C-014

対策回路に対するハードウェアトロイの検討
Hardware Trojan for countermeasure circuit

吉田　将之†，佐藤　隆亮†(名城大学)，熊木　武志‡(立命館大学)，吉川　雅弥*(名城大学)
Masayuki　Yoshida，　Satoh　Ryusuke，　Takeshi　Kumaki，　Masaya　Yoshikawa

1. はじめに

クレジットカードやキャッシュカードなどに用いられている暗号は，計算量的にその安全性が保障されている。しかし，ハードウェアに実装された場合，暗号処理中の消費電力や漏洩電磁波などの 2 次的な情報を用いて，秘密情報（鍵情報）を推定できることが報告されている。そのため，このような不正な攻撃に対する対策回路がいくつか発表されている。

一方で，LSI の製造時に，悪意のある攻撃回路を通常の回路に組み込むハードウェアトロイの問題が近年指摘されている[1]。これまでハードウェアトロイに関する先行研究では，基本的な動作原理について報告されている。そこで，本研究では暗号回路の電力解析攻撃に対する対策回路におけるハードウェアトロイを新たに考案して，シミュレーション実験を通して，対策回路の脆弱性を評価する。これまでに，本研究で提案する対策回路に対するハードウェアトロイの研究は見当たらない。

2. 準備

2.1 ハードウェアトロイとは

ハードウェアトロイとは，LSI 製造過程で LSI 内部に直接組み込まれ，攻撃者が予め定めた発動条件を満した場合，トリガがかかり，ユーザーに気づかれずに破壊工作を行うハードウェアのウィルスのことである。ここでトリガとは，回路の状態や信号線の値が，攻撃者が定めた発動条件を満たしたかどうかを判定する回路のことであり，発動条件を満たされた場合は，個人情報や機密情報の漏洩やシステムの停止，LSI の破壊など攻撃者が設定した攻撃動作を実行する。

2.2 相関電力解析(CPA)

CPA とは電力解析攻撃の一つであり，レジスタが遷移する際のハミング距離 H と消費電力 W に対して，式(1)に示すピアソンの相関係数を求め，相関係数 $\rho_i(W, H_i^{\hat{k}})$ を最大にする鍵の値が正解鍵であると推定する方法である。

$$\rho_i(W, H_i^{\hat{k}}) = \frac{\frac{1}{N}\sum_{n=1}^{N}\left[W_n - \overline{W}\right]\left[H_{n,i}^{\hat{k}} - \overline{H}_i^{\hat{k}}\right]}{\sqrt{\frac{1}{N}\sum_{n=1}^{N}\left[W_n - \overline{W}\right]^2}\sqrt{\frac{1}{N}\sum_{n=1}^{N}\left[H_{n,i}^{\hat{k}} - \overline{H}_i^{\hat{k}}\right]}} \quad (1)$$

W ：消費電力　H ：ハミング距離　N ：消費電力波形数
$\overline{W}$ ：平均消費電力波形　$\overline{H}$ ：平均ハミング距離

ピアソンの相関係数は，単位はなく，-1~1 の間の実数値を取り，絶対値が 1 に近づくほど，相関が高い。

3. 提案手法

本研究では電力解析攻撃に対する対策回路として，現在最も耐性が高い回路の 1 つである Threshold Implementations (TI)[4]を用いる。TI は標準暗号 AES を対象に，乱数マスクを用いる CPA の対策手法であり，秘密分散と並列計算をベースとしている。図 1 に TI の回路ブロック図を示す。TI では図 1 に示すように入力が 4 線式の回路構造になっており，入力された値と乱数生成器から出た値を用いて，4 分割され，最終ラウンドの XOR の部分でアンマスクされている。

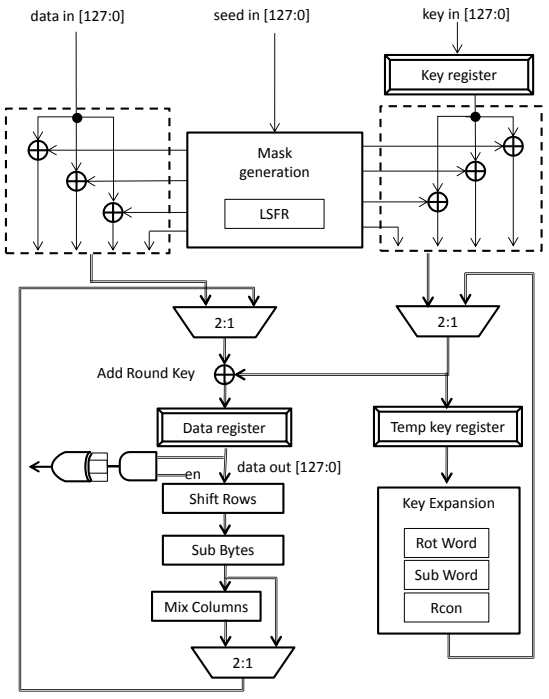

図 1 AES-TI 回路

† 名城大学 大学院理工学研究科 情報工学専攻,〒468-8502 愛知県名古屋市天白区塩釜口 1-501. Department of information Engineering Graduate School ofScience and Technology Meijo University 1-501, Shiogamaguchi, Tenpaku-ku, Nagoya-shi, Aichi, 468-8502 Japan
*名城大学 理工学部 情報工学科,〒468-8502 愛知県名古屋市天白区塩釜口 1-501. Department of information Engineering Faculty of Science and Technology Meijo University 1-501, Shiogamaguchi, Tenpaku-ku, Nagoya-shi, Aichi, 468-8502 Japan
‡ 立命館大学 理工学部, 〒525-8577 滋賀県草津市野路東 1-1-1. Department. of Science and Engineering, Ritsumeikan Unibersity, Noji-Higashi 1-1-1, Kusatsu, Shiga

この対策回路に対して，本研究では，直接秘密鍵を導出するのではなく，乱数マスクを無効化することで，電力解析攻撃を可能にするハードウェアトロイを導入する。具体的には，暗号処理が終了した直後にデータレジスタの値を強制的に all 0 にリセットし，乱数生成器で作られる乱数を 0 に強制変更する。これによち，Plain Text(以下 PT)とリセットしたレジスタ(初期値'0')は，攻撃者にとっては即知なので，K0 を 2^8 通り予想する（試行する）ことで，PT^K0 が予想することができ，その時のビットの数に応じて消費電力に相関を見つけることができるため，鍵を特定することが可能である．

さらに，提案手法では，ハードウェアトロイを発動させるトロイトリガの条件は，図 2 に示すような 2 つの状態を用いることで，攻撃者以外にトロイが発見されることを防ぐ。具体的には，入力される PT の最上位 8 ビットがすべて 1 の場合，通常状態からトロイが発動可能な状態に遷移し，暗号処理終了と共にハードウェアトロイが発動する形となっている。ただし，ハードウェアトロイが発動するには，トロイ状態にあり，かつ，入力される PT の最下位ビットが 1 でなければハードウェアトロイを維持できない，すなわち，それ以外の場合は，通常状態に戻るようになっている。このように，提案手法では，LSI 製造後の通常の機能テストでは，仕様書通りの動作（暗号処理）を行い，電力解析攻撃に対する耐性評価（耐タンパ性検証）[2]においても，トロイが検出されなくい。

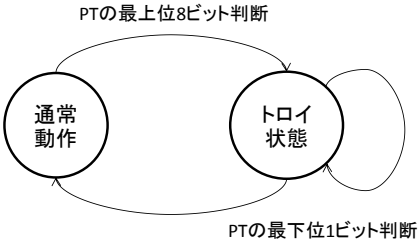

図 2 状態遷移

4. ハードウェアトロイの耐性評価

4.1 実験要領

提案するトロイの脅威を評価するために評価実験を行った。評価実験では，VerilogHDL でトロイを組み込んだ TI を記述し，消費電力データとしては PrimeTime を使用した。また，評価実験では，(1)通常の耐タンパ検証と同様にランダムに入力した PT を用いる場合と，(2)常にハードウェアトロイが発動する PT を入力した場合の 2 種類の PT を使い耐性評価を行った。ランダムに入力した PT に対しては 11CLK 目を対象に CPA の攻撃を行う。これは，LSI 製造過程の機能テストを行う際に，検査する人が攻撃者によってハードウェアトロイを回路に組み込まれていないと想定した上で耐性評価である。一方，常にハードウェアトロイが発動する PT に対しては 1CLK 目を対象に CPA の攻撃を行う。これは，攻撃者がハードウェアトロイを組み込まれた回路を事前に手に入れていると仮定し，即知からビット数に応じて消費電力に相関を見出すことがわかっていると想定した上で耐性評価を行う。

4.2 実験結果

評価実験の結果を図 3 に示す。図 3 で「PTp」はランダムに入力した PT に対して CPA を行った結果であり，「PTp_tro」は常にハードウェアトロイが発動する PT に対して CPA を行った結果を示している。図 3 に示すように，ランダムに入力された PT は，正解鍵が最高でも 1 つしか鍵が導出されておらず，他の文献で報告されている TI と同等の耐性を実現している。

一方で，トロイを発動させた場合では，全ての鍵が特定できた。このように，本研究で提案するハードウェアトロイは，攻撃者がハードウェアトロイを組み込んだ回路を入手したら容易に鍵が特定できるだけでなく，通常の機能検証や耐タンパ検証では，ハードウェアトロイを検出することが出来ない。

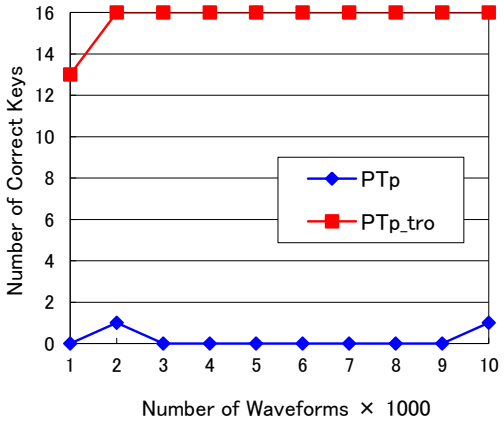

図 3 異なる PT の鍵導出個数

5. まとめ

本研究では，電力解析攻撃に対する対策回路に対するハードウェアトロイを考案し，評価実験を通して，その脅威を実証した。今後は，実機評価を行う予定である。

謝辞

本研究は JST,CREST「ディペンタブル VLSI システム基盤技術」の研究の一環として行われた。また，東京大学大規模集積システム設計教育センターを通し，シノプシス者の協力で行われたものである。関係各位に感謝する。

参考文献

[1] 熊木武志，望月陽平，藤野毅,「暗号処理用 LSI に組み込まれたハードウェアトロイに関する研究」，信学技報，vol. 111, no. 328, CPSY2011-46, pp. 21-26, (2011-11)

[2] 吉川雅弥，浅井稔也，汐崎充，藤野毅「上流設計工程でのサイドチャネル攻撃に対する耐タンパ検証手法とその評価」，電気学会論文誌C，Vol.131, No.11, pp.1940-1949, (2011-11)