A Countermeasure of Power Attack for Lightweight Cryptographic Algorithm Using Bit Permutation Operation

Lifu Cheng¹, Youyou Zhao², Jinjiang Yang²* and Leibo Liu¹

¹Institute of Microelectronics, Tsinghua University, Beijing 100084, China
²Wuxi Research Institute of Applied Technologies Tsinghua University, Wuxi, 214000, China
*yangjinjiang@tsinghua-wx.org

Abstract. The implantation security of cryptographic algorithm is very important. This paper proposes a method to resist power consumption attack for lightweight cryptographic algorithms. Using bit permutation operation as a countermeasure, we ensure that the position of each data of the original intermediate value data has changed after the bit is permutated, which greatly increases the difficulty of the attack. SKINNY is taken as an example for evaluate the effect of the proposed countermeasure. The experiment results show that the key will not reveal over 100,000 energy traces by using the countermeasure.

1. Introduction
With the current rise of 5G technology, large-throughput and low-latency data transmission is possible, which greatly promotes the development of the Internet of Things. And various IoT terminals have entered hundreds of homes, realizing intelligent family management[1]. IoT security includes application security, system security, firmware security, and underlying algorithm security. As the bottom layer of IoT security, algorithm security is the cornerstone of all levels of security. Therefore, modern cryptographic algorithms have received widespread attention. Compared with traditional encryption algorithms, lightweight passwords have lower resource requirements and have a certain degree of security. This type of encryption algorithm is mostly used in hardware devices [2], so it can be better applied to IoT devices. Typical lightweight cryptographic algorithms include PRESENT[3], SPECK[4], SIMON[4], PRINCE[5], SKINNY[6]. Their structure is similar to traditional block ciphers (such as SKINNY algorithm and AES algorithm), which is the SP network (Substitution Permutation Network) structure. SIMON algorithm structure and DES algorithm structure are similar, they are both Feistel network. The various physical information (such as sound, power consumption, time.) generated by the cryptographic device in the encryption and decryption process can be effectively used by the attacker, and the attacker can crack the key accordingly. This kind of attack is also called a side-channel attack (Side-Channel Attack, SCA). The most commonly used attack in the bypass attack is the power consumption attack. The principle is to analyse the key of the currently running cryptographic algorithm by collecting the energy consumption trajectory and the encryption and decryption data generated by the cryptographic device during the encryption and decryption process [7]. In article [8], the key of SKINNY algorithm was cracked by power attack, and the key of SPECK algorithm was cracked in article [14]. Therefore, similar to traditional cryptographic algorithms, lightweight cryptographic algorithms also need to consider the threat from side-channel attacks. However, lightweight cryptographic algorithms have strict requirements on additional area overhead
due to specific application scenarios. Therefore, additional resource overhead must also be considered while considering the anti-power attack capability of lightweight cryptographic algorithms.

2. Countermeasures Based on Bit Permutation for Lightweight Cryptographic Algorithm

2.1. Introduction to lightweight cryptographic algorithms

In this section, we will introduce two lightweight cryptographic algorithms, SKINNY and SIMON. SKINNY and SIMON are the commonly used structures of two cryptographic algorithms, SP network and Feistel network. These two structures are widely used in symmetric encryption. The lightweight encryption algorithm SKINNY is a new type of block cipher proposed based on CRYPTO 2016 [6]. SKINNY encryption algorithm has 6 forms. According to the difference between the length of the plain ciphertext and the key, there are different round numbers. Simon encryption algorithm is a cluster of lightweight encryption algorithms proposed by NSA in 2013[8]. There are 5 forms of plaintext grouping, and the length of each plaintext grouping corresponds to different key lengths. But no matter how much the plaintext length of SIMON algorithm is taken, its algorithm structure will not change.

2.2. Countermeasures based on Bit Permutation

For hardware-implemented cryptographic algorithm methods, the attacker's focus is often the operation of writing intermediate values into registers. In this operation, the energy consumption of the cryptographic device will change according to the flipping of the register. Therefore, if the data writing process can be confused, the anti-power attack capability of the cryptographic device can be improved to a certain extent. For example, the article [9] introduced a method of resisting power consumption attacks based on register randomization. After the calculation is completed, the data is divided into 4 groups, and then randomly stored in 4 registers, and the intermediate value data is restored to the normal order before the next round of calculation. In article [10], taking the DES algorithm as an example, an anti-power attack method based on dynamic intermediate value storage is introduced. By adding a pair of registers, the calculated intermediate value will be alternately stored in the two pairs of registers during the calculation process, so that the intermediate value of two adjacent calculations is stored in different pairs of registers. In this way, the anti-power attack capability of the cryptographic device is improved, but this method will double the register consumption.

Permutation operation is a frequently used method for cryptographic algorithms. In cryptographic algorithms based on SPN, there is generally a permutation operation. Before modern cryptographic algorithms were produced, permutation methods had been applied to cryptographic algorithms, and the permutation algorithms in classical cryptographic algorithms were mainly permutation operations. In this section, the permutation operation will be used to confuse the energy consumption when writing the intermediate value to the register. As shown in Figure 1, the plaintext is input to the calculation network. When a round of calculation is completed, different paths are entered according to the state. If the calculation is completed, the ciphertext is directly output. If the calculation is not completed, then the intermediate value is stored in the register after Bit Permutation operation. Before the start of the next round of calculation, first perform the Bit Permutation recovery operation to restore the intermediate value to the original order for subsequent correct calculations.

![Figure 1 Bit Permutation](image-url)
2.3. Bit Permutation based on fixed permutation table

The application of this permutation method needs to ensure that the position of each data of the original intermediate value data has changed after the position is permutated, which greatly increases the difficulty of the attack. Based on the consideration of security, take the SKINNY-128-128 algorithm as an example. Its basic unit is bytes. If you want to increase the difficulty of power consumption attacks as much as possible through the position-permutation strategy, the data should be dispersed as much as possible, that is, after the position is permutated, each bit of the data of each arithmetic unit (byte) comes from a different unit of the data (original data) before transformation.

Based on this basic idea, the Bit Permutation strategy shown in Figure 2 and Figure 3 is designed in this section.

![Fig.2 Intermediate value i-th Bit Permutation strategy](image)

![Fig.3 Intermediate value i+1-th Bit Permutation strategy](image)
difference is that the right picture of (a) divides the data by "bytes", while the left picture of (b) divides data by "bits". Then write the 8 bits from top to bottom (from high to low) in the leftmost column in the left picture of (b) into e1 in the right picture of (b). At this time, the 8-bit data of e1 comes from the highest bit of a1, a2, a3, a4, b1, b2, b3, and b4, respectively. The remaining part of the operation is similar, in left picture of (b), extract data by columns from left to right (one byte). In the right picture of (b), write data sequentially from left to right and top to bottom. When the write operation of the first row of 4 bytes is completed, then write data from left to right from the second row, that is, the writing order is as shown in the following formula. The Bit Permutation recovery operation is itself.

3. Experiment Results
Taking the SKINNY-128-128 algorithm as an example, the basic calculation unit is bytes. In the Bit Permutation method based on the Fixed Permutation Table, the attacker's position is fully considered, so that each bit of the data of each unit after the reorganization comes from a different original basic calculation unit, that is, the data of each byte after the reorganization comes from the original 8 bytes of data.

Figure 4 shows the leak point analysis of the known real key (based on the known specific implementation method to bring the specific leak point of the real key analysis), using 50,000 energy traces, it can be seen in the figure that even if it is known, the real key cannot analyse the leak point when the corresponding operation occurred.

![Fig. 4 Analysis of Leak Point of the Fixed Permutation Table Scheme](image)

In this paper, in the implementation of the SKINNY algorithm, considering the difficulty of the attack, try to select the attack point after the nonlinear operation, so in this article, the attack point is selected after the unit replacement, and the attack point is selected after the second round of SubCells, the attack method is CPA. Traverse all possible values of $k$, that is, $k=0,1,...,255$. For each assumed key, the maximum correlation coefficient can be obtained, and the value with the largest absolute value can be selected from it. As is shown in Figure 5, the corresponding assumed key is the largest possible key.

![Fig.5 CPA result of unprotected SKINNY algorithm](image)
For the anti-power attack method based on the fixed permutation table, 100,000 energy traces are also collected for CPA attack verification, and the results are shown in Figure 6. All the traces in the figure have ups and downs, but none of the traces are prominent, and the real key is hidden in all assumed keys, which is similar to the analysis in Chapter 3. At the real leak point (near 1712), the correlation coefficient is still very small and there is no obvious prominent sign, which further confirms the effectiveness of this method.

Fig. 6 CPA result of SKINNY algorithm with fixed permutation table

4. Conclusion
In this paper, we proposed a countermeasure of power attack for lightweight cryptographic algorithms. By using bit permutation method, the results show that, over 100,000 energy traces the CPA attack cannot get the key.

Acknowledgments
This work was supported by the Industry Foreseer Project (Grant No. BE2020016).

References
[1] Liu C, Jing X, Dong G. (2011) On the technical characteristics and wide application of Internet of things. Scientific consultation, 09:86
[2] Banik S, Pandey S K, Peyrin T, et al. (2016). GIFT: A Small Present. Cryptographic Hardware and Embedded Systems. 9813: 321–345
[3] Bogdanov A, Knudsen L R, Leander G, et al. (2007) Present: An Ultra-Lightweight Block Cipher. Cryptographic Hardware and Embedded Systems. 33(4): 462–478
[4] Beaulieu R, Shors D, Smith J, et al. (2015). The SIMON and SPECK lightweight block ciphers. Proceedings of the 52nd Annual Design Automation Conference on - DAC ’15, IEEE, 2015: 1–6
[5] Borghoff J, Canteaut A, Güneysu T, et al.(2012). PRINCE - A Low-Latency Block Cipher for Pervasive Computing Applications. Advances in Cryptology. Berlin, Heidelberg. pp. 208–225
[6] Beierle C, Jean J, Köbl S, et al. (2016) The SKINNY Family of Block Ciphers and Its Low-Latency Variant MANTIS. Advances in Cryptology. Berlin, Heidelberg. pp. 98-105
[7] Stefan Mangard. (2010) Energy Analysis Attack. Science Press, Beijing.
[8] Ge J, Xu Y, Liu R, et al. (2018) Power Attack and Protected Implementation on Lightweight Block Cipher SKINNY. 13th Asia Joint Conference on Information Security (AsiaJCIS). Beijing. pp. 69–74
[9] Chen S. Research on anti power attack for reconfigurable architecture of block cipher algorithm. (2018) Nanjing, Southeast University.
[10] Shan W, Fu X, Xu Z. (2015) A Secure Reconfigurable Crypto IC With Countermeasures Against SPA, DPA, and EMA. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems. 34(7):1201-1205