A tutorial of boomerang attack on SMALLPRESENT-[4]

I W Hutahaean, A A Lestari, and B H Susanti
Cryptography Engineering of Politeknik Siber dan Sandi Negara, Bogor, Indonesia
E-mail: ida.widya@student.poltekssn.ac.id, andriani.adii@poltekssn.ac.id, bety.hayat@poltekssn.ac.id

Abstract. In 2010, Leander proposed a new version of the block cipher PRESENT with smaller block size, namely SMALLPRESENT-[n]. This algorithm is designed to deepen understanding of how the running time of the algorithm and the vulnerability of attack during the round increase with the number of rounds and s-boxes not determined on the algorithm. The boomerang attack is a variation of the differential attack introduced by Wagner in 1999. This attack uses two differential characteristics that are mutually independent in short rounds with high probability. This paper intends to present a lucid explanation of the boomerang attack. We illustrate the practical application of the boomerang attacks on two rounds of the SMALLPRESENT-[4], that includes the steps to find differential characteristic until key recovery, and explain the concept of attack for novice cryptanalysis. Based on experiments conducted, we found a boomerang differential characteristic on two rounds of SMALLPRESENT-[4] with a probability $2^{-10}$ and 4-bit subkey in the first round of the algorithm.

1. Introduction

Confidentiality is one of the three main cryptographic services that play an important role in information security. Cryptography has been used for thousands of years to provide confidential communications and today many cryptographic systems are created by improving confidentiality services to secure information [1]. One of cryptographic system that is still used today is the symmetric key cryptographic system, block cipher.

Today, block ciphers are often used in hardware implementations. A lightweight block cipher is an algorithm that can be implemented into a device with small memory and computing [2]. Lightweight block ciphers are developing until now. In 2007, Bogdanov et al. proposed an ultra-lightweight block cipher with an SPN (Substitution-Permutation-Network) structure, PRESENT algorithm which consists of 31 rounds cipher with 64-bit input block and 80-bit or 128-bit key length [3]. In 2010, Leander proposed a small size variation of PRESENT algorithm, namely, SMALLPRESENT-[n] where $n$ is the number of blocks and s-boxes with 80 bit key length and the number of rounds of the cipher is not specifically determined [4]. Leander in [4] states that SMALLPRESENT-[n] is designed to facilitate the security analysis of PRESENT algorithm based on attacks which carried out on SMALLPRESENT-[n].

Boomerang attack is one type of differential attack that was proposed by Wagner in 1999 [7]. This attack is included of adaptive chosen plaintext and ciphertext attack [5]. Chen and Miyaji in [6] explain that a boomerang attack is more effective than differential attack because...
boomerang attack uses two independent differential characteristics, $A$ and $B$, on short rounds with high probability. The two differential characteristics can be used as boomerang differential characteristics, if the probability of two independent differential characteristics, $Pr[A], Pr[B]$, is greater than $2^{-i/2}$ where $i$ is the input length [7]. These boomerang differential characteristics can be used to find the correct quartet and if the quartet is found, then the boomerang differential characteristic is called as boomerang distinguisher. The quartet can be used to limit the amount of data required in the key recovery process [8].

There are many researches about boomerang attack as in [9], [10], and [11]. However, the steps to carry out a boomerang attack are not explained in detail on those researches. In this paper, we will present a lucid explanation of the boomerang attack on two rounds of SMALLPRESENT-[4]. This paper aims to provide an explanation the concept of attack for beginner cryptanalysts so they can analyze the security of an algorithm against boomerang attack easily.

2. Related Theories
2.1. SMALLPRESENT-[4]
SMALLPRESENT-[n] is a block cipher algorithm proposed by Gregor Leander in 2010. In general, SMALLPRESENT-[n] has the same structure as the PRESENT algorithm with $n$ as the number of blocks and s-boxes with 80-bit key length and the number of rounds of the cipher is not specifically determined [4].

SMALLPRESENT-[4] is a SMALLPRESENT-[n] algorithm which consists of 4 blocks and 4 s-boxes. This algorithm uses 16-bit plaintext input, 80-bit master key, and 16-bit subkey for each round. SMALLPRESENT-[4] consists of three main processes, i.e. key schedule, encryption, and decryption. See [3] and [4] for more detail discussion.

2.2. Boomerang Attack
Boomerang attack is an extension of differential cryptanalysis which includes in adaptive chosen plaintext and ciphertext attack [5]. This attack was first proposed by Wagner in 1999. This attack uses two independent differential characteristics, $A$ and $B$ [8]. Differential characteristic $A$ maps difference input $\alpha$ to the difference output $\beta$ which denoted by $A : (\alpha \rightarrow \beta)$ with probability $p$ and differential characteristic $B$ maps difference input $\lambda$ to the difference output $\delta$ which denoted by $B : (\gamma \rightarrow \delta)$ with probability $q$. If the probability of the combination differential characteristics $A$ and $B$ is greater than $2^{-i/2}$, then $A$ and $B$ can be used as boomerang characteristic differential. Boomerang characteristic differential which can produce the correct quartet will be a boomerang distinguisher and the quartet can be used to to limit the amount of data required in the key recovery process [7].

3. Research Metodology
In this research, the parameters that we use for SMALLPRESENT-[4] algorithm are $i = 16$ bit, the number of rounds are two rounds, the size of plaintext $P$ is 16-bit so we divided it into 4 blocks message and each block use 4-bit plaintext.

This experiment is carried out by applying the boomerang attack on two rounds SMALLPRESENT-[4] algorithm using the Java programming language. We use $2^8$ plaintext from $(0001)_H$ to $(0100)_H$ as the sample. To find a differential characteristic we limit the number of active s-boxes, which is 1 dan 2 active s-boxes in each round. Boomerang attack consists of the processes of finding differential characteristics, boomerang differential characteristic, boomerang distinguisher, and the key recovery.

3.1. Finding Differential Characteristic
The first step in boomerang attack is finding two differential characteristics $A : (\alpha \rightarrow \beta)$ and $B : (\gamma \rightarrow \delta)$ on a round of SMALLPRESENT-[4] with the following steps:
3.2. Finding Boomerang Differential Characteristic

After obtaining all the possible differential characteristics, find boomerang differential characteristics with the following steps:

a) Combine the two differential characteristics obtained previously, \( A : (\alpha \rightarrow \beta) \) and \( B : (\gamma \rightarrow \delta) \), with the condition that \( \beta \neq \gamma \).

b) Compute the probability of a combination of the two differential characteristics in the previous step by multiplying the differential characteristic probability.

c) If total probability is greater than \( 2^{-i/2} \), then the combination of two differential characteristics can be used as boomerang differential characteristic.

d) Calculate the probability of boomerang differential characteristic with the formula 1.

\[
(p.q)^2 = Pr[\alpha \rightarrow \beta]^2 \cdot Pr[\gamma \rightarrow \delta]^2
\]  

3.3. Finding Boomerang Distinguisher

After obtaining boomerang differential characteristics, then the boomerang distinguisher is searched based on the selected boomerang differential characteristic. The steps to find the boomerang distinguisher are as follows:

a) Generate \( 1/(pq)^2 \) plaintexts

b) Select the plaintext pair \( (P_1, P_2) \) which has difference value \( \alpha \) such that \( \alpha = P_1 \oplus P_2 \).

c) Encrypt \( (P_1, P_2) \) with two rounds of SMALLPRESENT-[4] to get ciphertext pair \( (C_1, C_2) \).

d) Calculate ciphertext pair \( (C'_1, C'_2) \) by XORing \( (C_1, C_2) \), from previous step, with output difference \( \delta \), such that \( C'_1 = C_1 \oplus \delta \) and \( C'_2 = C_2 \oplus \delta \).

e) Decrypt \( (C'_1, C'_2) \) with two rounds of SMALLPRESENT-[4] to get plaintext pair \( (P'_1, P'_2) \).

f) The quartet \( (P_1, P_2, P'_1, P'_4) \) will be obtained if \( P_1 \oplus P_2 = \alpha = P'_1 \oplus P'_2 \) and \( C_1 \oplus C'_1 = \delta = C_2 \oplus C'_2 \) occurred where \( \alpha \) and \( \delta \) is boomerang differential characteristic which has obtained in step 3.2.

g) The boomerang differential characteristic which can get correct quartet then called as boomerang distinguisher.

h) The process of finding boomerang distinguisher is carried out on another plaintext to find another quartet.

3.4. Key Recovery

The steps of key recovery on one round SMALLPRESENT-[4] process are as follows:

a) Select the boomerang distinguisher which has obtained in step 3.3.

b) Use the difference input \( \alpha \) from boomerang distinguisher to find the active subkey bit in the first round.

c) Generate \( 2^k \) subkey candidates with \( k \) is the number of active key bits.

d) Encrypt partially the entire quartet \( (P_1, P_2, P'_1, P'_2) \) of the boomerang distinguisher. Encryption is implemented only in first round using \( 2^k \) subkey candidates. The result of the one round encryption are denoted as \( (M_1, M_2, M'_1, M'_2) \).

e) After partial encryption in the first round, an XOR operation is used on the encryption result such that \( M_1 \oplus M_2, M'_1 \oplus M'_2, M_1 \oplus M'_1, \) and \( M_2 \oplus M'_2 \).
f) Two conditions should be satisfied in this process are $M_1 \oplus M_2 = \beta = M'_1 \oplus M'_2$ and $M_1 \oplus M'_1 = \gamma = M_2 \oplus M'_2$, where $\beta$ and $\gamma$ are output differential of boomerang differential characteristics which has obtained in step 3.2. If the results are satisfied with these conditions, then the subkey candidate used is the correct subkey candidate.

4. Boomerang Attack on Two Rounds SMALLPRESENT-[4]

The steps of a boomerang attack on two rounds SMALLPRESENT-[4] are described in section 3. In this section, we explain the example of boomerang attack on two round SMALLPRESENT-[4].

4.1. Finding Differential Characteristics

The first step to find differential characteristics is to generate all possible input differences that activate one and two s-boxes. There are 1,410 input differences that activate one and two s-boxes, 60 input differences that activate one s-box and 1,350 input differences that activate two s-boxes.

| Differential Input $\alpha$ | S-box Output | Permutation (Differential Output $\beta$) |
|-----------------------------|-------------|---------------------------------------|
| 0007                        | 0001        | 0001                                  |
| 0007                        | 0002        | 0010                                  |
| 0007                        | 0006        | 0110                                  |
| 0007                        | 0008        | 1000                                  |
| 0007                        | 000f        | 1100                                  |
| 0007                        | 000f        | 1111                                  |

Table 1. Example of differential characteristic in one round SMALLPRESENT-[4]

Each input difference will be processed in a round SMALLPRESENT-[4] through two s-box and permutation. In the s-box component, the difference input is used as input for distribution table (DDT table) which produces several outputs which become the permutation input. The output of permutation becomes the difference output and differential characteristics is obtained which consists of difference input and difference output pairs. Table 1 shown an example of the process to find a differential characteristic on a round of SMALLPRESENT-[4] with difference input is (0007)$_H$ and Figure 1 shown an example of the process when the difference input processed in a round SMALLPRESENT-[4]. In Figure 1, the black blocks shows the active plaintext bits.

4.2. Finding Boomerang Differential Characteristic

This process requires two characteristics of the boomerang differential obtained in the previous process. Based on the differential characteristics that have been obtained, the combination of two differential characteristics with the probability value $pq > 2^{-8}$ can be used as a boomerang differential characteristic. For example, we use the combination of two differential characteristics i.e., $(\alpha \rightarrow \beta) : ((0003)_H \rightarrow (0100)_H)$ with the probability is $2^{-3}$ and $(\gamma \rightarrow \delta) : ((0004)_H \rightarrow (0101)_H)$ with the probability is $2^{-2}$ such that the probability of the combination is $2^{-3} \times 2^{-2} = 2^{-5}$. Since $2^{-5} > 2^{-10}/2$, this combination can be used as boomerang differential characteristic with probability $2^{-10}$. 
4.3. Finding Boomerang Distinguisher

The first step to find boomerang distinguisher is generating $2^{10}$ plaintexts. However, in this research, we found the boomerang distinguisher using only $2^8$ plaintexts. In this research, we used a hexadecimal format to represent the differential characteristics. When we use boomerang differential characteristic ($A : ((0003)_H \rightarrow (0100)_H), B : ((0004)_H \rightarrow (0101)_H)$), we could find 16 correct quartets that are shown in Table 2.

Table 2. Correct quartets of boomerang differential characteristic

| Nu | $P_1$ | $P_2$ | $C_1$ | $C_2$ | $C'_1$ | $C'_2$ | $P'_1$ | $P'_2$ |
|----|-------|-------|-------|-------|--------|--------|--------|--------|
| 1  | 0009  | 000a  | 487b  | 0c7f  | 497a   | 0d7e   | 00d9   | 00da   |
| 2  | 0019  | 001a  | 4b78  | 0f7c  | 4a78   | 0e7d   | 00e9   | 00ea   |
| 3  | 0029  | 002a  | 0d7a  | 093e  | 0c7d   | 083f   | 0099   | 009a   |
| 4  | 0039  | 003a  | 0e79  | 0a3d  | 0f78   | 063c   | 0049   | 004a   |
| 5  | 0049  | 004a  | 0f78  | 063c  | 0e79   | 0a3d   | 0039   | 003a   |
| ... |      |       |      |       |        |        |        |        |
| 15 | 00c9  | 00ea  | 4a79  | 0e7d  | 4b78   | 0f7c   | 0019   | 001a   |
| 16 | 00fa  | 00f9  | 8b8c  | 8f8f  | 8ab8   | 8ef9   | 00aa   | 00a8   |

Based on Table 2, one of the quartet obtained from the boomerang differential characteristic ($A : ((0003)_H \rightarrow (0100)_H), B : ((0004)_H \rightarrow (0101)_H)$) is ($P_1, P_2, P'_1, P'_2 : (0009_H, (000a)_H, (00d9)_H, (00da)_H)$). This happened because of the quartet matches with the terms as follows:

$$(0009)_H \oplus (000a)_H = \alpha = (00d9)_H \oplus (00da)_H$$

$$(487b)_H \oplus (497a)_H = \delta = (0c7f)_H \oplus (0d7e)_H$$

4.4. Key Recovery

The key recovery process is carried out based on the correct quartet and boomerang distinguisher that has been obtained in previous process. In this process, we use ($A : ((0003)_H \rightarrow (0100)_H), B : ((0004)_H \rightarrow (0101)_H)$) as one of the quartet and boomerang distinguisher that has been obtained in previous process. In this process, we use ($A : ((0003)_H \rightarrow (0100)_H), B : ((0004)_H \rightarrow (0101)_H)$) as one of the quartet and boomerang distinguisher that has been obtained in previous process.
\((((0004)_H \rightarrow (0101)_H))\) with the probability is \(2^{-10}\) to find the subkey in the first round. We use \(\alpha : (0003)_H\) to find the active subkey bit in the first round. The number of active subkey bits is four and is in position \([k_{12}, k_{13}, k_{14}, k_{15}]\) as shown in Figure 2. In Figure 2, the red blocks show the active subkey bits.

We know the number of subkey candidates to be recovered based on the number of active subkey bits. Based on Figure 3, the number of subkey candidates will be generated in position \([k_{12}, k_{13}, k_{14}, k_{15}]\) are \(2^4\) or 16. Hence, we generate the subkey candidates from \((0000)_H\) to \((000f)_H\). Then, all of correct quartets in Table 2 will be encrypted using two rounds SMALLPRESENT-[4] which is assumed as a black box. To guess the subkey in the first round \([k_{12}, k_{13}, k_{14}, k_{15}]\), encrypt all of the correct quartet with one round SMALLPRESENT-[4] using \(2^4\) subkey candidates that have been generated. If the result is satisfy \(M_1 \oplus M_2 = \beta = M'_1 \oplus M'_2\) and \(M_1 \oplus M'_1 = \gamma = M_2 \oplus M'_2\), then the subkey candidate used is the correct candidate subkey.

In this research, we found two subkey candidates which are the results were able to construct different value \(\beta : (0100)_H\) and \(\gamma : (0004)_H\) as shown in Table 3.

| Nu | Subkey Candidates |
|----|-------------------|
| 1  | 000d              |
| 2  | 000e              |

Based on Table 3, we know that there is one false positive of the possible candidate subkeys that have been found. To recover all subkey in the first round SMALLPRESENT-[4], we need another boomerang distinguisher with the same steps as before.

Since we use boomerang differential characteristic \((A : ((0003)_H \rightarrow (0100)_H), B : ((0004)_H \rightarrow (0101)_H))\) in this experiment and get the master key of the algorithm, we ensure the correct quartet from boomerang differential characteristic create the right of boomerang attack.
structure. The quartet satisfy with the conditions as follows:

\[
\begin{align*}
(0009)_H \oplus (000a)_H &= \alpha = (0003)_H = (00d9)_H \oplus (00da)_H \\
(da89)_H \oplus (db89)_H &= \beta = (0100)_H = (da8d)_H \oplus (db8d)_H \\
(da89)_H \oplus (da8d)_H &= \gamma = (0004)_H = (db89)_H \oplus (db8d)_H \\
(487b)_H \oplus (497a)_H &= \delta = (0101)_H = (0c7f)_H \oplus (0d7e)_H
\end{align*}
\]

The structure of the correct quartet is shown in Figure 3.

![3.png](attachment:3.png)

**Figure 3.** An example of correct quartet from boomerang characteristic differential

5. Conclusion
In this research, we found boomerang differential characteristic on two rounds SMALLPRESENT-[4] with the probability is $2^{-10}$. The boomerang differential characteristic can be used as a boomerang distinguisher because the pair of $(P_1, P_2, P'_1, P'_2) : (0009, 000a, 00d9, 00da)$ could construct the four difference values $\alpha, \beta, \gamma, \text{ and } \delta$. The boomerang distinguisher and the correct quartet can be used in the key recovery process. The key recovery process was successfully carried out on four subkey bits in the first round using boomerang distinguisher $(A : ((0003)_H \rightarrow (0100)_H), B : ((0004)_H \rightarrow (0101)_H))$. In this research, the master key used in SMALLPRESENT-[4] algorithm has not been obtained. Therefore, this research can be continued by searching for all subkeys in all rounds so that the master key used in this research can be found.

Acknowledgements
The research was supported by Politeknik Siber dan Sandi Negara, Bogor, West Java. We would like to thank the reviewers who give their valuable comments.

References
[1] Stinson D R and Paterson M B 2019 Cryptography Theory and Practice 4th Edition Boca Raton CRC Press, Taylor & Francis: Library of Congress Cataloging-in-Publication Data.
[2] Katagi M and Moriai S 2008 Lightweight cryptography for the Internet of Things Song Corporation pp 710
[3] Bogdanov A, Knudsen L R, Leander G, Paar C, Poschmann A, Robshaw M J, Seurin Y, and Vikkelsoe C 2007 PRESENT: An Ultra-Lightweight Block Cipher In *International workshop on cryptographic hardware and embedded systems* 25 pp 450-466

[4] Leander G 2010 Small Scale Variants Of The Block Cipher PRESENT *IACR Cryptol* 2010 pp 143

[5] Biryukov A 2004 The Boomerang Attack on 5 and 6-round Reduced AES* In *International Conference on Advanced Encryption Standard* pp 11-15

[6] Chen J and Miyaji A 2013 Differential cryptanalysis and boomerang cryptanalysis of LBlock In *International Conference on Availability, Reliability, and Security* pp 115

[7] Dunkelman O and Biham E 2006 *Techniques for Cryptanalysis of Block Ciphers* (Doctoral dissertation, Computer Science Department, Technion)

[8] Wagner D 1999 The Boomerang Attack: A Generic View In *International Workshop on Fast Software Encryption* pp 156-170

[9] Biryukov A 2004 The Boomerang Attack on 5 and 6-Round Reduced AES In *International Conference on Advanced Encryption Standard* pp 11-15

[10] Dunkelman O, Keller N, Ronen E and Shamir A 2020 The Retracing Boomerang Attack In *Annual International Conference on the Theory and Applications of Cryptographic Techniques* pp 280-309

[11] Koo B, Yeom Y and Song J 2011 Related-Key Boomerang Attack on Block Cipher SQUARE *IEICE transactions on fundamentals of electronics, communications and computer sciences* 94 pp 3-9