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

2008－SLDM－137 (11)
2008 / 11 / 17

クロスバスイッチを用いたS-Box切替による AES暗号処理回路のパワーマスキング手法

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 は専用処理ハードウェアが搭載された IC チップ等の組込み機器上での使用例が多く，格納された共通鍵は外部に対して秘密であることが前提とされている．しかし，暗号処理演算中に発生する物理量を解析して共通鍵を解読するサイドチャネル攻撃と呼ばれる攻撃法が提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) は最も危険性が懸念されている攻撃法の一つであり，DPA への耐性を考慮した専用ハードウェアの設計が要求されている．本稿では，AES の SubBytes 処理にて複数の S-Box 回路を用いて並列処理させる場合に，クロスバスイッチを用いて消費電力の異なる複数の S-Box をランダムで切り替え消費電力を攪拌する手法を提案する．提案手法の実装をして評価および結果を報告する．

キーワード 電力差分解析攻撃，DPA，クロスバスイッチ, AES，IC チップ，組み込み機器

A Power Masking Method of AES Circuit by Using Cross Bar Switch to Switch S-Box Circuit.

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 the common key cryptosystems often used on an embedded systems, IC-chips and others. Teir common key must be kept secret from others. However, it can be deciphered by side channel attack, the method of cracking cryptosystems by analyzing physical quantity generated at the encryption processing. Especially in side channel attack, differential power analysis(DPA) is known as the most dangerous attacking method. AES circuit is needed to be designd with regard to anti-DPA. To design an anti-DPA AES circuit, we propose a power masking SubBytes circuit which switches several S-Boxes, each of which has a different power to each other. We demonstrate our evaluation and results.

Key words Differential power analysis, DPA, Cross bar switch, AES, IC-chip, Embeded system

1. まえがき

近年，情報化の急激な進展により，コンピュータを用いて金銭取引などの重要な情報処理をオンライン上でやりとりする機会が増加している．重要情報は外部漏洩防止のため暗号化してやりとりする必要がある．暗号処理の多くは複雑な数学的理論に基いているため暗号処理専用ハードウェアを搭載したICチップ等の組込み機器が用いられており，暗号処理に用いる秘密鍵を格納している．秘密鍵は外部に対して秘匿する必要があるが，暗号処理時にLSIから生じる消費電力，電磁波，熱，そして音などの物理量を測定，解析して秘密鍵を解読される脆弱性が指摘されており，これサイドチャネル攻撃と呼ぶ．サイドチャネル攻撃は理論上は脅威とされたが，物理量の正確な測定手段が未成熟であったため現実的には脅威とされなかった．しかし，近年の測定技術の進歩に伴い精密な物理量測定が可能となり，今後の攻撃手法として脅威となると予想される．中でも最も現実的な脅威と認識される攻撃法が電力差分解析攻撃(DPA) [6] 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．ICチップ等の組込み機器は暗号処理規格としてAES(Advanced Encryption Standard) が用いられることが多く，本稿では，DPAに耐性を持つAES暗号処理回路の設計を目指す．

AES暗号処理回路の耐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され，消費電力を攪拌する手法が提案されている．しかし無耐性で設計された暗号処理回路と比較して面積，遅延，消費電力は大きくなる．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．S-BoxはGF(2^8)上の数を扱うので，$X^{256} \equiv X$となり，X^{-1}の導出にはX^{254}を導出する必要がある．よってこの導出の処理負荷が重くなり，消費電力の約6割を占める [7], [9]．よってDPA対策設計の殆どはSubBytesの工夫であり，耐DPA指向かつ面積，遅延，消費電力の増加を極力抑える必要がある．特にAESは，ICカードなど組込みシステムで多く用いられるため小面積指向での設計を重視する．

S-Boxの逆元導出は

（1） メモリ参照：全結果をテーブル化してメモリに格納．

（2） テーブル回路：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．演算回路の利用が最も小面積で実現できる．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，既存の演算回路に用いるプリミティブゲートを改造する文献 [10], [11], [12] 等の手法がある．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 [11], [12] はハザードによって脆弱性が生じる可能性が文献 [4] 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 [10]，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，設計の非容易性が問題である．モジュールレベルでは，文献 [5] の演算回路モジュール自体の耐DPA指向設計，そして文献 [1], [9] にて紹介されている複数の処理モジュール切替による耐DPA指向設計が挙げられる．文献 [1] の手法はS-Boxを対象としていないがS-Boxにも適用できる．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，ハザードの影響が深刻ではなく，RTLなので設計・拡張が容易であるという利点がある．また，後者はSubBytes処理回路内のユニット切替に依拠するので既存のS-Boxが利用できるというメリットがある．

以上のような背景から本稿では，プリミティブゲートレベルに見られる回路規模の抑制とモジュールレベルに見られる設計容易性を同時に満たし，DPA耐性を持つSubBytes処理回路を提案する．文献 [1], [9] の手法をSubBytes処理回路に用いると1入力に対して消費電力が異なるn個のS-Boxを用意して1つをランダムに選ぶ回路になるが，これは入力数のn倍のS-Boxが必要となり回路規模の増大化を招く．本稿は，n入力に対して消費電力が異なるn個のS-Boxを用意して，乱数発生回路とクロスバスイッチを用いて各1入力に対して1つのS-Boxを割り当てた．これは入力数と同数のS-Boxのみが必要なので回路規模の増大化を抑える．回路規模の増大化を抑えつつ消費電力の攪拌を実現させた点で，本手法に優位性がある．

2. Differential Power Analysis (DPA)

DPAは暗号デバイス中の中間データのあるbit値の予想値を基に秘密鍵を解析する．測定した消費電力データを分類し，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．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．

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

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．

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

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．

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

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

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

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

(注1)：本稿では8bitのSubBytes処理モジュールを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．

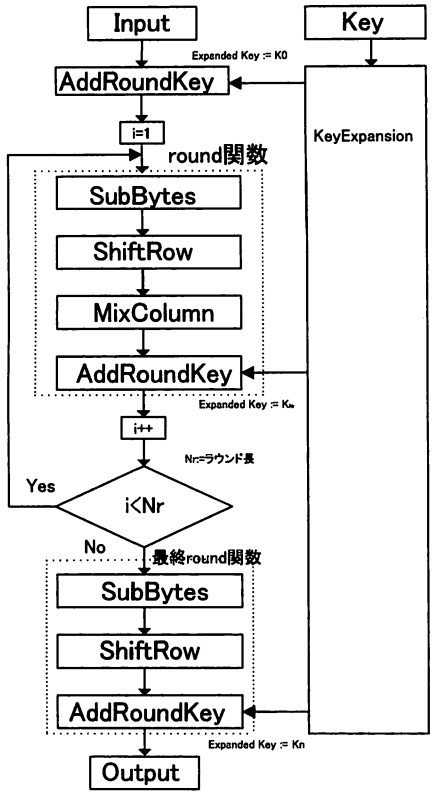

図 1 AES のラウンド構造.

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.

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ため 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．この理論は一次 DPA(First-order DPA) と呼ばれる．その他の電力解析手法としては，二次 DPA [13]，三次 DPA [3] が知られている．

2.1 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，最終ラウンド関数が対象とされやすい．AES のラウンド構造を図 1 に示す． 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 を観測可能で，平文は観測できないとする．図 2 より，関数 D は式 (6) となる．

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

2.2 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る．SubBytes は AES 全体の消費電力の 6 割を占めるので消費電力が大きい 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ため消費電力を攪拌できるような S-Box を設計するのが一般的である．ただし，無体策の S-Box と比較すると必ず回路面積，遅延，消費電力の増加を招く．故に，これらのオーバヘッドを抑えつつ電力攪拌をする必要がある．

2.3 電力相関係数

本稿で評価に用いる電力相関係数について説明する．電力相関係数とは，推定消費電力の分布と測定消費電力の分布との相関関係を指標とする評価係数である．

一般的に 2 変数 X,Y における相関係数 ρ は，2 変数の共分散 $cov(X,Y)$ と標準偏差 σ_X ,σ_Y により式 7 で定義される．

$$\rho(X,Y) = \frac{cov(X,Y)}{\sigma_X \sigma_Y} \quad (7)$$

式 7 を用いて推定消費電力サンプル H と測定消費電力サンプル Q との共分散，標準偏差を用いて電力相関係数が定義できる．

$$\rho(H,Q) = \frac{cov(H,Q)}{\sigma_H \sigma_Q} \quad (8)$$

また，電力相関係数の最大値である最大電力相関係数 ρ_{max} が評価指標として定義されている [7].

$$\rho_{max}(H,Q) = \frac{\rho(H,Q)}{\sqrt{1+\frac{1}{SNR}}} \quad (9)$$

SNR(Signal to Noise ratio) は回路の遷移などにより決定される雑音定数である．これらの相関係数が小さいほど電力差分解析攻撃に耐性を持つ.

3. クロスバスイッチを用いた消費電力攪拌手法

Benini [1]，森岡 [9] は一入力に対して消費電力が異なる 2 つのユニットを割り当てランダムで切り替えて消費電力を攪拌させる手法について提案，言及している. [1], [9] に基づいて作った S-Box を図 3 に示す．図 3 のように [1] に基いて SubBytes を設計する手法を Benini 手法と呼ぶ．しかし [1] は AES での利用に関しては触れておらず, [9] は AES で用いられていないとしている．既存手法では n 入力に対して 2n 個の S-Box を必要とするため回路規模の増大化を招く．そこで，回路規模の増大化を抑えた S-Box 切り替えによる消費電力の攪拌手法を提案する.

3.1 提案回路の構成

SubBytes は S-Box4 つの集合体からなる 32bit の提案回路により実現させる．提案回路の 32bit の入力値は入力後にクロスバスイッチによって 8bit ずつランダムに，互いに異なる 4 つ

表 1　n 入力のクロスバスイッチに必要な面積比較.

入力数 n	n 入力クロスバ [gate]	切り替え [通り]	面積/入力 [gate/通り]	面積/切り替え [gate/通り]
1	0	1	0	0
2	19	2	9.50	9.50
3	97	6	16.17	32.33
4	239	24	9.96	59.75
5	694	120	11.57	138.80

の S-Box のいずれかに一対一対応で割り当てられ処理される．処理後はクロスバスイッチと逆の処理をして元のビット箇所に戻す．ランダムな割り当ての実現には乱数を利用する．乱数生成はフィードバック長 8bit の LFSR を利用し，5bit からなる切り替え信号は入力値と LFSR の出力値との排他的論理和からなる簡単な計算により生成する．これにより，図 3 の Benini 手法と比較して無駄な S-Box の数を減らし面積のオーバヘッドを防ぐ．

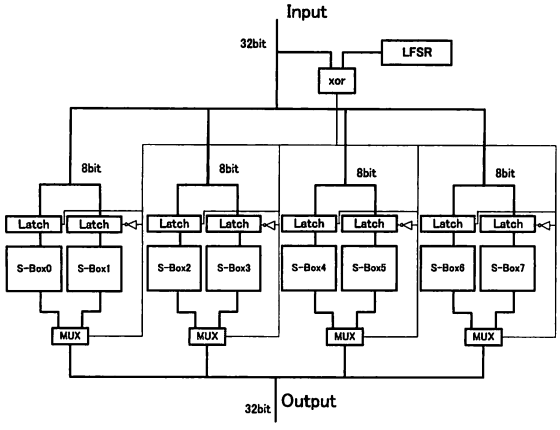

図 3　Benini 手法 [1] による S-Box 切り替え手法.

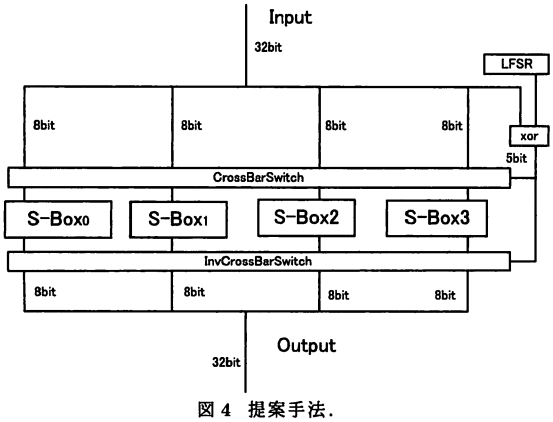

図 4　提案手法.

3.2　S-Box の個数

提案回路を S-Box4 つの集合体とした．これはクロスバスイッチの面積オーバヘッドの減少と AES の並列性の維持のためである．提案回路で用いる n 入力のクロスバスイッチ，逆クロスバスイッチは $n!$ 通りの切り替えを実現させるので全てを網羅した回路設計においてこの部分が面積オーバヘッドとなる．

クロスバスイッチ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 を用いてトポグラフィカルモード，遅延制約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．入力に対する面積，切り替えの組合せ，面積/入力，面積/切り替えの値を表 1 に示す．実際は対応する逆クロスバスイッチも必要なので表 1 の約 2 倍の回路面積が必要となる．表 1 では，入力数を n とすると $n \geqq 5$ において面積が急増している点，AES の 8bit 処理の並列性の維持を考慮して $n = 4$ を用いる．

3.3　異なる消費電力の S-Box

図 3 のクロスバ S-Box において異なる消費電力の 4 つの S-box として，合成体実装 [8]，テーブル実装の 2 種類を 2 つずつ用いた．合成体実装の S-Box2 つは各々

- 同型写像と $GF(((2^2)^2)^2)$ 逆元演算と逆同型写像とアフィン変換
- 同型写像と $GF(((2^2)^2)^2)$ 逆元演算と逆同型アフィン変換

により実装した．ここで，逆同型アフィン変換とは逆同型射影とアフィン変換を 1 回の射影演算で実施する回路である．

また，テーブル実装の S-Box2 つは各々

- $GF(2^8)$ 逆元テーブルとアフィン変換
- S-Box 全体のテーブル

により実装した．実装結果を表 2 に示す．提案するクロスバ S-Box に合成体 S-Box とテーブル S-Box を 2 つずつ搭載した回路を思索し，Synopsys 社の PrimeTime PX Z-2006.12-SP3 を用いて消費電力をシミュレートして得た値を割合化したものを図 5 に示す．本手法で用いるテーブル S-Box と合成体 S-Box は並列構造となり同一の動作周波数で動作させると，平均消費電力比は 1:4 程度となる．SubBytes は AES の消費電力全体の 6 割を占めるので，合成体 S-Box は AES の消費電力全体の約 4 割となり，電力攪拌のための電力幅が大きくなる．

(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．

表 2 各 S-Box の回路種類，面積，遅延値.

	回路構成	回路種類	面積 [gate]	遅延 [ns]
合成体 1	同型射影+合成体+逆同型アフィン変換	演算回路	945	2.49
合成体 2	同型射影+合成体+逆同型射影+アフィン変換	演算回路	942	3.28
テーブル 1	逆元テーブル+アフィン変換	テーブル回路	1970	1.29
テーブル 2	S-Box 全体テーブル化	テーブル回路	2866	1.16

表 3 実装した SubBytes の比較

SubBytes の構成	全 S-Box	合成体 1	合成体 2	テーブル 1	テーブル 2	面積 [gate]	遅延 [ns]	平均消費電力 [mW]
無耐性合成体 SubBytes	16	16	0	0	0	15172	3.40	10.17
無耐性テーブル SubBytes	16	0	0	16	0	31520	1.29	2.23
Benini 手法 [1]SubBytes	32	16	0	16	0	49120(1)	2.65(1)	11.44(1)
提案手法 SubBytes	16	4	4	4	4	29056(0.59)	4.49(1.69)	7.48(0.65)

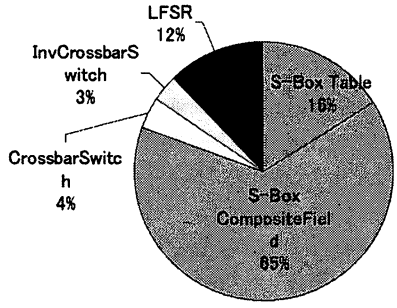

図 5 消費電力割合の比較.

4. 提案手法の評価

本手法は，面積比較，消費電力比較，電力相関係数の減少量を基に評価する．シミュレーションに用いる AES 暗号処理専用ハードウェアは，1 ラウンドを 1 クロックで処理し，その結果を逐次レジスタに書き込んでいくものにした．ただし，第 1 ラウンド前の AddRoundKey は第 1 ラウンドと同一サイクルで実施する．

回路の設計には Verilog-HDL を使用し，Synopsys 社の Design Compilier Z-2007.03-SP4 を用いてトポグラフィカルモード，遅延制約の論理合成を行った．また，セルライブラリには STARC (90[nm]) の設計ルールを用いた．回路動作のシミュレーションには Synopsys 社の VCS-NX Y-2006.06 を，消費電力の測定には Synopsys 社の PrimeTime PX Z-2006.12-SP3 を用いた．電圧は 1[V]，動作周波数は 166.67[MHz] とした．それぞれの回路は，

（1） 無耐性テーブル SubBytes：テーブル 1 のみで構成
（2） 無耐性合成体 SubBytes：合成体 1 のみで構成
（3） Benini 手法：テーブル 1 と合成体 1 で構成
（4） 提案手法：テーブル 1，2，3，4 で構成

として各々を比較と評価する．

4.1 面積，消費電力比較

比較のため，4 通りの SubBytes を構成した．表 2 中の合成体無耐性テーブル SubBytes，無耐性合成体 SubBytes，Benini 手法 SubBytes，提案手法 SubBytes について，各種 S-Box を 16 並列化して設計した．各 SubBytes 処理回路の全 S-Box 数，テーブル S-Box 数，合成体回路 S-Box 数，面積，遅延，平均消費電力の値を表 3 に示す．平均消費電力は 1 ラウンド中の SubBytes 部分の消費電力を計測した．Benini 手法 [1]SubBytes と比較して提案手法は面積を約 40%，平均消費電力を約 35%，低減しており，これらの点で優位である．

4.2 電力攪拌の評価

比較のため，AES 処理専用ハードウェア上に無耐性テーブル SubBytes，無耐性合成体 SubBytes，Benini 手法 SubBytes，提案手法 SubBytes をそれぞれ搭載して消費電力を測定した．入力データと秘密鍵は無作為に決定した 128bit の値とする．全ての回路に対して同一の入力，同一の秘密鍵を与えて比較する．電力サンプルの取得には PrimeTime PX のシミュレートを用いた．電力サンプルは 11 ラウンドの処理に要した消費電力の合計とする．電力攪拌は式 (7) の相関係数を用いて評価する．

ここで H は無耐性テーブルまたは無耐性合成体で実装した SubBytes を組み込んだ AES 暗号処理ハードウェアの消費電力，Q は Benini 手法及び提案手法を組み込んだ AES 暗号処理ハードウェアのそれぞれの消費電力とする．H は内部アーキテクチャにおけるハミング距離から推定する手法 [2] もあるが，本稿では同一の入力列に対して一様な消費電力分布を返す電力サンプル群を H，同一の入力列に対して攪拌された消費電力分布を返す電力サンプル群を Q とし，無対策の場合とそれに DPA 対策を加えた場合を比較して電力を攪拌できている度合いとして相関係数を導出した．

それぞれの値を表 4，表 5 に示す．ここで，$\Delta Area$ は消費電力攪拌手法によって生じた面積オーバヘッド，ρ は相関係数，$\Delta\rho$ は消費電力攪拌手法に拠る電力相関係数減少値，$\frac{\Delta\rho}{Area}$ は DPA 対策にて生じた面積オーバヘッドあたりの相関係数減少値を表す．Benini 手法，提案手法ともに電力相関係数は減少している．Benini 手法，提案手法を比較すると，相関係数は提案手法が上回る．

しかし，電力攪拌設計で生じた面積オーバヘッドと比較すると，表 4 では単位面積あたりの相関係数削減量は提案手法が Benini 手法よりも優位である．表 5 では提案手法は負の値なので Benini 手法よりも優位である．よって，面積効率を考慮した DPA 対策指向設計をする場合は本手法に優位性がある．

表 4 無耐性合成体 SubBytes を基準とした電力相関係数の評価.

	無耐性合成体	Benini 手法 [1]	提案手法
ΔArea[gate]	0	34334	13884
$\rho(H,Q)$	0.9849	0.1653	0.5735
$\Delta\rho$	0	0.8195	0.4113
$\frac{\Delta\rho}{Area}[gate^{-1}]$	not defined	2.3869E-5	2.9627E-5

表 5 無耐性テーブル SubBytes を基準とした電力相関係数の評価.

	無耐性テーブル	Benini 手法 [1]	提案手法
ΔArea[gate]	0	17986	-2464
$\rho(H,Q)$	0.9849	0.0273	0.3202
$\Delta\rho$	0	0.9575	0.6646
$\frac{\Delta\rho}{Area}[gate^{-1}]$	not defined	5.3236E-5	-26.9739E-5

5. むすび

本稿では，クロスバスイッチを用いた S-Box 切り替えによる消費電力撹拌手法を提案し AES 専用ハードウェア上に実装して計算機上でシミュレーションをした結果を基に評価をした．本手法は既存手法と比較して面積は消費電力，及び電力撹拌に伴って生じる面積オーバヘッドの効率を考慮した場合に優位性がある．今後の課題としては，相関係数の検討，面積を考慮しない有効性の実証，nth-oder-DPA などの実攻撃に対する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] Eric Brier, Christophe Clavier, and Francis Olivier, "Correlation Power Anaysis with a Leakage Model," *CHES2004*, Lecture Notes in Computer Science, vol.3156,pp. 16–29, Sep 2004.

[3] Catherine H. Gebotys, "A Table Masking Countrmeasure for Low-energy Secure Embedded System, " in *IEEE TRANSACTONS ON VERY LARGE SCALE INTEGRATION SYSTEMS*, July 2006.

[4] 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.

[5] 川畑伸幸, 奈良竜太, 戸川望, 柳澤政生, 大附辰夫, "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," 信学技報, Vol. 107, No.335, pp.37–42, 2007.

[6] P.C. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in *Proc. 19th Annual International Cryptology Conference on Advances in Cryptology* , pp. 388–397, Aug 1999.

[7] 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.

[8] 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.

[9] 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.

[10] 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.

[11] 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.

[12] 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.

[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.