軽量暗号の耐タンパ実装とその評価

野崎佑典[†1]　　吉川雅弥[†1]

近年小型デバイスでも利用可能な暗号化技術である軽量暗号アルゴリズムが注目されている．一方で，ハードウェアセキュリティでは回路動作時の消費電力や電磁波を利用して回路内部の秘密鍵を窃取するサイドチャネル攻撃の脅威が報告されている．そのため，軽量暗号においてもサイドチャネル攻撃への対策技術について検討することは非常に重要である．本研究では代表的な軽量暗号である PRESENT を対象に RSM に基づく耐タンパ実装を提案する．そして，FPGA を用いた評価実験によって，提案耐タンパ実装の有効性について検証する．

A Tamper Resistant Implementation for Lightweight Ciphers and its Evaluation

YUSUKE NOZAKI[†1]　MASAYA YOSHIKAWA[†1]

Lightweight ciphers, which can be utilized in a small device, have attracted attention. On the other hand, in the field of hardware security, the threat of side-channel attacks, which steal a secret key by using power consumption or electromagnetic waves generated in circuit operation, is reported. Therefore, the study of countermeasures against side-channel attacks for lightweight ciphers is very important. This study proposes a new tamper resistant implementation based on RSM for a lightweight cipher PRESENT. Experiments using an FPGA evaluate the effectiveness of the proposed tamper resistant implementation.

1. はじめに

近年様々なデバイスをネットワークに接続し，データをやり取りする Internet of Thing（IoT）によって，つながる電子デバイスのセキュリティへの関心が高まっている．しかし，IoT で用いられる組み込み機器では，利用できる回路規模や消費電力，レイテンシの観点から Advanced Encryption Standard（AES）などの通常の暗号技術を利用することは難しい．そこで小回路規模・低消費電力・低レイテンシで利用可能な軽量暗号アルゴリズムが注目されている [1][2][3][4]．これまでに利用用途に合わせて，様々な軽量暗号が提案されている．例えば，ハードウェアでの小回路規模実装を指向した SIMECK [2]や, 低消費電力実装を指向した Midori [3], 低レイテンシ実装を指向した PRINCE [4] などが提案されている．本研究で対象とする PRESENT [1] は，ISO/IEC2919-2 で標準化されており，軽量暗号のベンチマークとされる代表的な軽量暗号アルゴリズムである．

一方でハードウェアセキュリティにおいて，サイドチャネル攻撃の脅威が報告されている [5][6]．サイドチャネル攻撃は暗号デバイス処理時における消費電力や漏洩電磁波などのサイドチャネル情報と呼ばれる物理情報を利用した攻撃であり，暗号デバイス内部に格納された秘密情報を窃取する．これまでに軽量暗号に対する攻撃も報告されている [7][8][9]．そのため，軽量暗号のサイドチャネル攻撃に対する耐タンパ実装について検討することは非常に重要である．

そこで本研究では，代表的な軽量暗号である PRESENT のサイドチャネル攻撃に対する耐タンパ実装を提案する．そして，Field Programmable Gate Array（FPGA）を用いた評価実験を行い，提案耐タンパ実装の有効性について検証する．

†1 名城大学
Meijo University

2. 準備

2.1 軽量暗号 PRESENT

軽量暗号は AES 暗号よりも小リソースでの実装が可能なアルゴリズムである. 例えば, AES のブロック長が 128bit であるのに対して，軽量暗号はブロック長が 64bit，鍵長は 80bit を採用しているアルゴリズムが多い．また，暗号処理の非線形演算である S-BOX は，AES が 8bit 単位で行うのに対して，軽量暗号は小回路規模化を実現させるために，4bit の小型 S-BOX を採用しているものが多い．

本研究で対象とする PRESENT [1]は 2007 年に提案された軽量暗号であり，ISO/IEC2919-2 で標準化されている．ブロック長は 64bit であり，鍵長は 80bit または 128bit である．

PRESENT の暗号アルゴリズムの概要を図 1 に示す. 図 1 に示すように PRESENT のラウンド関数は, addRoundKey, sBoxLayer，pLayer で構成する．addRoundKey では，暗号中間値とラウンド鍵との XOR 演算を行う．このラウンド鍵は秘密鍵から各ラウンドで鍵スケジュールを用いて計算する．次に sBoxLayer では，16 個の 4bit ずつの暗号中間値に対して，それぞれ sBox で 4bit 単位での置換処理を適用する．そして pLayer では，ビット単位での転置処理を行う．この処理を 1 ラウンド目から 30 ラウンド目まで行い, 最終ラウンド（31 ラウンド）では addRoundKey のみを行い，暗号文を出力する．

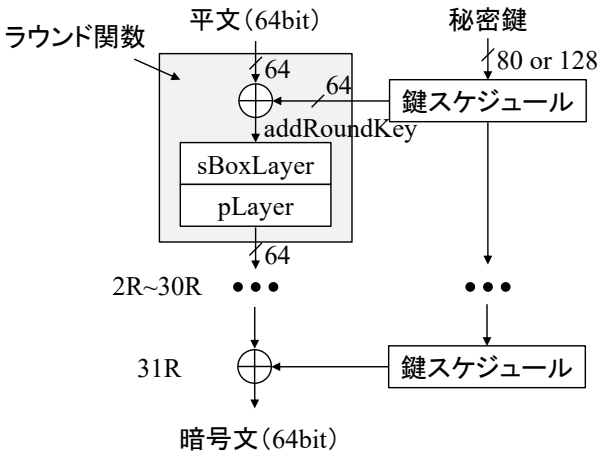

図 1　PRESENT

Figure 1　PRESENT.

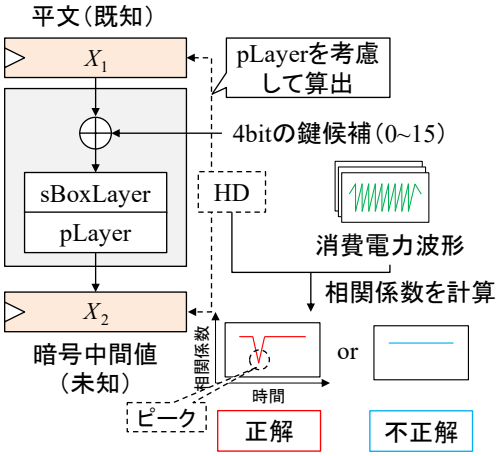

図 2　PRESENT に対する CPA

Figure 2　CPA for PRESENT.

2.2 PRESENT に対するサイドチャネル攻撃

これまでに PRESENT に対するサイドチャネル攻撃として，消費電力を用いた電力解析 [8]や電磁波を用いた電磁波解析 [9]などが報告されている．

特に PRESNET に対する相関電力解析（Correlation Power Analysis: CPA）について説明する．PRESENT に対する CPA の概要を図 2 に示す．CPA では，主にレジスタ間のデータ遷移ビット数であるハミング距離（Hamming Distance: HD）とサイドチャネル情報との相関関係を利用する．具体的には，1 ラウンド目のレジスタ間の HD を解析に利用する．この HD の導出では，図 2 に示すように既知の平文 X_1 と部分鍵との XOR 演算を行い，S-BOX による演算を行う．このとき，PRESENT は pLayer による転置処理を行うため，pLayer を考慮して HD を算出する．

解析では，導出した HD H と消費電力 W からピアソンの相関係数を以下の式で求める．

$$\rho_t = \frac{\sum_{i=1}^{D}(W_{i,t}-\overline{W_t})(H_i-\overline{H})}{\sum_{i=1}^{D}(W_{i,t}-\overline{W_t})^2\sum_{i=1}^{D}(H_i-\overline{H})^2} \quad (1)$$

ただし，$\overline{H}$ は HD の平均値，$\overline{W}$ は消費電力の平均，D は解析に使用したデータ数である．

そして，この計算を各鍵候補に対して行う．PRESESNT の解析対象となる部分鍵は 4bit であるため，その鍵候補は 0 から 15 の 16（2^4）通りである．そして，これらの値の中で相関係数が最大または最小となる鍵候補を正解鍵として推定する．

2.3 耐タンパ実装

一般的にサイドチャネル攻撃に対する耐タンパ実装はマスキングとハイディングに分類される．マスキング対策は，乱数を利用したマスク処理を施すことで，暗号中間値とサイドチャネル情報との相関関係を抑える対策である．代表的なマスキング対策には，Threshold Implementation（TI）[10]や Rotating Sboxes Masking（RSM） [11]がある．特に提案手法でベースとなる RSM は，AES 暗号を対象に提案された手法で，他のマスキング対策と比較して非常に小回路規模で実装できることが知られている．

ハイディング対策は，サイドチャネル情報の均一化やランダム化を引き起こすことで，耐タンパ性を高める対策である．代表的なハイディング対策には，相補動作を行う回路を利用した Wave Dynamic Differential Logic（WDDL） [12]や時間軸方向でのサイドチャネル情報のランダム化を引き起こす Randomizing [13][14]などがある．

これまでに PRESENT を対象とした耐タンパ実装として，TI を用いた対策 [15]が提案されている．しかし，RSM などの小回路実装を指向した耐タンパ実装についての検討は行われていない．

3. 提案耐タンパ実装

3.1 概要

本研究では，軽量暗号 PRESENT のサイドチャネル攻撃に対する耐タンパ実装を提案する．提案耐タンパ実装は，比較的小回路規模で実装可能な RSM [11]をベースとする．提案耐タンパ実装の概要を図 3 に示す．図 3 は特に 1 ラウンド目における処理を示したものである．提案耐タンパ実装では，データレジスタの値を含み全ての暗号中間値を乱数によってマスクし，秘密情報とサイドチャネル情報との相関を隠ぺいする．このマスク値について，PRESENT は 4bit 単位で処理を行っているため，16 種類の 4bit のマスク値（$m_0, m_1, \ldots, m_{15}$）を事前に乱数で決定し，これをベース

マスク値として回路内部で保持しておく．各ラウンドで使用するマスク値は，ベースマスク値（$m_0, m_1, \ldots, m_{15}$）で構成し，暗号処理毎に乱数値で与えられる 4bit のオフセット値 *offset* を用いて更新する．すなわち，64bit のマスク値 M_{offset} は式(2)で与えられる．

$$M_{offset} = m_{offset} \| m_{offset+1(\mathrm{mod}16)} \| \ldots \| m_{offset+15(\mathrm{mod}16)} \quad (2)$$

またオフセット値は，各ラウンドで，*offset* = *offset* + 1 (mod 16)によって更新される．

各処理の詳細について，まず平文 X_1 はマスク値 M_{offset} によって XOR 演算され，マスクされた値（$X_1 \oplus M_{offset}$）がデータレジスタへと格納される．そして，addRoundKey が行われ，変形 sBoxLayer へ値が入力される．変形 sBoxLayer では入力される値のアンマスク処理と新たなマスク値によるマスク処理が行われる．変形 sBoxLayer の詳細を図 4 に示す．

図 4 に示すように，変形 sBoxLayer は 16 個の変形 S-BOX（$S'_0, \ldots, S'_{15}$）と 2 つのシフター回路で構成する．変形 S-BOX $S'_{offset}(x')$では，ある 4bit のマスクされた入力値 x' に対して以下の計算を行う．

$$S'_{offset}(x') = S(x \oplus m_{offset}) \oplus m_{offset+1(\mathrm{mod}16)} \quad (3)$$

ただし，$S(\,)$は通常の PRESENT の S-BOX の処理である．

この変形 S-BOX は，16 種類のベースマスク値に対応して 16 種類生成する．そしてシフター回路では，オフセット値 *offset* から，マスクされた入力値に対応した変形 S-BOX を選択する．変形 S-BOX では，入力値と出力値が共にマスクされた値であるため，S-BOX を対象としたサイドチャネル攻撃への耐性を持つ．また，無対策の PRESENT でも，S-BOX は 16 個実装するため，変形 sBoxLayer での回路規模のオーバーヘッドはシフター回路の追加のみである．

次に，変形 sBoxLayer の出力値に対して pLayer を適用し，計算結果をデータレジスタへと格納する．このとき，レジスタに格納される値が次のラウンドのマスク値 $M_{offset+1}$ でマスクされた値（$X_2 \oplus M_{offset+1}$）になるように変換処理を行う．具体的には，マスク値 $M_{offset+1}$ に pLayer を適用した値（$p(M_{offset+1})$，ここで $p(\,)$は pLayer による転置処理）による XOR 演算を行うことでアンマスクし，新たにマスク値 $M_{offset+1}$ によるマスク処理を行う．

以上の操作を繰り返し行うことで暗号化を行う．

3.2 使用するマスク値

本節では，提案耐タンパ実装で利用するマスク値について説明する．ここで AES 暗号の RSM 対策について，文献[16][17]では，マスク値に依存したサイドチャネル攻撃の脆弱性が報告されている．具体的に，文献[16][17]で示されているマスク値を使用する場合，マスク値 M_{offset} と次のラウンドで使用するマスク値 $M_{offset+1}$ の HD には偏りが生じる．また，マスク値間の HD（$m_0 \oplus m_1$，$m_2 \oplus m_3$，…，$m_{15} \oplus m_0$）において，ビット単位で 1 が出現する確率も偏ることが指摘されており，この偏りが脆弱性に繋がることが報告されている．そこで文献 [17]では，ビット単位でマスク値間の HD の 1 の出現確率が 50%になるようなマスク値が提案されており，このマスク値を利用することで，耐タンパ性が向上することが報告されている．

一方で PRESENT では，詳細な評価結果は 4 章の実験で述べるが，文献 [17]で推奨されているようなマスク値（マスク値間のビット間 HD の 1 の出現確率が 50%になるマス

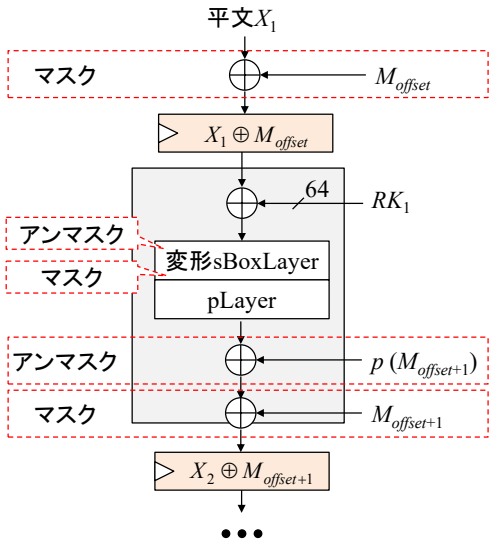

図 3　提案耐タンパ実装の概要

Figure 3　Outline of the proposed tamper resistant implementation.

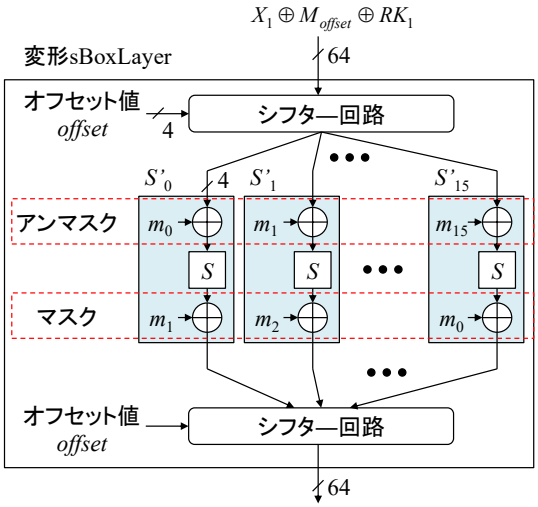

図 4　変形 sBoxLayer

Figure 4　Customized sBoxLayer.

ク値）を使用した場合でも，サイドチャネル攻撃に対する脆弱性が存在する．これは，AES 暗号のサイドチャネル攻撃で参照するレジスタ間 HD が $m_0 \oplus m_1$，$m_2 \oplus m_3$，…，$m_{15} \oplus m_0$ のマスク値に対応するのに対して，PRESENT のサイドチャネル攻撃では pLayer での転置を考慮するため，上記マスク値の位置関係に対応しないためである．

具体的に，文献 [17]で報告されているマスク値の条件に合い，提案耐タンパ実装で利用可能なマスク値として，マスク値 A「0x88379a65f0ee0145」について考える．ここで，マスク値 A について，マスク値同士（M_{offset} と $M_{offset+1}$）を XOR 演算した結果を表 1 に，ビット単位でマスク値間の HD が 1 になる確率を表 2 に示す．このとき，M'（$M' = M_{offset} \oplus M_{offset+1}$）はマスク値同士を XOR 演算した結果であり，$M'$の k bit 目の値を M'_k とする．表 1 と 2 から，ビット単位での 1 の出現確率は 50%であり，文献 [17]の条件に合うことが確認できる．

次に pLayer での転置を考慮して，マスク値間の HD H_m を計算した結果を表 3 に示す．表 3 から，特に $offset = 8$ では HD は 0 であり，全くマスク処理が行われていない．このように pLayer を考慮した場合には HD には偏りが生じる．

そこで提案耐タンパ実装では，pLayer での転置を考慮してマスク値間の HD が全て 2 になるようなマスク値を実装する．本研究では，この提案マスク値に「0x5adf11c5280feb9d」を利用する．提案マスク値でのマスク値間 HD を計算した結果を表 4 に示す．表 4 から pLayer を考慮した場合では各マスク値間 HD は全て 2 になっていることが確認できる．

表 1　マスク値間のハミング距離（マスク値 A）

Table 1　Hamming distance between mask values.

$offset$	0	1	2	3	4	5	6	7
M_{offset}	8	8	3	7	9	a	6	5
$M_{offset+1}$	8	3	7	9	a	6	5	f
M'	0	b	4	e	3	c	3	a
$offset$	8	9	10	11	12	13	14	15
M_{offset}	f	0	e	e	c	1	4	5
$M_{offset+1}$	0	e	e	c	1	4	5	8
M'	f	e	0	2	d	5	1	d

表 2　マスク値間の HD がビット単位で 1 になる確率

Table 2　Probability of 1 for HD between mask values in bitwise.

M'_k	M'_0	M'_1	M'_2	M'_3
$P(M'_k = 1)$	0.5	0.5	0.5	0.5

表 3　pLayer を考慮した場合のマスク値間 HD

Table 3　Hamming distance between mask values using pLayer.

$offset$	0	1	2	3	4	5	6	7
$p(M_{offset})$	f	3	2	6	c	0	4	1
$p(M_{offset+1})$	c	0	4	1	2	7	e	8
H_m	2	2	2	3	3	3	2	2
$offset$	8	9	10	11	12	13	14	15
$p(M_{offset})$	2	7	e	8	2	f	a	d
$p(M_{offset+1})$	2	f	a	d	f	6	4	c
H_m	0	1	1	2	3	2	3	1

4. 評価実験

4.1 実験環境

実験では，FPGA ボード SASEBO-GII を使用し，SASEBO-GII 上の FPGA（Virtex-5）に無対策の PRESENT と耐タンパ実装を施した PRESENT をそれぞれ実装した．そして，ランダム平文を利用して PRESENT を動作させ，このときに生じる消費電力を，オシロスコープを用いて測定した．実験環境を図 5 に示す．

4.2 実験結果

まず無対策の PRESENT に対して，CPA を行った．実験結果を図 6 に示す．図 6 の横軸は解析に使用した消費電力波形の数を，縦軸は解析に成功した PRESENT の 1 ラウ

表 4　pLayer を考慮した場合の提案マスク値間の HD

Table 4　HD between proposed mask values using pLayer.

$offset$	0	1	2	3	4	5	6	7
$p(M_{offset})$	1	9	3	c	b	0	9	5
$p(M_{offset+1})$	b	0	9	5	d	c	0	9
H_m	2	2	2	2	2	2	2	2
$offset$	8	9	10	11	12	13	14	15
$p(M_{offset})$	d	c	0	9	b	f	a	f
$p(M_{offset+1})$	b	f	a	f	2	3	6	9
H_m	2	2	2	2	2	2	2	2

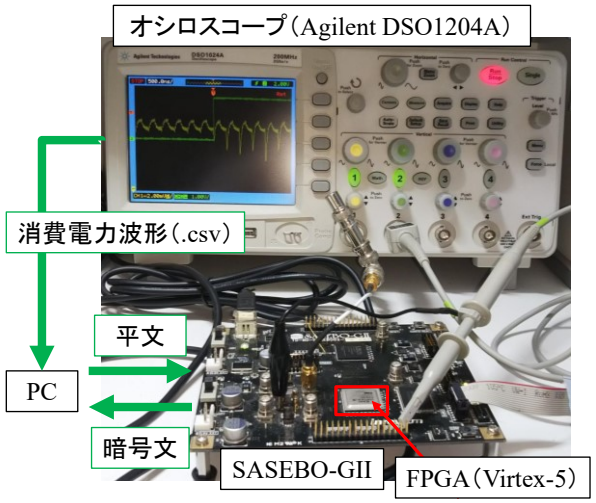

図 5　実験環境

Figure 5　Experimental environment.

ンド目のラウンド鍵のビット数を示している．図 6 から 3,000 個の消費電力波形を利用することで，1 ラウンド目のラウンド鍵を全て求めることに成功しており，無対策では PRESENT はサイドチャネル攻撃に対して，脆弱であることが確認できる．

次に，提案耐タンパ実装に対して CPA を行い，その耐タンパ性について評価した．提案耐タンパ実装に関して，内部で実装したマスク値には，2 種類のマスク値（マスク値 A「0x88379a65f0ee0145」とマスク値 B「0xe2df63a1b89c7045」）を使用した．マスク値 A は，3.2 節でも説明した，文献 [17] で推奨されているマスク値間のビット間 HD の 1 の出現確率に偏りのない乱数値であり，マスク値 B は条件を設定せずに乱数で決定したマスク値である．

耐タンパ性評価結果を図 7 に示す．図 7 に示すように 10,000 波形での正解鍵数は 24bit であり，無対策と比較して提案耐タンパ実装は耐タンパ性が向上していることが確認できる．一方で，一部の部分鍵については解析されている．ここで，10,000 波形を使用した解析における各部分鍵での相関係数の結果(マスク値 A での結果)を図 8 に示す．

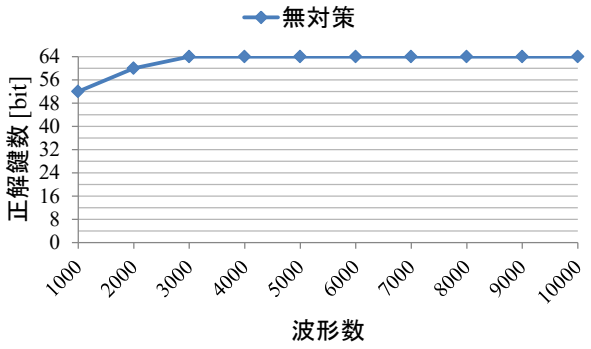

図 6　無対策の PRESENT の耐タンパ性評価

Figure 6　Tamper resistance evaluation of PRESENT without countermeasure.

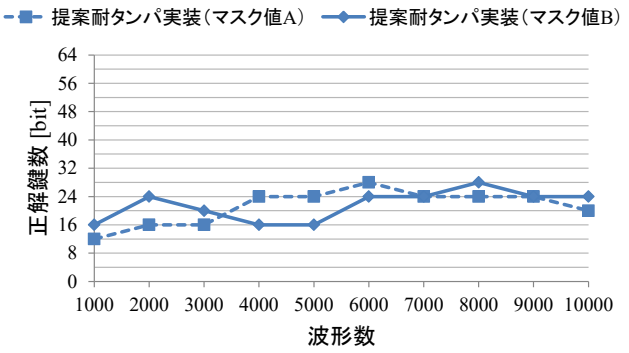

図 7　マスク値 A，B での耐タンパ性評価

Figure 7　Tamper resistance evaluation of the proposed tamper resistant implementation with mask values A and B.

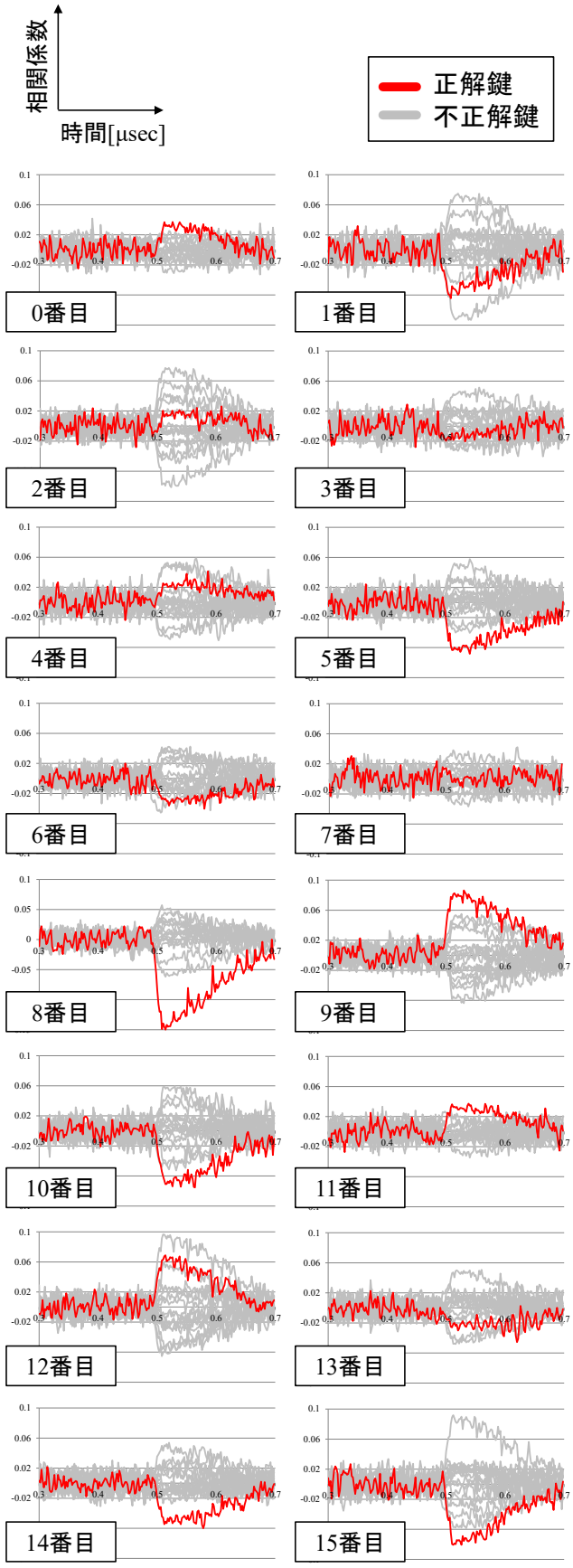

図 8　相関係数の比較

Figure 8　Comparison of correlation coefficient.

図 8 の横軸は時間を，縦軸は相関係数を，赤色は正解鍵での結果を，灰色は不正解鍵での結果をそれぞれ示している．図 8 に示すように解析に成功した 5，8，10，14，15 番目では正解鍵で相関係数のピークが表れていることが確認できる．これは 3.2 節と表 3 で説明した，マスク値間 HD の偏りが影響を与えていると考えられる．

次に，提案マスク値を使用した場合について評価した．評価結果を図 9 に示す．実験では合計で 40,000 個の消費電力波形を使用した．図 9 から 40,000 波形を用いた場合でも正解鍵数は 8bit であり，マスク値 A，B を使用するよりも耐タンパ性が改善していることが確認できる．

最後に回路規模について比較した．比較結果を表 5 にまとめる．ここで，先行研究の TI を用いた対策 [12]では，回路規模などの性能評価はシミュレーションで行われている．そして，回路規模 2,282 GE であり，無対策の PRESENT よりも 205%増加することが報告されている．表 5 から，提案耐タンパ実装の回路規模の増加割合は無対策と比較して 139%であり，TI と比較してもより小回路規模で実現できており，提案耐タンパ実装は有効であると考えられる．

5. まとめ

本研究では，軽量暗号 PRESENT を対象とした耐タンパ実装を提案した．提案耐タンパ実装では，小回路規模を指向したマスキング対策である RSM をベースとする．また耐タンパ実装では，PRESENT に適したマスク値を新たに提案した．そして，FPGA を用いた評価実験によって，提案耐タンパ実装の有効性を実証した．

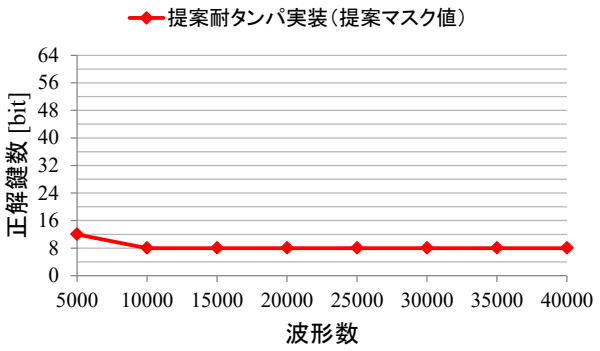

図 9　提案マスク値を用いた場合の評価

Figure 9　Evaluation of the proposed tamper resistant implementation with the proposed mask value.

表 5　回路規模の比較

Table 5　Comparison of circuit area.

	スライス数	レジスタ数	増減割合
無対策	126	153	100%
提案耐タンパ実装	232	157	139%
TI [12]	—	—	205%

今後は，ハイディングなどの他の耐タンパ実装や，更なる小回路規模化について検討する予定である．

謝辞　本研究の一部は，JSPS 科研費 16KT0188 の助成を受けたものです．

参考文献

1)　Bogdanav, A., Knudsen, L. R., Leander, G., Paar, C., Poschmann, A., Robshaw, M. J. B., Seurin, Y., and Vikkelsoe, C.: PRESENT: An Ultra-Lightweight Block Cipher, Proc. of CHES 2007, LNCS 4727, pp. 450–466, Springer-Verlag, (2007)

2)　Yang, G., Zhu, B., Suder, V., Aagaard, M. D., and Gong, G.: The Simeck Family of Lightweight Block Ciphers, Proc. of CHES 2015, LNCS 9293, pp. 307–329, Springer, (2015)

3)　Banik, S., Bogdanov, A., Isobe, T., Shibutani, K., Hiwatari, H., Akishita, T., and Regazzoni, F.: Midori: A Block Cipher for Low Energy, Proc. ASIACRYPT 2015, LNCS. 9453, pp. 411–436, Springer, (2015)

4)　Borghoff, J., Canteaut, A., Güneysu, T., Kavum, E. B., Knežević, M., Knudsen, L. R., Leander, G., Nikov, V., Paar, C., Rechberger, C., Rombouts, P., Thomsen, S. S., and Yalçin, T.: PRINCE - A Low-latency Block Cipher for Pervasive Computing Applications, Proc. of ASIACRYPT 2012, LNCS 7658, pp. 208–225, Springer, (2012)

5)　Kocher, P., Jaffe, J. and Jun, B.: Differential Power Analysis, Proc. of CRYPTO'99, LNCS 1666, pp. 388–397, Springer-Verlag (1999).

6)　Brier, E., Clavier, C., and Olivier, F.: Correlation Power Analysis with a Leakage Model, Proc. of CHES 2004, LNCS 3156, pp. 16–29, Springer-Verlag (2004).

7)　野崎佑典，吉川雅弥：低消費電力軽量暗号 Midori に対する階層的電力解析とその評価，電気学会論文誌 C，vol. 138，no. 12，pp. 1455–1463，2018 年 12 月

8)　Zhang, J., Gu, D., Guo, Z., and Zhang, L.: Differential power cryptanalysis attacks against PRESENT implementation, Proc. of IEEE ICACTE 2010, vol. 6, pp. 61–65 (2010)

9)　野崎佑典，吉川雅弥：軽量暗号に対する電磁波解析攻撃とその評価，電子情報通信学会技術研究報告，IEICE-DC，vol. 115，no. 382，pp. 29–34 (2015)

10)　Nikova, S., Rechberger, C., and Rijmen, V.: Threshold Implementations Against Side-Channel Attacks and Glitches, Proc. of ICICS 2006, LNCS 4307, pp. 529–545, Springer-Verlag, (2006)

11)　Nassar, M., Souissi, Y., Guilley, S.,and Danger, J.-L.: RSM: a Small and Fast Countermeasure for AES, Secure against 1st and 2nd-order Zero-Offset SCAs, Proc. of DATE, pp. 1173–1178 (2012)

12)　Poschmann, A., Moradi, A., Khoo, K., Lim, C.-W., Wang, H., and Ling, S.: Side-Channel Resistant Crypto for less than 2,300 GE, Journal of Cryptology, vol. 24, no. 2, pp. 322–345 (2011)

13)　Tiri, K. and Verbauwhede, I.: A Logic Level Design Methodology for a Secure DPA Resistant ASIC or FPGA Implementation, Proc. of DATE 2004, pp. 246–251 (2004)

14)　浅井稔也，汐崎　充，久保田貴也，藤野　毅，吉川雅弥：クロック変動機構を用いた耐タンパアーキテクチャ，電気学会論文誌 C，vol. 133，no. 12，pp. 2134–2142 (2013)

15)　Toyoshima, D., Ishikawa, T., Kurokawa, A., and Imai, M.: Random Delay Elements for Tamper Resistant Asynchronous Circuits based on 2-phase Handshaking Protocol, Proc. of SASIMI 2016, R2-7, pp.113–118 (2016)

16)　堤　大樹，中井綱人，汐崎　充，久保田貴也，藤野　毅：サイドチャネル攻撃対策 RSM 方式を用いた AES 暗号回路の電力解析攻撃耐性評価，2015 年暗号と情報セキュリティシンポジウム講演論文集，3A3-4，pp. 1–7 (2015)

17)　Moradi, A., Guilley, S., and Heuser, A.,: Detecting Hidden Leakages, Proc. of ACNS, LNCS 8479, pp. 324–342, Springer (2014)