Vol.2017-UBI-54 No.17
Vol.2017-CDS-19 No.17
2017/5/26

認証暗号 MORUS に対する電力解析手法

野崎佑典[†1]　吉川雅弥[†1]

概要：近年，白物家電や AV 機器などのコンシューマ機器に対する不正な攻撃が報告されている．そのため，これらの不正な攻撃を防ぐための技術として，認証暗号が注目されている．本研究で対象とする MORUS は代表的な認証暗号の 1 つであり，認証暗号の標準規格を制定する CAESAR の 2 次選考を通過している．一方で，ハードウェアに対するセキュリティでは，サイドチャネル攻撃の危険性が指摘されている．サイドチャネル攻撃は，電力解析，電磁波解析，故障利用解析の総称である．しかし，これまでに MORUS に対するサイドチャネル攻撃の研究は筆者らの知る限りにおいて報告されていない．そこで本研究では，新たに認証暗号 MORUS に対する電力解析手法を提案する．提案手法では，MORUS の初期化処理を対象に電力解析を行う．また，複数のラウンドを対象に解析を行うことで，解析効率を向上させる．さらに，Field Programmable Gate Array（FPGA）を用いた評価実験により提案手法の有効性を実証すると共に，MORUS の脆弱性を定量的に評価する．

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

Power Analysis Method for an Authenticated Cipher MORUS

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

Abstract: The illegal attacks for the various devices include consumer products have been recently reported. Therefore, authenticated ciphers have been attracted attention as countermeasures. MORUS is one of the most popular authenticated ciphers, and it passed the second round of CAESAR. On the other hand, the risk of side-channel attacks for a cryptographic circuit has been pointed out. However, side-channel attacks for MORUS have not been reported. Therefore, this study proposes a new power analysis method for an authenticated cipher MORUS. The proposed method performs the power analysis for the initialization. In addition, the proposed method analyzes the multiple rounds to improve the attack accuracy. To our knowledge, this is the first attack for MORUS. Experiments using a field programmable gate array show the validity of the proposed method.

Keywords: Hardware security, Authenticated encryption, MORUS, Power analysis, Tamper resistance

1. はじめに

モノのインターネット（Internet of Things: IoT）の普及により，多くのコンシューマ製品が外部と接続されるようになってきた．そして，これらの機器を対象に不正アクセスによる乗っ取りや，不正な攻撃を行うための踏み台として使用される危険性が指摘されている [1]．この対策として，秘匿性を高めるための通信データの暗号化や，不正アクセスを防ぐための認証を同時に実現する認証暗号が注目されている．現在，認証暗号はいくつか提案されている [2], [3], [4], [5], [6]．また，認証暗号の標準規格を制定する Competition for Authenticated Encryption: Security, Applicability, and Robustness（CAESAR [7]）では，2 次審査が終了し，現在最終審査が行われている．本研究で対象とする MORUS [2]は, CAESAR の 2 次審査を通過した認証暗号である．

一方で，暗号アルゴリズムは計算量的にその安全性が保障されているが，ハードウェアとして実現した際に，その秘密鍵を不正に解析するサイドチャネル攻撃の脅威が報告されている．サイドチャネル攻撃 [8], [9], [10], [11]は暗号ハードウェア処理時の消費電力や漏洩電磁波，処理時間などの副次的な情報を利用することで，不正に内部の秘密鍵を解析する攻撃手法である．そして，消費電力を利用したサイドチャネル攻撃を電力解析と呼び，その危険性が指摘されている[8], [9]．今後の IoT 機器の安全性を検証する上で，IoT 機器での利用が期待される認証暗号 MORUS の電力解析に対する耐性（耐タンパ性）を検証することは非常に重要である．しかし，現在 MORUS を対象にした電力解析は筆者らの知る限りにおいて報告されていない．

そこで本研究では，認証暗号 MORUS に対する電力解析手法を提案する．提案手法では，MORUS の初期化処理を対象に電力解析を行うことで秘密鍵を解析する．また，MORUS の構造を利用した複数ラウンドを利用した攻撃を導入することで，解析効率を向上させる．さらに，Field Programmable Gate Array（FPGA）を用いた評価実験により，提案手法の有効性を実証する．

†1 名城大学
Meijo University

Vol.2017-UBI-54 No.17
Vol.2017-CDS-19 No.17
2017/5/26

2. 準備

まず，2.1 節で MORUS について，2.2 節で電力解析の概要について説明する．

2.1 認証暗号 MORUS

MORUS [2]は Wu らによって提案された認証暗号であり，認証暗号の標準規格を決める CAESAR コンペティションの 2 次審査を通過している．また，MORUS はソフトウェア実装とハードウェア実装での高速性に優れている [2]．MORUS では，ブロック長は 640bit または 1280bit と，鍵長は 128bit または 256bit を選択することができ，その組み合わせは 3 種類ある．それぞれの組み合わせの MORUS を MORUS-640-128，MORUS-1280-128，MORUS-1280-256 と呼ぶ．ここでは，MORUS の処理について MORUS-640-128 を例に説明する．

MORUS の暗号処理は，初期化処理，Associated data 処理，平文の暗号処理，認証タグの生成処理の 4 つの処理で構成する．MORUS では，128bit の State レジスタを 5 つ用意し，

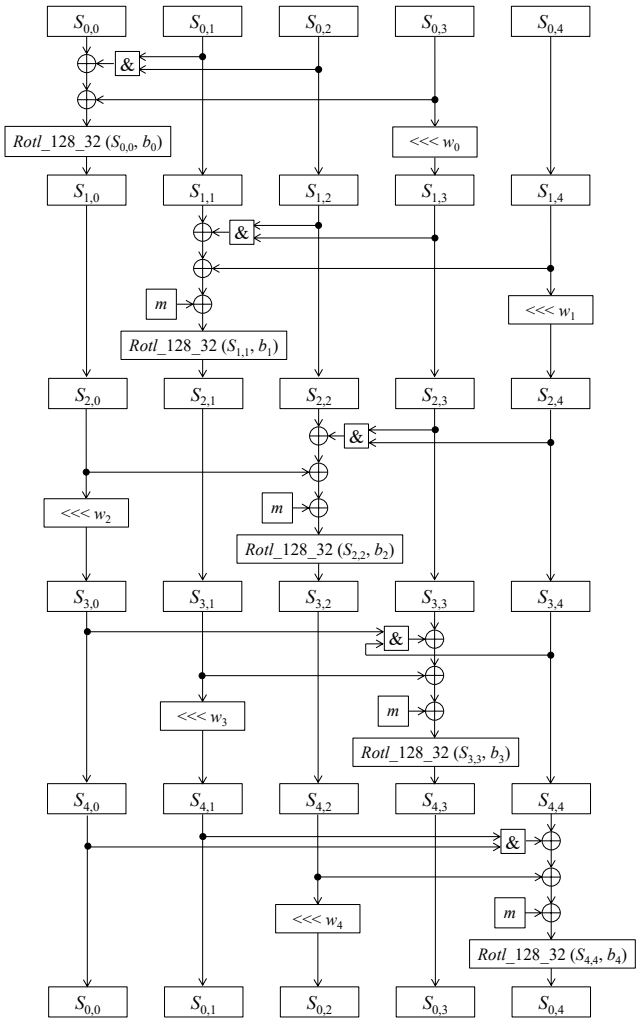

図 1　StateUpdate 関数の概要

Figure 1　Outline of the StateUpdate function.

各 State レジスタを更新することで，処理を行う．また各処理（初期化処理，Associated data 処理，平文の暗号処理，認証タグの生成処理）では，図 1 に示す StateUpdate 関数を繰り返し適用することで，State レジスタを更新する．

StateUpdate 関数は図 1 に示すように，排他的論理和演算，論理積演算，左ローテーション処理，*Rotl*_128_32 関数の 4 つの処理で構成する．StateUpdate 関数は 5 ラウンドの処理で構成し，各ラウンドでは，式(1)から式(5)に示す計算を行う．

$$\begin{cases} S_{1,0} = Rotl\_128\_32\left(S_{0,0} \oplus \left(S_{0,1} \,\&\, S_{0,2}\right) \oplus S_{0,3}, b_0\right) \\ S_{1,3} = S_{0,3} <<< w_0 \\ S_{1,1} = S_{0,1} \\ S_{1,2} = S_{0,2} \\ S_{1,4} = S_{0,4} \end{cases} \tag{1}$$

$$\begin{cases} S_{2,1} = Rotl\_128\_32\left(S_{1,1} \oplus \left(S_{1,2} \,\&\, S_{1,3}\right) \oplus S_{1,4} \oplus m, b_1\right) \\ S_{2,4} = S_{1,4} <<< w_1 \\ S_{2,0} = S_{1,0} \\ S_{2,2} = S_{1,2} \\ S_{2,3} = S_{1,3} \end{cases} \tag{2}$$

$$\begin{cases} S_{3,2} = Rotl\_128\_32\left(S_{2,2} \oplus \left(S_{2,3} \,\&\, S_{2,4}\right) \oplus S_{2,0} \oplus m, b_2\right) \\ S_{3,0} = S^i_{2,0} <<< w_2 \\ S_{3,1} = S_{2,1} \\ S_{3,3} = S_{2,3} \\ S_{3,4} = S_{2,4} \end{cases} \tag{3}$$

$$\begin{cases} S_{4,3} = Rotl\_128\_32\left(S_{3,3} \oplus \left(S_{3,4} \,\&\, S_{3,0}\right) \oplus S_{3,1} \oplus m, b_3\right) \\ S_{4,1} = S_{3,1} <<< w_3 \\ S_{4,0} = S_{3,0} \\ S_{4,2} = S_{3,2} \\ S_{4,4} = S_{3,4} \end{cases} \tag{4}$$

$$\begin{cases} S_{0,4} = Rotl\_128\_32\left(S_{4,4} \oplus \left(S_{4,0} \,\&\, S_{4,1}\right) \oplus S_{4,2} \oplus m, b_4\right) \\ S_{0,2} = S_{4,2} <<< w_4 \\ S_{0,0} = S_{4,0} \\ S_{0,1} = S^i_{4,1} \\ S_{0,3} = S_{4,3} \end{cases} \tag{5}$$

ここで，式(1)から式(5)において，それぞれ⊕はビット単位での排他的論理和演算を，&はビット単位での論理積演算を，<<<は *w*bit の左ローテーション処理を，*Rotl*_128_32( )は *Rotl*_128_32 関数を表している．また，左ローテーション処理で使用するパラメータ *w* を表 1 に示す．次に，*Rotl*_128_32 関数の概要を図 3 に示す．図 3 に示すように，*Rotl*_128_32 関数では，128bit の中間値を 32bit ずつに分割し，各 32bit の値に対してそれぞれ *b* bit ずつの左ローテーション処理を行う．また，Rotl_128_32 関数で使用するパラメータ *b* を表 1 に示す．

表 1　定数値 w

Table 1　Constant value w.

w	値
w_0	32
w_1	64
w_2	96
w_3	64
w_4	32

表 2　定数値 b

Table 2　Constant value b.

b	値
b_0	5
b_1	31
b_2	7
b_3	22
b_4	13

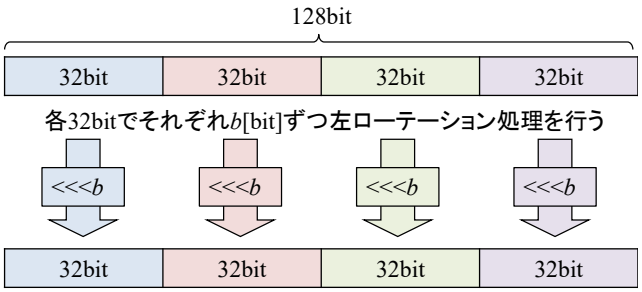

図 2　*Rotl*_128_32 関数

Figure 2　*Rotl*_128_32 function.

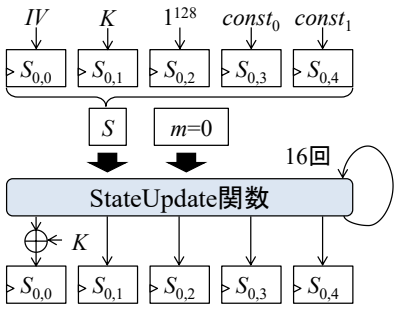

図 3　初期化処理

Figure 3　Initialization.

次に初期化処理の詳細について説明する．初期化処理を図 3 に示す．図 3 に示すように，初期化処理では各 State レジスタ（$S_{0,0}$, $S_{0,1}$, $S_{0,2}$, $S_{0,3}$, $S_{0,4}$）に初期値として，初期ベクトル IV，秘密鍵 K，全て 1 の定数値 1^{128}，定数値 $const_0$，定数値 $const_1$ を入力する．そして，$m = 0$ として，StateUpdate 関数の処理を適用する．初期化処理では，StateUpdate 関数を合計で 16 回適用する．すなわち，合計で 16 回×5 ラウンド=80 ラウンドの処理を行う．また，最終ラウンドである 80 ラウンド目の処理では，式(6)に示す処理を行う．

$$S_{0,1} = S_{0,1} \oplus K \tag{6}$$

2.2 電力解析

電力解析は，暗号ハードウェア処理時の消費電力を観測し，観測した消費電力情報や既知の平文，暗号文を利用することで内部の秘密鍵の解析を行う．代表的な電力解析には，差分電力解析（Differential Power Analysis: DPA [8]）や相関電力解析（Correlation Power Analysis: CPA [9]）などがある．CPA は暗号ハードウェア内部のデータレジスタ間のデータ遷移と消費電力との間に生じる相関関係を解析に利用する．具体的には，既知の平文（暗号文）と暗号処理に使用する鍵の予測値を利用することで，レジスタ間のデータ遷移を計算する．すなわち，レジスタ間のハミング距離（Hamming Distance: HD）を計算する．

そして，計算した HD と消費電力 w とのピアソンの相関係数 ρ を，式(7)を用いて算出する．このとき，$\overline{h}$ はハミング距離 h の平均値を，$\overline{w_t}$ は消費電力 w の平均値を，D は解析に使用したデータの数を，t は使用した消費電力波形の時間軸上のサンプル位置を表している．

$$\rho_t = \frac{\sum_{i=1}^{D}\left(w_{i,t} - \overline{w_t}\right)\left(h_i - \overline{h}\right)}{\sqrt{\sum_{i=1}^{D}\left(w_{i,t} - \overline{w_t}\right)^2 \sum_{i=1}^{D}\left(h_i - \overline{h}\right)^2}} \tag{7}$$

最後に，CPA ではピアソンの相関係数 ρ を最大とする鍵の予測値を正解鍵として推定する．

3. 提案手法

3.1 ベース電力解析

提案手法では，MORUS の初期化処理を対象に電力解析を行う．提案手法の概要を図 4 に示す．図 4 に示すように，初期化処理の 1 ラウンド目を対象に CPA をベースとした電力解析を行う．具体的には，1 番目の State レジスタの初期値 $S_{0,0}$（既知の初期ベクトル IV）と 1 ラウンド目終了後の値 $S_{1,0}$（未知の値）とのハミング距離を解析に用いるものとする．

このとき，対象とする中間値 $S_{1,0}$ は，式(1)より式(8)で計算することが出来る．ここで，初期ベクトル IV と定数値 1^{128}，$const_0$ は既知の値であるが，秘密鍵 K は未知の値である．そのため，秘密鍵 K の予測値を計算に用いる．この予

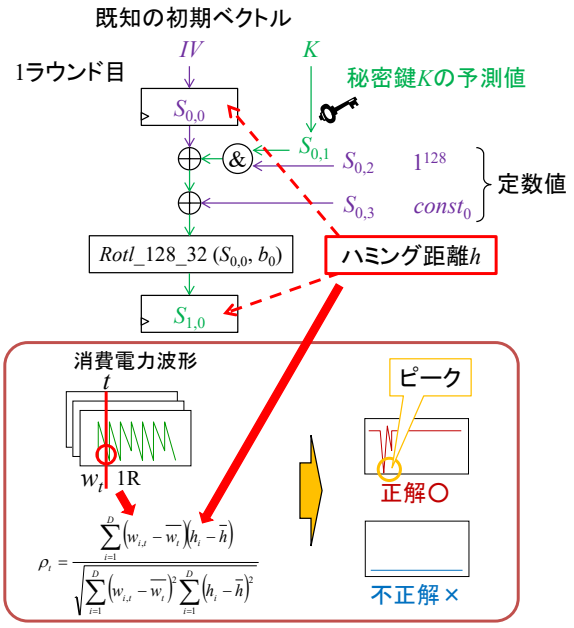

図 4　ベース電力解析の概要

Figure 4　Outline of the based power analysis.

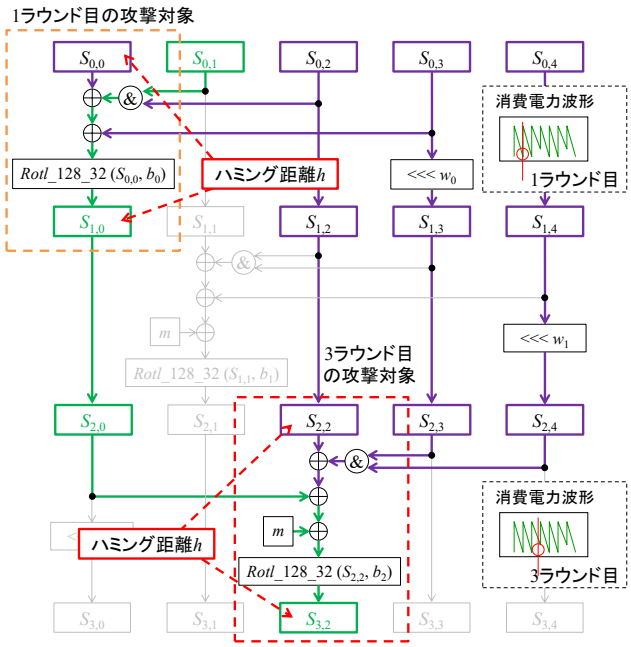

図 5　複数ラウンドを利用した電力解析で用いるハミング距離

Figure 5　Hamming distance for multiple rounds aware power analysis.

測値には，MORUS の計算がビット単位で行われていることから，$2^1 = 2$ 通りの候補を試す．したがって，秘密鍵は 128bit であるため，この計算を合計で $2^1 \times 128 = 256$ 通り行う．

$$S_{1,0} = Rotl\_128\_32\left(IV \oplus \left(K \,\&\, 1^{128}\right) \oplus const_0, b_0\right) \qquad (8)$$

そして，ハミング距離を求める関数を $HD(A, B)$とすると，$S_{0,0}$ と $S_{1,0}$ のハミング距離 h は式(9)で計算出来る．

$$h = HD\left(S_{0,0} \oplus S_{1,0}\right) \qquad (9)$$

最後に，求めたハミング距離 h と 1 ラウンド目の消費電力 w とのピアソンの相関係数を式(7)より計算する．そして，提案手法では，このピアソンの相関係数を最大とする秘密鍵 K の予測値を正解鍵として推定する．

3.2 複数ラウンドを利用した電力解析

提案手法では，MORUS の構造を利用した複数ラウンドを用いた電力解析を行うことで，解析効率を向上させる．ここでは，初期化処理の 1 ラウンド目と 3 ラウンド目を利用する場合を例に説明する．

MORUS では，図 5 に示すように 1 つの秘密鍵の予測値で，1 ラウンド目終了後の値 $S_{1,0}$ と 3 ラウンド目終了後の値 $S_{3,2}$ を計算することが出来る．具体的には，3 ラウンド目終了後の値 $S_{3,2}$ は，式(3)を用いて計算出来る．ここで，式(3)の $S_{2,2}$，$S_{2,3}$，$S_{2,4}$ は定数値 1^{128}，$const_0$，$const_1$ から計算出来るため，既知の値である．また，$S_{2,0}$ は式(2)より $S_{1,0}$ と等しく，$S_{1,0}$ は式(8)より秘密鍵 K の予測値を用いて計算

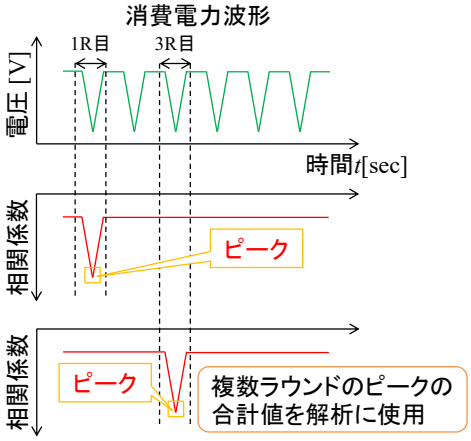

図 6　複数ラウンドで観測されるピーク

Figure 6　Peaks in multiple rounds.

することが出来る．

そのため，図 6 に示すように，それぞれ計算したハミング距離を用いて相関係数を算出することで，正解鍵において 1 ラウンド目と 3 ラウンド目にそれぞれ相関係数のピークが観測される．提案手法では，この複数のピークの合計値を解析に利用する．このように，複数のラウンドのより多くの情報を解析に利用することで，解析効率を向上させることが出来る．そして，相関係数のピークの合計値が最大となる秘密鍵 K の予測値を正解鍵として推定する．

4. 評価実験

4.1 実験環境

実験に使用した評価システムを図 7 に，評価システムの詳細を表 3 に示す．評価ボードには，サイドチャネル攻撃標準評価ボード SASEBO-GII [12]を使用した．そして，SASEBO-GII 上に搭載されている FPGA Virtex-5 に MORUS を FPGA 実装した．また，MORUS はブロック長が 640bit，鍵長が 128bit のもの（MORUS-640-128）を FPGA 実装した．そして，実験では乱数で生成した初期ベクトルと秘密鍵を用いて 20,000 回の処理を行い，20,000 個の消費電力波形をオシロスコープで取得した．

このとき，取得した消費電力波形は MORUS の消費電流を 1Ω のシャント抵抗で測定した電圧波形である．取得した消費電力波形を図 8 に示す．評価実験では，図 8 の 1 ラウンド目（1R）と 3 ラウンド目（3R）の処理に相当する部分の消費電力波形を解析に使用する．

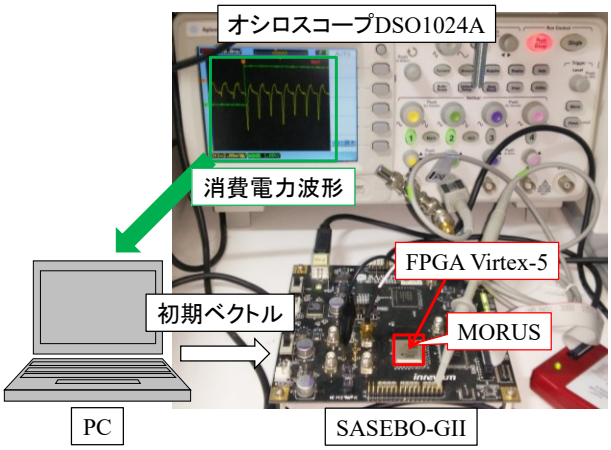

図 7　評価システム
Figure 7　Evaluation system.

表 3　実験環境
Table 3　Experimental environment.

暗号アルゴリズム	MORUS
評価ボード	SASEBO-GII [12]
FPGA	Virtex-5 XC5VLX30
開発環境	Xilinx ISE Design Suite 14.1
オシロスコープ	Agilent DSO 1024A
サンプリングレート	2 [Gsa/sec]
電源	PC からの USB 給電
PC	HP ProBook 6570b
OS	Windows7 Professional
メモリ	8.00 GB
CPU	Intel Core i7-3520M
解析ソフト	MATLAB 2013b

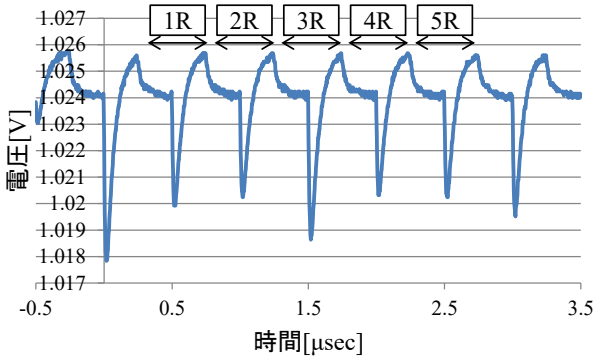

図 8　消費電力波形の例
Figure 8　Example of power consumption waveform.

4.2 実験結果

評価実験では，複数ラウンドを利用した電力解析（提案手法（1R+3R））と 1 ラウンド目のみを対象とした電力解析（提案手法（1R）），3 ラウンド目のみを対象とした電力解析（提案手法（3R））をそれぞれ実施した．実験結果を図 9 に示す．図 9 の(a)は実験結果の全体図，(b)は実験結果の拡大図である．図 9 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 数を示している．今回対象とした MORUS（MORUS-640-128）の秘密鍵は 128bit であるため，縦軸の最大値は 128 である．

図 9 に示すように，複数ラウンドを利用した解析（提案手法（1R+3R））では 10,000 個の消費電力波形で，提案手

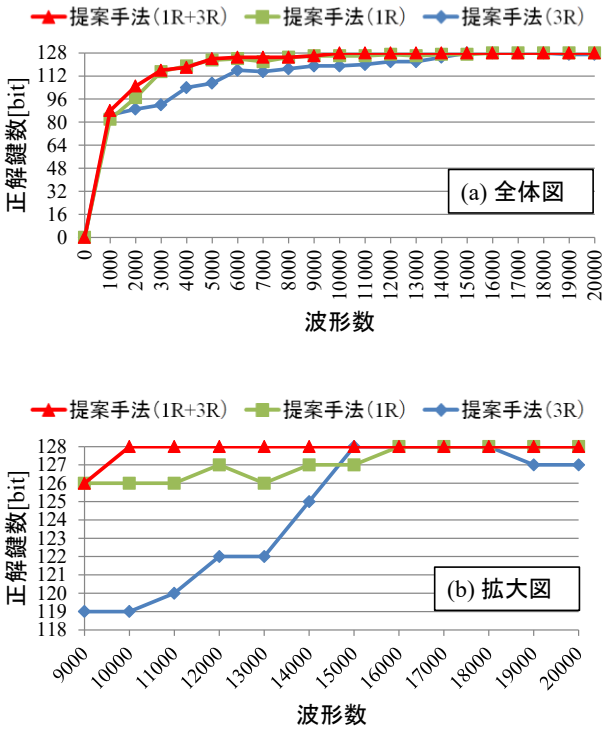

図 9　実験結果
Figure 9　Experimental results.

Vol.2017-UBI-54 No.17
Vol.2017-CDS-19 No.17
2017/5/26

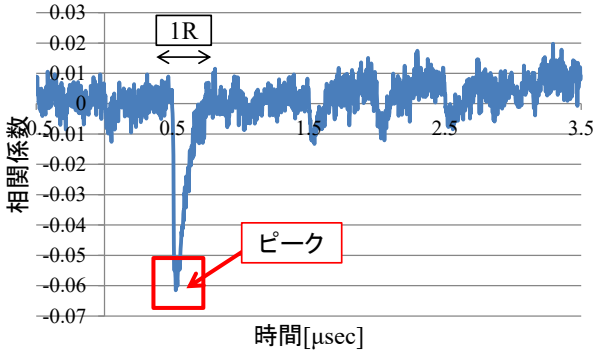

図 11　相関係数（1R）

Figure 11　Correlation coefficient with 1st round.

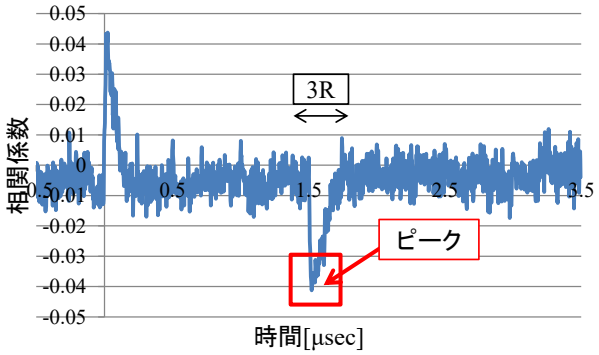

図 12　相関係数（3R）

Figure 11　Correlation coefficient with 3rd round.

法（1R）では 16,000 個の消費電力波形で，全ての秘密鍵の推定に成功していることが分かる．したがって，提案手法は有効であり，MORUS は提案手法に対して脆弱であることが分かる．一方で，提案手法（3R）では 15,000 個の消費電力波形で一時的に全ての秘密鍵の推定に成功しているが，19,000 個以降では，秘密鍵を全て推定することに失敗しており，解析が不安定であることが分かる．したがって，複数ラウンドを利用することで，安定して解析を行うことができ，解析効率の向上が可能であると考えられる．

次に，正解鍵における相関係数の結果を示す．提案手法（1R）における結果を図 11 に，提案手法（3R）における結果を図 12 に示す．図 11 と図 12 の横軸は処理時間を，縦軸は相関係数をそれぞれ示している．図 11 に示すように，1 ラウンド目の処理に相当する部分において，相関係数のピークが表れていることが確認出来る．また，図 12 に示すように，3 ラウンド目の処理に相当する部分において，相関係数のピークが表れていることが確認出来る．

5. まとめ

本研究では，認証暗号 MORUS に対する電力解析手法を提案した．提案手法では，MORUS の初期化処理を対象に電力解析を行うことで，秘密鍵の解析を行う．また，複数のラウンドを対象に電力解析を適用することで，解析効率を向上させる．さらに，FPGA を用いた評価実験により提案手法の有効性を実証し，MORUS が電力解析に対して脆弱であることを明らかにした．

今後は，より効率的な解析を行うための提案手法の改善や，提案手法に対する対策手法の検討などを行う予定である．

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] Pa Pa, M. Y., Suzuki, S., Yoshioka, K., Matsumoto, T., Kasama, T. and Rossow, C.: IoTPOT: Analysing the Rise of IoT Compromises, Proc. of the 9th USENIX Workshop on Offensive Technologies (WOOT'15), (2015). https://www.usenix.org/system/files/conference/woot15/woot15-paper-pa.pdf

[2] Wu, H. and Huang, T.: The Authenticated Cipher MORUS (v2), (2016). https://competitions.cr.yp.to/round3/morusv2.pdf

[3] Sasaki, Y., Todo, Y., Aoki, K., Naito, Y, Sugawara, T., Murakami, Y., Matsui, M. and Hirose, S.: Minalpher v1.1, (2015). http://info.isl.ntt.co.jp/crypt/minalpher/files/minalpherv11.pdf

[4] Minematsu, K.: AES-OTR v3, (2015). http://competitions.cr.yp.to/round2/aesotrv2.pdf

[5] NIST Special Publication 800-38D: Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC, (2007).

[6] Iwata, T., Minematsu, K., Guo, J., Morioka, S. and Kobayashi, E.: CLOC and SILC v3, (2016). https://competitions.cr.yp.to/round3/clocsilcv3.pdf

[7] CAESAR: Competition for Authenticated Encryption: Security, Applicability, and Robustness, http://competitions.cr.yp.to/caesar.html

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

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

[10] 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).

[11] 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).

[12] Research Institute for Secure Systems, AIST, : Evaluation Environment for Side-channel Attacks, http://www.risec.aist.go.jp/project/sasebo