Journal of Information Hiding and Multimedia Signal Processing ©2014 ISSN 2073-4212
Ubiquitous International Volume **5**, Number **3**, July **2014**

Improvements of SM4 Algorithm and Application in Ethernet Encryption System Based on FPGA

Hai Cheng, Shuxia Zhai, Lianzhong Fang, Qun Ding and Chunguang Huang

Key Laboratory of Electronic Engineering
University of Heilongjiang
74 Xuefu Road, Harbin, Heilongjiang, China
chengh@hlju.edu.cn; dahuangr@163.com; qunding@aliyun.cn

Received July, 2013; revised March, 2014

Abstract. *SM4 is an approved cryptographic 128-bit block cipher which is used in Wireless LAN WAPI. This paper applies the SM4 algorithm in Ethernet encryption system. The SM4 can be programmed in software or built with hardware. However, Field Programmable Gate Array (FPGA) offers a quicker and more customizable solution. This paper presents the SM4 algorithm with regard to FPGA and the Verilog Hardware Description Language (Verilog-HDL). This paper proposes a method to improve the SM4 algorithm to deliver a high data rate in both encryption/decryption operations. Resource consumption about FPGA is minimized by using the shared S-box. This paper proposes an improvement of SM4 algorithm as a security solution for Ethernet encryption system, which is a flexible and configurable PCI Ethernet interface card based on FPGA.*

Keywords: the SM4 Algorithm, Network Interface Card, Ethernet Encryption System

1. **Introduction.** For quite a long time, the world security plays a special role in our day-to-day lives. Vast amounts of personal data are maintained by Banks and credit-card companies. Report of losing account and cipher can be seen in the news. Identity theft is well on its way to become a flourishing industry. Cryptography now plays an important role in modern society, and it can solve the problem that involves secrecy, authentication, integrity, and dishonest people. Cryptography is well-established science.

Modern information theory was first published in 1948 by Claude Elmwood Shannon. There are two basic types of encryption. One is the asymmetric (public key) encryption; the other is symmetric (shared private key). Public key encryption means there are two keys, a public (shared) key, and a mathematical-related private key [1]. Shared private key means the same key is used for both encrypting and decrypting the data. Since the introduction of the data encryption standard (DES) which is a symmetric-key algorithm in the mid-1970s, block ciphers have played an increasing role in cryptology. The growing numbers of practical applications rely on the security. Now block ciphers have received, and still receiving a lot of attention from academic cryptanalysts.

Similar to DES and AES, SM4 algorithm [2] is the first commercial block cipher algorithm which was published by China in 2006 and named SMS4. SM4 algorithm is used in the Chinese National Standard for Wireless LAN WAPI (Wired Authentication and Privacy Infrastructure). And the WAPI became Chinas mandatory national standard. From the security and the communication performance WAPI is a good choice for the communications infrastructure. This paper applies the SM4 algorithm in Ethernet encryption system.

SM4 algorithm is a typical Feistel structure. The input, output and key of SM4 algorithm are 128 bits. And they are spliced into four parts, and each part has 32 bits referred to as word. SM4 algorithm consists of 32 identical rounds. The structure about encryption and decryption is same. The only operations used are XOR, circular shifts and S-box applications. The keys which are used for decryption are the same to which are used for encryption but only in the reverse order.

SM4 algorithm is easy to be realized by not only software but also hardware. And it is used in many areas [3, 4].

A new f8 key stream generator which is using SM4 as the core algorithm can be safely used for in 3G communication system [5]. Hardware/software co-design of SM4 algorithm is realized in embedded processor of MicroBlaze soft core to provide flexibility for designing cryptographic communication equipment [6]. SMS4 algorithm is also designed and implemented on Java Card [7].

The SM4 algorithm is designed to resist several attacks [8, 9] such as differential attack, (algebraic attack to sms4 and the comparison with AES), differential power attack, integral attack, rectangle attack and impossible differential attack. SM4 is resistant against many block cipher attacks such as different cryptanalysis, linear, boomerang, integral, impossible differential, higher order differential, interpolation, slide, XSL and related-key different attacks. This paper proposes improvements of SM4 algorithm by optimizing the sequential logical circuit to improve the efficiency of SM4 algorithm. The main contribution of this paper is to apply SM4 algorithm in network interface card (NIC) [10].

The rest of this paper is organized as follows. Section 2 talks about description and improvement of SM4 algorithm. The encryption transmission system is talked in Section 3. Finally, the paper is concluded in Section 4.

2. Description and Improvement of SM4 Algorithm.

2.1. Several definitions and theorems.

The SM4 algorithm is a block cipher which has a block size of 128 bits and a key size of 128 bits. And each block and encryption key is spliced into four parts; each part has 32 bits. Encryption algorithm and decryption algorithm takes 32 rounds of nonlinear substitutions. Encryption algorithm and decryption algorithm has the same structure, but the round key schedule for decryption is in the reverse order to the round key schedule for encryption. The only operations used are XOR, circular shifts and 8-bit S-box application.

2.1.1. *Terms and basic operations.* The following notations are used in SM4 algorithm:

Word and Byte:

Z_2^e is the set of e-bit vector. So the elements of Z_2^{32} are called 32-bit words, and the elements of Z_2^8 are called 8-bit characters or bytes.

S-box:

The S (substitution) box takes in 8 bits and outputs are 8 bits, which is written as Sbox(.).

Fundamental operations

There are two fundamental operations which are used by this algorithm:

$\oplus$ The bitwise XOR of two 32-bit vectors

$<<< i$ The circular shift of a 32-bit word, with i bits shifted left.

the key and the key vector

The security key for encryption is 128-bit $MK = (MK_0, MK_1, MK_2, MK_3)$, $MK_i(i = 0, 1, 2, 3)$.

The round key schedule, derived from the encryption key, is represented by $(rk_0, rk_1, ..., rk_{31})$, where each $rk_i(i = 0, 1, ..., 31)$ is 32-bit long.

The 128-bit output block consists of four 32-bit words $FK = (FK_0, FK_1, FK_2, FK_3)$. And $CK = (CK_0, CK_1, ..., CK_{31})$ is constant parameter to expand the round key.

2.1.2. *The round function F.* This algorithm uses a non-linear substitution structure, encrypting 32 bits each times which is called a one-round exchange.

Assume that the input plain text is $(X_0, X_1, X_2, X_3\ )$, the output cipher text is $(Y_0, Y_1, Y_2, Y_3\ )$, and the round key is rk_i , i=0, 1, 2, 31. X , Y and rk_i is a block which has a fixed size of 32-bit.

The encryption transformation is shown in (1) and (2).

$$\begin{aligned} X_{i+4} &= F(X_i, X_{i+1}, X_{i+2}, X_{i+3}, rk_i) \\ &= X_i \oplus T(X_{i+1} \oplus X_{i+2} \oplus X_{i+3} \oplus rk_i), i = 0, 1, ..., 31 \end{aligned} \tag{1}$$

$$(Y_0, Y_1, Y_2, Y_3) = (X_{35}, X_{34}, X_{33}, X_{32}) \tag{2}$$

Here T is a substitution that generates 32 bits output from 32 bits input. And this substitution can be reverse. It consists of a non-linear substitution τ which applies 4 S-boxes in parallel and a linear substitution L, i.e.$T(.) = L(\tau(.))$.

Non-linear substitution τ applied 4 S-boxes in parallel. The input word and the output word are 32-bit.

The 32-bit output word of non-linear substitution τ will be the input word of linear substitution L.

One single round of F function is shown in the Figure 1.

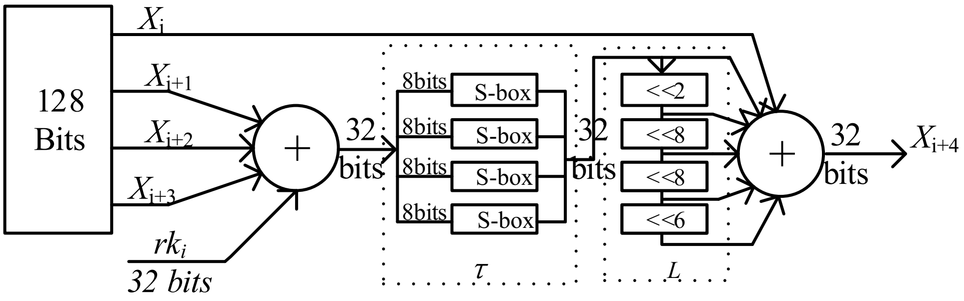


FIGURE 1. A round structure of SM4

2.1.3. *Key expansion when encrypting and decrypting.* The rk_i round key which is used for encryption is derived from the encryption key MK.

Let $MK = (MK_0, MK_1, MK_2, MK_3)$,$MK_i \in Z_2^{32}$,$i = 0, 1, 2, 3$

$K_i \in Z_2^{32}, i = 0, 1, ..., 31;$

$rk_i \in Z_2^{32}, i = 0, 1, ...31;$

First,

$(K_0, K_1, K_2, K_3) = (MK_0 \oplus FK_0, MK_1 \oplus FK_1, MK_2 \oplus FK_2, MK_3 \oplus FK_3)$

Then for $i = 0, 1, 2, ..., 31$:

$rk_i = K_{i+4} = K_i \oplus T^{'}(K_{i+1} \oplus K_{i+2} \oplus K_{i+3} \oplus CK_i)$

Here, $T^{'}$substitution uses the same T structure except the linear substitution. $FK_i, i \in 0, 1, 2, 3$ and $CK_i, i \in 0, 1, ..., 31$ are constant parameter.

2.1.4. *Realization of SM4 algorithm.* Figure 2. is a block diagram of one circle decryption. The left part is the data flow of one round reversal key generation. And the right part is the data flow of one round decryption.

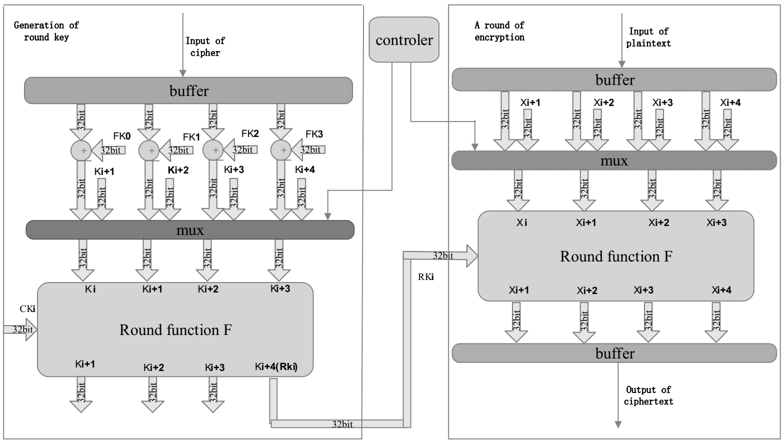


Figure 2. One Circle Encryption and Decryption of SM4

2.2. **Improvement of SM4.** Structure of SM4 algorithm is an unbalanced Feistel structure which is shown in Figure 3. The main feature about Generalized Feistel Structure is that leftmost bits and rightmost bits are not equal compare to Feistel structure.

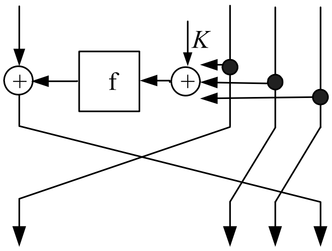


Figure 3. the Feistel Structure of SM4

The encryption and decryption process needs 32 identical rounds to takes up many processor resource. Balance should be made between the resource of FPGA and speed of system. It is important and challenges to optimize the design and implementation of SM4 cryptosystem to meet real-time requirement of applications. Figure 4. shows the normal flow of the SM4 algorithm which is designed based on FPGA.

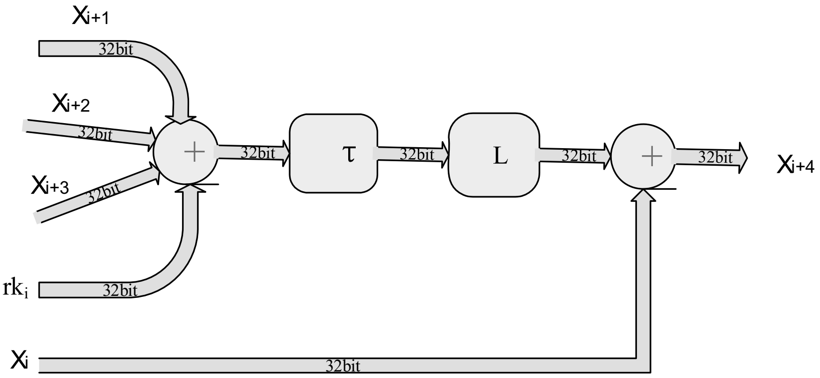


Figure 4. the Generation Flow of X_{i+4}

Because the round key is generated and stored at the first time, the time to generate the round key can be ignored. But the consuming time which the plain text exchanges to the cipher text should be considered seriously. The non-linear transformation $S-box$ is spliced into four 8×8 $S-boxes$ in parallel to the 32-bit input. $S-boxes$ which used in SM4 algorithm are often designed as a large lookup table stored in M4K memory blocks on FPGA. The linear transformation such as XOR and circular shift should be optimized to enhance the speed. If all these combinational circuits are accomplished in a single clock cycle, the delay on critical path can influence the clock cycle of hardware. So it is crucial to optimize the critical path to achieve the high speed.

The flow of X_{i+4} generation can be split into two segments. Optimization for segmentation is chosen in order to balance the consuming time of each part. And pipeline is chosen in order to balance the logic between them as evenly as possible.

As Figure 5. shown, pipeline is used to optimize the flow. The combinational circuit is spliced into two stages. In the stage one, the first XOR circuits ($X_{i+1}, X_{i+2}, X_{i+3}, rk_i$) and non-linear substitution τ are combined; in the second stage, linear substitutions L and the second XOR circuits are combined. In this way pipelines will be able to enhance the performance of SM4 algorithm.

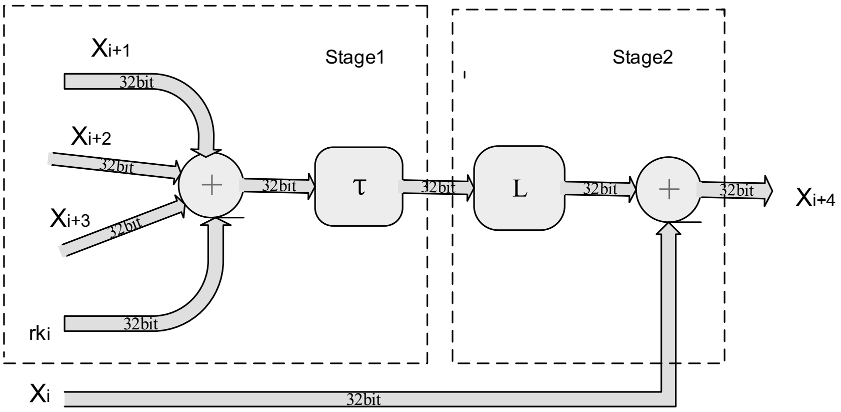


FIGURE 5. the Improvement Generation Flow of X_{i+4}

3. Data encryption transmission system based on SM4.

3.1. Architecture of NIC.

With the increase of the performance of network servers, network interface cards (NIC) [11] will have a significant influence on a systems performance. NIC allows the operating system to send and receive the packets, and the operating system communicates with NIC over the local interconnect; usually a peripheral component interconnects bus (PCI). NIC has a PCI hardware interface to the host server, and the device driver is used to communicate between the operating system and local receive and transmit storage buffers. In addition, NIC has a medium access control (MAC) unit to implement the physical (PHY) layer defined in the network.

The NIC based on FPGA is more programmable and flexible to implement new services in order to modify and improve the functionality. With a programmable network interface card, it is easy to implement additional service such as Data-Cryptography.

So the design aim of this paper is to develop a programmable FPGA-based NIC hardware [12] used SM4 algorithm to encrypt the information about the network. The block diagram of the NIC based on FPGA is shown in Figure 6.

The programmable NIC based on FPGA consists of two platforms: software platform and hardware platform [13].

Software platform includes the application and driver about NIC. Application about NIC is used to communicate between PC and the NIC and send the instruction including

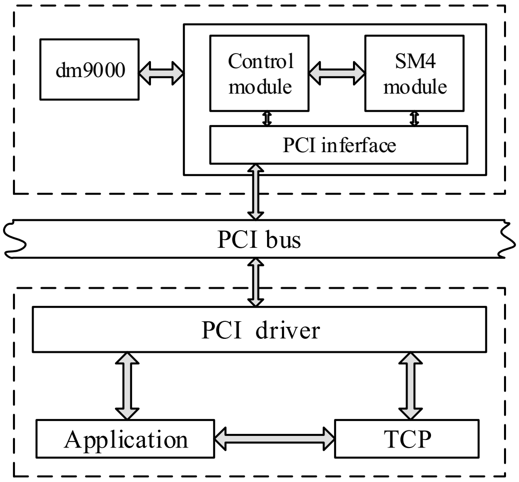


Figure 6. Architecture of SM4 Encryption System

instruction fetching, decoding, execution, memory access, write back to registers, cipher text sending and receiving, encoding and decoding. Driver about NIC is used to communicate between PC and NIC through peripheral component interconnects bus. And the instruction and data can be sent and received through the driver.

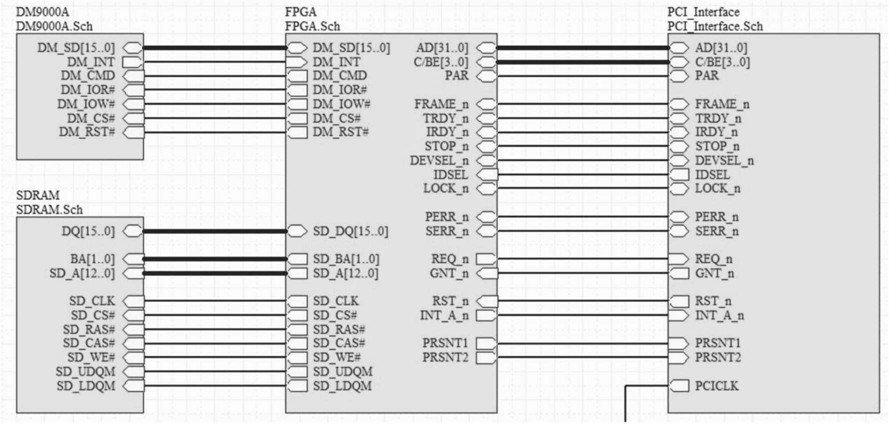


Figure 7. Architecture of Network Interface Card

Hardware platform shown in Figure 7 and Figure 8 based on FPGA includes the PCI interface, and a user interface design is implemented which connects the PCI interface. The Altera Cyclone II device is used for the NIC. The NIC is integrated with a 32M ram which is a large capacity, high- bandwidth memory to store data. PLL is used as frequency multipliers. The PHY chip DM9000A implements the physical layer to receive the data from PHY to MAC and sent data from MAC to PHY. Then the register of the NIC, IP address, MAC address is configured. If data is received, an interrupt is occurred to the host processor. Then the resource of NIC is locked and prevented from being used by other applications. The results show that the network interface card achieves 13 Megabit per second throughput.

3.2. **Application of SM4 algorithm in the NIC.** The input data or the output data of the SM4 algorithm consists of a sequence of 128 bits. And the cipher key for the SM4 algorithm is also a sequence of 128 bits. These sequences are spliced into four contiguous

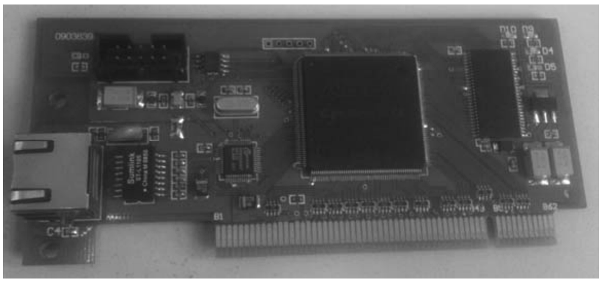
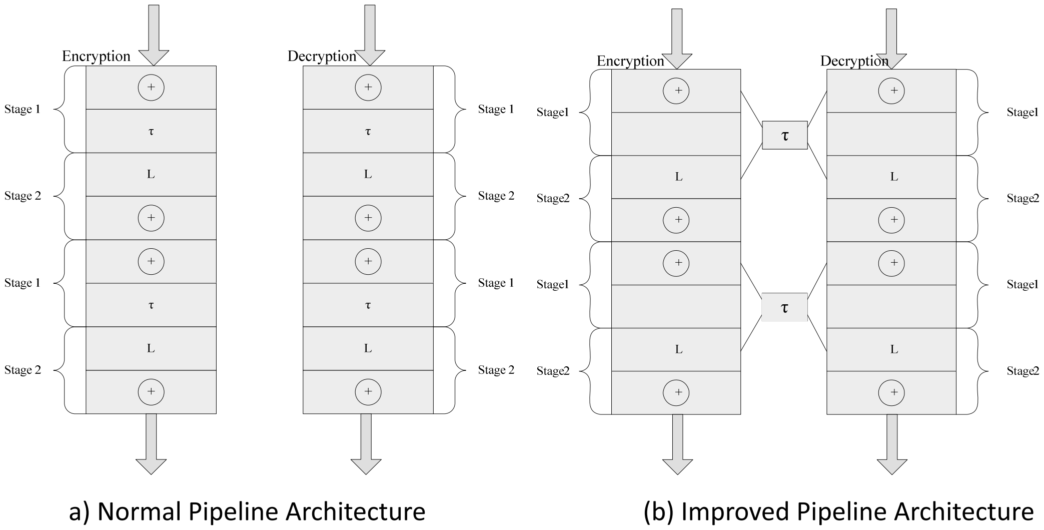


Figure 8. Network Interface Card

bits evenly. The cipher can calculated and stored in the NIC before encryption and decryption.

The data bus width of PCI is 16 and 32 bits adaptive, and the data width of the cipher key is 128 bits. So the cipher key is set by the application on the computer and sent to NIC through the PCI driver for several times. Before communication, the cipher key is stored in NIC RAM for encryption and decryption. Then the key expansion is processed to generate the expand key which is used for encryption and to inverse the expand key which is used for decryption. Both are stored in RAM until the cipher key changed. So the cost time can be neglected.



Encryption
Decryption
Stage 1
Stage 2
τ
L
+
Stage1
Stage2
a) Normal Pipeline Architecture
(b) Improved Pipeline Architecture

Figure 9. Pipeline of SM4 Algorithm

The plaintext of SM4 is 128-bit long. And they are spliced into four parts; each part has 32-bit long.

The SM4 algorithm encryption for a normal pipeline architecture is presented in Figure 9a. This design consists of 32 iterations. And each iteration consists of 2 stages which are mentioned in section 2.2. The encryption process and decryption process can be produced in the same time. But more resources of FPGA is consumed in this structure. In the pipeline structure of SM4 algorithm, the nonlinear substitution τ consumes more FPGA resources used by the design, and it can be shared by both encryption and decryption.

As shown in Figure 9b, the iteration consists of 2 stages; the nonlinear substitution can be used on the ping pong protocol. So the encryption and decryption can work together on the ping pong protocol.

Table 1. Resource consume Comparison among the Different Applications of SM4

structure	logic registers	memory bits	Max Frequency	Throughput
General structure	1496	16384	69.18MHz	1.16Mbps
Normal pipeline structure	21568	540672	86.1MHz	13.1Mbps
Improved pipeline structure	18192	278525	86.0MHz	13Mbps

Table 1 shows the result of the resource of FPGA and the speed of Ethernet encryption system. The table reports three implementations about SM4 algorithm which are described below:

General structure: general structure means that cipher text can be generated after 32 iterations in encryption process and the plain text can be generated after 32 iterations in decryption process. The two processes cant be executed together. The resource of FPGA is less than other structures. The max frequency of system is 69.18MHz, but the throughput is only 1.16Mbps.

Normal pipeline structure: normal pipeline structure is presented in Figure 9a. Both encryption process and decryption process can be executed in the same time. The data can be generated after 1 iteration. The throughput is much higher than general structure.

Improved pipeline structure: Improved pipeline structure is presented in Figure 9b. Both encryption process and decryption process can also be executed in the same time. And the logic registers and memory bits of FPGA is reduced than normal pipeline structure.

The result shows that improved pipeline structure can achieve the max frequency with fewer logic registers than normal pipeline structure.

4. **Conclusions.** In this paper, we have discussed the implementation of the SM4 algorithm in the Ethernet encryption system. The improvement pipeline structure of SM4 algorithm and ping pong protocol which is used to optimize the resource of FPGA is used in network interface card to improve the throughput and reduce the resource consumption of FPGA. The results show that the network interface card achieves 13 Megabit per second throughput. And the text, video and audio can be transmitted by Ethernet encryption system.

Acknowledgment. This work is supported by Scientific Research Fund of Heilongjiang Provincial Education Department (No.12521422) and supported by the Innovation Fund Designated for Graduate Students of Heilongjiang University(No.YJSCX2014-001HLJU).

REFERENCES

[1] T. Y. Wu, T. T. Tsai, and Y. M. Tseng, A revocable id-based signcryption Scheme, *Journal of Information Hiding and Multimedia Signal Processing*, vol. 3, no. 3, pp. 240-251, 2012.

[2] Office of State Commercial Cryptography Administration, P.R.China, Functionality and Interface Specification of Cryptographic Support Platform for Trusted Computing (in Chinese), `http://www.oscca.gov.cn`, 2012..

[3] R. Nishimura, S. I. Abe, N. Fujita , and Y. Suzuki, Reinforcement of VoIP security with multipath routing and secret sharing scheme, *Journal of Information Hiding and Multimedia Signal Processing*, vol. 1, no. 3, pp. 204-219, 2010.

[4] J. Toldinas, V. Stuikys, R. Damasevicius, et al., Energy efficiency comparison with cipher strength of AES and rijndael cryptographic algorithms in mobile devices, *Elektronika Ir Elektrotechnika*, vol. 182, no. 3, pp.11-14, 2011.

[5] Y. S. Wang, W. Chen, F8 keystream generator with SMS4 as core algorithm, *Proc. of 5th International Conference on Information Assurance and Security*, pp. 23-26, 2009.

[6] L. Zhang, and L. Li, Hardware/software co-design of sms4 algorithm based on microblaze, *Proc. of IEEE International Conference on Oxide Material for Electronic Engineering*, pp. 106-109, 2012.

[7] D. W. Zhang, Design and implementation of sms4 on java card, *Proc. of WRI World Congress on Software Engineering*, pp. 145-149, 2009.

[8] B. Z. Su, W. L. Wu, Security of the sms4 block cipher against differential cryptanalysis, *Journal of Computer Science Technology*, vol. 26, no. 1, pp. 130-138, 2011.

[9] T. Kim, J. Kim, Linear and differential cryptanalysis of reduced sms4 block cipher, *International Association for Cryptologic Research*, pp. 281, 2008.

[10] D. Denning, J. Irvine, An implementation of a gigabit ethernet AES encryption engine for application processing in SDR, *Proc. of the IEEE 60th Vehicular Technology Conference*, pp. 1963-1967, 2004.

[11] L. Henzen, W. Fichtner, FPGA parallel-pipelined AES-GCM core for 100G ethernet applications, *Proc. of European Solid-State Device Research Conference*, pp. 202-205, 2010.

[12] L. Zhang, L. Li, X. Gao, and J. Wang, Design and realization of sms4 algorithm based on microblaze, *Proc. of the 10th International Conference on Electronic Measurement & Instruments*, pp. 106-109, 2011.

[13] N. Sklavos, and P. Kitsos, Architectural optimizations & hardware implementations of WLANs encryption standard, *Proc. of the 5th International Conference on New Technologies, Mobility and Security*, pp. 1-5, 2012.