Related-key Neural Distinguisher on Lightweight Block Ciphers SPECK-32/64, HIGHT, SIMECK-32/64 and CHAM-64/128*

Erzhena Tcydenova*, Byoungjin Seok*, Changhoon Lee**†

Dept. of Computer Science and Engineering,
Seoul National University of Science and Technology
(Graduate Student*, Professor**)

Abstract

Neural networks have shown an excellent results in various areas such as image classification and natural language processing. Application of neural networks in cryptography has been around for many years, but results have not been significant until recently. At the CRYPTO'19 a new deep learning-based distinguisher on SPECK-32/64 was proposed, which was extended to a practical key recovery attack. The proposed distinguisher was constructed using the differential characteristics of the cipher and neural distinguisher performed better than classical one. Recently most researches are conducted on extending attack to other ciphers and constructing different attack scenarios. In this paper, we extend our method of constructing a neural distinguisher using related key characteristics to lightweight block ciphers SPECK, HIGHT, SIMECK and CHAM.

I. Introduction

Security of lightweight cryptography is a big issue since it has to be resistant to all cryptanalytic attacks while providing efficient performance. A large number of lightweight block ciphers have been proposed so far, and standardization of lightweight block ciphers is still in progress. Lightweight block ciphers are designed with a relatively simpler structure and because of this they might become a target of new cryptanalytic attacks. One of the new attack methods has recently attracted interest in the field of cryptography which is Neural cryptanalysis [1]. Neural cryptanalysis showed possibility to analyze a cipher without a great amount of time and cryptographic knowledge [2]. In particular, a research presented on CRYPTO'19 by Aron Gohr [3] proposed a key recovery attack conducted by constructing a differential neural distinguisher to the lightweight block cipher SPECK, and it achieved better results than conventional differential cryptanalysis. Further researches in this field are mostly conducted on applying attacks to other algorithms and building new attack scenarios.

In this paper, we extend our study on *Related-key neural distinguisher* [1] which is method of constructing neural distinguisher using relation between keys. We apply it to lightweight block ciphers SPECK-32/64, HIGHT, SIMECK-32/64 and CHAM-64/128. Also we apply Gohr's neural distinguisher on HIGHT, SIMECK-32/64 and CHAM-64/128 block ciphers and compare results of Gohr's distinguisher and Related-key neural distinguisher.

* This paper was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIT) (No. 2020R1F1A1076468).

† Corresponding Author: chlee@seoultech.ac.kr

II. Background

1.1. Related works

Neural Distinguisher proposed by Gohr on CRYPTO'19 is based on convolutional neural network model ResNet, the winning model of the image classification competition ILSVRC'15. Input of the distinguisher consist of two concatenated ciphertexts $C_0||C_1$ converted to binary, where $C_0 = SPECK_K(P_0)$ and $C_1 = SPECK_K(P_0 \oplus (0x0040, 0x0000))$. Ouput of the d is a result of determining whether the input data is a ciphertext or a random data. Their proposed neural distinguisher on Speck achieved better results than existing differential distinguisher and results are shown in the Table 1.

R	Model	Accuracy
5	Neural distinguisher	0.929
5	Differential distinguisher	0.911
6	Neural distinguisher	0.788
6	Differential distinguisher	0.758
7	Neural distinguisher	0.616
7	Differential distinguisher	0.591

Table 1. Differential Distinguisher on SPECK-32/64

Inspired by this work several studies were conducted. Anubhab Baksi et al. [4] proposed new neural network distinguisher scenario using the concept of an all-in-one differential that performs an attack using multiple differences. Tarun Yadav et al. [5] constructed distinguisher by extending classical differential distinguisher with high probability of r-round by using the s-round machine learning distinguisher and it distinguishes $r+s$ rounds.

1.2. Related-key attack.

A related-key attack is a type of cryptographic attack that exploits some mathematical relation between keys. Relation is a some function F known or selected by an attacker where $K_1 = F(K_0)$. One of the its forms is differential relation between keys such $K_1 = K_0 \oplus \Delta$. This relation exploits properties of differential distribution when plaintexts are encrypted with related keys [6].

1.3. Lightweight block ciphers

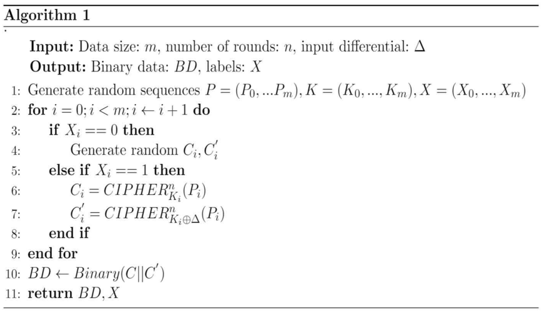
SPECK-32/64 is block cipher that has a Feistel structure with 32-bit block, 64-bit key and 32 rounds. Round function consists of simple operations: bitwise XOR, addition modulo 2^{16} and circular shifts [7]. Block cipher HIGHT has ARX based Feistel structure. It consists of operations such as XOR, addition modulo 2^8, and left bitwise rotation. HIGHT has 32 rounds, 64-bit block size and 128-bit key size [6]. SIMECK-32/64 is block cipher with Feistel structure. It consists of circular shift, bitwise AND and bitwise XOR operations and it has 32-bit block, 64-bit key and 32 rounds [8]. CHAM-64/128 is a block cipher with 64-bit block, 128-bit key, 80 rounds and it has Feistel structure. It consist of bitwise XOR, addition modulo 2^{16} and circular shifts [9].

III. Related-key Neural Distinguisher

Neural distinguisher proposed by Gohr was constructed by exploiting differential characteristics of the cipher and it had better performance than classical differential distinguisher. New method of constructing neural distinguisher which uses differential relation between keys - Related-key neural distinguisher was proposed in [1].

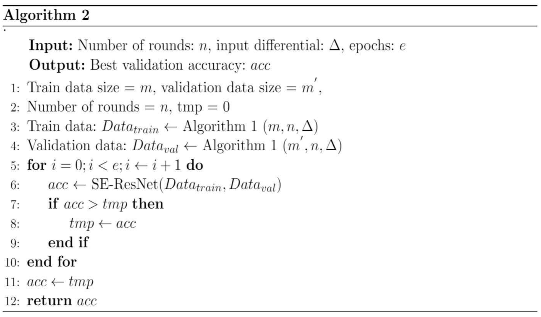
Input of the model consist of ciphertext pair $(C||C')$ where $C = CIPHER(P_K)$ and $C' = CIPHER(P_{K \oplus \Delta})$ encrypted using related key with input differential Δ. Output of the model is a result of distinguishing ciphertext of target cipher from random data.

Dataset for our distinguisher is generated using *Algorithm 1.* The algorithm generates labeled ciphertext pair $(C \| C')$ converted to binary which is result of encryption with related keys.



```
Algorithm 1
    Input: Data size: $m$, number of rounds: $n$, input differential: $\Delta$
    Output: Binary data: $BD$, labels: $X$
Generate random sequences $P = (P_0, ...P_m), K = (K_0, ..., K_m), X = (X_0, ..., X_m)$
for $i = 0; i < m; i \leftarrow i + 1$ do
    if $X_i == 0$ then
        Generate random $C_i, C_i'$
    else if $X_i == 1$ then
        $C_i = CIPHER^n_{K_i}(P_i)$
        $C_i' = CIPHER^n_{K_i \oplus \Delta}(P_i)$
    end if
end for
$BD \leftarrow Binary(C \| C')$
return $BD, X$
```

Using generated dataset we train neural network and get accuracy of distinguisher for target number of rounds by *Algorithm 2.* Neural network model used is SE-ResNet which is ResNet model with SE block from SENet. SENet is winning model of classification challenge ILSVRC‘17.



```
Algorithm 2
    Input: Number of rounds: $n$, input differential: $\Delta$, epochs: $e$
    Output: Best validation accuracy: $acc$
Train data size = $m$, validation data size = $m'$,
Number of rounds = $n$, tmp = 0
Train data: $Data_{train} \leftarrow$ Algorithm 1 $(m, n, \Delta)$
Validation data: $Data_{val} \leftarrow$ Algorithm 1 $(m', n, \Delta)$
for $i = 0; i < e; i \leftarrow i + 1$ do
    $acc \leftarrow$ SE-ResNet$(Data_{train}, Data_{val})$
    if $acc > tmp$ then
        $tmp \leftarrow acc$
    end if
end for
$acc \leftarrow tmp$
return $acc$
```

Choice of input differential is an important part of differential related-key attack. In most cases the differential that shows good probability is a one-bit difference. In the experiments differences were chosen by exhaustive search. *Algorithm 2* was run for every one-bit difference and the differential that had the best result was chosen as a final input differential.

IV. Experiments and results

4.1. Differential neural distinguisher on HIGHT, SIMECK and CHAM.

We applied Gohr's differential neural distinguisher on block cipher HIGHT, SIMECK-32/64 and CHAM-64/128. Ciphertext pairs for input of the model are generated as follows: $C_0 = CIPHER_K(P_0)$ and $C_1 = CIPHER_K(P_0 \oplus \Delta)$.

Input differentials are one-bit differentials that had best accuracy:

- SPECK: $(0x0040, 0x0000)$
- HIGHT: $(0x00800000, 0x00000000)$
- SIMECK: $(0x0400, 0x0000)$
- CHAM: $(0x8000, 0x0000, 0x0000, 0x0000)$

Data size for training = 10^6, for validation = 10^5. Results are shown in the Table 2.

R	SPECK	HIGHT	SIMECK	CHAM
1	1.0	1.0	1.0	1.0
...	...	...	...	...
5	0.9065	1.0	1.0	1.0
6	0.7540	1.0	0.9997	0.9999
7	0.5078	0.9999	0.9970	1.0
8	-	0.9990	0.9720	0.9999
9	-	0.7472	0.7888	1.0
10	-	-	0.6125	0.9999
...	-	-	-	...
27	-	-	-	0.5593
28	-	-	-	0.5603

Table 2. Results of Gohr' neural distinguisher on HIGHT, SIMECK and CHAM

4.2. Related-key neural distinguisher on SPECK, HIGHT, SIMECK and CHAM.

Ciphertext pairs are generated as follows: $C = CIPHER(P_K)$ and $C' = CIPHER(P_{K \oplus \Delta})$. Input differentials:

- SPECK: $(0x0040, 0x0000, 0x0000, 0x0000)$
- HIGHT: $(0x0000000080000000, 0x0000000000000000)$
- SIMECK: $(0x0000, 0x0000, 0x0000, 0x1000)$
- CHAM: $(0x0000, 0x0000, ..., 0x0000, 0x4000)$

Training data size – 10^6, validation – 10^5. Results are shown in the Table 3.

R	SPECK	HIGHT	SIMECK	CHAM
1	1.0	1.0	1.0	1.0
...	...	...	...	...
6	1.0	1.0	1.0	1.0
7	0.9773	0.9999	0.9999	0.9999
8	0.8467	0.9999	0.9998	1.0
9	0.5920	0.9998	0.9957	1.0
10	–	0.9991	0.9706	1.0
11	–	0.7493	0.7818	1.0
12	–	–	0.6088	0.9999
...	–	–	–	...
27	–	–	–	0.6496
28	–	–	–	0.5348

Table 3. Results of Related-key neural distinguisher

Related-key neural distinguisher on SPECK was able to improve a number of attacked rounds by 2 compared to Gohr's results. Similarly to results of SPECK, proposed distinguisher on HIGHT and SIMECK attacked 2 more rounds compared to Gohr's distinguisher. Results of proposed related-key distinguisher on CHAM did not show improvement of attacked rounds. By these results, we can assume that distribution of related-key characteristics have higher non-random behavior than differential characteristics for SPECK, HIGHT and SIMECK and similar for CHAM.

V. Conclusion

In this paper we extended our study [1] on neural distinguishers. We applied Related-key neural distinguisher on lightweight block ciphers SPECK, HIGHT, SIMECK and CHAM. Application of this method which uses differential relation between keys showed to have better results that Gohr's distinguisher for SPECK, HIGHT, SIMECK and similar for CHAM. These results show that we can improve performance of neural distinguisher by constructing new attack scenarios using different properties of ciphers.

[Reference]

[1] E. Tcydenova, Cryptanalysis of lightweight block ciphers based on neural distinguisher, Master's thesis, 2021.

[2] E. Tcydenova, M. Cho, B. Seok, C. Lee, Application of Neural Differential Distinguisher on SIMON-32/64, CISC-S, 2020

[3] A. Gohr, Improving attacks on round-reduced speck32/64 using deep learning, Annual International Cryptology Conference, Springer, Cham, 2019.

[4] A. Baksi, J. Breier, X. Dong, C. Yi, Machine Learning Assisted Differential Distinguishers For Lightweight Ciphers, IACR Cryptol. ePrint Arch, 2020

[5] T. Yadav, M. Kumar, Differential-ML Distinguisher: Machine Learning based Generic Extension for Differential Cryptanalysis.

[6] B. Koo, D. Hong, D. Kwon, D, Related-key attack on the full HIGHT, In International Conference on Information Security and Cryptology, Springer, Berlin, Heidelberg.

[7] R. Beaulieu, D. Shors, J. Smith, S. Treatman-Clark, B. Weeks, L. Wingers, The SIMON and SPECK lightweight block ciphers, Proceedings of the 52nd Annual Design Automation Conference, 2015.

[8] G. Yang, B. Zhu, V. Suder, M.D. Aagaard, G. Gong, The simeck family of lightweight block ciphers, International workshop on cryptographic hardware and embedded systems, Springer, Berlin, Heidelberg, 2015.

[9] B. Koo, D. Roh, H. Kim, Y. Jung, D.G. Lee, D. Kwon, CHAM: a family of lightweight block ciphers for resource-constrained devices, International Conference on Information Security and Cryptology, Springer, Cham, 2017.