論　文

セキュアスキャン設計のためのシフトレジスタ等価回路の列挙と合成

藤原　克哉[†a)]　　藤原　秀雄[††]　　オビエン　マリー　エンジェリン[††]
玉本　英夫[†]

Enumeration and Synthesis of Shift Register Equivalents for Secure Scan Design

Katsuya FUJIWARA[†a)], Hideo FUJIWARA[††], Marie E. J. OBIEN[††],
and Hideo TAMAMOTO[†]

あらまし　セキュリティとテスタビリティは相反する性質であるが，それらを両立させることは重要である．セキュア（安全）でテスタブル（テスト容易）な回路設計が望まれている．筆者ら [13] は，代表的なテスト容易化設計手法であるスキャン設計において，シフトレジスタ等価回路を利用した安全でかつテスト容易なスキャン設計法を提案した．そのセキュリティレベルとして，攻撃者がスキャンレジスタの構造を推定する確率は，シフトレジスタと等価な回路数の逆数に比例することから，シフトレジスタ等価回路の個数を明らかにすることは重要である．本論文では，いくつかの線形回路構造を対象に，それらのシフトレジスタ等価回路族の濃度（回路数）や，それらを含む全体のシフトレジスタ等価回路族の濃度を解析的及びシミュレーションにより明らかにする．更に，各種のシフトレジスタ等価回路を列挙する問題，所望のシフトレジスタ等価回路を合成する問題，シフトレジスタ等価回路の状態を正当化・観測する問題，シフトレジスタ等価回路の安全状態を同定する問題を考察し，それらを解くプログラム SREEP (Shift Register Equivalents Enumeration and Synthesis Program) を紹介する．

キーワード　テスト容易化設計，セキュアスキャン，シフトレジスタ，機能等価，列挙

1. まえがき

暗号 LSI を含む多くの VLSI において，セキュア（安全）でテスタブル（テスト容易）な回路の設計は重要な課題である．現在広く使われている代表的なテスト容易化設計であるスキャン設計においては，回路内部のフリップフロップを直列に接続するスキャンモードにより，それらフリップフロップを外部から容易に制御・観測できるように設計されており，テスト容易性を飛躍的に向上することに成功している [2]．しかし，回路内部のフリップフロップ，レジスタを容易に制御・観測できるため，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えいの危険性が高いことが指摘されている [3]．

スキャンベース攻撃に耐えられるセキュアなスキャン方式がこれまでに研究され多くの報告がある [3]〜[11], [13]．その中で，筆者らは，シフトレジスタ等価回路を利用したセキュアでかつテスト容易なスキャン設計法を提案した [13]．そのセキュリティレベルを見るための一つの尺度として，スキャン（シフトイン・アウト）操作だけによる入出力対応からスキャンレジスタの構造を推定する確率を考えた場合，その推定が当たる確率はシフトレジスタと等価な回路数の逆数に比例することから，シフトレジスタ等価回路の個数を明らかにすることは重要と考えられる．本論文では，いくつかの線形回路構造を対象に，それらのシフトレジスタ等価回路族の濃度（回路数）や，それらを含む全体のシフトレジスタ等価回路族の濃度を解析的に明らかにする．解析的に示せない一部の線形回路構造については，シミュレーションにより明らかにする．更に，各種のシフトレジスタ等価回路を列挙する問題，所望のシフトレジスタ等価回路を合成する問題，シフトレジスタ等価回路の状態を正当化・観測する問題，シフトレジスタ等

† 秋田大学工学資源学部情報工学科，秋田市
Department of Computer Science and Engineering, Faculty of Engineering and Resource Science, Akita University, 1–1 Tegata-gakuen-machi, Akita-shi, 010–8502 Japan
†† 奈良先端科学技術大学院大学情報科学研究科，生駒市
Graduate School of Information Science, Nara Institute of Science and Technology, Ikoma-shi, 630–0192 Japan
a) E-mail: fujiwara@ie.akita-u.ac.jp

価回路の安全状態を同定する問題を考察し，それらを解くプログラム SREEP (Shift Register Equivalents Enumeration and Synthesis Program) を紹介する．

2. 拡張ドブルイングラフと SR 等価性

［定義 1］ k 段シフトレジスタ（SR と略す）の状態グラフ（状態遷移図）を k 次ドブルイングラフ (de Bruijn graph) という（図 1 参照．文献 [1]）．

［定義 2］ k 次ドブルイングラフと同型な状態グラフを k 次拡張ドブルイングラフと呼ぶ．状態割当，入出力割当は必ずしも同じでなくてよい（図 2 (a)〜(c) 参照．下線部分は，ドブルイングラフと異なる割当部分）．

［定義 3］ 状態グラフが k 次拡張ドブルイングラフである回路を k 段拡張シフトレジスタという（図 2 (a)〜(c) 参照）．

［定義 4］ 回路 C に対して，C の状態グラフが k 次ドブルイングラフと同型で，入力割当が k 次ドブルイングラフと同じとなる（状態割当，出力割当は必ずしも同じでなくてよい）頂点の対応が存在するならば，回路 C は k 段 SR 入力等価であるという（図 2 (a) 参照）．

［定義 5］ 回路 C に対して，C の状態グラフが k 次ドブルイングラフと同型で，出力割当が k 次ドブルイングラフと同じとなる（状態割当，入力割当は必ずしも同じでなくてよい）頂点の対応が存在するならば，回路 C は k 段 SR 出力等価であるという（図 2 (b) 参照）．

［定義 6］ 回路 C に対して，C の状態グラフが k 次ドブルイングラフと同型で，入出力割当が k 次ドブルイングラフと同じとなる（状態割当は必ずしも同じでなくてよい）頂点の対応が存在するならば，回路 C は k 段 SR 機能等価（略して k 段 SR 等価）であるという（図 2 (c) 参照）．

注意として，回路 C が k 段 SR 入力等価でかつ k 段 SR 出力等価であっても必ずしも k 段 SR 等価とは限らない（図 3 参照）．

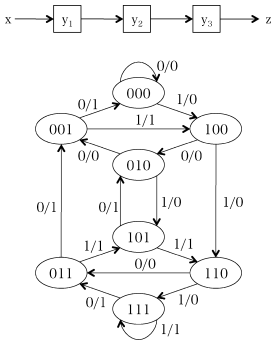


図 1　3 次ドブルイングラフ
Fig. 1　3-dimensional de Bruijn graph.

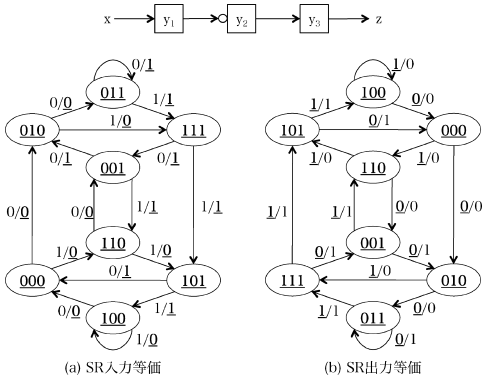


図 3　SR 入力等価で SR 出力等価だが SR 等価でない例
Fig. 3　An example of non SR equivalent.

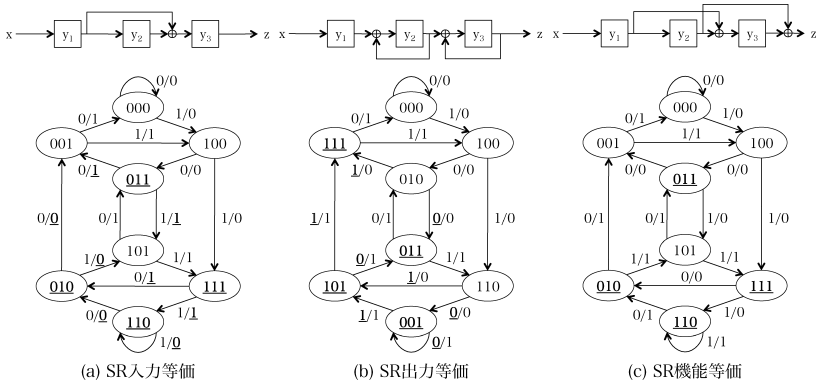


図 2　3 次拡張ドブルイングラフの例
Fig. 2　Examples of 3-dimensional extended de Bruijn graph.

3. シフトレジスタ等価回路族の濃度

拡張シフトレジスタを実現する線形回路構造として，I^2SR (Inverter Inserted Shift Register)，LF^2SR (Linear Feed-Forward Shift Register)，LFSR (Linear Feedback Shift Register)，LF^2SR+I^2SR，LFSR+I^2SR，LF^2SR+LFSR，LF^2SR+LFSR+I^2SR を考察する．

3.1 I^2SR

I^2SR はシフトレジスタに NOT ゲートを挿入した回路である．図 4 に示したように偶数個の NOT ゲートを含む I^2SR は SR 等価であることが分かる．一方，図 3 で示したように，奇数個の NOT ゲートを含む I^2SR は SR 入力等価であり SR 出力等価であるが SR 等価にはならない．

［定理 1］ 偶数個の NOT ゲートを含む I^2SR は SR 等価である．奇数個の NOT ゲートを含む I^2SR は SR 入力等価であり SR 出力等価であるが SR 等価でない．

k 段 I^2SR の総数は NOT ゲートの挿入箇所が $k+1$ あるので，総数 $2^{k+1}-1$ である．一方，SR 等価な k 段 I^2SR の総数は，定理 1 より偶数個の NOT ゲートを含む I^2SR だけの個数であり，2^k-1 となる．

［定理 2］ k 段 I^2SR の総数は $2^{k+1}-1$，SR 等価な k 段 I^2SR の総数は 2^k-1 である．

3.2 LF^2SR と LFSR

LF^2SR はシフトレジスタの入力側のフリップフロップから出力側のフリップフロップへ（前段から後段へ）XOR ゲートによるフィードフォワードの接続を（一般に複数個）付加した回路である．任意の LF^2SR は SR 入力等価であるが，図 5 (a) に示すように必ずしも SR 等価でない．しかし，図 5 (b) のように適当なフリップフロップから出力 z へのフィードフォワード接続を追加することで常に SR 等価にすることができる（後で考察するが，図 9 の記号シミュレーションの例を参照されたい）．

［定理 3］ 任意の LF^2SR は SR 入力等価である．LF^2SR は必ずしも SR 等価でないが，適当なフリップフロップから出力 z へのフィードフォワード接続を追加することで常に SR 等価にすることができる．ただし，LF^2SR が出力 z へのフィードフォワード接続だけの場合は，SR に変換される．

（証明） k 段 LF^2SR においては，初期状態に依存せず，長さ k の入力系列だけから最終状態が一意的に決まる．したがって，SR 入力等価であることが分かる．

長さ k の入力系列を $(x(1),x(2),\ldots,x(k))$，最終状態を $(y_1(k+1),y_2(k+1),\ldots,y_k(k+1))$ とするとき，長さ k の入力系列と最終状態とが 1 対 1 に対応しているので，最終状態 $(y_1(k+1),y_2(k+1),\ldots,y_k(k+1))$ から長さ k の入力系列 $(x(1),x(2),\ldots,x(k))$ を一意的に表現できる．線形回路であることからそれらは線形和で表現できる．したがって，最初の入力 $x(1)$ も $y_1(k+1),y_2(k+1),\ldots,y_k(k+1)$ のいくつかの変数の線形和で一意的に表現できる．この線形和が LF^2SR の出力となるように LF^2SR を変形すれば，$z(k+1)=x(1)$ となり，出力 $z(k+1)$ に k 時刻前の入力 $x(1)$ の値を出力できるので，LF^2SR は SR 等価となる．したがって，この線形和に現れる変数に対応するフリップフロップから出力 z へ XOR ゲートで接続するフィードフォワード接続を実現すれば，LF^2SR は SR 等価となる．

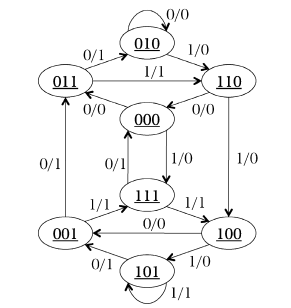


図 4 偶数個の NOT を含む I^2SR の例
Fig. 4 I^2SR with even number of inversions.

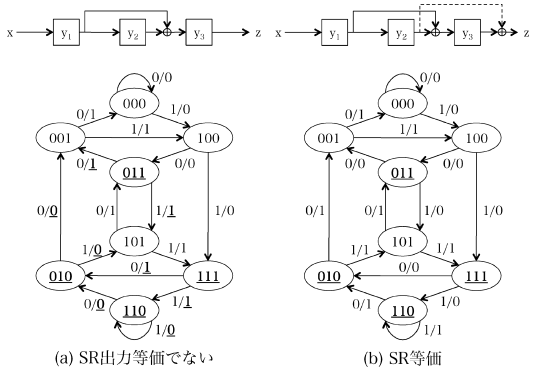


図 5 LF^2SR の SR 等価変更の例
Fig. 5 Modification to SR equivalent (LF^2SR).

その実現は次のように行うことができる．すなわち，それらのフィードフォワード接続が，もとの LF^{2}SR の出力 z に存在しない場合はそれを追加し，それらのフィードフォワード接続以外の出力 z への接続が既に存在すれば，その接続を消去するためにそれと同じフィードフォワード接続を追加する（線形和の性質から同じ接続を追加することは，その接続を消去することと等価）．ただし，もとの LF^{2}SR のフィードフォワード接続が出力 z への接続だけの場合，$y_k(k+1) = x(1)$ となる．その場合は，それらの接続がすべて消去すべき接続となり，SR そのものに変換される．

（証明終）

LFSR はシフトレジスタの出力側のフリップフロップから入力側のフリップフロップへ（後段から前段へ）XOR ゲートによるフィードバックの接続を（一般に複数個）付加した回路である．任意の LFSR は SR 出力等価であるが，図 6 (a) に示すように必ずしも SR 等価でない．しかし，図 6 (b) のように適当なフリップフロップから入力 x へのフィードバック接続を追加することで常に SR 等価にすることができる．

［定理 4］ 任意の LFSR は SR 出力等価である．LFSR は必ずしも SR 等価でないが，適当なフリップフロップから入力 x へのフィードバック接続を追加することで常に SR 等価にすることができる．ただし，LFSR が入力 x へのフィードバック接続だけの場合は，フィードバック接続追加で SR に変換される．

（証明） k 段 LFSR においては，入力系列に依存せず，長さ k の出力系列は初期状態だけから一意的に決まる．したがって，SR 出力等価であることが分かる．

初期状態を $(y_1(1), y_2(1), \ldots, y_k(1))$，長さ $k+1$ の出力系列を $(z(1), z(2), \ldots, z(k), z(k+1))$ とすると

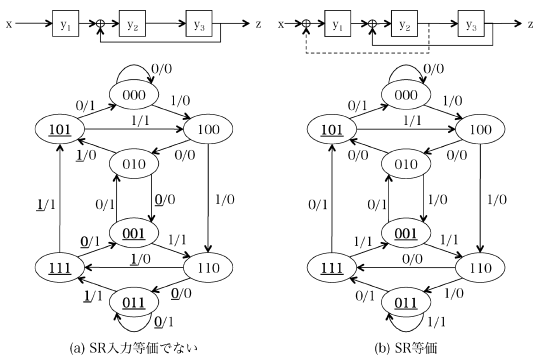


図 6　LFSR の SR 等価変更の例
Fig. 6　Modification to SR equivalent (LFSR).

き，各出力 $z(1), z(2), \ldots, z(k)$ は，初期状態から一意的に決まり，各々，$y_1(1), y_2(1), \ldots, y_k(1)$ のいくつかの変数の線形和で表現できる．出力 $z(t+1)$ は，初期状態 $(y_1(1), y_2(1), \ldots, y_k(1))$ と最初の入力 $x(1)$ とで一意的に決まり，$x(1)$ と $y_1(1), y_2(1), \ldots, y_k(1)$ のいくつかの変数の線形和で一意的に表現される．この線形和が LFSR の入力となるように LFSR を変形すれば，$z(k+1) = x(1)$ となり，出力 $z(k+1)$ に k 時刻前の入力 $x(1)$ の値を出力できるので，LFSR は SR 等価となる．したがって，この線形和に現れる変数に対応するフリップフロップから入力 x へ XOR ゲートで接続するフィードバック接続を実現すれば，LFSR は SR 等価となる．

その実現は次のように行うことができる．すなわち，それらのフィードバック接続が，もとの LFSR の入力 x に存在しない場合はそれを追加し，それらのフィードバック接続以外の入力 x への接続が既に存在すれば，その接続を消去するためにそれと同じフィードバック接続を追加する．ただし，もとの LFSR のフィードバック接続が入力 x への接続だけの場合，$z(k+1) = y_1(2)$ となる．その場合は，$z(k+1) = y_1(2) = x(1)$ とするために，それらの接続がすべて消去すべき接続となり，SR そのものに変換される．　（証明終）

k 段 LF^{2}SR の総数は，$2^{k(k+1)/2} - 1$ である．同様に，k 段 LFSR の総数も，$2^{k(k+1)/2} - 1$ である．

$(k-1)$ 段 LF^{2}SR の出力側にフリップフロップを 1 個追加して k 段 LF^{2}SR とする．この k 段 LF^{2}SR は必ずしも SR 等価でないので，定理 3 により SR 等価に変更する．ここでフリップフロップを 1 個追加しているので常に SR でない SR 等価回路にできる．このようにしてできる SR 等価な k 段 LF^{2}SR の個数は $(k-1)$ 段 LF^{2}SR の総数となり，$2^{k(k-1)/2} - 1$ である．したがって，SR 等価な k 段 LF^{2}SR は，少なくとも $2^{k(k-1)/2} - 1$ 個あることが分かる．

［定理 5］ k 段 LF^{2}SR の総数は，$2^{k(k+1)/2} - 1$ である．SR 等価な k 段 LF^{2}SR の個数は，少なくとも $2^{k(k-1)/2} - 1$ である．

同様に，LFSR について，$(k-1)$ 段 LFSR の入力側にフリップフロップを 1 個追加して k 段 LFSR とする．この k 段 LFSR は必ずしも SR 等価でないので，定理 4 により SR 等価に変更する．ここでフリップフロップを 1 個追加しているので常に SR でない SR 等価回路にできる．このようにしてできる SR 等価な k 段 LFSR の個数は $(k-1)$ 段 LFSR の総数と

なり，$2^{k(k-1)/2}-1$ である．したがって，SR 等価な k 段 LFSR は，少なくとも $2^{k(k-1)/2}-1$ 個あることが分かる．

［定理 6］ k 段 LFSR の総数は，$2^{k(k+1)/2}-1$ である．SR 等価な k 段 LFSR の個数は，少なくとも $2^{k(k-1)/2}-1$ である．

3.3 LF^{2}SR+I^{2}SR と LFSR+I^{2}SR

LF^{2}SR+I^{2}SR は LF^{2}SR に NOT ゲートを挿入した回路である．LFSR+I^{2}SR は LFSR に NOT ゲートを挿入した回路である．定理 3，4 と同様に次の定理 7，8 が成り立つ．

［定理 7］ 任意の LF^{2}SR+I^{2}SR は SR 入力等価である．LF^{2}SR+I^{2}SR は必ずしも SR 等価でないが，適当なフリップフロップから出力 z へのフィードフォワード接続を追加し，必要に応じて出力 z に NOT ゲートも追加することで常に SR 等価にすることができる．ただし，SR に変換される場合がある．

［定理 8］ 任意の LFSR+I^{2}SR は SR 出力等価である．LFSR+I^{2}SR は必ずしも SR 等価でないが，適当なフリップフロップから入力 x へのフィードバック接続を追加し，必要に応じて入力 x に NOT ゲートも追加することで常に SR 等価にすることができる．ただし，SR に変換される場合がある．

k 段 LF^{2}SR+I^{2}SR の総数は，k 段 LF^{2}SR と k 段 I^{2}SR の総数の積なので，$(2^{k(k+1)/2}-1)(2^{k+1}-1)$ である．同様に，k 段 LFSR+I^{2}SR の総数も，$(2^{k(k+1)/2}-1)(2^{k+1}-1)$ である．

$(k-1)$ 段 LF^{2}SR+I^{2}SR の出力側にフリップフロップを 1 個追加して k 段 LF^{2}SR+I^{2}SR とする．この k 段 LF^{2}SR+I^{2}SR は必ずしも SR 等価でないので，定理 7 により SR 等価に変更する．ここでフリップフロップを 1 個追加しているので常に SR でない SR 等価回路にできる．このようにしてできる SR 等価な k 段 LF^{2}SR+I^{2}SR の個数は $(k-1)$ 段 LF^{2}SR+I^{2}SR の総数となり，$(2^{k(k-1)/2}-1)(2^k-1)$ である．したがって，SR 等価な k 段 LF^{2}SR+I^{2}SR は，少なくとも $(2^{k(k-1)/2}-1)(2^k-1)$ 個あることが分かる．

［定理 9］ k 段 LF^{2}SR+I^{2}SR の総数は，$(2^{k(k+1)/2}-1)(2^{k+1}-1)$ である．SR 等価な k 段 LF^{2}SR+I^{2}SR の個数は，少なくとも $(2^{k(k-1)/2}-1)(2^k-1)$ である．

同様に，$(k-1)$ 段 LFSR+I^{2}SR の入力側にフリップフロップを 1 個追加して k 段 LFSR+I^{2}SR とする．この k 段 LFSR+I^{2}SR は必ずしも SR 等価でないので，定理 8 により SR 等価に変更する．ここでフリップフロップを 1 個追加しているので常に SR でない SR 等価回路にできる．このようにしてできる SR 等価な k 段 LFSR+I^{2}SR の個数は $(k-1)$ 段 LFSR+I^{2}SR の総数となり，$(2^{k(k-1)/2}-1)(2^k-1)$ である．したがって，SR 等価な k 段 LFSR+I^{2}SR は，少なくとも $(2^{k(k-1)/2}-1)(2^k-1)$ 個あることが分かる．

［定理 10］ k 段 LFSR+I^{2}SR の総数は，$(2^{k(k+1)/2}-1)(2^{k+1}-1)$ である．SR 等価な k 段 LFSR+I^{2}SR の個数は，少なくとも $(2^{k(k-1)/2}-1)(2^k-1)$ である．

3.4 LF^{2}SR+LFSR と LF^{2}SR+LFSR+I^{2}SR

LF^{2}SR+LFSR は LF^{2}SR と LFSR を，LF^{2}SR+LFSR+I^{2}SR は LF^{2}SR と LFSR と I^{2}SR を合成した回路である．定理 2，5，6 より次の定理が成り立つ．

［定理 11］ k 段 LF^{2}SR+LFSR の総数は $(2^{k(k+1)/2}-1)^2$ で，k 段 LF^{2}SR+LFSR+I^{2}SR の総数は，$(2^{k(k+1)/2}-1)^2(2^{k+1}-1)$ である．

SR 等価な k 段 LF^{2}SR+LFSR 及び LF^{2}SR+LFSR+I^{2}SR の個数については，SR 等価回路列挙合成プログラム SREEP で求めた実数を，この後，**5.** で紹介する．

3.5 全 SR 等価回路族の濃度

これまで考察した各回路族の濃度（回路数）を表 1 に，包含関係を図 7 に示す．図において，灰色の部分の濃度は，

$= (2^k-1)+2(2^{k(k-1)/2}-1)+2(2^{k(k-1)/2}-1)(2^k-1)$

$= 2\times 2^{k(k+1)/2}-2^k-1$

となる．

次に，k 段 SR 等価回路の総数を考察する．k 段 SR の状態グラフと同型な状態グラフで状態割当だけが異なる状態グラフは，2^k 個の状態に 2^k 個の状態値を割り当てる順列の数 $2^k!$ だけ存在する．各状態グラフに対応する状態遷移表において，状態変数を置換しても，実現される回路は状態変数の名前が変わるだけで

表 1 各クラスの濃度
Table 1 Cardinality of each class.

クラス	I^{2}SR	LF^{2}SR, LFSR	LF^{2}SR+I^{2}SR, LFSR+I^{2}SR	LF^{2}SR+LFSR	LF^{2}SR+LFSR+I^{2}SR
SR 等価回路数 各クラスの総数	$\frac{2^k-1}{2^{k+1}-1}$	$\frac{\geq 2^{k(k-1)/2}-1}{2^{k(k+1)/2}-1}$	$\frac{\geq (2^{k(k-1)/2}-1)(2^k-1)}{(2^{k(k+1)/2}-1)(2^{k+1}-1)}$	$\frac{?}{(2^{k(k+1)/2}-1)^2}$	$\frac{?}{(2^{k(k+1)/2}-1)^2(2^{k+1}-1)}$

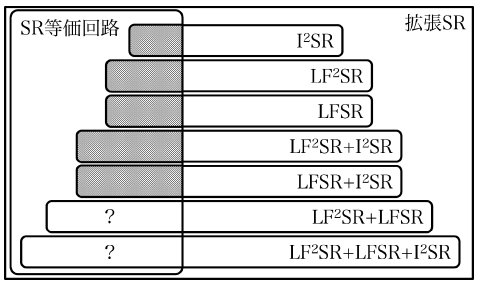


図 7　各クラスの包含関係
Fig. 7　Covering relation among classes.

表 2　SR 等価回路数（下限）/各クラスの総数（計算値）
Table 2　Cardinality of SR equivalents (lower bound)/extended SRs.

段数 k	I^2SR	LF^2SR, LFSR	LF^2SR+I^2SR, $LFSR+I^2SR$
1	$\frac{1}{3}$	$\frac{0}{1}$	$\frac{0}{3}$
2	$\frac{3}{7}$	$\frac{1}{7}$	$\frac{3}{49}$
3	$\frac{7}{15}$	$\frac{7}{63}$	$\frac{49}{945}$
4	$\frac{15}{31}$	$\frac{63}{1{,}023}$	$\frac{945}{31{,}713}$
5	$\frac{31}{63}$	$\frac{1{,}023}{32{,}767}$	$\frac{31{,}713}{2{,}064{,}321}$
6	$\frac{63}{127}$	$\frac{32{,}767}{2{,}097{,}151}$	$\frac{2{,}064{,}321}{266{,}338{,}177}$

同じ回路となる．このような置換同値となる個数は $k!$ 個存在する．$2^k!$ 個の状態グラフを同じ回路を実現する置換同値で分類すると，$2^k!/k!$ 個の同値類に分類できる．このことから，k 段 SR 等価回路数 $N(k)$ は，$N(k) \leq 2^k!/k! - 1$ がいえる．一方，二つの異なる状態遷移表（グラフ）T，T' が置換同値でないならば，T，T' を実現する回路 C，C' に対して各々のフリップフロップ y_i，$y_i{}'$ $(1 \leq i \leq k)$ の入力関数が等しくなるような対応が存在しないことになり，C と C' は等価でなく，異なる回路である．すなわち，異なる置換同値類に属する状態グラフは異なる回路を実現している．それらの同値類の数は $2^k!/k!$ であるので，SR そのものを除き，k 段 SR 等価回路数 $N(k)$ はちょうど，$N(k) = 2^k!/k! - 1$ となる．

表 2 に，I^2SR，LF^2SR，LFSR，LF^2SR+I^2SR，$LFSR+I^2SR$ の 5 種類のクラスについて，SR 等価回路数を示したが，$LF^2SR+LFSR$，$LF^2SR+LFSR+I^2SR$ のクラスについても，実際にどれだけの SR 等価回路数が存在するかを調べるためのプログラムを作成した．これについては次章で紹介する．

4. SREEP

前章で SR 等価回路数を解析的に明らかにしたが，一部のクラスについては示せていない．それらのクラスについても SR 等価回路数を調べるために，SR 等価回路を列挙し，SR 等価であるかを判定するプログラム SREEP (Shift Register Equivalents Enumeration and Synthesis Program) を作成した．更に SREEP では，SR 等価回路をスキャン設計に適用する際に考察する必要のある問題として，所望の SR 等価回路を合成する問題，SR 等価回路と SR の状態対応関係を表現する問題，SR 等価回路の安全状態を同定する問題についても，それらを解くプログラムを作成し，統合した．

列挙問題を解くモードでは，拡張 SR の各クラスの SR 等価回路の実数を求めるために，まず拡張 SR 回路を列挙し，各回路の SR 等価の判定を行い，判定結果を出力する．回路の等価性判定には，記号シミュレーションを用いる．k 段拡張 SR の場合，時刻 t の外部入力と，時刻 $t+k$ の外部出力を展開した論理式が一致すれば，その回路は SR 等価といえる．

列挙問題のほか，合成問題，状態対応問題，安全状態同定問題についての詳細は，次章以降で述べる．

SREEP では，計算結果を見やすくするために，結果を回路図と表形式で表示する GUI 機能を作成した．**3.** で対象とした拡張 SR を実現する 7 種類の線形回路の表現形式として，それらの線形回路のすべてを一意的に表現可能な SR-ID を用いる．それらの線形回路構造は，外部入力/各フリップフロップ出力/NOT 用定数 1 から，各フリップフロップ入力/外部出力への XOR 接続の有無で表現できる．SR-ID は，接続の有無をビット行列で表したものである．SR-ID の外部表現形式には，図 8 の中央に示すような 16 進表記を用いる．

SREEP では，より効率的に判定を行うために，対象回路に特化した記号シミュレータを実現した．対象の拡張 SR 回路は，フリップフロップと XOR ゲートのみで表現することで，中間変数の論理式は階層のない構造にできる．フリップフロップ入力に時刻ごとに中間変数をおき，簡単化を行いながら論理式を展開していくことで項数の増大を抑えた．簡単化を効率良く行うために，時刻 $t+k$ の変数から順に時刻 t までさかのぼりながら展開する．また，シミュレーションの前段階として，計算済みの結果から辞書を構築し，部

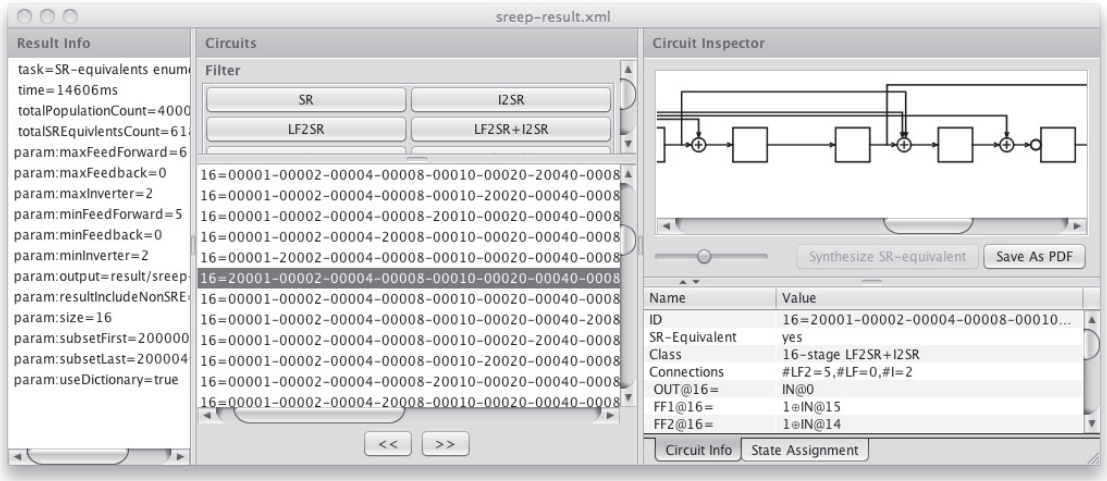


図 8　SREEP の実行結果表示例 1
Fig. 8　Outcome example 1 by SREEP.

分回路の構造が一致するものはあらかじめ辞書を用いて判定する．更に，項数の増加に備えて，論理式の構造を工夫した．論理式を変数を要素とする配列構造とした場合，項数に比例して論理式の展開や簡単化の計算効率が低下する．一方，変数の種類の増加には影響されない．論理式を変数の有無をビットで示すビット列構造とした場合，項数が増えても計算効率を一定にできる．ただし，変数の種類が増えると計算効率が低下する．そこで，よく使う変数をビット列構造で，それ以外の変数を配列構造で表現することにした．

7 種類の k 段 ($k = 1, 2, \cdots, 6$) 拡張 SR すべての SR 等価判定の実験では，辞書を利用しない場合，Xeon X5550 2.66 GHz × 2 搭載の計算機で 1 ミリ秒当り判定できる回路数は，$k = 4, 5, 6$ でそれぞれ約 1,590 回路，1,685 回路，1,785 回路であった．この計算機での計算時間は，$k = 4, 5$ でそれぞれ 21.1 秒，11 時間 19 分 51 秒かかった．$k = 6$ は，分散計算環境で約 4 週間かかった．SREEP は，Java SE 6 を用いて開発した．プログラムサイズは約 7,500 ステップ，Mac OS X，Windows 7 の各プラットホームで動作する．

5. SR 等価回路の列挙問題

SREEP を用いて，I^2SR, LF^2SR, LFSR, LF^2SR+I^2SR, LFSR+I^2SR, LF^2SR+LFSR, LF^2SR+LFSR+I^2SR の各クラスに対して，$k = 1, 2, 3, 4, \cdots$ と該当するすべての回路を列挙し，SR 等価判定を行った．

I^2SR，LF^2SR，LFSR，LF^2SR+I^2SR，LFSR+I^2SR の 5 種類のクラスについては，SR 等価回路数の実数が表 2 で示した計算値（下限）と一致した．このことから，定理 5，6，9，10 で示した SR 等価回路数の下限値は，実数値であることが予想される．

表 3　SREEP による SR 等価回路数/各クラスの総数
Table 3　Cardinality of SR equivalents by SREEP/extended SRs.

段数 k	LF^2SR+LFSR	LF^2SR+LFSR+I^2SR
1	$\frac{0}{1}$	$\frac{0}{3}$
2	$\frac{0}{49}$	$\frac{0}{343}$
3	$\frac{12}{3{,}969}$	$\frac{84}{59{,}535}$
4	$\frac{905}{1{,}046{,}529}$	$\frac{13{,}575}{32{,}442{,}399}$
5	$\frac{198{,}505}{1{,}073{,}676{,}289}$	$\frac{6{,}153{,}655}{67{,}641{,}606{,}207}$
6	$\frac{180{,}038{,}401}{4{,}398{,}042{,}316{,}801}$	$\frac{11{,}342{,}419{,}263}{558{,}551{,}374{,}233{,}727}$

LF^2SR+LFSR, LF^2SR+LFSR+I^2SR については，SREEP の求めた SR 等価回路数の実数を表 3 に示す．

SREEP では，所望のパラメータ，制約（回路構造，段数 k，フィードフォワード数の上下限，フィードバック数の上下限，等）を満たすすべての SR 等価回路を生成することができる．

図 8 に，$k = 16$ での実行例を示す．

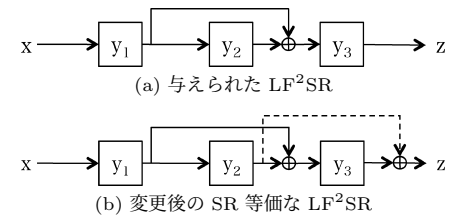
6. SR 等価回路の合成問題

セキュアスキャン設計に用いるシフトレジスタ等価な回路をどのように合成するかは，実用上重要な問題である．

SR 等価な回路としては，回路の状態正当化・状態観測を容易に行うために，接続情報からスキャン入出力系列を容易に構成できることが重要である．そのためには，I^2SR，LF^2SR，LFSR，LF^2SR+I^2SR，LFSR+I^2SR 等の線形回路構造での SR 等価回路が望ましい．また，スキャンテスト時の消費電力を削減するためにスキャンチェインに NOT ゲート挿入，XOR によるフィードフォワード接続を追加する方法が提案されており [12]，その意味で上記の線形回路構造での SR 等価回路は有効である．このように既に所望の拡張シフトレジスタが与えられたとき，更にセキュアとするために，SR 等価な回路に変更する問題が考えられる．すなわち，任意に与えられた拡張シフトレジスタに対して，それが SR 等価であるか否かを判定し，SR 等価でないときは，最少の変更で SR 等価回路を合成する問題は重要である．

そこで，与えられた拡張シフトレジスタを SR 等価な回路に変更する問題を考えよう．

図 9 (a) の 3 段 LF^2SR が与えられたとしよう．図 9 (c) の記号シミュレーションにより，$k+1=4$ 時刻目の出力が $a_2 \oplus a_3$ であるので，$k+1=4$ 時刻目で a_2 の値を有する y_2 の値を z へ線形加算すればいいので，y_2 から z へフィードフォワード線を追加すればよい．図 9 (b) が SR 等価に変更された回路である．このように k 段 LF^2SR の場合，記号シミュレーションによる $k+1$ 時刻目の出力から一意的に追加すべきフィードフォワード線が求まる．



(a) 与えられた LF^2SR

(b) 変更後の SR 等価な LF^2SR

		x	y_1	y_2	y_3	z
a_1	a_2	a_3	b_1	b_2	b_3	b_3
	a_1	a_2	a_3	b_1	$b_1 \oplus b_2$	$b_1 \oplus b_2$
		a_1	a_2	a_3	$a_3 \oplus b_1$	$a_3 \oplus b_1$
			a_1	a_2	$a_2 \oplus a_3$	$a_2 \oplus a_3$

(c) 記号シミュレーション

図 9　SR 等価回路への変更例
Fig. 9　Modification to SR equivalent.

図 9 の例を SREEP で求めた実行結果を図 10 に示す．

LFSR の場合は，記号シミュレーションによる $k+1$ 時刻目の出力から線形加算すべき値を求め，1 時刻目にその値を有するフリップフロップから入力 x へフィードバック線を追加する．追加すべきフィードバック線は複数の場合もあるが，一意的に決まる．

LF^2SR+I^2SR (LFSR+I^2SR) の場合は，記号シミュレーション結果の $k+1$ 時刻目の出力から出力 z（入力 x）に NOT ゲートを追加すべきかが決まる．図 11 に LFSR+I^2SR の例を示す．この場合，$1 \oplus b_2$ を削除するために，y_2 からのフィードバック線と NOT が入力 x に追加され，結果もとの NOT は削除されている．

7.　SR 等価回路の状態正当化・観測問題

合成された SR 等価回路において，回路を所望の状態に遷移させるための入力系列を求める状態正当化問題，出力系列から回路の初期状態を同定する状態観測問題は，SR 等価回路をシフトレジスタとして利用す

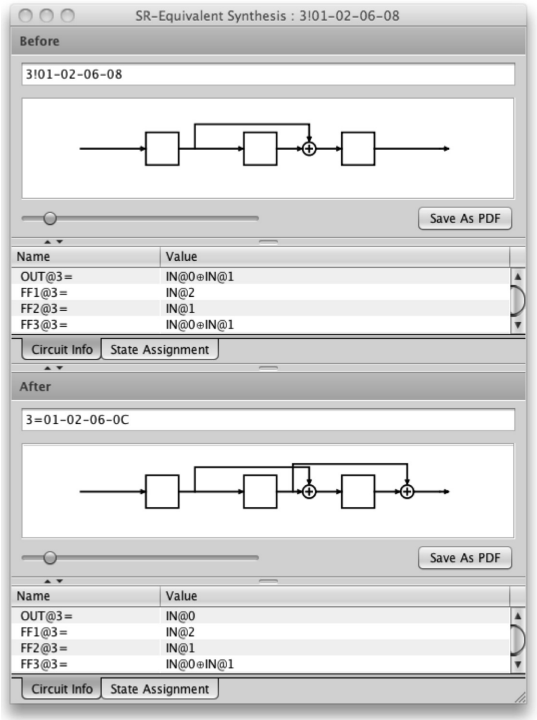
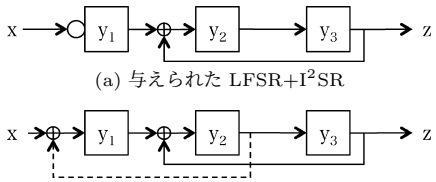


図 10　SREEP の実行結果表示例 2
Fig. 10　Outcome example 2 by SREEP.



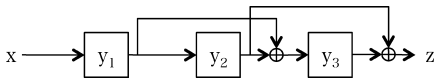
(a) 与えられた LFSR+I^{2}SR

(b) 変更後の SR 等価な LFSR

		x	y_1	y_2	y_3	z
a_1	a_2	a_3	b_1	b_2	b_3	b_3
	a_1	a_2	$a_3 \oplus 1$	$b_1 \oplus b_3$	b_2	b_2
		a_1	$a_2 \oplus 1$	$a_3 \oplus 1 \oplus b_2$	$b_1 \oplus b_3$	$b_1 \oplus b_3$
			$a_1 \oplus 1$	$a_2 \oplus 1 \oplus b_1 \oplus b_3$	$a_3 \oplus 1 \oplus b_2$	$a_3 \oplus 1 \oplus b_2$

(c) 記号シミュレーション

図 11　SR 等価回路への変更例 2
Fig. 11　Modification to SR equivalent.



(a) 与えられた LF^{2}SR

	x	y_1	y_2	y_3	z
t-3	x(t-3)= a_3	b_1	b_2	b_3	$b_2 \oplus b_3$
t-2	x(t-2)= a_2	a_3	b_1	$b_1 \oplus b_2$	b_2
t-1	x(t-1)= a_1	a_2	a_3	$a_3 \oplus b_1$	b_1
t		$y_1(t)=a_1$	$y_2(t)=a_2$	$y_3(t)=a_2 \oplus a_3$	a_3

$x(t-3)=a_3=a_2 \oplus a_2 \oplus a_3=y_2(t) \oplus y_3(t)$
$x(t-2)=a_2=y_2(t)$
$x(t-1)=a_1=y_1(t)$

(b) 最終状態から遷移入力系列を求める

	x	y_1	y_2	y_3	z
t	a_3	$y_1(t)=b_1$	$y_2(t)=b_2$	$y_3(t)=b_3$	$z(t)=b_2 \oplus b_3$
t+1	a_2	a_3	b_1	$b_1 \oplus b_2$	$z(t+1)=b_2$
t+2	a_1	a_2	a_3	$a_3 \oplus b_1$	$z(t+2)=b_1$
t+3		a_1	a_2	$a_2 \oplus a_3$	a_3

$y_1(t)=b_1=z(t+2)$
$y_2(t)=b_2=z(t+1)$
$y_3(t)=b_3=b_2 \oplus b_3 \oplus b_2=z(t) \oplus z(t+1)$

(c) 出力系列から初期状態を求める

図 12　状態対応問題の解法例
Fig. 12　State-justification and state-observation.

る際に必要な問題である．

図 12 (a) の SR 等価な 3 段 LF^{2}SR が与えられたとしよう．記号シミュレーション結果を用いて，最終状態の状態変数から，それに遷移させる入力系列は図 12 (b) のように求まる．同様に，出力系列から回路の初期状態を特定する問題は図 12 (c) のように求まる．他の SR 等価な線形回路に対しても，同様に求めることができる．したがって，次の定理 12，13 が成り立つ．

［定理 12］ SR 等価な k 段線形 SR に対して，状態 $(y_1(t), y_2(t), \cdots, y_k(t))$ に遷移するための入力系列 $x(t-k), x(t-k+1), \cdots, x(t-1)$ の各時刻の入力 $x(t-i)$ は，$y_1(t), y_2(t), \cdots, y_k(t)$，及び定数 1 の線形和で表現できる．

［定理 13］ SR 等価な k 段線形 SR に対して，状態 $(y_1(t), y_2(t), \cdots, y_k(t))$ の各状態変数 $y_i(t)$ は，各時刻の出力 $z(t), z(t+1), \cdots, z(t+k-1)$ 及び定数 1 の線形和として表現できる．

図 12 (b)，(c) の例を SREEP で求めた実行結果を図 13 に示す．

8. SR 等価回路の安全状態同定問題

与えられた回路が SR 等価回路であることが分かっているとき，その入出力対応だけからどれだけ回路内部に蓄えられた情報を観測できるかを考察しよう．まず，適当な長さの入力系列を印加し出力系列を観測することでこの SR 等価回路の段数 k を特定することができる．しかし，入出力対応は SR と同じであるため，入出力対応だけでは回路の構造（接続情報）を特定することはできない．回路構造を予測したとしても，その予測が当たる確率は $1/N(k)$ である．ここで，$N(k)$ は k 段 SR 等価回路の濃度．更に，その予測が当たったとしても攻撃者はそれを知ることができないので，回路構造を同定することはできない．

k 段 SR 等価回路においては，長さ k の出力系列からその初期状態を一意的に識別することができる（定理 13）．シフトレジスタ (SR) の場合は，その出力系列が初期状態の状態割当のビット列そのものである．したがって，k 段 SR 等価な回路において，状態割当のビット列がその状態から始まる長さ k の出力系列と

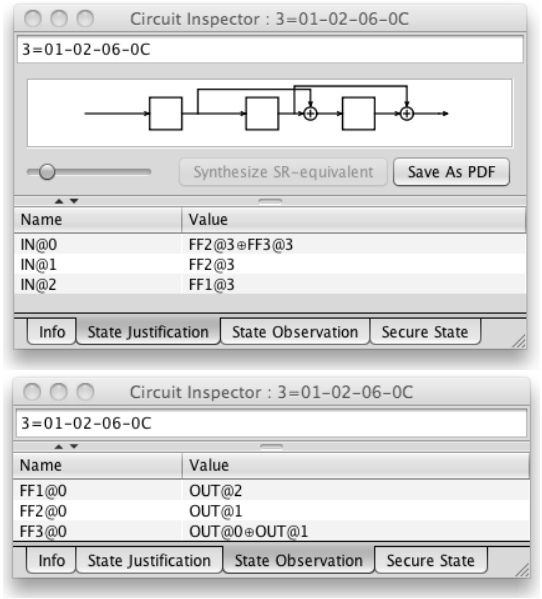


図 13　SREEP の実行結果表示例 3
Fig. 13　Outcome example 3 by SREEP.

同じ（すなわち，SR の状態割当と同じ）場合は，情報が漏えいするので安全でない状態と考え，異なる場合は安全な状態と考える．例えば，図 2 (c) において，010，011，110，111 の 4 状態は安全状態である．したがって，安全状態から始まる長さ k の出力応答系列はその状態割当のビット列と異なる．しかし，安全でない状態から始まる長さ k の出力系列はその状態割当と同じビット列となり，初期状態の状態割当が出力系列にそのまま現れてしまう．たとえ状態割当が出力系列に流れていても，攻撃者はその出力系列が初期状態のビット列と同じであるか否かを同定することはできない．しかし，情報は漏えいしていることになるため，秘密情報は安全状態にのみ蓄えることが望まれる．

そこで，安全状態を利用するためには，SR 等価回路の接続情報からどの状態が安全状態であるかを知ることが必要となる．図 12 (c) に示したように，SR 等価回路においては，初期状態 $(y_1(t), y_2(t), y_3(t))$ は出力系列 $z(t), z(t+1), z(t+2)$ の線形和で一意的に表現できる．

$y_1(t) = z(t+2)$，$y_2(t) = z(t+1)$，$y_3(t) = z(t) \oplus z(t+1)$

この初期状態が安全状態でない（すなわち，SR と同じ状態割当である）ための必要十分条件は

$y_1(t) = z(t+2)$，$y_2(t) = z(t+1)$，$y_3(t) = z(t)$

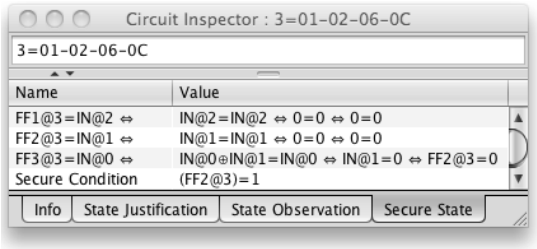


図 14　SREEP の実行結果表示例 4
Fig. 14　Outcome example 4 by SREEP.

であり，したがって，$y_3(t) = z(t) \oplus z(t+1) = z(t)$ となる．更に，$z(t) \oplus z(t+1) = z(t) \Leftrightarrow z(t+1) = 0 \Leftrightarrow y_2(t) = 0$ となる．このことから，初期状態 $(y_1(t), y_2(t), y_3(t))$ が安全状態であるための必要十分条件は，$y_2(t) = 1$ である．実際，図 12 の SR 等価回路では，状態割当の 2 ビット目が 1 となる，010，011，110，111 の 4 状態が安全状態である（図 2 (c) 参照）．

この例について SREEP で求めた実行結果を図 14 に示す．

このように，**7.** の SR 等価回路の状態対応問題で求めた線形和の関係式から安全状態の条件式を容易に求めることができる．

9. むすび

シフトレジスタ等価回路を利用したセキュアスキャン設計法 [13], [14] でのセキュリティレベルを明らかにするためには，シフトレジスタ等価回路族の濃度を明らかにすることが重要である．本論文では，7 種類の線形回路構造を対象に，それらのシフトレジスタ等価回路族の濃度や，それらを含む全体のシフトレジスタ等価回路族の濃度を解析的及びシミュレーションにより明らかにした．更に，各種のシフトレジスタ等価回路を列挙する問題，所望のシフトレジスタ等価回路を合成する問題，シフトレジスタ等価回路の状態を正当化・観測する問題，シフトレジスタ等価回路の安全状態を同定する問題を考察し，それらを解くプログラム SREEP を紹介した．

謝辞　本研究は一部，日本学術振興会科学技術研究費補助金基盤研究 (B)（課題番号 20300018）の研究助成による．

文　献

[1] S.W. Golomb, Shift Register Sequences, Aegean Park Press, 1982.
[2] H. Fujiwara, Logic Testing and Design for Testability,

The MIT Press, 1985.
[3] B. Yang, K. Wu, and R. Karri, “Scan based side channel attack on dedicated hardware implementations of data encryption standard,” International Test Conference 2004, pp.339–344, 2004.
[4] B. Yang, K. Wu, and R. Karri, “Secure scan: A design-for-test architecture for crypto chips,” IEEE Trans. Comput.-Aided Des. Integr. Circuits Syst., vol.25, no.10, pp.2287–2293, Oct. 2006.
[5] D. Hely, M.L. Flottes, F. Bancel, B. Rouzeyre, and N. Berard, “Scan design and secure chip,” 10th IEEE International On-Line Testing Symposium, pp.219–224, 2004.
[6] J. Lee, M. Tehranipoor, and J. Plusquellic, “A low-cost solution for protecting IPs against scan-based side-channel attacks,” 24th IEEE VLSI Test Symposium, pp.94–99, 2006.
[7] J. Lee, M. Tehranipoor, C. Patel, and J. Plusquellic, “Securing designs against scan-based side-channel attacks,” IEEE Trans. Dependable and Secure Computing, vol.4, no.4, pp.325–336, Oct.–Dec. 2007.
[8] S. Paul, R.S. Chakraborty, and S. Bhunia, “VIm-Scan: A low overhead scan design approach for protection of secret key inscan-based secure chips,” 25th IEEE VLSI Test Symposium, pp.455–460, 2007.
[9] G. Sengar, D. Mukhopadhyay, and D.R. Chowdhury, “Secured flipped scan-chain model for crypto-architecture,” IEEE Trans. Comput.-Aided Des. Integr. Circuits Syst., vol.26, no.11, pp.2080–2084, Nov. 2007.
[10] 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.
[11] U. Chandran and D. Zhao, “SS-KTC: A high-testability low-overhead scan architecture with multi-level security integration,” 27th IEEE VLSI Test Symposium, pp.321–326, May 2009.
[12] O. Sinanoglu and A. Orailoglu, “Modeling scan chain modifications for scan-in test power minimization,” International Test Conference 2003, pp.602–611, 2003.
[13] H. Fujiwara and M.E.J. Obien, “Secure and testable scan design using extended de Bruijn graph,” 15th Asia and South Pacific Design Automation Conference, pp.413–418, Jan. 2010.
[14] 藤原克哉，藤原秀雄，玉本英夫，“セキュアスキャン設計のためのシフトレジスタ等価回路の列挙と合成について，”信学技報，DC2009-58, 2009.

（平成 22 年 2 月 8 日受付，5 月 19 日再受付）

藤原　克哉　（正員）

1997 明治大・理工・情報科学卒．2002 同大大学院博士後期課程了．同年秋田大・工学資源・情報・助手，2007 同大・同学部・助教，現在に至る．平成 14 年度情報処理学会東北支部奨励賞受賞．ソフトウェア工学，ネットワークソフトウェアに関する研究に従事．情報処理学会，日本ソフトウェア科学会，IEEE Computer Society 各会員．

藤原　秀雄　（正員：フェロー）

1969 阪大・工・電子卒．1974 同大大学院博士課程了．同大・工・電子助手，明治大・工・電子通信助教授，情報科学教授を経て，現在奈良先端大・情報科学教授．1981 ウォータールー大客員助教授．1984 マッギル大客員准教授．論理設計論，フォールトトレランス，設計自動化，テスト容易化設計，テスト生成，並列処理，計算複雑度に関する研究に従事．著書「Logic Testing and Design for Testability」(MIT Press) など．大川出版賞，IEEE Computer Society Outstanding Contribution Award，IEEE Computer Society Meritorious Service Award など受賞．情報処理学会フェロー，IEEE Computer Society Golden Core Member，IEEE Fellow．

オビエン　マリー　エンジェリン

2005 Ateneo de Manila 大学・電子通信卒（フィリピン）．2008 同大・大学院・電子工学・修士課程了．2008 奈良先端大・情報科学研究科・博士後期課程入学．現在，同大学院博士後期課程 2 年在学中．VLSI のテスト，テスト容易化設計，セキュアスキャン設計に関する研究に従事．IEEE 学生員．

玉本　英夫　（正員）

1971 東大・工・電子卒．1976 同大大学院博士課程了．同年秋田大学鉱山学部電子工学科講師．1980 同電子工学科助教授．1991 同情報工学科助教授．1997 同工学資源学部情報工学科教授，現在に至る．この間，論理回路の故障診断，画像計測，マルチメディアなどの研究に従事．工博．情報処理学会，人工知能学会，計測自動制御学会，IEEE 各会員．