PRESENT Cipher

Walkie Talkie

Department of EECS
Indian Institute of Technology Bhilai

December 5, 2021

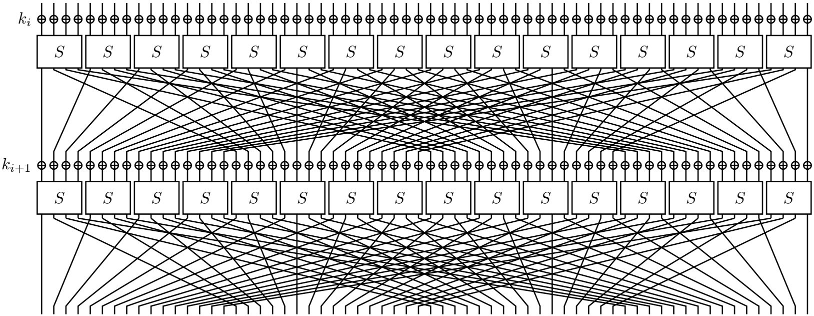
Outline

1. Introduction
2. Cipher Specifications
3. DC
4. Linear Cryptanalysis
5. Integral property
6. Brownie Point Nominations
7. Conclusion

The Present Cipher

- Ultra-Lightweight block cipher.
- Developed by the Orange Labs (France), Ruhr University Bochum (Germany) and the Technical University of Denmark in 2007.
- Supports 64 bits block size and 80 or 128 bits key sizes with 31 rounds.
- Designed to be used in micro-controllers and hardware where high chip performance and low power consumption are required.

Substitution / Permutation



x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$S[x]$	C	5	6	B	9	0	A	D	3	E	F	8	4	7	1	2

Outline

1. Introduction
2. Cipher Specifications
3. DC
4. Linear Cryptanalysis
5. Integral property
6. Brownie Point Nominations
7. Conclusion

Cipher Design

- PRESENT-80 is an example of SP-network.
- 4-bit S-Box is applied 16 times in parallel for the 64-bit input during each round.

High level psuedo-code of PRESENT algorithm

generateRoundKeys()
for $i = 1$ **to** 31 **do**
    addRoundKey($\textsc{State}$,K_i)
    sBoxLayer($\textsc{State}$)
    pLayer($\textsc{State}$)
addRoundKey($\textsc{State}$,K_{32})

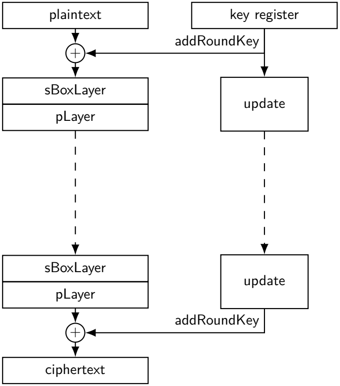
Cipher Design contd.

Add Round Key

- Round key $K_i = k_{63}, k_{62} \ldots k_0$ for $1 \leq i \leq 32$.
- Current state $S = s_{63}, s_{62} \ldots s_0$.

$$S \rightarrow S \oplus K_i$$
$$\Longrightarrow \; s_t \rightarrow s_t \oplus k_t$$

for $0 \leq t \leq 63$



Substitution Layer

Denote Fourier coefficient of S-Box.

$$S_b^W(a) = \sum_{x \in \mathbb{F}_2^4} (-1)^{\langle b, S(x)\rangle + \langle a, x\rangle} \tag{1}$$

PRESENT S-Box satisfies the following conditions.

- For any fixed input difference $\Delta_I \in \mathbb{F}_2^4, \Delta_I \neq 0$ and output difference $\Delta_O \in \mathbb{F}_2^4, \Delta_I \neq 0$, the following condition is satisfied

$$|\{x \in \mathbb{F}_2^4 \mid S(\Delta_I + x) + S(x) = \Delta_O\}| \leq 4$$

- For any fixed input difference $\Delta_I \in \mathbb{F}_2^4, \Delta_I \neq 0$ and output difference $\Delta_O \in \mathbb{F}_2^4$ such that $wt(\Delta_O) = wt(\Delta_I) = 1$, the following condition is satisfied

$$\{x \in \mathbb{F}_2^4 \mid S(\Delta_I + x) + S(x) = \Delta_O\} = \Phi$$

where $wt(x)$ is the hamming weight of x.

Substitution Layer

- For all $a \in \mathbb{F}_2^4, a \neq 0$ and $b \in \mathbb{F}_4$, $|S_b^W(a)| \leq 8$ holds.
- For all $a \in \mathbb{F}_2^4, a \neq 0$ and $b \in \mathbb{F}_4$ such that $wt(b) = wt(a) = 1$, $S_b^W(a) = \pm 4$ holds.

Cipher Design Contd.

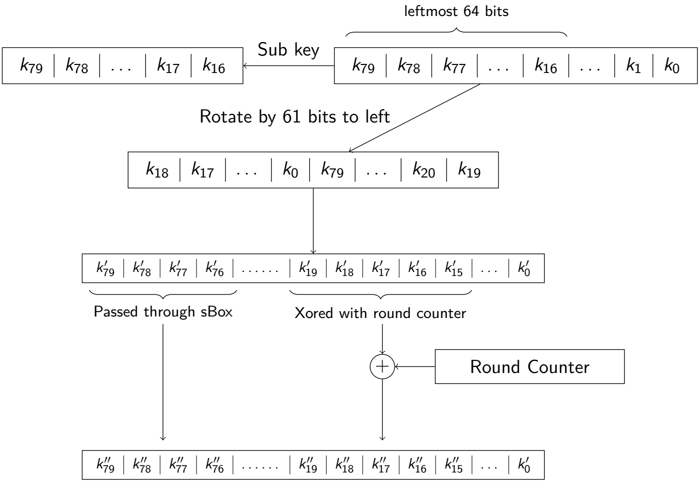
Permutation Layer

- Bit permutation.
- Bit i of STATE is moved to bit position $P(i)$.

$$P(i) = \begin{cases} 16.i \quad mod \quad 63 & i \in \{0, 1, \ldots 62\} \\ 63 & i = 63 \end{cases}$$

Key schedule Algorithm

We discuss the 80-bit key schedule algorithm.



Outline

1. Introduction
2. Cipher Specifications
3. DC
4. Linear Cryptanalysis
5. Integral property
6. Brownie Point Nominations
7. Conclusion

Round Reduced Attack

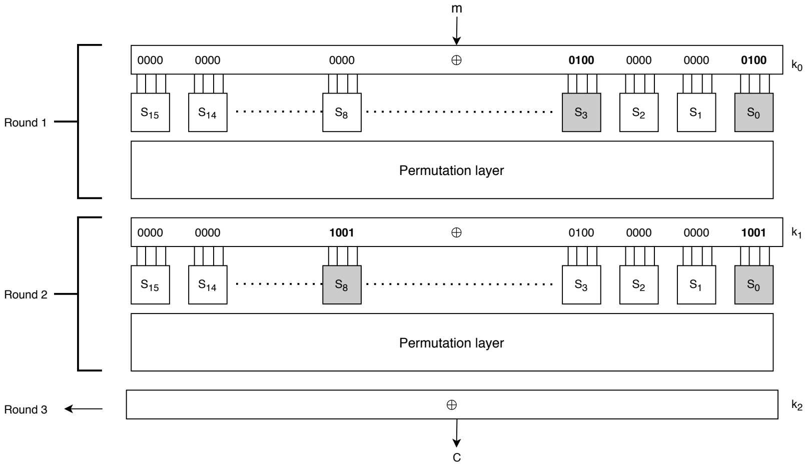


Figure: Attack Model

The Difference Distribution Table

Figure: DDT of the S-box

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	0	0	4	0	0	0	4	0	4	0	0	0	4	0	0
2	0	0	0	2	0	4	2	0	0	0	2	0	2	2	2	0
3	0	2	0	2	2	0	4	2	0	0	2	2	0	0	0	0
4	0	0	0	0	0	4	2	2	0	2	2	0	2	0	2	0
5	0	2	0	0	2	0	0	0	0	2	2	2	4	2	0	0
6	0	0	2	0	0	0	2	0	2	0	0	4	2	0	0	4
7	0	4	2	0	0	0	2	0	2	0	0	0	2	0	0	4
8	0	0	0	2	0	0	0	2	0	2	0	4	0	2	0	4
9	0	0	2	0	4	0	2	0	2	0	0	0	2	0	4	0
A	0	0	2	2	0	4	0	0	2	0	2	0	0	2	2	0
B	0	2	0	0	2	0	0	0	4	2	2	2	0	2	0	0
C	0	0	2	0	0	4	0	2	2	2	2	0	0	0	2	0
D	0	2	4	2	2	0	0	2	0	0	2	2	0	0	0	0
E	0	0	2	2	0	0	2	2	2	2	0	0	2	2	0	0
F	0	4	0	0	4	0	0	0	0	0	0	0	0	0	4	4

Differential Characteristics

Table: Characteristics

Rounds		Diff.	Prob.
I		$x_0 = 4,\ x_4 = 4$	
R_1	k_0	$x_0 = 4,\ x_4 = 4$	1
R_1	S	$x_0 = 5,\ x_3 = 5$	2^{-4}
R_1	P	$x_0 = 9,\ x_8 = 9$	1
R_2	k_1	$x_0 = 9,\ x_8 = 9$	1

Characteristic

$$(x_0 = 4,\ x_3 = 4) \xrightarrow{\text{R}} (x_0 = 9,\ x_8 = 9)$$

Idea of filtering

- Decrease Wrong pair $\rightarrow$ Idea of filtering
- Observe from the DDT that transitions from $9 \rightarrow \{2, 4, 6, 8, c, e\}$
- Thus, after the effect of permutation layer of the second round, $c_1 \oplus c_2$ must belong to the set given below : $\{\{x_4 = 1, x_6 = 1\}, \{x_6 = 1, x_8 = 1\}, \{x_4 = 1, x_6 = 1, x_8 = 1\}, \{x_6 = 1, x_{12} = 1\}, \{x_6 = 1, x_8 = 1, x_{12} = 1\}, ...\}$ We have written code for this.

Filtering

Thus, message pair leading to the cipher text difference other than the above set, can be discarded. So, after filtering only 2^{14} plaintext pairs are left in our case.

Key Guess

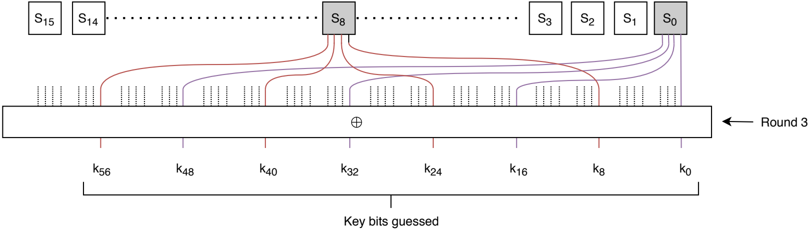


Figure: Guess 8 bits of the key k_2

We are able to find 8 bits of key k_2. In our case only 8 bit right subkey holds for all 2^{14} filtered pairs or in other word highest counter indicate the right 8 bit subkey.

Complexity Analysis

Complexity

(Data, Time, Memory) $= (2^{19}, 2^{25.17}, 2^{14})$

Outline

1 Introduction

2 Cipher Specifications

3 DC

4 Linear Cryptanalysis

5 Integral property

6 Brownie Point Nominations

7 Conclusion

LAT of the S-box

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	8	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
1	-	-	-	-	-	-4	-	-4	-	-	-	-	-	-4	-	4
2	-	-	2	2	-2	-2	-	-	2	-2	-	4	-	4	-2	2
3	-	-	2	2	2	-2	-4	-	-2	2	-4	-	-	-	-2	-2
4	-	-	-2	2	-2	-2	-	4	-2	-2	-	-4	-	-	-2	2
5	-	-	-2	2	-2	2	-	-	2	2	-4	-	4	-	2	2
6	-	-	-	-4	-	-	-4	-	-	-4	-	-	4	-	-	-
7	-	-	-	4	4	-	-	-	-	-4	-	-	-	-	4	-
8	-	-	2	-2	-	-	-2	2	-2	2	-	-	-2	2	4	4
9	-	4	-2	-2	-	-	2	-2	-2	-2	-4	-	-2	2	-	-
A	-	-	4	-	2	2	2	-2	-	-	-	-4	2	2	-2	2
B	-	-4	-	-	-2	-2	2	-2	-4	-	-	-	2	2	2	-2
C	-	-	-	-	-2	-2	-2	-2	4	-	-	-4	-2	2	2	-2
D	-	4	4	-	-2	-2	2	2	-	-	-	-	2	-2	2	-2
E	-	-	2	2	-4	4	-2	-2	-2	-2	-	-	-2	-2	-	-
F	-	4	-2	2	-	-	-2	-2	-2	2	4	-	2	2	-	-

Table: Linear Approximation Table

Observations

- Maximum bias $\leq 2^{-2}$
- For a Single bit $\leq 2^{-3}$
- Bias Computation

$$2^{m-1} \prod_{i=1}^{m} \epsilon_i$$

Analysis

- Total 3 Cases to analyse the linear approximation of 4 rounds
- Results to bound the linear approximation bias for 28 rounds
- Let ϵ_{4R} be the maximal bias of a linear approximation of four rounds of present, then $\epsilon_{4R} \leq \frac{1}{2^7}$

Proof. . .

- Bias Calculation for 4 S-boxes:

$$\epsilon_4^4 \leq 2^{4-1} \times (2^{-2})^2 \times (2^{-3})^2 \implies \epsilon_4^4 \leq 2^{-7}$$

- Bias Calculation for 5 S-boxes:

$$\epsilon_4^5 \leq 2^{5-1} \times (2^{-2})^4 \times (2^{-3}) \implies \epsilon_4^5 \leq 2^{-7}$$

Resistant to the Linear Attack

- Maximal Bias for 28-round linear approximation
- Now assume that the cryptanalyst needs to approximate only only 28 rounds
- So total 2^{86} known plaintexts are required
- Which are greater than the available plaintexts space, that is 2^{64}
- Proved

Outline

1. Introduction
2. Cipher Specifications
3. DC
4. Linear Cryptanalysis
5. Integral property
6. Brownie Point Nominations
7. Conclusion

5-round integral distinguishers for PRESENT

Input:
(ccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccaaaa)
Output:
(??bbbb)
c: constant bit, a: active bit, b: balanced bit, ?: unknown bit

Note

In this experiment, we are taking 2^{12} messages and varying right most 4 bits.

Outline

1. Introduction
2. Cipher Specifications
3. DC
4. Linear Cryptanalysis
5. Integral property
6. Brownie Point Nominations
7. Conclusion

Brownie Point

1. Using the idea of differential and filtering taught in the course, we have implemented a differential attack on 3 Rounds of PRESENT.
2. We have verified 5 Rounds integral property of PRESENT.

Outline

1 Introduction

2 Cipher Specifications

3 DC

4 Linear Cryptanalysis

5 Integral property

6 Brownie Point Nominations

7 Conclusion

Conclusion

- Understanding the design choices of PRESENT cipher.
- Properties of S-box
- Resistance against cryptographic attacks
- Implementation of 3-Rounds differential attack
- verify 5 round integral property
- Linear Cryptanalysis

Thanks

Team Members

- Ajay Tarole
- Ashish Kumar Suraj
- Rudraksh Kashyap

Implementation Info

- Github Link: https://github.com/ajay0090/PRESENT-Cipher