Correlation Power Analysis of Lightweight Block Cipher Algorithm LiCi

Xuan Xia*, Bowei Chen and Weidong Zhong

School of Cryptology, Engineering University of PAP, Xi'an Shanxi 710000, China.
*Corresponding Author Email: xx123401234@163.com

Abstract. The lightweight block cipher algorithm LiCi processes the input plaintexts into high 32-bits and low 32-bits respectively in Feistel structure, and the corresponding keys of these two parts are not related. Therefore, keys of the first round can be cracked independently, and the computational complexity can be reduced from $2^{64}$ to $2^{32}$. After studying the key update strategy, this paper proposed that the computational complexity of cracking the second round keys can reduce from $2^{64}$ to $2^{13}$ by using the key obtained in the first round attack. When cracking the sixth round, the complete 128-bit key can be recovered. In this paper, the LiCi encryption algorithm was deployed on FPGA, the power consumption curves were measured with Tektronix MSO5204B oscilloscope which are used to recover the key in the LiCi encryption algorithm. we choose 8 bits keys as attack goal and get the true keys.

1. Introduction

China has established the world's largest 5G network[1]. 5G has not only brought great improvement in the speed, but also greatly improved the large-scale connection of equipment, the reliability of information communication transmission, and the low latency. These good characteristics will become the catalyst of the era of Internet of Things(IoT), and the number of IoT devices will be greatly improved. Massive Internet of Thing data has followed, and the security of sensitive data produced in device communication are in urgent need of protection. The method used to protect sensitive information is encryption algorithm. The encryption algorithm AES[2] and the self-developed password algorithm SM4[3] in China are all commonly used in the protection of sensitive information. However, the computing ability of IoT devices cannot be compared with that of traditional computers. When running AES and SM4, the speed of IoT devices is slow and cannot meet the user’s needs. Moreover, due to the lack of stable power supply, some IoT devices need to reduce their operating power consumption as much as possible. Lightweight encryption algorithm has the advantages of compact structure, fast computing speed and less need of hardware and software resources, so it is suitable for resource-constrained IoT scenarios. Many excellent lightweight algorithms have been proposed, such as Present[4], Midori[5], Gift[6], Skinny[7], Simon[8], Saeb[9], etc.

The LiCi algorithm[10] is a lightweight encryption algorithm proposed by Patil on ICEI (International Conference on Emerging Trends & Innovation in ICT). The algorithm uses a 31-round balanced Feistel-SPN architecture and supports 128-bit keys. Both input and output of the sbox are 4 bits. In terms of algebraic security, LiCi can resist linear attacks and differential attacks and has excellent resistance to Biclique attacks and zero-correlation attacks. In recent years, side channel attack has become more and more destructive. There is no research about whether LiCi can resist the side channel analysis. LiCi encryption algorithms will be more widely used in the Internet of Things era, so the side channel security of LiCi encryption algorithms is worth of further research.
The side channel attack uses the time\cite{11}, energy consumption\cite{12}, electromagnetic radiation\cite{13} and other physical information closely related to the realization of the encryption algorithm to attack the cryptographic device during operation. The power consumption curves of the power consumption analysis is easy to obtain, and it is a non-intrusive attack, which is difficult to be found by the owner. Therefore it has been widely used. In 1999, Paul Kocher proposed a differential attack to perform a side-channel attack on DES to crack the encryption key. In 2004, Eric Brier proposed a more adaptable related power consumption attack. This article uses Correlation Power Analysis to attack the lightweight LiCi block cipher algorithm.

2. Basic Information Overview

2.1. LiCi Encryption Algorithm

LiCi is a symmetric lightweight encryption algorithm based on Feistel structure, it was proposed by Patil et al. in 2017 at ICEI (International Conference on Emerging Trends & Innovation in ICT). The input and output of the encryption algorithm are 64 bits, its key length is 128 bits, and it has 31 rounds Cyclic encryption structure. Its S box is a four bits input, four bits output structure. The LiCi encryption algorithm has good resistance to linear attacks such as differential attacks, Biclique attacks, and zero-correlation attacks.

The LiCi encryption algorithm divides the 64-bit input plaintext PT into two parts, PT\_MSB||PT\_LSB firstly, and each part contains 32 bits. When encrypting the low 32-bits PT\_LSB, the LiCi algorithm sends the high 32-bits PT\_MSB of the input plaintext into 8 S-boxes for replacement and obtains a total of 32-bits output of the S-box, and then this output is combined with the round key Rki1 XOR the low 32-bits input of the plaintext PT\_LSB, the XOR result is cyclically shifted to the left by 3 bits to get the output of this round. Then it will act as the high 32 bits of the next round of encryption; when encrypting the high 32 bits of PT\_MSB, LiCi will send the high 32 bits into the S box to obtain the 32-bits output, the output combined with the round key Rki2 XOR the output obtained by encrypting the lower 32 bits, then the result shifts 7 bits to the right cyclically to obtain the decryption result of the PT\_MSB in this round, which will be used as the lower 32 bits of the next round of encryption. The single-round encryption process of the LiCi algorithm is shown in Figure 1:

![Figure 1: Single encryption round of LiCi](image)

The pseudo code of LiCi’s 31-round cyclic encryption algorithm is as follows:

\[
\begin{align*}
PT &= PT\_MSB \| PT\_LSB \\
\text{For } i &= 0 \text{ to } 30 \\
PT\_MSB (i+1) &= S[PT\_MSB(i)] \\
PT\_LSB (i+1) &= ((PT\_LSB(i) \oplus PT\_MSB(i+1) \oplus Rki1) <<< 3) \\
PT\_MSB(i+1) &= ((PT\_MSB(i+1) \oplus PT\_LSB(i+1) \oplus Rki2) >>> 7)
\end{align*}
\]
Update Round Key ()
CT_MSB(i) = PT_LSB(i+1)
CT_LSB(i) = PT_MSB(i+1)
PT_MSB(i+1) = CT_MSB(i)
PT_LSB(i+1) = CT_LSB(i)
End for
CT = CT_MSB || CT_LSB

The input of the LiCi’s S-box is X=X_3X_2X_1X_0, and the output Y=Y_4Y_3Y_2Y_1. The S-box’s truth value table is shown in Table 1:

Table 1. Truth value table of S-box

| X  | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | A | B | C | D | E | F |
|----|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| S(X) | 3 | F | E | 1 | 0 | A | 5 | 8 | C | 4 | B | 2 | 9 | 7 | 6 | D |

LiCi is inspired by the key update strategy of the PRESENT encryption algorithm and adopts a similar update strategy. For 128 bits key K=K_127K_126K_125...K_2K_1K_0, where RKi1=K_31K_30K_29...K_2K_1K_0, RKi2=K_63K_62K_61...K_34K_33K_32, when the 64-bits key is extracted from the memory, the following strategy is adopted to update the key:

1. K \lll (K rotates 13 bits to the left)
2. \{K_3, K_2, K_1, K_0\} \leftarrow S[K_3, K_2, K_1, K_0]
3. \{K_3, K_2, K_1, K_0\} \leftarrow S[K_3, K_2, K_1, K_0]
4. \{K_3, K_2, K_1, K_0\} \leftarrow S[K_3, K_2, K_1, K_0] \oplus RC^i, RC^i is a cyclic round counter, which is represented by a 5-bits binary number.

2.2. Hamming Weight Model
The power consumption analysis assumes that the power consumption of the encryption device is related to the operation and the data processed by the device. The Hamming weight model simulates the actual power consumption of the encryption device, which is the basis of the power consumption analysis. The Hamming weight model uses the number of "1" in the intermediate value as an indicator of the power consumption of circuit components at a certain period. Assuming that the power consumption W of the cryptographic device at a certain period is related to the number of "1" in the intermediate value:

\[
W = ax + b
\]

In a specific circuit, a and b are constants. For example, when the intermediate value processed by the encryption device is ‘01100000’, the power consumption calculated using the Hamming weight model is 2a+b.

2.3. Correlation Power Analysis
The Correlation Power Analysis was proposed by E.brier in[14]. This attack is based on the known plaintexts, it calculates the correlation coefficients between the power consumption generated by encrypting the same plaintext with different keys and the actual measured power consumption curves of the encryption device. Then we can figure out the encryption keys used by the encryption device. The specific steps are as follows:

1. First, collect the power consumption curves generated by the encryption device when encrypting N groups of plaintexts. The power consumption curve of each plaintext contains Q sampling points to form an N*Q actual power consumption matrix P.
2. Choose an intermediate variable function f(d,k) of an encryption algorithm, which is a function of plaintext and key. That is, the intermediate value is related to the plaintext and key being processed.
in the device. Calculate the corresponding intermediate values of the N groups of plaintexts using different keys, and then the Hamming weight model is used to quantify the power consumption. Assuming that there are E possible keys in the key space, an N*E analog power consumption matrix H can be obtained.

3. The elements of the analog power consumption matrix H and each column of the actual power consumption matrix P are selected column by column to calculate the correlation coefficients, and finally the correlation coefficients matrix Corr of E*Q is obtained. The calculation method of the correlation coefficient is as follows:

$$\rho(H, P) = \frac{E(H \times P) - E(H) \times E(P)}{\sqrt{\text{var}(H) \times \text{var}(P)}} \quad (2)$$

$$H_i$$ denotes the i-th column of matrix H; $$P_j$$ denotes the i-th column of matrix P.

4. Find the maximum correlation coefficient value from the correlation coefficients matrix Corr, and the guess key corresponding to the maximum correlation coefficient value is the key used by the encryption device.

3. Correlation Power Analysis on LiCi

3.1. Experiment Environment of Performing Correlation Power Analysis on LiCi

FPGA is used as an encryption device for LiCi encryption algorithm. The clock frequency of this device is 50Mhz and the calculation speed is very fast, which can meet the application requirements of LiCi. The oscilloscope used to collect the power consumption signal is Tektronix MSO5204B, the bandwidth of this oscilloscope is 2GHz, the maximum sampling rate is 10GSa/s. The DH1719A power supply regulator ensures the stability of the circuit’s input voltage, which is of great help in improving the purity of the power consumption curves.

3.2. Steps of Performing Correlation Power Analysis on LiCi

After studying LiCi’s internal architecture, this article designs following steps to crack the key.

1. Use the Tektronix MSO5400B oscilloscope to collect the power consumption curves when the LiCi encryption algorithm encrypts N groups of plaintexts.

2. Since the key length of the LiCi encryption algorithm is 128 bits and only 64 bits are used in each round, the first attack position selected in this article is the end of the first round of the LiCi encryption algorithm. At this time, the high 32-bit output of the algorithm CT_MSB is ((PT_LSB $$\oplus$$ S[PT_MSB] $$\oplus$$ Rki1) <<< 3), where Rki1 is 32 bits, and different intermediate values corresponding to different Rki1 in the key space can be obtained according to different input plaintext, and then intermediate values were quantified as power consumption. At this time, the power consumption attack on the 32-bit key can be implemented, and the computational complexity of cracking the 64 key can be reduced from $$2^{64}$$ to $$2*2^{32}$$. At the end of the first round of encryption, the low 32-bit output of the algorithm is CT_LSB((S[PT_MSB] $$\oplus$$ CT_MSB $$\oplus$$ Rki2)>>7), and then get different intermediate values corresponding to different Rki2 and different input plaintexts. Intermediate values were quantified as power consumption curves using Hamming weight model. Finally, the Rki2 used in the first round was cracked, and the 64-bit key used in the first round was obtained.

3. The key update strategy of the LiCi encryption algorithm is based on the previous round’s keys. It performs a circular shift to the left by 13 bits, then performs S-box replacement on the lower 8 bits of the new key, and finally, $$K_{63}...K_{59}$$ xor round counter to get next rounds’ key. Therefore, we can derive the high 51 bits round key used in the second round according to the 64-bit key obtained from the first round of Correlation Power Analysis. The key space is reduced by 79.68%. This article selects the end of the second round of encryption as the second attack node, we calculated the high 32-bit and low 32-bit output of the second round corresponding to different input plaintexts and different keys in the key space. And then power consumption can be calculated by using Hamming weight model.
Finally, a Correlation Power Analysis is used to calculate the correlation coefficients, and the 64-bit round key used in the second round of encryption is cracked.

4. The attack moments are selected multiple times such as the end of the third round of encryption, the end of the fourth round of encryption, the end of the fifth round of encryption, and the end of the sixth round of encryption as the attack location. Repeat step 3 to crack the complete 128-bit master key gradually.

4. Experimental Results and Analysis

According to the attack steps in 3.2, we perform Correlation Power Analysis on the result of the first round of encryption firstly. We choose 8 of 128 bits key as attack goal as the result of PC’s poor performance. According to the attack’s result, it can be seen that the correlation coefficient of sharpest point is 0.97137. And this number is in the 68-th lines, it means when the lowest 8-bits of Rki1 is the ‘1011 0010’. The correlation coefficients of all keys and plaintexts show as Fig.2:

![Figure 2. Correlation coefficients of different keys and plaintexts](image)

In the Correlation Power Analysis of the LiCi encryption algorithm, its 128-bit key does enhance the security of the encryption algorithm, but there are no defensive measures for the physical information leakage used by the side channel attack. The attacker can easily crack the key by using relationship between operations of the encryption algorithm and leaked physical information.

5. Summary

Based on the understanding of the structure of the LiCi encryption algorithm, this article selects the end of the first round of encryption as the first attack moment. At the same time, the first round of keys is divided into high 32 bits and low 32 bits according to the encryption structure, which will make the calculation simpler. The computational Complexity is reduced from $2^{64}$ to $2*2^{32}$. Based on the key obtained in the previous round, the analysis’ key space is reduced from $2^{64}$ to $2^{13}$ according to the key update strategy, which greatly reduces the computational difficulty of cracking the LiCi cipher algorithm. It is necessary to strengthen side channel security of LiCi with theory of secret sharing and masked Look Up Table. These methods protect LiCi from side channel attack by break the relationship between keys and power consumption curves.

References

[1] Hu, G. (2021) Self-powered 5G NB-IoT system for remote monitoring applications. Nano Energy, Volume 87.

[2] Lin, S.K., Huang Y.L., et al. (2018) AES-128 Based Secure Low Power Communication for LoRa WAN IoT Environments[J]. IEEE Access. vol. 6, pp. 45325-45334.

[3] Zheng, X. (2019) The Software/Hardware Co-design and Implementation of SM2/3/4 Encryption/Decryption and Digital Signature System[J]. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, vol. 39, pp. 2055-2066.
[4] Bogdanov, A, Knudsen, L.R., Leander, G., et al. (2007) PRESENT: an ultra-lightweight block cipher[C]// International Conference on Cryptographic Hardware and Embedded Systems. Berlin: Springer, pp. 450-466.

[5] Banik, S., Bogdanov, A., Isobe, T., et al. (2015) Midori: A Block Cipher for Low Energy[C]// International Conference on the ASIACRYPT: Theory and Application of Cryptology and Information Security. Berlin: Springer, pp. 411-436.

[6] Banik, S., Pandey, S.K., Peyrin, T., et al. (2017) GIFT: a small PRESENT[C]// International Conference on Cryptographic Hardware and Embedded Systems. Cham: Springer, pp. 321-345.

[7] Beierle C, Jean J, Kößl S, et al. (2016) The SKINNY family of block ciphers and its low-latency variant MANTIS[C]// The Advances in Cryptology – CRYPTO 2016, Berlin: Springer pp. 123-153.

[8] Beaulieu, R., Treatman-Clark, S., Shors, D., et al. (2015) The SIMON and SPECK lightweight block ciphers [C]// The 52nd ACM/EDAC/IEEE Design Automation Conference. San Francisco: IEEE, pp. 1-6.

[9] Naito, Y., Matsui, M., Sugawara, T., et al. (2018) SAEB: a lightweight blockcipher-based AEAD mode of operation [J]. IACR Trans on Cryptographic Hardware and Embedded Systems, pp. 192-217.

[10] PATIL, J., BANSOD, G., KANT, K.S. (2017) LiCi: A new ultra-lightweight block cipher[C]// International Conference on Emerging Trends & Innovation in ICT. Pune: IEEE, pp. 40-45.

[11] Kocher, P.C., Jaffe, J., Jun, B. (2007) Differential Power Analysis[M]. Springer, US.

[12] AGRAWAL D., ARCHAMBEAULT B., RAO J.R, et al. The EM Side—Channel(s) [C]. //Proc. of CHES 2002. Lecture Notes in Computer Science, vol 2523. Springer, Berlin, Heidelberg.

[13] KOCHER, P.C. (1996) Timing Attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems [C] //Proc of the Advances in Cryptology— CRYPTO’96. Berlin: Springer, pp.104-113.

[14] BRIER, E., CLAVIER, C., OLIVIER, F. (2004) Correlation power analysis with a leakage model[C]//International Workshop on Cryptographic Hardware and Embedded Systems-CHES2004. Heidelberg: Springer, pp. 16-29.