Copyright© 2013 The Institute of Electronics, Information and Communication Engineers

SCIS 2013 The 30th Symposium on Cryptography and Information Security
Kyoto, Japan, Jan. 22- 25, 2013
The Institute of Electronics, Information and Communication Engineers

耐タンパ性向上のための乗算マスクと Dual-Rail RSL メモリ方式を用いた AES 暗号回路の設計

Tamper-Resistant AES Cryptographic Circuit utilizing Multiplicative Mask and Dual-Rail RSL Memory

鵜飼 慎太郎* Shintaro Ukai
HOANG Anh-Tuan†
汐崎 充† Mitsuru Shiozaki
浅川 俊介†† Shunsuke Asagawa
橋本 祐樹* Yuki Hashimoto
藤野 毅†† Takeshi Fujino

あらまし IC カード等に使用される暗号回路には電力差分攻撃等のサイドチャネル攻撃に耐性を持つ耐タンパ暗号回路が求められている．そこで，本研究室では標準 ASIC の設計フローで実装が可能でかつ小面積・低消費電力な対策手法として Dual-Rail RSL メモリ方式を提案してきた．この提案方式では，SubBytes 変換以外の演算処理は加算乱数マスクを用いて演算を行い，SubBytes 変換は，入出力値に依存せず均一な消費電力となる 2 線相補メモリを用いて演算を行っている．この方式を用いて実装した AES 暗号回路は，一般的な電力差分攻撃に対しては高い攻撃耐性を示し，100 万波形で 1 バイトの部分鍵も解明できなかった．しかしながら，SubBytes 変換においては加算乱数マスクのない状態で暗号処理を行っているため，高次の電力差分攻撃や，電磁波解析攻撃に対して脆弱性を持つ懸念がある．そこで，本論文では SubBytes 変換に乗算マスクを用いる Hybrid Masking Dual-rail RSL メモリ方式を提案する．本方式では，乗算マスクのかかった値に対して 2 線式 ROM を用いて逆元演算を行う．これにより SubBytes 変換時にはバランシングとマスキングの二重の対策が実現できる．さらに，逆元演算とアファイン変換を分けて用いることにより，暗号化と復号化で ROM を共用化できるためメモリ面積を半減できる．本方式を用いた AES 暗号回路を 0.18μmCMOS プロセスで設計・試作したので電力攻撃耐性評価と合わせて報告する．

キーワード サイドチャネル攻撃，DPA，CPA，Dual-Rail RSL メモリ，Hybrid Mask，CMOS 回路

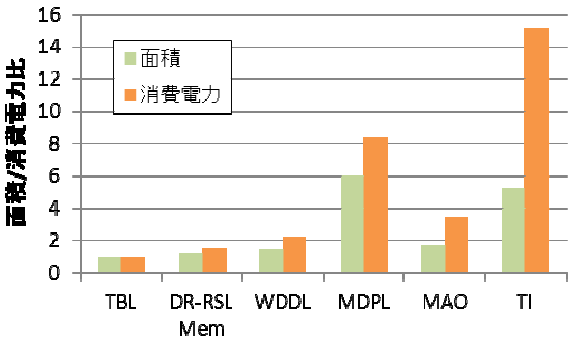
1 はじめに

近年，暗号モジュール動作時に生じる 2 次的な情報（消費電力や漏洩電磁波，処理時間等）を利用し秘密情報を推定するサイドチャネル攻撃の危険性が報告されている．中でも多数の消費電力波形の統計処理による電力解析攻撃は安価な装置で行うことができるため危険とされ，差分から秘密鍵を解読する Differential Power Analysis (DPA)[1]や，相関値を用いて解読する Correlation Power Analysis (CPA)[2]等がある．CPA は消費電力と回路内部の状態との相関をとるが，回路内部の状態としては 2 種類に分類される．一つは，OR や AND ゲートなどの非線形論理ゲートに対する入力値のハミングウエイトと消費電力との相関をとって秘密鍵情報を推定する Hamming Weight CPA (HW-CPA)である．もう一つは，DES，AES などの暗号ハードウェア回路はラウンドごとに計算した値を同一のレジスタに格納するループアーキテクチャが一般的であることから，ラウンド毎のレジ

* 立命館大学大学院理工学研究科，〒525-857，滋賀県草津市野路東 1-1-1, Graduate School of Science and Technology, Ritsumeikan University, 1-1-1 Nojihigashi, Kusatsu, Shiga, Japan, {ri001084 , ri007077}@ed.ritsumei.ac.jp
† 立命館大学大学院総合理工学研究機構，〒525-857，滋賀県草津市野路東 1-1-1, Research Organization of Science and Engineering, Ritsumeikan University, 1-1-1 Nojihigashi, Kusatsu, Shiga, Japan, {anh-tuan , mshio}@fc.ritsumei.ac.jp
†† 立命館大学理工学部，〒525-857,滋賀県草津市野路東 1-1-1, Department of Science and Engineering, Ritsumeikan University, 1-1-1 Nojihigashi, Kusatsu, Shiga, Japan, {sav29073@gst , fujino@se}.ritsumei.ac.jp

スタ格納値の遷移ビット数（ハミングディスタンス）と消費電力との相関から秘密鍵情報を推定する Hamming Distance DPA (HD-CPA)である．

これまでに DPA，CPA の対策手法は多くの提案があり，演算に用いる論理ゲートに対して変更を行うゲートレベル対策として，Wave Dynamic Differential (WDDL)方式[3][4] や Masked And Operation (MAO)方式[5]，Masked Dual-Rail Precharge Logic (MDPL)方式[6]等が提案されてきたが，これらの対策方式は LSI 設計において特別な配置配線ツールが必要であり，これを用いずに通常の ASIC 設計フローで AES 暗号回路を設計すると，50 万波形以下の消費電力波形の収集で全鍵を特定することができる[7]．一方，暗号演算のアルゴリズムを改良する Threshold Implementations (TI)方式[8]では高い攻撃耐性を有するが．面積や消費電力が大幅に増大する問題がある．図１に我々が評価した，消費電力と面積の結果を示すが，TI 方式では未対策回路の 5 倍の面積と 15 倍の電力を消費するため，低コスト・低消費電力が要求される用途では使用できない．



※注釈　TBL: 未対策
DR-RSL Mem: 我々の旧提案ゲートレベル対策
WDDL,MDPL,MAO: 既存のゲートレベル対策
TI: 既存のアルゴリズムレベル対策

図１．既存の対策方式 AES 暗号回路の性能

そこで我々は小面積・低消費電力かつ CPA 耐性を有する Dual-Rail RSL メモリ方式を提案し，この方式を適用した AES 暗号回路の LSI を設計試作した．本方式は，MixColumn 等の線形回路では，加算乱数マスクを用いた対策を行い，非線形回路である SBox 部ではどのような入力値に対しても消費電力を均一化できる Dual-Rail RSL メモリを用いる．その結果，図１に示すように，未対策回路の 6%の面積増加，50%の消費電力増加で設計が可能であった．また，100 万の消費電力波形を用いた HW-CPA を行っても鍵が１つも解析されない高い電力攻撃耐性を実現できた[7]．

しかしながら，開発した Dual-Rail RSL メモリ方式は，SubBytes 変換においては乱数マスクのない状態で暗号処理を行っているため，高次の電力差分解析攻撃や，電磁波解析攻撃に対して脆弱性を持つ懸念がある．そこで本稿では，Sub Bytes 変換において乗算マスクを用いることで，SubBytes 変換時にはバランシングとマスキングの二重の対策が実現できる Hybrid Masking Dual-Rail (HMD-)RSL メモリ方式を提案する．本方式では，SubBytes 変換に GF(2^8)逆元演算と Affine 変換を用いて行うため，メモリには GF(2^8)逆元演算テーブルを格納する．このため，暗号化・復号化でメモリを共用できるため，Dual-Rail RSL メモリ方式と比べてメモリ面積を半減でき，チップ面積の縮小も期待できる．

以降，第２章では提案方式のベースとなっている Dual-Rail RSL メモリ方式と Multiplicative Masking 方式の概要と問題点を整理する．第３章では，提案する HMD-RSL メモリ方式 AES 暗号回路の設計と耐性評価について述べ，第４章でまとめと今後の課題について記載する．

2　既存の対策技術と問題点

2.1　Dual-Rail RSL メモリ方式 AES の概要と問題点

まず我々が提案してきた Dual-Rail RSL メモリ方式を適用した AES の概要と問題点について整理する．図２に Dual-Rail RSL メモリ方式 AES の回路実装方法を示す．

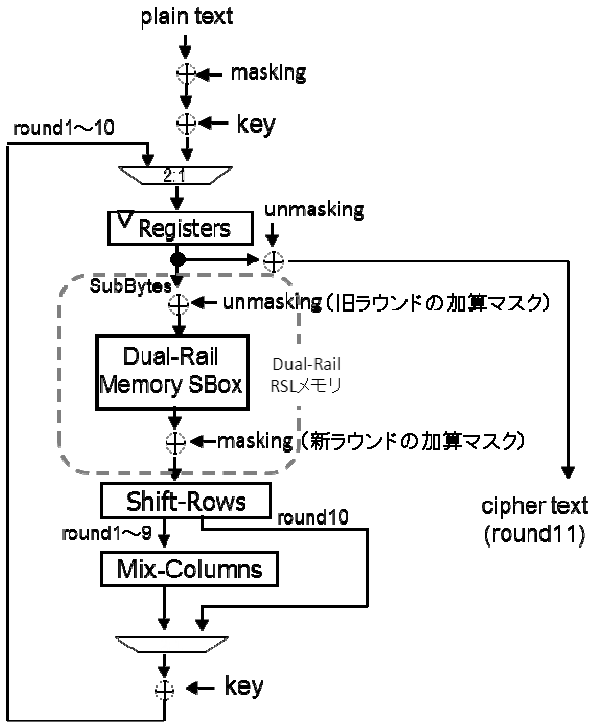


図２．Dual-Rail RSL メモリ方式 AES

暗号処理の１ラウンド毎の演算の結果がレジスタに保存されるが，そのレジスタにおける HD-CPA の対策として，ラウンドごとに新しい加算マスクを適用している．SubByte 変換を行う SBox 回路においてはメモリを用い

たテーブル変換を行うが，ここに 2 線相補動作を行う Dual-Rail RSL メモリを使用する．Dual-Rail RSL メモリにはマスクされた入力値と，前ラウンドおよび現ラウンドの加算乱数マスクデータの 3 種が入力される．メモリ内部では前ラウンドの加算乱数マスクを用いて，入力データのマスクが解除され SBox テーブル変換が行われる．また，メモリからの出力時には，次ラウンド用の新たな加算乱数マスクが適用されて出力される．メモリ内部ではマスクが解除されているが，後述の 2 線相補動作によるバランシングにより消費電力が均一化される．

すなわち，Dual-Rail RSL メモリでは，いかなる入力/出力値に対しても，消費電力を均一化できるため，SBox 部の入力または出力を用いた HW-CPA に対して耐性を有する．

ここで，SBox 回路を構成している Dual-Rail RSL メモリについて説明する．Dual-Rail RSL メモリ回路は Domino-RSL ゲート [9] を用いた XOR 回路（Domino-XOR ゲート），デコーダ回路，2 線式 ROM セル，マルチプレクサ回路で構成される（図３参照）また，ラウンド間の相関を無くす（HD 型攻撃耐性を持たせる）為に，回路全体をプリチャージ・ロジックで構成している．

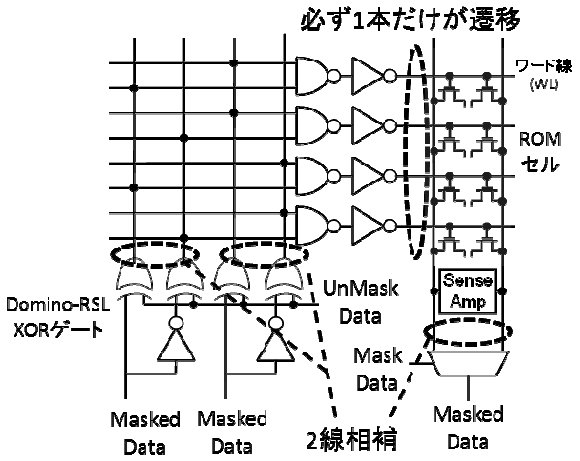


図３．Dual-Rail RSL メモリ

アンマスク処理は 1 ビットの入力データに対して 2 つの Domino-XOR ゲートを用い，プリチャージ期間には 2 本の相補出力データはどちらも 0 を出力し，評価期間では相補出力のうちどちらか一方が論理 1 を出力することで 2 線式論理へ変換している．ワード線は相補動作を行わないが，プリチャージ時はすべてのワード線が 0 であり，評価期間中はデコーダ回路で選択された 1 本のワード線だけが遷移するため，入力値に関係なく一定の電力が消費される．

一般的な ROM セルでは 1 本のビット線に Hi または Lo を読み出す為のトランジスタ 1 個が接続されているが，本 ROM セルでは動作時の消費電力がメモリ出力値“0”と“1”に依存しないようにする為，2 本のビット線と 2 個のトランジスタを使用した 2 線式 ROM セル（図４参照）を使用している．プリチャージ期間中に BL および /BL の電位が電源電圧にプリチャージされる．評価期間中にはビットラインのいずれか一方だけがグランドに接続される．したがってメモリセルデータが‘1’‘0’どちらであっても消費電力は一定となる．

出力部は出力マスク値により相補ビット線の片方をマルチプレクサで選択することにより，乱数マスクの掛かったデータを出力している．以上の動作により，Dual-Rail RSL メモリ回路内ではどのような入出力であろうと消費電力が均一となる．

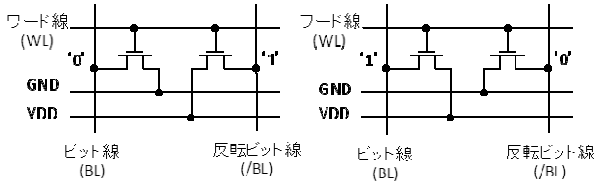


図４．2 線式 ROM セル

2 線相補動作によるバランシングを用いた，WDDL 方式で自動配置配線を用いて設計すると相補配線の寄生容量を均一にすることは大変困難であるため，情報リークにつながっていた，本メモリ方式では規則的に配線を配置する為，容易に寄生容量を均一化できる． また，WDDL 方式では，多段の論理ゲートを接続した際にアーリープロパゲーション効果によるリークがあるとされている[10][11]が，ワード線やセンスアンプの活性タイミングは制御されているため，この問題も回避できている．

Dual-Rail RSL メモリ方式を SBox に適用して設計した AES 暗号回路を 0.18μmCMOS で実際に設計し，サイドチャネル攻撃評価ボード SASEBO-RII を用いて電力差分解析攻撃を行った．本環境では MDPL 方式では 6 万波形，WDDL 方式では 20 万波形で全 16Byte の鍵が解析できている．一方，Dual-Rail RSL メモリ方式で設計したチップでは，100 万波形を用いて HW-CPA 攻撃を行っても 1 Byte の鍵も解析できていない[7]．

しかしながら，今後のより高度な攻撃，たとえば，高次の電力差分攻撃や，電磁波解析攻撃，フォールト攻撃に対して安全性を保証するためには Dual-Rail RSL メモリ内部でも乱数マスキングを適用する必要があると考えている．たとえば，情報リーク源としては，製造バラツキによる相補配線寄生容量の不均一，遷移するワード線の位置情報の漏えいが考えられる．次節に，この問題を解決するための技術として，乗算マスクを用いて DPA 対策を施している Multiplicative Masking 方式についてその概要と問題点を示す．

2.2 Multiplicative Masking 方式 AES の概要と問題点

本節では，Akkar らが提案した Multiplicative Masking 方式を適用した AES 暗号回路[12]について説明し，またこの対策技術だけでは耐性が不十分であることを示す．図 5 に Multiplicative Masking 方式 AES 暗号回路の SubBytes 変換アルゴリズムを示す．

SubBytes 処理は，前述のテーブル方式とは異なり，ガロア体 $GF(2^8)$上の逆元演算とアファイン変換を用いた演算により行う．逆元演算時には，加算マスク am でマスクされた入力データ $D \oplus am$ に乗算マスク mm を適用したうえで $am \otimes mm$ を加算することで，乗算マスクでマスクされたデータ $D \otimes mm$ を得る．$D \otimes mm$ に対して $GF(2^8)$上の逆元演算を行うと，$(D \otimes mm)^{-1}$ が得られる．この結果に対して，$(am \otimes mm^{-1})$ を加算し最後に，mm で乗算すると，$D^{-1} \oplus am$ が得られる．すなわち，演算の中間値として D を使うことなく，$D \oplus am$ から $D^{-1} \oplus am$ が得られていることがわかる．

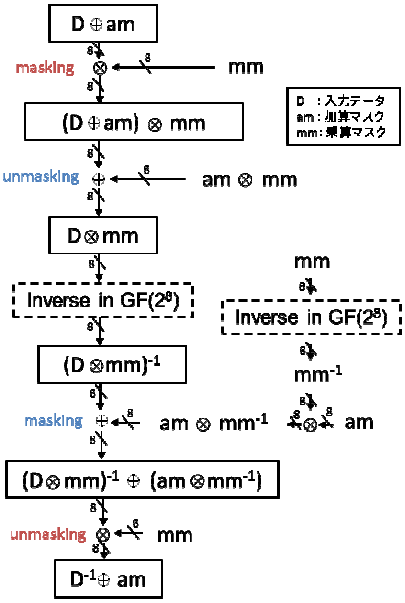


図 5．マスキングの流れ

このようにして，暗号化を行う上でのすべての過程においてマスクの掛かった状態で処理を行っている．よって，マスキングのみでも HW-DPA, HD-DPA の対策になっているかのように思われるかもしれない．しかし，この対策技術をそのままハードウエア実装に適用する場合には 2 つの問題点がある．1 つは全ラウンド処理で同じ乱数マスク am を利用している点であり，同じ乱数を用いた場合，レジスタ格納値の遷移情報から攻撃を行う HD 型の攻撃に弱いため，ラウンドごとに異なる乱数を用いる必要がある．これは，次節で述べるように容易であり，逆に乗算マスク mm の逆元を計算する必要がなくなるという点で，演算コストの低減が可能となる．

2 つ目は，SubByte 変換の入力値 D=0 であった場合に，図 5 中の演算において，いかなる mm に対しても $D \otimes mm=0$ となるという問題である．すなわち，D=0 だけはマスクされずに演算が行われるため，これを利用して DPA 攻撃を行う手法が Zero-Value 攻撃として知られている[13]．

Zero-Value 攻撃は，逆元の演算に合成体を使った回路を用いると脆弱である．図 6 に，合成体を用いて逆元演算を行う回路の消費電力を SPICE シミュレーションで求めた結果を示す．入力値 0 の場合と，それ以外の入力値の場合の平均値では明らかに異なった消費電力となっている．したがって 0 入力の場合とそれ以外の入力の差分波形を用いる Zero-Value 攻撃は危険であると判断できる．

一方，2.1 節で説明した Dual-Rail RSL メモリ方式を用いた場合，どのような入力に対しても SBox 回路の消費電力を均一化することができる．図 7 に SPICE シミュレーション波形を示すが，入力が 0 の場合の電力と他の入力時との消費電力波形は同一であり，この差分を用いた Zero Value 攻撃は無効化できる．

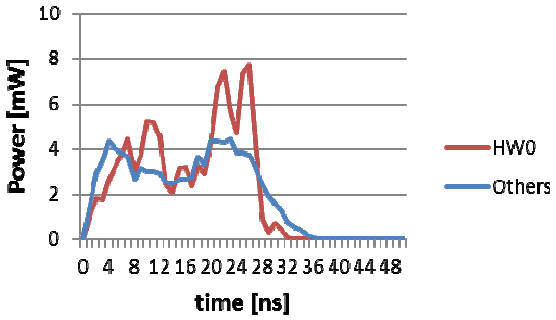


図 6．合成体 SBox に対する Zero Value 攻撃

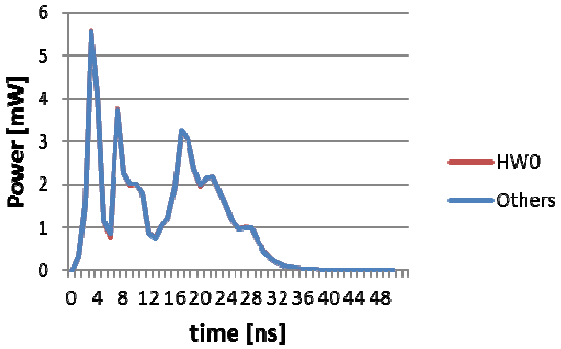


図 7．Dual-Rail RSL メモリ SBox に対する Zero Value 攻撃

このように，Multiplicative Masking 方式と Dual-Rail RSL メモリ方式の対策技術をうまく併用することで，より強い DPA 耐性，更には電磁波攻撃耐性が期待できる．

3　HMD-RSL メモリ方式を適用した AES 暗号回路の設計

3.1　HMD-RSL メモリ方式 AES の概要

本章では，2 章で示した Multiplicative Masking 方式 AES 及び Dual-Rail RSL メモリ方式 AES の対策技術を組み合わせた Hybrid Masking Dual-Rail(HMD-)RSL メモリ方式 AES を提案する．HMD-RSL メモリ方式では，SubBytes 変換において乗算マスクを用いることにより，SubBytes 変換時にはバランシングとマスキングの二重の対策が実現できる．これにより，メモリのワード線が SBox の入力値に依存することを利用する攻撃や，メモリ内の 2 線相補信号線の寄生容量が，LSI の製造バラツキによって微小に変動することを利用するような攻撃に対して攻撃耐性が向上することが期待できる．2.2 節で述べたとおり Zero value 攻撃にも耐性を持つと考えられる．

本方式の暗号化及び復号化の回路構成を図 8 に示す．SubBytes 変換に GF(2^8)逆元演算と Affine 変換を用いて行うため，メモリには GF(2^8)逆元演算テーブルを格納する．暗号化においては逆元演算後に Affine 変換，復号化処理においては逆 Affine 変換後に逆元演算を行うことができる．このため，従来の Dual-Rail RSL メモリ方式では暗号化・復号化でそれぞれ別に用意する必要があった Dual-Rail RSL メモリを共有できるため，メモリ面積を半分に削減することが可能になる．

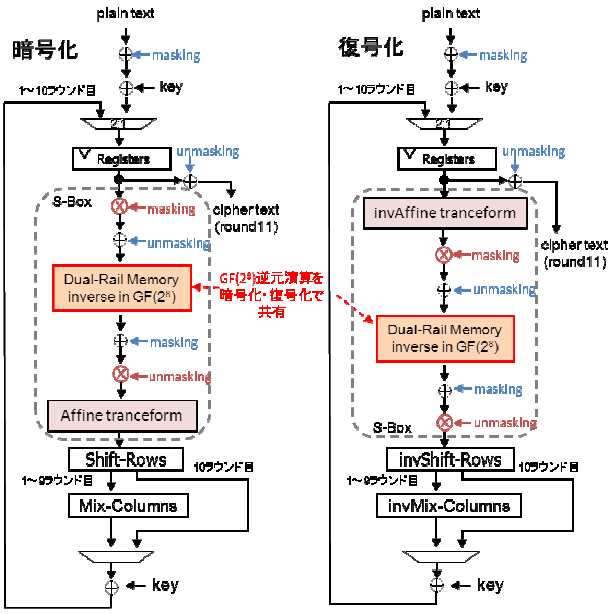


図 8．HMD-RSL メモリ方式 AES

新しく適用する乗算マスクは，Dual-Rail RSL メモリのデータ入力の前にマスキング，データ出力後にアンマスキングを行う．本方式のマスクの掛け方，1 ラウンド分の入力データの流れを図 9 に示す．Affine 変換前までは図 5 の従来提案されていた Multiplicative Masking とほぼ同様であるが，逆元演算後の再加算マスク処理において，am ⊗ mm^{-1} を加算するのではなくもとの加算マスクとは異なる am_1 を加算する．したがって，図 5 では，D ⊕ am から D^{-1} ⊕ am が得られていたのに対して，本方式では D ⊕ am_0 から D^{-1} ⊕ (am_1 ⊗ mm_1)が得られる．すなわち，従来法では逆元演算結果に同じ加算マスク am でマスクが行われていたのに対し，提案手法では，ラウンドごとに異なる加算マスクとなり，本例では am_1 ⊗ mm_1 が新しいラウンドの加算マスクとして使用されている．2.1 節でも述べたように，ラウンドごとに新しい加算マスクを適用することにより HD-CPA 攻撃に対する耐性を向上させることができるため，ラウンドごとに新しい加算マスクとなることは望ましい．さらに，従来法では，am ⊗ mm^{-1} の加算マスクを準備するために mm の逆元演算が必要であったが，本提案方式ではこの演算も不要になり回路面積の増加も抑えることができる．

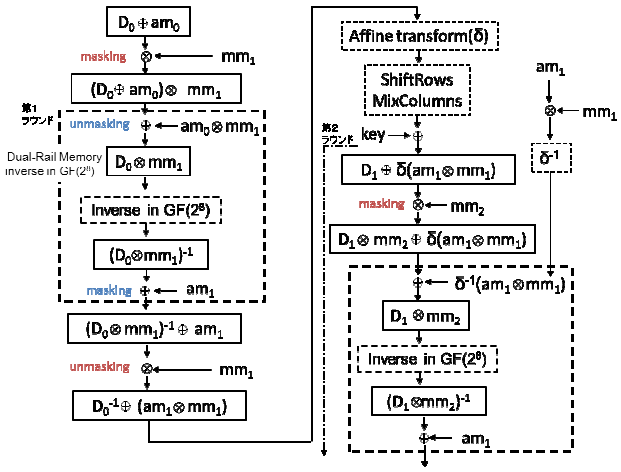


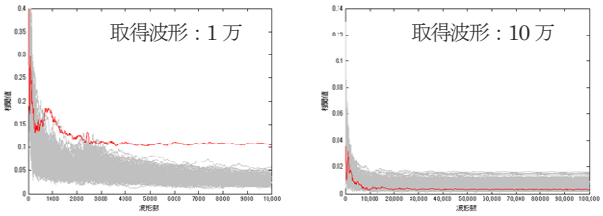
図 9．HMD-RSL メモリ方式のマスキングの流れ（暗号化時）

このような対策を施した HMD-RSL メモリ方式 AES 暗号回路を設計・試作したため，その耐性評価結果及び試作した LSI の面積や消費電力等を 3.2 節，3.3 節にて記述する．

3.2　HMD-RSL メモリ方式 AES の耐性評価

本節では，提案する HMD-RSL メモリ方式 AES に対し電力解析攻撃耐性評価を行った結果について示す．耐性評価には消費電力解析ツール Prime Time PX を用いて消費電力波形を 10 万波形取得し，HW-CPA, HD-CPA, Zero-Value DPA を行った．また，比較のためテーブル方式の未対策 AES 暗号回路（以下 TBL_AES）に対しても 1 万波形に対し攻撃を行った．図 1 0 に HW-CPA 攻撃を行った際の，1 つの SBox に対する，正解鍵とその他の鍵の相関値の遷移を示す．未対策回路では約 3 千波形で，正解鍵が特定できているが，HMD-RSL メモリ

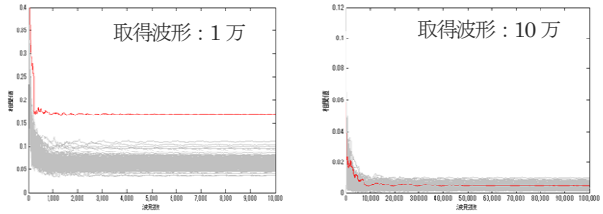
方式では10万波形でも全く正解鍵は特定できなかった．その他の鍵に対しても，同じ結果となり，結論として10万波形ではHW-CPA攻撃は成功しないことを確認した．



(a)TBL_AES　(b)HMD-RSLメモリ方式AES

図１０．HW-CPA結果（赤色：正解鍵）

図１１にHD-CPA攻撃を行った際の結果，図１２に提案方式AESに対し2.2節の図６図７でSBox回路においては耐性を示していたZero-Value DPAを行った結果を示すが，図１０と同様に，10万波形ではどちらの攻撃も成功しないことを確認した．図１３に，未対策回路と提案方式の鍵解明数の解析波形数依存性をまとめて示す．



(a)TBL_AES　(b)HMD-RSLメモリ方式AES

図１１．HD-CPA 結果（赤色：正解鍵）

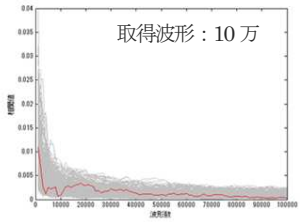


図１２．HMD-RSLメモリ方式AESに対するZero-Value DPA 結果（赤色：正解鍵）

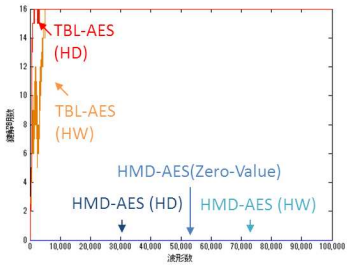


図１３．各攻撃による鍵解明数の比較

3.3　HMD-RSLメモリ方式AES暗号回路の試作

HMD-RSL メモリ方式を適用した AES 暗号回路を0.18μmCMOS プロセスを用いて設計・試作を行った．チップのレイアウト図を図１４に示す．Dual-Rail RSLメモリは2KbitのROMセルアレイで構成され，このメモリブロックを16個配置することで，SubByte変換に必要な逆元演算回路を構成している．

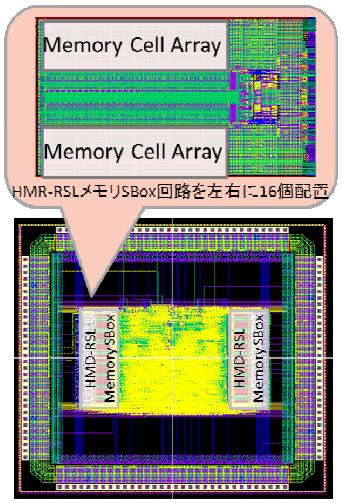


図１４．HMD-RSLメモリ方式を用いたSBox回路及びAES暗号回路のレイアウト

テーブル方式未対策回路と，Dual-Rail RSLメモリ方式，本論文で提案するHMD-RSLメモリ方式の，論理ゲート数と速度を表１に，メモリ面積を含む面積比較結果を図１５にまとめた．HMD-RSLメモリ方式の面積は，未対策回路の13%増，Dual-Rail RSL Memory方式の10%減であった．Dual-Rail RSL Memory方式の面積が１章より増加しているのは，電源配線等の改良によりメモリ部の面積が増加したためである．

表１．論理ゲート数と速度

	ゲート数[個]	クリティカルパス[ns]	速度[MHz]
Dual-Rail RSL メモリ方式	10211	34.68	28.83
HMD-RSL メモリ方式	19859	38.11	26.24

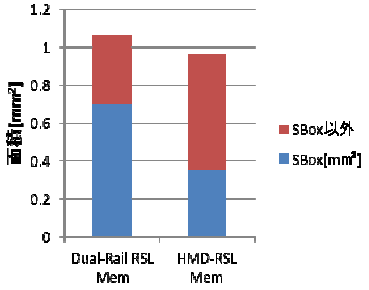


図１５．Dual-Rail RSLメモリ方式とHMD-RSLメモリ方式での各AES暗号回路の面積

従来のDual-Rail RSLメモリ方式では暗号化・復号化

でそれぞれの SBox 回路が必要だったところを，本方式ではメモリの格納内容を GF(2^8)逆元演算をとしたため，SBox 回路を共有化でき，SBox 回路の占める回路面積を半減させることができた．したがって表 1 に示すように乗算マスクの生成やアファイン変換等のため，論理ゲート数がほぼ倍増したのにもかかわらず，全体としては面積削減を達成することができた．

速度に関しては，HMD-RSL メモリ方式は演算処理が複雑化したために約 10%の速度低下であった．

4　まとめと今後の課題

本稿では，サイドチャネル攻撃に強い耐性を持つ対策手法として，我々が提案してきた Dual-Rail RSL メモリ方式に，Multiplicative masking を併用する HMD-RSL メモリ方式の提案を行った．本方式は SubByte 変換回路においてマスキング対策とバランシング対策の二重の対策を実現するため，高い再度チャネル攻撃耐性が期待できる．HMD-RSL メモリ方式は従来提案されてきた Multiplicative masking と異なり，Zero Value 攻撃には耐性があることを消費電力シミュレーションにより確認した．本方式では，SubByte 変換に GF(2^8)逆元演算を用いることで，メモリを暗号化・復号化で共有することができるため，SBox の面積を半減でき，AES 暗号回路全体としても面積を 10%縮小することができた．

今後は試作したチップを用いて，HW-CPA，HD-CPA，Zero Value 攻撃や高次の電力差分攻撃，さらに電磁波解析攻撃の評価を行っていく予定である．

謝辞

本研究は JST,CREST「ディペンダブル VLSI システムの基盤技術」の研究の一環として行われた．SASEBO-RII を用いたサイドチャネル攻撃環境の情報提供とボード改造にご協力いただいた産総研佐藤証様，片下敏宏様，堀洋平様に感謝いたします．また，チップ試作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，ローム(株)の協力で行われた．関係各位に感謝いたします．

参考文献

[1] P. Kocher, J. Jaffe, and B. Jun, “Differential Power Analysis,” In M. Wiener, editor, Advances in Cryptology CRYPTO’99, vol.1666 of Lecture Notes in Computer Science, pp.388-397, Berlin, Heidelberg.

[2] E.Brier, C. Clavier, F. Oliver, “Correlation Power Analysis with a leakage model,” CHES2004, LNCS3156 of Lecture Notes in Computer Science, pp.16-29, Springer, Berlin, Heidelberg, NewYork, 2004.

[3] K. Tiri and I. Verbauwhede, “A Logic Level Design Methodology for a Secure DPA Resistant ASIC or FPGA Implementation,” DATE’04 vol.1, pp.10246-10251, 2004.

[4] David D. Hwang, Kris Tiri, Alireza Hodjat, Student Bo-Cheng Lai, Shenglin Yang, Patrick Schaumont, Ingrid Verbauwhede, “AES-Based Security Coprocessor IC in 0.18-µm CMOS With Resistance to Differential Power Analysis Side-Channel Attacks,” IEEE JOURNAL OF SOLID-STATE CIRCUITS, VOL. 41, NO. 4, APRIL 2006.

[5] E. Trichina, “Combinational Logic Design For AES SubByte Transformation On masked Date,” Cryptologye Print Archive, 2003/236, 2003.

[6] T.Pop,S.Mangard, “Masked Dual-Rail Pre-charge Logic：DPA-Resistance Without Routing Constrain,” CHES2006, LNCS4249, pp.255-259, Springer-Verlag, 2006.

[7] 橋本祐樹，汐崎充，久保田貴也，藤野毅，“Dual-RailRSL メモリ方式を利用したサイドチャネル攻撃耐性を有する AES 暗号回路”, ICD2012-84, pp.43-48, 2012.

[8] S. Nikova, C. Rechberger, V. Rijmen, “Threshold Implementations Against Side-Channel Attacks and Glitches,” ICICS2006, LNCS4307, pp.529-545, Springer, 2006.

[9] 岩井克彦，汐崎充，小島憲司，浅川俊介，藤野毅，“Domino-RSL 方式を用いた DPA 耐性を持つ DES 暗号回路の設計試作と安全性評価”, VLD2010-126, pp. 57-62, 2011.

[10] D. Suzuki, M. Saeki, T. Ichikawa, “DPA Leakage Models for CMOS Logic Circuits,” CHES2005, LNCS3659, pp.366-382, 2005.

[11] 小島憲司，岩井克彦，汐崎充，藤野毅，“ドミノ RSL 方式を用いた DES 暗号回路におけるアーリープロパゲーション効果による DPA リークの評価, ” SCIS2011，小倉, 日本, 2011.

[12] M. Akkar, C. Giraud, ” An implementation of DES and AES, secure against some attacks”, Cryptographic Hardware and Embedded Systems, CHES 2001, LNCS 2162 (2001) 309–318

[13]J.D.Goli´c, C.Tymen, “Multiplicative Masking and Power Analysis of AES”, In: Kaliski Jr., B.S., Ko¸c, C¸ .K., Paar, C. (eds.) CHES 2002. LNCS, vol. 2523, pp.198–212. Springer, Heidelberg, 2003.