THE IEICE TRANSACTIONS ON INFORMATION AND SYSTEMS (JAPANESE EDITION)

電子情報通信学会 論文誌 D 情報・システム

VOL. J101-D NO. 8
AUGUST 2018

情報・システムソサイエティ

一般社団法人 電子情報通信学会
THE INFORMATION AND SYSTEMS SOCIETY
THE INSTITUTE OF ELECTRONICS, INFORMATION AND COMMUNICATION ENGINEERS

論　文

拡張シフトレジスタを用いた強セキュア回路設計とセキュリティの評価

山崎　紘史[†a)]　　細川　利典[†]　　藤原　秀雄[††]

Strongly Secure Scan Design Using Extended Shift Registers and Evaluation of Security

Hiroshi YAMAZAKI[†a)], Toshinori HOSOKAWA[†], and Hideo FUJIWARA[††]

あらまし　VLSI のテスト容易化技術として，フルスキャン設計が広く用いられている．フルスキャン設計は，回路内部のフリップフロップをスキャンフリップフロップとすることで，テスト容易性を大幅に向上させる．しかしながら，スキャンフリップフロップにより内部状態を任意に制御・観測できるため，暗号回路などにおいて秘密情報漏洩の危険性が指摘されている．そのため，安全なテスト容易化技術が求められている．安全なテスト容易化技術として，スキャンチェインを線形回路構造に変更するシフトレジスタ等価回路が提案されている．しかしながら，シフトレジスタ等価回路でも，一部の内部状態が制御・観測される可能性が残り，必ずしも安全ではない．そこで，シフトレジスタ等価回路より安全な強セキュア回路が提案された．本論文では，シフトレジスタ等価な拡張シフトレジスタに対して，シフトレジスタ等価性を失うことなく強セキュアな回路を設計する手法を提案する．また，シフトレジスタ等価かつ強セキュアな拡張シフトレジスタの回路数を明らかにし，セキュリティレベルを評価する．

キーワード　スキャン設計，シフトレジスタ等価回路，強セキュア，拡張シフトレジスタ，セキュリティ

1. まえがき

半導体微細化技術の進歩により，超大規模集積回路 (Very large scale integrated circuits：VLSI) の複雑化・高速化が進んでおり，VLSI のテストコストの増大が問題となっている．VLSI のテストコストは，VLSI の製品価格に影響を与えるため，VLSI のテストコストの削減は重要な課題である．VLSI のテストコスト削減技術の一つとして，テスト容易化設計 [1] が存在する．また，代表的なテスト容易化設計として，フルスキャン設計 [1] が広く利用されている．フルスキャン設計は回路内部のフリップフロップ (Flip-Flop：FF) をスキャン FF とすることで，FF を外部から容易に制御・観測できるようにする．そのため，フルスキャン設計が施された回路では，テスト容易性が大幅に向上する．しかしながら，フルスキャン設計が施された回路では，FF を外部から容易に制御・観測できるため，セキュリティの低下を招く可能性がある．特に，暗号回路などにおいては，スキャンベース攻撃による秘密鍵の情報漏洩の可能性が指摘されている [2]．そのため，安全かつテスト容易な回路設計が重要な課題である．

文献 [3]～[17] において，スキャンベース攻撃に対して安全かつテスト容易なセキュアスキャン設計法が提案されている．文献 [10], [12] において，シフトレジスタ (Shift Register：SR) に線形回路を追加した拡張 SR に対する SR 等価回路が提案されている．SR 等価回路は SR と機能等価であるが構造等価ではない．SR 等価回路は SR と機能等価であることから，与えられた入力系列に対して SR と同じ出力系列を得ることが可能である．しかしながら，構造等価ではないため，内部状態 (FF の状態) が SR と異なる．そのため，SR 等価回路は，スキャン FF の回路構造が特定

† 日本大学生産工学部，習志野市
College of Industrial Technology, Nihon University, 1–2–1 Izumi-cho, Narashino-shi, 275–8575 Japan
†† 大阪学院大学情報学部，吹田市
Faculty of Informatics, Osaka Gakuin University, 2–36–1 Kishibe-Minami, Suita-shi, 564–8511 Japan
a) E-mail: yamazaki.hiroshi@nihon-u.ac.jp
DOI:10.14923/transinfj.2018JDP7009

されにくく，スキャンベース攻撃に対して有効であることが報告されている [10]．文献 [11], [12] において，拡張 SR を SR 等価に設計する方法が提案さている．また，文献 [11], [12] では，拡張 SR の各クラスの回路数，SR 等価な拡張 SR の回路数が明らかにされている．文献 [13] では，拡張 SR よりもセキュリティレベルが高い非線形回路である一般化 SR と，一般化 SR の制御・観測の方法が提案されている．また，一般化 SR の各クラスの回路数が明らかにされている [13]．

シフトレジスタ (SR) では，初期状態の状態割当のビット列がそのまま出力系列として出力され，入力系列のビット列はそのまま最終状態の状態割当となる．SR 等価回路においても，このような初期状態や入力系列が存在する可能性がある．これは，特定の初期状態や入力系列において，SR 等価回路が SR と同じ動作をすることを意味する．このような初期状態や入力系列が存在すると，攻撃者に SR 等価回路が保持する FF 値を初期化または観測される可能性があり，安全ではない [14], [15]．そのため，セキュアスキャンに対する新しい概念として，強セキュア [14] が提案された．強セキュアな回路は，回路の状態割当が SR のそれと全て異なるように設計を行う．そのため，強セキュアな回路では，SR と同じ動作をすることがなく，SR 等価回路より，更にセキュリティを高めている．文献 [14] では，一般化 SR のクラスの一つである GF^2SR (Generalized feed-forward shift registers) に対して，SR 等価かつ強セキュアな回路を設計する手法が提案されている．文献 [15] では，一般化 SR のクラスの一つである GFSR (Generalized feedback shift registers) に対して，SR 等価かつ強セキュアな回路を設計する手法が提案されている．文献 [16] では，一般化 SR を SR 等価にする方法と，SR 等価な一般化 SR の回路数が明らかにされている．また，文献 [17] では，SR 等価かつ強セキュアな一般化 SR を設計する手法と，SR 等価かつ強セキュアな一般化 SR の回路数の下限が明らかにされている．

しかしながら，拡張 SR に対しては SR 等価かつ強セキュアな回路設計法は提案されていない．また，SR 等価かつ強セキュアな拡張 SR の回路数も明らかにされていない．拡張 SR は一般化 SR と比較して面積オーバーヘッドが小さいという利点がある．また，拡張 SR は NOT ゲートと XOR ゲートのみで構成されるため，論理値の変化を解析しやすく，回路設計が容易であるという利点がある．そのため，拡張 SR に対して，SR 等価かつ強セキュアな回路設計法を提案することは重要である．また，セキュリティレベルの観点から，SR 等価かつ強セキュアな拡張 SR 数を明らかにすることも重要である．本論文では，SR 等価な拡張 SR に対して，SR 等価かつ強セキュアな回路を設計する手法を提案する．また，SR 等価かつ強セキュアな拡張 SR の各クラスの回路数を明らかにし，セキュリティレベルを評価する．

本論文の構成は以下のとおりである．**2.** で，SR 等価回路について述べ，**3.** で，強セキュアについて述べる．**4.** で，SR 等価な Linear feed-forward SR (LF^2SR) と Inversion-inserted linear feed-forward SR (I^2LF^2SR) に対する強セキュア回路設計法を述べ，**5.** で SR 等価な Linear feedback SR (LFSR) と Inversion-inserted linear feedback SR (I^2LFSR) に対する強セキュア回路設計法を述べる．**6.** で，SR 等価かつ強セキュアな拡張シフトレジスタの回路数を明らかにし，最後に **7.** で，結論と今後の課題について述べる．

2. SR 等価回路

2.1 拡張シフトレジスタと一般化シフトレジスタ

SR 等価回路には，拡張 SR と一般化 SR の 2 種類が提案されている．SR 等価回路のセキュリティレベルを考えた場合，スキャン操作による入出力対応から攻撃者にシフトレジスタの構造を推定される確率を考えた場合，その推定が当たる確率は SR 等価な回路数の逆数に比例する．そのため，SR 等価回路数が多いほど攻撃者に回路構造を推定される確率が低くなるため，セキュリティレベルが高いと考える．

拡張 SR とは，スキャン FF に対して NOT ゲートや XOR ゲートを挿入し，線形回路で構成されたシフトレジスタである．拡張 SR を実現する線形回路構造として，Inversion-inserted SR (I^2SR), LF^2SR, I^2LF^2SR, LFSR, I^2LFSR の 5 種類が挙げられる [10]．拡張 SR は一般化 SR と比較して，面積オーバーヘッドが小さいという利点がある．また，NOT ゲートと XOR ゲートのみで構成されるため，強セキュア回路設計の際に，論理値の変化を解析しやすく，回路設計が容易であるという利点がある．

一般化 SR とは，拡張 SR のフィードフォワードまたはフィードバック接続に対して，任意の論理関数を入力とした XOR 演算を行う非線形回路で構成されたシフトレジスタである．一般化 SR と拡張 SR の面積

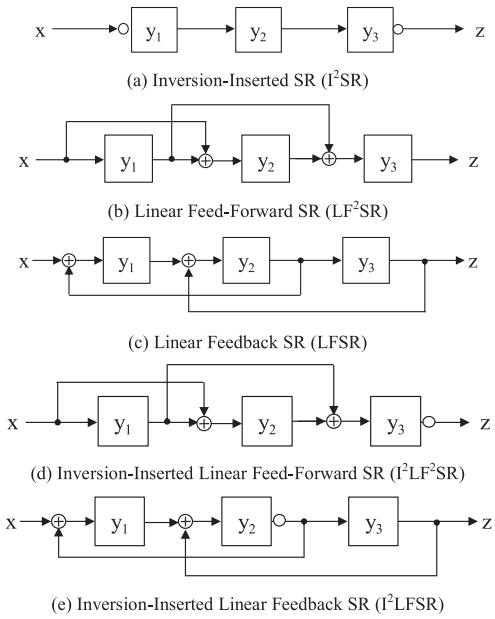


図 1　拡張シフトレジスタ例
Fig. 1　Examples of extended shift registers.

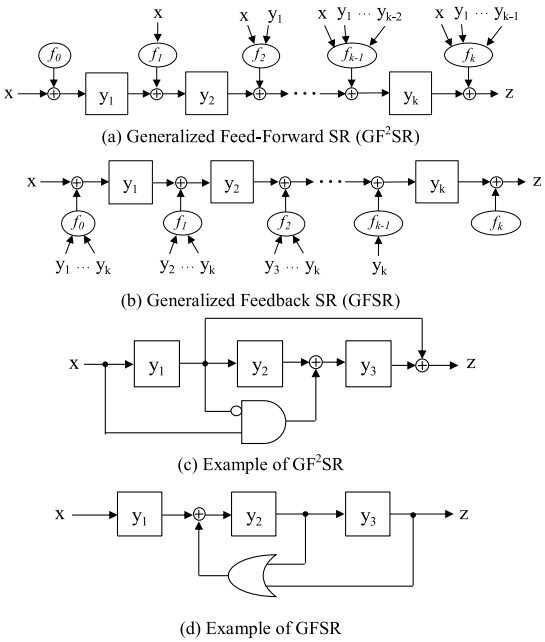


図 2　一般化シフトレジスタ例
Fig. 2　Examples of generalized shift registers.

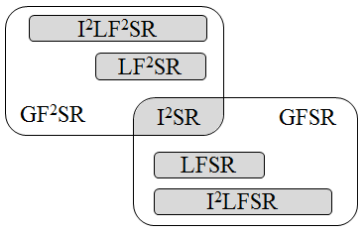


図 3　拡張 SR と一般化 SR の被覆関係
Fig. 3　Covering relationship between extended shift registers and generalized shift registers.

を比較した場合，フィードバックまたはフィードフォワードに追加された論理関数だけ一般化 SR のほうが面積オーバーヘッドは大きい．一般化 SR を実現する回路構造としては，GF^{2}SR と GFSR が挙げられる．

図 1 に 5 種類の 3 段の拡張 SR の例を示す．図 2 に k 段の一般化 SR と 3 段の一般化 SR の例を示す．図 1 と図 2 において，x はスキャンイン，z はスキャンアウト，y_1 から y_3 はスキャン FF を示す．図 2 (a) と (b) において，$f_0, f_1, \cdots, f_k$ は任意の論理関数を示す．一般化 SR では，この任意の論理関数だけ，拡張 SR よりも面積オーバーヘッドが大きくなる．

図 3 に，拡張 SR と一般化 SR の各クラスの被覆関係を示す．図 3 で示すように，拡張 SR は一般化 SR に被覆される．しかしながら，一般化 SR のクラス (GF^{2}SR，GFSR) と拡張 SR のクラス (I^{2}SR，LF^{2}SR，I^{2}LF^{2}SR，LFSR，I^{2}LFSR) を比較した場合，SR 等価な回路数は一般化 SR のクラスのほうが多い．そのため，セキュリティレベルは一般化 SR のクラスのほうが優れる．

本論文で扱う拡張 SR は，回路構造が異なっていても論理関数が同じであれば同一の回路と考える．そのため，NOT ゲートは FF に隣接し，FF と FF の間に高々1 個存在するものを対象とする．また，本論文では，攻撃者はゲートレベルの回路設計情報は知らず，テストピン (スキャンイン，スキャンアウト，スキャンイネーブル) の存在と，スキャンチェインが変更されたことのみを知っていると仮定する．また，攻撃者は拡張 SR のゲートレベル構造は知らないものと仮定する．

2.2　SR 等価回路

単一の入力 x，単一の出力 z，k 個の FF からなる回路 C の任意の時刻 t の入力 x の値 x(t) が k クロック周期後に出力 z に表れるとき (すなわち任意の時刻 t について $z(t+k) = x(t)$)，C は k 段 SR と機能等価である (SR 等価) という．

図 4 に SR 等価な回路 (LF^{2}SR, R_1) と，その記号シミュレーション結果を示す．図 4 (a) は SR 等価な 3 段 LF^{2}SR, R_1 である．図 4 (b) は R_1 に対する記号シ

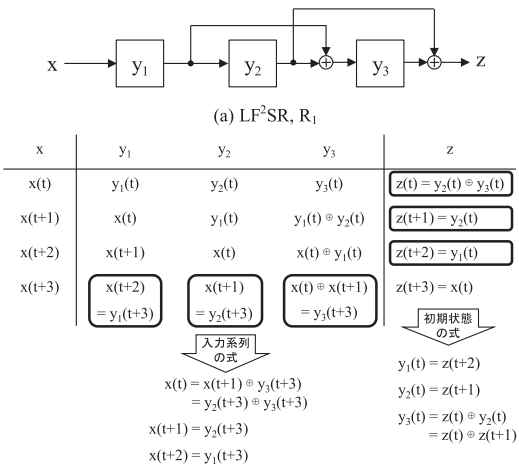


図 4　SR 等価な回路例
Fig. 4　Example of SR-equivalent circuit.

ミュレーション結果である．記号シミュレーションの結果より，出力系列 $z(t) = y_2(t) \oplus y_3(t)$, $z(t+1) = y_2(t)$, $z(t+2) = y_1(t)$, $z(t+3) = x(t)$ が得られる．このとき，時刻 t の入力 x(t) が 3 クロック周期後の時刻 $t+3$ の出力 $z(t+3) = x(t)$ として現れているため，R_1 は SR 等価となる．

3. 強セキュア

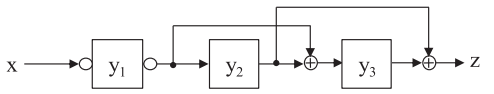
シフトレジスタ (SR) では，初期状態の状態割当のビット列がそのまま出力系列として出力され，入力系列のビット列はそのまま最終状態の状態割当となる．SR 等価回路においても，このような初期状態や入力系列が存在する可能性がある．このような初期状態や入力系列が存在すると，攻撃者に SR 等価回路が保持する FF 値を初期化または観測される可能性があり，安全であるとはいえない [14], [15].

図 4 の 3 段 LF^2SR, R_1 について考える．図 4 (b) の記号シミュレーション結果より，$y_2(t+3) = 0$ の場合，最終状態は $(y_3(t+3), y_2(t+3), y_1(t+3)) = (x(t), x(t+1), x(t+2))$ に固定される．すなわち，$y_2(t+3) = 0$ の場合はどのような入力系列 $(x(t), x(t+1), x(t+2))$ を印加しても，R_1 の最終状態 $(y_3(t+3), y_2(t+3), y_1(t+3))$ は $(x(t), x(t+1), x(t+2))$ に遷移する．例えば，R_1 に入力系列 $(x(t) = 0, x(t+1) = 0, x(t+2) = 0)$ を印加した場合，3 クロック周期後の最終状態は $(y_3(t+3) = 0, y_2(t+3) = 0, y_1(t+3) = 0))$ となり，入力系列と最終状態のビット列が等しくなる．つまり，$y_2(t+3) = 0$ の場合において，R_1 は SR と同じスキャンイン動作をすることとなる．このような入力系列が存在すると，攻撃者に SR 等価回路を初期化される可能性があり，安全であるとはいえない．同様に，$y_2(t) = 0$ の場合，$(y_1(t), y_2(t), y_3(t)) = (z(t+2), z(t+1), z(t))$ に固定される．すなわち，$y_2(t) = 0$ の場合は出力系列 $(z(t), z(t+1), z(t+2))$ は初期状態 $(y_3(t), y_2(t), y_1(t))$ のビット列と等しくなる．このような初期状態が存在すると，攻撃者に SR 等価回路が保持する FF 値を観測される可能性があり，安全であるとはいえない．このような問題を解決するために，セキュアに対する新しい概念として強セキュアが提案された [14].

単一の入力 x，単一の出力 z，k 個の FF からなる回路 C について考える．C の任意の内部状態 (最終状態) と，その状態に遷移可能な長さ k の入力系列が k 段 SR のそれと異なる場合，C をスキャンイン安全と呼ぶ [14]．C の任意の初期状態と，その状態を識別可能な長さ k の出力系列が k 段 SR のそれと異なる場合，C をスキャンアウト安全と呼ぶ [14]．C がスキャンイン安全かつスキャンアウト安全の場合，C を強セキュアと呼ぶ [14].

図 4 の R_1 は $y_2(t+3) = 0$ の場合，最終状態のビット列は入力系列と等しくなるため，R_1 はスキャンイン安全でない．また，$y_2(t) = 0$ の場合，出力系列は初期状態のビット列と等しくなるため，R_1 はスキャンアウト安全でない．このことから，R_1 は強セキュアではない．図 5 に SR 等価かつ強セキュアな回路例 (I^2LF^2SR, R_2) と，その記号シミュレーション結果を示す．図 5 (a) は SR 等価かつ強セキュアな 3 段 I^2LF^2SR, R_2 である．図 5 (b) は R_2 に対する記号シミュレーション結果である．記号シミュレーションの結果，出力系列 $(z(t+2) = y_1(t) \oplus 1, z(t+1) = y_2(t), z(t) = y_2(t) \oplus y_3(t))$ が得られ，内部状態は $(y_1(t+3) = x(t+2) \oplus 1, y_2(t+3) = x(t+1), y_3(t+3) = x(t) \oplus x(t+1))$ に遷移する．記号シミュレーション結果より，$y_1(t+3)$ は $x(t+2)$ と決して一致しないことがわかる．そのため，R_2 はスキャンイン安全である．同様に，$z(t+2)$ と $y_1(t)$ も決して一致しないことがわかる．そのため，R_2 はスキャンアウト安全である．よって R_2 は強セキュアである．また，$z(t+3) = x(t)$ から，R_2 は SR 等価である．

文献 [17] において，SR 等価な一般化 SR に対して，



(a) I^2LF2SR, R_2

x	y_1	y_2	y_3	z
x(t)	$y_1(t)$	$y_2(t)$	$y_3(t)$	$z(t) = y_2(t) \oplus y_3(t)$
x(t+1)	$x(t) \oplus 1$	$y_1(t) \oplus 1$	$y_1(t) \oplus y_2(t) \oplus 1$	$z(t+1) = y_2(t)$
x(t+2)	$x(t+1) \oplus 1$	$x(t)$	$x(t) \oplus y_1(t) \oplus 1$	$z(t+2) = y_1(t) \oplus 1$
x(t+3)	$x(t+2) \oplus 1 = y_1(t+3)$	$x(t+1) = y_2(t+3)$	$x(t) \oplus x(t+1) = y_3(t+3)$	$z(t+3) = x(t)$

入力系列の式:
$x(t) = x(t+1) \oplus y_3(t+3) = y_2(t+3) \oplus y_3(t+3)$
$x(t+1) = y_2(t+3)$
$x(t+2) = y_1(t+3) \oplus 1$

初期状態の式:
$y_1(t) = z(t+2) \oplus 1$
$y_2(t) = z(t+1)$
$y_3(t) = z(t) \oplus y_2(t) = z(t) \oplus z(t+1)$

(b) R_2 に対する記号シミュレーション結果

図 5　SR 等価かつ強セキュアな回路例
Fig. 5　Example of SR-equivalent and strongly secure circuit.

以下の定理 1 が証明されている．拡張 SR も一般化 SR に属するため，SR 等価な拡張 SR に対しても，定理 1 が成り立つ．定理 1 より，SR 等価な回路に対する強セキュア回路設計では，スキャンイン安全またはスキャンアウト安全のどちらか一方のみを考えればよい．

[定理 1] [17]　SR 等価な回路 C に対して，C がスキャンイン安全ならば，C はスキャンアウト安全であり，その逆も成り立つ．

4. SR 等価な LF^2SR と I^2LF^2SR に対する強セキュア回路設計法

本章では，SR 等価な LF^2SR と I^2LF^2SR に対する強セキュア回路設計法を提案する．本手法は，全ての SR 等価かつ強セキュアな $(I^2)LF^2SR$ を設計するものではない．また，定理 1 より SR 等価な拡張 SR に対する強セキュア回路設計は，スキャンイン安全かスキャンアウト安全のどちらか一方のみを考えればよい．

単一の入力 x，単一の出力 z，k 個の FF($y_1, y_2, \cdots, y_k$)，からなる $(I^2)LF^2SR$, C について考える．図 6 にフリップフロップ y_p と y_{p+1} の間に最左端の XOR ゲートを配置した $(I^2)LF^2SR$ を示す．図 6 において，外部入力 x からフリップフロップ y_p の間に少なくとも一つ NOT ゲートを挿入した場合，挿入した NOT ゲートの出力側に存在する FF には入力値とは逆の値が取り込まれるため，C の最終状態 ($y_1, y_2, \cdots, y_k$) は常に SR と異なる．よって，C はスキャンイン安全となり，定理 1 より強セキュアとなる．しかしながら，NOT ゲートを挿入することで $(I^2)LF^2SR$ が SR 等価性を失う可能性がある．これは，NOT ゲートの挿入による論理値の変化が外部出力 z まで伝搬するためである．このような場合，y_{p+1} から z の間に NOT ゲートを更に挿入し，論理値の変化を打ち消すことで，C を SR 等価にすることが可能である．

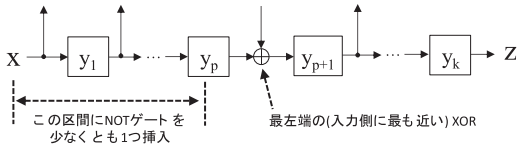
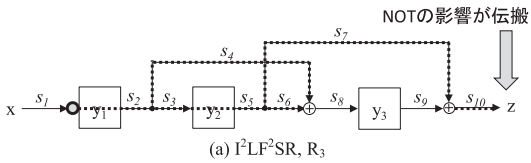


図 6　$(I^2)LF^2SR$ に対する強セキュア設計
Fig. 6　Design for strongly secure $(I^2)LF^2SRs$.



(a) I^2LF^2SR, R_3

x	y_1	y_2	y_3	z
x(t)	$y_1(t)$	$y_2(t)$	$y_3(t)$	$z(t) = y_2(t) \oplus y_3(t)$
x(t+1)	$x(t) \oplus \mathbf{1}$	$y_1(t)$	$y_1(t) \oplus y_2(t)$	$z(t+1) = y_2(t)$
x(t+2)	$x(t+1) \oplus \mathbf{1}$	$x(t) \oplus \mathbf{1}$	$x(t) \oplus y_1(t) \oplus \mathbf{1}$	$z(t+2) = y_1(t)$
x(t+3)	$x(t+2) \oplus \mathbf{1} = y_1(t+3)$	$x(t+1) \oplus \mathbf{1} = y_2(t+3)$	$x(t) \oplus x(t+1) = y_3(t+3)$	$z(t+3) = x(t) \oplus \mathbf{1}$

(b) R_3 に対する記号シミュレーション結果

図 7　NOT ゲート挿入により SR 等価でなくなった I^2LF^2SR
Fig. 7　I^2LF^2SR lost SR-equivalence by inserting NOT gate.

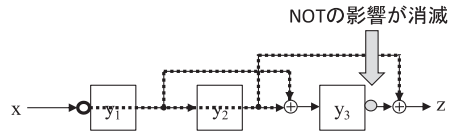
また，文献 [12] より，k 段 SR 等価な LF^2SR (I^2LF^2SR) は，(k − 1) 段 LF^2SR(I^2LF^2SR) の出力側に FF を 1 個追加し，定理 3 [12] (定理 7 [12]) より適当な FF から出力 z へのフィードフォワード接続（と必要に応じて出力 z に NOT ゲートを追加）することで設計される．そのため，k 段 SR 等価な LF^2SR(I^2LF^2SR) の入力 x からフリップフロップ y_{k-1} の出力までの間には必ず XOR が一つ以上存在し，p は $1 \leq p < k$ となる．

図 7 に NOT ゲートの挿入により，SR 等価でなくなった回路 (I^2LF^2SR, R_3) と，その記号シミュレーション結果を示す．図 7 (a) は図 4 の R_1 のフリップフロップ y_1 の入力側に NOT ゲートを挿入した回路

R_3 である．図 7 (a) において，最左端の XOR ゲートは y_2 と y_3 の間となるため，y_p はフリップフロップ y_2，y_{p+1} はフリップフロップ y_3 となる．また，点線は y_1 の入力側に挿入した NOT ゲートの影響を示し，$s_1, s_2, \cdots, s_{10}$ は各信号線名を示す．図 7 (b) は R_3 に対する記号シミュレーション結果である．記号シミュレーションの結果より，$y_1(t+3)$ は $x(t+2)$ と決して一致しない．また，$y_2(t+3)$ も $x(t+1)$ と決して一致しない．これは，y_1 の入力側に挿入した NOT ゲートにより，y_1 と y_2 には常に入力値とは逆の値が取り込まれるためである．そのため，R_3 はスキャンイン安全である．しかしながら，$z(t+3) = x(t) \oplus 1$ のため，R_3 は SR 等価でないことがわかる．これは y_1 の入力側に挿入した NOT ゲートの影響が z まで伝搬しているためである．

図 7 (a) より，y_1 の入力側に挿入した NOT ゲートによる論理値変化の経路を解析する．本論文では，拡張 SR 内の経路を $P = (s_1, s_2, \cdots, s_n)$ と表記し，入力側から出力側への信号線の並びで表現する．図 7 (a) より，y_1 の入力側に挿入した NOT ゲートにより論理値が変化した経路は $P_1 = (s_2, s_3, s_5, s_6)$ と $P_2 = (s_2, s_4)$ と $P_3 = (s_2, s_3, s_5, s_7, s_{10})$ の三つが存在する．経路 P_1 と P_2 に関しては，y_3 の入力側の XOR ゲートで NOT の影響が打ち消しあっているため y_3 には伝搬しないことが確認できる．しかしながら，経路 P_3 の論理値の変化は z まで伝搬しており，これにより R_3 は SR 等価性を失っている．そのため，P_3 の論理値の変化を z まで伝搬しないように y_3 から z の間に NOT ゲートを追加挿入し，P_3 の影響を打ち消すことで R_3 を SR 等価に変更する必要がある．R_3 に対して P_3 の影響を打ち消すことが可能な NOT ゲートの挿入位置を考えた場合，y_3 の出力に NOT ゲートを追加挿入すると s_9 と s_{10} の間に存在する XOR により P_3 の影響を打ち消すことが可能である．そのため，R_3 に対しては，y_3 の出力に NOT ゲートを追加挿入することで，R_3 を SR 等価に戻すことが可能である．

図 8 (a) に図 7 の R_3 に対して，y_3 の出力に NOT ゲートを追加挿入した SR 等価かつ強セキュアな回路 (I^2LF^2SR, R_4) を示す．図 8 (b) は R_4 に対する記号シミュレーション結果である．R_4 は R_3 のフリップフロップ y_3 の出力側に NOT ゲートを追加挿入したことで，y_1 の入力側に挿入した NOT ゲートの影響を打ち消している．記号シミュレーション結果より，3 クロック周期後の時刻 t + 3 の出力 z(t + 3) が t 時刻目の入力 x(t) と等しいため R_4 は SR 等価である．また，$y_1(t+3)$ は $x(t+2)$ と決して一致しないため，R_4 はスキャンイン安全であり，定理 1 より，R_4 は強セキュアである．よって，R_4 は SR 等価かつ強セキュアな I^2LF^2SR である．



(a) I^2LF^2SR, R_4

x	y_1	y_2	y_3	z
x(t)	$y_1(t)$	$y_2(t)$	$y_3(t)$	$z(t) = y_2(t) \oplus y_3(t) \oplus 1$
x(t+1)	$x(t) \oplus 1$	$y_1(t)$	$y_1(t) \oplus y_2(t)$	$z(t+1) = y_2(t) \oplus 1$
x(t+2)	$x(t+1) \oplus 1$	$x(t) \oplus 1$	$x(t) \oplus y_1(t) \oplus 1$	$z(t+2) = y_1(t) \oplus 1$
x(t+3)	$x(t+2) \oplus 1$ $= y_1(t+3)$	$x(t+1) \oplus 1$ $= y_2(t+3)$	$x(t) \oplus x(t+1)$ $= y_3(t+3)$	$z(t+3) = x(t)$

(b) R_4 に対する記号シミュレーション結果

図 8　NOT ゲートの追加挿入により SR 等価かつ強セキュアになった I^2LF^2SR

Fig. 8　SR-equivalent and strongly secure I^2LF^2SR designed by inserting additional NOT gate.

以下に，SR 等価な LF^2SR と I^2LF^2SR に対する，SR 等価かつ強セキュア回路設計手順を示す．

SR 等価な LF^2SR と I^2LF^2SR に対する強セキュア設計手順：

（1） 回路 C がスキャンイン安全 (強セキュア) ならば終了．回路 C がスキャンイン安全 (強セキュア) でないならば，外部入力 x と最も入力側に近い XOR ゲートの入力側に存在するフリップフロップ y_p $(1 \le p < k)$ の間に少なくとも一つ NOT ゲートを挿入し，スキャンイン安全 (強セキュア) にする．

（2） NOT ゲートの挿入により SR 等価でなくなった場合，追加した NOT ゲートによる論理値変化の経路を解析し，その変化を打ち消すようにフリップフロップ y_{p+1} $(1 \le p < k)$ と外部出力 z の間に NOT ゲートを追加挿入し，SR 等価に変更する．

5. SR 等価な LFSR と I^2LFSR に対する強セキュア回路設計法

本章では，SR 等価な LFSR と I^2LFSR に対する，強セキュア回路設計法を提案する．本手法は，全ての

SR 等価かつ強セキュアな (I^2)LFSR を設計するものではない．

単一の入力 x，単一の出力 z，k 個の FF($y_1, y_2, \cdots, y_k$)，からなる (I^2)LFSR, C について考える．図 9 にフリップフロップ y_{q-1} と y_q の間に最右端の XOR ゲートを配置した (I^2)LFSR を示す．図 9 において，外部出力 z からフリップフロップ y_q の間に少なくとも一つ NOT ゲートを挿入した場合，C の初期状態 $(y_1, y_2, \cdots, y_k)$ は常に SR と異なる．よって，C はスキャンアウト安全となり，定理 1 より強セキュアとなる．NOT ゲートの挿入により SR 等価性を失った場合，外部入力 x から y_{q-1} の間に NOT ゲートを更に挿入することで，C を SR 等価にすることが可能である．

図 10 (a) に SR 等価だが強セキュアではない LFSR, R_5 を示す．図 10 (b) に R_5 の y_2 の出力側に NOT ゲートを挿入した I^2LFSR, R_6 を示す．図 10 (b) において，$s_1, s_2, \cdots, s_{10}$ は各信号線名を示す．また，図 10 (c) に R_6 に対する記号シミュレーション結果を示す．**4.** と同様の議論により，図 10 (c) の記号シミュレーション結果から R_6 はスキャンイン安全かつスキャンアウト安全であるが，SR 等価でないことがわかる．

図 10 (b) より，y_2 の出力側に挿入した NOT ゲートによる論理値変化の経路を解析すると，論理値が変化した経路は経路 $P_1 = (s_5, s_7, s_8, s_{10})$ と $P_2 = (s_5, s_6, s_2, s_3)$ と $P_3 = (s_5, s_7, s_8, s_9)$ の三つが存在する．経路 P_2 と P_3 に関しては，y_1 と y_2 の間に存在する XOR ゲートで NOT の影響を打ち消しあっている．しかしながら，経路 P_1 の論理値の変化は z まで伝搬しており，これにより R_6 は SR 等価性を失っている．そのため，P_3 の論理値の変化を z まで伝搬しないように x から y_1 の間に NOT ゲートを追加挿入し，P_1 の影響を打ち消すことで R_6 を SR 等価に変更する必要がある．R_6 に対して P_1 の影響を打ち消すことが可能な NOT ゲートの挿入位置を考えた場合，x または y_1 の出力のどちらか一方に NOT ゲートを追加する 2 通りが考えられる．x に NOT ゲートを追加挿入した場合，追加挿入した NOT ゲートの影響が y_2 まで伝搬することで，P_3 の論理値の変化が y_2 の出力にある NOT ゲートにより打ち消される．これにより，R_6 を SR 等価に戻すことが可能である．また同様に，y_1 の出力に NOT ゲートを追加挿入した場合，追加挿入した NOT ゲートの影響が y_2 まで伝搬することで，P_3 の論理値の変化が y_2 の出力にある NOT ゲートにより打ち消される．このように，x または y_1 の出力のどちらか一方に NOT ゲートを追加挿入することで，R_6 を SR 等価に戻すことが可能である．

また，文献 [12] より，k 段 SR 等価な LFSR(I^2LFSR) は，$(k-1)$ 段 LFSR(I^2LFSR) の入力側に FF を 1 個追加し，定理 4 [12] (定理 8 [12]) より適当な FF から入力 x へのフィードバック接続（と必要に応じて入力 x に NOT ゲートを追加）することで設計される．そのため，k 段 SR 等価な LFSR(I^2LFSR) のフリップフロップ y_1 の出力から出力 z までの間には必ず XOR が一つ以上存在し，q は $1 < q \leq k$ となる．

図 11 (a) に R_6 に対して，NOT ゲートを追加挿入した SR 等価かつ強セキュアな回路 (I^2LFSR, R_7) を示す．図 11 (b) は R_7 に対する記号シミュレーション結果である．R_7 は R_6 のフリップフロップ y_1 の入力側に NOT ゲートを追加挿入したことで，y_2 の出力側

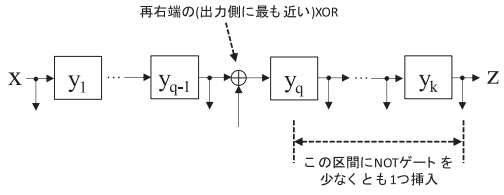
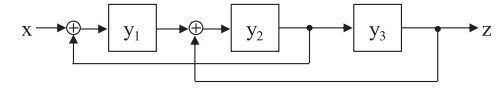
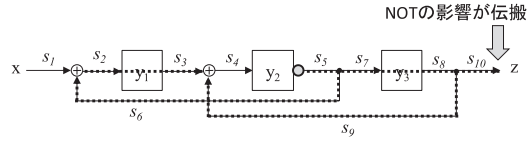


図 9　(I^2)LFSR に対する強セキュア設計
Fig. 9　Design for strongly secure (I^2)LFSRs.



(a) LFSR, R_5

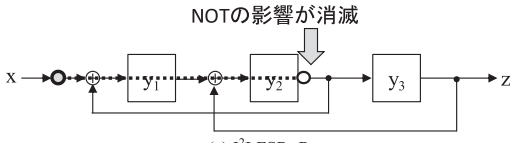


(b) I^2LFSR, R_6

x	y_1	y_2	y_3	z
x(t)	$y_1(t)$	$y_2(t)$	$y_3(t)$	$z(t) = y_3(t)$
x(t+1)	$x(t) \oplus y_2(t) \oplus \mathbf{1}$	$y_1(t) \oplus y_3(t)$	$y_2(t) \oplus \mathbf{1}$	$z(t+1) = y_2(t) \oplus \mathbf{1}$
x(t+2)	$x(t+1) \oplus y_1(t) \oplus y_3(t) \oplus \mathbf{1}$	x(t)	$y_1(t) \oplus y_3(t) \oplus \mathbf{1}$	$z(t+2) = y_1(t) \oplus y_3(t) \oplus \mathbf{1}$
x(t+3)	$x(t+2) \oplus x(t) \oplus \mathbf{1}$ $= y_1(t+3)$	$x(t+1)$ $= y_2(t+3)$	$x(t) \oplus \mathbf{1}$ $= y_3(t+3)$	$z(t+3) = x(t) \oplus \mathbf{1}$

(c) R_6 に対する記号シミュレーション結果

図 10　NOT ゲート挿入により SR 等価でなくなった I^2LFSR
Fig. 10　I^2LFSR lost SR-equivalence by inserting NOT gate.



(a) I^2LFSR, R_7

x	y_1	y_2	y_3	z
x(t)	$y_1(t)$	$y_2(t)$	$y_3(t)$	$z(t) = y_3(t)$
x(t+1)	$x(t) \oplus y_2(t)$	$y_1(t) \oplus y_3(t)$	$y_2(t) \oplus \mathbf{1}$	$z(t+1) = y_3(t) \oplus \mathbf{1}$
x(t+2)	$x(t+1) \oplus y_1(t) \oplus y_3(t)$	$x(t) \oplus \mathbf{1}$	$y_1(t) \oplus y_3(t) \oplus \mathbf{1}$	$z(t+2) = y_1(t) \oplus y_3(t) \oplus \mathbf{1}$
x(t+3)	$x(t+2) \oplus x(t) \oplus \mathbf{1}$ $= y_1(t+3)$	$x(t+1) \oplus \mathbf{1}$ $= y_2(t+3)$	$x(t)$ $= y_3(t+3)$	$z(t+3) = x(t)$

(b) R_7 に対する記号シミュレーション結果

図 11　NOT ゲートの追加挿入により SR 等価かつ強セキュアになった I^2LFSR

Fig. 11　SR-equivalent and strongly secure I^2LFSR designed by inserting additional NOT gate.

に挿入した NOT ゲートの影響を打ち消しており，**4.** と同様の議論により R_7 は SR 等価かつ強セキュアな I^2LFSR である．

以下に，SR 等価な LFSR と I^2LFSR に対する，SR 等価かつ強セキュア回路設計手順を示す．

SR 等価な LFSR と I^2 LFSR に対する強セキュア設計手順：

（1） 回路 C がスキャンアウト安全 (強セキュア) ならば終了．回路 C がスキャンアウト安全 (強セキュア) でないならば，最も出力側に近い XOR ゲートの出力側に存在するフリップフロップ y_q $(1 < q \leq k)$ と外部出力 z の間に少なくとも一つ NOT ゲートを挿入し，スキャンアウト安全 (強セキュア) にする．

（2） NOT ゲートの挿入により SR 等価でなくなった場合，追加した NOT ゲートによる論理値変化の経路を解析し，その変化を消すように外部入力 x とフリップフロップ y_{q-1} $(1 < q \leq k)$ の間に NOT ゲートを追加挿入し，SR 等価に変更する．

6. SR 等価かつ強セキュアな拡張シフトレジスタのセキュリティレベル

SR 等価かつ強セキュアな拡張 SR に対して，スキャン操作による入出力対応から SR 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 SR 等価かつ強セキュアな回路数の逆数に比例する．そのため，SR 等価かつ強セキュアな回路数が多いほどセキュリティに優れていると考えることができ，セキュリティレベルの観点から，SR 等価かつ強セキュアな回路数を明らかにすることは重要である．文献 [17] において，SR 等価かつ強セキュアな一般化 SR の回路数の下限は明らかにされているが，拡張 SR に関しては示されていない．本章では，SR 等価かつ強セキュアな拡張 SR の各クラスの回路数を明らかにする．また，本章で明らかにする SR 等価かつ強セキュアな拡張 SR の各クラスの回路数は，**4.** 及び **5.** の手法で設計可能な回路数だけではなく，SR 等価かつ強セキュアな拡張 SR の各クラスにおける全ての回路数である．SR 等価かつ強セキュアな拡張 SR に関して，以下の定理 2 から定理 6 が成り立つ．

[定理 2]　k 段 SR 等価で強セキュアな I^2SR の総数は $2^k - 1$ である．

(証明)　I^2SR はシフトレジスタに NOT ゲートを一つ以上挿入した回路である．入力側に最も近い NOT ゲートの出力となる FF は，スキャンイン動作時において，入力値とは必ず逆の論理値をとる．そのため，どのような I^2SR に対してもスキャンイン安全となる．そのため，定理 1 より，どのような I^2SR に対しても強セキュアであるといえる．また，文献 [12] の定理 1 より，偶数個の NOT ゲートを含む I^2SR は SR 等価であり，その総数は $2^k - 1$ であることから，k 段 SR 等価で強セキュアな I^2SR の総数は $2^k - 1$ である．

(証明終)

[定理 3]　k 段 SR 等価で強セキュアな LF^2SR の総数は 0 である．

(証明)　LF^2SR はシフトレジスタの入力側の FF から出力側の FF へ (前段から後段へ)XOR によるフィードフォワード接続を (一般的に複数個) 付加した回路である．単一の入力 x，単一の出力 z，k 個の FF$(y_1, y_2, \cdots, y_k)$ をもつ k 段 LF^2SR について考える．k 段 LF^2SR に対して，k サイクル間 0 を印加し続けると，k サイクル後の内部状態は $(y_1(k), y_2(k), \cdots, y_k(k)) = (0, 0, \cdots, 0)$ に初期化されるためスキャンイン安全でない．そのため，定理 1 より，どのような LF^2SR も強セキュアでない．よって，k 段 SR 等価で強セキュアな LF^2SR の総数は 0 である．

(証明終)

[定理 4]　k 段 SR 等価で強セキュアな LFSR の総数は 0 である．
(証明)　LFSR はシフトレジスタの出力側の FF から入力側の FF へ (後段から前段へ)XOR によるフィードバック接続を (一般的に複数個) 付加した回路である．単一の入力 x，単一の出力 z，k 個の FF$(y_1, y_2, \cdots, y_k)$ をもつ k 段 LFSR について考える．k 段 LFSR において，時刻 t の内部状態が $(y_1(t), y_2(t), \cdots, y_k(t)) = (0, 0, \cdots, 0)$ の場合，t＋k サイクル後の出力系列は，$(z(t), z(t+1), \cdots, z(t+k)) = (0, 0, \cdots, 0)$ となり，スキャンアウト安全でない．そのため，定理 1 より，どのような LFSR も強セキュアでない．よって，k 段 SR 等価で強セキュアな LFSR の総数は 0 である．
(証明終)

次に定理 5 を証明するために，捕題 1，2，3 を示す．
[補題 1]　k 段 SR 等価でスキャンイン安全な I^2LF^2SR の総数は $(k-1)$ 段スキャンイン安全な I^2LF^2SR の総数に等しいかそれより多い．
(証明)　$(k-1)$ 段スキャンイン安全な I^2LF^2SR に対して，出力側に FF を 1 個追加して k 段スキャンイン安全な I^2LF^2SR とする．このとき，$(k-1)$ 段スキャンイン安全な I^2LF^2SR が SR 等価であった場合，出力側に FF を追加するだけで k 段 SR 等価かつスキャンイン安全な I^2LF^2SR となる．一方，$(k-1)$ 段スキャンイン安全な I^2LF^2SR が SR 等価でない場合は出力側に FF を追加した後，文献 [12] の定理 7 より k 段 I^2LF^2SR の 1 から $(k-1)$ 段部分の適当な FF から出力 z へ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，k 段 SR 等価かつスキャンイン安全な I^2LF^2SR にすることが可能である．また，FF 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．この処理を SR 等価変換と呼ぶことにする．

SR 等価変換において，もし $(k-1)$ 段スキャンイン安全な I^2LF^2SR から，異なる二つの k 段 SR 等価でスキャンイン安全な I^2LF^2SR である B_1 と B_2 ができるとすると，B_1 と B_2 の出力 z は異なる FF からのフィードフォワード接続が追加されることとなる．これは B_1 の出力 z と，B_2 の出力 z が異なる値を出力することとなるため，B_1 と B_2 が両方 SR 等価であることに反する．よって，この対応は写像である．

この写像において，もし異なる二つの $(k-1)$ 段スキャンイン安全な I^2LF^2SR である A_1 と A_2 から，同じ k 段 SR 等価でスキャンイン安全な I^2LF^2SR，B ができるとすると，B の 1〜$(k-1)$ 段の回路部は等しくならなければならい．よって，この写像は単射である．

このように，この写像は単射であるため，k 段 SR 等価でスキャンイン安全な I^2LF^2SR の個数は，$(k-1)$ 段スキャンイン安全な I^2LF^2SR の総数に等しいかそれより多い．
(証明終)

[補題 2]　k 段スキャンイン安全な I^2LF^2SR の総数は，少なくとも $(2^{(k(k+1)/2)}-1)(2^k)$ である．
(証明)　k 段 LF^2SR の k 個の FF を入力側から $y_1, y_2, \cdots, y_k$ とする．k 段 LF^2SR のフリップフロップ y_1 の入力側に NOT ゲートを 1 個追加すると，スキャンイン動作において，y_1 には常に入力値とは逆の値が印加されるため，k 段スキャンイン安全な I^2LF^2SR にすることができる．k 段 LF^2SR に NOT ゲートを 1 個以上追加し，k 段 I^2LF^2SR とする場合，フリップフロップ y_1 の入力側に NOT ゲートを含む組合せは 2^k 通り存在する．また，文献 [12] より，k 段 LF^2SR の総数は $2^{(k(k+1)/2)}-1$ である．これらの積から，k 段スキャンイン安全な I^2LF^2SR の総数は，少なくとも $(2^{(k(k+1)/2)}-1)(2^k)$ である．
(証明終)

[補題 3]　k 段 SR 等価でスキャンイン安全な I^2LF^2SR の総数は，少なくとも $(2^{(k(k-1)/2)}-1)(2^{k-1})$ である．
(証明)　補題 1，補題 2 より，k 段 SR 等価でスキャンイン安全な I^2LF^2SR の総数は，少なくとも $(2^{(k(k-1)/2)}-1)(2^{k-1})$ である．
(証明終)

捕題 3 と定理 1 から，次の定理 5 が成立する．
[定理 5]　k 段 SR 等価で強セキュアな I^2LF^2SR の総数は，少なくとも $(2^{(k(k-1)/2)}-1)(2^{(k-1)})$ である．

また，定理 5 と同様の理由により，I^2LFSR のスキャンアウト安全を考えた場合，以下の定理 6 が成立する．
[定理 6]　k 段 SR 等価で強セキュアな I^2LFSR の総数は，少なくとも $(2^{(k(k-1)/2)}-1)(2^{(k-1)})$ である．

表 1 に，拡張 SR の各クラスの回路数と，定理 2 から定理 6 によって示された SR 等価かつ強セキュアな拡張 SR 数を示す．

表 1　各クラスの回路数
Table 1　Number of circuits for each class.

クラス	I^2SR	LF^2SR	LFSR	I^2LF^2SR	I^2LFSR
各クラスの総数	2^{k+1}-1	$2^{k(k+1)/2}$-1		$(2^{k(k+1)/2}-1)(2^{k+1}-1)$	
SR等価かつ強セキュアな回路数	2^k-1	0		$\geq (2^{k(k-1)/2}-1)(2^{k-1})$	

7. むすび

本論文では，SR 等価な拡張 SR のクラス LF^2SR，I^2LF^2SR，LFSR，I^2LFSR に対して，NOT ゲートを挿入することで，SR 等価かつ強セキュアな拡張 SR を設計する手法を提案した．また，提案手法によって対象の回路が SR 等価でなくなった場合，論理値の変化を解析することで SR 等価かつ強セキュアに再設計する手法を提案した．また，定理 2 から定理 6 より，拡張 SR の各クラスにおいて，SR 等価かつ強セキュアな回路数を明らかにし，セキュリティレベルの評価を行った．クラス I^2LF^2SR と I^2LFSR に関しては，SR 等価かつ強セキュアな回路数の下限だけが明らかになった．そのため，今後の課題として，計算機実験により，それらの回路数の実数を明らかにする必要がある．また，これまで提案されているセキュアスキャン回路のセキュリティを更に向上させるため，SR 等価かつ強セキュアな回路に対する新たな攻撃方法とその対策の考案が挙げられる．

文　献

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

[2] 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.

[3] D. Hély, F. Bancel, M.-L. Flottes, and B. Rouzeyre, “Securing scan control in crypto chips,” J. Electronic Testing, vol.23, no.5, pp.457–464, Oct. 2007.

[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, 2006.

[5] 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, 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. Comput.-Aided Des. Integr. Circuits Syst., vol.26, no.11, pp.2080–2084, 2007.

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

[9] M.A. Razzaq, V. Singh, and A. Singh, “SSTKR: Secure and testable scan design through test key randomization,” Proc. 20th IEEE Asian Test Symposium, pp.60–65, Nov. 2011.

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

[11] K. Fujiwara, H. Fujiwara, M.E.J. Obien, and H. Tamamoto, “SREEP: Shift register equivalents enumeration and synthesis program for secure scan design,” Proc. 13th IEEE International Symposium on Design and Diagnostics of Electronic Circuits and Systems, pp.193–196, April 2010.

[12] 藤原克哉，藤原秀雄，オビエン マリー エンジェリン，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，” 信学論（D），vol.J93-D, no.11, pp.2426–2436, Nov. 2010.

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

[14] H. Fujiwara and K. Fujiwara, “Strongly secure scan design using generalized feed forward shift registers,” IEICE Trans. Inf. & Syst., vol.E98-D, no.10, pp.1852–1855, Oct. 2015.

[15] H. Fujiwara and K. Fujiwara, “Properties of generalized feedback shift registers for secure scan design,” IEICE Trans. Inf. & Syst., vol.E99-D, no.4, pp.1255–1258, April 2016.

[16] H. Fujiwara and K. Fujiwara, “Realization of SR-equivalents using generalized shift registers for secure scan design,” IEICE Trans. Inf. & Syst., vol.E99-D, no.8, pp.2182–2185, Aug. 2016.

[17] H. Fujiwara and K. Fujiwara, “Synthesis and enumeration of generalized shift registers for strongly secure SR-equivalents,” IEICE Trans. Inf. & Syst., vol.E100-D, no.9, pp.2232–2236, Sept. 2017.

（平成 30 年 2 月 19 日受付，4 月 13 日早期公開）

山崎　紘史　（正員）

1987 年生．2010 年日大生産工学部卒．2012 年同大大学院博士前期課程修了．2015 年同大大学院博士後期課程修了．2015 年より日大助手．VLSI のテスト，テスト生成，テスト容易化設計，テスト圧縮，低消費電力テスト，セキュアスキャン設計に関する研究に従事．電子情報通信学会，情報処理学会各会員．

細川　利典　（正員）

1964 年生．1987 年明大・工・電子通信卒．博士（工学）．松下電器産業（株），(株) 半導体理工学研究センター（出向）を経て，現在日本大学教授．論理・故障シミュレーション，テスト生成，テスト容易化設計，テスト圧縮，上流テスト，テスト容易化高位合成，故障診断，ハードウェアトロイ検出，IP の論理暗号化の研究に従事．IEEE，電子情報通信学会各会員．

藤原　秀雄　（正員：フェロー）

1946 年生．1969 年阪大・工・電子卒．1974 年同大大学院博士課程了．工学博士．阪大助手，明治大・理工学部教授，奈良先端大・情報科学研究科教授を経て，現在大阪学院大学教授．1981 年ウォータールー大客員助教授．1984 年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 Meritorious Service Award, IEEE Computer Society Outstanding Contribution Award，など受賞．電子情報通信学会フェロー（終身），情報処理学会フェロー，IEEE Computer Society Golden Core Member, IEEE Life Fellow.