International Journal of Security and Its Applications
Vol. 10, No. 9 (2016), pp.1-8
http://dx.doi.org/10.14257/ijsia.2016.10.9.01

# High-speed Encryption & Decryption System Based on SM4 Algorithm

Lv Qian[1], Li Li[2] and Cao Yan-yan[3]

[1,2,3]*Binzhou Polytechnic, Binzhou, China*
[1]*ihappylucy@outlook.com,* [2]*lili_thesky@163.com,* [3]*yaya_sd@163.com*

***Abstract***

*Nowadays, the network transmission and video encryption areas have urgently needed high-speed encryption systems for SM4 algorithm. To speed up the SM4 system in small area, three aspects in existing system is analyzed and optimized. Firstly, aiming at the prior encryption must wait long until completing all 32 rounds key expansion, a method is proposed for outputting round key in each key expansion to accelerate encryption response. Secondly, considering most user passwords are unchanged, we adopt additional memory for comparing old and new keys, so that key expansion can be cancelled sometimes. Thirdly, the paper analyses the relationship between key expansion and encryption/decryption algorithm in SM4. Using module reused technology, the designed key expansion module can also encrypt and decrypt, and the designed another two modules can both encrypt and decrypt. Therefore, the system can achieve three tasks' synchronous encryption/decryption, which greatly improves the system's processing speed. This paper presents a hardware design scheme for the high-speed system. At last, the optimized design is realized in FPGA. The experimental results show that the design is feasible, and the SM4 encryption speed can increase fourfold.*

***Keywords****: SM4; High speed; Encryption and decryption*

## 1. Introduction

March 2012, Chinese National Security Agency formally promulgated commercial password SM1, SM2, SM3, SM4 and a series of industry standards. Wherein, SM4 is mainly applied to the wireless local area network [1]. The next decade, mobile communications, wireless LAN, finance, defense, e-commerce, video encryption, and other fields will require nearly 100 million SM4 encryption systems. SM4 algorithm provides excellent security. But because high computational complexity, it takes too long time for running an encryption or decryption. However, the network transmission, video encryption and other occasions all call for faster data transmission speed. To achieve real-time encryption or decryption for high-speed data flow, developing a rapid and low-cost hardware accelerator has become a key problem in recent SM4 system design.

Whole pipeline is adopted in existing high-speed SM4 system [2], which results in 32 times system area increase. So it can't be applied to the embedded systems that need small area and low cost. To reduce the size and redundancy, some SM4 systems [3,4] combine their key expansion module, encryption module and decryption module. But because their key expansion and data encryption / decryption can't synchronize, once encryption must cost total 64 iterations with 32 key expansions and 32 encryptions. In some designs [3] a decryption operation needs even 96 iterations. This reduces the data processing speed seriously, and it's very uncomfortable for the occasions with high-speed requirement.

In traditional SM4 systems, key expansion module, encryption module and decryption module are divided, and the encryption module usually doesn't start until all the 32 round keys are generated. Obviously, this can not meet the high-speed field's requirements.

ISSN: 1738-9976 IJSIA

Meanwhile, the same user's password is fixed most of the time, and the same round key can be continuously used for encrypting / decrypting multiple sets of data. But the traditional design still needs extra key expansion, which will not only reduce the processing speed, but also bring some unnecessary dynamic power. What is more, because one group of processed data is often far more than 128 bits, in most cases there will be continuous encryption or decryption tasks. So that encryption module will run continuously with decryption module long-term idle, and vice versa. All of these have reduced the system's utilization and affected the operation speed seriously.

For the deficiencies of existing designs, this paper presents a structure and its operation method, which can achieve high speed SM4 encryption in limited area.

## 2. SM4 Algorithm

SM4 is a block cipher algorithm. The lengths of the data and keys are both 128 bits, which are divided into four sets of 32-bit data for operations. In order to achieve high security of the cipher, key expansion and encryption/decryption processing must go through 32 rounds nonlinear iteration [1].

In encrypting, plaintext is firstly divided into four groups of 32-bit data named X0, X1, X2 and X3. This four plaintexts and the first round key named rk0 are transformed by F conversion as below.

$$X4=F(X0, X1, X2, X3, rk0) \quad (1)$$

According to the formula (1), the X4 is generated. The F transform is a round of iteration. If the XOR for 32-bit data is indicated by "⊕", and the i bits ring shift left for 32-bit data is represented by "<<<i", thus we have the formula as below.

$$Xi+4=F(Xi, Xi+1, Xi+2, Xi+3, rki)=Xi\oplus L(\tau(Xi+1\oplus X\,i+2\oplus X\,i+3\oplus rk\,i)) \quad (2)$$

Wherein, τ transform is comprised by the four S-box lookup table, and L transform is as the following equation.

$$L(B)=B\oplus(B<<<2)\oplus(B<<<10)\oplus(B<<<18)\oplus(B<<<24) \quad (3)$$

After operating formula (2) for 32 times, the data of the last four rounds is finally output in reverse order, that is the 128-bit cipher text.

The decryption algorithms is similar to the encryption algorithm, except that the using order of round keys is in the opposite

The key expansion algorithm is analogous to encryption algorithm. In fact, the only different is the L transform in encryption algorithm as formula (3) should be changed into the L' transform in key expansion, which is expressed with the formula (4) as below.

$$L'(B)=B\oplus(B<<<13))\oplus(B<<<23) \quad (4)$$

So in this paper, the authors refer once complete conversion in key expansion to F' transform. At first in key expansion, the cipher key named MK is divided into four sets of 32-bit data named MK0, MK1, MK2 and MK3, which should be respectively done XOR with system parameters FK0-FK3. There is the formula as below.

$$(K0, K1, K2, K3)=(MK0\oplus FK0, MK1\oplus FK1, MK2\oplus FK2, MK3\oplus FK3) \quad (5)$$

Secondly, K0, K1, K2, K3 and intrinsic parameters of CK0 are transformed by nonlinear iteration, generating the first round key called rk0. That is the following eqution.

$$rk0=K4=F'(K0, K1, K2, K3, CK0) \quad (6)$$

Therefore we have the iteration equation as below.

$$rki=Ki+4=F'(Ki, Ki+1, Ki+2,Ki+3,CKi)= Ki \oplus L'(\tau(Ki+1 \oplus Ki+2 \oplus Ki+3 \oplus CKi)) \quad (7)$$

And then, according to the formula (7), iteration operations are run 32 times to obtain the required 32 round keys.

## 3. Design Scheme for High-speed SM4 Encryption System

### 3.1. "Single cycle" in a Module and "Pipe Line" Inter Modules to Achieve a Small & High-Speed System

To increase the processing speed, the system is usually designed with 32-level pipeline, which can complete all of the key expansions or encryptions in only one clock cycle. But the attendant is around 32 times area increase [4]. Because this design requires significantly improving the system speed in a limited area resource, so we abandon the pipeline scheme, and still adopt the single cycle structure for key expansion, encryption and decryption module.

Analyzing the most current single-cycle systems, the key expansion part doesn't output 32 round keys to the encryption part until finishing all. This is bound to delay the start of encrypting. Researching SM4 encryption algorithm, i-th round key of encryption is also generated in i-th key expansion. In other words, the round keys which key expansion module just generated can be transported to the encryption module immediately. That is to say, encryption and key expansion can run at the same time by flow computing. Thus, we design inter-module pipeline by outputting round key every round and it will reduce the response time of encrypting by 32 folds.

### 3.2. Memory and Comparator to Save Additional Key Expansion

The study found that the same user's password is not changed in many occasions. In this case, more unnecessary key expansions will not only bring additional dynamic power consumption, but also reduce the processing speed. Thus, the program uses a special storage for cipher key and round keys of both old and new. When receiving a new key, a comparison for old and new is added, thereby extra key expansion is avoided and the system effectiveness is enhanced.

### 3.3. Module Reuse to Run Three Encrypting / Decrypting Tasks Synchronously

By researching SM4 key extension and decryption algorithm, the differences are the L' or L conversion, and their input data. Adding several shift registers internally can implement dual system with L' and L transform [2], and adding some data selectors and distributors can achieve selection of input and output data. Therefore, the designed expansion module can both encrypt and decrypt information. Moreover, the designed control module can select sending data and determine the order of the round key. So the encryption module can also decrypt data, and vice versa. This makes it possible to achieve three tasks working at the same time, and system's operating speed can greatly improve.

## 4. Hardware Design for SM4 System

### 4.1. Design of Top-level Module

According to the design scheme, the top module of this high-speed SM4 system is shown in Figure 1. As shown, the system consists of a control module, a data memory, three operation modules and four selectors/distributors. Among them, the operation

modules include the 'key-expansion/encryption/decryption module', the 'encryption/decryption module' and the 'decryption/encryption module'. And the selectors/distributors include 'key-expansion/encryption selector', 'round-key/result distributor', 'data distributor' and 'results selector'. The control module is responsible for controlling the input and output data, the operation mode of each module and data path of each selector. The key-expansion/encryption/decryption module prefers key expanding mode, and also it can do encryption or decryption. Encryption is the preferred mode of the encryption/decryption module, and also decryption can be done as needed. The first mode of decryption/encryption module is decryption, while the second choice is encryption. Therefore, three groups of data can be encrypted or decrypted in the meanwhile.

When the system works, firstly the data memory output the XOR results of key and system parameters, and the intrinsic parameters to the key-expansion/encryption selector. Meanwhile, the data memory outputs the plain/cipher text waiting for processing and the round key to the data distributor.

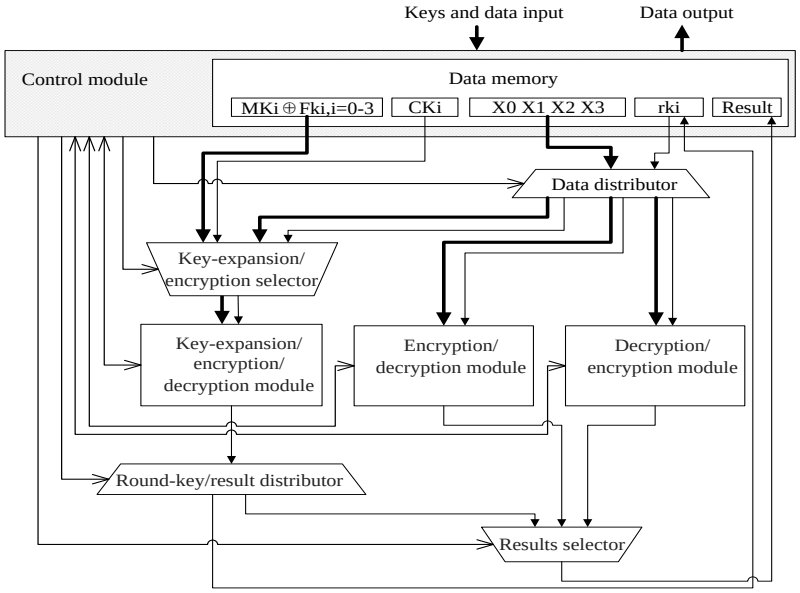



**Figure 1. Top Module Design of High-speed SM4 System**

Secondly, the data distributor transports them to one of the key-expansion/encryption selector, encryption/decryption module and the decryption/encryption module based on the controller's instruction. Next, under control the key-expansion/encryption selector transfers received key expansion data or encryption/decryption data to key-expansion/encryption/decryption module. Thirdly, three operation modules work. Then the key-expansion/encryption/decryption module output its running results to the round-key/result distributor. And then, the round-key/result distributor conveys the data to round key memory or results selector respectively, according to that's round key or encryption/decryption result. At the same time, the encryption/decryption module and the decryption/encryption module also output their operation results to the results selector. At last the results selector selects the data from one of the three operation modules, and puts it into result memory.

### 4.2. Design of Key-expansion/Encryption/Decryption Module

Key-expansion/encryption/decryption module is shown in Figure 2. As is shown, it includes the bidirectional shift register called U0_3 with four groups of 32-bit input, the

32-bit D flip-flop named U4 with hold function, a state machine, the F/F' transform module, and the 32-bit D flip-flop called Y with optional input and tri-state output.

The XOR results of key and system parameters or the plain texts enter into the module U0_3, while intrinsic parameters or round keys go to the module U4. And then U0_3 and U4 operate and output their results to the F/F' transform module. Simultaneously, according to the controller's signal, the state machine selects working mode for F/F' transform module to complete once F or F' transformation. Temporarily, the results of F transformation don't output and remain isolated by the module Y's tri-state gate. But the round keys F' conversion generated will go out through module Y after each key expansion, which can launch a new round of encryption much faster.

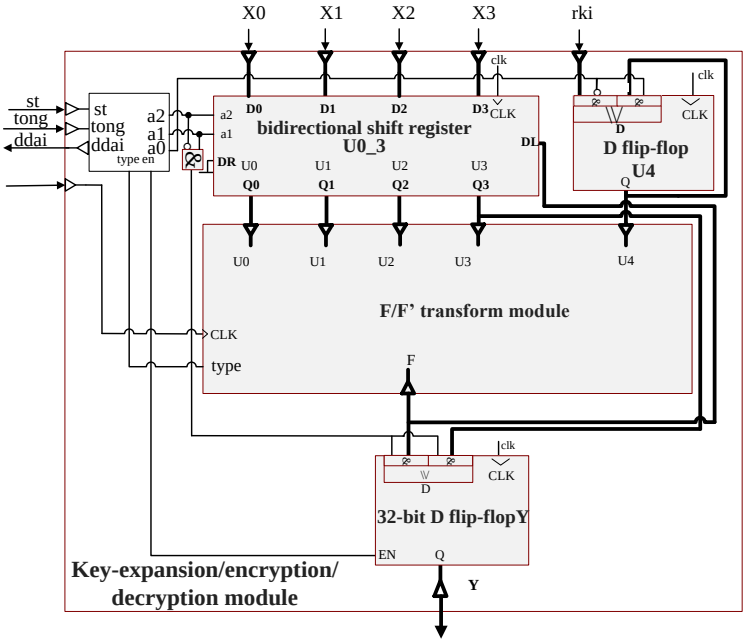



**Figure 2. Design of the Key-expansion/Encryption/Decryption Module**

Moreover, the output of F/F' transform module is also connected to U0_3's left input. Thus using U0_3's left shift and U4's input mode, the next round data can be simply loaded.

Furthermore, U0_3's right output is also link to Y's input. So through U0_3's right shift function, the final four rounds data can export when 32 rounds encryption/decryption completing.

### 4.3. Design of Encryption/Decryption Module and Decryption/Encryption Module

The hardware architecture of encryption/decryption module and decryption/encryption module are similar to the key-expansion/encryption/decryption module, with simply retaining the F conversion part from F/F' transform module.

### 4.4. Memory Design

Memory design is shown in Figure 3. As can be seen from the figure, we set new and old memory for both key and round key, and add a comparator and a selector for new or old round key. When the new key and the old key are the same, the new key expansion is no longer to be done, which accelerates the encryption's start. If the new key and the old key is different, key-expansion/encryption/decryption modules extend the new key, and use the new round key memory to storage it. At this time, the encryption/decryption module and the decryption/encryption module can still access the data from the old round

key memory to encrypt/decrypt. But also they can access new round keys to run after the first round key has been generated. Therefore, this system has achieved encrypting and decrypting information with different keys at the same time.

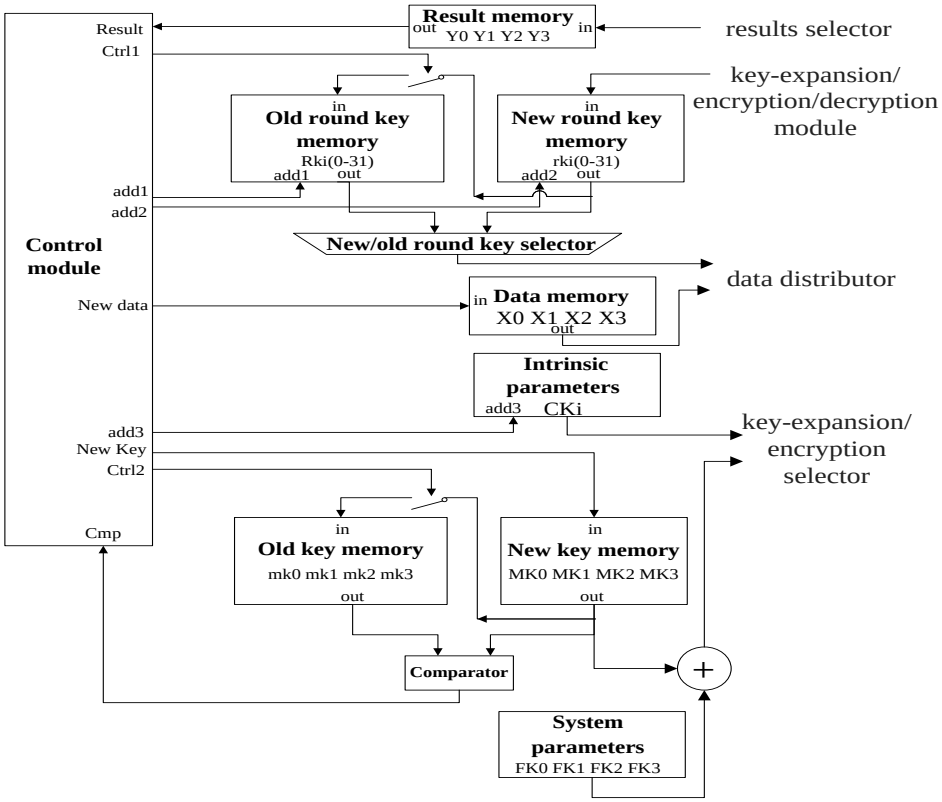



**Figure 3. Memory Design**

### 4.5. Design of Control Module

Control module is designed to number each round key that encryption/decryption needed and identify every key expanding process. Also, we arrange unified allocation mechanism to manage multiple data selectors and distributors, and reasonable choice mechanism to set the work modes and states for the multiple operation modules. Finally, the co-pipeline with all paths and modules is achieved. Meanwhile, the microprocessor interface is built in the controller, to make the data's input and output much faster and enhance the system's universality.

## 5. Hardware Implementation based on FPGA

Based on the hardware design mentioned above, VHDL language is used to design this SM4 encryption system. In Altera's FPGA of Cyclone III EP3C120F780, logic synthesis and optimization for the design are realized based on Quartus II. Furthermore, the traditional discrete system with independent key expansion module, encryption and decryption module is also synthesized on this FPGA. Contrasts of area and speed are shown respectively in Table 1 and Table 2 as below.

**Table 1. Contrast of Area from this Design and Traditional Design**

| Hardware Scheme | Memory Units/bit | Logic Units/bit |
|---|---|---|
| Traditional design | 5218 | 4789 |
| This design | 7064 | 5125 |

**Table 2. Contrast of Processing Speed from this Design and Traditional Design**

| Time Needed in One Encryption Task (ns) | | | Time Needed in Three Encryption Tasks (ns) | | |
|---|---|---|---|---|---|
| Traditional Design | This Design | | Traditional Design | This Design | |
| | Unchanged Key | Changed Key | | Unchanged Key | Twice-changed Key |
| 561 | 289 | 299 | 1129 | 298 | 587 |

Table 1 indicates that, although we added a key storage, a round key storage, and four data selectors, the design's area has increased by only less than one third than traditional designs.

As can be seen from Table 2, comparing with the traditional design, the computing speed of this design can almost double when dealing with individual encryption task of changeless key, and can greatly increase even with the changed key as well. In dealing with three encryption tasks of unchanged key, the operating speed of this design is improved nearly four times. It shows that the ultra high-speed SM4 encryption system in this paper can significantly enhance the running speed in the limited area resources.

## 6. Conclusions

Based on the low cost and single cycle scheme, combining with pipeline idea, this paper puts forward a SM4 hardware, which immediately starts the encryption after key expansion's first round. When key is unchanged, re-key expansion brings about extra power and inefficiency in traditional systems, which are all overcome in our design through the addition of memory and comparison link. Taking full advantages of the common with key expansion and encryption algorithm, according to the module reuse technology, synchronous encryption and decryption for three groups of tasks are achieved finally. The designed hardware is implemented in the FPGA Cyclone III EP3C120F780, whose area is increased by only one-third than conventional designs, and the processing speed is accelerated around four fold in dealing with multi task encryption of changeless key. In a word, it has a vast application prospect.

## Acknowledgements

This work is supported by the University Science and Technology Plan Project of Shandong Province, China. The project's name is Research and Application for Super-speed Encryption & Decryption System of National Cipher SM4 Algorithm, and its number is J15LN67. The work is also funded by Binzhou Polytechnic, China.

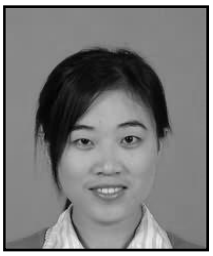
## References

[1] Chinese State Encryption Administration, "No.23 bulletin of Chinese State Encryption Administration", http://www.oscca.gov.cn/News/201204/News_1227.htm, **(2012)** March 21.
[2] C. Feng, B. Hu and H. Liu, "High-speed implementation of cryptographic algorithms SMS4 based on FPGA", Journal of Heibei Academy of Sciences, vol. 27, no. 2, **(2010)**, pp. 8-11.
[3] C. Wang, S. Qiao and Y. Hei, "Low complexity implementation of block cipher SM4", Computer Engineering, vol. 39, **(2013)**, pp. 177-180.

[4] Shenzhen Vision China microelectronics Co. LTD, "A SM4 cryptographic algorithm coprocessor realized in smart card", China Patent CN103746796 A, **(2014)** April 23.
[5] G. Xianwei, L. Erhong, X. Liqin and C. Hanlin, "FPGA Implementation of the SMS4 Block Cipher in the Chinese WAPI Standard", Proceeding of International Conference on Embedded Software and Systems Symposia, Sichuan, China, **(2008)** July 29-31.
[6] Lv Z., Halawani A. and Feng S., "Multimodal hand and foot gesture interaction for handheld devices[J]", ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM), **(2014)**, 11(1s)
[7] J. Hu and Z. Gao, "Distinction immune genes of hepatitis-induced heptatocellular carcinoma[J]", Bioinformatics, vol. 28, no. 24, **(2012)**, pp. 3191-3194.
[8] J. Hu, Z. Gao and W. Pan, "Multiangle Social Network Recommendation Algorithms and Similarity Network Evaluation[J]", Journal of Applied Mathematics, 2013 **(2013)**.
[9] J. Hu and Z. Gao, "Modules identification in gene positive networks of hepatocellular carcinoma using Pearson agglomerative method and Pearson cohesion coupling modularity[J]", Journal of Applied Mathematics, **(2012)**.
[10] Y. Geng, J. Chen, R. Fu, G. Bao and K. Pahlavan, "Enlighten Wearable Physiological Monitoring systems: On-Body RF Characteristics Based Human Motion Classification Using a Support Vector Machine", PP(99), 1-16.
[11] X. Song and Y. Geng, "Distributed Community Detection Optimization Algorithm for Complex Networks", Journal of Networks, vol. 9, no. 10, pp. 2758-2765.
[12] K. Pahlavan, P. Krishnamurthy and Y. Geng, "Localization Challenges for the Emergence of the Smart World", Access, IEEE, vol. 3, no. 1, pp. 1-11.
[13] J. He, Y. Geng, Y. Wan, S. Li and K. Pahlavan, **(2013)**, "A cyber physical test-bed for virtualization of RF access environment for body sensor network", Sensors Journal, IEEE, vol. 13, no. 10, pp. 3826-3836.
[14] Jiang D., Xu Z. and Lv Z., "A multicast delivery approach with minimum energy consumption for wireless multi-hop networks[J]", Telecommunication Systems, **(2015)**, pp. 1-12.

## Authors

**Lv Qian**, she received her Master of Engineering degree in Circuit and System from Shandong university in Jinan, China. She is currently a lecturer in the School of Electrical Engineering at Binzhou Polytechnic. Her research interest is mainly in the area of Circuit and System Design, Signal and Processing, Mechanical and Electrical Integration. She has published six research papers searched by EI index in scholarly journals in the above research areas and has participated in one book.



**Li Li**, she received her master degree from China Agriculture University in Beijing, China. She is currently a lecturer in the College of Electrical Engineering at Binzhou Vocational. Her research interest is mainly in the area of Electrical Automatic Control, Mechanical and Electrical Integration. She has published several research papers in scholarly journals in the above research areas.

**Cao Yan-yan**, she received her M.S. degree in Electronic Circuit and System from Shandong University, in Shandong, China. She is currently a associate professor in the Department of electrical engineering at Binzhou Polytechnic. Her research interest is mainly in the electromechanical engineering. She has published several research papers in scholarly journals in the above research areas.