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

2007－ＳＬＤＭ－132（８）
2007／11／20

暗号回路の電力差分解析攻撃に対して耐性があるドミノ型RSL回路の提案

豊田 善靖† 木戸 健太‡ 下林 義明‡ 藤野 毅‡

†立命館大学大学院 理工学研究科 〒525-8577 滋賀県草津市野路東1－1－1
‡立命館大学 理工学部 〒525-8577 滋賀県草津市野路東1－1－1
E-mail: † ‡ {re007020, ri002047, ri004042, fujino}@se.ritsumei.ac.jp

あらまし 耐タンパー性を備えた暗号回路を実現するためには、サイドチャネル攻撃に対する対策が必要である。特に電力差分解析(Differential Power Analysis: DPA)は、暗号鍵の推定にあたって最も有効な攻撃方法であるため、様々な対策法が提案されている。プリミティブゲートレベルでの対策法としては、ゲートの出力遷移確率を乱数により均一化するRSL(Random Switching Logic)方式が提案されている。この方式は原理的にもっとも優れた方式であると考えられるが、出力遷移確率を均一にするためにはハザードフリーであることが必要である。RSL 方式では、ハザードフリーを実現するために、ゲートを前段から順次駆動する非同期タイミング信号を用いているが、このタイミング信号の回路実装が難しく、動作速度を低下させるという欠点がある。本論文ではRSLと同様の動作をドミノ回路で実現する方式を提案する。ドミノ回路なので非同期許可信号を導入しなくても、ハザードフリーを実現できる。本方式の有効性を確認するため、ガロア体の乗算器回路を設計し、シミュレーションによるDPA耐性評価と、実レイアウトを使った回路実装面積の検証を行った。

キーワード サイドチャネル攻撃，電力差分解析，RSL，ドミノ回路，ガロア体

Proposal of domino-RSL circuit which is resistant to Differential Power Analysis attack on cryptographic circuit

Yoshinobu TOYODA† Kenta KIDO‡ Yoshiaki SHITABAYASHI‡ Takeshi FUJINO‡

† Graduate school of Science and Engineering, Ritsumeikan University

‡ Faculty of Science and Engineering, Ritsumeikan University
1-1-1 Nojihigashi, Kusatsu-shi, Shiga, 525-8577 Japan
E-mail: † ‡ {re007020, ri002047, ri004042, fujino}@ se.ritsumei.ac.jp

Abstract Countermeasures against Side Channel Attack are necessary to achieve cryptographic circuit that has tamper resistance. Many countermeasures, especially against DPA (Differential Power Analysis), are proposed because DPA is the most effective attack to estimate cipher key. RSL (Random Switching Logic) method that makes transition probability at each gate 1/2 using random value is proposed as a countermeasure at primitive gate level. The method is effective against DPA, but requires enable signal that controls drive timing at each gate to achieve hazard-free circuits. Therefore, the circuit becomes complex. In this paper, we propose domino-RSL circuit that achieves operation similar to RSL with the domino logic. The circuit doesn't require enable signal because domino logic is hazard-free. We evaluated our method about security against DPA and area of circuit using multiplier in Galois field.

Keyword Side Channel Attack, DPA, RSL, domino logic, Galois field

1. はじめに

情報化社会である現在ではデータの暗号化は必須であり、暗号技術はスマートカードなど多くのデバイスに実装されている。暗号アルゴリズムは非常に強固になってきており、これを直接解読するとなると膨大な時間と労力を費やすことになるため、暗号化されていればデータは安全であるといえる。

ところが、近年サイドチャネル攻撃の脅威が危惧されている。この攻撃は暗号アルゴリズムを直接解読するのではなく、暗号（復号）処理時にデバイスから生じる２次的な情報を解析することで秘密鍵を推定する。２次的な情報としては消費電力や電磁波、音響などが挙げられるが、特に消費電力の差分を統計処理する電力差分解析（Differential Power Analysis: DPA)はコストも少なく比較的容易に攻撃できるため、最も危険性が高いといわれている。

一般の CMOS 回路において、AND や OR ゲートのような非線形ゲートは出力値が'0'であるか'1'であるかに偏りがあるため、入力値に依存して消費電力が異なる。DPA ではこれを利用し以下の手順で暗号鍵を推定する。攻撃者はまず、多数の入力データに対する消費電力波形を取得する。次に秘密鍵の部分鍵の予測を行い、同時に秘密鍵に相関がある内部変数 1bit の値を選択関数 s と定め、その選択関数 s が入力データに対して'0'か'1'のどちらになるかを算出する。この値に従って消費電力波形を２つに分類し、それぞれのグループで波形を平均化してそれらの差分をとる。秘密鍵の予測が正しければ、s が処理されるタイミングで消費電力に明確な差が生まれ、波形に特徴的なスパイクが現れる。予測が外れていれば、波形をランダムに分類したことになり、スパイクは現れない。以上の攻撃をすべての部分鍵で繰り返すことで、秘密鍵が解読される[1]。

DPA 攻撃を無効にするためには、デバイスの内部変数の遷移確率と消費電力の相関がなくなるように、入力に依存せず各ゲートの遷移確率を一定にする対策が有効である。この概念を、乱数を用いて実現したものが RSL(Random Switching Logic)方式[2][3]である。この方式で出力遷移確率を均一にするためにはハザードフリーであることが必要である。RSL 方式では、ハザードフリーを実現するために、ゲートを前段から順次駆動する非同期タイミング信号を用いているが、このタイミング信号の回路実装が難しく、動作速度を低下させるという欠点がある。

本論文では、この RSL 方式を非同期タイミング信号の不要なドミノ回路で実現する方式を提案する。以下、第 2 章で DPA に関連する既存の技術を説明し、第 3 章で提案する方式を、第 4 章でガロア体への実装を、第 5 章で実装結果を、第 6 章でまとめと今後の課題を述べる。

2. 各種の DPA 対策方式

2.1. DPA 対策方式の分類

DPA対策はその対策法によってアルゴリズムレベルの対策とプリミティブゲートレベルの対策に分類される。アルゴリズムレベルの対策では、乱数を用いてデータをマスク（XOR 処理）することで、暗号アルゴリズムそのものを DPA 対策用に作り変える。

一方、プリミティブゲートレベルの対策では、AND や OR などのプリミティブゲートを DPA 対策用のものに置き換える。アルゴリズムレベルの対策とは異なり、DPA の原因を根本から絶つことになるため、より効果が高いと考えられる。また、プリミティブゲートに対策を施すので、様々な暗号回路で使用できるため汎用性が高いといえる。

プリミティブゲートレベルの対策はさらに２つの型に分類できる。１つはランダムマスク型であり、真のデータを乱数でマスクすることで消費電力を均一化する。初期のランダムマスク型としては、Masked-AND 方式[4]が挙げられるが、内部信号遅延によりハザードが発生し DPA に対する脆弱性が指摘された[5]。

もう１つは２線相補型である。これは、正論理動作と負論理動作を行うゲートを対に置き、同時に動作させることで、消費電力の均一化をはかるものである[6][7]。しかし、相補動作を行うゲートの入出力間の寄生容量が等しくなるように設計する必要があり、これを実現することは難しいことが指摘されている[8]。

2.2. RSL 方式による DPA 対策

2.1 節における問題点を解決するために、乱数を用いて２線相補型の概念を１線で実現したのが RSL 方式である。この方式は乱数によって正論理と負論理を切り替えることで、遷移確率の偏りをなくしている。

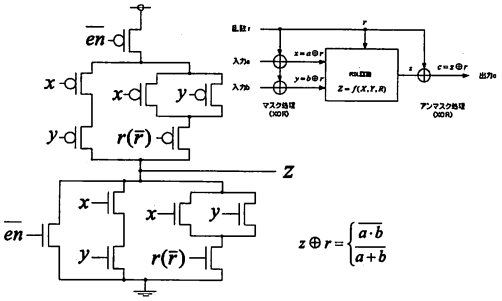


図 1　RSL-NAND/NOR

図 1 に示す RSL-NAND/NOR ゲートでは、乱数 r が 0 のときに正論理動作(NAND)を行い、1 のときに負論理動作(NOR)を行う。真の入力 a, b は乱数 r によってマスクされ、出力時に同じ乱数 r でアンマスクされる。また、すべての入力信号が到着してから非同期許可信号 en を 1 にすることでハザード問題を解決している。さらに、２線式ではないため、相補動作を行うノードの寄生容量を考慮する必要もない。

RSL 方式には、NAND/NOR, XOR/XNOR ゲートの両方に許可信号 en を与えて完全なハザードフリーを実現した初期の提案手法[2][3]と、非線形素子である NAND/NOR ゲートだけに許可信号 en を用い、線形素子である XOR には通常ゲートを用いる改良型 RSL[9][10]の２種類の方法がある。改良型 RSL では Second-order DPA 対策を行うため、RSL ゲートごとに異なった乱数を使う。これによりハザードの発生する通常の XOR ゲートを使用することが可能になっている。本論文では初期型の RSL 回路をリファレンスとして以降の議論を進める。

2.3. MRSL 方式による DPA 対策

RSL 回路における非同期タイミング信号 en を排除する目的で RSL を改良したのが、MRSL (Modified RSL) 方式[11][12]である。この方式では、図 2 のようにマルチプレクサを用いて動作前に入力信号の初期化処理を行う。積和回路などを実現する場合においては、ゲートごとに許可信号が必要になる RSL に対して、MRSL では回路の初段のみにマルチプレクサをおくだけでよい。したがって、設計が容易になり、また回路規模も削減できると紹介されている。

ただし、非線形回路（AND/OR 等）だけを用いた積和回路では初期化によってハザードフリーは実現されるが、線形回路（XOR 等）ではハザードが発生する。これに対しては乱数を用いて初期化を行うことで遷移確率を一定にすると紹介されている。

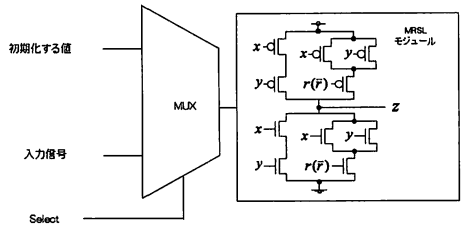


図 2　MRSL-NAND/NOR

3. domino-RSL 回路を用いた DPA 対策

3.1. 基本概念

我々は、RSL と同じ概念を用い、MRSL と同様に LSI の実装上難しい非同期タイミング信号を排除する方法の検討を行った結果、ドミノ回路をベースとする回路を提案する。

ドミノ回路は古くからハザードフリーの高速回路として知られており、これを用いて RSL 型の AND/OR 回路を実現すると図 3 のようになる。

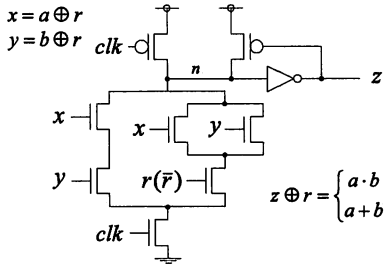


図 3　domino-RSL-AND/OR

ドミノ回路は clk=0 のプリチャージ期間に PMOS トランジスタでノード n を充電し、clk=1 の評価（evaluate）期間に演算論理が組まれた NMOS トランジスタで放電することにより動作する。出力ノード z は clk=1 の評価期間中に、0 から 1 に 1 度しか遷移しないため、ハザードは生じない。またプリチャージ開始時にはすべてゲート出力が一斉に 0 にされる。図 3 の回路では、乱数 r が 0 のときは AND 動作（正論理）、1 のときは OR 動作（負論理）を行う。MRSL とは異なり乱数 r はプリチャージ期間中に設定されるため、文献[13]で MRSL に対して指摘された乱数 r の信号伝達時間に伴う、DPA リークは無いと考えられる。また、1 つのゲートを作成するために必要なトランジスタ数は、図 1 に示される RSL-NAND/NOR ゲートが 12 個必要であるのに対し、domino-RSL-AND/OR ゲートは 10 個で実現でき、ゲート面積の観点からも有利である。

3.2. 積和標準形組み合わせ回路

ドミノ回路ではプリチャージ期間中は、すべてのゲートに 0 を入力しなければならない。つまり、組み合わせ回路中では、すべての入力が 0 のときに 0 を出力する素子しか使えない。すなわち、パイプラインの途中段では XNOR 回路や NOT 回路は使用できない。このため、実現すべき論理式は下記のように AND と OR で表される積和標準形に変更する必要がある。

$$f = a\cdot\bar{b} + \bar{a}\cdot b$$

たとえば、XOR を使用するときには、図 4 のように入力初段にのみ否定論理が存在する積和標準形を用いたゲートに展開する必要がある。

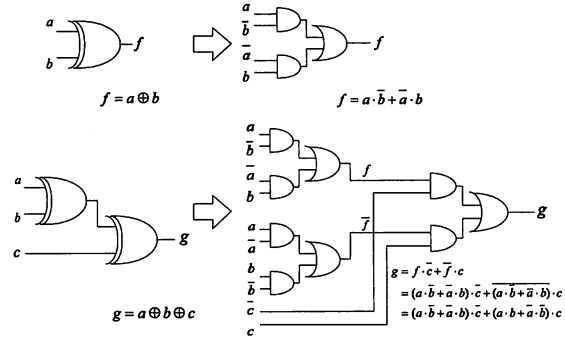


図 4　XOR を積和標準形に展開

3.3. 入力信号制御

上述のように積和標準形のゲート論理を用いた場合、パイプラインの入力初段に否定論理を使用する必要がある。この否定論理入力も、プリチャージ期間中（clk=0）は必ず 0 を出力し clk=1 となると同時に所定の論理に変化し、評価（evaluate）期間中は同じ信号を出力し続けなければならない。このパイプライン初段の入力制御回路を図 5 に示す。この回路をドミノ回路におけるすべての入力に設置することで、回路を正常に動作させることができる。

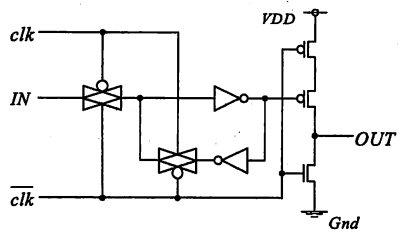


図5　入力信号制御回路

4. GF(2²)上の乗算器への実装

提案する domino-RSL 方式の効果を検証するため、ガロア体（GF(2²)）上の乗算器を作成した。ガロア体上の演算は次世代の共通鍵暗号である AES の S-box 等にも用いられており（GF(2⁸)の逆元演算）、共通鍵暗号に対する DPA 対策の検証としてこの演算を用いることは有効であるといえる。

4.1. ガロア体上の演算

ガロア体（GF(2ᵐ)）上の演算は通常の四則演算とは異なる。1bit 同士の加算は XOR で表され、キャリーがない。また、1bit 同士の乗算は AND で表される[14]。多ビットの乗算の流れは、まず部分積を求めるためにビットごとの AND をとり、得られた部分積同士で XOR を行う[15]。つまり、AND と XOR があれば、ガロア体上の乗算は実現できる。図6に GF(2²)上の乗算器（規約多項式：x^2+x+1）の論理式と回路図を、表1に真理値表を示す。

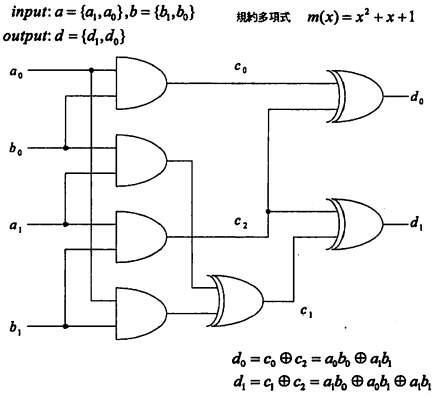


図6　GF(2²)上の乗算器（通常）

表1　GF(2²) 規約多項式 x^2+x+1 の乗算テーブル

·	00	01	10	11
00	00	00	00	00
01	00	01	10	11
10	00	10	11	01
11	00	11	01	10

4.2. RSL 回路を用いた実装

図6に示した演算回路を RSL で実装すると図7の回路図になる（RSL 回路は NAND/NOR 系）。この回路は en 信号制御部で buffer を用いて en 信号を遅延させることで、ハザード防止を行っている[10]。なお、3入力の素子を用いると、さらに回路規模は削減できるが、今回はすべて2入力の素子を用いるものとする。

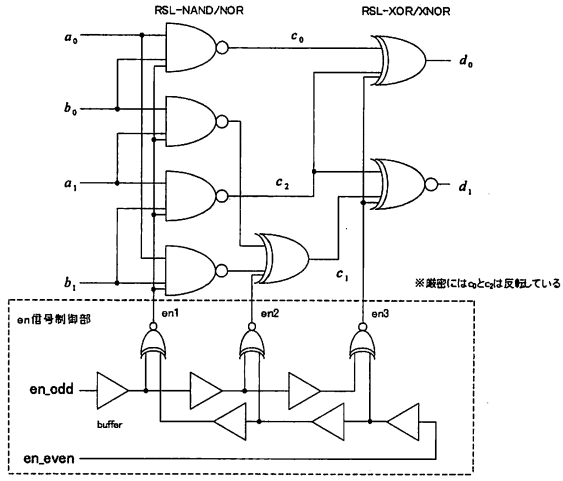


図7　GF(2²)上の乗算器（RSL）

4.3. domino-RSL 回路を用いた実装

図6の乗算回路をドミノ回路で実装できるように積和標準形に展開すると以下のようになり、回路図は図8のようになる。

$$
\begin{aligned}
d_0 &= c_0 \oplus c_2 = a_0b_0 \oplus a_1b_1 = a_0b_0\overline{a_1b_1} + \overline{a_0b_0}a_1b_1 \\
&= a_0b_0(\overline{a_1}+\overline{b_1}) + a_1b_1(\overline{a_0}+\overline{b_0}) \\
d_1 &= c_1 \oplus c_2 = a_1b_0 \oplus a_0b_1 \oplus a_1b_1 = (a_1b_0 \oplus a_0b_0)\overline{a_1b_1} + \overline{(a_1b_0 \oplus a_0b_0)}a_1b_1 \\
&= (a_1b_0\overline{a_0b_0} + \overline{a_1b_0}a_0b_0)(\overline{a_1}+\overline{b_1}) + (a_1b_0a_0b_0 + \overline{a_1b_0a_0b_0})a_1b_1 \\
&= \{a_1b_0(\overline{a_0}+\overline{b_0}) + (\overline{a_1}+\overline{b_0})a_0b_0\}(\overline{a_1}+\overline{b_1}) + \{a_1b_0a_0b_0 + (\overline{a_1}+\overline{b_0})(\overline{a_0}+\overline{b_0})\}a_1b_1
\end{aligned}
$$

まず部分積とその否定論理を演算する。この AND ゲートと OR ゲートはどちらも図3に示した domino-RSL-AND/OR であり、乱数 r を否定入力するかどうかで AND と OR が区別される。3.4節に示したように、XOR 演算はそれらの論理（部分積とその否定論理）を用いて積和演算を行うことで実現できる。図中2つの AND ゲートと1つの OR ゲートで構成された積和（Sum Of Product）形式で示された回路は15個のトランジスタで構成される1つの複合ゲートで表すことができる。このゲートも domino-RSL 型であり、以降 domino-RSL-SOP ゲートと呼ぶ。なお、図8の回路では乱数 r、clk 信号、入力信号制御回路（3.3節参照）、mask 処理部は省略してある。

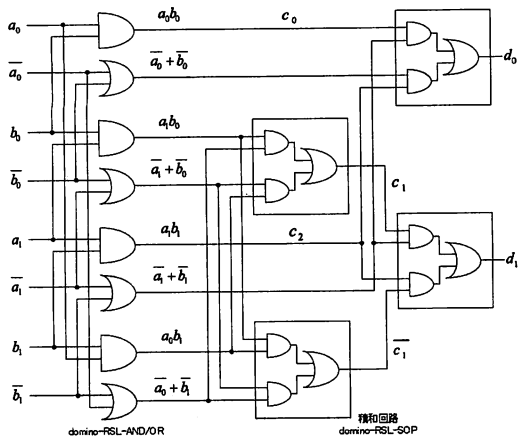


図８　GF(2^2)上の乗算器（domino-RSL 回路）

5. 実装結果

5.1. 消費電力測定結果

図７、８の回路で Synopsys 社の回路シミュレータ HSPICE を用いて消費電力測定を行った。入力信号は乱数 r も含めて 5bit であり、これらすべての入力パターンにおける消費電力を測定した。一般的には、前の演算状態からの遷移を考える必要があるが、どちらの回路も演算前に回路中のすべてのノードは 0 となる。したがって、すべての測定結果は全ノードが 0 の状態からの遷移における消費電力といえる。このようにして得られた全測定結果を選択関数 s で分類し、それぞれの平均消費電力の差分をとった。選択関数としては、入力 a_1, b_1, 出力 d_0, d_1（すべてマスクされていない状態を考える）を採用した。DPA 対策を考えない通常の演算の結果は、r=0 のときの測定結果のみを使用した。

表２ GF(2^2)上の乗算器の平均消費電力差分（RSL）

①選択関数s=a1とする

	平均消費電力(10^{-4}W)		消費電力差分	平均電力に対する
	s=1のとき	s=0のとき	(10^{-4}W)	割合(%)
対策なし(r=0)	2.9904	3.2481	-0.2577	8.28
対策あり(全て)	2.8040	2.7920	0.0121	0.43

②選択関数s=b1とする

	平均消費電力(10^{-4}W)		消費電力差分	平均電力に対する
	s=1のとき	s=0のとき	(10^{-4}W)	割合(%)
対策なし(r=0)	2.9727	3.2658	-0.2931	9.40
対策あり(全て)	2.7946	2.8014	-0.0069	0.25

③選択関数s=d1とする

	平均消費電力(10^{-4}W)		消費電力差分	平均電力に対する
	s=1のとき	s=0のとき	(10^{-4}W)	割合(%)
対策なし(r=0)	3.0186	3.1796	-0.1611	5.16
対策あり(全て)	2.7883	2.8039	-0.0156	0.56

④選択関数s=d0とする

	平均消費電力(10^{-4}W)		消費電力差分	平均電力に対する
	s=1のとき	s=0のとき	(10^{-4}W)	割合(%)
対策なし(r=0)	3.0853	3.1396	-0.0542	1.74
対策あり(全て)	2.8159	2.7873	0.0286	1.02

表３　GF(2^2)上の乗算器の平均消費電力差分（domino-RSL）

①選択関数s=a1とする

	平均消費電力(10^{-4}W)		消費電力差分	平均電力に対する
	s=1のとき	s=0のとき	(10^{-4}W)	割合(%)
対策なし(r=0)	2.0827	1.9964	0.0863	4.23
対策あり(全て)	2.0923	2.0918	0.0006	0.03

②選択関数s=b1とする

	平均消費電力(10^{-4}W)		消費電力差分	平均電力に対する
	s=1のとき	s=0のとき	(10^{-4}W)	割合(%)
対策なし(r=0)	2.0736	2.0055	0.0681	3.34
対策あり(全て)	2.0833	2.1008	-0.0175	0.84

③選択関数s=d1とする

	平均消費電力(10^{-4}W)		消費電力差分	平均電力に対する
	s=1のとき	s=0のとき	(10^{-4}W)	割合(%)
対策なし(r=0)	2.1752	1.9582	0.2170	10.64
対策あり(全て)	2.1017	2.0863	0.0154	0.74

④選択関数s=d0とする

	平均消費電力(10^{-4}W)		消費電力差分	平均電力に対する
	s=1のとき	s=0のとき	(10^{-4}W)	割合(%)
対策なし(r=0)	2.1560	1.9697	0.1863	9.13
対策あり(全て)	2.0856	2.0959	-0.0103	0.49

RSL 回路での測定結果を表２に、提案する domino-RSL 回路での測定結果を表３に示す。

表中の「平均電力に対する割合」とは、全測定結果の平均消費電力に対するそれぞれの消費電力差分の割合を示している。この割合が高いほど差分波形のスパイクがより顕著になり、DPA の危険性が高いといえる。測定結果より、DPA 対策をすることによってこの割合が約１％以下になっている。シミュレータの精度を考慮すると１％以下の消費電力差分は誤差とみなすことができ domino-RSL 回路の DPA 耐性は RSL 回路と同等であることが確認できた。

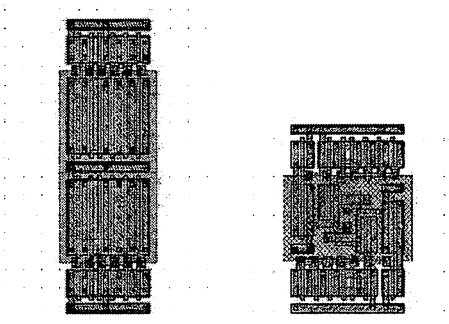
5.2. レイアウトによる面積計測と回路規模予測

domino-RSL 回路を作成するためには、3.2 節でも述べた様に積和標準形の組み合わせ回路を設計する必要があり、RSL-NAND/NOR 回路と異なる回路構成となるため、大規模な回路では LSI 実装面積の増大が危惧される。そこで、単体ゲートでのレイアウト面積と、多ビットのガロア体の乗算器を構成するために必要なトランジスタ数を RSL 回路と domino-RSL 回路で比較した。

0.18 μ mCMOS ルールで、図１、図３に示す RSL-NAND/NOR ゲートと domino-RSL-AND/OR ゲートをレイアウトし、２ゲートをならべた結果を図９に示す。また表４に２つの回路に対してトランジスタ数とレイアウト面積を比較した。トランジスタ数あたりの面積で比較すると、domino-RSL 型の方が面積が小さくなっているが、これは、RSL 型の方が、サイズを大きくしなければならない PMOS トランジスタ数が多いことに起因している。次にガロア体上の多ビットの乗算器を想定し、入力 bit 数の増加によってどの程度トランジスタ数が増加するのかを算出した。これを表５に示す。

ただし、RSLには非同期タイミング信号enの発生・制御回路が必要であるが、この評価にはそれらの回路は含まれていない。

XORゲートを積和標準形に展開することで、回路規模が大幅に増加する懸念があったが、domino-RSL回路ではRSLに比べてトランジスタ数にして20%程度増える程度に収まっており、表4に示したトランジスタ数あたりの面積がdomino-RSL型の方が小さいことを考慮すると回路面積はほぼ同等になると予測される。



(a) RSL-NAND/NOR (b) domino-RSL-AND/OR

図9 Virtuosoによるレイアウト

表4 トランジスタ数とレイアウトによる回路規模の比較

	トランジスタ数(個)	レイアウトによる素子1つ分の面積(μm^2)	トランジスタ1つあたりの面積(μm^2)
RSL-NAND/NOR	12	36.21	3.02
domino-RSL-AND/OR	10	28.92	2.89
RSLに対するdomino-RSLの比率(%)	83.33	79.87	95.84

表5 ガロア体上の乗算器における入力bit数の増加による合計トランジスタ数の推移

RSL

入力bit数	2	3	4	8
RSL-NAND/NOR (12)	4	9	16	64
RSL-XOR/XNOR (28)	3	8	14	76
合計	132	332	584	2896

domino-RSL

入力bit数	2	3	4	8
domino-RSL-AND (10)	8	18	32	128
domino-RSL-SOP (15)	4	13	26	144
合計	140	375	710	3440
規約多項式	x^2+x+1	x^3+x+1	x^4+x+1	$x^8+x^4+x^3+x+1$

※()内の数字は各ゲート1つあたりのトランジスタ数を表す。

6. まとめと今後の課題

本論文では、DPA対策手法としてRSL方式と同じ概念ではあるが、非同期タイミング信号enを必要としない回路をドミノ回路を用いて実現するdomino-RSL方式を提案した。さらに、提案する方式をガロア体$GF(2^2)$上の乗算器に実装してRSL方式と比較することで、DPA耐性や回路規模を検証した。その結果、ほぼ同等の回路規模で、RSL方式と同等のDPA耐性を持った完全にハザードフリーな回路を実現することができた。

今回は$GF(2^2)$上の乗算器という非常に小規模な回路で実装を行った。次の課題として、AESのs-boxなど実際にDPAのターゲットとなる回路を設計し回路規模・設計の容易性の評価を行うとともに、実際にチップを作成し実デバイスのDPA耐性の評価を実施する予定である。また、本方式はSecond-Order DPAに関しては検討を行っていないため、これも今後の課題である。

文 献

[1] P. Kocher, J. Jaffe, and B. Jun, "Introduction to Differential Power Analysis and Related Attacks" http://www.cryptography.com/resources/whitepapers/DPA-technical.html

[2] D. Suzuki, M. Saeki, and T. Ichikawa, "Random Switching Logic: A Countermeasure against DPA based on Transition Probability" Cryptology ePrint Archive, 2004/346, 2004.

[3] 鈴木大輔, 佐伯稔, 市川哲也, "遷移確率を考慮したDPA対策手法の提案" ISEC 2004, pp.127-134, July, 2004

[4] E. Trichina, "Combinational Logic Design for AES SubByte Transformation on Masked Data" Cryptology ePrint Archive, 2003/236, 2003

[5] 市川哲也, 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" ISEC 2004, pp. 119-126, July, 2004

[6] K. Tiri and I. Verbauwhede "A Logic Level Design Methodology for a Secure DPA Resistant ASIC or FPGA Implementation" DATE 2004, 2004

[7] T. Popp and S. Mangard "Masked Dual-Rail Pre-Charge Logic: DPA-Resistance without Routing Constraints" CHES 2005, LNCS 3659, pp.172-186, 2005

[8] 鈴木大輔, 佐伯稔, "2線式回路によるDPA対策方式の安全性評価" SCIS 2006, January, 2006

[9] 鈴木大輔, 佐伯稔, 市川哲也, "RSLの安全性評価とハイブリッド型DPAに対する改良" SCIS 2005, January, 2005

[10] D. Suzuki, M. Saeki, and T. Ichikawa, "Random Switching Logic: A New Countermeasure against DPA and Second-Order DPA at the Logic Level" IEICE TRANS. FUNDAMENTALS, vol.E90-A, No.1 January 2007, pp.160-168, January 2007

[11] 佐々木稔, 岩井啓輔, 黒川恭一, "MRSLで構成したAESのS-BOX回路のDPA耐性検証" ISEC 2006, pp37-44, September, 2006

[12] 佐々木稔, 岩井啓輔, 黒川恭一, "AESのS-BOX回路のDPA対策設計" RECONF 2006, pp.1-6, November, 2006

[13] 佐伯稔, "信号遅延を考慮したDPA耐性評価－MRSLとDRSLの場合－" SCIS 2007, January, 2007

[14] 今井秀樹, 符号理論, (社)電子情報通信学会, 東京, 1990

[15] 森岡澄夫, "エラー訂正や暗号処理で使われる演算回路を極める" Design Wave Magazine, pp.57-67, July, 2003