FPGAを用いたTriple-DESとAESの実装

2W−06　権 五俊　清家 秀律　梶崎 浩嗣　黒川 恭一

防衛大学校情報工学科

1 はじめに

近年のコンピュータ技術の向上により，インターネットが広範に普及し，それに応じてネットワーク産業等も盛んとなって来ている.それとともに，暗号の重要性も高まっている.

そこで本稿では，FPGAを用いて，現在広く使われている標準暗号 Triple-DES と次世代の標準暗号アルゴリズムである AES 暗号を搭載した PCI ボード(SEBSW-1:SEcret-key Block cipher SWitcher)を実装し，ハードウェア的な暗号の実装でこれらの性能評価を回路規模及び処理速度の面から比較・検討する.同様の検討が参考文献[1]で行われており，その結果と今回実装した結果の比較・検討を行う.

2 Triple-DESとAES暗号の概要

2.1 DESとTriple-DESの概要

DES(Data Encryption Standard)は1970年に秘密(機密)事項に対する暗号化アルゴリズムとして提案され，1973 年米国商務省標準局(NBS)が採用した.DES は転置と換字変換等の簡単な操作を組み合わせることで複雑な処理を実現するプロダクト暗号方式である.56bit の鍵長で，64bit の平文を暗号化・復号するが，鍵長が短く且つ固定長であるため，近年のコンピュータの計算技術向上により安全性が低下した.これの対策に提案されたのが Triple-DES 暗号アルゴリズムである.

Triple-DES は，DES のアルゴリズムを複数回適用することで暗号強度を強化し，安全性が低い DES の鍵長を伸ばした暗号である[2][3].Triple-DES の暗号化方式としては，異なる 2 つの共通鍵を用いて「1 つ目の鍵で暗号化・2 つ目の鍵で復号・1 つ目の鍵で暗号化」を行う E-D-E 方式と，3 つの異なる共通鍵を用いる E-E-E 方式がある.Triple-DES の暗号強度は，80bit または 112bit に相当と言われる.なお，今回の実験では前者の E-D-E 方式を利用して結果を得た.

2.2 AES暗号の概要

Triple-DES 暗号は現在でも広く使われているが，上記したように DES 暗号の固定長鍵の限界とコンピュータ技術の進歩により，Triple-DES 暗号の安全性も低下している.それの対策として，NIST は，その後継暗号 AES(Advanced Encryption Standard)を公募した．その最終候補となった暗号は，「MARS」(IBM)，「RC6」(RSALab)，「Rijndael」(J.Daemen, V.Rijmen)，「Serpent」(R.Anderson 他 2 名)，「Twofish」(B.Schneier, J.Kelsey 他)の 5 つだったが，2000 年 10 月に Rijndael が最終採用され，2001 年 11 月には，FIPS197 として標準化された[4].

2.3 Triple-DESとAESの基本構成

Triple-DES 暗号アルゴリズムは，基本的に共通鍵暗号である DES を3段階合成したものである．DES の暗号化・復号を行うラウンド部と，56bit の鍵を利用し連続鍵を生成する鍵スケジューリング部により構成されている.

AES 暗号アルゴリズムは，128bit の平文・暗号文と 128, 192, 256bit の秘密鍵を利用するブロック暗号アルゴリズムである．秘密鍵を利用して拡大鍵を生成する鍵スケジューリング部と，暗号処理を行うラウンド部により構成されている[4]．ただし，今回は 128bit の秘密鍵を利用して拡大鍵を生成する.

3 FPGAチップとPCIボードの概要

今回使用した FPGA は，Xilinx 社製の Virtex XCV300PQ240-4 である．このチップは，外部 ROM 等を接続して回路データをダウンロードすることにより，FPGA 内部の回路をその時の状態に応じて書き換えることも可能である．Virtex CLB の基本ビルディングブロックは，Logic Cell(LC)であり，1 個の LC には，4 個のファンクション・ジェネレータ，キャリ・ロジック，記憶エレメントが内蔵されている．Virtexはまた，CLB 内にインプリメントされる浅い RAM 構造を提供する分散型 LUT SelectRAM を補完するため，16 個の BlockRAM を内蔵している．XCV300PQ240-4 と[1]の実験で使われた Virtex XCV1000BG560-6 の特徴を表 1 に示し，XCV300PQ240-4 を自作の PCI ボードに実装した模様を図 1 に示す.

表1　XCV1000BG560-6とXCV300PQ240-4の特徴

FPGA種類	XCV1000BG560-6	XCV300PQ240-4
System Gate	1,124K	323K
CLB Slice	12,228	3,072
User I/O Pin	404	166
Block RAM	131,072	65,536

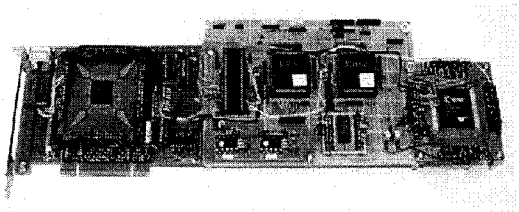

図1 PCIボード(SEBSW-1)の写真

4 実装結果及び評価比較

今回の実験では，Triple-DESとAESの基本設計[5]を，XCV300を用いた自作のPCIボード(SEBSW-1)に実装し，それぞれの結果を比較・検討した．Triple-DESとAESの基本設計・拡張設計をXCV1000-6チップを用い，PCIボードに実装した[1]の実験結果と比較した結果を表2に示す．[1]の実験では，ラウンド部分にパイプラインレジスタを追加し，データの処理速度を向上する拡張設計を行ったが，今回は基本設計だけを行って，その結果を比較・検討する．そこで基本設計とは，ループ設計とも言え，暗号回路の基本的な設計である．

自作のPCIボードにTriple-DESとAES暗号を実装した結果としては，Triple-DESよりAESが2倍の処理速度を有し，ハードウェアの利用率が高かったことを確認することができた．[1]の結果と比べて，AESの性能が良いのは同じであったが，本実験の結果より全体的に良い評価を得られたと思える．その原因として，前者で使われたXCV1000はXCV300より大きいチップであることを考慮する必要がある．

5 おわりに

本稿では，Triple-DESとAES暗号の基本設計を行い，さらにそれらを自作のPCIボード(SEBSW-1)に実装し，両者の最大クロック周波数，処理速度，CLBs及びBlockRAMs量の3面から，[1]の実験結果と比較・検討を行った．AESの回路をパイプライン化し，同じPCIボードに拡張設計を実装すると，1.5倍以上の評価を得らえる．また，Triple-DESも拡張設計により良い性能が得らえると推定できる．今回使われた回路設計に対してより簡単化及びパイプライン化を行うことにより，どの程度の性能向上が得られるかを確認することが今後の課題となる．

参考文献

[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] Douglas R.Stinson 著，櫻井幸一監訳，"暗号理論の基礎"，P.478，共立出版，Jan.1996.

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

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

[5] 清家，黒川，"FPGAを用いたAES暗号(Rijndael)のハードウェア化"，2001情報処理全大，分冊1，no.6N-8，pp.83-84，Mar.2001.

表2 実装結果と[1]の結果

		評価項目	[1]	今回の実験
FPGA			XCV1000BG560-6	XCV300PQ240-4
PCIボード			SLAAC-1V PCI board(64bit/66MHz)	SEBSW-1 PCI board(8bit/16MHz)
基本設計	Triple-DES	処理速度	91Mbit/s	83Mbit/s
		最大クロック周波数	72MHz	69MHz
		CLBs量	5%(614)	28%(983)
		BlockRAMs量	－	47%
	AES	処理速度	521Mbit/s(128bit鍵長)	167 Mbit/s(128bit鍵長)
			－	142Mbit/s(192bit鍵長)
			－	124Mbit/s(256bit鍵長)
		最大クロック周波数	47MHz	30MHz
		CLBs量	10%(1,228)	53%(1,628)
		BlockRAMs量	56%	75%