Vol.2016-MBL-80 No.7
Vol.2016-CDS-17 No.7
2016/8/24

改ざん検知暗号 Minalpher に対する電力解析

野崎佑典[†1]　吉川雅弥[†1]

概要：近年，コンシューマ製品を含む IoT 機器のセキュリティへの関心が高まっており，認証と暗号化を同時に実現可能な改ざん検知暗号が注目されている．本研究で対象とする Minalpher は代表的な改ざん検知暗号の 1 つである．一方で，ハードウェアセキュリティにおいて，電力解析の脅威が指摘されているが，Minalpher を対象とした電力解析の研究は行われていない．そこで本研究では，Minalpher に対する電力解析を提案する．そして，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．

キーワード：ハードウェアセキュリティ，改ざん検知暗号，Minalpher，電力解析，耐タンパ性

Power Analysis for Minalpher

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

Abstract: Recently, the security of IoT devices, which include consumer electronics, has attracted attention. So, falsification detection ciphers have attracted, because they can realize both authentication and encryption simultaneously. Minalpher is one of the most popular falsification detection ciphers. Regarding the hardware security, the risk of power analysis is pointed out. However, power analysis for Minalpher has not been reported. Therefore, this study proposes a new power analysis method for Minalpher. Experiments using FPGA prove the validity of the proposed method.

Keywords: Hardware security, Falsification detection cipher, Minalpher, Power analysis, Tamper resistance

1. はじめに

Internet of Things (IoT) によりコンシューマ製品など様々な機器が外部と接続される機会が増加してきた. また，これらの機器が外部のネットワークから攻撃される危険性が報告されている[1]．そのため，これらの攻撃への対策として暗号化と認証を同時に実現可能な改ざん検知暗号が注目されている[2]，[3]，[4]，[5]．本研究で対象とする Minalpher[2]は代表的な改ざん検知暗号の 1 つである．

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危険性が報告されている[6], [7], [8], [9], [10]. サイドチャネル攻撃は，暗号回路が動作する時に生じる消費電力や電磁波などを利用し，統計的な処理を行うことで内部の鍵情報を推定する攻撃手法である．特に，消費電力を利用したサイドチャネル攻撃である電力解析は，オシロスコープ等の安価な機器で実行出来るため非常に脅威とされている[8]，[9]，[10].

これまでに，標準暗号 Advanced Encryption Standard (AES[11]) に対する電力解析は数多く報告されている．しかし，改ざん検知暗号に対する電力解析はほとんど報告されておらず, Minalpher に対する具体的な電力解析の研究は見当たらない．また，今後の IoT 機器の安全性を保障するためにも，改ざん検知暗号に対する電力解析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, Minalpher に対する電力解析を提案する．提案手法では，Minalpher の暗号アルゴリズムに合わせた 2 段階での電力解析を行う．そして，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検証する．

2. 準備

まず，2.1 節で Minalpher 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 改ざん検知暗号 Minalpher

Minalpher[2]は 2014 年に発表された改ざん検知暗号であり，改ざん検知暗号の国際標準規格を制定するコンペティション Competition for Authenticated Encryption : Security, Applicability, and Robustness (CAESAR[12]) の一次選考を通過している．また，Minalpher は一般的に広く用いられている AES-GCM[4]よりも, 実装面や安全性で優れている[2]. Minalpher について，Authenticated Encryption with Associated Data (AEAD) モードの暗号文生成部分を中心に説明する．

†1 名城大学
Meijo University

Vol.2016-MBL-80 No.7
Vol.2016-CDS-17 No.7
2016/8/24

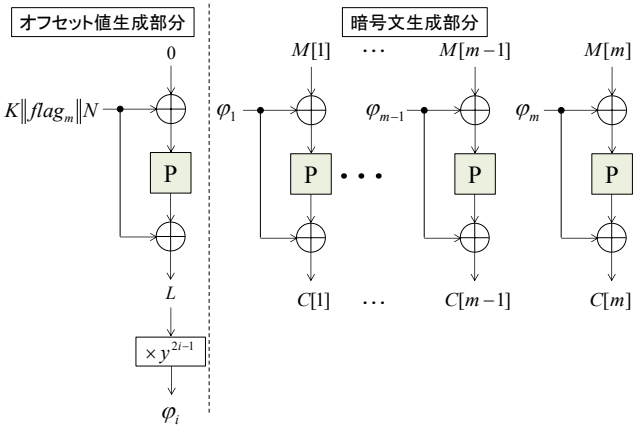

図 1　Minalpher の概要

Figure 1　Outline of Minalpher.

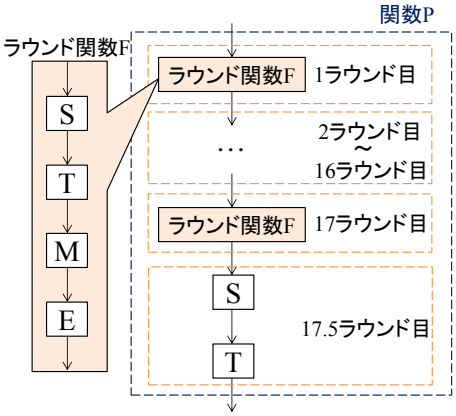

図 3　関数 P の概要

Figure 3　Outline of function P.

Minalpher の概要を図 1 に示す．図 1 に示すように，オフセット値生成部分と暗号文生成部分で構成し，256bit の置換を行う関数 P を繰り返し適用する．オフセット値生成部分では，128bit の秘密鍵 K と 24bit の定数値 $flag_m$，104bit のナンス N の合計 256bit の値 $K\|flag_m\|N$ を入力値として，関数 P に与える．そして，関数 P の出力値と $K\|flag_m\|N$ との排他的論理和演算を行い，出力 L を取得する．この出力 L を利用してオフセット値 φ_i を計算する．このとき，オフセット値の計算は文献[2], [3]より図 2 に示す処理で計算することが可能である．

暗号文生成部分では，メッセージ M とオフセット値 φ_i との排他的論理和演算を行った結果を関数 P の入力とする．そして，関数 P の出力とオフセット値 φ_i との排他的論理和演算を行うことで暗号文 C を計算する．ここで，メッセージ M は 256bit を 1 つのブロックとして，m 個のブロックに分割して処理を行う．

次に，関数 P について説明する．関数 P の概要を図 3 に示す．図 3 に示すように，合計で 17.5 ラウンドの処理で構成する．ラウンド関数は，関数 S，関数 T，関数 M，関数 E で構成しており，1 ラウンド目から 17 ラウンド目までではラウンド関数による処理を，17.5 ラウンド目では，関数 S と関数 T による処理を行う．

ラウンド関数の詳細について，図 4 を用いて説明する．Minalpher は 4bit 単位で各処理を行っており，ラウンド関数では，256bit の入力値を 4 × 8 の行列 A，B に分割して処理を行う．まず，関数 S では関数 Sub Nibbles (SN) による処理を行う．関数 SN では，行列 A，B に対して，表 1 を示す S-Box 表による置換処理を 4bit 単位で適用する．

次に，関数 T では関数 Shuffle Rows (SR) と関数 Swap Matrices (SM) による処理を行う．関数 SR では表 2 に示す SR 表による転置処理を行う．具体的には，行列 A に対しては，各行に対しそれぞれ SR_1，SR_2，SR_1^{-1}，SR_2^{-1} を適用す

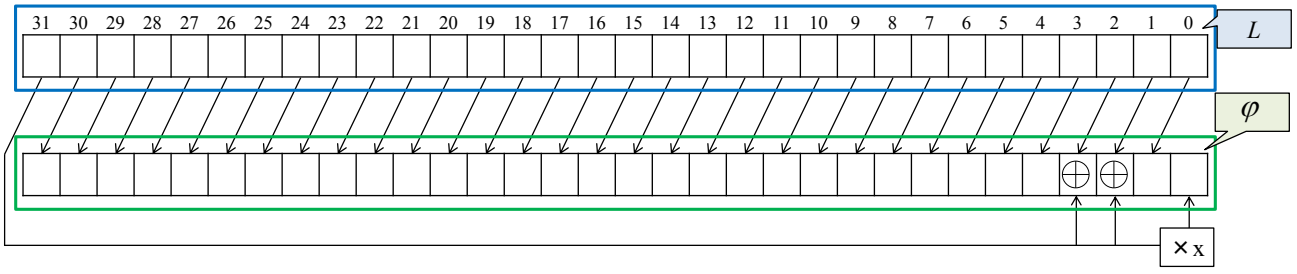

図 2　y の乗算[2]，[3]

Figure 2　Multiplication of y.

表 1　S-Box 表

Table 1　S-Box table.

x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$S(x)$	B	3	4	1	2	8	C	F	5	D	E	0	6	9	A	7

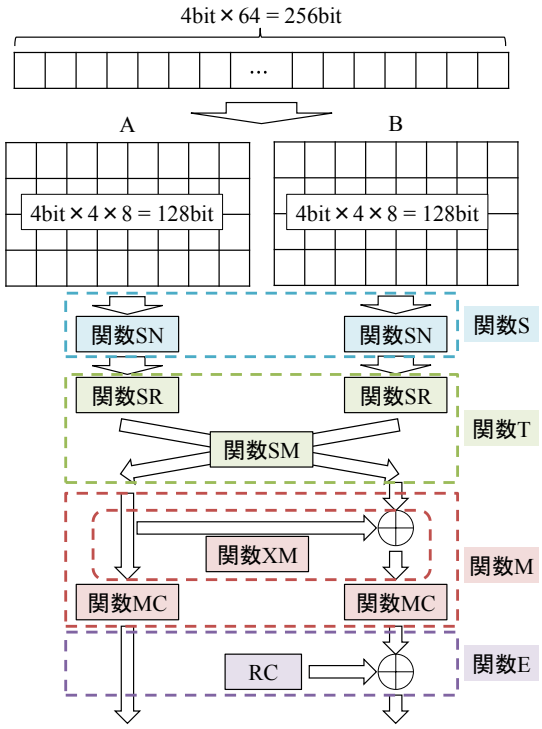

図 4　ラウンド関数
Figure 4　Round function.

る．行列 B に対しては，各行に対しそれぞれ SR_1^{-1}，SR_2^{-1}，SR_1，SR_2 を適用する．関数 SM では，2 つの行列を入れ替える処理を行う．

そして，関数 M では関数 Xor Matrix (XM) と関数 Mix Columns (MC) による処理を行う．関数 XM では，行列 A と行列 B との排他的論理和演算を行う．関数 MC では，式(1)による行列演算を行う．

$$\begin{bmatrix} 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \end{bmatrix} \tag{1}$$

最後に，関数 E ではラウンド定数 Round Constant (RC) との排他的論理和演算を行う．

表 2　SR 表
Table 2　SR table.

j	0	1	2	3	4	5	6	7
$SR_1(j)$	6	7	1	0	2	3	4	5
$SR_1^{-1}(j)$	3	2	4	5	6	7	0	1
$SR_2(j)$	4	5	0	1	7	6	2	3
$SR_2^{-1}(j)$	2	3	6	7	0	1	5	4

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，統計的に処理を行うことで内部の鍵情報を推定する．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]），テンプレート攻撃[10]などがある．

CPA では，データレジスタ間のデータ遷移数（ハミング距離）と消費電力との間に線形な相関関係があることを仮定する．そして，この相関関係を利用する．CPA はハミング距離を導出するために，対象とする暗号中間値を計算する．この計算は，既知の暗号文と鍵の予測値を用いて行う．暗号中間値を導出後，既知の暗号文とのハミング距離 h を計算し，このハミング距離 h と消費電力 w とのピアソンの相関係数 ρ を計算する．この計算式を式(2)に示す．ここで，$\overline{w_t}$ は消費電力 w_t の平均を，$\overline{h}$ はハミング距離 h の平均を，t は時間軸上のサンプル点を，D は解析に使用したデータ数を表している．

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

そして，この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 概要

Minalpher はオフセット値生成部分で秘密鍵を使用した処理を行っている．そのため，秘密鍵の解析ではオフセット値生成部分を対象とした電力解析を行う．この電力解析では，複数のオフセット値を利用して解析を行う．しかし，Minalpher の暗号アルゴリズムの構成上，オフセット値は外部に出力されない．したがって，攻撃者はオフセット値を直接取得することは出来ない．そこで，提案手法では，オフセット値を解析するための電力解析を行う．すなわち，2 段階での電力解析を行う．

提案手法の概要を図 5 に示す．図 5 に示すように，提案手法は 1 段階目の電力解析と 2 段階目の電力解析で構成する．1 段階目の電力解析では，暗号文生成部分を対象として，オフセット値の解析を行う．このオフセット値の解析では，既知の暗号文と消費電力波形のペアを D_1 個使用して，電力解析を行う．次に，2 段階目の電力解析では，1 段階目の電力解析を D_2 回行い，D_2 個のオフセット値を取得する．そして，D_2 個の消費電力波形とオフセット値のペアを使用して，オフセット値生成部分に対して電力解析を行い，秘密鍵 K を推定する．

Vol.2016-MBL-80 No.7
Vol.2016-CDS-17 No.7
2016/8/24

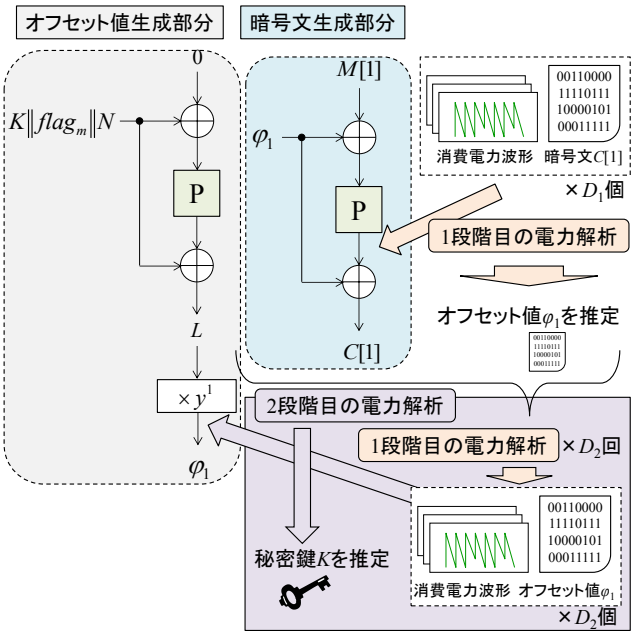

図 5　提案手法の概要

Figure 5　Outline of the proposed method.

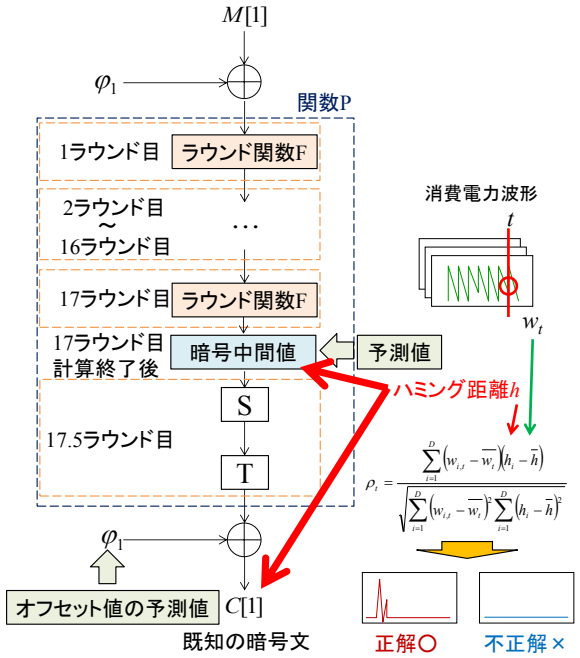

図 6　1 段階目の電力解析

Figure 6　Power analysis at the first stage.

3.2　1 段階目の電力解析

まず，1 段階目の電力解析について説明する．図 6 に示すように，1 段階目の電力解析は Minalpher の暗号文生成部分を対象として行う．具体的には，関数 P の 17.5 ラウンド目を対象として CPA をベースとした解析を行う．ハミング距離には，既知の暗号文 $C[1]$と 17 ラウンド目計算終了後の暗号中間値 x を利用する．対象とする暗号中間値 x は，既知の暗号文 $C[1]$とオフセット値 φ_1 の予測値を用いた計算により求める．この計算式を式(3)に示す．ここで，$S(\ )$ は関数 S による処理を，$T(\ )$は関数 T による処理を表している．

$$x = S\left(T\left(C[1] \oplus \varphi_1\right)\right) \tag{3}$$

そして，式(4)より暗号中間値 x と暗号文 $C[1]$とのハミング距離 h を計算する．ここで，$HD\ (A,B)$ は A と B とのハミング距離を計算する関数である．

$$h = HD\left(x, C[1]\right) \tag{4}$$

オフセット値の推定では，ハミング距離 h と消費電力 w のピアソンの相関係数 ρ を式(2)より計算する．そして，ピアソンの相関係数 ρ を最大とするオフセット値 φ_1 の予測値を正解値として推定する．

また，1 段階目の電力解析において，式(3)の $S(\ )$，$T(\ )$はそれぞれ 4bit 単位で計算を行うことが出来る．したがって，オフセット値の予測値には $2^4 = 16$ 通りの候補を試す．さらにオフセット値の導出に関して，全てのオフセット値である 256bit の値ではなく，秘密鍵 K に関連する部分である 128bit の値のみを導出する．

3.3　2 段階目の電力解析

次に，2 段階目の電力解析について説明する．図 7 に示すように，2 段階目の電力解析は Minalpher のオフセット値生成部分を対象として行う．具体的には，1 段階目の電力解析と同様にして，関数 P の 17.5 ラウンド目を対象とする．したがって，17 ラウンド目計算終了後の暗号中間値 x と L とのハミング距離を計算する．このとき，L は 1 段階目の電力解析で推定したオフセット値 φ_1 を利用して計算する．L の計算方法を図 8 に示す．図 8 に示す処理により，オフ

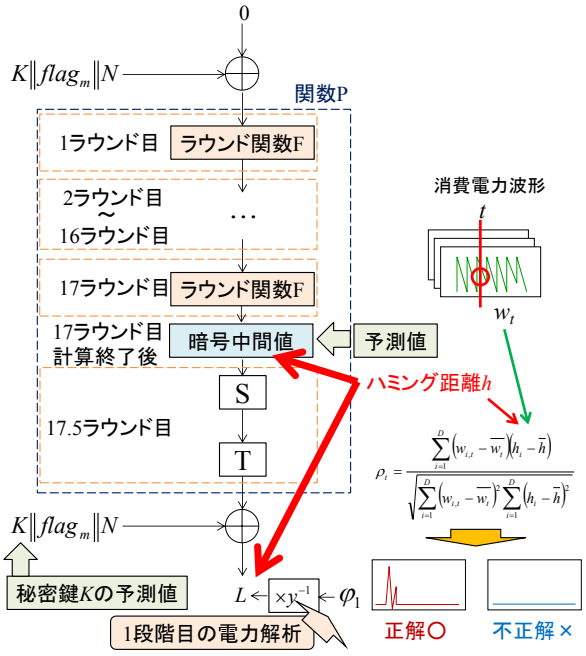

図 7　2 段階目の電力解析

Figure 7　Power analysis at the second stage.

Vol.2016-MBL-80 No.7
Vol.2016-CDS-17 No.7
2016/8/24

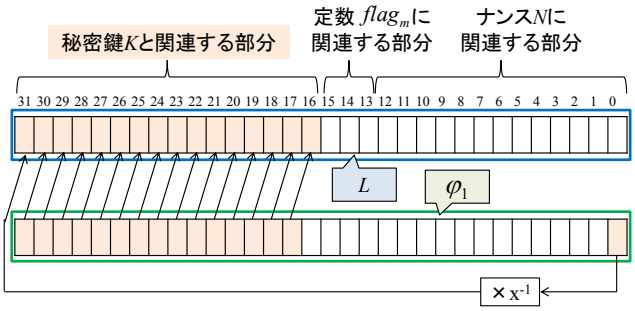

図 8　L の計算

Figure 8　Calculation of L.

セット値 φ_1 から秘密鍵 K に関連する 128bit の L の値を計算することが出来る．また，この 1 段階目の電力解析は 2 段階目の電力解析で使用するデータ数である D_2 回分行う．そして，対象とする暗号中間値は L と秘密鍵 K の予測値を用いて，式(5)で計算する．また，式(5)の計算は 4bit 単位で行う．そして，暗号中間値 x と L とのハミング距離 h を算出する．

$$x = S(T(L \oplus K)) \tag{5}$$

秘密鍵 K の推定では，1 段階目の電力解析と同様にして，算出したハミング距離 h と消費電力 w とのピアソンの相関係数 ρ を式(2)より計算する．そして，ピアソンの相関係数 ρ 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．

以上より，D_1 個のデータによる 1 段階目の電力解析を D_2 回，D_2 個のデータによる 2 段階目の電力解析を 1 回実行することで，秘密鍵の全てを推定することが出来る．

4. 評価実験

4.1 実験環境

実験環境を図 9 と表 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[13]を使用した．そして，SASEBO-GII 上の FPGA Virtex-5 に Minalpher を FPGA 実装した．消費電力の測定では，ナンスと平文は乱数で作成したものを利用する．また，実際に取得した消費電力波形の例を図 10 に示す．図 10 は暗号 LSI の消費電流を 1[Ω]のシャント抵抗により測定した電圧波形である．図 10 に示す消費電力波形を用いて解析を行う．

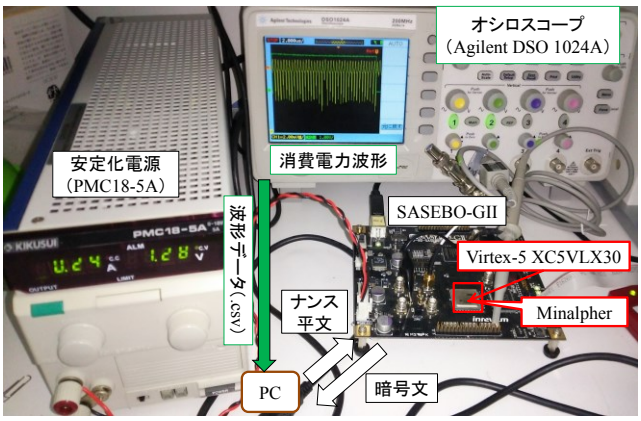

図 9　評価システム

Figure 9　Evaluation system.

表 3　実験環境

Table 3　Experimental Environment.

暗号アルゴリズム	Minalpher
評価ボード	SASEBO-GII
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	安定化電源 PMC18-5A
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

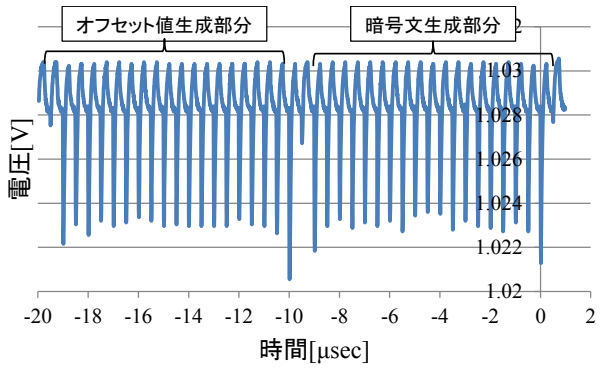

図 10　消費電力波形の例

Figure 10　Example of power consumption waveform.

4.2 実験結果

評価実験では，まず 1 段階目の電力解析を行った．1 段階目の電力解析では，オフセット値の解析を行う．実験結果を図 11 に示す．図 11 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オフセット値のビット

数を示している．図 11 に示すように，5,000 波形のデータを使用することで，全てのオフセット値の解析に成功した．したがって，1 段階目の電力解析が有効であることが分かる．

次に，2 段階目の電力解析を行った．2 段階目の電力解析では，秘密鍵 K の解析を行う．ここで，この実験では簡単化のために解析に使用するオフセット値を既知として扱う．実験結果を図 12 に示す．図 12 に示すように 4,000 波形のデータを使用することで全ての秘密鍵の解析に成功した．したがって，提案手法が有効であることが分かる．

また，1 段階目の電力解析と 2 段階目の電力解析において，正解と不正解の場合の相関係数について比較した．比較結果をそれぞれ図 13 と図 14 に示す．図 13 と図 14 の横軸は時間を，縦軸は相関係数を示している．図 13 に示すように，オフセット値の正解値において，相関係数のピークが表れていることが確認出来る．同様に，図 14 においても正解鍵において，相関係数のピークが表れていることが確認出来る．

最後に，解析に要した処理時間を表 4 に示す．表 4 は 1 段階目の電力解析において，全てのオフセット値の解析にかかった時間と，2 段階目の電力解析において，全ての秘密鍵の解析にかかった時間を示している．ここで，1 段階目の電力解析では，5,000 波形でオフセット値の解析に成功しているため，5,000 波形のデータを使用した場合の結果を示している．同様に，2 段階目の電力解析では，4,000 波形のデータを使用した場合の結果を示している．表 4 より，1 段階目の電力解析は 2,202[sec]の処理時間が，2 段階目の電力解析は 1,601[sec]の処理時間がかかっていることが分かる．

ここで本実験では簡単化のため，2 段階目の電力解析で使用するオフセット値を既知として扱ったが，提案手法では，オフセット値の解析のための 1 段階目の電力解析を，複数回行う．そのため，実際の攻撃には，「1 段階目の電力解析の処理時間 × 2 段階目の電力解析に必要なデータ数」の時間がかかる．表 4 の結果から，この処理時間を見積もると，2,202 × 4,000 = 8,808,000 [sec] = 2,447[h]となる．これ

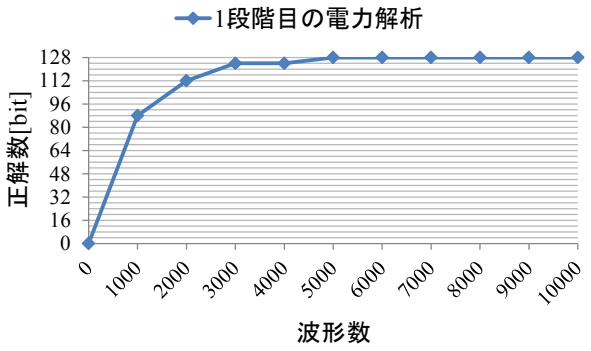

図 11　実験結果（1 段階目の電力解析）
Figure 11　Experimental result at the first stage.

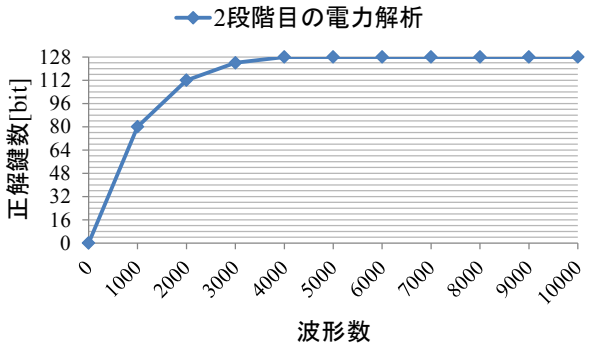

図 12　実験結果（2 段階目の電力解析）
Figure 12　Experimental result at the second stage.

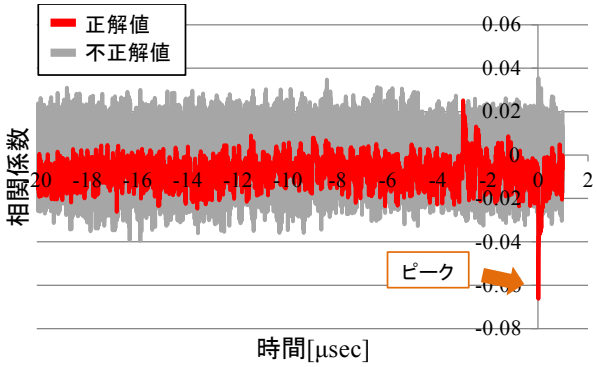

図 13　相関係数（1 段階目の電力解析）
Figure 13　Correlation coefficient at the first stage.

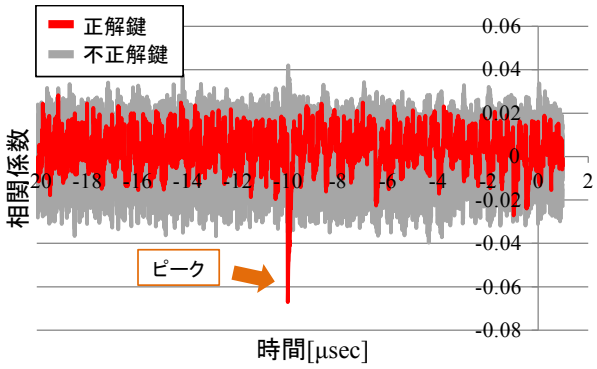

図 14　相関係数（2 段階目の電力解析）
Figure 14　Correlation coefficient at the second stage.

表 4　処理時間の比較
Table 4　Comparison of analytical time.

	1 段階目の電力解析	2 段階目の電力解析
波形取得[sec]	1,339	979
解析[sec]	863	622
合計[sec]	2,202	1,601

は，128bit の秘密鍵に対する $2^{128} = 3.4 \times 10^{38}$ 通りの総当たり攻撃よりも現実的である．また，テンプレート攻撃[10]のような強力な電力解析や，周波数電力解析[14]や鍵の組込み処理[15]などの解析効率の向上化手法を用いることで，解析に必要なデータ数を減らすことが可能であると考えられる．

5. まとめ

本研究では，改ざん検知暗号 Minalpher に対する電力解析を提案した．提案手法では，2 段階での電力解析を行うことで，秘密鍵の解析を行う．そして，FPGA を用いた評価実験により，提案手法の有効性を実証した．

今後は，提案手法をテンプレート攻撃のような強力な電力解析をベースとして適用することや，周波数電力解析や鍵の組込み処理などの解析効率向上手法を適用する予定である．

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] 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
[3] 佐々木悠，藤堂洋介，青木和麻呂，内藤祐介，菅原健，村上ユミコ，松井充，廣瀬勝一，高橋克己：改ざん検知暗号 Minalpher，暗号と情報セキュリティシンポジウム講演論文集，2E-1，pp.1–4，(2015)
[4] NIST Special Publication 800-38D, : Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC, (2007)
[5] Minematsu, K. : AES-OTR v2, (2015) http://competitions.cr.yp.to/round2/aesotrv2.pdf
[6] 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)
[7] 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)
[8] Kocher, P., Jaffe, J. and Jun, B. : Differential Power Analysis, Proc. of 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. of 6th Int. Workshop Cryptographic Hardware and Embedded Systems (CHES 2004), LNCS 3156, pp.16–29, Springer-Verlag (2004)
[10] Chari, S., Rao, R. J. and Rohatgi, P. : Template attacks, Proc. of 4th Int. Workshop on Cryptographic Hardware and Embedded Systems (CHES 2002), LNCS 2523, pp.13–28, Springer-Verlag, (2002)
[11] Federal Information Processing Standards (FIPS) Publication 197 : Advanced Encryption Standard (AES), U. S. Department of Commerce/National Institute of Standard and Technology (2001)
[12] CAESAR: Competition for Authenticated Encryption: Security, Applicability, and Robustness, http://competitions.cr.yp.to/caesar.html
[13] Research Institute for Secure Systems, AIST, : Evaluation Environment for Side-channel Attacks, http://www.risec.aist.go.jp/project/sasebo
[14] Gebotys, H. C., Ho, S. and Tiu, C. C. : EM analysis of Rijndael and ECC on a Wireless Java-based PDA, Proc. of 7th Int. Workshop on Cryptographic Hardware and Embedded Systems (CHES 2005), LNCS 3659, pp.250–264, (2005)
[15] Komano, Y., Shimizu, H. and Kawamura, S. : BS-CPA: Built-In Determined Sub-Key Correlation Power Analysis, IEICE Trans. Fundamentals, Vol.E93-A, No.9, pp.1632–1638, (2010)