1Z-3

二線式 RSA 暗号化回路の耐タンパー性に関する考察

大木 勇治† 出崎善久‡
†茨城大学理工学研究科メディア通信工学専攻
‡茨城大学工学部メディア通信工学科

1. はじめに

近年，回路の消費電力等から IC チップ内部の秘密情報を解読するサイドチャネル攻撃の危険性が現実的なものとなり，暗号化回路にサイドチャネル攻撃対策を施すことが必須となっている．回路レベルのサイドチャネル攻撃対策として，回路の非同期化が有効であると考えられている．

本稿では，非同期式設計手法の一つである二線式論理で設計した RSA 暗号化回路のサイドチャネル攻撃に対する耐タンパー性について考察する．

2. 暗号アルゴリズムの高速化

代表的な暗号アルゴリズムである RSA 暗号の実装では，べき乗剰余算の計算時間を短縮するためにバイナリ法や，k-ary 法等のアルゴリズムを使用することが多い．本稿で実装の対象とした RSA 暗号アルゴリズムを以下に示す．

バイナリ法を使用した RSA 暗号アルゴリズム

Input ：	$N, 0 < X < N, e$
Output ：	$A = X^e \bmod N$
Step1 ：	$A = X$
Step2 ：	$i = \lceil \log_2 e \rceil$
Step3 ：	$A = A \cdot A \bmod N, i = i - 1$
Step4 ：	if $(e_i = 1)$ $A = A \cdot X \bmod N$
Step5 ：	if $(i \neq 0)$ return Step3
	else output A

X：平文，A：暗号文，N, e：公開鍵

3. サイドチャネル攻撃

サイドチャネル攻撃とは，暗号化を行う際のサイドチャネル情報（消費電力，漏洩電磁波，処理時間等）を利用して秘密情報を読み取る攻撃手法である．

バイナリ法を使用して実装した RSA 暗号の消費電力波形の例を図 1 に示す．バイナリ法では，上述したアルゴリズム中の Step4 において条件分岐を行うため，図 1 に示すような乗算の消費電力と鍵のビットパターンとの相関が生じる．このように，1 つの観測信号のみで秘密情報を推測する電力解析攻撃は SPA（Simple Power Analysis：単純電力解析）と呼ばれている．

RSA 暗号で現実的に安全であるとされる鍵長は，現在では 2048 ビット以上であり，暗号化処理に要する時間は長くなる傾向にある．このため，処理時間の比較的短い共通鍵暗号等と比べて，RSA 暗号では SPA が比較的容易に実行可能であると言える．

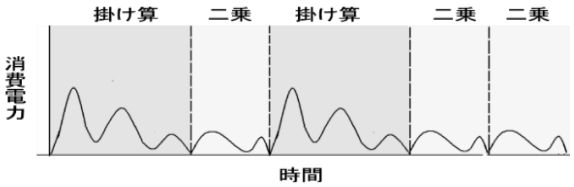


図 1 RSA 暗号に対する SPA

4. 二線式論理による非同期式回路

4.1 同期式回路と非同期式回路

同期式回路では，回路を構成する各ブロックはグローバルクロックに同期して動作する．このため，回路の消費電力や漏洩電磁波の強度のピークが顕著になり，サイドチャネル情報として利用されやすくなるという問題がある．

グローバルクロックを使用しない非同期式回路では，要求・応答信号の対からなるハンドシェーク信号によって回路を制御している(図 2)．必要なときに必要な回路ブロックのみが動作するので，回路全体の消費電力のピークが時間軸に対して平均化され，顕著な波形パターンが現れにくくなる．また，各回路ブロックの動作タイミングがばらつくことにより，消費電力パターンが時間軸方向にゆらぐ．非同期式回路のこの特徴は，多数の観測信号の位置合わせが必要になる DPA（Differential Power Analysis：差分電力解析）に対して有効に働く．

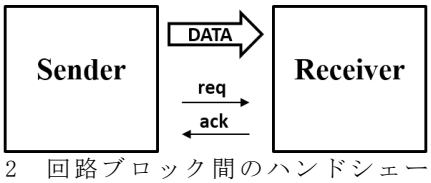


図 2 回路ブロック間のハンドシェーク

4.2 二線式論理

CMOS インバータでは，入力値のビット反転に伴って電力を消費する．この特徴を利用したサイドチャネル攻撃として，データ転送前にプリチャージ処理を行うバスに流れているデータのハミング重みを消費電力から推測する手法が知られている．一般に，CMOS で構成された回路の消費電力とハミング重みとの間には相関があるため，ハミング重みを平均化する等のサイドチャネル攻撃対策が必要になる．

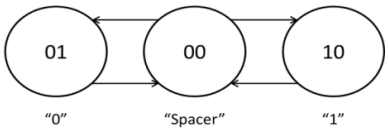
本稿で考察の対象とする二線式論理で使用する符号化規則を図 3(a)に示す[1-2]．1 ビットのデータ“1”，“0”に対する符号語(1,0)，(0,1)の他に，データ転送の区切りを表す Spacer として(0,0)を使

A study on the tamper resistance of asynchronous dual-rail RSA encoders
† Yuji OKI, Major in Media and Telecommunications Engineering, Graduate School of Science and Engineering, Ibaraki University
‡ Yoshihisa DESAKI, Department of Media and Telecommunications Engineering, Faculty of Engineering, Ibaraki University

用する．符号化された 2n ビットのデータは，全ての対が(0,0)であれば Spacer であり，全ての対が(0,1)もしくは(1,0)ならば符号語である．

二線式回路では，図 3(b)に示す状態遷移図に従ってデータ転送を行う．遷移(0,0)→(0,1)で「0 の到着」，遷移(0,0)→(1,0)で「1 の到着」を表す．回路動作時のデータバス上のハミング重みが平均化されるため，二線式回路の電力解析攻撃に対する耐タンパー性は極めて高くなる．

Data	d1	d0
Spacer	0	0
0	0	1
1	1	0



(a) 二線符号化　　(b) 状態遷移図

図 3　二線式論理

4.3 二線四相方式ハンドシェークプロトコル

回路ブロック間の通信では，四相ハンドシェーク信号によりデータ転送の制御を行う．図 4 に示すように，二線データが Spacer から符号語に遷移すると ack 信号が立ち上がり，符号語から Spacer に遷移すると ack 信号が立ち下がる．図 5 に二線四相方式回路の概念図を示す．送信側のレジスタから出力される二線符号化されたデータは req 信号の役割も果たす．受信側のレジスタからは，CTRL モジュールを介して ack 信号が返される．

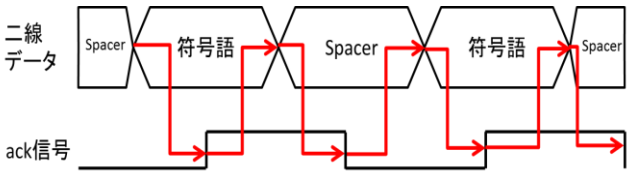


図 4　二線四相方式ハンドシェークプロトコル

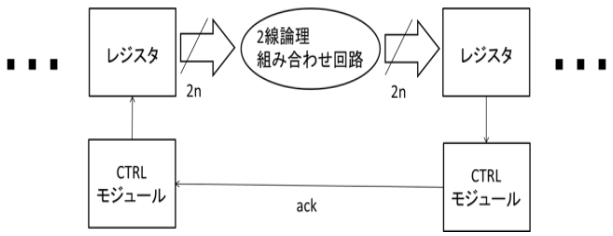
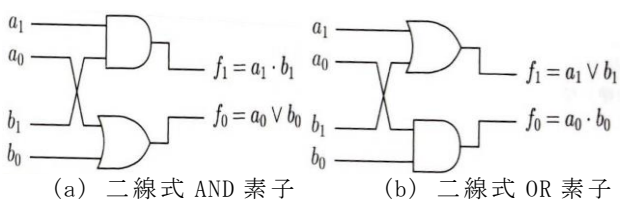


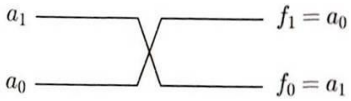
図 5　二線四相方式回路

5. 二線四相方式 RSA 暗号化回路

二線式論理で構成した非同期式回路では，組合せ回路で使用するゲートを全て二線式論理ゲートに置き換える必要がある．二線式論理の基本ゲートを図 6 に示す．



(a) 二線式 AND 素子　　(b) 二線式 OR 素子



(c) 二線式 NOT 素子

図 6　二線式論理の基本ゲート

本稿で設計対象とした暗号化回路には，加算器，乗算器，レジスタ，シフタ，セレクタが含まれているが，これらの回路は全て二線式論理ゲートを使用して構成されている．

設計した二線四相方式 RSA 暗号化回路のブロック図を図 7 に示す．レジスタ間の通信は，図 5 に示した二線四相方式で行う．また，全ての回路は，図 6 に示した二線式論理ゲートで実現されている．

図 7 中の回路ブロックの機能を以下に示す．

[ステート制御]
暗号化回路の状態遷移を制御する．

[DPL]
データの二線符号化処理を行う．

[Step3，4，シフタ，カウンタ]
暗号アルゴリズム中の各演算に対応する処理を行う．

[表示切替]
暗号化結果を表示する．

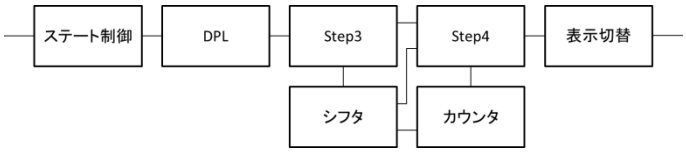


図 7　二線四相方式 RSA 暗号化回路

図 7 に示した二線四相方式 RSA 暗号化回路を Verilog-HDL で設計し，Xilinx 社製 FPGA に実装した．本稿で使用した開発環境を表 1 に示す．

表 1　開発環境

HDL	Verilog-HDL
開発ツール	ISE Design Suite 13.4
ターゲットデバイス	Virtex-5 XC5VLX30

今回採用した設計では，入力とする平文を 32bit，暗号化鍵（アルゴリズム中の e）を 16bit とした．これらのビット幅は Verilog-HDL のコード内でパラメータとして扱われているため，現実的な値（2048bit の鍵長）に容易に変更可能である．

参考文献

[1] 南谷崇，“論理回路の基礎，”サイエンス社，2009.
[2] 齋藤寛，“非同期式回路の設計技術，”
IEICE Fundamentals Review，Vol.3，No.3.