Related-Key Analysis of Generalized Feistel Networks with Expanding Round Functions*

Yuqing Zhao[1,2] Wenqi, Yu[1,2], and Chun Guo[1,2(✉)]

[1] School of Cyber Science and Technology, Shandong University, Qingdao, Shandong, China
[2] Key Laboratory of Cryptologic Technology and Information Security of Ministry of Education, Shandong University, Qingdao, Shandong, 266237, China,
[3] State Key Laboratory of Information Security (Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093)
yqzhao@mail.sdu.edu.cn,wenqiyu@mail.sdu.edu.cn,chun.guo@sdu.edu.cn

Abstract. We extend the prior provable related-key security analysis of (generalized) Feistel networks (Barbosa and Farshim, FSE 2014; Yu et al., Inscrypt 2020) to the setting of *expanding round functions*, i.e., n-bit to m-bit round functions with $n < m$. This includes *Expanding Feistel Networks (*EFN*s)* that purely rely on such expanding round functions, and *Alternating Feistel Networks (*AFN*s)* that alternate expanding and contracting round functions. We show that, when two independent keys K_1, K_2 are alternatively used in each round, (a) $2\lceil \frac{m}{n} \rceil + 2$ rounds are sufficient for related-key security of EFNs, and (b) a constant number of 4 rounds are sufficient for related-key security of AFNs. Our results complete the picture of provable related-key security of GFNs, and provide additional theoretical support for the AFN-based NIST format preserving encryption standards FF1 and FF3.

Keywords: Blockcipher · Expanding Feistel Networks · Alternating Feistel Networks · Related-key attack · CCA-security · H-coefficient technique

1 Introduction

Generalized Feistel networks. The well-known Feistel blockciphers, including the Data Encryption Standard (DES) [25], rely on the Feistel permutation $\Psi^F(A, B) := (B, A \oplus F(B))$, where $F : \{0,1\}^n \to \{0,1\}^n$ is a domain-preserving round function. This structure has been generalized along multiple axes, providing much more choices for the involved parameters and possibilities of applications. In particular, the so-called *Contracting Feistel Networks* (CFNs) employ *contracting round functions* $G : \{0,1\}^m \to \{0,1\}^n$, $m > n$ [44], while *Expanding Feistel Networks* (EFNs) employ the opposite *expanding round functions* $F : \{0,1\}^n \to \{0,1\}^m$ [44]. In some cases, the two sorts of round functions are

* Preliminary version will appear at CT-RSA 2021. Yuqing Zhao and Wenqi Yu are co-first authors of the article.

executed in a alternating manner [2,33], yielding *Alternating Feistel Networks* (AFNs). Following [28], these are now known as *generalized Feistel networks*. Well-known blockciphers that follow these Feistel variants include the Chinese standard SMS4 [19] (contracting) and BEAR/LION/LIONESS [2] (alternating). Besides, CFNs have supported full-domain secure encryption schemes [35], while AFNs have been proposed as blockcipher modes-of-operation for format-preserving encryption (FPE) [13,8,14] and adopted by the NIST format-preserving encryption standard FFX [23], in order to encrypt non-binary alphabet [23] or database records [18] into ciphertexts of the same format.

Provable security of Feistel networks and their variants was initiated by Luby and Rackoff [32]. The approach is to model the round functions as pseudorandom functions (PRFs). Via a generic standard-to-ideal reduction, the schemes are turned into networks using secret random round functions, for which *information theoretic indistinguishability* is provable, i.e., no *distinguisher* is able to distinguish the Feistel network from a random permutation on $2n$-bit strings. With this model, Luby and Rackoff proved CCA security for 4-round balanced Feistel networks, and subsequent works extended this direction to refined results [39,28,43,37] or to cover the aforementioned generalized Feistel networks [38,35,2,13,8,33,48,28,41]. It has been proved that CFNs, EFNs, and AFNs could all achieve CCA security up to nearly 2^m adversarial queries [28,45], at the cost of a logarithmic number of rounds. For CFNs and EFNs, m being the domain size of the round function while for AFNs m being the domain size of the input of contracting round function.

Related-key security. The above PRF or secret random function-based security argument assumed the network using a fixed secret key. We will henceforth refer to this as the *Single-Key (SK) setting*. The adversarial model, however, usually violates this assumption. In particular, the *Related-Key Attacks* (RKAs), first identified by Biham [9] and Knudsen [30], consider a setting where an adversary might be able to run a cryptosystem on multiple keys satisfying known or chose relations (due to key update [29,24] or fault injection [3]). Compared to the classical "single-key" setting, the increased adversarial power enables much more effective attacks against quite a number of blockciphers [21,10].

On the other hand, security against RKAs has become a desirable goal, particularly for blockciphers, as it increases the robustness of the primitive and eases its use. In this respect, Bellare and Kohno [7] initiated the theoretical treatment of security under related-key attacks by proposing definitions for RKA secure pseudorandom functions (PRFs) and pseudorandom permutations (PRPs), formalizing the adversarial goal as distinguishing the cipher oracles with related-keys from independent random functions or permutations, and presenting possibility and impossibility results. Since then, follow up works have established various important positive results for provably RKA secure constructions of complicated cryptographic primitives [6,5,1,26]. In particular, Barbosa and Farshim established RKA security for 4 rounds balanced Feistel networks with two master keys K_1 and K_2 alternatively used in each round [5], and Guo established RKA security for the so-called Feistel-2 or key-alternating Feistel ciphers [26].

RKA security of GFNs. GFNs remain far less understood in the RKA model. To our knowledge, this was only partly addressed in [47], which established RKA security for contracting Feistel networks using two keys alternatively. In contrast, the generalized Feistel variants using *expanding round functions* have never been analyzed w.r.t. RKAs. This includes expanding EFNs and alternating AFNs.

As already observed [33,36], expanding round functions are attractive in theory, in the sense that the amount of randomness needed to define an ideal expanding function is less than that of the contracting ones.[4] The shortage is that, information theoretic security is limited by the input size n of the round function, and turns vanishing for small n (8 bits for example). Though, even in this case, provable security is usually viewed as theoretical support for the structure (see e.g., [16]).[5] As such, expanding round functions are still used in practice. For example, EFNs can be made practical via storing truly random expanding functions for small input size n (e.g., 8 bits), as done in the hash function CRUNCH [31]. Meanwhile, as mentioned before, AFNs have been the structure of the NIST format-preserving encryption standards [23]. The contracting round functions are built from AES-CBC, while the expanding are from AES-CTR.

Regarding provable security, the landscape is very subtle. For EFNs, it was shown that $2\lceil\frac{m}{n}\rceil + 4$ rounds suffice for the classical SK CCA security up to $2^{n/2}$ queries (generic attacks have been exhibited in [42,46]). For AFNs, it was shown that $12\lceil\frac{m}{n}\rceil + 6$ rounds suffice for SK CCA security up to $2^{m/2}$ queries, which is birthday bound of the parameter m (m is larger than n). With fewer rounds, provable results were restricted to weaker models such as CPA security (3 rounds [33]) or key recovery security (4 rounds [33,34]).[6] In all, for EFNs and AFNs, while asymptotically optimal bounds have been proved, it remains unclear what's the minimal number of rounds necessary for CCA security.

Our results. As mentioned before, in the regime of RKA security, GFNs with contracting round functions have been studied in [47]. This paper aims to investigate GFNs with expanding round functions to complete the picture.

RKA SECURITY OF $2\lceil\frac{m}{n}\rceil + 2$-ROUND EFN. In detail, we first consider expanding Feistel networks using a keyed round function $F : \mathcal{K} \times \{0,1\}^n \to \{0,1\}^m$, where $m > n$. We first pinpoint the number of rounds that appear sufficient. In this respect, we note that the proof framework for balanced Feistel, contracting Feistel, and Naor-Reingold views the scheme as several middle rounds sandwiched by a number of outer rounds: the outer rounds ensure some sort of full diffusion, while the middle rounds ensure pseudorandomness of the final outputs. This framework has also been used for the RKA security of 3-round Even-Mansour cipher [17]. Following this idea, we identify that the number of expanding Feistel rounds sufficient for full diffusion is $\lceil\frac{m}{n}\rceil$. We also observe

[4] It consumes $n \cdot 2^m$ bits to describe the table of a contracting random function from $\{0,1\}^m$ to $\{0,1\}^n$, while $m \cdot 2^n$ bits for an expanding one from $\{0,1\}^n$ to $\{0,1\}^m$.

[5] For AFN-based modes we might have $n = 128$, and the bound would be meaningful. We hope to see concrete designs.

[6] Although many have mentioned the possibility of CCA security on 4 rounds [33].

that two middle rounds are sufficient as the randomness source. Therefore, we pinpoint $2\lceil \frac{m}{n} \rceil + 2$ as the number of rounds plausible for CCA security. This improves upon the aforementioned *SK CCA* result with $2\lceil \frac{m}{n} \rceil + 4$ rounds [28]. The improvement stems from the fine-grained H-coefficient-based analysis rather than the NCPA(Non-adaptive CPA)-to-CCA transformation used in [28].

The next step is to pinpoint a plausible correlated key assignment—as observed in the context of balanced Feistel networks [7,5], independent round keys actually admit related-key attacks. A natural idea is to alternate two independent keys $K_1, K_2 \in \mathcal{K}$ in each round, as in [5] and in some practical blockciphers [27,4]. Note that an odd number of Feistel rounds with such alternating key assignment yields an (insecure) involution.[7]

Fortunately, the aforementioned number of rounds $2\lceil \frac{m}{n} \rceil + 2$ is *even*. Therefore, we focus on this alternating key assignment, and prove that the $2\lceil \frac{m}{n} \rceil + 2$ rounds are sufficient for the classical birthday security, i.e., for RKA security up to $2^{n/2}$ adversarial queries.

RKA SECURITY OF 4-ROUND AFN. We then consider alternating Feistel networks, in which the odd rounds use contracting $G : \mathcal{K} \times \{0,1\}^m \to \{0,1\}^n$ while the even rounds use expanding $F : \mathcal{K} \times \{0,1\}^n \to \{0,1\}^m$. Somewhat interestingly,—and in contrast to contracting and expanding Feistel networks (see [47] for discussion on the former),—the number of rounds suffice for CCA security in an AFN is always 4, *independent of the ratio* m/n. Briefly, the reason is that AFNs actually behave quite similarly to the classical balanced Feistel networks, except that the domain and range of the round functions are different. The construction of AFN is shown Fig. 2.

To achieve RKA security, again we have to resort to non-independent key assignments. We consider again the aforementioned key assignment. With the above, we prove that the 4-round AFN using round keys (K_1, K_2, K_1, K_2) is RKA secure up to $2^{n/2}$ queries, which is the birthday bound with respect to the parameter n.

For AFN there is another interesting property, i.e., if all the round keys are identical, then an odd number of rounds constitutes an involution (*not* CCA secure), while an even number of rounds is not. As we are trying to establish security for 4 rounds, it seems appealing to employ such identical round keys. Unfortunately, another subtle issue hinders this attempt. In detail, technically, the classical generic standard-to-ideal reduction is unable to handle *two different keyed functions using the same secret key*: the reduction is just unable to simulate the other primitive with the target secret key. On the positive side, this issue can be overcame by using a *tweakable keyed function* that behaves as contracting for tweak input 0 while expanding for tweak 1. For the AFN using such a tweakable keyed function as the round function, the reduction is able to handle the case of identical round keys (it just idealizes all round functions "once for

[7] By this, even number of rounds are likely vulnerable to recent advanced slide attacks [20]. Though, we remark that slide attacks typically require *at least* $2^{n/2}$ complexities [11,12,22,20], and thus do not violate our birthday provable bounds. Seeking for beyond-birthday provable bounds is a promising future direction.

all"). Interestingly, this model appears closer to FF1 and FF3. Our analysis is easily adapted to this 4-round AFN variant, indicating RKA CCA security up to $2^{n/2}$ queries. For clearness, we summarize our new results and relevant existing results in Table 1.

As mentioned before, our results complete the picture of RKA security of generalized Feistel networks. They also provide additional theoretical support for the NIST standards FF1 and FF3. However, we remark important caveats. The concrete parameters involved in FF1 and FF3 are rather small, and our provable bounds (in fact, *any* information theoretic provable bounds) are too weak to be meaningful. FF1 and FF3 are intended to resist attacks with complexity far beyond the information theoretic upper bound. Therefore, the number of rounds have to be determined by cryptanalytic results rather than the provable ones. In fact, recently, FF1 and FF3 have been found insufficient.

We also mention that the blockcipher LIONESS of Anderson and Biham uses 4 independent keys in its two calls to a stream cipher and two calls to a hash function [2]. Our result can be applied to *halve* the amount of keys while *boosting* provable security (i.e., boosting birthday-bound CCA security to birthday-bound RKA CCA security).

Table 1. Provable security results on expanding and alternating Feistel networks. The scheme AFN* is the aforementioned tweakable function-based AFN. The second column lists the security models, where SK is the abbreviation of *Single-Key*. The third column list the number of rounds required by the provable results. The fourth column list the key assignment in use: **Independent** means independent round keys, **Alternating** means (our) alternating two keys, and **Identical** means identical round keys. Parameter $m > n$, m is the output length of the expanding function and the input length of the contracting function. Parameter n is the input length of the expanding function and the output length of the contracting function. The parameter t is an integer and determines the number of rounds.

Scheme	Model	Rounds	Round keys	Security	Ref.
EFN	SK CCA	$2\lceil \frac{m}{n} \rceil + 4$	Independent	$n/2$	[28,45]
EFN	SK CCA	$4t + 2\lceil \frac{m}{n} \rceil + 1$	Independent	$tn/(t+1)$	[45]
EFN	**RKA CCA**	$2\lceil \frac{m}{n} \rceil + 2$	Alternating	$n/2$	Theorem 1
AFN	Key recovery	3	-	-	[33,34]
AFN	SK CPA	3	Independent	$n/2$	[33]
AFN	SK CCA	$12\lceil \frac{m}{n} \rceil + 6$	Independent	$m/2$	[28]
AFN	SK CCA	$(12\lceil \frac{m}{n} \rceil + 2)t + 5$	Independent	$tm/(t+1)$	[45]
AFN	**RKA CCA**	4	Alternating	$n/2$	Theorem 2
AFN*	**RKA CCA**	4	Identical	$n/2$	Corollary 1

Technical insights. The RKA security proofs start with a generic standard-to-ideal reduction replacing the round functions with ideal keyed functions. Then the crux is to analyze the idealized EFN and AFN variants in the RKA setting.

This two-step approach follows [5], and actually appears the common denominator of security proofs of Feistel networks.

For the RKA analysis of the idealized networks, we employ the widely used H-coefficient technique [40,15]. As mentioned before, this step follows the same general paradigm as the H-coefficient-based single-key CCA security analysis (which, however, seems elusive for EFNs and AFNs). Though, the analysis has to consider: (i) the interaction between queries under different related keys (which is specific to the RKA setting), and (ii) the interference between different rounds that are using the same keys (due to the non-independent round keys, which is again crucial for RKA security). These distinguish our results from the relative simple single-key CCA analysis.

Organization. We serve necessary notations and definitions in Sect. 2. After that, we serve the RKA security analysis for EFN in Sect. 3. As the security proof is a bit complicated, we serve the analysis of the simplest setting of 6-round in Appendix A as an instructive example. We then present the analysis for 4-round AFN in Sect. 4. We finally conclude in Sect. 5.

2 Preliminaries

For two bit strings X, Y of any length, we denote by $X\|Y$ their concatenation. For $X \in \{0,1\}^m$, we denote by $X[a,b]$ the string consisting of the $b-a+1$ bits between the a-th position and the b-th position. This means $X = X[1,i]\|X[i+1,m]$ for any $i \in \{1,...,m-1\}$. For example, if $X =$ 0xA5A5 (in hexadecimal form), then $X[1,3] =$ 0x5, while $X[4,16] =$ 0x05A5.

Two of our three results focus on using two independent keys K_1, K_2 in the round functions. In this respect, we denote the master key of the network by $\mathbf{K} = (K_1, K_2) \in \mathcal{K}^2$, i.e., a vector of dimension 2. We denote by $\mathbf{K}[i]$ its i-th coordinate, where $i = 1$ or 2. We further denote by

$$\mathsf{KA}(\mathbf{K}) = (K_{i_1}, ..., K_{i_t})$$

the round key assignment of the network, where $i_1, ..., i_t$ are fixed indices in $\{1,2\}$. For such a vector of round keys $\mathsf{KA}(\mathbf{K})$, we denote by $\mathsf{KA}(\mathbf{K})[j]$ the j-th round key K_{i_j}. Thereby, a related-key derivation function ϕ maps a certain master key $\mathbf{K} = (K_1, K_2)$ to a new master key $\mathbf{K}' = (K_1', K_2')$. We will write $\mathsf{EFN}_{\mathsf{KA}(\mathbf{K})}$ and $\mathsf{AFN}_{\mathsf{KA}(\mathbf{K})}$ for the corresponding construction using the master key $\mathbf{K}$ and the key assignment KA.

For the case $\mathbf{K} = (K_1, K_2)$, we will specially pay attention to the alternating key assignment $\mathsf{Alter}(\mathbf{K}) = (K_1, K_2, K_1, K_2, ...)$. Formally, $\mathsf{Alter}(\mathbf{K}) := (K_{i_1}, ..., K_{i_t})$, where $i_j = 1$ for j odd and $i_j = 2$ for j even.

2.1 (Multi-user) RKA Security

The RKA security notion is parameterized by the so-called related-key deriving (RKD) sets. Formally, an ν-ary RKD set Φ consists of RKD functions ϕ mapping

a ν-tuple of keys $(K_1, ..., K_\nu)$ in some key space $\mathcal{K}^\nu$ to a new ν-tuple of key in $\mathcal{K}^\nu$, i.e., $\phi : \mathcal{K}^\nu \to \mathcal{K}^\nu$.

We need to formalize the multi-user RKA security model[8] (i.e., the model involving multiple independent secret keys) for the keyed round functions and the classical (single-user) RKA CCA security model for the blockcipher/Feistel networks. For the former, let $F : \mathcal{K} \times \{0,1\}^n \to \{0,1\}^m$ be a keyed function, and fix a key $K \in \mathcal{K}$. We define the Φ-restricted related-key oracle $\mathsf{RK}[F_K]$, which takes a RKD function $\phi \in \Phi$ and an input $X \in \{0,1\}^n$ as input, and returns $\mathsf{RK}[F_K](\phi, X) := F_{\phi(K)}(X)$. Then, we consider a Φ-restricted related-key adversary D which has access to u related-key oracles instantiated with either F or an ideal keyed function $\mathsf{RF} : \mathcal{K} \times \{0,1\}^n \to \{0,1\}^m$, and must distinguish between two worlds as follows:

- the "real" world, where it interacts with $\mathsf{RK}[F_{K_1}], ..., \mathsf{RK}[F_{K_u}]$, and $K_1, ..., K_u$ are randomly and independently drawn from $\mathcal{K}$;
- the "ideal" world, where it interacts with $\mathsf{RK}[\mathsf{RF}_{K_1}], ..., \mathsf{RK}[\mathsf{RF}_{K_u}]$, and K_1,..., K_u are randomly and independently drawn from $\mathcal{K}$.

The adversary is adaptive. Note that in the ideal world, each oracle $\mathsf{RK}[\mathsf{RF}_{K_i}]$ essentially implements an independent random function for each related-key $\phi(K_i)$. Formally, D's distinguishing advantage on F is defined as

$$\mathbf{Adv}_F^{\Phi\text{-rka}[u]}(D) := \Big| \Pr_{\mathsf{RF},K_1,...,K_u}\big[D^{\mathsf{RK}[\mathsf{RF}_{K_1}],\mathsf{RK}[\mathsf{RF}_{K_1}]^{-1},...,\mathsf{RK}[\mathsf{RF}_{K_u}],\mathsf{RK}[\mathsf{RF}_{K_u}]^{-1}} = 1\big] - \Pr_{K_1,...,K_u}\big[D^{\mathsf{RK}[F_{K_1}],\mathsf{RK}[F_{K_1}]^{-1},...,\mathsf{RK}[F_{K_u}],\mathsf{RK}[F_{K_u}]^{-1}} = 1\big] \Big| .$$

It was proved that, under some natural restrictions on RKD sets, the single-user and multi-user RKA notions are equivalent up to a factor of u. Moreover, our subsequent sections mainly focus on the case of $u = 2$. We refer to [5] for details.

Similarly, a blockcipher $E : \mathcal{K}^\nu \times \{0,1\}^m \to \{0,1\}^m$ shall be comparable with an ideal cipher. Formally, D's distinguishing advantage on E is defined as

$$\mathbf{Adv}_E^{\Phi\text{-rka}[1]}(D) := \Big| \Pr_{\mathsf{IC},\mathbf{K}}\big[D^{\mathsf{RK}[\mathsf{IC}_\mathbf{K}],\mathsf{RK}[\mathsf{IC}_\mathbf{K}]^{-1}} = 1\big] - \Pr_{\mathbf{K}}\big[D^{\mathsf{RK}[E_\mathbf{K}],\mathsf{RK}[E_\mathbf{K}]^{-1}} = 1\big] \Big|,$$

where $\mathsf{RK}[E_\mathbf{K}]^{-1}(\phi, Y) := E^{-1}_{\phi(\mathbf{K})}(Y)$.

As already noticed in [7], Φ-RKA security is achievable only if the RKD set Φ satisfies certain conditions that exclude trivial attacks. For this, we follow [5] and characterize three properties. Firstly, the *output unpredictability (UP)* advantage of an adversary $\mathcal{A}$ against an RKD set Φ is

$$\mathbf{Adv}_\Phi^{\mathsf{up}}(\mathcal{A}) := \Pr\big[\exists(\phi, \mathbf{K}^*) \in \mathsf{L}_1 \times \mathsf{L}_2 \quad \mathsf{s.t.} \quad \phi(\mathbf{K}) = \mathbf{K}^* : \mathbf{K} \leftarrow_\$ \mathcal{K};\ (\mathsf{L}_1, \mathsf{L}_2) \leftarrow \mathcal{A}\big].$$

[8] This was termed *multi-key RKA security* in [5]. As we refer to the classical security model with a single "static" secret key as "single-key (CCA) model", we use the terms *single-user and multi-user* here for distinction.

Secondly, the *claw-freeness* (CF) advantage of an adversary $\mathcal{A}$ against an RKD set Φ is

$$\mathbf{Adv}^{\mathsf{cf}}_{\Phi}(\mathcal{A}) := \Pr\big[\exists \phi_1, \phi_2 \in \mathsf{L} \quad \mathsf{s.t.} \quad \phi_1(\mathbf{K}) = \phi_2(\mathbf{K}) \wedge \phi_1 \neq \phi_2 : \mathbf{K} \leftarrow_{\$} \mathcal{K};\ \mathsf{L} \leftarrow \mathcal{A}\big].$$

Finally, when the master key is the aforementioned vector $\mathbf{K} = (K_1, K_2)$, the *switch-freeness* (SF) advantage of an adversary $\mathcal{A}$ against an RKD set Φ is

$$\mathbf{Adv}^{\mathsf{sf}}_{\Phi}(\mathcal{A}) := \Pr\big[(\exists \phi_1, \phi_2 \in \mathsf{L})(\exists i \neq j \in \{1,2\}) \quad \mathsf{s.t.} \quad \phi_1(\mathbf{K})[i] = \phi_2(\mathbf{K})[j] : \mathbf{K} \leftarrow_{\$} \mathcal{K};\ \mathsf{L} \leftarrow \mathcal{A}\big].$$

We require the three advantages to be sufficiently small. The necessity of UP and CF has already been noticed in [7]: if $\mathcal{A}$ is able to figure out $\phi \in \Phi$ such that $\phi(\mathbf{K}) = c$ for some constant c or $\phi(\mathbf{K}) = \phi'(\mathbf{K})$ for some $\phi' \neq \phi$, then distinguishing is always possible by comparing $\mathsf{RK}[E_{\mathbf{K}}](\phi, X)$ with $E_c(X)$ or with $\mathsf{RK}[E_{\mathbf{K}}](\phi', X)$ respectively. On the other hand, the SF property aims to ensure a definitive distinction between the round functions using K_1 and those using K_2. I.e., once a master key $\mathbf{K} = (K_1, K_2)$ is fixed, a round function using K_1 will never use K_2 for some RKD function ϕ.

2.2 The H-Coefficient Technique

The core step of our proofs consists of analyzing information theoretic indistinguishability of EFNs and AFNs built upon ideal keyed functions, which will employ the H-coefficient technique [40,15]. To this end, we assume a deterministic distinguisher that has unbounded computation power, and we summarize the information gathered by the distinguisher in a tuple

$$\mathcal{Q} = \big((\phi_1, X_1, Y_1), \ldots, (\phi_q, X_q, Y_q)\big)$$

called the *transcript*, meaning that the j-th query was either a forward query (ϕ_j, X_j) with answer Y_j, or a backward query (ϕ_j, Y_j) with answer X_j.

To simplify the definition of "bad transcripts", we reveal the key $\mathbf{K}$ to the distinguisher 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 $\mathbf{K}$ to τ and obtain what we call the *transcript* $\tau = (\mathcal{Q}, \mathbf{K})$ of the attack. With respect to some fixed distinguisher D, a transcript τ is said *attainable*, if there exists oracles IC such that the interaction of D with the ideal world $\mathsf{RK}[\mathsf{IC}_{\mathbf{K}}]$ yields $\mathcal{Q}$. 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.

With the above, the main lemma of H-coefficient technique is: (see [15]).

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

$$\frac{\Pr[T_{\text{re}} = \tau]}{\Pr[T_{\text{id}} = \tau]} \geq 1 - \varepsilon_1,$$

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

Given a transcript $\mathcal{Q}$, a blockcipher E, and a key $\mathcal{K} \in \mathcal{K}^{\nu}$, we say the related-key oracle $\mathsf{RK}[E_{\mathbf{K}}]$ *extends* $\mathcal{Q}$, denoted $\mathsf{RK}[E_{\mathbf{K}}] \vdash \mathcal{Q}$, if $E_{\phi(\mathbf{K})}(X) = Y$ for all $(\phi, X, Y) \in \mathcal{Q}$. It is easy to see that for any attainable transcript $\tau = (\mathcal{Q}, \mathbf{K})$, the interaction of the distinguisher with oracles $\mathsf{RK}[E_{\mathbf{K}}]$ produces $(\mathcal{Q}, \mathbf{K})$ if and only if $\mathbf{K}$ is sampled in the interaction and $\mathsf{RK}[E_{\mathbf{K}}] \vdash \tau$. We refer to [15] for a formal argument. With these, it is not hard to see that,

$$\Pr\big[T_{\text{id}} = \tau\big] = \Pr[\mathbf{K}] \cdot \Pr\big[\mathsf{RK}[\mathsf{IC}_{\mathbf{K}}] \vdash \mathcal{Q}\big] \leq \Pr[\mathbf{K}] \cdot \left(\frac{1}{2^{n+m} - q}\right)^q, \qquad (1)$$

where $n + m$ is the block size of the resulting $(n + m)$-bit generalized Feistel network, and $\Pr[\mathbf{K}] = \Pr_{\mathbf{K}^*}[\mathbf{K}^* = \mathbf{K}]$. Similarly,

$$\Pr\big[T_{\text{re}} = \tau\big] = \Pr[\mathbf{K}] \cdot \Pr\big[\mathsf{RK}[E_{\mathbf{K}}] \vdash \mathcal{Q}\big], \qquad (2)$$

and the analysis of $\Pr\big[\mathsf{RK}[E_{\mathbf{K}}] \vdash \mathcal{Q}\big]$ will constitute the core of the subsequent proofs.

3 Security Analysis of Expanding Feistel Networks

Let m and n be positive integers such that $m > n$. In this section, we consider the t-round $\mathsf{EFN}^{F^{n,m},t}_{\mathsf{KA}(\mathbf{K})}$ using an expanding round function $F^{n,m}$. Formally, for $X \in \{0,1\}^{n+m}$ and $i \in \{1, ..., t\}$, the ith round of the EFN uses the round key K_i, and is defined as

$$\Psi^{F^{n,m}_{K_i}}(X) := F^{n,m}_{K_i}\big(X[1,n]\big) \oplus X[n+1, n+m] \,\big\|\, X[1,n].$$

The t-round $\mathsf{EFN}^{F^{n,m},2\lceil \frac{m}{n} \rceil + 2}_{\mathsf{KA}(\mathbf{K})}$ using the key assignment $\mathsf{KA}(\mathbf{K}) = (K_1, ..., K_t)$ is a composition of t such rounds, i.e.,

$$\mathsf{EFN}^{F^{n,m},t}_{\mathsf{KA}(\mathbf{K})}(X) := \Psi^{F^{n,m}_{K_t}} \circ ... \circ \Psi^{F^{n,m}_{K_1}}(X).$$

As mentioned in the Introduction, for such EFNs, $2\lceil \frac{m}{n} \rceil + 2$ rounds and the alternating key assignment $\mathsf{Alter}(\mathbf{K}) = (K_1, K_2, K_1, K_2, \dots)$ would ensure RKA security.

Theorem 1. *For any distinguisher D making at most q queries to the oracles $\mathsf{RK}[\mathsf{EFN}^{F^{n,m},2\lceil\frac{m}{n}\rceil+2}_{\mathsf{Alter}(\mathbf{K})}]$ and $\mathsf{RK}[\mathsf{EFN}^{F^{n,m},2\lceil\frac{m}{n}\rceil+2}_{\mathsf{Alter}(\mathbf{K})}]^{-1}$ in total, it holds*

$$\mathbf{Adv}^{\Phi\text{-rka}[1]}_{\mathsf{EFN}^{F^{n,m},2\lceil\frac{m}{n}\rceil+2}_{\mathsf{Alter}(\mathbf{K})}}(D) \le \mathbf{Adv}^{\Phi\text{-rka}[2]}_{F^{n,m}}(D) + \mathbf{Adv}^{\mathsf{cf}}_{\Phi}(D) + \mathbf{Adv}^{\mathsf{sf}}_{\Phi}(D) + \frac{(\lceil\frac{m}{n}\rceil+1)^2q^2}{2^n} + \frac{q^2}{2^{n+m}}. \tag{3}$$

The bound appears independent of the unpredictability advantage $\mathbf{Adv}^{\mathsf{up}}_{\Phi}(D)$. Though, $\mathbf{Adv}^{\mathsf{up}}_{\Phi}(D)$ shall be small in order to ensure that $\mathbf{Adv}^{\Phi\text{-rka}[2]}_{F^{n,m}}(D)$ is sufficiently small.

The proof starts with a generic standard-to-ideal reduction, which replaces the keyed expanding round function $F^{n,m}$ with an ideal keyed expanding function $\mathsf{RF}^{n,m} : \mathcal{K} \times \{0,1\}^n \to \{0,1\}^m$. Clearly (see [5, Theorem 2] for a more detailed formalism),

$$\left|\ \mathbf{Adv}^{\Phi\text{-rka}[1]}_{\mathsf{EFN}^{\mathsf{RF}^{n,m},2\lceil\frac{m}{n}\rceil+2}_{\mathsf{Alter}(\mathbf{K})}}(D) - \mathbf{Adv}^{\Phi\text{-rka}[1]}_{\mathsf{EFN}^{F^{n,m},2\lceil\frac{m}{n}\rceil+2}_{\mathsf{Alter}(\mathbf{K})}}(D)\ \right| \le \mathbf{Adv}^{\Phi\text{-rka}[2]}_{F^{n,m}}(D),$$

and we could focus on analyzing $\mathbf{Adv}^{\Phi\text{-rka}[1]}_{\mathsf{EFN}^{\mathsf{RF}^{n,m},2\lceil\frac{m}{n}\rceil+2}_{\mathsf{Alter}(\mathbf{K})}}(D)$ for the idealized EFN. We'll employ the H-coefficient technique, define and analyze bad transcripts, and show that the probabilities to obtain any good transcript in the real world and the ideal world are sufficiently close.

3.1 Bad Transcripts

Definition 1. *An attainable transcript $\tau = (\mathcal{Q}, \boldsymbol{K})$ is bad, if either of the following conditions is fulfilled:*

(B-1) Claw in τ: there exist two triples (ϕ_1, X_1, Y_1) and (ϕ_2, X_2, Y_2) in $\mathcal{Q}$ such that $\phi_1 \neq \phi_2$, while $\phi_1(\mathbf{K}) = \phi_2(\mathbf{K})$;

(B-2) Switch in τ: there exist two triples (ϕ_1, X_1, Y_1) and (ϕ_2, X_2, Y_2) in $\mathcal{Q}$ and two distinct indices $i, j \in \{1, 2\}$ such that $\phi_1(\mathbf{K})[i] = \phi_2(\mathbf{K})[j]$.

Otherwise we say τ is good.

It is clear that $\Pr[\text{(B-1)}] \le \mathbf{Adv}^{\mathsf{cf}}_{\Phi}(D)$: an adversary against the claw-freeness of the RKD set Φ could simulate the related-key oracle with Φ against the distinguisher D, collecting D's transcript of queries and responses, and use the records in $\mathcal{Q}$ to break the claw-freeness of Φ. Similarly, $\Pr[\text{(B-2)}] \le \mathbf{Adv}^{\mathsf{sf}}_{\Phi}(D)$, and thus

$$\Pr\big[T_{\mathrm{id}} \in \mathcal{T}_{\mathrm{bad}}\big] = \Pr\big[\text{(B-1)} \vee \text{(B-2)}\big] \le \mathbf{Adv}^{\mathsf{cf}}_{\Phi}(D) + \mathbf{Adv}^{\mathsf{sf}}_{\Phi}(D). \tag{4}$$

3.2 Analyzing Good Transcripts

Fix a good transcript τ. The ideal world probability simply follows from Eq. (1), and it remains to analyze $\Pr\big[\mathsf{RK}[\mathsf{EFN}^{\mathsf{RF}^{n,m},2\lceil\frac{m}{n}\rceil+2}_{\mathsf{Alter}(\mathbf{K})}] \vdash \mathcal{Q}\big]$, i.e., an ideal keyed function $\mathsf{RF}^{n,m}$ satisfying $\mathsf{RK}[\mathsf{EFN}^{\mathsf{RF}^{n,m},2\lceil\frac{m}{n}\rceil+2}_{\mathsf{Alter}(\mathbf{K})}] \vdash \mathcal{Q}$. We proceed in two steps. First, given an ideal keyed function $\mathsf{RF}^{n,m}$, it is possible to derive the $(\lceil\frac{m}{n}\rceil+1)$ th and $(\lceil\frac{m}{n}\rceil+2)$ th round intermediate values involved during evaluating the queries in τ. We thus define a "bad predicate" $\mathsf{BadF}(\mathsf{RF}^{n,m})$ on $\mathsf{RF}^{n,m}$, such that once $\mathsf{BadF}(\mathsf{RF}^{n,m})$ is not fulfilled, the event $T_{\mathrm{re}} = \tau$ is equivalent to $\mathsf{RF}^{n,m}$ satisfying $2q$ distinct equations on these intermediate values, the probability of which is close to the ideal world probability. The bound then follows from some simple probabilistic arguments.

Formally, given an ideal keyed function $\mathsf{RF}^{n,m}$, for every $(\phi_i, X_i, Y_i) \in \tau$, we define the induced intermediate values in a "meet-in-the-middle" manner. In detail, we first define $X_{1,i} := X_i$, and

$$X_{\ell,i} := \mathsf{RF}^{n,m}_{\mathsf{Alter}(\phi_i(\mathbf{K}))[\ell-1]}\big(X_{\ell-1,i}[1,n]\big) \oplus X_{\ell-1,i}[n+1,n+m] \;\big\|\; X_{\ell-1,i}[1,n] \tag{5}$$

for $\ell = 2, ..., \lceil\frac{m}{n}\rceil + 1$. We then define $X_{2\lceil\frac{m}{n}\rceil+3,i} := Y_i$, and

$$X_{\ell,i} := X_{\ell+1,i}[m+1,n+m] \;\big\|\; \mathsf{RF}^{n,m}_{\mathsf{Alter}(\phi_i(\mathbf{K}))[\ell]}\big(X_{\ell+1,i}[m+1,n+m]\big) \oplus X_{\ell+1,i}[1,m] \tag{6}$$

for $\ell = 2\lceil\frac{m}{n}\rceil + 2, 2\lceil\frac{m}{n}\rceil + 1, ..., \lceil\frac{m}{n}\rceil + 3$.

Bad predicate. Informally, the conditions capture "unnecessary" collisions among calls to the round function $\mathsf{RF}^{n,m}$ during evaluating the q queries.

Definition 2. *Given a function $\mathsf{RF}^{n,m}$, the predicate $\mathsf{BadF}(\mathsf{RF}^{n,m})$ is fulfilled, if any of the following $\lceil\frac{m}{n}\rceil + 3$ conditions is fulfilled.*

– **(C-[ℓ])** *For $\ell = 1, ..., \lceil\frac{m}{n}\rceil$, the ℓ th condition addresses the $\ell+1$ th and $2\lceil\frac{m}{n}\rceil + 2 - \ell$ th round function "inputs": there exists two indices $i, j \in \{1, ..., q\}$ such that*

- *there exists $\ell' \in \{1, ..., \ell\}$ such that $\big(\mathsf{Alter}(\phi_i(\mathbf{K}))[\ell+1], X_{\ell+1,i}[1,n]\big) = \big(\mathsf{Alter}(\phi_j(\mathbf{K}))[\ell'], X_{\ell',j}[1,n]\big)$; or*
- *there exists $\ell' \in \big\{2\lceil\frac{m}{n}\rceil + 3 - \ell, ..., 2\lceil\frac{m}{n}\rceil + 3\big\}$ such that $\big(\mathsf{Alter}(\phi_i(\mathbf{K}))[\ell+1], X_{\ell+1,i}[1,n]\big) = \big(\mathsf{Alter}(\phi_j(\mathbf{K}))[\ell'-1], X_{\ell',j}[m+1,n+m]\big)$; or*
- *there exists an index $\ell' \in \{1, ..., \ell+1\}$ such that $\big(\mathsf{Alter}(\phi_i(\mathbf{K}))[2\lceil\frac{m}{n}\rceil + 2 - \ell], X_{2\lceil\frac{m}{n}\rceil+3-\ell,i}[m+1,n+m]\big) = \big(\mathsf{Alter}(\phi_j(\mathbf{K}))[\ell'], X_{\ell',j}[1,n]\big)$; or*
- *there exists $\ell' \in \big\{2\lceil\frac{m}{n}\rceil + 4 - \ell, ..., 2\lceil\frac{m}{n}\rceil + 3\big\}$ such that $\big(\mathsf{Alter}(\phi_i(\mathbf{K}))[2\lceil\frac{m}{n}\rceil + 2 - \ell], X_{2\lceil\frac{m}{n}\rceil+3-\ell,i}[m+1,n+m]\big) = \big(\mathsf{Alter}(\phi_j(\mathbf{K}))[\ell'-1], X_{\ell',j}[m+1,n+m]\big)$.*

– **(C-[$\lceil \frac{m}{n} \rceil + 1$])** *There exists distinct* $i, j \in \{1, ..., q\}$ *and* $\ell \in \{1, ..., \lceil \frac{m}{n} \rceil\}$ *such that* $\big(\mathsf{Alter}(\phi_i(\mathbf{K}))[\ell], X_{\ell,i}[1,n]\big) \neq \big(\mathsf{Alter}(\phi_j(\mathbf{K}))[\ell], X_{\ell,j}[1,n]\big)$*, while* $X_{\ell+1,i}[1,n] = X_{\ell+1,j}[1,n]$*;*

– **(C-[$\lceil \frac{m}{n} \rceil + 2$])** *There exists two distinct indices* $i, j \in \{1, ..., q\}$ *and an index* $\ell \in \{\lceil \frac{m}{n} \rceil + 4, ..., 2\lceil \frac{m}{n} \rceil + 3\}$ *such that* $\big(\mathsf{Alter}(\phi_i(\mathbf{K}))[\ell-1], X_{\ell,i}[m+1, n+m]\big) \neq \big(\mathsf{Alter}(\phi_j(\mathbf{K}))[\ell-1], X_{\ell,j}[m+1, n+m]\big)$*, yet* $X_{\ell-1,i}[m+1, n+m] = X_{\ell-1,j}[m+1, n+m]$*;*

– **(C-[$\lceil \frac{m}{n} \rceil + 3$])** *There exists two distinct indices* $i, j \in \{1, ..., q\}$ *such that either* $\big(\mathsf{Alter}(\phi_i(\mathbf{K}))[\lceil \frac{m}{n} \rceil + 1], X_{\lceil \frac{m}{n} \rceil + 1,i}[1,n]\big) = \big(\mathsf{Alter}(\phi_j(\mathbf{K}))[\lceil \frac{m}{n} \rceil + 1], X_{\lceil \frac{m}{n} \rceil + 1,j}[1,n]\big)$*, or* $\big(\mathsf{Alter}(\phi_i(\mathbf{K}))[\lceil \frac{m}{n} \rceil + 2], X_{\lceil \frac{m}{n} \rceil + 3,i}[m+1, n+m]\big) = \big(\mathsf{Alter}(\phi_j(\mathbf{K}))[\lceil \frac{m}{n} \rceil + 2], X_{\lceil \frac{m}{n} \rceil + 3,j}[m+1, n+m]\big)$.

To bound $\Pr[\mathsf{BadF}(\mathsf{RF}^{n,m})]$, we consider the conditions in turn.

Condition (C-[ℓ]), $\ell = 1, ..., \lceil \frac{m}{n} \rceil$. Consider any such two indices $i, j \in \{1, ..., q\}$. We distinguish two cases.

Case 1: ℓ is odd. In this case, the $\ell+1$ th round function uses the keys $\phi_i(\mathbf{K})[2]$ and $\phi_j(\mathbf{K})[2]$, while the $2\lceil \frac{m}{n} \rceil + 2 - \ell$ th uses $\phi_i(\mathbf{K})[1]$ and $\phi_j(\mathbf{K})[1]$. Note that for $\ell' \neq \ell + 1$, $\big(\mathsf{Alter}(\phi_i(\mathbf{K}))[\ell+1], X_{\ell+1,i}[1,n]\big) = \big(\mathsf{Alter}(\phi_j(\mathbf{K}))[\ell'], X_{\ell',j}[1,n]\big)$ only if ℓ' is even (so that $\mathsf{Alter}(\phi_i(\mathbf{K}))[\ell+1] = \mathsf{Alter}(\phi_j(\mathbf{K}))[\ell']$ means $\phi_i(\mathbf{K})[2] = \phi_j(\mathbf{K})[2]$), as otherwise the condition (B-2) is fulfilled and τ is not good. By this, the 1st subcondition is simplified as

$$X_{\ell+1,i}[1,n] \in \big\{X_{2,j}[1,n], X_{4,j}[1,n], ..., X_{\ell-1,j}[1,n]\big\}.$$

This is yet another composed condition. In this respect, we first consider the probability to have $X_{\ell+1,i}[1,n] = X_{2,j}[1,n]$. By construction, this means

$$\begin{aligned} &\Big(\mathsf{RF}^{n,m}_{\phi_i(\mathbf{K})[1]}\big(X_{\ell,i}[1,n]\big) \oplus X_{\ell,i}[n+1, n+m]\Big)\big[1,n\big] \\ = &\Big(\mathsf{RF}^{n,m}_{\phi_j(\mathbf{K})[1]}\big(X_{1,j}[1,n]\big) \oplus X_{1,j}[n+1, n+m]\Big)\big[1,n\big], \end{aligned}$$

where $\big(X_{\ell,i}[n+1, n+m]\big)\big[1,n\big]$ further depends some function values in the set

$$\mathcal{S}_{\ell,1} := \Big\{\mathsf{RF}^{n,m}_{\phi_j(\mathbf{K})[1]}\big(X_{1,j}[1,n], \mathsf{RF}^{n,m}_{\phi_j(\mathbf{K})[1]}\big(X_{3,j}[1,n]\big), ..., \mathsf{RF}^{n,m}_{\phi_i(\mathbf{K})[1]}\big(X_{\ell-2,i}[1,n]\big)\Big\}.$$

Conditioned on $\neg$(C-[$\ell-1$]), it holds $X_{\ell,i}[1,n] \notin \{X_{1,j}[1,n], X_{3,j}[1,n], ..., X_{\ell-2,i}[1,n]\}$. By this, $\Big(\mathsf{RF}^{n,m}_{\phi_i(\mathbf{K})[\ell]}\big(X_{\ell,i}[1,n]\big)\Big)\big[1,n\big]$ is independent of the function values in $\mathcal{S}_{\ell,1}$, and is uniformly distributed in $\{0,1\}^n$. Therefore, the probability to have $X_{\ell+1,i}[1,n] = X_{2,j}[1,n]$ is $1/2^n$.

We then consider the next equality $X_{\ell+1,i}[1,n] = X_{4,j}[1,n]$, which means

$$\begin{aligned} &\Big(\mathsf{RF}^{n,m}_{\phi_i(\mathbf{K})[1]}\big(X_{\ell,i}[1,n]\big) \oplus X_{\ell,i}[n+1, n+m]\Big)\big[1,n\big] \\ = &\Big(\mathsf{RF}^{n,m}_{\phi_j(\mathbf{K})[1]}\big(X_{3,j}[1,n]\big) \oplus X_{3,j}[n+1, n+m]\Big)\big[1,n\big]. \end{aligned}$$

where $\big(X_{\ell,i}[n+1,n+m]\big)\big[1,n\big]$ and $\big(X_{3,j}[n+1,n+m]\big)\big[1,n\big]$ further depend on some function values in the set $\mathcal{S}_{\ell,1}$ defined as before. Again, conditioned on $\neg$(C-$[\ell-1]$), $\big(\mathsf{RF}^{n,m}_{\phi_i(\mathbf{K})[\ell]}\big(X_{\ell,i}[1,n]\big)\big)[1,n]$ is independent of the function values in $\mathcal{S}_{\ell,1}$, and is uniform in $\{0,1\}^n$. Therefore, the probability to have $X_{\ell+1,i}[1,n] = X_{4,j}[1,n]$ is $1/2^n$. Similar reasoning holds for the next $(\ell-1)/2-2$ equations $X_{\ell+1,i}[1,n] = X_{6,j}[1,n], ..., X_{\ell+1,i}[1,n] = X_{\ell-1,j}[1,n]$, and thus

$$\Pr\Big[X_{\ell+1,i}[1,n] \in \big\{X_{2,j}[1,n], X_{4,j}[1,n], ..., X_{\ell-1,j}[1,n]\big\}\Big] = \frac{(\ell-1)}{2^{n+1}}.$$

We then consider the equality $X_{\ell+1,i}[1,n] = X_{2\lceil\frac{m}{n}\rceil+4-\ell,j}[m+1,n+m]$ due to the 2nd subcondition, which means

$$\begin{aligned}&\Big(\mathsf{RF}^{n,m}_{\phi_i(\mathbf{K})[1]}\big(X_{\ell,i}[1,n]\big) \oplus X_{\ell,i}[n+1,n+m]\Big)\big[1,n\big]\\ =\ &\Big(\mathsf{RF}^{n,m}_{\phi_j(\mathbf{K})[1]}\big(X_{2\lceil\frac{m}{n}\rceil+5-\ell,j}[m+1,n+m]\big) \oplus X_{2\lceil\frac{m}{n}\rceil+5-\ell,j}[1,m]\Big)\big[m-n+1,m\big].\end{aligned}$$

Again, $X_{\ell,i}[1,n] \neq X_{2\lceil\frac{m}{n}\rceil+5-\ell,i}[1,n]$ conditioned on $\neg$(C-$[\ell-1]$), and thus the values $\Big(\mathsf{RF}^{n,m}_{\phi_i(\mathbf{K})[1]}\big(X_{\ell,i}[1,n]\big)\Big)\big[1,n\big]$ and $\Big(\mathsf{RF}^{n,m}_{\phi_j(\mathbf{K})[1]}\big(X_{2\lceil\frac{m}{n}\rceil+5-\ell,j}[1,n]\big)\Big)\big[m-n+1,m\big]$ are independent and uniform. Therefore, the probability of $X_{\ell+1,i}[1,n] = X_{2\lceil\frac{m}{n}\rceil+4-\ell,j}[m+1,n+m]$ is $1/2^n$.

Similar reasoning holds for the next $(\ell-1)/2$ equations, except for the last one $X_{\ell+1,i}[1,n] = X_{2\lceil\frac{m}{n}\rceil+3,j}[m+1,n+m]$, which translates into

$$\Big(\mathsf{RF}^{n,m}_{\phi_i(\mathbf{K})[1]}\big(X_{\ell,i}[1,n]\big) \oplus X_{\ell,i}[n+1,n+m]\Big)\big[1,n\big] = X_{2\lceil\frac{m}{n}\rceil+3,j}[m+1,n+m],$$

and which is clearly $1/2^n$ due to the independence between $\mathsf{RF}^{n,m}_{\phi_i(\mathbf{K})[1]}\big(X_{\ell,i}[1,n]\big)$ and $X_{2\lceil\frac{m}{n}\rceil+3,j}[m+1,n+m]$. Summing over the $(\ell+1)/2$ equations, it can be seen that the probability of the 2nd subcondition is $\frac{(\ell+1)}{2^{n+1}}$.

The analyses for the 3rd and 4th subconditions are similar by symmetry, and also give rise to probabilities $\frac{(\ell+1)}{2^{n+1}}$ and $\frac{(\ell-1)}{2^{n+1}}$ resp. By the above, we eventually reach the union bound $2(\ell-1)/2^{n+1} + 2(\ell+1)/2^{n+1} \leq 2\ell/2^n$.

Case 2: ℓ is even. While being different in details, this case is in general similar to Case 1 by symmetry.

With all the above discussion, the probability that one of the four types of collisions occur with respect to a certain pair of indices (i,j) is at most $2\ell/2^n$. Since the number of such pairs is at most q^2, we have

$$\Pr\big[\text{(C-}[\ell]\text{)} \mid \neg\text{(C-}[\ell-1]\text{)}\big] \leq \frac{2\ell q^2}{2^n}. \tag{7}$$

Conditions (C-[$\lceil \frac{m}{n} \rceil + 1$]) and (C-[$\lceil \frac{m}{n} \rceil + 2$]). Consider (C-[$\lceil \frac{m}{n} \rceil$+1]) first, and consider any such three indices $i, j \in \{1, ..., q\}$ and $\ell \in \{1, ..., \lceil \frac{m}{n} \rceil\}$. The equality $X_{\ell+1,i}[1,n] = X_{\ell+1,j}[1,n]$ translates into

$$\begin{aligned} &\Big(\mathsf{RF}^{n,m}_{\mathsf{Alter}(\phi_i(\mathbf{K}))[\ell]}\big(X_{\ell,i}[1,n]\big) \oplus X_{\ell,i}[n+1,n+m]\Big)\big[1,n\big] \\ = &\Big(\mathsf{RF}^{n,m}_{\mathsf{Alter}(\phi_j(\mathbf{K}))[\ell]}\big(X_{\ell,j}[1,n]\big) \oplus X_{\ell,j}[n+1,n+m]\Big)\big[1,n\big]. \end{aligned}$$

Since $\big(\mathsf{Alter}(\phi_i(\mathbf{K}))[\ell], X_{\ell,i}[1,n]\big) \neq \big(\mathsf{Alter}(\phi_j(\mathbf{K}))[\ell], X_{\ell,j}[1,n]\big)$, the two values $\mathsf{RF}^{n,m}_{\mathsf{Alter}(\phi_i(\mathbf{K}))[\ell]}\big(X_{\ell,i}[1,n]\big)$ and $\mathsf{RF}^{n,m}_{\mathsf{Alter}(\phi_j(\mathbf{K}))[\ell]}\big(X_{\ell,j}[1,n]\big)$ are uniform in $\{0,1\}^m$ and independent. Therefore, the probability to have $X_{\ell+1,i}[1,n] = X_{\ell+1,j}[1,n]$ is $1/2^n$. Summing over the $\binom{q}{2} \cdot \lceil \frac{m}{n} \rceil \leq \frac{q^2}{2} \lceil \frac{m}{n} \rceil$ choices of i, j, ℓ, we reach

$$\Pr\Big[\text{(C-}[\lceil \frac{m}{n} \rceil + 1])\Big] \leq \frac{\lceil \frac{m}{n} \rceil q^2}{2^{n+1}}. \tag{8}$$

The analysis for (C-[$\lceil \frac{m}{n} \rceil + 2$]) is similar by symmetry, yielding

$$\Pr\Big[\text{(C-}[\lceil \frac{m}{n} \rceil + 2])\Big] \leq \frac{\lceil \frac{m}{n} \rceil q^2}{2^{n+1}}. \tag{9}$$

Condition (C-[$\lceil \frac{m}{n} \rceil + 3$]). Consider any distinct $(\phi_i, X_i, Y_i), (\phi_j, X_j, Y_j) \in \mathcal{Q}$. We consider the probability to have $\big(\mathsf{Alter}(\phi_i(\mathbf{K}))[\lceil \frac{m}{n} \rceil + 1], X_{\lceil \frac{m}{n} \rceil+1,i}[1,n]\big) = \big(\mathsf{Alter}(\phi_j(\mathbf{K}))[\lceil \frac{m}{n} \rceil + 1], X_{\lceil \frac{m}{n} \rceil+1,j}[1,n]\big)$ first. Wlog, assume that $\lceil \frac{m}{n} \rceil$ is even, as the case of $\lceil \frac{m}{n} \rceil$ odd exhibits no essential difference (as shown before). In this case, we have $\mathsf{Alter}(\phi_i(\mathbf{K}))[\lceil \frac{m}{n} \rceil + 1] = \phi_i(\mathbf{K})[1]$ and $\mathsf{Alter}(\phi_j(\mathbf{K}))[\lceil \frac{m}{n} \rceil + 1] = \phi_j(\mathbf{K})[1]$, and the condition is fulfilled only if $\phi_i(\mathbf{K})[1] = \phi_j(\mathbf{K})[1]$. With this in mind, we distinguish two cases.

Case 1: $\phi_i \neq \phi_j$. Then since τ is good and is claw-free, it holds $\phi_i(\mathbf{K}) \neq \phi_j(\mathbf{K})$, which further implies $\phi_i(\mathbf{K})[2] \neq \phi_j(\mathbf{K})[2]$. By this, the probability to have $X_{\lceil \frac{m}{n} \rceil+1,i}[1,n] = X_{\lceil \frac{m}{n} \rceil+1,j}[1,n]$, or to have

$$\begin{aligned} &\Big(X_{\lceil \frac{m}{n} \rceil,i}[n+1,n+m] \oplus \mathsf{RF}^{n,m}_{\phi_i(\mathbf{K})[2]}\big(X_{\lceil \frac{m}{n} \rceil,i}[1,n]\big)\Big)\big[1,n\big] \\ = &\Big(X_{\lceil \frac{m}{n} \rceil,j}[n+1,n+m] \oplus \mathsf{RF}^{n,m}_{\phi_j(\mathbf{K})[2]}\big(X_{\lceil \frac{m}{n} \rceil,j}[1,n]\big)\Big)\big[1,n\big], \end{aligned} \tag{10}$$

is $1/2^n$, since $\mathsf{RF}^{n,m}_{\phi_i(\mathbf{K})[2]}$ and $\mathsf{RF}^{n,m}_{\phi_j(\mathbf{K})[2]}$ can be viewed as two independent random functions from $\{0,1\}^n$ to $\{0,1\}^m$.

Case 2: $\phi_i = \phi_j$. For clearness we let $\phi = \phi_i = \phi_j$. Let $\Delta_1 := X_{1,i} \oplus X_{1,j}$. Since D does not make redundant queries, it has to be $\Delta_1 \neq 0$. We further distinguish two subcases.

– Subcase 2.1: $\Delta_1[1, \lceil \frac{m}{n} \rceil \cdot n] \neq 0$. Then, let $\ell \in \{0, ..., \lceil \frac{m}{n} \rceil - 1\}$ be the smallest index such that $\Delta_1[\ell n + 1, (\ell + 1)n] \neq 0$. By construction, this means $X_{\ell+1,i}[1, n] \neq X_{\ell+1,j}[1, n]$. Conditioned on $\neg$(C-[$\lceil \frac{m}{n} \rceil + 1$]), this further implies $X_{\ell+2,i}[1, n] \neq X_{\ell+2,j}[1, n]$, ..., and eventually $X_{\lceil \frac{m}{n} \rceil+1,i}[1, n] \neq X_{\lceil \frac{m}{n} \rceil+1,j}[1, n]$.
– Subcase 2.2: $\Delta_1[1, \lceil \frac{m}{n} \rceil \cdot n] = 0$. Then it has to be $\Delta_1[\lceil \frac{m}{n} \rceil \cdot n+1, n+m] \neq 0$, which necessarily implies $X_{\lceil \frac{m}{n} \rceil+1,i}[1, n] \neq X_{\lceil \frac{m}{n} \rceil+1,j}[1, n]$ by construction.

Therefore, conditioned on $\neg$(C-[$\lceil \frac{m}{n} \rceil$+1]), it is not possible to have $X_{\lceil \frac{m}{n} \rceil+1,i}[1, n] = X_{\lceil \frac{m}{n} \rceil+1,j}[1, n]$ for any two distinct indices (i, j).

The analysis for $\big(\mathsf{Alter}(\phi_i(\mathbf{K}))[\lceil \frac{m}{n} \rceil+2], X_{\lceil \frac{m}{n} \rceil+3,i}[m+1, n+m]\big) = \big(\mathsf{Alter}(\phi_j(\mathbf{K}))[\lceil \frac{m}{n} \rceil + 2], X_{\lceil \frac{m}{n} \rceil+3,j}[m + 1, n + m]\big)$ is similar by symmetry. More concretely, for any such two triples $(\phi_i, X_i, Y_i), (\phi_j, X_j, Y_j)$ such that $\phi_i(\mathbf{K})[2] = \phi_j(\mathbf{K})[2]$, we have:

– If $\phi_i \neq \phi_j$, then it holds $\phi_i(\mathbf{K})[1] \neq \phi_j(\mathbf{K})[1]$ by the claw-freeness and by $\phi_i(\mathbf{K})[2] = \phi_j(\mathbf{K})[2]$, and thus the probability to have $X_{\lceil \frac{m}{n} \rceil+3,i}[m + 1, n + m] = X_{\lceil \frac{m}{n} \rceil+3,j}[m + 1, n + m]$ or

$$\begin{aligned} &\Big(X_{\lceil \frac{m}{n} \rceil+4,i}[1, m] \oplus \mathsf{RF}^{n,m}_{\phi_i(\mathbf{K})[1]}\big(X_{\lceil \frac{m}{n} \rceil+4,i}[m + 1, n + m]\big)\Big)[m - n + 1, m] \\ = &\Big(X_{\lceil \frac{m}{n} \rceil+4,j}[1, m] \oplus \mathsf{RF}^{n,m}_{\phi_j(\mathbf{K})[1]}\big(X_{\lceil \frac{m}{n} \rceil+4,j}[m + 1, n + m]\big)\Big)[m - n + 1, m] \quad (11) \end{aligned}$$

  is $1/2^n$ due to the independence between $\mathsf{RF}^{n,m}_{\phi_i(\mathbf{K})[1]}$ and $\mathsf{RF}^{n,m}_{\phi_j(\mathbf{K})[1]}$.
– If $\phi_i = \phi_j$, then it is not possible to have $X_{\lceil \frac{m}{n} \rceil+3,i}[m+1, n+m] = X_{\lceil \frac{m}{n} \rceil+3,j}[m + 1, n + m]$ conditioned on $\neg$(C-[$\lceil \frac{m}{n} \rceil + 2$]).

In all, for each pair (i, j) of distinct indices, the probability to have $X_{\lceil \frac{m}{n} \rceil+1,i}[1, n] = X_{\lceil \frac{m}{n} \rceil+1,j}[1, n]$ or $X_{\lceil \frac{m}{n} \rceil+3,i}[m + 1, n + m] = X_{\lceil \frac{m}{n} \rceil+3,j}[m + 1, n + m]$ is no larger than $2/2^n$. Taking a union bound for the $\binom{q}{2} \leq q^2/2$ choices of (i, j) yields

$$\Pr\Big[(\text{C-}[\lceil \frac{m}{n} \rceil + 3]) \mid \neg(\text{C-}[1]) \wedge ... \wedge \neg(\text{C-}[\lceil \frac{m}{n} \rceil + 2])\Big] \leq \frac{q^2}{2^n}. \quad (12)$$

Gathering Eqs. (7), (8), (9), and (12), we reach

$$\begin{aligned} &\Pr\big[\mathsf{BadF}(\mathsf{RF}^{n,m})\big] \\ \leq &\left(\sum_{\ell=1,...,\lceil \frac{m}{n} \rceil} \Pr\big[(\text{C-}[\ell]) \mid \neg(\text{C-}[\ell - 1])\big]\right) + \Pr\Big[(\text{C-}[\lceil \frac{m}{n} \rceil + 1])\Big] + \Pr\Big[(\text{C-}[\lceil \frac{m}{n} \rceil + 2])\Big] \\ &+ \Pr\Big[(\text{C-}[\lceil \frac{m}{n} \rceil + 3]) \mid \neg(\text{C-}[1]) \wedge ... \wedge \neg(\text{C-}[\lceil \frac{m}{n} + 2 \rceil])\Big] \\ \leq &\left(\sum_{\ell=1,...,\lceil \frac{m}{n} \rceil} \frac{2\ell q^2}{2^n}\right) + \frac{\lceil \frac{m}{n} \rceil q^2}{2^{n+1}} + \frac{\lceil \frac{m}{n} \rceil q^2}{2^{n+1}} + \frac{q^2}{2^n} \leq \frac{(\lceil \frac{m}{n} \rceil + 1)^2 q^2}{2^n}. \quad (13) \end{aligned}$$

Completing the proof. Consider any good transcript $\tau = (\mathcal{Q}, \mathbf{K})$, where $\mathcal{Q} = \big((\phi_1, X_1, Y_1), ..., (\phi_q, X_q, Y_q)\big)$. With the values defined in Eqs. (5) and (6), it can be seen that, the event $\mathsf{RK}[\mathsf{EFN}^{\mathsf{RF}^{n,m},2\lceil\frac{m}{n}\rceil+2}_{\mathsf{Alter}(\mathbf{K})}] \vdash \mathcal{Q}$ is equivalent to $2q$ equations as follows.

$$\begin{aligned}\mathsf{RF}^{n,m}_{\phi_i(\mathbf{K})[b_1]}\big(X_{\lceil\frac{m}{n}\rceil+1,i}[1,n]\big) &= \Big(X_{\lceil\frac{m}{n}\rceil+1,i}[n+1,2n] \oplus X_{\lceil\frac{m}{n}\rceil+3,i}[m+1,n+m]\Big) \\ &\Big\| \Big(X_{\lceil\frac{m}{n}\rceil+1,i}[2n+1,n+m] \oplus X_{\lceil\frac{m}{n}\rceil+3,i}[1,m-n] \\ &\quad \oplus \mathsf{RF}^{n,m}_{\phi_i(\mathbf{K})[b_2]}\big(X_{\lceil\frac{m}{n}\rceil+3,i}[m+1,n+m]\big)[1,m-n]\Big) \quad \text{for} \quad i=1,...,q, \end{aligned} \tag{14}$$

$$\begin{aligned}&\mathsf{RF}^{n,m}_{\phi_i(\mathbf{K})[b_2]}\big(X_{\lceil\frac{m}{n}\rceil+3,i}[m+1,n+m]\big)[m-n+1,m] \\ &= \Big(X_{\lceil\frac{m}{n}\rceil+1,i}[1,n] \oplus X_{\lceil\frac{m}{n}\rceil+3,i}[m-n+1,m]\Big) \quad \text{for} \quad i=1,...,q, \end{aligned} \tag{15}$$

where $b_1 = 2, b_2 = 1$ when $\lceil\frac{m}{n}\rceil$ is odd, and $b_1 = 1, b_2 = 2$ when $\lceil\frac{m}{n}\rceil$ is even. We refer to Fig. 1 for illustration.

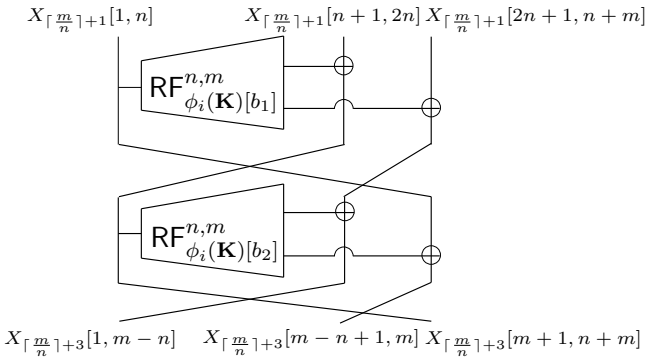

Fig. 1. The middle $\lceil\frac{m}{n}\rceil+1$ th and $\lceil\frac{m}{n}\rceil+2$ th rounds of $\mathsf{EFN}^{\mathsf{RF}^{n,m},2\lceil\frac{m}{n}\rceil+2}_{\mathsf{Alter}(\mathbf{K})}$.

We remark that, the equation on $\mathsf{RF}^{n,m}_{\phi_i(\mathbf{K})[b_1]}\big(X_{\lceil\frac{m}{n}\rceil+1,i}[1,n]\big)$ depends on the $m-n$ output bits $\mathsf{RF}^{n,m}_{\phi_i(\mathbf{K})[b_2]}\big(X_{\lceil\frac{m}{n}\rceil+3,i}[m+1,n+m]\big)[1,m-n]$. Since the first $m-n$ bits and the last n bits of the random function value $\mathsf{RF}^{n,m}_{\phi_i(\mathbf{K})[b_2]}\big(X_{\lceil\frac{m}{n}\rceil+3,i}[m+1,n+m]\big)$ are independent, the probability to have Eqs. (14) and (15) is $\frac{1}{2^m}\times\frac{1}{2^n} = \frac{1}{2^{n+m}}$ for every $i \in \{1,...,q\}$.

Then, for any $\mathsf{RF}^{n,m}$, as long as $\mathsf{BadF}(\mathsf{RF}^{n,m})$ is not fulfilled, the above random variables $\{\mathsf{RF}^{n,m}_{\phi_i(\mathbf{K})[b_1]}\big(X_{\lceil\frac{m}{n}\rceil+1,i}[1,n]\big)\}_{i=1,...,q}$ and $\{\mathsf{RF}^{n,m}_{\phi_i(\mathbf{K})[b_2]}\big(X_{\lceil\frac{m}{n}\rceil+3,i}[m+1,n+m]\big)[m-n+1,m]\}_{i=1,...,q}$ are $2q$ distinct and independent ones, as otherwise (C-$[\lceil\frac{m}{n}\rceil+3]$) is fulfilled. Furthermore, these random variables are not affected by the randomness in $\mathsf{RF}^{n,m}$ that determines the satisfiability of $\mathsf{BadF}(\mathsf{RF}^{n,m})$ (i.e.,

the values $\{\mathsf{RF}^{n,m}_{\mathsf{Alter}(\phi_i(\mathbf{K}))[\ell]}(X_{\ell,i}[1,n])\}_{i\in\{1,\ldots,q\},\ell\in\{1,\ldots,\lceil\frac{m}{n}\rceil,\lceil\frac{m}{n}\rceil+3,\ldots,2\lceil\frac{m}{n}\rceil+2\}}$), as otherwise (C-$[\lceil\frac{m}{n}\rceil]$) is fulfilled. Therefore, by Eq. (13), the real world probability has

$$\begin{aligned}
&\Pr\left[\mathsf{RK}[\mathsf{EFN}^{\mathsf{RF}^{n,m},2\lceil\frac{m}{n}\rceil+2}_{\mathsf{Alter}(\mathbf{K})}]\vdash\mathcal{Q}\right]\\
&\geq \Pr\left[\mathsf{RK}[\mathsf{EFN}^{\mathsf{RF}^{n,m},2\lceil\frac{m}{n}\rceil+2}_{\mathsf{Alter}(\mathbf{K})}]\vdash\mathcal{Q}\wedge\neg\mathsf{BadF}(\mathsf{RF}^{n,m})\right]\\
&= \Pr\left[\mathsf{RK}[\mathsf{EFN}^{\mathsf{RF}^{n,m},2\lceil\frac{m}{n}\rceil+2}_{\mathsf{Alter}(\mathbf{K})}]\vdash\mathcal{Q}\mid\neg\mathsf{BadF}(\mathsf{RF}^{n,m})\right]\cdot\left(1-\Pr\left[\mathsf{BadF}(\mathsf{RF}^{n,m})\right]\right)\\
&\geq \left(1-\frac{(\lceil\frac{m}{n}\rceil+1)^2q^2}{2^n}\right)\cdot\left(\frac{1}{2^{n+m}}\right)^q
\end{aligned}$$

In a similar construction to Figure.3, we have the probability

$$\begin{aligned}
\frac{\Pr\left[T_{\mathrm{re}}=\tau\right]}{\Pr\left[T_{\mathrm{id}}=\tau\right]} &\geq \left(1-\frac{(\lceil\frac{m}{n}\rceil+1)^2q^2}{2^n}\right)\cdot\left(\frac{1}{2^{n+m}}\right)^q\Bigg/\left(\frac{1}{2^{n+m}-q}\right)^q\\
&\geq \left(1-\frac{q}{2^{n+m}}\right)^q\cdot\left(1-\frac{(\lceil\frac{m}{n}\rceil+1)^2q^2}{2^n}\right)\\
&\geq 1-\left(\frac{q^2}{2^{n+m}}+\frac{(\lceil\frac{m}{n}\rceil+1)^2q^2}{2^n}\right). \qquad (16)
\end{aligned}$$

Gathering Eqs. (4) and (16) yields Eq. (3).

4 Security Analysis of Alternating Feistel Networks

Let m and n be positive integers such that $m\geq n$. In this section, we will first consider AFNs using a contracting round function $G^{m,n}$ and an expanding round function $F^{n,m}$.[9] Formally, for $X\in\{0,1\}^{n+m}$ and i odd, the ith round of the AFN using the key K_i employs $G^{m,n}$, and is defined as

$$\Psi^{G^{m,n}_{K_i}}(X) := G^{m,n}_{K_i}\big(X[n+1,n+m]\big)\oplus X[1,n]\ \|\ X[n+1,n+m].$$

On the other hand, for i even, the ith round using the key K_i employs $F^{n,m}$, and is defined as

$$\Psi^{F^{n,m}_{K_i}}(X) := X[1,n]\ \|\ F^{n,m}_{K_i}\big(X[1,n]\big)\oplus X[n+1,n+m].$$

Then, the t-round AFN is a composition of such t rounds.

As mentioned in the introduction, 4-round AFN with the alternating key assignment Alter, as depicted in Fig. 2 (left), is always RKA secure, regardless of the ratio m/n. Formally,

[9] We stress that $G^{m,n}$ and $F^{n,m}$ must be "independent", in the sense that $(G^{m,n}_{K_1},F^{n,m}_{K_2})$ using independent keys K_1,K_2 is indistinguishable from a pair of independent ideal keyed functions $(\mathsf{RG}^{m,n},\mathsf{RF}^{n,m})$. For example, $G^{m,n}$ and $F^{n,m}$ cannot be built from the same primitive such as the AES.

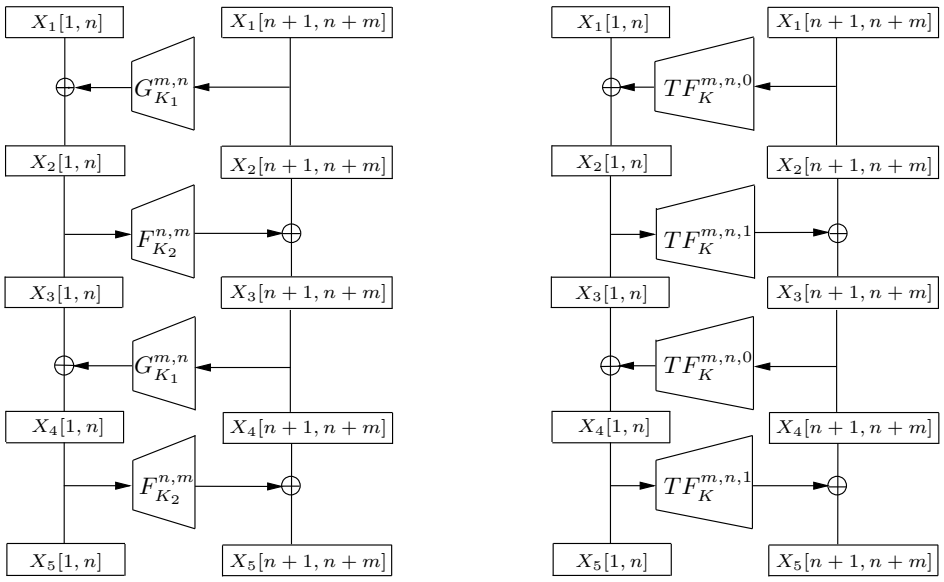

Fig. 2. (Left) The 4-round alternating Feistel network $\mathsf{AFN}^{G^{m,n},F^{n,m},4}$ using a contracting round function $G^{m,n}$ and an expanding round function $F^{n,m}$ and two keys K_1, K_2. (Right) The 4-round alternating Feistel network $\mathsf{AFN}^{TF^{m,n},4}$ using a tweakable round function $TF^{m,n}$ and a single key K.

Theorem 2. *For any distinguisher D making at most q queries to the oracles $\mathsf{RK}[\mathsf{AFN}^{G^{m,n},F^{n,m},4}_{\mathsf{Alter}(\mathbf{K})}]$ and $\mathsf{RK}[\mathsf{AFN}^{G^{m,n},F^{n,m},4}_{\mathsf{Alter}(\mathbf{K})}]^{-1}$ in total, it holds*

$$\mathbf{Adv}^{\Phi\text{-rka}[1]}_{\mathsf{AFN}^{G^{m,n},F^{n,m},4}_{\mathsf{Alter}(\mathbf{K})}}(D) \le \mathbf{Adv}^{\Phi\text{-rka}[1]}_{G^{m,n}}(D) + \mathbf{Adv}^{\Phi\text{-rka}[1]}_{F^{n,m}}(D) + \mathbf{Adv}^{cf}_{\Phi}(D) + \frac{q^2}{2^{n+m}} + \frac{3q^2}{2^n}. \tag{17}$$

The proof flow is similar to Theorem 1. We also start with a generic two-step standard-to-ideal reduction. In the first step, we replace the keyed contracting round function $G^{m,n}$ with an ideal keyed contracting function $\mathsf{RG}^{m,n} : \mathcal{K} \times \{0,1\}^m \to \{0,1\}^n$. This clearly introduces a gap of at most $\mathbf{Adv}^{\Phi\text{-rka}[1]}_{G^{m,n}}(D)$. We then replace the expanding round function $F^{n,m}$ with the ideal $\mathsf{RF}^{n,m} : \mathcal{K} \times \{0,1\}^n \to \{0,1\}^m$, with an additional gap of $\mathbf{Adv}^{\Phi\text{-rka}[1]}_{F^{n,m}}(D)$. As discussed in the introduction, the independence between the two involved keys K_1 and K_2 is crucial for this reduction.

Then, we focus on analyzing $\mathbf{Adv}^{\Phi\text{-rka}[1]}_{\mathsf{AFN}^{\mathsf{RG}^{m,n},\mathsf{RF}^{n,m},4}_{\mathsf{Alter}(\mathbf{K})}}(D)$ for the idealized AFN. We also use the H-coefficient technique, and follow the same (though simpler) flow as Theorem 1.

4.1 Bad Transcripts

An attainable transcript $\tau = (\mathcal{Q}, \mathbf{K})$ is *bad*, if a claw exists τ, i.e., there exist two triples (ϕ_1, X_1, Y_1) and (ϕ_2, X_2, Y_2) in $\mathcal{Q}$ such that $\phi_1 \neq \phi_2$, while $\phi_1(\mathbf{K}) = \phi_2(\mathbf{K})$. Otherwise we say τ is *good*. And it holds

$$\Pr\big[T_{\mathrm{id}} \in \mathcal{T}_{\mathrm{bad}}\big] \le \mathbf{Adv}^{\mathsf{cf}}_{\Phi}(D). \tag{18}$$

Compared with Sect. 3.1, it is natural to ask why switch-freeness turns useless here. Informally, switch-freeness prevents collisions between keys used in different rounds, i.e., $\phi_i(\mathbf{K})[1] = \phi_j(\mathbf{K})[2]$ for some (ϕ_i, X_i, Y_i) and (ϕ_j, X_j, Y_j). But such a collision is harmless here due to the *different* round functions in use.

4.2 Analyzing Good Transcripts

Fix a good transcript τ. The ideal world probability simply follows from Eq. (1), and it remains to analyze $\Pr\big[\mathsf{RK}[\mathsf{AFN}^{\mathsf{RG}^{m,n},\mathsf{RF}^{n,m},4}_{\mathsf{Alter}(\mathbf{K})}] \vdash \mathcal{Q}\big]$. Similarly to Sect. 3.2, we define a "bad predicate" $\mathsf{BadF}(\mathsf{RG}^{m,n}, \mathsf{RF}^{n,m})$ on $\mathsf{RG}^{m,n}$ and $\mathsf{RF}^{n,m}$, such that once $\mathsf{BadF}(\mathsf{RG}^{m,n}, \mathsf{RF}^{n,m})$ is not fulfilled, the event $T_{\mathrm{re}} = \tau$ is equivalent to $\mathsf{RG}^{m,n}$ and $\mathsf{RF}^{n,m}$ satisfying $2q$ distinct equations, the probability of which is close to the ideal world probability. This will enable the argument.

In detail, given a pair of ideal keyed functions $(\mathsf{RG}^{m,n}, \mathsf{RF}^{n,m})$, for every $(\phi_i, X_i, Y_i) \in \tau$, define

$$\begin{aligned}
&X_{1,i} := X_i, \quad X_{5,i} := Y_i,\\
&X_{2,i} := X_{1,i}[1,n] \oplus \mathsf{RG}^{m,n}_{\phi_i(\mathbf{K})[1]}\big(X_{1,i}[n+1, m+n]\big) \parallel X_{1,i}[n+1, m+n],\\
&X_{4,i} := X_{5,i}[1,n] \parallel X_{5,i}[n+1, m+n] \oplus \mathsf{RF}^{n,m}_{\phi_i(\mathbf{K})[2]}\big(X_{5,i}[1,n]\big).
\end{aligned} \tag{19}$$

Bad predicate. Informally, the conditions capture "unnecessary" collisions among calls to the round functions $\mathsf{RG}^{m,n}$ and $\mathsf{RF}^{n,m}$ while evaluating the q queries.

Definition 3. *Given a pair of random functions* $(\mathsf{RG}^{m,n}, \mathsf{RF}^{n,m})$*, the predicate* $\mathsf{BadF}(\mathsf{RG}^{m,n}, \mathsf{RF}^{n,m})$ *is fulfilled, if any of the following four conditions is fulfilled.*

(C-1) *There exists two indices* $i, j \in \{1, ..., q\}$ *such that* $(\phi_i(\mathbf{K})[2], X_{2,i}[1,n]) = (\phi_j(\mathbf{K})[2], X_{5,j}[1,n])$.
(C-2) *There exists two indices* $i, j \in \{1, ..., q\}$ *such that* $(\phi_i(\mathbf{K})[1], X_{4,i}[n+1, n+m]) = (\phi_j(\mathbf{K})[1], X_{1,j}[n+1, n+m])$.
(C-3) *There exists two distinct indices* $i, j \in \{1, ..., q\}$ *such that* $(\phi_i(\mathbf{K})[2], X_{2,i}[1,n]) = (\phi_j(\mathbf{K})[2], X_{2,j}[1,n])$.
(C-4) *There exists two distinct indices* $i, j \in \{1, ..., q\}$ *such that* $(\phi_i(\mathbf{K})[1], X_{4,i}[n+1, n+m] = (\phi_j(\mathbf{K})[1], X_{4,j}[n+1, n+m])$.

Consider the conditions in turn. First, for (C-1), note that $X_{2,i}[1,n] = X_{1,i}[1,n] \oplus \mathsf{RG}^{m,n}_{\phi_i(\mathbf{K})[1]}\big(X_{1,i}[n+1, m+n]\big)$, where $\mathsf{RG}^{m,n}_{\phi_i(\mathbf{K})[1]}\big(X_{1,i}[n+1, m+n]\big)$ is uniformly distributed and independent of $X_{5,j}[1,n]$ which is specified in τ. Therefore, the probability to have $X_{2,i}[1,n] = X_{5,j}[1,n]$ for any i, j is $1/2^n$, and thus $\Pr[\text{(C-1)}] \leq q^2/2^n$. Similarly by symmetry, $X_{4,i}[n+1, n+m] = X_{5,i}[n+1, m+n] \oplus \mathsf{RF}^{n,m}_{\phi_i(\mathbf{K})[2]}\big(X_{5,i}[1,n]\big)$, which means the probability to have $X_{4,i}[n+1, n+m] = X_{1,j}[n+1, n+m]$ is $1/2^m$, and further $\Pr[\text{(C-2)}] \leq q^2/2^m$.

The condition (C-3) is slightly more cumbersome. Consider any such two triples $(\phi_i, X_i, Y_i), (\phi_j, X_j, Y_j) \in \mathcal{Q}$. The condition is fulfilled only if $\phi_i(\mathbf{K})[2] = \phi_j(\mathbf{K})[2]$. With this in mind, we distinguish two cases.

Case 1: $\phi_i \neq \phi_j$. Then since τ is good and is claw-free, it holds $\phi_i(\mathbf{K}) \neq \phi_j(\mathbf{K})$, which further implies $\phi_i(\mathbf{K})[1] \neq \phi_j(\mathbf{K})[1]$. By this, the probability to have $X_{2,i}[1,n] = X_{2,j}[1,n]$, or to have

$$\begin{aligned} & X_{1,i}[1,n] \oplus \mathsf{RG}^{m,n}_{\phi_i(\mathbf{K})[1]}\big(X_{1,i}[n+1, m+n]\big) \\ = \; & X_{1,j}[1,n] \oplus \mathsf{RG}^{m,n}_{\phi_j(\mathbf{K})[1]}\big(X_{1,j}[n+1, m+n]\big), \end{aligned} \tag{20}$$

is $1/2^n$, since $\mathsf{RG}^{m,n}_{\phi_i(\mathbf{K})[1]}$ and $\mathsf{RG}^{m,n}_{\phi_j(\mathbf{K})[1]}$ can be viewed as two independent random functions from $\{0,1\}^m$ to $\{0,1\}^n$.

Case 2: $\phi_i = \phi_j$. For clearness we let $\phi = \phi_i = \phi_j$. Then we further distinguish two subcases.

- Subcase 2.1: $X_{1,i}[n+1, m+n] \neq X_{1,j}[n+1, m+n]$. Then the probability to have $X_{2,i}[1,n] = X_{2,j}[1,n]$, or to have Eq. (20), is $1/2^n$, since $\mathsf{RG}^{m,n}_{\phi(\mathbf{K})[1]}\big(X_{1,i}[n+1, m+n]\big)$ and $\mathsf{RG}^{m,n}_{\phi(\mathbf{K})[1]}\big(X_{1,j}[n+1, m+n]\big)$ are independent and uniform in $\{0,1\}^n$;
- Subcase 2.2: $X_{1,i}[n+1, m+n] = X_{1,j}[n+1, m+n]$. Then since the distinguisher does not make redundant queries, it has to be $X_{1,i}[1,n] \neq X_{1,j}[1,n]$, which means it is impossible to have $X_{2,i}[1,n] = X_{2,j}[1,n]$ or Eq. (20).

Therefore, for each pair (i,j) of indices, the probability to have $X_{2,i}[1,n] = X_{2,j}[1,n]$ is no larger than $1/2^n$. Summing over the $\binom{q}{2} \le q^2/2$ choices, we reach $\Pr[\text{(C-3)}] \le q^2/2^{n+1}$.

The analysis for (C-4) is similar by symmetry, yielding $\Pr[\text{(C-4)}] \le q^2/2^{m+1}$. Summing over the four probabilities and using $n \le m$, we reach

$$\Pr\big[\mathsf{BadF}(\mathsf{RG}^{m,n}, \mathsf{RF}^{n,m})\big] \le \frac{q^2}{2^n} + \frac{q^2}{2^m} + \frac{q^2}{2^{n+1}} + \frac{q^2}{2^{m+1}} \le \frac{3q^2}{2^n}. \tag{21}$$

Completing the proof. Consider any good transcript $\tau = (\mathcal{Q}, \mathbf{K})$, where $\mathcal{Q} = \big((\phi_1, X_1, Y_1), ..., (\phi_q, X_q, Y_q)\big)$. With the values defined in Eq. (19), it can be seen that, the event $\mathsf{RK}[\mathsf{AFN}^{\mathsf{RG}^{m,n},\mathsf{RF}^{n,m},4}_{\mathsf{Alter}(\mathbf{K})}] \vdash \mathcal{Q}$ is equivalent to $2q$ equations as follows.

$$\mathsf{RF}^{n,m}_{\phi_i(\mathbf{K})[2]}(X_{2,i}[1,n]) = X_{2,i}[n+1,n+m] \oplus X_{4,i}[n+1,n+m] \text{ for } i = 1,...,q,$$
$$\mathsf{RG}^{m,n}_{\phi_i(\mathbf{K})[1]}(X_{4,i}[n+1,n+m]) = X_{2,i}[1,n] \oplus X_{4,i}[1,n] \text{ for } i = 1,...,q.$$

For any $\mathsf{RG}^{m,n}$ and $\mathsf{RF}^{n,m}$, as long as $\mathsf{BadF}(\mathsf{RG}^{m,n}, \mathsf{RF}^{n,m})$ is not fulfilled, the above random variables $\{\mathsf{RF}^{n,m}_{\phi_i(\mathbf{K})[2]}(X_{2,i}[1,n])\}_{i=1,...,q}$ are q distinct ones, and $\{\mathsf{RG}^{m,n}_{\phi_i(\mathbf{K})[1]}(X_{4,i}[n+1,n+m])\}_{i=1,...,q}$ are also distinct, as otherwise either (C-3) or (C-4) will be fulfilled. Moreover, these random variables are not affected by the randomness in $\mathsf{RG}^{m,n}$ and $\mathsf{RF}^{n,m}$ that determines the satisfiability of $\mathsf{BadF}(\mathsf{RG}^{m,n}, \mathsf{RF}^{n,m})$ (i.e., the values $\{\mathsf{RG}^{m,n}_{\phi_i(\mathbf{K})[1]}(X_{1,i}[n+1,n+m])\}_{i=1,...,q}$ and $\{\mathsf{RF}^{n,m}_{\phi_i(\mathbf{K})[2]}(X_{5,i}[1,n])\}_{i=1,...,q}$), as otherwise either (C-1) or (C-2) will be fulfilled. Therefore, by Eq. (21), we have

$$\begin{aligned}
&\Pr\Big[\mathsf{RK}\big[\mathsf{AFN}^{\mathsf{RG}^{m,n},\mathsf{RF}^{n,m},4}_{\mathsf{Alter}(\mathbf{K})}\big] \vdash \mathcal{Q}\Big] \\
&\ge \Pr\Big[\mathsf{RK}\big[\mathsf{AFN}^{\mathsf{RG}^{m,n},\mathsf{RF}^{n,m},4}_{\mathsf{Alter}(\mathbf{K})}\big] \vdash \mathcal{Q} \;\mid\; \neg\mathsf{BadF}(\mathsf{RG}^{m,n}, \mathsf{RF}^{n,m})\Big] \\
&\qquad \cdot \Big(1 - \Pr\big[\mathsf{BadF}(\mathsf{RG}^{m,n}, \mathsf{RF}^{n,m})\big]\Big) \\
&\ge \Big(\frac{1}{2^{n+m}}\Big)^q \cdot \Big(1 - \frac{3q^2}{2^n}\Big).
\end{aligned}$$

With this, and further using Eqs. (1) and (2), we reach

$$\begin{aligned}
\frac{\Pr[T_{\mathrm{re}} = \tau]}{\Pr[T_{\mathrm{id}} = \tau]} &\ge \Big(\frac{1}{2^{n+m}}\Big)^q \cdot \Big(1 - \frac{3q^2}{2^n}\Big) \Big/ \Big(\frac{1}{2^{n+m} - q}\Big)^q \\
&\ge \Big(1 - \frac{q}{2^{n+m}}\Big)^q \cdot \Big(1 - \frac{3q^2}{2^n}\Big) \ge 1 - \Big(\frac{q^2}{2^{n+m}} + \frac{3q^2}{2^n}\Big).
\end{aligned} \tag{22}$$

Gathering Eqs. (18) and (22) yields Eq. (17).

4.3 AFN using a Tweakable Round Function and Single Key

While the standard-to-ideal reduction couldn't handle two different functions that use the same secret key, the situation could be remedied by using a *tweakable round function*. In detail, consider a tweakable round function $TF^{m,n}$ that has a tweak input of 1 bit, such that $TF^{m,n}(0,\cdot)$ maps $(K,x) \in \mathcal{K} \times \{0,1\}^m$ to $x \in \{0,1\}^n$ and $TF^{m,n}(1,\cdot)$ maps $(K,x) \in \mathcal{K} \times \{0,1\}^n$ to $x \in \{0,1\}^m$. This is quite different from the standard notion of tweakable blockciphers, as the domain of the standard formalism typically don't vary with the tweak. Here, however, depending on whether the tweak input is 0 or 1, the round function varies between contracting and expanding.

The security of such tweakable round function $TF^{m,n}$ shall be measured by its deviation from the ideal counterpart $\mathsf{RTF}^{m,n}$ that is uniformly picked from all the functions that have exactly the same signature as $TF^{m,n}$. Note that this means $\mathsf{RTF}^{m,n}(0,\cdot)$ and $\mathsf{RTF}^{m,n}(1,\cdot)$ are *independent* ideal keyed functions. Further define

$$\mathsf{Iden}(K) = (K_{i_1}, ..., K_{i_t}), \text{ where } K_{i_1} = ... = K_{i_t} = K.$$

Now, for the 4-round AFN using $TF^{m,n}$ as the round function and identical round key, as depicted in Fig. 2 (right), a RKA security proof is possible.

Corollary 1. *For any distinguisher D making at most q queries to $\mathsf{RK}[\mathsf{AFN}^{TF^{m,n},4}_{\mathsf{Iden}(K)}]$ and $\mathsf{RK}[\mathsf{AFN}^{TF^{m,n},4}_{\mathsf{Iden}(K)}]^{-1}$ in total, it holds*

$$\mathbf{Adv}^{\Phi\text{-rka}[1]}_{\mathsf{AFN}^{TF^{m,n},4}_{\mathsf{Iden}(K)}}(D) \leq \mathbf{Adv}^{\Phi\text{-rka}[1]}_{TF^{m,n}}(D) + \mathbf{Adv}^{cf}_{\Phi}(D) + \frac{q^2}{2^{n+m}} + \frac{3q^2}{2^n}, \qquad (23)$$

where $\mathbf{Adv}^{\Phi\text{-rka}[1]}_{TF^{m,n}}(D) =$

$$\left| \Pr_K\left[D^{RK[TF^{m,n}_K],RK[\mathsf{RTF}^{m,n}_K]^{-1}} = 1\right] - \Pr_{K,\mathsf{RTF}}\left[D^{RK[\mathsf{RTF}^{m,n}_K],RK[\mathsf{RTF}^{m,n}_K]^{-1}} = 1\right] \right|.$$

Proof (Sketch). The proof turns possible simply because a single standard-to-ideal reduction already suffices to turn $\mathsf{AFN}^{TF^{m,n},4}_{\mathsf{Iden}(K)}$ into the ideal $\mathsf{AFN}^{\mathsf{RTF}^{m,n},4}_{\mathsf{Iden}(K)}$. The subsequent analysis for $\mathbf{Adv}^{\Phi\text{-rka}[1]}_{\mathsf{AFN}^{\mathsf{RTF}^{m,n},4}_{\mathsf{Iden}(K)}}(D)$ basically follows the previous for $\mathbf{Adv}^{\Phi\text{-rka}[1]}_{\mathsf{AFN}^{\mathsf{RG}^{m,n},\mathsf{RF}^{n,m},4}_{\mathsf{Iden}(K)}}(D)$, and we sketch the crucial points below. Concretely, the definition and probability of bad transcripts here are the same as Sect. 4.1.

Whereas the definition of $\mathsf{BadF}(\mathsf{RTF}^{m,n})$ is a slight modification of Definition 3 as follows.

Definition 4. *Given a tweakable function $\mathsf{RTF}^{m,n}$, the predicate $\mathsf{BadF}(\mathsf{RTF}^{m,n})$ is fulfilled, if any of the following four conditions is fulfilled.*

(C-1) There exists two indices $i, j \in \{1, ..., q\}$ such that $(\phi_i(K), X_{2,i}[1,n]) = (\phi_j(K), X_{5,j}[1,n])$.

(C-2) There exists two indices $i, j \in \{1, ..., q\}$ such that $(\phi_i(K), X_{4,i}[n+1, n+m]) = (\phi_j(K), X_{1,j}[n+1, n+m])$.
(C-3) There exists two distinct indices $i, j \in \{1, ..., q\}$ such that $(\phi_i(K), X_{2,i}[1, n]) = (\phi_j(K), X_{2,j}[1, n])$.
(C-4) There exists two distinct indices $i, j \in \{1, ..., q\}$ such that $(\phi_i(K), X_{4,i}[n+1, n+m] = (\phi_j(K), X_{4,j}[n+1, n+m])$.

The analyses for the conditions simply exclude the case of $\phi_i \neq \phi_j$, which implies $\phi_i(K) \neq \phi_j(K)$ due to claw-freeness and excludes the possibility of collisions. Anyway, the bound $\Pr\big[\mathsf{BadF}(\mathsf{RTF}^{m,n})\big] \leq 3q^2/2^n$ remains, and the subsequent analysis just follows. □

5 Conclusion

We study provable related-key security (RKA security) of expanding Feistel networks and alternating Feistel networks. For the former built upon a round function $F : \mathcal{K} \times \{0,1\}^n \to \{0,1\}^m$, we prove that $2\lceil \frac{m}{n} \rceil + 2$ rounds with the alternating key assignment suffice for RKA security; for the latter that alternate round functions $F : \mathcal{K} \times \{0,1\}^n \to \{0,1\}^m$ and $G : \mathcal{K} \times \{0,1\}^m \to \{0,1\}^n$, we prove that 4 rounds with the alternating key assignment suffice. These complete the picture of provable RKA security of generalized Feistel networks, and provide further insights into the NIST standards FF1 and FF3.

Provable security of EFNs is limited by the input size of F. On the other hand, provable security of AFNs is upper bounded by G. We thus leave beyond n-bit RKA security of AFNs as an open question.

Acknowledgments

We appreciate the anonymous reviewers of CT-RSA 2021 for their invaluable comments that help greatly improving the quality of this paper. This work was partly supported by the Program of Qilu Young Scholars (Grant No. 61580089963177) of Shandong University, the National Natural Science Foundation of China (Grant No. 62002202), the National Key Research and Development Project under Grant No.2018YFA0704702, and the Shandong Nature Science Foundation of China (Grant No. ZR2020ZD02, ZR2020MF053).

References

1. Abdalla, M., Benhamouda, F., Passelègue, A., Paterson, K.G.: Related-key security for pseudorandom functions beyond the linear barrier. In: Garay, J.A., Gennaro, R. (eds.) CRYPTO 2014, Part I. LNCS, vol. 8616, pp. 77–94. Springer, Heidelberg (Aug 2014)
2. Anderson, R.J., Biham, E.: Two practical and provably secure block ciphers: BEARS and LION. In: Gollmann, D. (ed.) FSE'96. LNCS, vol. 1039, pp. 113–120. Springer, Heidelberg (Feb 1996)

3. Anderson, R.J., Kuhn, M.G.: Low Cost Attacks on Tamper Resistant Devices. In: Security Protocols, 5th International Workshop, Paris, France, April 7-9, 1997, Proceedings. pp. 125–136 (1997), https://doi.org/10.1007/BFb0028165
4. Banik, S., Bogdanov, A., Isobe, T., Shibutani, K., Hiwatari, H., Akishita, T., Regazzoni, F.: Midori: A block cipher for low energy. In: Iwata, T., Cheon, J.H. (eds.) ASIACRYPT 2015, Part II. LNCS, vol. 9453, pp. 411–436. Springer, Heidelberg (Nov / Dec 2015)
5. Barbosa, M., Farshim, P.: The related-key analysis of Feistel constructions. In: Cid, C., Rechberger, C. (eds.) FSE 2014. LNCS, vol. 8540, pp. 265–284. Springer, Heidelberg (Mar 2015)
6. Bellare, M., Cash, D.: Pseudorandom functions and permutations provably secure against related-key attacks. In: Rabin, T. (ed.) CRYPTO 2010. LNCS, vol. 6223, pp. 666–684. Springer, Heidelberg (Aug 2010)
7. Bellare, M., Kohno, T.: A theoretical treatment of related-key attacks: RKA-PRPs, RKA-PRFs, and applications. In: Biham, E. (ed.) EUROCRYPT 2003. LNCS, vol. 2656, pp. 491–506. Springer, Heidelberg (May 2003)
8. Bellare, M., Ristenpart, T., Rogaway, P., Stegers, T.: Format-preserving encryption. In: Jacobson Jr., M.J., Rijmen, V., Safavi-Naini, R. (eds.) SAC 2009. LNCS, vol. 5867, pp. 295–312. Springer, Heidelberg (Aug 2009)
9. Biham, E.: New types of cryptanalytic attacks using related keys. Journal of Cryptology 7(4), 229–246 (Dec 1994)
10. Biryukov, A., Dunkelman, O., Keller, N., Khovratovich, D., Shamir, A.: Key recovery attacks of practical complexity on AES-256 variants with up to 10 rounds. In: Gilbert, H. (ed.) EUROCRYPT 2010. LNCS, vol. 6110, pp. 299–319. Springer, Heidelberg (May / Jun 2010)
11. Biryukov, A., Wagner, D.: Slide attacks. In: Knudsen, L.R. (ed.) FSE'99. LNCS, vol. 1636, pp. 245–259. Springer, Heidelberg (Mar 1999)
12. Biryukov, A., Wagner, D.: Advanced slide attacks. In: Preneel, B. (ed.) EUROCRYPT 2000. LNCS, vol. 1807, pp. 589–606. Springer, Heidelberg (May 2000)
13. Black, J., Rogaway, P.: Ciphers with arbitrary finite domains. In: Preneel, B. (ed.) CT-RSA 2002. LNCS, vol. 2271, pp. 114–130. Springer, Heidelberg (Feb 2002)
14. Brightwell, M., Smith, H.: Using datatype-preserving encryption to enhance data warehouse security. 20th NISSC Proceedings (1997), available at http://csrc.nist.gov/nissc/1997.
15. Chen, S., Steinberger, J.P.: Tight security bounds for key-alternating ciphers. In: Nguyen, P.Q., Oswald, E. (eds.) EUROCRYPT 2014. LNCS, vol. 8441, pp. 327–350. Springer, Heidelberg (May 2014)
16. Cogliati, B., Dodis, Y., Katz, J., Lee, J., Steinberger, J.P., Thiruvengadam, A., Zhang, Z.: Provable security of (tweakable) block ciphers based on substitution-permutation networks. In: Shacham, H., Boldyreva, A. (eds.) CRYPTO 2018, Part I. LNCS, vol. 10991, pp. 722–753. Springer, Heidelberg (Aug 2018)
17. Cogliati, B., Seurin, Y.: On the provable security of the iterated Even-Mansour cipher against related-key and chosen-key attacks. In: Oswald, E., Fischlin, M. (eds.) EUROCRYPT 2015, Part I. LNCS, vol. 9056, pp. 584–613. Springer, Heidelberg (Apr 2015)
18. Council, P.S.S.: Payment card industry (pci) data security standard: Requirements and security assessment procedures, version 1.2.1. july (2009), available from www.pcisecuritystandards.org.
19. Diffie, W., (translators), G.L.: SMS4 encryption algorithm for wireless networks. Cryptology ePrint Archive, Report 2008/329 (2008), http://eprint.iacr.org/2008/329

20. Dunkelman, O., Keller, N., Lasry, N., Shamir, A.: New slide attacks on almost self-similar ciphers. In: Canteaut, A., Ishai, Y. (eds.) EUROCRYPT 2020, Part I. LNCS, vol. 12105, pp. 250–279. Springer, Heidelberg (May 2020)
21. Dunkelman, O., Keller, N., Shamir, A.: A practical-time related-key attack on the KASUMI cryptosystem used in GSM and 3G telephony. Journal of Cryptology 27(4), 824–849 (Oct 2014)
22. Dunkelman, O., Keller, N., Shamir, A.: Slidex attacks on the Even-Mansour encryption scheme. Journal of Cryptology 28(1), 1–28 (Jan 2015)
23. Dworkin, M.: Recommendation for block cipher modes of operation: Methods for format-preserving encryption. NIST Special Publication 800-38G (2016), available from http://dx.doi.org/10.6028/NIST.SP.800-38G.
24. EMVCo: EMV Integrated Circuit Card Speci
cations for Payment Systems, Book 2, Security and Key Management. June 2008. Version 4.2.
25. Feistel, H., Notz, W.A., Smith, J.L.: Some Cryptographic Techniques for Machine-to-Machine Data Communications. Proceedings of the IEEE 63(11), 1545–1554 (1975)
26. Guo, C.: Understanding the Related-Key Security of Feistel Ciphers From a Provable Perspective. IEEE Trans. Inf. Theory 65(8), 5260–5280 (2019), https://doi.org/10.1109/TIT.2019.2903796
27. Guo, J., Peyrin, T., Poschmann, A., Robshaw, M.J.B.: The LED block cipher. In: Preneel, B., Takagi, T. (eds.) CHES 2011. LNCS, vol. 6917, pp. 326–341. Springer, Heidelberg (Sep / Oct 2011)
28. Hoang, V.T., Rogaway, P.: On generalized Feistel networks. In: Rabin, T. (ed.) CRYPTO 2010. LNCS, vol. 6223, pp. 613–630. Springer, Heidelberg (Aug 2010)
29. Iwata, T., Kohno, T.: New security proofs for the 3GPP confidentiality and integrity algorithms. In: Roy, B.K., Meier, W. (eds.) FSE 2004. LNCS, vol. 3017, pp. 427–445. Springer, Heidelberg (Feb 2004)
30. Knudsen, L.R.: Cryptanalysis of LOKI91. In: Seberry, J., Zheng, Y. (eds.) AUSCRYPT'92. LNCS, vol. 718, pp. 196–208. Springer, Heidelberg (Dec 1993)
31. Louis Goubin, Mickael Ivascot, W.J.O.L.V.N.J.P.J.T., Volte, E.: Crunch. Submission to NIST (2008)
32. Luby, M., Rackoff, C.: How to Construct Pseudorandom Permutations from Pseudorandom Functions. SIAM J. Comput. 17(2), 373–386 (1988)
33. Lucks, S.: Faster Luby-Rackoff ciphers. In: Gollmann, D. (ed.) FSE'96. LNCS, vol. 1039, pp. 189–203. Springer, Heidelberg (Feb 1996)
34. Maines, L., Piva, M., Rimoldi, A., Sala, M.: On the provable security of BEAR and LION schemes. Appl. Algebra Eng. Commun. Comput. 22(5-6), 413–423 (2011), https://doi.org/10.1007/s00200-011-0159-z
35. Morris, B., Rogaway, P., Stegers, T.: How to encipher messages on a small domain. In: Halevi, S. (ed.) CRYPTO 2009. LNCS, vol. 5677, pp. 286–302. Springer, Heidelberg (Aug 2009)
36. Nachef, V., Patarin, J., Volte, E.: Feistel Ciphers - Security Proofs and Cryptanalysis. Springer (2017)
37. Nandi, M.: On the optimality of non-linear computations of length-preserving encryption schemes. In: Iwata, T., Cheon, J.H. (eds.) ASIACRYPT 2015, Part II. LNCS, vol. 9453, pp. 113–133. Springer, Heidelberg (Nov / Dec 2015)
38. Naor, M., Reingold, O.: On the construction of pseudorandom permutations: Luby-Rackoff revisited. Journal of Cryptology 12(1), 29–66 (Jan 1999)

39. Patarin, J.: Security of random Feistel schemes with 5 or more rounds. In: Franklin, M. (ed.) CRYPTO 2004. LNCS, vol. 3152, pp. 106–122. Springer, Heidelberg (Aug 2004)
40. Patarin, J.: The "coefficients H" technique (invited talk). In: Avanzi, R.M., Keliher, L., Sica, F. (eds.) SAC 2008. LNCS, vol. 5381, pp. 328–345. Springer, Heidelberg (Aug 2009)
41. Patarin, J.: Security of balanced and unbalanced Feistel schemes with linear non equalities. Cryptology ePrint Archive, Report 2010/293 (2010), http://eprint.iacr.org/2010/293
42. Patarin, J., Nachef, V., Berbain, C.: Generic attacks on unbalanced Feistel schemes with expanding functions. In: Kurosawa, K. (ed.) ASIACRYPT 2007. LNCS, vol. 4833, pp. 325–341. Springer, Heidelberg (Dec 2007)
43. Sadeghiyan, B., Pieprzyk, J.: A construction for super pseudorandom permutations from a single pseudorandom function. In: Rueppel, R.A. (ed.) EUROCRYPT'92. LNCS, vol. 658, pp. 267–284. Springer, Heidelberg (May 1993)
44. Schneier, B., Kelsey, J.: Unbalanced Feistel networks and block cipher design. In: Gollmann, D. (ed.) FSE'96. LNCS, vol. 1039, pp. 121–144. Springer, Heidelberg (Feb 1996)
45. Shen, Y., Guo, C., Wang, L.: Improved security bounds for generalized Feistel networks. IACR Trans. Symm. Cryptol. 2020(1), 425–457 (2020)
46. Volte, E., Nachef, V., Patarin, J.: Improved generic attacks on unbalanced Feistel schemes with expanding functions. In: Abe, M. (ed.) ASIACRYPT 2010. LNCS, vol. 6477, pp. 94–111. Springer, Heidelberg (Dec 2010)
47. Yu, W., Zhao, Y., Guo, C.: Provable Related-key Security of Contracting Feistel Networks. In: Inscrypt 2020 (to appear) (2020)
48. Zheng, Y., Matsumoto, T., Imai, H.: On the construction of block ciphers provably secure and not relying on any unproved hypotheses. In: Brassard, G. (ed.) CRYPTO'89. LNCS, vol. 435, pp. 461–480. Springer, Heidelberg (Aug 1990)

A Security Proof for $\mathsf{EFN}^{F^{n,2n}}$

In this section, we prove RKA-CCA security for $\mathsf{EFN}^{F^{n,2n}}$, i.e., the simplest case of $\frac{m}{n} = 2$. As mentioned in the Introduction, we consider the alternating key assignment Alter.

Theorem 3. *For any distinguisher D making at most q queries to $RK[\mathsf{EFN}^{F^{n,2n},6}_{\mathsf{Alter}(\mathbf{K})}]$ and $RK[\mathsf{EFN}^{F^{n,2n},6}_{\mathsf{Alter}(\mathbf{K})}]^{-1}$ in total, it holds*

$$\mathbf{Adv}^{\Phi\text{-}rka[1]}_{\mathsf{EFN}^{F^{n,2n},6}_{\mathsf{Alter}(\mathbf{K})}}(D) \leq \mathbf{Adv}^{\Phi\text{-}rka[2]}_{F^{n,2n}}(D) + \mathbf{Adv}^{cf}_{\Phi}(D) + \mathbf{Adv}^{sf}_{\Phi}(D) + \frac{9q^2}{2^n} + \frac{q^2}{2^{3n}}.$$

Outline of the proof. As the first step, we replace the keyed function $F^{n,2n}$ with a random function $\mathsf{RF}^{n,2n} : \mathcal{K} \times \{0,1\}^n \to \{0,1\}^{2n}$, which gives rise to the random network $\mathsf{EFN}^{\mathsf{RF}^{n,2n}}_{\mathsf{Alter}(\mathbf{K})}$. As two independent keys K_1 and K_2 are involved, it holds

$$\left| \mathbf{Adv}^{\Phi\text{-rka}[1]}_{\mathsf{EFN}^{F^{n,2n},6}_{\mathsf{Alter}(\mathbf{K})}}(D) - \mathbf{Adv}^{\Phi\text{-rka}[1]}_{\mathsf{EFN}^{\mathsf{RF}^{n,2n},6}_{\mathsf{Alter}(\mathbf{K})}}(D) \right| \leq \mathbf{Adv}^{\Phi\text{-rka}[2]}_{F^{n,2n}}(D)$$

by a standard hybrid argument.

The core step is to analyze $\mathbf{Adv}^{\Phi\text{-rka}[1]}_{\mathsf{EFN}^{\mathsf{RF}^{n,2n},6}_{\mathsf{Alter}(\mathbf{K})}}(D)$ for the random EFN, which will employ the H-coefficient technique. We will define bad transcripts and upper bound their probability in ideal world, and then show that the probabilities to obtain any good transcript in the real word and the ideal world are sufficiently close.

A.1 Bad Transcripts

Definition 5. *An attainable transcript $\tau = (\mathcal{Q}, \boldsymbol{K})$ is bad, if either of the following conditions is fulfilled:*

- *(B-1) Claw in τ: there exists two triples (ϕ_1, X_1, Y_1) and (ϕ_2, X_2, Y_2) in $\mathcal{Q}$ such that $\phi_1 \neq \phi_2$, while $\phi_1(\mathbf{K}) = \phi_2(\mathbf{K})$;*
- *(B-2) Switch in τ: there exists two triples (ϕ_1, X_1, Y_1) and (ϕ_2, X_2, Y_2) in $\mathcal{Q}$ and two indices $i, j \in \{1, 2\}$ such that $\phi_1(\mathbf{K})[i] = \phi_2(\mathbf{K})[j]$.*

Otherwise we say τ is good.

It is clear that $\Pr[\text{(B-1)}] \leq \mathbf{Adv}^{\mathsf{cf}}_{\Phi}(D)$: an adversary against the claw-freeness of the RKD set Φ could simulate the related-key oracle with Φ against the distinguisher D, collecting D's transcript of queries and responses, and use the records in $\mathcal{Q}$ to break the claw-freeness of Φ. Similarly, $\Pr[\text{(B-2)}] \leq \mathbf{Adv}^{\mathsf{sf}}_{\Phi}(D)$, and thus

$$\Pr\big[T_{\text{id}} \in \mathcal{T}_{\text{bad}}\big] = \Pr\big[\text{(B-1)} \vee \text{(B-2)}\big] \leq \mathbf{Adv}^{\mathsf{cf}}_{\Phi}(D) + \mathbf{Adv}^{\mathsf{sf}}_{\Phi}(D). \tag{24}$$

A.2 Analyzing Good Transcripts

Fix a good transcript τ. The ideal world probability simply follows from Eq. (1), and it remains to analyze $\Pr[\mathsf{RK}[\mathsf{EFN}^{\mathsf{RF}^{n,2n},6}_{\mathsf{Alter}(\mathbf{K})}] \vdash \mathcal{Q}]$. We define a "bad predicate" $\mathsf{BadF}(\mathsf{RF}^{n,2n})$ on the ideal keyed function $\mathsf{RF}^{n,2n}$, such that once $\mathsf{BadF}(\mathsf{RF}^{n,2n})$ is not fulfilled, the event $T_{id} = \tau$ is equivalent to $\mathsf{RF}^{n,2n}$ satisfying $2q$ new and distinct equations. To facilitate, for any $\mathsf{RF}^{n,2n}$ and every $(\phi_i, X_i, Y_i) \in \mathcal{Q}$, we define $X_{1,i} := X_i, X_{7,i} := Y_i$, and define the "induced intermediate values" as follows.

$$\begin{aligned} X_{2,i} &:= \Psi^{\mathsf{RF}^{n,2n}_{K_1}}(X_{1,i}), & X_{3,i} &:= \Psi^{\mathsf{RF}^{n,2n}_{K_2}}(X_{2,i}), \\ X_{5,i} &:= \big(\Psi^{\mathsf{RF}^{n,2n}_{K_1}}\big)^{-1}(X_{6,i}), & X_{6,i} &:= \big(\Psi^{\mathsf{RF}^{n,2n}_{K_2}}\big)^{-1}(X_{7,i}). \end{aligned}$$

Note that the 2nd and 3rd round intermediate values $X_{2,i}, X_{3,i}$ are derived along the "forward direction", while the 4th and 5th $X_{5,i}, X_{6,i}$ are derived along the "backward direction".

Bad predicate. The predicate $\mathsf{BadF}(\mathsf{RF}^{n,2n})$ captures various types of collisions among the "induced intermediate values". Formally, the specific definition and probability analysis are as follows.

Definition 6. *Given an ideal keyed function $\mathsf{RF}^{n,2n}$, the predicate $\mathsf{BadF}(\mathsf{RF}^{n,2n})$ is fulfilled, if any of the following nine conditions is fulfilled.*

(C-1) *There exists two indices $i, j \in \{1, ..., q\}$ such that $(\phi_i(\mathbf{K})[1], X_{1,i}[1, n]) = (\phi_j(\mathbf{K})[1], X_{3,j}[1, n])$.*
(C-2) *There exists two indices $i, j \in \{1, ..., q\}$ such that $(\phi_i(\mathbf{K})[2], X_{5,i}[2n + 1, 3n]) = (\phi_j(\mathbf{K})[2], X_{7,j}[2n + 1, 3n])$.*
(C-3) *There exists two indices $i, j \in \{1, ..., q\}$ such that $(\phi_i(\mathbf{K})[1], X_{1,i}[1, n]) = (\phi_j(\mathbf{K})[1], X_{6,j}[2n + 1, 3n])$.*
(C-4) *There exists two indices $i, j \in \{1, ..., q\}$ such that $(\phi_i(\mathbf{K})[2], X_{2,i}[1, n]) = (\phi_j(\mathbf{K})[2], X_{7,j}[2n + 1, 3n])$.*
(C-5) *There exists two indices $i, j \in \{1, ..., q\}$ such that $(\phi_i(\mathbf{K})[1], X_{3,i}[1, n]) = (\phi_j(\mathbf{K})[1], X_{6,j}[2n + 1, 3n])$.*
(C-6) *There exists two indices $i, j \in \{1, ..., q\}$ such that $(\phi_i(\mathbf{K})[2], X_{2,i}[1, n]) = (\phi_j(\mathbf{K})[2], X_{5,j}[2n + 1, 3n])$.*
(C-7) *There exists two distinct indices $i, j \in \{1, ..., q\}$ and an index $\ell \in \{1, 2\}$ such that $\big(\mathsf{Alter}(\phi_i(\mathbf{K}))[\ell], X_{\ell,i}[1, n]\big) \neq \big(\mathsf{Alter}(\phi_j(\mathbf{K}))[\ell], X_{\ell,j}[1, n]\big)$, yet $X_{\ell+1,i}[1, n] = X_{\ell+1,j}[1, n]$.*
(C-8) *There exists two distinct indices $i, j \in \{1, ..., q\}$ and an index $\ell \in \{6, 7\}$ such that $\big(\mathsf{Alter}(\phi_i(\mathbf{K}))[\ell-1], X_{\ell,i}[2n+1, 3n]\big) \neq \big(\mathsf{Alter}(\phi_j(\mathbf{K}))[\ell-1], X_{\ell,j}[2n+1, 3n]\big)$, yet $X_{\ell-1,i}[2n + 1, 3n] = X_{\ell-1,j}[2n + 1, 3n]$.*
(C-9) *There exists two distinct indices $i, j \in \{1, ..., q\}$ such that $(\phi_i(\mathbf{K})[1], X_{3,i}[1, n]) = (\phi_j(\mathbf{K})[1], X_{3,j}[1, n])$ or $(\phi_i(\mathbf{K})[2], X_{5,i}[2n+1, 3n]) = (\phi_j(\mathbf{K})[2], X_{5,j}[2n + 1, 3n])$.*

Otherwise we say τ is good.

To bound the probability, we analyze the conditions in turn.

Conditions (C-1) and (C-2). By construction, we can get that

$$X_{3,i}[1, n] = \mathsf{RF}^{n,2n}_{\phi_i(\mathbf{K})[2]}(X_{2,i}[1, n])[1, n] \oplus X_{2,i}[n + 1, 2n].$$

While for $X_{1,j}[1, n]$, which is determined by the transcripts, and dependent from $\mathsf{RF}^{n,2n}_{\phi_i(\mathbf{K})[2]}(X_{2,i}[1, n])[1, n]$. As the number of such indices is q^2, we have $\Pr\big[\text{(C-1)}\big] \leq q^2/2^n$. Similarly by symmetry, $\Pr\big[\text{(C-2)}\big] \leq q^2/2^n$.

Conditions (C-3) and (C-4). By construction, we have

$$X_{6,i}[2n + 1, 3n] = \mathsf{RF}^{n,2n}_{\phi_i(\mathbf{K})[2]}(X_{7,i}[2n + 1, 3n])[n + 1, 2n] \oplus X_{7,i}[n + 1, 2n].$$

Because of $\mathsf{RF}^{n,2n}$ is a random function, $\mathsf{RF}^{n,2n}_{\phi_i(\mathbf{K})[2]}(X_{7,i}[2n + 1, 3n])[n + 1, 2n]$ is independent of $X_{1,j}[1, n]$. Via an analysis similar as above, we reach $\Pr\big[\text{(C-3)}\big] \leq q^2/2^n$. Similarly by symmetry, $\Pr\big[\text{(C-4)}\big] \leq q^2/2^n$.

Conditions (C-5) and (C-6). Concretely, consider (C-5) first. We notice that the following equations are fulfilled.

$$X_{3,i}[1,n] = \mathsf{RF}^{n,2n}_{\phi_i(\mathbf{K})[2]}(X_{2,i}[1,n])[1,n] \oplus X_{2,i}[n+1,2n],$$
$$X_{6,i}[2n+1,3n] = \mathsf{RF}^{n,2n}_{\phi_i(\mathbf{K})[2]}(X_{7,i}[2n+1,3n])[n+1,2n] \oplus X_{7,i}[2n+1,3n].$$

The detailed analysis is as follows.
1. Case $\phi_i(\mathbf{K})[2] = \phi_j(\mathbf{K})[2]$.
Conditioned on $\neg(C-4)$, that is $X_{2,i}[1,n] \neq X_{7,j}[2n+1,3n]$. Thus $\mathsf{RF}^{n,2n}_{\phi_i(\mathbf{K})[2]}(X_{2,i}[1,n])[1,n]$ and $\mathsf{RF}^{n,2n}_{\phi_i(\mathbf{K})[2]}(X_{7,i}[2n+1,3n])[n+1,2n]$ are independent, so we have the probability of this situation is $1/2^n$. In detail,

$$\Pr\left[(C-5) \vee (C-4)\right] \leq \Pr[(C-4)] + \Pr[(C-5) \mid \neg(C-4)] \leq \frac{2q^2}{2^n}$$

2. Case $\phi_i(\mathbf{K})[2] \neq \phi_j(\mathbf{K})[2]$.
Because $\mathsf{RF}^{n,2n}$ is a ideal function, in this case the round keys are different, so $\mathsf{RF}^{n,2n}_{\phi_i(\mathbf{K})[2]}(X_{2,i}[1,n])[1,n]$ and $\mathsf{RF}^{n,2n}_{\phi_i(\mathbf{K})[2]}(X_{7,i}[2n+1,3n])[n+1,2n]$ are independent, we need not to think about whether the inputs of the round function are equal or not. So we have the probability is $\Pr[(C-5)] \leq q^2/2^n$.

In all we reach $\Pr\left[(C-5) \vee (C-4))\right] \leq 2q^2/2^n$. Similarly by symmetry, $\Pr\left[(C-6) \vee (C-3))\right] \leq 2q^2/2^n$

Conditions (C-7) and (C-8). Consider (C-7) first, and consider any such three indices $i, j \in \{1, ..., q\}$ and $\ell \in \{1, 2\}$. The equality $X_{\ell+1,i}[1,n] = X_{\ell+1,j}[1,n]$ translates into

$$\begin{aligned}&\left(\mathsf{RF}^{n,m}_{\mathsf{Alter}(\phi_i(\mathbf{K}))[\ell]}\big(X_{\ell,i}[1,n]\big) \oplus X_{\ell,i}[n+1,3n]\right)[1,n] \\ =\ &\left(\mathsf{RF}^{n,m}_{\mathsf{Alter}(\phi_j(\mathbf{K}))[\ell]}\big(X_{\ell,j}[1,n]\big) \oplus X_{\ell,j}[n+1,3n]\right)[1,n].\end{aligned}$$

Since $\big(\mathsf{Alter}(\phi_i(\mathbf{K}))[\ell], X_{\ell,i}[1,n]\big) \neq \big(\mathsf{Alter}(\phi_j(\mathbf{K}))[\ell], X_{\ell,j}[1,n]\big)$, the two function outputs $\mathsf{RF}^{n,m}_{\mathsf{Alter}(\phi_i(\mathbf{K}))[\ell]}\big(X_{\ell,i}[1,n]\big)$ and $\mathsf{RF}^{n,m}_{\mathsf{Alter}(\phi_j(\mathbf{K}))[\ell]}\big(X_{\ell,j}[1,n]\big)$ are uniform in $\{0,1\}^{2n}$ and independent. Therefore, the probability to have $X_{\ell+1,i}[1,n] = X_{\ell+1,j}[1,n]$ is $1/2^n$. Summing over the $\binom{q}{2} \cdot 2 \leq \frac{q^2}{2}2$ choices of i, j, ℓ, we reach

$$\Pr\Big[\text{(C-7)}\Big] \leq \frac{2q^2}{2^{n+1}}. \tag{25}$$

The analysis for (C-8) is similar by symmetry, yielding the same bound

$$\Pr\Big[\text{(C-8)}\Big] \leq \frac{2q^2}{2^{n+1}}. \tag{26}$$

Conditions (C-9). Consider any such two triples $(\phi_i, X_i, Y_i), (\phi_j, X_j, Y_j) \in \mathcal{Q}$. We consider the probability to have $(\phi_i(\mathbf{K})[1], X_{3,i}[1,n]) = (\phi_j(\mathbf{K})[1], X_{3,j}[1,n])$ first. In this case, the condition is fulfilled only if $\phi_i(\mathbf{K})[1] = \phi_j(\mathbf{K})[1]$. With this in mind, we distinguish two cases.

Case 1: $\phi_i \neq \phi_j$. Then since τ is good and is claw-free, it holds $\phi_i(\mathbf{K}) \neq \phi_j(\mathbf{K})$, which further implies $\phi_i(\mathbf{K})[2] \neq \phi_j(\mathbf{K})[2]$. By this, the probability to have $X_{3,i}[1,n] = X_{3,j}[1,n]$, or to have

$$\begin{aligned} &\Big(X_{2,i}[n+1,3n] \oplus \mathsf{RF}^{n,m}_{\phi_i(\mathbf{K})[2]}\big(X_{2,i}[1,n]\big)\Big)\big[1,n\big] \\ =\ &\Big(X_{2,j}[n+1,3n] \oplus \mathsf{RF}^{n,m}_{\phi_j(\mathbf{K})[2]}\big(X_{2,j}[1,n]\big)\Big)\big[1,n\big], \end{aligned} \tag{27}$$

is $1/2^n$, since $\mathsf{RF}^{n,m}_{\phi_i(\mathbf{K})[2]}$ and $\mathsf{RF}^{n,m}_{\phi_j(\mathbf{K})[2]}$ can be viewed as two independent random functions from $\{0,1\}^n$ to $\{0,1\}^{2n}$.

Case 2: $\phi_i = \phi_j$. For clearness we let $\phi = \phi_i = \phi_j$. Let $\Delta_1 := X_{1,i} \oplus X_{1,j}$. Since D does not make redundant queries, it has to be $\Delta_1 \neq 0$. We further distinguish two subcases.

- Subcase 2.1: $\Delta_1[1,2n] \neq 0$. Then, let $\ell \in \{0,1\}$ be the smallest index such that $\Delta_1[\ell n+1,(\ell+1)n] \neq 0$. By construction, this means $X_{\ell+1,i}[1,n] \neq X_{\ell+1,j}[1,n]$. Conditioned on $\neg$(C-7), this further implies $X_{3,i}[1,n] \neq X_{3,j}[1,n]$.
- Subcase 2.2: $\Delta_1[1,2n] = 0$. Then it has to be $\Delta_1[2n+1,3n] \neq 0$, which necessarily implies $X_{3,i}[1,n] \neq X_{3,j}[1,n]$ by construction.

Therefore, conditioned on $\neg$(C-7), it is not possible to have $X_{3,i}[1,n] = X_{3,j}[1,n]$ for any two distinct indices (i,j).

The analysis for $\big(\phi_i(\mathbf{K})[2], X_{5,i}[2n+1,3n]\big) = \big(\phi_j(\mathbf{K})[2], X_{5,j}[2n+1,3n]\big)$ is similar by symmetry. More concretely, for any such two triples $(\phi_i, X_i, Y_i), (\phi_j, X_j, Y_j)$ such that $\phi_i(\mathbf{K})[2] = \phi_j(\mathbf{K})[2]$, we have:

- If $\phi_i \neq \phi_j$, then it holds $\phi_i(\mathbf{K})[1] \neq \phi_j(\mathbf{K})[1]$ by the claw-freeness and by $\phi_i(\mathbf{K})[2] = \phi_j(\mathbf{K})[2]$, and thus the probability to have $X_{5,i}[2n+1,3n] = X_{5,j}[2n+1,3n]$ or

$$\begin{aligned} &\Big(X_{6,i}[1,2n] \oplus \mathsf{RF}^{n,2n}_{\phi_i(\mathbf{K})[1]}\big(X_{6,i}[2n+1,3n]\big)\Big)\big[n+1,2n\big] \\ =\ &\Big(X_{6,j}[1,m] \oplus \mathsf{RF}^{n,2n}_{\phi_j(\mathbf{K})[1]}\big(X_{6,j}[2n+1,3n]\big)\Big)\big[n+1,2n\big] \end{aligned} \tag{28}$$

  is $1/2^n$ due to the independence between $\mathsf{RF}^{n,2n}_{\phi_i(\mathbf{K})[1]}$ and $\mathsf{RF}^{n,2n}_{\phi_j(\mathbf{K})[1]}$.
- If $\phi_i = \phi_j$, then it is not possible to have $X_{5,i}[2n+1,3n] = X_{5,j}[2n+1,3n]$ conditioned on $\neg$(C-8).

In all, for each pair (i,j) of distinct indices, the probability to have $X_{3,i}[1,n] = X_{3,j}[1,n]$ or $X_{5,i}[2n+1,3n] = X_{5,j}[2n+1,3n]$ is no larger than $2/2^n$. Taking a union bound for the $\binom{q}{2} \leq q^2/2$ choices of (i,j) yields

$$\Pr\Big[\text{(C-9)} \mid \neg\text{(C-1)} \wedge \ldots \wedge \neg\text{(C-8)}\Big] \leq \frac{q^2}{2^n}. \tag{29}$$

Summing over the above, we reach

$$\Pr\big[\mathsf{BadF}(\mathsf{RF}^{n,2n})\big] \leq \frac{9q^2}{2^n}. \tag{30}$$

Completing the proof. Consider any good transcript $\tau = (\mathcal{Q}, \mathbf{K})$, where $\mathcal{Q} = \big((\phi_1, X_1, Y_1), ..., (\phi_q, X_q, Y_q)\big)$. It can be seen that the event $\mathsf{RK}[\mathsf{EFN}^{\mathsf{RF}^{n,2n},6}_{\mathsf{Alter}(\mathbf{K})}] \vdash \mathcal{Q}$ is equivalent to the event that $\mathsf{RF}^{n,2n}$ satisfies $2q$ equations as follows.

$$\begin{aligned}
&\mathsf{RF}_{\phi_i(\mathbf{K})[1]}(X_{3i}[1,n]) = X_{3i}[n+1,2n] \oplus X_{5i}[2n+1,3n] \\
&\qquad\qquad \big\| \;\; X_{3i}[2n+1,3n] \oplus \mathsf{RF}_{\phi_i(\mathbf{K})[2]}(X_{5i}[2n+1,3n])[1,n] \oplus X_{5i}[1,n] \\
&\mathsf{RF}_{\phi_i(\mathbf{K})[2]}(X_{5i}[2n+1,3n])[n+1,2n] = X_{3i}[1,n] \oplus X_{5i}[n+1,2n].
\end{aligned}$$

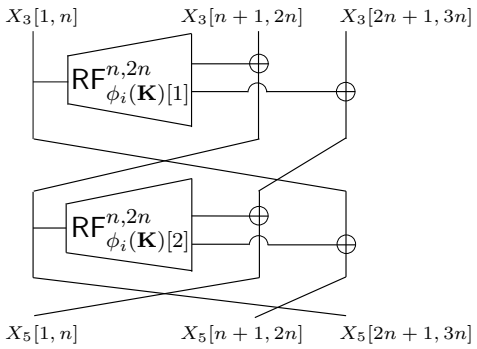

Fig. 3. 3-round and 4-round in $\mathsf{EFN}^{\mathsf{RF}^{n,2n},6}_{\mathsf{Alter}(\mathbf{K})}$

The probability to obtain τ in the real world is

$$\begin{aligned}
&\Pr[T_{\mathrm{re}} = \tau] = \Pr[\mathbf{K}] \cdot \Pr\big[\mathsf{RK}[\mathsf{EFN}^{\mathsf{RF}^{n,2n},6}_{\mathsf{Alter}(\mathbf{K})}] \vdash \mathcal{Q}\big] \\
&\geq \Pr[\mathbf{K}] \cdot \Pr\big[\mathsf{RK}[\mathsf{EFN}^{\mathsf{RF}^{n,2n},6}_{\mathsf{Alter}(\mathbf{K})}] \vdash \mathcal{Q} \wedge \neg\mathsf{BadF}(\mathsf{RF}^{n,2n})\big] \\
&= \Pr[\mathbf{K}] \cdot \Big(1 - \Pr\big[\mathsf{BadF}(\mathsf{RF}^{n,2n})\big]\Big) \cdot \Pr\big[\mathsf{RK}[\mathsf{EFN}^{\mathsf{RF}^{n,2n},6}_{\mathsf{Alter}(\mathbf{K})}] \vdash \mathcal{Q} \mid \neg\mathsf{BadF}(\mathsf{RF}^{n,2n})\big].
\end{aligned}$$

We refer to Fig. 3 for illustration. Conditioned on $\neg\mathsf{BadF}(\mathsf{RF}^{n,2n})$, these are $2q$ distinct and new equations. Therefore,

$$\begin{aligned}
&\Pr\big[\mathsf{RK}[\mathsf{EFN}^{\mathsf{RF}^{n,2n},6}_{\mathsf{Alter}(\mathbf{K})}] \vdash \mathcal{Q} \mid \neg\mathsf{BadF}(\mathsf{RF}^{n,2n})\big] \\
&= \prod_{i=1}^{q} \Big(\Pr\big[\mathsf{RF}_{\phi_i(\mathbf{K})[1]}(X_{3i}[1,n]) = X_{3i}[n+1,2n] \oplus X_{5i}[2n+1,3n] \\
&\qquad\qquad \big\| \;\; X_{3i}[2n+1,3n] \oplus \mathsf{RF}_{\phi_i(\mathbf{K})[2]}(X_{5i}[2n+1,3n])[1,n] \oplus X_{5i}[1,n]\big] \\
&\quad \times \Pr\big[\mathsf{RF}_{\phi_i(\mathbf{K})[2]}(X_{5i}[2n+1,3n])[n+1,2n] = X_{3i}[1,n] \oplus X_{5i}[n+1,2n]\big] \Big) \\
&= \Big(\frac{1}{2^{3n}}\Big)^q.
\end{aligned}$$

We remark that, the equation on $\mathsf{RF}_{\phi_i(\mathbf{K})[1]}(X_{3i}[1,n])$ depends on the function value $\mathsf{RF}_{\phi_i(\mathbf{K})[2]}(X_{5i}[2n+1,3n])[1,n]$. Though, this won't affect the distribution of $\mathsf{RF}_{\phi_i(\mathbf{K})[2]}(X_{5i}[2n+1,3n])[n+1,2n]$, as the two halves $\mathsf{RF}_{\phi_i(\mathbf{K}))[2]}(X_{5i}[2n+1,3n])[1,n]$ and $\mathsf{RF}_{\phi_i(\mathbf{K})[2]}(X_{5i}[2n+1,3n])[n+1,2n]$ are independent. In all, using Eq. (30), we have

$$\begin{aligned}\frac{\Pr[T_{\mathrm{re}}=\tau]}{\Pr[T_{\mathrm{id}}=\tau]} &\geq \Big(1-\frac{9q^2}{2^n}\Big)\times\Big(\frac{1}{2^{3n}}\Big)^q\Big/\Big(\frac{1}{2^{3n}-q}\Big)^q \\ &\geq 1-\Big(\frac{9q^2}{2^n}+\frac{q^2}{2^{3n}}\Big). \end{aligned} \tag{31}$$

Gathering Eqs (24) and (31), and using Lemma 1, we complete the proof of Theorem 3.