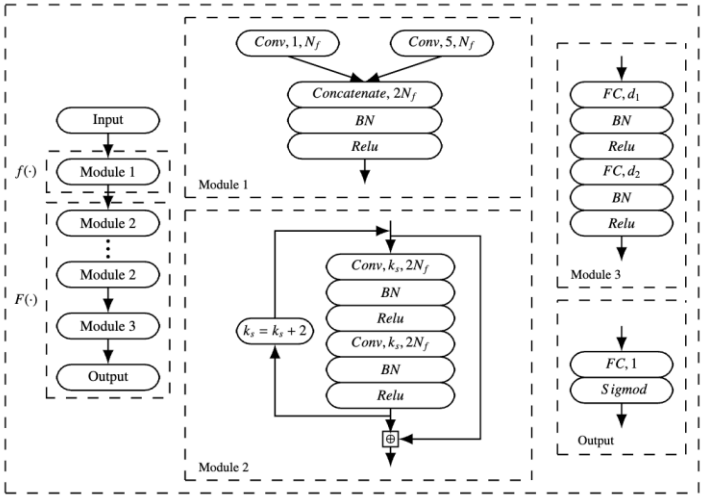
Improved Differential-neural Cryptanalysis for Round-reduced Simeck32/64

Liu ZHANG, Jinyu LU, Zilong WANG, Chao LI

Frontiers of Computer Science, DOI: 10.1007/s11704-023-3261-z

Problems & Ideas

- The question of how to improve differential-neural cryptanalysis:
  - Design the most reasonable and effective neural network for Simeck.
  - A fair and reasonable comparison of the performance of differential-neural distinguisher and DDT-distinguisher.
- Ideas: Use multiple parallel convolutional layers to capture the multi-dimensional features of the ciphertext, improve the performance of the distinguisher.



The network architecture for Simeck32/64.Module 2:Each convolutional block consists of two layers of $2N_f$ filters. Each block applies first the convolution with kernel size k_s, then a batch normalization, and finally a rectifier layer. At the end of the convolutional block, a skip connection is added. It transfers the result to the next block. After each convolutional block, the k_s increases by 2 where k_s=3.The number of convolutional blocks is 5 in our model.

Main Contributions

- Contributions:
  - Modify the Inception neural network according to the round function of Simeck32/64; Use multiple-ciphertext pairs as input of the neural network to capture the connections between ciphertext pairs .
  - Compute the full distribution of differences induced by the input difference (0x0000, 0x0040) up to 13 rounds for Simeck32/64.
  - Improve the 15-round and launch the first practical 16-, 17-round key recovery attacks for Simeck32/64 based on Neural Distinguisher.

Table 3 Summary of key recovery attacks on SIMECK32/64

R	Configure	m	n_b	n_{cts}	n_{it}	c_1	c_2	$n_{byit1/2}$	$n_{cand1/2}$	Success Rate	Data Complexity	Run Time	Time Complexity	Ref.
15	1+3+10+1	8	14	2^9	2^{10}	10	10	5	32	88%	2^{24}	-	$2^{33.90+5^\star}$	[2]
15	1+3+10+1	8	2^8	2^{10}	2^{11}	10	10	5	32	99.17%	2^{22}	407.90s	$2^{35.31}$	This work
16	1+3+11+1	8	2^{10}	2^{10}	2^{11}	10	10	5	32	100%	2^{24}	2889.65s	$2^{38.19}$	This work
17	1+3+12+1	8	2^{12}	2^{10}	2^{11}	20	-120	5	32	30%	2^{26}	25774.82s	$2^{45.04}$	This work

n_{cts}: the number of ciphertext structure; n_b: the number of ciphertext pairs in each ciphertext structure; n_{it}: the total number of iterations on the ciphertext structures; c_1 and c_2: the cutoffs with respect to the scores of the recommended last subkey and second to last subkey, respectively; n_{byit1}, n_{cand1} and n_{byit2}, n_{cand2}: the number of iterations and a number of key candidates within each iteration in the BAYESIANKEYSEARCH Algorithm for guessing each of the last and the second to last subkeys, respectively.
Note: Time complexity is calculated in terms of the number of full rounds of SIMECK32/64 encryption per second of $2^{23.304}$ in [2]. For a fair comparison, we convert the time complexity to be calculated in terms of the number of 1-round decryption performed per second. These two benchmarks differ by about 2^5.