Cryptogr. Commun. (2018) 10:59–77
DOI 10.1007/s12095-017-0244-7

Generic attacks with standard deviation analysis on a-feistel schemes

Valérie Nachef[1] · Jacques Patarin[2] · Emmanuel Volte[1]

Received: 29 November 2016 / Accepted: 7 July 2017 / Published online: 24 July 2017

Abstract A usual way to construct block ciphers is to apply several rounds of a given structure. Many kinds of attacks are mounted against block ciphers. Among them, differential and linear attacks are widely used. Vaudenay showed that ciphers achieving perfect pairwise decorrelation are secure against linear and differential attacks. It is possible to obtain such schemes by introducing at least one random affine permutation as a round function in the design of the scheme. In this paper, we study attacks on schemes based on classical Feistel schemes where we introduce one or two affine permutations. Since these schemes resist against linear and differential attacks, we will study attacks based on specific equations on 4-tuples of plaintext/ciphertext messages. We show that these schemes are stronger than classical Feistel schemes.

Keywords Affine permutations · Classical Feistel permutations · Pseudo-random permutations · Generic attacks · Luby-Rackoff theory · Block ciphers

Mathematics Subject Classification (2010) 94A60

This article is part of the Topical Collection on *Recent Trends in Cryptography*

✉ Valérie Nachef
valerie.nachef@u-cergy.fr

Jacques Patarin
jpatarin@club-internet.fr

Emmanuel Volte
emmanuel.volte@u-cergy.fr

[1] Department of Mathematics, University of Cergy-Pontoise, CNRS UMR 8088,
2 Avenue Adolphe Chauvin, 95011 Cergy-Pontoise Cedex, France

[2] Laboratoire de Mathématiques de Versailles, UVSQ CNRS, Université de Paris-Saclay,
78035 Versailles, France

1 Introduction

Many schemes have been designed in order to construct pseudo-random permutations using round functions. Examples of such schemes are given by classical Feistel schemes with random functions [7, 8, 14] or random permutations [6, 17], unbalanced Feistel schemes with expanding [5, 16, 21] or contracting functions [13, 15], Misty schemes [3, 11], generalized Feistel schemes of type 1, 2 and 3 [12]. Also, generic attacks on these different kinds of block ciphers have been extensively studied. By generic attacks, we mean that the keys are random functions.

In [18, 19], Vaudenay showed that if a block cipher has perfect pairwise decorrelation, then it is secure against linear and differential attacks. Moreover, adding an affine permutation as a round function in the construction of a block cipher allows to obtain perfect pairwise decorrelation and thus to prevent from linear and differential cryptanalysis. COCONUT and PEANUT [18] are examples of such schemes: they use any cipher then an affine permutation followed again by any cipher. In [13], the authors propose schemes for which there is first a pairwise independent permutation (an affine permutation is an example of a pairwise independent permutation) followed by a classical Feistel scheme or an unbalanced Feistel scheme with contracting functions, and with or without another affine permutation at the end. In [13], the security of these schemes is studied.

This is why it is quite natural and interesting to study generic attacks on schemes where we have a classical Feistel structure with several rounds together with one or two affine permutations as a round functions introduced at some stage of the construction. This defines a family of schemes that we will denote by A-Feistel schemes. For example, it is possible to apply first an affine permutation and then several rounds of a Feistel scheme. We can also begin with a Feistel scheme and end with an affine permutation. Another possibility is to introduce an affine permutation after several rounds of a Feistel scheme and then to go on with a Feistel scheme. It is also possible to have first an affine permutation then a Feistel scheme and again a random permutation. As far as we know, no systematic study of attacks has been done. This is the aim of this paper.

We will study Known Plaintext Attacks (KPA) and non adaptive Chosen Plaintext Attacks (CPA-1). Since we introduce an affine permutation at the beginning, at the end, inside the Feistel scheme, or both at the beginning and at the end, by symmetry, we will obtain results for Known Ciphertext Attacks (KCA) and non adaptive Chosen Ciphertext Attacks (CCA-1). The aim of our attacks is to distinguish a random permutation from a random permutation produced by the schemes. For some of our attacks, we will make a precise analysis of standard deviations.

The paper is organized as follows. In Section 2, we define A-Feistel schemes. In Section 3, we describe our best KPA and CPA-1 on schemes with one affine permutation. We show that it is possible to attack up to 3 rounds (for the Feistel scheme) with a number of messages less than 2^{2n} when the affine permutation is placed at the beginning or at the end of the scheme. When the affine permutation is situated between two Feistel schemes, we can attack up to 4 rounds with less than 2^{2n} messages (this means that when we add the number of rounds for each Feistel scheme, we obtain 4 rounds). Then we describe attacks against generators of permutations. We did some simulations of our attacks. The results of these simulations are given in Section 3.3. In Section 4, we present attacks on schemes for which we apply first an affine permutation, then a Feistel scheme with several rounds and then an affine permutation. Section 5 is devoted to the computation of standard deviations in the case of A-Feistel schemes since the computation for randoms permutation can be done automatically as we will explain in the next section.

2 Definition of A-Feistel schemes and overview of the attacks

We use the following standard notations. The number of messages is denoted by m. The set of the 2^n binary strings of length n is denoted by $\{0,1\}^n$. For $a, b \in \{0,1\}^n$, $[a, b]$ will be the string of length $2n$ of $\{0,1\}^{2n}$ which is the concatenation of a and b. For $a, b \in \{0,1\}^n$, $a \oplus b$ stands for bit by bit exclusive or of a and b. The composition of functions is denoted by $\circ$. The set of all functions from $\{0,1\}^n$ to $\{0,1\}^n$ is F_n. Let f be a function of F_n. Let L, R, S and T be elements of $\{0,1\}^n$. One round of A-Feistel scheme is defined by $\Psi(f)[L, R] = [S, T] \overset{\text{def}}{\Leftrightarrow} (S = R \text{ and } T = L \oplus f(R))$. More generally, let $f_1, f_2, \ldots, f_d$ be d functions of F_n. Then by definition: $\Psi^d(f_1, \ldots, f_d) = \Psi(f_d) \circ \cdots \circ \Psi(f_2) \circ \Psi(f_1)$. The permutation $\Psi^d(f_1, \ldots, f_d)$ is called a "Feistel scheme with d rounds" and is denoted by Ψ^d.

We now define A-Feistel Schemes. We consider an affine permutation from $\{0,1\}^{2n}$ to $\{0,1\}^{2n}$. It is written under the form $\varphi : M \to A{\cdot}M \oplus C$ where $A \in GL(2n, F_2)$ and $C \in \{0,1\}^{2n}$. In order to construct an A-Feistel scheme with "d rounds", we use one or two affine permutations and a classical Feistel scheme with d rounds. Here d is related to the Feistel scheme. Let φ and φ' be affine permutations, an A-Feistel scheme with d rounds is one of the following permutations: $\Psi^d \circ \varphi$, $\varphi \circ \Psi^d$, $\Psi^{d_2} \circ \varphi \circ \Psi^{d_1}$ with $d_1 + d_2 = d$ or $\varphi' \circ \Psi^d \circ \varphi$. Since A is a linear permutation from $\{0,1\}^{2n}$ to $\{0,1\}^{2n}$, it can be represented by a matrix, still denoted by A. We will write A under the form: $\begin{pmatrix} A_1 & A_2 \\ A_3 & A_4 \end{pmatrix}$ where each $A_i \in \mathcal{M}(n \times n, \mathbb{F}_2)$. We also set $C = [C_1, C_2]$ where $C_i \in \{0,1\}^n$.

Perfect pairwise decorrelation of affine permutations In [18, 19], Vaudenay showed how to construct perfect pairwise decorrelated ciphers on a field structure $\mathcal{F}$ by $F(M) = K_1 + K_2{\cdot}M$ where $(K_1, K_2) \in \mathcal{F} \times \mathcal{F}^*$. When the functions are defined on $\{0,1\}^{2n}$, the operations are taken over $GF(2^{2n})$. We can also consider $GF(2^{2n})$ as a vector space over $\{0,1\}$. The function $M \mapsto K_2{\cdot}M$ is linear and can be represented by a matrix. If we want to express this matrix in the canonical basis, the coordinates of K_2 are on the first column of the matrix. In this paper, we consider that any invertible matrix can be used as the linear part of the affine permutation we are using. We still have perfect pairwise decorrelation: for any M, M' such that $M \neq M'$ the random variable $(\varphi(M), \varphi(M'))$ is uniformly distributed among all the pairs (Y, Y') such that $Y \neq Y'$.

Notation for A-Feistel schemes

1. $\Psi^d \circ \varphi$

$$[L, R] \xrightarrow{\varphi} [P, Q] \xrightarrow{\Psi(f_1)} [Q, X^1] \xrightarrow{\Psi(f_2)} [X^1, X^2] \ldots$$
$$\xrightarrow{\Psi(f_{d-1})} [X^{d-2}, X^{d-1}] \xrightarrow{\Psi(f_d)} [S, T]$$

Thus we have introduced internal variables: $P = A_1{\cdot}L \oplus A_2{\cdot}R \oplus C_1$, $Q = A_3{\cdot}L \oplus A_4{\cdot}R \oplus C_2$, $X^1 = P \oplus f_1(Q)$, $X^2 = Q \oplus f_2(X^1)$ and for $j \geq 3$, $X^j = X^{j-2} \oplus f_j(X^{j-1})$.

2. $\varphi \circ \Psi^d$

$$[L, R] \xrightarrow{\Psi(f_1)} [R, X^1] \xrightarrow{\Psi(f_2)} [X^1, X^2] \ldots$$
$$\xrightarrow{\Psi(f_{d-1})} [X^{d-2}, X^{d-1}] \xrightarrow{\Psi(f_d)} [X^{d-1}, X^d] \xrightarrow{\varphi} [S, T]$$

The internal variables are: $X^1 = L \oplus f_1(R)$, $X^2 = R \oplus f_2(X^1)$ and for $j \geq 3$, $X^j = X^{j-2} \oplus f_j(X^{j-1})$. Since we apply φ at the end, we have: $S = A_1{\cdot}X^{d-1} \oplus A_2{\cdot}X^d \oplus C_1$, $T = A_3{\cdot}X^{d-1} \oplus A_4{\cdot}X^d \oplus C_2$.

3. $\Psi^{d_2} \circ \varphi \circ \Psi^{d_1}$ with $d_1 + d_2 = d$

$$[L, R] \xrightarrow{\Psi(f_1)} [R, X^1] \xrightarrow{\Psi(f_2)} [X^1, X^2] \dots \xrightarrow{\Psi(f_{d_1})} [X^{d_1-1}, X^{d_1}]$$

$$\xrightarrow{\varphi} [P, Q] \xrightarrow{\Psi(f_{d_1+1})} [Q, X^{d_1+1}] \xrightarrow{\Psi(f_{d_1+2})} [X^{d_1+1}, X^{d_1+2}] \dots \xrightarrow{\Psi(f_{d_1+d_2})} [S, T]$$

The internal variables are: $X^1 = L \oplus f_1(R)$, $X^2 = R \oplus f_2(X^1)$ and for $3 \leq j \leq d_1$, $X^j = X^{j-2} \oplus f_j(X^{j-1})$, $P = A_1 \cdot X^{d_1-1} \oplus A_2 \cdot X^{d_1} \oplus C_1$, $Q = A_3 \cdot X^{d_1-1} \oplus A_4 \cdot X^{d_1} \oplus C_2$, $X^{d_1+1} = P \oplus f_{d_1+1}(Q)$, $X^{d_1+2} = Q \oplus f_{d_1+2}(X^{d_1+1})$. For $d_1+3 \leq j \leq d_1+d_2$, $X^j = X^{j-2} \oplus f_j(X^{j-1})$.

4. $\varphi' \circ \Psi^d \circ \varphi$

$$[L, R] \xrightarrow{\varphi} [P, Q] \xrightarrow{\Psi(f_1)} [Q, X^1] \xrightarrow{\Psi(f_2)} [X^1, X^2] \dots$$

$$\xrightarrow{\Psi(f_{d-1})} [X^{d-2}, X^{d-1}] \xrightarrow{\Psi(f_d)} [X^{d-1}, X^d] \xrightarrow{\varphi'} [S, T]$$

With the internal variables: $P = A_1 \cdot L \oplus A_2 \cdot R \oplus C_1$, $Q = A_3 \cdot L \oplus A_4 \cdot R \oplus C_2$, $X^1 = P \oplus f_1(Q)$, $X^2 = Q \oplus f_2(X^1)$ and for $j \geq 3$, $X^j = X^{j-2} \oplus f_j(X^{j-1})$. Finally $S = A'_1 \cdot X^{d-1} \oplus A'_2 \cdot X^d \oplus C'_1$, $T = A'_3 \cdot X^{d-1} \oplus A'_4 \cdot X^d \oplus C'_2$.

Overview of the attacks We present attacks that allow us to distinguish a permutation computed by the scheme from a random permutation. Depending on the number of rounds, it is possible to find some relations between the input and output variables. These relations hold conditionally to equalities on some internal variables due to the structure of the Feistel scheme.

Our attacks consist in using plaintext/ciphertexts 4-tuples and in counting the number $\mathcal{N}$ of these 4-tuples that satisfy the relations between the input and output variables. We then compare $\mathcal{N}_{scheme}$, the number of such 4-tuples we obtain with an A-Feistel scheme, with $\mathcal{N}_{perm}$, the corresponding number for a random permutation. The attack is successful, i.e. we are able to distinguish a permutation generated by an A-Feistel scheme from a random permutation, if the difference $|\mathbb{E}(\mathcal{N}_{scheme}) - \mathbb{E}(\mathcal{N}_{perm})|$ is larger than both standard deviations $\sigma(\mathcal{N}_{perm})$ and $\sigma(\mathcal{N}_{scheme})$, where $\mathbb{E}$ denotes the expectation.

Indeed, thanks to the Chebychev formula, which states that for any random variable X, and any $\alpha > 0$, we have $\mathbb{P}(|X - \mathbb{E}(X)| \geq \alpha\sigma(X)) \leq \frac{1}{\alpha^2}$, it is then possible to construct a prediction interval for $\mathcal{N}_{scheme}$ for example, in which future computations will fall, with a good probability.This gives the number of messages needed for the attack. In order to compute $\mathbb{E}$ and σ for a scheme and a random permutation, we need to take into account the fact that the structures obtained from the plaintext/ciphertext 4-tuples are not independent.

However, their mutual dependence is very small. To compute $\sigma(\mathcal{N}_{perm})$ and $\sigma(\mathcal{N}_{scheme})$, we will use this well-known formula (see [4], p.97), that we will call the "Covariance Formula": if $x_1, \dots x_n$, are random variables, then if V represents the variance, we have

$$V\left(\sum_{i=1}^{n} x_i\right) = \sum_{i=1}^{n} V(x_i) + 2\sum_{i=1}^{n-1}\sum_{j=i+1}^{n} \left[\mathbb{E}(x_i\, x_j) - \mathbb{E}(x_i)\mathbb{E}(x_j)\right]$$

Recently, a tool has been developed in order to compute expectations and variances for $\mathcal{N}_{perm}$. This is a computer program that allows to avoid tedious computations. We will always use it throughout this paper. It is available at the following link: http://volte.u-cergy.fr/SitePerso/Articles/program.zip. This is also explained in [20].

3 A-Feistel schemes with one affine permutation

3.1 Preliminaries

Our attacks use 4-tuples of plaintext/ciphertexts. Suppose that we have 4 inputs $[L_i, R_i]$, $[L_j, R_j]$, $[L_k, R_k]$, $[L_\ell, R_\ell]$. The conditions on the inputs will be: $L_i = L_j$, $L_k = L_\ell \neq L_i$, $R_i = R_k$, $R_j = R_\ell \neq R_i$, see Fig. 1. The corresponding outputs are denoted by $[S_i, T_i]$, $[S_j, T_j]$, $[S_k, T_k]$, $[S_\ell, T_\ell]$. According to the construction of the scheme, we will set some conditions on the outputs.

As we have seen in the previous section, the affine permutation can be used as the first round, the last round, or any intermediate round. Notice that with an affine permutation, the two branches of the input are mixed, unlike with one round of a Feistel scheme where the right branch is only shifted. This will affect the choice of the conditions on the outputs.

When the affine permutation is used as the first or an intermediate round, the structure of the Feistel scheme will be dominant and the condition on the output will be: $S_i \oplus S_j \oplus S_k \oplus S_\ell = 0$. When the affine permutation is used as the last round, it will be dominant and we will have 2 conditions on the outputs: $S_i \oplus S_j \oplus S_k \oplus S_\ell = 0$ and $T_i \oplus T_j \oplus T_k \oplus T_\ell = 0$.

3.2 One affine permutation and a Feistel scheme with one round

$\Psi(f_1) \circ \varphi$: CPA-1 with 4 messages and KPA with $2^{\frac{n}{2}}$ messages Let $[L, R]$ denote the input. The output is denoted by $[S, T]$. After the affine permutation, the output is denoted by $[P, Q]$ where $P = A_1 \cdot L \oplus A_2 \cdot R \oplus C_1$, and $Q = A_3 \cdot L \oplus A_4 \cdot R \oplus C_2$. Then we apply a Feistel scheme and the output is given by $[S, T]$ where $S = Q$ and $T = X^1 = P \oplus f_1(Q)$ where $f_1 \in_R F_n$. Here, we have: $S = A_3 \cdot L \oplus A_4 \cdot R \oplus C_2$.

We first describe a CPA-1 with 4 messages. We choose L_1, L_2, R_1, R_2 such that $L_1 \neq L_2$ and $R_1 \neq R_2$. Then we construct the four following messages: $[L_1, R_1]$, $[L_1, R_2]$, $[L_2, R_1]$ and $[L_2, R_2]$. Let us write $[S_1, T_1] = \varphi[L_1, R_1]$, $[S_1', T_1'] = \varphi[L_1, R_2]$, $[S_2, T_2] = \varphi[L_2, R_2]$ and $[S_2', T_2'] = \varphi[L_2, R_1]$. With an A-Feistel scheme, the probability to obtain $S_1 \oplus S_1' \oplus S_2 \oplus S_2' = 0$ is equal to one. For a random permutation, the same probability is

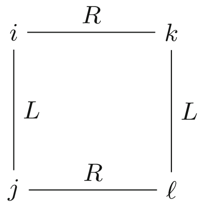

Fig. 1 Equalities in L and R for the 4 inputs

about $\frac{1}{2^n}$. Thus we need 4 messages to distinguish a random permutation from a permutation of the form $\Psi(f_1) \circ \varphi$.

We now give a KPA. If we have m messages, the number of (i, j, k, ℓ) such that $L_i \oplus L_j \oplus L_k \oplus L_\ell = 0$ and $R_i \oplus R_j \oplus R_k \oplus R_\ell = 0$ is about $\frac{m^4}{2^{2n}}$. Thus, when $m \simeq 2^{\frac{n}{2}}$, the probability to obtain a 4-tuple satisfying the above conditions is non-negligible. For such a 4-tuple, we check if $S_i \oplus S_j \oplus S_k \oplus S_\ell = 0$. The probability is 1 for an A-Feistel scheme and $\frac{1}{2^n}$ for a random permutation.

Remark 1 In this KPA, we can notice that the complexity in time is much bigger, because, in order to find such 4 messages, we have to consider all couples of messages (i, j) with $i < j$ and compute $L_i \oplus L_j$, then look for collisions in this list. This is about $\frac{m\times(m-1)}{2} \times m \ln m = O(m^3 \ln m) = O(n 2^{1.5n})$ operations.

$\varphi \circ \Psi(f_1)$: CPA-1 with 4 messages and KPA with $(n+1)2^{\frac{n}{2}}$ messages The CPA-1 is similar to the previous one except that the conditions on the outputs are $S_1 \oplus S_1' \oplus S_2 \oplus S_2' = 0$ and $T_1 \oplus T_1' \oplus T_2 \oplus T_2' = 0$, since φ is at the end of the structure. For the KPA, if we have $2^{\frac{n}{3}}$ messages then, by the birthday paradox, we can find, with a good probability, a pair $[L_i, R_i], [L_j, R_j]$ such that $R_i = R_j$. Let $d_1 = L_i \oplus L_j$, $d_2 = S_i \oplus S_j$ and $d_3 = T_i \oplus T_j$. Then we have: $d_2 = A_2(d_1)$ and $d_3 = A_4(d_1)$. This gives $2n$ (or a little less if A_2 and A_4 are not invertible) linear equations in the $2n^2$ unknown coefficients of A_2 and A_4. If we have $n 2^{\frac{n}{2}}$ known plaintexts, we can expect to find n pairs with equal R-parts. This shows that we get enough linear equations to determine A_2 and A_4 completely. Then we can distinguish the permutation generated by the A-Feistel from a random permutation by taking one more pair with $R_i = R_j$ and check, if they satisfy the linear system given by the known A_2 and A_4. This provides a KPA with about $(n+1)2^{\frac{n}{2}}$ messages.

3.3 One affine permutation and a Feistel scheme with two rounds

$\Psi(f_2) \circ \Psi(f_1) \circ \varphi$: CPA-1 with $2^{\frac{n}{2}}$ messages and KPA with $2^{\frac{5n}{4}}$ messages Here, the output is given by $[S, T]$ with $S = X^1 = P \oplus f_1(Q)$ and $T = X^2 = Q \oplus f_2(P \oplus f_1(Q))$ where $f_1, f_2 \in_R F_n$. Remind that $P = A_1{\cdot}L \oplus A_2{\cdot}R \oplus C_1$, and $Q = A_3{\cdot}L \oplus A_4{\cdot}R \oplus C_2$.

We first mount a CPA-1 with $2^{\frac{n}{2}}$ messages. We take only 2 distinct values for L: L_1 and L_2. Then, we choose m messages of the form $[L_1, R_i], [L_2, R_i]$, $1 \le i \le \frac{m}{2}$. We count the number $\mathcal{N}$ of (R_i, R_j) values, $R_i \neq R_j$ such that with the 4 following messages, $i : [L_1, R_i],\quad i' : [L_2, R_i] \quad j : [L_1, R_j], \quad j' : [L_2, R_j]$, we have $S_i \oplus S_j \oplus S_{i'} \oplus S_{j'} = 0$. The number of such 4-tuples is about $\frac{m^2}{4}$. Indeed, there are $\frac{m}{2}$ possibilities for R_i and $\left(\frac{m}{2} - 1\right)$ possibilities for R_j. Then the other inputs are fixed. This shows that $\mathcal{N}_{perm} \simeq \frac{m^2}{4\cdot 2^n}$.

We now explain the computation of the mean value for an A-Feistel scheme. We will use the following proposition whose proof is straightforward.

Proposition 1 *Let i, j, k, ℓ be four distinct indices. Suppose that $L_i = L_j$, $L_k = L_\ell \neq L_i$, $R_i = R_k$ and $R_j = R_\ell \neq R_i$ and we apply φ. Then we have the following properties:*

- *$Q_i = Q_j \Leftrightarrow A_4(R_i \oplus R_j) = 0$. Thus if A_4 is invertible, this condition will never be satisfied since $R_i \neq R_j$. If A_4 is not invertible, then the probability to have* (2) *is greater than $\frac{1}{2^n}$. Indeed, it is easy to check that if* $\dim \ker(A_4) = t$ *then the probability that $R_i \oplus R_j \in \ker(A_4) = \frac{2^t}{2^n} = \frac{1}{2^{n-t}} \geq \frac{1}{2^n}$.*

- *$Q_i = Q_k \Leftrightarrow A_3(L_i \oplus L_k) = 0$. Thus if A_3 is invertible, this condition will never be satisfied since $L_i \neq L_k$. Again, if A_3 is not invertible the probability to have* (3) *is greater than $\frac{1}{2^n}$.*
- *Condition* (4) *is not related to conditions on the dimension of the kernels of either A_3 or A_4. Thus, this condition is satisfied with probability about $\frac{1}{2^n}$.*

We suppose that A_3 and A_4 are invertible. The other cases are quite similar. The conditions on the inputs imply that:

$$P_i \oplus P_j \oplus P_{i'} \oplus P_{j'} = 0 \text{ and } Q_i \oplus Q_j \oplus Q_{i'} \oplus Q_{j'} = 0 \tag{1}$$

Thus we get $S_i \oplus S_j \oplus S_{i'} \oplus S_{j'} = f_1(Q_i) \oplus f_1(Q_j) \oplus f_1(Q_{i'}) \oplus f_1(Q_{j'})$. The equality (1) implies the following equivalences:

$$Q_i = Q_j \Leftrightarrow Q_{i'} = Q_{j'} \tag{2}$$
$$Q_i = Q_{i'} \Leftrightarrow Q_j = Q_{j'} \tag{3}$$
$$Q_i = Q_{j'} \Leftrightarrow Q_{i'} = Q_j \tag{4}$$

Thus if we have $Q_i = Q_j$ or $Q_i = Q_{i'}$, or $Q_i = Q_{j'}$, we will obtain $S_i \oplus S_j \oplus S_{i'} \oplus S_{j'} = 0$. To obtain $S_i \oplus S_j \oplus S_{i'} \oplus S_{j'} = 0$, we have to possibilities:

1. $Q_i = Q_{j'} \Leftrightarrow Q_{i'} = Q_j$
2. $Q_i \neq Q_{j'} \Leftrightarrow Q_{i'} \neq Q_j$ and $S_i \oplus S_j \oplus S_{i'} \oplus S_{j'} = 0$.

Then we obtain:

$$\mathbb{P}(S_i \oplus S_j \oplus S_{i'} \oplus S_{j'} = 0) = \mathbb{P}(S_i \oplus S_j \oplus S_{i'} \oplus S_{j'} = 0/Q_i = Q_{j'})\mathbb{P}(Q_i = Q_{j'})$$
$$+\mathbb{P}(S_i \oplus S_j \oplus S_{i'} \oplus S_{j'} 0/Q_i \neq Q_{j'})\mathbb{P}(Q_i \neq Q_{j'})$$

This shows that $\mathcal{N}_{scheme} \simeq \frac{m^2}{4}\left(\frac{1}{2^n} + \frac{1}{2^n}\left(1 - \frac{1}{2^n}\right)\right)$. Thus $\mathcal{N}_{scheme} \simeq \frac{m^2}{4}\left(\frac{2}{2^n} - \frac{1}{2^{2n}}\right)$ and $\mathcal{N}_{scheme} \simeq \mathcal{N}_{perm}$. Then we will be able to distinguish when the probability to have $\mathcal{N}_{perm} \geq 1$ is non-negligible, i.e. when $m \geq 2^{\frac{n}{2}}$. Remark that we can also try another $[L_1, L_2]$; for each $[L_1, L_2]$ the probability of success of this attack is non-negligible. We have obtain a CPA-1 with $m \simeq 2^{\frac{n}{2}}$ messages.

Remark 2 We can explain this computation as follows: we consider that the condition $S_i \oplus S_j \oplus S_{i'} \oplus S_{j'} = 0$ appears at random or due to equalities that are satisfied by internal variables. In the sequel, we will not perform all the computations but the ideas are the same.

Remark 3 In [13], it is proved that for $d = 2$, there is security against all adaptive chosen plaintext attacks (CPA-2) when the number of queries is $m \leq 2^{\frac{n}{2}}$. Since for $d = 2$, we have a CPA-1 with $2^{\frac{n}{2}}$ messages, the bound is tight. In their scheme, the authors use first a pairwise independent permutation and then a Feistel Scheme with 2 rounds. As said before, an affine permutation is an example of a pairwise independent permutation.

The previous attack can be transformed into a KPA with complexity $O(2^{\frac{5n}{4}})$: we count the number $\mathcal{N}$ of (i, j, k, ℓ) such that

$$\begin{cases} L_i = L_j \\ L_k = L_\ell \neq L_i \end{cases} \text{ and } \begin{cases} R_i = R_k \\ R_j = R_\ell \neq R_i \end{cases} \text{ and } S_i \oplus S_j \oplus S_k \oplus S_\ell = 0$$

Notice that there are $\binom{m}{4} \times \binom{4}{2}$ possibilities to obtain two distinct couples of pairs (i, j), (k, ℓ) with m indices. Thus, we have $\mathcal{N}_{perm} \simeq \frac{m^4}{4 \cdot 2^{5n}}$ and $\mathcal{N}_{scheme} \simeq \frac{m^4}{2 \cdot 2^{5n}}$ for an A-Feistel permutation. Therefore, this KPA succeeds when $m \geq 2^{\frac{5n}{4}}$.

$\varphi \circ \Psi(f_2) \circ \Psi(f_1)$: CPA-1 with $2^{\frac{n}{2}}$ messages and KPA with $2^{\frac{5n}{4}}$ messages Here, after one round the output is $[R, L \oplus f_1(R)]$. Let $X^1 = L \oplus f_1(R)$. After the second round of a Feistel scheme, the output is $[X^1, X^2]$ where $X^2 = R \oplus f_2(X^1)$. Then, after the affine permutation, we obtain $S = A_1 \cdot X^1 \oplus A_2 \cdot X^2 \oplus C_1$ and $T = A_3 \cdot X^1 \oplus A_4 \cdot X^2 \oplus C_2$.

We first describe a CPA-1 with $2^{\frac{n}{2}}$ messages. The inputs are chosen as in the previous attack, but since φ is at the end of the structure, the conditions on the outputs are: $S_i \oplus S_j \oplus S_{i'} \oplus S_{j'} = 0$ and $T_i \oplus T_j \oplus T_{i'} \oplus T_{j'} = 0$. With an A-Feistel scheme, the conditions on the inputs imply that $X^1_i \oplus X^1_{i'} \oplus X^1_j \oplus X^1_{j'} = 0$. If we impose for example $X^1_i = X^1_{j'}$, then we will obtain $X^2_i \oplus X^2_{i'} \oplus X^2_j \oplus X^2_{j'} = 0$ and the conditions on the outputs will be satisfied. The probability to have $X^1_i = X^1_{j'}$ is about $\frac{1}{2^n}$. Notice that the conditions on the outputs may also happen at random and in that case the probability is about $\frac{1}{2^{2n}}$. Thus $\mathcal{N}_{scheme} \simeq \frac{m^2}{4 \cdot 2^n} + O(\frac{m^2}{2^{2n}})$. For a random permutation, the probability to get $S_i \oplus S_j \oplus S_{i'} \oplus S_{j'} = 0$ and $T_i \oplus T_j \oplus T_{i'} \oplus T_{j'} = 0$ is about $\frac{1}{2^{2n}}$ and we have $\mathcal{N}_{perm} \simeq \frac{m^2}{4 \cdot 2^{2n}}$. Thus with $m \simeq 2^{\frac{n}{2}}$ messages, the attack succeeds and we can distinguish an A-Feistel scheme from a random permutation.

As usual, this CPA-1 can be transformed into a KPA with $2^{\frac{5n}{4}}$ messages.

$\Psi(f_2) \circ \varphi \circ \Psi(f_1)$: CPA-1 with 4 messages and KPA with $2^{\frac{n}{2}}$ messages Let as usual $[L, R]$ denote the input. Then we have: $S = Q = A_3 \cdot R \oplus A_4(L \oplus f_1(R)) \oplus C_2$ and $T = P \oplus f_2(Q)$ with $P = A_1 \cdot R \oplus A_2(L \oplus f_1(R)) \oplus C_1$.

We have the following CPA-1 with 4 messages. We choose 4 messages $[L_1, R_1]$, $[L_1, R_2]$, $[L_2, R_1]$, $[L_2, R_2]$ such that $L_1 \neq L_2$ and $R_1 \neq R_2$. Then again we check if $S_1 \oplus S'_1 \oplus S_2 \oplus S'_2 = Q_1 \oplus Q'_1 \oplus Q_2 \oplus Q'_2 = 0$.

Again, this CPA-1 can be transformed into a KPA with $2^{\frac{n}{2}}$ messages.

3.4 One affine permutation and a Feistel scheme with three rounds

$\Psi(f_3) \circ \Psi(f_2) \circ \Psi(f_1) \circ \varphi$: KPA with $2^{\frac{7n}{4}}$ messages and CPA-1 with $2^{\frac{3n}{2}}$ messages We have the following values: $[L, R] \longrightarrow [P, Q] \longrightarrow [Q, X^1] \longrightarrow [X^1, X^2] \longrightarrow [S, T]$. Here,the output is given by $[S, T]$ with $S = X^2 = Q \oplus f_2(X^1)$ and $T = X^3 = X^1 \oplus f_3(X^2)$ where $f_1, f_2, f_3 \in_R F_n$. Remind that $P = A_1 \cdot L \oplus A_2 \cdot R \oplus C_1$, $Q = A_3 \cdot L \oplus A_4 \cdot R \oplus C_2$ and $X^1 = P \oplus f_1(Q)$.

We begin with a KPA. We want count the number $\mathcal{N}$ of (i, j, k, ℓ) such that

$$\begin{cases} L_i = L_j \\ L_k = L_\ell \neq L_i \end{cases} \text{ and } \begin{cases} R_i = R_k \\ R_j = R_\ell \neq R_i \end{cases} \text{ and } S_i \oplus S_j \oplus S_k \oplus S_\ell = 0$$

When we have a random permutation, the computations have been done with the computer program as explained in Section 2 and we have obtained $\mathbb{E}(\mathcal{N}_{perm}) \simeq \frac{m^4}{4 \cdot 2^{5n}}$, $\sigma(\mathcal{N}_{perm}) = O\left(\frac{m^2}{2^{\frac{5n}{2}}}\right)$. With an A-Feistel scheme, these equalities may happen at random or because there are some conditions which can be satisfied by internal variables. For example, we may have the following conditions:

$$\begin{cases} L_i = L_j \\ L_k = L_\ell \neq L_i \end{cases} \text{and} \begin{cases} R_i = R_k \\ R_j = R_\ell \neq R_i \end{cases} \text{and} \begin{cases} Q_i = Q_\ell \\ X_i^1 = X_j^1 \end{cases}$$

Here we have condition (4) on the Q_i values. There are no conditions on the kernels. But we could also impose the other conditions since A_3 and A_4 are not invertible with a non-negligible probability. Moreover, when we have $Q_i = Q_\ell$, it is also possible to have $X_i^1 = X_k^1$. We may also have no condition on the Q_i values and 2 conditions on the X_i^1 values (for example $X_i^1 = X_j^1$ and $X_k^1 = X_\ell^1$). Thus, using the computations performed in Section 5, we get $\mathbb{E}(\mathcal{N}_{scheme}) \simeq \frac{m^4}{4.2^{5n}} + \alpha \frac{m^4}{2^{6n}}$, where α depends on the properties of the kernels of A_3 and A_4 ($2 \leq \alpha \leq 9$). We note here $\mathbb{E}(\mathcal{N}_{scheme}) \simeq \frac{m^4}{4.2^{5n}} + O\left(\frac{m^4}{2^{6n}}\right)$. As computed in Section 5, again $\sigma(\mathcal{N}_{scheme}) = O\left(\frac{m^2}{2^{\frac{5n}{2}}}\right)$. We can distinguish as soon as the difference of the mean values is greater than both standard deviations, i.e. $\frac{m^4}{2^{6n}} \geq \frac{m^2}{2^{\frac{5n}{2}}}$. This means we must have $m \simeq 2^{\frac{7n}{4}}$.

Then we transform the previous KPA into a CPA-1 as follows. We choose all the possible $[L, R]$ such that the first $\frac{n}{2}$ bits of L are equal to 0. Therefore we have $2^{\frac{n}{2}} \cdot 2^n = 2^{\frac{3n}{2}}$ possible inputs. We keep the same input and output conditions. Here $\mathbb{E}(\mathcal{N}_{perm}) \simeq \frac{m^4}{4.2^{4n}}$ and $\sigma(\mathcal{N}_{perm}) = O(\frac{m^2}{2^{2n}})$ since each collision on L has probability about $\frac{1}{2^{n/2}}$. The computation of the variance is similar to the computation done for the KPA. For an A-Feistel scheme, we get $\mathbb{E}(\mathcal{N}_{scheme}) \simeq \frac{m^4}{4 \cdot 2^{4n}} + \alpha \frac{m^4}{4 \cdot 2^{5n}}$ and $\sigma(\mathcal{N}_{scheme}) = O\left(\frac{m^2}{2^{2n}}\right)$. This shows that we can distinguish a random permutation from an A-Feistel permutation as soon as $\frac{m^4}{2^{5n}} \geq \frac{m^2}{2^{2n}}$. This gives a CPA-1 with $2^{\frac{3n}{2}}$ messages.

Computer simulations We have made computer simulations for this attack in the following way: for all values (or almost all values) of L, and all values of R, we compute S, T. Then for all i, j such that $L_i = L_j$ and $R_i < R_j$, we add to a list the 3-tuple $(S_i \oplus S_j, R_i, R_j)$. Finally we count how many collisions we have in this list. These simulations confirm our theoretical results (see Table 1). Here $\bar{\mathcal{N}}$ stands for the expectation for either a random permutation, or a $\Psi^3 \circ \varphi$ permutation.

Table 1 Simulation results

n	4	6	8
Number of tries	100000	10000	10000
Random cipher	$\bar{\mathcal{N}} = 899.9$	$\bar{\mathcal{N}} = 15624$	$\bar{\mathcal{N}} = 257042$
	$V = 848.5$	$V = 15481$	$V = 259744$
$\Psi^3 \circ \varphi$	$\bar{\mathcal{N}} = 972$	$\bar{\mathcal{N}} = 15717$	$\bar{\mathcal{N}} = 257146$
	$V = 3436$	$V = 19717$	$V = 264051$
(% good distinction) – (% false alarm)	+77.4%	+38.5%	+10.9%

$\varphi \circ \Psi(f_3) \circ \Psi(f_2) \circ \Psi(f_1)$: CPA-1 with 2^n messages and KPA with $2^{\frac{3n}{2}}$ messages We have the following values: $[L, R] \longrightarrow [R, X^1] \longrightarrow [X^1, X^2] \longrightarrow [X^2, X^3] \longrightarrow [S, T]$ with $X^1 = L \oplus f_1(R), X^2 = R \oplus f_2(X^1), X^3 = X^1 \oplus f_3(X^2), S = A_1{\cdot}X^2 \oplus A_2{\cdot}X^3 \oplus C_1$ and $T = A_3{\cdot}X^2 \oplus A_4{\cdot}X^3 \oplus C_2$. Let us describe a CPA-1 with 2^n messages. We take only 2 distinct values for L: L_1 and L_2. Then, we choose m messages of the form $[L_1, R_i], [L_2, R_i]$, $1 \leq i \leq \frac{m}{2}$. We count the number $\mathcal{N}$ of (R_i, R_j) values, $R_i \neq R_j$ such that with the 4 following messages, i : $[L_1, R_i]$, i' : $[L_2, R_i]$ j : $[L_1, R_j]$, j' : $[L_2, R_j]$, we have $S_i \oplus S_j \oplus S_{i'} \oplus S_{j'} = 0$ and $T_i \oplus T_j \oplus T_{i'} \oplus T_{j'} = 0$.

When we have an A-Feistel scheme, these two equalities may happen at random with probability about $\frac{1}{2^{2n}}$. But we may also have equalities on the internal variables that will imply the equalities on the outputs.

The conditions on the inputs imply that $X^1_i \oplus X^1_{i'} \oplus X^1_j \oplus X^1_{j'} = 0$. Moreover, some equalities between the X^1 values may be satisfied. For example, we may have $X^1_i = X^1_j \Leftrightarrow X^1_{i'} = X^1_{j'}$ or $X^1_i = X^1_{j'} \Leftrightarrow X^1_{i'} = X^1_j$ but we cannot have $X^1_i = X^1_{i'} \Leftrightarrow X^1_j = X^1_{j'}$ because this will imply $L_1 = L_2$. Suppose that we have $X^1_i = X^1_{j'} \Leftrightarrow X^1_{i'} = X^1_j$, which happens with probability about $\frac{1}{2^n}$. Then we get $X^2_i \oplus X^2_{i'} \oplus X^2_j \oplus X^2_{j'} = 0$. Again, some equalities on the X^2 values will imply $X^3_i \oplus X^3_{i'} \oplus X^3_j \oplus X^3_{j'} = 0$ and then the properties of the affine permutation will give the required conditions on the outputs.

We explain now the conditions on X^2. Suppose that we have $X^1_i = X^1_{j'} \Leftrightarrow X^1_{i'} = X^1_j$. Then it is possible to impose $X^2_i = X^2_j \Leftrightarrow X^2_{i'} = X^1_{j'}$ for example and again the probability that this condition is satisfied is about $\frac{1}{2^n}$. Notice that we cannot impose $X^2_i = X^2_{j'}$ since this will imply $R_i = R_j$. With a random permutation, the conditions on the outputs will only appear at random.

Thus we get $\mathcal{N}_{perm} \simeq \frac{m^2}{4 \cdot 2^{2n}}$ and $\mathcal{N}_{scheme} \simeq \frac{m^2}{2 \cdot 2^{2n}}$. This shows that when $m \simeq 2^n$ we can distinguish a random permutation from a permutation produced by an A-Feistel scheme.

This CPA-1 can be transformed into a KPA with $2^{\frac{3n}{2}}$ messages.

$\Psi(f_3) \circ \Psi(f_2) \circ \varphi \circ \Psi(f_1)$ or $\Psi(f_3) \circ \varphi \circ \Psi(f_2) \circ \Psi(f_1)$: CPA-1 with $2^{\frac{n}{2}}$ messages and KPA with $2^{\frac{5n}{4}}$ messages The attack is similar to the previous one, except that the conditions on the output is $S_i \oplus S_j \oplus S_k \oplus S_\ell = 0$. We obtain $\mathbb{E}(\mathcal{N}_{perm}) \simeq \frac{m^2}{4 \cdot 2^n}$ and $\mathbb{E}(\mathcal{N}_{scheme}) \simeq \frac{m^2}{2 \cdot 2^n}$. Thus when $m \simeq 2^{\frac{n}{2}}$, we can distinguish a random permutation from a permutation generated by an A-Feistel scheme. This CPA-1 can be transformed easily into a KPA with $2^{\frac{5n}{4}}$ messages.

3.5 One affine permutation and a Feistel scheme with four rounds

$\Psi(f_4) \circ \Psi(f_3) \circ \Psi(f_2) \circ \Psi(f_1) \circ \varphi$: attacks on generators of permutations Here we are going to attack generators of permutations and not only a single permutation. Thus we want to distinguish a generator of random permutations from a generator of A-Feistel permutations. We suppose that we have μ permutations. The values are given by: $[L, R] \longrightarrow [P, Q] \longrightarrow [Q, X^1] \longrightarrow [X^1, X^2] \longrightarrow [X^2, X^3] \longrightarrow [S, T]$. After round 4, the output is given by $[S, T]$ where $S = X^3$ and $T = X^4 = X^2 \oplus f_4(X^3)$. Remind that $P = A_1{\cdot}L \oplus A_2{\cdot}R \oplus C_1$, $Q = A_3{\cdot}L \oplus A_4{\cdot}R \oplus C_2$, $X^1 = P \oplus f_1(Q)$, $X^2 = Q \oplus f_2(X^1)$ and $X^3 = X^1 \oplus f_3(X^2)$. Again, we want to count the number $\mathcal{N}$ of (i, j, k, ℓ) such that

$$\begin{cases} L_i = L_j \\ L_k = L_\ell \neq L_i \end{cases} \text{and} \begin{cases} R_i = R_k \\ R_j = R_\ell \neq R_i \end{cases} \text{and } S_i \oplus S_j \oplus S_k \oplus S_\ell = 0$$

When we have μ random permutations, $\mathbb{E}(\mathcal{N}_{perm}) \simeq \mu\frac{m^4}{4\cdot 2^{5n}}$ and $\sigma(\mathcal{N}_{perm}) = O\left(\sqrt{\mu}\frac{m^2}{2^{\frac{5n}{2}}}\right)$. With an A-Feistel scheme, these equalities may happen at random or because there are some conditions which can be satisfied by internal variables. For example, we may have (other conditions are possible):

$$\begin{cases} L_i = L_j \\ L_k = L_\ell \neq L_i \end{cases} \text{and} \begin{cases} R_i = R_k \\ R_j = R_\ell \neq R_i \end{cases} \text{and} \begin{cases} Q_i = Q_\ell \\ X_i^1 = X_j^1 \\ X_i^2 = X_k^2 \end{cases}$$

For μ permutations produced be an A-Feistel scheme, we obtain $\mathbb{E}(\mathcal{N}_{scheme}) \simeq \mu\frac{m^4}{2^{5n}} + O\left(\mu\frac{m^4}{2^{7n}}\right)$ and $\sigma(\mathcal{N}_{scheme}) = O\left(\sqrt{\mu}\frac{m^2}{2^{\frac{5n}{2}}}\right)$. We can distinguish when $\mu\frac{m^4}{2^{7n}} \geq \sqrt{\mu}\frac{m^2}{2^{\frac{5n}{2}}}$. If we take the maximum number of messages (i.e. 2^{2n}), we obtain $\mu = 2^n$ and the number of needed computations is given by $\lambda = \mu \cdot 2^{2n} = 2^{3n}$.

Remark 4 It is not possible to have the same kind of conditions on successive variables. For example, we choose $Q_i = Q_\ell$ and then we have to change. If we impose again $X_i^1 = X_\ell^1$, then this will imply $P_i = P_\ell$ and we obtain a contradiction since we have permutations and $[L_i, R_i] \neq [L_\ell, R_\ell]$.

$\varphi \circ \Psi(f_4) \circ \Psi(f_3) \circ \Psi(f_2) \circ \Psi(f_1)$: KPA with 2^{2n} messages We have the following values:

$$[L, R] \longrightarrow [R, X^1] \longrightarrow [X^1, X^2] \longrightarrow [X^2, X^3] \longrightarrow [X^3, X^4] \longrightarrow [S, T]$$

with $X^1 = L \oplus f_1(R)$, $X^2 = R \oplus f_2(X^1)$, $X^3 = X^1 \oplus f_3(X^2)$, $X^4 = X^2 \oplus f_4(X^3)$, $S = A_1.X^3 \oplus A_2.X^4 \oplus C_1$ and $S = A_3{\cdot}X^3 \oplus A_4{\cdot}X^4 \oplus C_2$. We give here an attack which needs the maximal number of messages, i.e. 2^{2n}. We count the number $\mathcal{N}$ of (i, j, k, ℓ) such that

$$\begin{cases} L_i = L_j \\ L_k = L_\ell \neq L_i \end{cases} \text{and} \begin{cases} R_i = R_k \\ R_j = R_\ell \neq R_i \end{cases} \text{and} \begin{cases} S_i \oplus S_j \oplus S_k \oplus S_\ell = 0 \\ T_i \oplus T_j \oplus T_k \oplus T_\ell = 0 \end{cases}$$

Here we have $\mathbb{E}(\mathcal{N}_{perm}) \simeq \frac{m^4}{4\cdot 2^{6n}}$, $\sigma(\mathcal{N}_{perm}) = O\left(\frac{m^2}{2^{3n}}\right)$ and $\mathbb{E}(\mathcal{N}_{scheme}) \simeq \frac{m^4}{4\cdot 2^{6n}} + O\left(\frac{m^4}{2^{7n}}\right)$ and $\sigma(\mathcal{N}_{scheme}) = O\left(\frac{m^2}{2^{3n}}\right)$. We can distinguish when $\frac{m^4}{2^{7n}} \geq \frac{m^2}{2^{3n}}$. Thus the attack succeeds when $m \simeq 2^{2n}$.

$\Psi(f_4) \circ \Psi(f_3) \circ \Psi(f_2) \circ \varphi \circ \Psi(f_1)$ or $\Psi(f_4) \circ \Psi(f_3) \circ \varphi \circ \Psi(f_2) \circ \Psi(f_1)$ or $\Psi(f_4) \circ \varphi \circ \Psi(f_3) \circ \Psi(f_2) \circ \Psi(f_1)$: KPA with $2^{\frac{7n}{4}}$ messages and CPA-1 with $2^{\frac{3n}{2}}$ messages We only give the sketch of the attacks for $\Psi(f_4) \circ \Psi(f_3) \circ \Psi(f_2) \circ \varphi \circ \Psi(f_1)$. The other cases are quite similar. We can mount a KPA with $2^{\frac{7n}{4}}$ messages as follows. We count the number $\mathcal{N}$ of (i, j, k, ℓ) such that

$$\begin{cases} L_i = L_j \\ L_k = L_\ell \neq L_i \end{cases} \text{and} \begin{cases} R_i = R_k \\ R_j = R_\ell \neq R_i \end{cases} \text{and } S_i \oplus S_j \oplus S_k \oplus S_\ell = 0$$

When we have a random permutation, we obtain from the computer program, that $\mathbb{E}(\mathcal{N}_{perm}) \simeq \frac{m^4}{4\cdot 2^{5n}}$ and $\sigma(\mathcal{N}_{perm}) = O\left(\frac{m^2}{2^{\frac{5n}{2}}}\right)$. With an A-Feistel scheme, these equalitites may happen at random or because there are some conditions which can be satisfied by internal variables. For example, we may have the following conditions:

$$\begin{cases} L_i = L_j \\ L_k = L_\ell \neq L_i \end{cases} \text{ and } \begin{cases} R_i = R_k \\ R_j = R_\ell \neq R_i \end{cases} \text{ and } \begin{cases} Q_i = Q_\ell \\ X_i^2 = X_j^2 \end{cases}$$

Thus, using the computations similar to those performed in Section 5, we get we get $\mathbb{E}(\mathcal{N}_{scheme}) \simeq \frac{m^4}{4 \cdot 2^{5n}} + O\left(\frac{m^4}{2^{6n}}\right)$ and $\sigma(\mathcal{N}_{scheme}) = O\left(\frac{m^2}{2^{\frac{5n}{2}}}\right)$. We can distinguish an soon as the difference of the mean values is greater than both standard deviations, i.e. $\frac{m^4}{2^{6n}} \geq \frac{m^2}{2^{\frac{5n}{2}}}$. This means we must have $m \simeq 2^{\frac{7n}{4}}$. We now transform this KPA into a CPA-1. We choose all the possible $[L, R]$ such that the first $\frac{n}{2}$ bits of L are equal to 0. Therefore we have $2^{\frac{n}{2}} \cdot 2^n = 2^{\frac{3n}{2}}$ possible inputs. We keep the same input and output conditions. Here $\mathbb{E}(\mathcal{N}_{perm}) \simeq \frac{m^4}{4 \cdot 2^{4n}}$ and $\sigma(\mathcal{N}_{perm}) = O\left(\frac{m^2}{2^{2n}}\right)$ since each collision on L has probability about $\frac{1}{2^{n/2}}$. The computation of the variance is similar to the computation done for the KPA. For an A-Feistel scheme, we get $\mathbb{E}(\mathcal{N}_{scheme}) \simeq \frac{m^4}{4 \cdot 2^{4n}} + O\left(\frac{m^4}{4 \cdot 2^{5n}}\right)$ and $\sigma(\mathcal{N}_{scheme}) = O\left(\frac{m^2}{2^{2n}}\right)$. This shows that we can distinguish a random permutation from an A-Feistel permutation as soon as $\frac{m^4}{2^{5n}} \geq \frac{m^2}{2^{2n}}$. This gives a CPA-1 with $2^{\frac{3n}{2}}$ messages.

3.6 Complexities of attacks on A-Feistel with one affine permutation

For the following rounds, we always have to add one more condition on the internal variables and we perform the same computations. We need to alternate the conditions on the indices. For $d \geq 5$, the features of the attacks are summarized in Table 2.

The we have the following property:

$$Complexity(\Psi^d \circ \varphi) = 2^n Complexity(\varphi \circ \Psi^d) = 2^{2n} Complexity(\Psi^{d_2} \circ \varphi \circ \Psi^{d_1})$$

This comes from the fact that we have one more condition on the output of $\varphi \circ \Psi^d$ compared with the output of $\Psi^d \circ \varphi$ and that there is one more internal condition on $\Psi^d \circ \varphi$ compared with $\Psi^{d_2} \circ \varphi \circ \Psi^{d_1}$.

The complexities of our attacks are summarized in Table 3 (A-Feistel). We also mention the results for classical Feistel schemes Ψ^d [14]. As said before we only give the results

Table 2 Attacks for $d \geq 5$ with μ permutations

Scheme	Conditions	Expectation	μ	Complexity
$\Psi^d \circ \varphi$	4 conditions on the inputs 1 condition on the ouptut $d-1$ internal conditions	$\mu \frac{m^4}{4 \cdot 2^{5n}}$ $+O\left(\mu \frac{m^4}{2^{(d+3)n}}\right)$	$2^{(2d-7)n}$	$2^{(2d-5)n}$
$\Psi^{d_2} \circ \varphi \circ \Psi^{d_1}$ $d_1 + d_2 = d$	4 conditions on the inputs 1 condition on the ouptut $d-2$ internal conditions	$\mu \frac{m^4}{4 \cdot 2^{5n}}$ $+O\left(\mu \frac{m^4}{2^{(d+2)n}}\right)$	$2^{(2d-9)n}$	$2^{(2d-7)n}$
$\varphi \circ \Psi^d$	4 conditions on the inputs 2 conditions on the ouptut $d-1$ internal conditions	$\mu \frac{m^4}{4 \cdot 2^{6n}}$ $+O\left(\mu \frac{m^4}{2^{(d+3)n}}\right)$	$2^{(2d-8)n}$	$2^{(2d-6)n}$

Table 3 Complexities of attacks on A-Feistel with one affine permutation and on classical Feistel schemes Ψ^d

Ψ^d [14]		
d (round)	KPA	CPA-1
Ψ^1	1	1
Ψ^2	$2^{\frac{n}{2}}$	2
Ψ^3	$2^{\frac{n}{2}}$	$2^{\frac{n}{2}}$
Ψ^4	2^n	$2^{\frac{n}{2}}$
Ψ_2^5	$2^{\frac{3n}{2}}$	2^n
Ψ_2^6	2^{2n}	2^{2n}
$\Psi^d, d \geq 6$	$2^{(k-4)n}$	$2^{(k-4)n}$

	A-Feistel	
Structure	KPA	CPA-1
$\Psi^1 \circ \varphi$ $\varphi \circ \Psi^1$	$2^{\frac{n}{2}}$ $(n+1)2^{\frac{n}{2}}$	4 4
$\Psi^2 \circ \varphi$ $\Psi^1 \circ \varphi \circ \Psi^1$ $\varphi \circ \Psi^2$	$2^{\frac{5n}{4}}$ $2^{\frac{n}{2}}$ $2^{\frac{5n}{4}}$	$2^{\frac{n}{2}}$ 4 $2^{\frac{n}{2}}$
$\Psi^3 \circ \varphi$ $\Psi^2 \circ \varphi \circ \Psi^1$ $\Psi^1 \circ \varphi \circ \Psi^2$ $\varphi \circ \Psi^3$	$2^{\frac{7n}{4}}$ $2^{\frac{5n}{4}}$ $2^{\frac{5n}{4}}$ $2^{\frac{3n}{2}}$	$2^{\frac{3n}{2}}$ $2^{\frac{n}{2}}$ $2^{\frac{n}{2}}$ 2^n
$\Psi^4 \circ \varphi$ $\Psi^{d_2} \circ \varphi \circ \Psi^{d_1},\ d_1 + d_2 = 4$ $\varphi \circ \Psi^4$	2^{3n} $2^{\frac{7n}{4}}$ 2^{2n}	2^{3n} $2^{\frac{3n}{2}}$ 2^{2n}
$\Psi^5 \circ \varphi$ $\Psi^{d_2} \circ \varphi \circ \Psi^{d_1},\ d_1 + d_2 = 5$ $\varphi \circ \Psi^5$	2^{5n} 2^{3n} 2^{4n}	
$\Psi^d \circ \varphi\ , d \geq 5$ $\Psi^{d_2} \circ \varphi \circ \Psi^{d_1},\ d_1 + d_2 = d$ $\varphi \circ \Psi^d$	$2^{(2d-5)n}$ $2^{(2d-7)n}$ $2^{(2d-6)n}$	

for KPA and CPA-1. By symmetry, we obtain the corresponding complexities of a KCA and CCA-1: for example the complexity of KPA on $\Psi^3 \circ \varphi$ is the complexity of a KCA on $\varphi \circ \Psi^3$ and so on. For $d \geq 5$, we attack generators of permutations and not only a single permutation. Notice that for the same d, the scheme is stronger when the affine permutation is used as the first round. This comes from the fact that an affine permutation mixes the branches better than a Feistel scheme with one round.

4 A-Feistel schemes with two affine permutations

This Section is devoted to attacks on schemes for which we have first an affine permutation, then a Feistel scheme with several rounds, and finally an affine permutation. The attacks are very similar to the ones in Section 3. We will give an example and provide the general results. We explain a CPA-1 and a KPA when we apply first an affine function φ, then a Feistel scheme with 2 rounds and we finish with an affine permutation φ'. We have the following values: $[L, R] \longrightarrow [P, Q] \longrightarrow [Q, X^1] \longrightarrow [X^1, X^2] \longrightarrow [S, T]$, with $P = A_1{\cdot}L \oplus A_2{\cdot}R \oplus C_1$, $Q = A_3{\cdot}L \oplus A_4{\cdot}R \oplus C_2$, $X^1 = P \oplus f_1(Q)$, $X^2 = Q \oplus f_2(X^1)$, $S = A'_1{\cdot}X^1 \oplus A'_2{\cdot}X^2 \oplus C'_1$, $T = A'_3{\cdot}X^1 \oplus A'_4{\cdot}X^2 \oplus C'_2$. For the CPA-1, we take only 2 distinct values for L: L_1 and L_2. Then, we choose m messages of the form $[L_1, R_i], [L_2, R_i]$, $1 \leq i \leq \frac{m}{2}$. We count the number $\mathcal{N}$ of (R_i, R_j) values, $R_i \neq R_j$ such that with the 4 following messages, $i\ :\ [L_1, R_i],\quad i'\ :\ [L_2, R_i]\quad j\ :\ [L_1, R_j],\quad j'\ :\ [L_2, R_j]$, we have $S_i \oplus S_j \oplus S_{i'} \oplus S_{j'} = 0$ and $T_i \oplus T_j \oplus T_{i'} \oplus T_{j'} = 0$. Then, we obtain: $\mathbb{E}(\mathcal{N}_{perm}) \simeq \frac{m^2}{4{\cdot}2^{2n}}$

and $\mathbb{E}(\mathcal{N}_{scheme}) \simeq \frac{m^2}{2\cdot 2^{2n}}$. This shows that it is possible to distinguish a random permutation from a permutation produced by an A-Feistel scheme with 2 affine permutations when $m \simeq 2^n$. As usual, this CPA-1 can be transformed into a KPA with $m \simeq 2^{\frac{3n}{2}}$. The results of our attacks (CPA-1 and KPA) are given in Table 4. By symmetry, we also get the results for KCA and CCA-1. For $d \geq 4$, we give the complexity of the attacks on generators of permutations and on a single permutation.

Remark 5 Another possibility would be to alternate affine permutation and Feistel scheme with one round. This does not secure the scheme. Indeed, the diffusion is too slow. For example, we get the same complexities for $\Psi^3 \circ \varphi$ and $\Psi^1 \circ \varphi \circ \Psi^1 \circ \varphi \circ \Psi^1 \circ \varphi$. We have the same complexities for $\varphi' \circ \Psi^2 \circ \varphi$ and $\varphi \circ \Psi^1 \circ \varphi \circ \Psi^1 \circ \varphi$ as well.

5 Computation of the mean value and the variance for a $\Psi^3 \circ \varphi$ permutation

Here we compute the mean value and the standard deviation for a $\Psi^3 \circ \varphi$ permutation. With an A-Feistel scheme, the equalities that we want to be satisfied may happen at random or because there are some conditions which are verified by the internal variables. We consider a KPA such that:

$$\begin{cases} L_i = L_j \\ L_k = L_\ell \neq L_i \end{cases} \text{and} \begin{cases} R_i = R_k \\ R_j = R_\ell \neq R_i \end{cases} \text{and } S_i \oplus S_j \oplus S_k \oplus S_\ell = 0$$

Let $\delta_{ijk\ell}$ be the Bernoulli variable that is equal to 1 when the above conditions are satisfied and 0 otherwise. Then by using the symmetries of the conditions, we have: $\mathcal{N}_{scheme} = \frac{m(m-1)(m-2)(m-3)}{4}\delta_{ijk\ell}$.

5.1 Computation of the mean value

Here we have $S_i \oplus S_j \oplus S_k \oplus S_\ell = Q_i \oplus Q_j \oplus Q_k \oplus Q_\ell \oplus f_2(X_i^1) \oplus f_2(X_j^1) \oplus f_2(X_k^1) \oplus f_2(X_\ell^1)$. Since $Q_i \oplus Q_j \oplus Q_k \oplus Q_\ell = 0$ (by the conditions on the input variables), we get $S_i \oplus S_j \oplus S_k \oplus S_\ell = 0 \Leftrightarrow f_2(X_i^1) \oplus f_2(X_j^1) \oplus f_2(X_k^1) \oplus f_2(X_\ell^1) = 0$ $(*)$. Thus this may happen at random, or due to conditions satisfied by internal variables.

A_3 and A_4 are invertible As stated in Proposition 1, the conditions that may appear on the internal variables depend on the properties of the kernels of A_3 and A_4. Here we suppose that A_3 and A_4 are invertible. We want to have $f_2\left(X_i^1\right) \oplus f_2\left(X_j^1\right) \oplus f_2\left(X_k^1\right) \oplus f_2\left(X_\ell^1\right) = 0$. In our attacks, we use the difference between the mean value obtained when we have a random permutation and the one obtained with a scheme. Thus we will compute the first

Table 4 Complexities of attacks on A-Feistel with two affine permutations

Structure	KPA	CPA-1
$\varphi' \circ \Psi^1 \circ \varphi$	$2^{\frac{5n}{4}}$	$2^{\frac{n}{2}}$
$\varphi' \circ \Psi^2 \circ \varphi$	$2^{\frac{3n}{2}}$	2^n
$\varphi' \circ \Psi^3 \circ \varphi$	2^{2n}	2^{2n}
$\varphi' \circ \Psi^d \circ \varphi,\ d \geq 4$	$2^{(2d-4)n}$	

terms of the mean value. We now look at the conditions on the internal variables that will imply $(*)$:

1. Equalities on the Q variables. Since A_3 and A_4 are invertible, the only possibility is $Q_i = Q_\ell \Leftrightarrow Q_j = Q_k$. This happens with probability $\frac{1}{2^n}$. This implies $X_i^1 \oplus X_j^1 \oplus X_k^1 \oplus X_\ell^1 = 0$. Then we may have $X_i^1 = X_j^1 \Leftrightarrow X_k^1 = X_\ell^1$. The probability is $\frac{1}{2^n}$. It is also possible to have $X_i^1 = X_k^1 \Leftrightarrow X_j^1 = X_\ell^1$ but it is not possible to have $X_i^1 = X_\ell^1$ since this implies $P_i = P_\ell$. Remember that $Q_i = Q_\ell$ and we have an affine permutation. Then we multiply by the probability of $Q_i = Q_\ell$. The probability in this case is $\frac{2}{2^{2n}}$.
2. We now suppose that $Q_i \neq Q_\ell \Leftrightarrow Q_j \neq Q_k$. We want to have $f_2\left(X_i^1\right) \oplus f_2\left(X_j^1\right) \oplus f_2\left(X_k^1\right) \oplus f_2\left(X_\ell^1\right) = 0$. Then we can get $(*)$ if we have $X_i^1 = X_j^1$ and $X_k^1 = X_\ell^1$ or $X_i^1 = X_k^1$ and $X_j^1 = X_\ell^1$ or $X_i^1 = X_\ell^1$ and $X_j^1 = X_k^1$. The probability in that case is given by $3 \times \left(1 - \frac{1}{2^n}\right) \times \frac{1}{2^{2n}}$.
3. We are not in the previous case and we have $(*)$. Here the probability is $\left(1 - \frac{2}{2^{2n}} - 3\left(1 - \frac{1}{2^n}\right)\frac{1}{2^{2n}}\right)\frac{1}{2^n} = \frac{1}{2^n} - \frac{5}{2^{3n}} + \frac{3}{2^{4n}}$.

Thus the probability to get $(*)$ is $\frac{1}{2^n} + \frac{5}{2^{2n}} - \frac{8}{2^{3n}} + \frac{3}{2^{4n}}$. In order to compute the mean value, we have to consider the conditions on the inputs. The probability that the inputs satisfy the conditions is computed with the help of the computer program mentioned in Section 2 and is given by $\frac{1}{2^{4n}}\left(1 - \frac{2}{2^n} + \frac{13}{2^{2n}} - \frac{24}{2^{3n}} + \frac{98}{2^{4n}} + O\left(\frac{1}{2^{5n}}\right)\right)$. Thus we get $\mathbb{E}(\delta_{ijk\ell}) = \frac{1}{2^{5n}}\left(1 + \frac{3}{2^n} - \frac{5}{2^{2n}} + O\left(\frac{1}{2^{3n}}\right)\right)$ and $\mathbb{E}(\mathcal{N}_{scheme}) \simeq \frac{m(m-1)(m-2)(m-3)}{4 \cdot 2^{5n}} \left(1 + \frac{3}{2^n} - \frac{5}{2^{2n}} + O\left(\frac{1}{2^{3n}}\right)\right)$.

A_3 is invertible and A_4 is not invertible The case where A_3 in not invertible and A_4 is invertible is similar. If A_4 is not invertible, we can have $Q_i = Q_j$, since this is equivalent to have $R_i \oplus R_j \in \ker(A_4)$ whose probability is about $\frac{1}{2^{n-t}}$ where $t = \dim(\ker(A_4))$. Moreover, when we have $Q_i = Q_j$ then we get $X_i^1 \oplus X_j^1 \oplus X_k^1 \oplus X_\ell^1 = 0$ and we obtain $(*)$ by setting $X_i^1 = X_k^1$ or $X_i^1 = X_\ell^1$. The conditions on the inputs do not change. Here, we obtain $\mathbb{E}(\delta_{ijk\ell}) = \frac{1}{2^{5n}}\left(1 + \frac{2}{2^{n-t}} + \frac{3}{2^n} + O\left(\frac{1}{2^{2n-t}}\right)\right)$ and $\mathbb{E}(\mathcal{N}_{scheme}) \simeq \frac{m(m-1)(m-2)(m-3)}{4 \cdot 2^{5n}}\left(1 + \frac{2}{2^{n-t}} + \frac{3}{2^n} + O\left(\frac{1}{2^{2n-t}}\right)\right)$. In that case, the difference of the mean values (for a random permutation and for a scheme) is $\frac{2}{2^{n-t}}$. Thus if $t > 0$ then the attack will be better than the attack in the case where A_3 and A_4 are invertible.

A_3 and A_4 are not invertible Since A_3 is not invertible, we can have $Q_i = Q_k$. This is equivalent to $L_i \oplus L_k \in \ker(A_3)$ and the probability is about $\frac{1}{2^{n-t'}}$ where $t' = \dim(\ker(A_3))$. We proceed as previously and we obtain $\mathbb{E}(\delta_{ijk\ell}) = \frac{1}{2^{5n}}\left(1 + \frac{2}{2^{n-t}} + \frac{2}{2^{n-t'}} + \frac{3}{2^n} + O\left(\frac{1}{2^{2n-\max(t',t)}}\right)\right)$ and $\mathbb{E}(\mathcal{N}_{scheme}) \simeq \frac{m(m-1)(m-2)(m-3)}{4 \cdot 2^{5n}}\left(1 + \frac{2}{2^{n-t}} + \frac{2}{2^{n-t'}} + \frac{3}{2^n} + O\left(\frac{1}{2^{2n-\max(t,t')}}\right)\right)$. The difference of the mean values (for a random permutation and for a scheme) is $\min\left(\frac{2}{2^{n-t}}, \frac{2}{2^{n-t'}}\right)$.

5.2 Computation of the variance

We will make use of the "Covariance Formula" given in Section 2.

***A_3* and *A_4* are invertible** Here $\mathbb{E}(\delta_{ijk\ell})\mathbb{E}(\delta_{pqrs}) = \frac{1}{2^{10n}}\left(1+\frac{6}{2^n}-\frac{1}{2^{2n}}+O\left(\frac{1}{2^{3n}}\right)\right)$. Now, in order to compute the variance, the main issue is to know the value of $\mathbb{E}(\delta_{ijk\ell}\delta_{pqrs})$. Again, we have to consider several cases. Our aim is to show that the variance behaves like the mean value. For example, when in $\{i, j, k, \ell, p, q, r, s\}$ we have 8 pairwise distinct values, we want the dominant term in the covariance part of the covariance formula $\frac{m^4}{2^{5n}}$. This shows that we must not have terms in $\frac{m^8}{2^{10n}}$ and in $\frac{m^8}{2^{11n}}$. We have to look carefully on the first two terms of $\mathbb{E}(\delta_{ijk\ell}\delta_{pqrs}) - \mathbb{E}(\delta_{ijk\ell})\mathbb{E}(\delta_{pqrs})$.

Case 1. In $\{i, j, k, \ell, p, q, r, s\}$, there are 8 pairwise distinct values. We are looking for the terms in $\frac{m^8}{2^{10n}}$ and in $\frac{m^8}{2^{11n}}$ when computing $\mathbb{E}(\delta_{ijk\ell}\delta_{pqrs})$. We still have the following conditions on the inputs:

$$\begin{array}{llll} L_i = L_j, & R_i = R_k, & L_p = L_q, & R_p = R_r \\ L_k = L_\ell \neq L_i, & R_j = R_\ell \neq R_i, & L_r = L_s \neq L_p, & R_q = R_s \neq R_p \end{array}$$

Then we add

$$f_2\left(X_i^1\right) \oplus f_2\left(X_j^1\right) \oplus f_2\left(X_k^1\right) \oplus f_2\left(X_\ell^1\right) = 0 \qquad (5)$$

$$f_2\left(X_p^1\right) \oplus f_2\left(X_q^1\right) \oplus f_2\left(X_r^1\right) \oplus f_2\left(X_s^1\right) = 0 \qquad (6)$$

In order to get the first two terms of $\mathbb{E}(\delta_{ijk\ell}\delta_{pqrs})$, we have to consider the following cases:

1. ($Q_i = Q_\ell$ and $X_i^1 = X_j^1$) or ($Q_i = Q_\ell$ and $X_i^1 = X_k^1$) and there is no condition on the internal variables $Q_p, Q_q, Q_r, Q_s, X_p^1, X_q^1, X_r^1, X_s^1$ except (6). In that case, the probability is given by $\frac{2}{2^{2n}}\left(1-\frac{5}{2^{2n}}-\frac{3}{2^{3n}}\right)\frac{1}{2^n}$. Since there is also a symmetry in i, j, k, ℓ and p, q, r, s, we obtain $\frac{4}{2^{3n}}\left(1-\frac{5}{2^{2n}}-\frac{3}{2^{3n}}\right)$.
2. Here we have $Q_i \neq Q_\ell$, ($X_i^1 = X_j^1$ and $X_k^1 = X_\ell^1$) or ($X_i^1 = X_k^1$ and $X_j^1 = X_\ell^1$) or ($X_i^1 = X_\ell^1$ and $X_j^1 = X_k^1$) and there is no condition on the internal variables $Q_p, Q_q, Q_r, Q_s, X_p^1, X_q^1, X_r^1, X_s^1$ except (6). Again there is also a symmetry in i, j, k, ℓ and p, q, r, s. The probability is $\frac{6}{2^{3n}}\left(1-\frac{1}{2^n}\right)\left(1-\frac{5}{2^{2n}}-\frac{3}{2^{3n}}\right)$.
3. We do not have any conditions on $Q_i, Q_j, Q_k, Q_\ell, X_i^1, X_j^1, X_k^1, X_\ell^1$ and $Q_p, Q_q, Q_r, Q_s, X_p^1, X_q^1, X_r^1, X_s^1$ but we have (5) and (6). In that case, the probability is $\left(1-\frac{10}{2^{3n}}-\frac{50}{2^{5n}}+\frac{18}{2^{7n}}\right)^2\frac{1}{2^{2n}}$.

Thus the probability to get (5) and (6) is $\frac{1}{2^{2n}}\left(1+\frac{10}{2^n}-\frac{60}{2^{3n}}+O\left(\frac{1}{2^{4n}}\right)\right)$. In order to compute the mean value, we have to consider the conditions on the inputs. The probability on the inputs is obtained thanks to the computer program again and is given by

$$\frac{2^{2n}(2^n-1)^2(2^n-2)(2^n-3)(2^{2n}+3\times 2^n-6)}{2^{2n}(2^{2n}-1)(2^{2n}-2)(2^{2n}-3)(2^{2n}-4)(2^{2n}-5)(2^{2n}-6)(2^{2n}-7)}$$

The computation gives: $\frac{1}{2^{2n}}\left(1-\frac{4}{2^n}+\frac{18}{2^{2n}}-\frac{36}{2^{3n}}+0\left(\frac{1}{2^{4n}}\right)\right)$ Thus we get $\mathbb{E}(\delta_{ijk\ell}\delta_{pqrs})=\frac{1}{2^{10n}}\left(1+\frac{6}{2^n}-\frac{22}{2^{2n}}+O\left(\frac{1}{2^{3n}}\right)\right)$. In that case, the dominant term in $\mathbb{E}(\delta_{ijk\ell}\delta_{pqrs})-\mathbb{E}(\delta_{ijk\ell})\mathbb{E}(\delta_{pqrs})$, is in $O\left(\frac{1}{2^{12n}}\right)$ and when $m\simeq 2^{\frac{7n}{4}}$, we will have $\frac{m^4}{2^{5n}}\simeq\frac{m^8}{2^{12n}}$. In that case, we have $V(\delta_{ijk\ell})=O\left(\frac{1}{2^{5n}}\right)$.

Remark 6 There are other possibilities on the internal variables in order to get (5) and (6), but they involve too many equations and this is not useful since we are interested in finding the first two leading terms. For example, it is possible to have no conditions on $Q_i, Q_j, Q_k, Q_\ell, Q_p, Q_q, Q_r, Q_s$, but $X_i=X_j$, $X_k=X_\ell$ and $\left(X_i^1, X_j^1, X_k^1, X_\ell^1\right)=\left(X_p^1, X_q^1, X_r^1, X_s^1\right)$.

Case 2. In $\{i,j,k,\ell,p,q,r,s\}$, there are 7 pairwise distinct values. We may assume for example that $i=p$ (there are 16 possibilities of equalities between the indices). We have the following relations:

$$\begin{cases} L_i=L_j=L_q,\ R_i=R_k=R_r,\ f_2\left(X_i^1\right)\oplus f_2\left(X_j^1\right)\oplus f_2\left(X_k^1\right)\oplus f_2\left(X_\ell^1\right)=0\\ L_k=L_\ell\neq L_i,\ R_j=R_\ell\neq R_i,\ f_2\left(X_i^1\right)\oplus f_2\left(X_q^1\right)\oplus f_2\left(X_r^1\right)\oplus f_2\left(X_s^1\right)=0\\ L_r=L_s\neq L_i,\ R_q=R_s\neq R_i, \end{cases}$$

The number of inputs is given by $2^{3n}(2^n-1)^2(2^n-2)$.

In that case, we just have to check that there is no term in $\frac{1}{2^{10n}}$ in $\mathbb{E}(\delta_{ijk\ell}\delta_{pqrs})-\mathbb{E}(\delta_{ijk\ell})\mathbb{E}(\delta_{pqrs})$. This is the easy part of the computation, since the term in $\frac{1}{2^{10n}}$ appears when there is no relations between the internal variables. Thus the dominant term in $\mathbb{E}(\delta_{ijk\ell}\delta_{pqrs})-\mathbb{E}(\delta_{ijk\ell})\mathbb{E}(\delta_{pqrs})$, is in $O\left(\frac{1}{2^{11n}}\right)$ and $V(\delta_{ijk\ell})=O\left(\frac{1}{2^{5n}}\right)$.

Case 3. In $\{i,j,k,\ell,p,q,r,s\}$, there are 6 pairwise distinct values. The dominant term in $\mathbb{E}(\delta_{ijk\ell}\delta_{pqrs})-\mathbb{E}(\delta_{ijk\ell})\mathbb{E}(\delta_{pqrs})$ is in $O\left(\frac{1}{2^{6n}}\right)$.

Finally, from cases 1, 2 and 3, we have $V(\mathcal{N}_{scheme})=O\left(\frac{m^4}{2^{5n}}\right)+O\left(\frac{m^6}{2^{9n}}\right)$ and when $m\leq 2^{\frac{7n}{4}}$, we have $V(\mathcal{N}_{scheme})=O\left(\frac{m^4}{2^{5n}}\right)$. Then the difference of the mean values will be greater than the standard deviations and again the attack succeeds.

Remark 7 The conditions on the inputs imply that it is not possible to have 5 distinct indices in $\{i,j,k,\ell,p,q,r,s\}$.

***A_3* is invertible and *A_4* is not invertible** Here we are interested in obtaining the first three terms of $\mathbb{E}(\delta_{ijk\ell}\delta_{pqrs})$, i.e the terms in $\frac{1}{2^{10n}}+\frac{1}{2^{11n-t}}+\frac{1}{2^{11n}}$. We will show that the dominant term in $\mathbb{E}(\delta_{ijk\ell}\delta_{pqrs})-\mathbb{E}(\delta_{ijk\ell})\mathbb{E}(\delta_{pqrs})$ is in $O\left(\frac{1}{2^{12n-2t}}\right)$. Thus if $m\simeq 2^{\frac{7n-2t}{4}}$, we will get that the variance behave like the mean value and the attack will succeed if the difference of the mean value is greater than both standard deviations. This will be the case if $m = O(2^{\frac{7n-2t}{4}})$. In order to get this result, we proceed as in the case where A_3 and A_4 are invertible. When in $\{i, j, k, \ell, p, q, r, s\}$, there are 8 pairwise distinct values, we study the conditions in the internal variables in order to get (5) and (6). Again we take into account the cases that do not involve too many equations. We consider the same possibilities as in the previous case. The probability to get (5) and (6) is $\frac{1}{2^{2n}}\left(1 + \frac{4}{2^{n-t}} + \frac{10}{2^n} + O\left(\frac{1}{2^{2n-2t}}\right)\right)$. In order to compute the mean value, we have to consider the conditions on the inputs. We obtain $\mathbb{E}(\delta_{ijk\ell}\delta_{pqrs}) = \frac{1}{2^{10n}}\left(1 + \frac{4}{2^{n-t}} + \frac{6}{2^n} + O\left(\frac{1}{2^{2n-2t}}\right)\right)$. In that case, the dominant term in $\mathbb{E}(\delta_{ijk\ell}\delta_{pqrs}) - \mathbb{E}(\delta_{ijk\ell})\mathbb{E}(\delta_{pqrs})$, is in $O\left(\frac{1}{2^{12n-2t}}\right)$ when $m \simeq 2^{\frac{7n-2t}{4}}$, and we will have $\frac{m^4}{2^{5n}} \simeq \frac{m^8}{2^{12n-2t}}$. When in $\{i, j, k, \ell, p, q, r, s\}$, there are 7 or 6 pairwise distinct values, the computations are similar. Finally, when $m \simeq 2^{\frac{7n-2t}{4}}$, we obtain and $V(\mathcal{N}_{scheme}) = O\left(\frac{m^4}{2^{5n}}\right)$. Then the difference of the mean values will be greater than the standard deviations and again the attack succeeds.

***A*₃ and *A*₄ are not invertible** The computations are very similar to those performed previously. We just have to add the possibility to get the equality $Q_k = Q_\ell$. Then we obtain $\mathbb{E}(\delta_{ijk\ell}\delta_{pqrs}) = \frac{1}{2^{10n}}\left(1 + \frac{4}{2^{n-t}} + \frac{4}{2^{n-t'}} + \frac{6}{2^n} + O\left(\min\left(\frac{1}{2^{2n-2t}}, \frac{1}{2^{2n-2t'}}\right)\right)\right)$. When $m \simeq \min(2^{\frac{7n-2t}{4}}, 2^{\frac{7n-2t'}{4}})$, the dominant term in the variance will be in $\frac{m^4}{2^{5n}}$. Then the difference of the mean values will be greater than the standard deviations and again the attack succeeds.

6 Conclusion

In this paper, we provided 4-point attacks on A-Feistel schemes. Our results are given in Tables 2 and 3. With 4-point attacks, it is more difficult to attack A-Feistel schemes than classical Feistel schemes. Simulations of our attacks given in Table 1 (Section 3.4) confirm our theoretical analysis for the complexity of these attacks. The analysis of the attacks requires to study the standard deviations of random variables and the use of a computer program that gives exact values for expectations and standard deviations.

Acknowledgements The authors want to thank the anonymous referee for the KPA on $\varphi \circ \Psi(f_1)$ with $(n+1)2^{\frac{n}{2}}$ messages.

References

1. Biham, E., Shamir, A.: Differential cryptanalysis of DES-like cryptosystems. In: Menezes, A., Vanstone, P.S.A. (eds.) Advances in Cryptology – CRYPTO 1990, vol. 537 of Lecture Notes in Computer Science, pp. 2–21. Springer (1991)
2. Biham, E., Shamir, A.: Differential cryptanalysis of DES-like cryptosystems. J. Cryptol. **4**(1), 3–72 (1991)
3. Gilbert, H., Minier, M.: New results on the pseudorandomness of some blockcipher constructions. In: Matsui, M. (ed.) Fast Software Encrytion – FSE '01, vol. 2355 of Lecture Notes in Computer Science, pp. 248–266. Springer (2001)
4. Hoel, P.G., Port, S.C., Stone, C.J.: Introduction to Probability Theory. Houghton Mifflin Company (1971)

5. Jutla, C.S.: Generalized birthday attacks on unbalanced feistel networks. In: Krawczyk, H. (ed.) Advances in Cryptology – CRYPTO '98, vol. 1462 of Lecture Notes in Computer Science, pp. 186–199. Springer (1998)
6. Knudsen, L.R.: DEAL - A 128-Bit Block Cipher. Technical Report 151, University of Bergen, Department of Informatics, Norway (1998)
7. Luby, M., Rackoff, C.: How to construct pseudorandom permutations from pseudorandom functions. SIAM J. Comput. **17**(2), 373–386 (1988)
8. Lucks, S.: Faster luby-rackoff ciphers. In: Gollman, D. (ed.) Fast Software Encryption – FSE '96, vol. 1039 of Lecture Notes in Computer Science, pp. 189–203. Springer (1996)
9. Matsui, M.: Linear cryptanalysis methods for DES cipher. In: Goos, G., Hartmanis, J. (eds.) Advances in Cryptology – EUROCRYPT 1993, vol. 765 of Lecture Notes in Computer Science, pp. 386–397. Springer (1994)
10. Matsui, M.: The first experimental cryptanalysis of the data encryption standard. In: Goos, G., Hartmanis, J. (eds.) Advances in Cryptology – CRYPTO 1994, vol. 869 of Lecture Notes in Computer Science, pp. 1–11. Springer (1994)
11. Nachef, V., Patarin, J., Treger, J.: Generic attacks on misty schemes. In: Abdalla, M., Barretol, P.S.L.M. (eds.) Progress in Cryptology – LATINCRYPT 2010, vol. 6212 of Lecture Notes in Computer Science, pp. 222–240. Springer (2010)
12. Nachef, V., Volte, E., Patarin, J.: Differential attacks on generalized feistel schemes. In: Abdalla, M., Nita-Rotaru, C., Dahab, R. (eds.) CANS 2013, vol. 8257 of Lecture Notes in Computer Science, pp. 1–19. Springer (2013)
13. Naor, M., Reingold, O.: On the construction of pseudorandom permutations: Luby-rackoff revisited. J. Cryptol. **12**(1), 29–66 (1999)
14. Patarin, J.: Generic attacks on feistel schemes. In: Boyd, C. (ed.) Advances in Cryptology – ASIACRYPT 2001, vol. 2248 of Lecture Notes in Computer Science, pp. 222–238. Springer (2001)
15. Patarin, J., Nachef, V., Berbain, C.: Generic attacks on unbalanced feistel schemes with contracting functions. In: Lai, X., Chen, K. (eds.) Advances in Cryptology – ASIACRYPT 2006, vol. 4284 of Lecture Notes in Computer Science, pp. 396–411. Springer (2006)
16. Schneier, B., Kelsey, J.: Unbalanced feistel networks and block cipher design. In: Gollmann, D. (ed.) Fast Software Encrytion – FSE '96, vol. 1039 of Lecture Notes in Computer Science, pp. 121–144. Springer (1996)
17. Treger, J., Patarin, J.: Generic attacks on feistel networks with internal permutations. In: Preneel, B. (ed.) Progresses in Cryptology – AFRICACRYPT '09, Lecture Notes in Computer Science. Springer (2009)
18. Vaudenay, S.: Provable security for block ciphers by decorralation. In: Movan, M., Meinel, C., Krob, D. (eds.) STACS 1998, vol. 1373 of Lecture Notes in Computer Science, pp. 249–265. Springer (1998)
19. Vaudenay, S.: Decorrelation: A theory for block cipher security. J. Cryptol. **16**(4), 249–286 (2003)
20. Volte, E., Nachef, V., Marrière, N.: Improvements of attacks on various feistel schemes. In: MYCRYPT 2016, Lecture Notes in Computer Science. Springer (2016)
21. Volte, E., Nachef, V., Patarin, J.: Improved generic attacks on unbalanced feistel schemes with expanding functions. In: Abe, M. (ed.) Advances in Cryptology – ASIACRYPT 2010, vol. 6477 of Lecture Notes in Computer Science, pp. 94–111. Springer (2010)