Collision Attacks on PGV models Instantiated with Robin Suitable for Lightweight Platforms

Hangi Kim and Jonsung Kim

Abstract—In IoT service platform, lightweight cryptographic algorithms are required because of its limited computing and storage resource. PGV models and Robin are cryptographic algorithms with many advantages on lightweight platform. However, if they are used together, the security of the hash function is weakened by Robin's chosen-key differential paths. In this paper, we propose collision attacks on Robin-based PGV models which need less time complexity than the birthday attack.

Research Keywords—Block cipher-based hash functions, Collision attacks, Chosen-key differential paths, Robin, PGV

1 INTRODUCTION

As the number of IoT device users increases, the security in lightweight platforms such as lightweight protocol and low power environments are becoming important. Therefore, many cryptographic algorithms for lightweight platforms have been studied actively.

A hash function based on a lightweight block cipher is suitable for lightweight platform because it can be implemented with very small amount of code added to the base block cipher. Twelve PGV models are block cipher based hash functions that have provable security as hash functions [4]. Their security depends on the base block cipher.

LS-design is a family of block ciphers that can systematically take advantage of bitslicing [1]. And Robin is the one representative lightweight block cipher included in LS-design. It has a proper S-Box and linear operation for efficient masking implementation. This means that it is also possible to implement side-channel countermeasure on Robin even on the lightweight platform. Therefore, it is advantageous to use Robin itself and Robin-based hash functions as well in a lightweight platform.

- *Hangi Kim is with the Dept. of Finantial Information Security, Kookmin Univ., Seoul, Korea. E-mail: tiontta@kookmin.ac.kr*
- *Jongsung Kim (corresponding author) is with the Dept. of Dept. of Information Security, Cryptology and Mathematics / Dept. of Finantial Information Security, Kookmin Univ., Seoul, Korea. E-mail: jskim@kookmin.ac.kr.*

However, since the designers of Robin did not consider the related-key security, it may not be secure if it is used as a base block cipher in a hash function [5]. In this paper, we show how Robin's chosen-key differential paths can be applied to collision attacks on several PGV models.

2 ROBIN AND PGV MODELS

2.1 A Description of Robin

Robin is a 16-round LS-design block cipher using a 128-bit plaintext and a 128-bit master key [1]. Each round has S-Layer for S-Box operation, L-Layer for linear operation, and round key XOR operation (Figure 1). In order to apply the bitslicing

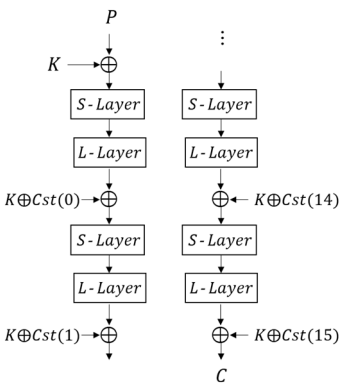

Fig. 1. Encryption process of Robin

technique, each operation is performed in row or column as shown in Figure 2. Therefore, 16 S-Box operation and 8 linear operations are performed every rounds.

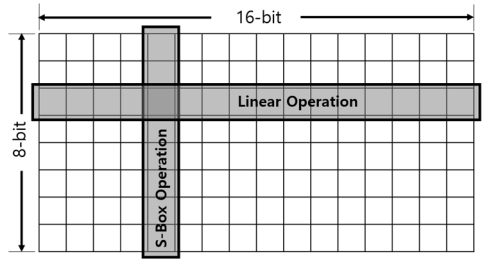

Fig. 2. L-Layer and S-Layer operation range

Robin uses an involutive 8-bit S-Box that is constructed by extending a Class13 4-bit S-Box with a Feistel structure [2], [3]. The 16-bit L-Box in Figure 3 is used for L-Layer. It is involutive and has branch number 8.

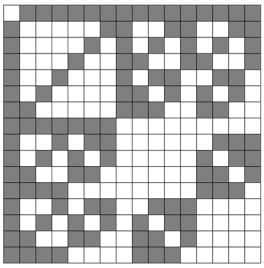

Fig. 3. 16-bit L-Box of Robin

2.2 A Discription of PGV Models

The PGV models are Single Block Length (SBL) hash modes that allow a block cipher to be used as part of a hash function. Among the 64 PGV models [4], only the twelve models listed in Table 1 are secure as hash functions.

Table 1. Twelve PGV models

PGV	Compression function
no.1	$H_i = E_{H_{i-1}}(M_i) \oplus M_i$
no.2	$H_i = E_{H_{i-1}}(M_i \oplus H_{i-1}) \oplus M_i \oplus H_{i-1}$
no.3	$H_i = E_{H_{i-1}}(M_i) \oplus M_i \oplus H_{i-1}$
no.4	$H_i = E_{H_{i-1}}(M_i \oplus H_{i-1}) \oplus M_i$
no.5	$H_i = E_{M_i}(H_{i-1}) \oplus H_{i-1}$
no.6	$H_i = E_{M_i}(M_i \oplus H_{i-1}) \oplus M_i \oplus H_{i-1}$
no.7	$H_i = E_{M_i}(H_{i-1}) \oplus M_i \oplus H_{i-1}$
no.8	$H_i = E_{M_i}(M_i \oplus H_{i-1}) \oplus H_{i-1}$
no.9	$H_i = E_{M_i \oplus H_{i-1}}(M_i) \oplus M_i$
no.10	$H_i = E_{M_i \oplus H_{i-1}}(H_{i-1}) \oplus H_{i-1}$
no.11	$H_i = E_{M_i \oplus H_{i-1}}(M_i) \oplus H_{i-1}$
no.12	$H_i = E_{M_i \oplus H_{i-1}}(H_{i-1}) \oplus M_i$

no.1: Matyas-Meyer-Oseas, no.3: Miyaguchi-Preneel, no.5: Davies-Meyer

In this paper, we denote the l-block message M as $(M_1, M_2, \cdots, M_l)$ and i^{th} compression function input as H_{i-1}. Naturally, IV becomes H_0 and message digest becomes H_l.

3 Collision Attacks on Robin-Based Hash Functions

3.1 Chosen-key Differential Paths of Robin

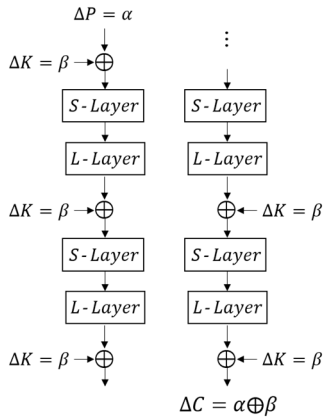

Fig. 4. Differential paths of Robin

As a result of our S-Box analysis, the maximum probability of differential characteristics is 2^{-4}, and there are total 168 such differential paths. For each of these differential paths, if we precomputes the difference after the L-Layer, one-round iterative differential paths can be derived using related-key. For the i^{th} round function R^i, this one-round iterative related-key differential paths can be expressed by the following equations (Figure 4).

$$R^i_{K\oplus\beta}(P\oplus\alpha) = L\big(S(P\oplus\alpha\oplus\beta)\big)\oplus K\oplus Cst(i) = L\big(S(P)\big)\oplus\alpha\oplus K\oplus Cst(i)$$

Since the S-Box is applied to each column, one-round iterative related-key differential paths with probability of 2^{-4} can exist if there is only one column difference. So one can induce $168\times 16 = 2{,}688$ one-round iterative related-key differential paths. Since each round has a probability of 2^{-4} and Robin proceeds 16 rounds, a total success rate to find each related-key differential path is 2^{-64}.

With chosen-key assumption, we can ensure the first round differential path with probability of 1 by fixing the value of first round S-Layer input. Then, the success rate to find each chosen-key differential path is 2^{-60}.

3.2 Collision Attack Framework

A collision attack framework for block cipher based hash function was proposed in [5]. The related-key differential paths of Robin derived from Section 3.1 are applicable to collision attack framework since the plaintext difference and the ciphertext difference are the same. The attack framework proposed in [5] is as follows.

Step 1. By trying sufficiently many random messages in the first compression function, find a chaining variable pair that satisfies one of the block cipher's chosen-key differential path.

Step 2. Set a second-block message pair having difference which satisfies the block cipher's chosen-key differential path.

Step 3. Find a second-block message pair satisfying the block cipher's related-key differential path.

3.3 Collision Attacks on Robin-based PGV models

The probability of the chosen-key differential paths of Robin presented in section 3.1 is 2^{-60}. We first describe our collision attack on PGV no.4 instantiated with Robin.

Since PGV no.4 takes chaining variable as block cipher's key and plaintext, the difference of chaining variable pair resulting from Step 1 should be β. There are 2,688 one-round iterative related-key differential paths having probability 2^{-4}, and their β are all different from each other. Therefore, for Step 1, we set the number of messages trying for the first compression function to $2^{59.4}$. Then the success rate to find a chaining variable pair that satisfies the block cipher's chosen-key differential path can be calculated as follows.

$$
\begin{aligned}
&1-(1-2{,}688/2^{128})^{119}\\
&=1-(1-2^{-116.6})^{117.8}\\
&=1-((1-2^{-116.6})^{-116.6})^{-1.2}\\
&=1-e^{-1.2}\\
&=0.70
\end{aligned}
$$

In Step *2*, we set a difference of second-block message pair as $\alpha \oplus \beta$ so that the block cipher's plaintext and key differences respectively be α, β.

For *Step 3,* we set the number of messages trying for the second compression function to 2^{60}. Then the success rate to find a collision digest pair can be calculated as follows.

$$
\begin{aligned}
&1-(1-2^{-60})^{60}\\
&=1-e^{-1}\\
&=0.63
\end{aligned}
$$

Therefore, the total success rate of collision attack on Robin-based PGV no.4 is about $(0.44 = 0.70 \times 0.63)$. The time complexity required for this collision attack is about $2^{60.7}(= 2^{59.4} + 2^{60})$

Table 2 shows our collision attack results on Robin-based twelve PGV models. The collision attack framework is feasible on PGV nos. 3, 4, 7, 8, 11, and 12 but infeasible on the other PGV models. In PGV nos. 8 and 11, the difference of chaining variable resulting from *Step 1* is $\alpha \oplus \beta$, and for PGV nos. 7 and 12, it is α. Since there are only 576 $\alpha \oplus \beta$ and 1,152 α in the Robin's chosen-key differential paths, the time complexities for collision attacks on them are higher than the others.

4 Conclusion

In this paper, we show various collision attacks on Robin-based PGV hash functions. This result implies that Robin is not suitable for use in several PGV hash modes. For future work, it is important to find block ciphers having related(or chosen)-key differential paths which can be used in collision attack framework.

Table 2. Results of collision attacks on PGV models instantiated with Robin

PGV	Time complexity	Success rate
no.3	$2^{60.7}$	0.44
no.4	$2^{60.7}$	0.44
no.7	2^{61}	0.44
no.8	$2^{61.3}$	0.44
no.11	$2^{61.3}$	0.44
no.12	2^{61}	0.44

Acknowledgment

This work was supported by Institute for Information & communications Technology Promotion(IITP) grant funded by the Korea government(MSIT) (No. 2017-0-00344, Deciphering and forensic analysis of recent mobile devices)

References

[1] Vincent Grosso, Gaëtan Leurent, François-Xavier Standaert, and Kerem Varici, "LS-designes: Bitslice encryption for efficient masked software implementations. In *FSE 2014,* volume 8540 of *Lecture Notes in Computer Science*, pages 18-37, Springer, 2014.

[2] Ullrich, M., Canniere, C.D., Indesteege, S., Küçük, Ö., Mouha, N., Preneel, B., Finding Optimal Bitsliced Implementations of 4x4-bit S-Boxes, *Symmetric Key Encryption Workshop*, 2011.
[3] Matsui, M., New Block Encryption Algorithm MISTY, *FSE 1997*, volume 1267 of *Lecture Notes in Computer Science,* page 54-68, Springer, 1997.
[4] Preneel, B., Govaerts, R., Vandewalle, J., Hash functions based on block ciphers: A synthetic approach, *CRYPTO 1993*, volume 773 of *Lecture Notes in Computer Science,* page 368-178, Springer, 1993.
[5] Hangi Kim, Dowon Kim, Okyeon Yi, and Jongsung Kim, Cryptanalysis of hash functions based on blockciphers suitable for iot service platform security, Accepted at *Multimedia Tools Applications*, 2018.

Hangi Kim has been a MS course student in Kookmin University, Korea since March 2016. His research interest is symmetric cryptography.

Jongsung Kim is currently associate professor in Kookmin University, Korea. His research interest is symmetric cryptography and digital forensic.