L-009

軽量ブロック暗号における S-BOX マスキング保護の検討・評価
Implementation and evaluation of masked S-box on lightweight block ciphers

加納 広太† 吉川 英機‡ 神永 正博‡ 志子田 有光†
Kouta Kanou Hideki Yoshikawa Masahiro Kaminaga Arimitsu Shikoda

1. はじめに

近年の IoT デバイスの普及に伴って、IoT デバイスの秘密情報を保護するために軽量暗号の必要性が増している。軽量暗号については、電力解析攻撃および対策技術の検討が十分ではない。代表的な軽量暗号に PRESENT [1]があり、電力解析攻撃に対し、マスキング [2]を施した様々な実装法が提案されてきた。本研究では、PRESENT に対し、S ボックスへのマスキングに新たな改良を加え、対策による実装規模の増加に関する評価や CPA(Correlation Power Analysis)に対する実験結果について報告する。

2. PRESENT

PRESENT は CHES2007 で発表された軽量ブロック暗号の一種であり、64 ビットのテキストサイズと 2 つの異なる鍵サイズ(80 ビットまたは 128 ビット)の SPN 構造を持つ、対称暗号化アルゴリズムである(図 1)。鍵サイズが 80 ビットと 128 ビットのどちらでも処理は変わらない、また PRESENT には主に 31 ラウンドの処理があり、一つのラウンドには、ラウンド毎のラウンド鍵との排他的論理和である Add Round Key、非線形処理である S-Box layer、ビットの置換を行う Permutation layer がある。本研究では、80 ビットの鍵長の場合の PRESENT 暗号について検討する。

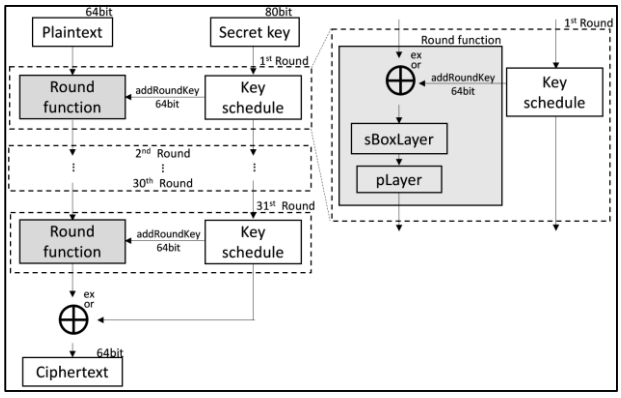

図 1　PRESENT ブロック図

3. 電力解析攻撃

電力解析攻撃とはサイドチャネル攻撃 [3]の一種であり、暗号化を行うデバイスで正規の手順を踏んで暗号化するときに発生する電力を測定、解析することで暗号化に用いられる秘密情報（秘密鍵）を推定することができるという攻撃手法である。電力解析攻撃にはいくつかの方法があり、電力の波形そのものから内部状態を把握する SPA(Simple Powering Analysis) [4]、消費電力を統計処理することで内部状態を推定する DPA(Differential Power Analysis) [4]、統計処理の手法にピアソンの相関係数を利用する CPA(Correlation Power Analysis)などが代表的である。DPA や CPA は暗号化デバイスが消費する電力がハミングウェイトモデルやハミングディスタンスモデルに比例するという仮定に基いている。この仮定から、Sbox などの秘密鍵を使用する処理と消費電力を統計処理することによって秘密鍵を推定することができるのである。本研究では CPA を用いて PRESENT に攻撃し、対策前と対策後で電力解析攻撃に対する耐性がどのように変化したかを述べる。

† 東北学院大学大学院 電子工学専攻
Tohoku Gakuin University Graduate School of Electronic Engineering
‡ 東北学院大学大学院 電気工学専攻
Tohoku Gakuin University Graduate School of Electrical Engineering

4. 対策

PRESENT 暗号は原理的に電力解析攻撃に対して抵抗がない。そこで本研究では、PRESENT 暗号に処理をいくつか追加することによって、電力解析攻撃から秘密情報を保護する方法を提案する。この対策の考え方は、処理の途中で生データが現れないようにすることである。PRESENT 暗号に追加する処理は 2 つある。まず一つは暗号処理の最初と最後で乱数による排他的論理和を行うこと。もう一つは暗号処理の Sbox layer で用いる Sbox を、乱数を用いたランダムなものに置き換えることである。このフローを図 2 に示す。

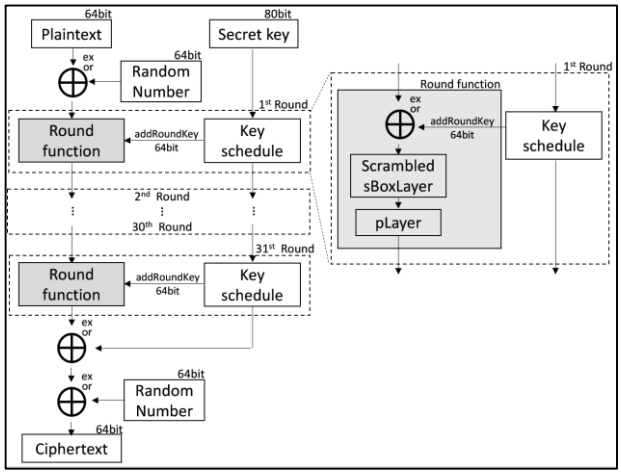

図 2　対策済み PRESENT ブロック図

暗号処理の最初と最後で排他的論理和を行うことで乱数による影響をリセットし、適切な方法で作成された Sbox を通して計算を行うことで、暗号計算の整合性を保ちながら暗号処理中に生データが現れるのを防ぐことができる。その結果、攻撃者は乱数を知らない限り、正しい統計処理を行うことができなくなるので、暗号デバイス中の秘密情報は守られる。図 2 で示した対策済み PRESENT のブロック図をアルゴリズムの形で表すと次のようになる。

(STEP1) Generate 64 bit random number R
(STEP2) Transform 16 S-boxes into S^R
(STEP3) state = plaintext xor R
(STEP4)
For i = 1 to 31
(STEP4-1) addRoundkey
(STEP4-2) SboxLayer（Scrambled）
(STEP4-3) pLayer
EndFor
(STEP5) addRoundkey
(STEP6) Output: ciphertext = state xor R

5. 実験環境

CPA システムは、主に３つの構成要素から成る。１つ目は暗号化装置に対してテキストを送出するパーソナルコンピュータ(PC)。２つ目はテキストを受けて、それを暗号化する暗号デバイス。３つ目は、暗号計算を行っている暗号装置の電力を測定するオシロスコープである。本研究では PC から暗号化装置へのテキスト送出には RS232C を介してシリアル通信を用いた。また、ランダムなテキストの作成、送信にはプログラム言語である Python を使用した。暗号計算は FPGA ボード上に実装した PRESENT 暗号を用いて行い、PC から送出されたテキストを暗号化するときに発生する漏洩電磁波を近磁界プローブによって測定し、その時の漏洩電磁波をオシロスコープ(Tektronix MSO4034)で取得した。PRESENT 暗号の暗号化が始まる直前に、トリガ信号を FPGA ボードの GPIO から送出し、それをオシロスコープのロジック・アナライザによって検知したタイミングを電力取得のタイミングとした。

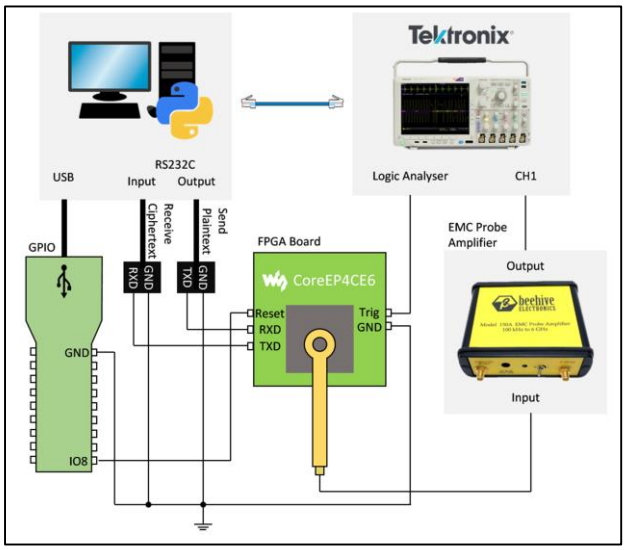

図３　測定システム

6. 実験結果

実験システムで取得した対策なしの PRESENT 実装暗号デバイスの消費電力データを CPA により解析した結果を図４に示す。図４からは統計処理の結果ピークが現れていることが確認でき、対策なしの PRESENT に対して理論に基づき CPA 攻撃が成立するということが確認できる。また、図５はマイクロコントローラ実装の PRESENT を CPA により解析した結果である。図５からもピークが現れていることがわかる。よって、PRESENT への CPA は実装デバイスに依らないということがわかった。

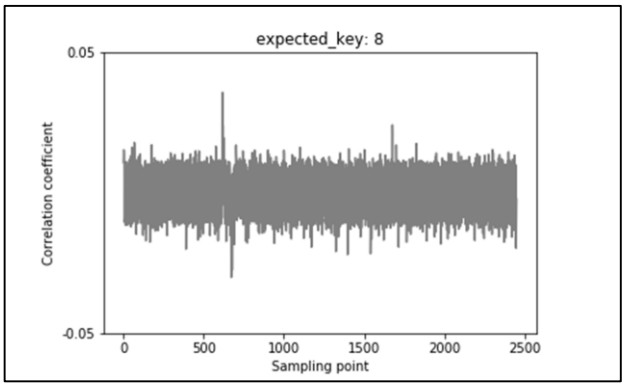

図４　CPA 結果（FPGA 実装）

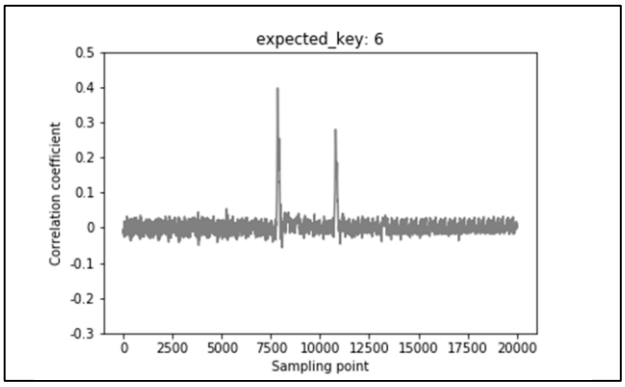

図５　CPA 結果（マイクロコントローラ実装）

7. おわりに

以上、市販の FPGA とマイクロコントローラを用い、我々が提案する S-BOX へのマスキング保護の原理と効果、および、今後実験による有効性の確認を行うための実験環境の構築と実験事例については解説した。更なる実験によるこのマスキング対策と効果、及び更なる攻撃に関する問題などについては講演時に補足させていただく。

謝辞

本研究は JSPS 科研費 JP17K00190 の助成を受けたものです。

参考文献

[1] A. Bogdanov, L.R. Knudsen, G. Leander, C.Paar, A. Poschmann, M.J.B. Robshaw, Y.Seurin, and C. Vikkelsoe, “PRESENT: An Ultra-Lightweight Block Cipher”, Lecture Notes in Computer Science, Vol.4247, pp. 450-466 (2007).
[2] S. Mangard, T. Popp, B. M. Gammel, “Side-Channel Leakage of Masked CMOS Gates”, Lecture Notes in Computer Science, Vol.3376, pp. 351-365, (2005).
[3] D. Agrawal, B. Archambeault, J.R. Rao, P. Rohatgi, “The EM side channel(s): Attacks and assessment methodologies”, Lecture Notes in Computer Science, Vol.2523, pp. 29–45, (2002)
[4] Paul Kocher, Joshua Jaffe, Benjamin Jun, “Differential Power Analysis”, Lecture Notes in Computer Science, Vol.1666, pp. 388-397 (1999).