可変遅延素子を付加した回路の耐タンパー性に関する考察

大森　裕介†　出崎　善久†

茨城大学‡

1. はじめに

近年，暗号処理デバイスに対する攻撃法の 1 つであるサイドチャネル攻撃に関する研究が盛んに行われている．サイドチャネル攻撃とは，暗号用 LSI に付随する物理的情報（電圧レベル，漏洩電磁波等）を観測し，I/O ピン等の正規の入出力経路以外から LSI 内部の秘匿情報を取得する非破壊攻撃である．本研究では，研究事例の比較的少ない RSA 暗号における離散フーリエ変換による多倍長乗算を対象とし，乗算部を束データ方式で実装した場合の耐タンパー性について検討する．

2. RSA 暗号に対するサイドチャネル攻撃

RSA 暗号で使用される演算を式(1)，(2)に示す．演算自体は，暗号化，復号のどちらも同じ形の式になる．これらの式中に現れる剰余演算は，モンゴメリ乗算を使用することで乗算とビットシフトに置き換えることが出来る．また RSA 暗号で現在安全とされる鍵長は 1024bit～2048bit ということもあり，多倍長乗算高速化に重点を置いて実装する場合がほとんどである．多倍長乗算には多種の実装法があるが，今回は FFT で実装した場合について考える．

$$\text{暗号化}：c = m^e \bmod N \quad (1)$$

$$\text{復号}　：m = c^d \bmod N \quad (2)$$

m ：平文　　c ：暗号文

e, N ：公開鍵　　d ：秘密鍵

3. FFT による多倍長乗算

FFT を利用した乗算では，オペランドのビット長が長くなるほど筆算法に比べ高速になる．現在安全とされる鍵長程度では浮動小数点複素数演算のオーバーヘッドが大きいため，FFT を使用するのはあまり適当ではないという報告[1]もあるが，束データ方式で実装する場合，FFT 演算回路の規模の大きさを逆に利用できると考えた．

文献[2]では，RSA 暗号で使用される演算が平方剰余算か剰余乗算かを推測する手法を提案している．例えば，剰余乗算を右向きバイナリ法で実装する場合，平文(暗号文)に $N-1$ (N は法)の固定値を入力することで，平方剰余算が 1^2 と $(N-1)^2$，剰余乗算が $1\times(N-1)$ の 3 パターンの演算しか出現しなくなり，観測された波形から実際に実行された演算を容易に判別できる．

右向きバイナリ法(左シフト法)による暗号化

```
Big_num module(Big_num m, Big_num e, Big_num N){
    Big_num c = 1;                          //初期化
    while(e != 0){
        c = c * c % N;                      //平方剰余算
        if(ei = 1) { c = c * m % N;}//剰余乗算
        e<<=1;                              //左シフト
        }
    return c                                //暗号文の出力
}
```

ei:MSB　　Big_num:多倍長構造体

FFT による乗算回路にサイドチャネル攻撃を行い平方剰余算か剰余乗算かを見分けるには，FFT を施した後の数の積が平方剰余算か剰余乗算かを判別できればよい．FFT 後の積で発生する乗算は式(3)の浮動小数点複素数乗算を成分ごとに行う．実験では 64 個の成分について順に乗算を行った．

$$(a+bj)\times(c+dj) \quad (3)$$

4. 束データ方式による実装

同期式回路の場合，回路を構成する各レジスタへのデータの入出力はクロックに同期して一斉に行われる．これにより，LSI からの漏洩電磁波のピークが観測し易くなる．これに対して，非同期式回路の場合，設計を工夫すれば，レジスタへのデータ移動のタイミングにばらつきを持たせることが可能である．

非同期式設計の一つである束データ方式では，同期式回路のクロックラインに相当する機能（タイミング信号生成回路）を他の回路と同じチップに作りこむという特徴がある．タイミング信号生成回路もそれ自体ノイズ源となるため，外部クロックを利用する同期式回路と比べてサイドチャネル攻撃に対する強度は増すと考えられる．

図 1 と図 2 に，同期式，及び束データ方式で設計した浮動小数点複素数乗算回路を示す．束データ方式の実装には最も単純な C 素子によるチェインを利用している．

A study on tamper-resistance of circuits with variable delay elements

†Yusuke OMORI, Yoshihisa DESAKI

‡Ibaraki University

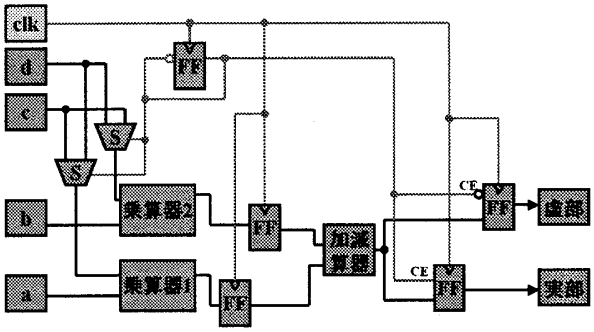

図 1　同期式複素数乗算回路

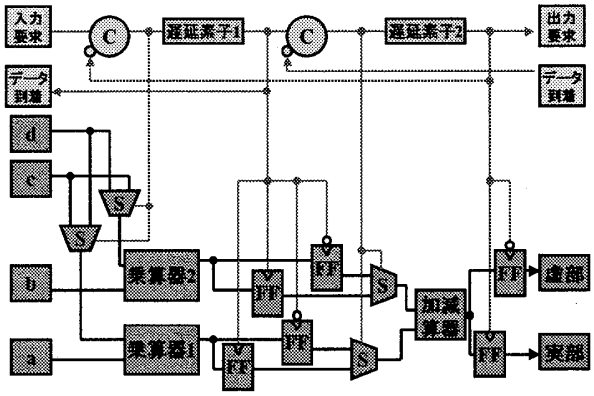

図 2　束データ方式複素数乗算回路

5. 測定と実験結果

実験では，FPGA 暗号評価基板 SASEBO 上の VirtexⅡPro(XCVP7)に回路を実装し，FPGA の GND ラインに挿入した抵抗の電位差をオシロスコープ (Agilent DSO3062A 50mV/div, 5us/div, 20MSa/s) にて測定した．回路全体の動作周波数は 6MHz とし，入力は FFT 後の IEEE754 倍精度浮動小数点データとした．従って，乗算器，加減算器ともに倍精度浮動小数点演算を行うことになるが，動作レベル記述を使用して設計したため内部回路のほとんどはハードウェアマクロの乗算器，加算器を使用している．

同期式で測定した結果を図 3～5 に，束データ方式で測定した結果を図 6～8 に示す．どちらの場合も乗数，被乗数の違いによって観測波形の違いがはっきりと見て取れる．

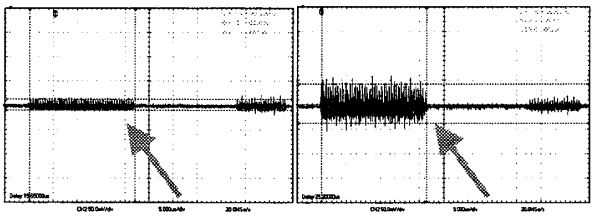

図 3 同期式の 1^2　　図 4 同期式の $1\times(N-1)$

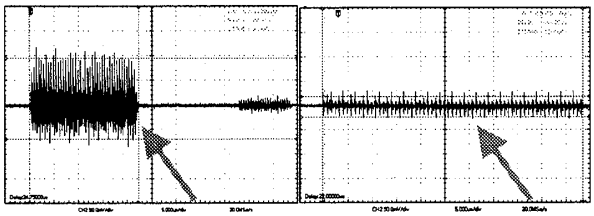

図 5 同期式の $(N-1)^2$　　図 6 非同期式の 1^2

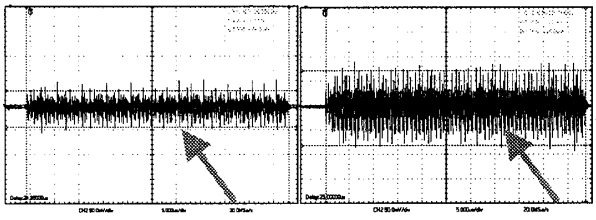

図 7 非同期式の $1\times(N-1)$　図 8 非同期式の $(N-1)^2$

6. 結論と考察

固定値入力を利用する手法により，同期式，束データ方式共に秘密鍵が推測可能という結果になった．これは，タイミング信号生成回路の消費電力よりも乗算器，加減算器，フリップフロップのビット遷移による消費電力の方が大きいためであると考えられる．

今回使用した束データ方式におけるハンドシェイクプロトコルは単純で設計が容易であるが，隣接する回路ブロック間の依存度が高く，各回路ブロックが並列に動作しているとは言い難い．また，図 2 で使用されている遅延素子が生成するのは固定遅延である．これを可変にして各回路ブロックの動作相と休止相を重ねることによる効果も検討すべきであるが，そのためには，回路全体の構成やハンドシェイクプロトコルの見直し[3]が必要になる．

謝辞

実験に使用した FPGA 暗号評価基板 SASEBO を貸与していただきました産業技術総合研究所に深謝いたします．

参考文献

[1]C.K.Koc,” High-speed RSA Implementation,” Technical Report TR 201, RSA Laboratories, Nov. 1994.

[2]本間尚文,宮本篤志,青木孝文,佐藤証,” 固定値入力を用いた RSA 暗号ハードウェアに対する SPA,” SCIS2007,Vol.3E3-2,pp.1-6, Jan. 2007.

[3]K.Shojaee, M.Gholipour, A.Afzali-Kusha and M.Nourani,” Comparative study of asynchronous pipeline design methods,” IEICE Electronics Express Vol.3, No.8, pp.163-171, 2006.