Research on Anti-power Attack Technology Based on AES Improved Algorithm

Kai Luo, Leibo Liu*

Institute of Microelectronics, Tsinghua University, Beijing, 100084, China

Corresponding Author: liulb@tsinghua.edu.cn

Keywords: AES algorithm; Anti-power; Power analysis; Attack.

Abstract. In the paper, an improved plan is proposed based on AES encryption algorithm. Complex mix-column operation in the AES implementation process is simplified by the improved plan, and an anti-power attack technology is further proposed on the basis of implementing the improved plan. The technology is based on hamming weight model theory of power consumption. Power consumption is balanced through complementary operations on the algorithm level. The operation power consumption is always not related with intermediate data produced by encryption algorithm at any time during hardware implementation, thereby hiding power consumption and data information and achieving the purpose of anti-power attack.

Introduction

People pay more and more attention to the problem of information security with development of information technology. Various cryptographic algorithms have been through continuous research and practice. AES (Advanced Encryption Standard) is widely used all over the world, and has become an international general symmetric encryption algorithm among various cryptographic algorithms. It has advantages of short key establishing time, high sensitivity, low memory requirements, etc., which has been widely applied in the field of information security, such as electronic commerce, communications encryption [1-2], etc. People analyze AES algorithm at different levels, therefore many attack breaking modes to AES algorithm are produced. In various attack modes, power attack refers that the keys inside the crypto chip using the algorithm is mathematically analyzed through analyzing the relationship between the cryptographic algorithm implementation and power consumption, such as simple power analysis (SPA), differential power analysis (DPA), etc., and the key can be finally obtained, thereby greatly threatening the security of crypto chip. Main arithmetic operations can be divided into four steps of 'S box transformation, line transformation, mix-column and XOR with expanded key' during implementation of traditional AES encryption algorithms. Many scholars proposed various different defense strategies about anti-power attack on the basis [3-5].

Implementation plan of existing technology

Existing AES-128 is adopted as an example. Byte is regarded as basic operation unit in the process of implementation. S box transformation, line transformation, mix-column and XOR with expanded key should be regarded as a round function, which is operated for 10 times in a cycled mode, wherein all mathematical operations aim at operation on the G (2^8) domain. People propose many different anti-power attack methods aiming at the AES encryption implementation, and common method includes masking operation on intermediate data. Such method implements certain associative operation with intermediate data produced by encoding operation through using random masking, thereby randomizing intermediate data, and there is no correlation between intermediate data and power consumption; or power consumption balance circuit is used for keeping power consumption constant at the circuit level. Meanwhile, there is no correlation between power consumption and operation data [6].

The encryption process can be free from complex mix-column operation through simplifying four-step operations of round functions in the improved implementation mode of AES encryption.

Only four lookup tables, four-time XOR for each round and each column as well as additional storage space for storing the data are required for the implementation mode. However, anti-power attack methods on existing AES are mainly designed aiming at traditional AES implementation plan, which is lack of anti-power attack strategies with no mix-column and more efficient encryption implementation process [7-8].

Improved AES encryption algorithm

Hamming weight model of power consumption.

Power attack refers that power consumption produced in the encoding operation process is utilized, the difference can be significant due to treatment of different intermediate data, hamming weight model (HWM) is an excellent mode for linking intermediate data and power consumption [9]. It assumes that the power consumption produced in operation is directly proportional to the quantity of '1' at all bits in intermediate data produced by operation, the '1' quantity is regarded as V hamming weight (HW), the computing power consumption is P, the power consumption formula approximate representation is as shown in formula (1), wherein k and d are constants determined by device characteristics [10].

$$P \approx k * HW(V) + d \tag{1}$$

Implementation process of improved AES encryption algorithm.

In the paper, improved AES algorithm implementation plan is proposed on the basis of AES algorithm. Main logic operations of the AES encryption implementation include the follows: byte replacement, shift and XOR operation with 8-bit input and 32-bit output. Hamming weight model of power consumption is combined on the basis of the implementation plan. A method of introducing one complementary operation is proposed at the algorithm level, thereby keeping power consumption in the operation process constant, hiding data information disclosed by power consumption, and realizing anti-power attack. The implementation flow of the improved AES encryption algorithm is shown in figure 1.

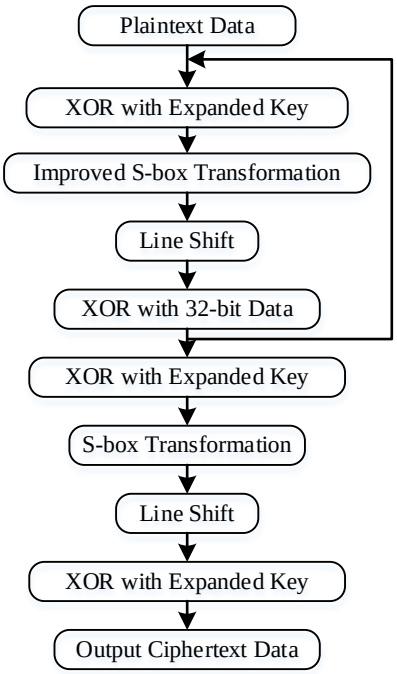

Figure 1 Implementation flowchart of improved AES encryption algorithm

Main required operations include table look-up, shift and XOR operation in the implementation process of the improved AES encryption algorithm. It is simpler and more efficient in logic implementation. In Figure 1 implementation flowchart of improved AES encryption algorithm, four steps of round function are changed into XOR with expanded key, improved S box transformation, line shift, and 32-bit data XOR. Therefore, mix-column is simplified, the encryption efficiency is

greatly improved, and the detailed algorithm implementation process is shown as follows:

a. XOR with expanded key: the step is completely the same as implementation of original AES, mode 2 addition operation is implemented on round function input and expanded key, and it is logically represented as XOR operation.

b. Improved S box transformation: byte replacement is implemented through using one improved S box with 8-bit input and 32-bit output. The 32-byte output is preset on the basis of S box transformation and 8-bit output data in the traditional AES encryption process, for example, 8-bit input is S, 32-bt data is output $\{S', S', 3S', 2S'\}$, wherein, represents the value of traditional AES implementation after byte replacement, and { } represents splicing.

c. Line shift operation: Data of one column for mix-column operation in original AES algorithm is obtained through shifting 32-bit data output by improved S box.

d. 32-bit data XOR: mode 2 addition (XOR) is correspondingly implemented on 32-bit data output by line shift operation, and the output value of one-time round function is finally obtained.

Analysis on improved AES encryption algorithm implementation flowchart shows that three steps of improved S transformation, line shift, 32-bit data XOR are different compared with traditional AES implementation plan. Operation implementation of the three steps is shown in Figure 2.

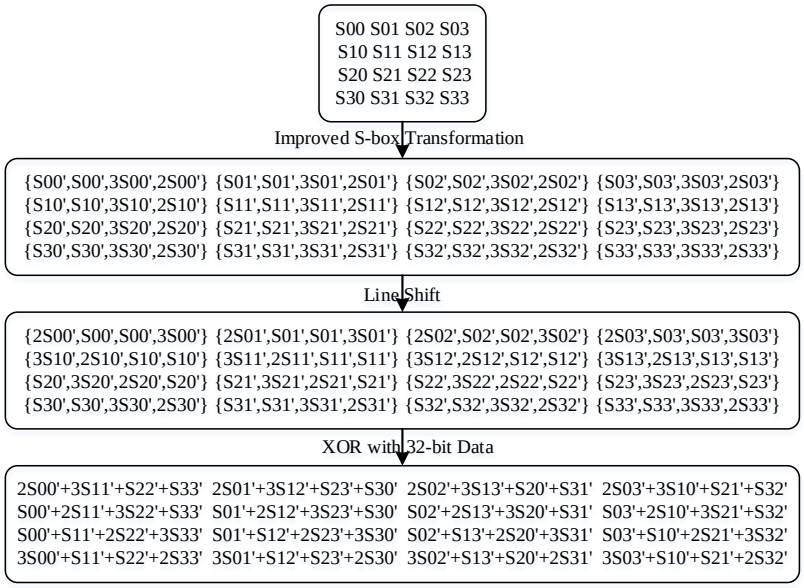

Figure 2 Data variation chart of some operations in improved AES algorithm

Data transformation condition of three operations is described in Figure 2 data variation chart of some operations in the improved AES algorithm. In the chart, each Sxx represents a byte data. The coefficient before the byte data represents the multiplication (multiplied by the coefficient) on G (2^8) finite field. "+" represents addition (logical XOR) operation on the G (2 ^ 8) finite field. {a, b, c, d} are on behalf of 32-bit data spliced by four byte data a, b, c and d.

The main loop part is called round function in traditional AES encryption algorithm process. Round function includes four steps, namely S box transformation, line transformation, mix-column and XOR with expanded key. Wherein, mix-column operation is more complicated, which requires larger resource and operation time. Therefore, improved AES algorithm can save storage space and improve the encryption efficiency of algorithm at the same time.

Research on anti-power attack method based on improved AES encryption algorithm

The hamming weight of intermediate data produced in the operation process is greatly different with different input data in improved AES encryption 32-bit algorithm. Hamming weight model shows that corresponding computing power difference is obvious. The typical power attack method (such as DPA) is realized through capturing power curves produced y different guessing keys, and utilizing the difference producing power in the process of operating different intermediate data.

In the paper, complementary operation is introduced in the encryption operation process aiming at the anti-power attack method based on improved AES encryption algorithm on the basis of realizing improved AES algorithms. Concrete conditions are shown in figure 2.

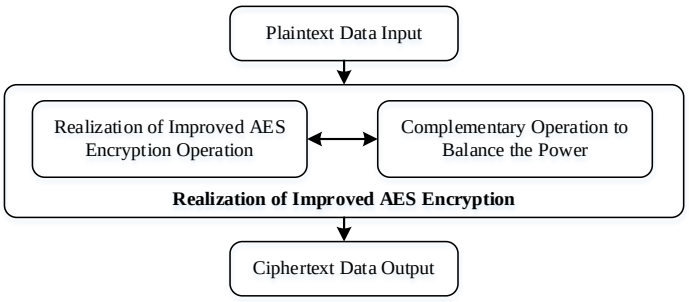

Figure 3 Overall chart of anti-power attack implementation based on improved AES algorithm

It is assumed in the encoding process that an operation can be regarded as function $F(x)$, the produced hamming weight is $HW(F(x))$, and corresponding power consumption is represented as formula (2).

$$P \approx k * HW(F(x)) + d \tag{2}$$

Meanwhile, the complementary operation undergoes $F'(x)$ operation, the produced hamming weight is $HW(F'(x))$, in addition, $F'(x)$ has similar operation mode of $F(x)$, and corresponding power is represented as formula (3).

$$P' \approx k * HW(F'(x)) + d \tag{3}$$

In the process, the whole hardware power consumption is $P_{total} = P + P'$, therefore it should be ensured that the power consumption is a constant value only as shown in figure (4).

$$HW(F(x)) + HW(F'(x)) = C \tag{4}$$

In formula (4), *C* is a constant value, therefore the power consumption sum produced by complementary operation and normal encryption operation is approximately constant, and it is not related to the intermediate value produced in encryption operation. Power consumption and data information in the operation process are hidden, thereby realizing the purpose of anti-power attack.

Specific implementation flow of anti-power attack based on improved AES algorithm is shown in figure 4.

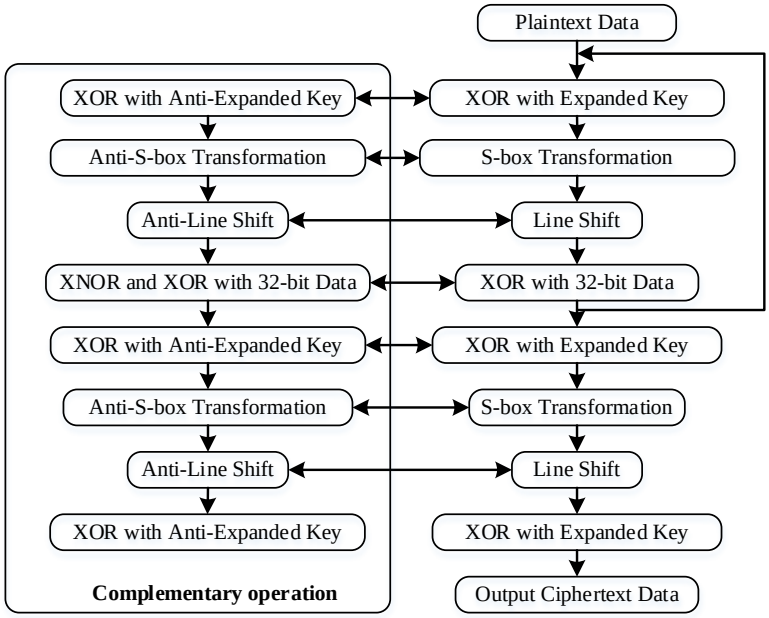

Figure 4 Specific implementation flowchart of anti-power attack based on improved AES algorithm

In the specific implementation flowchart of anti-power attack based on improved AES algorithm, concrete forms of complementary operation in all processes of cryptographic operations are described, and complementary operations of balanced power consumption mainly include the

follows: reverse XOR with expanded key, reverse S box byte replacement, reverse data line ship and XNOR operation. In addition, these complementary operations keep manipulation with original encryption operation synchronously. Four specific complementary operations are available in specific implementation flow of anti-power attack based on improved AES algorithm, and they are shown as follows. Reverse XOR with expanded key, reverse S box byte replacement, reverse data line ship and XNOR operation are respectively called complementary operation I, complementary operation II, complementary operation III and complementary operation IV as follows in order to facilitate description.

Complementary operation I refers to reverse XOR with expanded key. When XOR with expanded key is implemented, complementary operation and reverse XOR operation with expanded key are implemented, output of both aspects is mutually reverse data, the sum of hamming weight extend the key's exclusive or operation, both the output of each data, their hamming weight sum will be a constant, thereby realizing approximately balanced power consumption.

Data x XOR with key is represented as formula (5).

$$F_1(x) = x \oplus k_1 \tag{5}$$

Reverse XOR of data x with key is represented as formula (6).

$$F_1'(x) = x \oplus \overline{k_1} \tag{6}$$

Hamming weight sum of the above operations is a constant, which is represented as formula (7).

$$HW(F_1(x)) + HW(F_1'(x)) = C_1 \tag{7}$$

Complementary operation II refers to reverse S box byte replacement. The improved S box replaces 8-bit input and 32-bit output in the implementation process of improved AES. The process is implemented through a lookup table. Transformation function is as recorded as $F_2(x)$ as shown in formula (8).

$$F_2(x) = \{x', x', 3x', 2x'\} \tag{8}$$

Complementary operation is adopted, and its output is reverse normal encryption output as shown in formula (9).

$$F_2'(x) = \{\overline{x'}, \overline{x'}, 3\overline{x'}, 2\overline{x'}\} \tag{9}$$

In the above formula, x' represents the byte output obtained by S box transformation on traditional byte input. "{}" represents data splicing, thereby constant hamming weight is realized, total power consumption is constant correspondingly, and it is not related with the intermediate value of encrypted data as shown in formula (10).

$$HW(F_2(x)) + HW(F_2'(x)) = C_2 \tag{10}$$

Complementary operation III refers to reverse data line shift. When line shift is implemented, since one normal output and one reverse data output are included in the above operation, additional operation is introduced during data line shift. Namely, the same line shift is implemented on the reverse data, and their power consumption sum is balanced under the mode of hamming weight.

Complementary operation IV refers to XNOR operation. After XNOR operation is introduced in complementary operation IV, normal XOR operation principle shows that 32-bit XOR refers to XOR operation aiming at four data in the improved AES encryption implementation. XOR should be implemented for three times according to order. When XOR is implemented for the first time, XNOR operation is implemented by complementary operation, operation input data is the same as input data of normal encryption operation. Complementary operation also refers to XOR operation during the two last encryption XOR operations, the intermediate data obtained by introduction operation and usable encryption intermediate data are always in the complementary relationship. Similarly, constant hamming weight can be realized, approximate computing power consumption is still constant, which has nothing to do with the intermediate data.

In summary, balanced power consumption can be realized at algorithm level through the above four complementary operations. Therefore, the operational power consumption is always not related with intermediate data produced by encoding operation at different times during hardware implementation. Therefore, power consumption and data information can be hidden, and the purpose of anti-power attack can be achieved.

Conclusion

In the paper, an improved plan is proposed based on AES encryption algorithm. Complex mix-column operation in the AES implementation process is simplified by the improved plan, and an anti-power attack technology is further proposed on the basis of implementing the improved plan. The technology is based on hamming weight model theory of power consumption. Power consumption is balanced through complementary operations on the algorithm level. The operation power consumption is always not related with intermediate data produced by encryption algorithm at any time during hardware implementation, thereby hiding power consumption and data information and achieving the purpose of anti-power attack.

Acknowledgement

This research was financially supported by the project from State Grid Cooperation of China (No.SGRIDGKJ[2013]548).

References

[1] Shiozaki M, Kubota T, Nakai T, et al. Tamper-resistant authentication system with side-channel attack resistant AES and PUF using MDR-ROM[C]// Circuits and Systems (ISCAS), 2015 IEEE International Symposium on. IEEE, 2015.

[2] Fujimoto D, Miura N, Hayashi Y I, et al. A DPA/DEMA/LEMA-resistant AES cryptographic processor with supply-current equalizer and micro EM probe sensor[C]// Design Automation Conference (ASP-DAC), 2015 20th Asia and South Pacific. IEEE, 2015:26-27.

[3] Han M, Wachs M, Lan H. COUNTERMEASURE TO POWER ANALYSIS ATTACKS THROUGH TIME-VARYING IMPEDANCE OF POWER DELIVERY NETWORKS: , US20150195082[P]. 2015.

[4] Jayasinghe D, Ignjatovic A, Ambrose J A, et al. QuadSeal: quadruple algorithmic symmetrizing countermeasure against power based side-channel attacks[C]// Proceedings of the 2015 International Conference on Compilers, Architecture and Synthesis for Embedded Systems. IEEE Press, 2015.

[5] Lu S, Zhang Z, Papaefthymiou M. 1.32GHz high-throughput charge-recovery AES core with resistance to DPA attacks[C]// VLSI Circuits (VLSI Circuits), 2015 Symposium on. IEEE, 2015.

[6] Kamel D, Renauld M, Flandre D, et al. Understanding the limitations and improving the relevance of SPICE simulations in side-channel security evaluations[J]. Journal of Cryptographic Engineering, 2014, 4(3):187-195.

[7] Khatir M, Nazhandali L. Sense Amplifier Pass Transistor Logic for energy efficient and DPA-resistant AES circuit[C]// Quality Electronic Design (ISQED), 2014 15th International Symposium on. IEEE, 2014:517-522.

[8] Wang Y, Ha Y. A Performance and Area Efficient ASIP for Higher-Order DPA-Resistant AES[J]. Emerging & Selected Topics in Circuits & Systems IEEE Journal on, 2014, 4(2):1-13.

[9] Hussain I, Gondal M A. Impact of Error Detecting or Correcting Codes on the Sensitivity to DPA of an AES S-Box[J]. 3d Research, 2014, 5(3):1-7.

[10] Khedkar, Chandrakantrao G. Power Profile Obfuscation using RRAMs to Counter DPA Attacks[J]. Dissertations & Theses - Gradworks, 2014.