ISSN 2186-5647

2-29

セキュアスキャン設計のための 強セキュアなシフトレジスタ等価回路の列挙

日大生産工　○近藤 雅之　　日大生産工　山崎 紘史
日大生産工　細川 利典　　大阪学院大　藤原 秀雄

1. はじめに

暗号回路を含む多くの超大規模集積回路(Very Large Scale Integrated circuits: VLSI)において，安全(セキュア)かつテストが容易(テスタブル)な回路設計は重要な課題とされている．これらの問題を解決すべく，いくつかのテスト容易化設計法(Design For Testability: DFT)が提案されている．現在では，DFT の一種であるスキャン設計がもっとも利用されている．スキャン設計とは，回路内部に存在するフリップフロップ(Flip-Flop ： FF)をスキャンフリップフロップと呼ばれる記憶素子に置き換え，数珠状に接続することで FF の可制御・可観測性を向上させる．スキャンフリップフロップは，つのマルチプレクサ(multiplexer:MUX)と 1 つの FF で構成されており，スト実行時にはシフトレジスタ(以下 SR と略す)を形成するため，FF に任意の値を外部から制御・観測可能となりテスト容易性を飛躍的に向上させる[1].

スキャン設計は高いテスト容易性を達成可能であるが，同時に回路内の機密情報へのアクセスも容易になる．このため，スキャンベース攻撃による暗号回路の秘密鍵解読等の秘密情報漏洩の危険性が高いことが指摘されている[2].

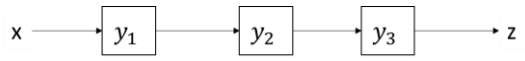
現在スキャンベース攻撃に耐えられる安全なスキャン設計法について研究が行われており，多くの研究が報告されている[2-9,10-13]．文献[10,11]では，SR 等価回路を利用したセキュアかつテスト容易なスキャン設計法を提案している．また，文献[12,13]では一般化フィードフォワード SR 回路(Generalized Feed-Forward Shift Registe:GF²SR に対して，強セキュアな回路の列挙と合成が報告されている[12,13].

回路の安全性を示す尺度として，攻撃者が SR の構造を特定する確率は SR と等価な回路数の逆数に比例することから，SR 等価回路の個数を明らかにすることは重要なことである．本論文では強セキュアな SR 等価回路の列挙を行い，強セキュアな SR 等価回路の個数を明らかにする．

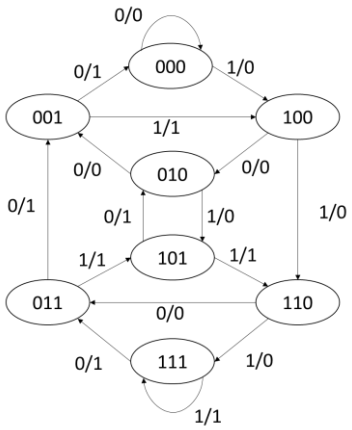
本論文の構成を次に示す．第 2 章で強セキュアな SR 等価回路について説明し，第 3 章で強セキュア SR 回路族を定義する．第 4 章で本論文のまとめと今後の方針を述べる．

2. 強セキュアな SR 等価回路

強セキュアな SR 等価回路とは，回路内のスキャンチェーンを暗号化することで，スキャンベース攻撃やサイドチャネル攻撃などの脅威より回路内の機密情報を守る SR 構造である．以下に強セキュアな SR 等価回路の構成に必要な基本構造を定義する．なお本論文において変数 k は SR 回路の FF の個数とする．



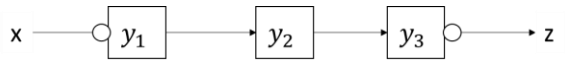
(a). SR 回路図



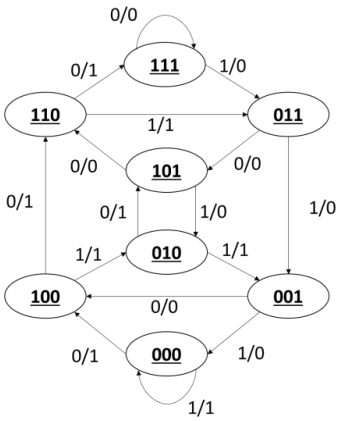
(b). SR の状態遷移図

図 1. k 次ドブルイングラフ

Enumeration of Strongly Shift Register Equivalents for Secure Scan Design
Masayuki KONDOU, Hiroshi YAMAZAKI, Toshinori HOSOKAWA and Hideo FUJIWARA



(a). k 段 SR



(b). k 次拡張ドブルイングラフ

図 2. 強セキュアな k 次拡張ドブルイングラフ

定義 1：***k 段 SR*** の状態遷移図を ***k 次ドブルイングラフ*** と呼ぶ(図 1).

定義 2：k 次ドブルイングラフと同型な状態遷移図を ***k 次拡張ドブルイングラフ*** と呼ぶ．このとき状態割当て，入出力割当ては同一でなくても良い(図 2(b)).

定義 3：状態遷移図が k 次拡張ドブルイングラフとなる回路を ***k 段 SR*** と呼ぶ(図 2(a)).

定義 4：回路 C の k 次拡張ドブルイングラフにおいて，対応する状態割当てが k 次ドブルイングラフと異なっている(入出力割当ては同一でなくても良い)場合，その状態を ***安全状態*** と呼ぶ(図 2).

定義 5：回路 C に対し，C の全状態が安全状態である(入出力割当ては同一でなくても良い)場合，C を ***強セキュアな SR 回路*** と呼ぶ(図 2(a)).

定義 6：回路 C に対し，C の全状態が安全状態かつ対応する入出力割当てが k 次拡張ドブルイングラフと同一の場合，C を ***強セキュアな SR 等価回路*** と呼ぶ.

2.1 強セキュアの判定

k 段ドブルイングラフを基に強セキュアの判定を行う場合，全状態を判定する必要がある．しかしながら，k 段 SR の状態数は 2^k となり，状態数は指数的に増加するため，k 段ドブルイングラフの生成は困難である．そのため，強セキュアであるか，否かの判定には記号シミュレーションを用いる.

記号シミュレーションを用いて判定を行う際，それぞれの状態が制御・観測からみて安全である必要がある.

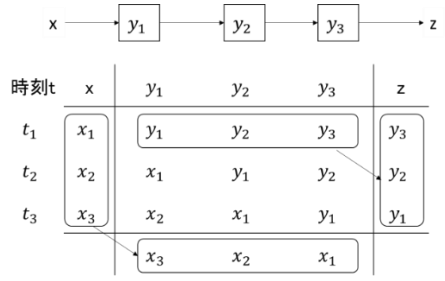
定義 7：回路 C において，任意の状態に遷移させる入力系列が，SR の入力系列と異なる場合，***スキャンイン安全*** と定義する.

定義 8：回路 C において，任意の状態から出力される長さ k の出力系列が，SR の出力系列と異なる場合，***スキャンアウト安全*** と定義する.

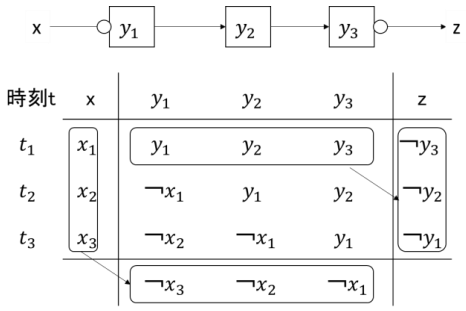
図 3(a)に，図 1(a)の回路に対する記号シミュレーションの結果，図 3(b)に，図 2(a)の回路に対する記号シミュレーションの結果を示す.

任意の状態$(y_1,y_2,y_3)=(x_3,x_2,x_1)$とし，この状態に遷移させる入力系列$\{x(t_1),x(t_2),x(t_3)\}$は記号シミュレーション結果より，SR では入力系列$\{x(t_1),x(t_2),x(t_3)\}=(x_1,x_2,x_3)$となり，図 3(b)の回路では入力系列$\{x(t_1),x(t_2),x(t_3)\}=(\neg x_1,\neg x_2,\neg x_3)$となる．二つの入力系列$(x_1,x_2,x_3)$，$(\neg x_1,\neg x_2,\neg x_3)$は異なっているため図 3(b)の回路はスキャンイン安全となる.

任意の状態を(y_1,y_2,y_3)とし，この状態から出力される出力系列$\{z(t_1),z(t_2),z(t_3)\}$は記号シミュレーション結果より，SR では出力系列$\{z(t_1),z(t_2),z(t_3)\}=(y_3,y_2,y_1)$となり，図 3(b)の回路では出力系列$\{z(t_1),z(t_2),z(t_3)\}=(\neg y_3,\neg y_2,\neg y_1)$となる．二つの出力系列$(y_3,y_2,y_1)$，$(\neg y_3,\neg y_2,\neg y_1)$は異なっているため図 3(b)の回路はスキャンアウト安全となる.

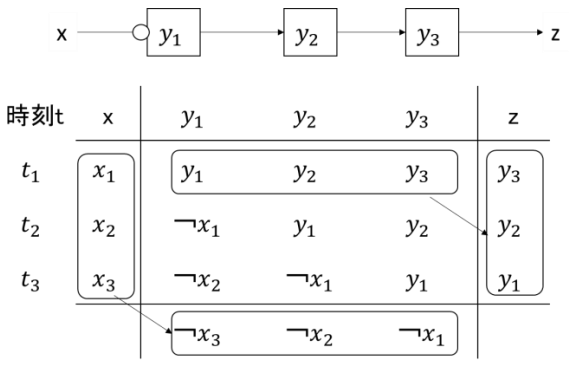


(a)SR 回路に対する記号シミュレーション結果

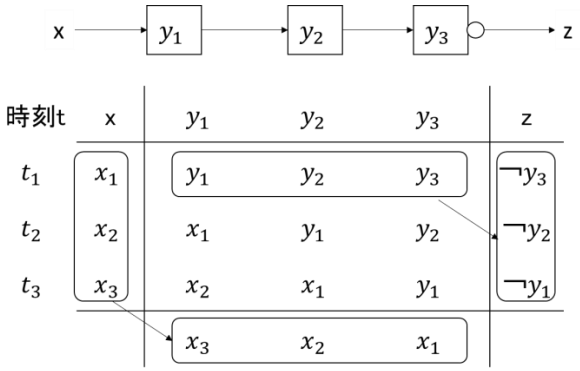


(b) 図 2(b)の回路に対する記号シミュレーション結果

図 3. 記号シミュレーションを用いた強セキュア判定



(a) スキャンアウト安全でない I²SR



(b) スキャンイン安全でない I²SR

図 4. 強セキュアでない I²SR

3. 強セキュアな SR 等価回路族と濃度

拡張 SR を実現する 5 種の線形回路，I²SR (Inverter Inserted Shift Register)，LF²SR (Linear Feed-Forward Shift Register)，LFSR (Linear Feedback Shift Register)，I²SR+LF²SR，I²SR+LFSR を用いて，強セキュアな SR 等価回路族と濃度について考察する．

3.1 I²SR

I²SR は SR 回路に NOT ゲートを挿入した回路である(図 2，図 3(b)参照)．

定理 1：外部入力を入力とする FF に対し、入力にのみ NOT ゲートを挿入し，回路全体で NOT ゲートがそれのみの I²SR はスキャンアウト安全ではない(図 4(a)参照)．

定理 2：FF からの出力が外部出力となる FF に対し，出力にのみ NOT ゲートを挿入し，回路全体で NOT ゲートがそれのみの I²SR はスキャンイン安全ではない(図 4(b)参照)．

k 段 I²SR の総数は NOT ゲートの挿入箇所が k+1 であることから，2^{k+1}-1 となる．強セキュアな k 段 I²SR は定理 1，定理 2 より 2^{k+1}-3 となる．また，SR 等価かつ強セキュアな k 段 I²SR は 2^k-1 となる．

3.2 LF²SR と LFSR

LF²SR は SR の入力方向から出力方向へ XOR ゲートによるフィードフォワードの接続を付加した回路である(図 5(a)参照)．

LFSR は SR の出力方向から入力方向へ XOR ゲートによるフィードバックの接続を付加した回路である(図 5(b)参照)．

定理 3：XOR ゲートのみを挿入された SR 回路で行われる演算は，排他的論理和のみとなる(図 5 参照)．すなわち，初期状態(0，0，…，0)に対して入力系列が(0，0，…，0)のときの遷移する状態は(0，0，…，0)かつ出力系列は(0，0，…，0)となる．したがって，LF²SR と LFSR に属する回路は，構造に関わらず強セキュアにならない．

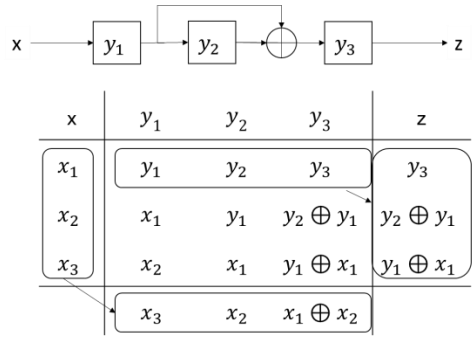
k 段 LF²SR，k 段 LFSR の総数は，どちらも $2^{k(k+1)/2}$-1 である．強セキュアな k 段 LF²SR，k 段 LFSR の数は定理 3 より 0(存在しない)となる．また，SR 等価かつ強セキュアな k 段 LF²SR，k 段 LFSR は，定理 3 より 0 となる．

3.3 I²SR+LF²SR と I²SR+LFSR

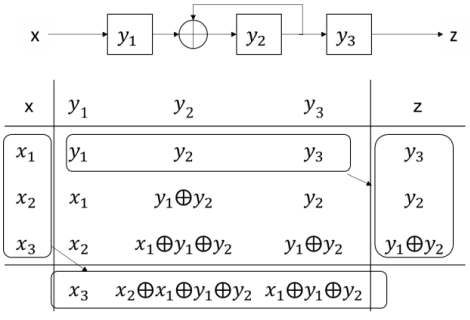
I²SR+LF²SR は LF²SR に NOT ゲートを，I²SR+LFSR は LFSR に NOT ゲートを挿入した回路である．

定理 4：SR 等価かつスキャンイン安全な I²SR+LF²SR は強セキュアである．

定理 5：SR 等価かつスキャンアウト安全な I²SR+LFSR は強セキュアである．



(a) LF²SR



(b) LFSR

図 5. LF²SR と LFSR

表 1. 定理 4，定理 5 の検証結果

	SR 等価回路総数	強セキュア回路数	非強セキュア回路数
I^2SR+LF^2SR	945	755	190
$I^2SR+LFSR$	945	758	187

定理 4，定理 5 の証明のため SREEP を用いて 4 段 $I^2SR+LF^2SR(I^2SR+LFSR)$を検証した(表 1 参照).

k 段 I^2SR+LF^2SR，k 段 $I^2SR+LFSR$ の総数は，どちらも$(2^{k(k+1)/2}-1)(2^{k+1}-1)$となる．定理 4，定理 5 より強セキュアな k 段 I^2SR+LF^2SR，k 段 $I^2SR+LFSR$ は少なくとも$(2^{k(k-1)/2}-1)(2^{k}-1)$となる．また，SR 等価かつ強セキュアな k 段 I^2SR+LF^2SR，k 段 $I^2SR+LFSR$ は，少なくとも$(2^{k(k-1)/2}-1)(2^{k}-1)$となる．

4. まとめと今後の方針

本論文では強セキュアな SR 等価回路の列挙を行い，強セキュアな SR 等価回路の個数を明らかにした．

今後の研究方針として[10, 11]で示されている SR 等価回路に対し，SR 等価性を維持しつつ SR 等価回路の強セキュアを実現する手法の提案を目指す．

参考文献

[1]. H. Fujiwara. *Logic Testing and Design for Testability.* The MIT Press,1985.

[2]. B.Yang, K. Wu, and R.Karri. “Scan based side channel attack on dedicated Hardware implementations of data eneryption standard,” International Test Conference 2004,pp339-344,2004

[3]. B. Yang, K.Wu, and R. Karri, “Secure scan: A design-for-test architecture for crypto chips,” IEEE Trans. on Computer-Aided Design of Integrated Circuits and Systems, vol.25, no.10, pp.2287–2293, 2006.

[4]. D. Hely, F. Bancel, M. L. Flottes, B. Rouzeyre, and N.Berard. “Scan design and secure chip” 10th IEEE Intertional On-line Testing Symposium,

[5]. J. Lee, M. Tehranipoor, C. Patel, and J. Plusquellic, “Securing designs against scan-based side-channel attacks,” IEEE Trans. on Dependable and Secure Computing, vol.4, no.4, pp.325–336, 2007.

[6]. S. Paul, R. S. Chakraborty, and S. Bhunia, “VIm-Scan: A low overhead scan design approach for protection of secret key in scan-based secure chips,” Proc. 25th IEEE VLSI Test Symposium. pp.455–460,2007.

[7]. G. Sengar, D. Mukhopadhyay, and D. R. Chowdhury, “Secured flipped scan-chain model for crypto-architecture,” IEEE Trans. On Computer-Aided Design of Integrated Circuits and Systems, vol.26, no.11, pp.2080–2084, Nov. 2007.

[8]. M.Inoue, T.Yoneda, M.Hasegawa, and H.Fujiwara,”Partial scan approach for secret information protection,”14th IEEE European Test Symposium, pp.143-148,May.2009

[9] U. Chandran, and D. Zhao, “SS-KTC: A high-testability lowoverhead scan architecture with multi-level security integration,” Proc. 27th IEEE VLSI Test Symposium, pp.321–326, 2009.

[10] H. Fujiwara, and M. E. J. Obien, “Secure and testable scan design using extended de Brujin graph,” Proc. 15th Asia and South Pacific Design Automation Conference, pp.413–418, 2010.

[11].H.Fujiwara,K.Fujiwara,and H.Tamamoto,”Enumeration and Synthesis of Shift Registar Equivalents for Secure Scan Design”, IEICE DC2009-58, pp13-18, 2009,12

[12]. K. Fujiwara, and H. Fujiwara, “Generalized feed-forward shift registers and their application to secure scan design,” IEICE Trans. on Inf. & Syst. vol.E96-D, no.5, pp.1125–1133, 2013.

[13]. Hideo FUJIWARA, Fellow and Katsuya FUJIWARA, Member, “Strongly Secure Scan Design Using Generalized Feed Forward Shift Registers”, IEICE Trans. on Information and Systems, Vol.E98-D, No.10, pp.1852-1855, October 2015