Project Report

on

Differential Cryptanalysis On Simeck Cipher

CS 417/617 Cryptography and Network Security

Submitted By

Priyanka Choudhary (2201101006)
Annapureddy venkata sai kumar reddy (2204101012)
Yogendra Singh (2201101010)

Submitted To

Dr. Bodhisatwa Mazumdar
Assistant Professor
Department of Computer Science and Engineering
IIT Indore

Contents

1 Introduction

cryptography is the art of investigating information security scientifically using a variety of protocols and algorithms to secure sensitive data from unauthorised access. securing the information includes privacy or secrecy, data integrity, authentication, non-repudiation, and access control. Including that the main goal of cryptography is enabling two people to communicate via an unsafe channel.(5)
There are various aspects of securities in different applications that need to be secure while transmitting faster. Basically, cryptography is divided into two types Asymmetric Key (Public Key)and Secret Key Cryptography. Public key utilises two different keys in the encryption process, and (which uses one key in encryption and decryption), while symmetric key uses one key for encryption as well as decryption. Asymmetric key typically takes longer than symmetric key.(7) When two persons want to communicate over a secure channel, they must first agree on a secret key that is shared between them.(2)
There are two types of stream ciphers and block ciphers in symmetric-key cryptography.A block cipher is an encryption technique that accepts a given size of input, say b bits, and returns a ciphertext of b bits. The input can be segmented further if it is larger than b bits. Symmetric-key block ciphers are composed of two algorithms, E (Encryption) and D (Decryption), and all of these algorithms accept n bits of plaintext as input and produce exactly the same amount of bits by utilising k bits of secret key.(1)

Cryptanalysis is the inverse process of cryptography. The goal of cryptanalyst is to be capable of decrypting cipher text.

Attacks Models

- Cipher text Only Attack- Here the attacker obtains a sample of cipher text without the plaintext associated with it.
- Chosen Plaintext Attack-The attacker can choose the quantity of plaintext and then obtain the correspondin encrypted cipher text.
- Chosen Ciphertext Attack-The attacker can choose the quantity of ciphers and then obtain the corresponding encrypted plain text.
- Known Plaintext Attack- The attacker obtains the sample of cipher text and the corresponding plaintext.
- Adaptive Chosen plaintext attack- A cryptanalyst can mount this attack when he has decryption hardware but is unable to extract the decryption key from it.
- Brute Force Attack: A brute force attack occurs when hackers use computers to feedback loop over each letter in a character set systematically. In the most general terms, a brute force attack is a method of trial and error that attempts all possible password combinations thus it takes a long time to try all possible passwords.
- Related Key Attack: Here the attacker can observe the operation of cipher under different keys whose values are initially unknown but where some mathematical relationship connecting the keys is known to the attacker.
- Differential Attacks: This attack traces the differences through transformations discovering the cipher exhibiting non random behaviour and exploiting them to recover secret key.

2 Basic Terminologies

- **Plain Text:** The initial message that we want to send to the other people is known as Plain Text. In cryptography, Plain Text refers to the real data that needs to be sent to the other party.

- **Cipher Text:** Cipher text is a term used to describe a message that has been altered by an encryption technique. The original communication is changed into an unreadable message in cryptography.
- **Encryption:** Encryption is the process of turning plain text into cipher text. Using cryptography, private information can be sent via an unsafe channel using an encryption method and a key.
- **Decryption:** Decryption is the process of transforming encrypted text into plain text, which is the opposite of encryption. Decryption requires a key and a decryption algorithm.

3 Differential Cryptanalysis

Differential cryptanalysis exploits the probability that the difference in the plaintext and the difference in the final round of the cipher will occur with a certain probability. For example, consider a system with inputs X = [X1 X2 ... Xn] and outputs Y = [Y1 Y2 ... Yn]. The two inputs to the system are $X^{'}$ and $X^{"}$, with corresponding outputs $Y^{'}$ and $Y^{"}$, respectively. The difference of input is given by $X = X^{"} \oplus X^{"}$ where $'\oplus'$ represents the bitwise exclusive OR of the n-bit vectors.(3)

$$\triangle X = [\triangle X_1 \oplus \triangle X_2 .... X_n]$$

In the randomized cipher, the probability of a given output difference $\triangle Y$ occurring given a given input difference $\triangle X$ is $1/2^n$, where n is a given is the number of bits in X that produce $\triangle Y$ given the input The difference $\triangle X$ with very high probability pD (that is, much larger than $1/2^n$). The pair $(\triangle X, \triangle Y)$ is called the derivative.

Differential cryptanalysis is a targeted plaintext attack. That is, an attacker can choose the input and examine the output to guess the key. In differential cryptanalysis, the attacker chooses input pairs $X^{'}$ and $X^{''}$ that satisfy a particular $\triangle X$, knowing that a particular Y value is likely to occur for a particular $\triangle X$ value. To do.

we anlyse the construction of the derivative $(\triangle X, \triangle Y)$ with the plaintext bits denoted by X and the input of the last round of the cipher denoted by Y. A feature is a sequence of input and output differences to a round such that the output difference from one round is equal to the next round's input difference. Using the probable delta property gives us the opportunity to leverage the information that goes into the last round of cryptography to derive bit from the last layer of the subkey.

4 Simeck Cipher

Simeck is denoted Simeck2n/mn, where n is the word size and n is required to be 16, 24 or 32; while 2n is the block size and mn is the key size. More specifically, our Simeck family includes Simeck32/64, Simeck48/96, and Simeck64/128. For example, Simeck32/64 refers to perform encryption or decryption on 32-bit message blocks using a 64-bit key.(6)

4.1 Round Function

The round of Simeck is defined as :

$$R_{k_i}(l_i,\ r_i) = (r_i \oplus f(l_i) \oplus k_i,\ l_i),$$

- bitwise XOR, ,

- bitwise AND, , and
- left circular shift, S^j, by j bits.

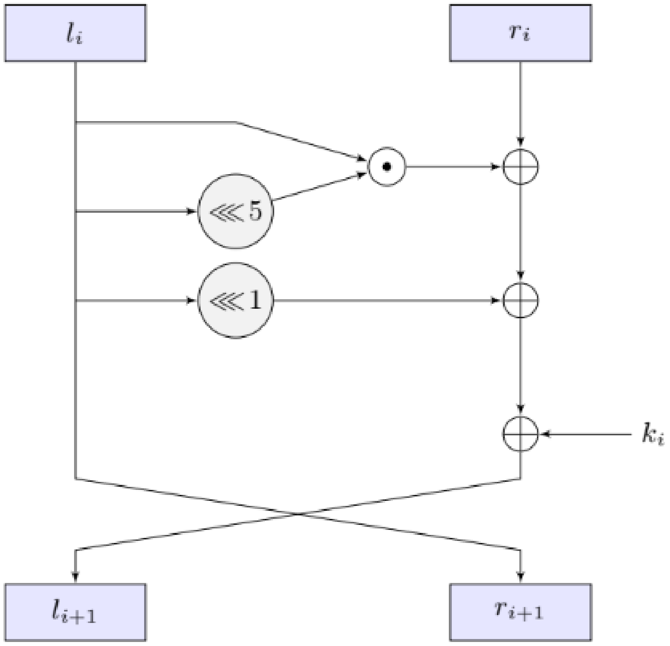


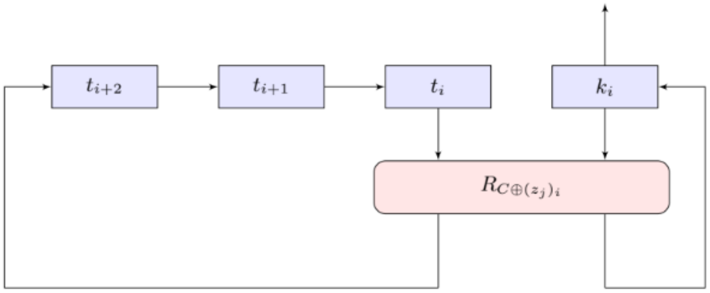
Figure 1: The Round Function of Simeck

where l_i and r_i are the two words for the internal state of Simeck, k_i is the round key, and the function f is defined as:

$$f(x) = (x \odot (x \lll 5)) \oplus (x \lll 1).$$

4.2 Key Schedule

key K, the master key K is first segmented into four words and loaded as the initial states (t_2, t_1, t_0, k_0) of the feedback shift registers shown in Figure 2. The least significant n bits of K are loaded into k_0; while the most significant n bits are put into t_2. To update the registers and generate round keys,



we reuse the round function with a round constant $C\oplus(z_i)_i$ acting as the round key, i.e. $R_C\oplus(z_i)_i$ The updating operation can be expressed as

$$\begin{cases} k_{i+1} = t_i, \\ t_{i+3} = k_i \oplus f(t_i) \oplus C \oplus (z_j)_i, \end{cases}$$

where $0 \leq i \leq T$-1. The value k_i is used as the round key of the i-th round.

The value of the constant C is defined by $C = 2^n\ -4$, where n is the word size. $(z_j)_i$ denotes the i-th bit of the sequence z_j . Simeck32/64 and Simeck48/96 use the same sequence z_0, i.e. j = 0, which is an m-sequence with period 31 and can be generated by the primitive polynomial $X^5 + X^2 + 1$ with the initial state (1, 1, 1, 1, 1). When the rounds number is larger than 31, the sequence repeats itself.

Number of Rounds: The number of rounds T for Simeck32/64, Simeck48/96, and Simeck64/128 are 32, 36, and 44, respectively.

4.3 Differential Probabilities of Simeck Round Functions

Theorem 4.3.1. *(4)*

Let

$$\text{varibits} = S^1(\alpha) \vee \alpha$$

and

$$\textit{doublebits}\ = \alpha \odot \overline{S^1(\alpha)} \odot S^2(\alpha).$$

Then the probability that difference α goes to difference β is

$$P(\alpha \to \beta) = \begin{cases} 2^{-n+1} & \textit{if } \alpha = 1 \textit{ and } wt(\beta) \equiv 0 \mod 2 \\ 2^{-wt(\ varibits+doub1obits\ )} & \textit{if } \alpha \neq 1 \textit{ and } \beta \odot \overline{\ varibits} = 0 \\ & \textit{and } \left(\beta + S^1(\beta)\right) \odot\ \textit{doublebits}\ = 0 \\ 0 & \textit{else }. \end{cases}$$

Theorem 4.3.2. *Let $f(x) = S^a(x) \odot S^b(x) + S^c(x)$, where $\gcd(n, a-b) = 1$, n even, and $a > b$ and let α and β be an input and an output difference. Then with*

$$\text{varibits} = S^a(\alpha) \vee S^b(\alpha)$$

and

$$\textit{doublebits}\ = S^b(\alpha) \odot \overline{S^a(\alpha)} \odot S^{2a-b}(\alpha)$$

and

$$\gamma = \beta + S^c(\alpha)$$

we have that the probability that difference α goes to difference β is

$$P(\alpha \to \beta) = \begin{cases} 2^{-n+1} & \textit{if } \alpha = 1 \textit{ and }\ wt\ (\gamma) \equiv 0 \textit{ mod } 2 \\ 2^{-\text{ wt(varibits+doublebits))}} & \textit{if } \alpha \neq 1 \textit{ and } \gamma \odot \overline{\text{varibits}} = 0 \\ & \textit{and } \left(\gamma + S^{a-b}(\gamma)\right) \odot\ \textit{doublebits}\ = 0 \\ 0 & \textit{else.} \end{cases}$$

Theorem 4.3.3. *(Upper bound on the differential probability (**?**)). Let $F(x) = ((x \lll)\ a) \wedge (x \lll b)) \oplus (x \lll c)$. Assume that $n \geq 6$ is even, $a > b$ and $\gcd(n, a-b) = 1$. Let α be an input difference of $F(x)$. Then for the differential probability, it holds that*

1. *If $wt(\alpha) = 1$, then $P_\alpha \leq 2^{-2}$;*
2. *If $wt(\alpha) = 2$, then $P_\alpha \leq 2^{-3}$;*
3. *If $wt(\alpha) \neq n$, then $P_\alpha \leq 2^{-wt(\alpha)}$;*
4. *If $wt(\alpha) = n$, then $P_\alpha \leq 2^{-n+1}$.*

5 Experiments, Results and Observations of Differential Cryptanalysis on Simeck Cipher

5.1 Experiments

Simeck is a lightweight block cipher. It has a feistel structure and operates on 2n-bit state, In our experiment n=32, and the key size composes of m n bit words where m=2,3,4. Simeck with block size 64 bits and key size 32(m) bits is referred to as SIMECK64/32(m).

$$f(x) = S^a(x) \odot S^b(x) + S^c(x)$$

Here, In Simeck Cipher we have $\boldsymbol{a = 0, b = 5, c = 1}$.

We have done two types of experiments

- The final observation can be done using various x_1, x_2 plaintext pairs for a fixed valued of α. To perform the experiment, five different alpha values were used and generated corresponding x_2 plaintext. Such pairs were encrypted for generating corresponding cipertexts (i.e., c_1 and c_2). For a single value of α, the analysis was performed over 20 randomly generated x_1's. β is the difference of the corresponding ciphertexts after the $(r-1)th$ round as shown in table $1-5$.

- To verify Theorem 4.3.2 We fix values of α=0x$ffffffff$ and β= 0x00080000(or 0x00080003,0x30080000) then recorded the corresponding differential probabilities $P(\alpha \to \beta)$ in experiment.

5.2 Observations

1. $\alpha = \mathbf{1} = (1, 1, 1 \ldots, 1)$
   $wt(\gamma) = 0 mod 2$
   $wt(\beta + s^2(\alpha)) = 0 mod 2$
   $wt(\beta + (1, 1, \ldots) = 0 mod 2$
   $wt(\beta + (1, 1, 1, \ldots) = even$
   No. of zeros in β is even

2. From the theorem 4.3.2 we observe the differential probability $P(\alpha \to \beta)$ is same for all possible output differences β.

3. From the theorem 4.3.3 the differential probability of Simeck function $P(\alpha \to \beta)$ depends only on the input difference α and the rotational constants a and b, if $\alpha \to \beta$ is a possible differential.

6 Conclusion

In this report, we present the overview of Simeck cipher and differential cryptanalysis. We do analyse theorems presented in this report and have following noteworthy points

- The differential probability $P(\alpha \to \beta)$ is same for all possible output differences β.

- The differential probability of Simeck function $P(\alpha \to \beta)$ depends only on the input difference α and the rotational constants a and b, if $\alpha \to \beta$ is a possible differential.

- By Theorem 4.3.1, if $\alpha = \mathbf{1} = (1, 1, 1 \ldots, 1)$ and number of zeros in β is even then $P(\alpha \to \beta)$ is $\frac{1}{2^{n-1}}$. We verify this observation by experimentally as well.

- Theorem 4..3.3 gives us the upper bound for $P(\alpha \to \beta)$, for different conditions of α, which is independent of choice of β.

Table 1: Difference Distribution Table 1

alpha = 0xffffffff		**alpha = 0x23452345**	
x1 (plaintext) = 0xc9bd3bd7	beta =0x341c5c91	x1 (plaintext) = 0xc9bd3bd7	beta =0x341c5c91
x1 (plaintext) = 0xd108fc07	beta =0x58a238bc	x1 (plaintext) = 0xd108fc07	beta =0x58a238bc
x1 (plaintext) = 0xdd52fcc0	beta =0x47c49f63	x1 (plaintext) = 0xdd52fcc0	beta =0x47c49f63
x1 (plaintext) = 0x692573d0	beta =0xfa1032f5	x1 (plaintext) = 0x692573d0	beta =0xfa1032f5
x1 (plaintext) = 0x889d49a0	beta =0x2df1adc7	x1 (plaintext) = 0x889d49a0	beta =0x2df1adc7
x1 (plaintext) = 0xe2342bc4	beta =0x9133945b	x1 (plaintext) = 0xe2342bc4	beta =0x9133945b
x1 (plaintext) = 0xff10ce2	beta =0xa370b662	x1 (plaintext) = 0xff10ce2	beta =0xa370b662
x1 (plaintext) = 0xc2e36d0f	beta =0xae4908c9	x1 (plaintext) = 0xc2e36d0f	beta =0xae4908c9
x1 (plaintext) = 0xd0543b64	beta =0x11b2f7da	x1 (plaintext) = 0xd0543b64	beta =0x11b2f7da
x1 (plaintext) = 0x253ce2a0	beta =0x2ea8682b	x1 (plaintext) = 0x253ce2a0	beta =0x2ea8682b
x1 (plaintext) = 0x828fe617	beta =0xdaa486e6	x1 (plaintext) = 0x828fe617	beta =0xdaa486e6
x1 (plaintext) = 0x544283a6	beta =0x97195f84	x1 (plaintext) = 0x544283a6	beta =0x97195f84
x1 (plaintext) = 0xa5bdc2b6	beta =0xc9518f97	x1 (plaintext) = 0xa5bdc2b6	beta =0xc9518f97
x1 (plaintext) = 0xdf187493	beta =0xd2d21606	x1 (plaintext) = 0xdf187493	beta =0xd2d21606
x1 (plaintext) = 0x4fc3996b	beta =0xbd9b0d12	x1 (plaintext) = 0x4fc3996b	beta =0xbd9b0d12
x1 (plaintext) = 0x1554968	beta =0x9c0c50b6	x1 (plaintext) = 0x1554968	beta =0x9c0c50b6
x1 (plaintext) = 0xf7b5a981	beta =0x86a11cd4	x1 (plaintext) = 0xf7b5a981	beta =0x86a11cd4
x1 (plaintext) = 0x6f1f5449	beta =0x62dc8468	x1 (plaintext) = 0x6f1f5449	beta =0x62dc8468
x1 (plaintext) = 0x20ebcba3	beta =0xd2ea9422	x1 (plaintext) = 0x20ebcba3	beta =0xd2ea9422
x1 (plaintext) = 0x406f33ef	beta =0x715ae61a	x1 (plaintext) = 0x406f33ef	beta =0x715ae61a

Table 2: Difference Distribution Table 2

alpha = 0x98765678		**alpha = 0x65434567**	
x1 (plaintext) = 0xc9bd3bd7	beta =0x341c5c91	x1 (plaintext) = 0xc9bd3bd7	beta =0x341c5c91
x1 (plaintext) = 0xd108fc07	beta =0x58a238bc	x1 (plaintext) = 0xd108fc07	beta =0x58a238bc
x1 (plaintext) = 0xdd52fcc0	beta =0x47c49f63	x1 (plaintext) = 0xdd52fcc0	beta =0x47c49f63
x1 (plaintext) = 0x692573d0	beta =0xfa1032f5	x1 (plaintext) = 0x692573d0	beta =0xfa1032f5
x1 (plaintext) = 0x889d49a0	beta =0x2df1adc7	x1 (plaintext) = 0x889d49a0	beta =0x2df1adc7
x1 (plaintext) = 0xe2342bc4	beta =0x9133945b	x1 (plaintext) = 0xe2342bc4	beta =0x9133945b
x1 (plaintext) = 0xff10ce2	beta =0xa370b662	x1 (plaintext) = 0xff10ce2	beta =0xa370b662
x1 (plaintext) = 0xc2e36d0f	beta =0xae4908c9	x1 (plaintext) = 0xc2e36d0f	beta =0xae4908c9
x1 (plaintext) = 0xd0543b64	beta =0x11b2f7da	x1 (plaintext) = 0xd0543b64	beta =0x11b2f7da
x1 (plaintext) = 0x253ce2a0	beta =0x2ea8682b	x1 (plaintext) = 0x253ce2a0	beta =0x2ea8682b
x1 (plaintext) = 0x828fe617	beta =0xdaa486e6	x1 (plaintext) = 0x828fe617	beta =0xdaa486e6
x1 (plaintext) = 0x544283a6	beta =0x97195f84	x1 (plaintext) = 0x544283a6	beta =0x97195f84
x1 (plaintext) = 0xa5bdc2b6	beta =0xc9518f97	x1 (plaintext) = 0xa5bdc2b6	beta =0xc9518f97
x1 (plaintext) = 0xdf187493	beta =0xd2d21606	x1 (plaintext) = 0xdf187493	beta =0xd2d21606
x1 (plaintext) = 0x4fc3996b	beta =0xbd9b0d12	x1 (plaintext) = 0x4fc3996b	beta =0xbd9b0d12
x1 (plaintext) = 0x1554968	beta =0x9c0c50b6	x1 (plaintext) = 0x1554968	beta =0x9c0c50b6
x1 (plaintext) = 0xf7b5a981	beta =0x86a11cd4	x1 (plaintext) = 0xf7b5a981	beta =0x86a11cd4
x1 (plaintext) = 0x6f1f5449	beta =0x62dc8468	x1 (plaintext) = 0x6f1f5449	beta =0x62dc8468
x1 (plaintext) = 0x20ebcba3	beta =0xd2ea9422	x1 (plaintext) = 0x20ebcba3	beta =0xd2ea9422
x1 (plaintext) = 0x406f33ef	beta =0x715ae61a	x1 (plaintext) = 0x406f33ef	beta =0x715ae61a

Table 3: Difference Distribution Table 3

alpha = 0x78654567

x1 (plaintext) = 0xc9bd3bd7	beta =0x341c5c91
x1 (plaintext) = 0xd108fc07	beta =0x58a238bc
x1 (plaintext) = 0xdd52fcc0	beta =0x47c49f63
x1 (plaintext) = 0x692573d0	beta =0xfa1032f5
x1 (plaintext) = 0x889d49a0	beta =0x2df1adc7
x1 (plaintext) = 0xe2342bc4	beta =0x9133945b
x1 (plaintext) = 0xff10ce2	beta =0xa370b662
x1 (plaintext) = 0xc2e36d0f	beta =0xae4908c9
x1 (plaintext) = 0xd0543b64	beta =0x11b2f7da
x1 (plaintext) = 0x253ce2a0	beta =0x2ea8682b
x1 (plaintext) = 0x828fe617	beta =0xdaa486e6
x1 (plaintext) = 0x544283a6	beta =0x97195f84
x1 (plaintext) = 0xa5bdc2b6	beta =0xc9518f97
x1 (plaintext) = 0xdf187493	beta =0xd2d21606
x1 (plaintext) = 0x4fc3996b	beta =0xbd9b0d12
x1 (plaintext) = 0x1554968	beta =0x9c0c50b6
x1 (plaintext) = 0xf7b5a981	beta =0x86a11cd4
x1 (plaintext) = 0x6f1f5449	beta =0x62dc8468
x1 (plaintext) = 0x20ebcba3	beta =0xd2ea9422
x1 (plaintext) = 0x406f33ef	beta =0x715ae61a

References

[1] Salah Albermany and Fatima Radi. Survey: Block cipher methods. 5, 11 2016.

[2] T. Rajani Devi. Importance of cryptography in network security. In *2013 International Conference on Communication Systems and Network Technologies*, pages 462–467, 2013.

[3] Howard M. Heys. A tutorial on linear and differential cryptanalysis. *Cryptologia*, 26(3):189–221, jul 2002.

[4] Stefan Kölbl, Gregor Leander, and Tyge Tiessen. Observations on the simon block cipher family. In Rosario Gennaro and Matthew Robshaw, editors, *Advances in Cryptology – CRYPTO 2015*, pages 161–185, Berlin, Heidelberg, 2015. Springer Berlin Heidelberg.

[5] Gangadhar Tiwari, Debashis Nandi, and Madhusudhan Mishra. Cryptography and cryptanalysis: A review. *International Journal of Engineering Research Technology.*

[6] Gangqiang Yang, Bo Zhu, Valentin Suder, Mark D. Aagaard, and Guang Gong. The simeck family of lightweight block ciphers. In Tim Güneysu and Helena Handschuh, editors, *Cryptographic Hardware and Embedded Systems – CHES 2015*, pages 307–329, Berlin, Heidelberg, 2015. Springer Berlin Heidelberg.

[7] Muneer Bani Yassein, Shadi Aljawarneh, Ethar Qawasmeh, Wail Mardini, and Yaser Khamayseh. Comprehensive study of symmetric key and asymmetric key encryption algorithms. In *2017 International Conference on Engineering and Technology (ICET)*, pages 1–7, 2017.