Xiaowei LI, Jiongjiong REN, Shaozhen CHEN, 2024. Improved deep learning aided key recovery framework: applications to large-state block ciphers. *Frontiers of Information Technology & Electronic Engineering*, 25(10):1406-1420. https://doi.org/10.1631/FITEE.2300848

Improved deep learning aided key recovery framework: applications to large-state block ciphers

Key words: Deep learning; Large-state block cipher; Key recovery; Differential cryptanalysis; SIMON; SPECK

Corresponding author: Jiongjiong REN
E-mail: jiongjiong_fun@163.com
ORCID: https://orcid.org/0000-0003-2223-4329

Motivation

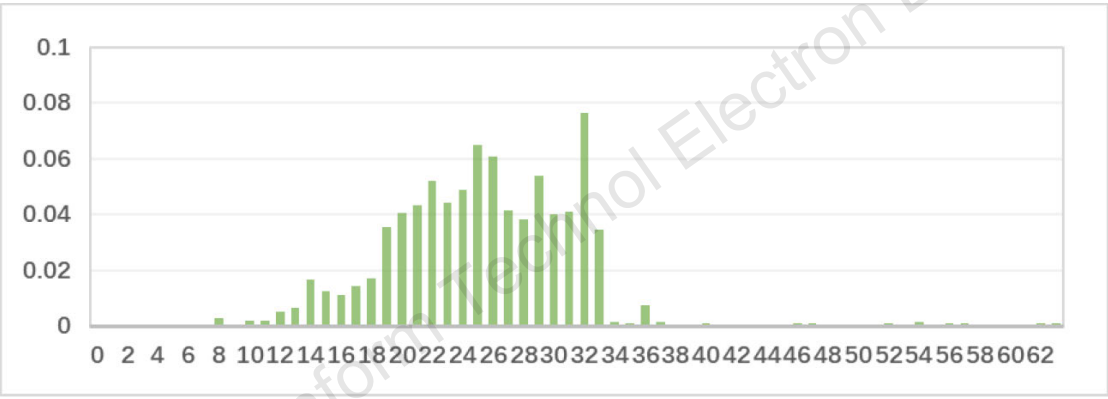
- At the Annual International Cryptology Conference in 2019, Gohr introduced a deep learning based cryptanalysis technique applicable to the reduced-round lightweight block ciphers with a short block of SPECK32/64. One significant challenge left unstudied by Gohr's work is the implementation of key recovery attacks on large-state block ciphers based on deep learning.
- Considering that Gohr's key recovery attack requires guessing all bits of the round key at once, the attack complexity is excessively high. The neural distinguisher suggested by Gohr uses only a portion of the available bit knowledge, making it difficult to recover bits with minimal or without impact on the neural distinguisher.

Main idea

- Design a deep learning based key bit sensitivity test (KBST) and divide the round key space. By using this technique, we aim to find an effective set of neural distinguishers that are trained with single-bit input differences, to achieve reduction of the round key.
- Propose a new method for constructing neural distinguisher combinations and improve a deep learning aided key recovery framework for large-state block ciphers.
- Propose a practical key recovery attack on large-state SIMON members and improve the results of the practical key recovery attack on large-state SPECK members.

Method

To achieve reduction of the round key, we design a deep learning based KBST.



The outcomes of KBST on the neural distinguisher for 15-round SIMON128. The input difference is (0x0, 0x200000000).

We propose a new method to construct neural distinguisher combinations based on the test results of the KBST technique. This will improve the deep learning aided key recovery framework for large-state block ciphers.

Results

Table 1 Summary of practical key recovery attacks on large-state SIMON and SPECK

Block cipher	Number of rounds	Time complexity	Data complexity	Success rate	hw(kg, rk)	Work
SIMON128	18	$2^{19.94}$	$2^{16.58}$	0.81	1.7	Ours in Section 5.1
	19	$2^{19.70}$	$2^{16.58}$	0.18	1.4	Ours in Section 5.1
SIMON96	14	$2^{19.16}$	$2^{16.32}$	0.35	3.3	Ours in Section 5.2
SIMON64	13	$2^{25.70}$	$2^{13.24}$	0.57	–	Hou et al. (2023)
	13	$2^{18.00}$	$2^{15.58}$	0.94	1.1	Ours in Section 5.3
	14	$2^{18.37}$	$2^{15.58}$	0.44	1.6	Ours in Section 5.3
SPECK128	12	$2^{23.30}$	$2^{16.32}$	0.52	3.2	Chen et al. (2022)
	12	$2^{22.96}$	$2^{16.32}$	0.70	1.4	Ours in Section 5.4
SPECK96	10	$2^{20.94}$	$2^{16.00}$	0.81	1.4	Chen et al. (2022)
	10	$2^{19.92}$	$2^{16.00}$	0.83	0.4	Ours in Section 5.4
SPECK64	9	$2^{18.13}$	$2^{15.58}$	0.90	1.6	Chen et al. (2022)
	9	$2^{18.10}$	$2^{15.58}$	0.96	0.6	Ours in Section 5.4

hw(kg, rk) is the average Hamming distance between the guessed key and the round key. "–" means that Hou et al. (2023) used the parameter $\text{hw}(\text{kg}, \text{rk}) \leq 7$ to calculate the success rate of key recovery. However, they did not disclose the specific value of hw(kg, rk). We use the parameter $\text{hw}(\text{kg}, \text{rk}) \leq 3$ to calculate the success rate of key recovery

Conclusions

In this paper, we first propose a deep learning based KBST method to divide the key space, and study the effect of different single-bit input differences on the accuracy of large-state SIMON and SPECK neural distinguishers. Furthermore, we investigate the key bit sensitivities of diverse neural distinguishers using this method. Meanwhile, we propose a new technique for constructing neural distinguisher combinations, and conduct a practical key recovery attack on SIMON and SPECK large-state members.

Xiaowei LI’s research interests include deep learning and cryptanalysis.

Jiongjiong REN’s research interests include the design and analysis of symmetric ciphers.

Shaozhen CHEN’s research interests include cryptanalysis and information security.