社団法人 情報処理学会 研究報告
IPSJ SIG Technical Reports

2007－ＳＬＤＭ－132（19）
2007／11／21

AESにおける合成体SubBytes向けパワーマスキング乗算回路の設計

川畑 伸幸† 奈良 竜太† 戸川 望† 柳澤 政生† 大附 辰夫†

† 早稲田大学大学院基幹理工学研究科 情報理工学専攻
〒169-8555 東京都新宿区新大久保3-4-1
Tel:03-5286-3396, Fax:03-3203-9184
E-mail: †kawahata@ohtsuki.comm.waseda.ac.jp

あらまし 共通鍵暗号規格の一つであるAESは主な利用方法の一つとしてICチップ等の組込み機器上での使用が挙げられる．第三者に対して共通鍵は知られてはならないが，暗号処理演算中に発する物理量を測定，解析して共通鍵を解読する攻撃法(サイドチャネルアタック)が考案されその危険性が指摘されている．中でも電力差分解析攻撃(DPA)は最も現実的かつ有力な攻撃方法として知られており，今後の攻撃手法として脅威になると予想されている．本稿では，AESの主な利用方法であるICチップ等の組込み機器上での使用を想定し，合成体理論を用いたAESのSubBytes処理回路に着目した．同一の演算に対してランダムに消費電力が返される拡大体演算回路を新たに提案し合成体SubBytes処理回路に対して適用することで，モジュールレベルでの合成体SubBytes回路に特化した小面積指向耐DPA設計をした．提案手法の実装をして評価及び結果を報告する．
キーワード 電力差分解析攻撃(DPA)，合成体，AES，ICチップ，組み込み機器

A power masking multiplier based on galois field for composite field AES

Nobuyuki KAWAHATA†, Ryuta NARA†, Nozomu TOGAWA†, Masao YANAGISAWA†, and Tatsuo OHTSUKI†

† Dept. of Computer Science and Engineering, Waseda University
3-4-1 Okubo, Shinjuku, Tokyo 169-8555, Japan
Tel:03-5286-3396, Fax:03-3203-9184
E-mail: †kawahata@ohtsuki.comm.waseda.ac.jp

Abstract AES is one of common key cryptosystems and mainly used on an embedded system, IC-chip and others, and the common key must not known by others. However the common key can be cracked by side channel attack(SCA). SCA, an attacking method of cracking common key by measuring and analyzing physical quantity at the encryption processing, is proposed and pointed as a dangerous for the security of AES. Especialy in SCA, the attacking method that is the most dangerous and realistic for security of AES is to be a deffirential power analysis(DPA). Hence against DPA, SubBytes circuit is needed to design as an anti-DPA. To design an anti-DPA SubBytes circuit, we propose a power masking multiplier based on galois field for composite field AES. With the multiplier, we design a circuit of inverse-element based on galois field for composite field and design SubBytes circuit oriented low area by using it. We report evaluation and result.
Key words Differential power analysis(DPA), Composite field, AES, IC-chip, Embeded system

1. まえがき

近年における情報化の進展速度は著しく，コンピュータを利用したシステムにより従来の文書的決済と同等の手続きを行う機会が増えてきた．それと同時に，第三者に対して機密情報をコンピュータを通してやり取りする機会が増加している．

現代では情報の記録や演算を行うための集積回路を積んだICチップ等の組込み機器が普及している．そして，重要なデータには暗号化処理が必須であるが，多くの暗号化処理は複雑な数学的理論に基づいているため暗号化処理に特化した専用HWを搭載したICチップ等の組込み機器が用いられており，暗号化処理に用いる秘密鍵が格納されている．

秘密鍵は第三者に知られてはならないが，ICチップ等の組込み機器内での暗号処理演算中に発する消費電力，熱，音などの物理量を測定，解析して秘密鍵を解読する方法が知られている．これを，サイドチャネルアタック (SCA) と呼ぶ．SCAは従来から既知であり，物理量の正確な測定手段が未成熟であったので脅威ではなかったが，近年の測定技術の進歩に伴い今後の攻撃手法として脅威となると予想される．その中でも最も脅威と考えられている手法が電力差分解析攻撃 (DPA) であり，DPAへの耐性を考慮した暗号処理回路の設計が必要である．特に暗号としてAES(Advanced Encryption Standard) が用いられることが多く，AES向け耐DPA設計が研究されている．

AES向け耐DPA設計では，消費電力とデータとの相関関係を無くす処理が必要となる．しかし無耐性の暗号処理回路と比較して面積，遅延，消費電力が大きくなってしまう．特にAESは，ICカードなど組込み系のシステムで多く用いられる為小面積指向での設計が必要となる．AES暗号処理モジュールの1つであるSubBytesではS-Box(注1)にて入力元 X の逆元 X^{-1} を導出するが，その為に X^{254} を求める必要があり，消費電力の6割を占めるので[4], [7]，DPAで最も狙われ易い処理部分である．その為DPA対策設計の殆どはSubBytesの逆元導出に対するものである．逆元導出の方法として，

（1） メモリ参照：全結果をテーブル化してメモリに格納．

（2） 論理回路：全結果をテーブル化して論理回路作成．

（3） 演算回路：逆元計算に特化した演算回路を作成．

が挙げられる．特徴として，(1)，(2)，(3) の順に面積が大きく，遅延は小さい．これらの逆元導出方法を用いた手法として，(2) の方法は文献[2]や汎用の論理自動合成で作られる一般的なS-Boxが知られている[6]．従来のDPAへの耐性を考慮したS-Boxの設計は，逆元導出の方法として (2) の方法を利用したものが多く，(3) の方法である演算回路を利用したものでは小面積で設計できる合成体理論を用いたものが知られているが全体としては多くない．AESの主な用途であるICチップ等の組込み機器上の利用を念頭に置けば，小面積で実現可能な演算回路を利用した耐DPA指向の回路設計が必要である．

逆元導出に演算回路を用いた耐DPA手法としてはプリミティブゲートレベル，モジュールレベルでの対策方法が知られている．プリミティブゲートレベルでは文献[8]，文献[10]，文献[11]等が知られている．これらはANDゲート自体にマスキングをかける手法であるが，文献[10]，文献[11]はハザードによって脆弱性が生じる可能性が文献[3]によって指摘されている．ハザード対策手法を導入したものが提案されているが[8]，回路設計の複雑化や初期化回路などによる回路規模の増大が問題として挙げられている．またプリミティブゲートレベルではライブラリレベルでの変更が必要な事から，リポジトリとしての再利用が困難であることが問題点である．モジュールレベルではユニットに対して対策をする文献[1]が挙げられ，一般的に回路規模の増大を招くという欠点がある一方で，DPA耐性が強く，ハザードの考慮が不要な事，RTLなので設計・拡張が容易であるという利点がある．

以上のような背景から本稿ではモジュールレベルにて小面積かつ強力なDPA耐性を持つSubBytesの提案をする．モジュールレベル対策の欠点である回路規模の増大化に対しては，小面積設計可能な事で知られている合成体理論[12]を導入し面積の増加を抑えている．合成体SubBytesに用いられる拡大体乗算において，ランダムに異なる消費電力が返されるような拡大体乗算回路を提案し，演算処理と消費電力の統計的解析による秘密鍵の解読を妨害するような合成体SubBytesを設計した．プリミティブゲートレベルでの合成体SubBytesは文献[8]があるが，ハザード対策が不要であること，設計・拡張の容易さの点において提案手法に優位性がある．

2. Differential Power Analysis(DPA)

2.1 DPA

DPAは暗号デバイス中の中間データのとあるbit値の予想値を基に解析する．測定した消費電力のデータを分類し，部分鍵を推定してそれと既知の暗号文から回路を辿ることで，bit値の予想値が得られる．この鍵の部分鍵と既知暗号文の情報からbit値の予想値を求める関数が選択関数 (式 (1)) である．

$$D := D(C, K_s) \in \{0, 1\} \quad (1)$$

C ： 出力された暗号文

K_s ： 推定した部分鍵 (AES の場合は $1bit$)

暗号デバイスに m 個の未知平文を入力し，消費電力 $T_1, T_2, ..., T_m$ と暗号文 $C_1, C_2, ..., C_m$ を得る．

$$D(C_i, K_s) = \left\{ \begin{array}{l} 0\ then\ T_i \text{をグループ} G_0 \text{に分類} \\ 1\ then\ T_i \text{をグループ} G_1 \text{に分類} \end{array} \right\} \quad (2)$$

以上のように消費電力を分類し，G_0，G_1 の消費電力の平均を A_0，A_1 とすると，式 (3),(4),(5) となる．

(注1)：本稿では8bitのSubBytes処理を行うモジュールをS-Boxと表記し，S-Boxを16回利用して入力ブロックをすべてS-Boxで処理できるようにしたモジュールをSubBytesと表記する．

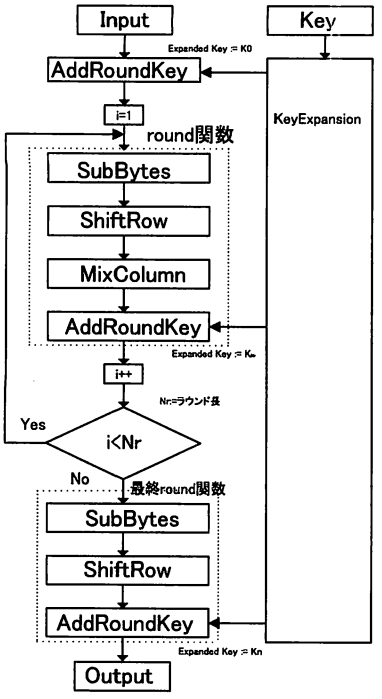


図 1　AES のラウンド構造.

Step1 K_s と対応する暗号文 C の排他的論理和を求める.
Step2 Step1 の値に対して逆 ShiftRow 変換を行う.
Step3 Step2 の値に対して逆 SubBytes 変換を行う.
Step4 Step3 の値の 1bit 目を出力とする.

図 2　最終ラウンドの選択関数.

$$A_0 = \frac{1}{|G_0|}\sum_{T_i \in G_0} T_i \tag{3}$$

$$A_1 = \frac{1}{|G_1|}\sum_{T_i \in G_1} T_i \tag{4}$$

$$\Delta P = A_0 - A_1 \tag{5}$$

$$(|G_0| + |G_1| = m)$$

K_s が正しければ ΔP は $D=0$ である時と $D=1$ である時の電力差となり，K_s が間違っていれば選択関数 D は 0 と 1 をほぼ同程度の確率で返す為 ΔP は 0 に近い微小な数値となる．この方法を使って部分鍵を全通り探索すれば鍵を全て解読できる.

2.2　AES への DPA

AES に対して DPA を仕掛ける場合の選択関数は対象とするラウンドによって変化する．AES は SubBytes にて消費電力の 6 割を占めるので，本稿では SubBytes に着目し出力値から選択関数を導出し易い最終ラウンド関数を対象とする．AES のラウンド構造を図 1 に示す.

2.3　AES の最終ラウンドに対する DPA の場合

図 1 中の最終ラウンドの SubBytes 処理に入力される値 (未知) から鍵の値を推定する場合を考える．鍵の内 8bit 分 (K_s と表記する) を 1 つの S-box への入力処理より解読する．この場合の関数 D は以下の処理より構成される．ただし，攻撃者は暗号化文 C を観測できるものとする．図 2 より，関数 D は式 (6) となる.

$$D = SubBytes^{-1}(ShiftRow^{-1}(AddRoundKey(K_s, C))) \oplus R_1 \ (R_i\text{は参照ビット}) \tag{6}$$

Step1 同型写像 δ を用いて $GF(2^8)$ の元を合成体 $GF(((2^2)^2)^2)$ へ写す.
Step2 $GF(((2^2)^2)^2)$ 上の逆元演算を $GF((2^2)^2)$ 上の逆元演算へ写す.
Step3 $GF((2^2)^2)$ 上の逆元演算を $GF(2^2)$ 上の逆元演算へ写す.
Step4 $GF(2^2)$ 上の逆元演算を $GF(2)$ 上の逆元演算へ写す.
Step5 Step2 から Step4 より $GF(((2^2)^2)^2)$ の逆元演算を $GF(2)$ の逆元演算として計算する.
Step5 同型写像 δ^{-1} を用いて Step4 の結果を $GF(2^8)$ へ戻す.

図 3　合成体を利用した逆元演算.

2.4　DPA からの防御

DPA は中間データと消費電力の相関関係から鍵を解読する手法であり，消費電力が大きく測定し易い SubBytes をターゲットとするのが一般的である．防御側は相関関係を減らす為ランダムな消費電力が得られるような S-Box を設計するのが一般的である.

3.　S-Box の設計

S-Box は 8bit の入力元の逆元を導出してアフィン変換をしたものである．アフィン変換は単純な $GF(2)$ 行列計算なので，逆元計算が重要となる.

3.1　逆元演算

AES の S-Box 内において，既約多項式 $f(x)$ は式 (7) であり，$f(x)$ を法とした拡大体 $GF(2^8)$ 上の逆元を求める.

$$f(x) = x^8 + x^4 + x^3 + x + 1 \tag{7}$$

$GF(2^8)$ では $X^{256} \equiv X$ が成り立つので逆元は $X^{-1} \equiv X^{254}$ で求まる．しかし，254 乗の回路規模を低減する為の工夫が必要となる.

3.2　合成体による逆元演算

合成体を用いた S-Box のアルゴリズムを図 3 に示す．合成体上においては，$GF(2^2)$ 乗算と $GF(2^2)$ 逆元演算を用いて $GF((2^2)^2)$ 乗算と $GF((2^2)^2)$ 逆元演算を求め，$GF((2^2)^2)$ 乗算と $GF((2^2)^2)$ 逆元演算を用いて $GF(((2^2)^2)^2)$ を求める．用いる合成体は式 (8),(9),(10) の基底と多項式基底の下で 2 次拡大を繰り返したものを用いる [5]．λ は MSB が 1 となる任意の 4bit の数，ϕ は MSB が 1 となる任意の 2bit の数で，回路規模が最も小さくなるのは $\lambda = 1100_2$，$\phi = 10_2$ である [5].

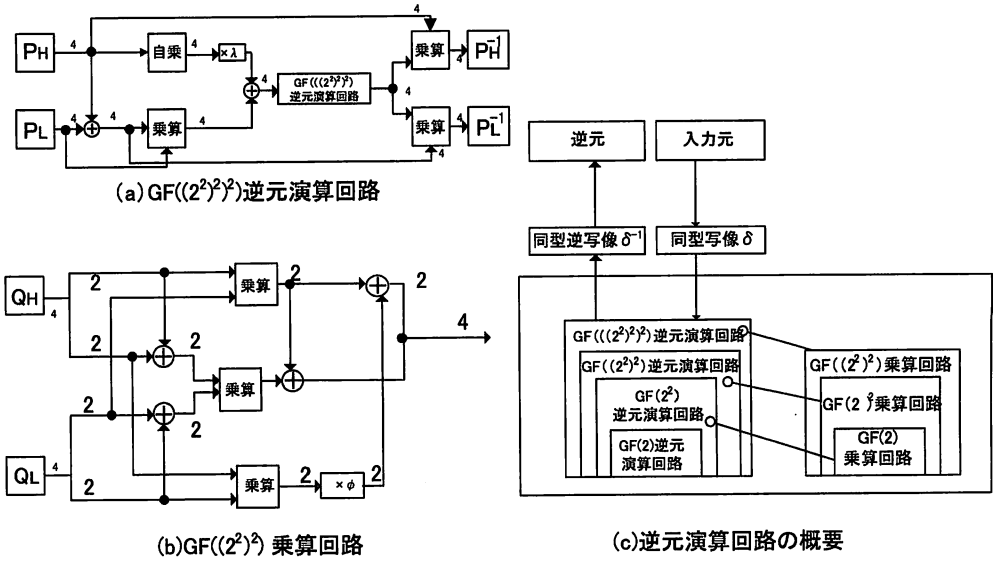


図 4　合成体を用いた $GF(2^8)$ 逆元演算回路の設計.

$$GF(2^2) : f(x) = x^2 + x + 1 \quad (8)$$

$$GF((2^2)^2) : f(x) = x^2 + x + \phi \quad (9)$$

$$GF(((2^2)^2)^2) : f(x) = x^2 + x + \lambda \quad (10)$$

$(\lambda = 1100_2 \ , \ \phi = 10_2)$

合成体による逆元演算回路の設計図を図 4 に示す．合成体 S-box は一般的なテーブル参照方式と比較して回路規模を低減できることが知られている [8]．遅延は大きくなる傾向にあるが，組み込み機器など大きな動作周波数を必要としない小面積指向の設計においては有用である．

4. パワーマスキング化した乗算回路の提案

SubBytes は DPA 対策指向の設計が求められている．DPA 対策指向設計は無対策の設計と比較して，面積，消費電力，遅延の増加は避けられない．本稿では IC チップなどの組み込み機器に搭載する AES 専用 HW を想定し，小面積の DPA 対策指向設計を目標とした合成体 SubBytes の設計に特化したパワーマスキング乗算回路を提案する．乗算を対象とした理由は，SubBytes モジュール中の演算は乗算が支配的である事が挙げられる．

4.1 パワーマスキング化した $GF(2^2)$ 乗算回路

合成体中の部分体 $GF(2^2)$ 上の乗算において，消費電力と演算の相関関係を無くすことで DPA への耐性を得るためにランダムに消費電力が返されるような乗算回路を設計する．

$GF(2^2)$ 上の乗算において，乗算の部分解がラッチを経由する場合とラッチを経由しない場合の 2 通りの出力を用意し，この 2 通りの出力をマルチプレクサで選択させる乗算回路を提案する．ラッチに対するクロックとマルチプレクサに対する選択制御信号を共通の乱数で入力する事で，同一の乗算に対してラッチ動作分の異なる電力が消費される．この乗算回路を図 6 に示す．また，提案 $GF(2^2)$ 乗算回路を利用して合成体 $GF((2^2)^2)$ 乗算回路，$GF(((2^2)^2)^2)$ 逆元演算回路を設計した (図 5)．ここで，本稿のパワー制御可能のランダム化可能な $GF(2^2)$ 乗算回路アーキテクチャは，文献 [1] の Benini 手法と異なる事を述べておく．Benini 手法で演算回路を設計する場合はパワーをランダム化するために基本の演算回路分もコピーする必要があるので面積の増加を招く．一方で，本稿のアーキテクチャにおいては余剰要素を利用しないで幾つかの制御要素を利用するのみなので面積の増加を抑えている．

4.2 $GF((2^2)^2)$ 逆元演算

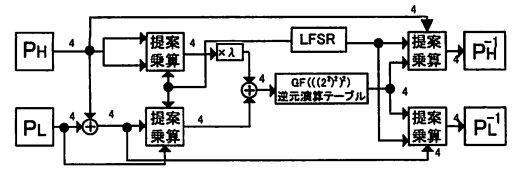
部分体 $GF((2^2)^2)$ 逆元演算回路を $GF(((2^2)^2)^2)$ 逆元演算回路に組み込んだ場合に提案手法を用いると構造的に提案 $GF((2^2)^2)$ 乗算回路が並列ではないので遅延の増加が避けられない．よって，$GF((2^2)^2)$ 逆元演算回路は無耐性にて実装した．

論理合成結果 (表 1) より $GF((2^2)^2)$ 逆元演算は合成体で設計するより予め元と逆元の対応関係をテーブル化した方が面積・遅延ともに優れていることが分かった．演算回路の設計にはハードウェア記述言語の一つである Verilog-HDL を使用し，Synopsys 社の Design Compilier Z-2007.03-SP4 を用いて制約無しの論理合成を行った．また，セルライブラリには STARC (注2) (90[nm]) の設計ルールを用いた．この結果を踏まえて $GF(((2^2)^2)^2)$ 逆元演算回路に用いる $GF((2^2)^2)$ 逆元演算はテーブル化した．

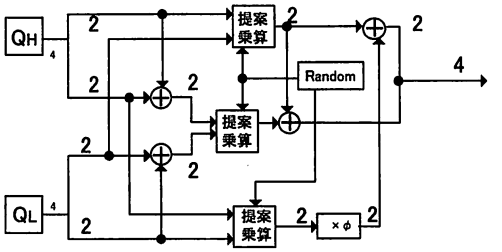
4.3 提案 $GF((2^2)^2)$ 乗算回路を用いた $GF(((2^2)^2)^2)$ 逆元演算回路

提案 $GF(2^2)$ 乗算回路を利用して $GF(((2^2)^2)^2)$ 逆元演算回

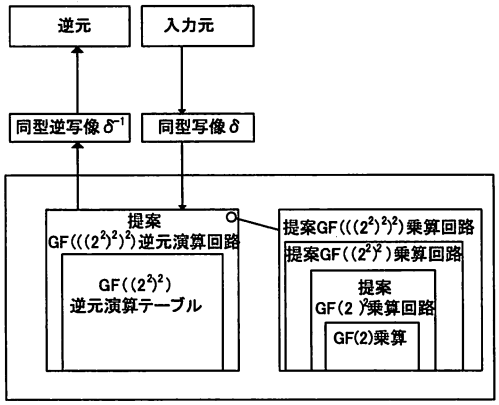
(注2)：STARC[90nm] ライブラリは東京大学大規模集積システム設計教育研究センターを通し，株式会社半導体理工研究センター (STARC) の協力で開発されたものである．



(a)提案GF(((2²)²)²)逆元演算回路



(b)提案GF((2²)²) 乗算回路



(c)提案逆元演算回路の概要

図 5　提案する $GF((2^2)^2)$ 乗算回路，$GF(((2^2)^2)^2)$ 逆元演算回路.

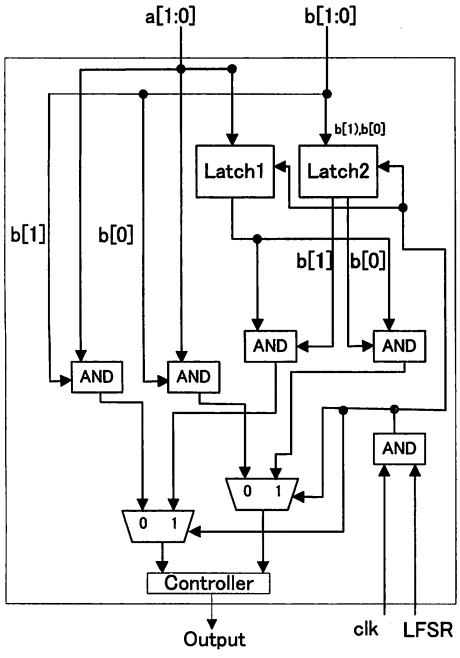


図 6　提案する $GF(2^2)$ 乗算回路.

路を設計した．乱数の発生には 8bitLFSR を利用した．合成体 $GF(((2^2)^2)^2)$ 逆元演算回路の設計に必要な各モジュールは，$GF((2^2)^2)$ 乗算回路は $\lambda = 1100_2$ で設計した提案乗算回路である．$GF((2^2)^2)$ 逆元演算は予め元と逆元の対応関係をテーブル化した論理回路である．そして $GF(((2^2)^2)^2)$ 逆元演算回路は外部から LFSR による乱数が入力されるようにした．提案乗算回路毎に LFSR を割り当てると面積の増大を招く為，LFSR

表 1　$GF((2^2)^2)$ 逆元演算.

実装方法	対 DPA	面積 [μm^2]	遅延 [ns]
提案手法を用いた合成体演算回路	○	980	0.72
合成体演算回路	×	240	0.43
テーブル化	×	132	0.15

を逆元演算回路上に 1 つのみ使用して面積を低減させた.

5. 評　　価

提案乗算回路を用いて設計した逆元演算回路を用いて S-Box を設計，実装した．図 7 のように S-Box は S-Box^{-1} と回路を共有させて作成した．アフィン変換と同型写像は通常の $GF(2)$ 行列計算なので，逆アフィン変換と同型写像，同型逆写像とアフィン変換が連続する箇所は予め計算しておいて 1 つの演算モジュールにすることで面積を低減できる．逆元演算回路と S-Box は Verilog-HDL を用いて実装し論理合成をした．セルライブラリには STARC(90[nm]) の設計ルールを用いた.

5.1 面　　積

一般的な無耐性テーブル逆元演算，耐性 BBD テーブル逆元演算 [2]，無耐性合成体逆元演算 [5]，及び本手法との結果を比較した結果を表 2 に示す．本手法と比較した場合，本手法のゲート数は無耐性テーブル逆元演算の約 1.59 倍，耐性 BBD

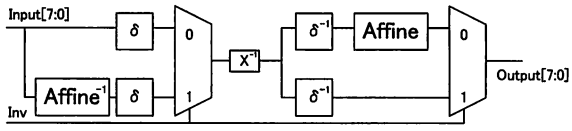


図 7　S-Box の構造図.

表 2 論理合成結果.

実装方法	Technology	DPA 対策	Area[μm^2]	gate	delay[ns]
テーブル化 S-Box	90nmCMOS	×	2552	638	0.44
BBD S-Box [2]	180nm HCMOS	○	13066	1111(注3)	–
合成体 S-box [5]	130nm CMOS	×	–	354	2.19
Ours	90nmCMOS	○	4067	1017	2.26

S-Box [2] の約 0.92 倍，無耐性合成体逆元演算 [5] の約 2.87 倍となった．提案 S-Box には 12 個の提案乗算回路が搭載されているので，提案乗算回路の個数と引き換えにこれより面積を小さくすることも可能である．

5.2 遅　　延

演算回路を用いた場合はテーブルを用いた場合よりも遅延は大きくなる傾向があり，提案手法が最も遅延が大きくなった．無耐性合成体逆元演算 [5] と比較して約 3% の遅延増加に抑えられた理由は，部分体 $GF((2^2)^2)$ 逆元演算のテーブル化，および提案乗算回路を構造的に並列に設置した事が挙げられる．本稿では IC チップなどの組み込み機器上での使用を想定しており高速な動作周波数は求められない事から十分である．

5.3 DPA への耐性

図 6，図 5 のアーキテクチャでは，ラッチの制御が各クロックサイクル毎にランダム化されている．これによって，入力の被乗数と乗数の同値に対して異なった消費電力が返されることになる．攻撃者はラッチの存在を推定したとしても一様な消費電力が測定できないので消費電力を正しく解析する事ができない．LFSR の遷移確率を P とする．S-Box1 つあたり提案乗算回路が 12 個搭載されており，SubBytes には S-Box が 16 個搭載されているので，P=$\frac{1}{2}$ とすれば 1 つの平文に対する消費電力の発生の仕方は $(2^{12})^{16}=2^{192} \approx 10^{58}$ 通りとなるので解析を妨害できる．

6. む　す　び

本稿では，IC チップ等の組込み機器における AES の利用を想定し DPA 耐性を持つ暗号処理回路の設計をした．ランダムに消費電力が返される合成体演算回路を新たに提案した．計算機上で論理合成した結果，面積は DPA 耐性を持つ既存 S-Box 構成手法 [2] と比較して約 8% 小さく，遅延は DPA 耐性を持たない合成体手法 [5] と比較して約 3% の増加に抑えられた．また，本手法は RTL で扱う事ができるので，ゲートレベルで扱っている文献 [8] と比較して設計や拡張の点において優位性がある．今後の方針としては消費電力の実測による DPA 耐性の検証が挙げられる．

文　　献

[1] L. Benini, E. Omerbegovic, A. Macii, M. Poncino, E. Macci and F. Pro, "Energy-aware design techniques for differential power analysis protection," in *Proceedings of the 40th Design Automation Conference(DAC 2003)*, pp. 36–41, Jun 2003.

[2] M. Giaconia, M. Macchett, F. Regazzoni, and K. Schramm, "Area and power efficient synthesis of DPA-resistant cryptographic S-boxes," in *Proceedings of 20th International Conference on VLSI Design*, pp. 731–737, Jan 2007.

[3] 市川哲哉，鈴木大輔，佐伯稔，"データマスクを利用した DPA 対策に対する攻撃，" CSEC 2004，pp. 313–320，Jul 2004.

[4] S.Mangard, "Hardware countermeasures against DPA - a statistical analysis of their effectiveness, " in *Topics in Cryptology - CT- RSA 2004*, Lecture Notes in Computer Science, vol.2964, pp .222–235, Feb 2004.

[5] 森岡澄夫，佐藤証，高野光司，宗藤誠治，"$GF(((2^2)^2)^2)$ 上の演算を用いた AES の S-Box 構成法，" 情報処理学会第 63 回全国大会，3G-4，Sep 2001.

[6] 森岡澄夫，佐藤証，"共通鍵暗号 AES の低消費電力論理回路構成法，" 情報処理学会論文誌，vol.44，No.5，pp. 1321–1328，May 2003.

[7] 森岡澄夫，システム LSI 設計における DPA 対策の指針と AES 暗号の対策例，Design wave magazine，pp. 125–134，Feb 2006.

[8] 佐々木稔，岩井啓輔，黒川恭一，"AES の S-box 回路の DPA 対策設計，" 信学技報，Reconf2006-44，vol.106，No.394，pp. 1–6，Nov 2006.

[9] STMicroelectronics, CB65000 Series, `http://www.ortodoxism.ro/datasheets/stmicroelectronics/8642.pdf`

[10] 鈴木大輔，佐伯稔，市川哲哉，"遷移確率を考慮した DPA 対策手法の提案，" 信学技報，ISEC2004–59，vol.104，No.200，pp. 127–134，Nov 2006.

[11] E, Trichina, "Combinational logic design for AES SubByte transformation on masked data, " International Association for Cryptologic Research, Cryptology eprint archive Report 2003/236, Nov 2003.

[12] 和田知久，共通かぎブロック暗号 AES 用 SubBytes 変換回路設計のポイント，Design wave magazine，pp. 92–99，Jun 2004.

[13] J.Waddle and D.Wagner, "Towards efficient seconde-order power analysis," *CHES2004*, Lecture Notes in Computer Science, vol.3156,pp. 1–15, Sep 2004.

(注3)：文献 [2] の gate 数は文献 [9] 中に記載されている 0.18μm HCMOS8D Technology の gate density より算出した．