SCIENCE CHINA
Information Sciences

• HIGHLIGHT •

September 2018, Vol. 61 098103:1–098103:3
https://doi.org/10.1007/s11432-017-9231-5

Differential attacks on reduced SIMON versions with dynamic key-guessing techniques

Ning WANG[1,2], Xiaoyun WANG[1,2,3*], Keting JIA[4] & Jingyuan ZHAO[5]

[1]*Key Laboratory of Cryptologic Technology and Information Security, Ministry of Education, Shandong University, Jinan* 250100*, China;*
[2]*School of Mathematics, Shandong University, Jinan* 250100*, China;*
[3]*Institute for Advanced Study, Tsinghua University, Beijing* 100084*, China;*
[4]*Department of Computer Science and Technology, Tsinghua University, Beijing* 100084*, China;*
[5]*Beijing Research Institute of Telemetry, Beijing* 100094*, China*

Received 16 June 2017/Accepted 16 August 2017/Published online 23 April 2018

Citation Wang N, Wang X Y, Jia K T, et al. Differential attacks on reduced SIMON versions with dynamic key-guessing techniques. Sci China Inf Sci, 2018, 61(9): 098103, https://doi.org/10.1007/s11432-017-9231-5

In 2013, NSA published the specifications of two lightweight block cipher families SIMON and SPECK [1]. Since the SIMON family was announced, it has attracted a lot of attention of the cryptanalysts. In this article, we use the existing differential characteristics given in [2–5] to analyze the reduced SIMON versions. Firstly, we extend the characteristics backward and forward for several rounds and get the full differential path we need. Similar to Wang et al.'s method in [6], we deduce the sufficient bit conditions corresponding to the differential propagations. We find that the bit conditions can be divided into two types. The conditions of the first type only depend on plaintexts or ciphertexts, which can be fulfilled by selecting the conforming plaintexts, ciphertexts and building the data structures. The other type of conditions is related to the secret key. Secondly, we find that there exists some information redundancy in the second type of conditions (equations) because of the single non-linear operation in the SIMON round function. Based on the observation, we can avoid guessing some subkey bits or equivalent key bits involved in these conditions, which depend on the specific bits or the bit differences of intermediate variables. Therefore, we propose a dynamic key-guessing technique which largely diminishes the number of key guesses. With the techniques above, we are able to extend the existing best differential results on Simon by 2 to 4 more rounds. Table 1 outlines our differential results compared with some other cryptanalysis on SIMON.

Table 1 Summary of some main attacks on SIMON

Cipher	Attacked rounds	Time	Data	Reference
SIMON32/64	21	$2^{55.25}$	2^{31}	This article
	22	$2^{58.76}$	2^{32}	[7]
SIMON48/72	20	2^{52}	2^{46}	[3]
	23	$2^{63.25}$	2^{47}	This article
SIMON48/96	24	$2^{87.25}$	2^{47}	This article
	24	$2^{78.99}$	2^{48}	[7]
SIMON64/96	29	$2^{86.94}$	2^{63}	[7]
	30	2^{88}	$2^{63.3}$	This article
SIMON64/128	30	$2^{110.99}$	2^{63}	[7]
	31	2^{120}	$2^{63.3}$	This article
SIMON96/96	35	$2^{93.3}$	$2^{93.2}$	[2]
	37	$2^{87.17}$	2^{95}	This article
SIMON96/144	35	$2^{101.1}$	$2^{93.2}$	[2]
	37	$2^{130.75}$	2^{95}	This article
SIMON128/128	46	$2^{125.7}$	$2^{125.6}$	[2]
	50	$2^{119.17}$	2^{127}	This article
SIMON128/192	46	$2^{142.0}$	$2^{125.6}$	[2]
	51	$2^{183.17}$	2^{127}	This article
SIMON128/256	46	$2^{206.0}$	$2^{125.6}$	[2]
	51	$2^{247.17}$	2^{127}	This article

Brief description of SIMON and some observations. The SIMON block cipher is a Feistel structure with a $2n$-bit state, where n is required to be 16, 24, 32, 48, or 64. SIMON$2n$ with an

* Corresponding author (email: xiaoyunwang@mail.tsinghua.edu.cn)

mn-bit key is referred to as SIMON$2n/mn$, where $m = 2, 3, 4$. There are 10 suggested versions with different numbers of rounds n_r. All versions of SIMON use similar round function. The function $F(x) = ((x \lll 1) \cap (x \lll 8)) \oplus (x \lll 2)$ is a non-linear transformation from $\{0,1\}^n$ to $\{0,1\}^n$, which is built by 3 bitwise operations $\oplus$, $\cap$ and $\lll$. Let the plaintext $P = (L^0, R^0)$, and the i-th round function is defined as $L^i = R^{i-1} \oplus F(L^{i-1}) \oplus K^{i-1}$, $R^i = L^{i-1}$, where $i = 1, \ldots, n_r$. (R^{n_r}, L^{n_r}) is the ciphertext C. For more details, please refer to [1].

Observation 1. Let $x,\ x',\ y,\ y' \in \{0,1\}$, and $\Delta x = x \oplus x'$, $\Delta y = y \oplus y'$, then

$$\begin{aligned}&(x \cap y) \oplus (x' \cap y')\\ &= (x \cap \Delta y) \oplus (\Delta x \cap y) \oplus (\Delta x \cap \Delta y).\end{aligned}$$

Especially when $\Delta y = 0$ (or $\Delta x = 0$), we can obtain the differential behavior in [8] as follows:

$$\begin{aligned}&(x \cap y) \oplus (x' \cap y) = \Delta x \cap y,\\ \text{or}\quad &(x \cap y) \oplus (x \cap y') = x \cap \Delta y.\end{aligned}$$

Observation 2. Given two inputs X^{i-1} and $(X^{i-1})'$ of the i-th round, where $\Delta X^{i-1} = X^{i-1} \oplus (X^{i-1})'$, and an equation $\Delta X^{i+1}_{j+n} = b$, where $b = 0$ or 1, we can find all the solutions of the 2-bit subkey $(K^{i-1}_{(j+1)\%n}, K^{i-1}_{(j+8)\%n})$ which satisfy the equation depending on the following 5 cases.

(1) When $(\Delta X^i_{(j+1)\%n+n}, \Delta X^i_{(j+8)\%n+n}) = (0,0)$ and $\Delta X^i_{(j+2)\%n+n} \oplus \Delta X^{i-1}_{j+n} = b \oplus 1$, there is no solution of the subkey $(K^{i-1}_{(j+1)\%n}, K^{i-1}_{(j+8)\%n})$.

(2) When $(\Delta X^i_{(j+1)\%n+n}, \Delta X^i_{(j+8)\%n+n}) = (0,0)$ and $\Delta X^i_{(j+2)\%n+n} \oplus \Delta X^{i-1}_{j+n} = b$, there are 4 solutions of $(K^{i-1}_{(j+1)\%n}, K^{i-1}_{(j+8)\%n})$.

(3) When $(\Delta X^i_{(j+1)\%n+n}, \Delta X^i_{(j+8)\%n+n}) = (0,1)$, there are two solutions of $(K^{i-1}_{(j+1)\%n}, K^{i-1}_{(j+8)\%n})$.

(4) When $(\Delta X^i_{(j+1)\%n+n}, \Delta X^i_{(j+8)\%n+n}) = (1,0)$, there are two solutions of $(K^{i-1}_{(j+1)\%n}, K^{i-1}_{(j+8)\%n})$.

(5) When $(\Delta X^i_{(j+1)\%n+n}, \Delta X^i_{(j+8)\%n+n}) = (1,1)$, there are two solutions of $(K^{i-1}_{(j+1)\%n}, K^{i-1}_{(j+8)\%n})$.

Dynamic key-guessing attack. The main idea of the dynamic key guessing technique aims to remove the redundancy of the guessed subkey according to the real immediate values of a given differential path. For the same differential, the dynamic key-guessing technique is adopted to reduce the number of key bits guessed by choosing a specific plaintext pair and solving their corresponding bit equations, which decreases the computational complexity. The complexity is determined by both the probability of the differential and the number of totally equivalent key bits involved in conditions in the extended rounds before and after the differential. The differential cryptanalysis results would be improved with a better differential or the fewer guessed equivalent key bits in the extended rounds.

The main contribution of our study is to compute sufficient conditions to conform the differential path, and obtain the corresponding subkey bits equations. Furthermore, we present a new method to build structures in data collection phase, and decrease the time complexity of sieving the collected pairs. Our technique has been applied to analyze other lightweight block ciphers depending on the bitwise operations successfully.

From Observation 2, we know that, the equation $\Delta X^{i+1}_{j+n} = b$ has all the 4 solutions only with probability $\frac{1}{8}$. It has 2 solutions with probability $\frac{3}{4}$ and no solution with probability $\frac{1}{8}$. This is an example of the dynamic key bit guessing. In our attacks, we can explore more strategies of the dynamic key bit guessing according to different bit conditions. The dynamic key-guessing technique proposed in this article has been applied to other studies successfully [7, 9], and got the obvious improvements compared to the classic attacks as well.

Differential attack on SIMON32. We take the attack on 21-round SIMON32 with 13-round differential in [3] by dynamic key-guessing technique as example. For this attack, basing the following 13-round differential with probability $2^{-28.56}$:

$$D_1 : (0000, 0040) \to (4000, 0000).$$

We add 4 rounds on the top and 4 rounds at the bottom to analyse 21-round SIMON32. We totally get 44 bit conditions which ensure the middle differential path from round 4 to round 17 hold. We call them a set of sufficient conditions resulting in the differential path. We select a plaintext-ciphertext pair to make the input difference in the first round and the output difference in the last round hold. It is easy to verify that 16 conditions of rounds 1 and 20 are independent of subkey bits, 28 conditions of rounds 2–4 and 17–19 are related to subkey bits.

The clue of our attack is to build the structures in the data collection phase to keep 16 key-independent conditions hold, get 28 equations from the other 28 key-dependent conditions, then find the possible subkey candidates by solving all the solutions to these equations instead of exhaustive searching. Since there are 8 conditions independent of the secret key in round 1, we make use of these conditions to construct structures, so as to

reduce the time complexity of collecting plaintext-ciphertext pairs. In the process of key recovery attack, we use a series of techniques as Observation 2 to reduce the key space greatly.

According to the specific bit-differences in the corresponding 21-round differential path, we can compute all the solutions to 28 equations. Every solution is a possible candidate of 49-bit subkey. This phase is called computing subkey candidates. We collect all the solutions of corresponding $2^{22.74}$ pairs, and the right subkey will occur with an obvious probability advantage. It is mentioned that, the key-guessing technique is dynamic. For the different pairs which results in the same differential path, we deduce the solutions of different subkey. The subkey solved is decided by the specific differences in the differential path.

Complexity evaluation. The time complexity of computing subkey candidates is denoted as $T_{\rm csc}$. It is computed as

$$T_{\rm csc} = 2^{|{\rm sk}|} \times N \times 2^{-n_c}/(n \times n_r),$$

where $|{\rm sk}|$ is the number of independent subkeys in the extended rounds which is used to deduce the input and output differences of the differential path. N is the pairs left in the data collection which are used to sieve the right key, n_c is the number of conditions related with subkeys sk, and n_r is the rounds of the attack. Here, $T_{\rm csc} = 2^{49} \times 2^{26} \times 2^{-28}/(16 \times 21) \approx 2^{38.6}$ encryptions.

We apply the Poisson distribution in the following to compute the number of the remaining subkeys. The probability that the event ξ occurs k times is $\Pr[\xi = k] = \frac{\lambda^k}{k!} \times e^{-\lambda}$, where λ is the expectation of ξ. The expected count of a wrong subkey for all remaining pairs in data collection can be also computed by the equation

$$\lambda_e = N \times 2^{-n_c}.$$

For 21-round SIMON32/64, we know the expected count of the right key is 2.7 in the data collection. We choose the subkeys whose counts are greater than or equal to 3, and exhaustively search them by trail encryption. Therefore, the number of the remaining subkeys which should be searched is

$$2^{49}(1-\Pr[\xi_e = 0]-\Pr[\xi_e = 1]-\Pr[\xi_e = 2]) = 2^{40.25}.$$

So, we search $2^{40.25}$ 49-bit subkeys and the rest 15-bit subkey, which needs $2^{55.25}$ encryptions. We denote the exhaustive search complexity as $T_{\rm es}$. Thus the total time complexity is about $2^{55.25} + 2^{38.6} \approx 2^{55.25}$ encryptions.

Since the expected count of the right key is $\lambda_r = 2.7$, the probability that the right key count is greater than or equal to 3 is $1-\Pr[\xi_r = 0]-\Pr[\xi_r = 1] - \Pr[\xi_r = 2] = 0.51$. Therefore, our attacks on 21-round SIMON32/64 need $2^{55.25}$ encryptions with 2^{31} chosen plaintexts, and the success probability is about 51%.

Applying this technique, we present the differential attacks on SIMON32, SIMON48, SIMON64, SIMON96, and SIMON128 that can mount 2–4 more rounds than previous existing differential results which did not use the dynamic key-guessing technique.

Especially, the attacks on 5 versions of SIMON including SIMON64/96, SIMON64/128, SIMON96/96, SIMON128/128 and SIMON128/192 are currently the best results, respectively.

Acknowledgements This work was supported by National Basic Research Program of China (973 Program) (Grant No. 2013CB834205), National Natural Science Foundation of China (Grant No. 61402256), National Key Research and Development Program of China (Grant No. 2017YFA0303903), National Cryptography Development Fund (Grant No. MMJJ20170121), and Zhejiang Province Key R&D Project (Grant No. 2017C01062).

References

1 Beaulieu R, Shors D, Smith J, et al. The simon and speck families of lightweight block ciphers. IACR Cryptology ePrint Archive, 2013. https://eprint.iacr.org/2013/404.pdf
2 Abed F, List E, Lucks S, et al. Differential cryptanalysis of round-reduced simon and Speck. In: Proceedings of International Conference on Fast Software Encryption, London, 2014. 525–545
3 Biryukov A, Roy A, Velichkov V. Differential analysis of block ciphers simon and speck. In: Proceedings of International Conference on Fast Software Encryption, London, 2014. 546–570
4 Dinur I, Dunkelman O, Gutman M, et al. Improved top-down techniques in differential cryptanalysis. In: Proceedings of International Conference on Cryptology and Information Security in Latin America, Guadalajara, 2015. 139–156
5 Sun S W, Hu L, Wang P, et al. Automatic security evaluation and related-key differential characteristic search: application to simon, present, lblock, desl and other bit-oriented block ciphers. In: Proceedings of International Conference on the Theory and Application of Cryptology and Information Security, Kaoshiung, 2014. 158–178
6 Wang X Y, Yin Y L, Yu H B. Finding collisions in the full SHA-1. In: Proceedings of Annual International Cryptology Conference, Santa Barbara, 2005. 17–36
7 Qiao K X, Hu L, Sun S W. Differential analysis on simeck and simon with dynamic key-guessing techniques. In: Proceedings of International Conference on Information Systems Security and Privacy, Rome, 2016. 428–449
8 Kühn U. Improved cryptanalysis of MISTY1. In: Proceedings of International Conference on Fast Software Encryption, Leuven, 2002. 61–75
9 Chen H F, Wang X Y. Improved linear hull attack on round-reduced simon with dynamic key-guessing techniques. In: Proceedings of International Conference on Fast Software Encryption, Bochum, 2016. 428–449