4-point Attacks with Standard Deviation Analysis on A-Feistel Schemes

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

[1] Department of Mathematics, University of Cergy-Pontoise, CNRS UMR 8088
2 avenue Adolphe Chauvin, 95011 Cergy-Pontoise Cedex, France
[2] PRISM, University of Versailles
45 avenue des Etats-Unis, 78035 Versailles Cedex, France
valerie.nachef@u-cergy.fr, emmanuel.volte@u-cergy.fr
jacques.patarin@prism.uvsq.fr

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. In [18, 19], it is shown that ciphers that achieve 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 stronger attacks based on specific equations on 4-tuples of cleartext/ciphertext messages. We give the number of messages needed to distinguish a permutation produced by such schemes from a random permutation, depending on the number of rounds used in the schemes, the number and the position of the random affine permutations introduced in the schemes.

Key words: affine permutations, classical Feistel permutations, pseudo-random permutations, generic attacks, Luby-Rackoff theory, block ciphers.

1 Introduction

Differential cryptanalysis on encryption schemes was invented in the early 90s by Biham and Shamir who applied it against DES [1, 2].Then Matsui developped linear cryptanalysis against DES [9, 10]. Differential cryptanalysis exploits the high probability of certain occurrences of plaintext differences and differences into the last round of the cipher. Consider two inputs M' and M'' with corresponding outputs Y' and Y''. The input difference is ΔM and the output difference is ΔY. In an ideally randomizing cipher the probability that a particular output difference ΔY occurs given a particular difference input ΔM is $\frac{1}{2^n}$ where n is the number of bits of M. Differential cryptanalysis seeks to exploit a scenario where a particular ΔY occurs given a particular input difference ΔM with a very high probability. Linear cryptanalysis tries to take advantage of high probability occurrences of linear expressions involving plaintext bits, ciphertext bits and subkey bits. Both methods use pairs of plaintext/ciphertexts. They allowed to produce attacks on classical Feistel schemes with random functions [7, 8, 14] or random permutations [6, 17], unbalanced Feistel schemes with expanding [5, 16, 20] or contracting functions [13, 15], Misty schemes [3, 11], generalized Feistel schemes of type 1, 2 and 3 [12]. In [18, 19], Vaudenay showed that if a block cipher has perfect pairwise decorrelation, then it is secure against linear and differential attacks. We recall that a function F has perfect pairwise decorrelation if for any $x_1 \neq x_2$, the random variables $F(x_1)$ and $F(x_2)$ are uniformly distributed and independent. Affine permutations are examples of functions achieving perfect pairwise decorrelation. Now suppose that we have r independent ciphers $C_1, \ldots, C_r$. If one of these cipher has perfect pairwise decorrelation, then $C = C_r \circ \ldots \circ C_1$ has also perfect pairwise decorrelation ([18, 19]). Thus if one of the ciphers is an affine permutation, then C has perfect pairwise decorrelation and is secure against linear and differential cryptanalysis. This gives a method to construct ciphers that are secure against linear and differential attacks. COCONUT and PEANUT ([18]) are examples of such schemes: they are of the form $C_3 \circ C_2 \circ C_1$ where C_1 and C_3 are any ciphers and C_2 performs perfect pairwise decorrelation. In [13], the authors studied the security of schemes of the form $C_2 \circ \psi \circ C_1$ or $\psi \circ C_1$ where C_1 and C_2 are pairwise independent permutation (they achieve perfect pairwise decorrelation) and ψ is a balanced Feistel scheme or an unbalanced Feistel scheme with contracting functions. By Vaudenay's result, we know that again these schemes are secure against linear and differential cryptanalysis. But we can consider different types of attacks. For example, we may have specific relations on tuples of cleartext/ciphertext messages. In this paper, we will study these kind of attacks on a family of schemes that are secure against linear and differential cryptanalysis. We will see that we can use 4-tuples of cleartext/ciphertext messages. We consider schemes of the form $\Psi^d \circ \varphi$, $\varphi' \circ \Psi^d \circ \varphi$, $\Psi^{d_2} \circ \varphi \circ \Psi^{d_1}$ where φ, φ' are affine permutations and $\psi^d, \psi^{d_1}, \Psi^{d_2}$ are classical Feistel schemes with respectively d, d_1, d_2 rounds. We will denote these schemes as A-Feistel schemes. As far as we know, no systematic study of attacks has been done on this family of schemes. We will study Known Plaintext Attacks (KPA) and non adaptive Chosen Plaintext Attacks (CPA-1).

We introduce an affine permutation at the beginning, at the end, inside the Feistel scheme, or both at the beginning and at the end. Thus, by symmetry, we will obtain results for Known Ciphertext Attacks (KCA) and non adaptive Chosen Ciphertext Attacks (CCA-1). The affine permutations and the functions used in the Feistel schemes are keyed dependent. With our attacks we want to distinguish a random permutation from a random permutation produced by a scheme. For some of our attacks, we will make a precise analysis of standard deviation. The paper is organized as follows. In section 2, we define our schemes that we name 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 after the affine permutation with a number of messages less than 2^{2n} and then we describe attacks against generators of permutations. We did some simulations of our attacks. The results of these simulations are given in section 3.4. In Section 4, we present attacks on schemes for which we apply first an affine permutation, then a Feistel scheme with several rounds and again an affine permutation. Appendices A and B are devoted to the computation of standard deviations. In appendix C, it is shown that A-Feistel permutations have even signature. This allows attacks by the signature when all the cleartext/ciphertext pairs are known.

2 Preliminaries

2.1 Notation

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 $\{0,1\}^n$. We define $\Psi(f)[L,R] = [S,T] \overset{\text{def}}{\Leftrightarrow} S = R$ and $T = L \oplus f(R)$. More generally, let d be an integer and $f_1, f_2, \ldots, f_d$ be d functions of F_n. We set: $\Psi^d(f_1, \ldots, f_d) = \Psi(f_d) \circ \cdots \circ \Psi(f_2) \circ \Psi(f_1)$. The permutation $\Psi^d(f_1, \ldots, f_d)$ is called a "Feistel scheme with d rounds" and is denoted by Ψ^d.

2.2 A-Feistel schemes

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: $M \to A.M \oplus c$ where $A \in GL(2n, K)$ 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 with 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 $c_i \in \{0,1\}^n$.

We introduce the internal variables that appear in the different rounds of 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 introduce internal variables: $P = A_1.L \oplus A_2.R \oplus c_1$, $Q = A_3.L \oplus A_4.R \oplus c_2$, $X^1 = P \oplus f_1(Q)$, $X^2 = Q \oplus f_2(X^1)$ and for $j \geq 3$, $X^j = X^{j-2} \oplus f_j(X^{j-1})$.

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

$$[L,R] \xrightarrow{\Psi(f_1)} [R,X^1] \xrightarrow{\Psi(f_2)} [X^1,X^2] \ldots$$

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

Here we have the internal variables: $X^1 = L \oplus f_1(R)$, $X^2 = R \oplus f_2(X^1)$ 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: $S = A_1.X^{d-1} \oplus A_2.X^d \oplus c_1$, $T = A_3.X^{d-1} \oplus A_4.X^d \oplus c_2$.

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

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

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

The internal variables are: $X^1 = L \oplus f_1(R)$, $X^2 = R \oplus f_2(X^1)$ and for $3 \leq j \leq d_1$, $X^j = X^{j-2} \oplus f_j(X^{j-1})$, $P = A_1.X^{d-1} \oplus A_2.X^d \oplus c_1$, $Q = A_3.X^{d-1} \oplus A_4.X^d \oplus c_2$, $X^{d_1+1} = P \oplus f_{d_1+1}(Q)$, $X^{d_1+2} = Q \oplus f_{d_1+2}(X^{d_1+1})$. We also have $S = X^{d_1+d_2-1}$ and $T = X^{d_1+d_2-2} \oplus f_{d_1+d_2}(X^{d_1+d_2-1})$.

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

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

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

The internal variables are: $P = A_1.L \oplus A_2.R \oplus c_1$, $Q = A_3.L \oplus A_4.R \oplus c_2$, $X^1 = P \oplus f_1(Q)$, $X^2 = Q \oplus f_2(X^1)$ and for $j \geq 3$, $X^j = X^{j-2} \oplus f_j(X^{j-1})$. Finally $S = A'_1.X^{d-1} \oplus A'_2.X^d \oplus c'_1$, $T = A'_3.X^{d-1} \oplus A'_4.X^d \oplus c'_2$.

2.3 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 of some internal variables due to the structure of the scheme. Our attacks consist in using 4-tuples of plaintext/ciphertexts 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-uples 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, by the Chebyshev's inequality, the difference $|E(\mathcal{N}_{scheme}) - E(\mathcal{N}_{perm})|$ is larger than both standard deviations $\sigma(\mathcal{N}_{perm})$ and $\sigma(\mathcal{N}_{scheme})$, where E denotes the expectancy function. This gives the number of messages needed for the attack. In order to compute 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 $V(\sum_{i=1}^{n} x_i) = \sum_{i=1}^{n} V(x_i) + 2\sum_{i=1}^{n-1}\sum_{j=i+1}^{n}\big[E(x_i\, x_j) - E(x_i)E(x_j)\big]$. Examples of computations are given in Appendices A and B.

3 A-Feistel schemes with one affine permutation

3.1 One affine permutation and a Feistel scheme with one round

$\Psi(f_1)\circ\varphi$. Let $[L, R]$ denote the input. The output is denoted by $[S, T]$. Then we have $[L, R] \to [P, Q] \to [S, T]$, where $P = A_1.L \oplus A_2.R \oplus c_1$, $Q = A_3.L \oplus A_4.R \oplus c_2$, $S = Q$ and $T = X^1 = P \oplus f_1(Q)$ and $f_1 \in_R F_n$. Thus $S = A_3.L \oplus A_4.R \oplus c_2$.

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 $[S_1, T_1] = \Psi(f_1)\circ\varphi[L_1, R_1]$, $[S_1', T_1'] = \Psi(f_1)\circ\varphi[L_1, R_2]$, $[S_2, T_2] = \Psi(f_1)\circ\varphi[L_2, R_2]$ and $[S_2', T_2'] = \Psi(f_1)\circ\varphi[L_2, R_1]$. 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 about $\frac{1}{2^n}$. Thus we need 4 messages to distinguish a random permutation from a permutation of the form $\Psi(f_1)\circ\varphi$.

KPA with 2^n messages. We can transform the previous CPA-1 into a KPA. With 2^n messages, by the birthday paradox, we can obtain with a good probability L_1, L_2, R_1, R_2 such that $L_1 \neq L_2$ and $R_1 \neq R_2$. As previously we construct the outputs $[S_1, T_1]$, $[S_1', T_1']$, $[S_2, T_2]$ and $[S_2', T_2']$. Then we check if $S_1 \oplus S_1' \oplus S_2 \oplus S_2' = 0$. The probability to obtain this value is one with an A-Feistel and $\frac{1}{2^n}$ for a random permutation.

$\boldsymbol{\varphi \circ \Psi(f_1)}$**.** Let $[L, R]$ denote the input and $[S, T]$ denote the output. We have $[L, R] \to [R, L \oplus f_1(R)], \to [S, T]$, where $S = A_1.R \oplus A_2(L \oplus f_1(R)) \oplus c_1$ and $T = A_3.R \oplus A_4(L \oplus f_1(R)) \oplus c_2$.

CPA-1 with 4 messages . We choose again L_1, L_2, R_1, R_2 such that $L_1 \neq L_2$ and $R_1 \neq R_2$ and we construct the 4 messages $[L_1, R_1], [L_1, R_2], [L_2, R_1], [L_2, R_2]$. Then with a permutation of the form $\varphi \circ \Psi(f_1)$ we obtain $S_1 \oplus S'_1 \oplus S_2 \oplus S'_2 = 0$ and $T_1 \oplus T'_1 \oplus T_2 \oplus T'_2 = 0$ with probability one. With a random permutation the probability to obtain theses equalities is about $\frac{1}{2^{2n}}$.

KPA with 2^n *messages.* We transform the previous CPA-1 into a KPA as previously and we need again 2^n messages to distinguish a random permutation from a permutation of the form $\varphi \circ \Psi(f_1)$.

3.2 One affine permutation and a Feistel scheme with two rounds

$\boldsymbol{\Psi(f_2) \circ \Psi(f_1) \circ \varphi}$**.** 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 $P = A_1.L \oplus A_2.R \oplus c_1$, and $Q = A_3.L \oplus A_4.R \oplus c_2$.

CPA-1 with $2^{\frac{n}{2}}$ *messages.* We choose only 2 values for L: L_1 and L_2. Then, we choose approximately $\frac{1}{2}.2^{\frac{n}{2}}$ distinct values for R_i. Therefore we can construct about $m \simeq 2^{\frac{n}{2}}$ messages. 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 $S_i \oplus S_j \oplus S_{i'} \oplus S_{j'} = 0$.

We are going to show that for an A-Feistel scheme, this number $\mathcal{N}$ is at least twice the number we get for a random permutation. Since for a random permutation, we have $\mathcal{N}_{perm} \simeq \frac{m^2}{2.2^n}$, we will be able to distinguish when the probability to have $\mathcal{N}_{perm} \geq 1$ is not negligible, i.e. when $m \geq 2^{\frac{n}{2}}$ (we can also try another $[L_1, L_2]$; for each $[L_1, L_2]$ the probability of success of this attack is not negligible). For A-Feistel schemes, the condition on the outputs may appear at random as well. They also may happen due to condition on the internal variables. First we notice that the conditions on the inputs imply:

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

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:

$$\begin{array}{ll} Q_i = Q_j \Leftrightarrow Q_{i'} = Q_{j'} & (2) \\ Q_i = Q_{i'} \Leftrightarrow Q_j = Q_{j'} & (3) \\ Q_i = Q_{j'} \Leftrightarrow Q_{i'} = Q_j & (4) \end{array}$$

Thus if we have $Q_i = Q_j$ or $Q_i = Q_{i'}$, or $Q_i = Q_{j'}$, we will obtain $S_i \oplus S_j \oplus S_{i'} \oplus S_{j'} = 0$.
We will use the following proposition whose proof is straightforward.

Proposition 1 *Suppose that $L_i = L_j$, $L_k = L_\ell \neq L_i$, $R_i = R_k$ and $R_j = R_\ell \neq R_i$. Then we have the following properties:*

1. *$Q_i = Q_j \Leftrightarrow A_4(R_i \oplus R_j) = 0$. Thus if A_4 is a bijection, this condition will never be satisfied since $R_i \neq R_j$. If A_4 is not a bijection, then the probability to have* (2) *is greater then $\frac{1}{2^n}$. Indeed, it is easy to check that if* $\dim\ker(A_4) =$ *t then the probability that $R_i \oplus R_j \in \ker(A_4) = \frac{2^t}{2^n} = \frac{1}{2^{n-t}} \geq \frac{1}{2^n}$.*
2. *$Q_i = Q_{i'} \Leftrightarrow A_3(L_1 \oplus L_2) = 0$. Thus if A_3 is a bijection, this condition will never be satisfied since $L_1 \neq L_2$. Again, if A_3 is not a bijection the probability to have* (3) *is greater than $\frac{1}{2^n}$ since it is equal to $\frac{1}{2^{n-t'}}$ where $t' = \dim(\ker(A_3))$.*
3. *The condition $Q_i = Q_\ell$ 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 $\frac{1}{2^n}$.*

If A_3 and A_4 are bijective, we can only have $Q_i = Q_\ell$. We obtain $\mathcal{N}_{scheme} \simeq \frac{m^2}{2^n}$. Thus $\mathcal{N}_{scheme}$ is at least twice $\mathcal{N}_{perm}$ and we get a CPA-1 with $m \simeq 2^{\frac{n}{2}}$ messages when both A_3 and A_4 are bijective. When A_3 is not bijective and A_4 is bijective, then we have $\mathcal{N}_{scheme} \simeq \frac{m^2}{2^n} + \frac{m^2}{2.2^{n-t'}}$ and $m \simeq 2^{\frac{n-t'}{2}}$ (it is also possible to have A_3 bijective and A_4 not bijective). If A_3 and A_4 are not bijective, then $\mathcal{N}_{scheme} \simeq \frac{m^2}{2^n} + \frac{m^2}{2.2^{n-t'}} + \frac{m^2}{2.2^{n-t'}}$ and $m \simeq \min(2^{\frac{n-t'}{2}}, 2^{\frac{n-t}{2}})$.
Remark 1: 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.

KPA with $2^{\frac{5n}{4}}$ messages. 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, i', j') such that

$$\begin{cases} L_i = L_j \\ L_{i'} = L_{j'} \neq L_i \end{cases} \text{and} \begin{cases} R_i = R_{i'} \\ R_j = R_{j'} \neq R_i \end{cases} \text{and } S_i \oplus S_j \oplus S_{i'} \oplus S_{j'} = 0$$

We have $\mathcal{N}_{perm} \simeq \frac{m^4}{4.2^{5n}}$ and $\mathcal{N}_{scheme} \simeq \frac{m^4}{2.2^{5n}}$ for a A-Feistel permutation when A_3 and A_4 are bijective. Therefore this KPA succeeds when $m \simeq 2^{\frac{5n}{4}}$. As in the previous CPA-1, if we want to take into account the properties of the kernels of A_3 and A_4, we obtain $m \simeq \min(2^{\frac{5n}{4}}, 2^{\frac{5n-t}{4}}, 2^{\frac{5n-t'}{4}})$.

$\varphi \circ \Psi(f_2) \circ \Psi(f_1)$ Here, after one round the output is $[R, L \oplus f_1(R)]$. Let $X^1 = R \oplus f_1(R)$. 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 $S = A_1.X^1 \oplus A_2.X^2 + c_1$ and $T = A_3.X^1 \oplus A_4.X^2 + c_2$.
We first describe a CPA-1 with $2^{\frac{n}{2}}$ messages. We proceed as in the case $\Psi(f_2) \circ \Psi(f_1) \circ \varphi$. We choose only 2 values for L: L_1 and L_2. Then, we choose approximately $\frac{1}{2}.2^{\frac{n}{2}}$ distinct values for R_i. Therefore we can construct about $m \simeq 2^{\frac{n}{2}}$ messages. We count the number $\mathcal{N}$ of (R_i, R_j) values, $R_i \neq R_j$ such that with the 4 following message: $i: \ [L_1, R_i], \quad i': \ [L_2, R_i] \quad j: \ [L_1, R_j], \quad j': \ [L_2, R_j]$, we have $S_i \oplus S_j \oplus S_{i'} \oplus S_{j'} = 0$ and $T_i \oplus T_j \oplus T_{i'} \oplus T_{j'} = 0$. When we have 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 $X^1_i = X^1_{j'}$ (or $X^1_i = X^2_k$, or $X^1_i = X^1_\ell$), 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 $\mathcal{N}_{scheme} \simeq \frac{m^2}{2.2^n} + \frac{3}{2} \times \frac{m^2}{2^{2n}}$. 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 $\mathcal{N}_{perm} \simeq \frac{m^2}{2^{2n}}$. Thus with $m \simeq 2^{\frac{n}{2}}$ messages, the attack succeed and we can distinguish an A-Feistel scheme from a random permutation.
This CPA-1 can be transformed into a KPA with $2^{\frac{5n}{4}}$ messages.

Remark 2: Here we do not need to take into account the properties of the kernels of A_3 and A_4.

$\boldsymbol{\Psi(f_2) \circ \varphi \circ \Psi(f_1)}$**.** Let as usual $[L, R]$ denote the input. Then we have: $S = Q = A_3.R \oplus A_4(L \oplus f_1(R))$ and $T = P \oplus f_2(Q)$ with $P = A_1.R \oplus A_2(L \oplus f_1(R))$. We give a 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 $S_1 \oplus S'_1 \oplus S_2 \oplus S'_2 = 0$. The probability to obtain this equality is equal to one with a scheme and to $\frac{1}{2^n}$ with a random permutation.
We can transform this attack into a KPA with 2^n messages.

Remark 3: In the next attacks, and in order to simplify the presentation, we will assume that A_3 and A_4 are bijective. It is not difficult to study the other possibilities. The properties of the kernels of A_3 and A_4 are not involved when the scheme ends with the affine permutation.

3.3 One affine permutation and a Feistel scheme with three rounds

$\boldsymbol{\Psi(f_3) \circ \Psi(f_2) \circ \Psi(f_1) \circ \varphi}$**.** 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 $S = X^2 = Q \oplus f_1(X^1)$ and $T = X^3 = X^1 \oplus f_3(X^2)$ where $f_1, f_2, f_3 \in_R F_n$. Remind that $P = A_1.L \oplus A_2.R \oplus c_1$, $Q = A_3.L \oplus A_4.R \oplus c_2$ and $X^1 = P \oplus f_1(Q)$.

KPA with $2^{\frac{7n}{4}}$ *messages.* 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 a random permutation, $E(\mathcal{N}_{perm}) \simeq \frac{m^4}{4\cdot 2^{5n}}$ (Appendix A), and when $m \simeq 2^{\frac{7n}{4}}$, we obtain from the computations of Appendix A, that $\sigma(\mathcal{N}_{perm}) = O(\frac{m^2}{2^{\frac{5n}{2}}})$. 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:

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

It is also possible to 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 Appendix B, we get $E(\mathcal{N}_{scheme}) \simeq \frac{m^4}{4.2^{5n}} + O(\frac{m^4}{2^{6n}})$, and $\sigma(\mathcal{N}_{scheme}) = O(\frac{m^2}{2^{\frac{5n}{2}}})$. We can distinguish an soon as the difference of the mean values is greater than both standard deviations, i.e. $\frac{m^4}{2^{6n}} \leq \frac{m^2}{2^{\frac{5n}{2}}}$. This means we must have $m \simeq 2^{\frac{7n}{4}}$.

CPA-1 with $2^{\frac{3n}{2}}$ *messages.* The previous KPA can be transformed 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 $E(\mathcal{N}_{perm}) \simeq \frac{m^4}{4.2^{4n}}$ 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 $E(\mathcal{N}_{scheme}) \simeq \frac{m^4}{4.2^{4n}} + O(\frac{m^4}{2^{5n}}) = \frac{m^4}{2^{4n}})$ and $\sigma(\mathcal{N}_{scheme}) = O(\frac{m^2}{2^{2n}})$. 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 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).

Table 1. Simulation results

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

$\varphi\circ\Psi(f_3)\circ\Psi(f_2)\circ\Psi(f_1)$ 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 $X^1=L\oplus f_1(R), X^2=R\oplus f_2(X^1), X^3=X^1\oplus f_3(X^2)$,
$S=A_1.X^2\oplus A_2.X^3\oplus c_1$ and $T=A_3.X^2\oplus A_4.X^3\oplus c_2$

CPA-1 with 2^n messages. We choose only 2 values for L: L_1 and L_2. Then, we choose approximately 2^n values for R_i (i.e. almost all the possible values for R_i). Therefore we have $m\simeq 2.2^n$ messages. We count the number $\mathcal{N}$ of (R_i,R_j) values, $R_i\neq R_j$ such that with the 4 following message: $i:\ [L_1,R_i],\quad i':\ [L_2,R_i]\quad j:\ [L_1,R_j],\quad j':\ [L_2,R_j]$, we have $S_i\oplus S_j\oplus S_{i'}\oplus S_{j'}=0$ and $T_i\oplus T_j\oplus T_{i'}\oplus T_{j'}=0$. 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 imply the equalities on the outputs. The conditions on the inputs imply that $X^1_i\oplus X^1_{i'}\oplus X^1_j\oplus X^1_{j'}=0$. Then 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 $X^2_i\oplus X^2_{i'}\oplus X^2_j\oplus X^2_{j'}=0$. Now we can impose either $X^2_i=X^2_j\Leftrightarrow X^2_{i'}=X^2_{j'}$ or $X^2_i=X^2_{j'}\Leftrightarrow X^2_{i'}=X^2_j$, but we cannot impose $X^2_i=X^2_{j'}$ since this will imply $R_i=R_j$. Then we obtain $X^3_i\oplus X^3_{i'}\oplus X^3_j\oplus X^3_{j'}=0$ and then the properties of the affine permutation will give the required conditions on the outputs. If we impose $X^1_i=X^1_j\Leftrightarrow X^1_{i'}=X^1_{j'}$, then there are again two possibilities for equalities between $X^2_i,X^2_j,X^2_{i'},X^2_{j'}$. With a random permutation, the conditions on the outputs will only appear at random. Thus we get $\mathcal{N}_{perm}\simeq\frac{m^2}{2.2^{2n}}$ and $\mathcal{N}_{scheme}\simeq 2.\frac{m^2}{2^{2n}}$. This shows that when $m\simeq 2^n$ we can distinguish a random permutation from a permutation produced by an A-Feistel scheme.

KPA with $2^{\frac{3n}{2}}$ messages. As usual, we can transform this CPA-1 into a KPA. We count the number $\mathcal{N}$ of (i,j,k,ℓ) such that

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

When we have a random permutation, $E(\mathcal{N}_{perm})\simeq\frac{m^4}{4\cdot 2^{6n}}$. With an A-Feistel scheme, these equalities may happen at random or, as previously, because there are some conditions which can be satisfied by internal variables.
Thus $E(\mathcal{N}_{scheme})\simeq\frac{m^4}{2^{6n}}$

We can distinguish a random permutation from a permutation produced by an A-Feistel scheme when $m\simeq 2^{\frac{3n}{2}}$

$\Psi(f_3)\circ\Psi(f_2)\circ\varphi\circ\Psi(f_1)$ or $\Psi(f_3)\circ\varphi\circ\Psi(f_2)\circ\Psi(f_1)$. We explain the attacks for $\Psi(f_3)\circ\Psi(f_2)\circ\varphi\circ\Psi(f_1)$. The other case is quite similar. The values are given by: $[L,R]\longrightarrow[R,X^1]\longrightarrow[P,Q]\longrightarrow[Q,X^2]\longrightarrow[S,T]$, with $X^1=L\oplus f_1(R), P=A_1.R\oplus A_2.X^1\oplus c_1, Q=A_3.R\oplus A_4.X^1\oplus c_2, S=X^2=P\oplus f_2(Q)$ and $T=X^3=Q\oplus f_3(X^2)$.

CPA-1 with $2^{\frac{n}{2}}$ messages Here, we choose only 2 values for L: L_1 and L_2. Then, we choose approximately $\frac{1}{2}.2^{\frac{n}{2}}$ distinct values for R_i. Therefore we can construct about $m \simeq 2^{\frac{n}{2}}$ messages. 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 $S_i \oplus S_j \oplus S_{i'} \oplus S_{j'} = 0$. We obtain $E(\mathcal{N}_{perm}) \simeq \frac{m^2}{2 \cdot 2^n}$ and $E(\mathcal{N}_{scheme}) \simeq \frac{m^2}{2^n}$. Thus when $m \simeq 2^{\frac{n}{2}}$, we can distinguish a random permutation from a permutation generated by an A-Feistel scheme.

KPA1 with $2^{\frac{5n}{4}}$ messages. 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, i', j') such that

$$\begin{cases} L_i = L_j \\ L_{i'} = L_{j'} \neq L_i \end{cases} \text{and} \begin{cases} R_i = R_{i'} \\ R_j = R_{j'} \neq R_i \end{cases} \text{and } S_i \oplus S_j \oplus S_{i'} \oplus S_{j'} = 0$$

We have $\mathcal{N}_{perm} \simeq \frac{m^4}{2^{5n}}$ and $\mathcal{N}_{scheme} \simeq 2.\frac{m^4}{2^{5n}}$ for a A-Feistel permutation. Therefore this KPA succeeds when $m \simeq 2^{\frac{5n}{4}}$.

3.4 One affine permutation and a Feistel scheme with four rounds

$\boldsymbol{\Psi(f_4) \circ \Psi(f_3) \circ \Psi(f_2) \circ \Psi(f_1) \circ \varphi}$**.** 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 $P = A_1.L \oplus A_2.R \oplus c_1$, $Q = A_3.L \oplus A_4.R \oplus c_2$, $X^1 = P \oplus f_1(P)$, $X^2 = Q \oplus f_2(X^1)$ 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 a random permutation, $E(\mathcal{N}_{perm}) \simeq \mu \frac{m^4}{4.2^{5n}}$ and $\sigma(\mathcal{N}_{perm}) = O(\sqrt{\mu} \frac{m^2}{2^{\frac{5n}{2}}})$. The computation of the standard deviation can be done as previously. With an A-Feistel scheme, these equalities may happen at random or because there are some conditions that can be satisfied by internal variables. For example, we may have (other conditions are possible like $(Q_i = Q_\ell, X_i^1 = X_j^1, X_i^2 = X_j^2)$ or $(Q_i \neq Q_\ell, X_i^1 = X_j^1, X_k^1 = X_\ell^1, X_i^2 = X_k^2)$):

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

Remark 4: It is not possible to have the same kind of conditions on successive variables. For example, it is not possible to have $Q_i = Q_\ell$ and and $X^1_i = X^1_\ell$, since this will imply $P_i = P_\ell$ and we obtain a contradiction since we have permutations and $[L_i, R_i] \neq [L_\ell, R_\ell]$. This is why we set the conditions $Q_i = Q_\ell, X^1_i = X^1_j, X^2_i = X^2_k$. For a permutation produced be an A-Feistel scheme, we obtain $E(\mathcal{N}_{scheme}) \simeq \mu\frac{m^4}{2^{5n}} + O(\mu\frac{m^4}{2^{7n}})$ and $\sigma(\mathcal{N}_{scheme}) = O(\sqrt{\mu}\frac{m^2}{2^{\frac{5n}{2}}})$. 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 $\lambda = \mu \cdot 2^n = 2^{3n}$.

$\boldsymbol{\varphi \circ \Psi(f_4) \circ \Psi(f_3) \circ \Psi(f_2) \circ \Psi(f_1)}$ 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 $S = A_3.X^3 \oplus A_4.X^4 \oplus c_2$. 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 $E(\mathcal{N}_{perm}) \simeq \frac{m^4}{4.2^{6n}}$, $\sigma(\mathcal{N}_{perm}) = O(\frac{m^2}{2^{3n}})$ and $E(\mathcal{N}_{scheme}) \simeq \frac{m^4}{4.2^{6n}} + O(\frac{m^4}{2^{7n}})$ and $\sigma(\mathcal{N}_{scheme}) = O(\frac{m^2}{2^{3n}})$. We can distinguish when $\frac{m^4}{2^{7n}} \geq \frac{m^2}{2^{3n}}$. Thus the attack succeeds when $m \simeq 2^{2n}$.

$\boldsymbol{\Psi(f_4) \circ \Psi(f_3) \circ \Psi(f_2) \circ \varphi \circ \Psi(f_1)}$ **or** $\boldsymbol{\Psi(f_4) \circ \Psi(f_3) \circ \varphi \circ \Psi(f_2) \circ \Psi(f_1)}$ **or** $\boldsymbol{\Psi(f_4) \circ \varphi \circ \Psi(f_3) \circ \Psi(f_2) \circ \Psi(f_1)}$**.** 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.

KPA with $2^{\frac{7n}{4}}$ *messages.* The values are given by: $[L, R] \longrightarrow [R, X^1] \longrightarrow [P, Q] \longrightarrow [Q, X^2] \longrightarrow [X^2, X^3] \longrightarrow [S, T]$, with $X^1 = L \oplus f_1(R), P = A_1.R \oplus A_2.X^1 \oplus c_1, Q = A_3.R \oplus A_4.X^1 \oplus c_2, X^2 = P \oplus f_2(Q)$, $S = X^3 = Q \oplus f_3(X^2)$ and $T = X^4 = X^2 \oplus f_4(X^3)$. 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, $E(\mathcal{N}_{perm}) \simeq \frac{m^4}{4.2^{5n}}$ and we obtain from computations similar to those permform in section A, that $\sigma(\mathcal{N}_{perm}) = O(\frac{m^2}{2^{\frac{5n}{2}}})$. 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:

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

Thus, using the computations similar to those performed in Section B, we get we get $E(\mathcal{N}_{scheme}) \simeq \frac{m^4}{4.2^{5n}} + O(\frac{m^4}{2^{6n}})$ and $\sigma(\mathcal{N}_{scheme}) = O(\frac{m^2}{2^{\frac{5n}{2}}})$. We can distinguish an soon as the difference of the mean values is greater than both standard deviations, i.e. $\frac{m^4}{2^{6n}} \leq \frac{m^2}{2^{\frac{5n}{2}}}$. This means we must have $m \simeq 2^{\frac{7n}{4}}$.

CPA-1 with $2^{\frac{3n}{2}}$ *messages.* The previous KPA can be transformed 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 $2^{\frac{n}{2}}.2^n = 2^{\frac{3n}{2}}$ possible inputs. We keep the same input and output conditions. Here $E(\mathcal{N}_{perm}) \simeq \frac{m^4}{4 \cdot 2^{4n}}$ 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 $E(\mathcal{N}_{scheme}) \simeq \frac{m^4}{4 \cdot 2^{4n}} + O(\frac{m^4}{4 \cdot 2^{5n}})$ and $\sigma(\mathcal{N}_{scheme}) = O(\frac{m^2}{2^{2n}})$. 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 $\frac{3n}{2}$ messages.

3.5 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. The complexities of our attacks are summarized in Table 2 (A-Feistel). We also mention the results for classical Feistel schemes (Ψ^d, see [15]). As said before we only give the results 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.

Remark 5: The attacks performed on classical Feistel schemes are 2-points attacks. These kind of attacks cannot be mounted in the case of A-Feistel schemes. There exist 4-points attacks on classical Feistel schemes for that achieve the same complexity as the attacks on $\Psi^{d_2} \circ \varphi \circ \Psi^{d_1}$ with $d_1 + d_2 = 4$ (see [14]).

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 schemes with several rounds, and finally an affine permutation. The attacks are very similar to the ones in section 3. We will give an overview of these attacks and provide the results. We give here 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 still suppose that A_3 and A_4 are bijective. We have the following values: $[L, R] \longrightarrow [P, Q] \longrightarrow [Q, X^1] \longrightarrow [X^1, X^2] \longrightarrow [S, T]$, with $P = A_1.L \oplus A_2.R \oplus c_1$, $Q = A_3.L \oplus A_4.R \oplus c_2$, $X^1 = P \oplus f_1(P)$, $X^2 = Q \oplus f_2(X^1)$, $S = A'_1.L \oplus A'_2.R \oplus c'_1$, $T = A'_3.L \oplus A'_4.R \oplus c'_2$.

Table 2. Complexities of attacks on A-Feistel with one affine permutation and on classical Feistel schemes Ψ^d.

Ψ^d

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	$2^{n/2}$
Ψ_2^5	$2^{3n/2}$	2^n
Ψ_2^6	2^{2n}	2^{2n}
$\Psi^d, d \geq 6$	$2^{(d-4)n}$	$2^{(d-4)n}$

A-Feistel

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

For the CPA-1, we choose only 2 values for L: L_1 and L_2. Then, we choose approximately 2^n values for R_i (i.e. almost all the possible values for R_i). Therefore we have $m \simeq 2.2^n$ messages. We count the number $\mathcal{N}$ of (R_i, R_j) values, $R_i \neq R_j$ such that with the 4 following message: $i : [L_1, R_i], \quad i' : [L_2, R_i] \quad j : [L_1, R_j], \quad j' : [L_2, R_j]$, 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: $E(\mathcal{N}_{perm}) \simeq \frac{m^2}{2.2^{2n}}$ and $E(\mathcal{N}_{scheme}) \simeq \frac{m^2}{2^{2n}}$. 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 transform into a KPA with $m \simeq 2^{\frac{3n}{2}}$. The results of our attacks (CPA-1 and KPA) are given in table 3. 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.

Table 3. 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}
$\varphi' \circ \Psi^d \circ \varphi, \ d \geq 4$	$2^{(2d-4)n}$	

Remark. 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 Conclusion

By [18, 19] we know that A-Feistel schemes are secure against linear and differential attacks In this paper, we provided attacks on A-Feistel schemes using 4-tuples of cleartext/ciphertext messages. Our results on A-Feistel schemes are given in Tables 2 and 3. The 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.

References

1. Eli Biham and Adi Shamir. Differential Cryptanalysis od DES-like Cryptosystems. In Alfred Menezes and Paulo Scott A. Vanstone, editors, *Advances in Cryptology – CRYPTO 1990*, volume 537 of *Lecture Notes in Computer Science*, pages 2–21. Springer-Verlag, 1991.
2. Eli Biham and Adi Shamir. Differential Cryptanalysis od DES-like Cryptosystems. *J. Cryptology*, 4(1):3–72, 1991.
3. Henri Gilbert and Marine Minier. New Results on the Pseudorandomness of Some Blockcipher Constructions. In Mitsuru Matsui, editor, *Fast Software Encrytion – FSE '01*, volume 2355 of *Lecture Notes in Computer Science*, pages 248–266. Springer-Verlag, 2001.
4. Paul G. Hoel, Sidney C. Port, and Charles J. Stone. *Introduction to Probability Theory.* Houghton Mifflin Company, 1971.
5. Charanjit S. Jutla. Generalized Birthday Attacks on Unbalanced Feistel Networks. In Hugo Krawczyk, editor, *Advances in Cryptology – CRYPTO '98*, volume 1462 of *Lecture Notes in Computer Science*, pages 186–199. Springer-Verlag, 1998.
6. Lars R. Knudsen. DEAL - A 128-bit Block Cipher. Technical Report 151, University of Bergen, Department of Informatics, Norway, february 1998.
7. Michael Luby and Charles Rackoff. How to Construct Pseudorandom Permutations from Pseudorandom Functions. *SIAM J. Comput.*, 17(2):373–386, 1988.
8. Stefan Lucks. Faster Luby-Rackoff Ciphers. In Dieter Gollman, editor, *Fast Software Encryption – FSE '96*, volume 1039 of *Lecture Notes in Computer Science*, pages 189–203. Springer-Verlag, 1996.
9. Mitsuru Matsui. Linear Cryptanalysis Methods for DES Cipher. In Gerahard Goos and Juris Hartmanis, editors, *Advances in Cryptology – EUROCRYPT 1993*, volume 765 of *Lecture Notes in Computer Science*, pages 386–397. Springer-Verlag, 1994.
10. Mitsuru Matsui. The First Experimental Cryptanalysis of the Data Encryption Standard. In Gerahard Goos and Juris Hartmanis, editors, *Advances in Cryptology – CRYPTO 1994*, volume 869 of *Lecture Notes in Computer Science*, pages 1–11. Springer-Verlag, 1994.

11. Valérie Nachef, Jacques Patarin, and Joana Treger. Generic Attacks on Misty Schemes. In Michel Abdalla and Paulo S.L.M. Barretol, editors, *Progress in Cryptology – LATINCRYPT 2010*, volume 6212 of *Lecture Notes in Computer Science*, pages 222–240. Springer-Verlag, 2010.
12. Valérie Nachef, Emmanuel Volte, and Jacques Patarin. Differential Attacks on Generalized Feistel schemes. In Michel Abdalla, Cristina Nita-Rotaru, and Ricardo Dahab, editors, *CANS 2013*, volume 8257 of *Lecture Notes in Computer Science*, pages 1–19. Springer-Verlag, 2013.
13. Moni Naor and Omer Reingold. On the Construction of Pseudorandom Permutations: Luby-Rackoff Revisited. *J. Cryptology*, 12(1):29–66, 1999.
14. Jacques Patarin. Generic Attacks on Feistel Schemes. In Colin Boyd, editor, *Advances in Cryptology – ASIACRYPT 2001*, volume 2248 of *Lecture Notes in Computer Science*, pages 222–238. Springer-Verlag, 2001.
15. Jacques Patarin, Valérie Nachef, and Côme Berbain. Generic Attacks on Unbalanced Feistel Schemes with Contracting Functions. In Xuejia Lai and Kefei Chen, editors, *Advances in Cryptology – ASIACRYPT 2006*, volume 4284 of *Lecture Notes in Computer Science*, pages 396–411. Springer-Verlag, 2006.
16. Bruce Schneier and John Kelsey. Unbalanced Feistel Networks and Block Cipher Design. In Dieter Gollmann, editor, *Fast Software Encrytion – FSE '96*, volume 1039 of *Lecture Notes in Computer Science*, pages 121–144. Springer-Verlag, 1996.
17. Joana Treger and Jacques Patarin. Generic Attacks on Feistel Networks with Internal Permutations. In Bart Preneel, editor, *Progresses in Cryptology – AFRICACRYPT '09*, Lecture Notes in Computer Science. Springer-Verlag, 2009.
18. Serge Vaudenay. Provable Security for Block Ciphers by Decorralation. In Michel Movan, Chritoph Meinel, and Daniel Krob, editors, *STACS 1998*, volume 1373 of *Lecture Notes in Computer Science*, pages 249–265. Springer-Verlag, 1998.
19. Serge Vaudenay. Decorrelation: A theory for block cipher security. *J. Cryptology*, 16(4):249–286, 2003.
20. Emmanuel Volte, Valérie Nachef, and Jacques Patarin. Improved Generic Attacks on Unbalanced Feistel Schemes with Expanding Functions. In Masayuki Abe, editor, *Advances in Cryptology – ASIACRYPT 2010*, 2010.

A Computation of the mean value and the variance for a random permutation (attack on $\Psi^3 \circ \varphi$)

In this section, we compute the mean value and the standard deviation for a random permutation. For $1 \leq i \leq m$, we choose randomly in $\{0,1\}^n$, and with a uniform distribution, variables L_i, R_i and S_i. Then we want to compute then number $\mathcal{N}_{perm}$ of (i,j,k,ℓ) such that $i \leq j$, $i \leq k$ and $i \leq \ell$ and

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

We introduce the following random variables:

$$\begin{cases} \delta_{ijk\ell} = 1 \qquad \Leftrightarrow & \begin{cases} L_i = L_j \\ L_k = L_\ell \neq L_i \\ R_i = R_k \\ R_j = R_\ell \neq R_i \end{cases} \text{and } S_i \oplus S_j \oplus S_k \oplus S_\ell = 0 \\ \delta_{ijk\ell} = 0 \text{ otherwise} \end{cases}$$

Let $D = \{(i,j,k,\ell)$ pairwise distinct, $i < j,\ i < k,\ i < \ell\}$. Then we have: $\mathcal{N}_{perm} = \sum_{(i,j,k,\ell)\in D} \delta_{ijk\ell}$.

A.1 Computation of the mean value

Since we have permutations, we assume that the inputs and the outputs are pairwise distinct. We compute $E(\delta_{ijk\ell})$. For $[L_i, R_i]$, there are 2^{2n} possibilities. For $[L_j, R_j]$, there are $(2^n - 1)$ possibilities since L_j is fixed and $R_j \neq R_i$. Now we have $L_k \neq L_i$ and R_k is fixed. Thus there are $(2^n - 1)$ possibilities for $[L_k, R_k]$ and then $[L_\ell, T_\ell]$ is fixed. The numbers of inputs satisfying the conditions is $2^{2n}.(2^n - 1)^2$. We count the number of distinct outputs $[S_i, T_i], [S_j, T_j], [S_k, T_k]$ and $[S_\ell, T_\ell]$ such that $S_i \oplus S_j \oplus S_k \oplus S_\ell = 0$. There are different cases:
Case 1: $S_i = S_j = S_k = S_\ell$. Then T_i, T_j, T_k, T_ℓ are pairwise distinct. There are $2^{2n}.(2^n - 1).(2^n - 2).(2^n - 3)$ possibilities for the outputs.
Case 2: Equalities of the form $S_i = S_j$ and $S_k = S_\ell \neq S_i$. We can also have $S_i = S_k$ and $S_j = S_\ell \neq S_i$ or $S_i = S_\ell$ and $S_j = S_k \neq S_i$. The number of possible pairwise distinct outputs is given by $3 \times 2^{2n}(2^n - 1)(2^n - 1)2^n.(2^n - 1) = 3 \times 2^{3n}(2^n - 1)^3$.
Case 3: S_i, S_j, S_k and S_ℓ are pairwise distinct. Here the numbers of outputs is equal to $2^{2n}(2^n - 1)2^n(2^n - 2)2^n 2^n = 2^{5n}(2^n - 1)(2^n - 2)$.
The total numbers of possible distinct inputs and outputs is given by $[2^{2n}(2^{2n} - 1)(2^{2n} - 2)(2^{2n} - 3)]^2$. Thus we obtain:

$$E(\delta_{ijk\ell}) = \frac{2^{4n}(2^n - 3)^3(2^{4n} + 2^{3n} - 5 \times 2^{2n} - 2 \times 2^n + 6)}{[2^{2n}(2^{2n} - 1)(2^{2n} - 2)(2^{2n} - 3)]^2} =$$

$$\frac{1}{2^{5n}}(1 - \frac{2}{2^n} + \frac{7}{2^{2n}} - \frac{9}{2^{3n}} + \frac{22}{2^{4n}} + O(\frac{1}{2^{5n}}))$$

This gives: $E(\mathcal{N}_{perm}) \simeq \frac{m(m-1)(m-2)(m-3)}{4 \cdot 2^{5n}}(1 - \frac{2}{2^n} + \frac{7}{2^{2n}} - \frac{9}{2^{3n}} + \frac{22}{2^{4n}} + O(\frac{1}{2^{5n}}))$.

A.2 Computation of the variance

We now compute the variance of $\mathcal{N}_{perm}$. Let $D = \{(i,j,k,\ell)$ pairwise distinct, $i < j,\ i < k,\ i < \ell\}$. We apply the covariance formula:

$$V(\mathcal{N}_{perm}) = \sum_{(i,j,k,\ell)\in D} V(\delta_{ijk\ell}) + \sum_{\substack{(i,j,k,\ell)\in D \\ (p,q,r,s)\in D \\ (i,j,k,\ell)\neq(p,q,r,s)}} [E(\delta_{ijk\ell}\delta_{pqrs}) - E(\delta_{ijk\ell})E(\delta_{pqrs})]$$

We have $V(\delta_{ijk\ell}) = E(\delta_{ijk\ell}) - (E(\delta_{ijk\ell}))^2$. We have to study the term second part of the formula. First $E(\delta_{ijk\ell})E(\delta_{pqrs}) = \frac{1}{2^{10n}}(1 - \frac{4}{2^n} + \frac{18}{2^{2n}} - \frac{46}{2^{3n}} + \frac{129}{2^{4n}} + O(\frac{1}{2^{5n}}))$. Then we compute $E(\delta_{ijk\ell}\delta_{pqrs})$. There are several cases.
Case 1. In $\{i, j, k, \ell, p, q, r, s\}$, there are 8 pairwise distinct values. First, we study the different possibilities for the inputs. We have the following conditions:

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

There are several sub-cases.

1. Equalities of the form:

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

   There are 4 possibilities for this kind of equalities. The number of inputs satisfying these conditions is: $2^{2n}(2_n - 1)^2(2^n - 2)(2^n - 3)$.
2. Equalities of the form:

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

   There are 8 possibilities for this kind of equalities. The number of inputs satisfying these conditions is: $2^{2n}(2^n - 1)^2(2^n - 2)^2(2^n - 3)$.
3. There is no relations between the inputs indexed by i, j, k, ℓ and the inputs indexed by p, q, r, s. In that case, the number of inputs is $2^{2n}(2^n - 1)^2(2^n - 2)^2(2^n - 3)^2$.

Finally, the total number of inputs in given by: $2^{2n}(2^n - 1)^2(2^n - 2)(2^n - 3)(2^{2n} + 3 \times 2^n - 6)$.

We now study the conditions on the outputs:

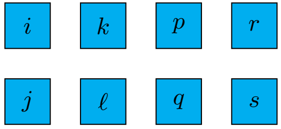
$$S_i \oplus S_j \oplus S_k \oplus S_\ell = 0,\ S_p \oplus S_q \oplus S_r \oplus S_s = 0$$

We have to consider several possibilities:

1. Relations of the form $S_i \oplus S_j = S_k \oplus S_\ell = S_p \oplus S_q = S_r \oplus S_s$. There are 9 ways to obtain such relations.

   When we have these conditions, several sub-cases appear. We represent in Figure 1 the indices $i, j, k, \ell, p, q, r, s$ in order to explain the relations that may appear between the outputs.

   Fig. 1. Representation of the indices

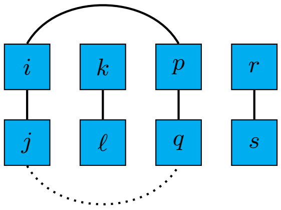
   

   (a) $S_i = S_j = S_k = S_\ell = S_p = S_q = S_r = S_s$. There are $2^{2n}(2^n - 1)(2^n - 2)(2^n - 3)(2^n - 4)(2^n - 5)(2^n - 6)(2^n - 7)$ outputs satisfying these conditions.

   (b) As represented in Figure 2, we may have 4 vertical equalities and one horizontal equality which implies another horizontal equality (dotted line):

   There are 6 ways to obtain these relations. The number of outputs is given by $6 \times 2^{4n}(2^n - 1)^4(2n - 2)^2(2^n - 3)$

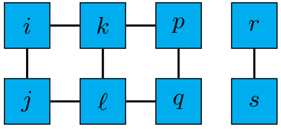
Fig. 2. 4 vertical equalities and one horizontal equality



(c) We only have vertical equalities. The number of outputs is: $2^{5n}(2^n - 1)^5(2^n - 2)(2^n - 3)$.

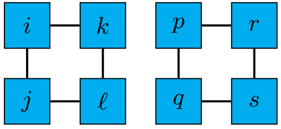
(d) As shown in Figure 3, we may have 4 vertical equalities and 4 horizontal equalities. There are 4 ways to get this kind of relations. The number of outputs is: $4 \times 2^{3n}(2^n - 1)^3(2^n - 2)(2^n - 3)(2^n - 4)(2^n - 5)$.

Fig. 3. 4 vertical equalities and 4 horizontal equalities



(e) Another possibility is to have two distinct groups with two vertical and horizontal equalities as shown in Figure 4. There are 6 such combinations. The number of outputs is $6 \times 2^{3n}(2^n - 2)^3(2^n - 2)^2(2^n - 3)^2$.

Fig. 4. Two distinct groups with two vertical and horizontal equalities



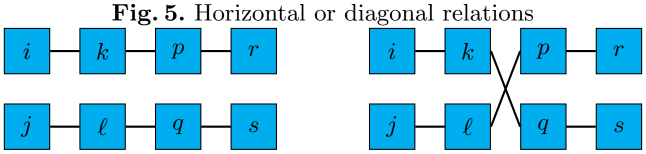
(f) Here we only have horizontal or diagonal relations as shown below (Figure 5). There are 8 possibilities. Then the number of outputs is given by: $8 \times 2^{3n}(2^n - 2)^3(2^n - 2)^2(2^n - 3)^2$.

(g) We have two horizontal or diagonal equalities. There are 16 possibilities and the number of out puts is $16 \times 2^{5n}(2^n - 5)^3(2^n - 2)^3$.

(h) We only have one horizontal or diagonal relation. There are 12 possibilities and the number of outputs is $12 \times 2^{7n}(2^n - 1)^3(2^n - 2)(2^n - 4)$.

(i) We do not have any relation. The number of outputs is given by $2^{9n}(2^n - 1)(2^n - 2)(2^n - 4)(2^n - 6)$.

Fig. 5. Horizontal or diagonal relations



2. No relations of the form $S_i \oplus S_j = S_p \oplus S_q$. Again we need to consider several sub-cases.
   (a) We have $S_i = S_j = S_k = S_\ell$ and S_p, S_q, S_r, S_s are pairwise distinct. We may also exchange the roles of the indices. First there is a link between the blocks of indices (i, j, k, ℓ) and (p, q, r, s). For example, we have $S_i = S_j = S_k = S_\ell = S_p$. There are 4 possible links. Or there is no link between the blocks. The number of outputs is given by $8 \times 2^{5n}(2^n - 1)^2(2^n - 2)^2(2^n - 3)(2^n - 4) + 2 \times 2^{6n}(2^n - 1)^2(2^n - 2)^2(2^n - 3)(2^n - 4)$.
   (b) We have for example $S_i = S_j$ and $S_k = S_\ell \neq S_i$ and S_p, S_q, S_r, S_s are pairwise distinct. Again we may have a link between the two blocks of indices or we may have no link. There are three ways to choose the relations between S_i, S_j, S_k and S_l and we can also exchange the roles of the indices. The number of outputs is given by $48 \times 2^{6n}(2^n - 1)^3(2^n - 2)^2(2^n - 4) + 6 \times 2^{7n}(2^n - 1)^3(2^n - 2)(2^n - 3)(2^n - 4)(2^n - 8)$.
   (c) S_i, S_j, S_k, S_ℓ and S_p, S_q, S_r, S_s are pairwise distinct and we may have or not a link between the blocks of indices. We obtain here $16 \times 2^{8n}(2^n - 1)^2(2^n - 2)(2^n - 4)(2^n - 8) + 2^{9n}(2^n - 1)(2^n - 2)(2^n - 4)(2^n - 8)(2^n - 16)$.

We now multiply the number of inputs and outputs we have obtained and we divide by the total number of pairwise distinct inputs and outputs and finally we get:

$$E(\delta_{ijk\ell}\delta_{pqrs}) = \frac{1}{2^{10n}}(1 - \frac{4}{2^n} + \frac{48}{2^{2n}} - \frac{346}{2^{3n}} + \frac{1265}{2^{4n}} + O(\frac{1}{2^{5n}}))$$

Thus in $E(\delta_{ijk\ell}\delta_{pqrs}) - E(\delta_{ijk\ell})E(\delta_{pqrs})$, the dominant term is in $O(\frac{1}{2^{12n}})$ and when $m \simeq 2^{\frac{7n}{4}}$, we will have $\frac{m^4}{2^{5n}} \simeq \frac{m^8}{2^{12n}}$.

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:

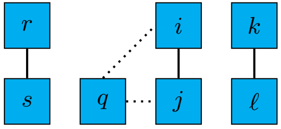
$$\begin{cases} L_i = L_j = L_q,\ R_i = R_k = R_r,\ S_i \oplus S_j \oplus S_k \oplus S_\ell = 0 \\ L_k = L_\ell \neq L_i,\ R_j = R_\ell \neq R_i,\ S_i \oplus S_q \oplus S_r \oplus S_s = 0 \\ L_r = L_s \neq L_i,\ R_q = R_s \neq R_i, \end{cases}$$

The number of inputs is given by $2^{3n}(2^n - 1)^2(2^n - 2)$.
There are several cases for the outputs.

1. We have relations of the type $S_i \oplus S_j = S_k \oplus S_\ell = S_i \oplus S_q = S_r \oplus S_s$. Thus is equivalent to $S_j = S_q$ and $S_i \oplus S_j = S_k \oplus S_\ell = S_r \oplus S_s$. There 9 possibilities to get this type of relations. Again, we have to consider several sub-cases.

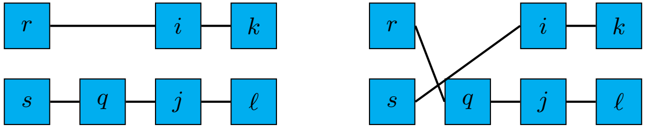
   (a) We have $S_i = S_i = S_k = S_\ell = S_q = S_r = S_s$. The number of outputs is $2^{2n}(2^n-1)(2^n-2)(2^n-3)(2^n-4)(2^n-5)(2^n-5)$.
   (b) We suppose we have vertical equalities. This will imply the dotted equalities (see Figure 6). Here we consider that we have 3 different blocks and we study the possible links between the blocks. We can either one link or no link. We notice that if we have two links, then the values are equal. There are 2 cases where we have the link between a vertical line and a triangle and on case where we have a link between two vertical lines. The number of outputs is given by $2 \times 2^{3n}(2^n-1)^3(2^n-2)(2^n-3)(2^n-4) + 2^{3n}(2^n-1)^3(2^n-2)^2(3^n-3)$. We may also have no link between the blocks and in that case the number of outputs is $2^{4n}(2^n-1)^4(2^n-2)^2$.

Fig. 6. Vertical equalities



   (c) We now suppose that we do not have vertical equalities and we study the possibility to horizontal or diagonal links. First we can have two horizontal or diagonal equalities as shown in Figure 7. There are 4 possibilities of equalities and the number of outputs is given by $4 \times 2^{3n}(2^n-1)^3(2^n-2)^2(2^n-4)$.

Fig. 7. Two horizontal or diagonal equalities



   (d) We may also have one horizontal or diagonal equality. There are $2 \times 2^{5n}(2^n-1)^3(2^n-2)^2 + 2^{5n}(2^n-1)^4(2^n-2)$ possible outputs.
   (e) There are no equalities. This gives $2^{7n}(2^n-1)^2(2^n-2)(2^n-4)$ outputs.

2. We do not have any relations of the type $S_i \oplus S_j = S_k \oplus S_\ell = S_i \oplus S_q = S_r \oplus S_s$. Again, we consider the 2 blocks of indices (i, j, k, ℓ) and (i, q, r, s) and we proceed as in the case where we had 8 different indices. The number of outputs is given by $2 \times 2^{5n}(2^n-1)^2(2^n-2)^2(2^n-3) + 6 \times 2^{6n}(2^n-1)^3(2^n-2)(2^n-4) + 2^{8n}(2^n-1)(2^n-2)(2^n-4)(2^n-8)$.

We now multiply the number of inputs and outputs we have obtained and we divide by the total number of pairwise distinct inputs and outputs and finally we get:

$$E(\delta_{ijk\ell}\delta_{pqrs}) = \frac{1}{2^{10n}}(1 - \frac{4}{2^n} + \frac{36}{2^{2n}} - \frac{62}{2^{3n}} - \frac{128}{2^{4n}} + O(\frac{1}{2^{5n}}))$$

Thus in $E(\delta_{ijk\ell}\delta_{pqrs}) - E(\delta_{ijk\ell})E(\delta_{pqrs})$, the dominant term is in $O(\frac{1}{2^{12n}})$. We have $\frac{m^7}{2^{12n}} \ll \frac{m^4}{2^{5n}}$.

Case 3. In $\{i, j, k, \ell, p, q, r, s\}$, there are 6 pairwise distinct values. Due to the conditions on the inputs, there are relations between the indices that are not allowed. For example, it is not possible to have $i = q$ and $j = r$ since this implies that $L_i = L_s$ and $R_i = R_s$. This is not possible since the inputs are pairwise distinct and $i \neq s$. We examined all the possible combinations and it turns out that there is 16 possibilities to choose the relation between the two 4-tuples of indices (i, j, k, ℓ) and (p, q, r, s). We have to link either vertical relations or horizontal relations but no diagonal relations. For example, we suppose that $i = p$ and $j = q$. Then we have the conditions:

$$\begin{array}{ll} L_i = L_j, & R_i = R_k = R_r, \\ L_k = L_\ell \neq L_i, & R_j = R_\ell = R_s \neq R_i, \\ L_r = L_s, & S_i \oplus S_j = S_k \oplus S_\ell = Sr \oplus S_s, \end{array}$$

The number of inputs is given by $2^{2n}(2^n - 1)^2(2^n - 2)$. In order to compute the number of outputs, we proceed as in the cases with 8 or 7 indices. We consider the different kind of equalities that may occur between $S_i, S_j, S_k, S_\ell, S_r, S_s$. We obtain that the number of outputs is given by

$$2^{2n}(2^n - 1)(2^n - 2)(2^n - 3)(2^n - 4) + 3 \times 2^{3n}(2^n - 1)^2(2^n - 2)^2(2^n - 3)+$$

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

We now multiply the number of inputs and outputs we have obtained and we divide by the total number of pairwise distinct inputs and outputs and finally we get:

$$E(\delta_{ijk\ell}\delta_{pqrs}) = \frac{1}{2^{9n}}(1 - \frac{4}{2^n} + \frac{14}{2^{2n}} - \frac{1}{2^{3n}} - \frac{162}{2^{4n}} + O(\frac{1}{2^{5n}}))$$

Thus in $E(\delta_{ijk\ell}\delta_{pqrs}) - E(\delta_{ijk\ell})E(\delta_{pqrs})$, the dominant term is in $O(\frac{1}{2^{9n}})$. We have $\frac{m^6}{2^{9n}} \ll \frac{m^4}{2^{5n}}$ since $m \ll 2^{2n}$ in this attack.

The conditions on the inputs do not allow to have 5 pairwise distinct indices in $\{i, j, k, \ell, p, q, r, s\}$.

The previous computations show that $V(\mathcal{N}_{perm}) = O(\frac{m^4}{2^{5n}}) + O(\frac{m^6}{2^{9n}})$ It is easy to check that the dominant term is $\frac{m^4}{2^{5n}}$ as soon as $m \leq 2^{2n}$ and then we obtain that $\sigma(\mathcal{N}_{perm}) \simeq \frac{m^2}{2^{\frac{5n}{2}}}$.

Remark 1: It is very important to notice that the variance does not always behave like the mean value. In the previous computation, if we do not include the condition on S, but we only keep the conditions on L and R, we obtain

$$E(\mathcal{N}_{perm}) \simeq \frac{m(m-1)(m-2)(m-3)}{4 \cdot 2^{4n}} \text{ and } V(\mathcal{N}_{perm}) = O(\frac{m^6}{2^{7n}}) + O(\frac{m^4}{2^{4n}})$$

Here when $m \geq 2^{\frac{3n}{2}}$, the dominant term in $V(\mathcal{N}_{perm})$ is $\frac{m^6}{2^{7n}}$ and not $\frac{m^4}{2^{4n}}$.

B 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 an A-Feistel 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 still want to have:

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

B.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 $S_i \oplus S_j \oplus S_k \oplus S_\ell = 0 \Leftrightarrow f_2(X_i^1) \oplus f_2(X_j^1) \oplus f_2(X_k^1) \oplus f_2(X_\ell^1)$ $(*)$. Thus this may happen at random, or due to conditions satisfied by internal variables.

A_3 and A_4 are bijective 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 bijective. We want to have $f_2(X_j^1) \oplus f_2(X_k^1) \oplus f_2(X_\ell^1) = 0$. 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 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 bijective, the only possibility is $Q_i = Q_\ell \Leftrightarrow Q_j = Q_k$. This happens with probability $\frac{1}{2^n}$. This implies $X_i^1 \oplus X_j^1 \oplus X_k^1 \oplus X_\ell^1 = 0$. The we may have $X_i^1 = X_k^1 \Leftrightarrow X_k^1 = X_\ell^1$. 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 $f_2(X_i^1) \oplus f_2(X_j^1) \oplus f_2(X_k^1) \oplus f_2(X_\ell^1)$. 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 $3 \times (1 - \frac{1}{2^n}) \times \frac{1}{2^{2n}}$.

3. We are not in the previous case and we have the $(*)$. Here the probability is $(1 - \frac{2}{2^{2n}} - 3(1 - \frac{1}{2^n})\frac{1}{2^{2n}})\frac{1}{2^n} = \frac{1}{2^n} - \frac{5}{2^{3n}} - \frac{3}{2^{4n}}$.

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 consider the conditions on the inputs. The probability that the inputs satisfy the conditions is $\frac{1}{2^{4n}}(1 - \frac{2}{2^n} + \frac{13}{2^{2n}} - \frac{24}{2^{3n}} + \frac{98}{2^{4n}} + O(\frac{1}{2^{5n}})$. Thus we get $E(\delta_{ijk\ell}) = \frac{1}{2^{5n}}(1 + \frac{3}{2^n} - \frac{5}{2^{2n}} + O(\frac{1}{2^{3n}}))$ and $E(\mathcal{N}_{scheme}) \simeq \frac{m(m-1)(m-2)(m-3)}{4 \cdot 2^{5n}}(1 + \frac{3}{2^n} - \frac{5}{2^{2n}} + O(\frac{1}{2^{3n}}))$.

***A_3* is bijective and *A_4* is not bijective.** The case where A_3 in not bijective and A_4 is bijective is similar. If A_4 is not bijective, 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 $E(\delta_{ijk\ell}) = \frac{1}{2^{5n}}(1 + \frac{2}{2^{n-t}} + \frac{3}{2^n} + O(\frac{1}{2^{2n-t}}))$ and $E(\mathcal{N}_{scheme}) \simeq \frac{m(m-1)(m-2)(m-3)}{4 \cdot 2^{5n}}(1 + \frac{2}{2^{n-t}} + \frac{3}{2^n} + O(\frac{1}{2^{2n-t}}))$. 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 that the attack in the case where A_3 and A_4 are bijective.

***A_3* and *A_4* are not bijective.** Since A_3 is not bijective, 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 $E(\delta_{ijk\ell}) = \frac{1}{2^{5n}}(1 + \frac{2}{2^{n-t}} + \frac{2}{2^{n-t'}} + \frac{3}{2^n} + O(\frac{1}{2^{2n-\max(t',t)}}))$ and $E(\mathcal{N}_{scheme}) \simeq \frac{m(m-1)(m-2)(m-3)}{4 \cdot 2^{5n}}(1 + \frac{2}{2^{n-t}} + \frac{2}{2^{n-t'}} + \frac{3}{2^n} + O(\frac{1}{2^{2n-\max(t,t')}}))$. The difference of the mean values (for a random permutation and for a scheme) is $\min(\frac{2}{2^{n-t}}, \frac{2}{2^{n-t'}})$.

B.2 Computation of the variance

***A_3* and *A_4* are bijective** Here $E(\delta_{ijk\ell})E(\delta_{pqrs}) = \frac{1}{2^{10n}}(1 + \frac{6}{2^n} - \frac{1}{2^{2n}} + O(\frac{1}{2^{3n}}))$. Now, in order to compute the variance, the main issue is to know the value of $E(\delta_{ijk\ell}\delta_{pqrs})$. 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 $E(\delta_{ijk\ell}\delta_{pqrs}) - E(\delta_{ijk\ell})E(\delta_{pqrs})$ to be smaller than $\frac{m^4}{2^{5n}}$. 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 $E(\delta_{ijk\ell}\delta_{pqrs}) - E(\delta_{ijk\ell})E(\delta_{pqrs})$.
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 $E(\delta_{ijk\ell}\delta_{pqrs})$. 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

$$f_2(X_i^1) \oplus f_2(X_j^1) \oplus f_2(X_k^1) \oplus f_2(X_\ell^1) = 0 \; (5)$$
$$f_2(X_p^1) \oplus f_2(X_q^1) \oplus f_2(X_r^1) \oplus f_2(X_s^1) = 0 \; (6)$$

In order to get the first two terms of $E(\delta_{ijk\ell}\delta_{pqrs})$, 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 $\frac{2}{2^{2n}}(1 - \frac{5}{2^{2n}} - \frac{3}{2^{3n}})\frac{1}{2^n}$. Since there is also a symmetry in i, j, k, ℓ and p, q, r, s, we obtain $\frac{4}{2^{3n}}(1 - \frac{5}{2^{2n}} - \frac{3}{2^{3n}})$.
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 $\frac{6}{2^{3n}}(1-\frac{1}{2^n})(1-\frac{5}{2^{2n}}-\frac{3}{2^{3n}})$.
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 $(1 - \frac{10}{2^{3n}} - \frac{50}{2^{5n}} + \frac{18}{2^{7n}})^2 \frac{1}{2^{2n}}$.

Thus the probability to get (5) and (6) is $\frac{1}{2^{2n}}(1 + \frac{10}{2^n} - \frac{60}{2^{3n}} + O(\frac{1}{2^{4n}}))$. In order to compute the mean value, we have consider the conditions on the inputs. The probability on the inputs 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: $\frac{1}{2^{2n}}(1-\frac{4}{2^n}+\frac{18}{2^{2n}}-\frac{36}{2^{3n}}+0(\frac{1}{2^{4n}}))$ Thus we get $E(\delta_{ijk\ell}\delta_{pqrs}) = \frac{1}{2^{10n}}(1 + \frac{6}{2^n} - \frac{22}{2^{2n}} + O(\frac{1}{2^{3n}}))$. In that case, the dominant term in $E(\delta_{ijk\ell}\delta_{pqrs}) - E(\delta_{ijk\ell})E(\delta_{pqrs})$, is in $O(\frac{1}{2^{12n}})$ 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 $V(\delta_{ijk\ell}) = O(\frac{1}{2^{5n}})$.

Remark 1: 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 two first 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 $(X_i^1, X_j^1, X_k^1, X_\ell^1) = (X_p^1, X_q^1, X_r^1, X_s^1)$.

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:

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

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 $E(\delta_{ijk\ell}\delta_{pqrs}) - E(\delta_{ijk\ell})E(\delta_{pqrs})$. 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 $E(\delta_{ijk\ell}\delta_{pqrs}) - E(\delta_{ijk\ell})E(\delta_{pqrs})$, is in $O(\frac{1}{2^{11n}})$ and $V(\delta_{ijk\ell}) = O(\frac{1}{2^{5n}})$.

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

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

***A_3* is bijective and *A_4* is not bijective.** Here we are interested in obtaining the first three terms of $E(\delta_{ijk\ell}\delta_{pqrs})$, 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 $E(\delta_{ijk\ell}\delta_{pqrs}) - E(\delta_{ijk\ell})E(\delta_{pqrs})$ is in $O(\frac{1}{2^{12n-2t}})$. 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 deviation. 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 bijective. 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 $\frac{1}{2^{2n}}(1 + \frac{4}{2^{n-t}} + \frac{10}{2^n} + O(\frac{1}{2^{2n-2t}}))$. In order to compute the mean value, we have consider the conditions on the inputs. We obtain $E(\delta_{ijk\ell}\delta_{pqrs}) = \frac{1}{2^{10n}}(1 + \frac{4}{2^{n-t}} + \frac{6}{2^n} + O(\frac{1}{2^{2n-2t}}))$. In that case, the dominant term in $E(\delta_{ijk\ell}\delta_{pqrs}) - E(\delta_{ijk\ell})E(\delta_{pqrs})$, is in $O(\frac{1}{2^{12n-2t}})$ and when $m \simeq 2^{\frac{7n-2t}{4}}$, 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 $V(\mathcal{N}_{scheme} = O(\frac{m^4}{2^{5n}})$. 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 bijective.** 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 $E(\delta_{ijk\ell}\delta_{pqrs}) = \frac{1}{2^{10n}}(1 + \frac{4}{2^{n-t}} + \frac{4}{2^{n-t'}} + \frac{6}{2^n} + O(\min(\frac{1}{2^{2n-2t}}, \frac{1}{2^{2n-2t'}})))$. 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.

C The signature of A-Feistel schemes is even

We want to compute the signature of A-Feistel schemes. We already know that classical Feistel schemes and unbalanced Feistel schemes with contracting functions have even signature [14, 15]. Thus we just have to study the signature of any affine permutation from $\{0, 1\}^N$ to $\{0, 1\}^N$. Affine functions are of the form $M \to A.M + C$ where $A \in GL(N, K)$.

For all $i \neq j$ we define $T_{ij,\lambda}$ to be the matrix with 1 on the diagonal and 0 elsewhere except in (i,j) where the coefficient is equal to $\lambda \in K$. Such matrices are called transvection matrices and generate $SL(N,K)$. When $\lambda = 1$, we just write T_{ij}.

If we want to generate $GL(N,K)$ we have to add the dilation matrices $D_{i,\lambda}$ with a 1 on the diagonal except in (i,i) where the coefficient is equal to $\lambda \in K^*$.

In the special case where $K = \mathbb{Z}/2\mathbb{Z}$, we have $SL(N,\mathbb{Z}/2\mathbb{Z}) = GL(N,\mathbb{Z}/2\mathbb{Z})$. So, $GL(N,\mathbb{Z}/2\mathbb{Z})$ is generated by the matrices T_{ij} and we have $T_{ij}^{-1} = T_{ij}$ for all $i \neq j$.

We want to show that the signature of A is even. It is enough to show that transvections have an even signature. Let T_{ij} be a transvection and $M \in \{0,1\}^N$, with $M = (M_1, \ldots, M_N)$ and $M_i \in \{0,1\}$. We set $\tilde{M} = T_{ij}(M)$. Then we have: $\tilde{M}_\ell = \sum_{k=1}^{N} t_{\ell k} M_k$. Since $t_{\ell k} = 1$ if $\ell = k$ or $(\ell,k) = (i,j)$ and 0 otherwise, we get: $\tilde{M}_\ell = M_\ell$ if $\ell \neq i$ and $\tilde{M}_i = M_j \oplus M_i$.

If $M_j = 0$, then $\tilde{M} = M$. If $M_j = 1$, then $A.M = \tilde{M} \Leftrightarrow A.\tilde{M} = M$. This means that in A, we have 2^{N-2} transpositions and the signature of A is even.

If we consider the function from $\{0,1\}^N$ to $\{0,1\}^N$ defined by $M \to M \oplus C$, then there are $\frac{2^N}{2} = 2^{N-1}$ transpositions. Thus the signature is even for $N \geq 3$. Finally the signature of an affine permutation is even.

The computations made previously and the results on Feistel schemes show that an A-Feistel scheme ($N = 2n$) and A-Unbalanced Feistel schemes with contracting functions ($N = kn$) have an even signature.
The consequence is that it is possible to distinguish a generator of Φ^d permutations (respectively $\mathcal{G}_k^d$ permutations from a generator of truly random permutations from $2n$ bits to $2n$ bits respectively kn bits to kn bits) after $O(2^{2n})$ (respectively $O(2^{kn})$) computations on $O(2^{2n})$ (respectively $O(2^{kn})$) input/output values.