Vol.2021-MBL-100 No.16
Vol.2021-UBI-71 No.16
Vol.2021-CDS-32 No.16
Vol.2021-ASD-21 No.16
2021/9/3

軽量認証暗号 SPARKLE の耐タンパ性評価

野崎佑典[1]　吉川雅弥[1]

概要：近年，小回路規模や低遅延，低消費電力で利用可能な軽量暗号が注目されている．また，現在 NIST では次世代の軽量暗号の標準規格を決めるプロジェクト Lightweight Cryptography（LWC）が実施されている．本研究で対象とする SPARKLE は NIST の LWC で Finalist に選ばれた軽量暗号である．一方で，暗号アルゴリズムの安全性に関して，サイドチャネル攻撃などの実装攻撃に対する耐タンパ性を検証することは非常に重要である．本研究では，SPARKLE を対象に，耐タンパ性に関する検討を行う．

キーワード：ハードウェアセキュリティ，軽量暗号，SPARKLE

Tamper Resistance Evaluation of A Lightweight Authenticated Encryption SPARKLE

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

Abstract: In recent years, lightweight block ciphers, which can be utilized in small circuit size, low latency, and low power, have attracted attention. In addition, NIST takes a Lightweight Cryptography (LWC) which decides the next-generation standard of lightweight cipher. The lightweight cipher Sparkle is one of the finalists in LWC. On the other hand, it is important to verify the tamper resistance against side-channel attacks. Therefore, this study evaluates the tamper resistance of a lightweight cipher Sparkle.

Keywords: Hardware security, lightweight cipher, SPARKLE

1. はじめに

組込み機器を含む様々な機器でセキュリティ技術が必要とされている．これらの機器の中には，回路規模やメモリサイズ，処理時間，消費エネルギーなどに関して実装制約が厳しいものも含まれている．そのため，小回路規模，低遅延，低エネルギーで実装可能な暗号技術である軽量暗号が注目されている．これまでに様々な軽量暗号が提案されており，現在米国立標準技術研究所（National Institute of Standards and Technology: NIST）では，次世代の軽量暗号の標準規格を決定する Lightweight Cryptography（LWC [1]）が実施されている．本研究で対象とする SPARKLE [2]は LWC に提出された軽量暗号であり，LWC の Finalist に選出されている．

暗号アルゴリズムの性能に関して，回路規模やレイテンシなどの実装性能に加えて，不正攻撃への安全性についても評価される．この安全性については，フォールト攻撃やサイドチャネル攻撃などの実装攻撃に対しても評価することが重要である [3][4][5][6][7]．フォールト攻撃は，暗号処理中に故意に演算の誤り（フォールト）を混入させて，このときに得られるフォールト入り暗号文と正規の暗号文を利用することで秘密鍵情報を解析する攻撃である．またサイドチャネル攻撃は，暗号回路の動作時における処理時間や消費電力，電磁波などのサイドチャネル情報を利用して秘密鍵を解析する攻撃である．LWC ではこれらの実装攻撃への安全性についても評価対象とされており，耐タンパ性評価は非常に重要である．

そこで本研究では，軽量認証暗号 SPARKLE の耐タンパ性を評価するための電力解析手法を提案する．そして，シミュレーション実験を行い，SPARKLE の耐タンパ性を評価する．

2. 準備

2.1 SPARKLE [2]

SPARKLE は NIST の LWC に提出された軽量認証暗号の一つであり，現在 LWC の Finalist に選出されている．LWC の提出要件では，AEAD 機能に加えてオプションとしてハッシュ関数の機能の実装が求められている．SPARKLE に関しては，SPARKLE をベースに AEAD 機能として SCHWAEMM（Sponge-based Cipher for Hardened but Weightless Authenticated Encryption on Many Microcontrollers）が，ハッシュ関数としては ESCH（Efficient, Sponge-based, and Cheap Hashing）が提案されている．

本研究では，特に認証機能と暗号化機能を持つ SCHWAEMM を対象とする．SCHWAEMM の概要を図 1 に示す．ここでは，鍵長が 128bit，ナンス長が 128bit のもの

1 名城大学
Meijo University

Vol.2021-MBL-100 No.16
Vol.2021-UBI-71 No.16
Vol.2021-CDS-32 No.16
Vol.2021-ASD-21 No.16
2021/9/3

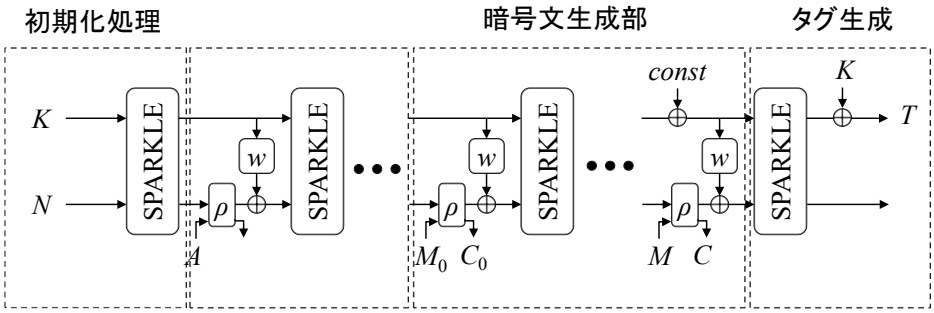

図 1　SCHWAEMM の概要

Figure 1　Outline of SCHWAEMM.

を例に説明する．図 1 に示すように，スポンジ構造の暗号アルゴリズムであり，SPARKLE を繰り返し適用することで，暗号化および認証用のタグの生成を行う．

ここで，SPARKLE では図 2 に示す置換処理を行う．図 2 の A_c はある定数値 c を利用した ARX Box Alzette による置換処理を示している．Alzette は 64bit の入力に対する置換処理を行う．この SPARKLE では，Alzette は 4 つあり，各計算結果に対して線形拡散層による転置処理を行う．

Alzette の詳細を図 3 に示す．Alzette は 4 ラウンドの処理で構成しており，各ラウンドでモジュラ加算処理と，XOR 演算，右ローテーション処理を行う．SPARKLE では，この Alzette と線形拡散層による処理を合計で 7 ラウンドまたは 10 ラウンド行う．ラウンド数については，初期化処理とタグ生成，Associated Date 部や暗号文生成部の最後のブロックでは，10 ラウンドの処理を行い，それ以外では 7 ラウンドの処理を行う．

2.2 電力解析

電力解析攻撃[3][4][5]は回路動作時の消費電力を利用して，暗号の秘密鍵を不正に解析する攻撃手法である．電力解析攻撃では，暗号処理時のデータ（暗号中間値）のハミング重み（Hamming Weight : HW）や，データレジスタにおける値の遷移（Hamming Distance : HD）を解析に利用する．

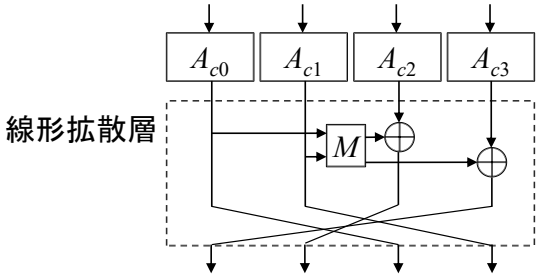

図 2　SPARKLE

Figure 2　SPARKLE.

具体的には，HW や HD と消費電力との線形な相関関係を利用する．HW を用いる解析を HW 型電力解析攻撃，HD を用いる解析を HD 型電力解析攻撃と呼ぶ．

代表的な電力解析攻撃には，差分電力解析（Differential Power Analysis : DPA [3]）や相関電力解析（Correlation Power Analysis : CPA [4]）などが提案されている．ここでは，DPA について説明する．DPA では，暗号中間値の HW やレジスタ遷移（HD）を計算する．この計算は，未知の鍵情報を候補値として与えることで行う．ここで，鍵候補が $n$bit の場合は 2^n 通りの計算を行う．次に，計算した HW や HD に基

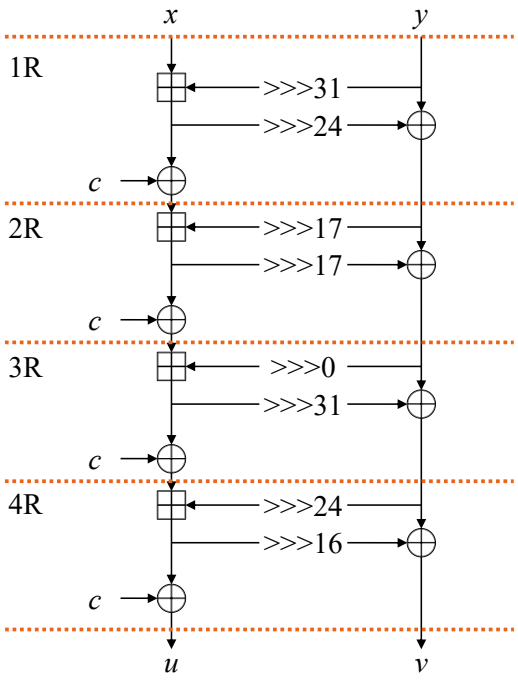

図 3　ARX Box Alzette

Figure 3　ARX Box Alzette.

Vol.2021-MBL-100 No.16
Vol.2021-UBI-71 No.16
Vol.2021-CDS-32 No.16
Vol.2021-ASD-21 No.16
2021/9/3

づいて消費電力波形を 2 つのグループに振り分ける．具体的には，HW や HD が大きいグループと小さいグループへの振り分けを行う．そして，各グループでの消費電力波形の平均値を算出する．最後に，各グループで算出した平均の消費電力波形の差分を計算し，差分電力波形を算出する．このとき，鍵の候補値が正しい値であり，HW や HD が正確に導出された場合，各グループには消費電力が小さい波形と，大きい波形がそれぞれ振り分けられるため，差分電力波形にはこの差がピークとなって現れる．一方で，鍵の候補値は間違っている場合は，このような差は生じないため，差分電力波形にピークは発生しない．そのため，DPA では，各鍵候補で差分電力波形を算出し，値が最大となる鍵値を正解の鍵として推定する．

3. 提案手法

本研究では，SPARKLE の耐タンパ性を評価するための電力解析手法を提案する．提案手法では，SCHWAEMM の初期化処理を対象とする．ここで，ナンス N は既知の値，秘密鍵 K は未知の値として扱う．提案手法では，初期化処理における SPARKLE の転置処理時におけるデータレジスタの遷移ビット数と消費電力との相関関係を解析へ利用する．

提案手法の概要を図 4 に示す．提案手法では，初期化処理において 2 回目に呼び出される SPARKLE を対象とする．ここで，1 回目の SPARKLE において，既知のナンス N を用いた計算結果は全て既知である．一方で，未知の秘密鍵 K に基づく計算結果は知ることができない．具体的には，2 回目の SPARKLE における A_{c2} と A_{c3} の入力値は既知である．また，2 回目の SPARKLE における A_{c0} と A_{c1} の入力値は未知である．ここで，A_{c0} と A_{c1} の入力値は N を用いた 1 回目の SPARKLE の処理結果（N_1 と N_2 とする）と，未知の値 K を用いた 1 回目の SPARKLE の処理結果（K_1 と K_2 とする）で計算できる．この計算式を以下に示す．

$$M(N_1) \oplus K_2 \tag{1}$$

提案手法では，2 回目の SPARKLE における Alzette の 1R 目のレジスタ遷移を解析に利用する．このとき 1R 目計算前のレジスタ値 reg_a と 1R 目計算終了後のレジスタ値 reg_b はそれぞれ未知の値である．2 回目の SPARKLE の Alzette の入力値を x, y とすると，レジスタ値 reg_a と reg_b は以下の式で計算できる．

$$reg\_a = x \tag{2}$$

$$reg_b = (x + (y >>> 24)) \oplus c \tag{3}$$

また，レジスタ遷移（HD）は下記で計算できる．

$$HD = reg\_a \oplus reg\_b \tag{4}$$

提案手法では，式(4)で導出した HD を利用した DPA を適用することで，秘密鍵に関連した K_2 の解析を行う．また，同様の解析を行うことで，K_1 の解析も行う．K_1 と K_2 を全て推定することができれば，Alzette の逆算処理によって，秘密鍵 K を全て推定する．

4. 評価実験

評価では，シミュレーションによる実験を行った．シミュレーションでは，特に SCHWAEMM の解析対象である，初期化処理における消費電力を算出した．具体的には，各ラウンド処理におけるデータの遷移（HD）をカウントし，

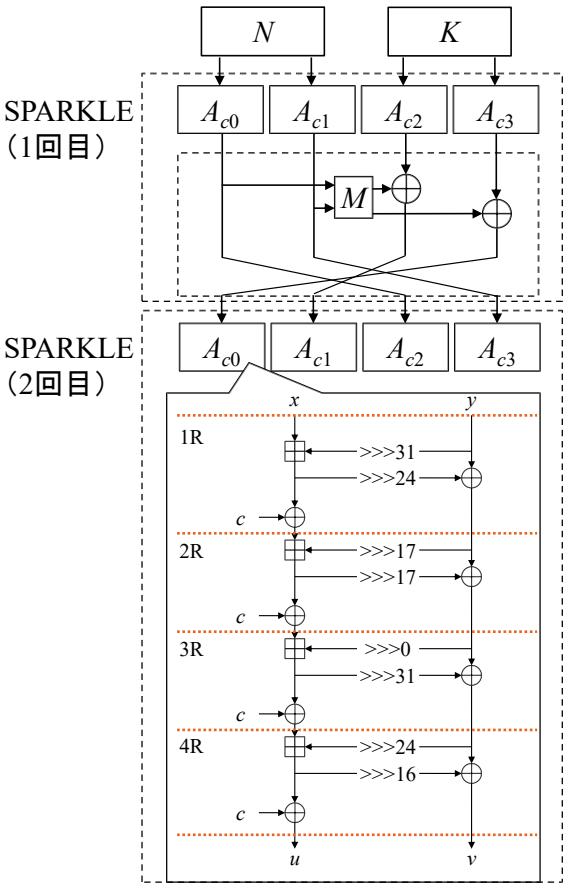

図 4　SPARKLE
Figure 4　SPARKLE.

Vol.2021-MBL-100 No.16
Vol.2021-UBI-71 No.16
Vol.2021-CDS-32 No.16
Vol.2021-ASD-21 No.16
2021/9/3

これを疑似的に消費電力としてシミュレートした．疑似生成した消費電力波形を図 5 に示す．実験では，この消費電力波形を 1,000 波形生成して利用した．

また，実験では正解の鍵値による計算によって，差分電力波形に差が生じるかどうかについて検証を行った．具体的には, 正解の鍵値に基づいて提案手法による計算を行い，HD を導出した．正解鍵を用いた場合の実験結果を図 6 に示す．図 6 の横軸は時間を，縦軸は差分電力をそれぞれ示している．図 6 に示すように，サンプル点 17 付近で大きな差分電力のピークが現れていることが確認できる．

また，ランダムな不正解の鍵を用いた場合の評価も行った．この実験結果を図 7 に示す．図 7 に示すように，ランダムな不正解鍵では差分電力波形のピークが現れないことが確認できる．以上から，提案手法によって SPARKLE の耐タンパ性が検証可能であると考えられる．

5. まとめ

本研究では，SPARKLE に対する耐タンパ性を検証するための電力解析手法を提案した．提案手法では，SCHWAEMM の初期化処理に着目した解析を行う．評価実験では，シミュレーションによる評価を行い，正解の鍵では差分電力波形にピークが現れることを確認した．

今後は，実際に鍵候補を試行した場合の耐タンパ性評価を行う予定である．また，実機を用いた評価や対策手法に関する評価なども行う予定である．

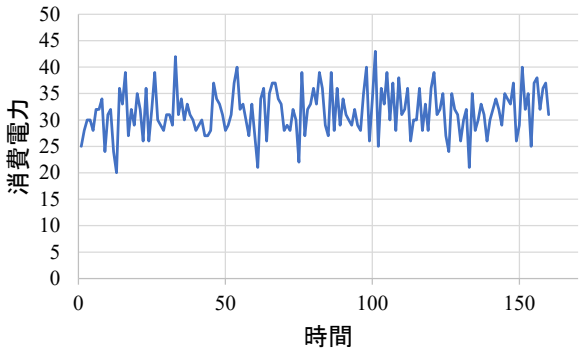

図 5　実験で使用した消費電力波形

Figure 5　Power consumption waveform for experiments.

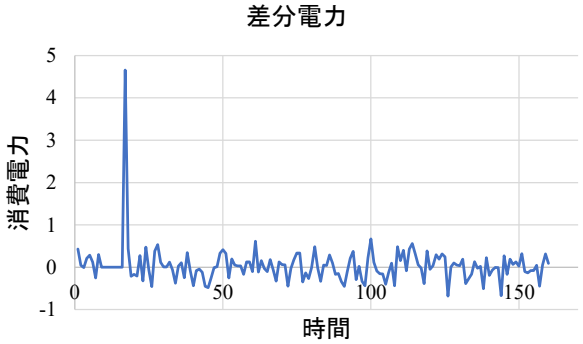

図 6　正解鍵を使用した場合の差分電力波形

Figure 6　Differential power waveform with correct key.

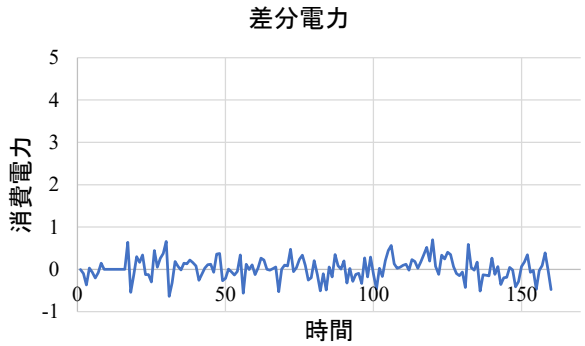

図 7　ランダムな不正解の鍵を使用した場合の差分電力波形

Figure 7　Differential power waveform with random incorrect key.

謝辞　本研究の一部は，JSPS 科研費 19K24357 の助成を受けたものです．

参考文献

[1] “Lightweight Cryptography”. https://csrc.nist.gov/Projects/lightweight-cryptography, (参照 2021-08-03).

[2] Beierle, C., Biryukov, A., Santos, L. C. dos, Großschädl, J., Moradi, A., Perrin, L., Shahmirzadi, A. R., Udovenko, A., Velichkov, V., and Wang, Q.: Schwaemm and Esch: Lightweight Authenticated Encryption and Hashing using the Sparkle Permutation Family, available from 〈https://csrc.nist.gov/CSRC/media/Projects/lightweight-cryptography/documents/finalist-round/updated-spec-doc/sparkle-spec-final.pdf〉

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

[4] 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).

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

[6] 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).

[7] 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).