推薦論文

共通鍵暗号 AES の低消費電力論理回路構成法

森岡澄夫[†] 佐藤証[†]

次期米国標準の 128 ビット共通鍵ブロック暗号 AES において，論理設計の工夫によって回路の消費電力を減らす方法を検討した．今回筆者らが行った調査では，AES の消費電力の大半を S-Box と呼ばれる非線形変換を行う組合せ回路が占めており，S-Box の消費電力は回路中を伝播するダイナミックハザードの量で決まる．本稿では，消費電力の少ない S-Box の論理回路構成法（multi-stage PPRM）を提案する．その方法では，合成体上で演算を行うことによって回路規模を減らすとともに，二段論理を何ステージか直列につなげることによって，各ゲートへの信号到達時間を揃えハザード発生を減らす．この結果，これまで知られている S-Box 回路と比べて半分から 3 分の 1 以下の消費電力を達成した．本手法は，S-Box にガロア体の逆元演算を用いたその他多くの共通鍵暗号回路にも有効である．

A Logic Design Methodology of Low-power AES Cryptographic Circuits

Sumio Morioka[†] and Akashi Satoh[†]

Reducing the power consumption of AES circuits is a critical problem when the circuits are used in low power embedded systems. We found the S-Boxes consume much of the total AES circuit power and the power for an S-Box is mostly determined by the number of dynamic hazards. In this paper, we propose a low-power S-Box circuit architecture: a multi-stage PPRM architecture. In this S-Box, (i) arithmetic operations are peformed over a composite field in order to reduce the total circuit size, and (ii) each arithmetic operation over sub-fields of the composite field is implemented as PPRM logic (AND-XOR logic) in order to reduce the generation and propagation of dynamic hazards. Low power consumptions of 29 μW at 10 MHz using 0.13 μm 1.5 V CMOS technology were achieved, while the consumptions of the conventional S-Boxes are two or more times larger. The proposed method is effective in the other common-key ciphers whose S-Boxes use Galois field inversion.

1. はじめに

DES（Data Encryption Standard）が共通鍵暗号のデファクトスタンダードとして 20 年以上用いられてきたが，2001 年に，NIST（National Institute of Standards and Technology）によって Rijndael が次期米国標準の 128 ビット共通鍵ブロック暗号 AES（Advanced Encryption Standard）[1),2)]に選定された．AES の回路実装においては，速度や回路規模はもちろんのこと，消費電力化も重要な最適化項目である．とくに，AES を組み込み用途や高速通信用途[3)]に利用する場合には，消費電力に対する制約が厳しくなる．しかし，AES の回路アーキテクチャや回路性能について近年多くの報告がなされているものの[3)~7)]，低消費電力化についての研究はいまだほとんどなされていない．

一般に，回路の低消費電力化のためには，システムレベルからトランジスタレベルに至るさまざまな設計抽象レベルで工夫が可能である[8)]．本稿では，CMOS デバイスの使用を前提とし，ゲートレベルにおける論理設計の工夫で消費電力を減少させることを考える．このレベルに着目した理由は次のとおりである．まず，先述のような用途では，使用できるテクノロジライブラリがあらかじめ決定されていることが多いので，ゲートレベルより下位の設計レベル（トランジスタレベルなど）での低消費電力化は難しい．また，スループットやクロック周波数に対する要求があらかじめ与えられる場合が多く，そのもとではビヘイビア（アルゴリズム）や回路アーキテクチャなど上位設計レベル

† 日本アイ・ビー・エム株式会社東京基礎研究所
IBM Research, Tokyo Research Laboratory, IBM Japan Ltd.

本論文の内容は 2001 年 10 月のコンピュータセキュリティシンポジウム 2001 にて報告され，CSEC 研究会主査により情報処理学会論文誌への掲載が推薦された論文である．

での工夫も難しい☆．これら2つの点から，ゲートレベルでの低消費電力化手法が実用上最も適用範囲が広いと考えられる．

CMOSデバイスの消費電力は，一般に，組合せ回路部のスイッチングによるものとクロックドライバのスイッチングによるものに大別される．今回筆者らがAES処理回路の各部の消費電力を調べたところ，そのうちS-Boxと呼ばれる組合せ回路による消費電力が大半（回路の構成の仕方にもよるが，典型的な回路構成では70%以上）を占めていた．そこで本稿では，組み込み用途向けに，S-Boxの消費電力を減少させるための論理回路構成法を検討した．

まず，代表的ないくつかの回路構成法に従って作ったS-Boxの消費電力を測定し，単に回路規模を減らすのではなく，回路中のダイナミックハザードの量を減らすことが低消費電力化に最も有効であることを見い出した．より具体的には，これまでに知られているうち最も回路規模が小さい合成体S-Box[9)~12)]の消費電力が，回路規模では数倍程度大きい二段論理[13)]によるS-Boxの消費電力と同程度であることなどが分かった．

次に，S-Box向けの新しい低消費電力論理構成法を考案した．提案方式（multi-stage PPRM）では，合成体S-Boxと演算アルゴリズムは同じであるものの，その回路各部が二段論理の1つであるPPRM（Positive Polarity Reed-Muller形式．AND-XORのこと）[13)]によって構成される．このような回路構成にすることで，各ゲートにおける入力への信号到達時刻がほぼ揃うため，ハザードの発生が抑えられる．また，合成体S-BoxではおくのXORゲート（ハザードがすべて通過してしまう）がANDゲート群の前に配置されるが，提案手法では逆にAND群がXOR群の前に配置されており，ハザードの伝播がブロックされる．これらの理由によって，提案手法ではハザードの発生や伝播が抑えられる．

実際に，提案手法で構成したS-Boxの消費電力をシミュレーションで測定してみたところ，0.13 μm CMOSスタンダードセル上で29 μW（10 MHz，1.5 V動作時）であり，これは他の構成法で作ったS-Boxと比べて半分から3分の1以下であった．回路規模は合成体S-Boxよりはやや大きくなるものの，それでも通常の半分程度である．なお，Camellia[14)]など最近の多くの共通鍵暗号のS-Boxでも，AESのS-Boxと類似した演算（ガロア体GF(2^8)上の逆元演算）が行われるので，本手法は有効と考えられる．

以下，2章ではAESのアルゴリズムと回路各部の消費電力解析結果について，3章ではS-Boxの各種論理構成法と消費電力の比較について，4章では提案するS-Box論理構成法とその評価について述べる．

2. AESの回路アーキテクチャと各部の消費電力解析

2.1 AESのアルゴリズムと標準的な回路アーキテクチャ

ここでは，AESの暗号化アルゴリズムと，その標準的な回路アーキテクチャについて説明する．

暗号化アルゴリズムは，128ビットの入力データに対し，4つの基本演算ShiftRows / SubBytes / MixColumns / AddRoundKeyをこの順に直列に並べた処理（ラウンド）を繰り返し適用するものである．ここでラウンド数は鍵長によって異なり，128ビット鍵では11，192ビットでは13，256ビットでは15である．最初のラウンドではAddRoundKeyだけが行われ，最終ラウンドではMixColumnsを除いた3つの演算が行われる．

各基本演算の内容は次のとおりである．ShiftRowsではデータを4バイト×4バイトの行列と見なしたうえで，各行を0〜3バイト巡回シフトする．SubBytesでは，データの各バイトにS-Boxと呼ばれる変換（詳しくは3章参照）を適用する．MixColumnsでは，上記行列の各列に対し，その要素を係数とする3次多項式と見なして多項式 $\{03\}_{16}x^3+\{01\}_{16}x^2+\{01\}_{16}x+\{02\}_{16}$（ここで $\{k\}_n$ は n 進表現の値 k を表す．以下同様）と乗じてから x^4+1 で剰余をとり，結果として得られる多項式の4係数を出力する．AddRoundKeyではデータとラウンド鍵（秘密鍵から生成される）のXORをとる．

図1 に，AESの暗号化処理を行う回路の標準的なアーキテクチャを示す．この回路は1クロックに1ラウンドの処理を実行するものであり，128ビット幅のデータレジスタと，先述の4つの基本演算を直列につなげた組合せ回路からなる．なお，処理中に用いる128ビットのラウンド鍵については，オンザフライで生成する場合と，あらかじめ計算してメモリないしレジスタに格納しておく場合とがあるが，図1ではラウンド鍵生成および格納のための回路は省略してある．

☆ AESを含め共通鍵暗号の多くでは，スループットやクロック周波数が与えられると，どのような回路アーキテクチャにすべきかがほとんど定まってしまう．このため，消費電力を下げる目的だけでアーキテクチャを変更することは困難な場合が多い．

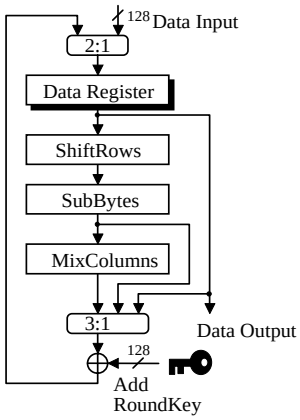

図 1 AES 暗号の標準的な回路アーキテクチャ
Fig. 1 A standard circuit implementation of AES.

2.2 消費電力の解析方法

本稿では，テクノロジマッピング後の回路☆にテストデータを与えてタイミングシミュレーションを行い，各ゲートのスイッチング回数から消費電力を見積もった．この方法では，かなり実際のチップに近い測定結果を得ることができる．消費電力を見積もる他の方法としては，ゲートのスイッチング確率を静的に解析する方法もあるが，これはハザードの影響を解析できず，AES のような演算主体の回路には向かない．また，トランジスタレベルなど，より下位レベルでシミュレーションを行えばさらに精度の高い測定が可能であるが，本稿で用いた方法でも，回路中クリティカルな部分を見い出したり異なる回路の性能比較を行ったりする用途には十分である．

2.3 各基本演算ユニットの消費電力

表 1 に，入力データとしてランダムパターンを 1,000 個与えた中での，回路の主要コンポーネントの最大消費電力を示す．ここで用いた AES 回路では，SubBytes として SOP S-Box（詳しくは 3.1 節）を利用した．ラウンド鍵については，あらかじめ計算された値が外部から与えられるものと仮定した☆☆．ShiftRows は単なる巡回シフトで論理ゲートは使用しないので，消費電力の測定は行わなかった．

表 1 から，消費電力の大半が SubBytes（S-Box）で占められていることが分かる．レジスタ数はそれほど多くないので，クロックドライバなどによる消費電力の割合は小さい．測定値はテストデータによって変動するが，筆者らの試した範囲ではたかだか 10%程度の差しかなかった．AES のような共通鍵暗号回路では，何らかの規則性のある入力データを与えてもラウンドを回るうちにランダム（に近い）データに変換されてしまうため，この点からもデータによる消費電力差はあまりないものと推定される．

表 1 AES の各基本コンポーネントの消費電力
Table 1 Power consumption of each AES component.

	Size (gate)	Observed Max Power (μW@10 MHz)
SubBytes (SOP S-Box × 16)	26,400	1,570
MixColumns	840	312
AddRoundKey	112	>10
FFs + Clock Drivers	—	400

(0.13 μm 1.5 V CMOS standard cell, 1gate = 2way-NAND)

3. S-Box 回路の構成法による消費電力の違い

ここでは，AES 処理回路の低消費電力化において最もクリティカルである S-Box 演算について，その回路構成法と性能比較結果を説明する．

3.1 代表的な回路構成法

S-Box は 8 ビット入出力の演算回路で，入力をガロア体 GF(2^8)（既約多項式は $x^8+x^4+x^3+x+1$，多項式基底）の要素と見なしてその乗法逆元（以下，単に逆元と呼ぶ）を求め，続いてアフィン変換を行って出力する．アフィン変換は GF(2) 上の定数行列演算である．

S-Box の回路構成法は，次の 2 つに大別される：

- S-Box の真理値表から，SOP（Sum of Products．積和形）や PPRM[13]などの二段論理や，BDD[15]（Binary Decision Diagram．二分決定グラフ．**図 2**）を構成して論理回路を導く方法．汎用の自動論理合成ツールで作った S-Box もこれに入る☆☆☆．
- 逆元演算回路とアフィン変換回路を別々に作り，直列につなぐ方法．逆元演算回路は，伊東・辻井のアルゴリズム[16),17)]（**図 3**）や合成体[9)~12)]（詳しくは次節）などガロア体の数学的性質・定義を利用して作る．

☆ 本稿では，論理合成ツールが回路構造を変えてしまうのを防ぐため，使用するセルを直接指定して回路を作成した．ただし，セルのストレングス調整は合成ツールにもある程度行わせた．

☆☆ オンザフライでラウンド鍵を生成する場合，そのための回路はいくつかの S-Box に XOR やセレクタを組み合わせたものとなり[11)]，やはり S-Box が消費電力の多くを占める．

☆☆☆ 論理自動合成によって得られる回路は，SOP や BDD，あるいはそれらの変形である場合が多い．

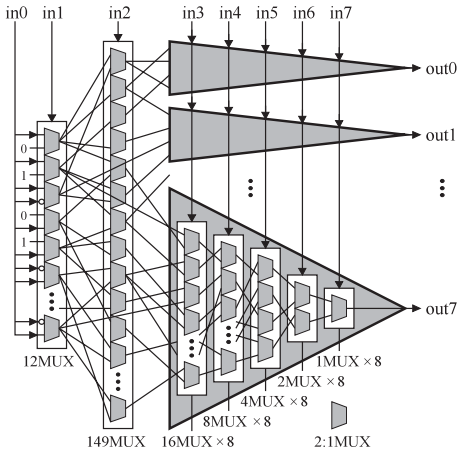

図 2 BDD で構成した S-Box 回路
Fig. 2 A BDD-based S-Box circuit implementation.

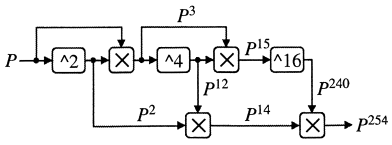

図 3 伊東・辻井のアルゴリズムによる逆元演算回路
Fig. 3 An inversion circuit based on Itoh and Tsujii's algorithm.

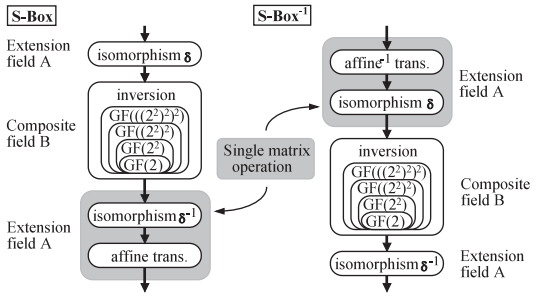

図 4 合成体を用いた S-Box における演算フロー
Fig. 4 Computation flow of composite-field S-Box.

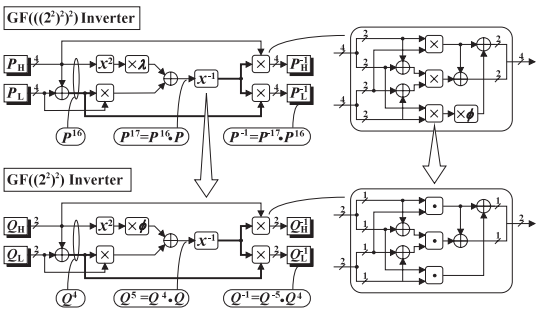

図 5 合成体を利用した逆元演算回路
Fig. 5 An inversion circuit based on composite-field technique.

ここで，前者では回路規模は大きいもののディレイの少ない回路を構成しやすく，後者ではディレイは大きいものの回路規模を小さくすることが可能，という傾向がある．

3.2 合成体を用いた小規模 S-Box 回路

本稿では合成体を用いた S-Box（以下，合成体 S-Box と呼ぶ．SOP などについても同様）をベースに低消費電力化を図るので，これについて説明する．合成体 S-Box は，現在知られている限り回路規模最小の S-Box である．

この手法は，要素数が同じガロア体が同形であることを利用し，逆元演算を合成体（素体から複数回の拡大で得られた体）上で行うものである．ここで，次の既約多項式を使って得られる合成体 $\mathrm{GF}(((2^2)^2)^2)$ 上の逆元演算回路は，$GF(2^8)$ と同形な体上の逆元演算回路としては，現在知られている限り最小のものである[11),12)]．本稿ではこれを用いる（ϕ=$\{10\}_2$, λ=$\{1100\}_2$）：

$$GF(2) \to GF(2^2): \quad x^2+x+1$$
$$GF(2^2) \to GF((2^2)^2): \quad x^2+x+\phi$$
$$GF((2^2)^2) \to GF(((2^2)^2)^2): \quad x^2+x+\lambda$$

逆元の計算は，もとの体 A の元を同形写像 δ で合成体 B へマップし，B 上で逆元を計算したのち同形写像 δ^{-1} で A へマップする，という 3 段階で行う（**図 4**）．合成体 $\mathrm{GF}(((2^2)^2)^2)$ 上の逆元計算は，部分体 $\mathrm{GF}((2^2)^2)$ の演算を用いて次の式で行える[9)]：

$$P^{-1} = (P \cdot P^{16})^{-1} \cdot P^{16} \qquad (1)$$

ここで右辺の乗算や逆元演算は，$\mathrm{GF}(((2^2)^2)^2)$ ではなく部分体 $\mathrm{GF}((2^2)^2)$ 上の演算であり，それらはさらに $\mathrm{GF}(2^2)$ 上の演算を組み合わせて行える．逆元回路は上式に従って構成され，階層的な構造を持つ（**図 5**）．

同型写像 δ，δ^{-1} の作り方については文献 11)，12) を参照されたい．同型写像は GF(2) 上の 8×8 定数行列乗算であり，アフィン変換とマージして 1 つの定数行列演算にできる．GF(2) 上の定数行列演算は，回路では XOR マトリックスとして実現される．

3.3 各 S-Box の消費電力解析

3.1 節で述べたさまざまな論理構成法のもとで S-Box の演算回路を作り，消費電力を測定した．**表 2** に 0.13 μm CMOS スタンダードセルにおける測定結果を，**表 3** に 0.18 μm CMOS スタンダードセルにおける測定結果を示す．測定は，プライマリ入力変化の全パターン（$2^8 \times 2^8 = 65,536$ パターン）を回路へ与え，消費電力の平均をとることで行った．

その結果，S-Box の消費電力は論理構成によってかなり大きく変化することが分かった．とくに，回路の一般的な傾向と異なり，回路規模が小さい S-Box が消

表 2 さまざまな S-Box 回路の平均消費電力（1）
Table 2 Power consumption of various S-Box architectures (1).

	Delay (ns)	Size (gate)	Average Power (μW @10 MHz)
伊東・辻井	2.79	1,771	2,100
PPRM (1-stage)	1.14	2,241	343
BDD	0.69	1,399	275
自動合成	0.68	2,623	144
合成体	2.19	354	136
SOP (1-stage)	0.69	1,650	95
提案手法 (3-stage PPRM)	1.43	712	29

(0.13 μm 1.5 V CMOS standard cell, 1gate = 2way-NAND)

表 3 さまざまな S-Box 回路の平均消費電力（2）
Table 3 Power consumption of various S-Box architectures (2).

	Delay (ns)	Size (gate)	Average Power (μW @10 MHz)
伊東・辻井	4.11	1,540	3,490
PPRM (1-stage)	1.32	2,242	408
BDD	0.96	857	332
自動合成	0.91	1,706	206
合成体	3.01	305	166
SOP (1-stage)	0.97	1,142	138
提案手法 (3-stage PPRM)	1.86	701	51

(0.18 μm 1.8 V CMOS standard cell, 1gate = 2way-NAND)

費電力も小さいとは限らない．筆者らは当初，合成体 S-Box が最も消費電力が少なくなるだろうと予測していた．しかし，数倍の回路規模である SOP S-Box や自動合成した S-Box の方が低消費電力である．BDD S-Box や PPRM S-Box，および伊東・辻井のアルゴリズムを用いた S-Box については，規模の割に消費電力がかなり大きい．

なお，一般にはテクノロジライブラリが変われば消費電力も変化するが，今回の AES S-Box の場合，S-Box 間の消費電力比は 0.13 μm と 0.18 μm で多少変動したものの，順位はほとんど変わらなかった[18)]☆．

以上の測定結果から，筆者らは，回路動作中のダイナミックハザードの量によって S-Box の消費電力が決まるものと推定した．ダイナミックハザードの量が決まる要因としては，以下に述べる 2 点があげられる．

☆ 組み込み用途などでは，今回用いた 0.13 μm ないし 0.18 μm よりも前世代のテクノロジを用いる場合もある．そのようなテクノロジでは，ここで示した例よりも各 S-Box 間の電力差がずっと大きくなる傾向がある[18),19)]．

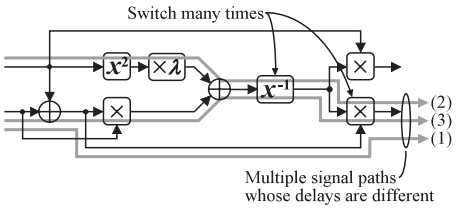

図 6 合成体 S-Box におけるさまざまな信号伝播経路
Fig. 6 Different signal transition paths in the composite field S-Box.

3.3.1 ゲートへの信号到達時間差

AND や XOR ゲートなど複数入力を持つゲートにおいて，その信号変化時刻が入力間でずれていると，そのゲート出力にダイナミックハザードが発生し，余分な電力が消費される．

合成体 S-Box は図 5 に示したように複雑に分岐や交差をする信号経路を持つ．このため，部分演算回路の入力への信号到達時刻がばらばらになり，何度も回路が動作してしまう（**図 6**）．これが合成体 S-Box の消費電力が予想外に大きくなったおもな理由と考えられる．伊東・辻井のアルゴリズムを用いた S-Box（図 3）についても，まったく同様と考えられる．また，BDD S-Box（図 2）については，2:1 セレクタのデータ入力信号と制御入力信号で到達時刻が大きく異なることに加え，初段側のデータ信号や制御信号のファンアウトが極端に大きく，それらの駆動に多くのドライバが必要であることも，消費電力が大きくなった理由と考えられる☆☆．

一方，SOP や PPRM などの二段論理を用いた場合，ゲートの各入力への信号到達時刻は比較的そろっていると考えられる．

3.3.2 信号変化の伝播しやすいゲートの配置

回路中で発生したハザードが後段へ伝播していくことによっても，余分な電力が消費される．ここで，ハザードの伝播確率は，通過するゲートの種類によって異なる．たとえば XOR ゲートではすべてのハザードが後段へ確率 1 で伝播するのに対し，AND ゲートや OR ゲートでの確率は 0.5 である．

合成体 S-Box では，図 5 における回路の前半部（P^{17} の計算）の大半が XOR のみで構成されている．これも，合成体 S-Box の消費電力が多い理由と考えられる．すなわち，プライマリ入力が変化するとそれらの XOR 群は必ずスイッチングしてしまうが，後半部は AND を含んでおり，それ以降で信号変化がブロック

☆☆ S-Box の BDD では，変数順を変えてもほとんど回路規模や速度などが変わらないという特徴がある[3)]．

されることがある．そのような場合，回路の前半部の動作は無駄になってしまう．

また，PPRM S-Box では，ゲート入力間の信号到達時刻はそろっているものの，多量の XOR ゲートが使われているので消費電力が大きくなってしまうと考えられる．

4. 提案する低消費電力 S-Box 回路とその評価

4.1 Multi-stage PPRM とその評価

今回，おもに組み込み用途向けに，低消費電力 S-Box の論理構成法を検討した．組み込み用途では，消費電力はもちろん，回路規模も小さいことが望ましい．筆者らは，合成体 S-Box の回路がきわだって小規模な点に着目し，これをベースにして低消費電力化を図ることにした．

提案手法（multi-stage PPRM）を**図 7** の下段に示す．合成体 S-Box（図 7 上段）の各ブロックがそれぞれ PPRM によって実装される．図 7 の各ブロックは，3.2 節の式 (1) における次の部分と対応している：(i) 入力 P に同型写像 δ を適用したうえで P^{16} と P^{17} を計算する部分，(ii) $(P^{17})^{-1}$ を GF$((2^2)^2)$ 上で計算する部分，および (iii) P^{-1} を計算して（同型写像 δ^{-1} も適用）アフィン変換を行う部分．なお，ブロック (i) と (iii) が (ii) を介さずにつながる経路があるが，それらについてはディレイラインを通し，信号をブロック (ii) と同程度に遅延させる．

以上の方法で構成した S-Box の性能を，3.3 節の表 2，表 3 に他手法と合わせて示す．0.13 μm，0.18 μm のいずれのテクノロジライブラリにおいても，消費電力は SOP S-Box や自動合成した S-Box などと比べて半分以下，合成体 S-Box と比べれば 3 分の 1 以下に抑えられた．回路サイズは合成体 S-Box よりは増えたものの，他と比べ半分以下である．回路速度は速くはないが，合成体よりも向上しており実用上問題ない．

このように消費電力が抑えられた理由は，次のとおりである：(1) 各ブロック内のゲートにおいて入力間の信号到達時刻差が小さく，ダイナミックハザードの発生が抑えられる，(2) 各ブロックの入力信号が変化したとき，それがまず AND ゲートを通過してから XOR ゲートへ伝播するので，無駄な信号変化（ハザード）がブロックされやすい，(3) 各ブロックのサイズが小さく抑えられている．

また，3 ステージの PPRM でなくステージを増減した場合や，PPRM ではなく multi-stage SOP にした場合の回路性能を**表 4** に示す．PPRM の場合，ステージ数を増やせば回路規模が減少していくが，それにつれて XOR ゲートが直列につながる段数は増えていくので，図 7 のように 3 ステージが消費電力の点では最適となった．なお，もとの合成体 S-Box は 5 ステージである．また，SOP の場合，ステージ分割によって回路規模が大きく増加してしまい，消費電力も増えてしまった．これは，回路をステージ分割することで論理簡単化の効果が出にくくなったためと推定される（一般に，XOR 主体の回路を SOP で構成すると回路規模は大きくなる）．

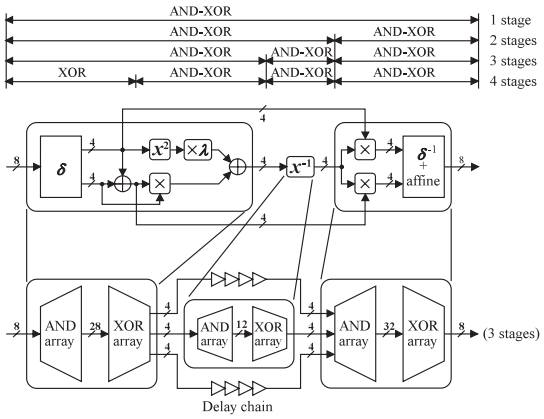

図 7 提案手法（multi-stage PPRM）に基づく S-Box
Fig. 7 A S-Box circuit based on the proposed multi-stage PPRM.

表 4 論理ステージ数と回路性能の比較
Table 4 Number of logic stages vs. S-Box performance.

	state	Size (gate)	Average Power (μW @10 MHz)
PPRM	1	2,241	343
	2	1,445	273
	3	712	29
	4	413	88
	5	354	136
SOP	1	1,650	95
	2	5,891	612
	3	6,114	697

(0.13 μm 1.5 V CMOS standard cell, 1gate = 2way-NAND)

4.2 S-Box と S-Box^{-1} のマージ

提案手法の重要な利点の 1 つとして，暗号化に用いる S-Box 回路と復号化に用いる S-Box^{-1}（逆演算）回路の間で，多くのゲートを共有できる点があげられる．そのような共有は合成体 S-Box でも可能であるが，SOP S-Box や自動合成した S-Box など，真理値表を直接回路化する場合には不可能である．

図 8 に，提案手法のもとで S-Box と S-Box^{-1} を

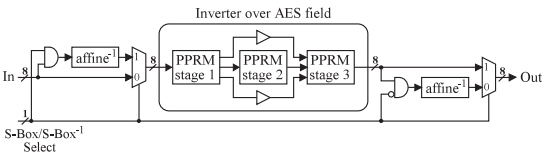

図 8 S-Box と S-Box^{-1} の回路共有
Fig. 8 Circuit sharing between S-Box and S-Box^{-1}.

表 5 共有を行った S-Box/S-Box^{-1} の回路性能
Table 5 Performance comparison of shared S-Box architectures.

	Delay (ns)	Size (gate)	Average Power (μW @10 MHz)
合成体	2.53	381	179 (S-Box) 189 (S-Box^{-1})
提案手法	2.00	725	79 (S-Box) 70 (S-Box^{-1})

(0.13 μm 1.5 V CMOS standard cell, 1gate = 2way-NAND)

マージした回路の構造を示す．提案手法によって逆元回路を構成し，その前後にアフィン変換回路を配置する．暗号化と復号化で，アフィン変換は別々の回路をセレクタで切り替えて用いるが，逆元回路は共通である．

表 5 に，共有を行った回路の性能を示す．回路規模は単体の 3-stage PPRM S-Box より若干大きい程度で済んだ．消費電力は増加したものの，SOP S-Box や自動合成した S-Box と比べ依然小さく，合成体において同様の共有を行った場合と比べれば半分以下である．なお，SOP S-Box や自動合成した S-Box では，暗号化と復号化の両機能をサポートするには 2,000 ゲートを超える回路規模になってしまう．

5. おわりに

本稿では，次期米国標準の 128 ビット共通鍵ブロック暗号 AES において，その回路の消費電力を減らす方法を検討した．AES の消費電力の大半を S-Box が占め，S-Box の消費電力は回路中を伝播するダイナミックハザードの量で決まる．そこで，低消費電力 S-Box の論理回路構成法として，multi-stage PPRM を考案した．この構成では，合成体上で演算を行って回路規模を縮小するとともに，回路各部を二段論理で構成して各ゲートへの信号到達時間を揃え，ハザード発生を抑える．その結果，これまで知られている S-Box と比べて半分から 3 分の 1 以下の消費電力を達成した．その他の最近の共通鍵暗号においても，S-Box では AES と類似の演算（ガロア体の逆元演算）が行われる場合が多く，本手法は有効である．

参考文献

1) Daemen, J. and Rijmen, V.: AES Proposal: Rijndael. http://csrc.nist.gov/encryption/aes/rijndael/Rijndael.pdf
2) National Institute of Standards and Technology (NIST): Advanced Encryption Standard (AES), *FIPS Publication 197* (2001). http://csrc.nist.gov/encryption/aes/index.html
3) Morioka, S. and Satoh, A.: A 10 Gbps Full-AES Crypto Design with a Twisted-BDD S-Box Architecture, *Proc. IEEE Intl. Conf. on Computer Design 2002* (*ICCD2002*), pp.98–103 (2002).
4) Kuo, H., et al.: Architectural Optimization for a 1.82 Gbits/sec VLSI Implementation of the AES Rijndael Algorithm, *Proc. CHES2001*, LNCS Vol.2162, pp.53–67 (2001).
5) Weeks, B., et al.: Hardware Performance Simulation of Round 2 Advanced Encryption Standard Algorithm. http://csrc.nist.gov/encryption/aes/round2/NSA-AESfinalreport.pdf
6) McLoone, M., et al.: High performance single-chip FPGA Rijndael algorithm implementations, *Proc. CHES2001*, LNCS Vol.2162, pp.68–80 (2001).
7) Fischer, V., et al: Two methods of Rijndael implementation in reconfigurable hardware, *Proc. CHES2001*, LNCS Vol.2162, pp.81–96 (2001).
8) Chandrakasan, A.P. and Brodersen, R.W. (Eds.): *Low Power Digital CMOS Design*, Kluwer Academic Publishers (1995).
9) Guajardo, J. and Paar, C.: Efficient Algorithms for Elliptic Curve Cryptosystems, *CRYPTO'97*, LNCS Vol.1294, pp.342–356 (1997).
10) Rudra, A., et. al: Eficient Rijndael encryption implementation with composite field arithmetic, *Proc. CHES2001*, LNCS Vol.2162, pp.175–188 (2001).
11) Satoh, A., Morioka, S., Takano, K. and Munetoh, S.: A Compact Rijndael Hardware Architecture with S-Box Optimization, *Advances in Cryptology — ASIACRYPT 2001*, LNCS Vol.2248, pp.239–254 (2001).
12) 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，第 63 回情報処理学会全国大会，3G-04 (2001).
13) Sasao, T.: Logic Synthesis and Optimization, Kluwer Academic Publishers (1993).

14) 128ビットブロック暗号 Camellia. http://info.isl.ntt.co.jp/camellia/index-j.html
15) Bryant, R.E.: Graph-Based Algorithms for Boolean Function Manipulation, *IEEE Trans. Comput.*, Vol.C-35, No.8, pp.677–691 (1986).
16) Itoh, T. and Tsujii, S.: A Fast Algorithm for Computing Multiplicative Inverses in GF(2^m) using Normal Bases, *Information and Computation*, Vol.78, No.3, pp.171–177 (1988).
17) Morioka, S. and Katayama, Y.: O($\log_2 m$) Iterative Algorithm for Multiplicative Inverse in GF(2^m), *IEEE Intl. Symp. on Info. Theory* (*ISIT2000*), p.449 (2000).
18) 森岡澄夫，佐藤　証：AESの低消費電力回路実装のための論理設計方式の検討，情報処理学会第4回コンピュータセキュリティシンポジウム（CSS2001），pp.307–312 (2001).
19) Morioka, S. and Satoh, A.: An Optimized S-Box Circuit Architecture for Low Power AES Design, *Proc. CHES2002*, LNCS Vol.2523, pp.172–186 (2002).

(平成14年8月23日受付)
(平成15年3月 4 日採録)

推　薦　文

暗号処理をハードウェア実装する場合は一般に処理速度の向上を第1目的とする．しかし今後は携帯装置の中に組み込まれる場合も多くなることを想定して，本論文では消費電力に着目している．暗号処理では，ビット構成をかく乱するという目的から，多くの信号線を多段にからませる形となっている．このような回路を低電力化する例が過去には少なかったが，ここでは，全体素子数を少なくすればよいという過去の考え方とは異なる設計原理を見出した．

（CSEC研究会主査　岡本 栄司）

森岡　澄夫（正会員）

1992年大阪大学基礎工学部情報工学科卒業．1997年同大学院基礎工学研究科博士課程修了．博士（工学）．同年，日本アイ・ビー・エム株式会社東京基礎研究所入所．高性能VLSI回路の研究に従事．著書「HDLによる高性能ディジタル回路設計」（CQ出版）．IEEE会員．

佐藤　　証（正会員）

1987年早稲田大学理工学部卒業．1989年同大学院理工学研究科修士課程修了．同年，日本アイ・ビー・エム株式会社東京基礎研究所入所．1998年，早稲田大学より博士（工学）授与．高性能VLSI回路の研究に従事．