논문 2010-47TC-11-15

무선 네트웤 라우터응용을 위한 고성능32비트 내장AES

(High Performance 32-bit Embedded AES for Wireless Network Router Applications)

등 린*, 유 영 갑**

(Deng Lin and Younggap You)

요 약

본 논문은 고성능32비트 AES구조를 제시한다. 재배열 구조는 5단 파이프라인을 사용한다. 그 안에 ShiftRows/InvShiftRows 모듈은 4단 파이프라인을 사용하고 MixColumn/InvMixColumn 모듈은 1단 파이프라인을 사용한다. Shift rows 와 inverse shift rows 같은 구조를 사용한다. Mix column 과 inverse mix column 도 같은 구조를 사용한다. 그리고 RCON구조를 단순화 하여 사이즈를 줄였다. 제안된 구조는 verilogHDL 을 이용하여 구현 하였다. 이 회로의 처리량은 415Mbits/s 이고 크기는 0.18um CMOS 공정에서 13,764 게이트 이다. 재배열 구조는 무선 네트워크 라우터에서 사용할 수 있다.

Abstract

This paper presents a high performance 32-bit single core AES architecture. The proposed architecture employs a 5-stage pipeline: four stages in the ShiftRows/InvShiftRows module, and one stage in the MixColumn/InvMixColumn module. Circuit size reduction has been achieved through merging of the shift rows and inverse shift rows. The mix column and inverse mix column share the same resources. Three 32-bit registers replace the conventional ten 32-bit registers in the RCON architecture. The proposed architecture has been implemented in Verilog HDL, and yields 415 Mbits/s throughput with the circuit size of 13764 gate equivalents on the 0.18um CMOS process technology. This high performance architecture is suitable for wireless network router applications.

Keywords: AES, high performance, single core, pipeline, wireless network router

Ⅰ. Introduction

The evolution of wireless networks and mobile devices brings increased concerns about performance and security of wireless systems.

Cryptographic processors may alleviate the security issues of wireless network routers. The conventional AES architecture suffers some limitation in portable wireless network applications due to larger size and slower speed[1~3]. Further innovation is necessary for circuit size reduction and improvements in processing speed.

This paper addresses the size reduction and speed enhancement of an embedded cryptographic processor comprising AES, a widely used block cypher algorithm. The proposed architecture employs two schemes to speed up circuit operation and to reduce the circuit size: pipelining and simplification of register files, sharing of common structure. Pipelining addresses the row and column shifting and

* 학생회원, 충북대학교 정보통신공학과
(Shool of Information and Communication Engineering, Chungbuk National University)
** 정회원-교신저자, 충북대학교 정자정보대학
(College of Electrical and Computer Engineering, Chungbuk National University)
※ 이 논문은 2010년도 충북대학교 학술연구지원사업의 연구비 지원에 의하여 연구되었음
접수일자: 2010년8월30일, 수정완료일: 2010년11월10일

mixing intermediate data of the AES algorithm. Excessive data registers are reduced to get smaller circuit while not impeding speed. Some of the repeatedly used circuit functions are shared among the relevant function. The resultant design will be small enough to be included in a very small and compact network routers.

The rest of paper is organized as follows. Section Ⅱ gives a brief description of the conventional AES architecture. Section Ⅲ introduces the proposed architecture and compares with conventional schemes. Section Ⅳ provides with a comparison of the simulation results. Section Ⅴ summarizes the design and simulation results of the proposed architecture.

Ⅱ. Background

1. AES For Wireless Networks

Information protection using software fire walls is popular in many wireless routers for private uses. The software-based approaches are too slow for wireless applications. Faster and safer approaches should be implemented in portable router systems to handle heavy real time traffic.

Cryptographic processors with embedded block cypher algorithm such as AES and ARIA can resolve this router security problem. Figure 1 shows an embedded AES wireless network system. Although many papers have presented the designs and implementations of crypto processors such as Wang[4], Alam[5], and Kim[6], further improvements are possible to accommodate wireless router environment. This paper introduces a new approach in

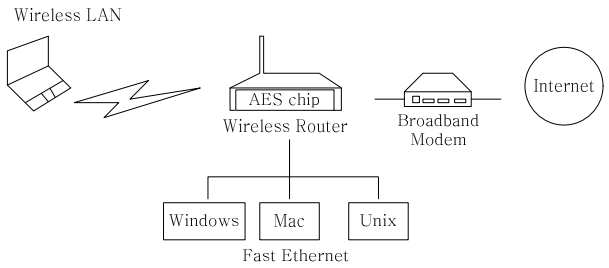

그림 1. 내장 AES 무선 네트워크 시스템
Fig. 1. Embedded AES wireless network system.

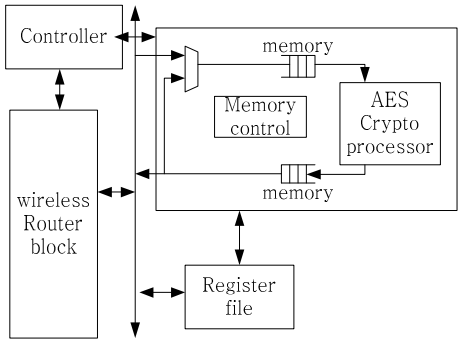

그림 2. 무선 네트워크 라우터에서 AES 암호 프로세서 구현의 블록도
Fig. 2. Block diagram of AES crypto processor implementation in wireless network router.

cryptographic circuit design aiming at higher throughput and smaller area. The block diagram of the proposed embedded AES wireless router is shown in Figure 2. This single chip comprises a wireless router, a dual port memory, a memory control, a register file, an AES crypto processor and a main controller. This chip better suits to be embedded in a wireless network router.

2. Conventional AES Architecture

The AES algorithm processes 128 bit plain text data at a time. The key length can be 128, 192, or 256bits. For the simplicity in discussion we concentrate the key length of 128 bits. The AES is an iteration algorithm comprising several identical rounds each receiving its subkey. The total number of rounds is 10 for the 128bit key. Normal AES architecture employs a 128bit datapath and 10 iterations of rounds.

There are some approaches to reduce the circuit size by simplifying the internal feature of every round. One such approach adopts four parallel 8-bit s-boxes in every round. This approach suffers slow operation due to the increase in clock cycles. It needs 64 clock cycles[7].

Schemes for faster operation introduces multiple cores in the cryptographic processors. Dual core may handle internal functions such as SubBytes, ShiftRows, and MixColumn and their inverses such as InvSubBytes, InvShiftRows, and InvMixColumn in

separate cores making the system simpler, and thereby increase the processing speed. The speed issues are further addressed by introducing circuit duplication of each round for pipelining, sub-pipelining and loop unrolling.[8] It is realized by inserting rows of registers among combinational logic.

Ⅲ. The Proposed Architecture

The 128 bit AES algorithm activates 32bits s-boxes eight times in every loop. The number of s-boxes are reduced in some conventional designs for smaller circuit area sacrificing encryption throughput. Reflecting the 802.11n standard, the maximal speed of WLAN is 500Mbps which is far slower than the speed of some designs with 77.6 G bits throughput with 473 K gates.[9]

The proposed architecture uses a 32bits data path. There are two parallel 32bit s-boxes in every loop. They can be used to get the text and key SubBytes data at the same time. This design not only reduces area but also yields a higher throughput. Figure 3 shows the proposed single core AES crypto processor architecture.

The proposed design uses single core encryption/ decryption architecture. Substantial amount of circuit may be shared by similar functions such as ShiftRows and InvShiftRows, MixColumn and InvMixColumn modules. We can take full advantage of these. Single core design may save area further reducing the number of registers by half with respect to the dual core counterpart.

The proposed architecture uses four 32-bit shift registers to build the ShiftRows or InvShiftRows module. The data block is shifted column by column. This architecture involves the whole 128bits ShiftRows and InvShiftRows operation. There is a 4-stage pipeline in this module to accommodate the column structure.

The proposed architecture of the MixColumn /InvMixColumn module uses the substructure sharing. The substructure sharing architecture has two parts. Encryption operation needs the part 1 only. Combination of the part 1 and the part 2 is for decryption operation. There are a pipeline in the middle of the two parts. Thus the design uses 5-stage pipelines in the proposed architecture in total. In the two parts, we use two opposite clock pulses respectively. This method can reduce the register delay. The total clock cycles are

reduced to 44. According to the function (1), these

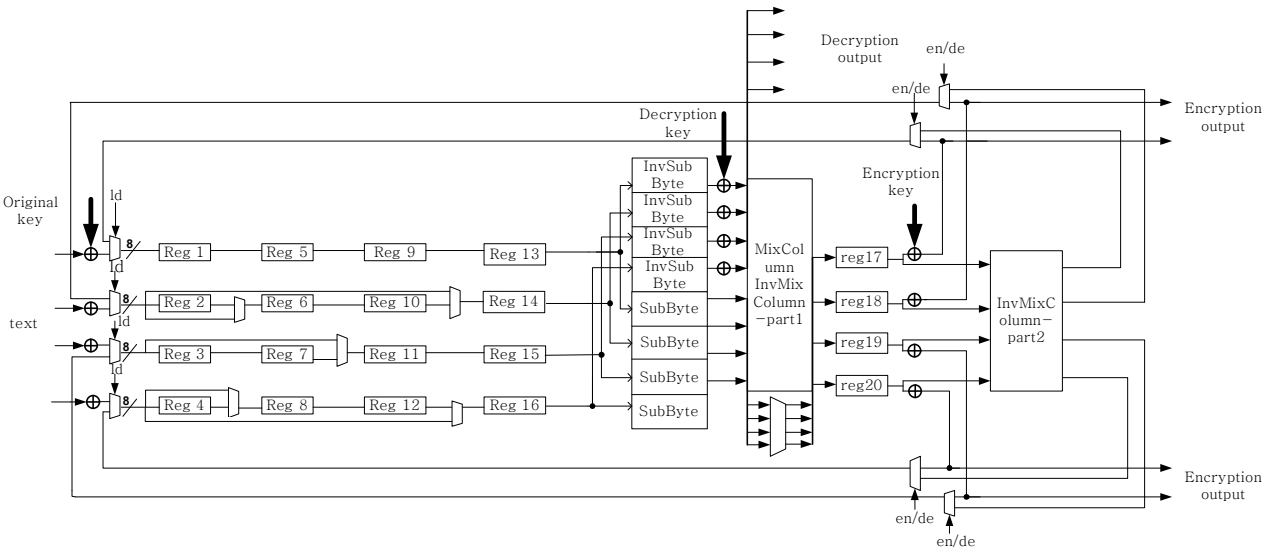

그림 3. 제안된 구조
Fig. 3. The proposed architecture.

methods can enhance the throughput obviously.

$$throughput_{sub-pipe} = datapath \times pipeline(stage) \times frequency / clockcycle \quad (1)$$

1. ShiftRows/InvShftRows

The circuit size reduction of internal circuit blocks can be achieved by sharing. Figure 4 shows the conventional architecture. The encryption or decryption round needs sixteen 8-bit registers to keep the data. Figure 5 shows the proposed ShiftRows/InvShiftRows architecture. The proposed architecture needs a smaller area. Both the proposed architecture and the conventional architecture accomplish 128-bit operation. But the conventional architecture needs 32 8-bit registers to save the data which is shifted in encryption or encryption. It can only add a 1-stage pipeline.

The proposed architecture just needs 16 8-bit registers that can make a 4-stage pipeline. The proposed architecture not only saves complex multiplexors and registers but also shortens the critical path.

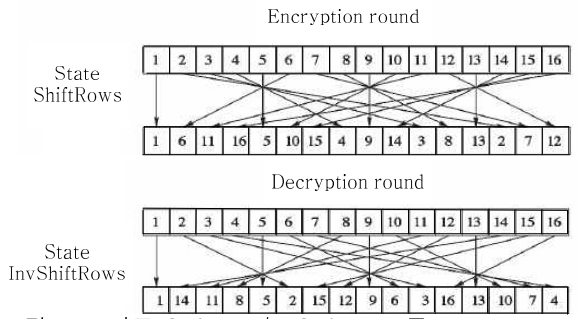

그림 4. 기존 ShiftRows/InvShiftRows 구조
Fig. 4. Conventional ShiftRows/InvShiftRows architecture.

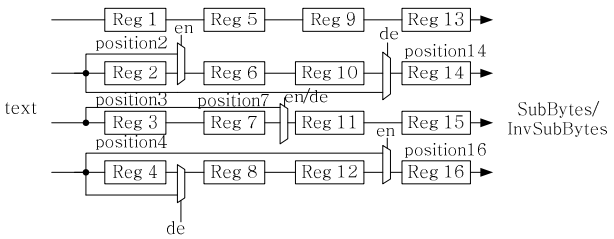

그림 5. 제안된 ShiftRows/InvShiftRows 구조
Fig. 5. The proposed ShiftRows/InvShiftRows architecture.

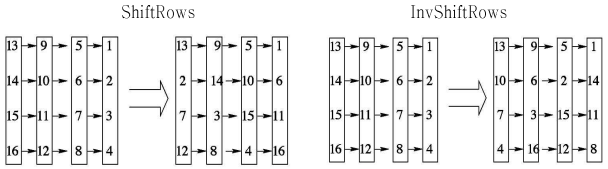

그림 6. ShiftRows 와 InvShiftRows 동작 원리
Fig. 6. ShiftRows and InvShiftRows principle of operation.

The operation of the proposed design begins with shifting of data. Sequential shifting is performed in the first row of the proposed design. The second row, the first data is keeping in the position 2. In decryption the last data is delayed to the position 14. The third row, the first two data is keeping in position the 3 and 7. Decryption is the same as encryption. The fourth row, the last data is delayed to the position 16. In decryption the first data is keep in the position 4. Figure 6 shows the final data position after these steps.

2. MixColumn/InvMixColumn

Sharing resources saves circuit area in the conventional design as shown in Figure 7 for MixColumn /InvMixColumn architecture.[10] The MixColumn and InvMixColumn functions share the same resource in this architecture. Fig. 8 shows the

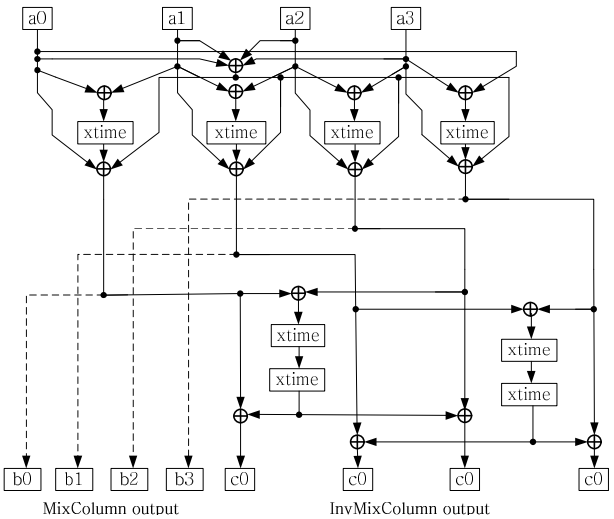

그림 7. 기존 MixColumn/InvMixColumn 구조
Fig. 7. Conventional MixColumn/InvMixColumn architecture.

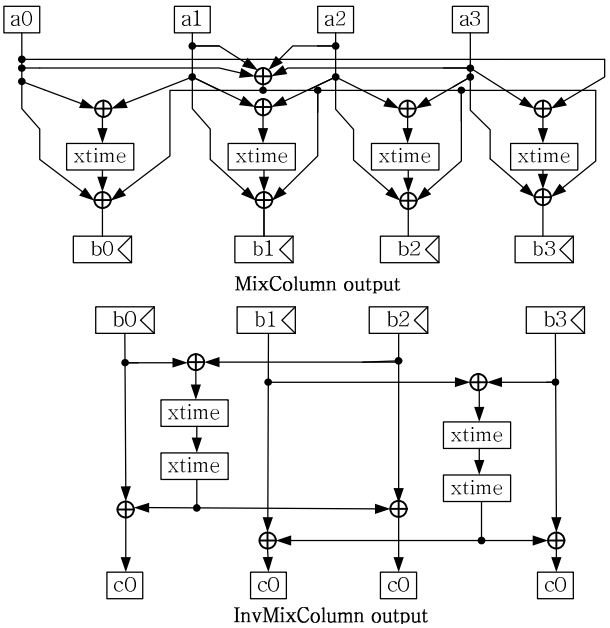

그림 8. 제안된 MixColumn/InvMixColumn 구조
Fig. 8. The proposed MixColumn/InvMixColumn architecture.

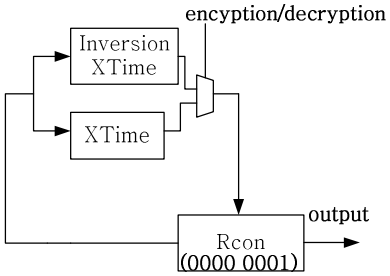

그림 9. 기존 RCON 구조
Fig. 9. Conventional RCON architecture.

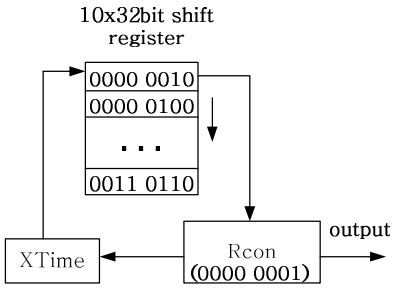

그림 10. 제안된 RCON 구조
Fig. 10. The proposed RCON architecture.

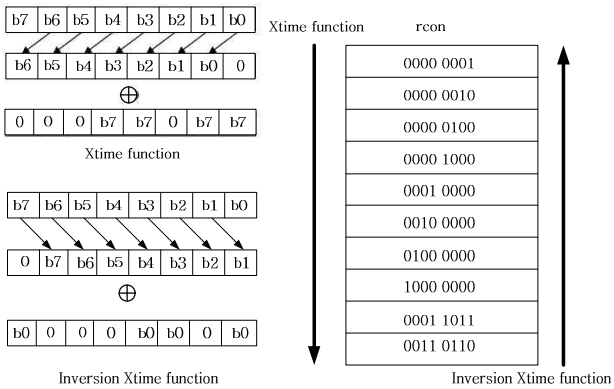

그림 11. Xtime 과 inverse Xtime 함수
Fig. 11. Xtime and inverse Xtime function.

proposed architecture.

The proposed architecture is based on the bit-level resource sharing MixColumn/InvMixColumn architecture, so it allows further reduction of logic. The proposed architecture adds pipelines between MixColumn and InvMixColumn parts resulting in higher throughput than conventional architecture. The proposed architecture uses two opposite clock pulses in MixColumn and InvMixColumn parts respectively taking the smaller number of the clock cycles.

The circuit operation of the proposed mix column processing begins with input data a0 through a3 of Figure 8, and ends with the output b0 through b3. The whole section of the input, a0, a1, a2, a3, and the output c0, c1, c2, c3, is the InvMixColumn section. In the middle of the whole section there are four 8-bit registers.

3. RCON

Figures 9 and 10 show the conventional and the proposed RCON architecture, respectively. The proposed architecture occupies smaller area and yields higher throughput. The on-the-fly key generation architecture[11] require RCON output 10 regular numbers in encryption and reversed sequence of the 10 numbers in decryption. Conventional design needs 10 32-bit shift registers to save the 10 numbers generated in encryption. Inversion in XTime is to generate the reverse sequence 10 numbers yielding smaller size.

The X-time function is to multiply {00000010} on the incoming data as shown in Figure 11. It is done by shifting one bit to the left and a subsequent conditional bitwise XOR with {00011011}. The inversion Xtime function is to divide incoming data with {00000010}. It is done by shifting one bit to

right and a subsequent conditional bitwise XOR with {10001101}. Rcon(i+1) can be generated on-the-fly from the stored Rcon(1) = {00000001} when the control signal is '1 which stands for the encryption mode. When the Rcon output the last data the control signal will change to '0', which stands for the decryption mode.

Ⅳ. Experimental Results

The proposed 32bit embedded AES has been designed and simulated employing the 0.18um CMOS process with IDEC support.

1. ShiftRows/InvShftRows

Conventional schemes use 128-bit ShiftRows and InvShiftRows. We add sub-pipelining in ShiftRows and InvShiftRows separately. A 128 bits block of data needs to be stored before the next state replaces its content. This scheme requires a 128-bit register for ShiftRows, and another one for InvShiftRows.

The proposed design has a different way to implement. It requires only four 32bits shift registers and five 8-bit 2-to-1 multiplexers. From the simulation we observe that the proposed architecture can reduce area 52.9% smaller than the conventionals. Because the proposed architecture has a 4-stage pipeline, it can yield 993.54Mbps throughput. The throughput is almost the same as the conventional 128bits pipeline.

표 1. ShiftRows/InvShiftRows 성능 비교
Table 1. ShiftRows/InvShiftRows performance comparison.

	Proposed design ShiftRows/InvShiftRows	Conventional ShiftRows/InvShiftRows	Proposed design performance
Throughput (Mbps)	993.54	1338.18	↓ 25.8%
Area(gate)	1330	2821	↓ 52.9%

2. MixColumn/InvMixColumn

Substantial circuits may be shared between the two functions of MixColumns and InvMixColumns. The circuit structure can be divided into two parts. The encryption operation needs part 1 only. The

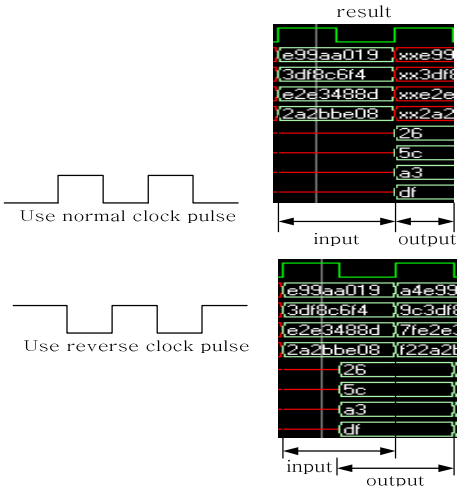

그림 12. 레지스터 지연을 줄이기 위한 반전 클럭 펄스 구현
Fig. 12. Reverse clock pulse implementation to reduce the register delay.

표 2. MixColumn/InvMixColumn 성능 비교
Table 2. MixColumn/InvMixColumn performance comparison.

	Proposed design MixColumn/InvMixColumn	Conventional MixColumn/InvMixColumn	Proposed design performance
Throughput (Mbps)	166.029	119.877	↑ 38.5%
Area(gate)	822	600	↑ 37%

combination of the part 1 and the part 2 are used for decryption purposes. One 32bits pipeline registers can be used for both encryption and decryption. In the module, the proposed design will use a reverse clock pulse to reduce the registers delay as shown in Figure 12.

From the simulation we can find the proposed design can yield 38.5% higher throughput than conventionals with only 222 gate increase.

3. RCON

This proposed architecture differs from conventional designs. The inversion Xtime function is the new feature introduced in the proposed design. This function is derived from the Xtime function. This function replaces the conventional shift registers resulting in a simpler data path. This approach enhances throughput and occupies smaller area. Form the simulation we can find the proposed architecture can yield 33.5% higher throughput and takes 60.1%

표 3. RCON 성능 비교
Table 3. RCON performance comparison.

	Proposed design RCON	Conventional RCON	Proposed design performance
Throughput (Mbps)	312.429	234.109	↑ 33.5%
Area(gate)	209	524	↓ 60.1%

smaller area than conventional designs.

4. Performance Comparison

The comparison with competing designs is shown in Table 4. Mangard[7] has used 128-bit datapath architecture although the clock cycles are least, but the frequency is low, so the throughput is low. Hua[14] has used 32-bit datapath architecture although the operating frequency is high. Since the smaller number of pipeline stages are used, its throughput is low. The proposed architecture is simpler for both the data unit and the key generation unit. From the simulation we can find the proposed architecture can yield 24 % higher throughput and 17% smaller area than Hua's design used in their 32-bit high performance architecture.[14]

표 4. 코어별 성능 비교
Table 4. Performance comparison with other cores.

Design & FPGA / Items Compared	Chodowiec[12] 32bit AES	Mangard[7] 128bit AES	Rouvroy[13] 32bit AES	Hua[14] 32bit AES	Proposed 32bit AES
Maximum clock Frequency(MHz)	60	64	71	115	114
Datapath Bits	32	128	32	32	32
Clock cycles	44	34	44	44	44
Area(gate)	17024	15493	17825	16629	13764
Throughput (Mbps)	166	241	208	335	415

Ⅴ. Conclusion

This paper presents a new compact 32-bit single-core architecture for encryption and decryption. This architecture is based on two new ideas. A 4-stage pipeline makes up a compact architecture that can achieve ShiftRows and InvShiftRows. A pipeline in the middle of the Mixcolumns and InvMixcolumns block; And the inverse XTime function makes the RCON architecture much simpler. Because of this architecture improving the proposed architecture of AES requires only 13,894 gate equivalents and provides a throughput of 415Mbits/s on the 0.18um CMOS process technologies. The size is 17% smaller and the performance is 24% higher than the 32bit high performance AES architecture[14]. The size is 11% smaller and the performance is 72% higher than 128bit high performance AES architecture.[7] It is suitable for applications in network routers. It is also suitable for applications in other wireless applications such as real time communication systems.

References

[1] A. Hodjat, "Speed-area trade-off for 10 to 100 Gbits/s throughput AES processor," *The 37th Asilomar Conference on Signals, Systems and Computer*, pp. 21-47-2150, 2003.

[2] S. Pomgyupinpanich, "A 32 bits architecture for an AES system," *Int'l Symp.on Communications and Information Technologies,* pp. 70-73, 2004.

[3] 김종환, 진경욱, "AES 기반 와이브로 보안 프로세서 설계," *전자공학회논문지,* 제44권 SD편, 제7호, 71-80쪽, 2007년 7월.

[4] M. Y. Wang, "Single-and multi-core configurable AES architectures for flexible security," *IEEE Trans. Very Large Scale Integration (VLSI) Systems,* vol. 18, no. 4, pp. 541-552, 2010.

[5] M. Alam, "Single chip encryptor/decryptor coor lementation of AES algooithm," *21st Int'l Confon VLSI Design,* pp. 693-698, 2008.

[6] H. W. Kim, "Design and implementation of a private and public key crypto processor and its application to a security system," *IEEE Trans. Consumer Electronics,* vol. 50, no. 1, pp. 214-224, 2004.

[7] S. Mangard, M. Aigner, and S. Dominikus,"A highly regular and scalable AES hardware architecture," *IEEE Trans. Comput.,* vol. 52, no. 4, pp. 483-491, 2003.

[8] X. Zhang, "Implementation approaches for the advanced encryption standard algorithmm," *IEEE Circuits and Systems Magazine,* vol. 2, no. 4, pp. 24-46, 2002.

[9] A. Hodjat, and I. Verbauwhede, "Minium area

cost for a 30 to 70 Gbits/s AES processor," *IEEE Computer society Annual Symposium on VLSI,* pp. 83-88, 2004.
[10] V. Fischer, "InvMixColumn decomposition and multilevel resource sharing in AESimplementations," *IEEE Transactions on VLSI System,* pp. 989-992, 2005.
[11] Ha-Kee Ahn and Kyung-Wook Shin, "On-the-fly 키 스케줄러를 갖는 AES-128/192/256 암호 프로세서," *전자공학회논문지,* 제39권 SD편, 제11호, 33-43쪽, 2002년 11월.
[12] H. Lin, "High performance AES cores for xilinx FPGA," http://www.helintech.com/, downloaded on Aug. 15. 2005.
[13] G. Rouvroy, F. X. Standaert, J. J. Quisquater, and J. D. Legat, "Compact and efficient encryption/decryption module for FPGA implementation of the AES (Rijndael) very well suited for small embedded application," *International Conference on Coding and Computing,* pp. 583-587, 2004.
[14] H. Li, and J. Z. Li, "A new compact dual-core architecture for AES encryption," *IEEE J. Elect. Comput.,* vol. 33, no. 3/4, pp. 209-213, 2008.

저 자 소 개

Deng Lin(학생회원)
2007년 Northeast Petroleum University 정보통신 공학부 학사 졸업
2009년~현재 충북대학교 정보통신공학과 석사과정
<주관심분야 : 암호학, VLSI 설계>

유 영 갑(정회원)
1975년 서강대학교 전자공학과 학사 졸업
1981년 Univ. of Michigan, Ann Arbor 전기전산학과 석사 졸업
1986년 Univ. of Michigan, Ann Arbor 전기전산학과 박사 졸업
1975년~1979년 국방과학연구소연구원
1986년~1988년 (주)금성반도체 책임 연구원
1993년~1994년 아리조나대학교 객원교수
1998년~2000년 오레곤 주립대학교 교한교수
2007년~2008년 일로노이 주립대학교 객원연구원
1988년~현재 충북대학교 정보통신공학과 교수
2010년~현재 충북대학교 전자정보대학장
<주관심분야 : VLSI 설계 및 테스트,고속 인쇄회로 설계,암호학>