SCIENCE CHINA
Information Sciences

• **Supplementary File** •

Secure Key-Alternating Feistel Ciphers Without Key Schedule

Yaobin SHEN[1], Hailun YAN[1], Lei WANG[1,2*] & Xuejia LAI[1,2]

[1]*Department of Computer Science and Engineering, Shanghai Jiao Tong University, Shanghai* 200240*, China;*
[2]*Westone Cryptologic Research Center, Beijing* 100070*, China*

Appendix A Preliminaries

Notation. If $\mathcal{X}$ is a set, then $X \xleftarrow{\$} \mathcal{X}$ denotes the operation of picking X from $\mathcal{X}$ uniformly at random. $\{0,1\}^n$ denotes the set of all n-bit strings. We denote $N = 2^n$ for simplicity. For any two strings X, Y of equal length, $X \oplus Y$ denotes their bitwise exclusive-or, and $X||Y$ denotes their concatenation. $|X|$ denotes the bit length of string X. $\mathrm{Func}(n)$ denotes the set of all functions from $\{0,1\}^n$ to $\{0,1\}^n$, and $\mathrm{Perm}(n)$ denotes the set of all permutation on $\{0,1\}^n$.

Key-Alternating Feistel Cipher. Given a function $f : \{0,1\}^n \to \{0,1\}^n$ and a n-bit key K, define the permutation Ψ_K^f on $\{0,1\}^{2n}$ as $\Psi_K^f(L\|R) = (R, L \oplus f(R \oplus K))$ where L and R are respectively the left and right n-bit halves of the input. A key-alternating Feistel cipher (`KAF`) with r rounds is specified by r public random functions $f = (f_1, \ldots, f_r)$ from $\{0,1\}^n$ to $\{0,1\}^n$ and a round-key vector $K = (K_1, \ldots, K_r)$ (denote by $\mathcal{K}$ the set of all key K):

$$\mathtt{KAF}_K^f(L\|R) = \Psi_{K_r}^{f_r} \circ \cdots \circ \Psi_{K_1}^{f_1}(L\|R).$$

These functions may be completely independent, or correlated or even identical. In particular, we denote by `KAFSF` the variant of `KAF` with identical round function, i.e.,

$$\mathtt{KAFSF}_K^f(L\|R) = \Psi_{K_r}^{f} \circ \cdots \circ \Psi_{K_1}^{f}(L\|R).$$

The key spaces of these schemes are not fixed and depend on the concrete contexts.

Security Definitions. We define two types of security notion with respect to the ability of the adversary $\mathcal{A}$, namely pseudorandomness permutation (PRP) and strong pseudorandomness permutation (SPRP), where in the former $\mathcal{A}$ can only make encryption queries to the blockcipher while in the latter $\mathcal{A}$ can make both encryption and decryption queries to the blockcipher. Formally, for any q_e and q_f, we define the PRP security of a r-round key-alternating Feistel cipher `KAF` as

$$\begin{aligned}&\mathbf{Adv}_{\mathtt{KAF}}^{\mathrm{prp}}(q_e, q_f)\\ =\ &\max_{\mathcal{A}} |\Pr[K \xleftarrow{\$} \mathcal{K}, f \xleftarrow{\$} (\mathrm{Func}(n))^r : \mathcal{A}^{\mathtt{KAF},f} = 1] - \Pr[\pi \xleftarrow{\$} \mathrm{Perm}(n), f \xleftarrow{\$} (\mathrm{Func}(n))^r : \mathcal{A}^{\pi,f} = 1]|\end{aligned}$$

where the maximal is taken over all distinguishers $\mathcal{A}$ that ask at most q_e encryption queries to the permutation oracle and at most q_f queries to each function oracle. Similarly, we define the SPRP security of `KAF` as

$$\begin{aligned}&\mathbf{Adv}_{\mathtt{KAF}}^{\mathrm{sprp}}(q_e, q_f)\\ =\ &\max_{\mathcal{A}} |\Pr[K \xleftarrow{\$} \mathcal{K}, f \xleftarrow{\$} (\mathrm{Func}(n))^r : \mathcal{A}^{\mathtt{KAF},\mathtt{KAF}^{-1},f} = 1] - \Pr[\pi \xleftarrow{\$} \mathrm{Perm}(n), f \xleftarrow{\$} (\mathrm{Func}(n))^r : \mathcal{A}^{\pi,\pi^{-1},f} = 1]|\end{aligned}$$

where the maximal is taken over all distinguishers $\mathcal{A}$ that asks at most q_e queries to the permutation oracle and at most q_f queries to each function oracle.

* Corresponding author (email: wanglei_hb@sjtu.edu.cn)

The H-coefficient Technique. Following the notation from Hoang and Tessaro [1], it is useful to consider interactions between an adversary $\mathcal{A}$ with an abstract system $\mathtt{S}$ which answers $\mathcal{A}$'s queries. The resulting interaction can then be recorded with a transcript $\tau = ((X_1, Y_1), \ldots, (X_q, Y_q)$. Let $\mathrm{p}_{\mathtt{S}}(\tau)$ denote the probability that $\mathtt{S}$ produces τ. It is known that $\mathrm{p}_{\mathtt{S}}(\tau)$ is the description of $\mathtt{S}$ and independent of the adversary $\mathcal{A}$. Let X denote the probability distribution of the transcript τ when $\mathcal{A}$ interacting with $\mathtt{S}$. We say that a transcript is attainable for system $\mathtt{S}$ if $\Pr[X = \tau] > 0$.

We now describe the H-coefficient technique of Patarin [2, 3]. Generically, it considers an adversary that aims at distinguishing a "real" system $\mathtt{S}_{\mathtt{re}}$ from an "ideal" system $\mathtt{S}_{\mathtt{id}}$. The interactions of adversary with those systems induce two transcript distributions $X_{\mathtt{re}}$ and $X_{\mathtt{id}}$ respectively. It is well known that the statistical distance $\mathtt{SD}(X_{\mathtt{re}}, X_{\mathtt{id}})$ is an upper bound on the distinguishing advantage of $\mathcal{A}$.

Lemma 1. [2, 3] Let $\Theta = \Theta_{\mathrm{good}} \sqcup \Theta_{\mathrm{bad}}$ be the set of attainable transcripts for ideal system $\mathtt{S}_{\mathtt{id}}$. If there exists $\epsilon \geqslant 0$ such that for any $\tau \in \Theta_{\mathrm{good}}$, it has

$$\frac{\mathrm{p}_{\mathtt{S}_{\mathtt{re}}}(\tau)}{\mathrm{p}_{\mathtt{S}_{\mathtt{id}}}(\tau)} \geqslant 1 - \epsilon.$$

Then $\mathtt{SD}(X_{\mathtt{re}}, X_{\mathtt{id}}) \leqslant \epsilon + \Pr[X_{\mathtt{id}} \in \Theta_{\mathrm{bad}}]$.

At the end of this section, we introduce a simple and efficient operation, i.e. one-bit rotation ε. It has been used in Luby-Rackoff construction [4, 5]. Note that the gap between Luby-Rackoff Feistel construction and key-alternating Feistel construction is non-negligible and one cannot simply borrow the security results of the former to the latter. We will use the following useful property of ε in our construction. The proof can be found in [4].

Lemma 2. Let ε be the rotation of one bit. Then for any $c \in \{0,1\}^n$,

$$\Pr[x \xleftarrow{\$} \{0,1\}^n : x \oplus \varepsilon(x) = c] \leqslant \frac{2}{N}.$$

Appendix B Proof for Theorem 1

Theorem 1. For the four-round single-key KAFSF without key schedule, it holds

$$\mathbf{Adv}^{\mathrm{sprp}}_{\mathtt{KAFSF}}(q_e, q_f) \leqslant \frac{4q_e q_f}{N} + \frac{13q_e^2}{N} + \frac{q_e^2}{2N^2}.$$

In the remaining of this section, we will use H-coefficient technique to prove Theorem 1. Following the H-coefficient framework in Appendix A, the real system $\mathtt{S}_{\mathtt{re}}$ here is a pair of oracles $(\mathtt{KAFSF}, f)$ while the ideal system $\mathtt{S}_{\mathtt{id}}$ is a pair of oracles (π, f), where f is the public random function in KAFSF and π is a perfect $2n$-bit random permutation. The adversary $\mathcal{A}$ is assumed to be computationally unbounded and hence deterministic without loss of generality. $\mathcal{A}$ is also assumed to never make repeated queries since it only receives the same response if asking the same query. The interactions of $\mathcal{A}$ with its system is recorded by a pair of $(\mathcal{Q}_E, \mathcal{Q}_F)$, where $\mathcal{Q}_E = ((L_1 \| R_1, S_1 \| T_1), \ldots, (L_{q_e} \| R_{q_e}, S_{q_e} \| T_{q_e}))$ is the q_e construction query-response tuples when interacting with the permutation oracle (KAFSF in system $\mathtt{S}_{\mathtt{re}}$ or π in system $\mathtt{S}_{\mathtt{id}}$), and $\mathcal{Q}_F = ((x_1, y_1), \ldots, (x_{q_f}, y_{q_f}))$ is the q_f primitive query-response tuples when interacting with the function oracle f. For convenience, we will slightly modify the security experiment by revealing to the adversary $\mathcal{A}$ the secret key K in the real system, or a "dummy" key K chosen uniformly at random from $\{0,1\}^n$ if in the ideal system. Note that this can only enlarge the distinguishing advantage of the adversary $\mathcal{A}$ because it can simply ignore this piece of information if it wants. All in all, the transcript of the attack is encoded by the triplet $\tau = (\mathcal{Q}_E, \mathcal{Q}_F, K)$.

Bad Transcripts. Denote by Θ the set of all attainable transcripts for ideal system $\mathtt{S}_{\mathtt{id}}$, denote by $\mathcal{Q}_F^+ = \{x_1, \ldots, x_{q_f}\}$ the set of input values to function f. We begin our proof by defining bad transcripts.

Definition 1. We say a transcript $\tau = (\mathcal{Q}_E, \mathcal{Q}_F, K)$ is bad if there exists $(L \| R, S \| T) \in \mathcal{Q}_E$ and $x \in \mathcal{Q}_F^+$ such that $R \oplus K = x$ or $S \oplus K = x$. Denote by Θ_{bad}, resp. Θ_{good} the set of bad, respectively good transcripts.

We upper bound the probability to obtaining a bad transcript in the ideal world.

Lemma 3. For any integers q_e and q_f, one has

$$\Pr[X_{\mathtt{id}} \in \Theta_{\mathrm{bad}}] \leqslant \frac{2q_e q_f}{N}.$$

Proof. For each of $q_e q_f$ pairs of (LR, ST) and x, the event $(K \oplus R = x \vee K \oplus S = x)$ happens with probability at most $2/N$ since K is uniformly chosen. Hence by the union bound, the probability that τ is bad is at most $2q_e q_f / N$.

Analysis of Good Transcripts. We now analyze good transcripts when adversary $\mathcal{A}$ interacting with these two systems. Let $\tau = (\mathcal{Q}_E, \mathcal{Q}_F, K)$ be a good transcript. Since in the ideal system, the construction oracle is a perfect $2n$-bit random permutation and independent of the function f, we simply have

$$\mathrm{p}_{\mathtt{S}_{\mathtt{id}}}(\tau) = \frac{1}{|\mathcal{K}| \cdot N^{q_f}} \cdot \prod_{i=0}^{q_e - 1} \frac{1}{N^2 - i}. \tag{B1}$$

We now proceed to lower bound the probability to obtain a good transcript in the real system. For $1 \leqslant i \leqslant q_e$, we denote by $X_i = \varepsilon(f(R_i \oplus K)) \oplus L_i$ the input to the second round function, and $Y_i = f(S_i \oplus K) \oplus T_i$ the input to the third round function. We define some bad conditions as follows:

c.1 there exists some i such that $X_i \in \mathcal{Q}_F^+$ or $Y_i \in \mathcal{Q}_F^+$;

c.2 there exists a pair of (i, j) for $i \neq j$ satisfying at least one of the following conditions:
c.2.1 $X_i \in \{R_i \oplus K, Y_i, S_i \oplus K, R_j \oplus K, X_j, Y_j, S_j \oplus K\}$;
c.2.2 $Y_i \in \{R_i \oplus K, S_i \oplus K, R_j \oplus K, X_j, Y_j, S_j \oplus K\}$;
c.2.3 $X_j \in \{R_i \oplus K, S_i \oplus K, R_j \oplus K, Y_j, S_j \oplus K\}$;
c.2.4 $Y_j \in \{R_i \oplus K, S_i \oplus K, R_j \oplus K, S_j \oplus K\}$.

If none of above conditions is fulfilled, then given tuples $\mathcal{Q}_F$ and a key K, the occurrence of τ in the real system is equivalent to the event of $2q_e$ new and distinct equations on the random round-function f, which is relatively easy to compute. We first consider the first bad condition. Since both $R_i \oplus K$ and $S_i \oplus K$ are fresh inputs to function f, the values X_i and Y_i remain uniformly distributed. Hence by the union bound

$$\Pr[\text{c.1}] \leqslant \frac{2q_e q_f}{N}.$$

We then analyze the condition *c*.2.1:

• For any element $x \in \{R_i \oplus K, S_i \oplus K, R_j \oplus K, S_j \oplus K\}$, the equation $X_i = x$ holds with probability at most $1/N$ because X_i is uniformly distributed.

• For $x = Y_i$, if $S_i = R_i$, then $\Pr[X_i = x] = \Pr[\varepsilon(f(R_i \oplus K)) \oplus f(R_i \oplus K) = L_i \oplus T_i] = 2/N$ due to Lemma 2. Otherwise $\Pr[X_i = x] = 1/N$ since both $f(R_i \oplus K)$ and $f(S_i \oplus K)$ are uniformly distributed and independent of each other.

• For $x = X_j$, if $R_i \neq R_j$, then $\Pr[X_i = x] = 1/N$ since both $\varepsilon(f(R_i \oplus K))$ and $\varepsilon(f(R_j \oplus K))$ are uniformly distributed and independent of each other. If $R_i = R_j$, then necessarily $X_i \neq x$ since otherwise this would contradict the hypothesis that $L_i R_i$ and $L_j R_j$ are two distinct queries.

• For $x = Y_j$, if $R_i \neq S_j$, then $\Pr[X_i = x] = 1/N$ since both $\varepsilon(f(R_i \oplus K))$ and $f(S_j \oplus K) \oplus T_j$ are uniformly distributed and independent of each other. Otherwise $\Pr[X_i = x] = \Pr[\varepsilon(f(R_i \oplus K)) \oplus f(S_j \oplus K) = L_i \oplus T_j] = 2/N$ which comes from Lemma 2.

By the union bound and summing over above terms, for any pair (i, j), we have

$$\Pr[c.2.1] \leqslant \frac{9}{N}.$$

By similar arguments, we can obtain

$$\Pr[c.2.2] \leqslant \frac{7}{N},$$

and

$$\Pr[c.2.3] \leqslant \frac{6}{N},$$

and

$$\Pr[c.2.4] \leqslant \frac{4}{N},$$

for any pair (i, j). Since there are at most $\binom{q_e}{2}$ such pairs, the probability of the occurrence of event *c*.2 is at most

$$\Pr[c.2] \leqslant \binom{q_e}{2} \cdot \frac{26}{N} \leqslant \frac{13q_e^2}{N}.$$

As mentioned before, if none of above bad conditions is fulfilled, then given tuples $\mathcal{Q}_F$ and a key K, the probability $\mathrm{ps}_{\mathtt{re}}(\tau)$ is equivalent to the probability of below event:

$$\begin{aligned} f(X_1) &= R_1 \oplus Y_1, \ldots, f(X_{q_e}) = R_{q_e} \oplus Y_{q_e}, \\ f(Y_1) &= S_1 \oplus X_1, \ldots, f(Y_{q_e}) = S_{q_e} \oplus X_{q_e}, \end{aligned}$$

where $X_1, \ldots, X_{q_e}, Y_1, \ldots, Y_{q_e}$ are $2q_e$ fresh and distinct input values to random function f. It is clear that this event holds with probability $1/N^{2q_e}$. Hence for any $\tau \in \Theta_{\mathrm{good}}$,

$$\begin{aligned} \frac{\mathrm{ps}_{\mathtt{re}}(\tau)}{\mathrm{ps}_{\mathtt{id}}(\tau)} &\geqslant \frac{\frac{1}{|\mathcal{K}| \cdot N^{q_f}} \cdot (1 - \frac{2q_e q_f}{N} - \frac{13q_e^2}{N}) \cdot \frac{1}{N^{2q_e}}}{\frac{1}{|\mathcal{K}| \cdot N^{q_f}} \cdot \prod_{i=0}^{q_e-1} \frac{1}{N^2 - i}} \\ &\geqslant (1 - \frac{2q_e q_f}{N} - \frac{13q_e^2}{N}) \cdot (1 - \frac{q_e^2}{2N^2}) \\ &\geqslant 1 - \frac{2q_e q_f}{N} - \frac{13q_e^2}{N} - \frac{q_e^2}{2N^2}. \end{aligned}$$

Applying Lemma 1 and combining above equation and Lemma 3, the distinguishing advantage of the adversary $\mathcal{A}$ can be bounded by

$$\mathtt{SD}(X_{\mathtt{re}}, X_{\mathtt{id}}) \leqslant \frac{4q_e q_f}{N} + \frac{13q_e^2}{N} + \frac{q_e^2}{2N^2},$$

which concludes the proof of Theorem 1.

Appendix C Proof for Theorem 2

Theorem 2. For 3-round single-key KAFSF using an orthomorphism φ as the key-schedule function, it holds

$$\mathbf{Adv}^{\mathrm{prp}}_{\mathtt{KAFSF}}(q_e, q_f) \leqslant \frac{3q_e q_f}{N} + \frac{6q_e^2}{N} + \frac{q_e^2}{2N^2}.$$

In the remaining of this section, we will use H-coefficient technique to prove Theorem 2.

Figure C1: Left: 3-round single-key KAFSF without key schedule, where ε is the rotation of one bit. Right: 3-round single-key KAFSF with key-schedule function φ.

Bad Transcripts. We use exactly the same notations as in the proof of 4-round KAFSF in Section Appendix B. Note that here we only allow the adversary $\mathcal{A}$ to make encryption queries since we are aiming at proving PRP security. Let $\tau = (\mathcal{Q}_E, \mathcal{Q}_F, K)$ be the transcript that records the interactions of the adversary $\mathcal{A}$ with those systems, where $\mathcal{Q}_E = ((L_1\|R_1, S_1\|T_1), \ldots, (L_{q_e}\|R_{q_e}, S_{q_e}\|T_{q_e}))$ and $\mathcal{Q}_F = ((x_1, y_1), \ldots, (x_{q_f}, y_{q_f}))$. Denote by $\mathcal{Q}_F^+ = \{x_1, \ldots, x_{q_f}\}$ the set of input values to function f. Denote by $X_{\mathtt{re}}$ resp. $X_{\mathtt{id}}$ the transcript distribution when $\mathcal{A}$ interacting with system $\mathtt{S}_{\mathtt{re}} = (\mathtt{KAFSF}, f)$, respectively system $\mathtt{S}_{\mathtt{id}} = (\pi, f)$. We then define bad transcripts.

Definition 2. We say that an attainable transcript $\tau = (\mathcal{Q}_E, \mathcal{Q}_F, K)$ is bad if at least one of the following conditions is fulfilled:

- there exists two distinct construction queries $(L_i\|R_i, S_i\|T_i)$ and $(L_j\|R_j, S_j\|T_j)$ in $\mathcal{Q}_E$ such that $S_i = S_j$;
- there exists $(L_i\|R_i, S_i\|T_i) \in \mathcal{Q}_E$ and $x_j \in \mathcal{Q}_F^+$ such that $K \oplus R_i = x_j$ or $\varphi(K) \oplus S_i = x_j$;
- there exists two (not necessarily distinct) $(L_i\|R_i, S_i\|T_i)$ and $(L_j\|R_j, S_j\|T_j)$ in $\mathcal{Q}_E$ such that $R_i \oplus K = S_j \oplus \varphi(K)$;

Denote by Θ_{bad}, resp. Θ_{good} the set of bad, respectively good transcripts.

We then upper bound the chance to obtain a bad transcript in the ideal world.

Lemma 4 (Bad Transcripts)**.** For any integers q_e and q_f, one has

$$\Pr[X_{\mathtt{id}} \in \Theta_{\text{bad}}] \leqslant \frac{q_e^2}{2(N+1)} + \frac{2q_eq_f + q_e^2}{N}.$$

Proof. We consider these three conditions one by one. Firstly, for each of the $\binom{q_e}{2}$ pairs of $(L_i\|R_i, S_i\|T_i)$ and $(L_j\|R_j, S_j\|T_j)$, the event of $S_i = S_j$ occurs with probability at most $N^2(N-1)/N^2(N^2-1) = 1/(N+1)$ because in the ideal world π is a perfect $2n$-bit random permutation and independent of the function f. For each of the q_eq_f pairs of $(L_i\|R_i, S_i\|T_i)$ and x_j, the chance of the event $(K \oplus R_i = x_j \vee \varphi(K) \oplus S_i = x_j)$ occurring is at most $2/N$ since K is uniformly chosen and φ is a permutation over $\{0,1\}^n$. On the other hand, for each of the q_e^2 pairs of $(L_i\|R_i, S_i\|T_i)$ and $(L_j\|R_j, S_j\|T_j)$ (not necessarily distinct), the probability of the event $R_i \oplus K = S_j \oplus \varphi(K)$ occurring is at most $1/N$ since K is uniformly chosen and φ is an orthomorphisms. Hence by the union bound,

$$\Pr[X_{\mathtt{id}} \in \Theta_{\text{bad}}] \leqslant \frac{q_e^2}{2(N+1)} + \frac{2q_eq_f + q_e^2}{N},$$

which concludes the proof.

Analysis for Good Transcripts. Let $\tau = (\mathcal{Q}_E, \mathcal{Q}_F, K)$ be a good transcript. Since in the ideal world, the construction π is a perfect $2n$-bit random permutation and independent of the internal function f, we simply have

$$\Pr[X_{\mathtt{id}} = \tau] = \frac{1}{|\mathcal{K}| \cdot N^{q_f}} \cdot \prod_{i=0}^{q_e-1} \frac{1}{N^2 - i}. \tag{C1}$$

We then lower bounding the probability to obtaining τ in the real world. For $1 \leqslant i \leqslant q_e$, we denote by $X_i = f(R_i \oplus K) \oplus L_i$ the input to the second round function. We define two bad conditions as follows:

c.1 there exists some i such that $X_i \in \mathcal{Q}_F^+$;

c.2 there exists a pair of (i, j) for $i \neq j$ satisfying at least one of the following conditions:

c.2.1 $X_i \in \{R_i \oplus K, S_i \oplus \varphi(K), R_j \oplus K, X_j, S_j \oplus \varphi(K)\}$;

c.2.2 $X_j \in \{R_i \oplus K, S_i \oplus \varphi(K), R_j \oplus K, S_j \oplus \varphi(K)\}$.

If none of above conditions is fulfilled, then given the tuples $\mathcal{Q}_F$ and a key K, the probability of $X_{\mathtt{re}} = \tau$ is equivalent to the probability of $2q_e$ new and distinct equations on the random round-function f. We bound the probability of above conditions first. We begin with the first condition. Since τ is good, the value of $f(R_i \oplus K)$ remains uniformly distributed, and hence

$$\Pr[c.1] \leqslant \frac{q_eq_f}{N}.$$

Next we consider the condition c.2.1:

• For any $x \in \{R_i \oplus K, S_i \oplus \varphi(K), R_j \oplus K, S_j \oplus \varphi(K)\}$, the event of $X_i = x$ happens with probability at most $1/N$ since $f(R_i \oplus K)$ is uniformly distributed;

• For $x = X_j$, if $R_i \neq R_j$, then $\Pr[X_i = x] = 1/N$ since both $f(R_i \oplus K)$ and $f(R_j \oplus K)$ are uniformly distributed and independent of each other. If $R_i = R_j$, then necessarily $X_i \neq x$ since otherwise this would contradict the hypothesis that $L_i \| R_i$ and $L_j \| R_j$ are two distinct queries.

By the union bound, for any pair (i, j), we have

$$\Pr[c.2.1] \leqslant \frac{5}{N}.$$

By similar arguments,

$$\Pr[c.2.2] \leqslant \frac{4}{N}.$$

Since there are $\binom{q_e}{2}$ such pairs, the event $c.2$ happens with probability at most

$$\Pr[c.2] \leqslant \binom{q_e}{2} \cdot \frac{9}{N} \leqslant \frac{9q_e^2}{2N}.$$

As mentioned before, if none of above bad conditions is met, given the tuples $\mathcal{Q}_F$ and a key K, the event $X_{\mathtt{re}} = \tau$ is equivalent to the event:

$$\begin{aligned} f(X_1) &= R_1 \oplus S_1, \ldots, f(X_{q_e}) = R_{q_e} \oplus S_{q_e}, \\ f(S_1 \oplus \varphi(K)) &= X_1 \oplus T_1, \ldots, f(S_{q_e} \oplus \varphi(K)) = X_{q_e} \oplus T_{q_e}, \end{aligned}$$

where $X_1, \ldots, X_{q_e}, S_1 \oplus \varphi(K), \ldots, S_{q_e} \oplus \varphi(K)$ are $2q_e$ fresh and distinct inputs to random function f due the goodness of τ and the excursion of bad conditions $c.1$ and $c.2$. Hence for any good τ,

$$\begin{aligned} \frac{\Pr[X_{\mathtt{re}} = \tau]}{\Pr[X_{\mathtt{id}} = \tau]} &\geqslant \frac{\frac{1}{|\mathcal{K}| \cdot N^{q_f}} \cdot (1 - \frac{q_e q_f}{N} - \frac{9q_e^2}{2N}) \cdot \frac{1}{N^{2q_e}}}{\frac{1}{|\mathcal{K}| \cdot N^{q_f}} \cdot \prod_{i=0}^{q_e - 1} \frac{1}{N^2 - i}} \\ &\geqslant (1 - \frac{q_e q_f}{N} - \frac{9q_e^2}{2N}) \cdot (1 - \frac{q_e^2}{2N^2}) \\ &\geqslant 1 - \frac{q_e q_f}{N} - \frac{9q_e^2}{2N} - \frac{q_e^2}{2N^2}. \end{aligned}$$

Combining above equation and Lemma 4 and applying Lemma 1, the distinguishing advantage of the adversary $\mathcal{A}$ can be bounded by

$$\begin{aligned} \mathtt{SD}(X_{\mathtt{re}}, X_{\mathtt{id}}) &\leqslant \frac{q_e q_f}{N} + \frac{9q_e^2}{2N} + \frac{q_e^2}{2N^2} + \frac{q_e^2}{2(N+1)} + \frac{2q_e q_f + q_e^2}{N} \\ &\leqslant \frac{3q_e q_f}{N} + \frac{6q_e^2}{N} + \frac{q_e^2}{2N^2}, \end{aligned}$$

which concludes the proof of Theorem 2.

References

1 Hoang V T, Tessaro S. Key-alternating ciphers and key-length extension: exact bounds and multi-user security[C]//Annual International Cryptology Conference. Springer, Berlin, Heidelberg, 2016: 3-32.

2 Patarin J. The "coefficients H" technique[C]//International Workshop on Selected Areas in Cryptography. Springer, Berlin, Heidelberg, 2008: 328-345.

3 Chen S, Steinberger J. Tight security bounds for key-alternating ciphers[C]//Annual International Conference on the Theory and Applications of Cryptographic Techniques. Springer, Berlin, Heidelberg, 2014: 327-350.

4 Patarin J. How to construct pseudorandom and super pseudorandom permutations from one single pseudorandom function[C]//Workshop on the Theory and Application of of Cryptographic Techniques. Springer, Berlin, Heidelberg, 1992: 256-266.

5 Nandi M. The characterization of Luby-Rackoff and its optimum single-key variants[C]//International Conference on Cryptology in India. Springer, Berlin, Heidelberg, 2010: 82-97.