Improved Differential Cryptanalysis on Generalized Feistel Schemes

Ivan Tjuawinata(✉), Tao Huang, and Hongjun Wu

Division of Mathematical Sciences, School of Physical and Mathematical Sciences, Nanyang Technological University, Singapore, Singapore
S120015@e.ntu.edu.sg, {huangtao,wuhj}@ntu.edu.sg

Abstract. Nachef *et al.* used differential cryptanalysis to study four types of Generalized Feistel Scheme (GFS). They gave the lower bound of maximum number of rounds that is indistinguishable from a random permutation. In this paper, we study the security of several types of GFS by exploiting the asymmetric property. We show that better lower bounds can be achieved for the Type-1 GFS, Type-3 GFS and Alternating Feistel Scheme. Furthermore, we give the first general results regarding to the lower bound of the Unbalanced Feistel Scheme.

Keywords: Generalized Feistel Network · Differential analysis
Chosen ciphertext attack · Known Plaintext Attack

1 Introduction

1.1 Background

The Feistel Network is a widely-used method used to construct iterated block ciphers. It has similar operations in encryption and decryption process which is hardware efficient and the round function is not required to be a bijective function. It has been applied in many block ciphers such as DES, DEAL [9] and Camellia [2]. The structure was generalized to allow more branches and different relations between the branches to form Generalized Feistel Network (GFN) [13]. Before the term GFN was proposed, Zheng *et al.* [24] described 3 types of transformations which were in fact Type-1, Type-2 and Type-3 Generalized Feistel Schemes. Anderson and Biham [1] and Lucks [11] proposed block cipher designs using Alternating Feistel Network. Another type of GFN is the Unbalanced Feistel Scheme, which was designed by Schneier and Kelsey [19]. Many block cipher designs employed the GFN, such as CLEFIA [20], Skipjack and Simpira [6]. The advantage of using a Generalized Feistel Network is that it allows for a design to handle a larger block size with a relatively small round function.

1.2 Previous Work

Many analysis on Feistel network and Generalized Feistel Network have been done [7,10,12,14,15,22]. However, as mentioned in [7], most analysis is specialized in some types instead of analysing many types at once.

A. Patra and N. P. Smart (Eds.): INDOCRYPT 2017, LNCS 10698, pp. 302–324, 2017.
https://doi.org/10.1007/978-3-319-71667-1_16

Nachef *et al.* [12] used differential cryptanalysis to study four types of GFS using Known Plaintext Attack (KPA) and Chosen Plaintext Attack (CPA) model. They established lower bounds of the maximum number of rounds distinguishable in Type-1, Type-2, Type-3 and Alternating Feistel Scheme in the two models.

Provable-security analysis has been applied to Feistel Networks in [7,10]. Luby and Rackoff [10] analysed the classical Feistel Networks which is then improved and generalised by Hoang and Rogaway in [7] to analyse Classical, Unbalanced, Alternating, Type-1, Type-2 and Type-3 Generalized Feistel Scheme. The theoretical analysis of Generalized Feistel also plays an important role in design and analysis of practical ciphers. In the design of DEAL [9], Knudsen considers this theoretical attack to provide a security bound for any key schedule that is used.

An interesting property existed in many the GFS designs is that the encryption and decryption are not exactly the same, which sometimes makes the differential propagation slower in the decryption than in the encryption. In the analysis on Skipjack [4,5], the difference in the decryption has been considered. Recently, Tjuawinata *et al.* [21] showed that the analysis of Simpira [6] can be improved by considering the asymmetry of Type-1 Generalized Feistel Scheme. While this property is exploited in cryptanalysis, it is undesired for the designer. In the design criterion of Keccak [3], it mentioned the property that the same permutation function is used in both encryption and decryption.

1.3 Our Contribution

In this paper, we study the asymmetric property in the Generalized Feistel Schemes. We provide better lower bounds of the maximum number of rounds distinguishable in 3 different types of Generalized Feistel Networks given in [12], which are Type-1 Feistel Scheme, Type-3 Feistel Scheme and Alternating Feistel Scheme.[1] We also provide a lower bound of the maximum number of rounds distinguishable in another type of Generalized Feistel Network, the Unbalanced Feistel Network. As far as we know, this is the first result on Unbalanced Feistel Network that is applicable to different values of k'. We exploit the asymmetry of certain types of GFS by observing that the backward differential diffusion is slower than the forward differential diffusion. This leads to the improvements on the lower bounds.

For Type-1 Feistel Scheme, we provide a chosen ciphertext distinguisher which distinguishes $k-1$ more rounds than the distinguisher given in [12] with the same complexity. Furthermore, when the number of rounds to distinguish is fixed to $ak-2$ rounds for some integer a in the range $4 \leq a \leq k-1$, the distinguisher in this paper has complexity $1/2^n$ of the distinguisher given in the CPA model in [12], from $\sqrt{2} \cdot 2^{(a-2)n}$ to $\sqrt{2} \cdot 2^{(a-3)n}$.

[1] We also examine Type-2 Feistel Scheme, but we cannot improve the previous results since it does not have asymmetric property.

In Type-3 Feistel Scheme, [12] only provides lower bound for the case when the number of branches is at least 6. We propose a distinguisher which can be used for any number of branches and can distinguish up to $k+2$ rounds in both KPA and CCA model with complexity $\sqrt{2} \cdot 2^{(k-1)n}$ and $\sqrt{2} \cdot 2^{(k-2)n}$ respectively. When k is at least 6, in the CCA model, a distinguisher for one more rounds than the one given in [12] is constructed.

In Alternating Feistel Scheme, our analysis shows that lower complexity can be achieved in some special cases. More specifically, when the number of rounds is odd, the complexity is improved by a factor of $2^{\frac{3n}{2}}$ from the distinguisher proposed in [12].

In our analysis of Unbalanced Feistel Scheme, let k be the total number of sub-blocks and k' be the number of sub-blocks that are used as the output of the round function. In this paper, we consider two special cases when k' or $k-k'$ divides k. When $k' = 1$, we can distinguish up to (k^2+k-1) rounds with complexity less than 2^{kn} in the KPA model. In the CCA model, the number of rounds that can be distinguished is up to $2k$ rounds with complexity less than 2^n. When $k' \geq 1$, a lower bound of the maximum number of rounds that is distinguishable from random permutation is given. In the KPA model, the bound is $\frac{k^2}{k'} - \frac{k}{2} + \frac{k}{k'}$ when k' is even and $\frac{k^2}{k'} - \frac{k(k-1)}{2k'}$ when k' is odd. In the CCA model, the bound is $\frac{k}{2} + 2\frac{k}{k'}$ when k' is even and $\frac{k(k'+3)}{2k'}$ when k' is odd. To the best of our knowledge, this is the first analysis on Unbalanced Feistel Scheme for any values of k.

1.4 Organization

We give some preliminaries in Sect. 2. The attack overview is then discussed in Sect. 3. The analysis on Type-1 Feistel Scheme is presented in Sect. 4. Sections 5 and 6 contains analysis of Type-3 and Alternating Feistel Scheme. The Unbalanced Feistel Scheme is analysed in Sect. 7. In Sect. 8, we conclude this paper.

2 Preliminaries

2.1 Generalized Feistel Schemes

A Generalized Feistel Scheme of branch k is defined as a (keyed)-permutation $\Pi : (\mathbb{F}_{2^n})^k \rightarrow (\mathbb{F}_{2^n})^k$. For the m input-output pairs of Π, for all $i \in \{0, \cdots, m-1\}$, the i-th input and output of Π are denoted by $(I_0(i), \cdots, I_{k-1}(i))$ and $(S_0(i), \cdots, S_{k-1}(i))$ respectively. Since the analysis is on the inverse of Π, in the remaining of the paper, "input" refers to $(S_0(i), \cdots, S_{k-1}(i))$ while "output" refers to $(I_0(i), \cdots, I_{k-1}(i))$. In this paper, four types of Generalized Feistel schemes are considered in details:

Type-1 Feistel Schemes. Π is an r-round Type-1 Feistel scheme if Π consists of r repetitions of $\mu_1 : (\mathbb{F}_{2^n})^k \rightarrow (\mathbb{F}_{2^n})^k$ where $\mu_1(x_0, \cdots, x_{k-1}) = (x_1 \oplus$

$F_i(x_0), x_2, \cdots, x_{k-1}, x_0)$. Assume that $F_i : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is a function from from n-bit input to n-bit output which may vary depending on the round where it is being called. Here $i = 1, \cdots, r$. Illustration of round i of Type-1 Feistel Scheme can be found in Fig. 1.

Type-3 Feistel Schemes. Π is an r-round Type-3 Feistel scheme if Π consists of r iterations of $\mu_3 : \mathbb{F}_{2^n}^k \to \mathbb{F}_{2^n}^k$. Given $(x_0, \cdots, x_{k-1})$, μ_3 maps

$$(x_0, \cdots, x_{k-1})$$

to

$$(x_1 \oplus F_{(i,0)}(x_0), x_2 \oplus F_{(i,1)}(x_1), \cdots, x_{k-1} \oplus F_{(i,k-2)}(x_{k-2}), x_0).$$

Figure 2 illustrates the i-th round of Type-3 Feistel Scheme.

Alternating Feistel Schemes. For this scheme, consider two different round functions $\mu_{A,0}, \mu_{A,1} : \mathbb{F}_{2^n}^k \to \mathbb{F}_{2^n}^k$ which are used alternatingly for each round.

- $\mu_{A,0}(x_0, \cdots, x_{k-1}) = (x_0 \oplus F_i(x_1, \cdots, x_{k-1}), x_1, \cdots, x_{k-1})$ where $F_i : \mathbb{F}_{2^n}^{k-1} \to \mathbb{F}_{2^n}$ is called in round $2i-1$. $\mu_{A,0}$ is called the contracting round.
- $\mu_{A,1}(x_0, \cdots, x_{k-1}) = (x_0, x_1 \oplus F_{(i,1)}(x_0), \cdots, x_{k-1} \oplus F_{(i,k-1)}(x_0))$. Here $F_{i,j} : \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is the function called in the j-th component in round $2i$. These rounds are called the expanding rounds.

Illustration of round $2i-1$ and $2i$ of Alternating Feistel Scheme can be found in Fig. 3. Note that round number and index i starts from 1 instead of 0. Alternatively, $\mu_{A,1}$ can be used in odd rounds and $\mu_{A,0}$ in even rounds but in this paper a contracting round is always used at round 1. Note that if $\mu_{A,1}$ is used in the first one instead, the backward analysis on this variant is equivalent to the forward analysis discussed in [12].

Unbalanced Feistel Schemes. This is a special case of the UFN defined in Fig. 1 of [7]. Let $k' = 1, \cdots, k-1$ and $F_s : \mathbb{F}_{2^n}^{k-k'} \to \mathbb{F}_{2^n}^{k'}$ be a map from $(k-k')n$ bit to $k'n$ bit with component functions denoted as $F_{s,0}, \cdots, F_{s,k'-1}$ with the round number s as its parameter. Then Π is an r-round UFN(k', k) if it contains r repetitions of $\mu_U : \mathbb{F}_{2^n}^k \to \mathbb{F}_{2^n}^k$. In round s, given an input $(x_0, \cdots, x_{k-1})$, μ_U maps it to

$$(x_{k'}, \cdots, x_{k-1}, x_0 \oplus F_{s,0}(x_{k'}, \cdots, x_{k-1}), \cdots, x_{k'-1} \oplus F_{s,k'-1}(x_{k'}, \cdots, x_{k-1})).$$

Figure 4 provides an illustration of round s of UFN(k', k).

In this paper, differential analysis on the inverse of Π is considered. So the attack starts with the image $(S_0(i), \cdots, S_{k-1}(i))$ and the differential path is built to the preimage, $(I_0(i), \cdots, I_{k-1}(i))$.

2.2 Random Variable

Given a random variable X, denote by $E(X), V(X), \sigma(X)$ the expected value, variance and standard deviation of X respectively. Note that $V(X) = E(X^2) - E(X)^2$ and $\sigma(X) = \sqrt{V(x)}$.

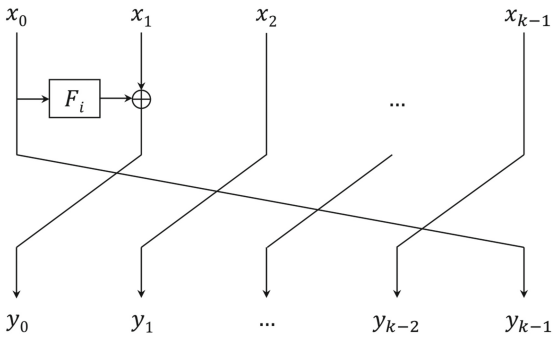

Fig. 1. Round i of Type-1 Feistel Scheme

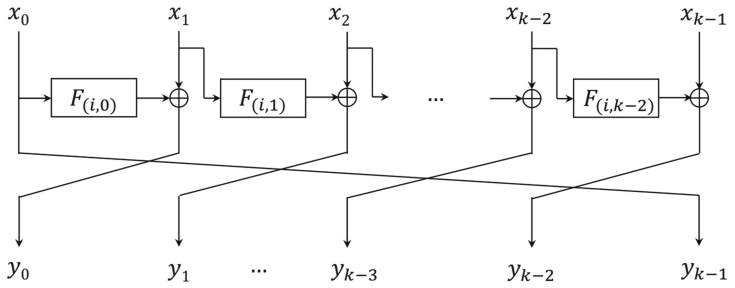

Fig. 2. Round i of Type-3 Feistel Scheme

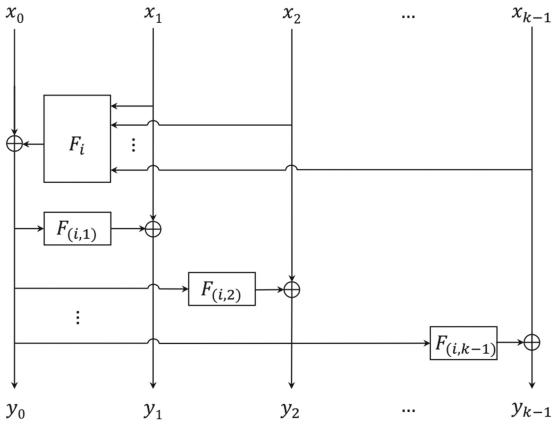

Fig. 3. Round $2i-1$ and Round $2i$ of Alternating Feistel Scheme

Now given n random variables $X_1, \cdots, X_n$, define the covariance of X_i and X_j as $Cov(X_i, X_j) = E(X_i X_j) - E(X_i)E(X_j)$. A simple calculation of the definition yields $V(\sum_{i=1}^{n} X_i) = \sum_{i=1}^{n} V(X_i) + \sum_{i \neq j, 1 \leq i,j \leq n} Cov(X_i, X_j)$.

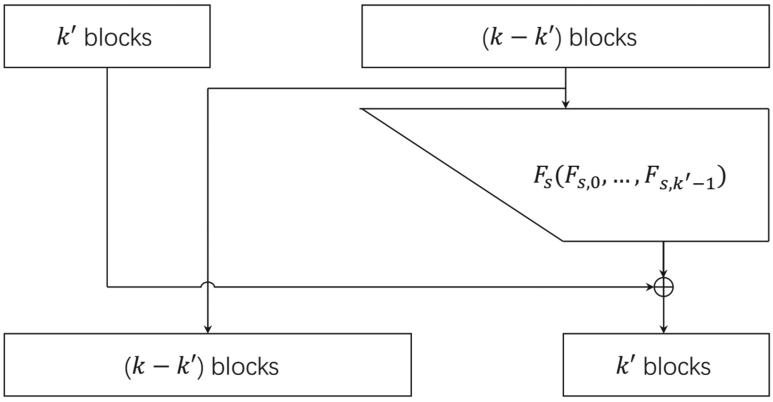

Fig. 4. Round s of Unbalanced Feistel Scheme

Proposition 1 [12]. *Let X and Y be two random variables. X is said to be distinguishable from Y if $|E(X) - E(Y)| \geq \max(\sigma(X), \sigma(Y))$.*

More specifically, let E_X, E_Y be the expected values of X and Y respectively while σ_X, σ_Y being the standard deviations of X and Y respectively. Without loss of generality, let $E_X < E_Y$. Then, if $E_Y - E_X \geq \max(\sigma(X), \sigma(Y))$:

1. $Pr\left(X \geq \frac{E_X+E_Y}{2}\right) \leq 0.30854$
2. $Pr\left(Y \leq \frac{E_X+E_Y}{2}\right) \leq 0.30854$.

Proof. We only prove the first claim since the second one can be proved by using the same method. A simple calculation tells us that:

$$\begin{aligned} Pr\left(X \geq \frac{E_X + E_Y}{2}\right) &= Pr\left(X - E_X \geq \frac{E_Y - E_X}{2}\right) \\ &\leq Pr\left(X - E_X \geq \frac{\sigma_X}{2}\right) \\ &= Pr\left(\frac{X - E_X}{\sigma_X} \geq \frac{1}{2}\right). \end{aligned}$$

Assuming that X is sampled large enough time, we can use the Central Limit Theorem to approximate $\frac{X-E_X}{\sigma_X}$ by a standard normal distribution. Hence by using this approximation and the standard normal distribution table, we get the upper bound claimed.

Remark 1. When we use Proposition 1, the random variables are actually the number of plaintext-ciphertext pairs that satisfy some equations. Now since the number of plaintext-ciphertext pairs is $\mathcal{O}(2^{\alpha n})$ for some constant α, we can apply Central Limit Theorem here. So if the random variable is $\mathcal{X}$ with mean μ and standard deviation δ, we can approximate $\frac{\mathcal{X}-\mu}{\delta}$ by the standard normal distribution.

3 Attack Overview

In this paper, as we have discussed in Sect. 1.2, we exploit the asymmetry of the scheme by considering the backward differential diffusion.

We will discuss two types of improvements:

Unconstrained environment. We aim for a better lower bound for the maximum number of rounds distinguishable than the bound given in [12]. By unconstrained environment, we mean that analysis considered in this environment aims to distinguish more rounds than the previous results with complexity strictly less than 2^{kn} where k is the number of sub-block and n is the number of bits in each sub-block. Throughout this paper, the complexity of the attack is measured by the number of queries performed to make the attack possible.

Constrained environment. There are two possible forms of this improvement. Firstly, we aim to improve the number of rounds that can be distinguished in the backward direction given the same complexity as the distinguisher given in [12]. Secondly, given the same number of rounds, we aim to reduce the complexity to distinguish the GFS from a random permutation.

Our analysis uses m plaintext-ciphertext pairs and considers the expected number of pairs $\mathcal{N}$ that satisfies certain conditions depending on the scheme analysed. Let $\mathcal{N}_{\text{perm}}$ be the value of $\mathcal{N}$ for a random permutation and $\mathcal{N}_{\mathcal{F}}$ be the value $\mathcal{N}$ for $\mathcal{F}$, the r-round Generalized Feistel Scheme. We use this information to calculate the maximum number of rounds such that $\mathcal{N}_{\text{perm}}$ is distinguishable from $\mathcal{N}_{\mathcal{F}}$.

The functions F_i (or $F_{(i,j)}$) used in the round function of GFS are assumed to be ideal keyed functions. Given the input, the output is a random n-bit string. Similarly, since it is ideal, given a nonzero input difference, the output difference is uniformly distributed.

Furthermore, let $\mathfrak{I}_1$ and $\mathfrak{I}_2$ be two distinct indices of the round function in the same cryptosystem (I_j can be a single integer or a pair or integers depending on the GFN we are considering). Given two different indices values $\mathfrak{I}_1$ and $\mathfrak{I}_2$, we also assume that $F_{\mathfrak{I}_1}$ and $F_{(\mathfrak{I}_2)}$ are independent from each other. Hence given the same input (or output) difference ΔS of $F_{\mathfrak{I}_1}$ and $F_{\mathfrak{I}_2}$, we can further assume that $F_{\mathfrak{I}_2}(\Delta S)$ is uniformly distributed even assuming that $F_{\mathfrak{I}_1}(\Delta S)$ is already known.

First we give an intuitive description on how to launch the attack. Suppose that given a Generalized Feistel Scheme f of $\mathfrak{r}$ rounds, we denote the differences in each stage as $\Delta_I - \Delta_1 - \cdots - \Delta_{\mathfrak{r}-1} - \Delta_O$. The first step of the attack is done by expressing Δ_I as a function of $\Delta_1, \cdots, \Delta_{\mathfrak{r}-1}$ and Δ_O. We are choosing the express Δ_I as a function of Δ_O instead of the other way around since we want to use the expression we get to launch a backward differential trail instead of the forward trail. To enable this, for each Δ, we partition Δ into k sub-blocks. Since each round function takes one of these sub-blocks as input, we can easily find the expression that we need.

Having these expressions, we can then choose carefully the input and output difference (truncated differences) to maximize the probability for the specified input difference focusing in some of the sub-blocks to lead to the output difference chosen. To calculate the success probability, we consider the number of ciphertext pairs with specified difference that can lead to the plaintext pairs with the chosen input difference in two scenarios; when the function is a random permutation, denoted by $\mathcal{N}_{\text{perm}}$ and when the function is in the form of the Generalized Feistel Network considered, denoted by $\mathcal{N}_{\mathcal{F}}$.

Now having the expected values and variances of both $\mathcal{N}_{\text{perm}}$ and $\mathcal{N}_{\mathcal{F}}$, those four values will be functions of the round number r and number of ciphertext pairs with the chosen difference m. By Definition 1, $\mathcal{N}_{\mathcal{F}}$ is distinguishable from $\mathcal{N}_{\text{perm}}$ if $|E(\mathcal{N}_{\mathcal{F}}) - E(\mathcal{N}_{\text{perm}})| \geq \max(\sigma(\mathcal{N}_{\mathcal{F}}), \sigma(\mathcal{N}_{\text{perm}}))$. So using this inequality, we obtain a relation between the number of rounds r and the number of ciphertext pairs m. This will give us a lower bound of m given r. Since we want the distinguisher to be useful, we require m to be less than the total number of possible ciphertext pairs. In the case of known ciphertext attack, this means that we need $m \leq 2^{kn}$. This gives us an upper bound for the round number, r, such that $\mathcal{F}$ is distinguishable from a random permutation using this backward differential attack.

As we described above, in fact the main idea of the attack is exactly the same for all the types of Generalized Feistel Scheme. We first calculate a relation between ciphertext and plaintext differences which is closely related to the structure of the scheme. Once the relation is established, the calculation of the expectation and standard deviation will be very similar and they will be independent of the scheme. Because of this similarity, we will just describe the calculation once and omit the others. In the following sections of this paper, we perform this attack on different types of Generalized Feistel Networks discussed in Sect. 2.1.

4 Type-1 Feistel Schemes

4.1 Analysis of the Type-1 Feistel Schemes

For this analysis, we assume the number of rounds is $r = ak + b$ where k is the number of branches in the scheme and a and b are non-negative integers where $0 \leq b \leq k-1$ and $k \geq 3$. We will be using the notation described in the previous section for our analysis, namely $I_0, \cdots, I_{k-1}$ for the k sub-blocks pre-image of Π while $S_0, \cdots S_{k-1}$ is used to denote the k sub-blocks image of Π. In this section we discuss in detail how we build the relations between the sub-blocks, then we discuss how we choose the differential trail. Having the differential trail, the expected value and the variance of the trail when Π is random permutation and a type-1 Generalized Feistel Scheme are calculated. This in turns tells us the maximum number of rounds that is distinguishable from a random permutation using the chosen differential.

Let X_i be the intermediate variables obtained in the second branch (indexed as 1) after the i-th round in the backward direction. By definition of the round function of Type-1 Feistel Scheme, we have the following relations:

$X_0 = S_{k-1}$,
$X_1 = S_0 \oplus F_{ak+b}(S_{k-1})$,
For $t = 2, \cdots, k-1, X_t = S_{k+1-t} \oplus F_{ak+b-(t-1)}(S_{k-t})$,
For $t \geq k, X_t = X_{t-k} \oplus F_{ak+b-(t-1)}(X_{t-(k-1)})$, Note that F_r is always used with input $X_{ak+b-r-k+2}$.
For $r \geq k-1$, the input of the r-th round in the backward direction is $(X_{r-(k-1)}, X_r, X_{r-1}, \cdots, X_{r-(k-2)})$.

After $r = ak + b$ rounds, the state becomes $(I_0, \cdots, I_{k-1})$ where $I_0 = X_{(ak+b)-(k-1)}$ and for $i = 1, \cdots, k-1, I_i = X_{(ak+b)-(i-1)}$. The following equalities can then be derived using the relations established above:

$I_0 = X_{b+1} \oplus \bigoplus_{i=0}^{a-2} F_{(a-i-1)k}(X_{ik+b+2})$,
For $j \in \{1, \cdots, \min(k-1, b+1)\}$,

$$I_j = X_{b+1-j} \oplus \bigoplus_{i=0}^{a-1} F_{(a-i-1)k+j}(X_{ik+(b+2-j)}),$$

For $j \in \{\min(k-1, b+1)+1, \cdots, k-1\}$,

$$I_j = X_{k+b+1-j} \oplus \bigoplus_{i=0}^{a-2} F_{(a-i-2)k+j}(X_{ik+(k+b+2-j)}).$$

In particular, for I_1,

$$\begin{aligned} I_1 &= X_b \oplus \bigoplus_{i=0}^{a-1} F_{(a-i-1)k+1}(X_{ik+(b+1)}) \\ &= X_b \oplus \bigoplus_{i=0}^{a-2} F_{(a-i-1)k+1}(X_{ik+(b+1)}) \oplus F_1(I_0) \\ &= \begin{cases} S_1 \oplus \bigoplus_{i=0}^{a-2} F_{(a-i-1)k+1}(X_{ik+1}) \oplus F_1(I_0) & \text{if } b = 0 \\ S_0 \oplus F_{ak+1}(S_{k-1}) \oplus \bigoplus_{i=0}^{a-2} F_{(a-i-1)k+1}(X_{ik+2}) \oplus F_1(I_0) & \text{if } b = 1 \\ S_{k+1-b} \oplus F_{ak+1}(S_{k-b}) \oplus \bigoplus_{i=0}^{a-2} F_{(a-i-1)k+1}(X_{ik+(b+1)}) & \\ \qquad \oplus F_1(I_0) & \text{otherwise.} \end{cases} \end{aligned}$$

We can further expand the sum by noting that when $i = 0$, the summand is $F_{(a-i-1)k+1}(X_{b+1})$ and

$$X_{b+1} = \begin{cases} S_0 \oplus F_{ak}(S_{k-1}) & \text{if } b = 0 \\ S_{k-b} \oplus F_{ak}(S_{k-b-1}) & \text{if } 1 \leq b \leq k-2 \\ S_1 \oplus F_{ak}(S_0 \oplus F_{ak+(k-1)}(S_{k-1})) & \text{if } b = k-1. \end{cases}$$

So in any value of $b \in \{0, \cdots, k-1, \}$, we can express I_1 as a function of several sub-blocks of the output $S_j, F_1(I_0)$ and $a-2$ terms determined by intermediate variables. More specifically, for $b \in \{0, \cdots, k-1\}$, we have:

1. When $b = 0$,

$$I_1 \oplus S_1 \oplus F_1(I_0) = \bigoplus_{i=1}^{a-2} F_{(a-i-1)k+1}(X_{ik+1}) \oplus F_{(a-1)k+1}(S_0 \oplus F_{ak}(S_{k-1})), \quad (1)$$

2. When $b = 1$,

$$I_1 \oplus S_0 \oplus F_1(I_0) = \bigoplus_{i=1}^{a-2} F_{(a-i-1)k+1}(X_{ik+2}) \oplus F_{(a-1)k+1}(S_{k-1} \oplus F_{ak}(S_{k-2})), \quad (2)$$

3. When $2 \leq b \leq k-2$,

$$I_1 \oplus S_{k+1-b} \oplus F_1(I_0) = \bigoplus_{i=1}^{a-2} F_{(a-i-1)k+1}(X_{ik+2}) \oplus F_{(a-1)k+1}(S_{k-b} \oplus F_{ak}(S_{k-b-1})), \quad (3)$$

4. When $b = k-1$,

$$I_1 \oplus S_2 \oplus F_1(I_0) = \bigoplus_{i=1}^{a-2} F_{(a-i-1)k+1}(X_{ik+1}) \oplus F_{(a-1)k+1}(S_1 \oplus F_{ak}(S_0 \oplus F_{(a+1)k-1}(S_{k-1}))). \quad (4)$$

To choose the truncated differential for each case, we try to utilize Eqs. (1), (2), (3) and (4). We will describe how we choose it for the case when $b = 0$. The same idea can then be applied to all the other cases.

Note that for this case, for any ciphertext and its plaintext, we have the relation

$$I_1 \oplus S_1 \oplus F_1(I_0) = \bigoplus_{i=1}^{a-2} F_{(a-i-1)k+1}(X_{ik+1}) \oplus F_{(a-1)k+1}(S_0 \oplus F_{ak}(S_{k-1})),$$

Now for any two ciphertexts $C = (S_0, \cdots, S_{k-1}), C' = (S'_0, \cdots, S'_{k-1})$ that we choose (and their corresponding plaintexts $P = (I_0, \cdots, I_{k-1}), P' = (I'_0, \cdots, I'_{k-1})$), we can only determine the value in the left hand side of Eq. (1). So based on this relation, we try to find the probability that $I_1 \oplus S_1 \oplus F_1(I_0) = I'_1 \oplus S'_1 \oplus F_1(I'_0)$. Since F_1 is always assumed to be ideal, after some rearrangement, this probability is the same as the probability that:

$$1. \quad I_0 = I'_0$$
$$2. \; I_1 \oplus I'_1 = S_1 \oplus S'_1.$$

So we will use this as the truncated differential for the case of Type-1 Scheme with $b = 0$. As mentioned before, this is done by collecting m ciphertexts with their respective plaintexts and we compute the number of ciphertext pairs (along with their corresponding plaintexts) that satisfies the above conditions. The same analysis is done to all the other cases.

Now to find a theoretical approximation for the probability of these conditions to be satisfied in various cases, we use the fact that if $I_0 = I'_0$ and $I_1 \oplus I'_1 = S_1 \oplus S'_1$, we must have

$$\bigoplus_{i=1}^{a-2} F_{(a-i-1)k+1}(X_{ik+1}) \oplus F_{(a-1)k+1}(S_1 \oplus F_{ak}(S_0 \oplus F_{(a+1)k-1}(S_{k-1})))$$

is equal to

$$\bigoplus_{i=1}^{a-2} F_{(a-i-1)k+1}(X'_{ik+1}) \oplus F_{(a-1)k+1}(S'_1 \oplus F_{ak}(S'_0 \oplus F_{(a+1)k-1}(S'_{k-1}))).$$

Now note that in this last equation, we have terms that are just functions of S_0, S_{k-1}, S'_0 and S'_{k-1}. So in the chosen ciphertext attack, to increase the probability, we can make sure that these terms are equal in both sides by making sure that $S_0 = S'_0$ and $S_{k-1} = S'_{k-1}$. So in the chosen ciphertext attack, instead of choosing m random ciphertexts, we choose them with their first and last sub-blocks being fixed to a predetermined value.

In summary, out of the m plaintext-ciphertext pairs, we count the number of $(s, t), 1 \leq s < t \leq m$ such that

$$\begin{aligned} &1. \quad I_0(s) = I_0(t) \\ &2. \ I_1(s) \oplus I_1(t) = \begin{cases} S_1(s) \oplus S_1(t) & \text{if } b = 0 \\ S_0(s) \oplus S_0(t) & \text{if } b = 1 \\ S_{k+1-b}(s) \oplus S_{k+1-b}(t) & \text{if } 2 \leq b \leq k-1. \end{cases} \end{aligned} \tag{5}$$

Note that in any of the equations that we have, we still have one term containing some sub-blocks of the ciphertext. To increase the probability that the equation is satisfied, we can set it to have no difference in any of the plaintext-ciphertext pairs. So in particular, in the CCA model, pick m different ciphertext such that:

If $b = 0$, pick all the ciphertext with fixed values of $S_0(s)$ and $S_{k-1}(s)$. Hence in the CCA attack, $m \leq 2^{(k-2)n}$.

If $b = 1, \cdots, k-2$, fix the values of $S_{k-b}(s)$ and $S_{k-b-1}(s)$ for all $s = 0, \cdots, m-1$. Again, in the CCA attack, $m \leq 2^{(k-2)n}$.

If $b = k-1$ and $k \geq 4$, fix the values of $S_0(s), S_1(s)$ and $S_{k-1}(s)$ for $s = 0, \cdots, m-1$. In this case, the CCA attack must have m to be at most $2^{(k-3)n}$.

So in summary, the differential trail for $r = ak + b$ rounds where $b \in \{0, \cdots, k-1\}$is as follows:

1. In the KPA setting, the input (ciphertext) differential is $(\nabla_0, \cdots, \nabla_{k-1})$ while the output (plaintext) differential is $(\Delta_0, \cdots, \Delta_{k-1})$ where it satisfies the following equations:
   - $\Delta_0 = 0$.
   - $\Delta_1 = \nabla_{(k+1-b) \pmod k}$
   - All other sub-blocks difference is arbitrary, which we denote by $\star$.
2. In the CCA setting, the differential is the same, however, we impose some requirement to the ciphertext that we pick:
   - If $b = 0$, we fix the value of $S_0(s)$ and $S_{k-1}(s)$.
   - If $b = 1, \cdots k-2$, the values of $S_{k-b}(s)$ and $S_{k-b-1}(s)$ are fixed.
   - If $b = k-1$, we fix the values of $S_0(s), S_1(s)$ and $S_{k-1}(s)$.

Let $\mathcal{N}_{F,M}$ be the random variable representing the number of sets of two plaintext-ciphertext pairs that satisfy the conditions given by (5) for F representing the function used, which has value in the set $\{\text{perm}, \mathcal{F}\}$, and $M \in \{\text{KPA}, \text{CCA}\}$. $F = \text{perm}$ is used for the random permutation while $F = \mathcal{F}$ is used for the r-round Type-1 Feistel Scheme.

Now it is easy to see that the probability that the requirement set above to be true is equal to the probability that the right hand side of the equations to agree, which can be computed since we can assume all the X_i is uniformly and independently distributed by the ideality of the round function (which has been discussed in Sect. 3).

Calculating the expected values and variance of the random variables,

$$E(\mathcal{N}_{(\text{perm,KPA})}), E(\mathcal{N}_{(\text{perm,CCA})}), V(\mathcal{N}_{(\text{perm,KPA})}), V(\mathcal{N}_{(\text{perm,CCA})})$$

are all approximately $\frac{m^2}{2 \cdot 2^{2n}}$. Calculating the random variables corresponding to $\mathcal{F}$, the expected values and variances are summarised in Table 3 which can be found in Appendix A. The details on the calculation of the expected values and variances of $\mathcal{N}_{\mathcal{F},\text{CCA}}$ for $b = 0$ can be found in the full version and is omitted here due to its similarity with the calculation done in [12]. The other results can be calculated using the same method.

Using the proposition of distinguishability of two random variables given in the preliminaries, the result is provided in Table 1.

In the KPA model, the maximum number of rounds is k^2 where from $k(k-1)+1$ up to k^2 rounds, the complexity is $\sqrt{2} \cdot 2^{(k-1)n}$. Furthermore, in the CCA model, the maximum number of rounds distinguishable is $k(k-1)+k-2 = k^2-2$ rounds with complexity $\sqrt{2} \cdot 2^{(k-3)n}$.

4.2 Comparison with Existing Result from [12]

To compare with the result given in [12] first note that there are some constant multipliers that are omitted in [12]. More specifically, all the expected values and variances should be multiplied by $\frac{1}{2}$. This constant adjustment comes from the

Table 1. Summary of distinguishability of Type-1 Feistel Scheme

b	Model	Complexity of distinguishing $ak+b$ rounds	Maximum a
0	KPA	$\sqrt{2} \cdot 2^{(a-1)n}$	k
	CCA	$\sqrt{2} \cdot 2^{(a-2)n}$	$k-1$
$1 \leq b \leq k-2$	KPA	$\sqrt{2} \cdot 2^{an}$	$k-1$
	CCA	$\sqrt{2} \cdot 2^{(a-2)n}$	$k-1$
$k-1$	KPA	$\sqrt{2} \cdot 2^{an}$	$k-1$
	CCA	$\sqrt{2} \cdot 2^{(a-2)n}$	$k-2$

fact that given m plaintext-ciphertext pairs, the number of sets of 2 distinct pairs should be $\frac{m(m-1)}{2} \approx \frac{m^2}{2}$ instead of m^2. Although the constant multiplier is very close to one compared to 2^n, it affects the maximum number of rounds that can be distinguished in the KPA and CPA model. This is because all the complexities of distinguishers should be multiplied by a factor of $\sqrt{2}$. The existence of this factor makes it impossible for a to reach the maximum number given in [12]. For $ak-2$ rounds distinguished in KPA model, the complexity should be $\sqrt{2} \cdot 2^{(a-2)n}$. Hence the maximum number of rounds that can be distinguished in the KPA model is k^2+k-2 rounds instead of k^2+2k-2 rounds. Similarly, for $ak-1$ rounds to be distinguishable in CPA, the complexity is again $\sqrt{2} \cdot 2^{(a-2)n}$. Therefore, the maximum number of rounds that is distinguishable in CPA model to be k^2-1 rounds instead of k^2+k-1.

Note that in both cases, the maximum number of rounds distinguishable without any complexity constraint is still better in the forward direction. So in this section, the advantage of using the backward direction analysis in a constrained environment is discussed.

We compare the results in the CCA model presented above with the CPA model.

1. When the complexity is fixed to $\sqrt{2} \cdot 2^{tn}$, in CPA model, the maximum number of rounds that is distinguishable is $(t+2)k-1$ while in CCA model, the maximum number of rounds that is distinguishable is $(t+2)k+(k-2) = (t+3)k-2 = (t+2)k-1+\mathbf{k-1}$ which is an increase of $k-1$ rounds.
2. Suppose that we want to distinguish r rounds for some positive integer r. Table 3 of [12] (after the adjustment by a factor of $\sqrt{2}$) tells us that when $pk-(p-2) = (p-1)k+k-p+2 \leq r \leq (p+1)k-p = pk+k-p$, the complexity is $\sqrt{2} \cdot 2^{(p-2)n}$. Using the same bound for r, the complexity is $\sqrt{2} \cdot 2^{(p-3)n} = \sqrt{2} \cdot 2^{(p-2)n} \cdot \mathbf{2^{-n}}$ when $r \leq pk-1$ and $\sqrt{2} \cdot 2^{(p-2)n}$ when $r \geq pk$ (see Table 1). So the complexity is reduced by a factor of $\frac{1}{2^n}$ when $(p-1)k+k-p+2 \leq r \leq pk$ for any value of p.

Now for all the following sections, since the method that is being used is exactly the same, we will not discuss in detail on how to choose the differential, the expected values and the distinguishability. Instead, only the final results will

be stated and compared. We note that since we are using Proposition 1, which is also used in the analysis in [12], has success probability at least 70 %.

5 Type-3 Feistel Scheme

5.1 Analysis of the Type-3 Feistel Scheme

As before, we denote the input as $S_0, \cdots, S_{k-1}$. Define intermediate variables X_i such that $(X_{tk}, \cdots, X_{tk+k-1})$ is the state value after t rounds. Assuming the number of rounds is r, for $0 \leq s \leq k-1, X_s = S_s$ and $X_{rk+s} = I_s$. Given the input of round $c, 1 \leq c \leq r$, by definition:

$$\begin{aligned} X_{ck} &= X_{(c-1)k+k-1} \\ X_{ck+s} &= X_{(c-1)k+(s-1)} \oplus F_{(r+1-c,s-1)}(X_{ck+s-1}),\ \forall 1 \leq s \leq k-1. \end{aligned}$$

Let $r = ak + b$ for $0 \leq b \leq k-1$. In this paper, we only consider $a = 1$ and $b > 0$. Expanding the equation for $X_{(k+b)k+s}$ using the equation given above, the following can then be derived:

- When $b = s$,

$$\begin{aligned} X_{(k+b)k+s} = &\bigoplus_{i=0}^{b-1} F_{(i+1,s-1-i)}(X_{(k+b-i)k+(s-1-i)} \\ &\oplus \bigoplus_{i=0}^{k-2} F_{(i+b+2,k-2-i)}(X_{(k-1-i)k+(k-2-i)}) \oplus S_0. \end{aligned}$$

- When $b = s + 1 \leq k - 1$,

$$\begin{aligned} X_{(k+b)k+s} = &\bigoplus_{i=0}^{s-1} F_{(i+1,s-1-i)}(X_{(k+b-i)k+(s-1-i)}) \oplus F_{(b+1,k-2)}(X_{(k)k+k-2}) \\ &\oplus \bigoplus_{i=0}^{k-3} F_{(i+b+2,k-3-i)}(X_{(k-1-i)k+k-3-i}) \oplus S_{k-1}. \end{aligned}$$

- When $s + 1 < b \leq k - 1$,

$$\begin{aligned} X_{(k+b)k+s} = &\bigoplus_{i=0}^{s-1} F_{(i+1,s-1-i)}(X_{(k+b-i)k+(s-1-i)}) \\ &\oplus \bigoplus_{i=0}^{b-s-1} F_{(s+i+2,k-2-i)}(X_{(k+b-s-1-i)k+k-2-i}) \\ &\oplus \bigoplus_{i=0}^{k-b+s-2} F_{(i+b+2,k-b+s-2-i)}(X_{(k-1-i)k+k-b+s-2-i}) \\ &\oplus \bigoplus_{i=0}^{b-s-2} F_{(k+s+i+2,k-2-i)}(X_{(b-s-1-i)k+(k-2-i)}) \oplus S_{k-1}. \end{aligned}$$

- When $s = b + 1 \leq k - 1$,

$$X_{(k+t)k+b} = \bigoplus_{i=0}^{b} F_{(i+1,b-i)}(X_{(k+b-i)k+b-i}) \oplus \bigoplus_{i=0}^{k-3} F_{(i+3,k-2-i)} F(X_{(k-2-i)k+(k-2-i)} \oplus S_1.$$

- When $b + 1 < s \leq k - 1$,

$$X_{(k+b)k+s} = \bigoplus_{i=0}^{b} F_{(i+1,b-i)}(X_{(k+b-i)k+b-i}) \oplus \bigoplus_{i=0}^{s-b-2} F_{(b+i+2,s-b-2-i)}(X_{(k-1-i)k+s-b-2-i}) \oplus \bigoplus_{i=0}^{k-s+b-2} F_{(s+2+i,k-2-i)}(X_{(k-s+b-1-i)k+(k-2-i)}) \oplus S_{s-b}.$$

Let $b \in \{1, \cdots, k-1\}$. For the m plaintext-ciphertext pairs, the distinguishing attack counts the number of sets of two pairs $(j, j'), 1 \leq j < j' \leq m$ that satisfies the following two conditions:

$$\begin{array}{ll} 1. & I_{(r-1)}(j) = I_{(r-1)}(j') \\ 2. & I_r(j) \oplus I_r(j') = S_0(j) \oplus S_0(j'). \end{array} \tag{6}$$

In the CCA model, fix the value of $S_{k-1}(j)$ of all the m ciphertexts. Hence $m \leq 2^{(k-1)n}$.

Calculating the random variables with the same method, $E(\mathcal{N}_{(\text{perm,KPA})})$, $V(\mathcal{N}_{(\text{perm,KPA})})$, $E(\mathcal{N}_{(\text{perm,CCA})})$, $V(\mathcal{N}_{(\text{perm,CCA})})$, $V(\mathcal{N}_{(\mathcal{F},\text{KPA})})$ and $V(\mathcal{N}_{(\mathcal{F},\text{CCA})})$ are all approximately $\frac{m^2}{2 \cdot 2^{2n}}$ while

$$E(\mathcal{N}_{(\mathcal{F},\text{KPA})}) = \frac{m^2}{2}\left(\frac{1}{2^{2n}} + \frac{1}{2^{(k+r-2)n}}\right)$$

and

$$E(\mathcal{N}_{(\mathcal{F},\text{CCA})}) = \frac{m^2}{2}\left(\frac{1}{2^{2n}} + \frac{1}{2^{(k+r-3)n}}\right).$$

In both KPA and CPA model, $\mathcal{F}$ is distinguishable from a random permutation when there are up to $k+2$ rounds and the complexity to distinguish $k+b$ rounds are $\sqrt{2} \cdot 2^{(k+b-3)n}$ and $\sqrt{2} \cdot 2^{(k+b-4)n}$ respectively.

5.2 Comparison with Existing Result from [12]

Now we compare our result with the one given in [12]. First of all, note that in [12], there is a restriction that $\lfloor \frac{k}{2} \rfloor \geq 3$. This means that k needs to be at

least 6 while the distinguisher proposed above can be used for all $k \geq 2$. So in any attack model, this analysis provides a new lower bound of the maximum number of distinguishable round for $2 \leq k \leq 5$. Furthermore, when $k \geq 6$, in KPA model, in both $k+1$ and $k+2$ rounds proposed above, the complexity is higher than the one given in [12]. The same thing happen in the distinguisher for $k+1$ rounds in the CCA model. However, the lower bound of maximum number of rounds distinguishable from random permutation in CCA model is increased to $k+2$ from $k+1$ proposed in [12].

6 Alternating Feistel Scheme

6.1 Analysis of Alternating Feistel Scheme

We divide this section into two cases based on the parity of the number of rounds. This is required due to the different round function in odd and even rounds.

Even Number of Rounds. Suppose that the number of rounds is $2r$. Let X_i be intermediate variables such that after $2t$ rounds the state value is

$$(X_{tk}, \cdots X_{tk+k-1}).$$

For any $0 \leq s \leq k-1, (I_s, S_s) = (X_{rk+s}, X_s)$. Then, given the state value after $2t$ rounds, $(X_{tk}, \cdots X_{tk+k-1})$ where $0 \leq t \leq r-1$, we have the following relations:

- $X_{(t+1)k} = X_{tk} \oplus F_{(r-t)}((X_{tk+s} \oplus F_{(r-t,s)}(X_{tk}))_{s=1}^{k-1})$ where

$$(Y_a)_{a=r}^{s} := (Y_r, Y_{r+1}, \cdots Y_s).$$

- $X_{(t+1)k+s} = X_{tk+s} \oplus F_{(r-t,s)}(X_{tk}),\ \forall s = 1, \cdots, k-1.$

Then expand the equation for I_s:

- $I_0 = S_0 \oplus \bigoplus_{i=0}^{r-1} F_{(r-i)}((X_{ik+s} \oplus F_{(r-i,s)}(X_{ik}))_{s=1}^{k-1})$
- $\forall s \in \{1, \cdots, k-1\}$,

$$I_s = S_s \oplus \bigoplus_{i=0}^{r-1} F_{(r-i,s)}(X_{ik}) = S_s \oplus F_{(r,s)}(S_0) \oplus \bigoplus_{i=1}^{r-1} F_{(r-i,s)}(X_{ik}).$$

The distinguishing attack finds the number of sets of two plaintext-ciphertext pairs $(p, q), 1 \leq p < q \leq m$ such that they satisfy the following conditions:

$$\begin{array}{ll} 1. & I_0(p) = I_0(q) \\ 2. & \forall s = 1, \cdots k-1,\ I_b(p) \oplus I_b(q) = S_b(p) \oplus S_b(q). \end{array} \tag{7}$$

Furthermore, in the CCA model, all the ciphertexts are chosen such that they have the same fixed value in $S_0(p)$. So we have, $m \leq 2^{(k-1)n}$.

Using the same calculation as before, $E(\mathcal{N}_{(\text{perm,KPA})})$, $V(\mathcal{N}_{(\text{perm,KPA})})$, $E(\mathcal{N}_{(\text{perm,CCA})}), V(\mathcal{N}_{(\text{perm,CCA})}), V(\mathcal{N}_{(\mathcal{F},\text{KPA})})$ and $V(\mathcal{N}_{(\mathcal{F},\text{KPA})})$ can all be approximated by $\frac{m^2}{2 \cdot 2^{kn}}$. Furthermore,

$$E(\mathcal{N}_{(\mathcal{F},\text{KPA})}) = \frac{m^2}{2}\left(\frac{1}{2^{kn}} + \frac{1}{2^{rn}}\right) \text{ and } E(\mathcal{N}_{(\mathcal{F},\text{CCA})}) = \frac{m^2}{2}\left(\frac{1}{2^{kn}} + \frac{1}{2^{(r-1)n}}\right).$$

Simplifying this, to distinguish $2r$ rounds, the complexity is $\sqrt{2} \cdot 2^{(r-\frac{k}{2})n}$ for KPA and $\sqrt{2} \cdot 2^{(r-\frac{k}{2}-1)n}$ for CCA. So when k is even, in both models, $\mathcal{F}$ can be distinguished from a random permutation when the round number is up to $3k-2$ with complexity $\sqrt{2} \cdot 2^{(k-1)n}$ and $\sqrt{2} \cdot 2^{(k-2)n}$ respectively. When k is odd, $\mathcal{F}$ can be distinguished from a random permutation when the round number is up to $3k-1$. In this case, the complexity is $\sqrt{2} \cdot 2^{(k-\frac{1}{2})n}$ and $\sqrt{2} \cdot 2^{(k-\frac{3}{2})n}$ respectively.

Odd Number of Rounds. Suppose that the number of rounds is $2r+1$ for some non-negative integers r. Let X_i be intermediate variables such that for any non-negative integer t, after $2t+1$ rounds, the state value is $(X_{tk}, \cdots, X_{tk+k-1})$. So $I_s = X_{rk+s}$ for all $0 \leq s \leq k-1$ while

$$X_s = \begin{cases} S_s, \text{ if } s = 1, \cdots, k-1, \\ S_0 \oplus F_{r+1}(S_1, \cdots, S_{k-1}) \text{ if } s = 0. \end{cases}$$

Following the expansion done before, the following equalities can be found:

- $I_0 = S_0 \oplus F_{r+1}(S_1, \cdots, S_{k-1}) \oplus \bigoplus_{i=0}^{r-1} F_{(r-i)}((X_{ik+s} \oplus F_{(r-i,s)}(X_{ik}))_{s=1}^{k-1})$
- $\forall s = 1, \cdots, k-1$, $I_s = S_s \oplus \bigoplus_{i=0}^{r-1} F_{(r-i,s)}(X_{ik}) = S_s \oplus F_{(r,s)}(S_0) \oplus \bigoplus_{i=1}^{r-1} F_{(r-i,s)}(X_{ik})$.

Because of this, all the distinguisher and calculation considered in the even number of rounds case can still be used in this case. Hence the complexity to distinguish $2r+1$ rounds is $\sqrt{2} \cdot 2^{(r-\frac{k}{2})n}$ for KPA and $\sqrt{2} \cdot 2^{(r-\frac{k}{2}-1)n}$ for CCA. When k is even, in both models, $\mathcal{F}$ can be distinguished from a random permutation when the round number is up to $3k-1$ with complexity $\sqrt{2} \cdot 2^{(k-1)n}$ and $\sqrt{2} \cdot 2^{(k-2)n}$ respectively. When k is odd, we can distinguish up to $3k$ rounds with complexity $\sqrt{2} \cdot 2^{(k-\frac{1}{2})n}$ and $\sqrt{2} \cdot 2^{(k-\frac{3}{2})n}$ respectively.

6.2 Comparison with Existing Result from [12]

We compare the result of previous subsection with the one given in Sect. 4.4 in [12]. As before, note all the expected values and variance should be multiplied by $\frac{1}{2}$, all the complexities should be multiplied by $\sqrt{2}$ and hence the maximum number of rounds, in this case, should be decreased by 2. After this adjustment, to distinguish t rounds, the complexities are summarised in Table 2:

Table 2. Summary of comparison of Alternating Feistel Schemes with fixed number of rounds t.

Parity of t	Attack model	Complexity [12]	Complexity (This Paper)
Odd ($t = 2p - 1$)	KPA	$\sqrt{2} \cdot 2^{(p-\frac{k}{2})n} \cdot \mathbf{2^{\frac{n}{2}}}$	$\sqrt{2} \cdot 2^{(p-\frac{k}{2})n} \cdot \mathbf{2^{-n}}$
	CPA/CCA	$\sqrt{2} \cdot 2^{(p-\frac{k}{2})n} \cdot \mathbf{2^{\frac{n}{2}}}$	$\sqrt{2} \cdot 2^{(p-\frac{k}{2})n} \cdot \mathbf{2^{-2n}}$
Even ($t = 2p$)	KPA	$\sqrt{2} \cdot 2^{(p-\frac{k}{2})n}$	$\sqrt{2} \cdot 2^{(p-\frac{k}{2})n}$
	CPA/CCA	$\sqrt{2} \cdot 2^{(p-\frac{k}{2})n}$	$\sqrt{2} \cdot 2^{(p-\frac{k}{2})} \cdot \mathbf{2^{-n}}$

In both models, when the number of rounds is odd, the complexity is better than the forward direction, which is a reduction by a factor of $2^{\frac{3n}{2}}$. However, when the number of rounds is even, backward direction requires the same complexity in the KPA model. In the CCA model, the complexity of backward direction is reduced by a factor of 2^n.

Note that after the adjustment to the result in [12], backward differential analysis achieves 2 more rounds in both models, from $3k-2$ rounds to $3k$ rounds.

7 Unbalanced Feistel Scheme

7.1 Analysis of Unbalanced Feistel Scheme

In this section we only consider two special cases of UFN(k', k). We discuss the analysis of the case when k is divisible by k'. This is a generalization of the UFN discussed in Sect. 6 of [16] where k is set to be 3 and k' is set to be 1. It can also be seen as a generalization of the UFN discussed in [17] where $k' = 1$. In Appendix D of the full version[2], the case when $k - k'$ is a factor of k is also considered. Due to the similarity of the technique used and also the page restriction, the detail of the analysis is omitted. This second case is a generalization of the analysis of UFN(k', k) when $k' = k - 1$ in [8,18,23].

Analysis of UFN(k',k) when k' divides k. Let A be a positive integer such that $k = Ak'$. Define intermediate variables X_i such that $(X_{sk}, \cdots X_{sk+(k-1)})$ is the state value after s rounds. So

$$(X_0, \cdots, X_{k-1}) = (S_0, \cdots, S_{k-1}).$$

Suppose that the number of rounds is $r = pA + q$ where $0 \leq q \leq A - 1$. So $(X_{rk}, \cdots, X_{rk+k-1}) = (I_0, \cdots, I_{k-1})$. Given the state value after $s - 1 (s \geq 1)$ backward rounds $(X_{(s-1)k}, \cdots, X_{(s-1)k+k-1})$, the output of the s-th backward round can be computed by:

- $X_{sk+t} = X_{(s-1)k+(t-k')}$ if $k' \leq t \leq k - 1$,

[2] The full version will be uploaded to Cryptology ePrint archive soon.

- $X_{sk+t} = X_{(s-1)k+(k-k'+t)} \oplus F_{r+1-s,t}(X_{(s-1)k}, \cdots X_{(s-1)k+k-k'-1}) = X_{(s-1)k+(k-k'+t)} \oplus F_{r+1-s,t}(X_{sk+k'}, \cdots, X_{sk+k-1})$ if $0 \leq t \leq k'-1$.
  Now for $0 \leq t \leq k'-1$, expanding the relation given above, we get:
  - If $q = 0$,

$$I_t = S_t \oplus \bigoplus_{s=1}^{p-1} F_{sA+2,t}(X_{(r-sA)k+k'}, \cdots, X_{(r-sA)k+k-1}) \oplus F_{2,t}(I_{k'}, \cdots, I_{k-1}),$$

  - Otherwise,

$$I_t = S_{(A-q)k'+t} \oplus \bigoplus_{s=1}^{p} F_{sA+2,t}(X_{(r-sA)k+k'}, \cdots, X_{(r-sA)k+k-1}) \oplus F_{2,t}(I_{k'}, \cdots, I_{k-1}).$$

The distinguisher counts the number of set of two plaintext ciphertext pairs $(i, j), 1 \leq i < j \leq m$ such that

$$\forall t = 0, \cdots, k'-1, I_t(i) \oplus I_t(j) = S_{(a-q)k'+t}(i) \oplus S_{(a-q)k'+t}(j).$$

In the CPA model, pick ciphertexts with a fixed value in $I_{k'}, \cdots, I_{k-1}$. In other words, the maximum number of plaintext-ciphertext pairs is $m \leq 2^{k'n}$.

The expected values and variances of the random variables can be found in Table 4 in Appendix A.

Using the definition of distinguishable, the complexity and maximum number of rounds distinguishable are summarised in Tables 5 and 6 which can be found in Appendix B.

A distinguisher for backward direction UFN(k', k) can be constructed by considering the forward propagation of the equation. Hence, given the value of $X_{sk}, \cdots, X_{sk+k-1}$, we have:

- $X_{sk+t} = X_{(s+1)k+(t+k')}$ if $0 \leq t \leq k-k'-1$,
- $X_{sk+t} = X_{(s+1)k+(t-k+k')} \oplus F_{r-s,t}(X_{(s+1)k+k'}, \cdots X_{(s+1)k+k-1})$
  $= X_{(s+1)k+(t-k+k')} \oplus F_{r-s,t}(X_{sk}, \cdots, X_{sk+k-k'-1})$ if $k-k' \leq t \leq k-1$.

Expanding S_t, the following equalities can be obtained:

- If $q = 0$,

$$S_t = I_t \oplus \bigoplus_{s=1}^{p-1} F_{r-sA,t}(X_{sAk}, \cdots, X_{sAk+k-k'-1}) \oplus F_{r,t}(S_0, \cdots, I_{k-k'-1}),$$

- Otherwise,

$$S_t = I_{t-(A-q)k'} \oplus \bigoplus_{s=1}^{p} F_{r-sA,t}(X_{iAk}, \cdots, X_{iAk+k-k'-1}) \oplus F_{r,t}(S_0, \cdots, S_{k-k'-1}).$$

The distinguisher finds the number of sets of two plaintext-ciphertext pairs (i, j) such that $\forall t = k - k', \cdots k - 1, S_t(i) \oplus S_t(j) = I_{t-(A-q)k'}(i) \oplus I_{t-(A-q)k'}(j)$ where $S_0, \cdots S_{k-k'-1}$ are fixed in the CCA model. It is easy to see that with this model, we have exactly the same expected values, variances and distinguishability as the ones found in Tables 4, 5 and 6.

8 Conclusion

In this paper, differential analysis on the inverse function of four different types of generic Generalized Feistel Scheme, namely Type-1, Type-3, Alternating Scheme and UFN(k', k) was considered. We show that for Type-1 Feistel Scheme, backward distinguisher performs better especially in the chosen ciphertext attack compared to the results in [12]. Using the same complexity, we can distinguish $k - 1$ more rounds while distinguishing the same number of rounds requires smaller complexity with factor of $\frac{1}{2^n}$.

In Type-2 and Alternating Feistel scheme, although there are some difference in the complexity, both directions can achieve almost the same number of rounds. This shows that these two types can be seen as almost symmetric from both direction.

We improve the differential cryptanalysis in Type-3 Feistel Scheme in several cases. In the KPA model with low number of branches, $2 \leq k \leq 5$, our analysis provides a lower bound of the number of rounds that is indistinguishable from random permutation. Secondly, in the CCA model, the lower bound of maximum number of rounds distinguishable is increased by 1 round, from $k + 1$ obtained in [12] to $k + 2$.

In Alternating Feistel Scheme, we achieve 2 more rounds than the one claimed in [12]. The complexity is reduced by a factor of $2^{\frac{3n}{2}}$ when distinguishing the same odd number of rounds.

Lastly, a lower bound for the maximum number of rounds that is distinguishable from random permutation in UFN(k', k) scheme is given through the forward direction distinguisher. To the best of our knowledge, this is the first bound given in a rather general case in which k' is arbitrary as long as k' is a divisor of k for any integer k.

A Expected Value and Variance of Random Variables Concerning Type-1 Feistel Scheme and UFN(k', k) When k' Divides k.

The following table summarises the expected value and variance of the random variables used in the analysis of Type-1 Feistel Schemes.

The next table summarises the expected values and variances for random variables used in the analysis of UFN(k', k) when k' divides k.

Table 3. Expected value and variance of random variables concerning Type-1 Feistel Schemes

b	Attack model	Expected value	Variance	Maximum value of m
0	KPA	$\frac{m^2}{2}\left(\frac{1}{2^{2n}}+\frac{1}{2^{an}}\right)$	$\frac{m^2}{2\cdot 2^{2n}}$	2^{kn}
	CCA	$\frac{m^2}{2}\left(\frac{1}{2^{2n}}+\frac{1}{2^{(a-1)n}}\right)$	$\frac{m^2}{2\cdot 2^{2n}}$	$2^{(k-2)n}$
$1 \le b \le k-2$	KPA	$\frac{m^2}{2}\left(\frac{1}{2^{2n}}+\frac{1}{2^{(a+1)n}}\right)$	$\frac{m^2}{2\cdot 2^{2n}}$	2^{kn}
	CCA	$\frac{m^2}{2}\left(\frac{1}{2^{2n}}+\frac{1}{2^{(a-1)n}}\right)$	$\frac{m^2}{2\cdot 2^{2n}}$	$2^{(k-2)n}$
$k-1$	KPA	$\frac{m^2}{2}\left(\frac{1}{2^{2n}}+\frac{1}{2^{(a+1)n}}\right)$	$\frac{m^2}{2\cdot 2^{2n}}$	2^{kn}
	CCA	$\frac{m^2}{2}\left(\frac{1}{2^{2n}}+\frac{1}{2^{(a-1)n}}\right)$	$\frac{m^2}{2\cdot 2^{2n}}$	$2^{(k-3)n}$

Table 4. Expected value and variance for various cases of UFN(k', k)

Attack model	q value	Π	E	V	σ
KPA	0	Perm	$\frac{m^2}{2\cdot 2^{k'n}}$	$\frac{m^2}{2\cdot 2^{k'n}}$	$\frac{m}{\sqrt{2}\cdot 2^{\frac{k'}{2}n}}$
		$\mathcal{F}$	$\frac{m^2}{2}\cdot\left(\frac{1}{2^{k'n}}+\frac{k'}{2^{(k'+p-1)n}}\right)$	$\frac{m^2}{2\cdot 2^{k'n}}$	$\frac{m}{\sqrt{2}\cdot 2^{\frac{k'}{2}n}}$
	$1 \le q \le A-1$	Perm	$\frac{m^2}{2\cdot 2^{k'n}}$	$\frac{m^2}{2\cdot 2^{k'n}}$	$\frac{m}{\sqrt{2}\cdot 2^{\frac{k'}{2}n}}$
		$\mathcal{F}$	$\frac{m^2}{2}\cdot\left(\frac{1}{2^{k'n}}+\frac{k'}{2^{(k'+p)n}}\right)$	$\frac{m^2}{2\cdot 2^{k'n}}$	$\frac{m}{\sqrt{2}\cdot 2^{\frac{k'}{2}n}}$
CPA	0	Perm	$\frac{m^2}{2\cdot 2^{k'n}}$	$\frac{m^2}{2\cdot 2^{k'n}}$	$\frac{m}{\sqrt{2}\cdot 2^{\frac{k'}{2}n}}$
		$\mathcal{F}$	$\frac{m^2}{2}\cdot\left(\frac{1}{2^{k'n}}+\frac{k'}{2^{(k'+p-2)n}}\right)$	$\frac{m^2}{2\cdot 2^{k'n}}$	$\frac{m}{\sqrt{2}\cdot 2^{\frac{k'}{2}n}}$
	$1 \le q \le A-1$	Perm	$\frac{m^2}{2\cdot 2^{k'n}}$	$\frac{m^2}{2\cdot 2^{k'n}}$	$\frac{m}{\sqrt{2}\cdot 2^{\frac{k'}{2}n}}$
		$\mathcal{F}$	$\frac{m^2}{2}\cdot\left(\frac{1}{2^{k'n}}+\frac{k'}{2^{(k'+p-1)n}}\right)$	$\frac{m^2}{2\cdot 2^{k'n}}$	$\frac{m}{\sqrt{2}\cdot 2^{\frac{k'}{2}n}}$

B Distinguishability Table for UFN(k', k)

The following tables contain the summary of distinguishability of UFN(k', k) from a random permutation.

Table 5. Complexity of Unbalanced Feistel Scheme

k'	q value	Attack model	Complexity of distinguishing $pA+q$ rounds
1	0	KPA	$\sqrt{2}\cdot 2^{(p-\frac{1}{2})n}$
		CPA/CCA	$\sqrt{2}\cdot 2^{(p-\frac{3}{2})n}$
	$1 \le q \le A-1$	KPA	$\sqrt{2}\cdot 2^{(p+\frac{1}{2})n}$
		CPA/CCA	$\sqrt{2}\cdot 2^{(p-\frac{1}{2})n}$
$k' \ge 2$	0	KPA	$\frac{\sqrt{2}}{k'}\cdot 2^{(\frac{k'}{2}+p-1)n}$
		CPA/CCA	$\frac{\sqrt{2}}{k'}\cdot 2^{(\frac{k'}{2}+p-2)n}$
	$1 \le q \le A-1$	KPA	$\frac{\sqrt{2}}{k'}\cdot 2^{(p+\frac{k'}{2})n}$
		CPA/CCA	$\frac{\sqrt{2}}{k'}\cdot 2^{(p+\frac{k'}{2}-1)n}$

Table 6. Summary of distinguishability of Unbalanced Feistel Scheme

k'	q value	Attack model	Maximum p distinguishable→Maximum round distinguishable
1	0	KPA	$k \to k^2$
		CPA/CCA	$2 \to 2k$
	$1 \le q \le A-1$	KPA	$k \to k^2 + k - 1$
		CPA/CCA	$1 \to k + k - 1$
$k' \ge 2$	0	KPA	$\begin{cases} k - \frac{k'}{2} + 1 \to \frac{k^2}{k'} - \frac{k}{2} + \frac{k}{k'} & \text{if } k' \text{ is even} \\ k - \frac{k'-1}{2} \to \frac{k^2}{k'} - \frac{k(k'-1)}{2k'} & \text{if } k' \text{ is odd} \end{cases}$
		CPA/CCA	$\begin{cases} \frac{k'}{2} + 2 \to \frac{k}{2} + 2\frac{k}{k'} & \text{if } k' \text{ is even} \\ \frac{k'+3}{2} \to \frac{k(k'+3)}{2k'} & \text{if } k' \text{ is odd} \end{cases}$
	$1 \le q \le A-1$	KPA	$\begin{cases} k - \frac{k'}{2} \to \frac{k^2}{k'} - \frac{k}{2} + \frac{k}{k'} - 1 & \text{if } k' \text{ is even} \\ k - \frac{k'+1}{2} \to \frac{k^2}{k'} - \frac{k(k'+1)}{2k'} + \frac{k}{k'} - 1 & \text{if } k' \text{ is odd} \end{cases}$
		CPA/CCA	$\begin{cases} \frac{k'}{2} + 1 \to \frac{k}{2} + \frac{k}{k'} + \frac{k}{k'} - 1 & \text{if } k' \text{ is even} \\ \frac{k'+1}{2} \to \frac{k(k'+1)}{2k'} + \frac{k}{k'} - 1 & \text{if } k' \text{ is odd} \end{cases}$

References

1. Anderson, R., Biham, E.: Two practical and provably secure block ciphers: BEAR and LION. In: Gollmann, D. (ed.) FSE 1996. LNCS, vol. 1039, pp. 113–120. Springer, Heidelberg (1996). https://doi.org/10.1007/3-540-60865-6_48
2. Aoki, K., Ichikawa, T., Kanda, M., Matsui, M., Moriai, S., Nakajima, J., Tokita, T.: *Camellia*: a 128-bit block cipher suitable for multiple platforms — design and analysis. In: Stinson, D.R., Tavares, S. (eds.) SAC 2000. LNCS, vol. 2012, pp. 39–56. Springer, Heidelberg (2001). https://doi.org/10.1007/3-540-44983-3_4
3. Bertoni, G., Daemen, J., Peeters, M., Van Assche, G.: Keccak Sponge Function Family Main Document. Submission to NIST (Round 2) (2009)
4. Biham, E., Biryukov, A., Dunkelman, O., Richardson, E., Shamir, A.: Initial observations on skipjack: cryptanalysis of skipjack-3XOR. In: Tavares, S., Meijer, H. (eds.) SAC 1998. LNCS, vol. 1556, pp. 362–375. Springer, Heidelberg (1999). https://doi.org/10.1007/3-540-48892-8_27
5. Biham, E., Biryukov, A., Shamir, A.: Cryptanalysis of skipjack reduced to 31 rounds using impossible differentials. In: Stern, J. (ed.) EUROCRYPT 1999. LNCS, vol. 1592, pp. 12–23. Springer, Heidelberg (1999). https://doi.org/10.1007/3-540-48910-X_2
6. Gueron, S., Mouha, N.: Simpira v2: a family of efficient permutations using the AES round function. In: Cheon, J.H., Takagi, T. (eds.) ASIACRYPT 2016. LNCS, vol. 10031, pp. 95–125. Springer, Heidelberg (2016). https://doi.org/10.1007/978-3-662-53887-6_4
7. Hoang, V.T., Rogaway, P.: On generalized feistel networks. In: Rabin, T. (ed.) CRYPTO 2010. LNCS, vol. 6223, pp. 613–630. Springer, Heidelberg (2010). https://doi.org/10.1007/978-3-642-14623-7_33
8. Jutla, C.S.: Generalized birthday attacks on unbalanced Feistel networks. In: Krawczyk, H. (ed.) CRYPTO 1998. LNCS, vol. 1462, pp. 186–199. Springer, Heidelberg (1998). https://doi.org/10.1007/BFb0055728
9. Knudsen, L.: DEAL - a 128-bit block cipher. In: NIST AES Proposal (1998)
10. Luby, M., Rackoff, C.: How to construct pseudo-random permutations from pseudo-random functions. In: Williams, H.C. (ed.) CRYPTO 1985. LNCS, vol. 218, pp. 447–447. Springer, Heidelberg (1986). https://doi.org/10.1007/3-540-39799-X_34

11. Lucks, S.: Faster Luby-Rackoff ciphers. In: Gollmann, D. (ed.) FSE 1996. LNCS, vol. 1039, pp. 189–203. Springer, Heidelberg (1996). https://doi.org/10.1007/3-540-60865-6_53
12. Nachef, V., Volte, E., Patarin, J.: Differential attacks on generalized Feistel schemes. In: Abdalla, M., Nita-Rotaru, C., Dahab, R. (eds.) CANS 2013. LNCS, vol. 8257, pp. 1–19. Springer, Cham (2013). https://doi.org/10.1007/978-3-319-02937-5_1
13. Nyberg, K.: Generalized Feistel networks. In: Kim, K., Matsumoto, T. (eds.) ASIACRYPT 1996. LNCS, vol. 1163, pp. 91–104. Springer, Heidelberg (1996). https://doi.org/10.1007/BFb0034838
14. Patarin, J.: Generic attacks on Feistel schemes. In: Boyd, C. (ed.) ASIACRYPT 2001. LNCS, vol. 2248, pp. 222–238. Springer, Heidelberg (2001). https://doi.org/10.1007/3-540-45682-1_14
15. 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 (2004). https://doi.org/10.1007/978-3-540-28628-8_7
16. 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
17. Patarin, J., Nachef, V., Berbain, C.: Generic attacks on unbalanced feistel schemes with contracting functions. In: Lai, X., Chen, K. (eds.) ASIACRYPT 2006. LNCS, vol. 4284, pp. 396–411. Springer, Heidelberg (2006). https://doi.org/10.1007/11935230_26
18. 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 (2007). https://doi.org/10.1007/978-3-540-76900-2_20
19. Schneier, B., Kelsey, J.: Unbalanced Feistel networks and block cipher design. In: Gollmann, D. (ed.) FSE 1996. LNCS, vol. 1039, pp. 121–144. Springer, Heidelberg (1996). https://doi.org/10.1007/3-540-60865-6_49
20. Shirai, T., Shibutani, K., Akishita, T., Moriai, S., Iwata, T.: The 128-bit blockcipher CLEFIA (extended abstract). In: Biryukov, A. (ed.) FSE 2007. LNCS, vol. 4593, pp. 181–195. Springer, Heidelberg (2007). https://doi.org/10.1007/978-3-540-74619-5_12
21. Tjuawinata, I., Huang, T., Wu, H.: Cryptanalysis of simpira v2. In: Pieprzyk, J., Suriadi, S. (eds.) ACISP 2017. LNCS, vol. 10342, pp. 384–401. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-60055-0_20
22. Treger, J., Patarin, J.: Generic attacks on feistel networks with internal permutations. In: Preneel, B. (ed.) AFRICACRYPT 2009. LNCS, vol. 5580, pp. 41–59. Springer, Heidelberg (2009). https://doi.org/10.1007/978-3-642-02384-2_4
23. 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 (2010). https://doi.org/10.1007/978-3-642-17373-8_6
24. 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 1989. LNCS, vol. 435, pp. 461–480. Springer, New York (1990). https://doi.org/10.1007/0-387-34805-0_42