Vol.2022-CDS-34 No.3
2022/6/9

# Midori128 に対する RSM を利用したサイドチャネル対策

野崎佑典[1]　竹本修[1]　池崎良哉[1]　吉川雅弥[1]

**概要**：近年，小回路規模・低消費電力・低遅延で利用可能な暗号技術として軽量暗号が注目されている．特に軽量暗号 Midori は低消費電力で利用可能なため，コンシューマ機器をはじめとした様々な分野での利用が期待されている．一方で，Midori128 に対するセキュリティ脅威としてサイドチャネル解析に対する脆弱性が報告されている．そのため，サイドチャネル解析への対策技術の研究は非常に重要である．そこで本研究では，Midori128 に対するサイドチャネル対策手法を提案する．提案手法は RSM を利用することで，サイドチャネル情報と鍵の相関関係を攪乱させ解析に対する耐性を向上させる．FPGA を利用した評価実験では，10 万個の消費電力波形を用いた解析に対して，推定に成功した秘密鍵は 0 個であり，提案手法が有効であることを明らかにした．

**キーワード**：ハードウェアセキュリティ，軽量暗号，Midori128，サイドチャネル解析，耐タンパ実装

# Side-Channel Countermeasure using RSM for Midori128

YUSUKE NOZAKI[†1]　SHU TAKEMOTO[†1]　YOSHIYA IKEZAKI[†1]　MASAYA YOSHIKAWA[†1]

***Abstract***: Lightweight ciphers, which can be used in small circuit are, low power consumption, and low latency, have been attracted attention. Since lightweight cipher Midori can be utilized in ultra-low power, it is expected to be used in various fields including consumer devices. On the other hand, Midori128 is reported to be vulnerable to side-channel analysis. Therefore, this study proposes a new side-channel countermeasure for Midori128. The proposed method reduces the correlation relationship between side-channel information and secret key by utilizing rotating s-boxes masking (RSM) method in order to improve the tamper resistance. Evaluation experiments using field programmable gate array (FPGA) showed that the number of revealed secret keys was zero against side-channel analysis using 100,000 power consumption waveforms and the proposed method had the tamper resistance.

***Keywords***: hardware security, lightweight cipher, Midori128, side-channel analysis, tamper resistant implementation

## 1. はじめに

近年，小回路規模・低消費電力・低遅延で利用可能な軽量暗号が注目されている [1][2][3]．特に本研究で対象とする Midori [1]は低消費電力で利用可能なため，コンシューマ機器をはじめとした様々な分野での利用が期待されている．Midori はブロック長に合わせてそれぞれ Midori64 と Midori128 が提案されているが，Midori64 はセキュリティ上の脆弱性 [4][5]を抱えているため，現在 Midori128 の利用が推奨されている．

一方で，暗号回路の利用において，サイドチャネル解析 [6][7][8][9][10][11][12]などの実装攻撃への対策を施すことが必要である．サイドチャネル解析は暗号回路動作時の消費電力や電磁波などの情報を利用して秘密鍵の推定を行う解析である．近年，Midori128 に対しても解析手法と対策手法の研究 [12]が行われているが，S-BOX などの非線形回路を対象とした対策の研究は行われていない．

そこで本研究では，Midori128 に対するサイドチャネル対策手法を提案する．提案手法では，Rotating S-boxes Masking（RSM [13]）を利用することでサイドチャネル解析への耐性を向上させる．また，Field Programmable Gate Array（FPGA）を用いた評価実験を行い，提案手法の有効性を定量的に評価する．

## 2. 準備

### 2.1 Midori [1]

Midori は低消費電力を指向した Substitution Permutation Network（SPN）構造を持つ軽量暗号である．鍵長は 128bit であり，ブロック長は 64bit と 128bit の 2 種類から選択可能である．ブロック長が 64bit のものを Midori64，128bit のものを Midori128 と呼ぶ．現在，Midori64 にはいくつかの脆弱性 [4][5]が報告されているため，Midori128 の利用が推奨されている．

Midori128 の概要を図 1 に，実装アーキテクチャを図 2 に示す．図 1 に示すように合計で 20 ラウンドの処理を行うブロック暗号である．1 ラウンド目から 19 ラウンド目までのラウンド関数は，SubCell，ShuffleCell，MixColumn とラウンド鍵 $RK$ との XOR 演算で構成する．0 ラウンド目は，平文と鍵 $WK$ との XOR 演算を行い，最終ラウンドである 20 ラウンド目では，SubCell と鍵 $WK$ との XOR 演算を行う

1 名城大学
Meijo University

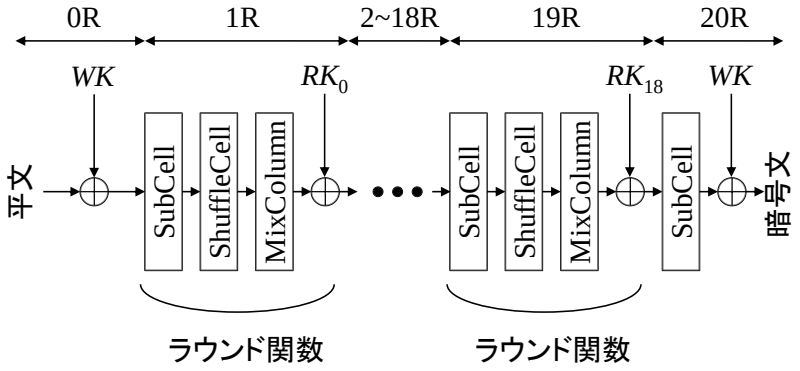



図 1　Midori128 の概要

Figure 1　Outline of Midori128.

表 1　$Sb_1$

Table 1　$Sb_1$.

| $x$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | a | b | c | d | e | f |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $Sb_1(x)$ | c | a | d | 3 | e | b | F | 7 | 8 | 9 | 1 | 5 | 0 | 2 | 4 | 6 |

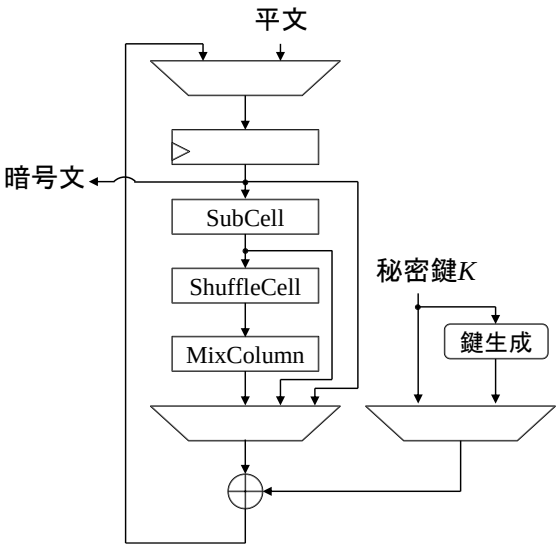



図 2　Midori128 の実装アーキテクチャ

Figure 2　Implementation Architecture of Midori128.

ことで，暗号文を生成する．ここで，暗号処理で利用する各鍵に関して，鍵$WK$については 128bit の秘密鍵$K$がそのまま使用する（$WK = K$）．また，ラウンド鍵$RK$については，各ラウンドでの定数値$\beta$と鍵$K$との XOR 演算を行うことで生成する（$RK = K \oplus \beta$）．

ラウンド関数の各処理の詳細について，SubCell では S-BOX と呼ばれる置換表による非線形処理を行う．SubCell の概要を図 3 に示す．図 3 に示すように，128bit の暗号中間値をバイトごとの State 構造で表現し，各バイトに対して S-BOX を適用する．Midori128 では，4 種類の 8-bit 置換

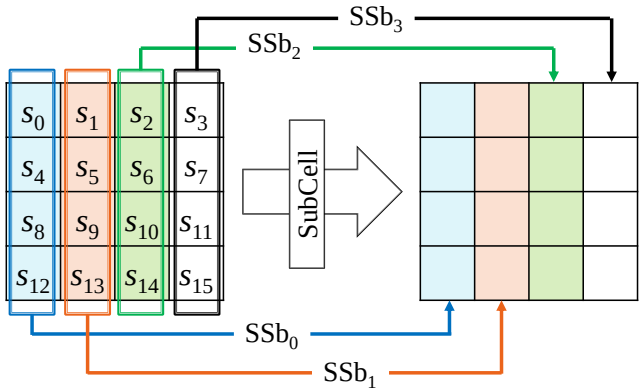



図 3　SubCell の概要

Figure 3　Outline of SubCell.

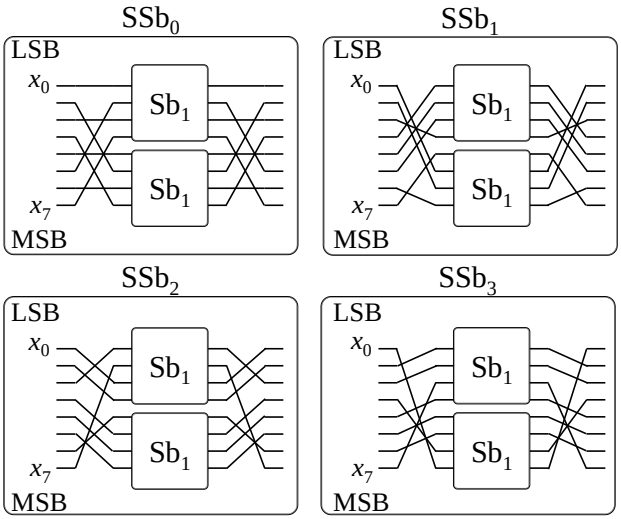



図 4　SubCell で使用する S-BOX

Figure 4　S-BOX used in SubCell.

を行う S-BOX である $SSb_0$，$SSb_1$，$SSb_2$，$SSb_3$ を使用しており，0，4，8，12 バイト目には $SSb_0$ を，1，5，9，13 バイト目には $SSb_1$ を，2，6，10，14 バイト目には $SSb_2$ を，3，7，11，15 バイト目には $SSb_3$ をそれぞれ適用する．これらの S-BOX の概要を図 4 に示す．図 4 に示すように，4-bit 置換を行う S-BOX である $Sb_1$ とその前後に 2 つの転置処理で構成する．それぞれ $SSb_0$，$SSb_1$，$SSb_2$，$SSb_3$ では，転置処理の構成が異なる．また，4bit 置換の S-BOX $Sb_1$ の置換表を表 1 に示す．

また，ラウンド関数の他の処理に関して，ShuffleCell では各 State で転置処理を行う．そして，MixColumn ではある行列に対する線形計算を行う．

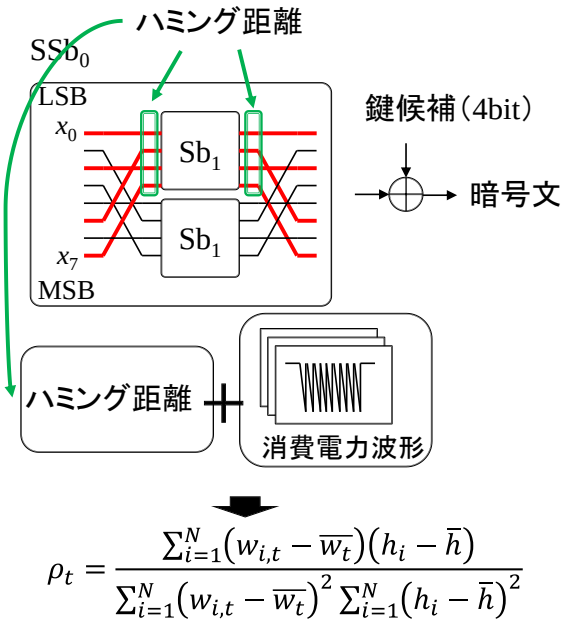
### 2.2 電力解析

電力解析は，暗号回路動作時の消費電力を利用したサイドチャネル解析である．代表的な電力解析には，差分電力解析（Differential Power Analysis：DPA [6]）や相関電力解析（Correlation Power Analysis：CPA [7]）などがある．これらの解析では，暗号処理におけるレジスタ間のデータ遷移であるハミング距離（Hamming Distance : HD）や S-BOX などの非線形ゲートでの入出力値（Hamming Weight: HW）における遷移確率差によって，消費電力にばらつきに着目することで解析を行う．例えば CPA では，計算した HD や HW を$h$，ある時間$t$における消費電力値を$w_t$とした場合，消費電力との相関関係$\rho_t$を式(1)で計算する．ここで，$N$は使用する消費電力波形の数を示しており，ある鍵候補に対してそれぞれ$h$を計算することで，相関係数$\rho_t$を計算している．CPA では，この相関値が最大となる鍵候補を正解鍵として推定する．

$$\rho_t = \frac{\sum_{i=1}^{N}\left(w_{i,t}-\overline{w_t}\right)\left(h_i-\bar{h}\right)}{\sum_{i=1}^{N}\left(w_{i,t}-\overline{w_t}\right)^2 \sum_{i=1}^{N}\left(h_i-\bar{h}\right)^2} \quad (1)$$

これまでに，Midori を対象とした電力解析手法や対策手法が提案されている．まず，Midori64 に対しては階層的な電力解析手法が提案されている [11]．文献 [11]では，Midori64 の最終ラウンドと，2 ラウンド目を対象に CPA を適用することで全ての秘密鍵の推定に成功している．また，対策手法としては，Threshold Implementation（TI）を用いたものが報告されている [14][15].

Midori128 については，近年 CPA を用いた電力解析手法が提案されている [12]．Midori128 に対する CPA では平文や暗号文を利用した解析によって秘密鍵を推定することができる．Midori128 に対する暗号文を利用した CPA の概要を図 5 に示す．図 5 に示すようにこの解析では，暗号文と鍵候補との XOR 演算を行った結果に対して SubCell を適用することで，暗号文と一つ前のラウンドとの HD を計算する．このとき，SubCell は 8bit 単位の S-BOX を利用しているが，各 SSb は 4bit 単位の $Sb_1$ で構成しているため，4bit ずつ計算する．4bit の鍵候補を利用するため，1 つの部分鍵の解析では $2^4 = 16$ 通りの計算を行う．秘密鍵は 128bit であるため，$N$個の波形データに対して合計で$N$×16×32 回の計算で解析することができる．




$$\rho_t = \frac{\sum_{i=1}^{N}\left(w_{i,t}-\overline{w_t}\right)\left(h_i-\bar{h}\right)}{\sum_{i=1}^{N}\left(w_{i,t}-\overline{w_t}\right)^2 \sum_{i=1}^{N}\left(h_i-\bar{h}\right)^2}$$

図 5　Midori128 に対する CPA
Figure 5　CPA for Midori128.

また，対策に関してはレジスタに乱数マスクを施すマスキング対策が提案されている [12]．しかし，非線形処理を行う S-BOX への対策手法は提案されていない．

## 3. 提案手法

本研究では，Midori128 に対するサイドチャネル対策手法を提案する．提案手法では，RSM [13]をベースとした手法を導入することによって，小回路規模で耐タンパ性を向上させる．RSM は AES 暗号を対象に小回路規模を指向して提案されたマスキング対策手法である．RSM では，乱数を利用した変形 S-BOX を導入することで，暗号中間値と消費電力との相関関係を隠蔽する．このとき，通常のマスキングでは，使用する乱数に合わせて複数の変形 S-BOX を導入する必要があるが，RSM では変形 S-BOX をローテーションさせ再利用することで，回路オーバーヘッドを抑制する．

本研究では，Midori128 の S-BOX が 4bit 単位の $Sb_1$ によって構成していることに着目し，8bit 単位の S-BOX である $SSb_0$，$SSb_1$，$SSb_2$，$SSb_3$ ではなく，最小単位である $Sb_1$ に対して RSM 対策を導入することで回路オーバーヘッドを抑える．ここで，従来の RSM 対策を Midori128 にそのまま適用させることは難しい．なぜなら，AES 暗号と比較して Midori128 の S-BOX の構造が大きく異なるからである．

具体的には，変形 S-BOX の構成では，事前に決められた乱数に対応したアンマスキングと S-BOX の置換処理，乱数によるマスキングを行う必要がある．AES 暗号では，ラウンド処理において S-BOX 前に他の転置処理などが含まれていないため，データレジスタに使用するマスク値のみを考慮して変形 S-BOX を生成することができる．一方で，Midori128 の SubCell は $Sb_1$ と前後の転置処理で構成しており，S-BOX の前に転置処理が含まれている．この場合，変形 S-BOX を作成するためには決められた乱数に対して転置処理も考慮する必要があり，非常に複雑な回路になる．

そこで，この課題を解決するために本研究では，SubCell の $Sb_1$ と，前後の転置処理を分割したループアーキテクチャを導入する．具体的には，$Sb_1$ の前後の転置処理をそれぞれ $P_x$，$P_y$ とする．本研究で使用する実装アーキテクチャを図 6 に示す．

図 7 に提案手法の概要を示す．提案手法では，データレジスタの値だけなく，計算途中の暗号中間値全てに対して乱数によるマスキングを行う．マスキングを行うことで，サイドチャネル情報と秘密情報の相関関係を隠蔽し，耐タンパ性を向上させる．このとき，提案手法で利用する乱数について，Midori128 の S-BOX の最小単位である $Sb_1$ が 4bit 単位で処理を行っているため，4bit 単位のマスク値を使用する．このとき，ブロック長は 128bit であるため，32 個のベースマスク値$m_0, \ldots, m_{31}$を利用する．

また，ベースマスク値は，実装前に事前に乱数で決定し，回路内部で保持する．実際に各ラウンドで使用するマスク値は，ある 5bit のオフセット値$offset$を利用することで生成する．具体的に，128bit の乱数値$M_{offset}$は式(2)で計算する．このとき，5bit のオフセット値$offset$は式(3)で更新する．

$$M_{offset} = m_{offset+0(\mathrm{mod}32)} \| \cdots \| m_{offset+31(\mathrm{mod}\,32)} \quad (2)$$

$$offset = offset + 1 \ (\mathrm{mod}\ 32) \quad (3)$$

提案手法の各処理に関して，暗号中間値$X_1$は $Sb_1$ の前処理である$P_x$による転置処理を適用し，この計算結果に対してマスク値$M_{offset}$による XOR 演算を行い，マスクした値

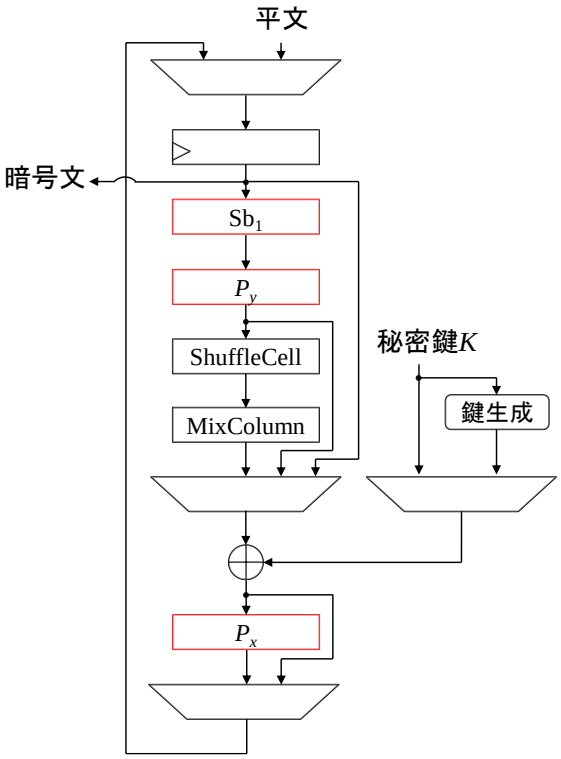



図 6　提案手法での Midori128 の実装アーキテクチャ
Figure 6　Implementation architecture of Midori128 in the proposed method.

（$X_1 \oplus M_{offset}$）をデータレジスタへ格納する．次に，変形 $Sb_1$ では暗号中間値をマスクしながら，$Sb_1$ による置換処理を行う．変形 Sb1 の詳細については後程説明する．そして，$Sb_1$ の後処理である$P_y$による転置処理，ShuffleCell，MixColumn，ラウンド鍵$RK_0$による XOR 演算に加えて，次のラウンドの $P_x$ の転置処理を行い，この計算結果をデータレジスタへ格納する．このとき，データレジスタへ格納する値は，暗号中間値$P_x(X_2)$に対して，次のラウンドのマスク値でマスキングした値になるように処理する．この処理では，変形 $Sb_1$ 以降で適用した$P_y$，ShuffleCell，MixColumn をマスク値$M_{offset}$に適用した値で XOR 演算することで，$M_{offset}$に関連する値のアンマスキングを行い，次のマスク値$M_{offset+1}$によるマスキングを適用する．

次に変形 $Sb_1$ の詳細について説明する．変形 $Sb_1$ の構成を図 8 に示す．図 8 に示すように，2 つのシフター回路と 32 個の$Sb_1'$で構成する．シフター回路では，入力される 5bit のオフセット値に対応した変形 Sb1 を選択する．ここで，$Sb_1'$はマスクされている暗号中間値$x'$に対して，式(4)による計算を行う．

$$Sb_1'_{offset}(x') = Sb_1(x \oplus m_{offset}) \oplus m_{offset+1 (\mathrm{mod}\ 32)} \quad (4)$$

このとき，$Sb_1(\ )$は $Sb_1$ の置換処理であり，置換処理を行う直前に$m_{offset}$によってアンマスクされ，置換処理の直後に次のマスク値によってマスキングされる．実際にはこれらの処理をまとめた処理を 1 つの置換処理として$Sb_1'(\ )$で実行される．この変形 $Sb_1$ では，入力 $(x')$ と出力 $(Sb_1'(x'))$ がそれぞれマスクされた値であるため，サイドチャネル解析に対する耐タンパ性を持つ．

また，変形 $Sb_1$ は，32 種類のベースマスク値$m_0, \ldots, m_{31}$に合わせて 32 種類生成する．通常対策を行わない図 2 のループアーキテクチャにおいても，実装する $Sb_1$ は 32 個であるため，提案手法では追加で実装するのはシフター回路のみであるため実装オーバーヘッドを抑えることができる．

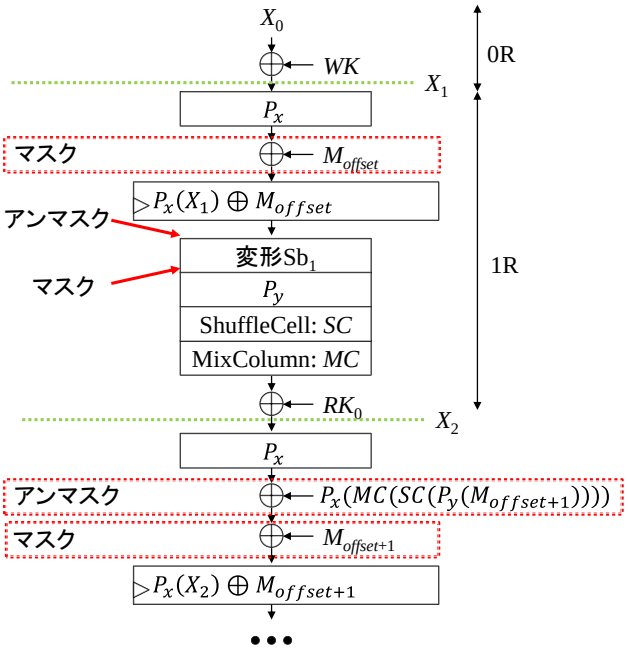



図 7　提案手法の概要

Figure 7　Outline of the proposed method.

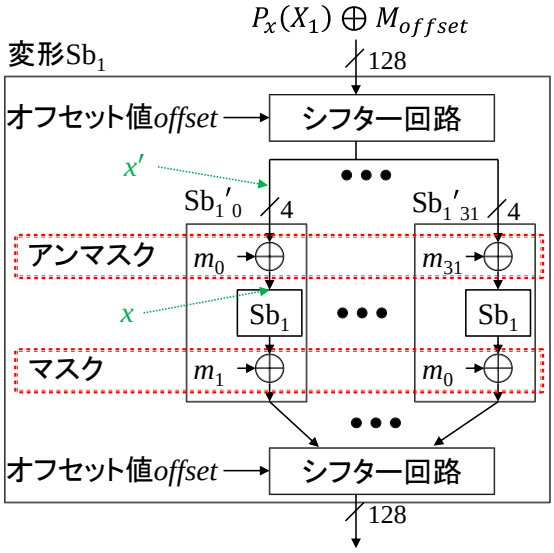



図 8　変形 $Sb_1$

Figure 8　Custom $Sb_1$.

## 4. 評価実験

評価では，提案する対策手法を適用した Midori128 と無対策の Midori128 をそれぞれ FPGA 実装した．評価ボードには SASEBO-GII を使用し，オシロスコープには Keysight DSOX1204G を使用した．実験環境を図 9 と表 2 に示す．実験では暗号処理時の消費電力波形を 10 万個測定し，それぞれ電力解析を適用することで，Midori128 の耐タンパ性を評価した．

実験結果を図 10 に示す．図 10 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秘密鍵の bit 数をそれぞれ示している．まず，図 10 から無対策の場合では，1 万波形で全ての秘密鍵を推定可能であることが確認でき，Midori128 が電力解析に対して脆弱であることが確認できる．一方で，提案手法では 10 万個の消費電力波形を用いた場合でも正解鍵数は 0 である．したがって，提案手法は電力解析に対して高い耐タンパ性を持っており，有効であると考えられる．

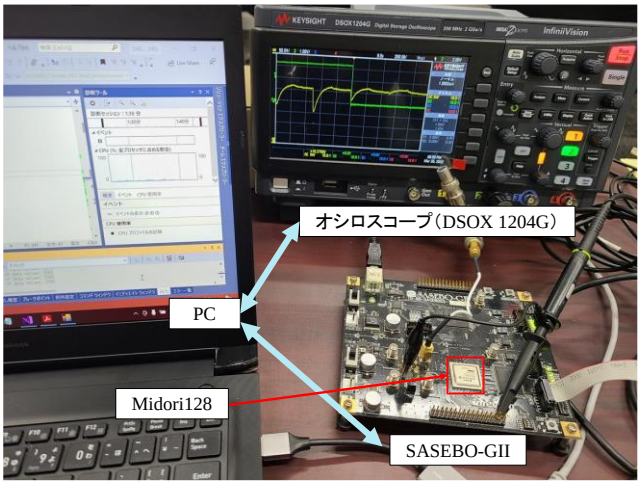



図 9　評価環境

Figure 9　Evaluation environment.

表 2　実験環境

Table 2　Experimental condition.

| | |
|---|---|
| オシロスコープ | Keysight DSOX 1024G |
| サンプリングレート | 2 GSa/sec |
| 周波数帯域 | 200MHz |
| 測定波形数 | 10 万波形 |
| 評価ボード | SASEBO-GII |
| FPGA | Xilinx Virtex-5 XC5VLX30 |
| ハードウェア記述言語 | Verilog HDL |
| 実装ツール | Xilinx ISE Design Suite 14.7 |
| 実装回路 | 提案対策手法を適用した Midori128 / 無対策の Midori128 |

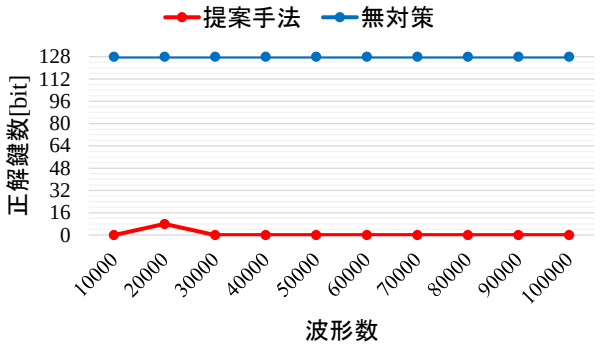



図 10　実験結果

Figure 10　Experimental results.

## 5. まとめ

本研究では, Midori128 に対するサイドチャネル解析対策手法を提案した．提案手法では，RSM を利用したマスキングを導入することで解析に対する耐タンパ性を向上させる．FPGA を用いた評価実験では，無対策の Midori128 が 1 万波形を用いた解析で全秘密鍵が推定されたのに対して，提案手法では 10 万個の消費電力波形を用いた場合でも鍵を推定することができず耐タンパ性が向上することを明らかにした．

今後は，他の解析手法である電磁波解析やフォールト解析に対する耐タンパ性評価や対策手法についての検討を進める予定である．

**謝辞**　本研究の一部は，JSPS 科研費 22K17891 の助成を受けたものです．

## 参考文献

[1] 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)

[2] 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)

[3] 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)

[4] Lin, L. and Wu, W.: Meet-in-the-Middle Attacks on Reduced-Round Midori64, IACR Trans. Symmetric Cryptology, vol. 2017, no. 1, pp. 215–239, (2017)

[5] Todo, Y., Leander, G., and Sasaki, Y.: Nonlinear In- variant Attack: Practical Attack on Full SCREAM, iSCREAM, and Midori64, Proc. ASIACRYPT, LNCS 10032, pp. 3–33, Springer, (2016)

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

[7] Brier, E., Clavier, C., and Olivier, F.: Correlation Power Analysis with a Leakage Model, Proc. of 6th Int. Workshop Cryptographic Hardware and Embedded Systems (CHES 2004), LNCS 3156, pp.16–29, Springer-Verlag (2004).

[8] Mangard, S., Oswald, E., and Popp, T.: Power Analysis Attacks. Springer, p.338 (2007).

[9] Gandolfi, K., Mourtel, C., and Olivier, F.: Electromagnetic Analysis: Concrete Results, Proc. 3rd Int. Workshop on Cryptographic Hardware and Embedded Systems (CHES 2001), LNCS 2162, pp.251–261, Springer-Verlag (2001).

[10] Meynard, O., Guilley, S., Danger, -L. J., and Sauvage, L.: Far Correlation-based EMA with a Precharacterized Leakage Model, Proc. Design, Automation and Test in Europe Conference and Exhibition (DATE 2010), pp.977–980 (2010).

[11] 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

[12] 竹本修，池崎良哉，野崎佑典，吉川雅弥：Midori128 に対する電力解析攻撃手法と低エネルギーなセキュア実装，情報処理学会論文誌，vol. 63，no. 3，pp. 831–839，2022 年 3 月

[13] 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)

[14] Moradi, A. and Schneider, T.: Side-Channel Analysis Protection and Low-Latency in Action - case study of PRINCE and Midori, Proc. of ASIACRYPT 2016, LNCS 10031, pp. 517–547, Springer, (2016)

[15] Shahmirzadi, A. R. and Moradi, A.: Re-Consolidating First-Order Masking Schemes - Nullifying Fresh Randomness, IACR Trans. Cryptographic Hardware and Embedded Systems, vol. 2021, no. 1, pp. 305–342, (2020)