SCIENCE CHINA
Information Sciences

• LETTER •

March 2022, Vol. 65 139102:1–139102:3
https://doi.org/10.1007/s11432-019-2629-y

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 Jiao Tong University, Shanghai* 200240*, China;*
[4]*Shanghai Key Laboratory of Integrate Administration Technologies for Information Security, Shanghai Jiao Tong University, Shanghai* 200240*, China;*
[5]*Department of Computer Science and Engineering, University of Shanghai for Science and Technology, Shanghai* 200093*, China*

Received 26 May 2019/Revised 9 August 2019/Accepted 19 August 2019/Published online 21 May 2021

Citation Li W, Cao S, Gu D W, et al. Ciphertext-only fault analysis of GIFT lightweight cryptosystem. Sci China Inf Sci, 2022, 65(3): 139102, https://doi.org/10.1007/s11432-019-2629-y

Dear editor,

The GIFT cryptosystem was proposed by Banik et al. [1] in CHES 2017. It can be widely applied to protect RFID tags and other low-resource devices. It has an SPN structure with a fixed 128-bit key size and two flexible variants of 64-bit and 128-bit block sizes. In simulations, GIFT achieves good performance and surpasses both SIMON and SKINNY [1]. In 2013, Fuhr et al. [2] proposed a ciphertext-only fault analysis (CFA) of AES for three types of faults: zero-byte fault, zero-nibble fault, and random-byte fault. Later, Li et al. [3] added new distinguishers (GF, MAP, and GF-SEI) to the LED cryptosystem with high resistance to fault injections. Moreover, the CFA in the random nibble/byte-oriented fault model is more effective and practical.

In this study, we propose a CFA with eight different distinguishers to successfully break GIFT in software simulations. Table 1 compares the CFA of AES, LED, and GIFT. Our contributions are listed as follows:

• GIFT cannot resist against the CFA with six previous distinguishers (SEI, GF, MAP, HW, ML, and GF-SEI) in the existing fault models (AND and OR);

• Two new distinguishers, ML-HW and MAP-ML-HW, are presented to improve the efficiency and reduce fault injections;

• Two novel fault models, double AND and double OR, are applied to expand the scope of implementations.

Notations. Let X and Y represent the plaintext and the ciphertext, respectively. Let K denote the secret key. Let R represent the number of rounds with $R \in \{28, 40\}$. Let RK_r denote the round key in the r-th round with $r \in [1, R]$. Let A_r, B_r, and C_r represent the output of the SubCell, PermBits, and AddRoundKey layers in the r-th round, respectively. Let SC^{-1} and PB^{-1} denote the inverse operation of the SubCell and PermBits layers, respectively. Let N represent the total number of fault injections. Let $\sum$ and $\prod$ denote the sum and the multiplication of the elements, respectively. Let $\|$ represent concatenation. Let $\ggg$ denote the right rotation. Let $\sharp$ represent the number of elements. Let $\wedge$ and $\vee$ denote AND and OR, respectively. Let $\tilde{}$, $\bar{}$, $\hat{}$ represent the faulty value, theoretical value, and hypothesis regarding the elements, respectively.

Main procedure. Step 1: The attackers start inducing random faults in some rounds of the encryption and then obtain the corresponding set of faulty ciphertexts from any set of plaintexts. The corresponding faulty ciphertext is derived when any plaintext is encrypted with the same secret key.

Step 2: This step focuses on breaking the round keys. The first fault can be injected into either A_{R-1} or B_{R-1} in the penultimate round. It leads to a faulty intermediate state and a corresponding faulty ciphertext as follows:

$$\tilde{B}_{R-1} = \mathrm{SC}^{-1}(\mathrm{PB}^{-1}(\mathrm{SC}^{-1}(\mathrm{PB}^{-1}(\tilde{Y} \oplus \mathrm{RK}_R)) \oplus \mathrm{RK}_{R-1})).$$

The attackers can exploit the statistical analysis of $\tilde{B}_{R-1}$ to recover eight bits of RK_R and two bits of RK_{R-1}. A list of possible hypotheses of B_{R-1} can be calculated on the candidates of RK_R and RK_{R-1}.

Step 3: This step aims at recovering the secret key of GIFT. The above procedure can be repeated until the secret key is decrypted on the key schedule. The last two or four round keys are required to break each version of GIFT.

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

Table 1 Comparison of fault injections to recover the last round key of AES, LED and GIFT

Distinguisher	Cipher					
	AES-128-128	LED-64-128	GIFT-128-128/GIFT-64-128			
	AND	AND	AND	OR	Double AND	Double OR
SEI	320	560	360/172	368/204	168/88	168/100
GF	–	480	456/252	408/256	216/108	144/92
MAP	–	304	256/160	264/152	112/52	104/64
HW	288	312	256/144	224/140	96/52	104/64
ML	224	320	232/132	304/148	88/64	112/60
GF-SEI	–	424	352/204	344/184	280/136	336/140
ML-HW	–	–	200/128	224/128	80/48	96/52
MAP-ML-HW	–	–	192/108	216/124	72/36	80/56

For GIFT-64-128,

$$\begin{aligned}&\mathrm{RK}_R||\mathrm{RK}_{R-1}||\mathrm{RK}_{R-2}||\mathrm{RK}_{R-3}\\&\quad=(k_7\ggg 12||k_6\ggg 8)||(k_5\ggg 12||k_4\ggg 8)\\&\qquad||(k_3\ggg 12||k_2\ggg 8)||(k_1\ggg 12||k_0\ggg 8).\end{aligned}$$

For GIFT-128-128,

$$\begin{aligned}&\mathrm{RK}_R||\mathrm{RK}_{R-1}\\&\quad=(k_3\ggg 4||k_2\ggg 8||k_7\ggg 2||k_6\ggg 12)\\&\qquad||(k_1\ggg 4||k_0\ggg 8||k_5\ggg 2||k_4\ggg 12).\end{aligned}$$

Thus, the attackers depend on values of k_0, k_1, k_2, k_3, k_4, k_5, k_6, and k_7 to deduce secret key K.

Fault model. We propose two new fault models, double AND and double OR, in the ciphertext-only fault analysis. These two fault models can be implemented in hardware applications by careful glitch injections to the clock line [4]. The above four fault models are described as follows:

$$\begin{cases}\text{AND}: & \tilde{B}^i_{r-1,j}=B^i_{r-1,j}\wedge e_1,\\ \text{OR}: & \tilde{B}^i_{r-1,j}=B^i_{r-1,j}\vee e_1,\\ \text{double AND}: & \tilde{B}^i_{r-1,j}=B^i_{r-1,j}\wedge e_1\wedge e_2,\\ \text{double OR}: & \tilde{B}^i_{r-1,j}=B^i_{r-1,j}\vee e_1\vee e_2,\end{cases}$$

where i denotes the i-th fault injection, j represents the j-th nibble, $B^i_{r-1,j}$ denotes the j-th nibble of the PermBits layer in the (r-1)-th round, e_1 and e_2 represent random values of a nibble, $i\geqslant 1$, $r\in[1,R]$, $e_1\in[0,15]$ and $e_2\in[0,15]$.

Distinguishers.

• Squared Euclidean imbalance (SEI) is an index to measure the distance from the unknown distribution to the uniform distribution [2]:

$$\mathrm{SEI}(\mathrm{R\hat{K}}_r)=\sum_{b=0}^{15}\left(\frac{\sharp\{i|\hat{B}^i_{r-1,j}=b\}}{N}-\frac{1}{16}\right)^2.$$

When $\mathrm{SEI}(\mathrm{R\hat{K}}_r)$ is maximal, the corresponding hypothesis of RK_r is correct.

• Goodness of fit (GF) is a measurement of how well the observed values and the theoretical values match. GF can test whether a sample meets a known distribution [3].

$$\begin{aligned}&\mathrm{GF}(\mathrm{R\hat{K}}_r)\\&=\sum_{b=0}^{15}\frac{(\sharp\{i|\hat{B}^i_{r-1,j}=b\}-\sharp\{i|\bar{B}^i_{r-1,j}=b\})^2}{\sharp\{i|\bar{B}^i_{r-1,j}=b\}}.\end{aligned}$$

When $\mathrm{GF}(\mathrm{R\hat{K}}_r)$ has the minimum value, the corresponding hypothesis of RK_r is correct.

• Maximum a posteriori (MAP) probability estimate is a method that estimates an unknown quantity, as a mode of the posterior distribution [3].

$$\mathrm{MAP}(\mathrm{R\hat{K}}_r)=\frac{f(\Psi|\mathrm{R\hat{K}}_r)\cdot g(\mathrm{R\hat{K}}_r)}{\sum_{t=0}^{1023}f(\Psi|\mathrm{R\hat{K}}^t_r)\cdot g(\mathrm{R\hat{K}}^t_r)},$$

where Ψ denotes the set of $\hat{B}^i_{r-1,j}$, $f(\Psi|\mathrm{R\hat{K}}_r)$ indicates the condition probability, and $g(\mathrm{R\hat{K}}_r)$ represents the prior probability distribution of $\mathrm{R\bar{K}}_r$, respectively. When $\mathrm{MAP}(\mathrm{R\hat{K}}_r)$ has the maximal value, $\mathrm{R\hat{K}}_r$ is the correct round key.

• Hamming weight (HW) calculates the Hamming distance between a binary string and a string of zero [2].

$$\mathrm{HW}(\mathrm{R\hat{K}}_r)=\frac{1}{N}\sum_{n=1}^{N}\mathrm{hw}(\hat{B}^i_{r-1,j}),$$

where $\mathrm{hw}(\hat{B}^i_{r-1,j})$ denotes the Hamming weight of $\hat{B}^i_{r-1,j}$. For the fault models of AND (OR) and double AND (double OR), the attackers need to compute the minimum (maximum) of the Hamming weight to distinguish $\mathrm{R\hat{K}}_r$.

• Maximum likelihood (ML) is an estimate of distribution parameters based on the samples from observations [2].

$$\mathrm{ML}(\mathrm{R\hat{K}}_r)=\prod_{n=1}^{N}p(\tilde{B}^i_{r-1,j}=\hat{B}^i_{r-1,j}),$$

where p represents the theoretical probability. If $\mathrm{ML}(\mathrm{R\hat{K}}_r)$ is maximized, the round key is correct.

• Goodness of fit-square Euclidean imbalance (GF-SEI) is a double distinguisher that combines the advantages of a GF distinguisher and an SEI distinguisher [3].

$$\{\mathrm{R\hat{K}}_r|\mathrm{GF}(\mathrm{R\hat{K}}_r)\leqslant\chi^2_\alpha\},$$

where χ^2_α represents the threshold in the upper percentile table of the chi-square distribution with precision α. Only the correct RK_r can satisfy the GF distinguisher, which is not more than χ^2_a and maximizes the value of SEI.

• Maximum likelihood-hamming weight (ML-HW) is our proposed double distinguisher that connects an ML distinguisher and an HW distinguisher. The correct round key satisfies both the maximum likelihood and the minimum (maximum) Hamming weight.

$$\{\mathrm{R\hat{K}}_r|\mathrm{ML}(\mathrm{R\hat{K}}_r)\geqslant\theta\},$$

where θ denotes the probability that satisfies a certain standard. For a series of fault models of AND (OR) and double AND (double OR), the attackers need to compute the minimum (maximum) of the Hamming weight to distinguish $\mathrm{R\hat{K}}_r$, respectively.

• Maximum a posteriori-maximum likelihood-hamming weight (MAP-ML-HW) is our proposed triple distinguisher to achieve effective results of attacks in all four fault models. The attackers can use the MAP distinguisher to filter out the round key candidates that do not conform to the MAP distribution. They calculate the likelihood values of the remaining round key candidates. The correct round key corresponds to the minimum (maximum) of the Hamming weight. Specifically,

$$\{\mathrm{R}\hat{\mathrm{K}}_r|\mathrm{MAP}(\mathrm{R}\hat{\mathrm{K}}_r) \geqslant \epsilon \text{ and } \mathrm{ML}(\mathrm{R}\hat{\mathrm{K}}_r) \geqslant \theta\},$$

where ϵ denotes the mean of posterior probability, and θ indicates the probability that satisfies a certain standard. For the fault models of AND (OR) and double AND (double OR), the attackers need to compute the minimum (maximum) of HW to distinguish $\mathrm{R}\hat{\mathrm{K}}_r$ as the correct round key, respectively.

Conclusion. This study proposes to implement a CFA analysis for GIFT with eight distinguishers for four fault models (AND, OR, double AND, and double OR). In our analysis, only 36 and 72 fault injections are required to break GIFT-64-128 and GIFT-128-128 in the best case. This shows that the CFA is a strong threat to the GIFT cryptosystem.

Acknowledgements This work was supported by National Natural Science Foundation of China (Grant Nos. 61772129, 61672347), National Cryptography Development Fund (Grant Nos. MMJJ20180101, MMJJ20180202), Shanghai Key Laboratory of Scalable Computing and Systems, Shanghai Key Laboratory of Integrated Administration Technologies for Information Security (Grant No. AGK201703), Shanghai Sailing Program (Grant No. 17YF1405500), and Graduate Student Innovation Fund of Donghua University (Grant No. GSIF-DH-M-2019013).

Supporting information Appendix A. The supporting information is available online at info.scichina.com and link.springer.com. The supporting materials are published as submitted, without typesetting or editing. The responsibility for scientific accuracy and content remains entirely with the authors.

References

1 Banik S, Pandey S K, Peyrin T, et al. GIFT: a small present-towards reaching the limit of lightweight encryption. In: Proceedings of Workshop on Cryptographic Hardware and Embedded Systems, Taiwan, 2017. 321–345
2 Fuhr T, Jaulmes E, Lomné V, et al. Fault attacks on AES with faulty ciphertexts only. In: Proceedings of Workshop on Fault Diagnosis and Tolerance in Cryptography, Los Alamitos, 2013. 108–118
3 Li W, Liao L F, Gu D W, et al. Ciphertext-only fault analysis on the LED lightweight cryptosystem in the Internet of Things. IEEE Trans Depend Secure Comput, 2019, 16: 454–461
4 Balasch J, Gierlichs B, Verbauwhede I. An in-depth and black-box characterization of the effects of clock glitches on 8-bit MCUs. In: Proceedings of Workshop on Fault Diagnosis and Tolerance in Cryptography, Nara, 2011. 105–114