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

2007－ＣＳＥＣ－38 (30)
2007／7／20

暗号回路のFPGA実装における簡易DPA対策

宋 長勲† 阿部 公輝†

† 電気通信大学 電気通信学研究科 情報工学専攻 〒 182-8585 東京都調布市調布ヶ丘 1-5-1
E-mail: †{corpsehoon,abe}@cacao.cs.uec.ac.jp

あらまし DPA 対策手法の 1 つである Random Switching Logic は乱数によりゲートごとの信号遷移を均等化してデータと消費電力の相関をなくす方法である．本研究では，暗号回路を FPGA へ実装する際，ゲートごとでなく演算ごとに入出力信号の遷移確率を均等化する DPA 対策を行った．AND ゲートで構成される暗号回路と DES の SBOX1 個を用いた暗号回路へこの対策を適用した結果，いずれの場合も DPA 耐性が向上することが分かった．この対策では，1 つの演算モジュールが複数の LUT(Look Up Table) に配置されることを考えると，これは FPGA のスイッチングマトリクス (Interconnect) による消費電力と回路からの情報リークの相関は大きくないことを意味する．ゲートごとでなく演算ごとにモジュール化されていればよいので，この対策の実装は簡易である．
キーワード サイドチャンネル攻撃，電力差分解析，FPGA，演算レベルでの対策

A Simple Countermeasure to DPA against FPGA Implementation of Cryptographic Device

Jang-hoon SONG† and Kôki ABE†

† Department of Computer Science, The University of Electro-Communications
1-5-1 Chofugaoka Chofu-shi,Tokyo 182-8585 Japan
E-mail: †{corpsehoon,abe}@cacao.cs.uec.ac.jp

Abstract Random Switching Logic is a countermeasure to DPA that removes the relation between data and power consumption by making the transition probability of each gate uniform using random numbers. In this paper, we applied a countermeasure to DPA against cryptographic devices implemented on FPGA. The countermeasure removes the relation between data and power consumption by making the transition probability of each operation instead of each gate. Results of experiments reveal that the countermeasure improves the DPA resistance. Considering that an operation module is placed on multiple LUTs, the results imply that the relation between information leak and power consumption of FPGA interconnects of switching matrix is insignificant. Implementation of the countermeasure is simple because the circuits are modularized at operation level instead of gate level.
Key words Side-channel Attack, Differential Power Analysis, FPGA, Countermeasure at Operation Level

1. はじめに

最近，Suica，PASMO，Edy などのスマートカードの普及が進んでいる．サイドチャンネル解析の一種である電力差分解析 (Differential Power Analysis, 以下 DPA) は，暗号デバイスの処理時間や消費電力などを測定することにより秘密情報を推定する攻撃であり [1], [2], [3]，DPA 対策を行っていない暗号回路のほとんどに対して有効である．スマートカードは偽造や変造ができないと言われているが，DPA には安全ではないため対策の重要性が高まっている．

DPA への対策は，演算素子を工夫するハードウェアレベルでの対策 [4], [5], [10] と演算方法やデータ表現方法を工夫するアルゴリズムレベルでの対策 [6], [7] がある．本論文では乱数により演算ごとに入出力信号の遷移確率を均等化する演算レベルでの DPA 対策を考え，FPGA へ実装する．

ゲートごとに入出力信号の遷移確率を均等化する RSL ゲート [10] は，FPGA 実装において 1 つの LUT(Look Up Table) に配置される．これは，FPGA のスイッチングマトリクスによる消費電力を考慮するためである．しかし，スイッチングマトリクスによる消費電力と回路からの情報リークとの相関は必ずしも明らかではない．この相関の程度によっては，ある演算の入出力信号の遷移確率が均等化されていさえすれば，その演

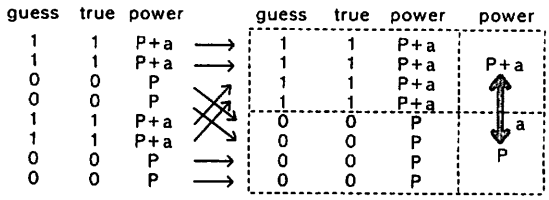

図 1 鍵の予想が正しい場合

Fig. 1 Case that the prediction of the key is correct.

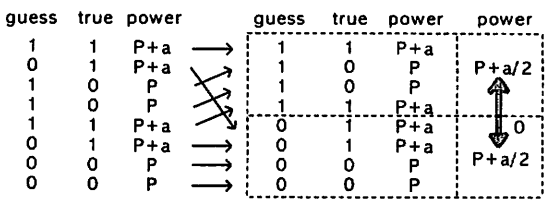

図 2 鍵の予想が正しくない場合

Fig. 2 Case that the prediction of the key is not correct.

算を複数の LUT に実装しても DPA 耐性が得られる可能性がある.

本研究では，上記の演算レベルでの DPA 対策を自動配置配線ツールを用いて FPGA へ実装し，DPA に対する耐性評価を行う．この DPA 対策実装は簡便であるので，実現される耐性が高ければ有用である.

以下，第 2 章で DPA の概要，第 3 章で関連研究，第 4 章で乱数を用いた演算レベルでの DPA 対策，第 5 章で評価実験の結果と考察を述べ，第 6 章でまとめる.

2. 電力差分解析

DPA は，繰り返し測定した消費電力波形をグループ分けし平均値の差分を取ることで，着目した演算以外の消費電力への影響を取り除き，鍵が消費電力に与える影響のみを取り出す手法である.

DPA では回路中のあるビット（参照値）に注目し，その参照値が 0 か 1 によって測定した消費電力のデータを 2 つのグループに分類する．演算に関係する鍵を予想すると，予想した鍵と既知の暗号文または平文から，参照値の予想値が得られる．この参照値の予想値を求める関数を選択関数と呼ぶ．鍵の予想が正しい場合，選択関数の値は実際の参照値と一致するため，選択関数の値により測定した消費電力のデータを分類すると，グループごとの消費電力の平均値には参照値による消費電力の差が生ずる (図 1)．これに対して鍵の予想が正しくない場合は，選択関数の値はほぼランダムになり，測定データもランダムに分類され，グループごとの消費電力の平均値の差はほぼ 0 になる (図 2)．よって，すべての鍵候補について選択関数の値により消費電力を分類してグループ毎の消費電力の平均値の差分を求めたとき，最大の差分を与える鍵が正しい鍵であることが期待される.

3. 関連研究

乱数によるデータマスクを用いたアルゴリズムレベルの対策として [6], [7] がある．文献 [6] は暗号回路の中の非線形部分への入力値をランダムで生成されるビット列を用いて XOR でマスクするものである．ここで使用するビット列は，非線形部分に入力されるビット長と同じ長さのビット列である．これは 1 ビットの乱数を使い，演算ごとに入出力の遷移確率を均等化する本手法と異なる．文献 [7] は AES において乱数を使い，アルゴリズムの最初にマスクし，別の演算を加えてアルゴリズムを実行し，最後にアンマスクする．これは演算ごとに乱数を用いて入出力の遷移確率を均等化する本手法と異なる.

ハードウェアレベルの対策として，Tiri ら [4] の SABL がある．これは基本演算素子で DPA 対策を行う．SABL をスタティック型 CMOS へ適用した SDDL と，SDDL を最適化した WDDL がある [5]．これらは 2 線式回路であるので，相補的な動作をするゲートが同じタイミングで動作し，かつ入出力間における配線容量が同じでなければ，DPA でピークがでる可能性がある．鈴木らは，相補動作を必要としない 1 線式の Random Switching Logic（以下 RSL）を提案した [10]．RSL は乱数成分をゲート内で同時に処理する方法でゲートごとの入出力の遷移確率を均等化させる．また，RSL ゲート [10] は，FPGA 実装において 1 つの LUT に配置される．これは，FPGA のスイッチングマトリクスによる消費電力を考慮したためである．しかし，スイッチングマトリクスによる消費電力と回路からの情報リークとの相関は必ずしも明らかではない．また RSL では，過度遷移を防ぐため許可信号を用いるが，過度遷移の程度によっては，許可信号を用いなくても DPA 耐性が得られる可能性がある.

4. 演算レベルでの DPA 対策

4.1 乱数マスクによる遷移確率の均等化

n 変数論理関数

$$z = f(a_1, \cdots, a_n) \tag{1}$$

を考える．均等分布乱数 $r \in \{0,1\}$ により，

$$z' = g(a_1, \cdots, a_n, r) = f(a_1 \oplus r, \cdots, a_n \oplus r) \oplus r \tag{2}$$

とすれば，

$$|g^{-1}(1)| = |g^{-1}(0)| \tag{3}$$

である．すなわち，関数 g のある入力 a_i，$i \in \{0,1\}$，の値に着目したとき，この関数の遷移確率は a_i の値によらず 1/2 になる．また関数 g の出力 z' の値に着目したとき，この関数の遷移確率は z' の値によらず 1/2 になる.

4.2 適用例 1

図 3 は AND ゲートを使った簡単な暗号回路である．この回路は 2 ビットの平文を入力とし，その平文と 2 ビット秘密鍵の XOR をとった値を AND ゲートへ入力し，その結果である 1

表 1　AND ゲートの遷移真理値表

Table 1　Truth table for AND-gate transition.

A	B	A'	B'	Y	Y'	Transition $Y \to Y'$
0	0	0	0	0	0	×
0	0	0	1	0	0	×
0	0	1	0	0	0	×
0	0	1	1	0	1	○
0	1	0	0	0	0	×
0	1	0	1	0	0	×
0	1	1	0	0	0	×
0	1	1	1	0	1	○
1	0	0	0	0	0	×
1	0	0	1	0	0	×
1	0	1	0	0	0	×
1	0	1	1	0	1	○
1	1	0	0	1	0	○
1	1	0	1	1	0	○
1	1	1	0	1	0	○
1	1	1	1	1	1	×

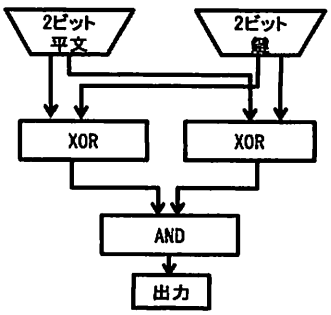

図 3　AND ゲートを使った暗号回路

Fig. 3　A cryptographic device using AND-gate.

ビットの値を暗号文とする．この回路の出力値に着目し，次の選択関数を採用したときの DPA を考える．

$$D(C_2, K_a) = AND(C_2 \oplus K_a) \tag{4}$$

ここで C_2 は予想する 2 ビット秘密鍵，K_a は 2 ビットの平文である．選択関数によって分けられたグループの波形の平均を求め，2 つのグループの差分を取る．秘密鍵 C_2 の範囲 $0 \leqq C_2 \leqq 3$ で，予想値を変えて行う．

表 1 は AND ゲートの遷移真理値表である．出力 Y' に着目して AND ゲートの遷移確率を求めると，$Y' = 0$ のときの遷移確率は $3/12 = 1/4$，$Y' = 1$ のときの遷移確率は $3/4$ である．よって，$Y' = 0$ のときと $Y' = 1$ のときの AND ゲートの DPA 電力差分の比は 1 : 3 となる．したがって，選択関数を AND ゲートの出力に設定して DPA を行った場合，参照値によって消費電力を分類すると，グループ毎の消費電力の平均値には差が生ずる [9]．

同じ暗号回路に対し 4.1 で述べた対策を施す（図 4）．図において RSL-AND と RSL-XOR は次式で表される関数である．

表 2　RSL-AND ゲートの遷移真理値表

Table 2　Truth table for RSL-AND-gate transition.

r	x_1	x_2	r'	x_1'	x_2'	Y	Y'	Transition $Y \to Y'$
0	0	0	0	0	0	0	0	×
0	0	0	0	0	1	0	0	×
0	0	0	0	1	0	0	0	×
0	0	0	0	1	1	0	1	○
0	0	0	1	0	0	0	1	○
0	0	0	1	0	1	0	1	○
0	0	0	1	1	0	0	1	○
0	0	0	1	1	1	0	0	×
1	0	0	0	0	0	1	0	○
1	0	0	0	0	1	1	0	○
1	0	0	0	1	0	1	0	○
1	0	0	0	1	1	1	1	×
1	0	0	1	0	0	1	1	×
1	0	0	1	0	1	1	1	×
1	0	0	1	1	0	1	1	×
1	0	0	1	1	1	1	0	○
0	0	1	0	0	0	0	0	×
0	0	1	0	0	1	0	0	×
0	0	1	0	1	0	0	0	×
0	0	1	0	1	1	0	1	○
0	0	1	1	0	0	0	1	○
0	0	1	1	0	1	0	1	○
0	0	1	1	1	0	0	1	○
0	0	1	1	1	1	0	0	×
1	0	1	0	0	0	1	0	○
1	0	1	0	0	1	1	0	○
1	0	1	0	1	0	1	0	○
1	0	1	0	1	1	1	1	×
1	0	1	1	0	0	1	1	×
1	0	1	1	0	1	1	1	×
1	0	1	1	1	0	1	1	×
1	0	1	1	1	1	1	0	○
0	1	0	0	0	0	0	0	×
0	1	0	0	0	1	0	0	×
0	1	0	0	1	0	0	0	×
0	1	0	0	1	1	0	1	○
0	1	0	1	0	0	0	1	○
0	1	0	1	0	1	0	1	○
0	1	0	1	1	0	0	1	○
0	1	0	1	1	1	0	0	×
1	1	0	0	0	0	1	0	○
1	1	0	0	0	1	1	0	○
1	1	0	0	1	0	1	0	○
1	1	0	0	1	1	1	1	×
1	1	0	1	0	0	1	1	×
1	1	0	1	0	1	1	1	×
1	1	0	1	1	0	1	1	×
1	1	0	1	1	1	1	0	○
0	1	1	0	0	0	1	0	○
0	1	1	0	0	1	1	0	○
0	1	1	0	1	0	1	0	○
0	1	1	0	1	1	1	1	×
0	1	1	1	0	0	1	1	×
0	1	1	1	0	1	1	1	×
0	1	1	1	1	0	1	1	×
0	1	1	1	1	1	1	0	○
1	1	1	0	0	0	0	0	×
1	1	1	0	0	1	0	0	×
1	1	1	0	1	0	0	0	×
1	1	1	0	1	1	0	1	○
1	1	1	1	0	0	0	1	○
1	1	1	1	0	1	0	1	○
1	1	1	1	1	0	0	1	○
1	1	1	1	1	1	0	0	×

$$\text{RSL-XOR} : z = x_1 \oplus x_2 \oplus r \tag{5}$$

$$\text{RSL-AND} : z = ((x_1 \oplus r) \cdot (x_2 \oplus r)) \oplus r \tag{6}$$

この対策により，RSL-AND の $Y' = 0$ のときと $Y' = 1$ のときの遷移確率は表 2 に示すように，各々 $32/64 = 1/2$ になって等しくなる．よって，DPA 電力差分は 0 になると期待される．

4.3　適 用 例 2

DES は 64 ビットの平文を 56 ビットの鍵を用いて暗号化を行う．暗号化は 16 ラウンドで行う．各々のラウンドではラウンド鍵との XOR や SBOX による転置が行われる．SBOX は

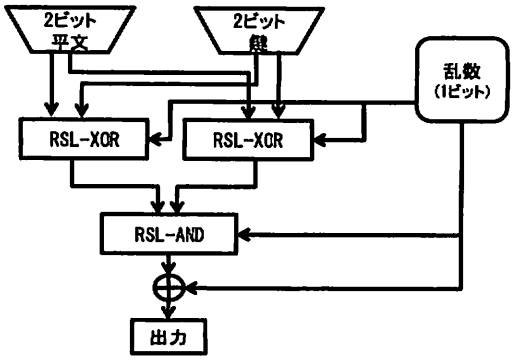

図 4　AND ゲートを使った暗号回路への DPA 対策

Fig. 4　Countermeasure applied to the cryptographic device using AND-gate.

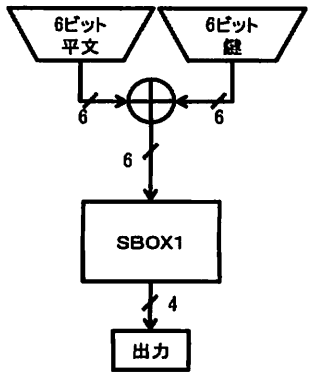

図 5　DES の SBOX1 個を用いた暗号回路

Fig. 5　A cryptographic device using an SBOX of DES.

表 3　SBOX1 の内容

Table 3　Contents of SBOX1.

14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

全部で 8 個あり，1 個の SBOX は 6 ビット入力 4 ビット出力である．ここでは DES 全体ではなく，1 個の SBOX を用いた暗号回路を考える（図 5）．

図において，SBOX1 は DES の SBOX 8 個のうち 1 番目のものである．SBOX1 への入力を $a_1, a_2, a_3, a_4, a_5, a_6$ とし，(a_1, a_6) の 2 進値を i，$(a_2, \cdots a_5)$ の 2 進値を j として，行 i，列 j の SBOX1 の値 $SBOX1(i, j)$ を表 3 に示す．

図 5 の回路に対し 4.1 で述べた対策を施す（図 6）．図において RSLT-SBOX1 への入力を $r, a_1, a_2, a_3, a_4, a_5, a_6$ とすると，出力 $z_1 z_2 z_3 z_4$ は次式で表される．

$$z_1 z_2 z_3 z_4 = SBOX1(a_1 a_2 a_3 a_4 a_5 a_6) \oplus r \tag{7}$$

$$a_1 = x_1 \oplus r, a_2 = x_2 \oplus r, a_3 = x_3 \oplus r,$$

$$a_4 = x_4 \oplus r, a_5 = x_5 \oplus r, a_6 = x_6 \oplus r$$

(r, a_1, a_6) の 2 進値を i，$(a_2, \cdots a_5)$ の 2 進値を j として，行

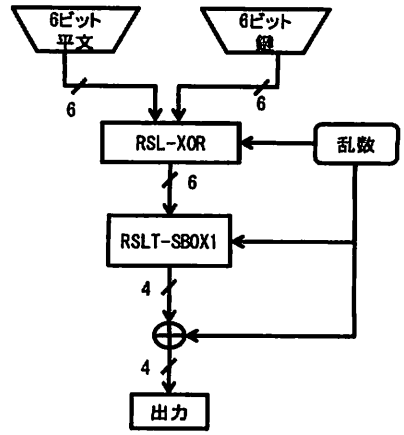

図 6　DES の SBOX1 個を用いた暗号回路への DPA 対策

Fig. 6　Countermeasure applied to the cryptographic device using an SBOX of DES.

i，列 j の RSLT-SBOX1 の値 $RSLT\text{-}SBOX1(i, j)$ を表 4 に示す．乱数でマスクした入力を，RSLT-SBOX1 に加え，結果をアンマスクする．この対策によって，RSLT-SBOX への入出力の遷移確率は等しくなり 2 つのグループの平均値の差分は 0 になると期待される．

この暗号回路の出力に着目した DPA を考える．DES に対して以下の選択関数が知られている [12]．

$$F_1(c_6, K_{16}) = SBOX1_1(c_6 \oplus K_{16}) \tag{8}$$

K_{16} は DES の第 16 ラウンドの $SBOX1$ への入力される 6 ビットの値に対応する秘密鍵，c_6 は K_{16} と XOR される既知の入力値，$SBOX1_1(x)$ は $SBOX1$ へ x が入力されたときの出力値の一番左の 1 ビットである．上記の式をこの暗号回路で考えると，c_6 が暗号回路への入力，K_{16} が 6 ビットの秘密鍵になる．

また参照値として複数ビットを用いた選択関数も知られている [13]．選択関数は次式で与えられる．

$$F_n(c_6, K_{16}) = SBOX1_n(c_6 \oplus K_{16}) \tag{9}$$

ここで，$SBOX1_n$ は $SBOX1$ の出力の第 n ビット $(1 \leqq n \leqq 4)$ である．これを基に，参照するビット数を 4 とし，平均の電力差分を次式で求める．

$$\Delta P = |\sum_{0 \leqq ||x|| < 2} A_x - \sum_{2 < ||y|| \leqq 4} A_y| \tag{10}$$

ここで，x, y は 4 ビットの列，$||x||, ||y||$ は x, y のハミングウェイト，A_x, A_y は参照値が x, y のグループの平均の消費電力である．式 (9) の $\sum_{0 \leqq ||x|| < 2} A_x$ は $A0000 + A0001 + A0010 + A0100 + A1000$，$\sum_{2 < ||y|| \leqq 4} A_y$ は $A1111 + A1110 + A1101 + A1011 + A0111$ を表す．

5. 評価実験

5.1 実験方法

前章で述べた対策を FPGA ディバイスへ実装する．実験に用

表 4　RSLT-SBOX1 の内容

Table 4　Contents of RSLT-SBOX1.

14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13
2	9	15	5	1	12	4	10	8	14	6	11	13	7	3	0
15	10	5	12	8	6	3	0	4	13	9	2	7	1	14	11
7	12	10	6	4	3	9	5	14	2	13	1	11	8	0	15
8	15	6	10	3	9	5	12	7	4	0	13	14	2	11	1

いる FPGA ディバイスは FLEX10K10LC84-4 [14] (Altera 社) である．FLEX10K は図 7 のように LAB(Logic Array Block) と EAB(Embedded Array Block) のマトリックスとそれらを繋ぐ Interconnect で構成されている．LAB は 8 つの LE(Logic Elements) の集まりである．各 LE は 4 入力 1 出力の LUT とフリップフロップなどで構成されている．FLEX10K10LC84-4 は 72 個の LAB と 3 つの EAB を持つ．

暗号アルゴリズムを構成する各演算ごとに，ハードウェア記述言語で記述し自動論理合成して得られたネットリストをモジュール化する．モジュール化により，演算ごとに入出力信号の遷移確率が均等化される．モジュール化されたネットリストを用いて暗号アルゴリズムを記述し，自動論理合成を行い自動配置配線して FPGA のコンフィグレーションを行う．

実装した暗号回路への DPA 攻撃回路を図 8 に示す．暗号回路の消費電力を測定するために電源供給端子に 10 Ω の抵抗を挿入し，両端を差動プローブを用いてオシロスコープで測定する．制御回路は暗号回路への平文と乱数およびオシロスコープへのトリガー信号を発生させる．暗号回路と制御回路の電源は各々独立とした [11]．測定周波数は 4MHz である．

表 5 に実験環境をまとめて示す．

表 5　実験環境

Table 5　Experimental environment.

記述言語	Verilog-HDL
実験デバイス	FLEX10K10LC84-4
論理合成配置配線	Altera QuartusII (Ver. 5.0)
デジタルオシロスコープ	YOKOGAWA DL1620

5.2　実験結果と考察

5.2.1　適用例 1

図 4 の回路を FPGA 上に実装したときのレイアウトを図 9 で示す．この回路は 1 つの LAB に配置されており，RSL-AND, RSL-XOR(2 個)，暗号文を乱数でアンマスクする XOR が上から順に 4 個の LE に配置されている．

図 10 は未対策の暗号回路（図 3）の消費電力波形を示す．クロック電圧は 50 で割って示してある．暗号回路の鍵は 01_2 である．(a) の波形は $AB \rightarrow A'B' = 00_2 \rightarrow 01_2$, $Y \rightarrow Y' = 0 \rightarrow 0$ のときの波形で，(b) の波形は $AB \rightarrow A'B' = 00_2 \rightarrow 10_2$, $Y \rightarrow Y' = 0 \rightarrow 1$ のときの波形である．クロック信号が立ち上がるとゲートへの入力値の変化に応じて出力値も変わる．図 10(a) では出力値の遷移がない（$Y \rightarrow Y' = 0 \rightarrow 0$）のに対し，(b) では出力値の遷移がある（$Y \rightarrow Y' = 0 \rightarrow 1$）．その違いが波形に現れている．

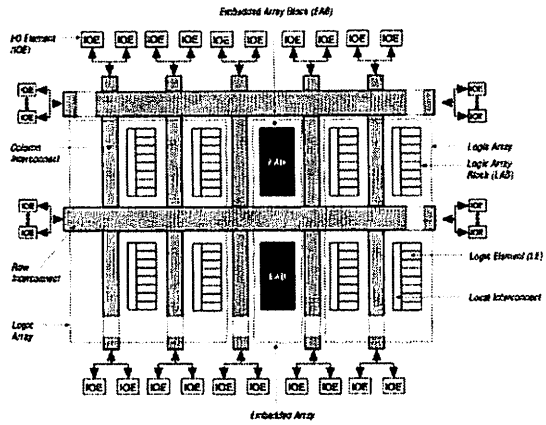

図 7　FLEX10K の内部構造

Fig. 7　Structure of FLEX10K device.

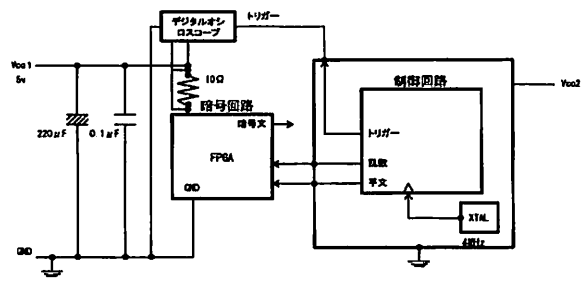

図 8　DPA 攻撃回路

Fig. 8　Experimental circuit for DPA attack.

図 9　図 4 の回路を FPGA 上に実装したときのレイアウト

Fig. 9　Layout of the FPGA implementation of Fig.4.

FPGA に実装した回路に対し，次のような DPA 攻撃を加える．2 ビットの平文を AB とし，表 1 の $ABA'B'$ 全遷移の波形を収集する．$ABA'B'$ の遷移は 0000_2, 0001_2, …, 1110_2, 1111_2 の 16 通りある．1 つの遷移を 256 回ずつ測定し，合計 4096 個の波形を収集する．収集した波形を式 (4) の選択関数によって 2 つのグループに分け，グループ間の平均値の差分波形の最大値を求める．この操作を予想鍵 $00_2, 01_2, 10_2, 11_2$ について行う．最大の差分を与える予想鍵を求める．

対策を加えた回路への DPA 攻撃では，$rABr'A'B'$=000000_2, …, 111111_2 の 64 通りを 256 回ずつ測定し、合計 16384 個の波形を収集することにより，均等分布の乱数を与えることと等

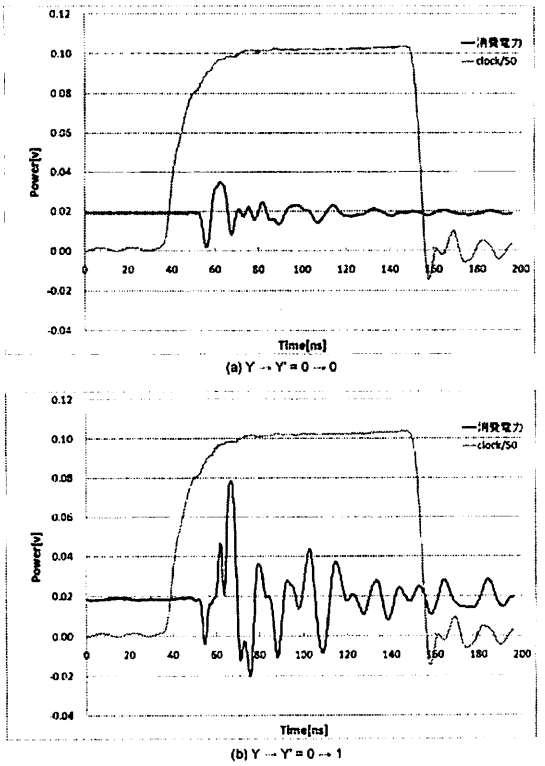

図 10 消費電力波形の例

Fig. 10 Examples of wave form of power consumption.

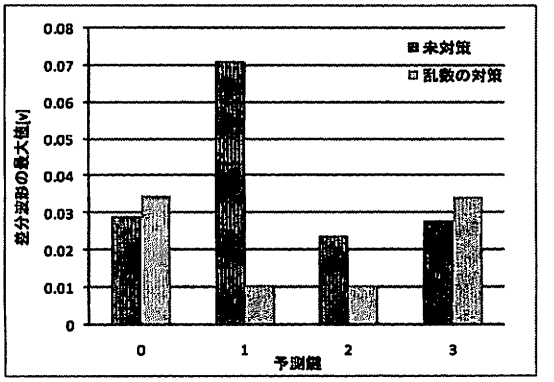

図 11 AND ゲートを使った暗号回路への DPA 攻撃の結果 (正解鍵 =1)

Fig. 11 Results of DPA attack to the cryptographic device using AND gate. (Secret key is 1.)

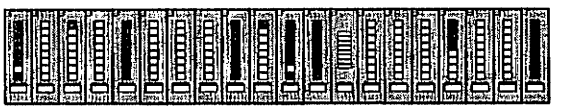

図 12 RSTL-SBOX1 を FPGA へ実装したときのレイアウト

Fig. 12 Layout of the FPGA implementation of RSLT-SBOX1.

価になるようにした．対策を加えた回路への DPA 攻撃は，未対策の回路への DPA 攻撃より強いことになる．

以上の実験の結果を図 11 に示す．暗号回路の鍵は 01_2 である．未対策の場合は，鍵の予想が正しいとき，正しくない場合と比べ差分波形の最大値が 2 倍以上大きい．したがって，DPA 攻撃は成功する．一方，対策した場合は，攻撃者は差分波形の最大値から鍵の値を 0 または 3 と予想する．すなわち DPA 攻撃は成功しない．

5.2.2 適用例 2

図 6 の RSTL-SBOX1 を FPGA へ実装したときのレイアウトを図 12 に示す．このモジュールは 9 個の LAB に配置されている．

平文の入力 $a_1 \cdots a_6$ を 6 ビットカウンターを用いて順に入力し，各入力遷移について 256 回ずつ測定し，合計 16384 個の消費電力波形を収集する．収集した波形を式 (8) の選択関数によって 2 つのグループに分け，グループの平均値の差分波形の最大値を求める．この操作を予想鍵 $0, \ldots, 63$ について行う．最大の差分を与える予想鍵を求める．式 (9) の選択関数についても調べる．

対策を加えた回路への DPA 攻撃では，各入力遷移 $a_1 \cdots a_6 a'_1 \cdots a'_6$ について，乱数入力も含めた $ra_1 \cdots a_6 r' a'_1 \cdots a'_6 = 0a_1 \cdots a_6 0a'_1 \cdots a'_6$, $0a_1 \cdots a_6 1a'_1 \cdots a'_6$, $1a_1 \cdots a_6 0a'_1 \cdots a'_6$, $1a_1 \cdots a_6 1a'_1 \cdots a'_6$ の 4 通り遷移を与える．すなわち，各入力遷移について 1024 回ずつ測定し，合計 65536 個の波形を収集することにより，均等分布の乱数を与えることと等価になるようにする．対策を加えた回路への DPA 攻撃は，未対策の回路への DPA 攻撃より強いことになる．

以上の実験の結果を図 13，図 14，図 15，図 16 に示す．図 13 と図 14 は式 (8) の選択関数を使った場合，図 15 と図 16 は式 (9) の選択関数を使った場合である．図 13 と図 15 は未対策の回路，図 14 と図 16 は対策を加えた回路についての結果である．暗号回路の鍵は 45 である．

図 13 と図 14 から，未対策の場合は，鍵の予想が正しいとき，正しくない場合と比べ差分波形の最大値は大きい．したがって，DPA 攻撃は成功する．一方，対策した場合は DPA 攻撃は成功しない．選択関数として式 (9) を使う場合，式 (8) を使う場合より DPA 攻撃は強力であることが分かるが，この場合も対策を施した回路では成功しない．

5.2.3 考　　察

図 11 において，未対策の回路では，鍵の予想が正しいとき，正しくない場合と比べ差分波形の最大値が 2 倍以上大きい．対策を施した回路では鍵の予想にかかわらず差分波形の最大値は 0.01v から 0.03v 程度である．このことを考察する．表 1 により，遷移があるときの消費電力を $P + a$ とし，遷移がないときの消費電力を P とすると，鍵の予想が正しいときの差分は $9a/12$，鍵の予想が正しくないときの差分は $3a/12$ となる．前者は後者の 3 倍であり，実験結果はこれに近い．一方，対策を施した回路では，鍵の予想にかかわらず差分は 0 になるはずである．図 11 の実験結果との差はノイズの影響と思われる．

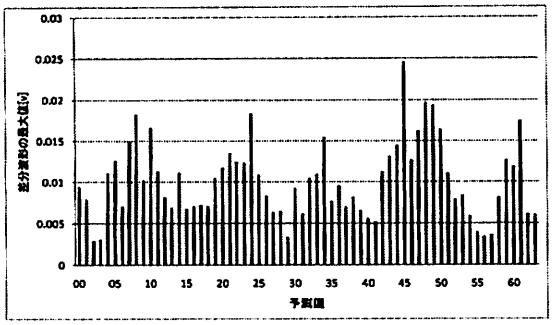

図 13 SBOX1 を用いた未対策の暗号回路に対し式 (8) により DPA 攻撃を行った結果 (正解鍵=45)

Fig. 13 Results of DPA attack to the cryptographic device using SBOX1 without countermeasure.(Secret key is 45.) Eq.(8) was used as the selection function.

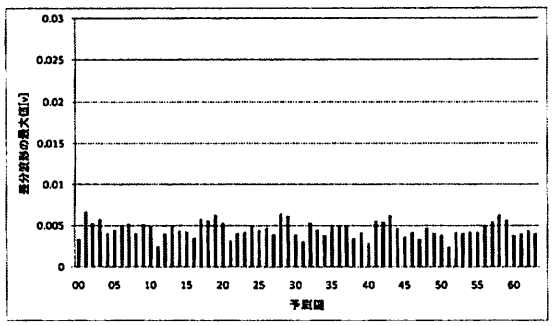

図 14 SBOX1 を用いた対策済みの暗号回路に対し式 (8) により DPA 攻撃を行った結果 (正解鍵=45)

Fig. 14 Results of DPA attack to the cryptographic device using SBOX1 with countermeasure.(Secret key is 45.) Eq.(8) was used as the selection function.

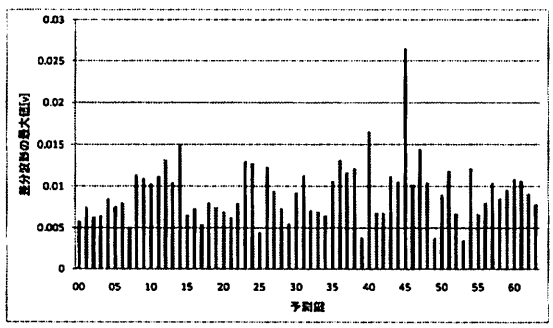

図 15 SBOX1 を用いた未対策の暗号回路に対し式 (9) により DPA 攻撃を行った結果 (正解鍵=45)

Fig. 15 Results of DPA attack to the cryptographic device using SBOX1 without countermeasure.(Secret key is 45.) Eq.(9) was used as the selection function.

6. おわりに

演算ごとに入出力信号の遷移確率を均等化することにより，DPA 耐性が向上することが分かった．この場合，1 つの演算

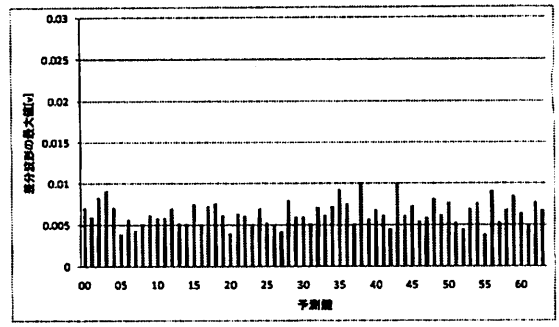

図 16 SBOX1 を用いた対策済みの暗号回路に対し式 (9) により DPA 攻撃を行った結果 (正解鍵=45)

Fig. 16 Results of DPA attack to the cryptographic device using SBOX1 with countermeasure.(Secret key is 45.) Eq.(9) was used as the selection function.

モジュールが複数の LUT に配置されることを考えると，これは FPGA のスイッチングマトリクス (Interconnect) による消費電力と回路からの情報リークの相関は大きくないことを意味する．ゲートごとでなく演算ごとにモジュール化されていればよいので，この対策の実装は簡易である．

消費電力波形の数をさらに増やしたときの DPA 耐性の評価は今後の課題である．

謝辞

本研究を進めるにあたり，有益なご議論をいただいた電気通信大学情報工学科阿部研究室の佐々木明彦氏に感謝する．実験環境の構築にご助力いただいた電気通信大学情報工学科の鈴木貢助教と奈良岡雅人技術専門職員に感謝する．本研究は，一部，日本学術振興会科学研究費補助金 (基盤研究 (C)(2)18500048) による．

文　献

[1] P. Kocher, J. Jaffe, and B. Jun, "Introduction to Differential Power Analysis and Related Attacks," 1998, available at http://www.cryptography.com/resources/whitepapers/DPA TechInfo.pdf

[2] P. Kocher, J. Jaffe, and B. Jun, "Differential Power Analysis," Proceedings of CRYPTO' 99, Springer-Verlag, pp.388-397, 1999.

[3] P. Kocher, "Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems," Proceedings of CRYPTO ' 96, Springer-Verlag, pp.104-113, 1996.

[4] K. Tiri, M. Akmal, and I. Verbauwhede, "A Dynamic and Differential CMOS Logic with Signal Independent Power Consumption to Withstand Differential Power Analysis on SmartCards," Proc. Of 28th European Solid-State Circuits Conference, pp.403-406, 2002.

[5] K. Tiri and I. Verbauwhede, "Securing Encryption Algorithms against DPA at the Logic Level: Next Generation Smart Card Technology," CHES 2003, LNCS 2779, pp.125-136, 2003.

[6] M. Akkar and C. Giraud, "An Implementation of DES and AES, Secure against Some Attacks," CHES 2001, LNCS 2163, pp.309-318, 2001.

[7] E. Trichina, D. De Seta, and L. Germani, "Simlified Adaptive Multiplicative Masking for AES and Its Secure Implementation," CHES 2002, LNCS 2523, pp.187-197, 2002.

[8] 佐々木明彦，阿部公輝，太田和夫，"暗号回路の耐タンパー性評価

手法の構築," SCIS2005 (The 2005 Symposium on Cryptography and Information Security), pp.613-618, Jan. 2005.
[9] 佐々木明彦, 阿部公輝, "暗号回路への電力差分解析攻撃に対するアルゴリズムレベルでの耐性評価," 電気学会論文誌 C (電子・情報・システム部門誌), Vol.126, No.10, pp.1221-1228, Oct. 2006.
[10] 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," ISEC2004, pp.127-134, 2004.
[11] 独立行政法人 情報処理推進機構, "CRYPTREC Report 2003 暗号モジュール委員会報告書," 2003.
[12] INSTAC, "耐タンパー性に関する標準化調査研究開発報告書 第一部," 2004.
[13] 角石洋輔, 佐々木明彦, 阿部公輝, "DES への差分電力解析攻撃における参照位置とビット数について," 電子情報通信学会研究会報告 (情報セキュリティ研究会), pp.51-56, Nov. 2005.
[14] FLEX 10K Embedded Programmable logic Family Data Sheet, Altera Corporation, available at http://www.ece.msstate.edu/ reese/EE4743/data_sheets /dsf10k.pdf/