ISSN 2186-5647

拡張シフトレジスタに対する強セキュア回路設計法

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 circuit : VLSI)において，セキュア(安全)でテスタブル(テスト容易)な回路設計は重要な課題である．現在広く使用されている代表的なテスト容易化設計であるフルスキャン設計[1]は，回路内部のフリップフロップ(Flip-Flop : FF)を直列に接続するスキャンモードにより，FF 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[1]．しかしながら，回路内部の FF を容易に制御・観測できるため，暗号回路などにおいてスキャンベース攻撃による秘密鍵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[2]．

文献[3-15]において，スキャンベース攻撃に有効な様々なセキュアスキャン設計手法が提案されている．文献[10]において，シフトレジスタ(Shift Register : SR)等価[10]な拡張 SR[10]を用いたセキュアでテスタブルなセキュアスキャン設計手法が提案されている．SR 等価な拡張 SR は，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が，内部状態(FF の状態)が SR と異なる．そのため，スキャン FF の回路構造が特定されにくく，スキャン攻撃からの防御に有効であることが報告されている[10]．しかしながら，SR 等価のみを考えた場合，拡張 SR の状態割当てが SR と同じ割当てを持つ可能性が存在する．このような状態が存在すると，攻撃者に拡張 SR が保持する FF 値を初期化または観測される可能性がある[14][15]．そのため，セキュアに対する新しい概念として強セキュア[14]が提案された．強セキュアでは，拡張 SR の状態割当が SR のそれとすべて異なる．そのため，強セキュアなスキャン設計は，文献[10]のセキュアなスキャン設計よりさらにセキュリティを高めている．文献[10]の手法では，SR 等価のみを考慮したスキャン設計のため，強セキュアでない回路が含まれる．そのため，さらなるセキュリティの向上が見込まれる．一方，文献[14][15]において，SR 等価な一般化 SR[14][15]に対して，SR 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が提案されている．文献[14]では，SR 等価な GF^{2}SR (Generalized feed-forward shift registers)に対して， SR 等価かつ強セキュアな回路を生成する．文献[15]では，SR 等価な GFSR (Generalized feedback shift registers)に対して， SR 等価かつ強セキュアな回路を生成する．

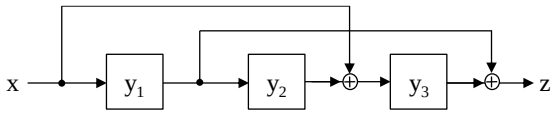
本論文では，文献[14][15]の手法を応用することで，SR 等価な拡張 SR を強セキュアに変更する手法を提案する．また，強セキュアに変更することで SR 等価でなくなった場合，拡張 SR の論理値の変化を解析することで，SR 等価に戻す手法を提案する．

2. SR 等価

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 1 に SR 等価な回路とその記号シミュレーション結果を示す．図 1(a)は SR 等価な 3 段 Linear feed-forward SR (LF^{2}SR), R_1 である．図 1(b)は R_1 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，出力系列 $z(t)=y_1(t)\oplus y_3(t)$，$z(t+1)=y_2(t)$，$z(t+2)=y_1(t)$，$z(t+3)=x(t)$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 等価といえる．

3. 強セキュア

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，リセット)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する．SR 等価のみを考えた場合，拡張 SR の状態割当てが SR と同じ割当てを持つ可能性が存在する．このような状態が存在すると，攻撃者に拡張 SR が保持する FF 値を初期化または観測される可能性がある[14][15]．たとえば，図 1 の 3 段 LF^{2}SR, R_1 について考える．図 1(b)の記号シミュレーション結果より， $y_1(t+3)=0$ の場合，最終



(a) LF^{2}SR, R_1

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

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

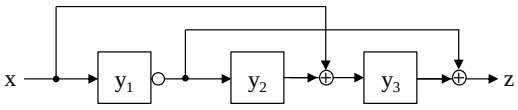
$y_1(t) = z(t+2)$
$y_2(t) = z(t+1)$
$y_3(t) = z(t) \oplus y_1(t)$
$= z(t) \oplus z(t+2)$

(b) R_1 に対する記号シミュレーション結果

図 1．SR 等価回路例

Strongly Secure Scan Design for Extended Shift Registers

Hiroshi YAMAZAKI, Toshinori HOSOKAWA, and Hideo FUJIWARA



(a) LF²SR, R_2

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

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

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

(b) R_2 に対する記号シミュレーション結果

図 2. 強セキュア回路例

状態は$(x(t), x(t+1), x(t+2)) = (y_3(t+3), y_2(t+3), y_1(t+3))$と固定される．すなわち，$y_1(t+3)=0$ 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，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．たとえば，入力系列$(x(t)=0, x(t+1)=0, x(t+2)=0)$を与えた場合，3 クロック周期後の最終状態は$(y_1(t+3)=0, y_2(t+3)=0, y_3(t+3)=0)$となり，入力系列と最終状態が等しくなる．同様に，$z(t+2)=0$ 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，$z(t+2)=0$ の場合は出力系列$(z(t+2), z(t+1), z(t))$は初期状態 $(y_3(t), y_2(t), y_1(t))$と等しくなる．たとえば，初期状態が$(y_1(t)=0, y_2(t)=0, y_3(t)=0)$である場合，出力系列は$(z(t+2)=0, z(t+1)=0, z(t)=0)$となる．このような状態が存在すると，攻撃者に拡張 SR が保持する FF 値を観測または初期化される可能性がある．このような問題を避けるために，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．

単一の入力，単一の出力，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 の任意の現在状態と，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 をスキャンイン安全と呼ぶ[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 1 の R_1 において $y_1(t+3)=0$ の場合，最終状態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，$z(t+2)=0$ の場合，出力系列は初期状態と等しくなるため，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 2 に強セキュアな回路を示す．図 2(a)は強セキュアな 3 段 LF²SR, R_2 である．図 2(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より，出力系列$(z(t+2)=y_1(t),\ z(t+1)=y_2(t) \oplus 1,\ z(t)=y_1(t) \oplus y_3(t) \oplus 1)$が得られ，内部状態は$(y_1(t+3)=x(t+2),\ y_2(t+3)=x(t+1) \oplus 1,\ y_3(t+3)=x(t+2) \oplus x(t) \oplus 1)$に遷移する．記号シミュレーション結果より，$y_2(t+3)$は $x(t+1)$と決して一致しない．そのため，R_2 はスキャンイン安全である．同様に，$z(t+1)$は $y_2(t)$と決して一致しない．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，SR 等価な回路に関しては，以下の定理 1 が成り立つ．

[定理 1] 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．

(証明) 回路 C の単一入力を x，単一出力を z，k 個の FF を入力側から y_1, y_2, …, y_k とする．時刻 t の入力を x(t)，出力を z(t)，状態を$(y_1(t), y_2(t), \cdots, y_k(t))$と表すことにすると，回路 C に長さ k の入力系列 x(t), x(t+1), …, x(t+k-1)を印加した後の時刻 t+k の状態は$(y_1(t+k), y_2(t+k), \cdots, y_k(t+k))$，時刻 t+k からの長さ k の出力系列は z(t+k), z(t+k+1), …, z(t+2k-1)と表される．ここで，回路 C は SR 等価であるので，z(t+k)=x(t), z(t+k+1)=x(t+1), …, z(t+2k-1)=x(t+k-1)となる．

(必要条件) C はスキャンアウト安全でないと仮定すると，$z(t+k)=y_k(t+k)$, …, $z(t+2k-1)=y_1(t+k)$となる出力系列 z(t+k), …, z(t+2k-1)と状態$(y_1(t+k), y_2(t+k), \cdots, y_k(t+k))$が存在する．C は SR 等価なので，z(t+k)=x(t), z(t+k+1)=x(t+1), …, z(t+2k-1)=x(t+k-1)である．したがって，$(y_1(t+k), y_2(t+k), \cdots, y_k(t+k))=(x(t+k-1), x(t+k-2), \cdots, x(t))$となる状態と入力系列が存在するので，C はスキャンイン安全でない．

(十分条件) C はスキャンイン安全でないと仮定すると，$x(t)=y_k(t+k)$, …, $x(t+k-1)=y_1(t+k)$となる入力系列 x(t), …, x(t+k-1)と状態$(y_1(t+k), y_2(t+k), \cdots, y_k(t+k))$が存在する．C は SR 等価なので，z(t+k)=x(t), z(t+k+1)=x(t+1), …, z(t+2k-1)=x(t+k-1)である．したがって，$(y_1(t+k), y_2(t+k), \cdots, y_k(t+k))=(z(t+2k-1), z(t+2k-2), \cdots, z(t+k))$となる状態と出力系列が存在するので，C はスキャンアウト安全でない．

(証明終)

4. $(I^2)LF^2SR$ に対する強セキュア回路設計

本章では，SR 等価な LF²SR と Inversion-inserted linear feed-forward SR (I^2LF^2SR)に対する，強セキュア化手法を提案する．定理 1 より SR 等価な拡張 SR に対する強セキュア化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, … , y_k)，からなる $(I^2)LF^2SR$，C について考える．図 3 にフリップフロップ y_p と y_{p+1} の間に再左端の XOR を配置した$(I^2)LF^2SR$ を示す．図 3 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 1 つの NOT ゲートを挿入した場合，スキャンイン安全となるため C の最終状態$(y_1, y_2, \cdots, y_p)$は常に SR と異なる．そのため，C は強セキュアとなる．しかしながら，NOT ゲートの挿入により $(I^2)LF^2SR$ が SR 等価でなくなる可能性が存在する．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．そのため，y_{p+1} から z の間に NOT ゲートをさらに挿入し，論理値の変化打ち消すことで SR 等価に変更する必要がある．

図 4 に NOT ゲートの挿入により，SR 等価でなくなった回路と記号シミュレーション結果を示す．図 4(a)は図 1 の R_1 のフリップフロップ y_2 の入力側に NOT ゲートを挿入した回路 R_3 である．図 4(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

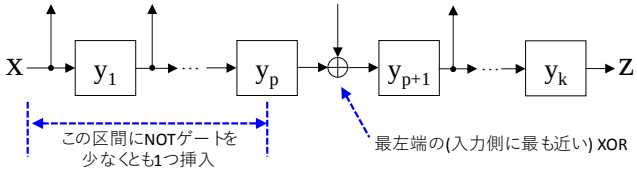
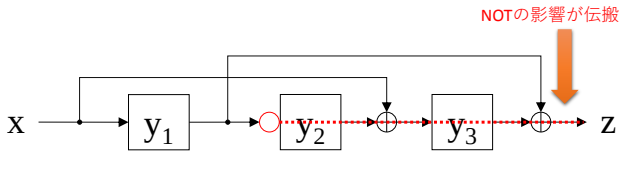


図 3. $(I^2)LF^2SR$ に対する強セキュア設計例

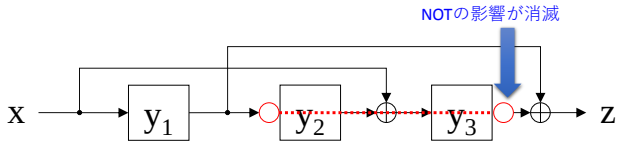


(a) I^2LF^2SR, R_3

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

(b) R_3 に対する記号シミュレーション結果

図 4. SR 等価な LF^2SR に NOT ゲートを挿入することで SR 等価でなくなる例



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

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

(b) R_4 に対する記号シミュレーション結果

図 5. SR 等価な LF^2SR に NOT ゲートを挿入することで SR 等価かつ強セキュアになる例

ョン結果より，$y_2(t+3)$は x(t+1)と決して一致しない．そのため，R_2 はスキャンイン安全である．同様に，z(t+2)は $y_1(t)$と決して一致しない．そのため，R_3 はスキャンアウト安全である．よって R_3 は強セキュアである．しかしながら，$z(t+3)=x(t) \oplus 1$ のため，SR 等価でないことがわかる．これは y_2 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．そのため，R_3 に対して y_2 から z の間にさらに NOT ゲートを挿入し，SR 等価にする必要がある．

図 5(a)に図 4 の R_3 に対して，さらに NOT ゲートを挿入した SR 等価かつ強セキュアな回路 R_4 を示す．図 5(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 ゲートを挿入することで，y_2 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，$y_2(t+3)$は x(t+1)と決して一致しないため，R_4 はスキャンイン安全である．このことから定理 1 より，R_4 は強セキュアである．以下に，SR 等価な LF^2SR と I^2LF^2SR に対する強セキュア化手順を示す．

LF^2SR と I^2LF^2SR に対する強セキュア化手順:

(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 とフリップフロップ y_p の間(図 3)に少なくとも 1 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，その変化を消すようフリップフロップ y_p と外部出力 z の間(図 3)に NOT ゲートを追加挿入し，SR 等価に変更する．

5. $(I^2)LFSR$ に対する強セキュア回路設計

本章では，SR 等価な Linear feedback SR (LFSR)と Inversion-inserted linear feedback SR (I^2LFSR)に対する，強セキュア化手法を提案する．定理 1 より SR 等価な拡張 SR に対する強セキュア化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$(I^2)LFSR$，C について考える．図 6 にフリップフロップ y_{q-1} と y_q の間に再右端の XOR を配置した$(I^2)LFSR$ を示す．図 6 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 1 つの NOT ゲートを挿入した場合，スキャンアウト安全となるため C の最終状態($y_q, y_{q+1}, \cdots, y_k$)は常に SR と異なる．そのため，C はスキャンアウト安全(強セキュア)となる．しかしながら，NOT ゲートの挿入により$(I^2)LFSR$ が SR 等価でなくなる可能性が存在する．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 まで伝搬しているためである．そのため，外部入力 x から y_q の間に NOT ゲートをさらに挿入し，論理値の変化打ち消すことで SR 等価に変更する必要がある．

図 7(a)に SR 等価だが強セキュアではない LFSR，R_5 を示す．図 7(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．また，図 7(c)に R_6 に対する記号シミュレーション結果を示す．R_6 の記号シミュレーション結果より，$y_3(t+3)$は x(t)と決して一致しない．そのため，R_6 はスキャンイン安全である．同様に，z(t+1)は $y_2(t)$と決して一致しない．そのため，R_6 はスキャンアウト安全である．よって R_3 は強セキュアである．しかしながら，$z(t+3)=x(t) \oplus 1$ のため，SR 等価でないことがわかる．これは y_2 の出力側に挿入した NOT ゲートの影響が，z まで伝搬しているためである．そのため，R_6 に対して x から y_2 の間にさらに NOT ゲートを挿入し，SR 等価にする必要がある．

図 8(a)に R6 に対して，さらに NOT ゲートを挿入した SR 等価かつ強セキュアな回路 R7 を示す．図 8(b)は R7 に対する記号シミュレーション結果である．R7 は R6 のフリップフロップ y1 の出力側に NOT ゲートを挿入することで，y2 の出力側に挿入した NOT ゲートの影響が z に伝搬しないようしている．記号シミュ

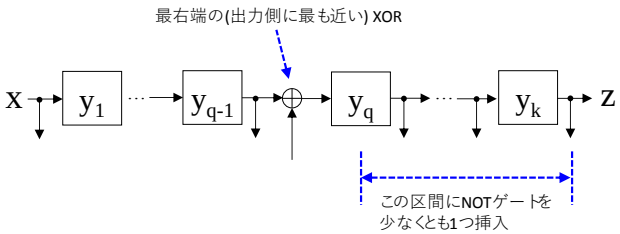
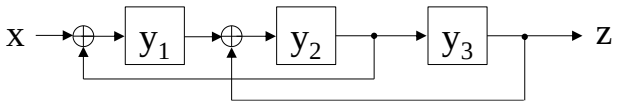
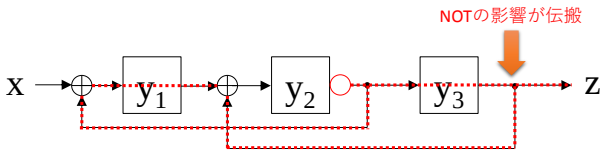


図 6. $(I^2)LFSR$ に対する強セキュア設計例



(a) LFSR, R_5

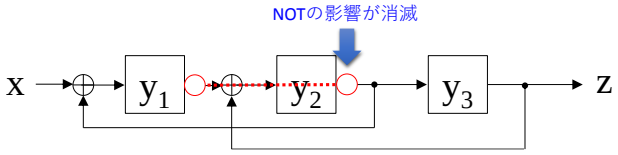


(b) I^2LFSR, R_6

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

(c)R_6 に対する記号シミュレーション結果

図 7. SR 等価な LFSR に NOT ゲートを挿入することで SR 等価でなくなる例



(a) LFSR, 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)	$x(t) \oplus y_2(t) \oplus 1$	$y_1(t) \oplus y_3(t)$	$y_2(t)$	$z(t+1) = y_2(t) \oplus 1$
x(t+2)	$x(t+1) \oplus y_1(t) \oplus y_3(t)$	$x(t) \oplus 1$	$y_1(t) \oplus y_3(t) \oplus 1$	$z(t+2) = y_1(t) \oplus y_3(t)$
x(t+3)	$x(t+2) \oplus x(t)$ $=y_1(t+3)$	$x(t+1) \oplus 1$ $=y_2(t+3)$	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 8. SR 等価な LFSR に NOT ゲートを挿入することで SR 等価かつ強セキュアになる例

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_7 は SR 等価である．また，z(t+1)は $y_2(t)$と決して一致しないため，R_7 はスキャンアウト安全である．このことから定理 1 より，R_7 は強セキュアである．以下に，SR 等価な LFSR と I^2LFSR に対する強セキュア化手順を示す．

LFSR と I^2LFSR に対する強セキュア化手順:

(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，フリップフロップ y_q と外部出力 z の間 (図 8)に少なくとも 1 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 の間(図 8)に NOT ゲートを追加挿入し，SR 等価に変更する．

6. まとめ

本論文では，SR 等価な拡張 SR のクラス $(I^2)LF^2SR$ と(I^2)LFSR に対して，強セキュアに変更する手法を提案した．強セキュアに変更することで，SR 等価性が失われた場合，論理値の変化を解析することで SR 等価に戻す手法を提案した．また，定理 1 で SR 等価な回路に対してスキャンイン安全であればスキャンアウト安全でもあり，その逆も成り立つことを証明した．今後の課題として，セキュリティ度合を明らかにするため，$(I^2)LF^2SR$ と(I^2)LFSR に対して，SR 等価かつ強セキュアな回路数の列挙が挙げられる．

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 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," Journal of 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.Tehranippr, C.Patel, and J.Plusquellic, "Securing Designs against Scan-Based Side-Channel Attacks," IEEE Trans. Dependable and Secure Computing, vol.4, no.4, pp.352-336, 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.Fujiwra and H.Fujiwara, and H.Tamamoto, "Secure and testable scan design utilizing shift register quasi-equivalents," IPSJ Trans. System LSI Design Methodology, vol.6, pp.27-33. 2013.

[12] K.Fujiwra and H.Fujiwara, "WAGSR: Web application for generalized feed forward shift registers," Proc. 13th IEEE Workshop on RTL and High Level Testing, pp.1.2.1-1.2.7, 2012.

[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, 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, Apr. 2016.