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

2004－ＣＳＥＣ－26 (46)
2004／7／21

データマスクを利用したDPA対策に対する攻撃

市川 哲也† 鈴木 大輔‡ 佐伯 稔‡

†三菱電機エンジニアリング（株） 鎌倉事業所〒247-8501 神奈川県鎌倉市大船 5-1-1
‡三菱電機（株） 情報技術総合研究所〒247-8501 神奈川県鎌倉市大船 5-1-1
E-mail: † ichikawa@kam.mee.co.jp, ‡ {dice, rebecca}@iss.isl.melco.co.jp

あらまし Trichinaにより提案されているデータマスクによるDPA対策（Masked-AND方式）を施したAESのハードウェア実装に対し，著者らが文献[12]で提案しているリークモデルを用い，Masked-AND方式のDPA対策の効果を評価した．その結果，伝搬遅延に伴う過渡遷移のある状態において，過渡遷移の影響だけで，DPAリークが発生する場合があることを示した．これらを確認するため，著者らが提案する論理シミュレーションによるDPA評価[12]と三菱電機が開発したサイドチャネルアタック評価用プラットフォーム(SCAPE: Side Channel Attack Platform for Evaluation)を用いた実機による検証を行った．その結果，伝搬遅延に伴う過渡遷移があるハードウェア実装においては，Masked-AND方式のDPA対策は不十分であり，DPAリークが発生していることを示した．

キーワード AES，サイドチャネルアタック，DPA，データマスク

An Attack on Cryptographic Hardware Design with Masking Method

Tetsuya ICHIKAWA† Daisuke SUZUKI‡ and Minoru SAEKI‡

† Mitsubishi Electric Engineering Company Limited, Kamakura Office
5-1-1 Ofuna, Kamakura, Kanagawa 247-8501, Japan
‡ Mitsubishi Electric Corporation, Information Technology R & D Center
5-1-1 Ofuna, Kamakura, Kanagawa 247-8501, Japan
E-mail: † ichikawa@kam.mee.co.jp, ‡ {dice, rebecca}@iss.isl.melco.co.jp

Abstract In this paper, we evaluate one of DPA countermeasures of hardware implementation of AES, which was proposed by Elena Trichina and is called Masked-AND method. We evaluate about protection effectiveness of the Masked-AND in hardware using our models of DPA-leakage, which we proposed in [12]. We also point out a new model of DPA-leakage, which is not included in [12]. We also evaluate the effectiveness using a simulator and using SCAPE (Side Channel Attack Platform for Evaluation), which was developed by Mitsubishi Electric Corporation. As a result, we point out the result that the Masked-AND is not strong enough for protection against DPA because of different propagation-delay time of every signal caused by dynamic hazard in the AES hardware.

Keyword AES, Side Channel Attack, DPA, Data Masking

1. はじめに

Smart Card等のセキュリティデバイスに格納されている秘密情報を，その消費電力，データ出力タイミングやデバイスが動作する際に生じる電磁波等のサイドチャネル情報を観測することにより推定する強力な攻撃法（DPA，SPA等）が提案されている[1], [2],[3],[4].

これらの提案をきっかけに，差分解読法や線形解読法等の暗号アルゴリズム自体を評価する強度評価に加え，アルゴリズム実装後に発生するサイドチャネル情報を利用し，秘密情報のリークに対する強度評価も重要になりつつある．

一方，サイドチャネル攻撃の対策技術の研究も盛んに行われている．例えば，公開鍵暗号の処理に対する様々な対策手法[5],[6],[17]や，共通鍵暗号の乱数によるデータマスクを用いた対策手法[7],[8],[16]などが提案されている．

しかし，これらの対策手法に関する文献は，Smart Cardを意識したソフトウェア実装への対策が多く，ハードウェア実装的な対策アプローチ，例えば，トランジスタレベルの対策[9], [10]や，論理積（AND），論理和（OR）等の論理回路レベルで表現された対策[11]は少ない．しかし，Smart Cardへの暗号アルゴリズムの実装を考えた場合，コプロセッサによるハードウェア実装も考えられる．このため，ハードウェア実装に対

する DPA 対策も重要となる.

ハードウェア実装に対する DPA 対策手法は, いくつか提案されているが, その中の 1 つである Trichina による提案手法(以下, "Masked-AND 方式"と呼ぶ)は, DPA 対策として効果があるとされるデータマスク[7]を論理回路レベルで実現する手法である.

本稿では, Masked-AND 方式による DPA 耐策を施した AES に対し, 著者らが文献[12]において提案したリークモデルおよび論理シミュレーションによる DPA 評価を用い, 理論的解析ならびに論理シミュレーションを行った. また, 実機を用いた検証も併せて行った.

本稿の構成は, 次のようになっている. まず, 2 章において Masked-AND 方式を示す. 次に, 3 章において, AES および SBOX の実装方法を示す. また 4 章では, Masked-AND 方式の論理シミュレーションによる評価および実機を用いた検証を行う. そして, 最後に, 5 章でまとめる.

2. Masked-AND 方式[11]

図 1 に Trichina により提案されている Masked-AND 方式のブロック図を示す.

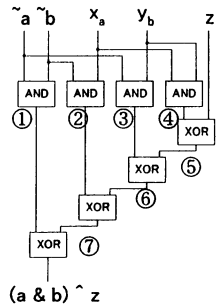


図 1 Masked-AND 方式のブロック図

Masked-AND 方式は, 真の入力データ a および b に, 互いに独立な乱数 x_a および y_b を用いてマスク (排他的論理和) している入力データ ~a および ~b の AND 演算を行い, 演算結果(a&b)を x_a および y_b とは独立な新たな乱数 z でマスクし, 出力する方式である. これにより, 秘匿したいデータ a, b および(a&b)を秘匿可能にするという方式である.

3. AES

本章では, 本稿で対象とした AES とその実装方法について簡単に述べる.

3.1. AES の実装方法

Smart Card 用コプロセッサ実装を考えた場合, 回路規模を押さえた実装が望ましい. 著者らが知る範囲では, AES の小型ハードウェア実装アーキテクチャの中で一番小さいものは, CHES2003 にて Chodowiec らが提案した実装方式[13]である.

そこで, 本稿では, AES 実装の基本的部分は, Chodowiec らの提案実装方式を採用した. Chodowiec らの提案実装方法のブロック図を図 2 に示す.

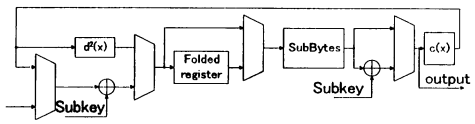


図 2 Chodowiec らの AES 実装のブロック図

以下に実装方法の概要を示す.

- 32bit 単位で演算処理を行う
- AES の 1 round を 4 クロックかけて実現する
- ShiftRow とデータ格納用レジスタを最大の深さが 16 の 8bit シフトレジスタ×4 本で実現している Folded register を持つ
- MixColumn を実現している c(x)を持つ
- InvMixColumn の 2 乗を実現している $d^2(x)$を持つ (c(x)処理後に $d^2(x)$を処理することにより InvMixColumn を実現している)
- SubByte (SBOX), InvSubByte (InvSBOX) を 2port の BlockRAM で実現している SubBytes を持つ

3.2. SBOX の実装方法

前節で示したように, Chodowiec らの実装では SBOX は, FPGA 特有の Embedded Memory (BlockRAM) を用いているため, そのままでは Masked-AND 方式を採用できない. そこで, SBOX の実装方式のみ, 盛岡らが提案している論理回路レベルで小型実装可能になる方式[14]を適用した SBOX を採用した. 図 3 にその場合の SBOX の構成図を示す.

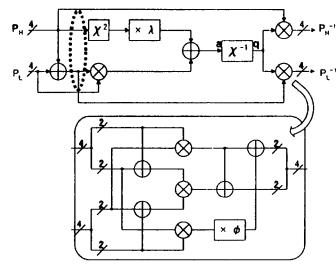


図 3 SBOX の構成図

ここで, χ^{-1} は, 入力 a (a_0,a_1,a_2,a_3), 出力を q (q_0,q_1,q_2,q_3) とするとき, 以下の式で表されるものとする. ここで, 記号「^」は, 排他的論理和 (XOR) を示し,「&」は, 論理積 (AND) を示す.

$$a_A = a_1 \hat{} a_2 \hat{} a_3 \hat{} (a_1 \& a_2 \& a_3)$$
$$q_0 = a_A \hat{} a_0 \hat{} (a_0 \& a_2)^{\cdot} (a_1 \& a_2)^{\cdot} (a_0 \& a_1 \& a_2)$$
$$q_1 = (a_0 \& a_1 1)^{\cdot} (a_0 \& a_2)^{\cdot} (a_1 \& a_2)^{\cdot} a_3 \hat{} (a_1 \& a_3) \hat{} (a_0 \& a_1 \& a_3)$$
$$q_2 = (a_0 \& a_1)^{\cdot} a_2 \hat{} (a_0 \& a_2)^{\cdot} a_3 \hat{} (a_0 \& a_1) \hat{} (a_0 \& a_2 \& a_3)$$
$$q_3 = a_A \hat{} (a_0 \& a_3)^{\cdot} (a_1 \& a_3)^{\cdot} (a_2 \& a_3)$$

4. Masked-AND 方式の評価および検証

著者らが文献[12]において提案したリークモデルを用いてリークを場合分けすると，以下のようになる．

1）信号の伝搬遅延に伴う過渡遷移のない環境(理想的な環境)下での遷移確率の差(信号が単位時間当たりに遷移する回数の期待値の差)

2）過渡遷移による，1）の増幅

一方，Masked-AND 方式の DPA 対策効果の根拠は，「内部信号の状態が乱数の効果によりランダム化されて予測できない」ということにある[11]．

1）の状況下では，Masked-AND 方式の内部信号の状態遷移はランダムであり予測できないと考えられる．しかし，一般にハードウェア実装された実機の回路では，信号の伝搬遅延が無視できない．すなわち，伝搬遅延の条件によっては，乱数の効果がなくなるような状態遷移も現れてくる可能性がある．このため，信号の伝搬遅延が存在する場合の考察も必要となる．

本章では，信号の伝搬遅延が“0”となる状態（以下，理想的な状態と呼ぶ），および，伝搬遅延に伴う過渡遷移のある状態における Masked-AND 方式の DPA 対策の評価を行った．

4.1. Masked-AND 方式の評価

本節では，理想的な状態での評価（ケース 1）および伝搬遅延に伴う過渡遷移のある状態を想定した評価（ケース 2）を行う．

ここで，ケース 1 では，乱数による対策効果によりリークが発生しないと予想される．しかし，ケース 2 においては，ある条件下では，リークが発生する場合があると予想される．この予想を確認するため，詳細な評価を行った．

4.1.1. ケース 1：理想的な状態

ケース 1 として，理想的な状態として評価を行う．

[条件]

- 入力信号 ~a, ~b, x_a, y_b, z は全て同時に到達する．
- 選択関数は a とする．
- b, x_a, y_b, z は互いに独立なランダムデータとする．

この場合，図 1 に示す Masked-AND 方式の真理値表は，表 1 のようになる．

表 1　図 1 における真理値表

a	b	~a	~b	xa	yb	z	①	②	③	④	⑤	⑥	⑦
0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	1	0	0	0	0	0	0	0	0
0	0	1	0	1	0	0	0	0	0	0	0	0	0
0	0	1	0	1	1	0	0	0	1	1	1	0	0
0	1	0	1	0	0	0	0	0	0	0	0	0	0
0	1	0	1	0	1	0	0	0	0	0	0	0	0
0	1	1	1	1	0	0	1	1	0	0	0	0	1
0	1	1	1	1	1	0	1	1	1	1	1	0	1
1	0	1	0	0	0	0	0	0	0	0	0	0	0
1	0	1	0	0	1	0	0	0	1	0	0	1	1
1	0	0	0	1	0	0	0	0	0	0	0	0	0
1	0	0	0	1	1	0	0	0	0	1	1	1	1
1	1	1	1	0	0	0	1	0	0	0	0	0	0
1	1	1	1	0	1	0	1	0	1	0	0	1	1
1	1	0	1	1	0	0	0	1	0	0	0	0	1
1	1	0	1	1	1	0	0	1	0	1	1	1	0
0	0	1	0	0	1	1	0	0	0	0	1	1	1
0	0	1	0	1	0	1	0	0	0	0	1	1	1
0	0	1	1	0	1	1	1	1	0	0	1	1	0
0	0	1	1	1	1	1	1	1	1	1	0	1	0
0	1	0	0	0	0	1	0	0	0	0	1	1	1
0	1	0	0	0	1	1	0	0	0	0	1	1	1
0	1	1	0	1	0	1	0	0	0	0	1	1	1
0	1	1	0	1	1	1	0	0	1	1	0	1	1
1	0	1	1	0	0	1	1	0	0	0	1	1	1
1	0	1	1	0	1	1	1	0	0	1	1	0	0
1	0	0	1	1	0	1	0	1	0	0	1	1	0
1	0	0	1	1	1	1	0	1	0	1	0	0	1
1	1	1	0	0	0	1	0	0	0	0	1	1	1
1	1	1	0	0	1	1	1	0	0	0	1	0	0
1	1	1	0	1	0	1	0	0	0	0	1	1	1
1	1	0	0	1	1	1	0	0	0	1	0	0	0

ここで，a および b は，解析者が予測できる値，すなわち，乱数が加えられていない真の値である．また，

①～⑦は，図 1 に示している各 AND または XOR の出力値である．

図 1 中の 4 つのポイント①～④の確率分布は，全て等しく以下のようになる．

p_0 … 各ポイントの出力が“0”になる確率

p_1 … 各ポイントの出力が“1”になる確率

状態 1［通常時(a は他の信号と同様にランダム)］

$$p_0 = 12/16, \quad p_1 = 4/16$$

状態 2［a=0 のとき］

$$p_0 = 6/8, \quad p_1 = 2/8$$

状態 3［a=1 のとき］

$$p_0 = 6/8, \quad p_1 = 2/8$$

ここで，状態 1 から状態 2 に遷移する際に，出力①～④の遷移確率[12]は，全て等しく以下のようになる．

$p_{0,0\to1}$ … a=0 において，各ポイントの出力が“0”から“1”になる遷移確率

$p_{0,1\to0}$ … a=0 において，各ポイントの出力が“1”から“0”になる遷移確率

$p_{0,TRAN}$ … a=0 において，各ポイントの出力が“0”から“1”または“1”になる各ポイントの総遷移確率

$$p_{0,0\to1} = 12/16 \times 2/8 = 3/16, \quad p_{0,1\to0} = 4/16 \times 6/8 = 3/16$$

$p_{0,TRAN} = p_{0,0\to1} + p_{0,1\to0} = 3/16 + 3/16 = 3/8$

また，状態1から状態3に遷移する際に，出力①～④の遷移確率は，全て等しく以下のようになる．

$p_{1,0\to1}$ … a=1において，各ポイントの出力が“0”から“1”になる遷移確率

$p_{1,1\to0}$ … a=1において，各ポイントの出力が“1”から“0”になる遷移確率

$p_{1,TRAN}$ … a=1において，各ポイントの出力が“0”から“1”または“1”になる各ポイントの総遷移確率

$$p_{1,0\to1} = 12/16 \times 2/8 = 3/16, \quad p_{1,1\to0} = 4/16 \times 6/8 = 3/16$$

$$p_{1,TRAN} = p_{1,0\to1} + p_{1,1\to0} = 3/16 + 3/16 = 3/8$$

よって，各ポイント，①～④の出力における遷移確率の差（p_{DIFF}）は，全て等しく，

$$p_{DIFF} = p_{0,TRAN} - p_{1,TRAN} = 0$$

となり，遷移確率の差，すなわち，遷移回数の期待値の差がないことがわかる．これは，消費電力の差がないことにほかならず，リークが発生しないことを意味する．

同様に，⑤～⑦のポイントを考えてみる．

状態1［通常時(aは他の信号と同様にランダム)］

$$p_0 = 16/32, \quad p_1 = 16/32$$

状態2［a=0のとき］ $p_0 = 8/16$ ， $p_1 = 8/16$

状態3［a=1のとき］ $p_0 = 8/16$ ， $p_1 = 8/16$

ここで，状態1から状態2に遷移する遷移確率，また，状態1から状態3に遷移する遷移確率は，それぞれ，以下のようになる．

$$p_{0,0\to1} = 16/32 \times 8/16 = 1/4, \quad p_{0,1\to0} = 16/32 \times 8/16 = 1/4$$

$$p_{0,TRAN} = p_{0,0\to1} + p_{0,1\to0} = 1/4 + 1/4 = 1/2$$

$$p_{1,0\to1} = 16/32 \times 8/16 = 1/4, \quad p_{1,1\to0} = 16/32 \times 8/16 = 1/4$$

$$p_{1,TRAN} = p_{1,0\to1} + p_{1,1\to0} = 1/4 + 1/4 = 1/2$$

よって，各ポイント，⑤～⑦のにおける出力の遷移確率の差（p_{DIFF}）は，全て等しく，

$$p_{DIFF} = p_{0,TRAN} - p_{1,TRAN} = 0$$

となり，リークが発生しないことを意味する．

以上より，図1の回路全体としての，総遷移確率の差，すなわち，総遷移回数の期待値の差がないことがわかる．これは，回路全体の消費電力の差がないことにほかならず，リークは発生しないことを意味する．

4.1.2. ケース2:伝搬遅延に伴う過渡遷移のある状態

ケース2として，伝搬遅延に伴う過渡遷移のある状態を考える．

[条件]

- 入力信号$^{-}$a, $^{-}$b, x_a, y_b, zが不揃いに遷移する．
- 選択関数はaとする．
- b, x_a, y_b, zは互いに独立なランダムデータとする．

このような条件のもとで，DPAのような，ある時刻のあるポイントの電力差分をとり，リークの有無を解析するような場合を想定する．

ここで，例として乱数による簡単なデータマスク$(\alpha \& \beta) \hat{} \gamma$ （ここで，γは乱数とする）を考える．この乱数によるデータマスクは，4.1.1における⑤のポイントと同じであると考えることができ，伝搬遅延に伴う過渡遷移のない理想的な状態では，リークが発生しない．一方，$(\alpha \& \beta) \hat{} \gamma$は，文献[12]より，リークが発生する項である，AND項$(\alpha \& \beta)$を持つため，もし，リークが発生する項$(\alpha \& \beta)$のみに依存した信号遷移が発生するタイミングがある場合，そのノードからリークが発生することになる．逆に，$(\alpha \& \beta)$のみに依存した信号遷移が発生しない場合は，ノードからリークが発生しないことになる．

したがって，伝搬遅延に伴う過渡遷移のある状態を考えた場合では，リークが発生する項のみに依存した遷移が発生するタイミングがある場合と無い場合に場合分けを行い，評価を行う必要がある．前述の例の場合では，入力データα, βに対する乱数γの到達タイミングによる場合分けが必要となってくる．

図1のMasked-AND方式において，入力信号，$^{-}$a, $^{-}$b, x_a, y_b, zが伝搬遅延に伴う過渡遷移のある状態の場合，乱数zとそれ以外の入力（$^{-}$a, $^{-}$b, x_a, y_b）の遷移状態により，以下のような場合分けが必要となる．

(1)（$^{-}$a, $^{-}$b, x_a, y_b）の最初のデータが変化し始めてから，最後の入力データが変化し終わるまでの間に，zが変化する場合．（リークが発生する項のみに依存した信号遷移が発生しない場合）

(2) 入力zが（$^{-}$a, $^{-}$b, x_a, y_b）が全て変化した後に変化し始めるか，または，zが変化後に（$^{-}$a, $^{-}$b, x_a, y_b）が変化し始める場合．（リークが発生する項のみに依存した信号遷移が発生する可能性がある場合）

(1)の場合，本稿5.1.1のケース1と同様に扱うことが可能となり，リークは発生しない．

(2)の場合，zは，固定値と考えることができる．これは，図1の④の遷移がzの値に関係なく，次の段のXORに伝わること示している．このため，⑤に関する評価を無視することができ，図1に示すMasked-AND

方式の真理値表は，表2のようになる．

表 2　図1における真理値表（z=固定）

a	b	~a	~b	xa	yb	①	②	③	④	⑥	⑦
0	0	0	0	0	0	0	0	0	0	0	0
0	0	0	1	0	1	0	0	0	0	0	0
0	0	1	0	1	0	0	0	0	0	0	0
0	0	1	1	1	1	1	1	1	1	0	1
0	1	0	1	0	0	0	0	0	0	0	0
0	1	0	0	0	1	0	0	0	0	0	0
0	1	1	1	1	0	1	1	0	0	0	1
0	1	1	0	1	1	0	0	1	1	0	0
1	0	1	0	0	0	0	0	0	0	0	0
1	0	1	1	0	1	1	0	1	0	1	1
1	0	0	1	0	0	0	0	0	0	0	0
1	0	0	0	1	1	0	1	0	0	1	0
1	1	1	0	0	0	1	0	0	0	0	0
1	1	1	1	0	1	0	1	0	0	0	1
1	1	0	0	1	0	0	1	0	1	1	1
1	1	0	1	1	1	0	0	1	1	1	1

図1中の4つのポイント，①～④の確率分布は，本稿5.1.1のケース1のz=0あるいはz＝1固定の場合と同様とみなすことができる．すなわち，遷移確率の差がなく，リークは発生しない．

次に，⑥のポイントを考えてみる．

状態1［通常時(a＝ 他の信号と同様にランダム)］

$p_0 = 12/16$ ，　$p_1 = 4/16$

状態2［a=0のとき］　$p_0 = 1$ ，　$p_1 = 0$

状態3［a=1のとき］　$p_0 = 1/2$ ，　$p_1 = 1/2$

ここで，状態1から状態2に遷移する遷移確率，また，状態1から状態3に遷移する遷移確率は，それぞれ，以下のようになる．

$$p_{0,0\to1} = 12/16 \times 0 = 0, \quad p_{0,1\to0} = 4/16 \times 1 = 1/4$$

$$p_{0,TRAN} = p_{0,0\to1} + p_{0,1\to0} = 0 + 1/4 = 1/4$$

$$p_{1,0\to1} = 12/16 \times 1/2 = 3/8, \quad p_{1,1\to0} = 4/16 \times 1/2 = 1/8$$

$$p_{1,TRAN} = p_{1,0\to1} + p_{1,1\to0} = 3/8 + 1/8 = 1/2$$

よって，ポイント⑥の出力の遷移確率の差（p_{DIFF}）は，

$$p_{DIFF} = p_{0,TRAN} - p_{1,TRAN} \neq 0$$

となり，遷移確率の差が生じていることがわかり，リークが発生することを意味する．

同様に，⑦のポイントを考えてみる．

状態1［通常時(a＝ 他の信号と同様にランダム)］

$p_0 = 10/16$ ，　$p_1 = 6/16$

状態2［a=0のとき］　$p_0 = 6/8$ ，　$p_1 = 2/8$

状態3［a=1のとき］　$p_0 = 4/8$ ，　$p_1 = 4/8$

ここで，状態1から状態2に遷移する遷移確率，また，状態1から状態3に遷移する遷移確率は，それぞれ，以下のようになる．

$$p_{0,0\to1} = 10/16 \times 2/8 = 5/32, \quad p_{0,1\to0} = 6/16 \times 6/8 = 9/32$$

$$p_{0,TRAN} = p_{0,0\to1} + p_{0,1\to0} = 5/32 + 9/32 = 7/16$$

$$p_{1,0\to1} = 10/16 \times 4/8 = 5/16, \quad p_{1,1\to0} = 6/16 \times 4/8 = 3/16$$

$$p_{1,TRAN} = p_{1,0\to1} + p_{1,1\to0} = 5/16 + 3/16 = 1/2$$

よって，ポイント⑦の出力の遷移確率の差（p_{DIFF}）は，

$$p_{DIFF} = p_{0,TRAN} - p_{1,TRAN} \neq 0$$

となり，遷移確率の差が生じており，リークが発生することを意味する．

よって，図1の回路全体としての，総遷移確率の差，すなわち，総遷移回数の期待値の差が生じていることがわかる．これは，回路全体の消費電力の差が生じていることにほかならず，リークが発生することを意味する．

また，出力(a&b)^zにおいても評価を行うと，⑥，⑦と同様に，リークが発生することがわかる．

以上のように，過渡遷移が無ければリークが発生しないような回路においても，様々な条件の過渡遷移を想定すると，その影響だけでリークが発生する場合があることが示された．このリークは，著者らが文献[12]で明示していなかったものである．

4.1.3. リークが発生しない条件

4.1.1および4.1.2より，Masked-AND方式によるリークが発生しない条件は以下のように考えられる．

(1) 入力信号を含め，回路全体に過渡遷移の影響による信号の到達時刻に差が生じない工夫をする．

(2) （~a, ~b, x_a, y_b）の一つが変化し始めてから，最後の入力データが変化し終わるまでの間に，zが遷移するようにzの到達時刻を調整する．

ここで，4.1.2において⑥のポイントでリークが発生しているため，(2)は，以下のように書き換えることが可能となる．

(2)' （~a, x_a, y_b）の一つが変化し始めてから，最後の入力データが遷移し終わるまでの間に，zが遷移するようにzの到達時刻を調整する．

しかし，(1), (2), (2)'の条件を実現するためには，配線遅延，信号線の負荷容量等のばらつきおよび動作条件のばらつきを考慮し，少なくともzの入力タイミングを計らなくてはならない．

ここで，入力信号~a, ~b, x_a, y_bは，図2および図3より，AESのデータパス上に存在しているデータであり，文献[11]より，同程度の論理段数を通過している．しかし，乱数zが通過する論理段数は，~a, ~b, x_a, y_bと比較するとはるかに少ない．このため，実際の回路

上で実現することは，非常に困難である．すなわち，Masked-AND 方式の DPA 対策だけでは不十分であることがわかる．

4.2. 論理シミュレーションによる評価

4.1 節において，伝搬遅延に伴う過渡遷移のある場合，Masked-AND 方式では DPA 対策として不十分であることを示した．本節では，これらのことを検証するために，著者らが文献[12]にて提案した論理シミュレーション手法を AES の SBOX に適用し，評価を行う．

4.2.1. 評価環境

以下に，論理シミュレーションによる評価環境を示す．これらの環境は，一般のソフトウェア開発等に用いられるものであり，特殊な環境は使用していない．

- ワークステーション … Sun Fire V480
- 使用言語 … Verilog-HDL および C
- シミュレータ … Verilog-XL
- ターゲット FPGA … XCV1000-6BG560C

4.2.2. 評価結果

図 4～図 7 に，10,000 データを用いた論理シミュレーション評価結果を示す．図 4～図 7 において，縦軸は，選択関数を図 3 の点線で囲んだ部分としたときの，各信号における単位時間当たりの総遷移回数の差分であり，横軸は時間である．また，各図は，図 3 の点線で囲んだ部分 8bit 分のグラフを一つのグラフに重ね，相対的な比較をしているため，縦軸と横軸のメモリおよび数値には意味はない．

図 4 は，無対策の SBOX に関して，配線遅延等の影響による過渡遷移が生じていないという条件(理想的，すなわち，遅延ゼロな論理シミュレーション）の結果である．図 5 は，無対策の SBOX に関し，仮想遅延による過渡遷移が生じているという条件（過渡遷移を考慮した論理シミュレーション）での結果である．図 4，図 5 を比較すると明らかなように，過渡遷移を考慮した論理シミュレーション結果が明らかに大きくリークが発生していることがわかり，過渡遷移の影響は，無視できないことがわかる．

図 6 は，Masked-AND 方式適用後の SBOX に関する，理想的な論理シミュレーション結果である．図 7 は，Masked-AND 方式適用後の SBOX に関し過渡遷移を考慮した論理シミュレーション結果である．図 6，図 7 を比較すると明らかなように，過渡遷移を考慮した論理シミュレーション結果は，明らかにリークが発生していることがわかる．ただし，図 4，図 6 を比較して明らかなように，Masked-AND 方式は，過渡遷移が生じていない状態では，リークが発生していない．したがって，DPA 対策の効果は確認できることに注意が必要である．

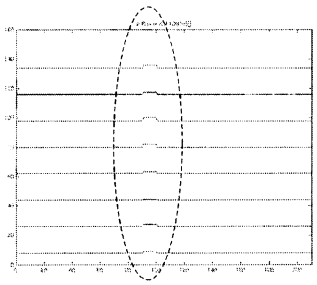


図 4　無対策（遅延なし）

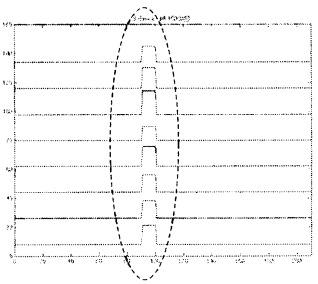


図 5　無対策（遅延あり）

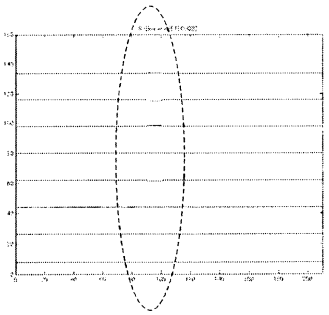


図 6　対策済み：Masked-AND 方式（遅延なし）

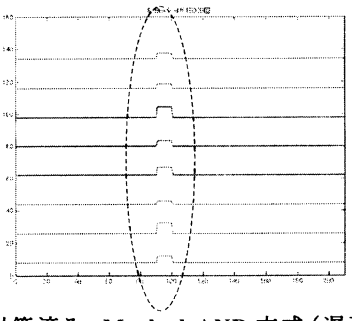


図 7　対策済み：Masked-AND 方式（遅延あり）

4.3. 実機による検証

本章では，Masked-AND 方式を採用した AES の SBOX 単体の回路を FPGA 上に実装し，実機による評価検証を行う．また，AES 全体の実装も行い，あわせて実機による評価検証を行う．

4.3.1. 検証環境

FPGA を用いた実機による検証には，三菱電機が開発を行ったサイドチャネルアタック評価用プラットフォーム（SCAPE : Side Channel Attack Platform for Evaluation）を用いて行った．（SCAPE の詳細な報告は別途行う予定）

以下に，SCAPE の主な特徴を示す．

1）親基板＋子基板から構成（子基板は最大 2 枚同時装着可能）され，子基板単体での評価も可能
2）評価対象の論理は子基板上の FPGA 内に格納
子基板のバリエーションとして異なる種類の FPGA，CPU を用意し，目的に応じて子基板を挿し換え可能
3）評価対象の入力クロックは，外部から入力，親基板にて各子基板共通生成，子基板ごとの独立生成を選択可能

次に，今回用いた検証環境を以下に示す．

・オシロスコープ … Tektronix TDS 7104
・評価ボード … SCAPE（子基板 1 枚単体）
・FPGA … XCV1000-6BG560C

また，図 8 に今回の検証に使用した SCAPE の概観（子基板 1 枚単体での検証環境）を示す．

4.3.2. 検証結果

図 9～図 13 に実機による検証結果を示す．ここで，縦軸は，選択関数を図 3 の点線で囲んだ部分としたときの，各信号の平均電力の差分値であり，横軸は，時間である．また，本章 4.2.2 のグラフと同様に，各図は，図 3 の点線で囲んだ部分の 8bit 分のグラフを一つに重ね，相対的な比較をしている．このため，縦軸と横軸のメモリおよび数値には意味はない．

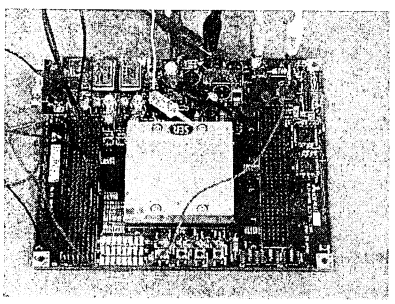
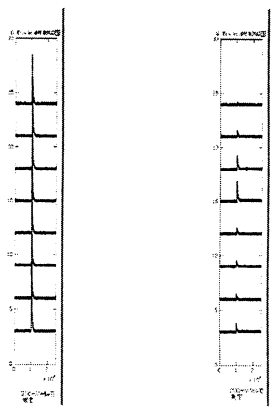


図 8　検証環境(子基板 1 枚単体での検証環境)

図 9 は，6,000 データを用いた SBOX の検証結果である．(a)と(b)を比較して明らかなように，対策の効果は認められるが，リークが発生していることが観測され，DPA 対策としては不十分であることがわかる．

また，図 10～図 13 に 20,000 データを用いた AES の検証結果を示す．

図 10 に無対策版の AES，図 11 に Masked-AND 方式を適用した AES の検証結果を示す．また，図 12 は，図 11 の縦軸を 5 倍に拡大した波形であり，図 13 は，検証データを 200,000 データ用いて検証した結果である．図 10，図 11 および図 12 を比較すると，DPA 対策の効果が確認できる．しかし，評価データ数を増加することにより，図 13 のようにリークが発生していることがわかる．よって，Masked-AND 方式での DPA 対策は不十分であることが確認された．



(a)マスク法なし　　(b)マスク法あり

図 9　SBOX 単体による実機評価結果

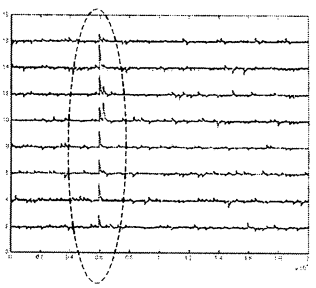


図 10　AES（無対策）

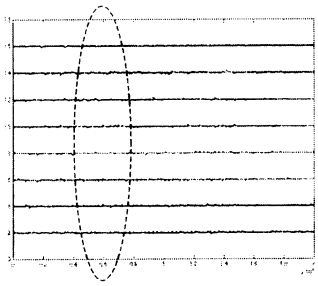


図 11　対策済み：Masked-AND 方式

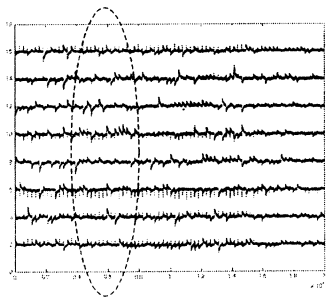


図 12　図 11 の 5 倍スケール波形

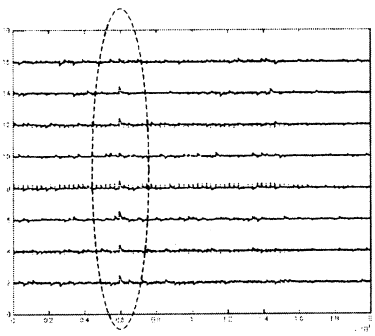


図 13　図 12 の測定回数 10 倍波形

5. まとめ

伝搬遅延に伴う過渡遷移のある状態において，Masked-AND 方式の DPA 対策の評価を行い，ある条件下では，リークが発生することを示した．

これは，著者らが文献[12]で明示していなかった，伝搬遅延に伴う過渡遷移のある状態において，過渡遷移の影響だけで，リークが発生する場合があることを示したことになる．

また，Masked-AND 方式を施した AES の SBOX 単体および AES 全体回路において，論理シミュレーション評価および SCAPE を用いた実機検証を行った．その結果，双方の回路からリークが発生していることを確認した．すなわち，Masked-AND 方式の DPA 対策だけでは不十分であることを示した．

以上より，著者らは，全てのハードウェア実装において，過渡遷移による信号の伝搬遅延や信号の変化タイミング等の差は生じるという前提にたち，評価，検証および対策を講じる必要があると強く主張する．また，著者らは，この結果を元に考案した DPA 対策手法を文献[15]において提案しているので参照されたい．

参 考 文 献

[1] P. Kocher, "Timing attacks on implementations of Diffe-Hellmann, RSA, DSS, and other systems", Proc. Advances in Cryptology - Crypto'96, LNCS 1109, pp. 104-113, 1996.

[2] P. Kocher, J. Jaffe, B. Jun, "Differential power analysis", Advances in Cryptology - CRYPTO'99, LNCS 1666, pp. 388-397, 1999.

[3] J.-J. Quisquater, D. Samyde,"ElectroMagnetic Analysis (EMA): Measures and Counter-Measures for Smart Cards", In Smart Card Programming and Security (E-smart 2001), LNCS 2140, pp. 200-210

[4] K. Gandolfi, C. Mourtel, F. Oliver, "Electromagnetic analysis : concrete results", Proc. Cryptographic Hardware and Embedded Systems: CHES2001, LNCS 2162, pp.251-261, 2001.

[5] J.-S. Coron, "Resistance against Differential Power Analysis for Elliptic Curve Cryptosystems", Proc. Cryptographic Hardware and Embedded Systems: CHES'99, LNSC 1717, p.292-302, 1999

[6] T. Messerges, E. Dabbish, R. Sloan, "Power Analysis Attacks of Modular Exponentiation in Smartcard", Proc. Cryptographic Hardware and Embedded Systems: CHES2003, LNSC 2779, p.397 ff

[7] M. Akkar, C. Giraud, "An implementation of DES and AES, secure against some attacks", Proc. Cryptographic Hardware and Embedded Systems: CHES 2001, LNCS 2162, pp. 309-318, 2001.

[8] E. Trichina, D. de Seta, L. Germani, "Simplified Adaptive Multiplicative Masking for AES", Cryptographic Hardware and Embedded Systems: CHES2002, LNCS 2523, p.187 ff

[9] K. Tiri, I. Verbauwhede, "Securing Encryption Algorithms against DPA at the Logic Level: Next Generation Smart Card Technology" , CHES2003, LNSC 2779,

[10] K. Tiri, I. Verbauwhede, "A Logic Level Design Methodology for a Secure DPA Resistant ASIC or FPGA Implementation", Design Automation and Test in Europe Conference (DATE 2004)

[11] E. Trichina, "Combinational Logic Design for AES SubByte Transformation on Masked Data", Cryptology ePrint Archive, 2003/236, http://eprint.iacr.org/complete/

[12] 佐伯，鈴木，市川：リークモデルの構築と論理シミュレーションによる DPA 評価，ISEC2004, 2004.7

[13] P. Chodowiec, K. Gaj, "Very Compact FPGA Implementation of the AES Algorithm", CHES 2003, LNCS 2779, p.319-333, 2003

[14] 盛岡，佐藤：共通鍵暗号 AES の低消費電力論理回路構成法，情報処理学会論文誌，Vol.44, No.5, pp.1321-1328, 2003.5.

[15] 鈴木，佐伯，市川：遷移確率を考慮した DPA 対策手法の提案，ISEC2004, 2004.7

[16] J.-S. Coron and L. Goubin, "On Boolean and arithmetic masking against differential power analysis," CHES 2000, LNCS 1965, pp. 231-237, 2000.

[17] C. Clavier and M. Joye, "Universal Exponentiation Algorithm – A First Step Towards Provable SPA Resistance," CHES 2001, LNCS 2162, pp. 300-308, 2001.