FPGA に実装された暗号に対するサイドチャネル情報を用いた解析

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

ブロードバンドや電子決済の普及といった情報化が進むなかで、データ通信や個人認証など多くの場面で、セキュリティシステムとして共通鍵暗号方式が用いられている。しかし、これに対抗する暗号解読技術も数多く研究されている。その対抗手段の一つとしてサイドチャネルアタックが挙げられる。サイドチャネルアタックは、平文・暗号文だけから秘密情報を推定するのではなく、暗号デバイスがもたらす入出力以外の情報を用いて秘密情報を特定しようとするものである。今回はそのなかでも、暗号デバイスの消費電力を用いて秘密情報を解読する電力解析攻撃に着目した。

暗号の実装対象には、FPGA を仮定した。FPGA は、再構成が可能であるという特性を持つため、設計の工程において非常に重要になってきている。また、この特性を用いて複数の暗号方式を切り替えてダイナミックに使用するシステムに関する研究も行われている。[3]　FPGA の消費電力の特性は、ASIC などと比較しうるものであるので、暗号専用デバイスへの応用といった展開の可能性もある。

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は多数行われているが、FPGA に実装されたものに対しての攻撃例は少ない。その中で FPGA に対する最初の電力攻撃とするものが文献[1]で報告されているが、まだ細部において不明な点が多い。今回、FPGA に実装された暗号の解析を念頭に必要な環境の整備を進めた結果について報告するものである。

2．FPGA

FPGA とは、Field Programmable Gate Array の略で、再構成可能な大規模集積回路である。Xilinx, Altera 等が開発を行っており、様々なゲート数や特徴を持った製品が発売されている。市場における FPGA のシェアは Xilinx 社の開発しているものが最も多く、FPGA に関する研究においても Xilinx 社製の FPGA を用いているものが非常に多い。これは、Xilinx 社製の FPGA が高い信頼性を持っているためであるとも考えられる。そのため、本研究においても Xilinx 社の Virtex を使用した。

Virtex は、外部ピンと内部とのインターフェースを行う IOB(Input/Output Block), 4,096 ビットを単位とした専用の RAM 領域である Block RAM,そして CLB(Configurable Logic Block)から構成されている。さらに CLB は CLB Slice 2 個から構成され、この CLB Slice は LC(Logic Cell)2 個から、そして LC は 4 入力 Lookup Table1 個、carry logic 及び記憶エレメントから構成されている。図 1 に Virtex の基本構造を示す。

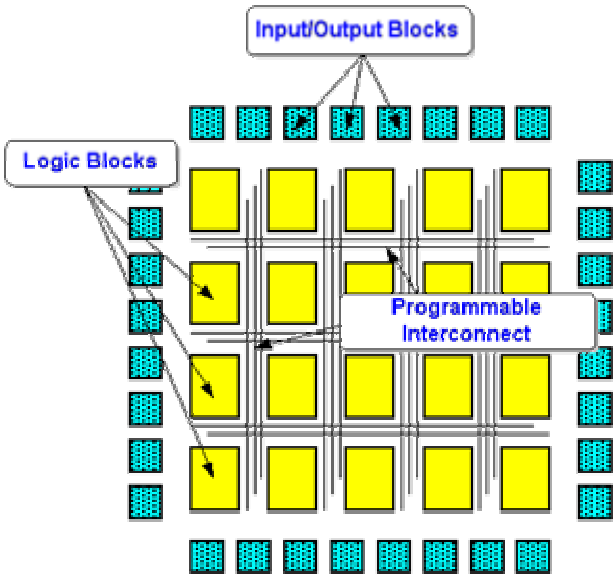

図 1．Virtex の基本構造

3．電力解析攻撃

電力解析攻撃は、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]　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。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が電力解析攻撃である。Kocher は、電力解析攻撃により IC カードに実装された DES についての解析を行っている。

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

消費電力の解析手法には単純電力解析(SPA)と電力差分解析(DPA)がある。単純電力解析は消費電力そのものから秘密情報を解析するもので、1 回の測定で解析できる。

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。

FPGA に対する電力解析攻撃例としては、Siddika らの研究が報告されている。

彼らは、Xilinx 社の Virtex XCV800 を用いて楕円曲線暗号を実装し、それに対する単純電力解析を行った。XCV800 は、IOB が８つのバンクに分かれており、それぞれに V_{INT}, V_{CO}, GND の外部ピンがある。彼らは、それぞれのピン毎に消費電力の測定を可能にするため、それぞれをジャンパーで切り分けられるような構成のボードを作成して解析を行った。

4．解析システムの概要

今回、解析の環境を作るため、消費電力測定用に FPGA を用いた暗号処理ボードを作成した。暗号を実装するターゲットデバイスには、Siddika らと同じ Xilinx 社の Virtex XCV800-HQ240-4 を用いた。電力供給線についても同じように、V_{INT}, V_{CO}, それぞれを切り分けられ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

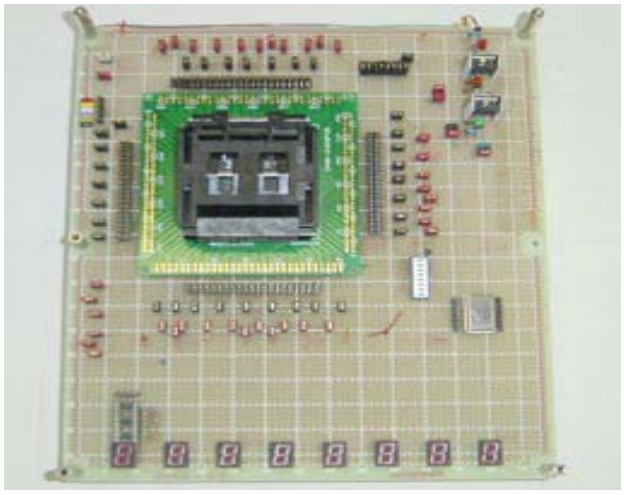

図 2-a．暗号処理ボード

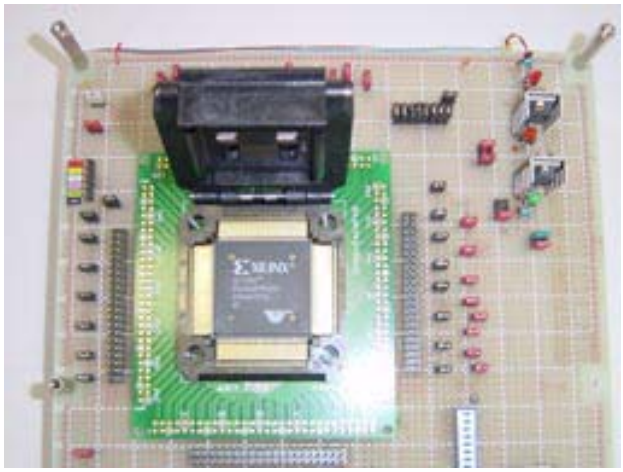

図 2-b．FPGA 部の拡大図

した。測定用に作成した暗号処理ボードとその FPGA 部の拡大写真を図 2-a 及び図 2-b に示す。

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 ISE4.2XST を用いた。暗号の実装においては、山内らの研究により、Camellia, AES, Hierocrypt-L1, MISTY1 について、すでに FPGA への実装を行っている。[4]　本研究では、それらの研究資料を利用して、上記の暗号について解析を試みる。

測定はデジタルオシロスコープで行い、データはパソコンにて解析を行う。

5．まとめ

本研究では，FPGA に実装した暗号に対してサイドチャネルアタックを行うため、電力解析攻撃に必要な環境と装置を整えた。

今後データの解析を進めるとともに、他の暗号アルゴリズムについても実装及び解析を行い、解析に最低限必要な測定機材の条件等についても検証を行っていく予定である。

参考文献

[1] Siddika Bernaors, Elisabeth Oswald, and Bart Preneel, Power-Analysis Attacks on an FPGA – First Experimental Results, CHES2003.

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

[3] 梶崎 浩嗣　黒川 恭一:“暗号処理ボード SEBSW-2 の設計と性能評価”,信学技報 VLD2002-123, CPSY2002-76, 2002.

[4] 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.