Understanding the Related-Key Security of Feistel Ciphers from a Provable Perspective

Chun Guo

***Abstract*—We initiate the provable related-key security treatment for models of *practical* Feistel ciphers. In detail, we consider Feistel networks with four whitening keys $w_i(k)$, $i = 0, 1, 2, 3$, and round-functions of the form $f(\gamma_j(k) \oplus X)$, where k is the master-key, w_i and γ_j are efficient transformations, and f is a *public* ideal function or permutation accessible by the adversary. We investigate key-schedule conditions that are sufficient for security against XOR-induced related-key attacks up to $2^{n/2}$ adversarial queries. When the key-schedules are *non-linear*, we prove security for 4 rounds. When only *affine* key-schedules are used, we prove security for 6 rounds. These also imply secure tweakable Feistel ciphers in the Random Oracle model.**

By shuffling the key-schedules, our model unifies both the DES-like structure (known as *Feistel-2* scheme in the cryptanalytic community, a.k.a. *key-alternating Feistel* due to Lampe and Seurin, FSE 2014) and the Lucifer-like model (previously analyzed by Guo and Lin, TCC 2015). This allows us to derive concrete implications on these two (more common) models, and helps understanding their related-key security difference.

***Index Terms*—blockcipher, provable security, indistinguishability, related-key, Feistel cipher, key-alternating paradigm.**

I. Introduction

Feistel-like blockciphers consist of several iterative applications of a simple Feistel permutation

$$\Phi_{G_{k_i}}(W_L \| W_R) = W_R \| W_L \oplus G_{k_i}(W_R) \tag{1}$$

for a keyed function $G : \{0,1\}^\kappa \times \{0,1\}^n \to \{0,1\}^n$ on n-bit strings, yielding a $2n$-bit blockcipher [1]. Such ciphers and their generalizations constitute a half proportion of modern blockciphers, including some most popular designs such as DES [2], Lucifer [3], GOST [4], and NSA's SIMON family [5]. This has made it the object of a very large (and still increasing) amount of analyses.

In information-theoretic model, the round-function G would be assumed somewhat random. Without additional hardness assumption, provable security is limited to *at most* 2^n queries [6], which is much smaller than 2^{2n}, the domain-size of the Feistel ciphers. Despite this limitation as well as the gap between the strong assumption on G and the weak round-functions in practical ciphers, this approach excludes any possibility of generic attacks and supplies insights into the cipher structures. Therefore, it has found applications in both Feistel ciphers [7], [6], [8], [9], [10], [11] and their counterpart Key-Alternating Ciphers (KACs) [12], [13], [14], [15].[1]

Related-Key Attacks (RKAs) were independently introduced by Biham [16] and Knudsen [17] in early 1990s, and was later formalized by Bellare and Kohno [18]. In this setting, the adversary is allowed to query the blockcipher under multiple secret keys that satisfy adversary-chosen relations. The presence of such related-keys may be the consequence of a protocol-level key update [19], or the user key being tampered by fault injections [20]. The adversarial goal is to either recover the secret key(s), or to distinguish the related-key oracles from independent random permutations [18].

RKAs can be classified according to the adversary-chosen relations between the keys. Likely, the most important category is the so-called XOR-induced Related-Key Attack ($\oplus$-RKA) [21], i.e., RKA that allows the adversary to XOR any constant of its choice to the secret user key. Such RKAs are important for at least three reasons. First, they arise naturally in a number of contexts, such as the f8 and f9 protocols of the 3GPP standard [19]. Second, from a theoretical point of view, they are the simplest kind of attacks to have the completeness property [22], namely, for any keys $k, k' \in \{0,1\}^n$, there exists $\Delta \in \{0,1\}^n$ such that $k \oplus \Delta = k'$.

Last—but most importantly,—$\oplus$-RKAs are the most relevant to cryptanalytic practice. Most practical ciphers mix the keys into the state via the XOR operation. As commented in [23], for such targets $\oplus$-RKAs are inherent to the majority of differential-based attacks, as XOR key-relations leave the chance of canceling the state difference with the (chosen) round-key difference (this phenomena was named *local collision* [24]) and extending differentials without decreasing their probabilities. Due to this, $\oplus$-RKAs have been the most widely used attack model in symmetric cryptanalysis (as another example, the powerful related-key boomerang and rectangle attacks were in the $\oplus$-RKA form when firstly introduced [25]). And they have given rise to a plenty of prominent results, including very efficient (distinguishing) attacks on many Feistel ciphers that will be mentioned in the next subsection, a practical-time attack on the 3GPP encryption algorithm KASUMI [26], and a forgery attack on 3-DES-based RMAC [27]. And their variants break full AES-192 and AES-256 [24] and 10-round AES-256 in practical-time [28].[2] The mentioned attack on RMAC is also a notable example of RKA weakness resulting in more disastrous attacks on high-level primitives, showing that pursuing RKA security is not purely theoretical.

Chun Guo is with the Department of ICTEAM/ELEN/Crypto Group, Université catholique de Louvain, Louvain-la-Neuve e-mail: (chun.guo.sc@gmail.com).

Manuscript received May xx, 2018; revised xxxxxx.

[1] KACs are blockciphers that alternatively apply key-additions and keyless permutations, i.e., $\mathsf{KAC}^{P_1,\ldots,P_t}_{k_0,k_1,\ldots,k_t}(M) = k_t \oplus P_t(\ldots(k_1 \oplus P_1(k_0 \oplus M)))$.

[2] These variants assumed XORing constants into the round-keys, and are thus called *related sub-key attacks*.

Our Question. With the above, $\oplus$-RKAs deserve special attention on the theoretical side. Recall that such a provable security requires that with a secret key k, the q blockcipher instances $\mathsf{E}_{k\oplus\Delta_1}, \ldots, \mathsf{E}_{k\oplus\Delta_q}$ queried by the attacker with distinct chosen constants $\Delta_1, \ldots, \Delta_q$ are indistinguishable from q independent random permutations. Such security has been established for KACs [21], [29] and their tweakable variants [30]. It's then natural to ask: under which conditions could Feistel ciphers be provably secure against $\oplus$-RKAs?

In fact, to a large extent, our motivation also stems from practice: certain structural features cause remarkable $\oplus$-RKA weakness in a lot of Feistel ciphers in reality. The most well-known example must be the complementation property in DES [31], i.e. $\mathrm{DES}_{\overline{k}}(\overline{M}) = \overline{\mathrm{DES}_k(M)}$ where $\overline{X}$ is the bit-by-bit complementation of X. This non-random behavior also exists in its variants 3-DES [32] and DESL [33]. This not only cinches efficient related-key distinguishers on DES, but also reduces its effective key-length by 1 bit in the traditional single-key attack setting. Although appearing harmless, it has been long asked how to overcome [34]. Other marvelous examples include $\oplus$-RKAs on GOST with *very low complexity* described in [35] and [36], and *very efficient* distinguisher on the SHA-3 candidate based on *Lesamnta* [37]. In all, it appears that the components (e.g. key-schedules) of Feistel ciphers have to be carefully designed in order to achieve RKA security. This is sharply contrast to the KAC model, for which even the simplest idea $k \oplus P(k \oplus P(k \oplus P(k \oplus M)))$ already buys some level of security (see [29]). A better understanding of Feistel ciphers in the RKA setting is thus crucial.

We have noticed two works that partially addressed our question. The first work of Barbosa and Farshim proved that the famous Luby-Rackoff model with round-keys rightfully reused is RKA secure [10]. Such models are Feistel networks using a pseudorandom function (PRF) G_{k_i} as the round-function [7], and have been extensively studied, with [6] and [8] to name a few. Unfortunately, this model overlooks many structural properties, e.g. the complementation property, and this leaves a huge gap between model and reality. In addition, it's arguably too strong to model the round-function as a PRF secure against RKAs—while the practice-motivated model $G_{k_i}(W_R) = f(k_i \oplus W_R)$ may be a PRF when f is not too weak, it's *never* an RKA-secure PRF. A comprehensive discussion is given later in page 4. In all, in the RKA setting, Luby-Rackoff results appear less convincing.

The second work of Guo and Lin proved that a Lucifer-like Feistel structure (will be clarified later: see Eq. (3), or Eq. (61) in Appendix A) could be indifferentiable from ideal ciphers [38], which implies $\oplus$-RKA security by [29]. But their extremely weak bound $q^{30}/2^n$ appears meaningless.

With these considerations, we'd like to bridge theory and reality: we'd like to *find a model that could well capture the structural features*—including the known RKA weakness—of practical Feistel ciphers, and *then study under which constraints the model could achieve $\oplus$-RKA security*. Hopefully, this will serve invaluable insights, and help address the challenge of designing RKA secure Feistel ciphers—and further tweakable Feistel ciphers, as RKA-secure ciphers and tweakable blockciphers [39] are strongly related [18].

A Unified Model for Feistel Ciphers in Reality. Practical Feistel ciphers usually employ keyless transformations for round-functions, and mix the keys into the structure via efficient group operations (usually xor). In addition, whitening keys may be used. This naturally motivates modeling the keyless round-functions as *public* (random) functions or permutations f_i, *explicitly xoring the round-keys somewhere*, and eventually adding whitening keys.

In detail, we consider Feistel networks in which the state at round i is updated according to

$$W_L \| W_R \mapsto W_R \| W_L \oplus \underline{f_i(k_i \oplus W_R)}, \tag{2}$$

and four n-bit whitening keys (wk_0, wk_1, wk_2, wk_3) are used. Among them, $wk_0 \| wk_1$ is used as the pre-whitening key, while $wk_2 \| wk_3$ is the post-whitening key. Its special case *without whitening keys* was named *Key-Alternating Feistel (KAF)* by Lampe and Seurin [9]. Thus we name our model *Key-Alternating Feistel with Whitening keys (KAFw)*.

To be closer to the reality, we do not assume the components *independent*. Instead, we assume: (i) all the round-functions $f_1, \ldots, f_t$ are **the same one** denoted f, and (ii) each sub-key is derived from an n-bit master-key k via an efficiently computable n-to-n-bit transformation, i.e. $k_i = \gamma_i(k)$ for $i = 1, \ldots, t$, and $wk_j = w_j(k)$ for $j = 1, 2, 3, 4$.[3] Please see Fig. 1 for the instances with 4 and 6 rounds. Denote by (w, γ) such a key-schedule function for t-rounds, $w = (w_0, w_1, w_2, w_3)$, $\gamma = (\gamma_1, \ldots, \gamma_t)$; and denote by $\mathsf{KAFw}^{f,(w,\gamma)}$ the "single-function" KAFw model with round-function f and key-schedule (w, γ).

On Other Models. We re-stress our model should be distinguished from the mentioned *Luby-Rackoff model* built upon a PRF $\underline{G_{k_i}(W_R)}$. In such a round-function the key is "embedded" in a *non-obvious way*, and it thus overlooks many structural properties in practical Feistel ciphers.

We did not notice any previous work on our KAFw model.[4] However, by appropriately shuffling the key-schedule $(w, \gamma) = ((w_0, \ldots, w_3), (\gamma_1, \ldots, \gamma_t))$, KAFw unifies existing famous theoretical models, and captures the structures of a large range of Feistel ciphers. To see this, we first note that (as mentioned) by setting the whitening keys to 0, we recover the KAF model, a.k.a. *Feistel-2 schemes* in the cryptanalytic community [41], which has been deeply understood from the cryptanalysis point of view [42], [36], [41] and frequently used as instructive examples for illustrating new attacks [43]. The KAF model roughly captures the structures of DES [2], GOST [4], and Camellia variant without FL/FL^{-1} functions [36].

We then note that in the aforementioned Lucifer-like structure, each round-key is xored *after* the corresponding round-function, i.e. the state at round i is updated according to

$$W_L \| W_R \mapsto W_R \| W_L \oplus \underline{f_i(W_R) \oplus k_i}. \tag{3}$$

[3] While n-bit master-keys may be uncommon in practice, it suffices for serving some insights (as will be seen). To address longer master-keys, the difficulty lies in modeling key-schedules: see the discussion in page 5.

[4] On the practical side, the cipher CLEFIA recommended by the ISO/IEC standard [40] is a 4-line generalization of KAFw.

This afterwards manner effectively eliminates the key interruption in the 1st round and in the last round and allows the analyst to analyze an equivalent two-round-reduced variant [44], using the original 1st and last round-keys as whitening keys: $0\|k_1$ for pre-whitening, and $k_t\|0$ for post-whitening (we include a formal clarification in Appendix A). We denote by KAFv the resulted whitening key-based KAF Variant. Roughly, KAFv or the Lucifer-like model and their multi-line generalizations capture Blowfish [45], TEA [46], XTEA [47], SIMON [5], Piccolo (multi-line KAFv) [48], and RC2 [49]. Most importantly to us, *each KAFv instance is also captured by a KAFw instance with a corresponding key-schedule* (a formal analysis is given in section V-B). Therefore, our model KAFw seems the most general.

By the above discussion, it seems the three models KAFw, KAF, and KAFv are cryptographically equivalent modulo different key-schedules. But this contradicts existing understandings. For example, it was commented that the Lucifer-like structure blocks the complementation property, while in KAF the first and last rounds are more effective [44]; and that KAFv seems stronger against RKAs, which appears one of the motivations to use it [37]. And, assuming **independent** random round-functions and **identical** round-keys, the 21-round KAFv variant is indifferentiable from ideal ciphers [50], while the KAF variant is *never* indifferentiable [38] (even worse, such KAF would collapse to a 1-round KAC built on a keyless multi-round Feistel permutation! see page 6). As will be unveiled in this paper, this distinction stems from the fact that *to achieve the same level of security, KAF and KAFv models require different properties from the involved key-schedules*; and *with common key-schedule designs, KAFv has a higher chance of being secure against RKAs than KAF*! (For details please see below.)

Our Contributions. We first focus on the $\mathsf{KAFw}^{f,(w,\gamma)}$ model and prove general results, and then derive concrete implications on the more popular KAF and KAFv models.

In detail, we analyze both the case of (w,γ) being (highly) non-linear (with respect to $\oplus$) and the case of (w,γ) being purely affine. In each case, (as mentioned) $\mathsf{KAFw}^{f,(w,\gamma)}$ uses **identical round-functions** and sub-keys derived from **an n-bit master-key**. For the round-function f, we consider both $f = F$ a random n-to-n-bit function (denoted $\mathsf{KAFw}^{F,(w,\gamma)}$) and $f = P$ a random n-bit permutation (denoted $\mathsf{KAFw}^{P,(w,\gamma)}$—distinguished by the superscript). The consideration here is two-fold. First, both choices have been adopted in practice, e.g. GOST uses a 32-bit permutation, while SIMON$2n/\kappa$ uses an n-to-n-bit non-bijective function. Second, both choices have advantages: random functions are theoretically attractive since they have less structural properties than random permutations, while the latter allow practical instantiations using e.g. SHA-3 permutations [51] (will be discussed later).

In all, we analyzed four cases: $\mathsf{KAFw}^{F,(w,\gamma)}$ and $\mathsf{KAFw}^{P,(w,\gamma)}$ with non-linear (w,γ), and $\mathsf{KAFw}^{F,(w,\gamma)}$ and $\mathsf{KAFw}^{P,(w,\gamma)}$ with affine (w,γ). With non-linear (w,γ), our main result states sufficient conditions on the key-schedule so that the 4-round $\mathsf{KAFw}^{F,(w,\gamma)}$ and $\mathsf{KAFw}^{P,(w,\gamma)}$ ciphers are secure against $\oplus$-RKAs up to $\widetilde{\mathcal{O}}(2^{n/2})$ queries, where

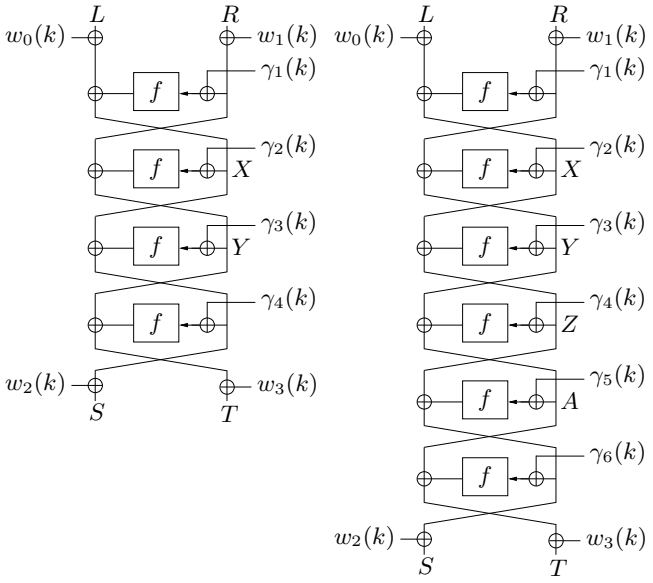

Figure 1. The $\mathsf{KAFw}^{f,(w,\gamma)}$ cipher variants with notations (for the intermediate values) used in this paper. f is a *public* round-function—either a random function F, or a random permutation P. (Left) 4-round $\mathsf{KAFw}^{f,(w,\gamma)}$; (Right) 6-round $\mathsf{KAFw}^{f,(w,\gamma)}$.

the $\widetilde{\mathcal{O}}(\cdot)$ notation hides factors that depend on (w,γ). Such good key-schedules can be instantiated via field arithmetics. For example, with the following key-schedule, the 4-round $\mathsf{KAFw}^{F,(w,\gamma)}$ and $\mathsf{KAFw}^{P,(w,\gamma)}$ are secure up to $c{\cdot}2^{n/2}$ queries for a small constant c (which is given in section VI):

- $w_0(k) = w_3(k) = \gamma_2(k) = \gamma_3(k) = 0$;
- $w_1(k) \oplus \gamma_1(k) = \mathbf{M}_1 \otimes k \oplus k^3$, and $w_2(k) \oplus \gamma_4(k) = \mathbf{M}_4 \otimes k \oplus k^3$, where $\mathbf{M}_1 \neq \mathbf{M}_4$ are two non-zero constants chosen from $\{0,1\}^n$, and $\otimes$ denotes multiplications taken over the finite field $\mathbb{F}_{2^n}$.

Interestingly, this means one could set $\gamma_1(k) = \gamma_4(k) = 0$, i.e., the security of the 4-round Feistel cipher can be fully based on carefully chosen pre- and post-whitening keys.

For any cipher with an n-bit master-key, an RKA adversary could leverage collisions between secret related-keys and offline guesses for distinguishing with $2^{n/2}$ queries [18]. Our birthday bound is thus tight. The 4 rounds are also tight, as otherwise a standard (i.e., non related-key), adaptive chosen-plaintext and ciphertext attack (CCA) is possible (see e.g. [6]).

Without non-linearity, using a related-key boomerang [25] distinguisher we break four rounds with any affine (w,γ), and further using the boomerang switch trick [24] we break five rounds under one more assumption on (w,γ). Our positive result states conditions on the key-schedule that suffice for $2^{n/2}$ security of 6-round $\mathsf{KAFw}^{F,(w,\gamma)}$ and $\mathsf{KAFw}^{P,(w,\gamma)}$. The (simple) conditions (roughly) prevent self-symmetry and complementation properties. An example, which also highlights the importance of the 1st and last round-keys, is as follows:

- $w_0(k) = w_1(k) = w_2(k) = w_3(k) = 0$, i.e., no whitening keys;
- $(\gamma_1(k), \gamma_2(k), \gamma_3(k), \gamma_4(k), \gamma_5(k), \gamma_6(k)) = (k, 0, 0, 0, 0, \pi(k))$, where $\pi(k_L\|k_R) = k_R\|k_L \oplus k_R$.

Note that this π is a linear orthomorphism, i.e., a permutation of $\{0,1\}^n$ for which $x \mapsto x \oplus \pi(x)$ is also a permutation. Orthomorphisms have been found helpful in establishing nice theoretical results, in particular minimal Luby-Rackoff models [52] and 2-round KACs [53]. We remark that such a key-schedule seems rather weak. Yet, it suffices for our birthday provable security. Stronger key-schedules might help establish beyond-birthday security, which is left for future work.

IMPLICATIONS ON KAF AND KAFV. From the general results on KAFw we can derive positive results on 4- and 6-round KAF and KAFv, and that which conditions on the key-schedules suffice for security.

For non-linear key derivation functions (KDFs) our results indicate they could increase the $\oplus$-RKA security of KAF. This confirms the theoretical soundness of designs with highly non-linear key-schedules, e.g. CAST-128 [54].[5]

For affine KDFs the situation is a bit complicated (and more interesting). Roughly speaking, for KAF (and also KAFw) ciphers, one should pay additional attention on the interaction between the KDFs at the odd rounds and even rounds respectively. On the other hand, for KAFv ciphers it (may) suffice to just focus on designing each round-KDF, without considering the interactions between different rounds. These explain the different behaviors of KAF and KAFv structures, and serve as theoretical evidence that *with common ad hoc key-schedule designs, KAFv variants do have a higher chance to achieve $\oplus$-RKA security than KAF and KAFw.* This confirms the theoretical soundness of reverting to KAFv structures to improve RKA security, which—as mentioned,—seems a folklore [44], [37], and seems the idea underlying many KAFv ciphers mentioned before. For clearness, more discussion is deferred to Section V, after we present the concrete key-schedule conditions.

Aside from clarifying KAF and KAFv models, our results also provide new insights into designing affine key-schedules for practical Feistel ciphers, which is a long-standing open problem hightlighted in e.g. [23], [12]. Note that affine key-schedules are usually preferred (e.g., DES, SIMON, etc.) due to their efficiency and compatibility with frequently rekeying.

TWEAKABLE FEISTEL CIPHERS. By the general result of Bellare and Kohno [18], given a $\oplus$-RKA secure blockcipher $\mathsf{E}_k(M)$ with n-bit k, XORing the tweak t into the key, i.e. $\mathsf{E}_{k\oplus t}(M)$, gives rise to a tweakable blockcipher (TBC) with n-bit tweaks and keys and provable security against $2^{n/2}$ queries. Therefore, efficient tweakable Feistel ciphers with birthday security could be obtained from our results. We stress that tweakable Feistel ciphers obtained via our approach are in the Random Oracle Model, i.e. with *public random* round-functions, which significantly deviates from the tweakable Luby-Rackoff ciphers [56] built upon *secret random* functions.

MODES FOR PERMUTATIONS. Alternatively, the variants $\mathsf{KAFw}^{P,(w,\gamma)}$, $\mathsf{KAF}^{P,\gamma}$, and $\mathsf{KAFv}^{P,\gamma^*}$ can be viewed as modes for cryptographic permutations. With the appearance of reliable permutations such as the permutations underlying SHA-3 [51] and the Simpira family [57], our results allow creating highly modular wide-block ciphers with some level of provable $\oplus$-RKA security support, or wide-block tweakable Feistel ciphers. These may find application in various settings, for example, instantiating provably secure robust authenticated encryption [60], [57], Onion-AE [58], and disk encryption [59].

For comparison, the KAC results [29], [21], [30], [61] also offered such permutation modes. But $\mathsf{KAFw}^{P,(w,\gamma)}$ achieves *domain extension* at the same time, i.e. it offers a provable TBC from "smaller" permutations. This may reduce implementation cost and increase security confidence.

Finally, we remind the reader that all of our results are derived in the Random Oracle Model. Once instantiated, arguments and security insurance turn heuristic [63].

Related Work and Comparison. As mentioned, Barbosa and Farshim (BF) have studied provable RKA-security of Luby-Rackoff models [10]. Here we make a comprehensive comparison. In detail, BF proved the following 4-round Luby-Rackoff variant (see Eq. (1) for the function $\Phi_{G_{k_i}}(X)$)

$$\mathsf{LR}_{k_1,k_2}(M) = \Phi_{G_{k_2}}(\Phi_{G_{k_1}}(\Phi_{G_{k_2}}(\Phi_{G_{k_1}}(M))))$$

is CCA secure against RKAs, if G is an RKA-secure PRF. BF's work has two advantages:

(i) Their results covered a much wider range of Related-Key Derivation (RKD) function set. Informally, this means LR_{k_1,k_2} is secure even if the attacker queries $\mathsf{LR}_{\psi(k_1,k_2)}$ for ψ more complicated than $(k_1\|k_2)\oplus\Delta$.

(ii) Their round-functions are more "generic", and could be instantiated under complexity assumptions.

For (i), as we argued, we aim at bridging theory and reality. The most widely-used attack model is $\oplus$-RKA, and it's not clear whether the complicated RKD functions are indeed possible in reality. Moreover, for KAFw, RKA security against larger RKD sets isn't "for-free": since the sufficient key-schedule conditions heavily depend on the concrete RKD function (e.g. see Definition 1), more complicated key-schedules are likely required. Random oracle KDFs should be sufficient for all "interesting" RKD sets, but they fall short of providing insights into practical designs. In all, it seems questionable to spend a lot of complexity on the key-schedules to buy security against somewhat artificial RKD sets. These clarify why we concentrate on $\oplus$-RKAs. Still, considering larger RKD sets is of theoretical interest, and is a possible future direction.

For (ii), we argue switching from Luby-Rackoff to KAFw is a significant step in cryptography along two axes.

First, viewing Feistel networks as abstract models of real-world blockciphers, we already argued that the Luby-Rackoff model $\mathsf{LR}_{k_1,k_2}(M)$, though seems generic, is arguably too far from cryptographic reality in the RKA setting. Even in theory there remains imperfectness: the Luby-Rackoff model doesn't show how to concretely design *keyed* primitives from (conceptually) simpler *keyless* primitives; it just "defers" the task to designing *keyed* round-function G_{k_i}. In the RKA setting, this requires an RKA-secure PRF G_{k_i} from keyless primitives, which is even harder.

[5] But in practice, this should be interpreted with caution. CLEFIA also employs a highly non-linear key-schedule, but suffers from weak-keys [55] in the RKA setting. Weak-keys couldn't be covered by these theoretical analyses.

In contrast, KAFw results demonstrate how to construct blockciphers from keyless permutations or functions, which fitted into a hot topic (see the KAC papers [12]), and has been recently re-emphasized by Diffie (in Leiden, March, 2018). This nicely fills in the gap left by Luby-Rackoff results.

Second, viewing Feistel networks as modes, this represents switching from *modes for PRFs/blockciphers* to *modes for keyless permutations*. Permutation-based modes not only offer more choices, but also reduce the burden of designers (they could focus on designing one permutation without considering RKA issues). Therefore, it has been a long trend, with prominent examples include the popular multi-purpose sponge functions [65], permutation-based hash functions [67], [68], and authenticated encryption modes [64], [66].

In summary, BF's work is more foundational, and shows how to build RKA secure PRPs from RKA secure PRFs, while our work tries to shed more light on the practical side. BF's Luby-Rackoff approach also gives rise to RKA-secure ciphers and TBCs, but it requires an RKA secure PRF, for which it may not be easy to find an efficient and reliable candidate (especially when a large block-size is desired).

A concurrent work of Cogliati et al. shows how to construct wide-block TBC from SPNs [62]. They focus on (better) beyond-birthday bounds, while we proved $\oplus$-RKA security which may not be implied by tweakable pseudorandomness. They shed lights on SPNs, while we on Feistel (that could use non-invertible functions). In all, the two works are complementary.

Concentrating on Feistel ciphers in the ideal model, previous works only considered KAF and KAFv. In the provable setting, KAF has been analyzed by Lampe and Seurin [9]. While they proved better bounds of $2^{\frac{tn}{t+1}}$ queries for $6t$ rounds, they assumed *completely independent* round-functions *and independent* round-keys and they only considered the *single-key security*. A recent improvement considered *correlated round-keys*, and proved *multi-user* security with birthday bounds $2^{n/2}$ at 4 rounds and beyond-birthday bounds $2^{2n/3}$ at 6 rounds [69]. The 4-round "minimal" KAF scheme given in [69] consumes a (linear) orthomorphism for the key-schedule, which is very similar to ours. Thus in some sense, our results indicate that stronger key-schedule assumptions (i.e., non-linearity) buy $\oplus$-RKA security. We additionally considered *round permutation case*, and this gives rise to permutation-modes. Another (mentioned) work is the indifferentiability of KAFv of [38], the security bound of which was however too weak.

Initiated in [70], a series of papers established efficient generic approaches to obtain RKA secure blockciphers from PRPs [10], [71], which are complementary to our "concrete" results. Generic transformations however fall short of deepening the understanding of widely-deployed structures.

Finally, in the ideal model, key-schedule conditions that suffice for some level of security have been characterized for single-key security of Luby-Rackoff [72], KACs [53], and SPNs [62], for $\oplus$-RKA security of KACs [21], and for indifferentiability of Luby-Rackoff [11] and KACs, see [15] and the reference therein. These results are complementary to ours. Since we identified *concrete* conditions, our work is closer to the series [53], [21], [62].

Possible Future Works include: investigating RKA security of KAFw with respect to larger RKD function sets, posing beyond-birthday secure tweakable KAFw variants, or studying key-schedules sufficient for chosen-key security [73]. The most attractive direction seems to prove beyond-birthday security for KAFw models with $\geq 2n$-bit master-keys. This is much closer to reality, but it requires modeling the combinatorial properties of "non-trivial" key-schedules for longer master-keys, which seems quite hard. For RKA security, some level of dependence has to be assumed between the round-keys [12]. The dependence should be both close to reality and enough for proofs. So which type of dependence is satisfying? A natural idea is to consider an alternating form of round-keys $\gamma_1(k)$, $\gamma_2(k')$, $\gamma_3(k)$, $\gamma_4(k')$, ..., where k and k' are the two halves of a $2n$-bit master-key. But this model seems too artificial.

Organization. Section II presents notations, definitions, and tools. In Sections III and IV, we analyze the $\oplus$-RKA security of $\mathsf{KAFw}^{f,(w,\gamma)}$ with non-linear and affine (w,γ) respectively. Then, from the KAFw results we derive results on KAF and KAFv in Section V, and make discussion on theoretically best possible results in Section VI. The complementing attacks are given in Appendix B to help understanding our proofs.

II. Preliminaries

General Notation. For integers $1 \leq b \leq a$, we write $(a)_b = a(a-1)\dots(a-b+1)$ and $(a)_0 = 1$ by convention. In all the following, we fix an integer $n \geq 1$ and denote $N = 2^n$. Further denote by $\mathcal{F}(n)$ the set of all functions from $\{0,1\}^n$ to $\{0,1\}^n$, by $\mathcal{P}(n)$ the set of all permutations on $\{0,1\}^n$, and by $\mathcal{BC}(n,2n)$ the set of all blockciphers with $2n$-bit block size and n-bit keys. For a finite set $\mathcal{X}$, $X \xleftarrow{\$} \mathcal{X}$ means that an element X is selected from $\mathcal{X}$ uniformly at random. For $X, Y \in \{0,1\}^n$, $X\|Y$ or simply XY denotes their concatenation. Finally, throughout this paper, we denote $k \oplus \Delta$ by k_Δ for simplicity.

Non-linear and Affine Functions. For a function $\gamma : \{0,1\}^n \to \{0,1\}^n$, its non-linearity could be measured by

$$\max_{a,b\in\{0,1\}^n, a\neq 0} \left|\{k \in \{0,1\}^n : \gamma(k\oplus a)\oplus\gamma(k) = b\}\right|. \quad (4)$$

Viewing the n-bit input k as an n-dimensional vector over $\mathbb{F}_2$, an n-bit affine function γ can be defined as

$$\gamma(k) = M \cdot k \oplus C$$

for a fixed $n \times n$ matrix over $\mathbb{F}_2$ and a fixed n-dimensional vector C over $\mathbb{F}_2$. By these, a t-round affine key-schedule $(w,\gamma) = ((w_0,w_1,w_2,w_3),(\gamma_1,\dots,\gamma_t))$ (as mentioned in the Introduction) would be specified by $t+4$ fixed matrices $M_0^{(w)}$, $M_1^{(w)}, M_2^{(w)}, M_3^{(w)}, M_1, \dots, M_t$, and $t+4$ fixed vectors/n-bit constants $C_0^{(w)}, C_1^{(w)}, C_2^{(w)}, C_3^{(w)}, C_1, \dots, C_t$:

$$w_i(k) = M_i^{(w)} \cdot k \oplus C_i^{(w)},\ i = 1,2,3,4, \quad (5)$$

and

$$\gamma_j(k) = M_j \cdot k \oplus C_j,\ j = 1,\dots,t. \quad (6)$$

We stress that the multiplication $M \cdot k$ should be distinguished from the aforementioned field multiplication $\mathbf{M} \otimes k$.

Uniform AXU Functions. For conciseness, we characterize good non-linear key-schedules using standard notions of almost XOR-universality (AXU) and uniformity for keyed (hash) functions. To this end, we serve their definitions below. First, a keyed function $H_k(\cdot)$ from the domain $\mathcal{X}$ to $\{0,1\}^n$ is said to be δ-*uniform*, if for any $x \in \mathcal{X}$ and $y \in \{0,1\}^n$,

$$\Pr[k \xleftarrow{\$} \mathcal{K} : H_k(x) = y] \leq \delta,$$

where $\mathcal{K}$ is its key space. H is said δ'-*almost XOR-universal (δ'-AXU)* if for all distinct $x, x' \in \mathcal{X}$ and all $y \in \{0,1\}^n$,

$$\Pr[k \xleftarrow{\$} \mathcal{K} : H_k(x) \oplus H_k(x') = y] \leq \delta'.$$

KAFw Ciphers. As mentioned in the Introduction, we focus on $\mathsf{KAFw}^{f,(w,\gamma)}$, the KAFw variants with two features:

(i) the same function $f : \{0,1\}^n \to \{0,1\}^n$ is used at each round, and
(ii) the key-schedule is $(w, \gamma) = ((w_0, w_1, w_2, w_3), (\gamma_1, \ldots, \gamma_t))$, i.e. the i-th whitening key wk_i is derived from the n-bit master-key k via $wk_i = w_i(k)$, and the i-th round-key k_i is $k_i = \gamma_i(k)$.

For such variants, the i-th round transformation is defined as

$$\Psi^f_{\gamma_i(k)}(W_L \| W_R) = W_R \| W_L \oplus f(\gamma_i(k) \oplus W_R), \quad (7)$$

where W_L and W_R are respectively the left and right n-bit halves of the input. Then the t-round $\mathsf{KAFw}^{f,(w,\gamma)}$ variant is defined as (cf. Fig. 1)

$$\mathsf{KAFw}^{f,(w,\gamma)}_k(W) = wk_{out} \oplus \Psi^f_{\gamma_t(k)} \circ \ldots \circ \Psi^f_{\gamma_1(k)}\big(wk_{in} \oplus W\big),$$

where $wk_{in} = w_0(k) \| w_1(k)$ and $wk_{out} = w_2(k) \| w_3(k)$. To make it more precise, we give formal descriptions for the 4- and 6-round $\mathsf{KAFw}^{f,(w,\gamma)}$ that will be studied later. For the 4-round $\mathsf{KAFw}^{f,(w,\gamma)}_k$, on the $2n$-bit input W which is parsed into $L \| R$, the computation proceeds in 4 steps:

(i) $x_1 \leftarrow \gamma_1(k) \oplus w_1(k) \oplus R$, $y_1 \leftarrow f(x_1)$, $X = w_0(k) \oplus L \oplus y_1$;
(ii) $x_2 \leftarrow \gamma_2(k) \oplus X$, $y_2 \leftarrow f(x_2)$, $Y \leftarrow w_1(k) \oplus R \oplus y_2$;
(iii) $x_3 \leftarrow \gamma_3(k) \oplus Y$, $y_3 \leftarrow f(x_3)$, $S \leftarrow X \oplus y_3 \oplus w_2(k)$;
(iv) $x_4 \leftarrow \gamma_4(k) \oplus w_2(k) \oplus S$, $y_4 \leftarrow f(x_4)$, $T \leftarrow Y \oplus y_4 \oplus w_3(k)$.

One could see Fig. 1 (left) for illustration. For the 6-round $\mathsf{KAFw}^{f,(w,\gamma)}_k$, on input $W = L \| R$, the computation proceeds in 6 steps (as in Fig. 1 (right)):

(i) $x_1 \leftarrow \gamma_1(k) \oplus w_1(k) \oplus R$, $y_1 \leftarrow f(x_1)$, $X = w_0(k) \oplus L \oplus y_1$;
(ii) $x_2 \leftarrow \gamma_2(k) \oplus X$, $y_2 \leftarrow f(x_2)$, $Y \leftarrow w_1(k) \oplus R \oplus y_2$;
(iii) $x_3 \leftarrow \gamma_3(k) \oplus Y$, $y_3 \leftarrow f(x_3)$, $Z \leftarrow X \oplus y_3$;
(iv) $x_4 \leftarrow \gamma_4(k) \oplus Z$, $y_4 \leftarrow f(x_4)$, $A \leftarrow Y \oplus y_4$;
(v) $x_5 \leftarrow \gamma_5(k) \oplus A$, $y_5 \leftarrow f(x_5)$, $S \leftarrow Z \oplus y_5 \oplus w_2(k)$;
(vi) $x_6 \leftarrow \gamma_6(k) \oplus w_2(k) \oplus S$, $y_6 \leftarrow f(x_6)$, $T \leftarrow A \oplus y_6 \oplus w_3(k)$.

As noted in [74], a KAFw cipher (even with independent round-functions) with an even number of rounds can be seen as a special case of a KAC. In detail, the i-th and $(i+1)$-th rounds with round-functions f_i and f_{i+1} and round-keys k_i and k_{i+1} can be rewritten as

$$\Psi^{f_{i+1}}_{k_{i+1}} \circ \Psi^{f_i}_{k_i}(W) = (k_{i+1} \| k_i) \oplus \Psi^{f_{i+1}}_0 \circ \Psi^{f_i}_0((k_{i+1} \| k_i) \oplus W),$$

where $\Psi^{f_{i+1}}_0 \circ \Psi^{f_i}_0$ is a keyless 2-round Feistel permutation. However, provable results on KAFw **cannot** be derived by black-box composition of existing results on KACs and keyless Feistel, since **no** provable results can be seen on $\Psi^{f_{i+1}}_0 \circ \Psi^{f_i}_0$ (let alone the even weaker $\Psi^f_0 \circ \Psi^f_0$).

As a side remark, for a $2t$-round KAFw cipher, if the $2t$ round-keys are identical $k' = \gamma_1(k) = \ldots = \gamma_{2t}(k)$, then it can be seen it's essentially a 1-round KAC, i.e. $(w_2(k) \oplus k' \| w_3(k) \oplus k') \oplus \pi\big((w_0(k) \oplus k' \| w_1(k) \oplus k') \oplus W\big)$, where $\pi = \Psi^{f_{2t}}_0 \circ \ldots \circ \Psi^{f_1}_0$ is a keyless permutation. This is known to be insecure against RKAs [21].

$\oplus$-RKA Security. We follow Cogliati and Seurin [21] to formalize $\oplus$-RKA security in the ideal model. In detail, let E be a $(n, 2n)$-blockcipher, and fix a key $k \in \{0,1\}^n$. We define the $\oplus$-restricted related-key oracle $\mathsf{RK}[\mathsf{E}_k]$, which takes as input an "offset" $\Delta \in \{0,1\}^n$ and a plaintext $LR \in \{0,1\}^{2n}$, and returns $\mathsf{RK}[\mathsf{E}_k](\Delta, LR) := \mathsf{E}_{k \oplus \Delta}(LR)$. It allows inverse queries, which we denote $\mathsf{RK}[\mathsf{E}_k]^{-1}(\Delta, ST) := \mathsf{E}_{k \oplus \Delta}(ST)$. Then, we consider a $\oplus$-restricted related-key adversary D which has access to a function oracle f and a related-key oracle, and must distinguish between two worlds as follows:

- the "real" world, where it interacts with $(\mathsf{RK}[\mathsf{E}_k], f)$, and k is randomly drawn;
- the "ideal" world where it interacts with $(\mathsf{RK}[\mathsf{IC}_k], f)$, where IC is an ideal cipher independent from f, and k is randomly drawn.

The distinguisher is adaptive, and can make two-sided queries to the related-key oracle. Note that in the ideal world, the oracle $\mathsf{RK}[\mathsf{IC}_k]$ essentially implements an independent random permutation for each offset $\Delta \in \{0,1\}^n$. Formally, when $f = F$ is a random function, D's distinguishing advantage on $\mathsf{KAFw}^{F,(w,\gamma)}$ is defined as

$$\mathbf{Adv}^{\oplus\text{-rka}}_{\mathsf{KAFw}^{F,(w,\gamma)}_k}(D) = \Big|\Pr_{\mathsf{IC},k,F}[D^{\mathsf{RK}[\mathsf{IC}_k],F} = 1] - \Pr_{k,F}[D^{\mathsf{RK}[\mathsf{KAFw}^{F,(w,\gamma)}_k],F} = 1]\Big|,$$

where the former probability is taken over the random draw of $\mathsf{IC} \xleftarrow{\$} \mathcal{BC}(n, 2n), k \xleftarrow{\$} \{0,1\}^n, F \xleftarrow{\$} \mathcal{F}(n)$, and the latter probability is taken over $k \xleftarrow{\$} \{0,1\}^n, F \xleftarrow{\$} \mathcal{F}(n)$.

For $\mathbf{Adv}^{\oplus\text{-rka}}_{\mathsf{KAFw}^{P,(w,\gamma)}_k}(D)$, P is randomly picked from the set $\mathcal{P}(n)$, i.e. $P \xleftarrow{\$} \mathcal{P}(n)$. Here the superscripts help distinguish between random function- and permutation-based KAFw.

Furthermore, we consider computationally unbounded distinguishers, and we assume without loss of generality (wlog) that the distinguisher is deterministic and never makes redundant queries. For non-negative integers q_e, q_f, we define the insecurity of the $\mathsf{KAFw}^{f,(w,\gamma)}$ cipher against $\oplus$-restricted related-key attacks as

$$\mathbf{Adv}^{\oplus\text{-rka}}_{\mathsf{KAFw}^{f,(w,\gamma)}_k}(q_f, q_e) = \max_D \mathbf{Adv}^{\oplus\text{-rka}}_{\mathsf{KAFw}^{f,(w,\gamma)}_k}(D),$$

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

The H-Coefficients Technique. We employ the H-coefficient technique [75], and follow the paradigm of Chen and Steinberger [13]. To this end, we summarize the information gathered by the distinguisher in tuples $\mathcal{Q}_E$ and $\mathcal{Q}_f$. The tuple

$$\mathcal{Q}_E = ((\Delta_1, L_1R_1, S_1T_1), \ldots, (\Delta_{q_e}, L_{q_e}R_{q_e}, S_{q_e}T_{q_e}))$$

summarizes the queries to the related-key oracle, and means that the j-th query was either a forward query (Δ_j, L_jR_j) with answer S_jT_j, or a backward query (Δ_j, S_jT_j) with answer L_jR_j. Throughout the remaining, we'll use the bold letter $\mathbf{t}$ as a simplified notation for a tuple (Δ, LR, ST) in $\mathcal{Q}_E$.

Similarly to $\mathcal{Q}_E$, the tuple

$$\mathcal{Q}_f = ((x_1, y_1), \ldots, (x_{q_f}, y_{q_f}))$$

summarizes the queries to the round-function f, and

- when $f = P$ is an invertible permutation, it means the j-th query was either a forward query x_j with answer y_j or a backward query y_j with answer x_j;
- when $f = F$ is a non-invertible function, it means F was queried on $x_1, \ldots, x_{q_f}$ and answered $y_1, \ldots, y_{q_f}$ correspondingly.

To simplify the arguments (in particular, the definition of "bad transcripts"), we reveal to the distinguisher the key k at the end of the interaction. This is wlog since D is free to ignore this additional information to compute its output bit. Formally, we append k to $(\mathcal{Q}_E, \mathcal{Q}_f)$ and obtain what we call the *transcript* $\tau = (\mathcal{Q}_E, \mathcal{Q}_f, k)$ of the attack. With respect to some fixed distinguisher D, a transcript τ is said *attainable* if there exists oracles (IC, f) such that the interaction of D with the ideal world $(\mathsf{RK}[\mathsf{IC}_k], f)$ yields τ. We denote $\mathcal{T}$ the set of attainable transcripts. In all the following, we denote T_{re}, resp. T_{id}, the probability distribution of the transcript τ induced by the real world, resp. the ideal world (note that these two probability distributions depend on the distinguisher). By extension, we use the same notation for a random variable distributed according to each distribution. And we define $\Pr_{re}(\tau) = \Pr[T_{re} = \tau]$ and $\Pr_{id}(\tau) = \Pr[T_{id} = \tau]$.

Given a tuple $\mathcal{Q}_f$ of function queries and a function f, we say that f *extends* $\mathcal{Q}_f$, denoted $f \vdash \mathcal{Q}_f$, if $f(x) = y$ for all $(x, y) \in \mathcal{Q}_f$. Similarly, given a related-key oracle transcript $\mathcal{Q}_E$, a blockcipher E, and a key $k \in \{0,1\}^n$, we say the related-key oracle $\mathsf{RK}[\mathsf{E}_k]$ *extends* $\mathcal{Q}_E$, denoted $\mathsf{RK}[\mathsf{E}_k] \vdash \mathcal{Q}_E$, if $\mathsf{E}_{k\oplus\Delta}(LR) = ST$ for all $(\Delta, LR, ST) \in \mathcal{Q}_E$. It is easy to see that for any attainable transcript $\tau = (\mathcal{Q}_E, \mathcal{Q}_f, k)$, the interaction of the distinguisher with oracles $(\mathsf{RK}[\mathsf{E}_k], f)$ produces τ if and only if $\mathsf{RK}[\mathsf{E}_k] \vdash \mathcal{Q}_E$ and $f \vdash \mathcal{Q}_f$.

With all the above definitions, the main lemma of H-coefficients technique is as follows.

Lemma 1 (Lemma 1 in [53]) *Fix a distinguisher D. Let $\mathcal{T} = \mathcal{T}_{good} \cup \mathcal{T}_{bad}$ be a partition of the set of attainable transcripts $\mathcal{T}$. Assume that there exists ε_1 such that for any $\tau \in \mathcal{T}_{good}$, one has*

$$\frac{\Pr_{re}(\tau)}{\Pr_{id}(\tau)} \geq 1 - \varepsilon_1,$$

and that there exists ε_2 such that $\Pr[T_{id} \in \mathcal{T}_{bad}] \leq \varepsilon_2$. Then $\mathbf{Adv}(D) \leq \varepsilon_1 + \varepsilon_2$.

A proof could be found in [53].

Finally, it's not hard to see

$$\begin{aligned}\Pr_{id}(\tau) &= \Pr[f \vdash \mathcal{Q}_f] \cdot \Pr[\mathsf{RK}[\mathsf{IC}_k] \vdash \mathcal{Q}_E] \\ &\leq \Pr[f \vdash \mathcal{Q}_f] \cdot \left(\frac{1}{N^2 - q_e}\right)^{q_e}.\end{aligned}$$

III. KAFw with Non-linear Key-Schedules

It is well-known that 3-round Feistel networks are not CCA secure even in the single-key setting. So we consider 4-round KAFw. First, in section III-A, we present key-schedule conditions that are sufficient for the $\oplus$-RKA security of the 4-round $\mathsf{KAFw}^{P,(w,\gamma)}$ (which also turn out sufficient for 4-round $\mathsf{KAFw}^{F,(w,\gamma)}$). Then, we start from $\mathsf{KAFw}^{P,(w,\gamma)}$, analyze it in section III-B, and then discuss how to adapt the proof for the 4-round $\mathsf{KAFw}^{F,(w,\gamma)}$ variant (by "dropping" some modules from the proof for $\mathsf{KAFw}^{P,(w,\gamma)}$) in section III-C.

A. Conditions on the Key-Schedules

4-round key-schedules defined as follows would suffice.

Definition 1 (Good Key-Schedule for 4 Rounds) *Consider a 4-round key-schedule (w, γ), where $w = (w_0, w_1, w_2, w_3)$ for $w_i : \{0,1\}^n \to \{0,1\}^n$, and $\gamma = (\gamma_1, \gamma_2, \gamma_3, \gamma_4)$ for $\gamma_i : \{0,1\}^n \to \{0,1\}^n$. Then (w, γ) is* good*, if $\varphi_1(k) = w_1(k) \oplus \gamma_1(k)$ and $\varphi_4(k) = w_2(k) \oplus \gamma_4(k)$ satisfy two conditions as follows:*

(i) *for $i = 1, 4$, the function $H_k(\Delta) := \varphi_i(k \oplus \Delta)$ is δ_1-uniform and δ_2-AXU;*

(ii) *the function $H_k(\Delta, \Delta') := \varphi_1(k \oplus \Delta) \oplus \varphi_4(k \oplus \Delta')$ is δ_3-uniform.*

An example of good key-schedules with $\delta_1, \delta_2, \delta_3 \leq 3/N$ was exhibited in the Introduction, cf. *Our Contributions*.

Note that $\varphi_1(k)$ and $\varphi_4(k)$ effectively mask (and protect) the inputs to the 1st and last round-functions respectively. This protection would be ineffective if the δ_1-uniformness is seriously compromised. An extreme example is $\varphi_1(k) = 0$, for which an adversary could freely compute the 2nd-round intermediate value as $R \| L \oplus F(R)$.

Further note that, $\varphi_i(k \oplus \Delta)$ is δ_2-AXU essentially means the non-linearity (see Eq. (4)) of φ_i is $\delta_2 N$. This condition is intended to reduce the probability of 1-round related-key differentials with non-zero master-key differences; see the argument for condition (B-2) in page 8.

Finally, the 2nd condition is intended to prevent the derived round-keys from harmful "palindrome-like" properties [72] in the RKA setting. For example, consider a key-schedule (w, γ) such that $w(k) = (0, 0, 0, 0)$ and it's easy to derive Δ for which $\gamma(k) = (k'', 0, 0, k')$ and $\gamma(k \oplus \Delta) = (k', 0, 0, k''')$

for any master-key k, i.e., $\varphi_1(k \oplus \Delta) \oplus \varphi_4(k) = \gamma_1(k \oplus \Delta) \oplus \gamma_4(k) = 0$. Then it can be distinguished by querying $\mathsf{RK}[\mathsf{E}_k](0, LR) \to ST$, $\mathsf{RK}[\mathsf{E}_k](\Delta, TS) \to R'L'$, and checking if $R = R'$.

Actually, it might be possible to prove security without the 2nd condition. But this requires γ_2 and γ_3 to fulfill more involved conditions. Therefore, our Definition 1, with no requirement on γ_2 and γ_3 at the expense of slightly more requirements on φ_1 and φ_4, captures a "minimal" group of conditions to some extent.

B. Security for 4 Rounds with Good Key-Schedules and f=P

Instantiated with a good key-schedule, the 4-round $\mathsf{KAFw}^{P,(w,\gamma)}$ is secure against $\oplus$-RKAs.

Theorem 1 *When $q_f + 2q_e \le N/2$, for the 4-round, random permutation-based $\mathsf{KAFw}^{P,(w,\gamma)}$ cipher with a good key-schedule (w, γ) as specified in Definition 1, it holds*

$$\mathbf{Adv}^{\oplus\text{-}rka}_{\mathsf{KAFw}^{P,(w,\gamma)}_k}(q_f, q_e) \le 2\delta_1 q_e q_f + (\delta_2+\delta_3)q_e^2 + \frac{8q_eq_f + 27q_e^2 + 4q_e}{N}.$$

Proof. We first introduce some notations that will ease the subsequent analysis. Let $\tau = (\mathcal{Q}_E, \mathcal{Q}_P, k)$ be an attainable transcript, with $|\mathcal{Q}_E| = q_e$ and $|\mathcal{Q}_P| = q_f$. For convenience, for the involved $\mathcal{Q}_P = ((x_1, y_1), \ldots, (x_{q_f}, y_{q_f}))$, we define two sets

$$\mathcal{X}(\tau) \stackrel{\text{def}}{=\!=} \{x_1, \ldots, x_{q_f}\}, \text{ and } \mathcal{Y}(\tau) \stackrel{\text{def}}{=\!=} \{y_1, \ldots, y_{q_f}\}.$$

For any tuple $\mathbf{t} = (\Delta, LR, ST)$ in $\mathcal{Q}_E$ and any function f ($f = P$ or F; the former is the focus of this subsection), we define 10 functions

$$\begin{aligned}
x_1(\mathbf{t}) &= \varphi_1(k \oplus \Delta) \oplus R,\\
y_1(\mathbf{t}, f) &= f(x_1(\mathbf{t})),\\
X(\mathbf{t}, f) &= L \oplus w_0(k \oplus \Delta) \oplus y_1(\mathbf{t}, f),\\
x_2(\mathbf{t}, f) &= \gamma_2(k \oplus \Delta) \oplus X(\mathbf{t}, f),\\
y_2(\mathbf{t}, f) &= R \oplus w_1(k \oplus \Delta) \oplus Y(\mathbf{t}, f),\\
Y(\mathbf{t}, f) &= T \oplus w_3(k \oplus \Delta) \oplus y_4(\mathbf{t}, f),\\
x_3(\mathbf{t}, f) &= \gamma_3(k \oplus \Delta) \oplus Y(\mathbf{t}, f),\\
y_3(\mathbf{t}, f) &= S \oplus w_2(k \oplus \Delta) \oplus X(\mathbf{t}, f),\\
x_4(\mathbf{t}) &= \varphi_4(k \oplus \Delta) \oplus S,\\
y_4(\mathbf{t}, f) &= f(x_4(\mathbf{t})).
\end{aligned}$$

The suffix f emphasizes that the functions depend on f. Note that these values are derived in an "$LR \to X, Y \leftarrow ST$" manner, rather than the "$LR \to X \to Y \to ST$" manner. Moreover, $x_1(\mathbf{t})$ and $x_4(\mathbf{t})$ only depend on τ.

To ease understanding our proofs, below we serve an overview of our strategy.

1) **Proof Strategy***:* Following Lemma 1, with respect to a fixed (q_f, q_e)-distinguisher D, below in section III-B2 we define bad transcripts, and upper bound their probability of occurring in the ideal world. This probability is computed over the random choice of the key, and thus we could leverage the properties of good key-schedules.

Later in section III-B3, we lower bound $\Pr_{re}(\tau)$ (and thus the ratio $\Pr_{re}(\tau)/\Pr_{id}(\tau)$) for any good τ. In this step we follow [62] and define a "bad" predicate $\mathsf{B}(P)$ on P, such that collisions in the $2q_e$ inputs in the 2nd and 3rd rounds

$$x_2(\mathbf{t}_1, P), \ldots, x_2(\mathbf{t}_{q_e}, P), x_3(\mathbf{t}_1, P), \ldots, x_3(\mathbf{t}_{q_e}, P) \quad (8)$$

and collisions in the $2q_e$ corresponding outputs

$$y_2(\mathbf{t}_1, P), \ldots, y_2(\mathbf{t}_{q_e}, P), y_3(\mathbf{t}_1, P), \ldots, y_3(\mathbf{t}_{q_e}, P) \quad (9)$$

are classified as conditions of $\mathsf{B}(P)$. These values are determined by P and thus random. Consequently, $\Pr[\mathsf{B}(P)]$ could be upper bounded. In addition, as long as $\mathsf{B}(P)$ is not fulfilled, it is easy to transform the probability $\Pr_{re}(\tau)$ into the (easy-to-bound) probability that

$$\Pr[\forall i \in \{1, \ldots, q_e\}, j = 2, 3 : P(x_j(\mathbf{t}_i, P)) = y_j(\mathbf{t}_i, P)],$$

i.e., P is consistent with the inputs/outputs of the middle two rounds. These cinch the final bound.

2) **Bad Transcripts***:* defined as follows.

Definition 2 (Bad Transcripts for 4-Round $\mathsf{KAFw}^{P,(w,\gamma)}$) *An attainable transcript $\tau = (\mathcal{Q}_E, \mathcal{Q}_P, k)$ is* bad*, if at least one of the following conditions is fulfilled:*

- *(B-1) $\exists \mathbf{t} \in \mathcal{Q}_E : x_1(\mathbf{t}) \in \mathcal{X}(\tau)$ or $x_4(\mathbf{t}) \in \mathcal{X}(\tau)$;*
- *(B-2) $\exists \mathbf{t} = (\Delta, LR, ST)$ and $\mathbf{t}' = (\Delta', L'R', S'T')$ in $\mathcal{Q}_E$ such that $\Delta \neq \Delta'$, and $x_1(\mathbf{t}) = x_1(\mathbf{t}')$ or $x_4(\mathbf{t}) = x_4(\mathbf{t}')$;*
- *(B-3) $\exists \mathbf{t} = (\Delta, LR, ST)$ and $\mathbf{t}' = (\Delta', L'R', S'T')$ in $\mathcal{Q}_E$ such that $x_1(\mathbf{t}) = x_4(\mathbf{t}')$ (it could be $\mathbf{t} = \mathbf{t}'$);*
- *(B-4) there exist two distinct queries (Δ, LR, ST) and $(\Delta', L'R', S'T')$ in $\mathcal{Q}_E$ such that $\Delta = \Delta'$, and*
  - *$L \oplus L' = S \oplus S'$, or $R \oplus R' = T \oplus T'$.*
- *(B-5) there exists $(\Delta, LR, ST) \in \mathcal{Q}_E$ such that*
  - *$L \oplus w_0(k \oplus \Delta) = S \oplus w_2(k \oplus \Delta)$, or $R \oplus w_1(k \oplus \Delta) = T \oplus w_3(k \oplus \Delta)$.*

Otherwise we say τ is good. Denote by $\mathcal{T}_{bad}$ the set of bad transcripts.

We analyze the conditions in turn, with (B-1) the first. For any $\mathbf{t} = (\Delta, LR, ST)$ in $\mathcal{Q}_E$ and any x, as $H_k(\Delta) = \varphi_1(k \oplus \Delta)$ is δ_1-uniform (cf. Definition 1), we immediately have

$$\Pr[x_1(\mathbf{t}) \in \mathcal{X}(\tau)] = \Pr[\exists x \in \mathcal{X}(\tau) : \varphi_1(k_\Delta) = R \oplus x] \le \delta_1 q_f.$$

Similarly, $\Pr[x_4(\mathbf{t}) \in \mathcal{X}(\tau)] \le \delta_1 q_f$. Since there are q_e choices for $\mathbf{t}$, we have

$$\Pr[\text{(B-1)}] \le 2\delta_1 q_e q_f.$$

For (B-2), since $H_k(\Delta) = \varphi_i(k \oplus \Delta)$ is δ_2-AXU for $i = 1, 4$, for each pair $(\mathbf{t}, \mathbf{t}')$ with $\mathbf{t} = (\Delta, LR, ST)$ and $\mathbf{t}' = (\Delta', L'R', S'T')$ we have

$$\begin{aligned}
&\Pr[x_1(\mathbf{t}) = x_1(\mathbf{t}') \text{ or } x_4(\mathbf{t}) = x_4(\mathbf{t}')]\\
=&\Pr[\varphi_1(k \oplus \Delta) \oplus R = \varphi_1(k \oplus \Delta') \oplus R'\\
&\quad \text{or } \varphi_4(k \oplus \Delta) \oplus S = \varphi_4(k \oplus \Delta') \oplus S'] \le 2\delta_2.
\end{aligned}$$

As we have at most $\binom{q_e}{2} \le \frac{q_e^2}{2}$ choices for $(\mathbf{t}, \mathbf{t}')$ it holds $\Pr[\text{(B-2)}] \le \delta_2 q_e^2$.

For (B-3), since $H_k(\Delta,\Delta') = \varphi_1(k\oplus\Delta)\oplus\varphi_4(k\oplus\Delta')$ is δ_3-uniform, for each pair $(\mathbf{t},\mathbf{t}')$ we have

$$\begin{aligned}&\Pr[x_1(\mathbf{t}) = x_4(\mathbf{t}')]\\ =&\Pr[\varphi_1(k\oplus\Delta)\oplus\varphi_4(k\oplus\Delta') = R\oplus S'] \le \delta_3.\end{aligned}$$

Summing over the q_e^2 choices of $(\mathbf{t},\mathbf{t}')$ yields $\Pr[\text{(B-3)}] \le \delta_3 q_e^2$.

For (B-4), consider a pair $(\mathbf{t},\mathbf{t}')$. Wlog assume that $\mathbf{t}'$ comes after $\mathbf{t}$. If $\mathbf{t}'$ was forward $\mathsf{RK}[\mathsf{IC}_k](\Delta, L'R') \to S'T'$, then the obtained $S'T'$ is uniform in a set of size at least $N^2 - q_e$, and since $q_e \le N$ we have

$$\Pr_{\mathsf{IC}}[S' = L\oplus L'\oplus S] \le \frac{N}{N^2-q_e} \le \frac{1}{N-1} \le \frac{2}{N}.$$

Similarly, $\Pr_{\mathsf{IC}}[T' = R\oplus R'\oplus T] \le \frac{2}{N}$. If $\mathbf{t}'$ was backward $\mathsf{RK}[\mathsf{IC}_k]^{-1}(\Delta, S'T') \to L'R'$, then similarly

$$\Pr_{\mathsf{IC}}[L' = L\oplus S\oplus S'] \le \frac{2}{N},\ \Pr_{\mathsf{IC}}[R' = R\oplus T\oplus T'] \le \frac{2}{N}.$$

Therefore, for each of the $\binom{q_e}{2} \le \frac{q_e^2}{2}$ pairs $(\mathbf{t},\mathbf{t}')$, (B-4) is fulfilled with probability at most $4/N$. Thus $\Pr[\text{(B-4)}] \le \frac{2q_e^2}{N}$.

Finally consider (B-5). Fix a query $\mathbf{t} = (\Delta, LR, ST)$. For $k \in \{0,1\}^n$, denote by $\mathcal{R}_1$ the set of possible values of $w_0(k_\Delta)\oplus w_2(k_\Delta)$, and by $\mathcal{R}_2$ the set of values of $w_1(k_\Delta)\oplus w_3(k_\Delta)$. If $\mathbf{t}$ was forward, then the obtained ST is uniform in $\ge N^2 - q_e$ values, and (as argued) $\Pr_{\mathsf{IC}}[L\oplus S = v] \le \frac{2}{N}$ for any fixed value $v \in \mathcal{R}_1$ and $\Pr_{\mathsf{IC}}[R\oplus T = v'] \le \frac{2}{N}$ for any $v' \in \mathcal{R}_2$. Therefore,

$$\begin{aligned}&\Pr_{\mathsf{IC}}[L\oplus w_0(k_\Delta) = S\oplus w_2(k_\Delta)]\\ =&\sum_{v\in\mathcal{R}_1}\Pr_{\mathsf{IC}}[L\oplus S = v]\cdot\Pr_k[w_0(k_\Delta)\oplus w_2(k_\Delta) = v]\\ \le&\frac{2}{N}\cdot\underbrace{\sum_{v\in\mathcal{R}_1}\Pr_k[w_0(k_\Delta)\oplus w_2(k_\Delta) = v]}_{=1} \le \frac{2}{N}.\end{aligned}$$

Similarly, $\Pr_{\mathsf{IC}}[R\oplus w_1(k_\Delta) = T\oplus w_3(k_\Delta)] \le \frac{2}{N}$. When $\mathbf{t}$ was backward, LR is uniform, and similar bounds hold. Taking a union bound for the q_e queries gives $\Pr[\text{(B-5)}] \le \frac{4q_e}{N}$. Summing over the above yields

$$\Pr[T_{id}\in\mathcal{T}_{bad}] \le 2\delta_1 q_e q_f + (\delta_2+\delta_3)q_e^2 + \frac{2q_e^2+4q_e}{N}. \quad (10)$$

3) **Ratio $\Pr_{re}(\tau)/\Pr_{id}(\tau)$ for Good τ:** Fix a good transcript τ. As per our remark before, we define the bad predicate $\mathsf{B}(P)$ in paragraph III-B3a. Then, it's easy to see

$$\begin{aligned}\Pr_{re}(\tau) &= \Pr_P\left[\mathsf{RK}[\mathsf{KAFw}_k^{P,(w,\gamma)}] \vdash \mathcal{Q}_E \wedge P \vdash \mathcal{Q}_P\right]\\ &\ge \Pr_P\left[\mathsf{RK}[\mathsf{KAFw}_k^{P,(w,\gamma)}] \vdash \mathcal{Q}_E \wedge P \vdash \mathcal{Q}_P \wedge \neg\mathsf{B}(P)\right]\\ &\ge \mathsf{p}\cdot\Big(1-\Pr_P[\mathsf{B}(P)\mid P\vdash\mathcal{Q}_P]\Big)\cdot\Pr_P[P\vdash\mathcal{Q}_P], \quad (11)\end{aligned}$$

where

$$\mathsf{p} = \Pr_P\left[\mathsf{RK}[\mathsf{KAFw}_k^{P,(w,\gamma)}] \vdash \mathcal{Q}_E \mid P\vdash\mathcal{Q}_P\wedge\neg\mathsf{B}(P)\right].$$

We next argue

$$\mathsf{p} \ge \frac{1}{N^{2q_e}} \quad (12)$$

in paragraphs III-B3b and III-B3c. Gathering this and Eq. (11) yields

$$\Pr_{re}(\tau) \ge \frac{\Pr_P[P\vdash\mathcal{Q}_P]}{N^{2q_e}}\Big(1-\Pr_P[\mathsf{B}(P)\mid P\vdash\mathcal{Q}_P]\Big), \quad (13)$$

which allows us to conclude in paragraph III-B3d.

a) The Bad Predicate $\mathsf{B}(P)$: For any $P \vdash \mathcal{Q}_P$, the predicate $\mathsf{B}(P)$ holds, if any of the following is fulfilled:

- (C-1) $\exists \mathbf{t},\mathbf{t}' \in \mathcal{Q}_E : x_1(\mathbf{t}) \ne x_1(\mathbf{t}')$, yet either $x_2(\mathbf{t},P) = x_2(\mathbf{t}',P)$ or $y_3(\mathbf{t},P) = y_3(\mathbf{t}',P)$.
- (C-2) $\exists \mathbf{t},\mathbf{t}' \in \mathcal{Q}_E$ (could be $\mathbf{t}=\mathbf{t}'$):
  - $x_2(\mathbf{t},P) \in \mathcal{X}(\tau)$ or $y_3(\mathbf{t},P)\in\mathcal{Y}(\tau)$, or
  - $x_2(\mathbf{t},P) = x_1(\mathbf{t}')$ or $x_2(\mathbf{t},P) = x_4(\mathbf{t}')$, or
  - $y_3(\mathbf{t},P) = y_1(\mathbf{t}',P)$ or $y_3(\mathbf{t},P) = y_4(\mathbf{t}',P)$.
- (C-3) $\exists \mathbf{t},\mathbf{t}' \in \mathcal{Q}_E : x_4(\mathbf{t}) \ne x_4(\mathbf{t}')$, yet either $x_3(\mathbf{t},P) = x_3(\mathbf{t}',P)$ or $y_2(\mathbf{t},P) = y_2(\mathbf{t}',P)$.
- (C-4) $\exists \mathbf{t},\mathbf{t}' \in \mathcal{Q}_E$ (could be $\mathbf{t}=\mathbf{t}'$):
  - $x_3(\mathbf{t},P)\in\mathcal{X}(\tau)$ or $y_2(\mathbf{t},P)\in\mathcal{Y}(\tau)$, or
  - $x_3(\mathbf{t},P) \in \{x_1(\mathbf{t}'), x_2(\mathbf{t}',P), x_4(\mathbf{t}')\}$, or
  - $y_2(\mathbf{t},P) \in \{y_1(\mathbf{t}',P), y_3(\mathbf{t}',P), y_4(\mathbf{t}',P)\}$.

Remark. As per our discussion before, collisions in the $2q_e$ values in Eq. (8) and in the $2q_e$ values in Eq. (9) are captured by (C-1) and (C-3) resp. Moreover, there should be no "conflict" between these $4q_e$ values and the inputs/outputs in 1st and 4th rounds, as captured by (C-2) and (C-4). This is crucial, as the values of the forms $P(x_1(\mathbf{t}))$ and $P(x_4(\mathbf{t}))$ will be used for bounding $\Pr[\mathsf{B}(P)]$, and it's unclear how this affects their distribution. Finally, note that $x_2(\mathbf{t},P)$ and $y_3(\mathbf{t},P)$ depends on the same random value $P(x_1(\mathbf{t}))$ (and could be analyzed at the same time), while $x_3(\mathbf{t},P)$ and $y_2(\mathbf{t},P)$ depends on $P(x_4(\mathbf{t}))$: this clarifies the order of the above bad conditions.

We now analyze $\Pr[\mathsf{B}(P)]$. Let $\mathbf{t} = (\Delta, LR, ST)$. Consider (C-1) first. For each pair $(\mathbf{t},\mathbf{t}')$, the event $x_2(\mathbf{t},P) = x_2(\mathbf{t}',P)$ implies

$$\begin{aligned}&\gamma_2(k_\Delta)\oplus L\oplus w_0(k_\Delta)\oplus P(x_1(\mathbf{t}))\\ =&\gamma_2(k_{\Delta'})\oplus L\oplus w_0(k_{\Delta'})\oplus P(x_1(\mathbf{t}')). \quad (14)\end{aligned}$$

Define a set of function values $\mathcal{S} = \{P(x_i(\mathbf{t}')) \mid \mathbf{t}' \in \mathcal{Q}_E, i = 1,4, x_i(\mathbf{t}') \ne x_1(\mathbf{t})\}$. Then $|\mathcal{S}| \le 2q_e$, and $P(x_1(\mathbf{t}')) \in \mathcal{S}$ since $x_1(\mathbf{t}) \ne x_1(\mathbf{t}')$. Furthermore, by $\neg$(B-1) we have $x_1(\mathbf{t}) \notin \mathcal{X}(\tau)$. Thus conditioned on $P\vdash\mathcal{Q}_P$ and further the function values in $\mathcal{S}$, $P(x_1(\mathbf{t}))$ is uniform in a set of size *at least* $N - q_f - 2q_e$. This means the left hand side of Eq. (14) is random conditioned on the right hand side, thus $\Pr[x_2(\mathbf{t},P) = x_2(\mathbf{t}',P)] \le \frac{1}{N-q_f-2q_e}$. Similarly, $\Pr[y_3(\mathbf{t},P) = y_3(\mathbf{t}',P)] \le \frac{1}{N-q_f-2q_e}$. As we have $\binom{q_e}{2} \le \frac{q_e^2}{2}$ pairs $(\mathbf{t},\mathbf{t}')$, it holds $\Pr[\text{(C-1)}] \le \frac{q_e^2}{N-q_f-2q_e}$. A symmetrical analysis yields $\Pr[\text{(C-3)}] \le \binom{q_e}{2}\cdot\frac{2}{N-q_f-2q_e} \le \frac{q_e^2}{N-q_f-2q_e}$.

We next consider (C-2). As argued, for any $\mathbf{t}$, $X(\mathbf{t},P)$ is uniform in $\ge N - q_f - 2q_e$ possibilities. On the other hand,

all the values in $\mathcal{X}(\tau)$ are fixed by τ and thus independent from the function values of P. Therefore,

$$\Pr[x_2(\mathbf{t},P) \in \mathcal{X}(\tau)] = \Pr[\gamma_2(k \oplus \Delta) \oplus X(\mathbf{t},P) \in \mathcal{X}(\tau)] \leq \frac{q_f}{N - q_f - 2q_e}. \quad (15)$$

Similarly,

$$\Pr[\exists \mathbf{t}' : x_2(\mathbf{t},P) = x_1(\mathbf{t}') \text{ or } x_2(\mathbf{t},P) = x_4(\mathbf{t}')] \leq \frac{2q_e}{N - q_f - 2q_e}, \quad (16)$$

$$\Pr[y_3(\mathbf{t},P) \in \mathcal{Y}(\tau)] \leq \frac{q_f}{N - q_f - 2q_e}. \quad (17)$$

Now consider $\Pr[\exists \mathbf{t}' : y_3(\mathbf{t},P) = y_4(\mathbf{t}',P)]$. If this event happens, then

$$L \oplus w_0(k_\Delta) \oplus P(x_1(\mathbf{t})) \oplus w_2(k_\Delta) \oplus S = P(x_4(\mathbf{t}')).$$

By ¬(B-3) we have $x_1(\mathbf{t}) \neq x_4(\mathbf{t}')$, so $P(x_4(\mathbf{t}'))$ is random conditioned on the left hand side. Therefore,

$$\Pr[\exists \mathbf{t}' : y_3(\mathbf{t},P) = y_4(\mathbf{t}',P)] \leq \frac{q_e}{N - q_f - 2q_e}. \quad (18)$$

Finally consider $\Pr[\exists \mathbf{t}' : y_3(\mathbf{t},P) = y_1(\mathbf{t}',P)]$. If this event happens, then for $\mathbf{t}$ there exists $\mathbf{t}' \in \mathcal{Q}_E$ such that

$$L \oplus w_0(k_\Delta) \oplus P(x_1(\mathbf{t})) \oplus w_2(k_\Delta) \oplus S = P(x_1(\mathbf{t}')). \quad (19)$$

We distinguish two cases:

(i) Case 1: $x_1(\mathbf{t}) \neq x_1(\mathbf{t}')$. Then $P(x_1(\mathbf{t}'))$ is random conditioned on $P(x_1(\mathbf{t}))$, and $\Pr[\text{Eq. (19)}] \leq \frac{1}{N-q_f-2q_e}$;

(ii) Case 2: $x_1(\mathbf{t}) = x_1(\mathbf{t}')$. Then for this tuple $\mathbf{t}$ we have $L \oplus w_0(k_\Delta) = w_2(k_\Delta) \oplus S$, which contradicts ¬(B-5) (Definition 2).

As we have q_e choices for $\mathbf{t}'$ we obtain

$$\Pr[\exists \mathbf{t}' : y_3(\mathbf{t},P) = y_1(\mathbf{t}',P)] \leq \frac{q_e}{N - q_f - 2q_e}. \quad (20)$$

Summing over (15), (16), (17), (18), and (20), and taking union bound on the q_e choices of $\mathbf{t}$, we obtain

$$\Pr[\text{(C-2)}] \leq \frac{q_e(q_f + 2q_e + q_f + q_e + q_e)}{N - q_f - 2q_e} \leq \frac{2q_e(q_f + 2q_e)}{N - q_f - 2q_e}. \quad (21)$$

The analysis for (C-4) is similar by symmetry: for each $\mathbf{t} = (\Delta, LR, ST) \in \mathcal{Q}_E$, $P(x_4(\mathbf{t}))$ and further $Y(\mathbf{t},P) = T \oplus w_3(k_\Delta) \oplus P(x_4(\mathbf{t}))$, $x_3(\mathbf{t},P)$, and $y_2(\mathbf{t},P)$ are uniform. By this, for $\mathbf{t}$,

$$\Pr[x_3(\mathbf{t},P) \in \mathcal{X}(\tau) \text{ or } y_2(\mathbf{t},P) \in \mathcal{Y}(\tau)] \leq \frac{2q_f}{N - q_f - 2q_e}, \quad (22)$$

$$\Pr[\exists \mathbf{t}' : x_3(\mathbf{t},P) = x_1(\mathbf{t}') \text{ or } x_3(\mathbf{t},P) = x_4(\mathbf{t}')] \leq \frac{2q_e}{N - q_f - 2q_e}, \quad (23)$$

Now consider $\Pr[\exists \mathbf{t}' : x_3(\mathbf{t},P) = x_2(\mathbf{t}',P)]$. If it happens, then for $\mathbf{t}$ there exists $\mathbf{t}' = (\Delta', L'R', S'T')$ such that

$$\gamma_3(k_\Delta) \oplus T \oplus w_3(k_\Delta) \oplus P(x_4(\mathbf{t})) = \gamma_2(k_{\Delta'}) \oplus L' \oplus w_0(k_{\Delta'}) \oplus P(x_1(\mathbf{t}')). \quad (24)$$

By ¬(B-3) we have $x_4(\mathbf{t}) \neq x_1(\mathbf{t}')$, so the right hand side of (24) is random conditioned on $P(x_4(\mathbf{t}))$. Thus we have $\Pr[\text{Eq. (24)}] \leq \frac{1}{N-q_f-2q_e}$, and further

$$\Pr[\exists \mathbf{t}' : x_3(\mathbf{t},P) = x_2(\mathbf{t}',P)] \leq \frac{q_e}{N - q_f - 2q_e}. \quad (25)$$

By similar arguments, it can be shown

$$\Pr[\exists \mathbf{t}' : y_2(\mathbf{t},P) = y_1(\mathbf{t}') \text{ or } y_2(\mathbf{t},P) = y_3(\mathbf{t}',P)] \leq \frac{2q_e}{N - q_f - 2q_e}. \quad (26)$$

Finally consider $\Pr[\exists \mathbf{t}' : y_2(\mathbf{t},P) = y_4(\mathbf{t}',P)]$. For $\mathbf{t}$ if it happens then there exists $\mathbf{t}' = (\Delta', L'R', S'T')$ such that

$$R \oplus w_1(k_\Delta) \oplus T \oplus w_3(k_\Delta) \oplus P(x_4(\mathbf{t})) = P(x_4(\mathbf{t}')). \quad (27)$$

If $x_4(\mathbf{t}) \neq x_4(\mathbf{t}')$ then the right hand side of (27) is random conditioned on $P(x_4(\mathbf{t}))$ and thus $\Pr[\text{Eq. (27)}] \leq \frac{1}{N-q_f-2q_e}$; otherwise i.e. $x_4(\mathbf{t}) = x_4(\mathbf{t}')$, then it implies $R \oplus w_1(k_\Delta) = T \oplus w_3(k_\Delta)$, contradicting ¬(B-5). So

$$\Pr[\exists \mathbf{t}' : y_2(\mathbf{t},P) = y_4(\mathbf{t}',P)] \leq \frac{q_e}{N - q_f - 2q_e}. \quad (28)$$

Summing over (22), (23), (25), (26), and (28), and taking union over q_e yield

$$\Pr[\text{(C-4)}] \leq \frac{q_e(2q_f + 2q_e + q_e + 2q_e + q_e)}{N - q_f - 2q_e} \leq \frac{2q_e(q_f + 3q_e)}{N - q_f - 2q_e}.$$

Finally, summing over the four conditions yields

$$\Pr[P \xleftarrow{\$} \mathcal{P}(n) : \mathsf{B}(P) \mid P \vdash \mathcal{Q}_P] \leq \frac{4q_eq_f + 12q_e^2}{N - q_f - 2q_e}. \quad (29)$$

b) The Probability p: For any $P^* \vdash \mathcal{Q}_P$ such that $\mathsf{B}(P^*)$ doesn't hold, we define an "extended transcript"

$$\mathcal{Q}^{out}(P^*) = \left\{\left(x_1(\mathbf{t}), y_1(\mathbf{t},P^*)\right), \left(x_4(\mathbf{t}), y_4(\mathbf{t},P^*)\right)\right\}_{\mathbf{t} \in \mathcal{Q}_E}.$$

We further define $\mathcal{T}^{out}$ as the set of all such extended transcripts, i.e.,

$$\mathcal{T}^{out} = \left\{\mathcal{Q}^{out}(P)\right\}_{P \in \mathcal{P}(n)},$$

and a set of "good" extended transcripts based on permutations that don't fulfill the bad predicate, i.e.,

$$\mathcal{T}^{out}_{good} = \left\{\mathcal{Q}^{out}(P^*)\right\}_{P^* \vdash \mathcal{Q}_P, \neg\mathsf{B}(P^*)}.$$

Next, for any instance $\mathcal{Q}^{out} \in \mathcal{T}^{out}$, we define another extended transcript $\mathcal{Q}^{mid}(\mathcal{Q}^{out})$. Formally, let P^* be a permutation such that $\mathcal{Q}^{out}(P^*) = \mathcal{Q}^{out}$, then

$$\mathcal{Q}^{mid}(\mathcal{Q}^{out}) = \left\{\left(x_2(\mathbf{t}), y_2(\mathbf{t},P^*)\right), \left(x_3(\mathbf{t}), y_3(\mathbf{t},P^*)\right)\right\}_{\mathbf{t} \in \mathcal{Q}_E}.$$

It's easy to see that such a choice of P^* may not be unique, but for all P^* with $\mathcal{Q}^{out}(P^*) = \mathcal{Q}^{out}$, the transcripts $\mathcal{Q}^{mid}(\mathcal{Q}^{out})$ defined as above are the same since the condition $\mathcal{Q}^{out}(P^*) = \mathcal{Q}^{out}$ ensures that P^* is consistent with the input-output relations defined in $\mathcal{Q}^{out}$ which will fully characterize $\mathcal{Q}^{mid}(\mathcal{Q}^{out})$.

With these, by the definitions of KAFw we have

$$\begin{aligned}\mathsf{p} &= \sum_{\mathcal{Q}^{out}\in\mathcal{T}^{out}} \Pr[P\vdash\mathcal{Q}^{out} \mid P\vdash\mathcal{Q}_P\wedge\neg\mathsf{B}(P)] \\ &\qquad\cdot\Pr[P\vdash\mathcal{Q}^{mid}(\mathcal{Q}^{out}) \mid P\vdash(\mathcal{Q}^{out}\cup\mathcal{Q}_P)\wedge\neg\mathsf{B}(P)] \\ &\geq \underbrace{\sum_{\mathcal{Q}^{out}\in\mathcal{T}^{out}_{good}} \Pr[P\vdash\mathcal{Q}^{out} \mid P\vdash\mathcal{Q}_P\wedge\neg\mathsf{B}(P)]}_{=1} \\ &\qquad\cdot\Pr[P\vdash\mathcal{Q}^{mid}(\mathcal{Q}^{out}) \mid P\vdash(\mathcal{Q}^{out}\cup\mathcal{Q}_P)\wedge\neg\mathsf{B}(P)]\end{aligned}$$

For any $\mathcal{Q}^{out}\in\mathcal{T}^{out}_{good}$, the conditions ¬(C-2) and ¬(C-4) ensure that

$$\begin{aligned}&\{x \mid \exists y:(x,y)\in\mathcal{Q}^{mid}(\mathcal{Q}^{out})\} \\ &\qquad\bigcap\{x' \mid \exists y':(x',y')\in(\mathcal{Q}^{out}\cup\mathcal{Q}_P)\}=\emptyset, \\ &\{y \mid \exists x:(x,y)\in\mathcal{Q}^{mid}(\mathcal{Q}^{out})\} \\ &\qquad\bigcap\{y' \mid \exists x':(x',y')\in(\mathcal{Q}^{out}\cup\mathcal{Q}_P)\}=\emptyset.\end{aligned}$$

Thus

$$\Pr[P\vdash\mathcal{Q}^{mid}(\mathcal{Q}^{out}) \mid P\vdash(\mathcal{Q}^{out}\cup\mathcal{Q}_P)\wedge\neg\mathsf{B}(P)]\geq\frac{1}{N^{|\mathcal{Q}^{mid}(\mathcal{Q}^{out})|}}.$$

In the next paragraph, we show $|\mathcal{Q}^{mid}(\mathcal{Q}^{out})|=2q_e$ to complete the proof of Eq. (12) and further (13).

c) $2q_e$ Relations for Good P: By the definitions, for any $\mathcal{Q}^{out}\in\mathcal{T}^{out}_{good}$, there exists $P\vdash\mathcal{Q}_P$ such that $\mathsf{B}(P)$ doesn't hold, and $\mathcal{Q}^{out}(P)=\mathcal{Q}^{out}$. Now we can write

$$\mathcal{Q}^{mid}(\mathcal{Q}^{out})=\{(x_2(\mathbf{t},P),y_2(\mathbf{t},P)),(x_3(\mathbf{t},P),y_3(\mathbf{t},P))\}.$$

We show $\left|\{x_2(\mathbf{t},P),x_3(\mathbf{t},P)\mid\mathbf{t}\in\mathcal{Q}_E\}\right|=2q_e$ and $\left|\{y_2(\mathbf{t},P),y_3(\mathbf{t},P)\mid\mathbf{t}\in\mathcal{Q}_E\}\right|=2q_e$. First, by $\neg\mathsf{B}(P)$ (i.e., ¬(C-4)), for any pair $(\mathbf{t},\mathbf{t}')$, it holds $x_2(\mathbf{t},P)\neq x_3(\mathbf{t}',P)$ and $y_2(\mathbf{t},P)\neq y_3(\mathbf{t}',P)$. It remains to show

- $x_2(\mathbf{t},P)\neq x_2(\mathbf{t}',P)$, $y_2(\mathbf{t},P)\neq y_2(\mathbf{t}',P)$, and
- $x_3(\mathbf{t},P)\neq x_3(\mathbf{t}',P)$, $y_3(\mathbf{t},P)\neq y_3(\mathbf{t}',P)$.

Consider $(x_2(\mathbf{t},P),x_2(\mathbf{t}',P))$ and $(y_3(\mathbf{t},P),y_3(\mathbf{t}',P))$ first: their proof flows are similar. In detail, let $\mathbf{t}=(\Delta,LR,ST)$ and $\mathbf{t}'=(\Delta',L'R',S'T')$, then we exclude possibility of $x_2(\mathbf{t},P)=x_2(\mathbf{t}',P)$ or $y_3(\mathbf{t},P)=y_3(\mathbf{t}',P)$ for each case:

(i) Case 1: $\Delta\neq\Delta'$. Then $x_1(\mathbf{t},P)\neq x_1(\mathbf{t}',P)$ by ¬(B-2) (see Definition 2), and further $x_2(\mathbf{t},P)\neq x_2(\mathbf{t}',P)$ and $y_3(\mathbf{t},P)\neq y_3(\mathbf{t}',P)$ by ¬(C-1);

(ii) Case 2: $\Delta=\Delta'$, yet $R\neq R'$. Then still $x_1(\mathbf{t},P)\neq x_1(\mathbf{t}',P)$, thus further $x_2(\mathbf{t},P)\neq x_2(\mathbf{t}',P)$ and $y_3(\mathbf{t},P)\neq y_3(\mathbf{t}',P)$;

(iii) Case 3: $\Delta=\Delta'$ and $R=R'$. Then it has to be $L\neq L'$ since $\mathbf{t}'\neq\mathbf{t}'$. Now:

- On one hand, $L\neq L'$ immediately implies $x_2(\mathbf{t},P)=L\oplus w_0(k_\Delta)\oplus y_1(\mathbf{t},P)\oplus\gamma_2(k_\Delta)$ and $x_2(\mathbf{t}',P)=L'\oplus w_0(k_\Delta)\oplus y_1(\mathbf{t},P)\oplus\gamma_2(k_\Delta)$ are distinct;
- On the other hand, $\Delta=\Delta'$ and $R=R'$ imply $X(\mathbf{t},P)\oplus X(\mathbf{t}',P)=L\oplus L'$. By this, $y_3(\mathbf{t},P)=X(\mathbf{t},P)\oplus w_2(k_\Delta)\oplus S=y_3(\mathbf{t}',P)=X(\mathbf{t}',P)\oplus w_2(k_\Delta)\oplus S'$ would imply $L\oplus L'=S\oplus S'$, contradicting ¬(B-4).

By the above, it does hold $x_2(\mathbf{t},P)\neq x_2(\mathbf{t}',P)$ and $y_3(\mathbf{t},P)\neq y_3(\mathbf{t}',P)$ for any $\mathbf{t}'\neq\mathbf{t}'$. A symmetrical argument could establish $x_3(\mathbf{t},P)\neq x_3(\mathbf{t}',P)$ and $y_2(\mathbf{t},P)\neq y_2(\mathbf{t}',P)$ for any $\mathbf{t}'\neq\mathbf{t}'$.

d) The Final Counting: By the above discussion and (13) and (29), when $q_f+2q_e\leq N/2$, for any $\tau\in\mathcal{T}_{good}$ we have

$$\begin{aligned}\frac{\Pr_{re}(\tau)}{\Pr_{id}(\tau)}&\geq\frac{\Pr_P[P\vdash\mathcal{Q}_P]}{N^{2q_e}}\left(1-\Pr_P[\mathsf{B}(P)]\right)\Big/\frac{\Pr_P[P\vdash\mathcal{Q}_P]}{(N^2-q_e)^{q_e}} \\ &\geq\left(1-\frac{4q_eq_f+12q_e^2}{N-q_f-2q_e}\right)\left(\frac{N^2-q_e}{N^2}\right)^{q_e} \\ &\geq\left(1-\frac{8q_eq_f+24q_e^2}{N}\right)\left(1-\frac{q_e^2}{N^2}\right) \\ &\geq 1-\frac{8q_eq_f+25q_e^2}{N}.\end{aligned}$$

Gathering this, (10), and Lemma 1 yields Theorem 1.

C. When f=F is a Random Function

With a good key-schedule specified in Definition 1, the $\oplus$-RKA security claim still holds when we use a random function F for f. For the proof, we make some moderate modifications to the previous proof for $\mathsf{KAFw}^{P,(w,\gamma)}$. First, (of course) the helper functions $y_1(\mathbf{t},P),X(\mathbf{t},P),\ldots$ here are defined on F instead of P, i.e. $y_1(\mathbf{t},F),X(\mathbf{t},F),\ldots$

Then, note that since F is a random function, for the to-be-derived $2q_e$ equalities

$$\left\{F(x_2(\mathbf{t},F))=y_2(\mathbf{t},F),F(x_3(\mathbf{t},F))=y_3(\mathbf{t},F)\mid\mathbf{t}\in\mathcal{Q}_E\right\},$$

collisions within the image set $\{y_2(\mathbf{t},F),y_3(\mathbf{t},F)\mid\mathbf{t}\in\mathcal{Q}_E\}$ would not be troublesome. Therefore, the main task is to drop definitions and arguments concerning these image values.

In detail, we recall that in the definition of bad transcripts (Definition 2),

- the condition (B-4) is only used for proving $\left|\{y_2(\mathbf{t},F)\mid\mathbf{t}\in\mathcal{Q}_E\}\right|=\left|\{y_3(\mathbf{t},F)\mid\mathbf{t}\in\mathcal{Q}_E\}\right|=q_e$ in the subsequent analysis, cf. the Case 3 in page 11, and
- (B-5) is only used for bounding $\Pr[\exists\mathbf{t},\mathbf{t}':y_2(\mathbf{t},F)=y_4(\mathbf{t}',F)]$ and $\Pr[\exists\mathbf{t},\mathbf{t}':y_3(\mathbf{t},F)=y_1(\mathbf{t}',F)]$, cf. Eq. (19) and (27) in page 10.

So both (B-4) and (B-5) could be dropped. On the other hand, (B-1), (B-2), and (B-3) and their probabilities remain unchanged. Subtracting the corresponding terms from (10) yields the following bound for 4-round $\mathsf{KAFw}^{F,(w,\gamma)}$

$$\Pr[T_{id}\in\mathcal{T}_{bad}]\leq 2\delta_1q_eq_f+(\delta_2+\delta_3)q_e^2. \tag{30}$$

We then modify the definition of $\mathsf{B}(P)$ into $\mathsf{B}(F)$. We remark that for any value x such that $F(x)$ remains unknown, the function value $F(x)$ is uniform in $\{0,1\}^n$, which slightly deviates from the permutation case. Then, following the idea as before, we make the following modifications:

(i) Dropping $y_3(\mathbf{t},F)=y_3(\mathbf{t}',F)$ in (C-1). This decreases $\Pr[\text{(C-1)}]$ to $\frac{q_e^2}{2N}$ (with the above remark in mind);

(ii) Dropping the condition(s) $\exists\mathbf{t},\mathbf{t}':y_3(\mathbf{t},F)\in\mathcal{Y}(\tau)\vee y_3(\mathbf{t},F)=y_1(\mathbf{t}',F)\vee y_3(\mathbf{t},F)=y_4(\mathbf{t}',F)$ in (C-2). This decreases $\Pr[\text{(C-2)}]$ to $\frac{q_e(q_f+2q_e)}{N}$;

(iii) Dropping $y_2(\mathbf{t}, F) = y_2(\mathbf{t}', F)$ in (C-3). This decreases $\Pr[\text{(C-3)}]$ to $\frac{q_e^2}{2N}$;
(iv) Dropping the condition(s) $\exists \mathbf{t}, \mathbf{t}' : y_2(\mathbf{t}, F) \in \mathcal{Y}(\tau) \vee y_2(\mathbf{t}, F) = y_1(\mathbf{t}', F) \vee y_2(\mathbf{t}, F) = y_3(\mathbf{t}', F) \vee y_2(\mathbf{t}, F) = y_4(\mathbf{t}', F)$ in (C-4). This decreases $\Pr[\text{(C-2)}]$ to $\frac{q_e(q_f+3q_e)}{N}$.

In total we have

$$\Pr[F \xleftarrow{\$} \mathcal{F}(n) : \mathsf{B}(F) \mid F \vdash \mathcal{Q}_F] \leq \frac{2q_eq_f + 6q_e^2}{N}.$$

Finally,

$$\Pr[F \xleftarrow{\$} \mathcal{F}(n) : \mathsf{RK}[\mathsf{KAFw}_k^{F,(w,\gamma)}] \vdash \mathcal{Q}_E \mid F \vdash \mathcal{Q}_F \wedge \neg \mathsf{B}(F)]$$
$$\geq \Pr_F\big[\forall \mathbf{t} \in \mathcal{Q}_E : F(x_2(\mathbf{t}, F)) = y_2(\mathbf{t}, F) \wedge F(x_3(\mathbf{t}, F)) = y_3(\mathbf{t}, F)\big] = \frac{1}{N^{2q_e}}.$$

Therefore,

$$\frac{\Pr_{re}(\tau)}{\Pr_{id}(\tau)} \geq 1 - \frac{2q_eq_f + 6q_e^2}{N} - \frac{q_e^2}{N^2}. \tag{31}$$

Gathering (30) and (31) yields

Theorem 2 *For the 4-round, random function-based $\mathsf{KAFw}^{F,(w,\gamma)}$ cipher with a good key-schedule (w, γ) as specified in Definition 1, it holds*

$$\mathbf{Adv}^{\oplus\text{-rka}}_{\mathsf{KAFw}_k^{F,(w,\gamma)}}(q_f, q_e) \leq 2\delta_1 q_e q_f + (\delta_2 + \delta_3)q_e^2 + \frac{2q_eq_f + 7q_e^2}{N}.$$

IV. KAFw with Affine Key-Schedules

This section provides a comprehensive analysis of KAFw with affine key-schedules. First, in section IV-A, we describe attacks against 4- and 5-round KAFw. These attacks can be easily adapted to KAF (of more general interest for attacks). Then, we prove security for 6-round $\mathsf{KAFw}^{P,(w,\gamma)}$ and $\mathsf{KAFw}^{F,(w,\gamma)}$ in sections IV-B and IV-C respectively.

A. Insecurity for 4 and 5 Rounds

We stress that, for attacks we consider KAFw built upon *any* round-functions, and thus notations used in this subsection have slightly different meanings than those from section II. In detail, let (w, γ) be a t-round key-schedule, and $\overrightarrow{f} = (f_1, \ldots, f_t)$ be any t functions. Then we define a t-round KAFw variant

$$\mathsf{KAFw}_k^{\overrightarrow{f},(w,\gamma)}(W) = wk_{out} \oplus \Psi^{f_t}_{\gamma_t(k)} \circ \ldots \circ \Psi^{f_1}_{\gamma_1(k)}\big(wk_{in} \oplus W\big),$$

where $wk_{in} = w_0(k)\|w_1(k)$ and $wk_{out} = w_2(k)\|w_3(k)$. And for any distinguisher D, we define

$$\mathbf{Adv}^{\oplus\text{-rka}}_{\mathsf{KAFw}_k^{\overrightarrow{f},(w,\gamma)}}(D) = \Big|\Pr_{\mathsf{IC},k}[D^{\mathsf{RK}[\mathsf{IC}_k],\overrightarrow{f}} = 1] - \Pr_k[D^{\mathsf{RK}[\mathsf{KAFw}_k^{\overrightarrow{f},(w,\gamma)}],\overrightarrow{f}} = 1]\Big|.$$

With these notations, subsubsections IV-A1 and IV-A2 below present negative results on 4 and 5 rounds respectively.

1) **Insecurity for 4 Rounds with Any Affine Key-Schedules***:* From a cryptanalytic point of view, note that for KAFw with affine key-schedules, we have 2-round related-key differential characteristics with probability 1: see Eq. (32) and (33) below. Concatenating them would yield a 4-round related-key boomerang distinguisher [25] that consumes only four related-key oracle queries. Formally, we have

Theorem 3 *There exists a $(0, 4)$-distinguisher D such that, for any 4 functions $\overrightarrow{f} = (f_1, f_2, f_3, f_4)$ and any 4-round affine key-schedule (w, γ) where w and γ are as defined in Eq. (5) and (6), it holds*

$$\mathbf{Adv}^{\oplus\text{-rka}}_{\mathsf{KAFw}_k^{\overrightarrow{f},(w,\gamma)}}(D) \geq 1 - \frac{1}{N^2 - 1}.$$

Proof: We denote generically $(\mathsf{RK}[\mathsf{E}_k], \overrightarrow{f})$ the oracles to which the adversary has access, where E is either $\mathsf{KAFw}^{\overrightarrow{f},(w,\gamma)}$ or IC. The distinguisher D proceeds as:

(1) choose arbitrary values $L, R, \Delta \in \{0,1\}^n$, $\Delta \neq 0$, let $\nabla_1 = (M_0^{(w)} \oplus M_2) \cdot \Delta$, $\nabla_2 = (M_1^{(w)} \oplus M_1) \cdot \Delta$, $\nabla_3 = (M_4 \oplus M_2^{(w)}) \cdot \Delta$, and $\nabla_4 = (M_3 \oplus M_3^{(w)}) \cdot \Delta$. Make two queries $\mathsf{RK}[\mathsf{E}_k](0, L\|R) \to S\|T$ and $\mathsf{RK}[\mathsf{E}_k](\Delta, L \oplus \nabla_1\|R \oplus \nabla_2) \to S'\|T'$;
(2) make two decryption queries $\mathsf{RK}[\mathsf{E}_k]^{-1}(\Delta, S''\|T'') \to L''\|R''$ and $\mathsf{RK}[\mathsf{E}_k]^{-1}(0, S'''\|T''') \to L'''\|R'''$, for $S''\|T'' = S \oplus \nabla_3\|T \oplus \nabla_4$ and $S'''\|T''' = S' \oplus \nabla_3\|T' \oplus \nabla_4$;
(3) if $(L''\|R'') \oplus (L'''\|R''') = \nabla_1\|\nabla_2$ then output 1 to indicate E is $\mathsf{KAFw}^{\overrightarrow{f},(w,\gamma)}$, and otherwise 0: E is IC.

We show the output is always 1 when E is $\mathsf{KAFw}^{\overrightarrow{f},(w,\gamma)}$. It's not hard to see for any i and any $V, \Delta \in \{0,1\}^n$, it holds

$$\gamma_i(k) \oplus V = \gamma_i(k_\Delta) \oplus V \oplus M_i \cdot \Delta$$

for $k_\Delta = k \oplus \Delta$. By this, for any Δ, it holds

$$\Pr_{k,V,W}\big[\Psi^{f_i}_{\gamma_i(k)}(V\|W) \oplus \Psi^{f_i}_{\gamma_i(k)}(V \oplus M_{i+1} \cdot \Delta\|W \oplus M_i \cdot \Delta) = M_i \cdot \Delta\|M_{i+1} \cdot \Delta\big] = 1.$$

This is essentially a 1-round related-key differential with probability 1. To ease exposition, we follow the notation in [23] and denote this phenomena by

$$\Pr\Big(M_{i+1} \cdot \Delta\|M_i \cdot \Delta \xrightarrow[\Delta]{\Psi^{f_i}_{\gamma_i(k)}} M_i \cdot \Delta\|M_{i+1} \cdot \Delta\Big) = 1.$$

Concatenating two such differentials gives rise to two 2-round related-key differentials with probability 1 as follows

$$\Pr\Big(\nabla_1\|\nabla_2 \xrightarrow[\Delta]{\Psi^{f_2}_{\gamma_2(k)} \circ \Psi^{f_1}_{\gamma_1(k)} \circ \mathsf{XOR}_{wk_{in}}} M_2 \cdot \Delta\|M_1 \cdot \Delta\Big) = 1, \tag{32}$$

$$\Pr\Big(M_4 \cdot \Delta\|M_3 \cdot \Delta \xrightarrow[\Delta]{\mathsf{XOR}_{wk_{out}} \circ \Psi^{f_4}_{\gamma_4(k)} \circ \Psi^{f_3}_{\gamma_3(k)}} \nabla_3\|\nabla_4\Big) = 1, \tag{33}$$

where $wk_{in} = w_0(k)\|w_1(k)$, $wk_{out} = w_2(k)\|w_3(k)$, and $\mathsf{XOR}_{wk}(W) = wk \oplus W$.

Therefore, for the two forward queries, if we assume

$$\big(\Psi^{f_2}_{\gamma_2(k)} \circ \Psi^{f_1}_{\gamma_1(k)}\big)\big(wk_{in} \oplus (L\|R)\big) = X\|Y, \tag{34}$$

then by (32) it holds

$$\begin{aligned}&\big(\Psi^{f_2}_{\gamma_2(k_\Delta)} \circ \Psi^{f_1}_{\gamma_1(k_\Delta)}\big)(wk^{\Delta}_{in} \oplus (L \oplus \nabla_1 \| R \oplus \nabla_2))\\ =&X \oplus M_2 \cdot \Delta \| Y \oplus M_1 \cdot \Delta \end{aligned} \tag{35}$$

for $wk^{\Delta}_{in} = w_0(k_\Delta)\|w_1(k_\Delta)$. Eq. (34) and (35) also mean

$$\begin{aligned}&\big(\Psi^{f_4}_{\gamma_4(k)} \circ \Psi^{f_3}_{\gamma_3(k)}\big)^{-1}\big(wk_{out} \oplus (S\|T)\big) = X\|Y,\\ &\big(\Psi^{f_4}_{\gamma_4(k_\Delta)} \circ \Psi^{f_3}_{\gamma_3(k_\Delta)}\big)^{-1}\big(wk^{\Delta}_{out} \oplus (S'\|T')\big)\\ =&X \oplus M_2 \cdot \Delta \| Y \oplus M_1 \cdot \Delta,\end{aligned}$$

where $wk^{\Delta}_{out} = w_2(k_\Delta)\|w_3(k_\Delta)$, and S, T, S', T' are the values appeared during the attack. Consider the two backward queries, and assume that

$$\begin{aligned}X''\|Y'' &= \big(\Psi^{f_4}_{\gamma_4(k_\Delta)} \circ \Psi^{f_3}_{\gamma_3(k_\Delta)}\big)^{-1}\big(wk^{\Delta}_{out} \oplus (S''\|T'')\big),\\ X'''\|Y''' &= \big(\Psi^{f_4}_{\gamma_4(k)} \circ \Psi^{f_3}_{\gamma_3(k)}\big)^{-1}\big(wk_{out} \oplus (S'''\|T''')\big).\end{aligned}$$

By (33) we have

$$\begin{aligned}X''\|Y'' &= X \oplus M_4 \cdot \Delta \| Y \oplus M_3 \cdot \Delta,\\ X'''\|Y''' &= X \oplus M_2 \cdot \Delta \oplus M_4 \cdot \Delta \| Y \oplus M_1 \cdot \Delta \oplus M_3 \cdot \Delta,\end{aligned}$$

thus $(X''\|Y'') \oplus (X'''\|Y''') = M_2 \cdot \Delta \| M_1 \cdot \Delta$. By this and (32) it can be seen $(L''\|R'') \oplus (L'''\|R''') = \nabla_1\|\nabla_2$.

On the other hand, when interacting with $\mathsf{RK}[\mathsf{IC}_k]$, the last response $L'''\|R'''$ is uniform in $\{0,1\}^{2n}\backslash\{LR\}$. So $\Pr_{\mathsf{IC}}[(L''\|R'') \oplus (L'''\|R''') = (\nabla_1\|\nabla_2)] = \frac{1}{N^2-1}$, which is also the probability that the distinguisher outputs 1 in the ideal world. Thus the claimed bound. □

2) **(In)security for 5 Rounds***:* We first exhibit an attack with only one additional assumption on the key-schedule: it's easy to derive $\Delta \neq 0$ such that $M_1 \cdot \Delta = M_5 \cdot \Delta$. This is possible: e.g., if γ_1 and γ_5 are bit-permutations, then for $\Delta = 0\text{xFF}\ldots\text{FF}$ it holds $M_1 \cdot \Delta = M_5 \cdot \Delta = 0\text{xFF}\ldots\text{FF}$.

From a cryptanalytic point of view, the core trick is: in the boomerang attack setting, under some conditions, Feistel schemes allow a *Feistel boomerang switch* trick [24], which enables penetrating one more round. Applying this trick to the 4-round related-key boomerang mentioned before yields a 5-round related-key boomerang distinguisher. Formally,

Theorem 4 *There exists a $(0,4)$-distinguisher D such that, for any 5 functions $\overrightarrow{f} = (f_1, f_2, f_3, f_4, f_5)$ and any 5-round affine key-schedule (w, γ) where w and γ are as defined in Eq. (5) and (6) and satisfy that it's easy to derive $\Delta \neq 0$ such that $M_1 \cdot \Delta = M_5 \cdot \Delta$, it holds*

$$\mathbf{Adv}^{\oplus\text{-}rka}_{\mathsf{KAFw}^{\overrightarrow{f},(w,\gamma)}_k}(D) \geq 1 - \frac{1}{N^2-1}.$$

Proof: The distinguisher D proceeds as:

(1) derive a difference $\Delta \neq 0$ such that $M_1 \cdot \Delta = M_5 \cdot \Delta$;
(2) choose two arbitrary values $L, R \in \{0,1\}^n$, and let $\nabla_1 = (M_0^{(w)} \oplus M_2) \cdot \Delta$, $\nabla_2 = (M_1^{(w)} \oplus M_1) \cdot \Delta$, $\nabla_3 = (M_5 \oplus M_2^{(w)}) \cdot \Delta$, and $\nabla_4 = (M_4 \oplus M_3^{(w)}) \cdot \Delta$. Make two queries $\mathsf{RK}[\mathsf{E}_k](0, L\|R) \to S\|T$ and $\mathsf{RK}[\mathsf{E}_k](\Delta, L \oplus \nabla_1\|R \oplus \nabla_2) \to S'\|T'$;
(3) query $\mathsf{RK}[\mathsf{E}_k]^{-1}(\Delta, S \oplus \nabla_3\|T \oplus \nabla_4) \to L''\|R''$ and $\mathsf{RK}[\mathsf{E}_k]^{-1}(0, S' \oplus \nabla_3\|T' \oplus \nabla_4) \to L'''\|R'''$;
(4) if $(L''\|R'') \oplus (L'''\|R''') = \nabla_1\|\nabla_2$ then output 1 to indicate E is $\mathsf{KAFw}^{\overrightarrow{f},(w,\gamma)}$, and otherwise 0: E is IC.

We show the output is always 1 when E is $\mathsf{KAFw}^{\overrightarrow{f},(w,\gamma)}$. Assume that $wk_{in} = w_0(k)\|w_1(k)$, and

$$\big(\Psi^{f_2}_{\gamma_2(k)} \circ \Psi^{f_1}_{\gamma_1(k)}\big)\big(wk_{in} \oplus (L\|R)\big) = X\|Y,$$

then by (32) we have

$$\begin{aligned}&\big(\Psi^{f_2}_{\gamma_2(k_\Delta)} \circ \Psi^{f_1}_{\gamma_1(k_\Delta)}\big)\big(wk^{\Delta}_{in} \oplus (L \oplus \nabla_1\|R \oplus \nabla_2)\big)\\ =&X \oplus M_2 \cdot \Delta \| Y \oplus M_1 \cdot \Delta\end{aligned}$$

for $k_\Delta = k \oplus \Delta$ and $wk^{\Delta}_{in} = w_0(k_\Delta)\|w_1(k_\Delta)$. Computing one more round, we obtain

$$\begin{aligned}&\big(\Psi^{f_3}_{\gamma_3(k)} \circ \Psi^{f_2}_{\gamma_2(k)} \circ \Psi^{f_1}_{\gamma_1(k)}\big)\big(wk_{in} \oplus (L\|R)\big)\\ =&Y\|X \oplus f_3(\gamma_3(k) \oplus Y)\end{aligned} \tag{36}$$

and

$$\begin{aligned}&\big(\Psi^{f_3}_{\gamma_3(k_\Delta)} \circ \Psi^{f_2}_{\gamma_2(k_\Delta)} \circ \Psi^{f_1}_{\gamma_1(k_\Delta)}\big)\big(wk^{\Delta}_{in} \oplus (L \oplus \nabla_1\|R \oplus \nabla_2)\big)\\ =&Y \oplus M_1 \cdot \Delta \| X \oplus M_2 \cdot \Delta\\ &\oplus f_3(\gamma_3(k) \oplus M_3 \cdot \Delta \oplus Y \oplus M_1 \cdot \Delta).\end{aligned} \tag{37}$$

The differential Eq. (33) should be adapted to 5 rounds:

$$\Pr\Big(M_5 \cdot \Delta \| M_4 \cdot \Delta \xrightarrow[\Delta]{\mathsf{XOR}_{wk_{out}} \circ \Psi^{f_5}_{\gamma_5(k)} \circ \Psi^{f_4}_{\gamma_4(k)}} \nabla_3\|\nabla_4\Big) = 1, \tag{38}$$

where $wk_{out} = w_2(k)\|w_3(k)$. By this and Eq. (36) and (37), if we assume $wk^{\Delta}_{out} = w_2(k_\Delta)\|w_3(k_\Delta)$,

$$\begin{aligned}Y''\|Z'' =&\big(\Psi^{f_5}_{\gamma_5(k_\Delta)} \circ \Psi^{f_4}_{\gamma_4(k_\Delta)}\big)^{-1}\big(wk^{\Delta}_{out} \oplus (S \oplus \nabla_3\|T \oplus \nabla_4)\big),\\ X''\|Y'' =&\big(\Psi^{f_3}_{\gamma_3(k_\Delta)}\big)^{-1}\big(Y''\|Z''\big),\\ Y'''\|Z''' =&\big(\Psi^{f_5}_{\gamma_5(k)} \circ \Psi^{f_4}_{\gamma_4(k)}\big)^{-1}\big(wk_{out} \oplus (S' \oplus \nabla_3\|T' \oplus \nabla_4)\big),\\ X'''\|Y''' =&\big(\Psi^{f_3}_{\gamma_3(k)}\big)^{-1}\big(Y'''\|Z'''\big),\end{aligned}$$

then it necessarily holds

$$\begin{aligned}Y''\|Z'' &= Y \oplus M_5 \cdot \Delta \| X \oplus f_3(\gamma_3(k) \oplus Y) \oplus M_4 \cdot \Delta,\\ X'' &= X \oplus f_3(\gamma_3(k) \oplus Y) \oplus M_4 \cdot \Delta\\ &\quad \oplus f_3(\gamma_3(k) \oplus M_3 \cdot \Delta \oplus Y \oplus M_5 \cdot \Delta),\\ Y'''\|Z''' &= \underbrace{Y \oplus M_1 \cdot \Delta \oplus M_5 \cdot \Delta}_{=Y,\text{ since } M_1 \cdot \Delta = M_5 \cdot \Delta} \| X \oplus M_2 \cdot \Delta\\ &\quad \oplus f_3(\gamma_3(k) \oplus M_3 \cdot \Delta \oplus Y \oplus M_1 \cdot \Delta) \oplus M_4 \cdot \Delta,\\ X''' &= X \oplus M_2 \cdot \Delta \oplus f_3(\gamma_3(k) \oplus M_3 \cdot \Delta \oplus Y \oplus M_1 \cdot \Delta)\\ &\quad \oplus M_4 \cdot \Delta \oplus f_3(\gamma_3(k) \oplus Y).\end{aligned}$$

Now since $M_5 \cdot \Delta = M_1 \cdot \Delta$, it can be seen

$$(X''\|Y'') \oplus (X'''\|Y''') = M_2 \cdot \Delta \| M_5 \cdot \Delta = M_2 \cdot \Delta \| M_1 \cdot \Delta,$$

which further indicates $(L''\|R'') \oplus (L'''\|R''') = \nabla_1\|\nabla_2$ by Eq. (32).

We've proved that the probability of outputting 1 in the ideal world is $1/(N^2-1)$ in the proof of Theorem 3. Thus the claim. □

Note that we did not assume $\exists \Delta \neq 0$ such that $M_1 \cdot \Delta \neq M_3 \cdot \Delta$ or $M_3 \cdot \Delta \neq M_5 \cdot \Delta$. In this case, the scheme suffers from simpler complementation-based attacks, see Appendix B. On the other hand, if there is no $\Delta \neq 0$ such that $M_1 \cdot \Delta =$

$M_5 \cdot \Delta$, then the above attack is not effective. In fact, we conjecture security in this (latter) case, but the proof would be a significantly different from those in this paper. Moreover, it's inferior in the sense that it requires *additional assumptions* on the key-schedule (i.e. $\forall \Delta \neq 0, M_1 \cdot \Delta \neq M_5 \cdot \Delta$). We thereby leave it for future, and revert to 6 rounds.

B. Security for 6 Rounds when f=P

We first present the conditions on the key-schedule (w, γ) that are sufficient for security proof for 6-round $\mathsf{KAFw}^{f,(w,\gamma)}$.

Definition 3 (Good Affine Key-Schedule for 6 Rounds) *We say that a 6-round key-schedule (w, γ), for which $w = (w_0, w_1, w_2, w_3)$, $w_i(k) = M_i^{(w)} \cdot k \oplus C_i^{(w)}$, $\gamma = (\gamma_1, \gamma_2, \gamma_3, \gamma_4, \gamma_5, \gamma_6)$, and $\gamma_i(k) = M_i \cdot k \oplus C_i$, is* good*, if it satisfies the following conditions:*

(1) *φ_1, φ_6, and $\varphi_1 \oplus \varphi_6$ are bijective maps of $\{0,1\}^n$, where $\varphi_1(k) = w_1(k) \oplus \gamma_1(k)$, $\varphi_6(k) = w_2(k) \oplus \gamma_6(k)$;*
(2) *for any $\Delta \neq 0$, $M_1 \cdot \Delta \neq M_3 \cdot \Delta$, $M_4 \cdot \Delta \neq M_6 \cdot \Delta$.*

The 1st condition resembles those in Definition 1. On the other hand, the 2nd condition prevents the complementing attacks. One could see Appendix B for further insights.

Theorem 5 *When $q_f + 4q_e \leq N/2$, for the 6-round, random permutation-based $\mathsf{KAFw}^{P,(w,\gamma)}$ cipher with a good key-schedule (w, γ) as specified in Definition 3, it holds*

$$\mathbf{Adv}^{\oplus\text{-}rka}_{\mathsf{KAFw}_k^{P,(w,\gamma)}}(q_f, q_e) \leq \frac{14q_eq_f + 57q_e^2 + 4q_e}{N}.$$

Proof. The proof strategy is similar to that described in section III-B1. For any function transcript $\mathcal{Q}_f = ((x_1, y_1), \ldots, (x_{q_f}, y_{q_f}))$, we define $\mathcal{X}(\tau)$ and $\mathcal{Y}(\tau)$ as the sets $\{x_1, \ldots, x_{q_f}\}$ and $\{y_1, \ldots, y_{q_f}\}$. We also define 16 functions for any tuple $\mathbf{t} = (\Delta, LR, ST)$ in $\mathcal{Q}_E$ and any function f ($f = P \in \mathcal{P}(n)$ in this subsection):

- $x_1(\mathbf{t}) = \varphi_1(k \oplus \Delta) \oplus R$,
- $y_1(\mathbf{t}, f) = f(x_1(\mathbf{t}))$,
- $X(\mathbf{t}, f) = L \oplus w_0(k \oplus \Delta) \oplus y_1(\mathbf{t}, f)$,
- $x_2(\mathbf{t}, f) = \gamma_2(k \oplus \Delta) \oplus X(\mathbf{t}, f)$,
- $y_2(\mathbf{t}, f) = f(x_2(\mathbf{t}, f))$,
- $Y(\mathbf{t}, f) = R \oplus w_1(k \oplus \Delta) \oplus y_2(\mathbf{t}, f)$,
- $x_3(\mathbf{t}, f) = \gamma_3(k \oplus \Delta) \oplus Y(\mathbf{t}, f)$,
- $y_3(\mathbf{t}, f) = X(\mathbf{t}, f) \oplus Z(\mathbf{t}, f)$,
- $Z(\mathbf{t}, f) = S \oplus w_2(k \oplus \Delta) \oplus y_5(\mathbf{t}, f)$,
- $x_4(\mathbf{t}, f) = \gamma_4(k \oplus \Delta) \oplus Z(\mathbf{t}, f)$,
- $y_4(\mathbf{t}, f) = Y(\mathbf{t}, f) \oplus A(\mathbf{t}, f)$,
- $A(\mathbf{t}, f) = T \oplus w_3(k \oplus \Delta) \oplus y_6(\mathbf{t}, f)$,
- $x_5(\mathbf{t}, f) = \gamma_5(k \oplus \Delta) \oplus A(\mathbf{t}, f)$,
- $y_5(\mathbf{t}, f) = f(x_5(\mathbf{t}, f))$,
- $x_6(\mathbf{t}) = \varphi_6(k \oplus \Delta) \oplus S$,
- $y_6(\mathbf{t}, f) = f(x_6(\mathbf{t}))$.

Bad Transcripts are then defined as follows.

Definition 4 (Bad Transcripts for 6-Round $\mathsf{KAFw}^{P,(w,\gamma)}$) *An attainable transcript $\tau = (\mathcal{Q}_E, \mathcal{Q}_P, k)$ is* bad*, if at least one of the following conditions is fulfilled:*

- *(B-1) $\exists \mathbf{t} \in \mathcal{Q}_E : x_1(\mathbf{t}) \in \mathcal{X}(\tau)$ or $x_6(\mathbf{t}) \in \mathcal{X}(\tau)$;*
- *(B-2) $\exists \mathbf{t}, \mathbf{t}' \in \mathcal{Q}_E : x_1(\mathbf{t}) = x_6(\mathbf{t}')$;*
- *(B-3) there exist two queries $\mathbf{t} = (\Delta, LR, ST)$ and $\mathbf{t}' = (\Delta', L'R', S'T')$ in $\mathcal{Q}_E$ such that $\Delta \neq \Delta'$, and $R \oplus R' = (M_1^{(w)} \oplus M_1) \cdot (\Delta \oplus \Delta')$ and $S \oplus S' = (M_6 \oplus M_2^{(w)}) \cdot (\Delta \oplus \Delta')$.*

Otherwise we say τ is good. Denote by $\mathcal{T}_{bad}$ the set of bad transcripts.

Recall that

$$\varphi_1(k) = w_1(k) \oplus \gamma_1(k) = M_1^{(w)} \cdot k \oplus C_1^{(w)} \oplus M_1 \cdot k \oplus C_1, \text{ and}$$
$$\varphi_6(k) = w_2(k) \oplus \gamma_6(k) = M_2^{(w)} \cdot k \oplus C_2^{(w)} \oplus M_6 \cdot k \oplus C_6.$$

Since both φ_1 and φ_6 are bijective maps of $\mathbb{F}_2^n$, $\Pr[\text{(B-1)}] \leq \frac{2q_eq_f}{N}$ is obvious. On the other hand, since $\varphi_1 \oplus \varphi_6$ is also bijective, for each choice of $\mathbf{t} = (\Delta, LR, ST)$ and $\mathbf{t}' = (\Delta', L'R', S'T')$ it holds

$$\begin{aligned}
&\Pr[x_1(\mathbf{t}) = x_6(\mathbf{t}')] \\
=&\Pr\big[(M_1^{(w)} \oplus M_1) \cdot (k_\Delta) \oplus C_1^{(w)} \oplus C_1 \oplus R \\
&\quad = (M_2^{(w)} \oplus M_6) \cdot (k_\Delta) \oplus (M_2^{(w)} \oplus M_6) \cdot (\Delta \oplus \Delta') \\
&\quad\quad \oplus C_2^{(w)} \oplus C_6 \oplus S'\big] \\
=&\Pr\big[(\varphi_1 \oplus \varphi_6)(k_\Delta) = (M_2^{(w)} \oplus M_6) \cdot (\Delta \oplus \Delta') \oplus R \oplus S'\big] \\
=&\frac{1}{N}.
\end{aligned}$$

Therefore, $\Pr[\text{(B-2)}] \leq \frac{q_e^2}{N}$. Ultimately, for (B-3), for any such two queries (Δ, LR, ST) and $(\Delta', L'R', S'T')$, following an analysis similar to (B-4) in Definition 2, the probability that $R \oplus R' = (M_1^{(w)} \oplus M_1) \cdot (\Delta \oplus \Delta')$ and $S \oplus S' = (M_6 \oplus M_2^{(w)}) \cdot (\Delta \oplus \Delta')$ are both fulfilled is at most $2/N$ when $q_e \leq N$. Thus $\Pr[\text{(B-3)}] \leq \frac{q_e^2}{N}$. In all,

$$\Pr[T_{id} \in \mathcal{T}_{bad}] \leq \frac{2q_eq_f + 2q_e^2}{N}. \tag{39}$$

Ratio $\Pr_{re}(\tau)/\Pr_{id}(\tau)$ for Good τ. We define two bad predicates on P in turn. Then, using an argument similar to subsection III-B3, we show that if neither of the two predicates holds, then $\Pr[\mathsf{KAFw}_k^{P,(w,\gamma)} \vdash \mathcal{Q}_E] \geq \frac{1}{N^{2q_e}}$. These cinch the bounds.

First Bad Predicate. For any $P \vdash \mathcal{Q}_P$, the predicate $\mathsf{B1}(P)$ holds, if any of the following conditions is fulfilled:

- (C-11) there exist $\mathbf{t} = (\Delta, LR, ST)$ and $\mathbf{t}' = (\Delta', L'R', S'T')$ in $\mathcal{Q}_E$ such that $x_1(\mathbf{t}) \neq x_1(\mathbf{t}')$, yet $x_2(\mathbf{t}, P) = x_2(\mathbf{t}', P)$ or $X(\mathbf{t}, P) \oplus X(\mathbf{t}', P) = M_6 \cdot (\Delta \oplus \Delta')$;
- (C-12) $\exists \mathbf{t}, \mathbf{t}' \in \mathcal{Q}_E$ (could be $\mathbf{t} = \mathbf{t}'$): $x_2(\mathbf{t}, P) \in \mathcal{X}(\tau)$, or $x_2(\mathbf{t}, P) = x_1(\mathbf{t}')$, or $x_2(\mathbf{t}, P) = x_6(\mathbf{t}')$;
- (C-13) there exist $\mathbf{t} = (\Delta, LR, ST)$ and $\mathbf{t}' = (\Delta', L'R', S'T')$ in $\mathcal{Q}_E$ such that $x_6(\mathbf{t}) \neq x_6(\mathbf{t}')$, yet $x_5(\mathbf{t}, P) = x_5(\mathbf{t}', P)$ or $A(\mathbf{t}, P) \oplus A(\mathbf{t}', P) = M_1 \cdot (\Delta \oplus \Delta')$;
- (C-14) $\exists \mathbf{t}, \mathbf{t}' \in \mathcal{Q}_E$ (could be $\mathbf{t} = \mathbf{t}'$): $x_5(\mathbf{t}, P) \in \mathcal{X}(\tau)$, or $x_5(\mathbf{t}, P) \in \{x_1(\mathbf{t}'), x_2(\mathbf{t}', P), x_6(\mathbf{t}')\}$;
- (C-15) there exists a query $\mathbf{t} = (\Delta, LR, ST)$ in $\mathcal{Q}_E$ such that

– $L \oplus w_0(k \oplus \Delta) \oplus S \oplus w_2(k \oplus \Delta) = P(x_1(\mathbf{t}))$, or
– $R \oplus w_1(k \oplus \Delta) \oplus T \oplus w_3(k \oplus \Delta) = P(x_6(\mathbf{t}))$.

For (C-11), for each pair $(\mathbf{t}, \mathbf{t}')$ with $\mathbf{t} = (\Delta, LR, ST)$ and $\mathbf{t}' = (\Delta', L'R', S'T')$, the event $x_2(\mathbf{t}, P) = x_2(\mathbf{t}', P)$ is equivalent to $X(\mathbf{t}, P) \oplus X(\mathbf{t}', P) = M_2 \cdot (\Delta \oplus \Delta')$, which is further equivalent to

$$\begin{aligned} &L \oplus w_0(k_\Delta) \oplus P(x_1(\mathbf{t})) \\ =&L' \oplus w_0(k_{\Delta'}) \oplus P(x_1(\mathbf{t}')) \oplus M_2 \cdot (\Delta \oplus \Delta'). \end{aligned} \tag{40}$$

Since τ is good, it holds $x_1(\mathbf{t}) \notin \mathcal{X}(\tau)$. Conditioned on $P \vdash \mathcal{Q}_P$ and the $\leq 2q_e$ function values $\{P(x_i(\mathbf{t}')) \mid \mathbf{t}' \in \mathcal{Q}_E, i = 1, 6, x_i(\mathbf{t}') \neq x_1(\mathbf{t})\}$ (which includes $P(x_1(\mathbf{t}'))$ since $x_1(\mathbf{t}) \neq x_1(\mathbf{t}')$), $P(x_1(\mathbf{t}))$ is uniform in at least $N - q_f - 2q_e$ possibilities. Therefore, for each pair $(\mathbf{t}, \mathbf{t}')$, $\Pr[x_2(\mathbf{t}, P) = x_2(\mathbf{t}', P)] = \Pr[\text{Eq. (40)}] \leq \frac{1}{N - q_f - 2q_e}$. For the same reason, $\Pr[X(\mathbf{t}, P) \oplus X(\mathbf{t}', P) = M_6 \cdot (\Delta \oplus \Delta')] \leq \frac{1}{N - q_f - 2q_e}$. Thus

$$\Pr[\text{(C-11)}] \leq \binom{q_e}{2} \cdot \frac{2}{N - q_f - 2q_e} \leq \frac{q_e^2}{N - q_f - 2q_e}.$$

Then, the value $x_2(\mathbf{t}, P)$ relies on $P(x_1(\mathbf{t}))$, and is thus uniform. Since the values in $\mathcal{X}(\tau)$ and the values of the form $x_1(\mathbf{t}')$ and $x_6(\mathbf{t}')$ are all independent from $P(x_1(\mathbf{t}))$, it holds

$$\Pr[\text{(C-12)}] \leq \frac{q_e q_f}{N - q_f - 2q_e} + \frac{q_e \cdot 2q_e}{N - q_f - 2q_e} = \frac{q_e(q_f + 2q_e)}{N - q_f - 2q_e}.$$

For (C-13) the analysis is similar to (C-11) by symmetry, yielding the same bound

$$\Pr[\text{(C-13)}] \leq \binom{q_e}{2} \cdot \frac{2}{N - q_f - 2q_e} \leq \frac{q_e^2}{N - q_f - 2q_e}.$$

Similarly, the main claim in (C-14) can be bounded:

$$\begin{aligned} &\Pr[\exists \mathbf{t}, \mathbf{t}' : x_5(\mathbf{t}, P) \in \mathcal{X}(\tau) \text{ or } x_5(\mathbf{t}, P) = x_1(\mathbf{t}') \text{ or } x_5(\mathbf{t}, P) = x_6(\mathbf{t}')] \\ \leq &\frac{q_e(q_f + 2q_e)}{N - q_f - 2q_e} \end{aligned}$$

The remaining subevent of (C-14), i.e. $\exists \mathbf{t}, \mathbf{t}' : x_5(\mathbf{t}, P) = x_2(\mathbf{t}', P)$, is equivalent to

$$\begin{aligned} &\gamma_5(k \oplus \Delta) \oplus T \oplus w_3(k \oplus \Delta) \oplus P(x_6(\mathbf{t})) \\ =&\gamma_2(k \oplus \Delta') \oplus L' \oplus w_0(k \oplus \Delta') \oplus P(x_1(\mathbf{t}')). \end{aligned} \tag{41}$$

By ¬(B-2), $x_1(\mathbf{t}') \neq x_6(\mathbf{t})$, thus $P(x_1(\mathbf{t}'))$—as well as the entire right hand side—is random conditioned on $P(x_6(\mathbf{t}))$. Thus $\Pr[\exists \mathbf{t}, \mathbf{t}' : \text{Eq. (41) holds}] \leq \frac{q_e^2}{N - q_f - 2q_e}$, and

$$\Pr[\text{(C-14)}] \leq \frac{q_e(q_f + 2q_e)}{N - q_f - 2q_e} + \frac{q_e^2}{N - q_f - 2q_e} \leq \frac{q_e(q_f + 3q_e)}{N - q_f - 2q_e}.$$

Finally, since both $P(x_1(\mathbf{t}))$ and $P(x_6(\mathbf{t}))$ are uniform for each $\mathbf{t}$, we immediately obtain $\Pr[\text{(C-15)}] \leq \frac{2q_e}{N - q_f - 2q_e}$. Summing over $\Pr[\text{(C-11)}]$ to $\Pr[\text{(C-15)}]$, we reach

$$\Pr[P \xleftarrow{\$} \mathcal{P}(n) : \mathsf{B1}(P) \mid P \vdash \mathcal{Q}_P] \leq \frac{2q_e q_f + 7q_e^2 + 2q_e}{N - q_f - 2q_e}. \tag{42}$$

Second Bad Predicate. We then consider a random permutation P such that $P \vdash \mathcal{Q}_P$ and ¬$\mathsf{B1}(P)$. For this P, the predicate $\mathsf{B2}(P)$ holds if any of the following conditions is fulfilled:

- (C-21) $\exists \mathbf{t}, \mathbf{t}' \in \mathcal{Q}_E : x_2(\mathbf{t}, P) \neq x_2(\mathbf{t}', P)$, yet either $x_3(\mathbf{t}, P) = x_3(\mathbf{t}', P)$ or $y_4(\mathbf{t}, P) = y_4(\mathbf{t}', P)$;
- (C-22) $\exists \mathbf{t}, \mathbf{t}' \in \mathcal{Q}_E$ (could be $\mathbf{t} = \mathbf{t}'$):
  – $x_3(\mathbf{t}, P) \in \mathcal{X}(\tau)$ or $y_4(\mathbf{t}, P) \in \mathcal{Y}(\tau)$, or
  – $x_3(\mathbf{t}, P) \in \{x_1(\mathbf{t}'), x_2(\mathbf{t}', P), x_5(\mathbf{t}', P), x_6(\mathbf{t}')\}$, or
  – $y_4(\mathbf{t}, P) \in \{y_1(\mathbf{t}', P), y_2(\mathbf{t}', P), y_5(\mathbf{t}', P), y_6(\mathbf{t}', P)\}$.
- (C-23) $\exists \mathbf{t}, \mathbf{t}' \in \mathcal{Q}_E : x_5(\mathbf{t}, P) \neq x_5(\mathbf{t}', P)$, yet either $x_4(\mathbf{t}, P) = x_4(\mathbf{t}', P)$ or $y_3(\mathbf{t}, P) = y_3(\mathbf{t}', P)$;
- (C-24) $\exists \mathbf{t}, \mathbf{t}' \in \mathcal{Q}_E$ (could be $\mathbf{t} = \mathbf{t}'$):
  – $x_4(\mathbf{t}, P) \in \mathcal{X}(\tau)$ or $y_3(\mathbf{t}, P) \in \mathcal{Y}(\tau)$, or
  – $x_4(\mathbf{t}, P) \in \{x_1(\mathbf{t}'), x_2(\mathbf{t}', P), x_3(\mathbf{t}', P), x_5(\mathbf{t}', P), x_6(\mathbf{t}')\}$, or
  – $y_3(\mathbf{t}, P) \in \{y_1(\mathbf{t}', P), y_2(\mathbf{t}', P), y_4(\mathbf{t}', P), y_5(\mathbf{t}', P), y_6(\mathbf{t}', P)\}$.

First, for each $\mathbf{t} = (\Delta, LR, ST)$, conditioned on $P \vdash \mathcal{Q}_P$ and the $\leq 4q_e$ values

$$\{P(x_i(\mathbf{t}')), P(x_j(\mathbf{t}', P)), \mid \mathbf{t}' \in \mathcal{Q}_E, i = 1, 6, j = 2, 5, \\ x_j(\mathbf{t}', P) \neq x_2(\mathbf{t}, P)\},$$

the value $y_2(\mathbf{t}, P) = P(x_2(\mathbf{t}, P))$ remains uniform in at least $N - q_f - 4q_e$ possibilities. So $Y(\mathbf{t}, P)$, $x_3(\mathbf{t}, P)$, and $y_4(\mathbf{t}, P)$ derived from $y_2(\mathbf{t}, P)$ are all uniform. These show:

$$\Pr[\text{(C-21)}] \leq \binom{q_e}{2} \cdot \frac{2}{N - q_f - 4q_e} \leq \frac{q_e^2}{N - q_f - 4q_e},$$

$$\Pr[\exists \mathbf{t} : x_3(\mathbf{t}, P) \in \mathcal{X}(\tau)] \leq \frac{q_e q_f}{N - q_f - 4q_e}, \tag{43}$$

$$\Pr[\exists \mathbf{t}, \mathbf{t}' : x_3(\mathbf{t}, P) \in \{x_1(\mathbf{t}'), x_6(\mathbf{t}')\}] \leq \frac{q_e \cdot 2q_e}{N - q_f - 4q_e}, \tag{44}$$

$$\Pr[\exists \mathbf{t} : y_4(\mathbf{t}, P) \in \mathcal{Y}(\tau)] \leq \frac{q_e q_f}{N - q_f - 4q_e}. \tag{45}$$

Second, for cleanness let $k_\Delta = k \oplus \Delta$ and $k_{\Delta'} = k \oplus \Delta'$, then

$$\begin{aligned} &\Pr[\exists \mathbf{t}, \mathbf{t}' : x_3(\mathbf{t}, P) = x_2(\mathbf{t}', P)] \\ =&\Pr[\exists \mathbf{t}, \mathbf{t}' : \underbrace{\gamma_3(k_\Delta) \oplus R \oplus w_1(k_\Delta)}_{CON_1, \text{ will be used below}} \oplus \underline{P(x_2(\mathbf{t}, P))} \\ &= \gamma_2(k_{\Delta'}) \oplus L' \oplus w_0(k_{\Delta'}) \oplus \underline{P(x_1(\mathbf{t}'))}]. \end{aligned}$$

By ¬(C-12), $x_2(\mathbf{t}, P) \neq x_1(\mathbf{t}')$, $x_2(\mathbf{t}, P) \neq x_6(\mathbf{t}')$, $x_2(\mathbf{t}, P) \neq x_6(\mathbf{t})$, so for the involved equality the right hand side is random conditioned on the left hand side. Therefore,

$$\Pr[\exists \mathbf{t}, \mathbf{t}' : x_3(\mathbf{t}, P) = x_2(\mathbf{t}', P)] \leq \frac{q_e^2}{N - q_f - 4q_e}. \tag{46}$$

For similar reasons,

$$\begin{aligned}
&\Pr[\exists \mathbf{t}, \mathbf{t}' : x_3(\mathbf{t}, P) = x_5(\mathbf{t}', P)] \\
=&\Pr[\exists \mathbf{t}, \mathbf{t}' : CON_1 \oplus \underline{P(x_2(\mathbf{t}, P))} \\
&\qquad = \gamma_5(k_{\Delta'}) \oplus T' \oplus w_3(k_{\Delta'}) \oplus \underline{P(x_6(\mathbf{t}'))}] \\
\leq&\frac{q_e^2}{N - q_f - 4q_e}, \qquad (47) \\
&\Pr\left[\exists \mathbf{t}, \mathbf{t}' : y_4(\mathbf{t}, P) = y_1(\mathbf{t}', P)\right] \\
=&\Pr\left[\exists \mathbf{t}, \mathbf{t}' : \big(R \oplus w_1(k_\Delta) \oplus P(x_2(\mathbf{t}, P))\big)\right. \\
&\qquad \left. \oplus \big(T \oplus w_3(k_\Delta) \oplus P(x_6(\mathbf{t}))\big) = P(x_1(\mathbf{t}'))\right] \\
=&\Pr\left[\exists \mathbf{t}, \mathbf{t}' : P(x_2(\mathbf{t}, P)) = R \oplus w_1(k_\Delta) \oplus T\right. \\
&\qquad \left. \oplus w_3(k_\Delta) \oplus P(x_6(\mathbf{t})) \oplus P(x_1(\mathbf{t}'))\right] \\
\leq&\frac{q_e^2}{N - q_f - 4q_e}. \qquad (48) \\
&\Pr\left[\exists \mathbf{t}, \mathbf{t}' : y_4(\mathbf{t}, P) = y_6(\mathbf{t}', P)\right] \\
=&\Pr\left[\exists \mathbf{t}, \mathbf{t}' : P(x_2(\mathbf{t}, P)) = R \oplus w_1(k_\Delta) \oplus T\right. \\
&\qquad \left. \oplus w_3(k_\Delta) \oplus P(x_6(\mathbf{t})) \oplus P(x_6(\mathbf{t}'))\right] \\
\leq&\frac{q_e^2}{N - q_f - 4q_e}. \qquad (49)
\end{aligned}$$

Furthermore, by ¬(C-14), $\forall \mathbf{t}, \mathbf{t}', x_2(\mathbf{t}, P) \neq x_5(\mathbf{t}', P)$. So

$$\begin{aligned}
&\Pr[\exists \mathbf{t}, \mathbf{t}' : y_4(\mathbf{t}, P) = y_5(\mathbf{t}', P)] \\
=&\Pr[\exists \mathbf{t}, \mathbf{t}' : R \oplus w_1(k_\Delta) \oplus \underline{P(x_2(\mathbf{t}, P))} \oplus T \oplus w_3(k_\Delta) \\
&\qquad \oplus P(x_6(\mathbf{t})) = \underline{P(x_5(\mathbf{t}', P))}] \\
\leq&\frac{q_e^2}{N - q_f - 4q_e}. \qquad (50)
\end{aligned}$$

Finally, for a pair $(\mathbf{t}, \mathbf{t}')$, $y_4(\mathbf{t}, P) = y_2(\mathbf{t}', P)$ would imply

$$\begin{aligned}
&R \oplus w_1(k_\Delta) \oplus \underline{P(x_2(\mathbf{t}, P))} \oplus T \oplus w_3(k_\Delta) \oplus P(x_6(\mathbf{t})) \\
=&\underline{P(x_2(\mathbf{t}', P))}. \qquad (51)
\end{aligned}$$

Then,

(1) If $x_2(\mathbf{t}, P) = x_2(\mathbf{t}', P)$, then for $\mathbf{t} = (\Delta, LR, ST)$ it holds

$$R \oplus w_1(k \oplus \Delta) \oplus T \oplus w_3(k \oplus \Delta) = P(x_6(\mathbf{t})),$$

contradicting ¬(C-15);

(2) Otherwise, $P(x_2(\mathbf{t}', P))$ is random conditioned on the left hand side of (51), thus $\Pr[\text{Eq. (51)}] \leq \frac{1}{N - q_f - 4q_e}$.

As the number of pairs $(\mathbf{t}, \mathbf{t}')$ is at most q_e^2,

$$\Pr[\exists \mathbf{t}, \mathbf{t}' : y_4(\mathbf{t}, P) = y_2(\mathbf{t}', P)] \leq \frac{q_e^2}{N - q_f - 4q_e}. \qquad (52)$$

Summing over (43)-(52), we obtain

$$\Pr[\text{(C-22)}] \leq \frac{2q_e(q_f + 4q_e)}{N - q_f - 4q_e}.$$

Third, symmetrically, for each $\mathbf{t} = (\Delta, LR, ST) \in \mathcal{Q}_E$, the value $y_5(\mathbf{t}, P) = P(x_5(\mathbf{t}, P))$ remains random. So $Z(\mathbf{t}, P)$, $x_4(\mathbf{t}, P)$, and $y_3(\mathbf{t}, P)$ are all uniform. Therefore, $\Pr[\text{(C-23)}] \leq \frac{q_e^2}{N - q_f - 4q_e}$. In addition, in a similar vein to the analysis of (C-22), we have

- $\Pr[\exists \mathbf{t} : x_4(\mathbf{t}, P) \in \mathcal{X}(\tau) \text{ or } y_3(\mathbf{t}, P) \in \mathcal{Y}(\tau)] \leq \frac{2q_e q_f}{N - q_f - 4q_e}$;
- $\Pr[\exists \mathbf{t}, \mathbf{t}' : x_4(\mathbf{t}, P) = x_1(\mathbf{t}') \text{ or } x_4(\mathbf{t}, P) = x_6(\mathbf{t}')] \leq \frac{2q_e^2}{N - q_f - 4q_e}$.

By ¬(C-14), $\forall \mathbf{t}, \mathbf{t}', x_5(\mathbf{t}, P) \neq x_1(\mathbf{t}')$. So: ($k_\Delta = k \oplus \Delta$, $k_{\Delta'} = k \oplus \Delta'$)

$$\begin{aligned}
&\Pr[\exists \mathbf{t}, \mathbf{t}' : x_4(\mathbf{t}, P) = x_2(\mathbf{t}', P)] \\
=&\Pr[\underbrace{\gamma_4(k_\Delta) \oplus S \oplus w_2(k_\Delta)}_{CON_2, \text{ will be used below}} \oplus \underline{P(x_5(\mathbf{t}, P))} \\
&\qquad = \gamma_2(k_{\Delta'}) \oplus L' \oplus w_0(k_{\Delta'}) \oplus \underline{P(x_1(\mathbf{t}'))}] \\
\leq&\frac{q_e^2}{N - q_f - 4q_e}, \text{ and} \\
&\Pr[\exists \mathbf{t}, \mathbf{t}' : y_3(\mathbf{t}, P) = y_1(\mathbf{t}', P)] \\
=&\Pr[\big(L \oplus w_0(k_\Delta) \oplus P(x_1(\mathbf{t}))\big) \oplus \big(S \oplus w_2(k_\Delta) \\
&\qquad \oplus P(x_5(\mathbf{t}, P))\big) = P(x_1(\mathbf{t}'))] \\
=&\Pr\left[P(x_5(\mathbf{t}, P)) = \underbrace{L \oplus w_0(k_\Delta) \oplus S \oplus w_2(k_\Delta)}_{CON_3, \text{ will be used later}}\right. \\
&\qquad \left. \oplus P(x_1(\mathbf{t})) \oplus \underline{P(x_1(\mathbf{t}'))}\right] \\
\leq&\frac{q_e^2}{N - q_f - 4q_e}.
\end{aligned}$$

By ¬(C-14), $\forall \mathbf{t}, \mathbf{t}', x_5(\mathbf{t}, P) \neq x_2(\mathbf{t}', P)$. So

$$\begin{aligned}
&\Pr[\exists \mathbf{t}, \mathbf{t}' : x_4(\mathbf{t}, P) = x_3(\mathbf{t}', P)] \\
=&\Pr[CON_2 \oplus \underline{P(x_5(\mathbf{t}, P))} \\
&\qquad = \gamma_3(k_{\Delta'}) \oplus R' \oplus w_1(k_{\Delta'}) \oplus \underline{P(x_2(\mathbf{t}', P))}] \\
\leq&\frac{q_e^2}{N - q_f - 4q_e}, \text{ and} \\
&\Pr[\exists \mathbf{t}, \mathbf{t}' : y_3(\mathbf{t}, P) = y_2(\mathbf{t}', P)] \\
=&\Pr[P(x_5(\mathbf{t}, P)) = CON_3 \oplus P(x_1(\mathbf{t})) \oplus \underline{P(x_2(\mathbf{t}', P))}] \\
\leq&\frac{q_e^2}{N - q_f - 4q_e}.
\end{aligned}$$

By ¬(C-14), $\forall \mathbf{t}, \mathbf{t}', x_5(\mathbf{t}, P) \neq x_6(\mathbf{t}')$. So

$$\begin{aligned}
&\Pr[\exists \mathbf{t}, \mathbf{t}' : x_4(\mathbf{t}, P) = x_5(\mathbf{t}', P)] \\
=&\Pr[CON_2 \oplus \underline{P(x_5(\mathbf{t}, P))} \\
&\qquad = \gamma_5(k_{\Delta'}) \oplus T' \oplus w_3(k_{\Delta'}) \oplus \underline{P(x_6(\mathbf{t}'))}] \\
\leq&\frac{q_e^2}{N - q_f - 4q_e}, \text{ and} \\
&\Pr[\exists \mathbf{t}, \mathbf{t}' : y_3(\mathbf{t}, P) = y_6(\mathbf{t}', P)] \\
=&\Pr[P(x_5(\mathbf{t}, P)) = CON_3 \oplus P(x_1(\mathbf{t})) \oplus \underline{P(x_6(\mathbf{t}'))}] \\
\leq&\frac{q_e^2}{N - q_f - 4q_e}.
\end{aligned}$$

By ¬(C-14), $\forall \mathbf{t}, \mathbf{t}', x_5(\mathbf{t}, P) \neq x_2(\mathbf{t}', P)$ and $x_5(\mathbf{t}, P) \neq x_6(\mathbf{t}')$. So

$$\begin{aligned}
&\Pr[\exists \mathbf{t}, \mathbf{t}' : y_3(\mathbf{t}, P) = y_4(\mathbf{t}', P)] \\
=&\Pr[P(x_5(\mathbf{t}, F)) = CON_3 \oplus P(x_1(\mathbf{t})) \oplus \big(R' \oplus w_1(k_{\Delta'}) \\
&\qquad \oplus \underline{P(x_2(\mathbf{t}', P))}\big) \oplus \big(T' \oplus w_3(k_{\Delta'}) \oplus \underline{P(x_6(\mathbf{t}'))}\big)] \\
\leq&\frac{q_e^2}{N - q_f - 4q_e}
\end{aligned}$$

Finally consider $\Pr[\exists \mathbf{t}, \mathbf{t}' : y_3(\mathbf{t}, P) = y_5(\mathbf{t}', P)]$. If it happens then we have

$$\begin{aligned} &L \oplus w_0(k_\Delta) \oplus P(x_1(\mathbf{t})) \oplus S \oplus w_2(k_\Delta) \oplus \underline{P(x_5(\mathbf{t}, P))} \\ =&\underline{P(x_5(\mathbf{t}', P))}. \end{aligned} \tag{53}$$

If $x_5(\mathbf{t}, P) \neq x_5(\mathbf{t}', P)$ then the right hand side of (53) is random given $P(x_5(\mathbf{t}, P))$ and $\Pr[\text{Eq. (53)}] \leq \frac{1}{N - q_f - 2q_e}$; otherwise we reach $L \oplus w_0(k \oplus \Delta) \oplus S \oplus w_2(k \oplus \Delta) = P(x_1(\mathbf{t}))$, contradicting ¬(C-15). So

$$\Pr[\exists \mathbf{t}, \mathbf{t}' : y_3(\mathbf{t}, P) = y_5(\mathbf{t}', P)] \leq \frac{q_e^2}{N - q_f - 2q_e}. \tag{54}$$

In all, we have

$$\Pr[\text{(C-24)}] \leq \frac{2q_e(q_f + 5q_e)}{N - q_f - 4q_e},$$

and further

$$\Pr[P \xleftarrow{\$} \mathcal{P}(n) : \mathsf{B2}(P) \mid P \vdash \mathcal{Q}_P \wedge \neg \mathsf{B1}(P)] \leq \frac{4q_e q_f + 20q_e^2}{N - q_f - 4q_e}. \tag{55}$$

Define $\mathsf{B}(P) = \mathsf{B1}(P) \vee \mathsf{B2}(P)$. Then Eq. (42) and (55) yield

$$\Pr[P \xleftarrow{\$} \mathcal{P}(n) : \mathsf{B}(P) \mid P \vdash \mathcal{Q}_P] \leq \frac{6q_e q_f + 27q_e^2 + 2q_e}{N - q_f - 4q_e}. \tag{56}$$

$\underline{2q_e \textit{ Equations}}$. Similarly to the 4-round case, we show

$$\Pr_P[\mathsf{RK}[\mathsf{KAFw}_k^{P,(w,\gamma)}] \vdash \mathcal{Q}_E \mid P \vdash \mathcal{Q}_P \wedge \neg \mathsf{B}(P)] \geq \frac{1}{N^{2q_e}}.$$

Here $\neg\mathsf{B}(P)$ indicates

- $\forall \mathbf{t} \in \mathcal{Q}_E, i = 3, 4$, $x_i(\mathbf{t}, P) \notin \mathcal{X}(\tau)$, $y_i(\mathbf{t}, P) \notin \mathcal{Y}(\tau)$, and
- $\{x_i(\mathbf{t}, P) \mid i = 3, 4, \mathbf{t} \in \mathcal{Q}_E\} \cap \{x_j(\mathbf{t}, P) \mid j = 1, 2, 5, 6, \mathbf{t} \in \mathcal{Q}_E\} = \emptyset$, and
- $\{y_i(\mathbf{t}, P) \mid i = 3, 4, \mathbf{t} \in \mathcal{Q}_E\} \cap \{y_j(\mathbf{t}, P) \mid j = 1, 2, 5, 6, \mathbf{t} \in \mathcal{Q}_E\} = \emptyset$, and
- $\forall \mathbf{t}, \mathbf{t}' \in \mathcal{Q}_E, x_3(\mathbf{t}, P) \neq x_4(\mathbf{t}', P), y_3(\mathbf{t}, P) \neq y_4(\mathbf{t}', P)$.

By an analysis similar to subsection III-B3, we only need to show

$$\left|\{x_i(\mathbf{t}, P) \mid \mathbf{t} \in \mathcal{Q}_E\}\right| = \left|\{y_i(\mathbf{t}, P) \mid \mathbf{t} \in \mathcal{Q}_E\}\right| = q_e$$

for $i = 3, 4$. For this, we argue $\mathbf{t} \neq \mathbf{t}' \Rightarrow x_3(\mathbf{t}, P) \neq x_3(\mathbf{t}', P)$ and $y_4(\mathbf{t}, P) \neq y_4(\mathbf{t}', P)$ for any $\mathbf{t} = (\Delta, LR, ST)$ and $\mathbf{t}' = (\Delta', L'R', S'T')$:

$\underline{\text{Case 1:}}$ $\mathbf{t}$ and $\mathbf{t}'$ are such that $R \oplus R' = (M_1^{(w)} \oplus M_1) \cdot (\Delta \oplus \Delta')$ and $L \oplus L' = (M_0^{(w)} \oplus M_2) \cdot (\Delta \oplus \Delta')$. By the definition of $\varphi_0, \varphi_1, \gamma_1$, and γ_2, the former implies $\varphi_1(k \oplus \Delta) \oplus R = \varphi_1(k \oplus \Delta') \oplus R'$, i.e. $x_1(\mathbf{t}) = x_1(\mathbf{t}')$; and the latter further implies

$$\begin{aligned} &\gamma_2(k \oplus \Delta) \oplus L \oplus w_0(k \oplus \Delta) \oplus P(x_1(\mathbf{t})) \\ =&\gamma_2(k \oplus \Delta') \oplus L' \oplus w_0(k \oplus \Delta') \oplus P(x_1(\mathbf{t})), \end{aligned}$$

i.e. $x_2(\mathbf{t}, P) = x_2(\mathbf{t}', P)$. And it necessarily be $\Delta \neq \Delta'$, otherwise $\Delta \oplus \Delta' = 0$ and thus $R = R'$ and $L = L'$ and $\mathbf{t} = \mathbf{t}'$, a contradiction. Then:

- $x_3(\mathbf{t}, P) \neq x_3(\mathbf{t}', P)$, otherwise it implies

  $$\begin{aligned} &\gamma_3(k \oplus \Delta) \oplus R \oplus w_1(k \oplus \Delta) \oplus P(x_2(\mathbf{t}, P)) \\ =&\gamma_3(k \oplus \Delta') \oplus R' \oplus w_1(k \oplus \Delta') \oplus P(x_2(\mathbf{t}', P)). \end{aligned}$$

  Then we have

  $$\begin{aligned} \underbrace{\gamma_3(k \oplus \Delta) \oplus \gamma_3(k \oplus \Delta')}_{= M_3 \cdot \Delta \oplus M_3 \cdot \Delta'} &= R \oplus R' \oplus M_1^{(w)} \cdot (\Delta \oplus \Delta') \\ &= M_1 \cdot (\Delta \oplus \Delta'), \end{aligned}$$

  thus $M_3 \cdot (\Delta \oplus \Delta') = M_1 \cdot (\Delta \oplus \Delta')$, contradicting condition (2) in Definition 3 (*good key-schedule for 6 rounds*);
- $y_4(\mathbf{t}, P) \neq y_4(\mathbf{t}', P)$. Because the assumption on $R \oplus R'$ implies $S \oplus S' \neq (M_6 \oplus M_2^{(w)}) \cdot (\Delta \oplus \Delta')$ by ¬(B-3). By ¬(C-13) we further have $A(\mathbf{t}, P) \oplus A(\mathbf{t}', P) \neq M_1 \cdot (\Delta \oplus \Delta')$. However, in this case, it necessarily be

  $$\begin{aligned} Y(\mathbf{t}, P) \oplus Y(\mathbf{t}', P) &= R \oplus R' \oplus w_1(k_\Delta) \oplus w_1(k_{\Delta'}) \\ &= M_1 \cdot (\Delta \oplus \Delta'). \end{aligned}$$

  Therefore, we must have $Y(\mathbf{t}, P) \oplus Y(\mathbf{t}', P) \neq A(\mathbf{t}, P) \oplus A(\mathbf{t}', P)$, i.e. $y_4(\mathbf{t}, P) \neq y_4(\mathbf{t}', P)$;

$\underline{\text{Case 2:}}$ for $(\mathbf{t}, \mathbf{t}')$, $x_1(\mathbf{t}) = x_1(\mathbf{t}')$, yet $x_2(\mathbf{t}, P) \neq x_2(\mathbf{t}', P)$. Then by ¬(C-21) we immediately have $x_3(\mathbf{t}, P) \neq x_3(\mathbf{t}', P)$ and $y_4(\mathbf{t}, P) \neq y_4(\mathbf{t}', P)$;

$\underline{\text{Case 3:}}$ for $(\mathbf{t}, \mathbf{t}')$, $x_1(\mathbf{t}) \neq x_1(\mathbf{t}')$. This implies $x_2(\mathbf{t}, P) \neq x_2(\mathbf{t}', P)$ by ¬(C-11), and further $x_3(\mathbf{t}, P) \neq x_3(\mathbf{t}', P)$ and $y_4(\mathbf{t}, P) \neq y_4(\mathbf{t}', P)$ by ¬(C-21).

So $\left|\{x_3(\mathbf{t}, P) \mid \mathbf{t} \in \mathcal{Q}_E\}\right| = \left|\{y_4(\mathbf{t}, P) \mid \mathbf{t} \in \mathcal{Q}_E\}\right| = q_e$. The argument for $x_4(\mathbf{t}, P)$ and $y_3(\mathbf{t}, P)$ is similar by symmetry (utilizing the property $M_4 \cdot \Delta \neq M_6 \cdot \Delta$ for $\Delta \neq 0$ given in Definition 3 and the condition ¬(C-13)). By all the above discussion and (56), for any good τ, when $q_f + 4q_e \leq N/2$, via a counting similar to that in the previous section we reach

$$\begin{aligned} \frac{\Pr_{re}(\tau)}{\Pr_{id}(\tau)} \geq& \frac{\Pr[P \vdash \mathcal{Q}_P]}{N^{2q_e}} \left(1 - \frac{6q_e q_f + 27q_e^2 + 2q_e}{N - q_f - 4q_e}\right) \Big/ \frac{\Pr[P \vdash \mathcal{Q}_P]}{(N^2 - q_e)^{q_e}} \\ \geq& \left(1 - \frac{12q_e q_f + 54q_e^2 + 4q_e}{N}\right) \left(\frac{N^2 - q_e}{N^2}\right)^{q_e} \\ \geq& 1 - \frac{12q_e q_f + 55q_e^2 + 4q_e}{N}. \end{aligned}$$

Gathering this and (39) and Lemma 1 yields Theorem 5.

C. When f=F is a Random Function

For the proof, we need the following modifications on the proof for 6-round $\mathsf{KAFw}^{P,(w,\gamma)}$:

(1) in Definition 4 (bad transcripts), (B-3) is only used for proving $\forall (\mathbf{t}, \mathbf{t}') : y_3(\mathbf{t}, F) \neq y_3(\mathbf{t}', F), y_4(\mathbf{t}, F) \neq y_4(\mathbf{t}', F)$, cf. page 17. We thus drop it and obtain

$$\Pr[T_{id} \in \mathcal{T}_{bad}] \leq \frac{2q_e q_f + q_e^2}{N}; \tag{57}$$

(2) in the definition of $\mathsf{B1}(F)$, the two conditions $X(\mathbf{t}, F) \oplus X(\mathbf{t}', F) = M_6 \cdot (\Delta \oplus \Delta')$ in (C-11) and $A(\mathbf{t}, F) \oplus$

$A(\mathbf{t}', F) = M_1 \cdot (\Delta \oplus \Delta')$ in (C-13) are only used for proving $\forall(\mathbf{t}, \mathbf{t}') : y_3(\mathbf{t}, F) \neq y_3(\mathbf{t}', F), y_4(\mathbf{t}, F) \neq y_4(\mathbf{t}', F)$, cf. page 17. In addition, (C-15) is only used for proving $\forall(\mathbf{t}, \mathbf{t}') : y_2(\mathbf{t}, F) \neq y_4(\mathbf{t}', F), y_3(\mathbf{t}, F) \neq y_5(\mathbf{t}', F)$, cf. page 16. We thus drop them, which decreases $\Pr[\mathsf{B1}(F)]$ to $\frac{2q_eq_f+6q_e^2}{N}$;

(3) in the definition of $\mathsf{B2}(F)$, we drop
- $y_4(\mathbf{t}, F) = y_4(\mathbf{t}', F)$ in (C-21), and
- $\exists \mathbf{t}, \mathbf{t}' : y_4(\mathbf{t}, F) \in \mathcal{Y}(\tau)$ or $y_4(\mathbf{t}, F) \in \{y_1(\mathbf{t}', F), y_2(\mathbf{t}', F), y_5(\mathbf{t}', F), y_6(\mathbf{t}', F)\}$ in (C-22), and
- $y_3(\mathbf{t}, F) = y_3(\mathbf{t}', F)$ in (C-23), and
- $\exists \mathbf{t}, \mathbf{t}' : y_3(\mathbf{t}, F) \in \mathcal{Y}(\tau)$ or $y_3(\mathbf{t}, F) \in \{y_1(\mathbf{t}', F), y_2(\mathbf{t}', F), y_4(\mathbf{t}', F), y_5(\mathbf{t}', F), y_6(\mathbf{t}', F)\}$ in (C-24).

These decrease $\Pr[\mathsf{B2}(F)]$ to $\frac{2q_eq_f+10q_e^2}{N}$.

Therefore,

$$\frac{\Pr_{re}(\tau)}{\Pr_{id}(\tau)} \geq 1 - \frac{4q_eq_f + 16q_e^2}{N} - \frac{q_e^2}{N^2}. \tag{58}$$

Gathering (57) and (58) gives rise to the following Theorem.

Theorem 6 *For the 6-round, random function-based* $\mathsf{KAFw}^{F,(w,\gamma)}$ *cipher with a good key-schedule* (w, γ) *as specified in Definition 3, it holds*

$$\mathbf{Adv}^{\oplus\text{-rka}}_{\mathsf{KAFw}^{F,(w,\gamma)}_k}(q_f, q_e) \leq \frac{6q_eq_f + 18q_e^2}{N}.$$

V. Deriving Results on KAF and KAFv Ciphers

A. Results on KAF

Since KAF ciphers are KAFw ciphers with no whitening keys, results on the latter can be immediately transposed to the former. In detail, denote by $\gamma = (\gamma_1, \ldots, \gamma_t)$ a t-round key-schedule of KAF, then with the function Ψ^f_k defined by Eq. (7) in section II, the t-round $\mathsf{KAF}^{f,\gamma}$ cipher is defined as

$$\mathsf{KAF}^{f,\gamma}_k(W) = \Psi^f_{\gamma_t(k)} \circ \ldots \circ \Psi^f_{\gamma_1(k)}(W).$$

Setting $\varphi_i = \gamma_i$ for $i = 1, 4, 6$ in Definitions 1 and 3 (good key-schedules for $\mathsf{KAFw}^{f,(w,\gamma)}$) yields the corollary.

Corollary 1 *A 4-round non-linear key-schedule* $\gamma = (\gamma_1, \gamma_2, \gamma_3, \gamma_4)$ *is good for* $\mathsf{KAF}^{f,\gamma}$*, if* $\varphi_1 = \gamma_1$ *and* $\varphi_4 = \gamma_4$ *satisfy the uniformness and AXU conditions defined in Definition 1.*

A 6-round affine key-schedule $\gamma = (\gamma_1, \ldots, \gamma_6)$*, where* $\gamma_i(k) = M_i \cdot k \oplus C_i$*, is good for* $\mathsf{KAF}^{f,\gamma}$*, if:*

(1) γ_1, γ_6, *and* $\gamma_1 \oplus \gamma_6$ *are bijective maps of* $\{0,1\}^n$*, and*
(2) *for any* $\Delta \neq 0$, $M_1 \cdot \Delta \neq M_3 \cdot \Delta$, $M_4 \cdot \Delta \neq M_6 \cdot \Delta$.

With such good key-schedules, 4- and 6-round idealized $\mathsf{KAF}^{P,\gamma}$ *and* $\mathsf{KAF}^{F,\gamma}$ *ensure the same security bounds as described in Theorems 1, 2, 5, and 6.*

For affine schedules, both Corollary 1 and Definition 3 require the "inner" KDFs γ_3 and γ_4 to fulfill some conditions, i.e. $M_1 \cdot \Delta \neq M_3 \cdot \Delta$ and $M_4 \cdot \Delta \neq M_6 \cdot \Delta$. This means for KAF instances that suffer from $\oplus$-RKAs, adding whitening keys derived by affine KDFs would probably *not* be beneficial for RKA security (since the "inner" KDFs remain "bad"). For example, consider the attempt to prevent DES from the complementation property via using a DESX-like [76] structure $\mathrm{DESX}^*_k(M) = k \oplus \mathrm{DES}_{k'}(k \oplus M)$, where the 56-bit DES key k' are 56 bits chosen from the 64-bit master-key k. It can be seen while $\mathrm{DESX}^*_k(\overline{M}) = \overline{\mathrm{DESX}^*_k(M)}$ does not necessarily hold, the $\mathrm{DESX}^*_k(M)$ still suffers from a (less trivial) complementation-based property $\mathrm{DESX}^*_k(M) = \mathrm{DESX}^*_k(M)$.

B. Results on KAFv

The transition to KAFv is a bit more complicated. Formally, KAFv relies on the following round transformation

$$\widetilde{\Psi}^f_k(W_L \| W_R) = W_R \| W_L \oplus \underline{f(W_R) \oplus k}. \tag{59}$$

With this, a t-round KAFv needs $t + 2$ sub-keys. To make a clear distinction from the notations for KAF, we denote by $\gamma^* = (\gamma^*_0, \gamma^*_1, \ldots, \gamma^*_t, \gamma^*_{t+1})$ a t-round key-schedule for KAFv: $\gamma^*_1, \ldots, \gamma^*_t$ for the t round-keys, while γ^*_0 and γ^*_{t+1} for the two whitening keys. Then the entire $\mathsf{KAFv}^{f,\gamma^*}$ variant is

$$\mathsf{KAFv}^{f,\gamma^*}_k(W) = (\gamma^*_{t+1}(k) \| 0) \oplus \widetilde{\Psi}^f_{\gamma^*_t(k)} \circ \ldots \circ \widetilde{\Psi}^f_{\gamma^*_1(k)}\big((0 \| \gamma^*_0(k)) \oplus W\big).$$

For $\mathsf{KAFv}^{f,\gamma^*}$ we have

Corollary 2 *A 4-round non-linear key-schedule* $\gamma^* = (\gamma^*_0, \ldots, \gamma^*_5)$ *is good for* $\mathsf{KAFv}^{f,\gamma^*}$*, if* $\varphi_1 = \gamma^*_0$ *and* $\varphi_4 = \gamma^*_5$ *satisfy the two conditions defined in Definition 1.*

A 6-round affine key-schedule $\gamma^* = (\gamma^*_0, \ldots, \gamma^*_7)$*, where* $\gamma^*_i(k) = M^*_i \cdot k \oplus C^*_i$*, is good for* $\mathsf{KAFv}^{f,\gamma^*}$*, if:*

(1) γ^*_0, γ^*_7, *and* $\gamma^*_0 \oplus \gamma^*_7$ *are bijective maps of* $\{0,1\}^n$*, and*
(2) *for any* $\Delta \neq 0$, $\underline{M^*_2 \cdot \Delta \neq 0,\ M^*_5 \cdot \Delta \neq 0}$.

With such good key-schedules, 4- and 6-round idealized $\mathsf{KAFv}^{P,\gamma^*}$ *and* $\mathsf{KAFv}^{F,\gamma^*}$ *ensure the same security bounds as described in Theorems 1, 2, 5, and 6.*

Proof: For a t-round KAFv key-schedule γ^*, define a t-round KAFw schedule (w, γ) as follows:
- $\gamma_{2\ell+1} = \bigoplus_{i=0}^{\ell} \gamma^*_{2i}$, where $\ell = 0, \ldots, \lfloor \frac{t-1}{2} \rfloor$, and
- $\gamma_{2\ell+2} = \bigoplus_{i=0}^{\ell} \gamma^*_{2i+1}$, where $\ell = 0, \ldots, \lfloor \frac{t-2}{2} \rfloor$, and
- $w_2 = \gamma_t \oplus \gamma^*_{t+1}$, $w_3 = \gamma_{t-1} \oplus \gamma^*_t$, while $w_0(k) = w_1(k) = 0$.

Then it can be seen a t-round KAFv with the key-schedule γ^* is a KAFw instance with (w, γ), i.e.

$$\mathsf{KAFv}^{f,\gamma^*}_k(W) = \mathsf{KAFw}^{f,(w,\gamma)}_k(W). \tag{60}$$

Concretely, the 4-round $\mathsf{KAFv}^{f,\gamma^*}$ schedule $(\gamma^*_0, \ldots, \gamma^*_5)$ corresponds to the 4-round $\mathsf{KAFw}^{f,(w,\gamma)}$ schedule (w, γ) with $w_0(k) = w_1(k) = 0$, $\gamma_1 = \gamma^*_0$ (thus $\varphi_1 = w_1 \oplus \gamma_1 = \gamma^*_0$), and $\varphi_4 = \gamma_4 \oplus w_2 = \gamma^*_5$. The first half of the corollary thus follows from Definition 1.

The 6-round affine key-schedule $\gamma^* = (\gamma^*_0, \ldots, \gamma^*_7)$ corresponds to the 6-round affine schedule (w, γ), in which $\varphi_1 = w_1 \oplus \gamma_1 = \gamma^*_0$, $\varphi_6 = \gamma_6 \oplus w_2 = \gamma^*_7$, and:

(1) $\gamma_1 \oplus \gamma_3 = \gamma^*_2$, and thus $M^*_2 = M_1 \oplus M_3$;
(2) $\gamma_4 \oplus \gamma_6 = \gamma^*_5$, and thus $M^*_5 = M_4 \oplus M_6$.

Therefore, the second half follows from Definition 3. □

We believe the requirements on schedules of $\mathsf{KAFv}^{f,\gamma^*}$ are more relaxed than those required by $\mathsf{KAF}^{f,\gamma}$ (Corollary 1), since its condition (2) only requires to carefully design γ_2 and γ_5, without considering the more complicated interactions between different round-KDFs (comparing with the second condition in Definition 3). In particular, when designing affine key-schedules in practice, one tends to choose *invertible matrices* for $M_0, \ldots, M_{t+1}$ in order to ensure the largest possible amount of entropy in the round-keys, e.g. the bit-permutation-based key-schedules in DES. In this case, condition (2) is naturally satisfied, yet the second condition in Definition 3 may not be satisfied! (And when $M_1 \cdot k$ and $M_3 \cdot k$ define two bit-permutations, the latter condition is indeed violated since $M_1 \cdot \Delta = M_3 \cdot \Delta = \Delta$ for $\Delta = 0\text{xFF}\ldots\text{FF}$. This matches that DES is vulnerable to complementing attacks.)

Finally, we remark that whitening keys play a crucial role in the transformation Eq. (60). This means KAFv—as well as the Lucifer-like model—cannot be precisely captured by KAF, the variant of KAFw without whitening keys.

VI. Towards Minimalism

To maximize the efficiency of the resulted permutation modes, we derive theoretically "minimal" constructions. We focus on $\mathsf{KAF}^{P,\gamma}$ as it's of the most general interest, and it's wlog, since minimal $\mathsf{KAFw}^{P,(w,\gamma)}$ and $\mathsf{KAFv}^{P,\gamma^*}$ schemes can be easily derived similarly.

First, for the 4-round $\mathsf{KAF}^{P,\gamma}$, $\gamma_1(k) = \mathbf{M}_1 \otimes k \oplus k^3$, $\gamma_2(k) = \gamma_3(k) = 0$, and $\gamma_4(k) = \mathbf{M}_4 \otimes k \oplus k^3$ is a group of good choices, where $\mathbf{M}_1 \neq \mathbf{M}_4$ are two non-zero constants in $\{0,1\}^n$, and $\otimes$ denotes multiplications taken over the finite field $\mathbb{F}_{2^n}$. With this choice, it can be seen the three parameters mentioned in Definition 1 are such that $\delta_1 \leq 3/N$, $\delta_2 \leq 2/N$, and $\delta_3 \leq 2/N$, and the concrete advantage bound is a classical birthday one $\frac{14q_eq_f+31q_e^2+4q_e}{N}$.

Our choice of γ_1 and γ_4 is motivated by [77]. On the other hand, since no requirement is placed on γ_2 and γ_3 (see Corollary 1 or Definition 1), they are completely absent: this matches the existing result that the two middle round-functions of 4-round Feistel do *not* need to be secret/"protected" by round-keys [78]. This $\mathsf{KAF}^{P,\gamma}$ variant seems "minimal" in the sense that removing any component harms security: reducing rounds ruins CCA security, choosing $\mathbf{M}_1 = \mathbf{M}_4$ introduces the weakness $\mathsf{KAF}_k^{P,\gamma}(LR) = ST \Leftrightarrow \mathsf{KAF}_k^{P,\gamma}(TS) = RL$ and allows trivially distinguishing, while reducing the non-linearity of KDFs would introduce related-key differentials with higher probability and compromise the concrete security.

Second, for 6-round $\mathsf{KAF}^{P,\gamma}$, using a linear orthomorphism π, the key-schedule $k \mapsto (k,0,0,0,0,\pi(k))$ is sufficient. It may be quite hard to believe many carefully designed sophisticated key-schedules (e.g. DES) are insufficient to prevent complementing attacks, while such an exotic design should be good. The reason is that the absence of the 3rd and 4th round-keys incidently prevents the complementation properties.

We stress that the key-schedule instances with many "blanks" mentioned here *are for theoretically minimalism rather than for general purpose Feistel ciphers.* For the latter purpose, one could (actually, *should*) "fill in the blanks". For example, using $\pi(k_L\|k_R) = k_R\|k_L \oplus k_R$ mentioned in the Introduction, it can be seen $k \mapsto (k,k,\pi(k),k,k,\pi(k))$ is a good key-schedule for 6-round $\mathsf{KAF}^{P,\gamma}$.

1) **A Tweakable KAC**: Finally, in 4-round $\mathsf{KAFw}^{f,(w,\gamma)}$, we can set $w_1(k) = \mathbf{M}_1 \otimes k \oplus k^3$ and $w_2(k) = \mathbf{M}_4 \otimes k \oplus k^3$, while omit all the other sub-keys. This results in a variant of the 1-round tweakable KAC of [21], with the permutation instantiated by a 4-round keyless Feistel network.

VII. Conclusion

We've studied provable security of key-alternating Feistel/Feistel-2 variants against $\oplus$-induced related-key attacks, which better model the reality of Feistel blockciphers. Assuming key-schedules being non-linear or purely affine, we identify (different) conditions on the key-schedules that are sufficient for a birthday-type security up to $2^{n/2}$ queries. The results and implications make a step towards understanding the behaviors of existing different Feistel cipher structures, and offer new insights.

Appendix A
Lucifer-like Model and KAFv

The Lucifer-like model Luc also relies on the round transformation $\widetilde{\Psi}_k^f$ in Eq. (59). With this, a t-round Luc model built upon t round-functions $f_1, \ldots, f_t$ uses t round-keys $k_1, \ldots, k_t$, and is

$$\mathsf{Luc}_{k_1,\ldots,k_t}^{f_1,\ldots,f_t}(W) = \widetilde{\Psi}_{\gamma_t^*(k)}^{f_t} \circ \ldots \circ \widetilde{\Psi}_{\gamma_1^*(k)}^{f_1}(W). \tag{61}$$

From section V-B we know a $(t$–$2)$-round KAFv uses $t-2$ round-functions $f_1, \ldots, f_{t-2}$ and t sub-keys $k_1, \ldots, k_t$:

$$\mathsf{KAFv}_{k_1,\ldots,k_t}^{f_1,\ldots,f_{t-2}}(W) = (k_t\|0) \oplus \widetilde{\Psi}_{k_{t-1}}^{f_{t-2}} \circ \ldots \circ \widetilde{\Psi}_{k_2}^{f_1}\big((0\|k_1) \oplus W\big).$$

By these, it's not hard to see when $t \geq 2$,

$$\mathsf{Luc}_{k_1,\ldots,k_t}^{f_1,\ldots,f_t}(W) = \widetilde{\Psi}_0^{f_t} \circ \mathsf{KAFv}_{k_1,\ldots,k_t}^{f_2,\ldots,f_{t-1}} \circ \widetilde{\Psi}_0^{f_1}(W),$$

where $\widetilde{\Psi}_0^{f_1}$ and $\widetilde{\Psi}_0^{f_t}$ are two keyless permutations that can be freely evaluated by the adversary. It can be seen within a large range, any CCA attack $\mathcal{A}$ on $(t$–$2)$-round KAFv can be turned into a CCA attack $\mathcal{A}'$ on t-round Luc: whenever $\mathcal{A}$ queries $\mathsf{RK}[\mathsf{KAFv}_k^{f_2,\ldots,f_{t-1}}](\Delta, LR)$, $\mathcal{A}'$ queries $\mathsf{RK}[\mathsf{Luc}_k^{f_1,\ldots,f_t}](\Delta, (\widetilde{\Psi}_0^{f_1})^{-1}(LR))$; whenever $\mathcal{A}$ queries $\mathsf{RK}[\mathsf{KAFv}_k^{f_2,\ldots,f_{t-1}}]^{-1}(\Delta, ST)$, $\mathcal{A}'$ queries $\mathsf{RK}[\mathsf{Luc}_k^{f_1,\ldots,f_t}]^{-1}(\Delta, \widetilde{\Psi}_0^{f_t}(ST))$. The formal characterization is out of the scope of this paper.

Appendix B
Complementing Attacks

We don't claim novelty for these attacks, see [36]. We just include them to help understanding our provable results. We focus on KAFw variants with key-schedules that do not satisfy condition (2) in Definition 3. We first brief how to break more than 4 rounds, then describe the attack against any number of rounds for "bad enough" key-schedules.

On 5 Rounds. Consider a 5-round key-schedule (w,γ), where $w = (w_0, w_1, w_2, w_3)$ and $\gamma = (\gamma_1, \gamma_2, \gamma_3, \gamma_4, \gamma_5)$, and γ is

such that $M_1 \cdot \Delta = M_3 \cdot \Delta$ for a non-zero value Δ. Then there exists a 1-round related-key differential for the 3rd round, i.e.

$$\Pr\left(M_2 \cdot \Delta \| M_1 \cdot \Delta \xrightarrow[\Delta]{\Psi^{f_3}_{\gamma_3(k)}} M_1 \cdot \Delta \| M_2 \cdot \Delta\right) = 1.$$

Concatenating this differential with the mentioned 2-round related-key differential Eq. (32) gives a 3-round differential:

$$\Pr\left(\nabla_1 \| \nabla_2 \xrightarrow[\Delta]{\Psi^{f_3}_{\gamma_3(k)} \circ \Psi^{f_2}_{\gamma_2(k)} \circ \Psi^{f_1}_{\gamma_1(k)} \circ \mathsf{XOR}_{wk_{in}}} M_1 \cdot \Delta \| M_2 \cdot \Delta\right) = 1,$$

where $\nabla_1 = (M_0^{(w)} \oplus M_2) \cdot \Delta$, $\nabla_2 = (M_1^{(w)} \oplus M_1) \cdot \Delta$, and $wk_{in} = w_0(k) \| w_1(k)$. Further concatenating this differential with the 2-round related-key differential Eq. (38) yields a 5-round related-key boomerang distinguisher, which allows distinguishing 5 rounds with 4 queries.

On Any Rounds. Consider a $2t$-round schedule (w, γ) with $w = (w_0, w_1, w_2, w_3)$ and $\gamma = (\gamma_1, \gamma_2, \ldots, \gamma_{2t})$, and γ satisfies: it's easy to derive $\Delta \neq 0$ such that

- $\Delta_1 = M_1 \cdot \Delta = M_3 \cdot \Delta = M_5 \cdot \Delta = \ldots = M_{2t-1} \cdot \Delta$, and
- $\Delta_2 = M_2 \cdot \Delta = M_4 \cdot \Delta = M_6 \cdot \Delta = \ldots = M_{2t} \cdot \Delta$.

Then it can be seen there exists related-key differentials with any number of rounds:

$$\Pr\Big(\nabla_1 \| \nabla_2 \xrightarrow[\Delta]{\Psi^{f_1}_{\gamma_1(k)} \circ \mathsf{XOR}_{wk_{in}}} \Delta_1 \| \Delta_2 \xrightarrow[\Delta]{\Psi^{f_2}_{\gamma_2(k)}} \Delta_2 \| \Delta_1 \xrightarrow[\Delta]{\Psi^{f_3}_{\gamma_3(k)}} \cdots \xrightarrow[\Delta]{\mathsf{XOR}_{wk_{out}} \circ \Psi^{f_t}_{\gamma_t(k)}} \delta\Big) = 1,$$

where $\nabla_1 = (M_0^{(w)} \oplus M_2) \cdot \Delta$, $\nabla_2 = (M_1^{(w)} \oplus M_1) \cdot \Delta$, $wk_{out} = w_2(k) \| w_3(k)$, the output difference $\delta = \Delta_2 \oplus M_2^{(w)} \cdot \Delta \| \Delta_1 \oplus M_3^{(w)} \cdot \Delta$ when t is even, and $\delta = \Delta_1 \oplus M_3^{(w)} \cdot \Delta \| \Delta_2 \oplus M_2^{(w)} \cdot \Delta$ otherwise. This allows distinguishing any t rounds with 2 queries. To save space we omit detailed descriptions of these two (innovel) variants of complementing attacks.

Acknowledgements

I'd like to thank all the five anonymous reviewers of IEEE TIT and CRYPTO 2018 for carefully reading, identifying bugs and typos, supplying invaluable comments that significantly refine the presentations, and pointing the insights in section VI-1 to me. As a post-doc paid by François-Xavier Standaert by the ERC project SWORD (724725), I sincerely appreciate him for allowing (and encouraging) to complete this work.

References

[1] H. Feistel, W. A. Notz, and J. L. Smith, "Some Cryptographic Techniques for Machine-to-Machine Data Communications," *Proceedings of the IEEE*, vol. 63, no. 11, pp. 1545–1554, Nov 1975.

[2] N. B. of Standards, "Data Encryption Standard (DES)," *Federal Information Processing Standards Publication 46*, 1977.

[3] A. Sorkin, "Lucifer, a Cryptographic Algorithm," *Cryptologia*, vol. 8, no. 1, pp. 22–42, 1984.

[4] "Government Committee of the USSR for Standards. GOST, Gosudarstvennyi Standard 28147-89, Cryptographic Protection for Data Processing Systems," 1989.

[5] R. Beaulieu, D. Shors, J. Smith, S. Treatman-Clark, B. Weeks, and L. Wingers, "The SIMON and SPECK Families of Lightweight Block Ciphers," Cryptology ePrint Archive, Report 2013/404, 2013, https://eprint.iacr.org/2013/404.pdf.

[6] J. Patarin, "Security of Random Feistel Schemes with 5 or More Rounds," in *CRYPTO 2004*, ser. LNCS, M. Franklin, Ed. Springer Berlin Heidelberg, 2004, vol. 3152, pp. 106–122.

[7] M. G. Luby and C. Rackoff, "How to Construct Pseudorandom Permutations from Pseudorandom Functions," *SIAM Journal on Computing*, vol. 17, no. 2, pp. 373–386, 1988.

[8] V. T. Hoang and P. Rogaway, "On Generalized Feistel Networks," in *CRYPTO 2010*, ser. LNCS, T. Rabin, Ed. Springer Berlin Heidelberg, 2010, vol. 6223, pp. 613–630.

[9] R. Lampe and Y. Seurin, "Security Analysis of Key-Alternating Feistel Ciphers," in *FSE 2014*, ser. LNCS, C. Cid and C. Rechberger, Eds. Springer Berlin Heidelberg, 2014, vol. 8540, pp. 243–264.

[10] M. Barbosa and P. Farshim, "The Related-Key Analysis of Feistel Constructions," in *FSE 2014*, ser. LNCS, C. Cid and C. Rechberger, Eds. Springer Berlin Heidelberg, 2014, vol. 8540, pp. 265–284.

[11] J.-S. Coron, T. Holenstein, R. Künzler, J. Patarin, Y. Seurin, and S. Tessaro, "How to Build an Ideal Cipher: The Indifferentiability of the Feistel Construction," *Journal of Cryptology*, vol. 29, no. 1, pp. 61–114, 2016.

[12] A. Bogdanov, L. R. Knudsen, G. Leander, F.-X. Standaert, J. Steinberger, and E. Tischhauser, "Key-Alternating Ciphers in a Provable Setting: Encryption Using a Small Number of Public Permutations," in *EUROCRYPT 2012*, ser. LNCS, D. Pointcheval and T. Johansson, Eds. Springer Berlin Heidelberg, 2012, vol. 7237, pp. 45–62.

[13] S. Chen and J. Steinberger, "Tight Security Bounds for Key-Alternating Ciphers," in *EUROCRYPT 2014*, ser. LNCS, P. Q. Nguyen and E. Oswald, Eds. Springer Berlin Heidelberg, 2014, vol. 8441, pp. 327–350.

[14] V. T. Hoang and S. Tessaro, "Key-Alternating Ciphers and Key-Length Extension: Exact Bounds and Multi-user Security," in *CRYPTO 2016, Part I*, ser. LNCS, M. Robshaw and J. Katz, Eds. Springer Berlin Heidelberg, 2016, vol. 9814, pp. 3–32.

[15] Y. Dai, Y. Seurin, J. Steinberger, and A. Thiruvengadam, "Indifferentiability of Iterated Even-Mansour Ciphers with Non-idealized Key-Schedules: Five Rounds Are Necessary and Sufficient," in *CRYPTO 2017, Part III*, ser. LNCS, J. Katz and H. Shacham, Eds. Springer Berlin Heidelberg, 2017, vol. 10403, pp. 524–555.

[16] E. Biham, "New Types of Cryptanalytic Attacks Using Related Keys," *Journal of Cryptology*, vol. 7, no. 4, pp. 229–246, 1994.

[17] L. R. Knudsen, "Cryptanalysis of LOK191," in *AUSCRYPT '92*, ser. LNCS, J. Seberry and Y. Zheng, Eds. Springer Berlin Heidelberg, 1992, vol. 718, pp. 196–208.

[18] M. Bellare and T. Kohno, "A Theoretical Treatment of Related-Key Attacks: RKA-PRPs, RKA-PRFs, and Applications," in *EUROCRYPT 2003*, ser. LNCS, E. Biham, Ed. Springer Berlin Heidelberg, 2003, vol. 2656, pp. 491–506.

[19] T. Iwata and T. Kohno, "New Security Proofs for the 3GPP Confidentiality and Integrity Algorithms," in *FSE 2004*, ser. LNCS, B. Roy and W. Meier, Eds. Springer Berlin Heidelberg, 2004, vol. 3017, pp. 427–445.

[20] R. J. Anderson and M. G. Kuhn, "Low Cost Attacks on Tamper Resistant Devices," in *Security Protocols – '97*, ser. LNCS, B. Christianson, B. Crispo, T. M. A. Lomas, and M. Roe, Eds., vol. 1361, 1997, pp. 125–136.

[21] B. Cogliati and Y. Seurin, "On the Provable Security of the Iterated Even-Mansour Cipher Against Related-Key and Chosen-Key Attacks," in *EUROCRYPT 2015, Part I*, ser. LNCS, E. Oswald and M. Fischlin, Eds. Springer Berlin Heidelberg, 2015, vol. 9056, pp. 584–613.

[22] D. Goldenberg and M. Liskov, "On Related-Secret Pseudorandomness," in *TCC 2010*, ser. LNCS, D. Micciancio, Ed. Springer Berlin Heidelberg, 2010, vol. 5978, pp. 255–272.

[23] J. Kim, S. Hong, B. Preneel, E. Biham, O. Dunkelman, and N. Keller, "Related-Key Boomerang and Rectangle Attacks: Theory and Experimental Analysis," *IEEE Transactions on Information Theory*, vol. 58, no. 7, pp. 4948–4966, July 2012.

[24] A. Biryukov and D. Khovratovich, "Related-Key Cryptanalysis of the Full AES-192 and AES-256," in *ASIACRYPT 2009*, ser. LNCS, M. Matsui, Ed. Springer Berlin Heidelberg, 2009, vol. 5912, pp. 1–18.

[25] E. Biham, O. Dunkelman, and N. Keller, "Related-Key Boomerang and Rectangle Attacks," in *EUROCRYPT 2005*, ser. LNCS, R. Cramer, Ed. Springer Berlin Heidelberg, 2005, vol. 3494, pp. 507–525.

[26] O. Dunkelman, N. Keller, and A. Shamir, "A Practical-Time Related-Key Attack on the KASUMI Cryptosystem Used in GSM and 3G Telephony," *Journal of Cryptology*, vol. 27, no. 4, pp. 824–849, 2014.

[27] L. R. Knudsen and T. Kohno, "Analysis of RMAC," in *FSE 2003*, ser. LNCS, T. Johansson, Ed. Springer Berlin Heidelberg, 2003, vol. 2887, pp. 182–191.

[28] A. Biryukov, O. Dunkelman, N. Keller, D. Khovratovich, and A. Shamir, "Key Recovery Attacks of Practical Complexity on AES-256 Variants with up to 10 Rounds," in *EUROCRYPT 2010*, ser. LNCS, H. Gilbert, Ed. Springer Berlin Heidelberg, 2010, vol. 6110, pp. 299–319.

[29] P. Farshim and G. Procter, "The Related-Key Security of Iterated Even-Mansour Ciphers," in *FSE 2015*, ser. LNCS, G. Leander, Ed. Springer Berlin Heidelberg, 2015, vol. 9054, pp. 342–363.

[30] B. Mennink, "XPX: Generalized Tweakable Even-Mansour with Improved Security Guarantees," in *CRYPTO 2016, Part I*, ser. LNCS, M. Robshaw and J. Katz, Eds. Springer Berlin Heidelberg, 2016, vol. 9814, pp. 64–94.

[31] M. E. Hellman, R. Merkle, R. Schroeppel, W. Diffie, S. Pohlig, and P. Schweitzer, "Results of an Initial Attempt to Cryptanalyze the NBS Data Encryption Standard," Technical report, Stanford University, USA, 1976.

[32] W. C. Barker, *Recommendation for the triple data encryption algorithm (TDEA) block cipher*. US Department of Commerce, Technology Administration, National Institute of Standards and Technology, 2004.

[33] G. Leander, C. Paar, A. Poschmann, and K. Schramm, "New Lightweight DES Variants," in *FSE 2007*, ser. LNCS, A. Biryukov, Ed. Springer Berlin Heidelberg, 2007, vol. 4593, pp. 196–210.

[34] D. W. Davies, "Some Regular Properties of the 'Data Encryption Standard' Algorithm," in *CRYPTO '82*, D. Chaum, R. L. Rivest, and A. T. Sherman, Eds. Springer Berlin Heidelberg, 1983, pp. 89–96.

[35] Y. Ko, S. Hong, W. Lee, S. Lee, and J.-S. Kang, "Related Key Differential Attacks on 27 Rounds of XTEA and Full-Round GOST," in *FSE 2004*, ser. LNCS, B. Roy and W. Meier, Eds. Springer Berlin Heidelberg, 2004, vol. 3017, pp. 299–316.

[36] A. Biryukov and I. Nikolić, "Complementing Feistel Ciphers," in *FSE 2013*, ser. LNCS, S. Moriai, Ed. Springer Berlin Heidelberg, 2013, pp. 3–18.

[37] C. Bouillaguet, O. Dunkelman, G. Leurent, and P.-A. Fouque, "Another Look at Complementation Properties," in *FSE 2010*, ser. LNCS, S. Hong and T. Iwata, Eds. Springer Berlin Heidelberg, 2010, vol. 6147, pp. 347–364.

[38] C. Guo and D. Lin, "On the Indifferentiability of Key-Alternating Feistel Ciphers with No Key Derivation," in *TCC 2015, Part I*, ser. LNCS, Y. Dodis and J. B. Nielsen, Eds. Springer Berlin Heidelberg, 2015, vol. 9014, pp. 110–133.

[39] M. Liskov, R. L. Rivest, and D. Wagner, "Tweakable Block Ciphers," *Journal of Cryptology*, vol. 24, no. 3, pp. 588–613, 2011.

[40] "Information technology - Security techniques - Lightweight cryptography - Part 2: Block ciphers," ISO/IEC 29192-2, 2012.

[41] T. Isobe and K. Shibutani, "Generic Key Recovery Attack on Feistel Scheme," in *ASIACRYPT 2013, Part I*, ser. LNCS, K. Sako and P. Sarkar, Eds. Springer Berlin Heidelberg, 2013, vol. 8269, pp. 464–485.

[42] H. M. Heys, "Information leakage of Feistel ciphers," *IEEE Transactions on Information Theory*, vol. 47, no. 1, pp. 23–35, Jan 2001.

[43] A. Bar-On, E. Biham, O. Dunkelman, and N. Keller, "Efficient Slide Attacks," *Journal of Cryptology*, Aug 2017.

[44] I. Ben-Aroya and E. Biham, "Differential Cryptanalysis of Lucifer," *Journal of Cryptology*, vol. 9, no. 1, pp. 21–34, Mar 1996. [Online]. Available: https://doi.org/10.1007/BF02254790

[45] B. Schneier, "Description of a New Variable-Length Key, 64-bit Block Cipher (Blowfish)," in *FSE '93*, ser. LNCS, R. Anderson, Ed. Springer Berlin Heidelberg, 1993, vol. 809, pp. 191–204.

[46] D. J. Wheeler and R. M. Needham, "TEA, a Tiny Encryption Algorithm," in *FSE '94*, ser. LNCS, B. Preneel, Ed. Springer Berlin Heidelberg, 1994, vol. 1008, pp. 363–366.

[47] R. M. Needham and D. J. Wheeler, "Tea Extensions," *Report (Cambridge University, Cambridge, UK, 1997) Google Scholar*, 1997.

[48] K. Shibutani, T. Isobe, H. Hiwatari, A. Mitsuda, T. Akishita, and T. Shirai, "*Piccolo*: An Ultra-Lightweight Blockcipher," in *CHES 2011*, ser. LNCS, B. Preneel and T. Takagi, Eds. Springer Berlin Heidelberg, 2011, vol. 6917, pp. 342–357.

[49] R. L. Rivest, "A Description of the RC2™ Encryption Algorithm," File draft-rivest-rc2desc-00.txt available from ftp://ftp.ietf.org/internet-drafts/.

[50] U. Maurer, R. Renner, and C. Holenstein, "Indifferentiability, Impossibility Results on Reductions, and Applications to the Random Oracle Methodology," in *TCC 2004*, ser. LNCS, M. Naor, Ed. Springer Berlin Heidelberg, 2004, vol. 2951, pp. 21–39.

[51] G. Bertonı, J. Daemen, M. Peeters, and G. V. Assche, "The Keccak Reference," Submission to NIST (Round 3), 2011, http://keccak.noekeon.org/Keccak-reference-3.0.pdf.

[52] B. Sadeghiyan and J. Pieprzyk, "A Construction for Super Pseudorandom Permutations from A Single Pseudorandom Function," in *EUROCRYPT '92*, ser. LNCS, R. A. Rueppel, Ed. Springer Berlin Heidelberg, 1992, vol. 658, pp. 267–284.

[53] S. Chen, R. Lampe, J. Lee, Y. Seurin, and J. Steinberger, "Minimizing the Two-Round Even–Mansour Cipher," *Journal of Cryptology*, May 2018.

[54] C. Adams, "The CAST-128 Encryption Algorithm," Tech. Rep.

[55] S. Emami, S. Ling, I. Nikolić, J. Pieprzyk, and H. Wang, "Low Probability Differentials and the Cryptanalysis of Full-Round CLEFIA-128," in *ASIACRYPT 2014, Part I*, ser. LNCS, P. Sarkar and T. Iwata, Eds. Springer Berlin Heidelberg, 2014, vol. 8873, pp. 141–157.

[56] D. Goldenberg, S. Hohenberger, M. Liskov, E. Schwartz, and H. Seyalioglu, "On Tweaking Luby-Rackoff Blockciphers," in *ASIACRYPT 2007*, ser. LNCS, K. Kurosawa, Ed. Springer Berlin Heidelberg, 2007, vol. 4833, pp. 342–356.

[57] S. Gueron and N. Mouha, "Simpira v2: A Family of Efficient Permutations Using the AES Round Function," in *ASIACRYPT 2016, Part I*, ser. LNCS, J. H. Cheon and T. Takagi, Eds. Springer Berlin Heidelberg, 2016, vol. 10031, pp. 95–125.

[58] P. Rogaway and Y. Zhang, "Onion-AE: Foundations of Nested Encryption," *PoPETs*, vol. 2018, no. 2, pp. 85–104, 2018.

[59] P. Sarkar, "Efficient Tweakable Enciphering Schemes From (Block-Wise) Universal Hash Functions," *IEEE Transactions on Information Theory*, vol. 55, no. 10, pp. 4749–4760, Oct 2009.

[60] V. T. Hoang, T. Krovetz, and P. Rogaway, "Robust Authenticated-Encryption AEZ and the Problem That It Solves," in *EUROCRYPT 2015, Part I*, ser. LNCS, E. Oswald and M. Fischlin, Eds., vol. 9056, 2015, pp. 15–44.

[61] D. Dachman-Soled, A. Park, and B. S. Nicolas, "Towards a Characterization of the Related-Key Attack Security of the Iterated Even-Mansour Cipher," Cryptology ePrint Archive, Report 2016/707, 2016, http://eprint.iacr.org/2016/707.pdf.

[62] B. Cogliati, Y. Dodis, J. Katz, J. Lee, J. P. Steinberger, A. Thiruvengadam, and Z. Zhang, "Provable Security of (Tweakable) Block Ciphers Based on Substitution-Permutation Networks," in *CRYPTO 2018, Part I*, 2018, pp. 722–753.

[63] R. Canetti, O. Goldreich, and S. Halevi, "The Random Oracle Methodology, Revisited," *J. ACM*, vol. 51, no. 4, pp. 557–594, Jul. 2004.

[64] K. Kurosawa, "Power of a Public Random Permutation and Its Application to Authenticated Encryption," *IEEE Transactions on Information Theory*, vol. 56, no. 10, pp. 5366–5374, Oct 2010.

[65] G. Bertoni, J. Daemen, M. Peeters, and G. Van Assche, "Sponge functions," in *Ecrypt Hash Workshop 2007*, 2007.

[66] F. Abed, C. Forler, and S. Lucks, "General classification of the authenticated encryption schemes for the CAESAR competition," *Computer Science Review*, vol. 22, pp. 13–26, 2016. [Online]. Available: https://doi.org/10.1016/j.cosrev.2016.07.002

[67] J. Lee and D. Hong, "Collision Resistance of the JH Hash Function," *IEEE Transactions on Information Theory*, vol. 58, no. 3, pp. 1992–1995, March 2012.

[68] J. Lee, "Indifferentiability of the Sum of Random Permutations Toward Optimal Security," *IEEE Transactions on Information Theory*, vol. 63, no. 6, pp. 4050–4054, June 2017.

[69] C. Guo and L. Wang, "Revisiting Key-alternating Feistel Ciphers for Shorter Keys and Multi-user Security," in *ASIACRYPT 2018, Part I*, ser. LNCS, T. Peyrin and S. Galbraith, Eds. Springer Berlin Heidelberg, 2018, vol. 11272, pp. 213–243.

[70] S. Lucks, "Ciphers Secure against Related-Key Attacks," in *FSE 2004*, ser. LNCS, B. Roy and W. Meier, Eds. Springer Berlin Heidelberg, 2004, vol. 3017, pp. 359–370.

[71] S. Tessaro, "Optimally Secure Block Ciphers from Ideal Primitives," in *ASIACRYPT 2015, Part II*, ser. LNCS, T. Iwata and J. H. Cheon, Eds. Springer Berlin Heidelberg, 2015, vol. 9453, pp. 437–462.

[72] M. Nandi, "The Characterization of Luby-Rackoff and Its Optimum Single-Key Variants," in *INDOCRYPT 2010*, ser. LNCS, G. Gong and K. C. Gupta, Eds. Springer Berlin Heidelberg, 2010, vol. 6498, pp. 82–97.

[73] A. Mandal, J. Patarin, and Y. Seurin, "On the Public Indifferentiability and Correlation Intractability of the 6-Round Feistel Construction," in *TCC 2012*, ser. LNCS, R. Cramer, Ed. Springer Berlin Heidelberg, 2012, vol. 7194, pp. 285–302.

[74] J. Daemen and V. Rijmen, "Probability Distributions of Correlation and Differentials in Block Ciphers," *Journal of Mathematical Cryptology*, vol. 1, no. 3, pp. 221–242, 2007.

[75] J. Patarin, "The "Coefficients H" Technique," in *SAC 2008*, ser. LNCS, R. M. Avanzi, L. Keliher, and F. Sica, Eds. Springer Berlin Heidelberg, 2008, vol. 5381, pp. 328–345.
[76] J. Kilian and P. Rogaway, "How to Protect DES Against Exhaustive Key Search (an Analysis of DESX)," *Journal of Cryptology*, vol. 14, no. 1, pp. 17–35, 2001.
[77] P. Wang, Y. Li, L. Zhang, and K. Zheng, "Related-Key Almost Universal Hash Functions: Definitions, Constructions and Applications," in *FSE 2016*, ser. LNCS, G. Leander, Ed. Springer Berlin Heidelberg, 2016, vol. 9783, pp. 514–532.
[78] Z. Ramzan and L. Reyzin, "On the Round Security of Symmetric-Key Cryptographic Primitives," in *CRYPTO 2000*, ser. LNCS, M. Bellare, Ed. Springer Berlin Heidelberg, 2000, vol. 1880, pp. 376–393.

Chun Guo was born in China in 1989. He received his BSc from East China Normal University in 2011 and his PhD from University of Chinese Academy of Sciences in 2017 respectively. His research interests include theoretical aspects of symmetric cryptography such as provable security, generic attacks, and leakage resilience.