SCIENCE CHINA
Information Sciences

• LETTER •

March 2023, Vol. 66 139106:1–139106:2
https://doi.org/10.1007/s11432-022-3466-x

A revisited security evaluation of Simeck family ciphers against impossible differential cryptanalysis

Kai ZHANG[1,2*], Xuejia LAI[2*], Lei WANG[2], Jie GUAN[1] & Bin HU[1]

[1]*PLA SSF Information Engineering University, Zhengzhou* 450000*, China;*
[2]*Department of Computer Science and Engineering, Shanghai Jiao Tong University, Shanghai* 201100*, China*

Received 15 January 2022/Revised 12 March 2022/Accepted 24 March 2022/Published online 30 January 2023

Citation Zhang K, Lai X J, Wang L, et al. A revisited security evaluation of Simeck family ciphers against impossible differential cryptanalysis. Sci China Inf Sci, 2023, 66(3): 139106, https://doi.org/10.1007/s11432-022-3466-x

Simeck is a family of lightweight block ciphers proposed at CHES 2015 [1]. The round function and key schedule of Simeck were inspired by SIMON and SPECK, which were proposed by the U.S. National Security Agency in 2013. Compared with these two lightweight ciphers, Simeck has a more compact hardware implementation. In addition, in 2019, the U.S. National Institute of Standards and Technology proposed a lightweight cryptography standardization project. In this project, some proposals have applied modified Simeck as a basic module, such as ACE, SPIX, and SPOC, which implies a more practical potential for Simeck.

Impossible differential cryptanalysis was originally proposed by Knudsen [2] and Biham et al. [3], respectively. It is one of the most effective cryptanalytic methods to date. The basic idea of impossible differential cryptanalysis is to establish an impossible differential distinguisher, then filter the wrong key candidates with this distinguisher until the correct key is recovered.

The security evaluation of Simeck against impossible differential cryptanalysis has lasted for years. In the specification, on the basis of impossible differential cryptanalysis, 20/24/25-round key recovery attacks can be achieved for Simeck32/48/64 [1]. In these attacks, the 24/25-round attacks are based on 13/15-round distinguishers. In 2018, Sadeghi et al. [4] proposed a method for modifying some bit differences of the internal state to derive longer distinguishers, and 15/17-round distinguishers were discovered for Simeck48/64. At ICISC 2018, Wang et al. [5] proposed single-bit impossible differential distinguishers for 11/15/17-round Simeck32/48/64 based on MILP optimization. In 2021, Wang et al. [6] presented impossible differential distinguishers with multi-active bits for the same length based on MILP optimization in the journal cybersecurity.

Key results. (1) By releasing the constraints on the number of active bits, new longest distinguishers are derived. In our experiment, the number of active bits is limited to two. For Simeck48/Simeck64, 42/240 more distinguishers are derived, which improves the ratios of all the previously reported longest distinguishers by 41.2%/300%, respectively. Moreover, the structural property of these longest distinguishers is analyzed. Among these distinguishers, 32/48 subspaces for Simeck32/Simeck48 are discovered. (2) Combined with previous techniques and these distinguishers, better key recovery attacks are proposed for all variants of Simeck. For Simeck48/Simeck64, 25/27-round key recovery attacks are proposed, which are one/two more rounds than the current best impossible differential attacks. For Simeck32, the overall complexity is reduced. A summary of all the impossible differential cryptanalysis of Simeck is included in Table 1.

Methodology. For distinguisher construction, based on the idea of [4] and the automatic searching method in [7], an overview of the longest impossible differential distinguishers is provided. In our research, the limitation of the single-bit difference is relaxed to two bits, and the structure for the longest distinguishers is analyzed. For a better key recovery attack, the equivalent-subkey technique is used to reduce the number of involved subkey bits. This technique was first used by Isobe et al. [8] to explore generic key recovery attacks on the Feistel scheme, and it is successively applied to SIMON [9] and Simeck [4, 10]. For more efficient impossible differential cryptanalysis of Simeck, the framework proposed by Boura et al. [11] at ASIACRYPT 2014 is used.

For Simeck32, the structure for a class of 11-round impossible differential distinguishers is illustrated as follows, where ΔX_i (ΔY_i) represents a single-bit difference at the i-th bit of the input (output).

(ΔX_{21}, ΔX_{27}, ΔX_0, ΔX_1, ΔX_5, ΔX_{16}, ΔX_{17}, ΔX_{18}, ΔX_{22}, ΔX_{26}, ΔY_0) =

(1) (∗, ∗, 0, 0, 0, 0, 0, 0, 0, 0, 1);
(2) (0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 1);
(3) (0, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1);
(4) (0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1);
(5) (0, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1);
(6) (0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1);
(7) (0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1);
(8) (0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 1);
(9) (0, 1, 0, 0, 0, 0, 0, 0, 0, 1, 1).

For Simeck48, the structure for a class of 15-round impossible differential distinguishers is illustrated as follows.

* Corresponding author (email: zhkai2010@139.com, lai-xj@cs.sjtu.edu.cn)

Table 1 Summary of impossible differential cryptanalysis on Simeck

Algorithm	Attacked rounds	Length of the distinguisher	Time complexity	Data complexity	Memory complexity	Ref.
Simeck32	20	–	$2^{62.6}$	2^{32}	2^{56}	[1]
	20	**11**	$\mathbf{2^{61.11}}$	$\mathbf{2^{32}}$	$\mathbf{2^{51}}$	**This paper**
Simeck48	24	13	$2^{94.7}$	2^{48}	2^{74}	[1]
	22	15	$2^{93.71}$	2^{48}	2^{40}	[4]
	25	**15**	$\mathbf{2^{94.23}}$	$\mathbf{2^{46}}$	$\mathbf{2^{67}}$	**This paper**
Simeck64	25	15	$2^{126.6}$	2^{64}	2^{79}	[1]
	24	17	$2^{127.04}$	2^{64}	2^{40}	[4]
	27	**17**	$\mathbf{2^{126.56}}$	$\mathbf{2^{63}}$	$\mathbf{2^{68}}$	**This paper**

$(\Delta X_{25},\ \Delta X_{29},\ \Delta X_{43},\ \Delta X_{47},\ \Delta Y_0) = (1)\ (*,\ *,\ 0,\ 0,\ 1)$; (2) (0, 0, 1, 0, 1); (3) (0, 0, 0, 1, 1).

For Simeck64, the structure for the 17-round impossible differential distinguishers can also be constructed in a similar approach. However, no more subspaces are discovered.

Key recovery attack. For Simeck48, we use the following 15-round impossible differential distinguisher to launch our attack: (000000000000000000000000, 000000000000000000100000) $\nrightarrow$ (000000000000000000000001, 000000000000000000000000)

By appending five rounds before and after the distinguisher, we can achieve a 25-round key recovery attack. For our 25-round attack on Simeck48, 95 equivalent-subkey bits are involved. The number of bit-conditions for each round is 10, 9, 7, 5, and 2 for partial encryption and 2, 5, 7, 9, and 10 for partial decryption. The dimension of the input space (output space) is 33. For each fixed output (input) difference, there are four single-bit input (output) differences. To sum up, the parameters for our attack are as follows.

According to the formula in [11], the complexities of our 25-round attack on Simeck48 are as follows: $k_{\text{in}} = 54, k_{\text{out}} = 41, c_{\text{in}} = 33, c_{\text{out}} = 33, n_{\text{in}} = 4, n_{\text{out}} = 4, |\Delta'_{\text{in}}| = 35, |\Delta'_{\text{out}}| = 35, C'_E = \frac{95}{24\cdot 25} = 2^{-2.66}$

- Data complexity: $C_N = \max\{\sqrt{2^{67} \times 2^{48+1-35}}, 2^{67} \times 2^{48+1-35-35}\} = 2^{46}$.

- Memory complexity: 2^{67} plaintext pairs and corresponding ciphertext pairs.

- Time complexity: $T = (2^{46} + (2^{67} + 2^{95} \times \frac{2^{67}}{2^{66}}) \times 2^{-2.66} + 2^{96} \times (1 - 2^{-66})^{2^{67}}) \times C_E \approx 2^{94.23}$ 25-round encryptions.

For Simeck64, we use the following 17-round impossible differential distinguisher to launch our attack. (000000000000000000000000000000000, 001000000000000000000000000000000) $\nrightarrow$ (000000000000000000000000000000001, 000000000000000000000000000000000).

By appending five rounds before and after the distinguisher, we can achieve a 27-round key recovery attack. For our 27-round attack on Simeck64, 107 equivalent-subkey bits are involved. The number of bit-conditions for each round is 11, 9, 7, 5, and 2 for partial encryption and 2, 5, 7, 9, and 11 for partial decryption. The dimension of the input space (output space) is 34. For each fixed output (input) difference, there are two single-bit input (output) differences. To sum up, the parameters for our attack are as follows: $k_{\text{in}} = 62, k_{\text{out}} = 45, c_{\text{in}} = 34, c_{\text{out}} = 34, n_{\text{in}} = 2, n_{\text{out}} = 2, |\Delta'_{\text{in}}| = 35, |\Delta'_{\text{out}}| = 35, C'_E = \frac{107}{32\cdot 27} = 2^{-3.01}$.

The complexities to attack 27-round Simeck64 are as follows.

- Data complexity: $C_N = 2^{63}$.

- Memory complexity: 2^{68} plaintext pairs and corresponding ciphertext pairs.

- Time complexity: $T \approx 2^{126.56}$ 27-round encryptions.

For Simeck32, based on an 11-round impossible differential distinguisher, we append four rounds on the top and five rounds on the bottom to derive a 20-round key recovery attack. As the process of the attack is very similar, we omit the details to avoid redundancy. The concrete result has been illustrated in Table 1.

Acknowledgements This work was partially supported by National Natural Science Foundation of China (Grant Nos. 61802437, 61972248, 61902428, 62102448) and China Postdoctoral Science Foundation (Grant No. 2020M681314).

References

1 Yang G, Zhu B, Suder V, et al. The simeck family of lightweight block ciphers. In: Proceedings of International Workshop on Cryptographic Hardware and Embedded Systems. Berlin: Springer, 2015. 307–329
2 Knudsen L. DEAL-a 128-bit block cipher. Complexity, 1998, 258: 216
3 Biham E, Biryukov A, Shamir A. Cryptanalysis of skipjack reduced to 31 rounds using impossible differentials. In: Proceedings of International Conference on the Theory and Applications of Cryptographic Techniques. Berlin: Springer, 1999. 12–23
4 Sadeghi S, Bagheri N. Improved zero-correlation and impossible differential cryptanalysis of reduced-round SIMECK block cipher. IET Inf Secur, 2018, 12: 314–325
5 Wang X, Wu B, Hou L, et al. Automatic search for related-key differential trails in SIMON-like block ciphers based on MILP. In: Proceedings of International Conference on Information Security. Cham: Springer, 2018. 116–131
6 Wang X, Wu B, Hou L, et al. Searching for impossible subspace trails and improved impossible differential characteristics for SIMON-like block ciphers. Cybersecurity, 2021, 4: 1–14
7 Zhang K, Guan J, Hu B. Automatic search of impossible differentials and zero-correlation linear hulls for ARX ciphers. China Commun, 2018, 15: 54–66
8 Isobe T, Shibutani K. Generic key recovery attack on Feistel scheme. In: Proceedings of International Conference on the Theory and Application of Cryptology and Information Security. Berlin: Springer, 2013. 464–485
9 Sun L, Fu K, Wang M. Improved zero-correlation cryptanalysis on SIMON. In: Proceedings of International Conference on Information Security and Cryptology. Cham: Springer, 2015. 125–143
10 Zhang K, Guan J, Hu B, et al. Security evaluation on Simeck against zero-correlation linear cryptanalysis. IET Inf Security, 2018, 12: 87–93
11 Boura C, Naya-Plasencia M, Suder V. Scrutinizing and improving impossible differential attacks: applications to CLEFIA, Camellia, LBlock and SIMON. In: Proceedings of International Conference on the Theory and Application of Cryptology and Information Security, 2014. 8873: 179–199