PRESENT Cipher

Thunderspy

Department of Electrical Engineering and Computer Science
Indian Institute of Technology Bhilai

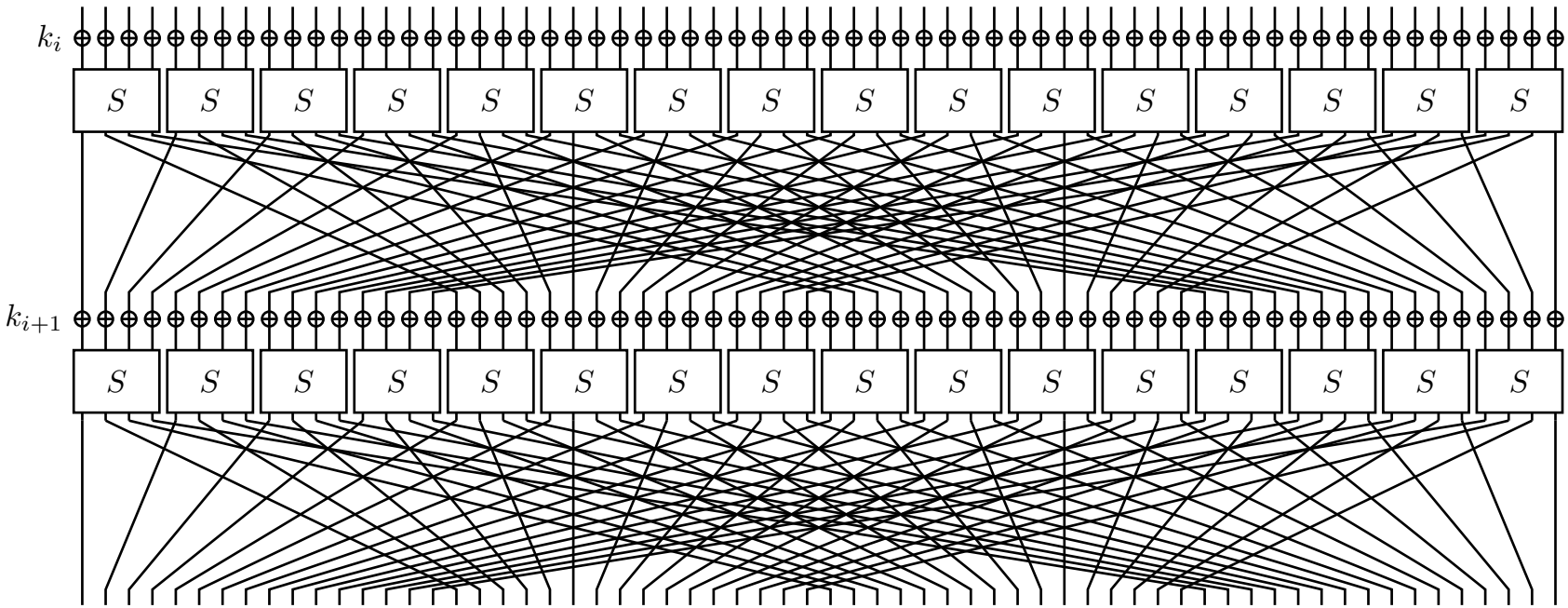
November 27, 2020

Outline

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.
- Intended to be used in circumstances 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

Image source : iacr.org/authors/tikz/

Outline

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

1: generateRoundKeys()
2: **for** $i = 1$ **to** 31 **do**
3: addRoundKey(STATE,K_i)
4: sBoxLayer(STATE)
5: pLayer(STATE)
6: addRoundKey(STATE,K_{32})

Cipher Design contd.

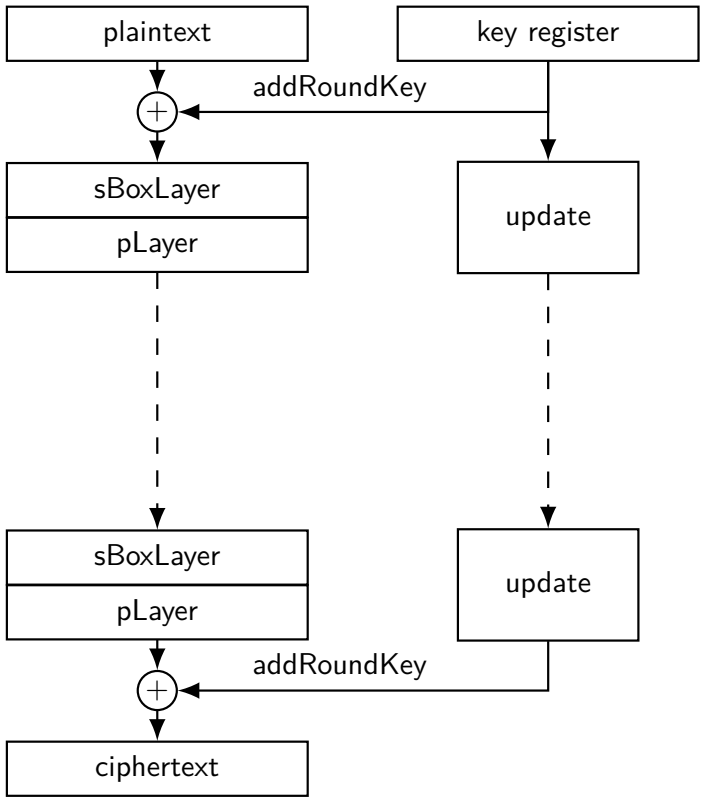
Add Round Key

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

$$S \rightarrow S \oplus K_i$$

$$\Longrightarrow \quad s_t \rightarrow s_t \oplus k_t$$

for $0 \leq t \leq 63$



Substitution Layer $S : \mathbb{F}_2^4 \rightarrow \mathbb{F}_2^4$

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.

Cipher Design Contd.

- 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.

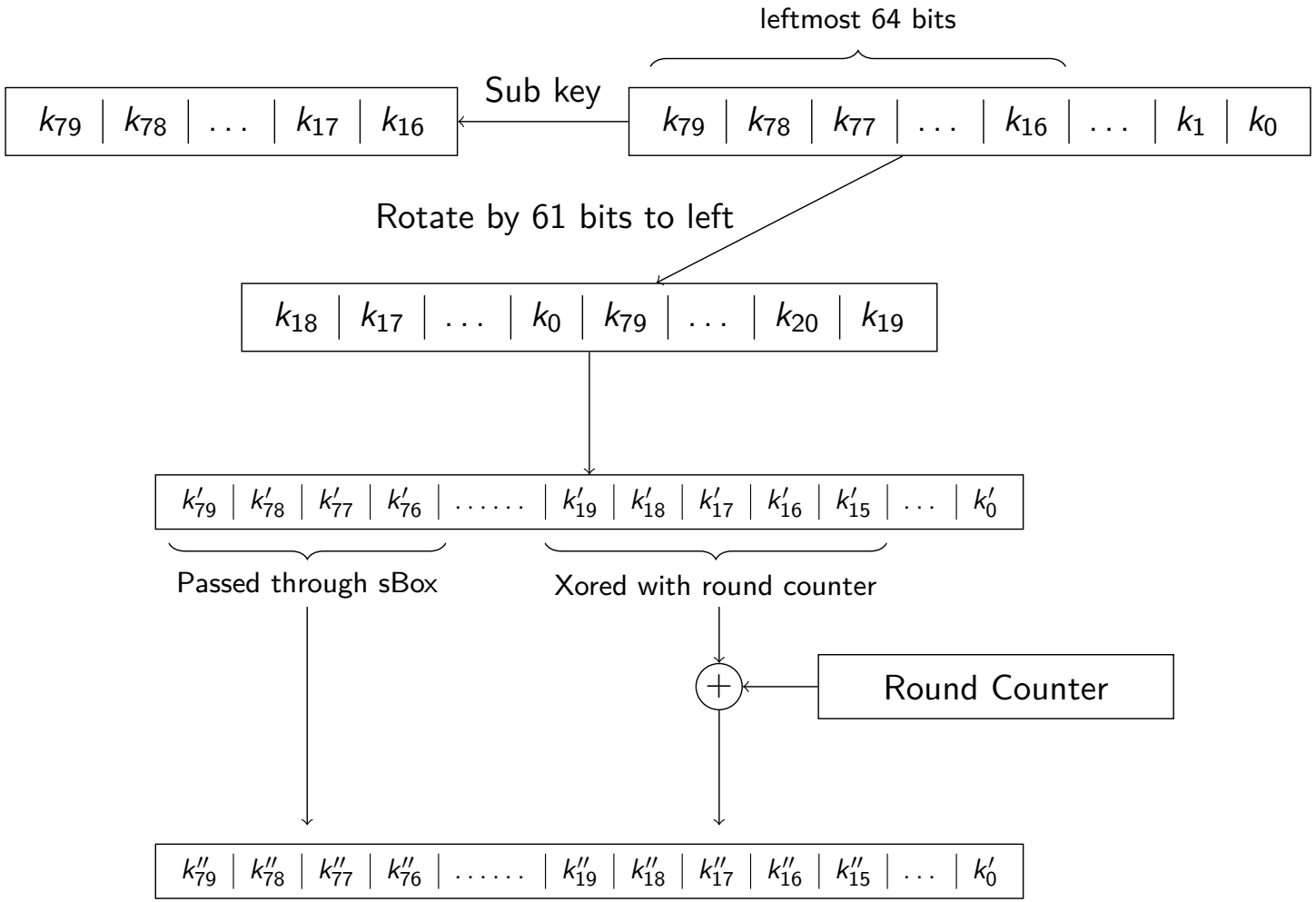
Permutation Layer

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

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

Key schedule Algorithm

We discuss the 80-bit key schedule algorithm.



Outline

Round Reduced Attack

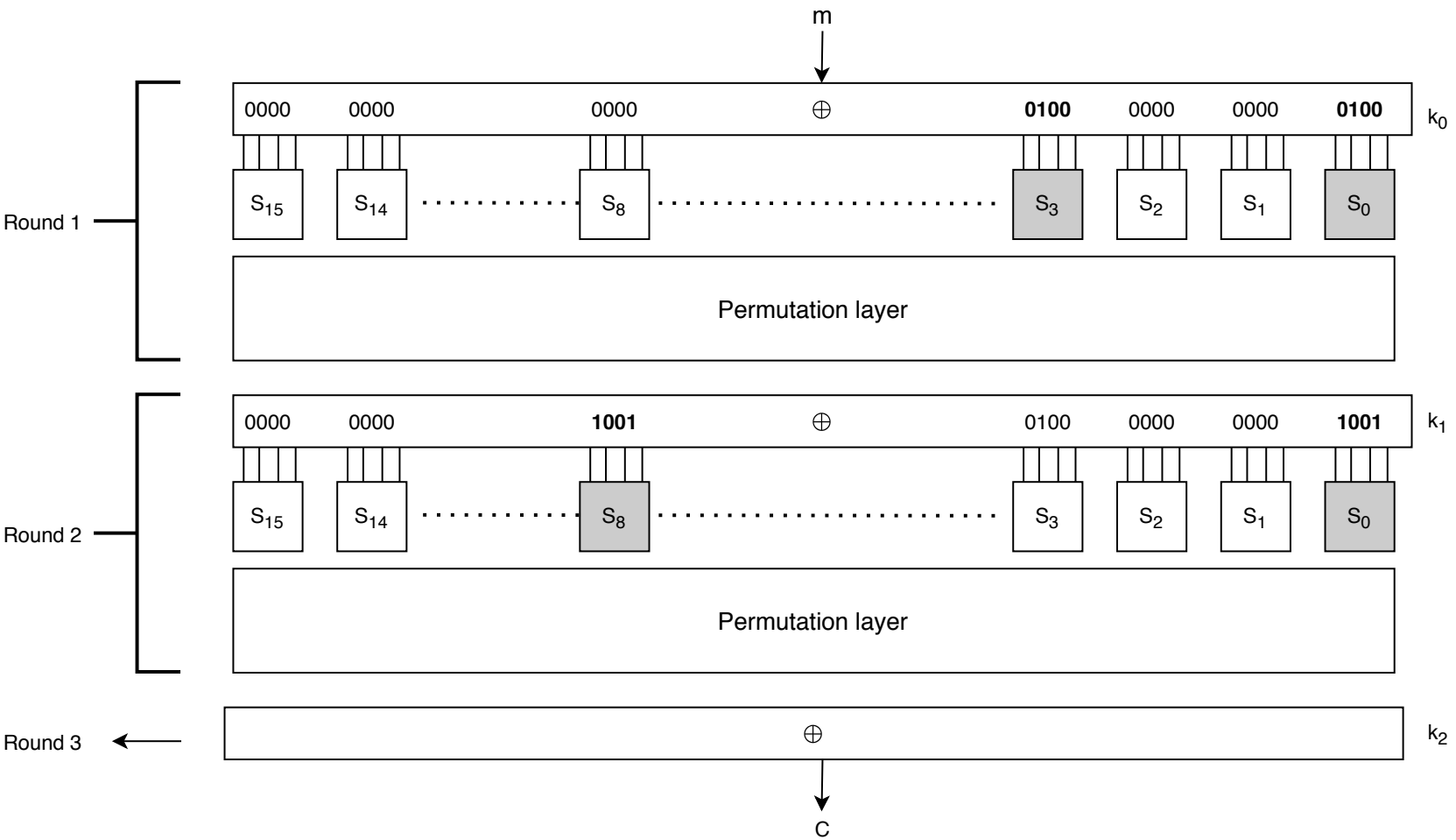


Figure: Attack Model

The Difference Distribution Table

	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

Table: DDT of the S-box

Differential 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

Table: Characteristics

Characteristic

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

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.

Key Guess

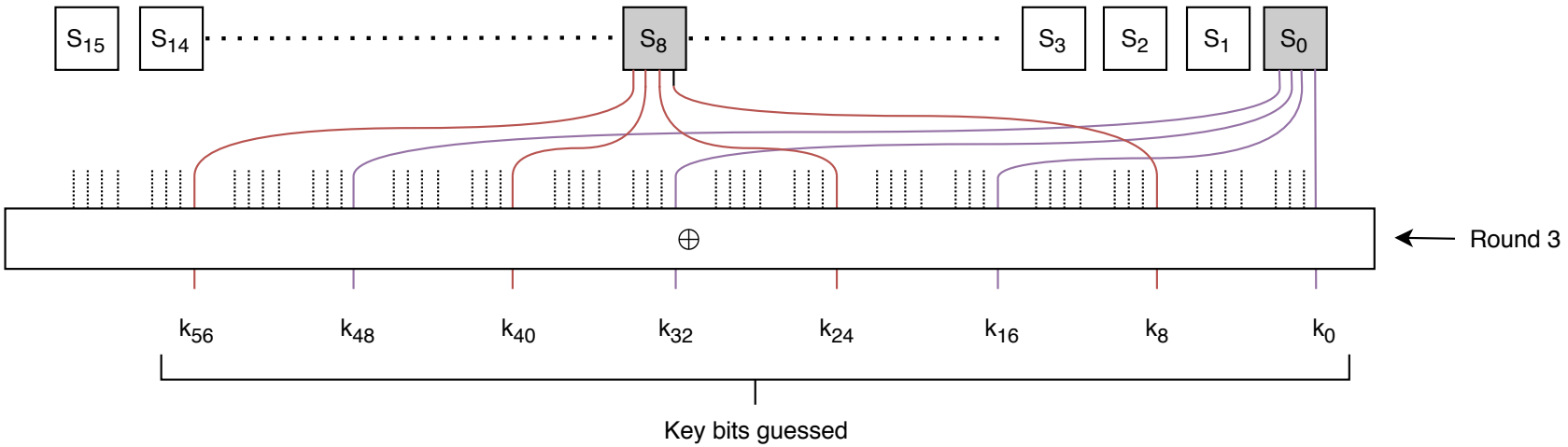


Figure: Attack Model

- Guess 8 bits of the key k_2 as shown in the figure.
- The probability that the result of partial decryption probabilistically matches Δout is $<< 1$.
- Thus, the right guess reaches Δout more than any other wrong guess

Outline

The Linear Approximation Table

	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: LAT of the S-box

Observations from the LAT

- Maximum bias of all linear approximations $\leq 2^{-2}$
- Maximum linear approximation of a single bit is $\leq 2^{-3}$.

Recall

- The Pilling-up lemma
- It allows us to compute the **bias** of a set of combined linear approximations.

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

Analysis

- We analyse the best linear approximation of 4 rounds of PRESENT.
- We then use it directly to bound the maximal bias of a 28-round linear approximation.

Theorem

Let ϵ_4 be the maximal bias of a linear approximation of four rounds of present. Then $\epsilon_4 \leq 2^{-7}$.

Outline of the Proof

- Depending upon the number of active S-boxes involved, we analyse three possible cases.
- Case 1 : 1 Active S-box in each Round

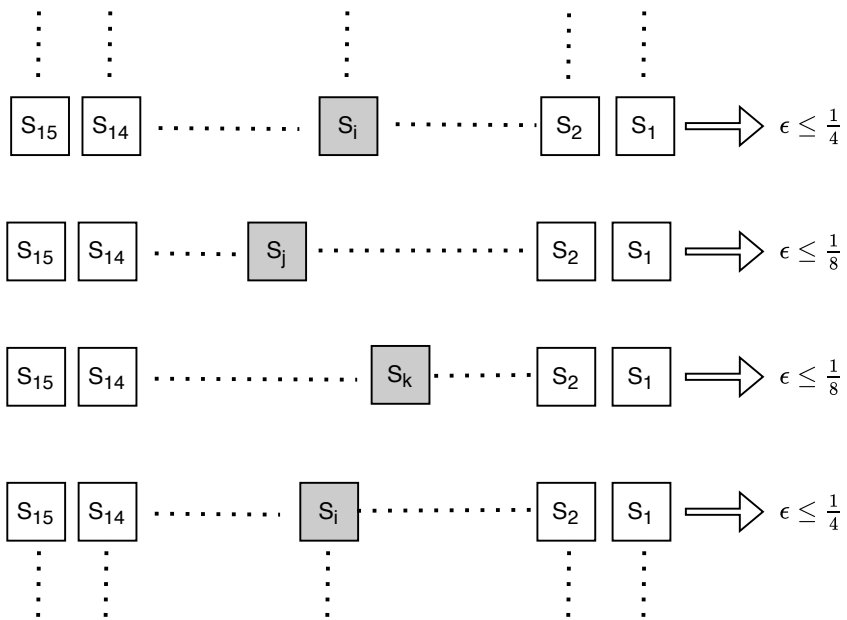


Figure: Bias Calculation

Outline of the Proof Cont..

- Bias Calculation :

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

$$\epsilon_4^{(4)} \leq 2^{-7}$$

- Case 2 : 5 Active S-boxes involved

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

$$\epsilon_4^{(5)} \leq 2^{-7}$$

- Case 3 : More than 5 Active S-boxes involved

$$\epsilon_4^{(i)} \leq 2^{i-1} \times (2^{-2})^i \quad \textit{for} \quad i > 5$$

Detailed Proof is given in the report.

Requirements for a Successful LC attack

- Maximal Bias of 28-round linear approximation

$$\epsilon_{28} \leq 2^6 \times \epsilon_4^7 = 2^6 \times (2^{-7})^7 \implies \epsilon_{28} \leq 2^{-43}$$

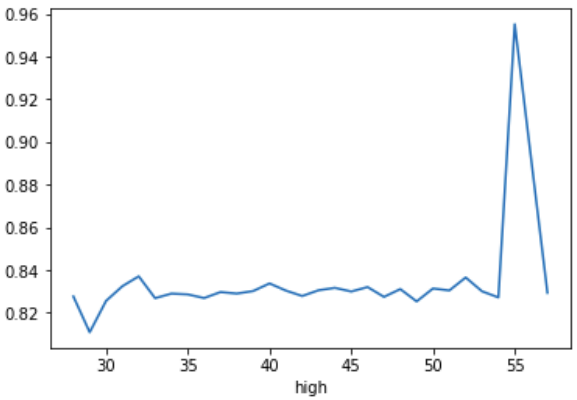
- Assuming the cryptanalyst needs to approximate only 28 Rounds.
- Even for single bit key recovery, $N = c|\epsilon|^{-2}$, where constant $c \geq 2$ known plain-texts are required.
- Thus, 2^{86} known plain-texts are required.
- The data requirement exceeds the total plain-text space available, which is 2^{64}.
- PRESENT-80 is resistant to Linear attack.

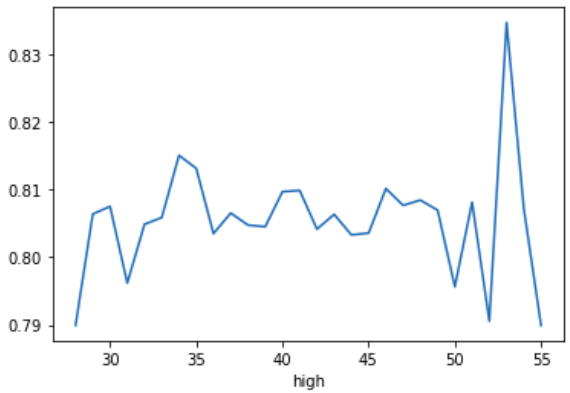
Outline

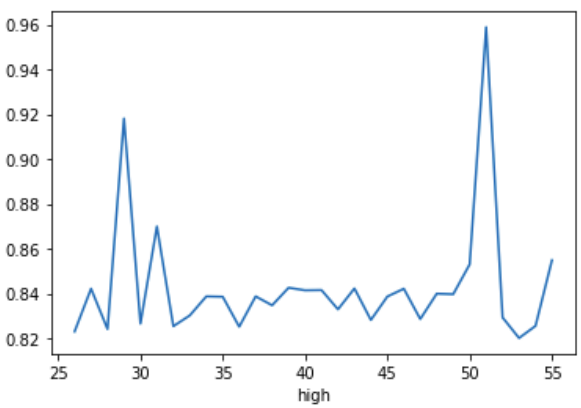
The Experiment

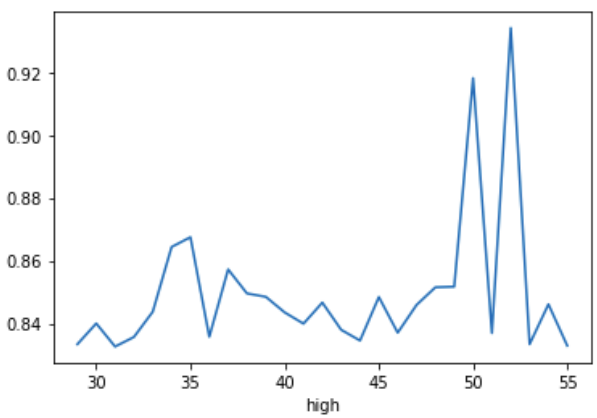
- Correlation between the encryption time of PRESENT algorithm and the number of set bits in the key.
- Generate random messages of 64 bit and corresponding to each message generate random keys with count of set bits varying from 1 to 79.

The Experiment Cont..

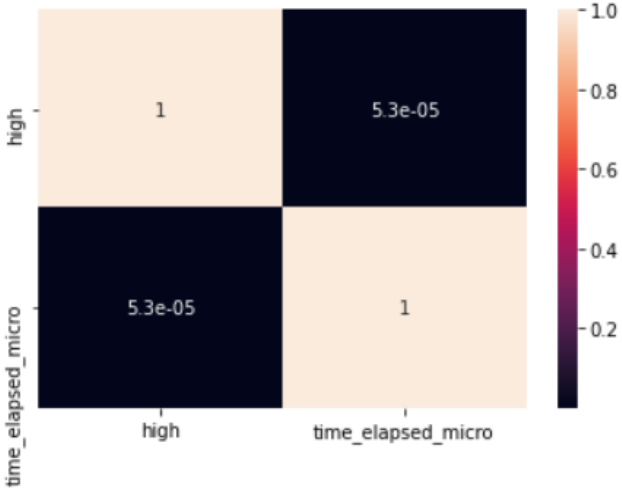


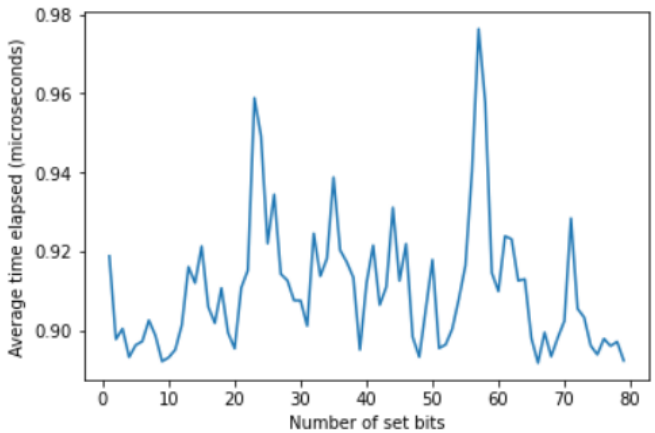






The Experiment Cont..





- Near to zero correlation exists.
- No or very weak linear relationship between the variables.

Outline

Brownie Points

Implementation of DC of Reduced Round PRESENT Cipher

We could not find any implementation of Differential analysis on the round reduced version of PRESENT. So, using the idea of differential and filtering taught in the course, we have implemented a differential attack on 3 Rounds of PRESENT.

Brownie Points Cont..

Correlation Analysis

We experimented on various side-channel characteristics of PRESENT that could affect the run time of encryption function. Although on initial experimentation, we found some correlation between number of bits high in the key and the time taken for encryption. But, on randomising the messages also, we could not find any effective correlation. We believe that, this should be further experimented, as there are no paper available on this topic.

Outline

Conclusion

- Understanding the design choices of PRESENT cipher.
- Properties of S-box
- Resistance against cryptographic attacks
- Analysis of theoretical differential attack on 16-rounds PRESENT
- Implementation of 3-Rounds differential attack
- Linear Cryptanalysis
- Side channel Attack developed by us

Thanks

Team Members

- Abhishek Shingane
- Gopal Ramesh Dahale
- Kumari Rani

Implementation Info

- Github Link: Present-Cipher