

LED 暗号ハードウェアに対する相関電力解析とその対策

ヴィッレ ウリマウル 遠藤 翔 本間 尚文 青木 孝文

東北大学大学院情報科学研究科

1. はじめに

近年、RFID やスマートカードなど演算リソースの少ない機器や省電力が求められる機器への暗号技術の応用が期待されている。軽量暗号は、従来の暗号と比較して単純な構成要素からなり、そうした省リソース・省電力な組み込み機器に適した暗号として注目されている。近年、軽量暗号の一つとして LED (Light Encryption Device)[1] が提案され、従来と比べて小さな面積で実装可能であることが示されている。一方、暗号処理中の消費電力、電磁波、計算時間などの物理的情報を利用して暗号解読を試みるサイドチャンネル解析が問題となっている[2]。本稿では、代表的なサイドチャンネル解析の1つである相関電力解析 (Correlation Power Analysis: CPA)[3] を LED に対して適用し、秘密鍵を取得できることを示すとともに、その解析法に対する乱数マスキングに基づく対策法を示す。

2. LED に対する相関電力解析

LED 暗号は、64 ビットまたは 128 ビットの鍵長を持つブロック暗号アルゴリズムである。ここでは 64 ビットの LED に対する攻撃法を示す。LED のアーキテクチャを図 1 に示す。LED では、入力データを 4 ビットごとに分割し、 4×4 の行列として処理する。ラウンドごとに、データに定数を加える AddConstants、換字処理を行う SubCells、転置処理を行う ShiftRows、列内での置換を行う MixColumnsSerial の 4 つの処理を実行し、このラウンドを 32 回繰り返すことにより暗号文 C を得る。また、内部状態のデータと鍵 K との XOR を計算する addRoundKey は、4 ラウンドに 1 回実行される。

本稿の LED に対する相関電力解析では、64 ビットの鍵のうち 16 ビットを仮定し、消費電力を予測する。消費電力の予測にはハミング距離モデルを使用する。すなわち、CMOS 回路において、レジスタが状態を遷移するときに電力を消

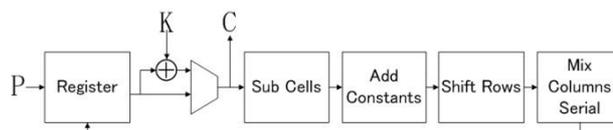


図 1: LED のアーキテクチャ

費することに着目し、あるクロックサイクルにおいて状態が遷移するレジスタの個数を予測することで消費電力を予測する。この個数は、連続するラウンド間のレジスタ値のハミング距離として求められる。本解析法では、レジスタの初期値として平文が格納されていることを利用して、平文と第一ラウンド終了後のレジスタ値のハミング距離から予測電力値を求める。

電力予測に用いる第一ラウンド後のレジスタ値の計算方法を以下に示す。図 1 における第一ラウンド終了時のある 4 ビットレジスタの値を i_n ($0 \leq n \leq 15$) とする。また、秘密鍵 4 ビットの値を k_n ($0 \leq n \leq 15$) で表す。このとき、レジスタ i_0 — i_3 の値はそれぞれ式(1)—(4) で表される。

$$i_0 = 4 \times S(p_0 \oplus k_0) \oplus 1 \times S(p_5 \oplus k_5 \oplus 1) \oplus 2 \times S(p_{10} \oplus k_{10}) \oplus 2 \times S(p_{15} \oplus k_{15}) \quad (1)$$

$$i_1 = 4 \times S(p_1 \oplus k_1) \oplus 1 \times S(p_6 \oplus k_6) \oplus 2 \times S(p_{11} \oplus k_{11}) \oplus 2 \times S(p_{12} \oplus k_{12}) \quad (2)$$

$$i_2 = 4 \times S(p_2 \oplus k_2) \oplus 1 \times S(p_7 \oplus k_7) \oplus 2 \times S(p_8 \oplus k_8 \oplus 2) \oplus 2 \times S(p_{13} \oplus k_{13} \oplus 1) \quad (3)$$

$$i_3 = 4 \times S(p_3 \oplus k_3) \oplus 1 \times S(p_4 \oplus k_4 \oplus 1) \oplus 2 \times S(p_9 \oplus k_9) \oplus 2 \times S(p_{14} \oplus k_{14}) \quad (4)$$

ここで、 p_n ($0 \leq n \leq 15$) は、64 ビットの平文の各 4 ビットの値を示す。

各 16 ビットの鍵を推定するアルゴリズムを Algorithm 1 に示す。ここで、平文数を n 、使用した平文の組を P 、測定した電力波形の組を T とする。まず、 i_0 — i_3 (式 (1)—(4)) の一つに注目し、その中に含まれる平文 16 ビットをランダムに変化させて消費電力を測定する。平文中のその他のビットは 0 に固定する。一方、注目した i に含まれる 16 ビットの鍵を kg として予測して当該 i の値を求め、対応する平文とのハミング距離 (予測電力値 H_{kg}) を導出する。

Alg. 1 Proposed CPA algorithm

Input: Plaintext array P , Power trace array T
Number of plaintexts n

Output: Estimated key k

```

for  $kg = 0 \dots 65535$ 
  for  $j = 0 \dots n$ 
     $H_{kg}[j] \leftarrow \text{Hamming distance}(P[j], i_x(P[j], kg))$ 
  end for
   $Co[kg] \leftarrow \text{correlation}(H_{kg}, T)$ 
end for
 $k \leftarrow \text{index}(\max(Co))$ 
return  $k$ 

```

次に、予測電力値と測定した電力波形との相関値 Co を求める。16ビット全て（65,536通り）の鍵候補に対して相関値を求めると、正しく鍵を予測した場合に予測電力値と実測値に最も高い相関値が得られると予想される。そこで、最も高い相関値を得た予測鍵を秘密鍵の推定結果 k とする。ここでは、16ビットごとの総当たり攻撃で $i_0 \sim i_3$ それぞれに含まれる鍵の16ビットの部分を探るため、鍵の探索空間は 2^{64} から 2^{18} ($=2^{16} \times 4$) に縮小できる。この程度の鍵空間であれば一般的なPCを用いても数分程度で探索が可能となる。

3. 相関電力解析のシミュレーション

上記相関電力解析の論理シミュレーション実験を実施し、提案攻撃で秘密鍵を取得できることを確認した。

シミュレーションでは、Algorithm 1において、電力波形 T の代わりにシミュレーションにより求めた電力値を用いる。図2にシミュレーションの結果を示す。図の最も高い値は予測した鍵の16ビットが秘密鍵の一部と同一なときである。このシミュレーションを i_0 から i_3 まで計4回実行することにより、式(1)–(4)に含まれる鍵64ビット全てを推定できた。

4. 電力解析攻撃への対策

乱数マスキングを用いた上記電力解析への対策を実装し、その効果を確認した。乱数マスキングでは、マスクされる値を x 、マスク値を m とすると、レジスタに $x \oplus m$ を保存することにより、消費電力と値の中間値の相関を隠ぺいすることが可能となる [4]。ここでは、図1中のレジスタに乱数マスクを施したLEDを実装し、CPAを行った。図3にCPAによる相関値を示す。正解鍵に対応するピークが表れておらず、対策により秘密鍵を推定できないことが分かる。

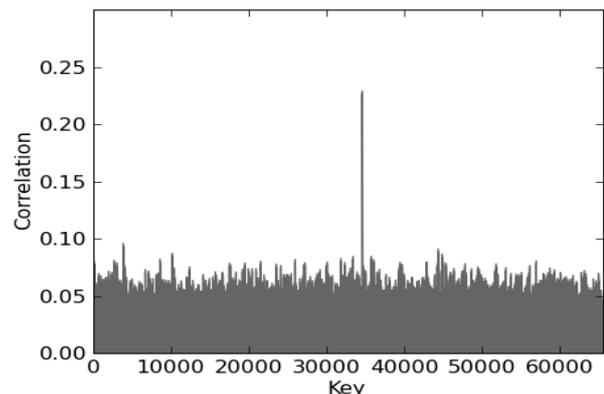


図2：推定された鍵

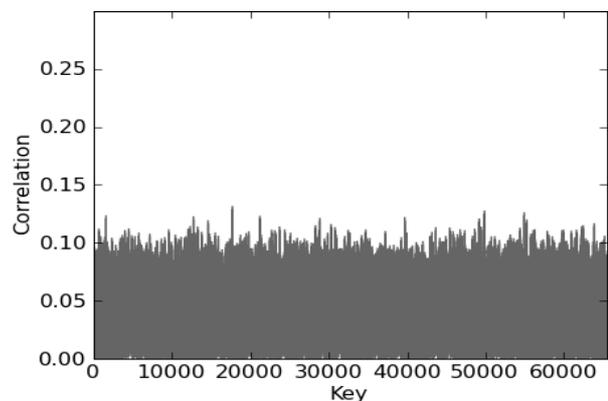


図3：マスクを用いたLED暗号へのCPAにおける相関値

5. まとめと今後の課題

本稿では、LEDへの相関電力解析の適用法について述べ、秘密鍵を短時間で取得できる可能性があることを示した。また、乱数マスキングによる対策を適用し、上記の攻撃を防止できることを示した。今後の課題としては、他のサイドチャンネル解析に対するLEDの安全性評価が挙げられる。また、本解析法の他の軽量暗号への適用の可否も検討課題である。

参考文献

- 1) J. Guo, T. Peyrin, A. Poschmann, M. Robshaw “The LED Block Cipher”, Proc. CHES, Lecture Notes in Computer Science, vol. 6917, pp. 326-341, 2011
- 2) P. Kocher, J. Jaffe, and B. Jun, “Differential Power Analysis”, Proc. CRYPTO '99, Lecture Notes in Computer Science, vol. 1666 pp.388-397
- 3) E. Brier, C. Clavier, F. Olivier, “Correlation power analysis with a leakage model”, Proc. CHES, Lecture Notes in Computer Science, vol.3156, pp.16-29,2004.
- 4) M. Akkar, C. Giraud “An Implementation of DES and AES, secure against some attacks”, Proc. CHES, Lecture Notes in Computer Science, vol. 2162, pp.309-318, 2001