Generic Attacks on Feistel Networks With Internal Permutations

Joana Treger, Jacques Patarin

PRiSM, Université de Versailles

2008-03-21

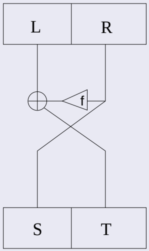
Summary

Plan

Definitions

Let B_n *be the permutation set of* $[1, 2^n]$*,* $f \in B_n$ *and* $L, R, S, T \in [1, 2^n]$*. A 1-round Feistel network with internal permutation is the permutation* $\psi(f)$ *(or* ψ*) :*

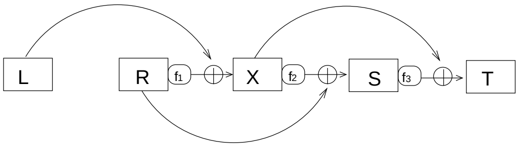
$$\psi([L, R]) = [R, L \oplus f(R)] = [S, T]$$



A k-round Feistel network with internal permutations :
$\psi^k(f_1, \ldots, f_k) := \psi(f_k) \circ \ldots \circ \psi(f_1)$

Motivation

- Feistel networks widely used
- Little work done on Feistel networks with round permutations ([Knudsen-02] : attack on 5 rounds, [Piret-05] : security proofs for 3 and 4 rounds).
- These networks have been used to design some symmetric ciphers (DEAL, Camellia,...).
- Different behavior of these Feistel networks and the classical ones. Example (3 rounds) :



$R_1 \oplus S_1 = R_2 \oplus S_2$ with probability :

- $1/2^n$: random permutation
- $2/2^n$: Feistel network with internal functions
- $1/2^n$: Feistel network with internal permutations

Generic attacks

Definition

A **generic attack** *on a Feistel network with internal permutations, is an attack allowing to distinguish, with high probability, a Feistel network from a random permutation when the round permutations are randomly chosen.*

- We interest ourselves in generic attacks, working with complexity $< \mathcal{O}(2^{2n})$ (exhaustive search on the inputs).
- When the complexity is $\geq \mathcal{O}(2^{2n})$, we interest ourselves in attacks on Feistel permutation generators.
- We consider attacks using correlations between pairs of messages.

Plan

Chebyshev formula

Theorem (Chebyshev formula)

Let X be a random variable and $\alpha \in \mathbb{R}_+^*$. Then :

$$P\{|X - E(X)| \geq \alpha \cdot \sigma(X)\} \leq \frac{1}{\alpha^2}$$

Let us consider m messages and the random variables :

- X_p counts the number of pairs of these messages verifying some equations on the inputs and outputs when they correspond to a random permutation
- X_{ψ^k} counts the same number for a k-round Feistel network with internal permutation.

We distinguish with high probability ψ^k from a random permutation if $|E(X_{\psi^k}) - E(X_p)| > \sigma(X_{\psi^k}) + \sigma(X_p)$

H-coefficient

Definition

$[L_1, R_1] \neq [L_2, R_2]$ *and* $[S_1, T_1] \neq [S_2, T_2] \ \in [1, 2^{2n}]$. *The* ***H*-coefficient** *for that case computes the number of* $(f_1, \ldots, f_k) \in B_n^k$, *such that* $\psi^k(f_1, \ldots, f_k)([L_i, R_i]) = [S_i, T_i]$, $i = 1, 2$.

- This notion enables the study of X_{ψ^k}.
- From the study of X_{ψ^k} we get an attack.
- We consider all possible relations between pairs of messages and compute the corresponding H-coefficient value.
- All values are considered, thus we get the best attacks using correlation between two messages.

Attacks on Feistel networks

We consider a case where we have n_e equations between the inputs and outputs.

- $E(X_p) \simeq \frac{M}{2^{n_e \cdot n}}$ (M : number of pairs considered)
  $|E(X_{\psi^k}) - E(X_p)| \simeq \frac{M}{2^{n_e \cdot n}} \cdot |\frac{H \cdot 2^{4n}}{|B_n|^k} - \frac{1}{1-1/2^{2n}}|$
  $\sigma(X_p) + \sigma(X_{\psi^k}) \simeq \sqrt{\frac{M}{2^{n_e \cdot n}}}$
- We can solve $\frac{M}{2^{n_e \cdot n}} \cdot |\frac{H \cdot 2^{4n}}{|B_n|^k} - \frac{1}{1-1/2^{2n}}| > \sqrt{\frac{M}{2^{n_e \cdot n}}}$ and find M.
- We deduce the number m of messages needed to get these M pairs.
- We get an attack with complexity $\mathcal{O}(m)$.

Remark : best attacks : n_e minimal and $|\frac{H \cdot 2^{4n}}{|B_n|^k} - \frac{1}{1-1/2^{2n}}|$ maximal.

Example on 3 rounds, *KPA*. Table of values of $\frac{H \cdot 2^{4n}}{|B_n|^3} - \frac{1}{1-1/2^{2n}}$

case : equalities :	1 0 eq.					
$\frac{H \cdot 2^{4n}}{|B_n|^3} - \frac{1}{1-1/2^{2n}}$	$1/2^{2n}$					
case : equalities :	2 1 eq.	3 1 eq.	4 1 eq.	5 1 eq.		
$\frac{H \cdot 2^{4n}}{|B_n|^3} - \frac{1}{1-1/2^{2n}}$	$1/2^n$	$1/2^n$	$1/2^n$	$1/2^n$		
case : equalities :	6 2 eq.	7 2 eq.	8 2 eq.	9 2 eq.	10 2 eq.	11 2 eq.
$\frac{H \cdot 2^{4n}}{|B_n|^3} - \frac{1}{1-1/2^{2n}}$	$1/2^n$	1	1	1	$1/2^n$	$1/2^n$
case : equalities :	12 3 eq.	13 3 eq.				
$\frac{H \cdot 2^{4n}}{|B_n|^3} - \frac{1}{1-1/2^{2n}}$	1	1				

FIG.: Order of the leading term of $\frac{H \cdot 2^{4n}}{|B_n|^3} - \frac{1}{1-1/2^{2n}}$ in different cases

Example on 3 rounds, *KPA*

In case 1 :

- $E(X_p) \simeq M$ (M : number of pairs of messages)
- $\mathcal{O}(\frac{H \cdot 2^{4n}}{|B_n|^3} - \frac{1}{1-1/2^{2n}}) = 1/2^{2n} \Rightarrow |E(X_p) - E(X_{\psi^3})| \simeq \frac{M}{2^{2n}}$
- $\frac{M}{2^{2n}} > \sqrt{M} \Leftrightarrow M > 2^{4n}$

In cases 2 to 5 :

- $E(X_p) \simeq \frac{M}{2^n}$ (M : number of pairs of messages)
- $\mathcal{O}(\frac{H \cdot 2^{4n}}{|B_n|^3} - \frac{1}{1-1/2^{2n}}) = 1/2^{n} \Rightarrow |E(X_p) - E(X_{\psi^3})| \simeq \frac{M}{2^{2n}}$
- $\frac{M}{2^{2n}} > \frac{\sqrt{M}}{\sqrt{2^n}} \Leftrightarrow M > 2^{3n}$

In cases 7, 8 and 9 :

- $E(X_p) \simeq \frac{M}{2^{2n}}$ (M : number of pairs of messages)
- $\mathcal{O}(\frac{H \cdot 2^{4n}}{|B_n|^3} - \frac{1}{1-1/2^{2n}}) = 1 \Rightarrow |E(X_p) - E(X_{\psi^3})| \simeq \frac{M}{2^{2n}}$
- $\frac{M}{2^{2n}} > \frac{\sqrt{M}}{2^n} \Leftrightarrow M > 2^{2n}$

Cases 7,8 and 9 are the cases leading to the best attack. $\mathcal{O}(2^n)$ computations are needed to get $\mathcal{O}(2^{2n})$ pairs. **Complexity of the attack** : $\mathcal{O}(2^n)$.

3-round Feistel network ([Patarin-01]) :

- *KPA* with $\mathcal{O}(2^{n/2})$ computations.
- in case $R^1 \oplus S^1 = R^2 \oplus S^2$, $\mathcal{O}(\frac{H \cdot 2^{4n}}{|B_n|^3} - \frac{1}{1-1/2^{2n}}) = 1$.

3-round Feistel network with round permutations :

- *KPA* with $\mathcal{O}(2^n)$ computations.
- no case with 1 equation and $\mathcal{O}(\frac{H \cdot 2^{4n}}{|B_n|^3} - \frac{1}{1-1/2^{2n}}) = 1$.

$\Rightarrow$ Not just transposing attacks !

Attacks on Feistel permutation generators

When $m > 2^{2n}$, we decide to attack a permutation generator. (λ number of permutations needed)
Here :

- $E(X_p) \simeq \frac{M \cdot \lambda}{2^{n_e \cdot n}}$
  $|E(X_{\psi^k}) - E(X_p)| \simeq \frac{M \cdot \lambda}{2^{n_e \cdot n}} \cdot |\frac{H \cdot 2^{4n}}{|B_n|^k} - \frac{1}{1 - 1/2^{2n}}|$
  $\sigma(X_p) + \sigma(X_{\psi^k}) \simeq \sqrt{\frac{M \cdot \lambda}{2^{n_e \cdot n}}}$
- We can solve $\frac{M \cdot \lambda}{2^{n_e \cdot n}} \cdot |\frac{H \cdot 2^{4n}}{|B_n|^k} - \frac{1}{1 - 1/2^{2n}}| > \sqrt{\frac{M \cdot \lambda}{2^{n_e \cdot n}}}$, with M maximal per permutation, and find λ.
- We get an attack with complexity $\mathcal{O}(2^{2n} \cdot \lambda)$.

Remark : best attacks : n_e minimal, $|\frac{H \cdot 2^{4n}}{|B_n|^k} - \frac{1}{1 - 1/2^{2n}}|$ maximal and M maximal.

Example on 6 rounds, *CPA*. Table of values of $\frac{H\cdot 2^{4n}}{|B_n|^6} - \frac{1}{1-1/2^{2n}}$

case :	1	2	3		
equalities :	0 eq.	0 eq.	0 eq.		
maximal M :	2^{4n}	2^{3n}	2^{3n}		
$\frac{H\cdot 2^{4n}}{\lvert B_n\rvert^6} - \frac{1}{1-1/2^{2n}}$	$1/2^{3n}$	$1/2^{3n}$	$1/2^{3n}$		
case :	4	5	6	7	8
equalities :	1 eq.	1 eq.	1 eq.	1 eq.	1 eq.
maximal M :	2^{4n}	2^{3n}	2^{3n}	2^{3n}	2^{3n}
$\frac{H\cdot 2^{4n}}{\lvert B_n\rvert^6} - \frac{1}{1-1/2^{2n}}$	$1/2^{2n}$	$1/2^{3n}$	$1/2^{2n}$	$1/2^{2n}$	$1/2^{2n}$
case :	9	10	11		
equalities :	2 eq.	2 eq.	2 eq.		
maximal M :	2^{4n}	2^{4n}	2^{3n}		
$\frac{H\cdot 2^{4n}}{\lvert B_n\rvert^6} - \frac{1}{1-1/2^{2n}}$	$1/2^{3n}$	$1/2^{2n}$	$1/2^{n}$		

FIG.: Order of the leading term of $\frac{H\cdot 2^{4n}}{|B_n|^6} - \frac{1}{1-1/2^{2n}}$ in different cases

Example on 6 rounds, *CPA*

In case 1 :

- $E(X_p) \simeq \lambda \cdot 2^{4n}$
- $\mathcal{O}(\frac{H \cdot 2^{4n}}{|B_n|^6} - \frac{1}{1-1/2^{2n}}) = 1/2^{3n} \Rightarrow |E(X_p) - E(X_{\psi^6})| \simeq \lambda \cdot 2^n$
- $\lambda \cdot 2^n > \sqrt{\lambda} \cdot 2^{2n} \Leftrightarrow \lambda > 2^{2n}$

In case 4 :

- $E(X_p) \simeq \frac{\lambda \cdot 2^{4n}}{2^n}$
- $\mathcal{O}(\frac{H \cdot 2^{4n}}{|B_n|^6} - \frac{1}{1-1/2^{2n}}) = 1/2^{2n} \Rightarrow |E(X_p) - E(X_{\psi^3})| \simeq \lambda \cdot 2^n$
- $\lambda \cdot 2^n > \sqrt{\lambda \cdot 2^{3n}} \Leftrightarrow \lambda > 2^n$

In case 11 :

- $E(X_p) \simeq \frac{\lambda \cdot 2^{3n}}{2^{2n}}$
- $\mathcal{O}(\frac{H \cdot 2^{4n}}{|B_n|^6} - \frac{1}{1-1/2^{2n}}) = 1/2^n \Rightarrow |E(X_p) - E(X_{\psi^6})| \simeq \lambda$
- $\lambda > \sqrt{\lambda \cdot 2^n} \Leftrightarrow \lambda > 2^n$

Cases 4 and 11 are the cases leading to the best attacks. $\mathcal{O}(2^n)$ permutations and $\mathcal{O}(2^{2n})$ computations per permutation are needed. **Complexity of the attacks** : $\mathcal{O}(2^{3n})$.

Plan

General idea

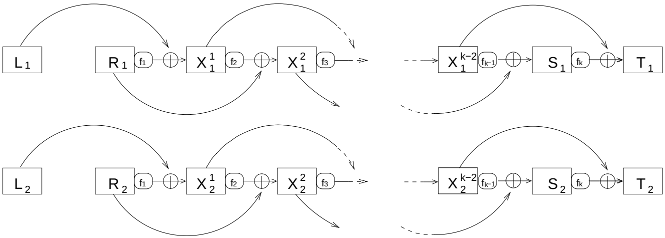


FIG.: $\psi^k(f_1, \ldots, f_k)([L_i, R_i]) = [S_i, T_i], \ i = 1, 2$

- Fix a possible sequence $\mathbf{s} \in \{=, \neq\}^k$, such that $X_1^i \ s_i \ X_2^i$.
- $\mathbf{N(d_i)}$: number of possible values for $X_1^i \oplus X_2^i$.
- Then $N(d_i) \cdot 2^n$: number of possibilities for (X_1^i, X_2^i).

General idea

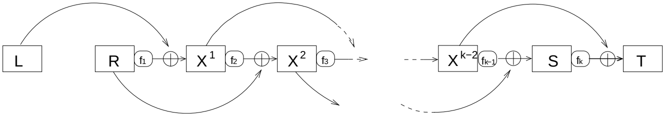


FIG.: $\psi^k(f_1, \ldots, f_k)([L, R]) = [S, T]$

$f_i(X^{i-1}) = X^{i-2} \oplus X^i$,

- $N(d_i) \cdot 2^n$: number of possibilities for $(f_i(X_1^{i-1}), f_i(X_2^{i-1}))$.
- If $X_1^{i-1} \neq X_2^{i-1}$, number of possibilities for f_i :

$$\mathbf{F_i(s)} := 2^n \cdot N(d_i) \cdot (2^n - 2)!$$

- If $X_1^{i-1} = X_2^{i-1}$, number of possibilities for f_i :

$$\mathbf{F_i(s)} := 2^n \cdot N(d_i) \cdot (2^n - 1)!$$

Formula

Then, given a specific pair of input/output couples, the wanted number H is :

$$\begin{aligned}\mathbf{H} &= \sum_{\text{possible } s} \left(\prod_{i=1}^{k} F_i(s) \right) \\ &= \sum_{\text{possible } s} (2^n-1)!^{n_e(s)}(2^n-2)!^{n_d(s)} \cdot N(d_1)\cdots N(d_k).\end{aligned}$$

We have to :

- find the possible sequences s for each input/output couples
- for each one, compute the product $N(d_1)\dots N(d_k)$.

This can be done using combinatorial facts. Thus :

- We obtain general formulae for the H-coefficients
- We obtain all attacks using correlations between two messages.

Plan

Table of results

number k of rounds	KPA	CPA-1	CPA-2	CPCA-1	CPCA-2
1	1	1	1	1	1
2	$2^{n/2}$	2	2	2	2
3	$2^{n}(+)$	$2^{n/2}$	$2^{n/2}$	$2^{n/2}$	3
4	2^{n}	$2^{n/2}$	$2^{n/2}$	$2^{n/2}$	$2^{n/2}$
5	$2^{3n/2}$	2^{n}	2^{n}	2^{n}	2^{n}
6	$2^{3n}(+)$	$2^{3n}(+)$	$2^{3n}(+)$	$2^{3n}(+)$	$2^{3n}(+)$
7	2^{3n}	2^{3n}	2^{3n}	2^{3n}	2^{3n}
8	2^{4n}	2^{4n}	2^{4n}	2^{4n}	2^{4n}
9	$2^{6n}(+)$	$2^{6n}(+)$	$2^{6n}(+)$	$2^{6n}(+)$	$2^{6n}(+)$
10	2^{6n}	2^{6n}	2^{6n}	2^{6n}	2^{6n}
11	2^{7n}	2^{7n}	2^{7n}	2^{7n}	2^{7n}
12	$2^{9n}(+)$	$2^{9n}(+)$	$2^{9n}(+)$	$2^{9n}(+)$	$2^{9n}(+)$
$k \geq 6,\ k = 0 \mod 3$	$2^{(k-3)n}$	$2^{(k-3)n}$	$2^{(k-3)n}$	$2^{(k-3)n}$	$2^{(k-3)n}$
$k \geq 6,\ k = 1$ or $2 \mod 3$	$2^{(k-4)n}$	$2^{(k-4)n}$	$2^{(k-4)n}$	$2^{(k-4)n}$	$2^{(k-4)n}$

FIG.: Maximum number of computations needed to get an attack on a k-rounds Feistel network with internal permutations.

Conclusion

- Similar results for Feistel networks with internal permutations and for classical Feistel networks, when the number of rounds is ≤ 5, except for KPA on 3 rounds.
- For $k \geq 6$ rounds, different results on all $3i$ rounds.
- The attacks fit with the results of Gilles Piret.
- When the complexities are $\ll 2^{n/2}$, same results for Feistel networks with round permutations and round functions.
- The attacks on Feistel networks with internal permutations seem to be as difficult or sometimes more difficult to perform as the ones on classical Feistel networks.