SCIENCE CHINA
Information Sciences

• **Supplementary File** •

Optimal Model Search for Hardware Trojan based Bit-level Fault Attacks on Block Ciphers

Xinjie ZHAO[1], Fan ZHANG[2,3*], Shize GUO[1] & Zheng GONG[4]

[1]*Institute of North Electronic Equipment, Beijing,* 100000*, P.R.China;*
[2]*College of Information Science and Electronic Engineering, Zhejiang University,* 310027*, P.R.China;*
[3]*School of Computing, National University of Singapore,* 117417*, Singapore;*
[4]*School of Computer Science, South China Normal University, Guangzhou,*510631*, China*

Appendix A Details of the application to DES

We propose three metrics when the fault is injected to the q-th round: η_q, the average number of faulty ciphertext bytes (or nibbles) in the last round, D_q, the depth of the fault, and $\theta_q = \frac{\eta_q}{D_q}$ which denotes the speed of the fault propagation in the last D_q rounds). To verify the generic feature of the proposed metrics, we also apply them to search the optimal fault model for hardware trojan horse based bit-level fault attack (HTH-BLFA) on the DES block cipher with a Feistel structure.

DES uses a 56-bit key (usually represented on 64 bits including 8 parity check bits) and it operates on 64-bit blocks. It has 16 iterative rounds. There is also an initial and final permutation, termed as IP and FP respectively. Before the main rounds, the block is divided into two 32-bit halves and processed alternately. In each DES round, the 32-bit right block is expanded to 48 output bits by duplicating 16 of them. The round key is then introduced by bitwise addition afterward the block is split into eight 6-bit blocks, each entering into a different S-box producing a 4-bit output. Finally, the 32 bits from the eight S-box outputs are permuted through a bit-permutation which yields the 32-bit output block.

Since DES applies many bit-based permutations, as did in [1], we apply the HTH to flip $X_{q,j}$, the j-th bit of the left half block at the end of the q-th DES round ($(0 \leqslant j \leqslant 31)$,$1 \leqslant q \leqslant 16$).

Determine the optimal round index I_o. For each q we randomly choose the value of j for 100,000 times with different plaintexts and calculate A_i ($1 \leqslant i \leqslant 16$), the average number of faulty nibbles in each round. The results are shown in Fig.A1(a). When $14 \leqslant q \leqslant 16$, only very few S-boxes in R_{16} are faulty. When $q \geqslant 10$, the values of A_i in the last two or three rounds are all close to 8, which means that the time complexity and the memory complexity are quite large for key elimination. Fig.A1(b) presents θ_q, the fault propagation speed in the last D_q rounds. We can see that the value of θ_{12} is the maximum. Thus, $I_o = 12$.

Determine the optimal bit index J_o. when $I_o = 12$, for each j, we collect 100,000 instances and calculate η_{16}, the average number of active S-boxes in the last round. The results are shown in Fig.A1(c). We can see that when $j \in \{0, 3, 4, 7, 8, 11, 12, 15, 16, 19, 20, 23, 24, 27, 28, 31\}$, η_{12} is much larger than that in other cases. The reason behind lies in the fact that, since the expansion layer E duplicates some bits, the single bit fault on those locations propagates to two S-boxes instead of one. J_o can be selected from $\{0, 3, 4, 7, 8, 11, 12, 15, 16, 19, 20, 23, 24, 27, 28, 31\}$.

Verify the fault model $\mathbb{F}_o = X_{I_o,J_o}$. As to $I_o = 12, J_o = 3$, we build a small tool to convert both of the DES cipher and C, C^* into algebraic equations and conduct AFA. The attack is repeated for 100 times with $N = 1$. The statistics of the remained key entropy $\phi(K)$ are shown in Fig.A1(d) where $\phi(K)$ is in the range $[0, 14]$ and the average value is 5.58. The average solving time is about 7.12 seconds.

Design and implement the HTH. We also design a HTH for DES on SASEBO-GII. The HTH is carefully designed to implement the optimal fault model and only one single fault injection is required to recover the secret key of DES. More details of the implementation can be referred to [2]

References

1 M. Rivain. Differential Fault Analysis on DES Middle Rounds. In CHES, Springer, 2009. 457-469.
2 F. Zhang, X. Zhao, W. He, et al. Low-cost design of stealthy hardware trojan for bit-level fault attacks on block ciphers. Science China Information Sciences, 2017, 60: 048102.

* Corresponding author (email: fanzhang@zju.edu.cn)

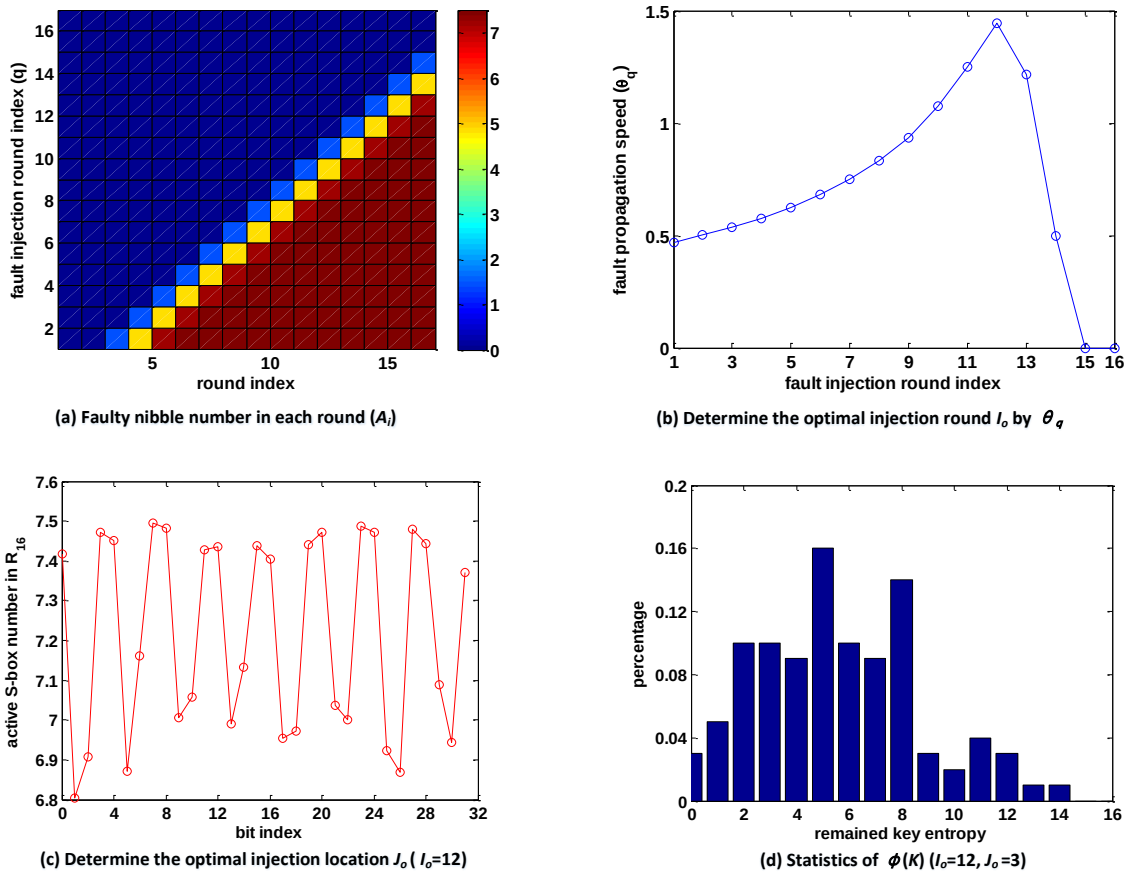

Figure A1 Optimal model search for a HTH-BLFA on DES