# RSA暗号回路に対するテスタビリティ解析

日大生産工（学部）　○早川 鉄平　　日大生産工　　細川 利典

## 1 はじめに

近年パーソナルコンピュータや携帯電話をはじめとする個人向けの情報機器の普及によって、様々な通信を個人レベルでも利用できるようになった．そのため通信情報の暗号化など，プライバシー保護の面で暗号アルゴリズムが重要な役割を担っている．一般的に，暗号アルゴリズムは高速化や低消費電力化などの理由からソフトウェアでなくハードウェアで実装している．(1)

ハードウェアで実装した暗号回路は，回路の出力が入力と回路内部のフリップフロップ（Flip-Flop:FF）に依存する順序回路で生成される．

順序回路では，各レジスタに値の設定を行うことや観測を行うことが困難なため，高い故障検出率を達成するためのテスト生成が困難である．スキャンチェインを用い，フルスキャン設計(2)にすれば全てのレジスタに任意の値を設定しながら値を観測することが可能である．しかしながら，テストのためテストピンが使用可能である場合，スキャンチェインを利用したサイドチャネル攻撃(3)を受ける危険性が生じる．暗号回路に対しては，正規の通信経路以外から取得できる情報を用いたサイドチャネル攻撃が考えられており，スキャンチェインを利用したサイドチャネル攻撃も問題の一つである．暗号回路では暗号化及び復号化のための秘密鍵，復号された平文が回路内のレジスタに格納されているため，その安全性が重要な問題となっている．

本稿では，パーシャルスキャン設計を用いた安全なスキャン設計法でRSA暗号回路(4)を生成し，そのテスタビリティを評価する．パーシャルスキャン設計を採用することにより，一部のレジスタをスキャンチェインに含まないことで秘密情報を持つレジスタを保護する．

## 2 RSA暗号回路

本稿で用いるRSA暗号回路について説明する．公開暗号であるRSA暗号では，暗号文yを秘密鍵d，公開鍵mを用いて平文xに復号する。平文xと暗号文yには$x = y^d \bmod m$という関係がある．

べき乗計算を行うとき，yをd回かけるとすると，べき乗計算でのかけ合わせは$2^d-1$回行われるので，dの大きさが大きくなると計算に莫大な時間が掛かってしまう。そこでdを2進数表記し，1になったビットの大きさだけべき乗を繰り返し，$y^d$を作る．また$y^d$を計算し終わってから剰余(mod)を行うのではなく，べき乗途中でも行うようにし，ビット数の増加を防ぐ．

例えば，$V^{137} \bmod m$を計算する場合について考える．137は2進数表記で10001001となるので，ビット7，3，0が1となる。そのため，Vを$2^7$乗，$2^3$乗，$2^0$乗したものそれぞれにmod mをし，全てを掛け合わせてからさらにmod mをすることで計算することが可能となる．この手法はBinaryMethod(5)といい，本稿のRSA暗号回路にも用いられている。

## 3 攻撃者に関する前提

暗号回路に対する攻撃は，攻撃者の知識によりさまざまなレベルが考えられる．本稿では，一般的に得られる情報のみを利用する攻撃者を想定し，攻撃者の知識を以下のように仮定する．

（1） 暗号回路として実装される暗号アルゴリズムを知っている．さらに，実装されるレジスタ転送レベル（RTL）回路を知っているか，いくつかの候補を想定できる．

（2） テスト容易化設計としてスキャン設計が採用されている場合，テスト用外部ピンを認識できる．

---

Testability Analysis for RSA Cypher Circuits

Teppei HAYAKAWA and Toshinori HOSOKAWA

（３）　ゲートレベル回路の設計情報を知らない．
（４）　スキャンチェインでのFFの順序を知らない．

## ４　暗号回路の脆弱性

前章の仮定のように攻撃者がゲートレベル回路やテスト容易化設計の詳細を予め知らなくても，一般的によく用いられるいくつかの暗号回路の脆弱性が知られている．共通鍵暗号であるDES(Data Encryption Standard)，AES(Advanced Encryption Standard)を安全性を考慮せずフルスキャン設計を用いて実装したとき，暗号回路に対するスキャンチェインを利用したサイドチャネル攻撃が報告されている[(6)(7)]．これらの攻撃法では，攻撃者は複数の入力パターンを用いてスキャンチェイン上でのFFの順序を特定し，秘密鍵を得ることに成功している．

また本稿で扱うRSAの復号アルゴリズムでは，2乗剰余算と乗剰余算が繰り返し行われる．乗剰余算を行うかどうかは秘密鍵のビットパターンに依存するため，乗剰余算の結果を格納するレジスタを特定できれば秘密鍵を求めることが可能である．RSA復号回路の各レジスタは2乗剰余算と乗剰余算の計算周期に応じて特有の値の遷移をもつため，レジスタの値を定期的に観測することでスキャンチェイン上のFFとレジスタの対応を解析することも可能である．以上の考察により，RSA復号回路はスキャンチェインを利用したサイドチャネル攻撃に対し脆弱であるといえる[(8)]．

## ５　パーシャルスキャン設計

故障検出効率の向上と安全性を両立させるために，秘密情報を持つレジスタ（危険レジスタ）をスキャンチェインに含めず，残りの秘密情報を持たないレジスタをスキャンチェインに含めるパーシャルスキャン設計を考える．このパーシャルスキャン設計ならばノンスキャン設計と同等のセキュリティを維持しつつ，ノンスキャン設計以上に故障検出効率を向上することができる．

しかしながら，回路中にフィードバックループが残る可能性があり，故障検出効率が十分に高くならない可能性がある．そのため，テストポイントを用いて回路中のフィードバックループを破壊する方法を検討する必要がある．

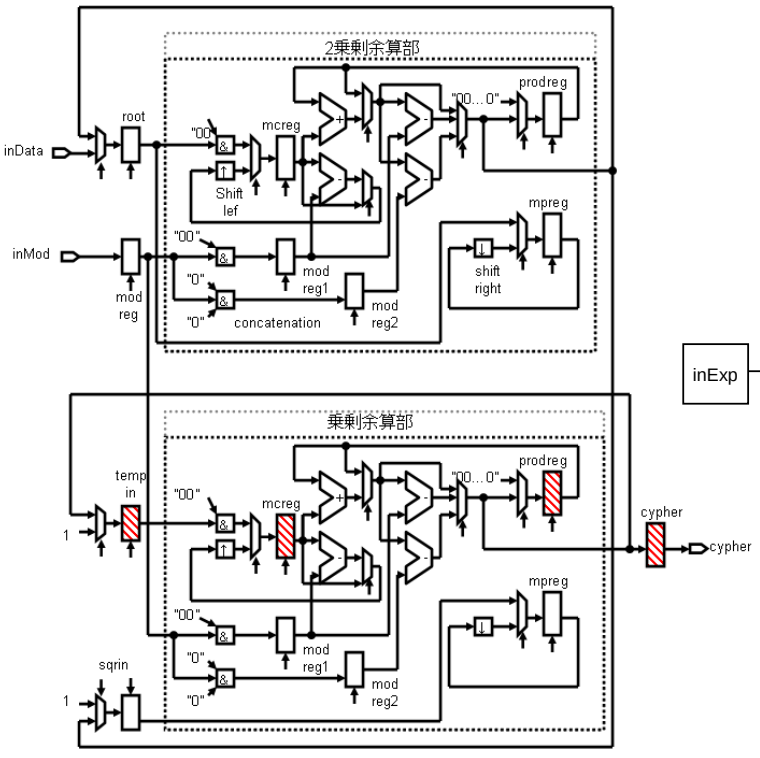


図１　RSA復号回路計算部ブロック図

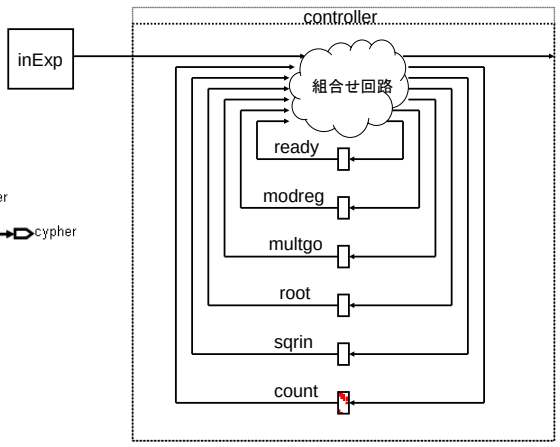


図２　RSA復号回路
コントローラ部ブロック図

## 6　実験結果

256ビットRSA復号器を用い，フルスキャン設計を適用した場合，ノンスキャン設計を適用した場合，パーシャルスキャン設計を適用した場合において面積と故障検出効率を比較した．RSA復号器は，オープンソースIPコアとして公開されているRSA回路[9]を用いた．

RSA復号回路はデータパス部とコントローラ部からなり，データパス部は２乗剰余算部（modsqr）と乗剰余算部（modmult）から構成されている．

RSA復号回路のデータパス部のブロック図を図１に示し，RSA復号回路のコントローラのブロック図を図２に示す．図１のRSA復号回路のデータパス部では，斜線の付いたレジスタ，すなわち剰余算部の結果に依存するレジスタ（cypher，tempin，modmult内のprodreg，mcreg）が危険レジスタとなり，図２のRSA復号回路のコントローラでは，斜線の付いたレジスタ，すなわち秘密鍵に依存するレジスタ（count）が危険レジスタとなる．

パーシャルスキャン設計に関しては，これらの危険レジスタをスキャンチェインに含めず，それ以外のレジスタをスキャンレジスタとした．

スキャンチェインに含まれたレジスタは，２乗剰余算部（modsqr）内のmpreg，mcreg，modreg1，modreg2，prodregと，乗剰余算部（modmult）内のmpreg，modreg1，modreg2とコントローラ内のready，modreg，multgo，root，sqrinであった．

評価実験は自動テスト生成ソフトTetraMAX（Synopsys）を用いて面積，スキャン化率，故障検出率，故障検出効率を求め，フルスキャン設計，ノンスキャン設計，パーシャルスキャン設計についてそれらの評価項目を比較した．

表１に面積を示す．NSはノンスキャン設計を適用した場合の評価を，FSはフルスキャン設計を適用した場合の評価を，PSはパーシャルスキャン設計を適用した場合の評価を表す．数値は1NOTゲートを2とした値である．表１より，パーシャルスキャン設計では，フルスキャン設計と比べ，面積オーバーヘッドが抑えられていることがわかる．これは，スキャン化するFF数（スキャンFF）が回避した危険レジスタ分だけ面積オーバーヘッドが少ないことに起因する．

表２にテスト生成結果を示す．故障モデルは単一縮退故障モデルである．全故障，検出，テスト不可能，未検出はそれぞれ，全故障数，検出故障数，テスト不可能故障数，テスト生成アルゴリズムでバックトラックの制限により処理が打ち切られた故障数を表す．FCは故障検出率，FEは故障検出効率を表す．

表２より，パーシャルスキャン設計では，フルスキャン設計に比べ，検出故障数が少なくなっていることがわかる．これは回路中にフィードバックループが残り，テスト生成アルゴリズムで処理が打ち切られた故障数が増加したことによる．

## 7 おわりに

本稿では，パーシャルスキャンを利用した安全なスキャン設計法を評価した。スキャンチェインを利用したサイドチャネル攻撃に対し脆弱であると考えられる危険レジスタをスキャンチェインに含まないことで被テスト回路にノンスキャン設計と同等の安全性を実現する。また，パーシャルスキャン設計はノンスキャン設計と比べテスト容易となる。

今後の課題としては，パーシャルスキャン設計に加え，危険レジスタから構成されるフィードバックループを切断するためのテ

表２　テスト生成結果

| | 面積 | スキャンFF | スキャン化率 |
|---|---|---|---|
| NS | 75049 | 0 | 0.00% |
| FS | 91733 | 16684 | 100.00% |
| PS | 86361 | 11312 | 67.80% |

表１　面積オーバーヘッド

| | 全故障 | 検出 | テスト不能 | 未検出 | FC | FE |
|---|---|---|---|---|---|---|
| NS | 218692 | 0 | 218692 | 0 | 0.00% | 0.00% |
| FS | 235382 | 235375 | 5 | 2 | 99.99% | 100.00% |
| PS | 230256 | 144500 | 85746 | 10 | 62.76% | 62.76% |

ストポイント[10]挿入法を検討する。

「参考文献」


1）盛岡澄夫，HDLによる高性能ディジタル回路設計，CQ出版社，2002年
2) 藤原秀雄，ディジタルシステムの設計とテスト, 工学図書株式会社, 2004年, pp. 202−213
3) 佐藤証，高橋芳夫，森岡澄夫，LSIを盗聴から守る―暗号回路のサイドチャネル攻撃とその対策―，デザインウェーブマガジン，2月号，2006年，pp.100−134
4) 結城浩，暗号技術入門　秘密の国のアリス，ソフトバンクパブリッシング，2004年，pp.113−138
5) 森岡澄夫, アルゴリズムのハードウェア化手法，デザインウェーブマガジン，1月号，　2008年，pp.20−70
6) B.Yang, K.wu, and R.Karri，Secure scan: A design-for-test architecture for crypto chips, IEEE Transactions on Computer -Aided Design of Intergrated Circuit and Systems, 2006年10月，　pp.2287-2293
7）B.Yang, K.wu, and R.Karri，Scan based side channel attack on dedicated hard ware implementations o data encryption standard, Proceedings of International Test Conference 2004 (ITC'04)，2004年, pp.339-344
8）長谷川宗士,井上美智子,藤原秀雄，平衡構造を利用した安全なスキャン設計，DC研究会，2008年2月，pp. 39−44
9）OPEMCORES, RSA processor, http://www.opencores.org/projects.cgi/web/rsa/overview
10）C.Schotten and H.Meyr, Test Point insertion for an area efficient bist.Proc, Of the IEEE Int. Test Conf. 1995，1995年，pp. 515-523