第3章

電力，電磁波から暗号回路の内部動作を解析する

―― DES暗号回路を実測し，差分電力解析を行う

高橋芳夫，佐藤 証

ここでは，実際に暗号LSIからデータを収集し，どのようにして秘密かぎが抽出されるかを解説する．筆者らは，FPGAにDES（Data Encryption Standard）暗号回路を実装し，差分電力解析（DPA）を行った．その結果，数千サンプルのデータから，秘密かぎ全56ビットを取り出せることがわかった．なお，今回の実験は使用したFPGA固有の性質によるものではなく，LSIが動作する際の消費電力の変動や電磁波の放射など，一般的な現象を利用している．（編集部）

筆者らは，実際にDES暗号回路を動作させて消費電力と電磁波の観察を行い，LSIの漏えい情報を解析して秘密かぎを取り出す実験を行いました．ここでは，電力や電磁波の測定がどのように行われるのか，また測定波形からどのようなことが分析できるのかを解説します．

サイドチャネル攻撃（正規の入出力経路以外からの情報を利用した攻撃）の評価用として，耐タンパ性（攻撃に対して，秘密情報の守秘や機能の改変を困難にする性質）に関する標準化のための調査・研究を行っているINSTAC（Information Technology Reseach and Standardization Center）などが専用評価ボードを開発しています．こうした評価ボードには，高性能な電源回路やコンデンサ（OS-CONやPOSCAPなど）を使ってノイズを抑えたり，電力（電流）測定用にシャント抵抗を実装して精密に測定できるようにくふうされたものがありますが，非常に高価なうえに入手も困難です．

DES程度の小さな暗号回路で簡単な実験を行うには，このような専用ボードよりも，シンプルな構成のFPGAボードが適しています．そこで，今回の実験では本誌2005年1月号付属のFPGA基板を利用しました．なお，この実験はFPGA（XC3S50）に固有の機能や性質に依存したものでは

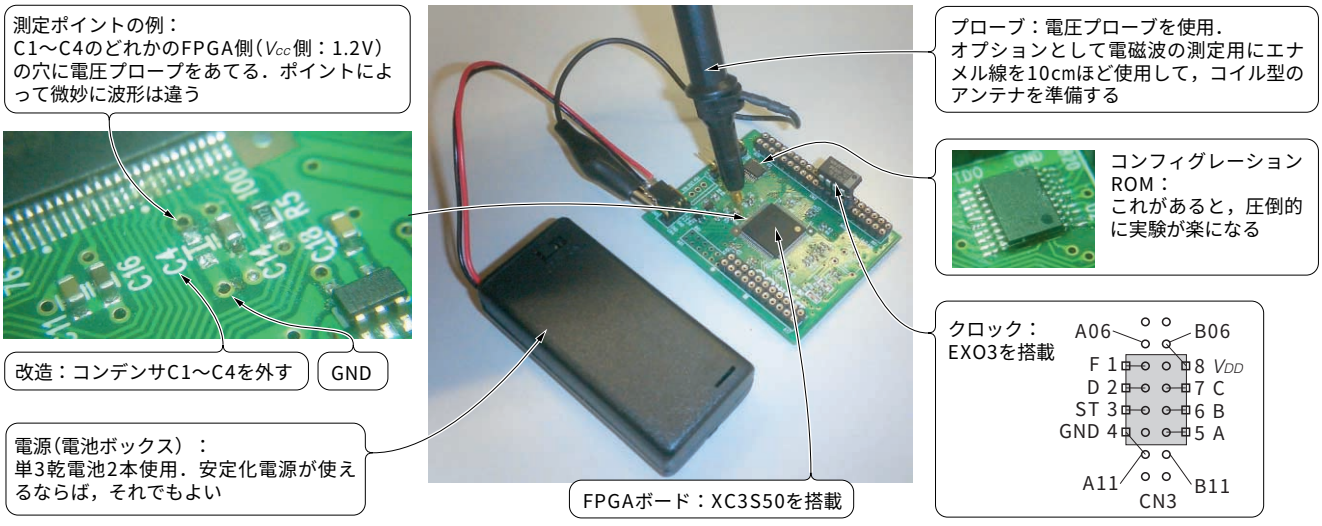

図1　実験環境

図に，今回の実験のために行ったFPGA基板の改造内容と測定環境をまとめる．

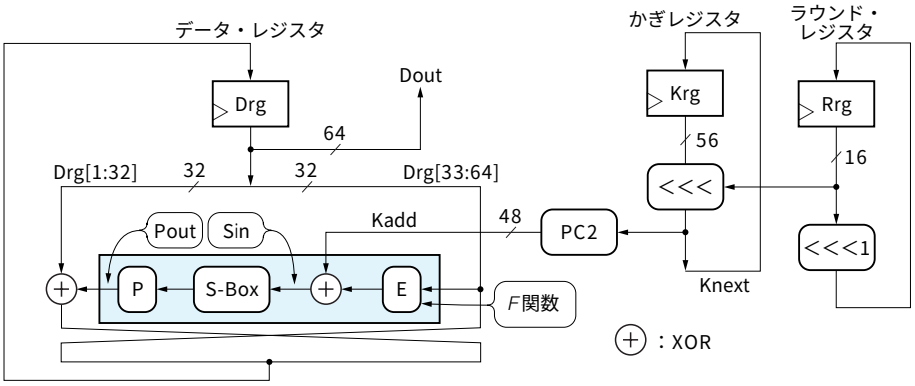

図2
DESのループ・アーキテクチャ
中間データを保持するための64ビットのレジスタ(Drg)，ラウンドかぎをラウンドごとに生成保持するための56ビットのレジスタ(Krg)，ラウンド制御用のレジスタ(Rrg)があり，クロックに同期して値が更新される．レジスタの値が変化すると，Drg [33：64]がE→XOR→S-Box→Pと処理され，Drg [1：32]とXORされた後，次のクロックでDrgに格納される．

表1　主要部品

部　品	個 数	備　考
FPGA基板	1枚	本誌2005年1月号付属FPGA基板
コンフィグレーションROM	1個	使用を推奨
クロック発振器EXO3(16MHz)	1個	内部分周して4MHzを使用
丸ピンICソケット(1×20)	1本	CN2とCN3の必要部分に使用
L字型ヘッダピン(1×40)	1本	CN1とCN4(4ピン，6ピン)に使用
2ピン・ソケット	1個	電池ボックスの端子に使用
電池ボックス(単3，2本入り)	1個	—
乾電池(単3)	2本	—
エナメル線	少々	電磁波測定用(オプション)

ありません．LSIが動作する際の消費電力の変動や電磁波の放射という一般的な現象を利用したもので，ほかのデバイスでも同様に適用可能なものです．

サイドチャネル攻撃のための準備

以下に，今回の実験のために必要な準備を述べます．また，**表1**と**図1**に，実験で使用するおもな部品と改造内容，そして測定環境をまとめておきます．

● FPGA基板を準備する

まず，FPGA基板上にクロック発振器「EXO3(16MHz, DIP 8ピン型)」を載せます．ここでは，観測結果が良好であった内部分周の4MHzをクロックとして使います．EXO3の16MHzクロックをFPGA内で分周するほうが自由度は高いのですが，今回はDES以外の回路をできるだけ少なくするためにEXO3で内部分周します．もちろん，4MHzのクロック・モジュールを実装してもかまいません．

クロック配線を短くするために，EXO3のV_{CC}とGNDピンを少し延ばしてコネクタCN3上に載せました(**図1**)．ただし，EXO3の仕様では電源電圧は5V±0.5Vなので，3.3Vでの使用は実験目的以外では推奨できません．

電源は，FPGA基板の仕様では3.3Vとなっていますが，今回は単3の乾電池を2本直列につないで使用します．比較的軽い処理ということもあり，筆者の手元の3枚の基板では問題なく動作しています．スイッチング・レギュレータを使用したACアダプタは便利ですが，電源ラインにノイズが入るため，今回の実験には向きません．低ノイズの安定化電源が使えるのであれば，そちらを使用するのもよいでしょう．FPGA基板には3.3Vレギュレータ用のパターンがありますが，これは使用しませんでした．

そのほか，基板に用意されたパターンに従って，コンフィグレーションROM(U2)，電源供給用ヘッダ・ピン(CN4, 4ピン，3.3V側を使う)，コンフィグレーション用ヘッダ・ピン(CN1，6ピン)，トリガ出力用モニタ・ピン(CN2，1ピン)を取り付けます．

● FPGAにDES回路を実装する

DES暗号は，かぎを変形しながらラウンド処理を16回繰り返します(詳細は第2章を参照)．**図2**に示すように，今回の実装では1ラウンド分のデータパスを16回使用するループ・アーキテクチャと呼ばれる方式をとっています．また，サイドチャネル攻撃への対策や特別な高速化は行っていません．

DESのラウンド処理でLUT(look-up table)が割り当てられるのは，XOR(排他的論理和)とS-Boxとセレクタです．拡大転置Eや32ビット転置Pといったビットの転置は，単なる配線となります．XORは1ビット当たり1個のLUTを使用します．ただし，Pout(F関数の出力)とDrg [1：32]のXORは，データ・レジスタDrgのセレクタと合成されて1個のLUTとなります．また，S-Boxは6ビット入力，4ビット出力の置換テーブル八つで構成され，**図3**のよう