3T-2

# FPGA に実装された暗号回路に対するサイドチャネル攻撃

後藤　兼人† 岩井　啓輔† 黒川　恭一†

防衛大学校情報工学科†

## 1 はじめに

情報保護や個人認証などに暗号が一般的に使用されているが,これらの暗号に対する攻撃手法としてサイドチャネル攻撃と呼ばれるものが近年注目されている.これは,従来の暗号に対する攻撃とは異なり,実際に暗号デバイスが動作する際のサイドチャネル情報（漏洩情報）を用いて攻撃を行う手法である.これまで,IC カードに実装された暗号に対する電力解析などのサイドチャネル攻撃は多数行われているが,FPGA に実装された暗号回路に対しての攻撃例は少ない.

そのような中で,FPGA に対する最初の電力解析に関する成果[1] が報告されているが,未だ細部は不明な点が多い.今回,FPGA に実装された暗号の解析を念頭に,必要な環境を整備し,サイドチャネル攻撃を行った.

## 2 サイドチャネル攻撃

### 2.1 概要

実際に暗号を使用する場合,暗号化を行う際に暗号デバイスから各種の情報が漏洩している.それらの漏洩情報としては,暗号デバイスの消費電力や暗号化時間,発生する電磁波などである.サイドチャネル攻撃は,これまでの暗号理論では考慮されていなかったこれらのサイドチャネル情報を利用して暗号を解析しようとするものである.サイドチャネル攻撃には,消費電力を利用する電力解析,暗号デバイスの動作時間を利用するタイミング攻撃,暗号デバイスから外部に放射される電磁波を利用する電磁波解析,そして IC 内の回路に人為的に故障を発生させて正常な出力と故障時の出力の差を利用する故障解析などがある.

本研究では,サイドチャネル攻撃の中でも強力であるとされている電力解析[2] に着目した.回路は一般的に 0 よりも 1 を出力する場合の方が電力を消費する.また,実行中の演算や使用しているデータの値によっても消費電力は変化する.この消費電力から,内部で行われている演算を推測して鍵情報を解析しようとするものである.消費電力の解析手法は,消費電力データをそのまま解析に使用する単純電力解析と,消費電力データを統計的に処理して解析に使用する電力差分解析とに分けられる.

### 2.2 電力差分解析 (Differential Power Analysis: DPA)

消費電力には,暗号鍵に関連して暗号デバイスに一時的に蓄えられた秘密パラメータ(内部変数)に関する情報も含まれている.一般的にこれらの情報はノイズ等により打ち消される場合が多い.電力差分解析は,消費電力を統計的に解析することで,消費電力データに含まれるノイズの影響を取り除いて暗号鍵の推定を行うものである.単純電力解析とは異なり,統計的な解析を行うため,1,000 回程度の測定が必要とされる.

DES 暗号の場合,最終ラウンドで S-box から出力されるビットを推定すると,6 ビットの探索を 8 個の S-box について行うことで拡大鍵が推定できるため,残りの 8 ビットのみを全数探索するか,さらに 15 ラウンドの出力に対して電力差分解析を行うことで全ての鍵を求めることができる.

Kocher らは,電力差分攻撃により IC カードに実装された DES 暗号に対して解析を行い,鍵の推定に成功している.

## 3 解析システムの構築

### 3.1 解析システムの概要

本研究では,まず電力解析のための環境を整えた.解析システムの全体図を図 1 に示す.

システムの構成は,暗号処理を行う暗号処理ボード,ボードへの電源とデジタルオシロスコープ

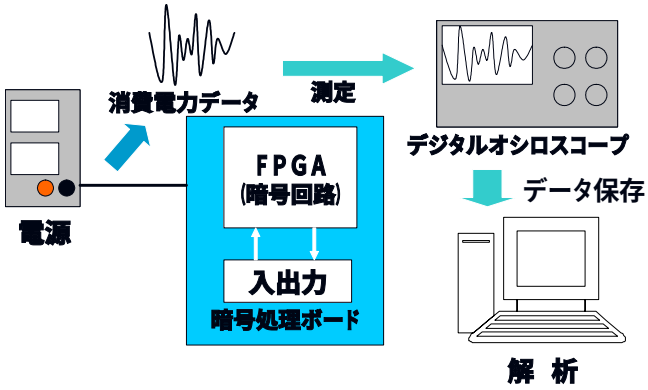


図 1　システムの全体図

Side-channel Attack to cipher circuit implemented on FPGA
†Kaneto GOTO, Keisuke IWAI, Takakazu KUROKAWA
Department of Computer Science, National Defense Academy

及びデータ解析用の PC によって構成される.暗号処理ボードにおける暗号処理実行中の消費電力データは,デジタルオシロスコープによって測定及び記録され,そのデータは解析用の PC に転送され解析を行う.また,FPGA のコンフィギュレーションにもこの PC を使用することとした.

### 3.2 暗号処理ボード

システム構築にあたり,消費電力測定用の暗号処理ボードを作成した.暗号処理用のデバイスとしては,再構成可能な大規模集積回路である FPGA を用いた.暗号を実装する FPGA には,ユニバーサル基盤を用いて暗号処理ボードを作成することを考慮し,ソケットを使用することができる FPGA の中で最も規模の大きなものを選定した.この結果,Xilinx 社の Virtex XCV800-HQ240-4 を使用した.作成したボードの電力供給線は,$V_{INT}$, $V_{CO}$ それぞれを切り分け,その間に抵抗を挿入できるようにジャンパーを取り付けた.また,バンク毎にもジャンパーを取り付け,測定出来るようにした.電力供給線は,FPGA に対するものとその他のデバイスに対するものとを分けて作成した.図２に作成した暗号処理ボードを示す.

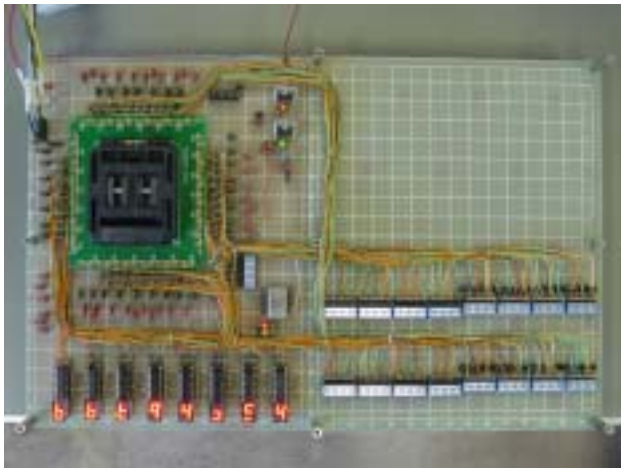

図２　暗号処理ボード

### 3.3 暗号回路の実装

実装する暗号は Verilog-HDL を用いて記述し,論理合成及び配置配線は ISE6.0XST を用いた.すでに我々は FPGA への暗号回路の実装として,Camellia, AES, Hierocrypt-L1, MISTY1 について報告している.[3] 本研究では,その実装結果をもとにして,今回作成した暗号処理ボードのインターフェースに合わせた変更を行っている.

## 4 解析結果

ここでは一例として DES の Sbox1 に対して消費電力解析を行った結果を示す.DES の Sbox1 を FPGA に実装し,Sbox1 が動作中の消費電力データを測定し,鍵の推定を行った.図３に推定した鍵が正しい場合の電力差分を,また図４に推定した鍵が誤っている場合の電力差分をそれぞれ示す.推定鍵が正しい場合は,差分値が大きくなる部分が現れる.しかし推定鍵が誤っている場合はそのような波形が現れず,鍵を推定することができた.

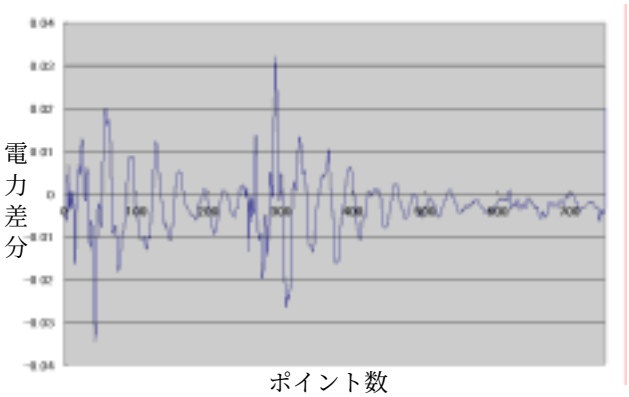


図３　推定鍵が正しい場合の電力差分

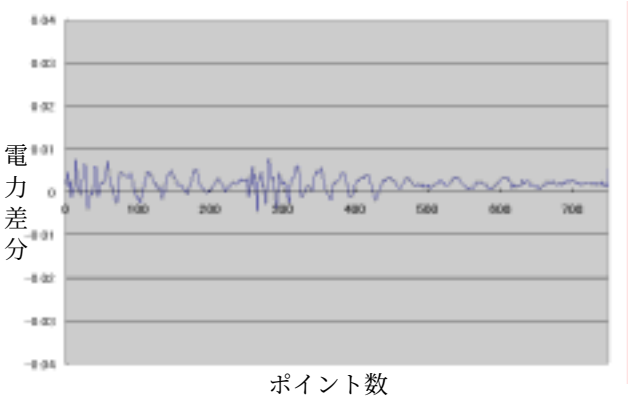


図４　推定鍵が誤っている場合の電力差分

## 5 まとめ

本研究では,サイドチャネル攻撃をハードウェアの面からアプローチするために,FPGA を用いた暗号処理ボードを作成し,電力解析に必要な環境と装置を整えた.また,暗号回路動作中の電力波形を測定し,電力差分解析による鍵の推定を行った.

### 参考文献

[1] Siddika Bernors, Elisabeth Oswald, and Bart Preneel, ”Power-analysis Attacks on an FPGA – First Experimental Results-,” CHES2003, pp.35-50, 2003.

[2] P. Kocher, J. Jaffe, and B. Jun, “Differential power analysis,” Advances in Cryptology: Proc. CRYPTO’99, pp.388-397, Springer-Verlag, 1999.

[3] 山内 剛,梶崎 浩嗣,黒川 恭一,”暗号処理ボード SEBSW-2 への暗号回路の実装,”FIT2003, C-034, 2003.