情報処理学会論文誌 Vol.63 No.3 831–839 (Mar. 2022)

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

竹本 修[1,a)] 池崎 良哉[1] 野崎 佑典[1] 吉川 雅弥[1]

受付日 2021年5月22日, 採録日 2021年12月3日

概要：近年のIoTの拡大にともない，デバイスの低エネルギー動作によって電力供給の課題解決が重要である．それにともない，安全なデータ収集の実現に低エネルギー動作を指向した軽量暗号Midoriが提案されている．一方で，計算量的に安全なブロック長が128 bitsであるMidori128はこれまでに耐タンパ性評価がされていない．したがって，Midori128に対する耐タンパ性の評価とセキュア実装の確立が重要である．そこで本研究はMidori128に対して新たに電力解析攻撃手法を提案する．提案手法は攻撃条件や攻撃対象によって使い分けることで効率的に解析できる．評価実験の結果，ループアーキテクチャ実装の暗号回路が提案手法に脆弱であることを示した．さらに，1暗号化あたりの消費エネルギーと耐タンパ性の観点からアンロールドアーキテクチャ実装がセキュア実装として適している．

キーワード：ハードウェアセキュリティ，軽量暗号，Midori，電力解析，耐タンパ性

Power Analysis Attack Method and Low Energy Secure Implementation for Midori128

Shu Takemoto[1,a)] Yoshiya Ikezaki[1] Yusuke Nozaki[1] Masaya Yoshikawa[1]

Received: May 22, 2021, Accepted: December 3, 2021

Abstract: With the expansion of IoT in recent years, it is important to solve the problem of power supply by low energy operation of devices. Accordingly, a lightweight block cipher, Midori, has been proposed for secure data collection with low energy operation. On the other hand, Midori128, which has a computationally secure block length of 128 bits, has not been evaluated for tamper resistance so far. Therefore, it is important to evaluate tamper resistance and establish secure implementation in Midori128. This study proposes several power analysis attack methods against Midori128. The proposed method can be efficiently analyzed by using different attack conditions and targets. The evaluation experiments show that the cryptographic circuit with loop architecture implementation is vulnerable to the proposed method. Furthermore, an unrolled architecture implementation is suitable as a secure implementation in terms of energy consumption per encryption and tamper resistance.

Keywords: hardware security, lightweight block cipher, Midori, power analysis, tamper resistance

1. はじめに

近年，IoTは急速な普及を続けており，世界のIoTデバイスは250億台を超えて幅広い分野で活用されている[1]．一方で，IoTデバイスに関して，配線やバッテリ等の電源供給関するという課題が残されている[2]．そのため，IoTデバイスは低エネルギー動作が重要な要素の1つであり，これまでにIoTを指向したアーキテクチャ[3], [4]や通信方式[5], [6]が提案されている．

一方，IoTデバイスに対するサイバー攻撃は増加の一途をたどっている[7]．そのため，安全なデータ収集のために，暗号技術として軽量暗号の実装がセキュリティ対策の1つとして重要である．様々な軽量暗号の中でも低エネルギー動作を指向した代表的な軽量暗号としてMidori[8]が

[1] 名城大学
Meijo University, Nagoya, Aichi 468–8502, Japan
[a)] 193426008@ccmailg.meijo-u.ac.jp

ある．Midori は暗号処理 1 回あたりの消費電力量が少なく，回路規模を抑えたうえで高スループットを実現することができるアルゴリズムである [9]．また，ブロック長が 128 bits である Midori128 は計算量的安全性が保障されている．

これまでに，軽量暗号はサイドチャネル攻撃に脆弱であることが指摘されている [10]．特に，ブロック長が 64 bits である Midori64 は消費電力を用いたサイドチャネル攻撃である電力解析攻撃に脆弱であることが指摘されている [11], [12]．文献 [11] では，Midori64 のループアーキテクチャ実装に対し，実デバイス上で電力解析攻撃を行い，耐タンパ性について評価している．文献 [12] では，Midori64 のループアーキテクチャ実装だけでなくアンロールドアーキテクチャ実装について実装方式の違いによる T 検定を用いた耐タンパ性評価を報告している．しかし，Midori128 に対しては電力解析攻撃に対する耐タンパ性評価が行われていない．Midori128 は，計算量的安全性の観点から Midori64 よりも利用が期待されており [9], [13], [14]，Midori64 と比較してブロック長および暗号アルゴリズムが異なる．具体的に，ブロック長の増加は，並列処理される組合せ回路が増加することで消費電力波形内に生じるノイズも増加する．また，電力解析攻撃の要となる非線形処理 SubCell の構造が異なり，従来の解析手法 [11], [12] をそのまま適用することが難しい．したがって，Midori128 の暗号アルゴリズムを指向した解析手法を提案し，耐タンパ性を評価することが安全性を担保するために非常に重要である．また，電力解析攻撃に対する耐タンパ性評価では暗号化アルゴリズムだけでなく実装方式によっても消費電力のノイズの影響が異なることから，解析手法が異なる．

そこで本研究では，まず，Midori128 の耐タンパ性評価に必要な電力解析攻撃手法を提案する．提案手法では攻撃時に取得可能な情報や暗号ハードウェアの実装方式によって消費電力の着目点が異なるため，攻撃条件に応じたアルゴリズムを導入する．次に，FPGA 評価ボードを用いた実装実験によって Midori128 の耐タンパ性を評価し，IoT デバイスに最適な低エネルギー動作でかつ耐タンパ性の高い実装方式について考察する．

2. 準備

本章では，本研究に必要な要素技術として，軽量暗号 Midori のアルゴリズムを 2.1 節，電力解析攻撃の概要を 2.2 節でそれぞれ述べる．

2.1 Midori

Midori はハードウェア実装において低エネルギー動作を指向した代表的な軽量暗号の暗号アルゴリズムである [8]．Midori のブロック長，鍵長，ラウンド数の対応について **表 1** に示す．Midori64 は計算量の観点から脆弱性が指摘されており [13], [14]，現在では Midori128 の利用が推奨されている．

表 1 Midori のパラメータ
Table 1 Parameters at Midori.

	block size	key size	rounds
Midori64	64	128	16
Midori128	128	128	20

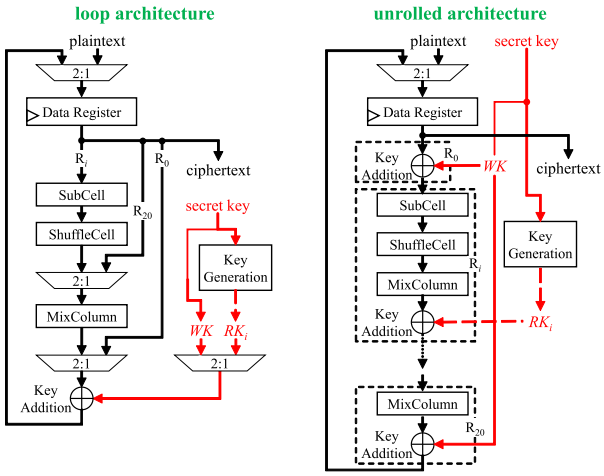


図 1 Midori128 の暗号化アルゴリズム
Fig. 1 Encryption algorithm for Midori128.

表 2 Sb_1
Table 2 Sb_1.

x	0	1	2	3	4	5	6	7
S(x)	c	a	d	3	e	b	f	7
x	8	9	a	b	c	d	e	f
S(x)	8	9	1	5	0	2	4	6

図 1 に示すように Midori128 は SPN 構造の暗号化アルゴリズムである．ここで，R_i はラウンド関数，WK は秘密鍵，RK_i はラウンド関数ごとに演算する鍵（ラウンド鍵）を示している．ラウンド関数には SubCell，ShuffleCell，MixColumn，KeyAddition が含まれており，最後のラウンド関数 R_{20} は Subcell と KeyAddition のみ計算する．また，最初のラウンド関数 R_1 の前には事前処理（以下，R_0 と呼ぶ）として，KeyAddition を計算する．

SubCell は置換表 S-box を用いた非線形な置換処理である．Midori128 では，**表 2** に示す 4 bits 入出力の置換表 Sb_1 をベースとし，4 種類の 8 bits 入出力置換表 SSb_0，SSb_1，SSb_2，SSb_3 を構成する．**図 2** に示すように SubCell は，128 bits の入力について，1 byte ごとのブロック（State）に切り分け，対応した置換表 SSb に値を与える．各 State の s_i に対応する置換表 SSb_j について，i と j の関係は式 (1) で示される．

$$j = i \pmod 4 \tag{1}$$

8 bits の入力は Sb_1 の前後でビットの位置の入れ替えを

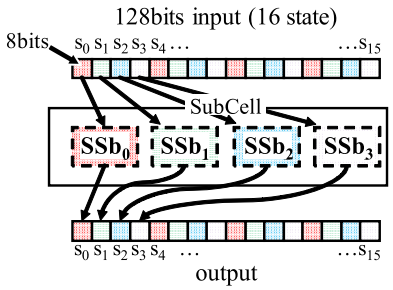


図 2 SubCell の概要
Fig. 2 Outline of SubCell.

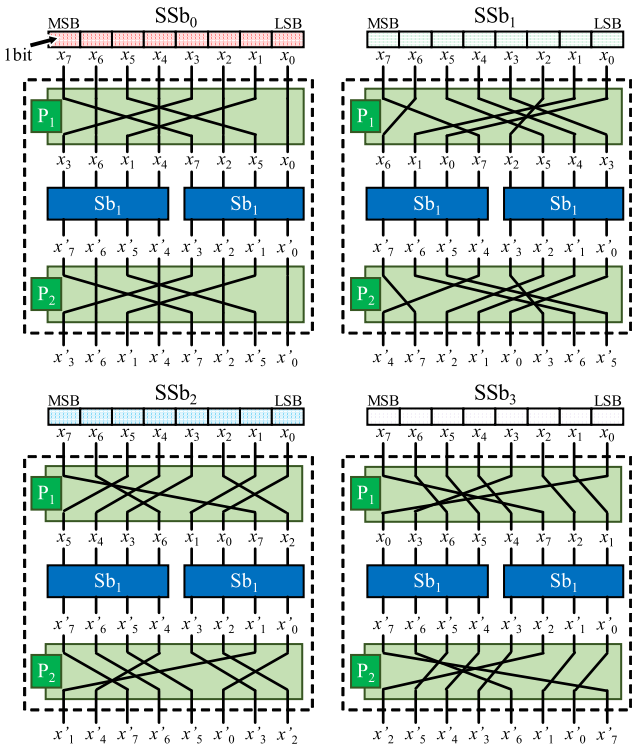


図 3 SSb_j
Fig. 3 SSb_j.

行う転置処理が含まれており，SSb ごとに異なる．それぞれ，Sb_1 の直前に行われる転置処理 P_1 および直後の転置処理 P_2 について**図 3** に示す．また，P_1 と P_2 は式 (2) の関係にある．

$$P_2(P_1(x_{7,6,5,4,3,2,1,0})) = x_{7,6,5,4,3,2,1,0} \tag{2}$$

暗号をハードウェア実装する際はいくつかの実装方式がある．代表的な方式には，図 1 の左側に示すようにクロックごとに 1 つのラウンド関数を計算するループアーキテクチャ実装と，図 1 の右側に示すように 1 クロックですべてのラウンド関数を計算するアンロールドアーキテクチャ実装がある．

2.2 電力解析攻撃

ハードウェア実装した暗号回路について，暗号回路動作時の消費電力から秘密鍵の値を解析する電力解析攻撃が報告されている．電力解析攻撃は暗号に含まれる非線形処理に着目して解析が行われる．非線形処理では，入力値によって暗号中間値の遷移確率が偏る．また，CMOS 回路である暗号回路は，暗号中間値の遷移確率と消費電力量との間に比例関係を持つ．これらのことから，暗号回路動作時の消費電力を測定することで，暗号中間値の遷移確率を推測でき，鍵加算処理で使用された未知の秘密鍵の値を解析することができる．

解析時には，測定した消費電力と既知の暗号回路の入出力値を用いて統計処理を行う．統計処理では，代表的な手法として Correlation Power Analysis（CPA）[15] があり，式 (3) に示すピアソンの相関係数に基づいて相関関係を算出する．

$$\rho = \frac{\sum_{i=1}^{D}(w_{i,t} - \bar{w}_t)(h_t - \bar{h})}{\sqrt{\sum_{i=1}^{D}(w_{i,t} - \bar{w}_t)^2 \sum_{i=1}^{D}(h_i - \bar{h})^2}} \tag{3}$$

ここで，w は消費電力，h は暗号中間値のハミング距離，D は使用する最大波形数である．

また，秘密鍵の解析では攻撃者が得られる情報に応じて攻撃条件が次のように分類される．

- 既知平文攻撃（KPA: Known-Plaintext Attack）：既知の平文を用いて未知の秘密鍵を解析する攻撃
- 選択平文攻撃（CPA: Chosen-Plaintext Attack）：任意の平文を用いて未知の秘密鍵を解析する攻撃
- 既知暗号文攻撃（KCA: Known-Ciphertext Attack）：既知の暗号文を用いて未知の秘密鍵を解析する攻撃
- 選択暗号文攻撃（CCA: Chosen-Ciphertext Attack）：任意の暗号文を用いて未知の秘密鍵を解析する攻撃

3. 提案手法

本研究では，Midori128 を指向した電力解析攻撃手法を提案する．提案手法は暗号回路の実装方式に応じて攻撃手法が異なり，ループアーキテクチャ実装については 3.1 節，アンロールドアーキテクチャ実装については 3.2 節で述べる．

3.1 ループアーキテクチャ実装に対する電力解析攻撃

ループアーキテクチャ実装ではラウンド関数を演算し終えるたびに暗号中間値がレジスタに格納されるため，暗号回路の消費電力はレジスタの遷移数が支配的となる．そのため，ループアーキテクチャ実装に対する提案電力解析攻撃は，レジスタの遷移数に着目する．提案手法は，Midori128 を効率的に解析するために，AES に対する解析とは異なる SubCell の構造に着目したアプローチを採用する．AES と Midori128 はどちらも非線形処理の入出力長が 8 bits であり，AES の手法をそのまま適用すると，128 bits の鍵に対し 8 bits 部分鍵の解析を 16 回繰り返すため，$2^8 \times 16$ 回の試行回数を必要とする．Midori128 の非線形処理 SubCell

は内部に 4 bits ごとの置換処理 Sb_1 とその前後の転置処理によって構成されていることから，提案手法では Sb_1 に着目した解析手法を採用することで，4 bits 部分鍵の解析を 32 回繰り返し，計算量を 8 分の 1 に削減できる．また，秘密鍵の解析は既知の入出力データによって手法が異なる．

3.1.1 既知平文攻撃下での解析手法

既知平文攻撃では，入力側のラウンド関数から秘密鍵を推定するため，Midori128 の非線形処理が含まれる最初のラウンドである R_1 に着目する．そして，R_0 から R_1 のレジスタ遷移数と観測した消費電力量との間に相関関係があると仮定し，秘密鍵を解析する．

R_0 後の暗号中間値 x^0 は，未知の秘密鍵 K_g と既知の平文 P を用いて式 (4) で求められる．

$$x^0 = P \oplus K_g \tag{4}$$

また，R_1 後の暗号中間値 x^1 は，x^0 を用いて式 (5) で求められる．

$$x^1 = \mathrm{MixColumn}(\mathrm{ShuffleCell}(\mathrm{SubCell}(x^0))) \oplus K_g \oplus \alpha \tag{5}$$

次に，x^0 と x^1 とのハミング距離 h を求め，暗号回路動作時の R_1 の近傍の消費電力を測定し，式 (3) を算出する．ハミング距離はすべての鍵候補値（推測鍵）で計算しておき，最も高い相関係数値が得られた推測鍵は正解の秘密鍵と考えられる．効率的な解析のため，秘密鍵は置換表の最小単位である Sb_1 の 4 bits ごとに解析し，128 bits 分まで繰り返すことですべてのビットを解析する．

3.1.2 既知暗号文攻撃下での解析手法

既知暗号文攻撃では，出力側のラウンド関数から秘密鍵を推定するため，Midori128 の最終ラウンドの R_{20} に着目する．そして，既知平文攻撃と同様に，R_{19} から R_{20} のレジスタ遷移数と消費電力の相関関係を用いて秘密鍵を解析する．

R_{19} の暗号中間値 x^{19} は既知の暗号文 C を用いて式 (6) で求められる．

$$x^{19} = \mathrm{InvMixColumn}(C \oplus K_g) \tag{6}$$

ここで，InvMixColumn は MixColumn の逆演算である．

次に，x^{19} と C とのハミング距離 h を求め，R_{19} の近傍の消費電力を測定し，式 (3) を算出する．秘密鍵の導出は既知平文攻撃と同様である．

3.2 アンロールドアーキテクチャ実装に対する電力解析攻撃

アンロールドアーキテクチャ実装した暗号回路はすべての演算が組合せ回路で構成されるため，R_1 といった入力側に近い回路と比較して R_{20} といった出力側に近い回路はクロックスキューの影響によって演算のタイミングに揺らぎが生じる．このため，出力側の回路を対象とした解析では，測定した消費電力との相関が得られず，解析が困難である．実際に，低遅延実装した PRINCE [16] といった軽量暗号に対しては，出力側のラウンド関数になるにつれて，攻撃により特定された部分鍵数が減少することが報告されている [17], [18]．

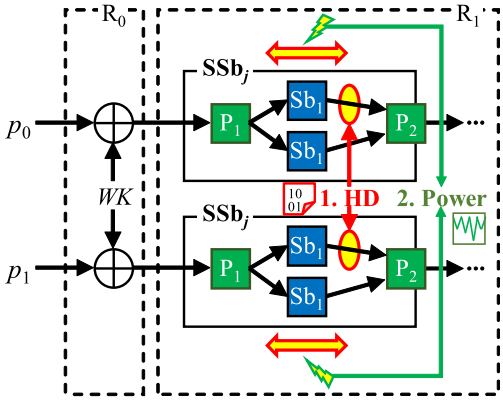


図 4 アンロールドアーキテクチャ実装の解析位置と 2 階攻撃
Fig. 4 POI and 2nd-order attack for unrolled architecture.

したがって，アンロールドアーキテクチャ実装に対する電力解析手法では，Midori128 に対して平文を用いて R_1 を対象に解析を行う．また，ハードウェアデバイスではレジスタ間の遷移数と線形な関係のある消費電力が支配的であり，組合せ回路の遷移数による消費電力はそれよりも非常に小さい．ループアーキテクチャ実装はレジスタ間の遷移数を活用できる一方で，アンロールドアーキテクチャ実装では組合せ回路内のわずかな消費電力量に着目する．そこで，従来手法 [17] をベースとして，2 階の電力解析攻撃（2nd-order attack）[19] によって解析する．

図 4 に示すように提案手法では 2 回の暗号化処理を組み合わせて統計処理を行う．まず，式 (7) のように 2 種類の入力 p_0，p_1 を与えたときにそれぞれについて Sb_1 後の値を計算し，暗号中間値間のハミング距離（HD）を計算する（図 4 の 1）．

$$\begin{aligned} h = \mathrm{HD}\ & (\mathrm{Sb}_1(\mathrm{P}_1(p_0 \oplus WK) \gg 4) \times n \\ & \oplus \mathrm{Sb}_1(\mathrm{P}_1(p_0 \oplus WK) \oplus \mathrm{0x0f}) \times |n-1|, \\ & \mathrm{Sb}_1(\mathrm{P}_1(p_1 \oplus WK) \gg 4) \times n \\ & \oplus \mathrm{Sb}_1(\mathrm{P}_1(p_1 \oplus WK) \oplus \mathrm{0x0f}) \times |n-1|) \end{aligned} \tag{7}$$

ここで，n（$0 \le n \le 15$）は解析で着目する Sb_1 の位置を示しており，$\mathrm{HD}(a, b)$ はデータ a とデータ b のハミング距離について示す．従来手法 [17] では非線形処理後の暗号中間値のハミング距離を計算するが，提案手法では，非線形処理内部の Sb_1 に着目することで，8 bits 入出力の SubCell であっても 4 bits の単位の暗号中間値に対して解析を実現する．これにより，120 bits だけでなく 124 bits 分の暗号中間値の遷移数の差分を 0 にでき信号対ノイズ比（Signal-Noise Ratio: SNR）を向上させることができる．

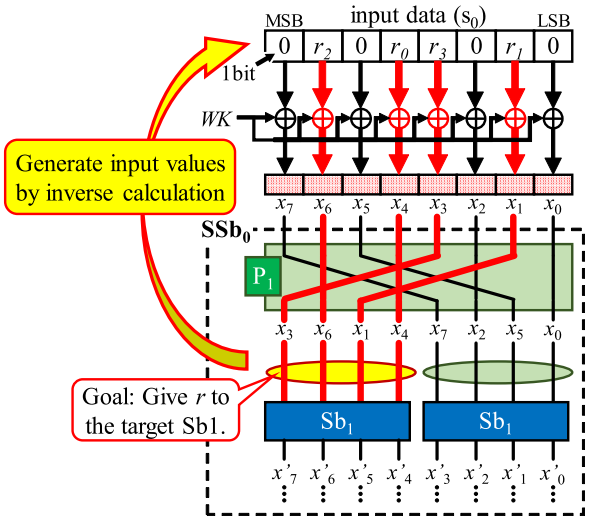


図 5 提案選択平文による演算の流れ

Fig. 5 Flow of proposed chosen-paintext attack.

次に，2 回の暗号処理における Sb_1 周辺の消費電力について差分を計算し，消費電力波形を得る（図 4 の 2）．最後に，これらのデータを数十万ペア収集し，式 (3) を算出することで秘密鍵を解析する．

さらに，解析精度を向上させるため，解析は選択平文攻撃を想定し，解析対象の S-box の特徴量のみが含まれるような差分消費電力を生成する．従来手法 [18] では，アルゴリズムが 4 bits の State ごとに分離できることに着目し，4 bits の乱数値をシフトさせながら選択平文を生成することで，解析対象の部分鍵に対し解析精度を向上させている．提案手法では，SubCell の構造に着目し，式 (8) および式 (9) に示す転置処理を考慮した選択平文アルゴリズムを提案する．

$$p_0 = \mathrm{P}_2(r_0 \ll (4 \times n)) \ll (8 \times m) \tag{8}$$

$$p_1 = \mathrm{P}_2(r_1 \ll (4 \times n)) \ll (8 \times m) \tag{9}$$

ここで，n は解析で着目する Sb_1 の位置を，m は SSb の解析位置を，r_0 および r_1 は 0 から 15 までの 4 bits の乱数値を示している．**図 5** のように，解析対象で注目している Sb_1 の入力は乱数 r_i と秘密鍵 WK が加算された値となり，それ以外の値は WK がそのまま入力される．解析時には WK が入力された Sb_1 の値は 2 回の暗号処理間でハミング距離はつねにゼロとなり，消費電力間の差分も生じない．そして，解析対象の State に関するハミング距離とノイズによる影響が抑えられた消費電力が得られる．

4. 評価実験

本章では，Midori128 に対する評価ボードを用いた実証実験について述べる．4.1 節では実験要領について，4.2 節では実装時の動作性能と暗号回路の脆弱性に関する実験結果について，4.3 節では実験結果に対する考察について述べる．

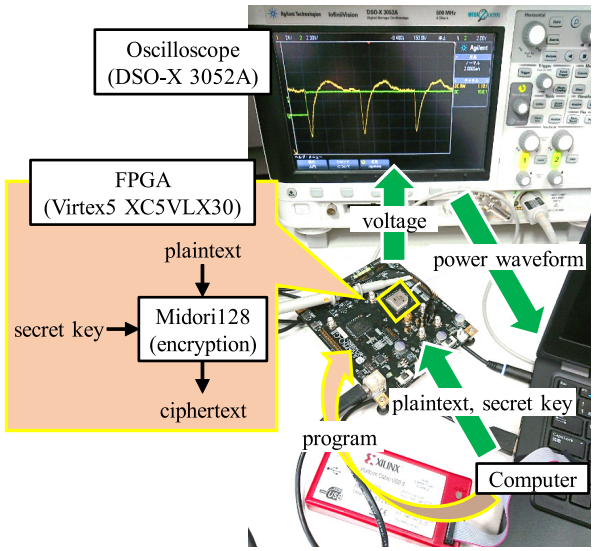


図 6 実験環境

Fig. 6 Experimental setup.

表 3 評価回路の一覧

Table 3 Evaluation circuits.

name	algorithm	architecture	countermeasures
circuit A	Midori128	rolled	unprotect
circuit B	Midori128	rolled	mask
circuit C	Midori128	unrolled	unprotect

4.1 実験要領

評価ボードに暗号を実装し，実装方式ごとの動作性能や電力解析に対する耐タンパ性を評価することで，IoT デバイスに最適な低エネルギーでセキュアな Midori128 の実装方式を検討する．

4.1.1 実験環境

図 6 に示すように実験環境には，PC，SASEBO-GII およびオシロスコープを用いる．SASEBO-GII 上には FPGA（Virtex5 XC5VLX30）が搭載されており，コンフィグレーションケーブルから Xilinx 社の ISE Design Suite 14.7 を用いて Midori128 を実装する．Midori128 の実装方式は 4.1.2 項で具体的に述べる．これらの回路は同時に書き込むことはせず，4.1.3 項で述べる評価項目を終えるたびに暗号回路を切り替える．また，いずれの実装方式においても，論理合成および配置配線の際には 1 つの論理ゲートにつき 1 つの Loop-Up Table（LUT）に展開するプリミティブ実装を行う．オシロスコープは Agilent 社の DSO-X 3052A を用い，プローブは N2863B である．

4.1.2 評価対象

実験では，**表 3** に示すいくつかの実装方式の Midori128 を評価する．まず，評価回路 A は，電力解析対策回路を組み込んでいない通常の暗号アルゴリズムの Midori128 をループアーキテクチャ実装で実装した暗号回路である．次に，評価回路 B は，電力解析の対策手法としてマスク対策を組み込んだ Midori128 である．マスク対策は**図 7** に示

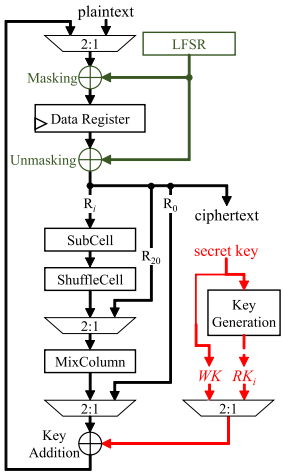


図 7 マスキング対策
Fig. 7 Masking countermeasure.

すように，線形帰還シフトレジスタ（LFSR）から得られる疑似乱数をマスク値とし，レジスタの前後でマスキングとアンマスキングを行う．疑似乱数は暗号化処理ごとに新たなマスク値を出力し，実装方式はループアーキテクチャ実装である．最後に，評価回路 C は，通常の暗号アルゴリズムの Midori128 をアンロールドアーキテクチャ実装で実装した暗号回路である．また，攻撃条件によって次の 5 つの組合せについて評価する．

(1) 評価回路 A に対する既知平文攻撃：KPA
(2) 評価回路 B に対する既知平文攻撃：KPA
(3) 評価回路 C に対する選択平文攻撃：CPA
(4) 評価回路 A に対する既知暗号文攻撃：KCA
(5) 評価回路 B に対する既知暗号文攻撃：KCA

4.1.3 評価項目

評価項目は，暗号回路の動作性能と耐タンパ性に大別される．

動作性能の評価項目とその概要は以下のとおりである．

(1) 消費電力量：暗号回路から推測されるピーク電力である．ISE Design Suite 内の XPower Analyzer [20] で得られる，回路の静的消費電力と動的消費電力の合計値を参照する．
(2) 最大動作周波数：暗号回路のクリティカルパスから推測される最大動作周波数である．ISE Design Suite で得られる値を参照する．
(3) 消費エネルギー量：1 ブロックの暗号化処理あたりに消費するエネルギー量である．演算サイクル数，消費電力量，最大動作周波数を用いて計算できる．
(4) 回路規模：FPGA に配置配線を行った後のスライス数と LUT 数である．ISE Design Suite で得られる値を参照する．

また，消費エネルギー量 E は式 (10) を用いて求められる [21]．

$$E = \frac{p \times c}{f} \tag{10}$$

ここで，p は 1 クロックあたりのピーク電力，c は演算サイクル数，f は動作周波数である．演算サイクル数は，ループアーキテクチャ実装の場合ラウンド数，アンロールドアーキテクチャ実装の場合ラウンド数にかかわらず 1 となる．暗号処理では，実装方式によって演算に要するサイクル数や，1 クロックで生じる消費電力（ピーク電力）が大きく異なる．具体的に，ループアーキテクチャ実装はサイクル数が多いがピーク電力が小さく，アンロールドアーキテクチャ実装はサイクル数が少ないがピーク電力が大きくなる．そこで，暗号回路に関する電力について実装方式に依存せずに比較評価するため，式 (10) ではピーク電力と暗号の演算時間として演算サイクル数をかけあわせ，暗号化処理 1 回あたりのエネルギー量を算出する．

耐タンパ性の評価項目とその概要は以下のとおりである．

(1) T 検定：測定した消費電力に対し Weltch の T 検定 [22] を行う．与えた入出力値から 2 つのデータセットに分類し，データセット間の消費電力に有意の差が生じているか評価する．有意の差が生じていた場合，入出力値と消費電力量との間に相関関係が生じており，電力解析攻撃に脆弱であることを示す [22]．
(2) 電力解析攻撃：暗号に使用した入出力値と消費電力量を用いて電力解析攻撃を行い，秘密鍵の解析数について評価する．

暗号回路に入力する平文について，既知平文攻撃と既知暗号文攻撃の場合はランダムな平文を重複なしで 40 万データを用意し，同一の数の消費電力波形を取得する．選択平文攻撃の場合は 3.2 節で述べた形式で平文を生成する．

T 検定では，提案手法を用いた秘密鍵の解析過程で得られたハミング距離に応じて，1 以下のグループを G_1，3 以上のグループを G_2 として，データセットを 2 つの母集団に分類する．次に，仮説は 2 つの母集団の母平均に差はないとし，両側検定の有意水準 5%で評価する．電力解析攻撃における消費電力波形のどのサンプル点を解析に用いるかを示す Point of Interest（POI）は，既知平文攻撃または選択平文攻撃の場合は Midori128 の R_1 が演算されている点を，既知暗号文攻撃の場合は Midori128 の R_{20} が演算されている点を選択する必要がある．そこで，T 検定結果においてピークが生じている範囲を対象のラウンド関数が演算されている時間と仮定し，その範囲を POI として手動で設定する．また，3 章で述べたように秘密鍵 WK の 4 bits の部分鍵について最大 32 個を解析する．

4.2 実験結果

まず，動作性能の評価結果について**表 4** に示す．表 4 より，消費電力量は評価回路 A であるループアーキテクチャ実装が最も少ないという結果が得られた一方で，暗号処理

表 4 動作性能の結果
Table 4 Results of implementation performance.

	circuit A	circuit B	circuit C
cycles	20	20	1
power [mW]	292	303	373
maximum frecency [MHz]	116.455	113.546	18.000
energy per encryption [nJ]	50.2	53.4	20.7
slices	940	999	4,030
LUTs	1,265	1,435	8,385

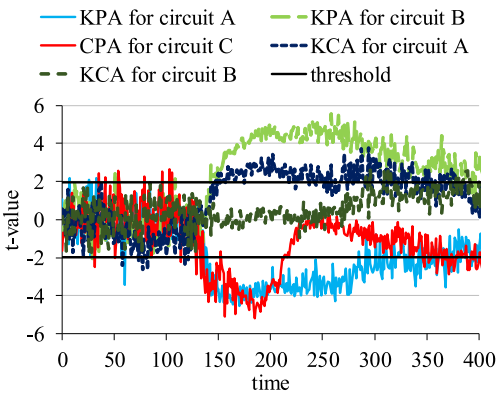


図 8 消費電力波形に対する T 検定の結果
Fig. 8 Resuls of t-test for power consumption waveforms.

1 回あたりの消費エネルギー量の比較では，評価回路 C であるアンロールドアーキテクチャ実装が最も少ないという結果が得られた．また，動作周波数・スライス数・LUT 数について，評価回路 A と評価回路 C の差はそれぞれ約 6.5 倍，約 4.3 倍，約 6.6 倍であった．また，対策手法を適用した評価回路 B は，評価回路 A と比較して消費電力量・消費エネルギー量・回路規模のいずれも増加することが確認された．

次に，T 検定の結果について**図 8** に示す．縦軸は消費電力から計算された T 値，横軸は時間であり，4.1.3 項で示した 5 つの評価項目の T 値と仮説の棄却に関する閾値のグラフを示している．仮説が棄却されるか否かの閾値に関して，標本から近似された自由度は時間によって多少のばらつきが生じるが約 2,480 となり，有意水準 5%の両側検定という条件から，約 2.24 と算出されている．T 検定の評価項目では，5 つすべての評価項目において T 値が閾値を上回るという結果が得られた．

最後に，提案手法を適用した電力解析攻撃の結果について，40 万波形を使用した際の推測鍵の順位を**表 5** に示す．表 5 には，State ごとに順位が示されており，これは全通りの推測鍵の相関係数値に対して順位付けした後，正解鍵の順位を示したものである．つまり，表 5 において 1 はその State において解析に成功したことを示す．評価回路 A に対する既知平文攻撃と既知暗号文攻撃では，それぞれ 32 個の部分鍵のうち 29 個，26 個の解析に成功した．また，順位が 1 位でなかった部分鍵においても上位 25%の順位に含まれており，相関係数値が比較的高いことが分かった．評価回路 B に対する既知平文攻撃と既知暗号文攻撃では，暗号化処理ごとにマスク値が切り替わるため原理的に解析に成功しないが，偶然 2 個の解析に成功したことが確認された．評価回路 C に対する選択平文攻撃では，評価回路 B よりも多い 8 個の解析に成功したが，秘密鍵全体としては半分未満の解析数となった．

表 5 各ステートにおける推測鍵順位
Table 5 Ranking of guess keys in each state.

state	KPA for A	KPA for B	CPA for C	KCA for A	KCA for B
0	1	9	2	1	13
1	1	8	1	1	3
2	1	12	14	1	10
3	1	5	9	1	10
4	1	3	5	1	4
5	1	14	1	1	3
6	1	4	1	1	3
7	1	10	12	1	13
8	1	14	1	8	4
9	1	15	16	1	11
10	1	15	11	1	9
11	2	3	5	1	15
12	1	5	14	2	10
13	2	15	15	1	2
14	1	13	4	1	5
15	1	3	4	1	1
16	1	12	9	1	1
17	1	1	2	1	8
18	1	11	1	8	11
19	1	5	13	1	12
20	1	12	12	1	4
21	1	14	4	1	5
22	1	16	6	3	9
23	1	1	16	1	4
24	1	14	13	1	10
25	1	5	1	1	16
26	1	4	9	1	16
27	3	10	1	1	2
28	1	12	1	4	3
29	1	11	5	1	11
30	1	3	7	3	6
31	1	11	11	1	11

4.3 考察

まず，動作性能の結果では，消費エネルギー量が最も少ない実装方式がアンロールドアーキテクチャ実装であることが分かった．ピーク電力はループアーキテクチャ実装と比較して大きいものの，ループアーキテクチャ実装は暗号文を出力するまでに多くのクロックを要するため，エネルギーの観点ではアンロールドアーキテクチャ実装が優れて

表 6 HW モデル電力解析による評価回路 C の推測鍵順位
Table 6 Guess keys rank of evaluation circuit C by HW model power analysis.

state	CPA-HW for C	state	CPA-HW for C	state	CPA-HW for C
0	11	11	9	22	1
1	5	12	14	23	4
2	9	13	7	24	14
3	2	14	16	25	15
4	7	15	4	26	15
5	16	16	7	27	1
6	16	17	6	28	6
7	15	18	10	29	10
8	13	19	16	30	5
9	15	20	15	31	11
10	8	21	15		

いると考えられる．また，同様に最大動作周波数はループアーキテクチャ実装と比較して低いが，Midori128 のループアーキテクチャ実装が 20 クロック必要ということを考慮すると，レイテンシはアンロールドアーキテクチャ実装が小さく，低遅延であるといえる．これらの結果から，Midori128 のアンロールドアーキテクチャ実装はエネルギーとレイテンシを指向した実装方式として有効である．

次に，耐タンパ性の結果について述べる．T 検定の結果では，すべての評価回路から脆弱性が検出された一方で，電力解析の結果では解析数に差が生じた．暗号への電力解析攻撃に対する安全性の指標として Global Success Rate（GSR）[23] があり，部分鍵の解析成功率が 8 割を超える回路は脆弱と判断する．評価回路 A は 128 bits の秘密鍵のうち，いずれの攻撃条件においても解析数は 8 割を超えており，最も脆弱な回路であるといえる．他の評価回路では解析数が 8 割を下回っていることから，マスク対策をしたループアーキテクチャ実装だけでなく，未対策のアンロールドアーキテクチャ実装も耐タンパ性が高いといえる．

3.2 節で述べたアンロールドアーキテクチャ実装に対する提案解析手法について，有効性を示すために詳細な耐タンパ性評価を行う．提案手法と比較するために，提案した選択平文を用い，ハミングウェイト（HW）モデルでの解析を行う．使用する平文には同一の平文値が複数含まれており，解析を行う過程で平滑化処理が行われる．提案手法では，2 回の暗号処理間の差分を解析に用いたが，この実験では SubCell 演算直後の暗号中間値の HW に着目する．解析結果を**表 6** に示す．完全に部分鍵が解析された数は 2 個であり，提案手法の 8 個よりも解析数が低下している．この結果より，提案手法で用いた 2 回の処理間の差分が解析数の向上に寄与したといえる．

評価回路 C が未対策回路であっても耐タンパ性を有していた要因として，低遅延実装であることが考えられる．実装した暗号回路はレイテンシを小さくするために，非線形処理等の組合せ回路について並列に実装されており，解析時に注目する消費電力には注目対象の State 以外のノイズが比較的多く含まれ，解析数の低下が生じたと考える．

以上のことより，Midori128 を指向した IoT デバイスに最適な低エネルギーでセキュアな実装方式として，最も消費エネルギー量が少なくすべての解析が困難な，アンロールドアーキテクチャ実装が最も適しているといえる．

5. まとめ

本研究では，Midori128 の 2 つの実装方式に対する電力解析攻撃手法を提案した．また，実証実験では FPGA 上にいくつかの実装方式を採用した暗号回路を実装し，実装性能ならびに耐タンパ性を評価した．実験結果から，Midori128 のアンロールドアーキテクチャ実装はエネルギーおよび耐タンパ性の観点から最適な実装方式であることを明らかにした．

謝辞 本研究の一部は，JSPS 科研費 JP19K11976 の助成を受けたものである．

参考文献

[1] Ministry of Internal Affairs and Communications, Japan: Information and Communications in Japan, available from ⟨https://www.soumu.go.jp/johotsusintokei/whitepaper/eng/WP2020/2020-index.html⟩ (accessed 2021-04-20).
[2] Mittal, M., Tanwar, S., Agarwal, B. and Goyal, L.M. (Eds.): Energy Conservation for IoT Devices, *SSDC*, Vol.206, pp.1–356, Springer (2019).
[3] Kaur, N. and Sood, S.K.: An Energy-Efficient Architecture for the Internet of Things (IoT), *IEEE Systems Journal*, Vol.11, No.2, pp.796–805, IEEE (2017).
[4] Arshad, R., Zahoor, S., Shah, M.A., Wahid, A. and Yu, H.: Green IoT: An Investigation on Energy Saving Practices for 2020 and Beyond, *IEEE Access*, Vol.5, pp.15667–15681, IEEE (2017).
[5] Gomez, C., Oller, J. and Paradells, J.: Overview and Evaluation of Bluetooth Low Energy: An Emerging Low-Power Wireless Technology, *Sensors*, Vol.12, No.9, pp.11734–11753, MDPI (2012).
[6] Darroudi, S.M. and Gomez, C.: Bluetooth Low Energy Mesh Networks: A Survey, *Sensors*, Vol.17, No.7, pp.1–19, MDPI (2017).
[7] NICTER 観測レポート 2020：国立研究開発法人情報通信研究機構，入手先 ⟨https://www.nict.go.jp/cyber/report/NICTER_report_2020.pdf⟩（参照 2021-04-20）．
[8] Banik, S., Bogdanov, A., Isobe, T., Shibutani, K., Hiwatari, H., Akishita, T. and Regazzoni, F.: Midori: A Block Cipher for Low Energy, LNCS, Vol.9453, pp.441–436, Springer (2015).
[9] CRYPTREC Cryptographic Technology Guideline (Lightwight Cryptography): CRYPTREC, available from ⟨https://www.cryptrec.go.jp/report/cryptrec-gl-2003-2016en.pdf⟩ (accessed 2021-04-20).
[10] Chawla, N., Singh, A., Rahman, N.M., Kar, M. and Mukhopadhyay, S.: Extracting Side-Channel Leakage from Round Unrolled Implementations of Lightweight Ciphers, *Proc. 2019 IEEE Int. Symp. on Hardware Oriented Security and Trust* (*HOST*), pp.31–40, IEEE

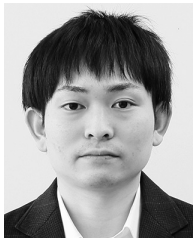
(2019).
[11] 野崎佑典，吉川雅弥：低消費電力軽量暗号 Midori に対する階層的電力解析とその評価，電気学会論文誌 C，Vol.138, No.12, pp.1455–1463，電気学会 (2018).
[12] Moradi, A. and Schneider, T.: Side-Channel Analysis Protection and Low-Latency in Action – case study of PRINCE and Midori, LNCS, Vol.10031, pp.517–547, Springer (2016).
[13] Todo, Y., Leander, G. and Sasaki, Y.: Nonlinear Invariant Attack: Practical Attack on Full SCREAM, iSCREAM, and Midori64, *Journal of Cryptology*, Vol.32, pp.1383–1422, Springer (2019).
[14] Guo, J., Jean, J., Nikolic, I., Qiao, K., Sasaki, Y. and Sim, S.M.: Invariant Subspace Attack Against Midori64 and The Resistance Criteria for S-box Designs, *IACR Transactions on Symmetric Cryptology*, pp.33–56, IACR (2016).
[15] Brier, E., Clavier, C. and Olivier, F.: Correlation Power Analysis with a Leakage Model, LNCS, Vol.3156, pp.16–29, Springer (2004).
[16] Borghoff, J., Canteaut, A., Güneysu, T., Kavun, E.B., Knezevic, M., Knudsen, L.R., Leander, G., Nikov, V., Paar, C., Rechberger, C., Rombouts, P., Thomsen, S.S. and Yalçın, T.: PRINCE – A Low-Latency Block Cipher for Pervasive Computing Applications, LNCS, Vol.7658, pp.208–225, Spriger (2012).
[17] ヴィッレウリマウル，本間尚文，青木孝文：アンロールド軽量暗号ハードウェアに対する選択平文型高効率サイドチャネル解析，2017 年暗号と情報セキュリティシンポジウム予稿集，Vol.3C1-5, pp.1–6 (2017).
[18] Yli-Mäyry, V.，上野　嶺，本間尚文，青木孝文，三浦典之，松田航平，永田　真，Bhasin, S., Mathieu, Y., Graba, T., Danger, J.L.：低遅延暗号における中間ラウンドからのサイドチャネル漏洩とその RSM に基づく効率的な対策，2019 年暗号と情報セキュリティシンポジウム予稿集，Vol.3D3-1, pp.1–6 (2019).
[19] Peeters, E., Standaert, F.X., Donckers, N. and Quisquater, J.J.: Improved Higher-Order Side-Channel Attacks with FPGA Experiments, LNCS, Vol.3659, pp.309–323, Springer (2005).
[20] Xilinx: Xilinx Power Estimator User Guide, available from ⟨https://www.xilinx.com/support/documentation/sw_manuals/xilinx2018_1/ug440-xilinx-power-estimator.pdf⟩ (accessed 2021-10-01).
[21] Zhang, X., Heys, H.M. and Li, C.: FPGA Implementation and Energy Cost Analysis of Two Light-Weight Involutional Block Ciphers Targeted to Wireless Sensor Networks, *Mobile Network and Applications*, Vol.18, pp.222–234, Springer (2013).
[22] Becker, G., Cooper, J., DeMulder, E., Goodwill, G., Jaffe, J., Kenworthy, G., Kouzminov, T., Leiserson, A., Marson, M., Rohatgi, P. and Saab, S.: Test Vector Leakage Assessment (TVLA) methodology in practice, *International Cryptographic Module Conference* (2013).
[23] Clavier, C., Danger, J.L., Duc, G., Elaabid, M.A., Gérard, B., Guilley, S., Heuser, A., Kasper, M., Li, Y., Lomné, V., Nakatsu, D., Ohta, K., Sakiyama, K., Sauvage, L., Schindler, W., Stöttinger, M., Nicolas V.C., Walle, M. and Wurcker, A.: Practical improvements of side-channel attacks on AES: feedback from the 2nd DPA contest, *Journal of Cryptographic Engineering*, Vol.4, pp.259–274, Springer (2014).

竹本 修 （学生会員）

2021 年 3 月名城大学大学院理工学研究科情報工学専攻修士課程修了．同年 4 月同大学院理工学研究科電気・情報・材料・物質専攻博士後期課程入学，現在に至る．暗号 LSI のセキュリティに関する研究に従事．第 17 回情報学ワークショップ最優秀賞，2021IEEE 名古屋支部学生奨励賞等受賞．IEEE 各会員．

池崎 良哉

2018 年 3 月名城大学大学院理工学研究科情報工学専攻修士課程修了．2020 年 4 月同大学院理工学研究科電気・情報・材料・物質工専攻博士後期課程入学，現在に至る．暗号 LSI のセキュリティに関する研究に従事．第 42 回東海ファジィ研究会優秀発表賞等受賞．電子情報通信学会，IEEE 各会員．



野崎 佑典 （正会員）

2019 年 3 月名城大学大学院理工学研究科電気電子・情報・材料工学専攻博士後期課程修了．博士（工学）．2019 年 4 月より同大学理工学部特任助手，2020 年 4 月より同大学理工学部情報工学科助教．2017 年 4 月～2019 年 3 月まで日本学術振興会特別研究員（DC2）．暗号 LSI のセキュリティに関する研究に従事．IEEE CEDA AJJC Academic Research Award 2018 等受賞．電子情報通信学会，日本知能情報ファジィ学会，IEEE 各会員．

吉川 雅弥 （正会員）

2001 年 3 月立命館大学大学院理工学研究科博士課程修了．博士（工学）．同大学理工学部第 1 号助手・講師を経て，2007 年 4 月より名城大学理工学部准教授，2012 年 4 月より教授．2009 年から 2015 年 CREST 研究員．LSI 設計・設計自動化技術の研究に従事．第 3 回 LSI IP デザインアワード開発奨励賞，第 10 回 LSI IP デザインアワード研究助成賞，FIT2003 ベストペーパー賞，2007 年度システム制御情報学会産業技術賞，CAINE2010 Best Paper Award，WCECS2011 Best Paper Award 等受賞．電気学会，電子情報通信学会，システム制御情報学会，日本知能情報ファジィ学会，IEEE 各会員．