L-006

SAKURA-X の FPGA に実装した LED に対する相関電力解析
Correlation power analysis for LED implemented in SAKURA-X FPGA

田中 隼人† 岩井 啓輔† 松原 隆† 黒川 恭一†
Hayato Tanaka Keisuke Iwai Takashi Matsubara Takakazu Kurokawa

1. はじめに

低コスト・低消費電力で動作可能な軽量暗号技術は，さまざまな小型デバイスで利用される可能性がある．その軽量暗号のひとつに LED（Light Encryption Device）[1]が提案されている．一方，暗号処理中の消費電力，電磁波，演算処理時間などの情報から暗号解読を試みるサイドチャネル攻撃があり，その危険性が報告されている[2][3].

相関電力解析[3]は有力なサイドチャネル攻撃のひとつであり，ハードウェア実装した鍵長 64bits の LED（LED-64）は，シミュレーションではあるものの，相関電力解析に成功している[4]．しかし，実際のハードウェアに実装した LED-64 の処理波形を用いて解析した文献及び同じくハードウェアに実装した鍵長 128bits の LED（LED-128）に対する相関電力解析に言及した文献も我々が知る限り存在しない.

そこで本稿では，サイドチャネル攻撃評価ボード SAKURA-X に搭載されている FPGA（Xilinx 社 Kintex-7）に実装した LED に対して相関電力解析を実施し，鍵を解析できることを示す.

2. LED への相関電力解析

LED は，2011 年に発表された軽量暗号であり，AES のようなラウンド構造で，鍵スケジュール部がなくハードウェア上での軽量化に特化している．ブロック長は 64bits，鍵長は，64bits（LED-64）または 128bits（LED-128）が選択可能である．図 1 に LED のアーキテクチャを示す.

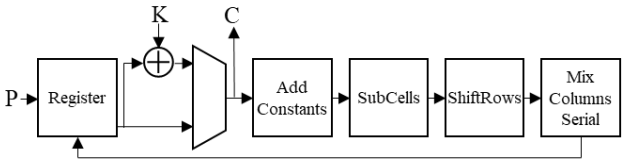

図 1　LED のアーキテクチャ

入力された平文 P は，4bits（ニブル）毎に分割され 4×4 の行列として演算される.

AddConstants は定数との XOR，SubCells は S-box による換字変換，ShiftRows は一定規則による行の右シフト，MixColumnsSerial は定められた行列との乗算である．LED-64 の場合，ラウンド数は 32 であり，鍵スケジュールはなく，鍵はそのまま平文と XOR されたのち，以降 4 ラウンド毎に同じく鍵と XOR されてゆく．LED-128 の場合，ラウンド数は 48 であり，鍵は前半と後半に分割され，まず平文と前半の鍵 64bits が XOR される．次に 4 ラウンド後に後半の鍵 64bits が XOR され，以降 4 ラウンド毎に交互に前半と後半の鍵が XOR されてゆく.

†防衛大学校　National Defense Academy

相関電力解析は，暗号モジュールのレジスタの遷移 bit 数（ハミング距離）と消費電力が比例するという関係を利用し，多量の平文及び電力波形を取得して解析を実施する.

本稿では，LED がラウンド実装されていることを前提とし，相関係数算出方法は，[4]において示された計算法を基として，以下のように解析をしてゆく.

LED-64 においては，平文中のある 4bits と関連する鍵 16bits を全て予測して計算した 1 ラウンド目の処理後の値 4bits とのハミング距離及びその際の電力波形を使用して相関係数を算出し，解析することにより鍵 16bits の値が判明する．着目する平文 4bits を変更しながら上記の解析を 4 回実施することにより鍵 64bits 全てを導出できる.

LED-128 においては，LED-64 に対して実施した解析を 2 回繰り返すことにより解析できる．まずは，LED-64 と同様 1 ラウンド目を解析することにより前半の鍵 64bits を導き出す（1 段階目の解析）．その正解鍵を用いて後半の鍵 64bits が演算される直前のラウンド（4 ラウンド目）まで計算をする．その値を用いて 1 ラウンド目と同様に 5 ラウンド目を解析することにより後半 64bits の鍵を導出できる（2 段階目の解析）.

3. 実験環境

実験は，まずサイドチャネル攻撃評価ボード SAKURA-X 上の FPGA（Kintex-7）に LED-64 及び LED-128 を実装した.

LED-64 は LED-128 の前半の鍵を導出することと同意となるため，本稿では LED-128 の実験の概要のみ示す．実験環境と機器構成についてそれぞれ表 1 と図 2 に示す.

なお LED は，消費電力が極めて小さいため，その実装では，暗号のコア部を 100 に複製して電力を増幅させて測定した.

表 1　実験環境

暗　号	LED
ブロック長	64bits
鍵　長	128bits
評価ボード	SAKURA-X
FPGA	Kintex-7
オシロスコープ	Agilent MSO9104A

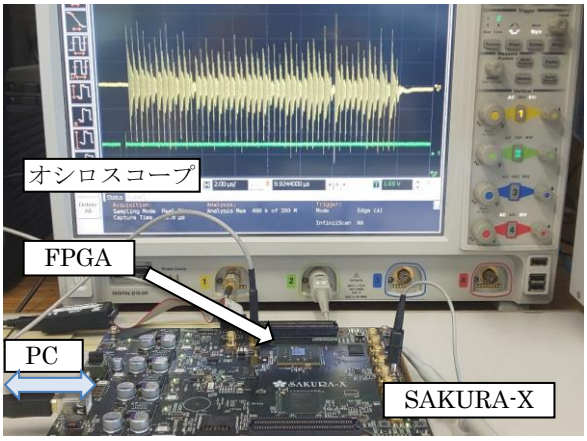

図 2　機器構成

4. 実験結果

1 段階目の解析では，1 ラウンド目を対象として解析した．測定波形数と正解鍵数の関係を図 3 に示す．図 3 から約 420 波形で前半の鍵 64bits 全ての鍵を導出できたことが分かる．LED-64 についても，本稿では結果は載せていないものの，LED-128 の 1 段階目の解析と同様の手法で鍵を導出できた．

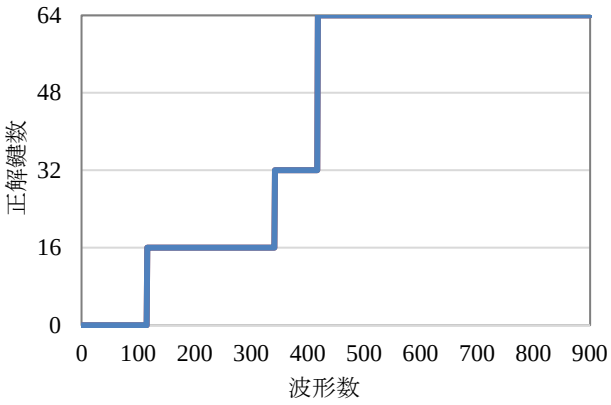

図 3　測定波形数と正解鍵数の関係
（1 段階目の解析）

2 段階目の解析では，1 段階目の解析で求めた前半の鍵を用いて，5 ラウンド目を対象として解析した．測定波形数と正解鍵数の関係を図 4 に示す．図 4 から約 860 波形で後半の鍵 64bits 全ての鍵を導出できたことが分かる．これにより 128bits 全ての鍵の導出ができたこととなる．

図 5 は，予測した 16bits の鍵と相関係数の関係の一例である．相関係数がひとつだけ突出している箇所があり，その鍵が一例の中の正解鍵である．測定波形数を増やすことにより不正解鍵の相関係数が低くなってゆき，相対的に正解鍵の相関係数が突出する．

LED-64 と LED-128 の労力や時間に関する解析コストについて，LED-128 は，LED-64 と同様の解析を 2 回繰り返すこととなるものの，2 段階目の解析の際は，1 段階目の解析で，すでに波形データの取得を終わらせているので，波形解析のみを行うこととなる．したがって，LED-128 の解析コストは，LED-64 の解析コストに波形解析コストを追加するのみである．

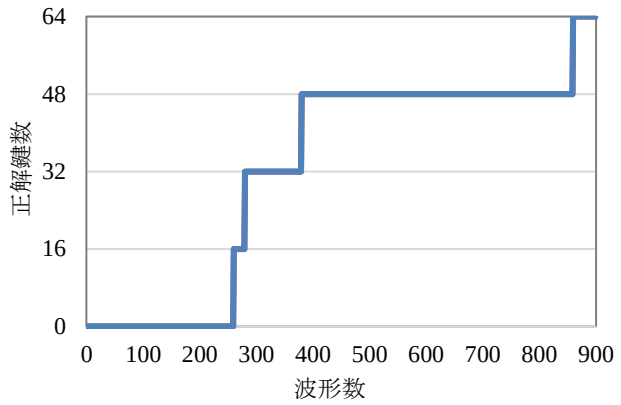

図 4　測定波形数と正解鍵数の関係
（2 段階目の解析）

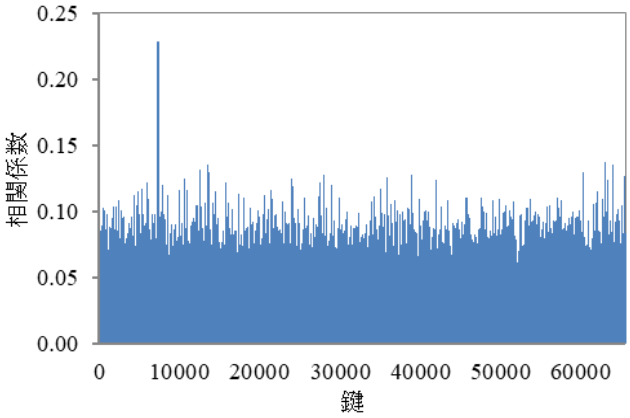

図 5　鍵と相関係数の関係

5. まとめ

本稿では，SAKURA-X の FPGA 上に実装した LED に対して相関電力解析を適用し，実機上でも鍵を導出可能であることを明らかにした．また，LED-128 について，相関電力解析においては，LED-64 の解析コストに波形解析のコストが追加されるのみであり，鍵長を増やすことによる相関電力解析に対する大きな耐タンパ性向上は見受けられず，短時間で解析できてしまう可能性があることを明らかにした．

参考文献

[1] J. Guo, T Peyrin, A. Poschmann, M. Robshaw “The LED Block Cipher,” Proc. of CHES, LNCS, vol. 6917, pp. 326-341, 2011.
[2] P.Kocher, J. Jaffe, and B.Jun, “Differential Power Analysis,” Proc. of CRYPTO’99, LNCS, vol. 1666,pp.388-397, 1999.
[3] E. Brier, C. Clavier, and F. Olivier, “Correlation Power Analysis with a Leakage Model,” Proc. of CHES 2004, LNCS, vol. 3156, pp. 16-29, 2004.
[4] ヴィッレ ウリマウル, 遠藤翔, 本間尚文, 青木孝文, “LED 暗号ハードウェアに対する相関電力解析とその対策,” 情報処理学会全国大会講演論文集, Vol.75th, No.3 pp.3.533-3.534, 2013.