Implementation of AES and Triple-DES cryptography using a PCI-based FPGA board

Ohjun KWON, Hidenori SEIKE, Hirotsugu KAJISAKI and Takakazu KUROKAWA
Department of Computer Science,
National Defense Academy
1-10-20 Hasirimizu, Yokosuka-shi, 239-8686 Japan
Tel. +81-468-41-3810(ext.2219), Fax. +81-468-44-5911
E-mail: g40044@nda.ac.jp

Abstract: This paper presents hardware implementations of the two representative cryptographic algorithms, Advanced Encryption Standard (Rijndael), and the present American federal standard (Triple DES) using a PCI- based FPGA board named "SEBSW-1". This board bases on a FPGA chip (XilinxVirtex300 XCV300PQ240-4). The implementation results of these two algorithms were tested successfully.

AES circuit could proceed an encryption as well as a decryption two times faster than the Triple-DES circuit, while the former circuit used higher rates of CLBs. Besides, if these architectures use pipeline-registers, the processing speed will be increased about 1.5 times than the presented circuits.

1. Introduction

Recently, internet has been spreading all over the world by the advancement of the computer technology. Internets has been promoting the advancement of the cipher-technology. Concerning with the research on the cipher-technology, hardware implementations of cryptographic algorithms to be a high speed computational machine has also becoming important and popular.

Among these research on hardware implementations of cryptographic algorithms, reference [1] had implemented AES and Triple-DES on a PCI-based FPGA board named SLAAC-1C, and proved their hardware implementations to be very effective and fast. This board is equipped with Virtex XCV1000BG560-6, while we are researching the possibility of Triple-DES and AES to be implemented into a smaller device such as XCV300PQ240-4. This report presents our implementation results of AES and Triple-DES on a PCI-based FPGA board including one XCV300PQ240 -4 chip.

2. Standard Cryptographic algorithms

2.1 Triple-DES

DES (Data Encryption Standard) was proposed as the algorithm for the secure and secret items in 1970, and was adopted as an American federal standard by NBS in 1973.

DES algorithm uses 16 rounds for encryption of 64-bit plain text using 64-bit key. However the key of actual use requires only 56-bit. Because of the limited key-length of DES, it's security level have been falling down by the progress of computer science and computer technologies. For the counterplan of DES, Triple-DES was proposed as the next generation algorithm.

Triple DES is a minor variation of DES algorithms. It is three times slower than regular DES, but can be billions of times more secure if used properly. Triple DES is emploied in much wider application fields than DES, because DES is so easy to break with today's rapidly advancing technology.

2.2 AES

The counterplan for the falling down of the security level of Triple-DES, NIST has invited public contributions for the next generation cipher-algorithms, shall be named as AES (Advanced Encryption Standard). Rijndael was adopted finally on Oct. 2000 among the six candidated algorithms. After that Rijndael was published as FIPS197 on Nov.

3. Architectures

There are two representative methods for the hardware implementations of ciphers, a basic architecture and an extended architecture.

A basic (or loop) architecture is a general way of designing. All rounds of encryptions and decryption are designed, and tied in a line. This architecture is simple and easy, but not so good for the processing speed. An extended architecture is another way of designing using pipe-lines on each round. This architecture is faster and higher-leveled designing method for the hardware implementaions of algorithms. In reference [1], both architectures were discussed. However, we have designed Triple-DES and AES based on the basic architecture only, because of the limited hardware size.

3.1 Triple-DES

Triple-DES is usually composed of three-DES rounds [E-E-E logic] or two-DES rounds [E-D-E logic]. We designed and implemented it using the E-D-E logic architecture as shown in Fig. 1 following the designing method presented in reference [1].

We designed 16 rounds in DES, for an encryption circuit as well as decryption circuit using the Fully-loop-unrolled architecture as shown in Fig. 2, and two kinds of DES circuits are arranged as shown in Fig. 1. Thus, our architecture composes the loop architecture.

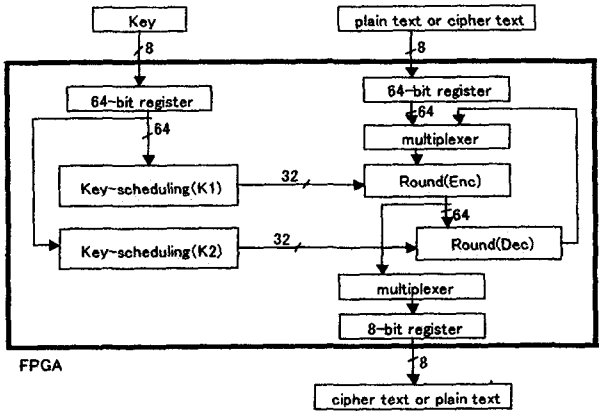

Fig. 1. Block diagram of Triple-DES.

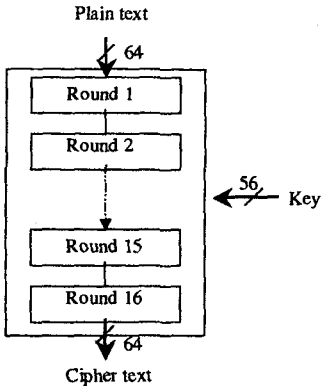

Fig. 2. Block diagram of DES encryption.

3.2 AES

AES(Rijndael) is a symmentric key block cipher with a variable key size and 128-bit input/output block size. Our design supports all three key sizes 128, 192, 256 bits reqired by the draft version of the AES standard. Our key scheduling unit is referred to 3-in-1, which means that it can process all three key sizes. Switching from one key size to the other size is instantaneos, and is triggered by the control signals.

The only block size required by Advanced Encryption Standard is 128-bits [3], but we implemented all three sizes for the detail comparations. Fig. 3 shows our design architecture of AES. For designing Round scheduling part, we employed the loop-architecture as shown in Fig. 4. We also designed key-scheduling part by the same method.

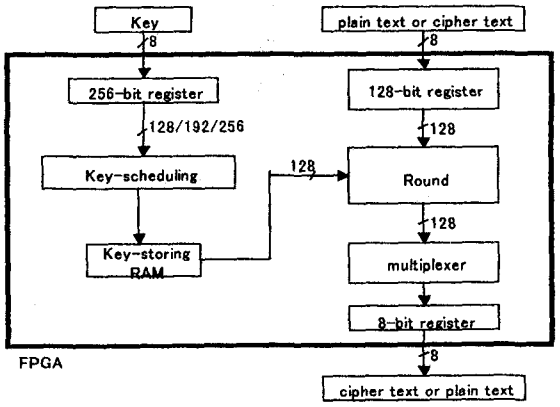

Fig. 3. Block diagram of AES.

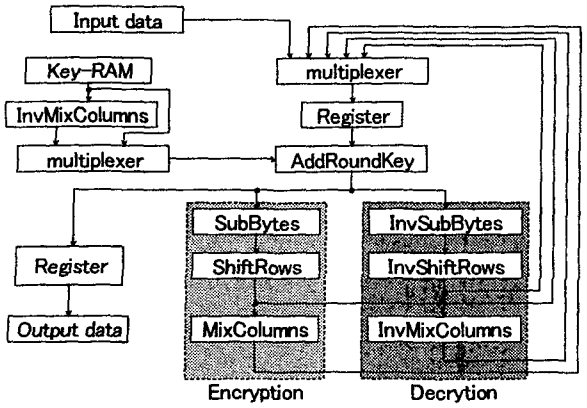

Fig. 4. Block diagram of round-scheduling.

4. PCI-based FPGA board

4.1 SEBSW-1

For the implementations of Triple-DES and AES, we developed an PCI-based FPGA accerlerator board named "SEBSW-1 (SEcret-key Block cipher Switcher)" as shown in Fig. 5. SEBSW-1 is composed of PCI controller, IO controller, local-bus conroller, SRAM, and FPGA chip. PCI controller is a device for the interface between the host PC and SEBSW-1. IO controller outputs control signals to local-bus controller, SRAM, and FPGA chip. Local-bus controller controls local buses in SEBSW-1. Configuration data of FPGA chip is temporally stored in SRAM chip. Fig. 6 shows a block diagram of SEBSW-1 including its host PC.

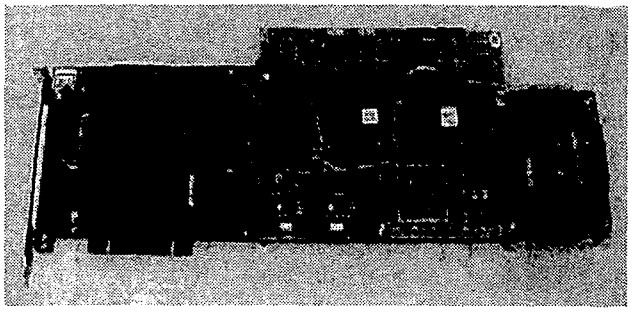

Fig. 5 SEBSW-1.

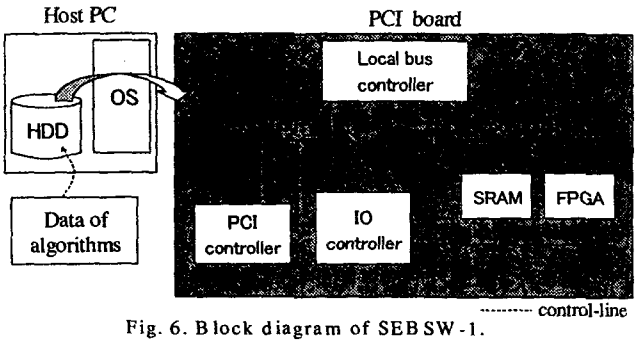

Fig. 6. Block diagram of SEBSW-1.

4.2 FPGA chip

SEBSW-1 is equipped with user programmable FPGA chip (Xilinx Virtex XCV300PQ240-4). FPGA chips in Virtex family are composed of basic logic cells referred as "CLB (Configurable Logic Block) slices", and synchronous dual-ported RAMs. For their configuration, SelectMap mode was used on the standpoint of its fast processing speed.

Table 1. shows the characteristics of Virtex XCV300PQ240-4. In this table, the characteristics of Virtex XCV1000BG560-6, which was used on the SLAAC-1C PCI board [1] are also shown. We used Foundation3.1i for the design and implementations of Triple-DES and AES.

Table 1 Characteristics of XCV300 PQ240-4 and XCV1000 BG560-6.

FPGA chip	XCV300 PQ 240-4	XCV1000BG 560-6
System Gate	323K	1,124K
CLB Slice	3,072	12,228
User I/O Pin	166	404
Block RAM	65,536	131,072

5. Evaluation results

Here, we will evaluate the implementation results of Triple-DES and AES for some viewpoints and compare them with the implementation results presented in reference [1]. As shown in Table 2, the processing speed of AES (167Mbit/s) is about two times faster than that of Triple-DES (83Mbit/s). This comparison agrees with reference [1].

Overall performance of [1] was superior to our implementation results. These can be found the following three reasons for their comparison results;

① the characteristics of FPGA chips (XCV300 PQ240-4 vs. XCV1000 BG560-6),
② communication speed between the developed boards and their host PCs, and
③ designing tool.

6. Conclusion

Hardware implementatons of Triple-DES and AES on the PCI-based FPGA board (SEBSW-1) are presented. These implementation results show the superiority of AES to Triple-DES on the

standpoint of their processing speed, regardless of the key length, while AES requires much hardware resources. Our hardware implementation results agreed with those of reference [1].

We employed the basic loop architecture and fully-loop unrolled architecture for the circuit designing of Triple-DES and AES. By employing the pipeline architecture, the throughputs will be increased about 1.5 times than the presented circuits.

References

[1] Pawel Chodowiec et.al.,"Experimental Testing of the Gigabit IPSec-Compliant Implementations of Rijndael and Triple DES Using SLAAC-1V FPGA Accelerator Board", Proc. Information Security Conference, Oct.2001.

[2] NIST, "Advanced Encrypyion Standard(AES) ", FIPS PUB197, Nov.2001.

[3] NIST Special Pubilication 800-20, "Modes of Operation Validation System for the Triple Data Encryption Algorithm", National Institute of Standard and Technology, 2000.

Table 2 Implementation results of Triple-DES and AES.

		Comparison items	Our implementations	[1]
FPGA			XCV300 PQ240-4	XCV1000 BG560-6
PCI board			SEBSW-1 PCI board (8bit/16MHz)	SLAAC-1V PCI board (64bit/66MHz)
Basic architecture	Triple-DES	Processing speed	83Mbit/s	91Mbit/s
		fmax	69MHz	72MHz
		CLBs	28% (983)	5% (614)
		BlockRAMs	47%	-
	AES	Processing speed	167 Mbit/s (128bit key-length)	521Mbit/s (128bit key-length)
			142Mbit/s (192bit key-length)	-
			124Mbit/s (256bit key-length)	-
		fmax	30MHz	47MHz
		CLBs	53% (1,628)	10% (1,228)
		BlockRAMs	75%	56%