Vol.2018-CDS-22 No.4
2018/5/31

環境発電デバイスの耐タンパ実装の検討

野崎佑典[†1]　吉川雅弥[†1]

概要：近年，環境発電が IoT を支える技術として注目されている．環境発電は，身の回りのエネルギーを電気エネルギーへと変換する技術であり，コンシューマへの応用が期待されている．また，環境発電デバイスは IoT により様々な機器と接続されるため，暗号化などのセキュリティ対策を行うことが重要である．一方で，ハードウェアセキュリティでは，暗号回路を対象に回路動作時に漏洩する物理情報を利用したサイドチャネル攻撃の危険性が指摘されている．そのため，今後の IoT を支える環境発電デバイスに関しても耐タンパ性についての検証は非常に重要である．そして，これまでに我々は環境発電デバイスにおける耐タンパ検証環境を構築し，環境発電デバイスの耐タンパ性について検証してきた．本研究では，環境発電デバイスの耐タンパ実装について検討する．提案手法では低消費電力での実装が期待されるシャッフリングを用いた対策を行う．そして，TWELITE 環境発電デバイスを用いた評価実験により，提案手法の有効性について検証する．

キーワード：環境発電，サイドチャネル攻撃，ハードウェアセキュリティ，軽量暗号，耐タンパ性

A Study of Tamper Resistant Implementation for Energy Harvester

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

Abstract: Recently, energy harvesting techniques have attracted attention for internet of things (IoT). Energy harvesting converts various energy to electric power and it has been expected to be applied to consumer electronics. Also, since energy harvesters are connected to various devices due to IoT, security countermeasure such as encryption technique is important. On the other hand, in the field of hardware security, the risk of side-channel attacks, which reveal the secret information by utilizing physical information leaked from the circuit operation, is pointed out. Therefore, for energy harvesters supporting IoT, the tamper resistance verification is very important. Then, we have developed the tamper resistance verification system for energy harvesters, and verified the tamper resistance. This study proposes a tamper resistant implementation for energy harvesters. The proposed method performs the countermeasure using shuffling, which is expected the implementation with low power, against side-channel attacks. Experiments using a TWELITE energy harvester verify the validity of the proposed method.

Keywords: Energy harvesting, Side-channel attack, Hardware security, Lightweight cipher, Tamper resistance

1. はじめに

Internet of Things (IoT) を支える技術として，環境発電が注目されている [1]–[5]．環境発電は身の周りに存在する様々なエネルギーを収集し，電気エネルギーへと変換する技術である．環境発電を導入することで，電池の交換や電源の配線などが不要となるため，コンシューマエレクトロニクスを含めた様々な分野への応用が期待されている．一方で，環境発電デバイスは IoT により様々な機器と接続されるため，暗号化を含めたセキュリティ対策を施すことは非常に重要である．

一方で，ハードウェアセキュリティにおいて，暗号回路に対するサイドチャネル攻撃 [6]–[13]の危険性が指摘されている．サイドチャネル攻撃は，暗号回路動作時に漏洩する消費電力や電磁波などの物理情報（サイドチャネル情報）を使用することで，内部の秘密鍵を推定する攻撃手法である．そのため，今後の IoT を支える環境発電デバイスにおいても，サイドチャネル攻撃に対する耐性（耐タンパ性）を評価することは非常に重要である．そして，我々はこれまでに環境発電デバイスの耐タンパ性検証環境を構築し，環境発電デバイスがサイドチャネル攻撃に対して脆弱であることを明らかにしてきた [14]．そのため，環境発電デバイスのサイドチャネル攻撃に対する対策手法についての研究は非常に重要である．

そこで本研究では，環境発電デバイスにおける耐タンパ実装についての検討を行う．本研究では，実行サイクル数の増加が少ない，すなわち消費電力が小さい対策手法であるシャッフリングを環境発電デバイスに適用する．そして，TWELITE 環境発電デバイスを使用した評価実験により，提案手法の有効性について検証する．

†1 名城大学
Meijo University

2. 準備

2.1 環境発電デバイス

環境発電は，太陽光や電波，振動，熱などの身の回りの自然エネルギーを収集し，電気エネルギーへと変換する技術である[3]．主に，太陽光を利用した太陽光発電や振動を利用した振動発電などがある．本研究では，太陽光発電を利用する TWELITE 環境発電デバイス [15]を使用する．TWELITE 環境発電デバイスはモノワイヤレス株式会社[15]から販売されている環境発電デバイスである．TWELITE 環境発電デバイスの外観を図 1 に示す．

図 1 に示すように，TWELITE 環境発電デバイスは，太陽光発電用のソーラーパネル（Panasonic AM-5815），電源管理ユニット（TWE-EH SOLAR），TWELITE 無線マイコンモジュール（TWELITE-DIP）で構成する．TWELITE-DIP は 32bit の RISC マイコンを内蔵している．また，TWELITE-DIP に搭載されたアンテナにより，データを無線送信する．動作に関して，ソーラーパネルで発電したエネルギーでデバイスを動作させる．具体的には，以下の処理を行う．

① ソーラーパネルでは入射された光から発電を行い，発電した電力を TWE-EH SOLAR 内部のコンデンサ（220μF）へと充電する．
② 内蔵コンデンサの電圧が一定の値（約 2.9V）に達したとき，TWELITE マイコンの電源をオンにし，繰り返しデータの無線送信を行う．
③ TWELITE マイコンはデータの無線送信のたびに一旦スリープ状態となり，任意のスリープ時間経過後，再び無線送信を開始する．
④ 内蔵コンデンサの値が一定の値（約 2.0V）に下がると，電源をオフにする．
⑤ ①から④の操作を繰り返し行う．

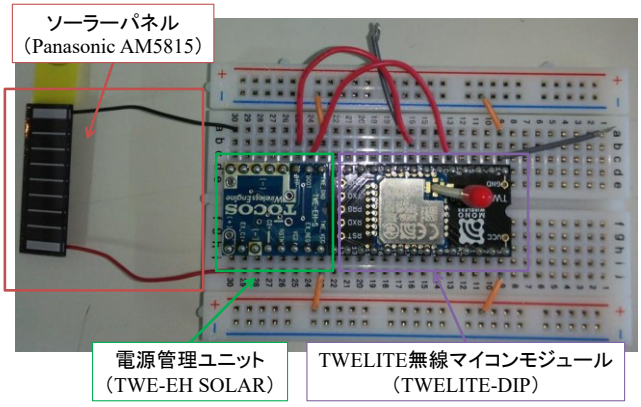

図 1 本研究で使用する TWELITE 環境発電デバイス
Figure 1 TWELITE energy harvester.

2.2 軽量暗号 TWINE [16]

本研究では，環境発電デバイスに実装する暗号として軽量暗号 TWINE [16]を利用する．TWINE は NEC によって，開発された代表的な軽量暗号の 1 つであり，ソフトウェア実装において回路規模・処理速度に関して良好な性能を持つ [16]．TWINE の概要を図 2 に示す．TWINE は 16 分割一般化 Feistel 構造をブロック暗号であり，ブロック長は 64bit，鍵長は 80bit と 128bit の 2 種類から選択することができる．本研究では，80bit の秘密鍵を利用する．そして，暗号処理では 64bit の平文に対して，合計で 36 回のラウンド処理を行うことで，64bit の暗号文を生成する．

ラウンド処理の詳細について図 3 を用いて説明する．図 3 に示すように，ラウンド処理は 8 つの関数 F（関数 F0 から関数 F7）と拡散層（転置処理）で構成する．具体的に，各関数 F は S-BOX による非線形な置換処理と，ラウンド鍵 RK や暗号中間値 x との排他的論理和演算で構成する．また，演算はそれぞれ 4bit 単位で行う．具体的には r ラウンド目のラウンド処理は式(1)で表される．

$$\begin{cases} x_{h(2j)}^{r+1} = x_{2j}^{r} \\ x_{h(2j+1)}^{r+1} = S\left(x_{2j}^{r} \oplus RK_{j}^{r}\right) \oplus x_{2j+1}^{r} \end{cases} \tag{1}$$

ただし，$S(\ )$は S-BOX の置換処理，$h(\ )$は拡散層による転置処理，$\oplus$ は排他的論理和演算，$j = 0, 1, \ldots, 7$ である．

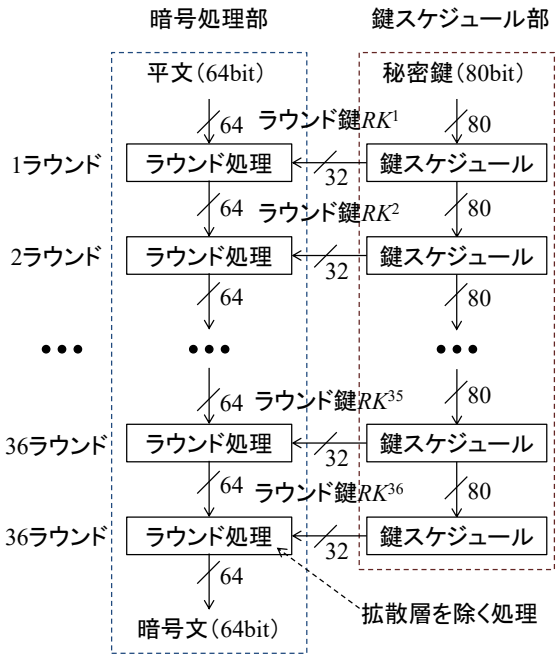

図 2 TWINE の概要
Figure 2 Outline of TWINE.

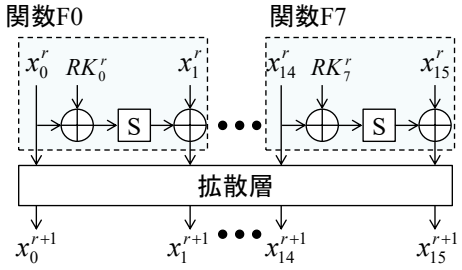

図 3　TWINE のラウンド処理
Figure 3　Round processing of TWINE.

TWINE では 1 ラウンド目から 35 ラウンド目まで，式(1)に示す処理を繰り返し行う．そして，最終ラウンドである 36 ラウンド目では，拡散層を除いた処理を行う．したがって，暗号文 c は式(2)で計算される．

$$\begin{cases} c_{2j} = x_{2j}^{36} \\ c_{2j+1} = S\left(x_{2j}^{36} \oplus RK_j^{36}\right) \oplus x_{2j+1}^{36} \end{cases} \tag{2}$$

2.3 環境発電デバイスの耐タンパ性検証環境 [14]

本研究で使用する耐タンパ検証環境 [14]について説明する．耐タンパ検証環境は，主に TWELITE 環境発電デバイスとオシロスコープなどの測定系，制御用 PC で構成する．TWELITE 環境発電デバイスには，軽量暗号 TWINE などの暗号アルゴリズムをソフトウェア実装する．そして，暗号処理時における漏洩電磁波を電磁波測定用アンテナやオシロスコープなどの測定系で取得し，PC に保存する．このとき，測定のためのトリガ信号は，暗号処理に合わせて TWELITE 環境発電デバイスから外部へと出力させる．また，暗号結果は無線通信により，PC に接続された親機（受信機）へと送信される．このとき，耐タンパ検証環境では，暗号処理と波形取得の同期をとるために，環境発電デバイスのソフトウェア処理にカウンタ処理を導入する．そして，このカウンタ値を照合することで，取得波形と暗号文が同期されているかを確認する．そして，取得した波形データと暗号文の組を耐タンパ検証に利用する．

次に，耐タンパ検証手法について説明する．一般的に電磁波解析などのサイドチャネル攻撃 [12][13]は，暗号中間値のハミング重み（Hamming Weight：HW）や，暗号中間値間のハミング距離により，漏洩する物理情報が異なることを利用する．TWINE に対する耐タンパ検証では，HW 型相関電磁波解析（Correlation Electromagnetic Analysis：CEMA）[13]により行う [14]．耐タンパ検証手法の概要を図 4 に示す．図 4 に示すように，TWINE の最終ラウンド（36 ラウンド目）における S-BOX の出力値のハミング重み H を利用する．また，対象とするハミング重み H は式(3)で計算できる．

$$H = HW\left(S\left(c_{2j} \oplus RK_j^{36}\right)\right) \tag{3}$$

ただし，$HW(\ )$はハミング重みを求める関数である．このとき，暗号文 c は既知であるが，ラウンド鍵 RK_j^{36} は未知の値である．そのため，耐タンパ検証ではラウンド鍵には予測値を利用する．このとき，式(3)のラウンド鍵 RK_j^{36} は 4bit であるため，この予測値には 0 から 15 までの 16 通りの値を全て試す．そして，求めたハミング重み H と電磁波 W のピアソンの相関係数 ρ を式(4)により計算する．

$$\rho_t = \frac{\sum_{i=1}^{N}\left(W_{i,t} - \overline{W_t}\right)\left(H_i - \overline{H}\right)}{\sum_{i=1}^{N}\left(W_{i,t} - \overline{W_t}\right)^2 \sum_{i=1}^{N}\left(H_i - \overline{H}\right)^2} \tag{4}$$

ただし，$\overline{W_t}$ は電磁波 W の平均，$\overline{W_t}$ はハミング重み H の平均，N は解析に使用する波形の数，t は波形データの時間軸上のサンプル点である．そして，相関係数を最大とするラウンド鍵の予測値を正解鍵として推定する．

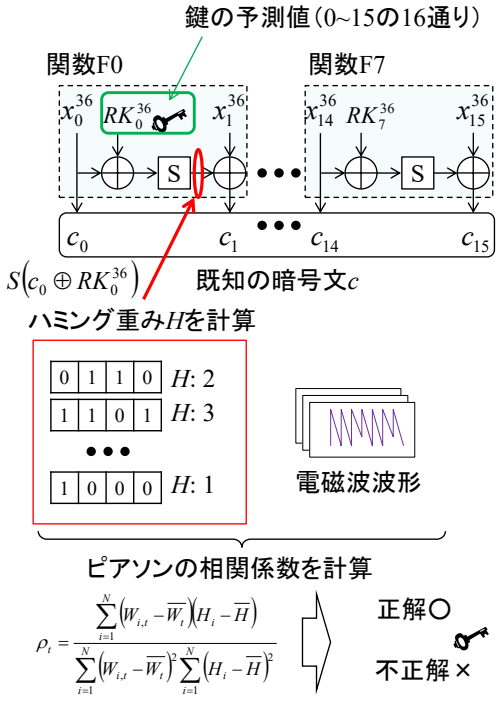

図 4　耐タンパ検証手法
Figure 4　Tamper resistance verification method.

3. 提案手法

本研究では，環境発電デバイスの耐タンパ実装について検討する．環境発電デバイスは，環境発電によって得られる微小な電力により動作する．そのため，耐タンパ実装では低消費電力で実現可能な対策が求められる．ここで，一般的にソフトウェア実装における消費電力はマイコンの命令の実行サイクル，すなわち処理時間に依存する [17].

サイドチャネル攻撃に対する対策手法に関して，代表的なものとしてマスキングとハイディングが知られている [8]–[11]．マスキングは乱数による排他的論理和演算（マスク処理）を施すことで，秘密情報との相関を隠ぺいする対策手法である [8]．具体的には，各演算の前後にマスキングとアンマスキング（マスクを外す処理）を適用する．このとき，S-BOX などの非線形な演算では，マスクされた値の非線形処理後にアンマスキングを適用した場合，正規の S-BOX 計算結果とは異なる値になる．そのため，マスキングでは処理の整合性を満たすために，予め，マスクされた計算結果に合わせた S-BOX を複数用意する．そのため，事前に多くの計算を行う必要があるため，回路規模や処理時間が増加する [8]–[10].

ハイディング対策には，ダミー演算対策やシャッフリングなどがある [8]．ダミー演算対策では，正規の演算とは異なるダミー演算をランダムに挿入することで，消費電力を時間軸方向でランダム化する [8]．また，挿入するダミー演算の数を増やすほど，耐タンパ性を向上させることができる．しかし，ダミー演算対策では新たに演算を挿入するため，挿入するダミー演算の数だけ処理時間が増加する [8]．次にシャッフリングでは，各演算を実行する順番をランダムに入れ替えることで，時間軸方向で消費電力をランダム化させる [8][11]．シャッフリングでは，演算を入れ替えるだけであるため，新たなに追加する処理は少なく，処理時間の増加を抑えることができる．

本研究では，最も少ない命令実行サイクルで実現可能だと考えられる，シャッフリングにより対策手法について検討する．提案手法では，TWINE の各 S-BOX 処理部に対応する関数 F（関数 F0 から F7）に対して，シャッフリングを適用する．提案手法の概要を図 5 に示す．図 5 の①は無対策（通常の命令の実行順番）の場合の例を，図 5 の②はシャッフリングを適用した場合をそれぞれ示している．図 5 の②に示すように，シャッフリングを行うことで，各関数 F の実行順番をランダムに変化させることができる．

また，各ラウンド処理のシャッフリングに使用する乱数には，3bit の乱数値をシード値とした線形帰還シフトレジスタ（Linear Feedback Shift Register：LFSR）を使用する．この LFSR には，周期が 7 となる帰還多項式 $x^3 + x^2 + 1$ を使用し，LFSR の出力値に対応した関数 F を実行することで，ランダム化を実現させる．

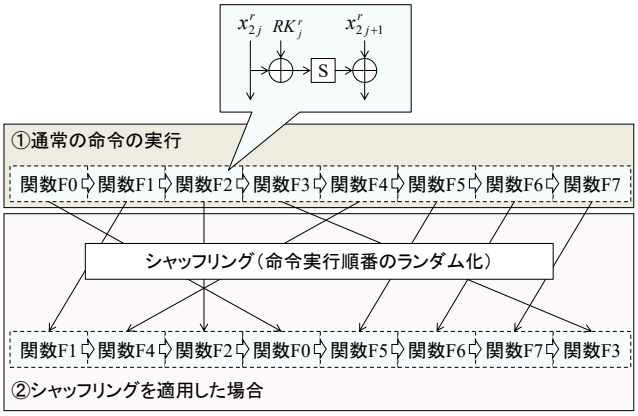

図 5　提案手法の概要

Figure 5　Outline of the proposed method.

4. 評価実験

4.1 実験環境

実験で使用した耐タンパ検証環境の外観を図 6 に示す．また，実験環境の詳細を表 1 に示す．実験では，TWELITE 環境発電デバイスに提案手法を適用した TWINE と無対策の TWINE をそれぞれソフトウェア実装した．そして，暗号処理時の電磁波を電磁波測定用アンテナとオシロスコープを用いて取得した．また，TWELITE から無線送信される暗号文の取得に関して，親機には MONOSTICK [15]を使用し，Tera Term を用いて取得した．さらに，実験では安定して発電を行うために，LED ライトを使用して常に光をソーラーパネルへ照射し続けた．

また，取得した電磁波波形の例を図 7 と図 8 に示す．図 7 は無対策における TWINE の 36 ラウンド目の関数 F0 から F7 の処理における電磁波波形である．また，図 8 はシャッフリング後の関数 F の電磁波波形である．耐タンパ検証では，これらの波形データを対象として実験を行った．

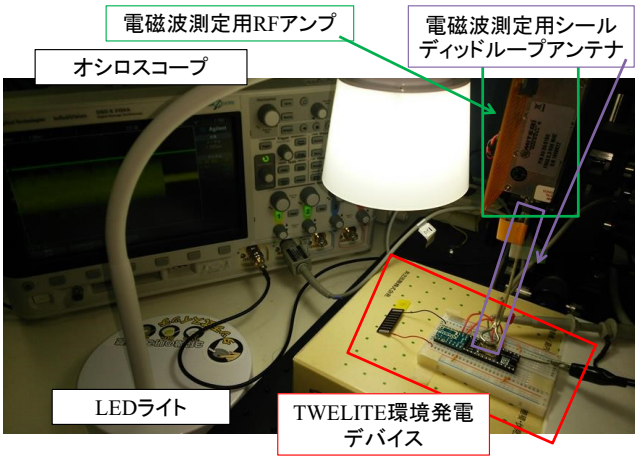

図 6　実験環境

Figure 6　Experimental environment.

表 1　実験環境の詳細
Table 1　Detail of experimental condition.

TWELITE 環境発電デバイス	Panasonic AM-5815 TWE-EH SOLAR TWELITE-DIP
親機（受信機）	MONOSTICK
LED ライト	DS-LS06-W
暗号アルゴリズム	TWINE
平文	ランダムに生成
オシロスコープ	Agilent DSO-X 3104A
サンプリングレート	5 [Gsa/sec]
電磁波測定用アンテナ	シールディッドループアンテナ
電磁波測定用 RF アンプ	MITEQ AU-3A-0150

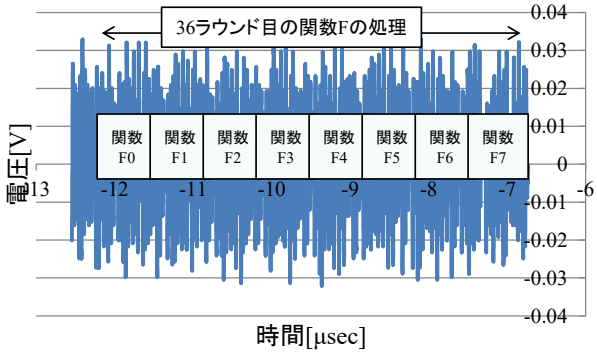

図 7　TWINE の 36 ラウンド目の電磁波波形（無対策）
Figure 7　Electromagnetic waveform in 36th round without countermeasure.

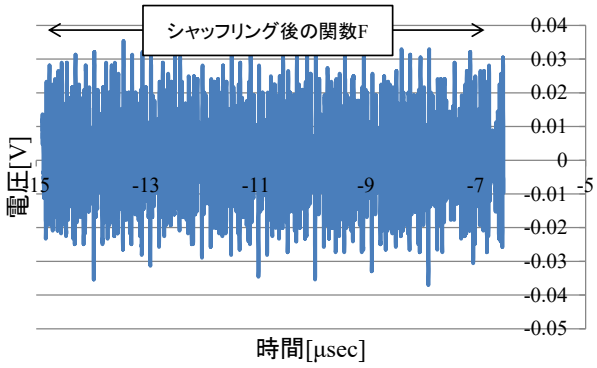

図 8　TWINE の 36 ラウンド目の電磁波波形（提案手法）
Figure 8　Electromagnetic waveform in 36th round with the proposed method.

4.2 実験結果

まず, 無対策の TWINE の耐タンパ性について検証した．実験結果を図 9 に示す．この実験では，合計で 500 個の波形データを用いて解析を行った．図の横軸は解析に使用した電磁波波形の数を，縦軸は解析に成功した鍵の数を示している．今回対象とするラウンド鍵 RK^{36} は，合計で 8 個あるため，縦軸の最大値は 8 である．実験結果より，無対策では 300 個の波形データを使用することで，8 個中 7 個の鍵の解析に成功した．したがって，環境発電デバイス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，提案手法を適用した場合の耐タンパ性について検証した．実験結果を図 10 に示す．この検証では、合計で 1,500 個の波形データを使用した．実験結果より，1,500 個の波形データを使用した場合でも, 正解鍵数は 0 個であり, 提案手法を適用することで, 時間軸方向でランダム化され, 耐タンパ性が向上していることが確認できる．

また，無対策と提案手法における正解鍵での相関係数を図 11 と図 12 に示す. 図 11 に示すように無対策では相関係数のピークが表れていることが確認できる．一方で，提案手法ではシャッフリングによる時間軸方向でのランダム化により，1,500 波形を用いた解析では，あまりピークが表れていないことが確認できる．

最後に，実行時間について比較した．比較結果を表 2 に示す. 表 2 に示すように, 提案手法では無対策と比較して, 実行時間を大きくなっていることが確認できる．これは，シャッフリングのための乱数生成を行っていることが原因だと考えられる．また，無対策と比較して，実行時間の増大は約 1.25 倍程度であることが確認できる．

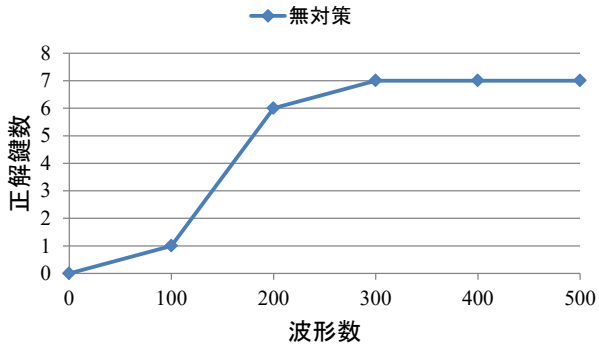

図 9　実験結果（無対策）
Figure 9　Experimental result for without the countermeasure.

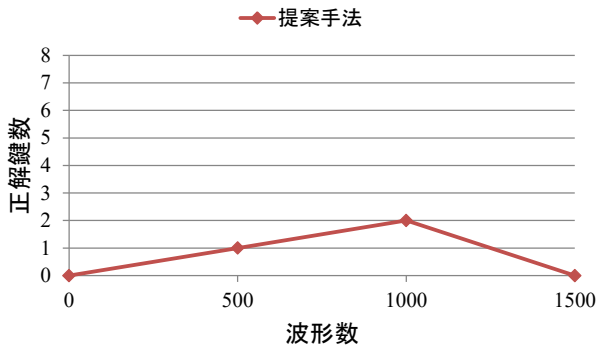

図 10　実験結果（提案手法）
Figure 10　Experimental result for the proposed method.

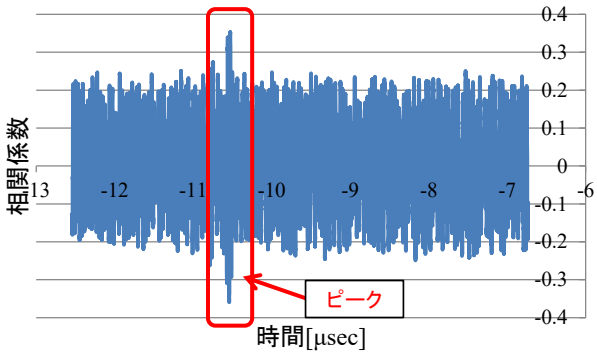

図 11　正解鍵における相関係数（無対策）

Figure 11　Correlation coefficient in the correct key without countermeasure.

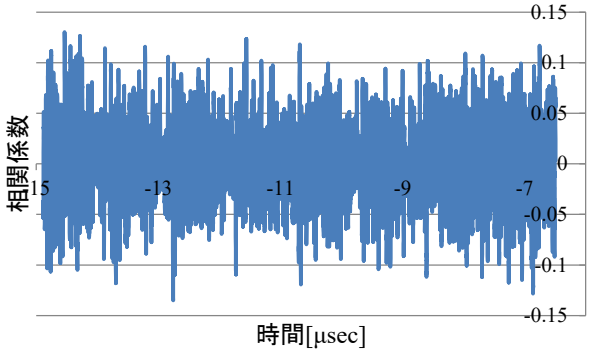

図 12　正解鍵における相関係数（提案手法）

Figure 12　Correlation coefficient in the correct key with the proposed method.

表 2　実行時間の比較

Table 2　Comparison of execution time.

	時間[μsec]
無対策	623
提案手法	782

5. まとめ

本研究では，環境発電デバイスの耐タンパ実装について検討した．提案手法では，実行サイクルの増加が少ない，すなわち消費電力の小さい対策手法であるシャッフリングを環境発電デバイスに適用した．そして，TWELITE 環境発電デバイスを使用した評価実験により，提案手法による対策を施した場合，1,500 個の電磁波波形を用いた場合でも解析に成功したラウンド鍵は 0 個であり，耐タンパ性が向上することを明らかにした．

今後は，提案手法に対して，より多くの波形データを使用した耐タンパ検証や，他の耐タンパ実装についての検討などを進める予定である．

謝辞　本研究の一部は，JSPS 科研費 17J11408 の助成を受けたものです．

参考文献

[1] Chalasani, S. and Conrad, J. M.: A Survey of Energy Harvesting Sources for Embedded Systems, Proc. of IEEE SoutheastCon 2008, pp. 442–447, (2008)
[2] Tentzeris, M. M., Georgiadis, A., and Roselli, L.: Energy Harvesting and Scavenging, Proc. of the IEEE, vol. 102, no. 11, pp. 1644–1648, (2014).
[3] 竹内敬治：エネルギーハーベスティング技術，電気評論，vol. 97，no. 11，pp. 51–55，(2012).
[4] 堀越　智，竹内敬治，篠原真毅：エネルギーハーベスティング　身の周りの微小エネルギーから電気を創る“環境発電”，日刊工業新聞社，(2014).
[5] Nicosia, A., Pau, D., Giacalone, D., Plebani, E., Bosco, A., and Iacchetti, A.: Efficient Light Harvesting for Accurate Neural Classification of Human Activities, Proc. of IEEE Int. Conf. Consumer Electronics (ICCE 2018), pp. 1–4, (2018).
[6] Kocher, P., Jaffe, J. and Jun, B.: Differential Power Analysis, Proc. of 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] Messerges, T. S.: Securing the AES Finalists Against Power Analysis Attacks, Proc. of Int. Workshop on Fast Software Encryption (FSE 2000), LNCS 1978, pp. 150–164, Springer (2000).
[9] Akkar, M.-L. and Giraud, C.: An Implementation of DES and AES, Secure against Some Attacks, Proc. of 2nd Int. Workshop Cryptographic Hardware and Embedded Systems (CHES 2001), LNCS 2162, pp. 309–318, Springer-Verlag (2001).
[10] Herbst, C., Oswald, E., and Mangard, S.: An AES Smart Card Implementation Resistant to Power Analysis Attacks, Proc. of Int. Conf. Applied Cryptography and Network Security (ACNS 2006), LNCS 3989, pp. 239–252, Springer (2006).
[11] Mangard, S., Oswald, E., and Popp, T.: Power Analysis Attacks. Springer, p.338, (2007).
[12] Gandolfi, K., Mourtel, C., and Olivier, F.: Electromagnetic Analysis: Concrete Results, Proc. of 3rd Int. Workshop on Cryptographic Hardware and Embedded Systems (CHES 2001), LNCS 2162, pp. 251–261, Springer-Verlag (2001).
[13] Meynard, O., Guilley, S., Danger, -L. J., and Sauvage, L.: Far Correlation-based EMA with a Precharacterized Leakage Model, Proc. of Design, Automation and Test in Europe Conference and Exhibition (DATE 2010), pp. 977–980 (2010).
[14] 野崎佑典，吉川雅弥：環境発電デバイスの耐タンパ性検証，2018 年暗号と情報セキュリティシンポジウム講演論文集，3D3-1，pp. 1–6，(2018).
[15] モノワイヤレス株式会社，https://mono-wireless.com/jp/index.html
[16] Suzaki, T., Minematsu, K., Morioka, S., and Kobayashi, E.: TWINE: A Lightweight, Versatile Blockcipher, Proc. of ECRYPT Workshop on Lightweight Cryptography (LC11), pp. 146–149, (2011).
[17] 坂本純一，松本　勉：環境発電無線センサモジュールにソフトウェア実装可能な共通鍵暗号，2016 年暗号と情報セキュリティシンポジウム講演論文集，2C4-1，pp. 1–8，(2016).