Power Analysis Attack on a Lightweight Block Cipher GIFT

Jian Zhang, Lang Li, Qiuping Li, Junxia Zhao, and Xiaoman Liang

Abstract GIFT is a new lightweight block cipher with smaller area and higher efficiency, which is very suitable for the Internet of Things (IoT) devices with constrained resources. The power analysis attack is an efficient method to extract the key from the cryptographic equipment. However, it is not easy to reveal the key by means of power analysis attack, when the cipher is implemented by hardware. In this article, we present the method of power analysis attack against GIFT. Firstly, we implemented GIFT on FPGA using the SAKURA-G board. Then, we explored the impact of point of interest (POI) on power analysis attack. We proposed the method of power analysis attack against the diffusion layer of GIFT. The experimental results show that the result of power analysis attack is affected by POI, and the key can be recovered when POI is registered. We can reveal the key using correlation power analysis, when targeting the diffusion layer of GIFT.

Keywords Power analysis attack · Lightweight block cipher · GIFT · SAKURA-G

1 Introduction

In recent years, with the development of new generation IoT technologies such as NB-IoT and LoRa, embedded devices are widely used in smart water meters, smart street lamps, consumer electronics, and agriculture. These devices have constrained resources and are mostly battery powered, and it is not suitable for running traditional cryptographic algorithms like AES. Therefore, many scholars have designed lightweight block cipher algorithms to ensure the data security of these resource-constrained devices. GIFT is a new lightweight block cipher proposed by Banik

J. Zhang (✉) · L. Li · Q. Li · J. Zhao · X. Liang
College of Computer Science and Technology, Hengyang Normal University, 421002 Hengyang, China
e-mail: zhangjian2100@126.com

L. Li
Hunan Provincial Key Laboratory of Intelligent Information Processing and Application, 421002 Hengyang, China

Q. Liu et al. (eds.), *Proceedings of the 9th International Conference on Computer Engineering and Networks*, Advances in Intelligent Systems and Computing 1143, https://doi.org/10.1007/978-981-15-3753-0_55

et al. [1]. GIFT has an excellent performance in power consumption and hardware resources. In addition, GIFT is highly resistant to differential and linear attacks [2], which is particularly suitable for the IoT devices.

GIFT is mathematical secure. However, power analysis attack can recover the secret key using power consumption during encryption processing. Various power analysis attacks have been proposed in the past decades, which mainly include simple power analysis (SPA) attack, differential power analysis (DPA) attack, and correlation power analysis (CPA) [3] attack. In some literature, research on power analysis attacks is based on simulation [4] or software [5, 6]. The characteristic of power consumption is quite different [7], when the cipher is implemented by hardware. Many factors influenced the result of our experiment, when we performed power analysis attack on the cipher. Point of interest (POI) is an important factor that affects the success of our experiment.

In this paper, we focus on the power analysis attack of GIFT. GIFT is written in Verilog HDL and downloaded to an FPGA in the SAKURA-G board. The power consumption of the cipher is measured during encryption processing. We used different POIs in our experiment to explore the impact of POI on power analysis attacks. Besides, we explored the method of power analysis attack on the diffusion layer of GIFT.

2 Preliminaries

2.1 GIFT

GIFT is a lightweight block cipher using SPN structure. Its key length is 128 bits, and its block length can be 64 or 128 bits. So there are two versions of GIFT: GIFT-64 with 64-bit block and GIFT-128 with 128-bit block. In our work, we use the version of GIFT-64. In this paper, we abbreviate the GIFT-64 as GIFT.

The encryption process of GIFT is shown in Fig. 1. GIFT contains 28 iterative rounds, and each round includes three operations: Substitution (S-box), Permutation (P-layer), and AddRoundKey. The GIFT algorithm uses a 4-bit S-box with 4-bit input and 4-bit output in subcells. The permutation layer changes the bit position of the cipher state according to the permutation table. The AddRoundKey contains adding the round key and round constant; the LSB 32 bits of round key and the 7 bits round constant are XORed with part of the cipher state.

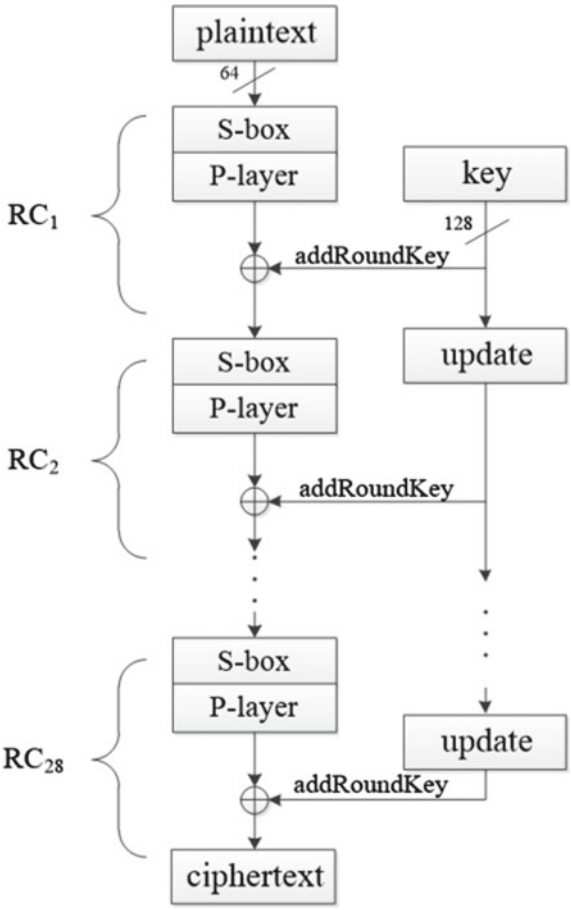

Fig. 1 Encryption process of GIFT

2.2 Power Analysis Attacks

As CPA attack has the advantages of low cost and high success rate, it has been widely used in power analysis attack. In our work, we used CPA attack to reveal the key of GIFT. The steps of a CPA attack are as follows [8]:

(1) Identify POI of the cipher;
(2) Measure power consumption during encryption processing;
(3) Guess the key and calculate hypothetical intermediate values using the input plaintext;
(4) Convert hypothetical intermediate value to hypothetical power consumption;
(5) Calculate the correlation coefficient between hypothetical and real power consumption.

2.3 *Power Analysis Model*

There are two methods to convert intermediate value to hypothetical power consumption: hamming distance model and hamming weight model [9]. Hamming distance model describes power consumption of the register. In CMOS-integrated circuit, dynamic power consumption is much larger than static power consumption. When the register stores a high or low level, there is almost no power to be consumed. If the value of the register changes from R to R', the power consumed can be expressed as:

$$W = a\mathrm{HD}(R \oplus R') + b \tag{1}$$

where $\mathrm{HD}(R \oplus R')$ is the hamming distance between the two values of the register, and a and b are constants related to the actual circuit. Hamming weight model is a simplification of hamming distance model, which assumes that the power consumption is only related to the high level of the register. Hamming weight model has a good performance in some microcontrollers with pre-charge bus [6, 9].

3 Experimental Environment

Our power analysis attack platform is shown in Fig. 2, which consists of three parts: the SAKURA-G board, PicoScope oscilloscope, and computer.

The SAKURA-G board has two spartan-6 FPGAs which serve as the controller and main security circuits. The main FPGA runs the GIFT encryption algorithm written in Verilog HDL. The controller FPGA communicates with the computer through USB, receives plaintext and key sent by the block cipher algorithm control software on computer, and controls the encryption process of the main FPGA. The

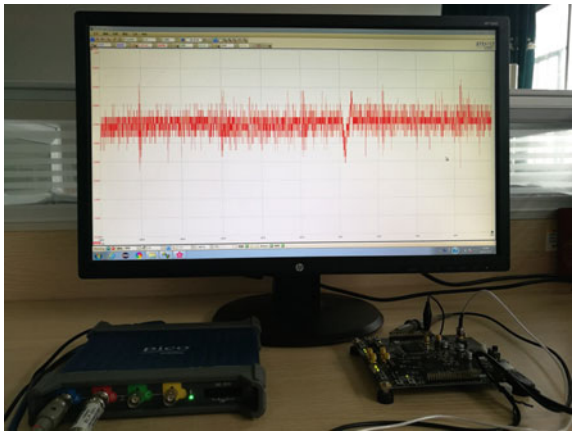

Fig. 2 Power analysis attack platform

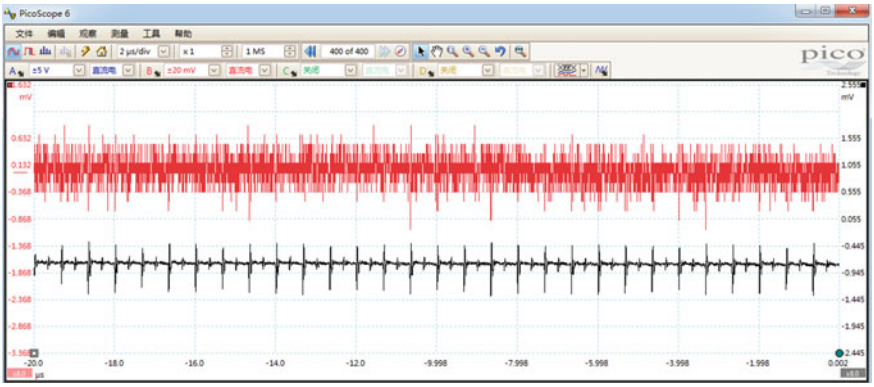

Fig. 3 Power trace of GIFT

power consumption was measured at 500 MHz frequency using the PicoScope oscilloscope. MATLAB is used to analyze the correlation between hypothetical power consumption and real power consumption.

Figure 3 depicts the power trace of GIFT, the red power trace above is the original power trace, and the black power trace below is the noise-reduced power trace. The original power trace contains a lot of noise; it will bring difficulty to power analysis attack. The noise is generated by circuits such as power supplies and clocks, and obeys normal distribution $N(0, \sigma^2)$ [10]. We use two methods to reduce the noise. On the one hand, we connected the low-pass filter to the input channel of the oscilloscope. On the other hand, we calculated the average value of the power consumption.

4 Proposed Method

4.1 Point of Interest (POI)

Figure 4 shows the rolled-based implementation of GIFT. In this architecture, the register is used to store the value of the AddRoundKey output. The register is initialized by plaintext in the first round and updated in each round.

It is not easy to recover the key by means of power analysis attack. Actually, many factors will affect the result of the experiment. POI is an important factor that affects the success of the experiment. There are many points in GIFT that can be selected as POI, such as the output of S-box, bit permutation, and AddRoundKey. In our experiment, we used two different POIs to explore the impact of POI on power analysis attack: AddRoundKey and S-box output. As the key and plaintext are known, we can calculate hypothetical power consumption of GIFT. Then, we can get the correlation coefficient between hypothetical power consumption and real power consumption.

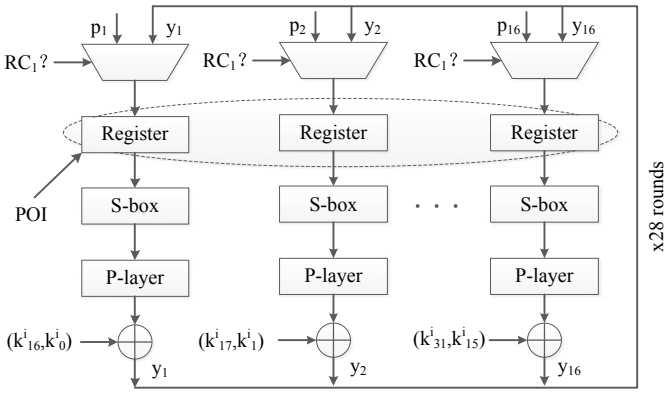

Fig. 4 Rolled-based implementation of GIFT

Firstly, we performed power analysis attack on AddRoundKey, where POI is registered. The experiment result is shown in Fig. 5. We can see that there is a significant peak near the 1000th point of the power trace, indicating that we can recover the key of GIFT using power consumption of these points.

Then, we performed power analysis attack on S-box output, where POI is not registered. The experiment result is shown in Fig. 6. The correlation coefficient of all points is approximately 0, which indicates that hypothetical power consumption has no relationship with real power consumption. Therefore, the key of GIFT cannot be recovered by power analysis attack.

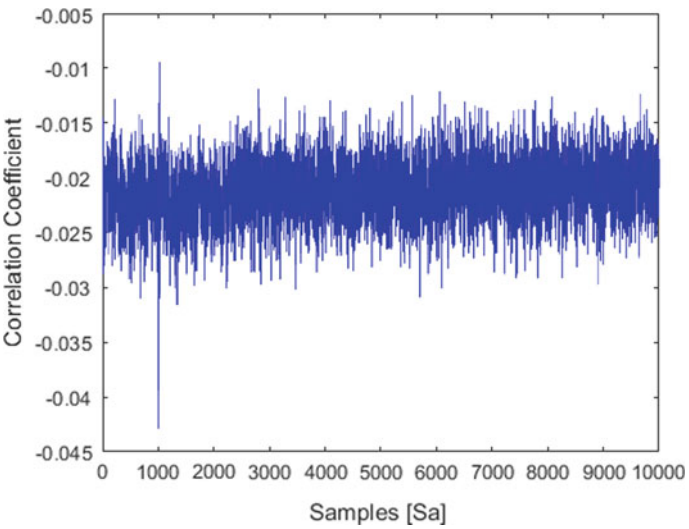

Fig. 5 Power analysis attack on AddRoundKey

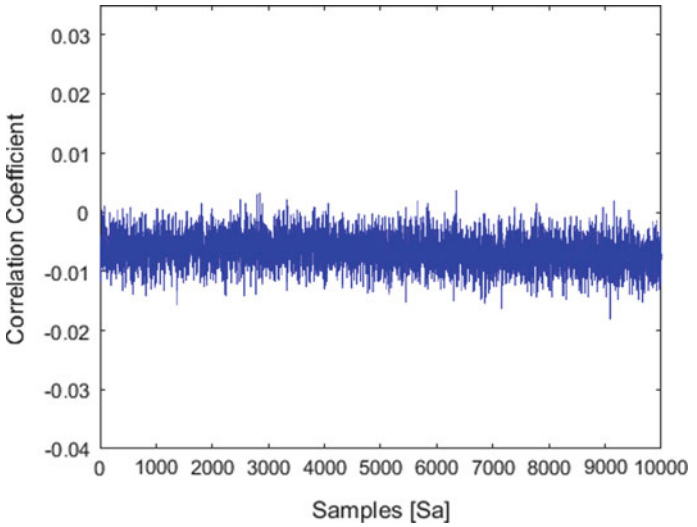

Fig. 6 Power analysis attack on S-box output

4.2 Power Analysis Attack on the Diffusion Layer of GIFT

In practical applications, in order to improve the ability to resist power analysis attacks, the register is usually set in the diffusion layer. In this case, the value stored by the register is related to multiple keys and it is impossible to reveal the key in segments by divide-and-conquer method.

Figure 7 shows power analysis attack on the diffusion layer of GIFT. In this architecture, the register is used to store the output of the diffusion layer. It seems

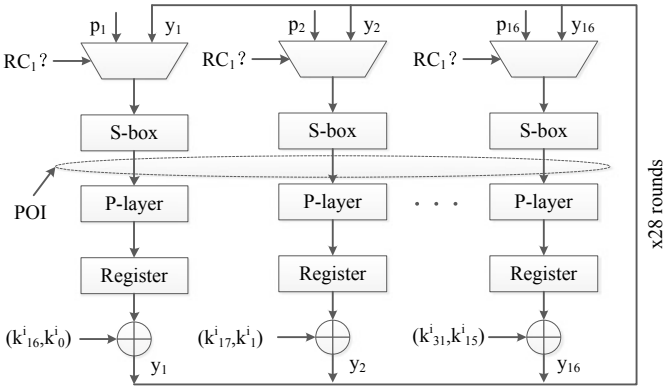

Fig. 7 Power analysis attack on the diffusion layer

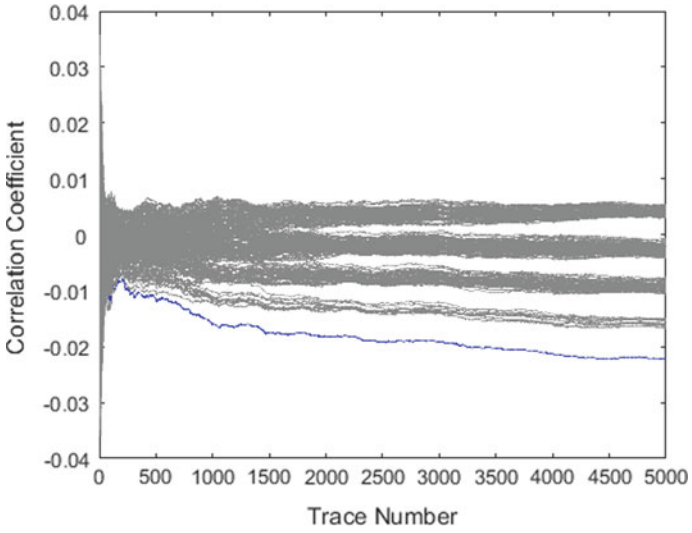

Fig. 8 Correlation coefficient of different number of traces

impossible to reveal the key using power analysis attack. However, the diffusion layer of GIFT only permutes the bits of S-box output. Therefore, we can attack the S-box output of GIFT and recover the key.

In this experiment, we set the key to 0xfedcba9876543210fedcba9876543210 and encrypted random plaintext. Figure 8 depicts the impact of the number of power traces on power analysis attack, and the minimum number of power traces to reveal the key is about 1000.

We used 1000 power traces to reveal the key in our experiment. Guessing LSB 8 bits of the key (k19k18k17k16k3k2k1k0) and calculating hypothetical intermediate values of GIFT. According to Hamming distance model, the lowest 16 bits of the plaintext are XORed with the lowest 16 bits of the S-box output at the first round, and the result is hypothetical power consumption. Then, we calculated the correlation coefficient between hypothetical power consumption and real power consumption. Figure 9 shows the result of power analysis attack. In the figure, the abscissa is the guess key, and the ordinate is the correlation coefficient. The correlation coefficient is the largest when the guess key is 64. Therefore, we believe that the correct key is 64, which is consistent with the real key we use, meaning that we successfully recovered the key of GIFT. Using the same method, we can reveal the remaining keys.

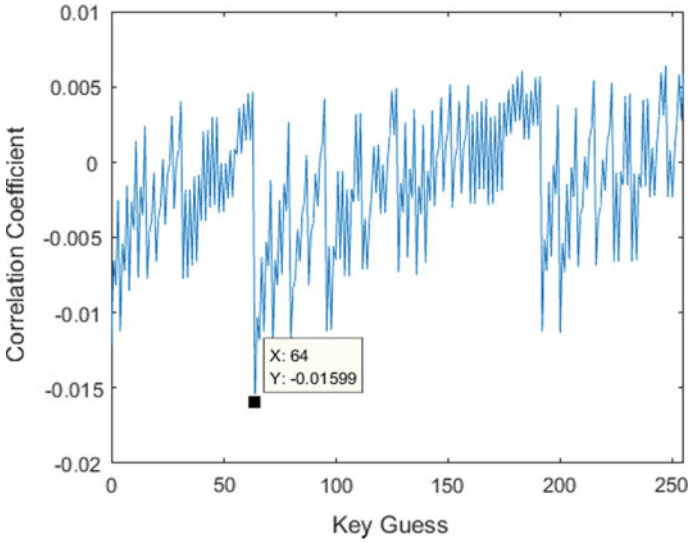

Fig. 9 Power analysis results

5 Conclusion

In this paper, we have proposed the method of power analysis attack on GIFT implemented by hardware. Our research includes the impact of POI on power analysis attack and the method to reveal the key targeting the diffusion layer of GIFT. Although there are many intermediate values associated with the key in the cipher, POI should be registered; otherwise, we will not be able to reveal the key. The diffusion layer of GIFT is bit permutation; hence, it did not bring more difficulties to our experiments, and the key can be recovered using correlation power analysis. The experimental results show that the GIFT cryptographic algorithm without protection cannot resist power analysis attack. In the future, we will study the countermeasures of GIFT with low power consumption and small area.

Acknowledgements This research is supported by the Science Foundation Project of Hengyang Normal University (18A14), National Natural Science Foundation of China under Grant No. 61572174, Application-oriented Special Disciplines. The Double First-Class University Project of Hunan Province is supported by Hunan Province Office of Education (Xiangjiaotong [2018] 469), Hunan Province Special Funds of Central Government for Guiding Local Science and Technology Development No. 2018CT5001, Hunan Provincial Natural Science Foundation of China with Grant No. 2019JJ60004, the Science and Technology Plan Project of Hunan Province No. 2016TP1020, Subject group construction project of Hengyang Normal University No. 18XKQ02.

References

1. Banik, S., Pandey, S.K., Peyrin, T., Sasaki, Y., Sim, S.M., Todo, Y.: GIFT: a small present towards reaching the limit of lightweight encryption. In: Fischer, W., Homma, N. (eds.) CHES 2017, LNCS 10529, pp. 321–345. Springer, Cham (2017)
2. Zhao, J.Y., Xu, S.Y., Zhang, Z.J., Dong, X.Y., Li, Z.: Differential analysis of lightweight block cipher GIFT. J. Cryptol. Res. **5**(4), 335–343 (2018)
3. Cai, C., Chen, Y., Wan, W.N., Chen, J., Hu, X.X.: Correlation power analysis for AES based-on principal component analysis. Appl. Electr. Tech. **41**(8), 101–105 (2015)
4. Hu, W.J., Wang, A., Wu, L.J., Xie, X.J.: Power attack of SM4 hardware implementation based on SAKURA-G board. Microelectr. Comput. **32**(4), 15–20 (2015)
5. Li, L., Li, R.F., Li, K.L., Wang, Y., Jiao, G., Zou, Y.: Differential power analysis attacks on PRESENT. Appl. Res. Comput. **31**(3), 843–845 (2014)
6. Zhang, X.Y., Chen, K.Y., Zhang, Y., Gui, W.L.: Improved correlation power analysis based on difference variability. Appl. Res. Comput. **34**(9), 2791–2794 (2017)
7. Zhang, S.W., Yang, X.Y., Zhong, W.D., Wei, Y.C.: Combinational side-channel attack on S-box in block cipher. Appl. Res. Comput. **33**(2), 498–501 (2016)
8. Wang, Z.Y., Zhang, P., Chen, C.S., Hu, H.G.: Pre-processing of power traces in power analysis. Commun. Technol. **50**(4), 765–770 (2017)
9. Luo, P., Feng, D.G., Zhou, Y.B.: Power model in power analysis attack. J. Commun. **33**(S1), 276–281 (2012)
10. Zhang, Y., Chen, K.Y., Li, X.W., Chen, J.G., Li, Y.: Side channel attack of cipher chips based on difference variability. J. Commun. **36**(3), 104–109 (2015)