International Journal of Security and Its Applications
Vol.8, No.2 (2014), pp.59-66
http://dx.doi.org/10.14257/ijsia.2014.8.2.06

Parallel Architecture for High-Speed Block Cipher, HIGHT

Je-Hoon Lee[1] and Duk-Gyu Lim[1]

[1]*Div. of Electronics, Information and Communication Eng., Kangwon National University, Samcheok, Gangwon, 245-711, Rep. of Korea*
limdg@kangwon.ac.kr

Abstract

This paper presents the implementation of high-speed block, cipher, HIGHT. The proposed architecture employs parallel architecture to enhance throughput. In addition, it shares key scheduling block for encryption and decryption to reduce hardware complexity. It also introduces an efficient protocol applicable to RFID systems, implementing the HIGHT block cipher algorithm. The new HIGHT structure yields a size small enough to afford tag applications and twice as high performance with respect to conventional HIGHT implementation. The proposed protocol overcomes the security vulnerability of RFID tags, and reduces energy consumption per transaction by sharing key generation.

Keywords: *block cipher, RFID, parallel processing, security*

1. Introduction

Recent information security addresses the ubiquitous mobile network environment. The USN (ubiquitous sensor network) emphasizes availability of network access without limitation of time and location. The portable nature of USN, however, raises critical problems of limited energy sources along with protection of personal data. Some wireless systems comprise the RFID (radio frequency identification) as a major component in USN [1]. However, it suffers from a security risk in the data communication between a RFID reader and a tag.

Block cipher algorithms, AES (advanced encryption standard) and HIGHT (high security and light weight), were evaluated for USN applications [2-5]. They yield a size small enough to be used for RFID tag applications. Because of the ever-increasing communication speed and fluent access environment, the needs for high throughput of block ciphers become a more critical design issue. However, the maximum throughput of AES presented by M. Feldhofer et al is 9.9 Mbps at 80MHz clock frequency, and the maximum throughput of the state-of-the-art HIGHT design is 235Mbps at 125MHz clock frequency [3-4]. This high speed operation brings higher energy consumption into RFID based systems. Thus, it is desirable to devise a new parallel architecture that can enhance its throughput without significant hardware complexity.

This paper presents an efficient implementation of HIGHT. It introduces a new parallel architecture for the HIGHT algorithm aimed at small size, high speed, and low power that will be applicable for RFID systems. The implementation results show that the proposed HIGHT meets the fulfilment of mandatory requirements for a passive RFID tag application that are specified in RFID standards. This paper also introduces an efficient protocol applicable to RFID systems with the HIGHT algorithm.

[1]J. H. Lee and D. G. Lim, "Parallel architecture for high-speed block cipher, HIGHT"

ISSN: 1738-9976 IJSIA

2. The Proposed Architecture of HIGHT Block Cipher

A HIGHT consists of 4 major blocks of key schedule, initial transform, 32 iterative round operations, and the final transform as shown in Figure 1(a). It encrypts a 64 bit plain text into a corresponding 64 bit cipher text with 128-bit master key. It employs an unbalanced Feistel network of 8 branches at each round. It encrypts a 64 bit plain text into a corresponding 64 bit cipher text as shown in Figure 1(a). Key scheduling can be performed in parallel with the round function; and the "on-the-fly" generation scheme is possible.

A key schedule process is responsible for generating the whitening keys and sub-keys for all round blocks using 128 bit master keys. It generates eight whitening keys from WK0 through WK7. WK0 through WK3 and WK4 through WK7 are transferred to the initial and the final transform, respectively. In addition, a key scheduler generates 128 sub-keys from SK0 through SK127 for 32 iterative rounds. It transfers four sub-keys to each round function. The initial and the final transform use whitening keys concealing information used for internal operations. Those whitening keys and round sub-keys are obtained by permuting the input master key and constants generated by a LFSR (linear feedback shift register). The detailed operation is described in [4, 5].

The three steps of encryption stages of HIGHT are as follows: the initial transform, 32 repetitions of the round function, and the final transform. The encryption process of HIGHT commences with the initial transform that processes 64-bit plaintext with four whitening keys. It performs 32 iterative round functions: each of them uses four sub-keys. The output values of a round become the input values of the next round transform. Two linear subround functions F_0 and F_1 process an 8-bits input and yield an 8-bits output defined as described in Eq. (1). The final transform is applied to the output of the last round together with the other four whitening keys. Consequently, the 64-bits cipher text is obtained from the output of the final transform.

$$\begin{aligned} F_0(x) &= (x <<< 1) \oplus (x <<< 2) \oplus (x <<< 7) \\ F_1(x) &= (x <<< 3) \oplus (x <<< 4) \oplus (x <<< 6) \end{aligned} \quad \textbf{(1)}$$

HIGHT algorithm uses simpler primitive operations such as addition, XOR and rotation than other AES-like block cipher algorithms. In the conventional HIGHT that presented by D. Hong, *et al.*, the key scheduler requires 1,648 gates and the round and others require 1,400 gates. Furthermore, Y. Lim presented the compact implementation of the HIGHT algorithm. In this work, the key scheduler is slightly reduced to 1,591 gates, while the size of round and control logics is reduced to 1,017 gates by replacing four bitwise permutation and g-functions to two bitwise rotations and addition operation in all iterative rounds.

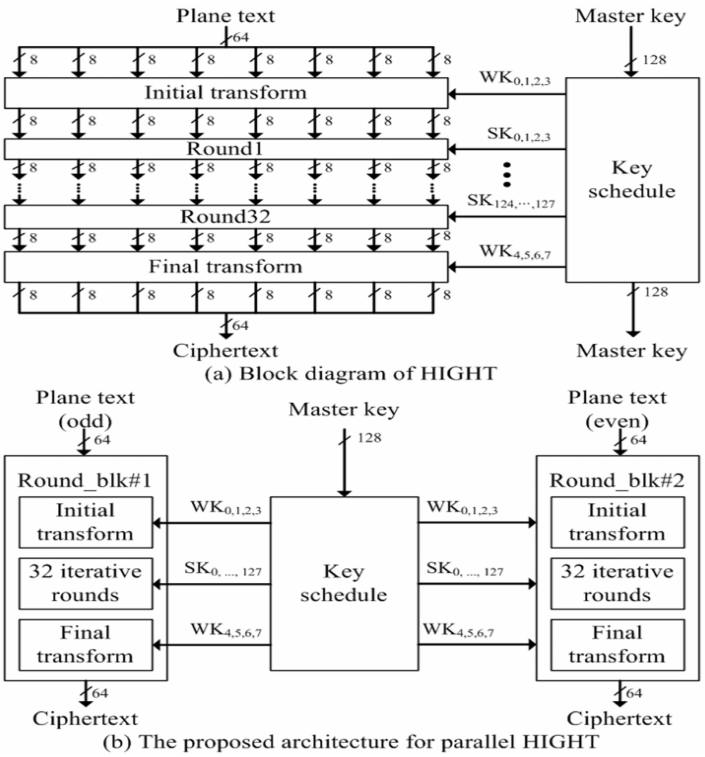

Figure 1. The Architecture for Original HIGHT and the Proposed Parallel HIGHT

In conventional HIGHT, the logic size of key schedule block is larger than that of their round and control blocks. This fact provides an efficient way to accomplish new parallel HIGHT architecture since the RFID standard limits the circuit area under 5,000 gates [1]. Even though the proposed HIGHT employs two round logics and added control logic, it can meet this mandatory requirement. The proposed design employs parallel architecture of the HIGHT algorithm carrying two round logics in order to perform the round function in parallel. Two round block streams of the parallel architecture can share the common key scheduling blocks to reduce the power consumption.

The proposed parallel architecture of HIGHT comprises FSM, key schedule, and two round blocks as shown in Figure 1(b). A key schedule and each round block work in exactly the same way as the conventional HIGHT algorithm. An original HIGHT encrypts a 64 bits plain text into a corresponding 64 bits cipher text using 128 bits master keys. While the input plain text changes, the value of master keys remains the same. Two consecutive 64 bits plain texts can be encrypt separately because they do not have any data dependency. The proposed HIGHT encrypts two plain texts into two 64 bits cipher texts concurrently. Consequently, it processes 128 bits plain text, not 64 bits one.

The key scheduler is responsible to generate 128 sub-keys from SK_0 to SK_{127} for one encryption operation using a master key as shown in Figure 1(b). As shown in Figure 2, 128 bit master key is inputted to key scheduler. Then, it performs bit-wise permutation and inverse bit-wise permutation. Then, it outputs the corresponding sub-key at each clock cycle to round block.

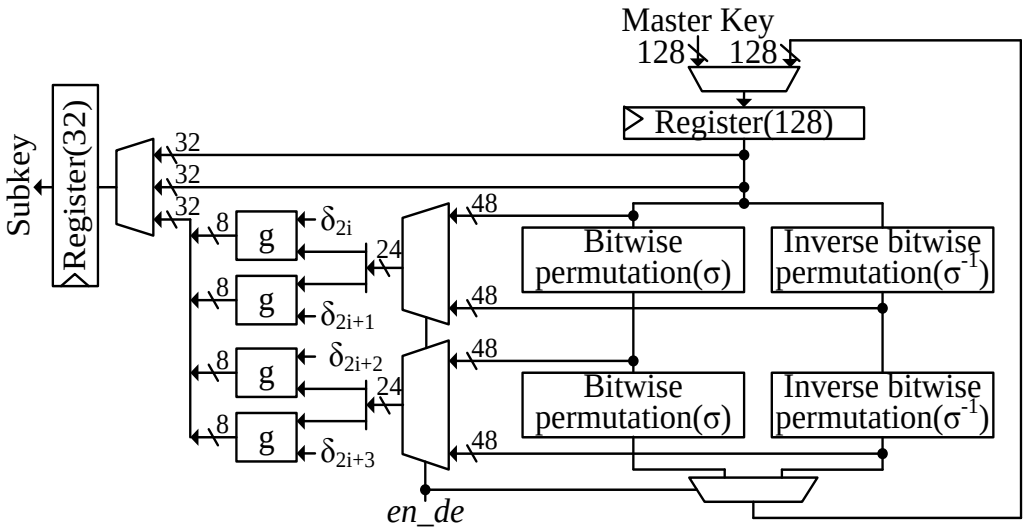

Figure 2. The Architecture of Key Scheduler for the Proposed HIGHT Design

A FSM is responsible for transferring whitening keys and sub-keys obtained from a key scheduler to two round blocks in the order which they shall be performed. It also generates the I/O control signals for each round function. Two parallel round blocks share the keys and control signals transferred from the FSM logics to avoid the area overhead caused by parallel processing of round functions.

3. The Proposed Protocol for RFID System in UHF Band

Due to the wireless data communication between a RFID reader and a tag system, illegal accesses may corrupt the personal information and control signal. We propose the protocol that alleviates a security risk in data communication between a RFID tag and a reader in the UHF band. Figure 3(a) shows the logical memory map in a RFID tag. The information used for data security is stored in the USER field. A HIGHT encrypts the data in the USER field and it transfers the encrypted data to the host system as shown in Figure 3(b). The data is transferred from a tag system to its host system via a RFID reader. Figure 4 shows the sequence of transaction within the encryption process between the RFID reader, the tag and the host system.

In order to minimize the difference between the proposed protocol and the conventional one for a RFID system in the UHF band, we add a reader key and a tag key to a RFID reader and a tag, respectively. They are used as the master key for HIGHT encryption and decryption. In addition, a host system shares the keys, RID and TID, which are the corresponding reader key and the tag key, respectively. Thus, a host system can authorize the reader and the tag system in parallel because it can use the reader key and the tag key that is accessed as a master key of HIGHT.

The proposed protocol encrypts the information of a RFID tag as well as the control information for data encryption. Then, the RFID tag and the reader communicate each other in wireless without exposure of the encryption information. In addition, each RFID reader has a different master key stored in the host system.

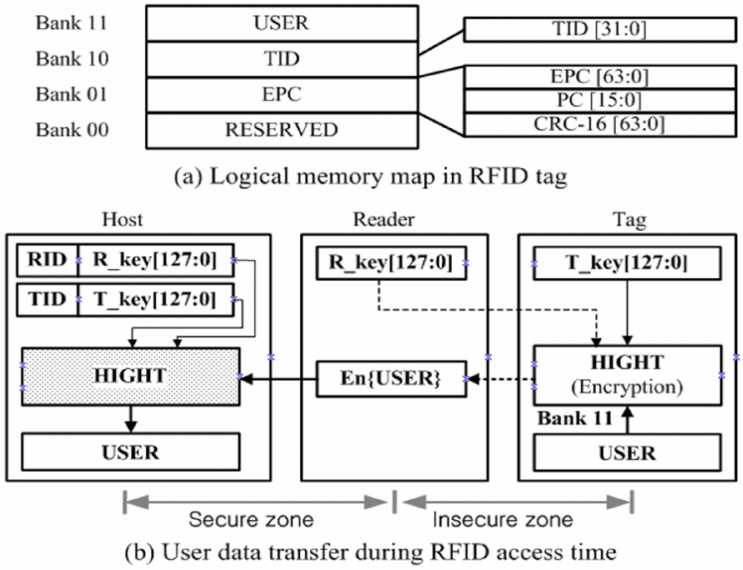

Figure 3. Example of Timing Simulation of the Proposed 2-input Ternary NAND Gate

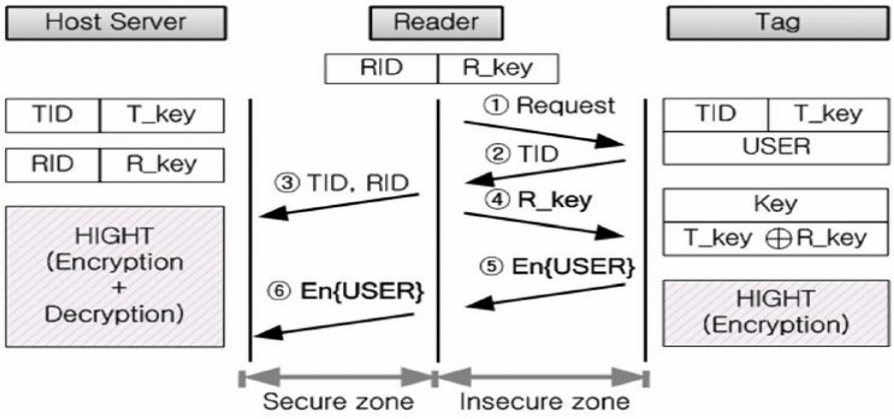

Figure 4. The Proposed Security Protocol for RFID System in UHF Band

4. Simulation Results

This section describes the performance evaluation of the proposed parallel architecture of HIGHT and the comparison results between the proposed HIGHT and an original design. The new HIGHT employing parallel architecture was fabricated using the MagnaChips 0.25μm standard CMOS process.

Table 1 shows the comparison of some HIGHT implementations. The number of gates of the conventional HIGHT design and the proposed design is 2,608 and 3,898 gates, respectively. In the proposed parallel HIGHT, control logics, key scheduler, and round blocks require 189, 1,630, and 2,078 gates, respectively. Our implementation has 50% area overhead comparing to the conventional HIGHT due to the replication of additional round blocks. Both of them can be applicable to a passive RFID tag because they meet the mandatory requirement of the RFID standard [1]. The conventional HIGHT and the proposed parallel design have an average power consumption of 10.8μW and 15,7μW at the 100 kHz clock

frequency, respectively. Even though the power consumption of the round blocks is twice bigger than that of the conventional HIGHT, the total power consumption increases about 45% of common key generation and other factors such as scale down. The conventional HIGHT and the proposed parallel design implementation have an average current consumption of 4.3μA and 6.3μA at 100kHz clock frequency which are equivalent to the energy consumption of 3.69nJ and 5.34nJ, respectively.

The proposed design saves energy substantially. Energy consumption per transaction is a critical factor of power plan of a RFID system design. The parallel design consumes 38% lower energy than the conventional scheme. Processing two 64bit plain texts in parallel yields twice higher throughput. By lowering operating frequency by half, we can maintain the same throughput while lowering energy consumption by the sharing of the key schedule.

The maximum throughput of the parallel design is 470Mbps with 125MHz clock. This high throughput is the main advantage of the proposed HIGHT design because it can be applicable for to the other application such as home network transferring multimedia data on a high speed network.

Table 1. Comparison Results with Original HIGHT

	Conventional HIGHT[5] (data block : 64-bit)			The proposed HIGHT (data block : 128-bit)		
Component	Circuit Area (EG)	Ave. power (μW)	Max. Throughput	Circuit Area (EG)	Ave. power (μW)	Max. Throughput
Control logic	189	0.4	235 Mbps	189	0.3	470 Mbps
Key scheduler	1,591	4.5		1,630	3.4	
Round block	828	5.9		2,078	12.0	
Total	2,608	10.8		3,898	15.7	

5. Conclusions

This paper proposes a parallel architecture to enhance the performance of the block cipher algorithm HIGHT. It also introduces an efficient protocol applicable to RFID systems with HIGHT. The proposed HIGHT enhances the performance as twice higher comparing to the conventional design. Our design consumes the average power under 15.7μW at 100 kHz clock frequency and it has only 3,898 gates. An implementation of the proposed HIGHT meets all the mandatory requirement for RFID systems with respect to the circuit area and power consumption. It achieves the maximum throughput of 470Mbps at 125MHz clock. The proposed protocol overcomes the security vulnerability of RFID tags and saves energy consumption per data transaction by sharing key generation.

Acknowledgement

This research was financially supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Science, ICT & Future Planning (2011-0013219) and this research was financially supported by the Ministry of Education (MOE) and National Research Foundation of Korea (NRF) through the Human Resource Training Project for Regional Innovation (2012H1B8A2026055).

References

[1] K. Finkenzeller and D. Muller, "RFID-Handbook: Fundamentals and Applications in Contactless Smart Cards, Radio Frequency Identification and Near-Field Communication", 3rd Edition, Wiley, **(2010)**.
[2] National Inst. of Standard and Technology (NIST), FIPS-197: Advanced Encryption Standard, **(2001)**.
[3] M. Feldhofter, J. Wolkerstorfer and V. Rijmen, "AES implementation on a grain of sand", Proc. of IEE Information Security, vol. 152, no. 1, **(2005)**, pp. 13-20.
[4] D. Hong, "HIGHT: A new block cipher suitable for low-resource device", Proc. of CHES 2006, LNCS 4249, Springer, Heidelberg, **(2005)**, pp. 46-59.
[5] Y. I. Lim, J. H. Lee, Y. You and K. R. Cho, "Implementation of HIGHT cryptic circuit for RFID tag", IEICE Electronics Express, vol. 6, no. 4, **(2009)**, pp. 180-186.