SCIENCE CHINA
Information Sciences

• Supplementary File •

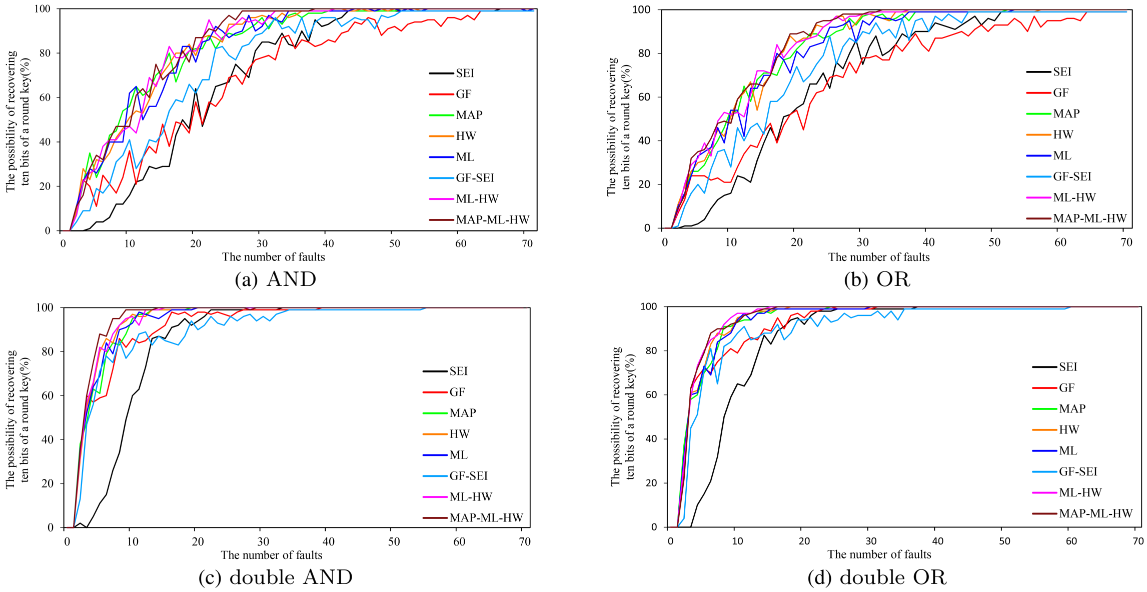
Ciphertext-Only Fault Analysis of GIFT Lightweight Cryptosystem

Wei LI[1,2,3,4], Shan CAO[1], Dawu GU[2], Jiayao LI[1],
Tianpei CAI[1], Menglin WANG[1], Li SUN[1*], Zhiqiang LIU[2] & Ya LIU[5,2]

[1] *School of Computer Science and Technology, Donghua University, Shanghai* 201620*, China;*
[2] *Department of Computer Science and Engineering, Shanghai Jiao Tong University, Shanghai* 200240*, China;*
[3] *Shanghai Key Laboratory of Computing and Systems, Shanghai* 200240*, China;*
[4] *Shanghai Key Laboratory of Integrate Administration Technologies for Information Security, Shanghai* 200240*, China;*
[5] *Department of Computer Science and Engineering, University of Shanghai for Science and Technology* 200093*, China*

Appendix A Simulation

The simulation is implemented using Java on a personal computer with 128GB memory and 16GB RAM. The attacking procedures are simulated with 10000 process units by computer software. The evaluation metrics used in the experiments are the number of fault injections, time, and time complexity. The attackers continue deriving ten bits of two round keys before recovering a whole round key. For example, in the first set of fault injections, ten bits are composed of eight bits of RK_R and two bits of RK_{R-1}.



(a) AND (b) OR

(c) double AND (d) double OR

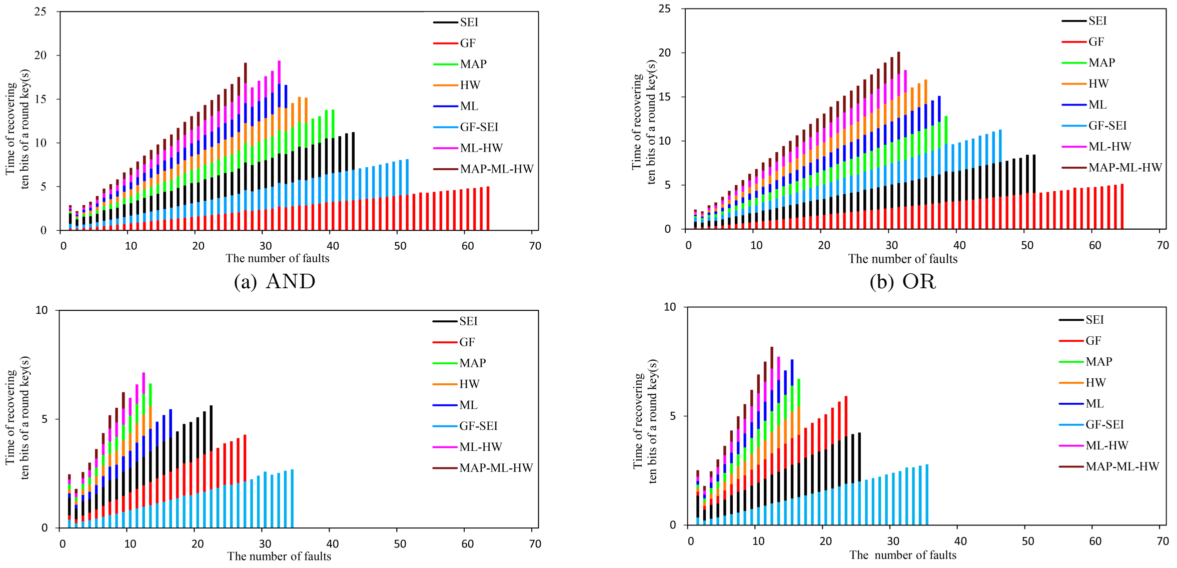
Figure A1 The recovery of ten bits on possibility.

Figure A1 shows the possibility of breaking ten bits of two round keys, where the x-coordinate represents the number of fault injections and the y-coordinate indicates the probability of recovering ten bits of two round keys. The different colored lines reflect the trend of eight distinguishers (SEI, GF, MAP, HW, ML, GF-SEI, ML-HW, and MAP-ML-HW). As Table 1 shows, at least 36 fault injections and 72 fault injections with over 99% probability are required to break GIFT-64-128 and

[*] Corresponding author (email: sli@dhu.edu.cn)

GIFT-128-128, respectively, by using the MAP-HW-ML distinguisher. Among fault models, double AND and double OR outperform AND and OR.

Figure A2 shows the time from the first set of fault injections to the recovery of ten bits in the software simulation. According to the experiment results, at least 2.8 seconds and 5.6 seconds are required to recover a round key of GIFT-64-128 and GIFT-128-128, respectively, by the MAP-HW-ML distinguisher. Thus, breaking the 128-bit secret key only requires 11.2 seconds in the best case. Among fault models, double AND and double OR require less time than AND and OR.



(a) AND

(b) OR

(c) double AND

(d) double OR

Figure A2 The recovery of ten bits on time with stacked charts.

Time complexity of distinguishers can be computed by using T, M, and N in Table A1, where $T = 2^{10}$, $M = 2^4$,, and N represents the total number of fault injections. These best results of attacks are calculated by using the MAP-ML-HW distinguisher in the fault model of double AND. With regard to attack complexity, the attackers only require the time complexity of $2^{17.21}$ and $2^{18.34}$ to break each version of GIFT.

Figures A1 and A2 and Table A1 show the probability, time, and time complexity for eight distinguishers (SEI, GF, MAP, HW, ML, GF-SEI, ML-HW and MAP-ML-HW). Compared with the AES and LED cryptosystems, two new ML-HW and MAP-ML-HW distinguishers can be applied in GIFT to improve the attack efficiency and reduce the number of faults. The experimental results for the novel fault models of double AND and double OR have a higher probability, less time, and time complexity than the previous fault models of AND and OR.

Table A1 Summary of time complexities of attacking GIFT.

Time complexities / Version & Model / Distinguisher	GIFT-64-128					GIFT-128-128				
	Formula	AND	OR	double AND	double OR	Formula	AND	OR	double AND	double OR
SEI	$4T(M+N)$	$2^{19.55}$	$2^{19.78}$	$2^{18.70}$	$2^{18.86}$	$8T(M+N)$	$2^{20.55}$	$2^{20.58}$	$2^{19.52}$	$2^{19.52}$
GF	$4T(M+N)$	$2^{20.07}$	$2^{20.09}$	$2^{18.95}$	$2^{18.75}$	$8T(M+N)$	$2^{20.88}$	$2^{20.73}$	$2^{19.86}$	$2^{19.32}$
MAP	$4T(N+1)$	$2^{19.33}$	$2^{19.26}$	$2^{17.72}$	$2^{18.02}$	$8T(N+1)$	$2^{20.01}$	$2^{20.05}$	$2^{18.82}$	$2^{18.71}$
HW	$4TN$	$2^{19.17}$	$2^{19.13}$	$2^{17.70}$	$2^{18.00}$	$8TN$	$2^{20.00}$	$2^{19.81}$	$2^{18.58}$	$2^{18.70}$
ML	$4TN$	$2^{19.04}$	$2^{19.21}$	$2^{18.00}$	$2^{18.00}$	$8TN$	$2^{19.86}$	$2^{20.25}$	$2^{18.46}$	$2^{18.81}$
GF-SEI	$4T(M+N)$	$2^{19.78}$	$2^{19.64}$	$2^{19.25}$	$2^{19.29}$	$8T(M+N)$	$2^{20.52}$	$2^{20.49}$	$2^{20.21}$	$2^{20.46}$
ML-HW	$4TN$	$2^{19.00}$	$2^{19.00}$	$2^{17.58}$	$2^{17.70}$	$8TN$	$2^{19.64}$	$2^{19.81}$	$2^{19.32}$	$2^{18.58}$
MAP-ML-HW	$4T(N+1)$	$2^{18.77}$	$2^{18.97}$	$2^{17.21}$	$2^{17.83}$	$8T(N+1)$	$2^{19.59}$	$2^{19.76}$	$2^{19.19}$	$2^{18.34}$