3T-1

INSTAC-8を用いたサイドチャネル攻撃に関する一考察

和田　崇臣†　甲斐切　皇男†　岩井　啓輔†　黒川　恭一†

防衛大学校情報工学科†

1　はじめに

情報化社会が発達した現在、通信のセキュリティを確保するために、暗号機能を搭載した製品（暗号デバイス）が利用されている。

利用される暗号の安全性評価のために、暗号攻撃法とその対策の研究が盛んに行われている。それらの研究の一つとしてサイドチャネル攻撃に関するものがある。従来の研究は暗号アルゴリズムの数学的安全性に関するものであった。これに対して、サイドチャネル攻撃は、デバイスが暗号化処理を行う際の計算時間や電力消費量などの入出力以外の外部から観測可能な漏洩情報を利用して、鍵を解読する攻撃方法である。理論上安全と考えられていた暗号であっても、デバイスへの実装においてサイドチャネル攻撃への対策を施さなかった場合、容易に鍵が解読されるおそれがある。

近年盛んに様々なサイドチャネル攻撃の手法やその対策案が論文で発表されているが、それぞれの実験評価環境が統一されていないために、攻撃の脅威や対策案の客観的な評価ができないという問題がある。そこで、（財）日本規格協会　情報技術標準化研究センター（INSTAC）耐タンパー性調査研究委員会から業務を受託した東芝が、8bit　CPU を搭載した評価プラットフォーム（INSTAC-8）の使用策定し、この使用に準拠した基板を作成した。[1]

我々は独立行政法人　情報処理推進機構（IPA）の委託を受け、INSTAC-8 を用いたサイドチャネル攻撃に関する検証を行った。今回はサイドチャネル攻撃の中でも、暗号デバイスの消費電力を用いて鍵を解読する電力差分解析（DPA）に着目した。

Side-channel Attack for cryptograph implemented on INSTAC-8

†Takatomi WADA, Kimio KAIKIRI, Keisuke IWAI, Takakazu KUROKAWA

†Department of Computer Science, National Defense Academy

2　INSTAC-8 の概要

INSTAC-8 は CPU として Zilog 社 Z80 を搭載している。メモリ（RAM 及び ROM）、プログラマブルカウンタと、RS232C インターフェースを備えている。ROM は 28pin の DIP タイプソケットを利用しており、利用する暗号ソフトウェアを容易に変更できる仕組みとなっている。

INSTAC-8 は、消費電力に関するサイドチャネル攻撃の追試験を行う事を考慮された仕様となっており、CPU 単体の消費電力と基板全体の消費電力を測定することができる。

3　DPA の概要

DPA は、Kocher によって考案された攻撃手法で、暗号デバイスの消費電力を測定することで秘密情報を解析する手法である。[2]

DPA は以下のようにして秘密情報を推定する。まず、攻撃者は複数の入力（平文）に対する DES 実行時の消費電力波形を測定する。次に各入力時の中間データ（以下では参照値）を出力データから計算する。 鍵候補について、各入力時の消費電力は警を、その入力時の参照値を基にグループ分けする。各グループの消費電力波形を平均化し、グループ間の平均消費電力波形の差分を取る。測定した消費電力波形には秘密鍵に関する情報も含まれており、参照値を用いて求めた平均消費電力波形の差分のうち、いずれか一つの鍵候補に対しては大きな差分を持つ。すなわち参照値と消費電力波形の間に強い相関を持つものがあり、これが内部で使用されている部分鍵である。それ以外の鍵候補の場合は参照値と消費電力間に相関がないため、平均消費電力波形の差分は小さくなる。藤崎らは INSTAC-8 を用いて DES 実装に対する DPA 実験を行っており、DPA 対策が施していない実装の場合、部分鍵の推定が可能であることを示している。

4　測定

我々は今回、INSTAC-8 に共通鍵暗号を実装し、DPA 実験を行うこととした。まず、6bit の平文と鍵との排他的論理和をとり、その後、置換表を通り 4bit の暗号文が出力されるという簡易な暗号を INSTAC-8 に実装した。置換表は DES の S-BOX1 である。この簡易暗号に対して DPA を実験した。

測定に利用した機器は、（A）デジタルオシロスコープ、（B）波形収集およびデータ解析用 PC、（C）定電圧定電流安定化電源を用いた。測定環境を図 1 に示す。

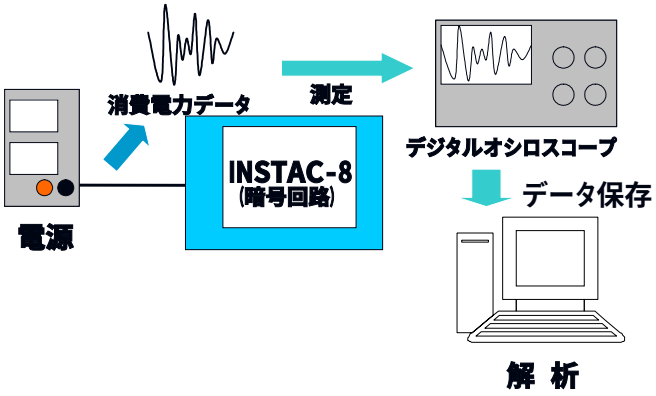

図 1　測定環境

ROM 上に繰り返し実行される簡易暗号のプログラムを書き込み、実行中の CPU の消費電力を測定した。毎暗号化の開始ポイントを明確にするために、プログラム内にデジタルオシロスコープ用のトリガとなりうる信号を出力するコードを埋め込んでいる。測定した図 2 のような波形は 10Base-T Ethernet を介して PC に取り込み、解析を行った。

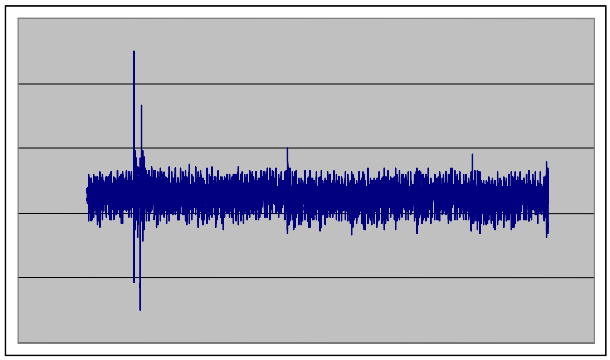

図 2　測定した電力波形

解析の結果を図 3 に示す。この図において濃い線は推定した鍵が正しかった時の電力差分トレースであり、薄い線が推定した鍵が誤っていた時の電力差分トレースの一つである。図に示した通り電力差分のトレースの変動の差から正しい鍵を推定することが可能であることを確認できた。

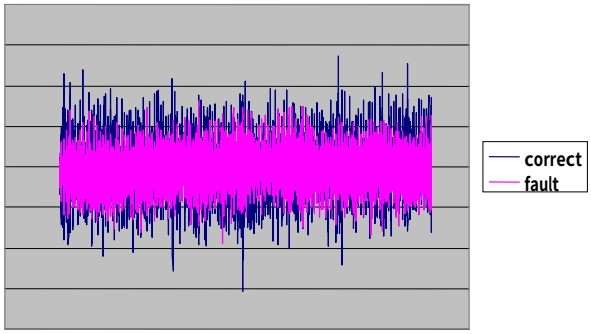

図 3　簡易暗号の電力差分トレース

5 まとめ

本研究では、INSTAC-8 に実装した簡易な暗号に対する DPA を行った。その結果、鍵と消費電力に強い相関関係があることが確認できた。

今後は他の暗号を実装し、データの収集、解析を行うとともに、DPA に対する有効な対策の検討を行っていく。

参考文献

[1]藤崎　浩一　友枝　裕樹　三宅　秀享　駒野　雄一　新保　淳:“8bitCPU を対象とした電力解析用評価環境の開発と実証実験”,信学技報 ISEC2004-55，2004.

[2] P. Kocher, J. Jaffe and B. Jun, Differential Power Analysis, Crypto99.