SCIENCE CHINA
Information Sciences

• **Supplementary File** •

Ciphertext-only Fault Analysis on the Midori Lightweight Cryptosystem

Wei LI[1,2,3,4], Linfeng LIAO[1], Dawu GU[2], Shan CAO[1], Yixin WU[1], Jiayao LI[1], Zhihong ZHOU[4], Zheng GUO[5], Ya LIU[6,2*] & Zhiqiang LIU[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 Scalable Computing and Systems, Shanghai* 200240, *China;*
[4]*Shanghai Key Laboratory of Integrate Administration Technologies for Information Security, Shanghai* 200240, *China;*
[5]*School of Microelectronics, Shanghai Jiao Tong University, Shanghai* 200240, *China;*
[6]*Department of Computer Science and Engineering, University of Shanghai for Science and Technology, Shanghai* 200093, *China*

Appendix A Simulation of ciphertext-only fault analysis on Midori

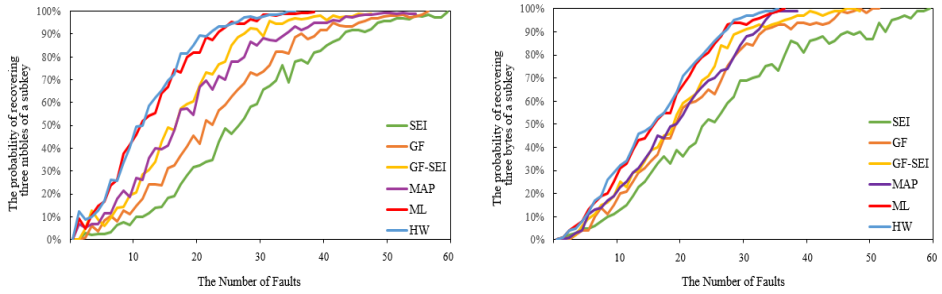

Figure A1 The recovery of three nibbles or bytes on possibility.

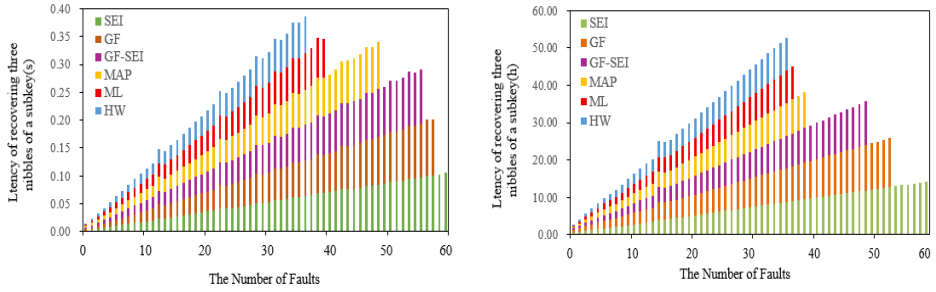

Figure A2 The recovery of three nibbles or bytes on Latency with stacked charts.

The attacking procedures are simulated with 1000 process units using computer software. The number of faults, latency, and time complexity to recover a subkey are considered for evaluate the experimental results. Figure A1 illustrates the possibility of recovering three nibbles or bytes of a subkey with different faults. The x-coordinate denotes the number of

* Corresponding author (email: liuya@usst.edu.cn)

faults, and the y-coordinate represents the probability of recovering three nibbles or bytes of a subkey. The colored lines depict the trend of six distinguishers among SEI, GF, GF-SEI, MAP, ML, and HW. To retrieve three nibbles of a subkey of Midori-64, the faults are between 60, 56, 48, 50, 37, and 35, among different distinguishers. Referring to the experimental results, breaking Midori-64 requires at most 480 faults and at least 280 faults. Breaking Midori-128 requires at most 240 faults and at least 132 faults. Latency is the time between initiating the first fault injection to break the whitening key or a subkey. The latencies are measured in seconds for Midori-64 and hours for Midori-128 as shown in Figure A2. According to the experimental results, the whole attacking procedure requires 0.52s and 35.66h to break Midori-64 and Midori-128, respectively, with 99% probability in the best case. The time complexities of all distinguishers are listed in Table A1, where $T = 2^{16}$, $M \in \{2^4, 2^8\}$, and N represents the number of all injecting faults. Both Figure A1 and Table A1 show that the probability, latency, and time complexity of the GF, GF-SEI, MAP, ML, and HW distinguishers are better than those of the SEI distinguisher. Compared with a single SEI distinguisher or a single GF distinguisher, the double GF-SEI distinguisher has higher probability, less latency, and less time complexity. Furthermore, the experimental results of the MAP, ML, and HW distinguishers are very close.

Table A1 Summary of time complexities of attacking Midori.

CFA	Time complexity	Midori-64	Midori-128
SEI	$T * (M + N + 1)$	$2^{20.96}$	$2^{32.96}$
GF	$T * (M + N + 1)$	$2^{20.86}$	$2^{32.83}$
GF-SEI	$T * (M + N + 1)$	$2^{20.65}$	$2^{32.78}$
MAP	$T * (N + 2)$	$2^{20.63}$	$2^{31.19}$
ML	$T * (N + 1)$	$2^{20.21}$	$2^{31.14}$
HW	$T * (N + 1)$	$2^{20.13}$	$2^{31.05}$