AESとDESの回路性能比較

3G－5

宗藤誠治　佐藤証　森岡澄夫　高野光司
日本アイ・ビー・エム株式会社東京基礎研究所

1 はじめに

1978年に米国の暗号標準となったDESは，デファクト・スタンダードとしての地位も確立し，80%以上の暗号製品に実装されていると言われる．しかし鍵長が56ビットと短いため，1997年には鍵の全数探索によって破られてしまった．そこで鍵を2つ，あるいは3つ用いて暗号化-復号化-暗号化と3回繰り返すTriple-DESが1998年から暫定的な米国標準となっている．

DESに次ぐ米国暗号標準AESの選定にあたっては，Triple-DESよりも高速かつ効率的なソフトウェア/ハードウェア実装が可能であることがひとつの条件であった．AESとして採用されたRijndaelでは，ガロア体GF(2^8)上の8ビット演算と，そしてその元を四つ集めて四項式とみなした演算（つまり32ビット演算）が組み合わされており，デスクトップPCの主流である32ビットMPUと，組み込み用途に広く使われている8ビットMPUの双方で効率的なソフトウェア実装が行える．

しかしながらDESが64ビットブロック暗号であるのに対し，AESはデータ幅が2倍の128ビットで，またDESはFeistel構造のため1ラウンドの処理単位は32ビットであるが，RijndaelのSPN構造は全データ128ビットを1ラウンドで処理しなければならない．さらにSPN構造は一般に暗号化と復号化が別のデータパスあるため，単純計算でAESはDESの8倍の回路規模となってしまう．特に暗号の要であるS-Boxのサイズを ROMベース実装で比較すると，DESの2,048ビットに対して，AESは20倍の4,960ビットが必要である．

そこで我々はAESの小型回路実装を目的として，様々な数学的な工夫を取り入れ，また論理構成上の最適化を行った回路アーキテクチャを提案し実装した．そのパフォーマンスをTriple-DESおよび従来のAES回路実装と比較検討する．

2 DESのアルゴリズム

図1にDESの概要を示す．64ビットのデータを左右32ビットずつに分け，右半分をF関数で変換した後に左半分とXORする操作を16回繰り返すFeistelネットワークと呼ばれる構造を持つ．基本的に暗号化と復号化は同じデータパスで実現され，Triple-DESでは計48回のF関数変換が実行される．暗号化の最初と最後に行われる初期転置と最終転置，F関数内の転置Pと32ビット→48ビット変換の拡大転置E，また6ビット→4ビット変換の8つのS-Box（S0～S7）は全てDESのスペックにおける変換テーブルによって定められている．しかしその設計基準が不明で，トラップ・ドアが仕掛けられているのではないかという憶測を生んだことから，AESをはじめとする近年の暗号ではS-Boxに算術演算が多く用いられている．また，AESの鍵スケジューリングはS-Boxを使用するが，DESは56ビットの鍵をシフトしながら定められた位置から48ビットを抜き出して16個のラウンド鍵が生成する単純なものである．

このようにシンプルなアルゴリズムのため，DESの回路化は簡単である．今回は，このアルゴリズムを素直に実装したものを評価に用いる．

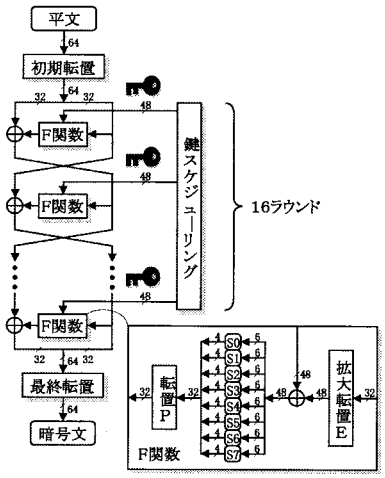

図1 DESのアルゴリズム

3 実装比較

表1に，0.11μm CMOSスタンダードセル・ライブラリによるワースト条件下でのAESとDESの実装結果を，従来実装とともに示す．回路面積は80%の配線効率を仮定している．

また図2は各実装の回路規模対スループットをグラフにしたものである．AESは高速な反面，回路が大きいので，128ビット／サイクルで処理し暗号化全体を11クロックで実行する高速なものから，サイクル数を増やす代わりにバス幅を1/2あるいは1/4に減らして処理ブロックの小型化を行ったものまで，複数のタイプを実装した．なお，21サイクル版は11サイクル版と同じ128ビットバスであるが，暗号化と鍵スケジューリングでS-Boxを共有する点が異なる．32サイクル版は64ビットバス，54サイクル版は32ビットバスである．これらの論理合成は速度優先で行ったが，54サイクル版だけは回路規模優先の合成も行った．表1の結果から，我々のAES実装は6.5Kgatesと，DESの5.3kgatesに匹敵するほど小さく組み込みに適したものから2.3Gbpsとサーバー用途に使用可能なものまで，幅広いアプリケーションに適応可能なことがわかる．

Hardware Performance Comparison between AES and DES
Seiji MUNETOH, Akashi SATOH, Sumio MORIOKA, Kohji TAKANO
Tokyo Research Laboratory, IBM Japan Ltd.
1623-14, Shimotsuruma, Yamato-shi, Kanagawa 242-8502, Japan

AES では回路縮小のために 1 ラウンドの処理を分割したが，DES は1ラウンド分の処理の分割による回路縮小が難しいので，本論文では逆に複数ラウンドを 1 サイクルで処理することで全サイクル数を減らし，それによってスループットを向上させる実装をいくつか行った．Triple-DES は 48 ラウンドを要するため，1 ラウンド／サイクル版は 48 サイクル，2 ラウンド／サイクル版は 24 サイクル，2 ラウンド／サイクル版は 12 サイクルで実行される．サイクルあたりのラウンド数を増やせばクリティカルパスが長くなり最大動作周波数は低下するが，レジスタのアクセス回数が減少するため，全体ではスループットが向上する．

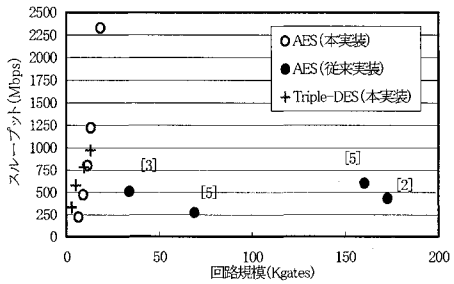

図 2 各 ASIC 実装の回路規模とスループット

図 3 に，各実装の回路使用効率を比較するため，スループットをゲート数で割った値（Kbps/Gate）を示す．値が大きいものほど性能が高い．最小実装では，我々の AES がデータパス分割で効率が落ちて 34.20Kbps/gate と低いのに対し，Triple-DES は 1round/clock の標準的な実装での効率が最も高く，63.22Kbps/gate と AES の 2 倍近くとなっている．AES では分割数を減らすほど効率がよくなり，最速実装時の 126.63Kbps/gates が最も高い．Triple-DES は高速化のためデータパスのラウンド数を増やすにつれて効率が低下し，最速実装時は 56.57Kbps/gates と AES の半分に低下する．一方，従来の AES 実装は，いずれも非常に低い効率しか達成しておらず，我々の AES 実装はそれらに対し 2〜50 倍ときわめて高いパフォーマンスが示された．

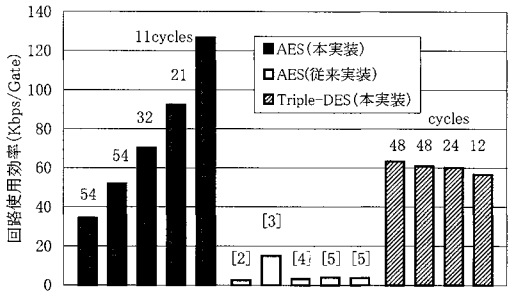

図 3 各 ASIC 実装の回路効率

4 むすび

我々の提案アーキテクチャに基づく AES 回路が，6.5Kgates と小型実装から 2.3Gbps と高速実装まで柔軟に対応できることが示された．回路効率は Triple-DES との 0.5〜2 倍と実装形態によって異なるが，高速化においては我々の AES が有利であることが明らかとなった．また従来の AES 実装に対して，我々の実装が 2〜50 倍も優れていることも示された．

文献

[1] “Advanced Encryption Standard (AES) Development Effort”, http://csrc.nist.gov/encryption/aes/index2.html.

[2] H. Kuo, et. al, “Architectural Optimization for a 1.82 Gbits/sec VLSI Implementation of the AES Rijndael Algorithm,” Proc. CHES2001, pp.53-67, 2001.

[3] T. Ichikawa, et. al, “Hardware Evaluation of the AES Finalists,” Proc. AES3, pp. 279-285, 2000.

[4] 市川 他, “128 ビットブロック暗号のハードウェア実装について(III)”,SCIS2001 予稿集, pp.669-674, 2001.

[5] M. Bean, et. al, “Hardware Performance Simulation of Round 2 Advanced Encryption Standard Algorithm,” http://csrc.nist.gov/encryption/aes/round2/NSA-AESfinalreport.pdf.

表1. 回路実装比較 (ワースト条件)

暗号方式	文献	サイクル数	CMOS Process (μm)	回路規模 (gates)	回路規模 (mm^2)	動作周波数 (MHz)	スループット (Mbps)	スループット/回路規模 (Kbps/gate)	備考
AES	本論文	54	0.11	6,479	0.062	93.5	222	34.20	回路規模優先
		54		9,142	0.088	200.0	474	51.86	動作速度優先
		32		11,419	0.131	200.0	800	70.06	
		21		13,189	0.143	200.0	1,219	92.43	
		11		18,378	0.199	200.0	2,327	126.63	
	[2]	11	0.18	173,000	3.96	47.6	435	2.51	復号化未実装
	[3]	11	0.35	33,850	-	-	510	15.06	
	[4]	1	0.35	612,834	-	15.23	1,950	3.18	11 段分実装
	[5]	11	0.5	68,872	20.74	21.18	271	3.94	回路規模優先
				160,421	33.85	47.36	606	3.78	動作速度優先
Triple-DES	本論文	48	0.11	5,273	0.051	250.0	333	63.22	回路規模優先
		48		9,536	0.092	434.8	580	60.82	動作速度優先
		24		13,053	0.125	294.1	784	60.08	2 段分実装
		12		17,140	0.165	181.8	970	56.57	4 段分実装