Research and Application of Encryption System Based on Quantum Circuit for Mobile Internet Security

Yuehua Li, School of Information Science and Technology, Nantong University, Nantong, China

Chengcheng Wang, School of Information Science and Technology, Nantong University, Nantong, China

Jiahao Sun, School of Information Science and Technology, Nantong University, Nantong, China

Zhijin Guan, School of Information Science and Technology, Nantong University, Nantong, China

Jiaqing Chen, School of Information Science and Technology, Nantong University, Nantong, China

Zelin Wang, School of Information Science and Technology, Nantong University, Nantong, China

ABSTRACT

Information technology is developing rapidly, which not only brings opportunities to the society, but also causes various problems of mobile internet information security. Quantum circuits have many characteristics, such as high-complexity and no feedback. This paper applies quantum circuits to the field of encryption technology. A quantum circuit encryption system is designed based on AES. The system uses quantum circuits to construct the encryption algorithm and realizes the mathematical operations and transformation in quantum logic which can be realized through quantum logic gates. Encryption system of quantum circuits can improve the encryption complexity. Its anti-attack ability is $(2^n - 1)!$ times of the traditional method, thus it can effectively protect the information security of the IoT. In order to increase the practicability of the system, an interface module is also designed to facilitate the interaction of the system with the outside world. Finally, the encryption rate, resource utilization, and encryption effect of the quantum circuit encryption system are tested, which shows the advantages of it.

KEYWORDS

Encryption System, Information Security, IoT, Quantum Circuit

1 INTRODUCTION

With the booming of new information technologies, all kinds of information are expanding rapidly (Xu et al., 2014). However, the protection technology of information security is still in the initial stage of development, so there will inevitably be security problems such as information theft, tampering and disclosure when a large number of sensitive information is processed, transmitted and stored on the network. Therefore, reliable and efficient technology of encryption has become a research hotspot in all walks of life (Natalia & Alexander, 2018). Quantum circuits have the characteristics of high complexity and no feedback. The encryption system based on quantum circuits can improve the encryption efficiency. Its anti-attack ability is $(2^n - 1)!$ times of the traditional method. If the system

DOI: 10.4018/IJCINI.20211001.0a26

This article published as an Open Access article distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/4.0/>) which permits unrestricted use, distribution, and production in any medium, provided the author of the original work and original publication source are properly credited.

is applied to the IoT technology, it can effectively guarantee information security and increase the difficulty of decoding.

Regarding the research on the encryption system of quantum circuits, document (Chen et al., 2018) proposes a construction method of quantum circuits for multiplication in finite field, and constructs encryption algorithm based on the method. However, it only completes the hardware design of the encrypted part and the decrypted part based on quantum circuit. In reference (Liu & Zhu, 2008), a quantum circuit implementation method is proposed for S-box transformation in AES algorithm, and the idea of constructing encryption algorithm based on quantum circuits is proposed. Literature (Liang, 2015) proposes a Quantum fully homomorphic encryption scheme based on universal quantum circuits and does research on the process of quantum information. In reference (Datta & Sengupta, 2013), the authors describe the advantages and feasibility of applying reversible Logic to cryptography and coding theory on the basis of confirmatory study. Document (Zhang et al., 2018) proposes a method of synthesis and optimization for linear nearest neighbour quantum circuits by parallel processing which can reduce the quantum cost for the design of quantum circuits. In reference (Wang et al., 2018), a hybrid particle swarm optimization algorithm based on adaptive learning strategy is proposed to improve the convergence accuracy and speed of quantum circuits. In reference (Wang et al., 2019), an adaptive weight vector guided evolutionary algorithm for preference-based multi-objective optimization is proposed, which can optimize the arrangement of two-dimensional quantum logic circuits and generate the simplest circuits. The existing literatures provide a theoretical idea for the research of encryption system based on quantum circuits. However, the encryption system needs a complete encryption and decryption module in practical application, and the encryption and decryption process needs the key. The complexity and security of the key largely determine the encryption complexity and anti-attack ability of the encryption system, so the complete design of the encryption and decryption module and the key extension part is particularly important; Furthermore, the encryption system must have an interface to interact with users or devices in practical application, so the design of the interface part is also essential.

To solve these problems, the encryption system of quantum circuits designed in this paper consists of four parts: encryption module, decryption module, key extension module and interface module. The construction of encryption module, decryption module and key extension module are all based on quantum circuits. The encryption and decryption modules are composed of four parts: Add Round Keys, Substitute Bytes, Shift Rows and Mix Columns. The key extension module is composed of G function and algorithm design. Meanwhile the interface module is designed by hardware language which can adapt to the characteristics of quantum circuits and work with encryption and decryption modules. Figure 1 illustrates the framework of the encryption system which shows the logical relationship of the four modules. The encryption and decryption modules can encrypt and decrypt information. The key extension module and interface module are used to work with the encryption module and the decryption module to improve the performance of them. The key extension module is connected to the encryption and decryption modules to provide the required keys for them. Similarly, the I/O interface module is connected to the encryption and decryption modules to enable users to exchange information with them conveniently. The design idea of encryption and decryption modules is similar to that of key extension module, so this paper mainly introduces the design of key extension module and I/O interface module.

2 KEY EXTENSION MODULE BASED ON QUANTUM CIRCUITS

2.1 Quantum Gates and Circuits

Quantum gates are basic units of quantum circuits, and they can be expressed by matrix or vector multiplication which means states of quantum bit (Li et al., 2017). Common quantum gates are CNOT gates and SWAP gates. Quantum circuit is a logic circuit with function and is built by a series of

Figure 1. Structural framework of encryption system

quantum gates (Li et al., 2017). Quantum circuit has 2^n ! kinds of substitutions for the input of n-bits, its input number is equal to the output number and it has no heat loss, no fan-in, no fan-out, no feedback (Liang, 2015).

2.2 Key and Key Extension

In cryptography, the key is secret data used to complete cryptographic applications (Du et al., 2015). In the encryption system designed in this paper, the key is used for the encryption and decryption modules to complete the encryption and decryption operations.

Key extension refers to the extension of the initial key with a small number of bits into the key with large number of bits (Du et al., 2015). In the encryption system designed in this paper, the initial key has 128 bits, which needs to be extended to 1408 bits, and the extended keys are called round key. The necessities of key extension are as follows:

- (1) The key extension can eliminate the symmetry and similarity of the generation methods for different keys, and increase the complexity of the key, thus improving the encryption complexity of the encryption system.
- (2) The key extension can expand the differences of the key, therefore, each bit of the initial key can directly or indirectly affect many bits in the process which will make key cracking more difficult.
- (3) The key extension makes the key sufficiently non-linear to prevent the difference of the keys from being determined completely by the initial key, thus the key extended from the initial key can also affect the other extended keys, and it will expand the difference of many steps in the encryption process to enhance the encryption effect.

2.3 Key Extension Algorithms

Key extension is the process of expanding 128-bit initial key to 1408-bit round key. For convenience, we regard 128-bit initial key as a matrix with four rows and four columns, each element of the matrix has 8-bit data. The key extension process is as follows:

- (1) The four elements in a column of matrix is counted as $W[j]$, it has 32 bits, therefore, the initial keys are counted as $W[0]$, $W[1]$, $W[2]$, $W[3]$;
- (2) The extended keys are also expressed in the form of $W[j]$, where j is an integer and the range of it is (Liu & Zhu, 2008).
- (3) If $j\%4=0$, $w[j]=w[j-4]\mathring{\wedge}g(w[j-1])$, otherwise, $w[j]=w[j-4]\mathring{\wedge}w[j-1]$. Where “g()” represents g-function which will be described below and “ $\mathring{\wedge}$ ” denotes XOR.

The contents of g-function are as follows:

- a. Move the corresponding $W[j]$ cycle to the left by 8 bits;
- b. S-box substitution for each byte in the corresponding $W[j]$;
- c. XOR the corresponding $W[j]$ with constants $(Rcon[j/4], 0, 0, 0)$, $Rcon$ is a one-dimensional array, $Rcon[1]=0x01$, $Rcon[i]=Rcon[i-1]*(02)$ ($i>1$, “*(02)” represent multiplication over finite fields).

2.4 Feasibility and Necessity of Designing Key Extension algorithm Based on Quantum Circuits

- (1) The step (b) of g-function in key extension algorithm involves S-box replacement, which maps an 8-bit data to another 8-bit data by searching the S-box table. The traditional way to realize S-box replacement is to store the S-box table in read-only memory, and then compare the input 8-bit data with the memory to find the corresponding 8-bit data. Using quantum circuits to realize S-box replacement does not need the tedious operation of looking up tables. It evolves the logic of S-box table into the conversion relationship between finite field and compound field and the result can be obtained only by conversion between different fields. In the whole process, only addition on the finite field is involved, which can be implemented by using simple CNOT gates. Therefore, realizing S-box replacement based on quantum circuits can not only accelerate the replacement rate and reduce the delay time, but also reduce power consumption and hardware size (Guan et al., 2018).
- (2) The step (c) of g-function in key extension algorithm involves XOR, division and multiplication over finite fields. Traditional methods to implement division operation of hardware is to expand the digits of the dividend, and then continuously compare the high digits of the dividend with the divisor to determine the value of quotient until the end of the calculation. The whole process involves many operations such as comparison, subtraction and shift. If we implement division operations with quantum circuits, it generally involves only shift operation which can be implemented by SWAP gates in quantum circuits. In addition, XOR is equivalent to addition over finite fields. Document (Chen et al., 2018) designs a method for quantum circuits to implement operations over finite fields and draws a conclusion that the operation rate is higher. Therefore, the implementation of this step based on quantum circuits can simplify the process, make the operation faster and reduce the delay (Nayak & Sen, 2012).
- (3) The key extension algorithm contains many operations. The operations of dividing, XOR and g-function in formulas have been introduced in the preceding article, For the step of controlling the XOR of two data according to the value of “ $j\%4$ ”, the traditional methods will design the data selector, while the quantum circuits realize it by using the TOFFOLI gates which have double control bits. So quantum circuits can realize critical path with high working frequency and reduce the occupancy of resources in hardware.

2.5 Advantages of Designing Key Extension Algorithm Based on Quantum Circuits

Designing Key Extension Algorithm based on quantum circuits does not change the algorithm itself and the complexity. What changes is the implementation method of the algorithm. Therefore, the characteristics of quantum circuits will be applied to the algorithm, add the following three advantages for the key extension:

- (1) Quantum circuit's input number is equal to output number, it has no fan-in, no fan-out, no heat loss (Datta & Sengupta, 2013). Therefore, using quantum circuits to implement key extension

algorithm can greatly reduce energy consumption in the process of key extension, reduce the occupancy rate of hardware resources, and improve the rate at which the key expands.

- (2) There are 2^n ! kinds of reversible networks for input and output vectors of quantum circuits, and there are 2^n ! kinds of permutations for input of n-bit data (Datta & Sengupta, 2013). Therefore, the implementation of key extension algorithm with quantum circuits can increase the complexity of the key extension process by $(2^n - 1)!$ times and it is difficult to get all the secret keys from the partially extended keys. As a result, it greatly increases the security of key extension.
- (3) In the encryption system, the key extension module is connected to the encryption and decryption modules to work with them. The encryption and decryption module are constructed by quantum circuits, so implementing the key extension algorithm based on quantum circuits can make the key extension module combine with the encryption and decryption modules more closely, and improve the ability of the whole cooperative work.

2.6 Implementation of Key Extension Algorithm Based on Quantum Circuits

The implementation of the key extension module is shown in **Figure 2** and it is mainly divided into two steps. Firstly, we complete the design of g-function, and then complete the implementation of key extension according to the formula.

2.6.1 Realization of g-Function

1. Left Shift of Circulation

Left shift of circulation is to move the $W[j]$ to the left for 8 bits. Since the operation of left shift is only a change of bit's position, the quantum circuit can be constructed by using the quantum SWAP gate, when converting it to hardware circuit we can change the output sequence of circuit layout.

2. S-box Replacement

S-box replacement is to replace the four bytes in $W[j]$ with another four bytes. In the implementation, the data $W[j]$ in the finite domain $GF(2^8)$ is transformed into its composite domain $GF((2^4)^2)$, after inversion in the composite domain, the data is transformed back into the finite domain (Guan et al., 2018), finally the reversible affine transformation is carried out and S-box replacement is finished.

3. XOR of Rcon

XOR of Rcon is an operation that realizes XOR of $W[j]$ and 32-bit constant (Rcon $[j/4]$, 0, 0, 0). Since the (Rcon $[j/4]$, 0, 0, 0) is all zero except Rcon, the first step is to construct the circuit to generate the values of Rcon. In addition, using different values in Rcon array for XOR depends on the value of " $j/4$ ", so it is necessary to construct the circuit to generate the value of " $j/4$ ".

(1) Circuit Construction of Generating Rcon Values

Rcon is a one-dimensional array, $Rcon[1]=0x01$, $Rcon[i]=Rcon[i-1]*(02)$ ($i>1$, " $*(02)$ " is the multiplication over finite fields). Since 128-bit seed keys are expressed as $W[0]$ to $W[3]$, the extended secret keys are expressed as $W[4]$ to $W[43]$, therefore the range of " j " in $W[j]$ is (Liu & Zhu, 2008), and the range of " $j/4$ " is (Li et al., 2017; Xu et al., 2014), Rcon array only needs to calculate the values

Figure 2 Implementation flow of key extension algorithm

of Rcon (Xu et al., 2014) to Rcon (Li et al., 2017). The quantum circuits of generating Rcon value are shown in Figure 3. It is necessary to prepare quantum bits with initial state of $|00000001\rangle$ to initialize the value of Rcon (Xu et al., 2014), then we use SWAP gate and CNOT gate to realize multiplication of 2 over finite fields, the circuit of multiplication is encapsulated as U device (Chen et al., 2018), and after Cascading 9 U devices with 8 CNOT gates (Li, Wang, & Li, 2019), the construction of quantum circuit is finished. When converting it into hardware circuit, we represent quantum auxiliary bit $|1\rangle$ with high levels, and quantum auxiliary bits $|0\rangle$ with low levels, then cascade them with nine U devices to build hardware circuit. The hardware circuit in Quartus environment is shown in Figure 4.

(2) Circuit Construction of “j/4” Operation

First of all, we turn mathematical problems into physical problems according to literature (Li et al., 2018), “j/4” means that j is divided by 4 to take an integer.

The operation of dividing 8-bits data by 4 can be obtained by shifting the data to the right by two bits, Suppose that the value of “j” is $b_7b_6b_5b_4b_3b_2b_1b_0$, then the two digits (b_1b_0) removed from the low bits are the remainder, and the value $(00b_7b_6b_5b_4b_3b_2)$ is the integral value divided by four. When constructing the operation of “j/4” based on quantum circuits, we use auxiliary bits $|0\rangle$ to supplement the two high bits (Chen et al., 2018), the right-shift operation can be implemented by SWAP gates. When converting quantum circuits into hardware circuits, we represent quantum bit

Figure 3. Quantum circuit of value generation of the Rcon array

$|1\rangle$ with high level, and quantum bit $|0\rangle$ with low level, the shift operation requires changing position during layout. Quantum circuit of dividing four operation designed in this paper is shown in Figure 5.

4. ENCAPSULATION OF G-FUNCTION CIRCUIT

The construction of key extension based on quantum circuits is complex. In order to introduce the construction of subsequent quantum circuits, we simplify the circuits of g-Function logically, encapsulate the g-Function circuits in steps 1, 2 and 3 as G devices, as shown in Figure 6.

2.6.2 Algorithm Design of Key Extension

Since the whole quantum circuits of key extension is complex and every four lines is a construction cycle, we only show the partial quantum circuits of the key extension in Figure 7. In the figure, the left side is the input, the right side is the output, “ $|0000\dots\rangle$ ” represents $|0\rangle$ auxiliary bits of 32 bits.

When implementing the algorithm, we use the differential evolution algorithm based on dynamic fitness landscape (Li, Liang, Yang et al, 2019) to optimize the logical order of quantum gates. XOR can be implemented by CNOT gates. The g-function has been realized before which is represented by a G device. After cascading 80 CNOT gates and 10 G devices according to the rules, we finish the overall design of key extension based on quantum circuits. When converting it to hardware circuit, we can use logical gate XOR to implement CNOT gate.

The partial hardware circuit in the Quartus environment is shown in Figure 8, the left side is the input, the right side is the output, and the “0000...” means 0 bit which length is 32-bit.

Figure 4. Hardware circuit of value generation of the Rcon array

3 I/O INTERFACE MODULE

Figure 5. Quantum circuit graph of the operation of dividing 4

In order to make it easier for users to use the encryption and decryption modules, we study the characteristics of the

encryption and decryption modules and design the I/O interface module to match them. The I/O interface module has multiple types of interface, such as UART, SPI, and the different interfaces can

Figure 6. G device

Figure 7. Quantum circuit diagram of key extension module

meet different needs of users. The following takes the SPI interface as an example to describe how the interface module is designed.

3.1 The Necessity of Designing I/O Interface Module

In order to complete the encryption and decryption of information, the user must interact with the encryption and decryption modules. Because the interface is the bridge between the device and the external communication, it is necessary to design the corresponding interface for the user to complete the sending and receiving of information (Bossuet et al., 2016), and realize the encryption and decryption of information.

3.2 SPI Interface

SPI is a high-speed, full-duplex, synchronous communication bus (Wei et al., 2018) with four IO pins: SCLK, MOSI, MISO, CS. When the SPI data is transmitted, the host selects the slave to communicate according to “CS”, and then sends data according to the clock “SCLK” via the “MOSI” line, the slave reads the data through the line. After that, the slave sends data from the MISO line, and the host reads

Figure 8. Hardware circuit diagram of key extension module

data from the same line (Wei et al., 2018). This process loops until the data transfer is complete. In addition, the SPI interface needs to set the phase and polarity, the polarity (CPOL) sets the level of the idle clock, and the phase (CPHA) sets the clock edge for transmission of data. The phase and polarity of the master and slave must be the same.

3.3 The Design of SPI Interface

The encryption and decryption modules perform operations on the data sent by the user, so the encryption and decryption modules are slave devices, and the interface designed in this paper is an interface of the slave devices.

Since the encryption and decryption modules perform operations on every 128 bits of data, a cache is needed to temporarily store data received and to transmit the data from the device. We set the phase and polarity to zero. In addition, when the operations of encryption and decryption are finished, the processed information needs to be output, so the interface module is divided into an input interface module and an output interface module. This paper uses the Verilog language to implement the design of the SPI interface.

3.3.1 Input Interface Module

The users or devices can input data into the encryption or decryption modules through the input interface module. Figure 9 is a logical representation of the SPI input interface in the Quartus environment. In the Figure, “SPI_in_8” implements the function of receiving one byte of data and it stores the 8-bit data received each time into the buffer “Buffer_128”.

When the buffer is full of 128-bit data, the 128-bit data is output to the corresponding encryption module or decryption module (Xie, 2011). The main implementation steps are as follows:

(1) Capture the Trigger Edge

Each step of the SPI must be performed after the trigger edge of the clock is generated and this paper sets the rising edge as the trigger edge. “sck_r1” is used to record the high or low of the previous clock, and “sck_r0” is used to record the high or low of the next clock. If “sck_r1” is low and “sck_r0” is high, the rising edge is captured.

(2) Receive and Store 8-bit Data

Figure 9. Logic diagram of input interface module

The first step is to determine whether the user wants to send data for encryption and decryption. This step can be achieved by determining whether the selection signal is low level. If the selection signal is low, the value obtained by the pin “MOSI” will be stored in the register under the clock. When the rising edge is captured and the select signal is 0, the data will be received. Meanwhile, the number of the received data is recorded and when the number is full of 8 bits, the value of corresponding flag is set to 1 and it indicates the completion of data transmission in one byte.

(3) Setting 128-bit Buffer

The data of the register in step 2 will be input into the buffer, and when the buffer is stored in 128-bit data, the data will be output to the encryption module or the decryption module. In implementation, we can define memory data which is 16 bits long and 8 bits wide to store 8-bit data received at a time. In addition, a switch is needed to determine whether the data in buffer enter the encryption module or decryption module.

(4) Data Filling

When the number of bits needed to be encrypted is not a multiple of 128, it is necessary to fill in the data to meet the requirements of data size in buffer. We record the number of bytes entering the buffer. If the number is less than 16, all the bytes in the vacancy are set at 0-bit. When the data is restored, the original data can be obtained only by clearing all the parts that is set to 0-bit.

3.3.2 Output Interface Module

The data processed by encryption or decryption module is output by output interface module. The output interface module and the input interface module are inverse processes and their implementation methods are similar, therefore, this article does not make a superfluous introduction for it.

4 PERFORMANCE ADVANTAGE AND TEST OF QUANTUM CIRCUIT ENCRYPTION SYSTEM

4.1 Performance Advantage

(1) Hard to crack

Quantum circuits have 2^n ! reversible networks of input and output vectors and 2^n ! Permutations for n-bit input. The design of encryption system based on quantum circuits can improve the complexity

of encryption and make the anti-attack ability of information $(2^n - 1)!$ times of the traditional method, which greatly increases the difficulty of decoding.

(2) High Encryption Rate

Designing encryption system based on quantum circuit can realize the transformation of operation in quantum logic and realize the complex process with simple logic. Therefore, the power consumption and delay are reduced to improve the encryption rate of the encryption system.

(3) Low Resource Utilization

Quantum circuits transform the nonlinear transformation in encryption algorithm into linear transformation and use fewer logic gates to realize the corresponding operation, which makes the combination degree of each operation and each module higher and reduces the occupation rate of software and hardware resources.

(4) Can Be Optimized

At present, there are many optimization methods for neighbor quantum circuits, which can reduce the quantum circuit size and quantum cost and make the encryption system better.

(5) Interface Diversification

Quantum circuit encryption system can design different interfaces according to different requirements to realize information interaction.

4.2 Performance Test

(1) Test of Encryption Rate

In order to test the advantages of quantum circuit encryption system in encryption rate, this paper tests the average encryption time of quantum circuit encryption system and common AES encryption system under different file sizes. Table 1 shows the comparison results of average encryption time, in which “quantum”_AES “represents the quantum circuit encryption system designed in this paper, “common _ AES” represents the AES encryption system implemented by hardware description language. The second column shows a total of 19 files of different sizes from top to bottom, and the third column and the fourth columns are the average encryption time of the same file encryption for 30 times. It can be seen from the table that under the same file size, the encryption time of quantum circuit encryption system is basically less than that of common AES encryption system, and the larger the file, the more time advantage. Therefore, the encryption rate of quantum circuit encryption system is relatively high.

(2) Test of Resource Utilization

In order to test the resource utilization of quantum circuit encryption system, this paper tests the resource utilization of quantum circuit encryption system and common AES encryption system in QUARTUS environment.

Table 1. Comparison of average encryption time

NO	File size(kb)	Average encryption time /ms	
		Quantum_AES	Common_AES
0	10240	22301	18846
1	15360	32109	44356
2	20480	44551	45583
3	25600	54704	69349
4	30720	67219	62894
5	35840	76857	86437
6	40960	88301	97708
7	46080	98829	107341
8	51200	109501	112921
9	56320	119744	145227
10	61440	123090	156678
11	66560	139470	151500
12	71680	140898	159538
13	76800	164044	175594
14	81920	170570	185374
15	87040	177596	218662
16	92160	164304	193180
17	97280	195905	249485
18	102400	199199	258412

Figure 10 is the comparison result of resource occupation between them. The left of the figure “quantum_design” means quantum circuit encryption system, and the “aes_128” on the right side represents AES encryption system implemented by hardware description language. As can be seen from the figure, the “total logic elements” on the left is 7590, and the right is 9093, which means that the total number of logic elements in the quantum circuit encryption system is far less than that of the ordinary AES encryption system, only 80% of it. In addition, the resources of “dedicated logic register” and “total memory bits” on the left side are smaller than those on the right side, which shows that the resource utilization rate of quantum circuit encryption system is relatively low.

(3) Test of Encryption Effect

The most important part of the encryption system is the encryption effect. In order to test the encryption practicability of the quantum circuit encryption system, this paper uses the quantum circuit encryption system to encrypt the documents in the PC. Figure 11 shows the encryption result, with the document content before encryption on the left and the document content after encryption on the right. The right side of the figure is unreadable ciphertext, and the content of the decrypted document is exactly the same as the left side of the figure, which proves the practicability and effectiveness of the quantum circuit encryption system.

Figure 10. Comparison of resource occupation

Revision Name	quantum_deign	Revision Name	aes_128
Top-level Entity Name	quantum_aes_128	Top-level Entity Name	aes_128
Family	Cyclone II	Family	Cyclone II
Device	EP2C35F672C6	Device	EP2C35F672C6
Timing Models	Final	Timing Models	Final
Total logic elements	7,590 / 33,216 (23 %)	Total logic elements	9,093 / 33,216 (27 %)
Total combinational functions	7,590 / 33,216 (23 %)	Total combinational functions	9,009 / 33,216 (27 %)
Dedicated logic registers	0 / 33,216 (0 %)	Dedicated logic registers	660 / 33,216 (2 %)
Total registers	0	Total registers	660
Total pins	768 / 475 (162 %)	Total pins	390 / 475 (82 %)
Total virtual pins	0	Total virtual pins	0
Total memory bits	0 / 483,840 (0 %)	Total memory bits	352 / 483,840 (< 1 %)
Embedded Multiplier 9-bit elements	0 / 70 (0 %)	Embedded Multiplier 9-bit elements	0 / 70 (0 %)
Total PLLs	0 / 4 (0 %)	Total PLLs	0 / 4 (0 %)

4.3 Limitations and Disadvantages

The quantum circuit encryption system designed in this paper has many advantages, but at present, the design is not perfect, and there are still several problems and limitations. In the future, we will do further research on the following problems:

- (1) The quantum circuit encryption system designed in this paper is still in the stage of perfection. The number of bits of information processed by one encryption thread is not large enough, so the advantage of high encryption rate has not been fully displayed.
- (2) The implementation of quantum circuits is complex and strict. In this paper, there are inevitably errors in the process of implementation, and there are some deviations from the ideal results.
- (3) This design aims to be applied in mobile Internet to ensure its communication security. In the future, we will realize the independence and intelligence of encryption system. On the one hand, reduce the size and make it chip, on the other hand, increase its practicability to adapt to more application environment.
- (4) In this paper, we only implement the SPI, UART and IIC interface for the encryption system, which is not fast enough. We will increase the design of high-speed and widely used interfaces according to the actual needs, such as network port, USB, etc.

5 SUMMARY

This paper builds encryption algorithm based on quantum circuit and the encryption system of quantum circuits is designed. The encryption system can improve the encryption complexity, and its

Figure 11. Encryption effect of encryption system.

With the booming of new information technologies such as IOT, all kinds of information are expanding rapidly. However, most kinds of emerging technologies are still in the initial stage of development with the immature information protection technology, so there will inevitably be security problems such as Information theft, tampering and disclosure when a large number of sensitive information is	:??G+ G??;C!!^:G?:<;:??獭C:?!?;+G) !G裡0區L:: 味dτ::?:?3I;3!) G馱 ?:??G?+!^: ?!:I^CGvly禪^p;株E;) 簇 幡::<0+I:C!6栢: ?;?璉G)!G獭C:??C?+; Z 3: 栢!^G:??3+!3+G^?G:?) 髻醅6 Z; 簇: C:3!+ G鯀<+?G+?+?G?+!)^ 馱攀:? G ++y?:?+;?) +3?;0;!p味C:G+::G?簪3 Z G!^ p:??p區3: 橄Φ?味排鱗Φ:3??:!^:d ?:??G^6++0 G++?) Z 醴??I音!叭^G?I;C:3? ^)?獭:?? C::??G?厯:!!?株+G:??G?+G!^:) ?噪I:: 株Gy?璉I!+!+ 栢:+捏:?? ? ;
---	--

anti-attack ability is $(2^n - 1)!$ times of the traditional method. It can be applied to the system of information security transmission, which greatly increases the difficulty of information stealing and ensures the information security of the system. In addition, the encryption rate, resource utilization and encryption effect of the quantum circuit encryption system are tested, which shows the advantages of it. In the future, we will consider the chip design of the encryption system and apply it to other hot technologies in urgent need of security.

ACKNOWLEDGMENT

This work was partially supported by National Natural Science Foundation of China (NO. 62072259), Postgraduate Research & Practice Innovation Program of Jiangsu Province (NO. SJCX20_1151).

REFERENCES

- Bossuet, L., Datta, N., Mancillas-Lopez, C., & Nandi, M. (2016). ELmD: A Pipelineable Authenticated Encryption and Its Hardware Implementation. *Int. J. IEEE Transactions on Computers*, 65(11), 3318–3329. doi:10.1109/TC.2016.2529618
- Chen, Guan, & Chen. (2018). Design and Hardware Implementation of Quantum Reversible Logic Encryption Algorithms. *Int. J. Journal of PLA University of Science and Technology (Natural Science Edition)*, 1-3.
- Datta, , KSengupta, , I. (2013). Applications of reversible Logic in cryptography and coding theory. In *International Conference on Vlsi Design and International Conference on Embedded Systems*. IEEE Computer Society.
- Du, Z., Xu, Q., & Zhang, J. (2015). The Design of a Key Extension Algorithm Based on Dynamic Dislocation Counts. In *11th International Conference on Computational Intelligence and Security (CIS)*. IEEE.
- Guan, Chen, & Chen. (2018). *Implementation Method of Quantum Byte Replacement Hardware Module for AES Hardware Encryption System*. CN108322305A.
- Li, K., Chen, Y., Li, W., He, J., & Xue, Y. (2018). Improved gene expression programming to solve the inverse problem for ordinary differential equations. *Swarm and Evolutionary Computation*, 38, 231–239. doi:10.1016/j.swevo.2017.07.005
- Li, K., Liang, Z., Yang, S., Chen, Z., Wang, H., & Lin, Z. (2019). Performance Analyses of Differential Evolution Algorithm Based on Dynamic Fitness Landscape. *International Journal of Cognitive Informatics and Natural Intelligence*, 13(1), 36–61. doi:10.4018/IJCINI.2019010104
- Li, K., Wang, H., & Li, S. (2019). A mobile node localization algorithm based on an overlapping self-adjustment mechanism. *Information Sciences*, 481, 635–649. doi:10.1016/j.ins.2018.12.006
- Li, Z., Chen, S., Song, X., Perkowski, M., Chen, H., & Zhu, W. (2017). Quantum Circuit Synthesis using a New Quantum Logic Gate Library of NCV Quantum Gates. *Int. J. International Journal of Theoretical Physics*, 56(4), 1023–1038. doi:10.1007/s10773-016-3245-y
- Liang, M. (2015). Quantum fully homomorphic encryption scheme based on universal quantum circuit. *Int. J. Quantum Information Processing*, 14(8), 2749–2754. doi:10.1007/s11128-015-1034-9
- Liu, , & Zhu, . (2008). Quantum Circuit Implementation of S-Box Transform in AES. *Int. J. Information Security and Communication Secrecy*, 5(5), 92–94.
- Natalia, M., & Alexander, T. (2018). Internet of Things: Information security challenges and solutions. *Int. J. Cluster Computing*, 22(2), 103–106.
- Nayak, A., & Sen, P. (2012). Invertible Quantum Operations and Perfect Encryption of Quantum States. *Int. J. Quantum Information & Computation*, 7(2), 103–110.
- Wang, F., Li, Y., Zhang, H., Hu, T., & Shen, X. (2019). An adaptive weight vector guided evolutionary algorithm for preference-based multi-objective optimization. *Swarm and Evolutionary Computation*, 49, 220–233. doi:10.1016/j.swevo.2019.06.009
- Wang, F., Zhang, H., Li, K., Lin, Z., Yang, J., & Shen, X.-L. (2018). A Hybrid Particle Swarm Optimization Algorithm Using Adaptive Learning Strategy. *Information Sciences*, 436-437, 162–177. doi:10.1016/j.ins.2018.01.027
- Wei, , Zhang, , & Huang, . (2018). Design of a high-performance and dynamic reconFigureurable SPI IP core with master and slave mode. *Int. J. Dianzi Jishu Yingyong*, 44(3), 15–18.
- Xie, Z. (2011). A Design of PCI Target Interface Based on FPGA. *Int. J. Advanced Materials Research*, 186(3), 342–347. doi:10.4028/www.scientific.net/AMR.186.342
- Xu, L., Jiang, C., & Wang, J. (2014). Information Security in Big Data. *Int. J. Privacy and Data Mining*, 4(2), 1149–1176.
- Zhang, , Guan, , & Zhan, . (2018). A method of synthesis and optimization for linear nearest neighbor quantum circuits by parallel processing. *Int. J. Quantum Information and Computation A*, 18(13), 1095–1114.

Yuehua Li was born in 1977. He received the M.S. degree from Soochow University in 2005. Now he is an associate professor in School of Information Science and Technology, Nantong University, China. His current research interests are embedded system and wireless sensor network.

Chengcheng Wang was born in Suqian, Jiangsu Province, China. He is studying in the school of information science and technology of Nantong University, with a master's degree. The main research direction is information security and embedded system.

Jiahao Sun, male of gender, was born in 1997 in Nantong, Jiangsu, China. He is studying at the School of Information Science and Technology of Nantong University for a master's degree. The main research directions are: IoT applications and embedded systems.

Zelin Wang was born in 1973. He received the MS degree from Soochow University, China in 2005 and PHD degree from Wuhan University, China in 2015. Now he is an associate professor in School of Information Science and Technology, Nantong University. His current research interests are intelligent algorithm and network security.