

Classical and Quantum Attacks on 6-round Feistel Schemes

Selected Areas in Cryptography (SAC) 2024

Maya Chartouny, Benoît Cogliati, Jacques Patarin

Thales DIS, Université Paris-Saclay - LMV

29 August 2024

THALES



Overview

1. Introduction

2. Feistel Schemes

2.1 Definition

2.2 Distinguishing Attack

2.3 State of the Art

3. Classical Generic Attacks on 6-round Feistel with Internal Permutations

3.1 Classical attack

3.2 Computer Simulations

4. Quantum Generic Attacks on 6-round Feistel

4.1 Ambainis's Algorithm for Distinctness Problem

4.2 Childs and Eisenberg Algorithm for Subset Finding

4.3 Application to 6-round Feistel Schemes

Plan

1. Introduction

2. Feistel Schemes

3. Classical Generic Attacks on 6-round Feistel with Internal Permutations

4. Quantum Generic Attacks on 6-round Feistel

Introduction

A **Feistel scheme** is a symmetric structure used to construct block ciphers such as 3DES, Twofish ...

Motivations:

- Gap between attacks on Feistel with internal functions/permutations
- Enhance attacks using the power of quantum computers

Our contributions:

- Classical attack on 6 rounds Feistel networks with internal permutations
- Detailed analysis for Child's and Eisenberg quantum algorithm time complexity
- Quantum attack on 6 rounds Feistel networks

Plan

1. Introduction

2. Feistel Schemes

2.1 Definition

2.2 Distinguishing Attack

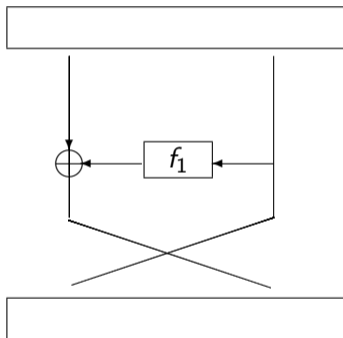
2.3 State of the Art

3. Classical Generic Attacks on 6-round Feistel with Internal Permutations

4. Quantum Generic Attacks on 6-round Feistel

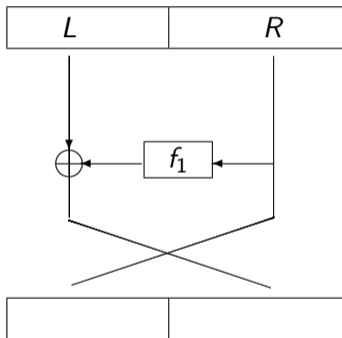
Feistel schemes on $2n$ bits

1-round



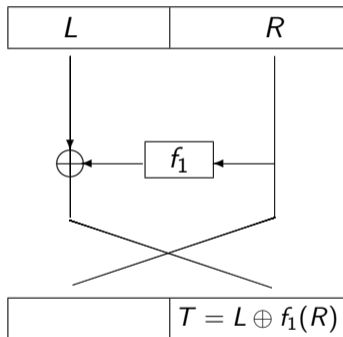
Feistel schemes on $2n$ bits

1-round



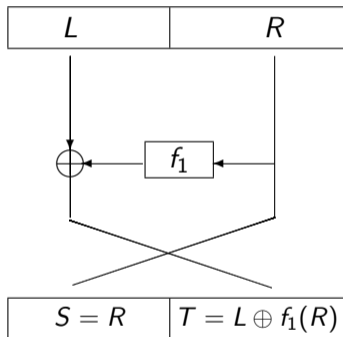
Feistel schemes on $2n$ bits

1-round



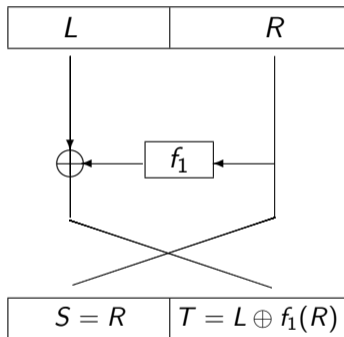
Feistel schemes on $2n$ bits

1-round

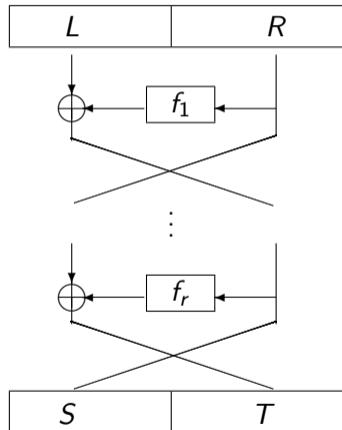


Feistel schemes on $2n$ bits

1-round



r -round



f_1, \dots, f_r are internal random functions or internal random permutations on n bits

6-round Feistel scheme (Ψ^6)

$$1 \text{ round: } \begin{cases} R \\ L \oplus f_1(R) = X \end{cases}$$

$$2 \text{ rounds: } \begin{cases} X \\ R \oplus f_2(X) = Y \end{cases}$$

$$3 \text{ rounds: } \begin{cases} Y \\ X \oplus f_3(Y) = Z \end{cases}$$

$$4 \text{ rounds: } \begin{cases} Z \\ Y \oplus f_4(Z) = U \end{cases}$$

$$5 \text{ rounds: } \begin{cases} U \\ Z \oplus f_5(U) = S \end{cases}$$

$$6 \text{ rounds: } \begin{cases} S \\ U \oplus f_6(S) = T \end{cases}$$

Distinguishing attack

Goal: differentiate between Feistel schemes/random permutations

-



Distinguishing attack

Goal: differentiate between Feistel schemes/random permutations



Distinguishing attack

Goal: differentiate between Feistel schemes/random permutations



- Advantage: $\text{Adv}(A) = |\Pr[A(F) = 1] - \Pr[A(G) = 1]|$
 - F : Feistel scheme
 - G : Random permutation
 - A : Probabilistic algorithm

State of the art - Feistel with internal functions

	KPA	CPA	CCA	QCPA	QCCA
Ψ^1	1	1	1	1	1
Ψ^2	$2^{n/2}$	2	2	2	2
Ψ^3	$2^{n/2}$	$2^{n/2}$	3	n	3
Ψ^4	2^n	$2^{n/2}$	$2^{n/2}$	$2^{n/2}$	n
Ψ^5	$2^{3n/2}$	2^n	2^n	$2^{2n/3}$	$2^{2n/3}$
Ψ^6	2^{2n}	2^{2n}	2^{2n}	$2^{8n/5}$	$2^{8n/5}$

Table: Number of computations to distinguish Feistel schemes with **random internal functions** from random permutations (best-known attacks)

■: New (this work) $2^{8n/5}$ instead of 2^{2n} for the best known attack before us

State of the art - Feistel with internal permutations

	KPA	CPA	CCA	QCPA	QCCA
Ψ^1	1	1	1	1	1
Ψ^2	$2^{n/2}$	2	2	2	2
Ψ^3	$2^n(+)$	$2^{n/2}$	3	n	3
Ψ^4	2^n	$2^{n/2}$	$2^{n/2}$	$2^{n/2}$	n
Ψ^5	$2^{3n/2}$	2^n	2^n	$2^{2n/3}$	$2^{2n/3}$
Ψ^6	2^{2n}	2^{2n}	2^{2n}	$2^{8n/5}$	$2^{8n/5}$

Table: Number of computations to distinguish Feistel schemes with **random internal permutations** from random permutations (best-known attacks)

- \blacksquare : New (this work) instead of 2^{3n} everywhere for the best known attack before us
+: Worse complexity than for Feistel with internal functions

Plan

1. Introduction

2. Feistel Schemes

3. **Classical Generic Attacks on 6-round Feistel with Internal Permutations**

3.1 Classical attack

3.2 Computer Simulations

4. Quantum Generic Attacks on 6-round Feistel

Classical attack on Ψ^6 with internal permutations

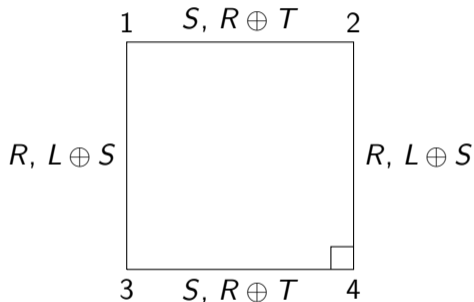
Assume the following system

$$(\mathcal{S}) \left\{ \begin{array}{l} R_1 = R_3 \\ R_2 = R_4 \\ S_1 = S_2 \\ S_3 = S_4 \\ L_1 \oplus L_4 = L_2 \oplus L_3 \\ L_1 \oplus S_1 = L_3 \oplus S_3 \\ R_1 \oplus T_1 = R_2 \oplus T_2 \\ R_3 \oplus T_3 = R_4 \oplus T_4 \end{array} \right.$$

Goal: number of collisions is $\approx 2 \times$ higher for Ψ_{perm}^6 compared to random permutations

Classical attack on Ψ^6 with internal permutations

System (S) can be geometrically represented as



(The small square in the right-hand corner below represents $L_1 \oplus L_2 \oplus L_3 \oplus L_4 = 0$)

Note: Same system as [Patarin, 2001] for the attack of Ψ_{func}^6

The number of collisions is $\approx 12\times$ higher for Ψ_{func}^6 compared to random permutations

Classical attack on Ψ^6 with internal permutations

Theorem

Assume that (1) $\begin{cases} R_1 = R_3 \\ R_2 = R_4 \\ S_1 = S_2 \\ L_1 \oplus L_4 = L_2 \oplus L_3 \end{cases}$ and that (2) $\begin{cases} X_1 = X_4 \\ Y_1 = Y_2 \\ Z_1 = Z_3 \\ U_1 = U_4 \end{cases}$

Then we will necessarily have for a Ψ^6 with internal permutations

$$(3) \begin{cases} S_3 = S_4 \\ L_1 \oplus S_1 = L_3 \oplus S_3 \\ R_1 \oplus T_1 = R_2 \oplus T_2 \\ R_3 \oplus T_3 = R_4 \oplus T_4 \end{cases}$$

\implies Number of collisions is $\approx 2 \times$ higher for Ψ_{perm}^6 compared to random permutations

Classical attack on Ψ^6 with internal permutations

Proof. Suppose we have (1) and (2), let us show that (3) is verified

- $X_1 = X_4 \iff L_1 \oplus f_1(R_1) = L_4 \oplus f_1(R_4) \underset{L_1 \oplus L_4 = L_2 \oplus L_3}{\iff} L_3 \oplus f_1(R_3) = L_2 \oplus f_1(R_2) \iff X_3 = X_2$

Classical attack on Ψ^6 with internal permutations

Proof. Suppose we have (1) and (2), let us show that (3) is verified

- $X_1 = X_4 \iff L_1 \oplus f_1(R_1) = L_4 \oplus f_1(R_4) \underset{L_1 \oplus L_4 = L_2 \oplus L_3}{\iff} L_3 \oplus f_1(R_3) = L_2 \oplus f_1(R_2) \iff X_3 = X_2$
- $Y_1 = Y_2 \iff R_1 \oplus f_2(X_1) = R_2 \oplus f_2(X_2) \iff R_3 \oplus f_2(X_4) = R_4 \oplus f_2(X_3) \iff Y_3 = Y_4$

Classical attack on Ψ^6 with internal permutations

Proof. Suppose we have (1) and (2), let us show that (3) is verified

- $X_1 = X_4 \iff L_1 \oplus f_1(R_1) = L_4 \oplus f_1(R_4) \underset{L_1 \oplus L_4 = L_2 \oplus L_3}{\iff} L_3 \oplus f_1(R_3) = L_2 \oplus f_1(R_2) \iff X_3 = X_2$
- $Y_1 = Y_2 \iff R_1 \oplus f_2(X_1) = R_2 \oplus f_2(X_2) \iff R_3 \oplus f_2(X_4) = R_4 \oplus f_2(X_3) \iff Y_3 = Y_4$
- $Z_1 = Z_3 \iff X_1 \oplus f_3(Y_1) = X_3 \oplus f_3(Y_3) \iff X_4 \oplus f_3(Y_4) = X_2 \oplus f_3(Y_2) \iff Z_4 = Z_2$
- $U_1 = U_4 \iff Y_1 \oplus f_4(Z_1) = Y_4 \oplus f_4(Z_4) \iff Y_2 \oplus f_4(Z_2) = Y_3 \oplus f_4(Z_3) \iff U_2 = U_3$
- $S_1 = S_2 \iff Z_1 \oplus f_5(U_1) = Z_2 \oplus f_5(U_2) \iff Z_3 \oplus f_5(U_3) = Z_4 \oplus f_5(U_4) \iff S_3 = S_4$

Classical attack on Ψ^6 with internal permutations

Moreover, we have

- $T_1 = U_1 \oplus f_6(S_1), T_2 = U_2 \oplus f_6(S_2) \implies U_1 \oplus U_2 = T_1 \oplus T_2$
- $U_1 = Y_1 \oplus f_4(Z_1), U_3 = Y_3 \oplus f_4(Z_3) \implies U_1 \oplus U_3 = Y_1 \oplus Y_3 \implies U_1 \oplus U_2 = Y_1 \oplus Y_3$
- $Y_1 = R_1 \oplus f_2(X_1), Y_4 = R_4 \oplus f_2(X_4) \implies Y_1 \oplus Y_4 = R_1 \oplus R_4 \implies Y_1 \oplus Y_3 = R_1 \oplus R_2$

Hence $T_1 \oplus T_2 = R_1 \oplus R_2$

Classical attack on Ψ^6 with internal permutations

Moreover, we have

- $T_1 = U_1 \oplus f_6(S_1), T_2 = U_2 \oplus f_6(S_2) \implies U_1 \oplus U_2 = T_1 \oplus T_2$
- $U_1 = Y_1 \oplus f_4(Z_1), U_3 = Y_3 \oplus f_4(Z_3) \implies U_1 \oplus U_3 = Y_1 \oplus Y_3 \implies U_1 \oplus U_2 = Y_1 \oplus Y_3$
- $Y_1 = R_1 \oplus f_2(X_1), Y_4 = R_4 \oplus f_2(X_4) \implies Y_1 \oplus Y_4 = R_1 \oplus R_4 \implies Y_1 \oplus Y_3 = R_1 \oplus R_2$

Hence $T_1 \oplus T_2 = R_1 \oplus R_2$

- $T_3 = U_3 \oplus f_6(S_3), T_4 = U_4 \oplus f_6(S_4) \implies U_3 \oplus U_4 = T_3 \oplus T_4 \implies T_3 \oplus T_4 = U_1 \oplus U_2$

So $R_3 \oplus R_4 = T_3 \oplus T_4$

Classical attack on Ψ^6 with internal permutations

- $S_1 = Z_1 \oplus f_5(U_1), S_4 = Z_4 \oplus f_5(U_4) \implies S_1 \oplus S_4 = Z_1 \oplus Z_4 \implies S_1 \oplus S_3 = Z_1 \oplus Z_2$
- $Z_1 = X_1 \oplus f_3(Y_1), Z_2 = X_2 \oplus f_3(Y_2) \implies Z_1 \oplus Z_2 = X_1 \oplus X_2$
- $X_1 = L_1 \oplus f_1(R_1), X_3 = L_3 \oplus f_1(R_3) \implies X_1 \oplus X_3 = L_1 \oplus L_3 \implies X_1 \oplus X_2 = L_1 \oplus L_3$

Hence $S_1 \oplus S_3 = L_1 \oplus L_3$



Computer simulations for $n = 8$ with 10 000 trials

Nb of solutions	Random permutations	Feistel with internal permutations	Feistel with internal functions
0	7 756	6 023	530
2	1 980	3 069	1 570
4	242	754	2 198
6	21	133	2 154
8	1	19	1 670
10	0	1	980
12	0	1	510
14	0	0	224
16	0	0	99
18	0	0	40
20	0	0	17
22	0	0	5
24	0	0	3

Computer simulations for $n = 8$ with 10 000 trials

$$\text{Adv}_{\Psi_{\text{perm}}^6} = 0.1733 \text{ and } \text{Adv}_{\Psi_{\text{func}}^6} = 0.7636$$

Moreover we have

- $\mathcal{N}_{\text{rand}} \approx 0.5062$
- $\mathcal{N}_{\Psi_{\text{perm}}^6} \approx 1.0126$
- $\mathcal{N}_{\Psi_{\text{func}}^6} \approx 6.0098$

$$\text{Therefore } \mathcal{N}_{\Psi_{\text{perm}}^6} \approx 2 \mathcal{N}_{\text{rand}} \text{ and } \mathcal{N}_{\Psi_{\text{func}}^6} \approx 12 \mathcal{N}_{\text{rand}}$$

Classical attack on Ψ^6 with internal permutations

Conclusion of the first result:

- 4 points classical attack on Ψ_{perm}^6
- For Ψ_{perm}^6 the nb of collisions is $\approx 2\times$ higher compared to random permutations
- Complexity is in $\mathcal{O}\left(\frac{q^4}{2^{8n}}\right)$ since we have 8 equations on 4 indices
 \implies Complexity reduced to $\mathcal{O}(2^{2n})$ from $\mathcal{O}(2^{3n})$

Plan

1. Introduction

2. Feistel Schemes

3. Classical Generic Attacks on 6-round Feistel with Internal Permutations

4. Quantum Generic Attacks on 6-round Feistel

- 4.1 Ambainis's Algorithm for Distinctness Problem
- 4.2 Childs and Eisenberg Algorithm for Subset Finding
- 4.3 Application to 6-round Feistel Schemes

Ambainis' algorithm overview

Problem: Given N values x_1, \dots, x_N from a set \mathcal{X} where $|\mathcal{X}| = M$, are there k distinct indices $1 \leq i_1 < i_2 < \dots < i_k \leq N$ such that $x_{i_1} = x_{i_2} = \dots = x_{i_k}$?

Ambainis' result [Ambainis, 2004]

Let $r \geq k$, $r = o(N)$

There is a quantum algorithm that solves element k -distinctness with

- Time: $\tilde{O}\left(\max\left(\frac{N^{k/2}}{r^{(k-1)/2}}, r\right)\right)$
- Queries: $\mathcal{O}\left(\max\left(\frac{N^{k/2}}{r^{(k-1)/2}}, r\right)\right)$
- Memory: $\tilde{O}(r)$

Ambainis' algorithm overview

Problem: Given N values x_1, \dots, x_N from a set \mathcal{X} where $|\mathcal{X}| = M$, are there k distinct indices $1 \leq i_1 < i_2 < \dots < i_k \leq N$ such that $x_{i_1} = x_{i_2} = \dots = x_{i_k}$?

Ambainis' result [Ambainis, 2004]

Let $r \geq k$, $r = N^{k/(k+1)}$

There is a quantum algorithm that solves element k -distinctness with

- Time: $\tilde{O}(N^{k/(k+1)})$
- Queries: $\mathcal{O}(N^{k/(k+1)})$
- Memory: $\tilde{O}(N^{k/(k+1)})$

Childs and Eisenberg algorithm overview

Problem: Given $f : \mathcal{X} \rightarrow \mathcal{Y}$ where

- \mathcal{X}, \mathcal{Y} are finite sets
- $|\mathcal{X}| = M$
- \mathcal{R} a relation in $(\mathcal{X} \times \mathcal{Y})^k$

are there some k -subset $\{x_1, \dots, x_k\} \subset \mathcal{X}$ such that $((x_1, f(x_1)), \dots, (x_k, f(x_k))) \in \mathcal{R}$?

Childs and Eisenberg algorithm overview

Childs and Eisenberg algorithm [Childs - Eisenberg, 2005]

Let $r \geq k$, $r = o(N)$

There is a quantum algorithm that solves the k -subset problem with

- Queries: $\mathcal{O}\left(\max\left(\left(\frac{N}{r}\right)^{k/2}(\sqrt{r} + g(r)), r\right)\right)$
- Memory: $\tilde{\mathcal{O}}(r)$

g is related to \mathcal{R} and the data structures (more details in the paper)

Our revised analysis of Childs and Eisenberg

Our revised analysis on Childs and Eisenberg algorithm

Let $r \geq k$, $r = o(N)$

There is a quantum algorithm that solves the k -subset problem with

- Time: $\tilde{\mathcal{O}}\left(\max\left(\left(\frac{N}{r}\right)^{k/2}(\sqrt{r} + f(r)), r\right)\right)$
- Queries: $\mathcal{O}\left(\max\left(\left(\frac{N}{r}\right)^{k/2}(\sqrt{r} + g(r)), r\right)\right)$
- Memory: $\tilde{\mathcal{O}}(r)$

f and g are related to \mathcal{R} , but in our case, they are negligible compared to \sqrt{r}

Our revised analysis of Childs and Eisenberg

Our revised analysis on Childs and Eisenberg algorithm

Let $r \geq k$, $r = N^{k/(k+1)}$

There is a quantum algorithm that solves the k -subset problem with

- Time: $\tilde{O}(N^{k/(k+1)})$
- Queries: $\tilde{O}(N^{k/(k+1)})$
- Memory: $\tilde{O}(N^{k/(k+1)})$

Quantum attack on Ψ^6

For Ψ^6 we need to find

$$(\mathcal{S}) \left\{ \begin{array}{l} R_1 = R_3 \\ R_2 = R_4 \\ S_1 = S_2 \\ S_3 = S_4 \\ L_1 \oplus L_4 = L_2 \oplus L_3 \\ L_1 \oplus S_1 = L_3 \oplus S_3 \\ R_1 \oplus T_1 = R_2 \oplus T_2 \\ R_3 \oplus T_3 = R_4 \oplus T_4 \end{array} \right.$$

Child and Eisenberg's algorithm will find solutions to this system with a complexity of $O(2^{8n/5})$ since $k = 4$ and $N = 2^{2n}$




Conclusion

- First result:
 - 4 points classical attack on Ψ^6 with internal permutations
 - Complexity reduced to $\mathcal{O}(2^{2n})$ from $\mathcal{O}(2^{3n})$
 - Detailed analysis on Ψ^6 with internal functions
- Second result:
 - Detailed analysis on Childs and Eisenberg quantum algorithm time complexity
 - Quantum attack on Ψ^6
 - Complexity reduced to $\mathcal{O}(2^{8n/5})$
- Open problem: Complexity worse for $\Psi^3, \Psi^9, \Psi^{12}, \Psi^{15} \dots$ with internal permutations than for internal functions, but not for Ψ^6 as explained here

Conclusion

Thank You
Questions?

References

-  Andris Ambainis (2004)
Quantum walk algorithm for element distinctness
45th Symposium on Foundations of Computer Science (FOCS) pages 22–31
-  Andrew M. Childs and Jason M. Eisenberg (2005)
Quantum algorithms for subset finding
Quantum Inf. Comput. pages 593–604
-  Jacques Patarin (2001)
Generic attacks on Feistel schemes
AsiaCrypt pages 222-238