $2n/3$ | $\boldsymbol{2n/3}$ | Section 5 |

**Discussion, and Comparison to Related Works.** It would be tempting to ask how we are able to halve the round complexity for $2n/3$ security (compared with LS [36]). Briefly, LS divided a $\mathsf{KAF}$ cipher into two halves, proved NCPA (non-adaptive chosen-plaintext attack) security for each half, and then applied a composition to obtain CCA security. And (informally) their *coupling* argument could only reduce certain collision probability every 3 rounds. Consequently, they only obtained $2n/3$ NCPA security at 6 rounds and $2n/3$ CCA security at 12 rounds. In comparison, we follow a "two-step" approach [16,17] for analyzing the *transcripts* of queries and answers of the distinguisher, transform the transcripts into input-output pairs of the inner four rounds, and then employ a more fine-grained and dedicated analysis. This allows us to remove much redundancy from the structures and successfully halve the rounds. Due to the randomness of the 1st and 6th round functions, every resulted input-output pair of the inner four rounds would only be involved in a single collision (one could see Fig. 4 for illustration), and this significantly simplifies the analysis. Still, the analysis for 4 rounds remains complicated, and the complexity is further increased by the aim of "super-additiveness" (as mentioned). We remark that such an analysis for 4-round KAF seems missing in the literature—Patarin's mirror theory-based analysis for 4-round LR [44, chapter 17] does not seem to be transposable to KAF.

On the other hand, our 6-round construction(s) could probably be further simplified while retaining $2n/3$-bit security. However, we figured out some difficulties, see the full version. Since verifiability of the proof is equally important, we favored the current construction and its relatively simpler proof. Despite this, our 6-round construction with $2n$-bit main-keys has significantly improved upon existing results. In Table 1, we make comparison with the results of LS [36] and GR [24]. We remark that GR's main motivation was to deepen the understanding of the Even-Mansour cipher [22], rather than to study KAF ciphers.

Also, we list the relevant results on the popular LR and IEM models in Table 2 for comparison. We remark that LR results are in the *standard model*, and are better than the *ideal model* results on IEM and KAF in some theoretical sense. Yet, as emphasized before, KAF is closer to reality.

The results in Table 2 in particular include the aforementioned work of Gilboa et al., which proved $n/2$ security for a 2-round IEM variant with identical round-permutations and identical round-keys [25]. Moreover, the round-permutation is instantiated with a 2-round LR construction built upon *a public random permutation*. This construction is somewhat related to KAF: but it can only be transformed into a KAF variant with whitening keys rather than the "bare" KAF model studied in this paper (thus we denote KAFSP$^*$). Consequently, our result on 4-round KAFSF—as well as the usefulness of orthomorphisms in this setting—could not be derived from [25].

In addition, Ramzan and Reyzin proved birthday-type security for a variant of 4-round LR, in which the middle two round functions are *public* rather than secret [50]. As mentioned before, an interesting fact is that our 4-round minimal construction also captures the idea of leaving the middle two round functions "unprotected" (as the middle two round-keys are absent). In this sense, our minimal construction also deepen the understanding of the secrecy of round functions in Feistel ciphers.

Last, a series of papers analyzed idealized BCs in the indifferentiability framework, which is a different security model. Please see [19] and the references therein. Among them is a positive result [27] on a variant of KAF abstracted from NSA's cipher SIMON [4]. These works shed lights on designing key-schedules from a different point of view, and are thus complementary to ours.

**Table 2.** Comparison to LR and IEM *super pseudorandom* provable results. For the LR results, $\kappa$ is the key-size of the underlying PRFs. For the first row: the proof used the mirror theory [44, chapter 14], and was only sketched in [44, chapter 17.5]. For row 2: it's the best result to our knowledge. For row 4 & 5, the MU bounds of EMIP and EMSP models were not given, yet are trivial: (a) with $2n$ key bits, it $\leq n$-bit [8], while (b) it $\geq n$-bit, which is the MU security of the 1-round single-key IEM [32].

| Model | Block Size | Prim. Size | Key Size | Rounds | Number of Prim. | SU Bound | MU Bound | Reference |
|---|---|---|---|---|---|---|---|---|
| LR | $2n$ | $n$ | $5\kappa$ | 5 | 5 | $\approx n$ | missed | [44] |
| LR | $2n$ | $n$ | $\kappa$ | 4 | 1 | $n/2$ | missed | Nandi [45] |
| IEM | $2n$ | $2n$ | $2tn$ | $t$ | $t$ | $2tn/(t+1)$ | $2tn/(t+1)$ | CS&HT[15,32] |
| EMIP | $2n$ | $2n$ | $2n$ | 2 | 2 | $4n/3$ | $n$ | Chen et al. [14] |
| EMSP | $2n$ | $2n$ | $2n$ | 1 | 2 | $4n/3$ | $n$ | Chen et al. [14] |
| KAFSP* | $2n$ | $n$ | $2n$ | 4 | 1 | $n/2$ | missed | Gilboa et al. [25] |
| KAF | $2n$ | $n$ | $6tn$ | $6t$ | $6t$ | $tn/(t+1)$ | missed | LS [36] |
| KAFSF | $2n$ | $n$ | $n$ | 4 | 1 | $n/2$ | $n/2$ | Section 4 |
| KAF | $2n$ | $n$ | $2n$ | 6 | 6 | $2n/3$ | $2n/3$ | Section 5 |

**Organization.** Section 2 supplies notations and definitions. Section 3 describes the generic distinguishing attack against any number of rounds. Then, Sections 4 and 5 respectively present our results on 4-round KAFSF and 6-round KAF and their security proofs. After these, based on our results, Section 6 presents our key-schedule proposal, while Section 7 makes discussion on the implications.

## 2 Preliminaries

**Notation and General Definitions.** In all the following, we fix an integer $n \geq 1$ and denote $N = 2^n$. Further denote $\mathcal{F}(n)$ the set of all functions of domain $\{0,1\}^n$ and range $\{0,1\}^n$, and $\mathcal{P}(2n)$ the set of all permutations on $\{0,1\}^{2n}$. For a random variable $\epsilon(s)$ that relies on another random variable $s$, we denote by $\mathbb{E}_{s\in\mathcal{S}}[\epsilon(s)]$ the expectation of $\epsilon(s)$ taken over all $s \in \mathcal{S}$, and $\mathbb{E}_s[\epsilon(s)]$ for short when the set $\mathcal{S}$ is clear from the context. For $X, Y \in \{0,1\}^n$, $X\|Y$ or simply $XY$ denotes their concatenation.

Assume that the $i$-th round function of KAF is $F_i : \{0,1\}^n \to \{0,1\}^n$, and the corresponding $n$-bit round-key is $k_i$, then the $i$-th round transformation of KAF is the permutation on $\{0,1\}^{2n}$ defined as

$$\Psi_{k_i}^{F_i}(W_{i-1}\|W_i) = W_i\|W_{i+1} = W_i\|W_{i-1} \oplus F_i(K_i \oplus W_i),$$

where $W_{i-1}$ and $W_i$ are the left and right $n$-bit halves of the inputs of the $i$-th round respectively. And the $t$-round KAF is specified by $t$ public round functions $F = (F_1, \ldots, F_t)$ and a round-key vector $k = (k_1, \ldots, k_t)$:

$$\mathsf{KAF}_k^F(W_0\|W_1) = \Psi_{k_t}^{F_t} \circ \ldots \circ \Psi_{k_1}^{F_1}(W_0\|W_1).$$

These functions may be completely independent, or correlated, or even identical. To highlight, we denote by KAFSF the variant with identical round function, i.e.

$$\mathsf{KAFSF}_k^F(M) = \Psi_{k_t}^F \circ \ldots \circ \Psi_{k_1}^F(M).$$

Note that the key spaces of these schemes are not fixed, and depend on the concrete contexts.

As noted in [18], a $\mathsf{KAF}$ cipher with an even number of rounds can be seen as a special case of an *IEM cipher*. In detail, two rounds of a $\mathsf{KAF}$ cipher can be rewritten as:

$$\Psi_{k_{i+1}}^{F_{i+1}} \circ \Psi_{k_i}^{F_i}(W_{i-1}\|W_i) = (k_{i+1}\|k_i) \oplus \Psi_0^{F_{i+1}} \circ \Psi_0^{F_i}((k_{i+1}\|k_i) \oplus (W_{i-1}\|W_i)),$$

where $\Psi_0^{F_{i+1}} \circ \Psi_0^{F_i}$ is a two-round keyless Feistel permutation. As a consequence, *in general*, $\mathsf{KAF}$ ciphers should *avoid* using identical round-key, as otherwise the round-keys would cancel each other and the cipher would collapse to a single round $\mathsf{IEM}$ cipher using a keyless Feistel as the permutation and $k\|k$ as the pre- and post-whitening key.[7]

For convenience—in particular, to simplify subscripts,—we follow a classical notation system (which has been used for Luby-Rackoff schemes [49]):

– for 4-round $\mathsf{KAF}(\mathsf{SF})$, we take $L, R, X, Y, S, T$ as $W_0, W_1, W_2, W_3, W_4, W_5$ correspondingly, as depicted in Fig. 1 (left);
– for 6-round $\mathsf{KAF}(\mathsf{SF})$, we take $L, R, X, Y, Z, A, S, T$ as $W_0, W_1, \ldots, W_6, W_7$ correspondingly, as in Fig. 2 (left).

**Multi-User (MU) Security of Blockciphers.** We concentrate on the MU security with $m$ users. The SU security definition corresponds to the special case of $m = 1$. Concretely, consider a $t$-round $\mathsf{KAF}$ built from $t$ $n$-to-$n$-bit function oracles $\mathbf{F} = (\mathbf{F}_1, \ldots, \mathbf{F}_t)$. Only the round-key vectors $k$ with certain context-dependent properties (will be identified) can ensure security. We denote by $\mathcal{K}$ the set of all $k$ with such desired properties. To study the indistinguishability, we consider a distinguisher $D$ interacting with $\mathbf{F}$. In the MU setting, $D$ has access to additional $m$ $2n$-bit permutation oracles, which are either $m$ instances $\mathsf{KAF}^{\mathbf{F}}_{k^{(1)}}, \ldots, \mathsf{KAF}^{\mathbf{F}}_{k^{(m)}}$ with $m$ independent keys uniformly picked from $\mathcal{K}$, or $m$ independent random permutations $\mathbf{P}^{(1)}, \ldots, \mathbf{P}^{(m)}$. The goal of $D$ is to tell apart the two worlds $(\mathsf{KAF}^{\mathbf{F}}_{k^{(1)}}, \ldots, \mathsf{KAF}^{\mathbf{F}}_{k^{(m)}}, \mathbf{F})$ (termed the *real world*) and $(\mathbf{P}^{(1)}, \ldots, \mathbf{P}^{(m)}, \mathbf{F})$ (the *ideal world*) by adaptively making forward and backward queries to each of the permutations and the functions. Formally, $D$'s distinguishing advantage is defined as

$$\begin{aligned}\mathbf{Adv}^{\mathrm{MU}}_{\mathsf{KAF}}(D) = &\Pr[(\mathbf{P}^{(1)}, \ldots, \mathbf{P}^{(m)}) \xleftarrow{\$} (\mathcal{P}(2n))^m, \mathbf{F} \xleftarrow{\$} (\mathcal{F}(n))^t : D^{\mathbf{P}_1, \ldots, \mathbf{P}_m, \mathbf{F}} = 1] \\ &- \Pr[(k^{(1)}, \ldots, k^{(m)}) \xleftarrow{\$} (\mathcal{K})^m, \mathbf{F} \xleftarrow{\$} (\mathcal{F}(n))^t : D^{\mathsf{KAF}^{\mathbf{F}}_{k^{(1)}}, \ldots, \mathsf{KAF}^{\mathbf{F}}_{k^{(m)}}, \mathbf{F}} = 1].\end{aligned}$$

Furthermore, we consider computationally unbounded distinguishers, and we assume without loss of generality that the distinguisher is deterministic and never makes redundant queries. For non-negative integers $q_f$ and $q_e$, we define the insecurity of the idealized $\mathsf{KAF}$ cipher as:

$$\mathbf{Adv}^{\mathrm{MU}}_{\mathsf{KAF}}(q_f, q_e) = \max_D \mathbf{Adv}^{\mathrm{MU}}_{\mathsf{KAF}}(D),$$

[7] In page 8, we indeed take the implication on $\mathsf{PKEM}$ as an interesting one. But that implication concentrates on *specific theoretical models*, and does not intend to say anything about *general purpose* Feistel ciphers.

where the maximum is taken over all distinguishers $D$ making exactly $q_f$ queries to each function oracle and in total $q_e$ queries to the permutation oracles (termed as $(q_f, q_e)$-distinguishers).

If a collision occurs among the $m$ user keys, e.g. $k^{(i)} = k^{(j)}$, then $D$ can easily distinguish: in the real world, $\mathsf{KAF}^{\mathbf{F}}_{k^{(i)}}$ and $\mathsf{KAF}^{\mathbf{F}}_{k^{(j)}}$ are the same, while in the ideal world the corresponding oracles $\mathbf{P}^{(i)}$ and $\mathbf{P}^{(j)}$ are independent. For $(q_f, q_e)$-distinguishers, the number of involved users $m$ cannot exceed $q_e$. Thus such a collision happens with probability at most $\frac{q_e^2}{2|\mathcal{K}|}$. For simplicity, throughout the remaining, we only consider the MU setting in which all the involved user keys are *distinct*; and the bounds in the "normal" MU setting can be derived as our bounds plus the term $\frac{q_e^2}{2|\mathcal{K}|}$ (this approach resembles [32]).

As mentioned, setting $m \leftarrow 1$, we obtain $\mathbf{Adv}^{\mathsf{SU}}_{\mathsf{KAF}}$, which measures the advantage of $D$ on distinguishing one $\mathsf{KAF}$ instance from a random permutation.

**H-Coefficients.** We utilize the H-coefficient technique [47,15], and follow the paradigm of Hoang and Tessaro (HT) [32]. For this, we summarize the interaction of $D$ with its oracles in the *queries transcripts*. Suppose $D$ making $q_i$ queries to the $i$-th permutation oracle ($\mathbf{P}^{(i)}$ or $\mathsf{KAF}^{\mathbf{F}}_{k^{(i)}}$), which are recorded as a set

$$\mathcal{Q}_{E_i} = \{(L_1R_1, S_1T_1), \ldots, (L_{q_i}R_{q_i}, S_{q_i}T_{q_i})\},$$

where for $j = 1, \ldots, q_i$ the tuples $(L_jR_j, S_jT_j) \in \{0,1\}^{2n} \times \{0,1\}^{2n}$ indicate the queries and answers. On the other hand, for $i = 1, \ldots, t$, the queries made to $F_i$ are recorded as

$$\mathcal{Q}_{F_i} = \{(x_{i,1}, y_{i,1}), \ldots, (x_{i,q_f}, y_{i,q_f})\},$$

in which for each $j \in [1, \ldots, q_f]$, it indicates $F_i$ was queried on $x_{i,j}$ and answered with $y_{i,j}$. Let $\mathcal{Q}_E = (\mathcal{Q}_{E_1}, \ldots, \mathcal{Q}_{E_m})$ and $\mathcal{Q}_F = (\mathcal{Q}_{F_1}, \ldots, \mathcal{Q}_{F_t})$. Then the pair $\tau = (\mathcal{Q}_E, \mathcal{Q}_F)$ will be called the *transcript* of the distinguisher in the MU setting: it contains all the information obtained by $D$ during the interaction. In the SU setting, we have to focus on only one permutation oracle; therefore, we drop the index $i$ and simply write $\mathcal{Q}_E = \{(L_1R_1, S_1T_1), \ldots, (L_{q_i}R_{q_i}, S_{q_i}T_{q_i})\}$ for the permutation query transcript and write $\tau = (\mathcal{Q}_E, \mathcal{Q}_F)$. Note that queries are recorded in a directionless (for permutation queries) and unordered fashion, but since $D$ is assumed deterministic, there is a one-to-one mapping between this representation and the raw transcript of the interaction of $D$ with its oracles (a formal proof could be found in [15]). Also, the output of $D$ is a deterministic function of $\tau$.

Given a set $\mathcal{Q}_{F_i}$ of function queries and a function $\mathbf{F}_i$, we say that $\mathbf{F}_i$ *extends* $\mathcal{Q}_{F_i}$, denoted $\mathbf{F}_i \vdash \mathcal{Q}_{F_i}$, if $\mathbf{F}_i(x) = y$ for all $(x, y) \in \mathcal{Q}_{F_i}$. Similarly, given a transcript of permutation queries $\mathcal{Q}_{E_i}$ and a permutation $\mathbf{P}^{(i)}$, we say $\mathbf{P}^{(i)}$ *extends* $\mathcal{Q}_{E_i}$, denoted $\mathbf{P}^{(i)} \vdash \mathcal{Q}_{E_i}$, if $\mathbf{P}^{(i)}(LR) = ST$ for all $(LR, ST) \in \mathcal{Q}_{E_i}$. The latter definition also extends to the $t$-round $\mathsf{KAF}$ cipher built upon $\mathbf{F}$ and a key $k^{(i)}$; in that case, we write $\mathsf{KAF}^{\mathbf{F}}_{k^{(i)}} \vdash \mathcal{Q}_{E_i}$. Finally, for $\mathcal{Q}_F = (\mathcal{Q}_{F_1}, \ldots, \mathcal{Q}_{F_t})$ and $\mathbf{F} = (\mathbf{F}_1, \ldots, \mathbf{F}_t)$, if $\mathbf{F}_1 \vdash \mathcal{Q}_{F_1} \wedge \ldots \wedge \mathbf{F}_t \vdash \mathcal{Q}_{F_t}$, then $\mathbf{F} \vdash \mathcal{Q}_F$.

For all possible transcript $\tau$ that describes a possible interaction with either a tuple of oracles $(\mathbf{P}^{(1)}, \ldots, \mathbf{P}^{(m)}, \mathbf{F})$ or $(\mathsf{KAF}^{\mathbf{F}}_{k^{(1)}}, \ldots, \mathsf{KAF}^{\mathbf{F}}_{k^{(m)}}, \mathbf{F})$, we denote

$\Pr_{re}(\tau)$, resp. $\Pr_{id}(\tau)$, the probability that $D$'s interaction with the real world, resp. the ideal world, produces $\tau$. Formally,

$$\begin{aligned}\Pr_{re}(\tau) = \Pr[(k^{(1)}, \ldots, k^{(m)}) \xleftarrow{\$} (\mathcal{K})^m, \mathbf{F} \xleftarrow{\$} (\mathcal{F}(n))^t :\\ \mathsf{KAF}^{\mathbf{F}}_{k^{(1)}} \vdash \mathcal{Q}_{E_1} \wedge \ldots \wedge \mathsf{KAF}^{\mathbf{F}}_{k^{(m)}} \vdash \mathcal{Q}_{E_m} \wedge \mathbf{F} \vdash \mathcal{Q}_F],\\ \Pr_{id}(\tau) = \Pr[(\mathbf{P}^{(1)}, \ldots, \mathbf{P}^{(m)}) \xleftarrow{\$} (\mathcal{P}(2n))^m, \mathbf{F} \xleftarrow{\$} (\mathcal{F}(n))^t :\\ \mathbf{P}^{(1)} \vdash \mathcal{Q}_{E_1} \wedge \ldots \wedge \mathbf{P}^{(m)} \vdash \mathcal{Q}_{E_m} \wedge \mathbf{F} \vdash \mathcal{Q}_F].\end{aligned}$$

With these definitions, the core lemma of the H-coefficients technique states that the distinguishing advantage could be inferred from the ratio of $\Pr_{re}(\tau)$ and $\Pr_{id}(\tau)$ (which is a function of $q_f$ and $q_e$).

**Lemma 1 (From [32]).** *Assume that in the atk setting (atk $\in \{SU, MU\}$), there is a function $\varepsilon(q_f, q_e) > 0$ such that for every possible transcript $\tau$ with $q_e$ and $q_f$ queries of the two types it holds*

$$\Pr_{id}(\tau) - \Pr_{re}(\tau) \leq \Pr_{id}(\tau) \cdot \varepsilon(q_f, q_e), \tag{2}$$

*then it holds*

$$\mathbf{Adv}^{atk}_{\mathsf{KAF}}(q_f, q_e) \leq \varepsilon(q_f, q_e).$$

Following [32], the lower bound (2) is named "$\varepsilon$-point-wise proximity" of $\tau$. We partition the key set $\mathcal{K}$ into two disjoint subsets $\mathcal{K}_{good}$ and $\mathcal{K}_{bad}$ such that $\mathcal{K} = \mathcal{K}_{good} \cup \mathcal{K}_{bad}$. Let $\Pr_{re}(\tau, k)$ be the probability that $D$ interacts with the real world, where $k \in \mathcal{K}$ is sampled as the key, and receives a transcript $\tau$. Moreover, we assume there is a fake key variable $k$ in the ideal world that is uniformly selected from the key space $\mathcal{K}$, i.e., $k \xleftarrow{\$} \mathcal{K}$, and define $\Pr_{id}(\tau, k)$ similarly. It is trivial that $\Pr_{id}(\tau, k) = \Pr_{id}(\tau) \times \Pr[k \xleftarrow{\$} \mathcal{K}]$. With these, HT provided a general lemma for establishing point-wise proximity.

**Lemma 2 (Lemma 1 of [32]).** *Fix a transcript $\tau$ with $\Pr_{id}(\tau) > 0$. Assume that: (i) $\Pr[k \in \mathcal{K}_{bad}] \leq \delta$, and (ii) there is a function $g : \mathcal{K} \to [0, \infty)$ such that for all $k \in \mathcal{K}_{good}$, it holds $\frac{\Pr_{re}(\tau,k)}{\Pr_{id}(\tau,k)} \geq 1 - g(k)$. Then we have*

$$\Pr_{id}(\tau) - \Pr_{re}(\tau) \leq \Pr_{id}(\tau) \cdot (\delta + \mathbb{E}_{k \in \mathcal{K}}[g(k)]). \tag{3}$$

HT also proved that once such point-wise proximity results have been established for the SU setting, similar results could be established for the MU setting via a general transformation. For this we restate Lemma 3 of [32] in our $\mathsf{KAF}$ setting.

**Lemma 3.** *Let $t$ be the number of calls to $\mathbf{F}$ that a single call to $\mathsf{KAF}/\mathsf{KAF}^{-1}$ makes. Let $\varepsilon : \mathbb{N} \times \mathbb{N} \to \mathbb{R}^{\geq 0}$ be a function such that*

- *$\varepsilon(q_f, q_e) + \varepsilon(q_f, q'_e) \leq \varepsilon(q_f, q_e + q'_e)$ for every $q_f$, $q_e$, $q'_e \in \mathbb{N}$, and*
- *$\varepsilon(\cdot, q)$ and $\varepsilon(q, \cdot)$ are non-decreasing functions on $\mathbb{N}$ for every $q \in \mathbb{N}$.*

*Assume that in the SU setting, for every transcript $\tau$ with $q_f$ and $q_e$ queries of the two types, one has*

$$\Pr_{id}(\tau) - \Pr_{re}(\tau) \leq \Pr_{id}(\tau) \cdot \varepsilon(q_f, q_e),$$

*then in the MU setting, for every transcript $\tau$ with $q_f$ and $q_e$ queries, one has*

$$\Pr_{id}(\tau) - \Pr_{re}(\tau) \leq \Pr_{id}(\tau) \cdot 2\varepsilon(q_f + t \cdot q_e, q_e).$$

## 3 Security Upper Bound: A Distinguishing Attack

Combining the idea of *enumerating all the possible round-keys* from [11] and the *(round) function reduction* technique of [33], the $t$-round KAF can be *distinguished* by $O(N^{\frac{t-2}{t-1}})$ *queries*:

(1) Chooses $\lambda$ plaintexts $L_1R_1, \ldots, L_\lambda R_\lambda$, with $L_1, \ldots, L_\lambda$ pair-wise distinct, and $R_1 = \ldots = R_\lambda = R$, and makes $\lambda$ encryption queries $\textsc{Enc}_k(L_1, R_1) \to (S_1, T_1)$, …, $\textsc{Enc}_k(L_\lambda, R_\lambda) \to (S_\lambda, T_\lambda)$;

(2) For $\ell$ from 2 to $t-1$, asks $\lambda$ arbitrary distinct queries $x_\ell^{(1)}, x_\ell^{(2)}, \ldots, x_\ell^{(\lambda)}$ to $F_\ell$:
- $F_\ell(x_\ell^{(1)}) \to y_\ell^{(1)}$,
- …
- $F_\ell(x_\ell^{(\lambda)}) \to y_\ell^{(\lambda)}$;

(3) Denote $CON = F_1(k_1 \oplus R)$. For *all* $k = (k_1, \ldots, k_t) \in \mathcal{K}$ and *all* $2^n$ *possible values of* $CON$, if there exists $t-1$ query-answer pairs $(L_iR, S_iT_i)$, $(x_2, y_2)$, $(x_3, y_3)$, …, $(x_{t-1}, y_{t-1})$ such that an almost completed computation chain is formed:
- $k_2 \oplus CON = L_i \oplus x_2$, and
- $k_3 = R \oplus y_2 \oplus x_3$, and
- …
- $k_{\ell+1} = (k_{\ell-1} \oplus x_{\ell-1}) \oplus y_\ell \oplus x_{\ell+1}$, and
- …
- $k_{t-1} = (k_{t-3} \oplus x_{t-3}) \oplus y_{t-2} \oplus x_{t-1}$,

and further $S = (k_{t-2} \oplus x_{t-2}) \oplus y_{t-1}$, then outputs 1 to indicates it's the real world (otherwise 0).

When $\lambda = N^{\frac{t-2}{t-1}}$ and thus $\frac{\lambda^{t-1}}{N^{t-2}} = 1$, the probability of forming a chain is approximately 1. By this, a 6-round KAF ensure at most $4n/5$-bit security. This should be contrasted with the results on the classical LR model (as discussed in the Introduction).

We also note that the $t$-round IEM ciphers built upon $n$*-bit* random permutations and *independent* round-keys tightly ensure $\frac{tn}{t+1}$-bit security [32], which is better than the upper bound $\frac{(t-2)n}{t-1}$-bit here. This matches the folklore that compared to IEM ciphers, Feistel ciphers have more structural properties that are helpful for attacks (as a consequence, to ensure the same amount of security, KAF needs more rounds). Tight security bounds for $t$-round KAF remains an open problem.

# 4 Four Rounds for Birthday-Type Security

We first present a general positive result for 4-round KAFSF in subsection 4.1. Then in subsection 4.2, we discuss how to schedule the desired round-keys from a short main-key, and present our "minimal" provably secure construction.

## 4.1 A General Positive Result

The first step is to specify conditions on the round-key vector that will allow us to upper bound the probability to obtain a round-bad key vector in the ideal world (the definition of bad key vectors will appear later).

**Definition 1 (Suitable Round-Key Vector for 4 Rounds).** *A round-key vector $k = (k_1, k_2, k_3, k_4)$ is suitable if it satisfies the following conditions:*

*(i) $k_1$ and $k_4$ are uniform in $\{0,1\}^n$ (but they need not to be independent);*
*(ii) $k_1 \oplus k_4$ is also uniformly distributed in $\{0,1\}^n$.*

If condition (i) is seriously compromised, the cipher would essentially lost 1 or 2 rounds. E.g., when $k_1$ is only uniform in $n$ possibilities, an adversary could derive the second-round intermediate value $X = L \oplus F(k_1 \oplus R)$ with $n$ guesses. The less obvious condition (ii) is intended to prevent palindrome-like relations in the derived round-keys, which have been found harmful [45]. To further help understanding, in the full version we present attacks against some round-keys that do not fulfill condition (ii).

Instantiated with such a suitable round-key vector, KAFSF ensures birthday security.

**Theorem 1.** *For the 4-round idealized KAFSF cipher with a suitable round-key vector as specified in Definition 1, it holds*

$$\mathbf{Adv}^{SU}_{\mathsf{KAFSF}}(q_f, q_e) \leq \frac{9q_e^2 + 4q_eq_f}{N}, \text{ and } \mathbf{Adv}^{MU}_{\mathsf{KAFSF}}(q_f, q_e) \leq \frac{50q_e^2 + 8q_eq_f}{N}.$$

*Proof.* We devote to prove that in the SU setting, for any transcript $\tau$, it holds

$$\Pr_{id}(\tau) - \Pr_{re}(\tau) \leq \Pr_{id}(\tau) \cdot \frac{9q_e^2 + 4q_eq_f}{N}. \quad (4)$$

This along with Lemmas 1 and 3 would yield the two main claims. Due to page limits, the proof of Eq. (4) is deferred to the full version [28]. □

## 4.2 How to Schedule the Key: The Minimal Construction

By Definition 1, it can be seen that if pair-wise independence is ensured between round-keys, then the key vector is suitable. We refer to Section 6 for how to derive such round-keys. Here it would be tempting to ask how to schedule a single $n$-bit key $K$ into a suitable key vector. Below we identify a condition on a key-schedule $\gamma = (\gamma_1, \gamma_2, \gamma_3, \gamma_4)$ (setting $k_i = \gamma_i(K)$ for $i = 1, 2, 3, 4$) that suffices for this purpose. We call such key-schedules *good*:

**Definition 2 (Good Key-Schedule for 4-Round KAFSF).** *We say that a key-schedule $\gamma = (\gamma_1, \gamma_2, \gamma_3, \gamma_4)$, where $\gamma_i : \{0,1\}^n \to \{0,1\}^n$, is good if $\gamma_1$, $\gamma_4$, and $\gamma_1 \oplus \gamma_4$ are all bijective maps of $\mathbb{F}_2^n$.*

As mentioned in the Introduction, one could take for $\gamma_1$ the identity, and $\gamma_4 = \varphi$, where $\varphi$ is an orthomorphism of $\mathbb{F}_2^n$, as in Fig. 1 (right).

## 5 Six Rounds for Beyond-Birthday Security

Similarly to Section 4, we also specify conditions on the round-key vectors first.

**Definition 3 (Suitable Round-Key Vector for 6 Rounds).** *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) $k_1$, $k_3$, and $k_5$ are uniformly distributed in $\{0,1\}^n$;*
*(ii) $k_2$, $k_4$, and $k_6$ are uniformly distributed in $2^{n-r}$ possibilities;*
*(iii) for $(i,j) \in \{(1,2),(2,3),(4,5),(5,6),(1,6)\}$, $k_i$ and $k_j$ are independent.*

Unlike Section 4, in the subsequent analysis we find the uniformness of every round-key crucial. This is why we require all of them to be uniform (this is also understandable, since beyond-birthday security requires various types of collisions can be bounded by small enough probability, and thus requiring a larger amount of randomness). The (mild) independence is also crucially used in the analysis. To further understand the necessity, please see [28, Appendix A].

Instantiated with such a suitable round-key vector, KAF ensures beyond-birthday security.

**Theorem 2.** *For the 6-round idealized cipher KAF with a suitable round-key vector as specified in Definition 3, it holds*

$$\mathbf{Adv}^{SU}_{\mathsf{KAF}}(q_f, q_e) \le \frac{7q_e^3 + 13q_eq_f^2 + 22q_e^2q_f}{N^2} + \frac{2^r(8q_eq_f^2 + 2q_e^2q_f)}{N^2}, \text{ and}$$
$$\mathbf{Adv}^{MU}_{\mathsf{KAF}}(q_f, q_e) \le \frac{1214q_e^3 + 26q_eq_f^2 + 356q_e^2q_f}{N^2} + \frac{2^r(600q_e^3 + 16q_eq_f^2 + 196q_e^2q_f)}{N^2}.$$

Note that when $r < n/2$, the security is beyond-birthday—and when $r = 0$, the bound is of "typical" beyond-birthday form $O(\frac{q^3}{N^2})$.

We devote to prove the following point-wise proximity result for the SU setting: for any transcript $\tau$, it holds

$$\Pr_{id}(\tau) - \Pr_{re}(\tau) \le \Pr_{id}(\tau) \cdot \frac{7q_e^3 + 13q_eq_f^2 + 22q_e^2q_f + 2^r(8q_eq_f^2 + 2q_e^2q_f)}{N^2}. \quad (5)$$

Gathering this and Lemmas 1 and 3 yields the claims.

Fix a transcript $\tau = (\mathcal{Q}_E, \mathcal{Q}_F)$ with $\mathcal{Q}_F = (\mathcal{Q}_{F_1}, \mathcal{Q}_{F_2}, \mathcal{Q}_{F_3}, \mathcal{Q}_{F_4}, \mathcal{Q}_{F_5}, \mathcal{Q}_{F_6})$, $|\mathcal{Q}_E| = q_e$, and $|\mathcal{Q}_{F_i}| = q_f$ for $i = 1, \ldots, 6$, we first define bad key-vectors, then lower bound the probability $\Pr_{re}(\tau, k)$. These two steps correspond to the following two subsections respectively.

### 5.1 Bad Round-Key Vectors and Probability

Similarly to subsection 4.1, for any $x_i \in \{0,1\}^n$, if there exists a corresponding record $(x_i, y_i)$ in $\mathcal{Q}_{F_i}$, then we write $x_i \in Dom\mathcal{F}_i$ (and $x_i \notin Dom\mathcal{F}_i$ otherwise), and write $ImgF_i(x_i)$ for the corresponding $y_i$. Now, the definition is as follows.

**Definition 4 (Bad Round-Key Vector for 6 Rounds).** *With respect to $\tau = (\mathcal{Q}_E, \mathcal{Q}_F)$, a suitable key vector $k$ fulfilling one of the conditions is bad:*

- *(B-1) there exists $(LR, ST) \in \mathcal{Q}_E$, $(x_1, y_1) \in \mathcal{Q}_{F_1}$, and $(x_6, y_6) \in \mathcal{Q}_{F_6}$ such that $k_1 = R \oplus x_1$ and $k_6 = S \oplus x_6$;*
- *(B-2) there exists $(LR, ST) \in \mathcal{Q}_E$, $(x_1, y_1) \in \mathcal{Q}_{F_1}$, and $(x_2, y_2) \in \mathcal{Q}_{F_2}$ such that $k_1 = R \oplus x_1$ and $k_2 = L \oplus y_1 \oplus x_2$;*
- *(B-3) there exists $(LR, ST) \in \mathcal{Q}_E$, $(x_5, y_5) \in \mathcal{Q}_{F_5}$, and $(x_6, y_6) \in \mathcal{Q}_{F_6}$ such that $k_6 = S \oplus x_6$ and $k_5 = T \oplus y_6 \oplus x_5$.*

*Otherwise we say $k$ is good. Denote by $\mathcal{K}_{bad}$ the set of bad key vectors.*

We now prove

$$\Pr[k \xleftarrow{\$} \mathcal{K} : k \in \mathcal{K}_{bad}] \leq \frac{3 \cdot 2^r \cdot q_e q_f^2}{N^2}. \tag{6}$$

Consider (B-1) first. Since we have at most $q_e q_f^2$ choices for $(LR, ST) \in \mathcal{Q}_E$ and $(x_1, y_1) \in \mathcal{Q}_{F_1}$ and $(x_6, y_6) \in \mathcal{Q}_{F_6}$ and since $k_1$, resp. $k_6$, is uniform in $2^n$, resp. $2^{n-r}$ possibilities, and further since $k_1$ and $k_6$ are independent (cf. Definition 3), it holds $\Pr[\text{(B-1)}] \leq \frac{q_e q_f^2}{2^{2n-r}} \leq \frac{2^r q_e q_f^2}{N^2}$.

Similarly, since $k_1$ and $k_2$ are random and independent, and we have at most $q_e q_f^2$ choices for $(LR, ST) \in \mathcal{Q}_E$ and $(x_1, y_1) \in \mathcal{Q}_{F_1}$ and $(x_2, y_2) \in \mathcal{Q}_{F_2}$, we have $\Pr[\text{(B-2)}] \leq \frac{2^r q_e q_f^2}{N^2}$; by symmetry, $\Pr[\text{(B-3)}] \leq \frac{2^r q_e q_f^2}{N^2}$. The sum yields (6).

### 5.2 Analysis for Good Keys

Fix a good round-key vector $k$, we are to derive a lower bound for the probability $\Pr[\mathbf{F} \xleftarrow{\$} (\mathcal{F}(n))^6 : \mathsf{KAF}_k^{\mathbf{F}} \vdash \mathcal{Q}_E \mid \mathbf{F} \vdash \mathcal{Q}_F]$. It consists of two steps. In the first step, we will lower bound the probability that a pair of functions $(\mathbf{F}_1, \mathbf{F}_6)$ satisfies certain "bad" conditions that will be defined. With the values given by a "good" pair of functions $(\mathbf{F}_1, \mathbf{F}_6)$, a transcript of the distinguisher on 6 rounds can be transformed into a special transcript on 4 rounds; in this sense, we "peel off" the outer two rounds. Then in the second step, assuming $(\mathbf{F}_1, \mathbf{F}_6)$ is good, we analyze the induced 4-round transcript to yield the final bounds. In the following, each step would take a subsubsection. As mentioned in the Introduction, this two-step approach is motivated by Cogliati et al. [17,16].

**Peeling off the Outer Two Rounds.** Pick a pair of functions $(\mathbf{F}_1, \mathbf{F}_6)$ such that $\mathbf{F}_1 \vdash \mathcal{Q}_{F_1}$ and $\mathbf{F}_6 \vdash \mathcal{Q}_{F_6}$, and for each $(LR, ST) \in \mathcal{Q}_E$ we set $X \leftarrow L \oplus \mathbf{F}_1(k_1 \oplus R)$ and $A \leftarrow T \oplus \mathbf{F}_6(k_6 \oplus S)$. In this way we obtain $q_e$ tuples of the form $(RX, AS)$; for convenience we denote the set of such induced tuples by $\mathcal{Q}_E^*(\mathbf{F}_1, \mathbf{F}_6)$. We further denote by $\mathcal{EQ}(X)$ the set that contains all such induced tuples with their second coordinate equaling $X$—formally,

- $\mathcal{EQ}(X) = \{(RX, AS) : (RX, AS) \in \mathcal{Q}_E^*(\mathbf{F}_1, \mathbf{F}_6)\}$.
- Similarly, $\mathcal{EQ}(A) = \{(RX, AS) : (RX, AS) \in \mathcal{Q}_E^*(\mathbf{F}_1, \mathbf{F}_6)\}$.

And we define several key-dependent quantities characterizing $\tau$:

$$\alpha_1(k) \overset{\text{def}}{=\!=} |\{((LR, ST), (x_1, y_1)) \in \mathcal{Q}_E \times \mathcal{Q}_{F_1} : k_1 = R \oplus x_1\}|,$$
$$\alpha_2(k) \overset{\text{def}}{=\!=} |\{((LR, ST), (x_6, y_6)) \in \mathcal{Q}_E \times \mathcal{Q}_{F_6} : k_6 = S \oplus x_6\}|,$$
$$\alpha_{2,3}(k) \overset{\text{def}}{=\!=} |\{((LR, ST), (x_2, y_2), (x_3, y_3)) \in \mathcal{Q}_E \times \mathcal{Q}_{F_2} \times \mathcal{Q}_{F_3} : k_3 = R \oplus y_2 \oplus x_3\}|,$$
$$\alpha_{4,5}(k) \overset{\text{def}}{=\!=} |\{((LR, ST), (x_4, y_4), (x_5, y_5)) \in \mathcal{Q}_E \times \mathcal{Q}_{F_4} \times \mathcal{Q}_{F_5} : k_4 = S \oplus y_5 \oplus x_4\}|.$$

Then we define a predicate $\mathsf{Bad}(\mathbf{F}_1, \mathbf{F}_6)$ on the pair $(\mathbf{F}_1, \mathbf{F}_6)$, which holds if the corresponding induced set $\mathcal{Q}_E^*(\mathbf{F}_1, \mathbf{F}_6)$ fulfills at least one of the following five "collision" conditions (see Fig. 3 for illustration):

- (C-1) there exists three records $(RX, AS) \in \mathcal{Q}_E^*(\mathbf{F}_1, \mathbf{F}_6)$, $(x_2, y_2) \in \mathcal{Q}_{F_2}$, and $(x_5, y_5) \in \mathcal{Q}_{F_5}$ such that $k_2 = X \oplus x_2$ and $k_5 = A \oplus x_5$;
- (C-2) there exists three records $(RX, AS) \in \mathcal{Q}_E^*(\mathbf{F}_1, \mathbf{F}_6)$, $(x_2, y_2) \in \mathcal{Q}_{F_2}$, and $(x_3, y_3) \in \mathcal{Q}_{F_3}$ such that $k_2 = X \oplus x_2$ and $k_3 = R \oplus y_2 \oplus x_3$;
- (C-3) there exists three records $(RX, AS) \in \mathcal{Q}_E^*(\mathbf{F}_1, \mathbf{F}_6)$, $(x_4, y_4) \in \mathcal{Q}_{F_4}$, and $(x_5, y_5) \in \mathcal{Q}_{F_5}$ such that $k_5 = A \oplus x_5$ and $k_4 = S \oplus y_5 \oplus x_4$;
- (C-4) there exists two distinct $(RX, AS)$, $(R'X', A'S')$ in $\mathcal{Q}_E^*(\mathbf{F}_1, \mathbf{F}_6)$, and a pair $(x_2, y_2)$ in $\mathcal{Q}_{F_2}$ such that $X = X'$ and $k_2 = X \oplus x_2$; or, symmetrically, two distinct $(RX, AS)$, $(R'X', A'S')$ in $\mathcal{Q}_E^*(\mathbf{F}_1, \mathbf{F}_6)$ and a pair $(x_5, y_5)$ in $\mathcal{Q}_{F_5}$ such that $A = A'$ and $k_5 = A \oplus x_5$;
- (C-5) there exists two distinct $(RX, AS)$, $(R'X', A'S')$ in $\mathcal{Q}_E^*(\mathbf{F}_1, \mathbf{F}_6)$ and a pair $(x_2, y_2)$ in $\mathcal{Q}_{F_2}$ such that $A = A'$ and $k_2 = X \oplus x_2$; or, symmetrically, two distinct $(RX, AS)$, $(R'X', A'S')$ in $\mathcal{Q}_E^*(\mathbf{F}_1, \mathbf{F}_6)$ and a pair $(x_5, y_5)$ in $\mathcal{Q}_{F_5}$ such that $X = X'$ and $k_5 = A \oplus x_5$.

For convenience, if $\mathsf{Bad}(\mathbf{F}_1, \mathbf{F}_6)$ does not hold, then we say $(\mathbf{F}_1, \mathbf{F}_6)$ is *good*; in this case, the induced tuples $(RX, AS)$ are easier to analyze. For $\Pr[\mathsf{Bad}(\mathbf{F}_1, \mathbf{F}_6)]$ we have the following bound.

**Lemma 4.** *It holds*

$$\Pr_{\mathbf{F}_1, \mathbf{F}_6}[\mathit{Bad}(\mathbf{F}_1, \mathbf{F}_6) \mid \mathbf{F}_1 \vdash \mathcal{Q}_{F_1} \wedge \mathbf{F}_6 \vdash \mathcal{Q}_{F_6}]$$
$$\leq \frac{q_e q_f^2}{N^2} + \frac{4q_e^2 q_f}{N^2} + \frac{\alpha_{2,3}(k) + \alpha_{4,5}(k)}{N} + \frac{q_f(\alpha_1(k) + \alpha_2(k))}{N}.$$

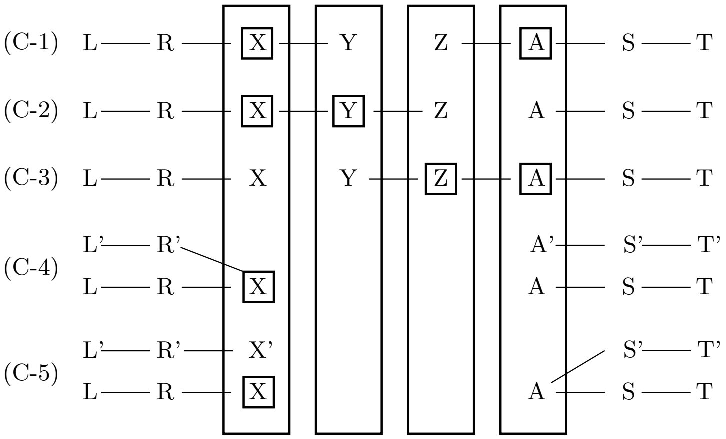

**Fig. 3.** The five "collision" conditions characterizing a pair of functions $(\mathbf{F}_1, \mathbf{F}_6)$ such that $\mathsf{Bad}(\mathbf{F}_1, \mathbf{F}_6)$ holds. The values $X$, $Y$, $Z$, $A$ in squares satisfy $k_2 \oplus X \in Dom\mathcal{F}_2$, $k_3 \oplus Y \in Dom\mathcal{F}_3$, $k_4 \oplus Z \in Dom\mathcal{F}_4$, and $k_5 \oplus A \in Dom\mathcal{F}_5$ respectively.

*Proof.* Due to page limits please see the full version [28] for the proofs for:

$$\Pr[\text{(C-1)}] \le \frac{q_e q_f^2}{N^2}, \quad \Pr[\text{(C-2)}] \le \frac{\alpha_{2,3}(k)}{N}, \quad \Pr[\text{(C-3)}] \le \frac{\alpha_{4,5}(k)}{N},$$
$$\Pr[\text{(C-4)}] \le \frac{2q_e^2 q_f}{N^2}, \text{ and } \Pr[\text{(C-5)}] \le \frac{2q_e^2 q_f}{N^2} + \frac{q_f(\alpha_1(k) + \alpha_2(k))}{N}.$$

Summing over them gives the result. All the arguments rely on the uniformness of entries of $\mathbf{F}$, which are uniform in $2^n$ values rather than $2^{n-r}$. This clarifies why the bounds have nothing to do with the term $2^r$. □

**Analyzing the Inner Four Rounds.** Let $\mathbf{F}^* = (\mathbf{F}_2, \mathbf{F}_3, \mathbf{F}_4, \mathbf{F}_5)$. We denote

$$\mathsf{p}(\tau, \mathbf{F}_1, \mathbf{F}_6) = \Pr[\mathbf{F}^* \xleftarrow{\$} (\mathcal{F}(n))^4 : \mathsf{KAF}_k^{\mathbf{F}^*} \vdash \mathcal{Q}_E^*(\mathbf{F}_1, \mathbf{F}_6) \mid \mathbf{F}_i \vdash \mathcal{Q}_{F_i}, i = 1,2,3,4,5,6].$$

This captures the probability that the inner four rounds of $\mathsf{KAF}$ "extend" the tuples in $\mathcal{Q}_E^*(\mathbf{F}_1, \mathbf{F}_6)$. The probability $\Pr_{re}(\tau, k)$ can be related to it.

**Lemma 5.** *Assume that there exists a function* $\epsilon : (\mathcal{F}(n))^2 \times \mathcal{K} \to [0, \infty)$ *such that for any good* $(\mathbf{F}_1, \mathbf{F}_6)$*, it holds*

$$\mathsf{p}(\tau, \mathbf{F}_1, \mathbf{F}_6) \Big/ \prod_{i=0}^{q_e - 1} \left( \frac{1}{N^2 - i} \right) \ge 1 - \epsilon(\mathbf{F}_1, \mathbf{F}_6, k). \tag{7}$$

*Then we have*

$$\frac{\Pr_{re}(\tau, k)}{\Pr_{id}(\tau, k)} \ge 1 - \Pr[\mathit{Bad}(\mathbf{F}_1, \mathbf{F}_6) \mid \mathbf{F}_1 \vdash \mathcal{Q}_{F_1}, \mathbf{F}_6 \vdash \mathcal{Q}_{F_6}]$$
$$- \mathbb{E}_{\mathbf{F}_1, \mathbf{F}_6}[\epsilon(\mathbf{F}_1, \mathbf{F}_6, k) \mid \mathbf{F}_1 \vdash \mathcal{Q}_{F_1}, \mathbf{F}_6 \vdash \mathcal{Q}_{F_6}].$$

*Proof.* Define $\mathsf{p}(\mathbf{F}_1, \mathbf{F}_6) \overset{\text{def}}{=\!=} \Pr[(\mathbf{F}_1^*, \mathbf{F}_6^*) \overset{\$}{\leftarrow} (\mathcal{F}(n))^2 : (\mathbf{F}_1^*, \mathbf{F}_6^*) = (\mathbf{F}_1, \mathbf{F}_6)]$ for convenience. Then, clearly, once $\mathbf{F}_1$ and $\mathbf{F}_6$ are fixed such that $\mathbf{F}_1 \vdash \mathcal{Q}_{F_1}$ and $\mathbf{F}_6 \vdash \mathcal{Q}_{F_6}$, the event $\mathsf{KAF}_k^{\mathbf{F}} \vdash \mathcal{Q}_E$ is equivalent to $\mathsf{KAF}_k^{\mathbf{F}^*} \vdash \mathcal{Q}_E^*(\mathbf{F}_1, \mathbf{F}_6)$. Hence

$$\Pr_{re}(\tau, k) \geq \sum_{\mathbf{F}_1 \vdash \mathcal{Q}_{F_1}, \mathbf{F}_6 \vdash \mathcal{Q}_{F_6} : (\mathbf{F}_1, \mathbf{F}_6) \text{ good}} \mathsf{p}(\mathbf{F}_1, \mathbf{F}_6) \cdot \frac{\mathsf{p}(\tau, \mathbf{F}_1, \mathbf{F}_6)}{|\mathcal{K}| \cdot N^{4q_f}}.$$

Therefore,

$$\begin{aligned}
\frac{\Pr_{re}(\tau, k)}{\Pr_{id}(\tau, k)} &\geq \frac{\sum_{\mathbf{F}_1 \vdash \mathcal{Q}_{F_1}, \mathbf{F}_6 \vdash \mathcal{Q}_{F_6} : (\mathbf{F}_1, \mathbf{F}_6) \text{ good}} \mathsf{p}(\mathbf{F}_1, \mathbf{F}_6) \cdot \mathsf{p}(\tau, \mathbf{F}_1, \mathbf{F}_6)}{\Pr[\mathbf{F}_1 \vdash \mathcal{Q}_{F_1}, \mathbf{F}_6 \vdash \mathcal{Q}_{F_6}] \cdot \prod_{i=0}^{q_e - 1} \frac{1}{N^2 - i}} \\
&\geq \frac{\sum_{\mathbf{F}_1 \vdash \mathcal{Q}_{F_1}, \mathbf{F}_6 \vdash \mathcal{Q}_{F_6} : (\mathbf{F}_1, \mathbf{F}_6) \text{ good}} \mathsf{p}(\mathbf{F}_1, \mathbf{F}_6)(1 - \epsilon(\mathbf{F}_1, \mathbf{F}_6, k))}{\Pr[\mathbf{F}_1 \vdash \mathcal{Q}_{F_1}, \mathbf{F}_6 \vdash \mathcal{Q}_{F_6}]} \quad \text{(by (7))} \\
&\geq 1 - \Pr[\mathsf{Bad}(\mathbf{F}_1, \mathbf{F}_6) \mid \mathbf{F}_1 \vdash \mathcal{Q}_{F_1}, \mathbf{F}_6 \vdash \mathcal{Q}_{F_6}] \\
&\qquad - \underbrace{\sum_{\mathbf{F}_1 \vdash \mathcal{Q}_{F_1}, \mathbf{F}_6 \vdash \mathcal{Q}_{F_6}} \mathsf{p}(\mathbf{F}_1, \mathbf{F}_6) \epsilon(\mathbf{F}_1, \mathbf{F}_6, k)}_{= \mathbb{E}_{\mathbf{F}_1, \mathbf{F}_6}[\epsilon(\mathbf{F}_1, \mathbf{F}_6, k) | \mathbf{F}_1 \vdash \mathcal{Q}_{F_1}, \mathbf{F}_6 \vdash \mathcal{Q}_{F_6}]}.
\end{aligned}$$

as claimed. □

We now prove the assumption of Lemma 5.

**Lemma 6.** *For any fixed good tuple* $(\mathbf{F}_1, \mathbf{F}_6)$*, there exists a function* $\epsilon(\mathbf{F}_1, \mathbf{F}_6, k)$ *of the function pair and the round-key vector* $k$ *such that the inequality (7) mentioned in Lemma 5 holds. Moreover,*

$$\mathbb{E}_{\mathbf{F}_1, \mathbf{F}_6, k}[\epsilon(\mathbf{F}_1, \mathbf{F}_6, k)] \leq \frac{7q_e^3 + 10q_e q_f^2 + 18q_e^2 q_f + 3 \cdot 2^r \cdot q_e q_f^2 + 2 \cdot 2^r \cdot q_e^2 q_f}{N^2}. \tag{8}$$

*Proof.* The general expression of $\epsilon(\mathbf{F}_1, \mathbf{F}_6, k)$ is a function of several variables defined before, which suffers from a bad readability. Therefore, we directly establish (and present) the bound on its expectation. However, due to space constraints, the full proof has to be deferred to [28].

Below we present a sketch and the core results. According to the type of the involved collisions, we divide the tuples in $\mathcal{Q}_E^*(\mathbf{F}_1, \mathbf{F}_6)$ into four groups (see Fig. 4 for an illustration):

- $\mathcal{G}_1 = \{(RX, AS) \in \mathcal{Q}_E^*(\mathbf{F}_1, \mathbf{F}_6) : |\mathcal{EQ}(X)| = |\mathcal{EQ}(A)| = 1$, and further $k_2 \oplus X \notin Dom\mathcal{F}_2 \wedge k_5 \oplus A \notin Dom\mathcal{F}_5\}$,
- $\mathcal{G}_2 = \{(RX, AS) \in \mathcal{Q}_E^*(\mathbf{F}_1, \mathbf{F}_6) : k_2 \oplus X \in Dom\mathcal{F}_2\}$,
- $\mathcal{G}_3 = \{(RX, AS) \in \mathcal{Q}_E^*(\mathbf{F}_1, \mathbf{F}_6) : k_5 \oplus A \in Dom\mathcal{F}_5\}$,
- $\mathcal{G}_4 = \{(RX, AS) \in \mathcal{Q}_E^*(\mathbf{F}_1, \mathbf{F}_6) : |\mathcal{EQ}(X)| \geq 2, \text{ or } |\mathcal{EQ}(A)| \geq 2\}$.

Let $\beta_1 = |\mathcal{G}_2|$, $\beta_2 = |\mathcal{G}_3|$, and $\beta_3 = |\mathcal{G}_4|$. Note that by definition, these sets form a partition of $\mathcal{Q}_E^*(\mathbf{F}_1, \mathbf{F}_6)$:

- $\mathcal{G}_1 \cap \mathcal{G}_2 = \mathcal{G}_1 \cap \mathcal{G}_3 = \mathcal{G}_1 \cap \mathcal{G}_4 = \emptyset$ by definition;

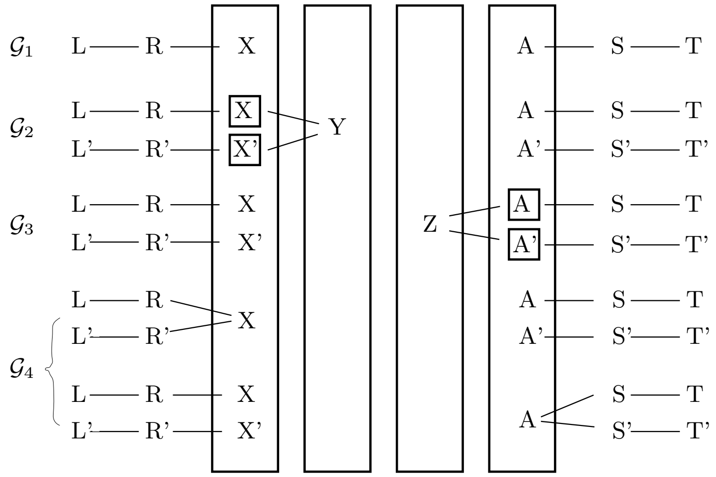

**Fig. 4.** Partition of the tuples in $\mathcal{Q}^*_E(\mathbf{F}_1, \mathbf{F}_6)$. The value $X$, resp. $A$, in square satisfies $k_2 \oplus X \in Dom\mathcal{F}_2$, resp. $k_5 \oplus A \in Dom\mathcal{F}_5$.

- $\mathcal{G}_2 \cap \mathcal{G}_3 = \emptyset$ since otherwise $\mathcal{Q}^*_E(\mathbf{F}_1, \mathbf{F}_6)$ would satisfy (C-1);
- $\mathcal{G}_2 \cap \mathcal{G}_4 = \emptyset$, since for any $(RX, AS) \in \mathcal{G}_2$, $|\mathcal{EQ}(X)| \geq 2$ would imply $\mathcal{Q}^*_E(\mathbf{F}_1, \mathbf{F}_6)$ fulfilling (C-4), while $|\mathcal{EQ}(A)| \geq 2$ would imply (C-5);
- $\mathcal{G}_3 \cap \mathcal{G}_4 = \emptyset$, since for any $(RX, AS) \in \mathcal{G}_3$, $|\mathcal{EQ}(X)| \geq 2$ implies (C-5), while $|\mathcal{EQ}(A)| \geq 2$ implies (C-4).

We denote respectively $\mathsf{E}_{\mathcal{G}_1}$, $\mathsf{E}_{\mathcal{G}_2}$, $\mathsf{E}_{\mathcal{G}_3}$, and $\mathsf{E}_{\mathcal{G}_4}$ the event that $\mathsf{KAF}^{\mathbf{F}^*}_k \vdash \mathcal{G}_1$, $\mathcal{G}_2$, $\mathcal{G}_3$, and $\mathcal{G}_4$. It can be seen

$$\mathsf{p}(\tau, \mathbf{F}_1, \mathbf{F}_6) = \Pr[\mathsf{E}_{\mathcal{G}_1} \wedge \mathsf{E}_{\mathcal{G}_2} \wedge \mathsf{E}_{\mathcal{G}_3} \wedge \mathsf{E}_{\mathcal{G}_4} \mid \mathbf{F} \vdash \mathcal{Q}_F].$$

We next analyze the four groups in turn. The first one, i.e. $\Pr[\mathsf{E}_{\mathcal{G}_1} \mid \mathbf{F} \vdash \mathcal{Q}_F]$, involves the most complicated analysis. Briefly, for each tuple $(RX, AS)$ in $\mathcal{G}_1$, it consists of three cases:

(i) In the first case, neither of the two corresponding intermediate values $Y$ and $Z$ derived from $\mathbf{F}_2$ and $\mathbf{F}_5$ collides with values that have been in the history. The probability that $\mathsf{KAF}^{\mathbf{F}}_k$ extends $(RX, AS)$ in this case is roughly at least

$$\left(1 - \frac{q_f + q_e + \beta_1}{N}\right)\left(1 - \frac{q_f + q_e + \beta_2}{N}\right)\frac{1}{N^2}.$$

(ii) In the second case, the corresponding intermediate value $Y$ collides with some "existing" values, yet the further derived $Z$ is "free". The probability that $\mathsf{KAF}^{\mathbf{F}}_k$ extends $(RX, AS)$ in this case is roughly at least

$$\left(\frac{q_f + q_e}{N} - O\left(\frac{2^r \cdot q_f^2}{N^2} + \frac{(q_f + q_e)^2}{N^2}\right)\right)\frac{1}{N^2}.$$

(iii) The third case is symmetrical to the second one: $Z$ collides with "existing" values, yet $Y$ is "free". The probability is roughly at least

$$\left(\frac{q_f + q_e}{N} - O\left(\frac{(q_f + q_e)^2}{N^2}\right)\right)\frac{1}{N^2}.$$

Summing over the above, we obtain

$$\Pr[\mathsf{E}_{\mathcal{G}_1} \mid \mathbf{F} \vdash \mathcal{Q}_F] \geq \prod_{\ell=1}^{|\mathcal{G}_1|}\left(1 - \frac{\beta_1}{N} - \frac{\beta_2}{N} - O\left(\frac{2^r \cdot q_f^2}{N^2} + \frac{(q_f + q_e)^2}{N^2}\right)\right)\frac{1}{N^2}.$$

Yet, the above results are oversimplified due to the page limits. We in fact used many additional notations, cf. [28]. The concrete bound is

$$\begin{aligned}&\mathbb{E}_k\big[\Pr[\mathsf{E}_{\mathcal{G}_1} \mid \mathbf{F} \vdash \mathcal{Q}_F]\big]\\ &\geq \left(1 - \frac{2^r \cdot q_e q_f^2}{N^2} - \frac{2q_e(2q_f + q_e)(q_f + q_e)}{N^2} - \frac{(q_f + 2q_e)(\beta_1 + \beta_2)}{N}\right)\frac{1}{N^{2|\mathcal{G}_1|}}. \qquad (9)\end{aligned}$$

To analyze $\mathsf{E}_{\mathcal{G}_2}$, $\mathsf{E}_{\mathcal{G}_3}$, and $\mathsf{E}_{\mathcal{G}_4}$, we again apply the bad predicate approach. These groups involve collisions, and have relatively small sizes: $|\mathcal{G}_2|, |\mathcal{G}_3|, |\mathcal{G}_4| = O(2^r \cdot q^2/N)$ (will be proved later). Therefore, any collisions between tuples in these groups and values related to $\mathcal{Q}_F$ or $\mathcal{G}_1$ can be included in the bad predicates: for each tuple in these three groups the probability would be $O(q/N)$ with $q = \max\{q_e, q_f\}$, yet it remains $O(q/N) \cdot O(2^r \cdot q^2/N) = O(2^r \cdot q^3/N^2)$ in total. See [28] for the formal analyzes. In all, the results are

$$\Pr[\mathsf{E}_{\mathcal{G}_2} \wedge \mathsf{E}_{\mathcal{G}_3} \mid \mathsf{E}_{\mathcal{G}_1} \wedge \mathbf{F} \vdash \mathcal{Q}_F] \geq \left(1 - \frac{(\beta_1 + \beta_2)(q_f + q_e)}{N}\right)\frac{1}{N^{2(|\mathcal{G}_2| + |\mathcal{G}_3|)}}, \qquad (10)$$

$$\Pr[\mathsf{E}_{\mathcal{G}_4} \mid \mathsf{E}_{\mathcal{G}_1} \wedge \mathsf{E}_{\mathcal{G}_2} \wedge \mathsf{E}_{\mathcal{G}_3} \wedge \mathbf{F} \vdash \mathcal{Q}_F] \geq \left(1 - \frac{2\beta_3(q_f + q_e)}{N}\right)\frac{1}{N^{2|\mathcal{G}_4|}}. \qquad (11)$$

**Summing Up** would yield a lower bound of the form

$$\begin{aligned}\mathsf{p}(\tau, \mathbf{F}_1, \mathbf{F}_6) &= \Pr[\mathsf{E}_{\mathcal{G}_1} \wedge \mathsf{E}_{\mathcal{G}_2} \wedge \mathsf{E}_{\mathcal{G}_3} \wedge \mathsf{E}_{\mathcal{G}_4} \mid \mathbf{F} \vdash \mathcal{Q}_F]\\ &\geq (1 - \epsilon_1)(1 - \epsilon_2)(1 - \epsilon_3)\frac{1}{N^{2(|\mathcal{G}_1| + |\mathcal{G}_2| + |\mathcal{G}_3| + |\mathcal{G}_4|)}}\\ &\geq (1 - (\epsilon_1 + \epsilon_2 + \epsilon_3))\,\frac{1}{N^{2q_e}} \text{ (since } |\mathcal{G}_1| + |\mathcal{G}_2| + |\mathcal{G}_3| + |\mathcal{G}_4| = q_e),\end{aligned}$$

where $\epsilon_1$, $\epsilon_2$, $\epsilon_3$ are in (9), (10), and (11) respectively. We note

$$\frac{1}{N^{2q_e}} \bigg/ \left(\prod_{i=0}^{q_e - 1}\frac{1}{N^2 - i}\right) \geq \left(1 - \frac{q_e}{N^2}\right)^{q_e} \geq 1 - \frac{q_e^2}{N^2} \geq 1 - \frac{q_e^3}{N^2},$$

Thus using $(1 - A)(1 - B) \geq 1 - (A + B)$ we obtain

$$\frac{\mathsf{p}(\tau, \mathbf{F}_1, \mathbf{F}_6)}{\prod_{i=0}^{q_e - 1}\frac{1}{N^2 - i}} \geq 1 - \epsilon(\mathbf{F}_1, \mathbf{F}_2, k),$$

for which

$$\begin{aligned}\mathbb{E}_k\left[\epsilon(\mathbf{F}_1,\mathbf{F}_6,k)\right] \leq & \frac{(2q_f+3q_e)(\beta_1+\beta_2)+2\beta_3(q_f+q_e)}{N} \\ & + \frac{2^r\cdot q_e q_f^2}{N^2}+\frac{2q_e(2q_f+q_e)(q_f+q_e)+q_e^3}{N^2}.\end{aligned}$$

We now derive $\mathbb{E}_{\mathbf{F}_1,\mathbf{F}_6}[\mathbb{E}_k[\epsilon(\mathbf{F}_1,\mathbf{F}_2,k)] \mid \mathbf{F}_1 \vdash \mathcal{Q}_{F_1}, \mathbf{F}_6 \vdash \mathcal{Q}_{F_6}]$. To this end, note that by definition, $\beta_1,\beta_2$, and $\beta_3$ are quantities that depend on $(\mathbf{F}_1,\mathbf{F}_6)$:

$$\begin{aligned}\beta_1 &= |\{(RX,AS)\in\mathcal{Q}_E^*(\mathbf{F}_1,\mathbf{F}_6): k_2\oplus X = k_2\oplus L\oplus \mathbf{F}_1(k_1\oplus R)\in Dom\mathcal{F}_2\}|,\\ \beta_2 &= |\{(RX,AS)\in\mathcal{Q}_E^*(\mathbf{F}_1,\mathbf{F}_6): k_5\oplus A = k_5\oplus T\oplus \mathbf{F}_6(k_6\oplus S)\in Dom\mathcal{F}_5\}|,\\ \beta_3 &= |\{(RX,AS)\in\mathcal{Q}_E^*(\mathbf{F}_1,\mathbf{F}_6): \exists(R'X',A'S') \text{ such that } X=X', \text{ or:}\\ &\qquad \exists(R'X',A'S')\in\mathcal{Q}_E^*(\mathbf{F}_1,\mathbf{F}_6) \text{ such that } A=A'\}|.\end{aligned}$$

We consider $\beta_1$ first. For each $(RX,AS)\in\mathcal{Q}_E^*(\mathbf{F}_1,\mathbf{F}_6)$, if $k_1\oplus R\in Dom\mathcal{F}_1$, then $k_2\oplus X\notin Dom\mathcal{F}_2$ by $\neg$(B-2). Thus conditioned on $\mathbf{F}_1\vdash\mathcal{Q}_{F_1}$, $\mathbf{F}_1(k_1\oplus R)$ remains uniform, and $\Pr[k_2\oplus L\oplus\mathbf{F}_1(k_1\oplus R)\in Dom\mathcal{F}_2]\leq\frac{q_f}{N}$. Therefore,

$$\mathbb{E}_k[\beta_1]\leq\frac{q_e q_f}{N}.$$

Similarly by symmetry, using the randomness supplied by $\mathbf{F}_6$, $\mathbb{E}_k[\beta_2]\leq\frac{q_e q_f}{N}$.

Then we consider $\beta_3$. We fix a record $(LR,ST)$ such that $k_1\oplus R\notin Dom\mathcal{F}_1$, and consider another $(L'R',S'T')$. If $R=R'$ then it has to be $L\neq L'$ and thus $X\neq X'$. Otherwise, as $k_1\oplus R\notin Dom\mathcal{F}_1$, $\mathbf{F}_1(k_1\oplus R)$ remains random conditioned on $\mathbf{F}_1\vdash\mathcal{Q}_{F_1}$, and $\Pr[X=X']=\Pr[\mathbf{F}_1(k_1\oplus R)=L\oplus L'\oplus\mathbf{F}_1(k_1\oplus R')]=\frac{1}{N}$. The number of distinct pairs of such tuples is at most $q_e^2$. Thus we know the expectation of the number of pairs $((RX,AS),(R'X',A'S'))$ such that $X=X'$ is at most $\frac{q_e^2}{N}$. Thus

$$\mathbb{E}_k[|\{(RX,AS):k_1\oplus R\notin Dom\mathcal{F}_1, \text{ and } \exists(R'X',A'S') \text{ s.t. } X=X'\}|]\leq\frac{q_e^2}{N}.$$

As the number of $(LR,ST)$ such that $k_1\oplus R\in Dom\mathcal{F}_1$ is $\alpha_1(k)$, we obtain

$$\mathbb{E}_k[|\{(RX,AS):\exists(R'X',A'S') \text{ s.t. } X=X'\}|]\leq\frac{q_e^2}{N}+\alpha_1(k).$$

Symmetrically, $\mathbb{E}_k[|\{(RX,AS):\exists(R'X',A'S') \text{ s.t. } A=A'\}|]\leq\frac{q_e^2}{N}+\alpha_2(k)$. Thus $\mathbb{E}_k[\beta_3]\leq\frac{2q_e^2}{N}+\alpha_1(k)+\alpha_2(k)$.

Finally, since $k_1$, resp. $k_6$, are uniform in $2^n$, resp. $2^{n-r}$ possibilities,

$$\mathbb{E}_k[\alpha_1(k)]=\sum_{(LR,ST)\in\mathcal{Q}_E}\sum_{(x_1,y_1)\in\mathcal{Q}_{F_1}}\Pr[k_1=R\oplus x_1]\leq\frac{q_e q_f}{N}$$

and $\mathbb{E}_k[\alpha_2(k)] \leq \frac{2^r \cdot q_e q_f}{N}$. Gathering all the above yields

$$\begin{aligned}\mathbb{E}_{\mathbf{F}_1,\mathbf{F}_6,k}\big[\epsilon(\mathbf{F}_1,\mathbf{F}_6,k)\big] \leq & \frac{4q_e q_f^2 + 6q_e^2 q_f}{N^2} + \frac{2(q_e+q_f)(2q_e^2 + q_e q_f + 2^r q_e q_f)}{N^2} \\ & + \frac{2^r \cdot q_e q_f^2}{N^2} + \frac{2q_e(2q_f+q_e)(q_f+q_e) + q_e^3}{N^2} \\ = & \frac{7q_e^3 + 10q_e q_f^2 + 18q_e^2 q_f + 3\cdot 2^r \cdot q_e q_f^2 + 2\cdot 2^r \cdot q_e^2 q_f}{N^2},\end{aligned}$$

as claimed in (8). □

### 5.3 Concluding the Point-Wise Proximity Proof

Gathering Lemma 2, Lemma 5, and (6), we obtain

$$\begin{aligned}\frac{\Pr_{re}(\tau)}{\Pr_{id}(\tau)} \geq 1 - \bigg(& \frac{3\cdot 2^r q_e q_f^2}{N^2} + \mathbb{E}_k\big[\Pr[\mathsf{Bad}(\mathbf{F}_1,\mathbf{F}_6) \mid \mathbf{F}_1 \vdash \mathcal{Q}_{F_1}, \mathbf{F}_6 \vdash \mathcal{Q}_{F_6}]\big] \\ & + \mathbb{E}_k\big[\mathbb{E}_{\mathbf{F}_1,\mathbf{F}_6}[\epsilon(\mathbf{F}_1,\mathbf{F}_6,k) \mid \mathbf{F}_1 \vdash \mathcal{Q}_{F_1}, \mathbf{F}_6 \vdash \mathcal{Q}_{F_6}]\big]\bigg),\end{aligned}$$

where $\epsilon(\mathbf{F}_1,\mathbf{F}_6,k)$ is the function specified in (7). Note that its expectation has been bounded in Lemma 6.

For $\mathbb{E}_k[\Pr[\mathsf{Bad}(\mathbf{F}_1,\mathbf{F}_6) \mid \mathbf{F}_1 \vdash \mathcal{Q}_{F_1}, \mathbf{F}_6 \vdash \mathcal{Q}_{F_6}]]$, since $k_3$ and $k_4$ are both uniformly distributed (in $2^n$ and $2^{n-r}$ values, respectively), we have

$$\mathbb{E}_k[\alpha_{2,3}(k)] \leq \frac{q_e q_f^2}{N}, \text{ and } \mathbb{E}_k[\alpha_{4,5}(k)] \leq \frac{2^r q_e q_f^2}{N}.$$

At the end of the previous subsection we have shown $\mathbb{E}_k[\alpha_1(k)] \leq q_e q_f/N$ and $\mathbb{E}_k[\alpha_2(k)] \leq 2^r q_e q_f/N$. Injecting them into the bound of Lemma 4 yields

$$\mathbb{E}_k[\Pr[\mathsf{Bad}(\mathbf{F}_1,\mathbf{F}_6) \mid \mathbf{F}_1 \vdash \mathcal{Q}_{F_1}, \mathbf{F}_6 \vdash \mathcal{Q}_{F_6}]] \leq \frac{3q_e q_f^2}{N^2} + \frac{2\cdot 2^r q_e q_f^2}{N^2} + \frac{4q_e^2 q_f}{N^2}.$$

Gathering all the above eventually establishes (5).

### 5.4 $(2n-r)/3$-bit Security from $2n-r$ bits Main-Key, and PKEM

According to Definition 3, a suitable round-key vector could be derived from two independent main keys $K$ and $K'$, where $|K| = n$ and $|K'| = n - r$. A specific case is to alternatively apply the two keys. In this case, the construction collapses to a "partial-key" Even-Mansour variant

$$\mathsf{PKEM}^{\mathsf{LR}_6}_{0^r\|K'\|K}(M) = (0^r\|K'\|K) \oplus \mathsf{LR}_6((0^r\|K'\|K) \oplus M) \tag{12}$$

for $\mathsf{LR}_6$ the 6-round keyless Feistel permutation built from 6 independent random functions; see Fig. 2 (right). On the other hand, with an orthomorphisms $\varphi$ one could set the key vector to $(K, K', \varphi(K), \varphi(K'), K, K')$, with which the $\mathsf{KAF}$ would be a "normal" Feistel cipher rather than "collapsing" to $\mathsf{PKEM}$.

# 6 Application: A Proposal for KAF Key-Schedules

To further demonstrate the usefulness of our theoretical results, we propose some concrete key-schedules for KAF ciphers. In detail, we propose to consider key-schedules with produced round-keys $(k_1, \ldots, k_t)$ satisfying the following three conditions:

(i) *Uniformness*: every $k_i$ is uniform in $\{0,1\}^n$;
(ii) *Pair-Wise Independence (PWI)*: any two round-keys $k_i$ and $k_j$ are independent;
(iii) *Distinctness*: it's hard to find weak keys $K$ that gives rise to identical round-keys $k_1 = \ldots = k_t$.

The considerations behind PWI are two-fold. First, such round-keys satisfy both Definitions 1 and 3, and are thus supported by our theoretical results. Second, it's intuitively good: independence between round-keys plays a crucial role in our analysis, and would probably help simplify the proof for tighter bounds for 5 and 6 rounds.

The property *distinctness* is rather informal. It's intended to prevent the KAF cipher from collapsing to 1-round IEM. Note that PWI is able to prevent such collapsing with "significant probability"; however, this is not enough, since the number of (weak) main-keys that would cause such collapsing may not be small enough from the viewpoint of practitioners; see [28] for an example.

As discussed in the Introduction, common "word-aligned" key-schedules usually ensure *independence between adjacent round-keys*. This deviates from PWI, and the latter is not clear to be achieved by ad hoc designs. Fortunately, the three properties can be achieved from a $2n$-bit main-key $K = K_1 \| K_2$ by efficient linear functions [37]. Below we exhibit an example. Let $\mathbb{F}_2^n$ be the set $\{0,1\}^n$ seen as the field with $2^n$ elements defined by some irreducible polynomial of degree $n$ over $\mathbb{F}_2$, the field with two elements, and denote $a \otimes b$ the field multiplication of two elements $a, b \in \mathbb{F}_2^n$. In addition, for $1 \le t \ll 2^n$, let the constants $a_t$ and $a_{t+1}$ be the $t$ and $(t+1)^{\text{th}}$ values in the prime sequence $1, 2, 3, 5, 7, 11, 13, \ldots$ respectively. Then, for $t \ll 2^n$ rounds (which is usually the case), one can set

$$\begin{aligned} k_1 &= K_1 + 2 \otimes K_2, & k_2 =& 2 \otimes K_1 + 3 \otimes K_2, \\ k_3 &= 3 \otimes K_1 + 5 \otimes K_2, & k_4 =& 5 \otimes K_1 + 7 \otimes K_2, \\ &\ldots, & k_t =& a_t \otimes K_1 + a_{t+1} \otimes K_2, \end{aligned}$$

The proof for PWI is quite simple, and is given in the full version [28].

PWI cannot be achieved from $\kappa < 2n$ main-key bits. However, nowadays it's rather uncommon for a BC to have key-size smaller than its block-size. On the other hand, instances of Feistel ciphers with $2n$-bit blocks *and* $2n$-bit keys do exist: e.g. SIMON96/96 and SIMON128/128 [4].

More generally, with a $cn$-bit main-key for $c$ integer we conjecture $c$-wise independent round-keys are desirable. This is however not revealed by our results. We leave this as an interesting future direction.

# 7 Other Implications

As multi-user secure BCs, our provable $\mathsf{KAF}$ constructions could be plugged into many BC-based modes to reduce the size of (ideal) primitives in use. In some cases, this even does not result in a security loss.

For example, Gaži et al. proved that when the adversary makes $q$ queries of length $\ell < 2^{n/4}$, the PRF security bound of the truncated CBC mode built upon a $2n$-bit random permutation is roughly $\frac{q(q+\ell)}{2^{2n-d}} + \frac{\ell q^2}{2^{2n}}$, where $d$ is the length of the output [23]. By this, instantiated with our 6-round $\mathsf{KAF}$ (with $r = 0$), the resulted bound is

$$\frac{(\ell q)^3}{2^{2n}} + \frac{(\ell q)^2 q_f}{2^{2n}} + \frac{(\ell q) q_f^2}{2^{2n}} + \frac{q(q+\ell)}{2^{2n-d}} + \frac{\ell q^2}{2^{2n}},$$

where $q_f$ is the number of adversarial function queries. It can be seen that this is the same as the original when $d \geq 7n/6$ (i.e. the output is sufficiently long) and $q_f \ll 2^{2n/3}$.

## 7.1 Lightweight Keyed Sponges

A more interesting implication is on keyed sponges. Many lightweight keyed sponges with permutation $\pi$ have their security rely on the (MU) security of the Even-Mansour variant $\mathsf{PKEM}^{\pi}_{0^r\|K'\|K}$ defined in (1) [43,1,23]. As our results imply the MU security of $\mathsf{PKEM}^{\mathsf{LR}_6}_{0^r\|K'\|K}$ (subsection 5.4, (12)), these keyed sponges could be based on $\mathsf{PKEM}^{\mathsf{LR}_6}_{0^r\|K'\|K}$ instead. And after the keys are canceled, we obtain keyed sponge variants using $\mathsf{LR}_6$ as the permutation. This means the permutation underlying many keyed sponges can be securely instantiated with $\mathsf{LR}_6$. This results in an improved implementation efficiency (maybe at the expense of a decreased security). And when $r < n/2$, security of resulted construction is beyond-birthday with respect to $n$, the size of the underlying ideal functions. This is usually fulfilled in lightweight sponges, since relatively large $c = 2n - r$ is desired: e.g. all the members in the Photon family [30].

Concretely, consider the "inner-keyed" sponge with a $2n$-bit permutation $\pi$ first. By [1], for any distinguisher making $q_c$ queries to the sponge and $q_\pi$ queries to $\pi$, the corresponding distinguishing advantage (from a random oracle) is $\frac{q_c^2}{2^{2n-r}} + \mathbf{Adv}^{\mathsf{SU}}_{\mathsf{PKEM}^{\pi}_{0^r\|K\|K'}}(q_\pi, \sigma)$, where $\sigma$ is the total number of blocks in the $q_c$ construction queries. Therefore, by our results, the security bound of the inner-keyed sponge with $\mathsf{LR}_6$ is

$$\frac{q_c^2}{2^{2n-r}} + \frac{\sigma^3}{2^{2n}} + \frac{\sigma^2 q_f}{2^{2n}} + \frac{\sigma q_f^2}{2^{2n}},$$

where $q_f$ is the number of adversarial random function queries. It's not hard to see similar implications can be derived on "outer-keyed" sponge; however, we are unable to derive concrete bounds.

Another example is Chaskey [43], which is a sponge-like MAC of Mouha et al. With a $2n$-bit permutation $\pi$, the designers proved that the MAC security bound of Chaskey$^{\pi}$ is (roughly) $\frac{\sigma^2}{2^{2n}} + \frac{1}{d} + \mathbf{Adv}^{\mathrm{MU}}_{\mathsf{PKEM}^{\pi}_{K\|K'}}(q_\pi, \sigma)$, where $d$ is the tag size, $\sigma$ is total number of blocks in the adversarial MAC queries, and $q_\pi$ is the number of adversarial queries to $\pi$. Therefore, the security bound of the variant Chaskey$^{\mathsf{LR}_6}$ is $\frac{\sigma^2}{2^{2n}} + \frac{1}{d} + \frac{\sigma^3}{2^{2n}} + \frac{\sigma^2 q_f}{2^{2n}} + \frac{\sigma q_f^2}{2^{2n}}$, where $q_f$ is the number of adversarial random function queries.

## Acknowledgements

We thank the reviewers for invaluable comments, and for pointing [25] to us. Chun Guo is funded in part by the ERC project 724725 (acronym SWORD), and would like to thank François-Xavier Standaert for the invaluable support. Lei Wang is supported by National Natural Science Foundation of China (61602302, 61472250, 61672347), Natural Science Foundation of Shanghai (16ZR1416400), Shanghai Excellent Academic Leader Funds (16XD1401300), 13th five-year National Development Fund of Cryptography (MMJJ20170114).

Finally we thank Yaobin Shen for identifying a flaw (in Lemma 5) in an earlier version of the proof, and Christian Rechberger and Damian Vizár for the discussion on multi-party computation.

## References

1. Andreeva, E., Daemen, J., Mennink, B., Assche, G.V.: Security of Keyed Sponge Constructions Using a Modular Proof Approach. In: FSE 2015. pp. 364–384 (2015)
2. Bar-On, A., Biham, E., Dunkelman, O., Keller, N.: Efficient Slide Attacks. Journal of Cryptology (Aug 2017)
3. Barbosa, M., Farshim, P.: The Related-Key Analysis of Feistel Constructions. In: Cid, C., Rechberger, C. (eds.) FSE 2014, LNCS, vol. 8540, pp. 265–284. Springer Berlin Heidelberg (2014)
4. Beaulieu, R., Shors, D., Smith, J., Treatman-Clark, S., Weeks, B., Wingers, L.: The SIMON and SPECK Families of Lightweight Block Ciphers. Cryptology ePrint Archive, Report 2013/404 (2013), https://eprint.iacr.org/2013/404.pdf
5. Bellare, M., Boldyreva, A., Micali, S.: Public-Key Encryption in a Multi-user Setting: Security Proofs and Improvements. In: Preneel, B. (ed.) EUROCRYPT 2000, LNCS, vol. 1807, pp. 259–274. Springer New York (2000)
6. Bellare, M., Tackmann, B.: The Multi-user Security of Authenticated Encryption: AES-GCM in TLS 1.3. In: Robshaw, M., Katz, J. (eds.) CRYPTO 2016, Part I, LNCS, vol. 9814, pp. 247–276. Springer Berlin Heidelberg (2016)
7. Bertoni, G., Daemen, J., Peeters, M., Van Assche, G.: Sponge functions. In: Ecrypt Hash Workshop 2007 (2007)
8. Biham, E.: How to decrypt or even substitute DES-encrypted messages in $2^{28}$ steps. Information Processing Letters 84(3), 117–124 (2002)
9. Biryukov, A., Nikolić, I.: Complementing Feistel Ciphers. In: Moriai, S. (ed.) FSE 2013, pp. 3–18. LNCS, Springer Berlin Heidelberg (2013)

10. Biryukov, A., Wagner, D.: Advanced Slide Attacks. In: Preneel, B. (ed.) EUROCRYPT 2000, LNCS, vol. 1807, pp. 589–606. Springer Berlin Heidelberg (2000)
11. Bogdanov, A., Knudsen, L.R., Leander, G., Standaert, F.X., Steinberger, J., Tischhauser, E.: Key-Alternating Ciphers in a Provable Setting: Encryption Using a Small Number of Public Permutations. In: Pointcheval, D., Johansson, T. (eds.) EUROCRYPT 2012, LNCS, vol. 7237, pp. 45–62. Springer Berlin Heidelberg (2012)
12. Bose, P., Hoang, V.T., Tessaro, S.: Revisiting AES-GCM-SIV: Multi-user Security, Faster Key Derivation, and Better Bounds. In: EUROCRYPT 2018, Part I. pp. 468–499 (2018)
13. Canetti, R., Goldreich, O., Halevi, S.: The Random Oracle Methodology, Revisited. J. ACM 51(4), 557–594 (Jul 2004)
14. Chen, S., Lampe, R., Lee, J., Seurin, Y., Steinberger, J.: Minimizing the Two-Round Even–Mansour Cipher. Journal of Cryptology (May 2018)
15. 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 Berlin Heidelberg (2014)
16. Cogliati, B., Lampe, R., Seurin, Y.: Tweaking Even-Mansour Ciphers. In: Gennaro, R., Robshaw, M. (eds.) CRYPTO 2015, Part I, LNCS, vol. 9215, pp. 189–208. Springer Berlin Heidelberg (2015)
17. 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, Part II, LNCS, vol. 9453, pp. 134–158. Springer Berlin Heidelberg (2015)
18. Daemen, J., Rijmen, V.: Probability Distributions of Correlation and Differentials in Block Ciphers. Journal of Mathematical Cryptology 1(3), 221–242 (2007)
19. Dai, Y., Seurin, Y., Steinberger, J., Thiruvengadam, A.: Indifferentiability of Iterated Even-Mansour Ciphers with Non-idealized Key-Schedules: Five Rounds Are Necessary and Sufficient. In: Katz, J., Shacham, H. (eds.) CRYPTO 2017, Part III, LNCS, vol. 10403, pp. 524–555. Springer Berlin Heidelberg (2017)
20. Dodis, Y., Katz, J., Steinberger, J., Thiruvengadam, A., Zhang, Z.: Provable Security of Substitution-Permutation Networks. Cryptology ePrint Archive, Report 2017/016 (2017), http://eprint.iacr.org/2017/016.pdf
21. Dunkelman, O., Keller, N., Shamir, A.: Slidex Attacks on the Even-Mansour Encryption Scheme. Journal of Cryptology 28(1), 1–28 (2015)
22. Even, S., Mansour, Y.: A Construction of a Cipher From a Single Pseudorandom Permutation. Journal of Cryptology 10(3), 151–161 (1997)
23. Gaži, P., Pietrzak, K., Tessaro, S.: The Exact PRF Security of Truncation: Tight Bounds for Keyed Sponges and Truncated CBC. In: Gennaro, R., Robshaw, M. (eds.) CRYPTO 2015, Part I, LNCS, vol. 9215, pp. 368–387. Springer Berlin Heidelberg (2015)
24. 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 Berlin Heidelberg (2004)
25. Gilboa, S., Gueron, S., Nandi, M.: Balanced Permutations Even-Mansour Ciphers. Cryptography 1(1), 2 (2017)
26. Gueron, S., Lindell, Y.: Better Bounds for Block Cipher Modes of Operation via Nonce-Based Key Derivation. In: CCS 2017. pp. 1019–1036 (2017)
27. Guo, C., Lin, D.: On the Indifferentiability of Key-Alternating Feistel Ciphers with No Key Derivation. In: Dodis, Y., Nielsen, J.B. (eds.) TCC 2015, Part I, LNCS, vol. 9014, pp. 110–133. Springer Berlin Heidelberg (2015)

28. Guo, C., Wang, L.: Revisiting Key-alternating Feistel Ciphers for Shorter Keys and Multi-user Security. Cryptology ePrint Archive, Report 2018/816 (2018), http://eprint.iacr.org/2018/816.pdf. The full version of this paper.
29. Guo, J., Jean, J., Nikolić, I., Sasaki, Y.: Meet-in-the-Middle Attacks on Generic Feistel Constructions. In: Sarkar, P., Iwata, T. (eds.) ASIACRYPT 2014, Part I, LNCS, vol. 8873, pp. 458–477. Springer Berlin Heidelberg (2014)
30. Guo, J., Peyrin, T., Poschmann, A.: The PHOTON Family of Lightweight Hash Functions. In: CRYPTO 2011. pp. 222–239 (2011)
31. Hoang, V.T., Rogaway, P.: On Generalized Feistel Networks. In: Rabin, T. (ed.) CRYPTO 2010, LNCS, vol. 6223, pp. 613–630. Springer Berlin Heidelberg (2010)
32. 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, Part I, LNCS, vol. 9814, pp. 3–32. Springer Berlin Heidelberg (2016)
33. Isobe, T., Shibutani, K.: Generic Key Recovery Attack on Feistel Scheme. In: Sako, K., Sarkar, P. (eds.) ASIACRYPT 2013, Part I, LNCS, vol. 8269, pp. 464–485. Springer Berlin Heidelberg (2013)
34. Izadi, M., Sadeghiyan, B., Sadeghian, S., Khanooki, H.: MIBS: A New Lightweight Block Cipher. In: Garay, J.A., Miyaji, A., Otsuka, A. (eds.) CANS 2009, LNCS, vol. 5888, pp. 334–348. Springer Berlin Heidelberg (2009)
35. Jager, T., Stam, M., Stanley-Oakes, R., Warinschi, B.: Multi-key Authenticated Encryption with Corruptions: Reductions Are Lossy. In: TCC 2017, Part I. pp. 409–441 (2017)
36. 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 Berlin Heidelberg (2014)
37. Luby, M., Wigderson, A.: Pairwise Independence and Derandomization. Foundations and Trends in Theoretical Computer Science 1(4) (2005)
38. Luby, M.G., Rackoff, C.: Pseudo-random Permutation Generators and Cryptographic Composition. In: Proceedings of the Eighteenth Annual ACM Symposium on Theory of Computing. pp. 356–363. STOC '86, ACM, New York, NY, USA (1986)
39. Mandal, A., Patarin, J., Seurin, Y.: On the Public Indifferentiability and Correlation Intractability of the 6-Round Feistel Construction. In: Cramer, R. (ed.) TCC 2012, LNCS, vol. 7194, pp. 285–302. Springer Berlin Heidelberg (2012)
40. Maurer, U., Pietrzak, K.: The Security of Many-Round Luby-Rackoff Pseudo-Random Permutations. In: Biham, E. (ed.) EUROCRYPT 2003, LNCS, vol. 2656, pp. 544–561. Springer Berlin Heidelberg (2003)
41. Miles, E., Viola, E.: Substitution-Permutation Networks, Pseudorandom Functions, and Natural Proofs. In: Safavi-Naini, R., Canetti, R. (eds.) CRYPTO 2012, LNCS, vol. 7417, pp. 68–85. Springer Berlin Heidelberg (2012)
42. Mouha, N., Luykx, A.: Multi-key Security: The Even-Mansour Construction Revisited. In: Gennaro, R., Robshaw, M. (eds.) CRYPTO 2015, Part I, LNCS, vol. 9215, pp. 209–223. Springer Berlin Heidelberg (2015)
43. Mouha, N., Mennink, B., Herrewege, A.V., Watanabe, D., Preneel, B., Verbauwhede, I.: Chaskey: An Efficient MAC Algorithm for 32-bit Microcontrollers. In: SAC 2014. pp. 306–323 (2014)
44. Nachef, V., Patarin, J., Volte, E.: Feistel Ciphers - Security Proofs and Cryptanalysis. Springer (2017)

45. Nandi, M.: The Characterization of Luby-Rackoff and Its Optimum Single-Key Variants. In: Gong, G., Gupta, K.C. (eds.) INDOCRYPT 2010, LNCS, vol. 6498, pp. 82–97. Springer Berlin Heidelberg (2010)
46. Nandi, M.: On the Optimality of Non-Linear Computations of Length-Preserving Encryption Schemes. In: Iwata, T., Cheon, J.H. (eds.) ASIACRYPT 2015, Part II, LNCS, vol. 9453, pp. 113–133. Springer Berlin Heidelberg (2015)
47. Patarin, J.: How to Construct Pseudorandom and Super Pseudorandom Permutations from One Single Pseudorandom Function. In: Rueppel, R.A. (ed.) EUROCRYPT '92, LNCS, vol. 658, pp. 256–266. Springer Berlin Heidelberg (1992)
48. Patarin, J.: Improved Security Bounds for Pseudorandom Permutations. In: CCS '97, pp. 142–150. ACM (1997)
49. Patarin, J.: Security of Random Feistel Schemes with 5 or More Rounds. In: Franklin, M. (ed.) CRYPTO 2004, LNCS, vol. 3152, pp. 106–122. Springer Berlin Heidelberg (2004)
50. Ramzan, Z., Reyzin, L.: On the Round Security of Symmetric-Key Cryptographic Primitives. In: Bellare, M. (ed.) CRYPTO 2000, LNCS, vol. 1880, pp. 376–393. Springer Berlin Heidelberg (2000)
51. Rotaru, D., Smart, N.P., Stam, M.: Modes of Operation Suitable for Computing on Encrypted Data. IACR Trans. Symmetric Cryptol. 2017(3), 294–324 (2017)
52. Sadeghiyan, B., Pieprzyk, J.: A Construction for Super Pseudorandom Permutations from A Single Pseudorandom Function. In: Rueppel, R.A. (ed.) EUROCRYPT '92, LNCS, vol. 658, pp. 267–284. Springer Berlin Heidelberg (1992)
53. Soni, P., Tessaro, S.: Public-Seed Pseudorandom Permutations. In: Coron, J.S., Nielsen, J.B. (eds.) EUROCRYPT 2017, Part II, LNCS, vol. 10211, pp. 412–441. Springer Berlin Heidelberg (2017)
54. Standaert, F., Pereira, O., Yu, Y.: Leakage-Resilient Symmetric Cryptography under Empirically Verifiable Assumptions. In: CRYPTO 2013, Part I. pp. 335–352 (2013)
55. Suzaki, T., Minematsu, K., Morioka, S., Kobayashi, E.: TWINE: A Lightweight Block Cipher for Multiple Platforms. In: Knudsen, L.R., Wu, H. (eds.) SAC 2012, LNCS, vol. 7707, pp. 339–354. Springer Berlin Heidelberg (2013)
56. Tessaro, S.: Optimally Secure Block Ciphers from Ideal Primitives. In: Iwata, T., Cheon, J.H. (eds.) ASIACRYPT 2015, Part II, LNCS, vol. 9453, pp. 437–462. Springer Berlin Heidelberg (2015)
57. Wu, W., Zhang, L.: LBlock: A Lightweight Block Cipher. In: ACNS 2011. pp. 327–344 (2011)