Generic Attacks on Feistel Ciphers With Internal Permutations

Joana Treger, Jacques Patarin

PRiSM, Université de Versailles

2008-11-27

Summary

1. Introduction
2. Generic attacks on the first 5 rounds
3. Generic attacks for any number of rounds
   - General method
   - Computation of the H-coefficients
   - Example on 3 rounds
   - Attacking Feistel permutation generators
   - Example on 6 rounds
4. Table of results and conclusion

Feistel ciphers (1/3)

Definition

Let f be a function from $\{1, \ldots, 2^n\}$ to $\{1, \ldots, 2^n\}$.
A Feistel cipher with round function f is defined by :

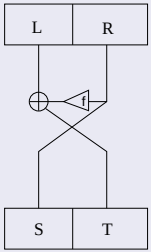


FIG.: 1-round Feistel scheme

We call $\psi(f)$ or simply ψ such a construction.

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

Feistel ciphers (2/3)

ψ is a permutation of $\{1, \ldots, 2^{2n}\}$:

$$\psi^{-1}([S, T]) = [T \oplus f(S), S] = [L, R]$$

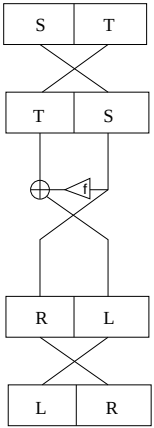
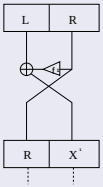


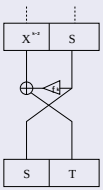
FIG.: $\psi^{-1} = \tau \circ \psi \circ \tau$

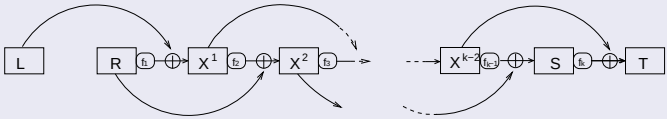
Feistel ciphers 3/3

Definition

Let $f_1, \ldots, f_k$ be k functions from $\{1, \ldots, 2^n\}$ to $\{1, \ldots, 2^n\}$.
A k-round Feistel cipher with round functions $f_1, \ldots, f_k$ is defined by the succesion of k rounds of a Feistel cipher with round function f_i :
$\psi^k(f_1, \ldots, f_k) := \psi(f_k) \circ \ldots \circ \psi(f_1)$







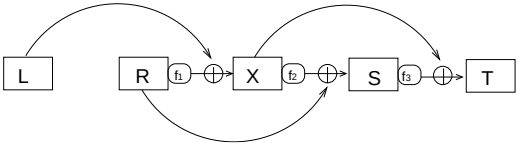
Luby-Rackoff revisited

Derived structures :

- Classical Feistel ciphers.
- Unbalanced Feistel ciphers with expanding internal functions.
- Unbalanced Feistel ciphers with contracting internal functions.
- Feistel ciphers with internal permutations.
  - Used in the design of Twofish, Camellia, DEAL.
  - [Knudsen-02] : attack on 5 rounds, impossible differential
    [Piret-05] : security proofs for 3 and 4 rounds, $\geq \mathcal{O}(2^{n/2})$ messages 3-round $CPA-2$, 4-round $CPCA-2$

Feistel ciphers with internal permutations

Different behaviour of these Feistel networks and the classical ones.
Example (3 rounds) :

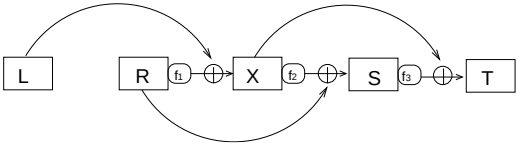


Attack on 3 round classical Feistel ciphers :

- Relations considered between two input/output couples : $R_1 \oplus S_1 = R_2 \oplus S_2$.
- **Random permutation** : probability $1/2^n$; **Feistel cipher** : probability $2/2^n$
  - $R_1 \oplus S_1 = R_2 \oplus S_2 \Leftrightarrow f_2(X_1) = f_2(X_2)$
  - $f_2(X_1) = f_2(X_2) \Leftrightarrow X_1 = X_2$ or $(X_1 \neq X_2$ and $f_2(X_1) = f_2(X_2))$.
- **Chosen plaintext attack** : $\mathcal{O}(2^{n/2})$ messages.

Feistel ciphers with internal permutations

Different behaviour of these Feistel networks and the classical ones.
Example (3 rounds) :



Attack on 3 round classical Feistel ciphers :

- Relations considered between two input/output couples : $R_1 \oplus S_1 = R_2 \oplus S_2$.
- **Random permutation** : probability $1/2^n$; **Feistel cipher** : probability $2/2^n$
  - $R_1 \oplus S_1 = R_2 \oplus S_2 \Leftrightarrow f_2(X_1) = f_2(X_2)$
  - $f_2(X_1) = f_2(X_2) \Leftrightarrow X_1 = X_2$ or $(X_1 \neq X_2$ and $f_2(X_1) = f_2(X_2))$.
- **Chosen plaintext attack** : $\mathcal{O}(2^{n/2})$ messages.
- **Known plaintext attack** : $\mathcal{O}(2^{n/2})$ messages.

Does not work on Feistel cipher with round permutations !

Generic attacks

Definition

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

- We interest ourselves in generic attacks, necessiting $< \mathcal{O}(2^{2n})$ messages (exhaustive search on the inputs).
- When the complexity is $\geq \mathcal{O}(2^{2n})$, we interest ourselves in attacks on Feistel permutation generators.

Two-point attacks

Definition

two-point attacks *are attacks using correlations between blocks of pairs of distinct messages.*

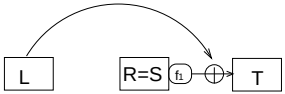
Example : previous attack on 3 rounds, relations considered between 2 messages were $R_1 \oplus S_1 = R_2 \oplus S_2$.

- Best known attacks against **classical Feistel ciphers** (except on 3 rounds, CPCA-2).
- Efficient against Feistel ciphers with internal permutations : the complexities of the two-point attacks found (except on 3 rounds, $CPCA-2$) **coincide with the known bounds of security** (3 and 4 rounds, [Piret-05]).

Notations

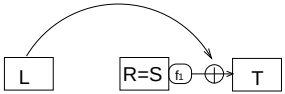
- **KPA** : known plaintext attack
- **CPA** $-$ **1** : non-adaptive chosen plaintext attack
- **CPA** $-$ **2** : adaptive chosen plaintext attack
- **CPCA** $-$ **1** : non-adaptive chosen plaintext and ciphertext attack
- **CPCA** $-$ **2** : adaptive chosen plaintext and ciphertext attack
- $\mathbf{B_n}$: permutation on n bits.

Generic attack by hand : 1 and 2 rounds

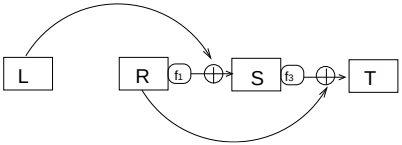


- Relation considered : $R = S$.
- **Random permutation** : probability $1/2^n$; **Feistel cipher** : probability 1.
- **KPA** : 1 message.

Generic attack by hand : 1 and 2 rounds

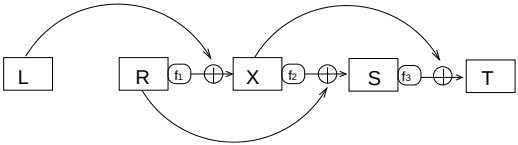


- Relation considered : $R = S$.
- **Random permutation** : probability $1/2^n$; **Feistel cipher** : probability 1.
- **KPA** : 1 message.



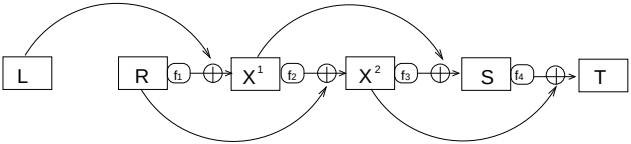
- Relations considered : $R_1 = R_2$, $S_1 \oplus S_2 = L_1 \oplus L_2$.
- $CPA - 1$. **Random permutation** : probability $1/2^n$; **Feistel cipher** : probability 1.
- **CPA** $-$ **1** : 2 messages.
- **KPA** : $\mathcal{O}(2^{n/2})$ messages.

Generic attacks by hand : 3 rounds



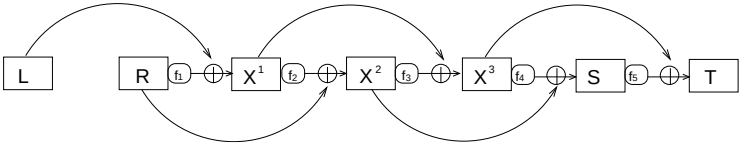
- Relation considered : $L_1 = L_2$, $R_1 \oplus R_2 = S_1 \oplus S_2$.
- $CPA - 1$. **Random permutation** : probability $1/2^n$; **Feistel cipher** : probability 0
  - $R_1 \oplus R_2 = S_1 \oplus S_2 \Rightarrow X_1 = X_2 \Rightarrow R_1 = R_2$.
- **CPA − 1** : $\mathcal{O}(2^{n/2})$ messages.
- **KPA** : $\mathcal{O}(2^n)$ messages.

Generic attack by hand : 4 rounds



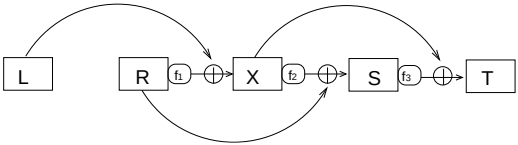
- Relation considered : $R_1 = R_2$, $L_1 \oplus L_2 = S_1 \oplus S_2$.
- $CPA - 1$. **Random permutation** : probability $1/2^n$; **Feistel cipher** : probability 0
  - $R_1 = R_2 \Rightarrow X_1^1 \oplus X_2^1 = L_1 \oplus L_2$.
  - $L_1 \oplus L_2 = S_1 \oplus S_2 = X_1^1 \oplus X_2^1 \Rightarrow X_1^2 = X_2^2 \Rightarrow L_1 = L_2$.
- **CPA** $- \mathbf{1}$: $\mathcal{O}(2^{n/2})$ messages.
- **KPA** : $\mathcal{O}(2^n)$ messages.

Generic attack by hand : 5 rounds [Knudsen-02]



- Relation considered : $R_1 = R_2$, $S_1 = S_2$, $L_1 \oplus L_2 = T_1 \oplus T_2$.
- $CPA - 1$. **Random permutation** : probability $1/2^{2n}$; **Feistel cipher** : probability 0.
  - $S_1 = S_2 \Rightarrow X_1^3 \oplus X_2^3 = T_1 \oplus T_2$.
  - $R_1 = R_2 \Rightarrow X_1^1 \oplus X_2^1 = L_1 \oplus L_2$.
  - $T_1 \oplus T_2 = L_1 \oplus L_2 \Rightarrow X_1^2 = X_2^2 \Rightarrow X_1^1 = X_2^1 \Rightarrow L_1 = L_2$.
- **CPA** $- \mathbf{1}$: $\mathcal{O}(2^n)$ messages.
- **KPA** : $\mathcal{O}(2^{3n/2})$ messages.

Special case : 3 rounds, $CPCA-2$



Best attack is 3-point attack. The same attack as for classical Feistel ciphers [LR-88].

- 3 messages : $[L_1, R_1]/[S_1, T_1]$, $[L_2, R_1]/[S_2, T_2]$ and $[L_3, R_3]/[S_1, T_1 \oplus L_1 \oplus L_2]$. Relation considered : $R_2 \oplus R_3 = S_2 \oplus S_3$.
- $CPCA-2$. **Feistel cipher** : probability 1 ; **Random permutation** : probability $1/2^n$
  - $R_1 = R_2 \Rightarrow X_1 \oplus X_2 = L_1 \oplus L_2$.
  - $S_1 = S_3 \Rightarrow X_1 \oplus X_3 = T_1 \oplus T_3$.
  - $T_3 \oplus T_1 = L_1 \oplus L_2 \Rightarrow X_2 = X_3$.
  - $X_2 = X_3 \Rightarrow R_2 \oplus R_3 = S_2 \oplus S_3$.
- **CPCA** $-$ **2** : 3 messages.

Remark, complexity $\ll 2^{n/2}$

Remark :

- Distinguishing a random permutation on n bits from a random function : $\mathcal{O}(2^{n/2})$ messages.
- $\Rightarrow$ When an attack needs $\ll 2^{n/2}$ messages, it works on Feistel ciphers with internal permutations and functions.

Plan

1. Introduction
2. Generic attacks on the first 5 rounds
3. Generic attacks for any number of rounds
   - General method
   - Computation of the H-coefficients
   - Example on 3 rounds
   - Attacking Feistel permutation generators
   - Example on 6 rounds
4. Table of results and conclusion

Towards a systematical analysis

We want the best generic two-point attack on a k-round Feistel cipher, for any k.

1. Enumerate all possible cases $\mathcal{C}$ (equalities/inequalities between the input and output blocks of 2 distinct messages).
2. For each case, evaluate the probability (depending on k) to get one specific output pair from a specific input pair, for both a random permutation and a Feistel permutation.
3. For each k and each type of attack (KPA, CPA,..), estimate the case leading to the best attack.
4. Evaluate the number of messages needed to realize the attack.

1 : Enumerating all possible cases

Possible equalities between the blocks :

$$\begin{cases} L_1 = L_2, \text{ or not} \\ R_1 = R_2, \text{ or not} \\ S_1 = S_2, \text{ or not} \\ T_1 = T_2, \text{ or not} \\ L_1 \oplus L_2 = S_1 \oplus S_2, \text{ or not, when } k \text{ is even} \\ R_1 \oplus R_2 = T_1 \oplus T_2, \text{ or not, when } k \text{ is even} \\ L_1 \oplus L_2 = T_1 \oplus T_2, \text{ or not, when } k \text{ is odd} \\ R_1 \oplus R_2 = S_1 \oplus S_2, \text{ or not, when } k \text{ is odd} \end{cases}$$

- For k even : 13 cases.
- For k odd : 11 cases.

2 : Computing the probabilities (1/2)

Given one input/output pair. Computing the probabilities $\mathbf{P_1}$ to get **these two precise outputs from the inputs** :

- In the case of a random permutation : easy.
- In the case of a Feistel cipher with internal permutations : based on the H-coefficient values.

2 : Computing the probabilities (1/2)

Given one input/output pair. Computing the probabilities $\mathbf{P_1}$ to get **these two precise outputs from the inputs** :

- In the case of a random permutation : easy.
- In the case of a Feistel cipher with internal permutations : based on the H-coefficient values.

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** *computes the number of* $(f_1, \ldots, f_k) \in B_n^k$, *such that* $\psi^k(f_1, \ldots, f_k)([L_i, R_i]) = [S_i, T_i]$, $i = 1, 2$.

$\rightarrow$ The H value is the same for all pairs belonging to a same case $\mathcal{C}$.

2 : Computing the probabilities (2/2)

Proposition

Suppose the H-coefficients computed. Then the previous probability P_1 *to get one precise outpout from a given input pair is :*

- $\frac{1}{2^{2n}(2^{2n}-1)}$ *in the case of a random permutation.*
- $\frac{H}{|B_n|^k}$ *in the case of a k-round Feistel cipher.*

3 : Estimating the cases leading to the best attack

- A case $\mathcal{C}$ with a largest difference between the previous probability $\mathbf{P_1}$ should lead to a better attack.

3 : Estimating the cases leading to the best attack

- A case $\mathcal{C}$ with a largest difference between the previous probability $\mathbf{P_1}$ should lead to a better attack.
- **But** : to get an attack, the difference in the probabilities has to result in a difference in the number of couples verifying the specific constraints on their blocks.

3 : Estimating the cases leading to the best attack

- A case $\mathcal{C}$ with a largest difference between the previous probability $\mathbf{P_1}$ should lead to a better attack.
- **But** : to get an attack, the difference in the probabilities has to result in a difference in the number of couples verifying the specific constraints on their blocks.
- **Thus** : find the cases which realize a compromise between :

HUGE DIFFERENCE between the probabilities to obtain one specific pair of input/ouput couples	AND	NUMBER OF RELATIONS on the blocks, that cannot be imposed by the type of attack.

4 : Evaluating the number of messages needed to realize the attack (1/2)

Let $\mathcal{C}$ be one specific case. Let us consider m messages and the random variables :

- $\mathbf{X_p}$ counts the number of pairs of these messages verifying the equations of $\mathcal{C}$ on the inputs and outputs when they correspond to a random permutation
- $\mathbf{X_{\psi^k}}$ counts the same number for a k-round Feistel cipher with internal permutation.

From the Chebytchev formula :

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

we distinguish with high probability ψ^k from a random permutation if

$$|E(X_{\psi^k}) - E(X_p)| > \sigma(X_{\psi^k}) + \sigma(X_p).$$

For each case $\mathcal{C}$, those values can be obtained from $\mathbf{P_1}$.

4 : Evaluating the number of messages needed to realize the attack (2/2)

We consider a case $\mathcal{C}$ with n_e equations between the input and output blocks that cannot be imposed by the type of attack considered.

- We can solve $|E(X_{\psi^k}) - E(X_p)| > \sigma(X_p) + \sigma(X_{\psi^k})$ and find M :

$$\frac{M}{2^{n_e \cdot n}} \cdot \left| \frac{H \cdot 2^{4n}}{|B_n|^k} - \frac{1}{1 - 1/2^{2n}} \right| > \sqrt{\frac{M}{2^{n_e \cdot n}}},$$

  where $\left| \frac{H \cdot 2^{4n}}{|B_n|^k} - \frac{1}{1-1/2^{2n}} \right|$ is 2^{4n} times the differences of the P_1's.
- 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 $\left| \frac{H \cdot 2^{4n}}{|B_n|^k} - \frac{1}{1-1/2^{2n}} \right|$ maximal.

Plan

1. Introduction
2. Generic attacks on the first 5 rounds
3. Generic attacks for any number of rounds
   - General method
   - Computation of the H-coefficients
   - Example on 3 rounds
   - Attacking Feistel permutation generators
   - Example on 6 rounds
4. Table of results and conclusion

The reasoning

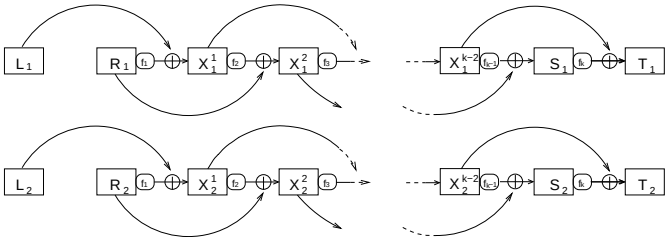


FIG.: $\psi^k(f_1, \ldots, f_k)([L_i, R_i]) = [S_i, T_i],\ i = 1, 2$

- Fix a possible sequence $s \in \{=, \neq\}^k$, such that $X_1^i\ s_i\ X_2^i$.
- For such a fixed sequence s, evaluate the number $H(s)$ of possibilities for $(f_1, \ldots, f_k)$.
- Find all possible sequences s and sum up :

$$\mathbf{H} = \sum_{\text{possible } s} H(s).$$

H-coefficients

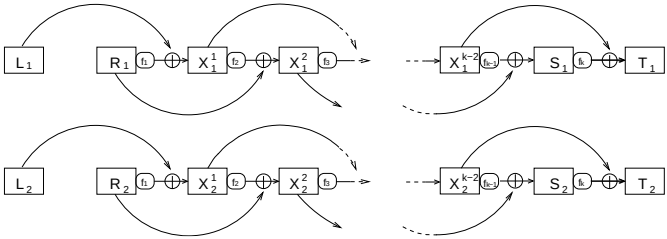


FIG.: $\psi^k(f_1, \ldots, f_k)([L_i, R_i]) = [S_i, T_i],\ i = 1, 2$

The preceding steps can be done using combinatorial facts.

H-coefficients

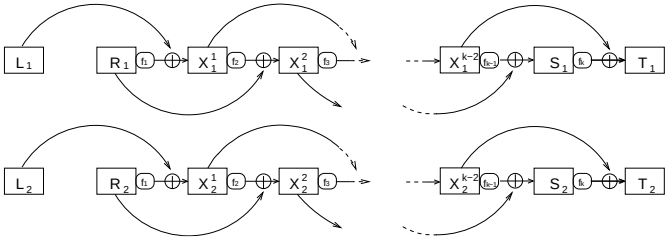


FIG.: $\psi^k(f_1, \ldots, f_k)([L_i, R_i]) = [S_i, T_i],\ i = 1, 2$

The preceding steps 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

1. Introduction
2. Generic attacks on the first 5 rounds
3. Generic attacks for any number of rounds
   - General method
   - Computation of the H-coefficients
   - Example on 3 rounds
   - Attacking Feistel permutation generators
   - Example on 6 rounds
4. Table of results and conclusion

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

case :	1					
equalities :	0 eq.					
$\frac{H \cdot 2^{4n}}{\lvert B_n \rvert^3} - \frac{1}{1-1/2^{2n}}$	$1/2^{2n}$					
case :	2	3	4	5		
equalities :	1 eq.	1 eq.	1 eq.	1 eq.		
$\frac{H \cdot 2^{4n}}{\lvert B_n \rvert^3} - \frac{1}{1-1/2^{2n}}$	$1/2^{n}$	$1/2^{n}$	$1/2^{n}$	$1/2^{n}$		
case :	6	7	8	9	10	11
equalities :	2 eq.	2 eq.	2 eq.	2 eq.	2 eq.	2 eq.
$\frac{H \cdot 2^{4n}}{\lvert B_n \rvert^3} - \frac{1}{1-1/2^{2n}}$	$1/2^{n}$	1	1	1	$1/2^{n}$	$1/2^{n}$
case :	12	13				
equalities :	3 eq.	3 eq.				
$\frac{H \cdot 2^{4n}}{\lvert B_n \rvert^3} - \frac{1}{1-1/2^{2n}}$	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)
- $\mathcal{O}(\frac{H \cdot 2^{4n}}{|B_n|^3} - \frac{1}{1-1/2^{2n}}) = 1/2^{2n} \Rightarrow |E(X_p) - E(X_{\psi^3})| \simeq \frac{M}{2^{2n}}$
- $\frac{M}{2^{2n}} > \sqrt{M} \Leftrightarrow M > 2^{4n}$

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

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

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 :

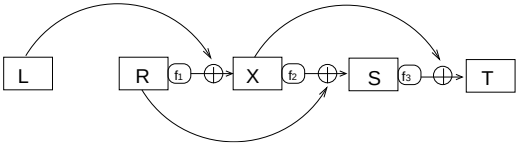
- $E(X_p) \simeq \frac{M}{2^n}$ (M : number of pairs of messages)
- $\mathcal{O}(\frac{H \cdot 2^{4n}}{|B_n|^3} - \frac{1}{1-1/2^{2n}}) = 1/2^{n} \Rightarrow |E(X_p) - E(X_{\psi^3})| \simeq \frac{M}{2^{2n}}$
- $\frac{M}{2^{2n}} > \frac{\sqrt{M}}{\sqrt{2^n}} \Leftrightarrow M > 2^{3n}$

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. $\mathcal{O}(2^n)$ messages are needed to get $\mathcal{O}(2^{2n})$ pairs. **Complexity of the attack** : $\mathcal{O}(2^n)$.

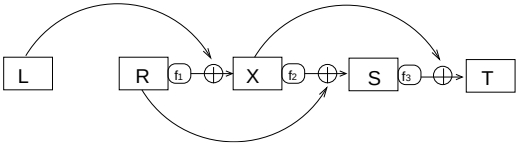
Example on 3 rounds, comments



Not just one best attack. Here, 3 cases lead to the best attack :

- case 7 : $S_1 = S_2$ and $L_1 \oplus L_2 = T_1 \oplus T_2$,
- case 8 : $R_1 = R_2$ and $S_1 = S_2$,
- case 9 : $L_1 = L_2$ and $R_1 \oplus R_2 = S_1 \oplus S_2$ (the one exposed in the first part).

Example on 3 rounds, comments



Not just one best attack. Here, 3 cases lead to the best attack :

- case 7 : $S_1 = S_2$ and $L_1 \oplus L_2 = T_1 \oplus T_2$,
- case 8 : $R_1 = R_2$ and $S_1 = S_2$,
- case 9 : $L_1 = L_2$ and $R_1 \oplus R_2 = S_1 \oplus S_2$ (the one exposed in the first part).

We could have deduced from the table that no *KPA* on 3 rounds comparable to the one on classical Feistel ciphers was possible :

- there, for the case $R_1 \oplus R_2 = S_1 \oplus S_2$, the difference $|\frac{H \cdot 2^{4n}}{|B_n|^3} - \frac{1}{1-1/2^{2n}}|$ is of about 1 for just 1 condition on the inputs and outputs.
- here, there is no comparable case $\Rightarrow$ no comparable *KPA*.

Plan

1. Introduction
2. Generic attacks on the first 5 rounds
3. Generic attacks for any number of rounds
   - General method
   - Computation of the H-coefficients
   - Example on 3 rounds
   - Attacking Feistel permutation generators
   - Example on 6 rounds
4. Table of results and conclusion

Attacks on Feistel permutation generators

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

- are multiplied by λ for $E(X_p), E(X_{\psi^k})$,
- are multiplied by $\sqrt{(\lambda)}$ for $\sigma(X_p), \sigma(X_{\psi^k})$ by $\sqrt{\lambda}$.

We can solve

$$\frac{M \cdot \lambda}{2^{n_e.n}} \cdot |\frac{H \cdot 2^{4n}}{|B_n|^k} - \frac{1}{1 - 1/2^{2n}}| > \sqrt{\frac{M \cdot \lambda}{2^{n_e.n}}},$$

with M maximal per permutation ($\Rightarrow m = 2^{2n}$), and find λ.
$\Rightarrow$ We get an attack with complexity $\mathcal{O}(m \cdot \lambda) = \mathcal{O}(2^{2n} \cdot \lambda)$.

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

Plan

1. Introduction
2. Generic attacks on the first 5 rounds
3. Generic attacks for any number of rounds
   - General method
   - Computation of the H-coefficients
   - Example on 3 rounds
   - Attacking Feistel permutation generators
   - Example on 6 rounds
4. Table of results and conclusion

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}		
$\frac{H \cdot 2^{4n}}{\|B_n\|^6} - \frac{1}{1-1/2^{2n}}$	$1/2^{3n}$	$1/2^{3n}$	$1/2^{3n}$		
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}
$\frac{H \cdot 2^{4n}}{\|B_n\|^6} - \frac{1}{1-1/2^{2n}}$	$1/2^{2n}$	$1/2^{3n}$	$1/2^{2n}$	$1/2^{2n}$	$1/2^{2n}$
case :	9	10	11		
equalities :	2 eq.	2 eq.	2 eq.		
maximal M :	2^{4n}	2^{4n}	2^{3n}		
$\frac{H \cdot 2^{4n}}{\|B_n\|^6} - \frac{1}{1-1/2^{2n}}$	$1/2^{3n}$	$1/2^{2n}$	$1/2^{n}$		

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 :

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

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 :

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

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 :

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

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 $\mathcal{O}(2^{2n})$ messages per permutation are needed. **Complexity of the attacks** : $\mathcal{O}(2^{3n})$.

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	$2^{9n}(+)$	$2^{9n}(+)$	$2^{9n}(+)$	$2^{9n}(+)$	$2^{9n}(+)$
$k \geq 6,\ k=0 \ mod\ 3$	$2^{(k-3)n}$	$2^{(k-3)n}$	$2^{(k-3)n}$	$2^{(k-3)n}$	$2^{(k-3)n}$
$k \geq 6,\ k=1 \text{ or } 2 \ mod\ 3$	$2^{(k-4)n}$	$2^{(k-4)n}$	$2^{(k-4)n}$	$2^{(k-4)n}$	$2^{(k-4)n}$

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

Table of results for classical Feistel ciphers [Patarin-01]

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	$2^{n/2}$	$2^{n/2}$	$2^{n/2}$	$2^{n/2}$	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^{2n}	2^{2n}	2^{2n}	2^{2n}	2^{2n}
7	2^{3n}	2^{3n}	2^{3n}	2^{3n}	2^{3n}
8	2^{4n}	2^{4n}	2^{4n}	2^{4n}	2^{4n}
9	2^{5n}	2^{5n}	2^{5n}	2^{5n}	2^{5n}
10	2^{6n}	2^{6n}	2^{6n}	2^{6n}	2^{6n}
11	2^{7n}	2^{7n}	2^{7n}	2^{7n}	2^{7n}
12	2^{8n}	2^{8n}	2^{8n}	2^{8n}	2^{8n}
$k \geq 6$	$2^{(k-4)n}$	$2^{(k-4)n}$	$2^{(k-4)n}$	$2^{(k-4)n}$	$2^{(k-4)n}$

FIG.: Maximum number of messages needed to get an attack on a k-round Feistel network with internal functions.

Conclusion

We gave the best generic two-point attacks on Feistel ciphers with internal permutations.

- These are the best known generic attacks on such ciphers.
- The complexities reach the known bounds on security (3 and 4 rounds, [Piret-05]).
- However, other attacks may be possible, we did not concentrate on proofs of security.
- Complexities found often close to the complexity of the attacks on classical Feistel chiphers. This could not be predicted.