スキャンベース攻撃とその防御法に対する定量的なセキュリティ評価

伊藤, 侑磨
九州大学大学院システム情報科学府情報工学専攻

吉村, 正義
九州大学大学院システム情報科学研究院

安浦, 寛人
九州大学大学院システム情報科学研究院

出版情報：電子情報通信学会技術研究報告. 109 (316), pp.73-78, 2009-12. 電子情報通信学会
バージョン：
権利関係：

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

信学技報
TECHNICAL REPORT OF IEICE.

スキャンベース攻撃とその防御法に対する定量的なセキュリティ評価

伊藤　侑磨†　　吉村　正義††　　安浦　寛人††

† 九州大学大学院システム情報科学府情報工学専攻　〒 819–0395 福岡県福岡市西区元岡 744
†† 九州大学大学院システム情報科学研究院　〒 819–0395 福岡県福岡市西区元岡 744
E-mail: †{yuma,yosimura,yasuura}@c.csce.kyushu-u.ac.jp

あらまし　スキャンチェーンを悪用して，暗号 LSI 上で扱われる秘密情報を特定するスキャンベース攻撃の危険性が指摘されている．スキャンベース攻撃に対する防御法には様々な手法が存在する．回路設計時には，これらの防御法を適用した回路のセキュリティを定量的に評価し，防御法を選択する必要がある．しかしながら，スキャンベース攻撃に対する回路の定量的なセキュリティ評価については，あまり議論されていない．そこで本稿では，スキャンベース攻撃に対する回路のセキュリティ評価手法を提案する．提案手法では，攻撃者が取得できる取得情報と攻撃者が特定したい秘密情報との相互情報量を指標として評価を行う．回路構成の異なる DES 回路を例に提案評価手法を用いてセキュリティを評価し，回路構成によって回路のセキュリティが異なることを定量的に示す．

キーワード　スキャンベース攻撃，セキュリティ，相互情報量，DES，BIST

A Quantitative Evaluation of Security for Scan-based Side Channel Attack and Countermeasures

Yuma ITO†, Masayoshi YOSHIMURA††, and Hiroto YASUURA††

† Graduate School of Information Science and Electrical Engineering, Kyushu University　Motooka 744, Nishi-ku, Fukuoka-shi, Fukuoka, 819–0395 Japan
†† Faculty of Information Science and Electrical Engineering, Kyushu University　Motooka 744, Nishi-ku, Fukuoka-shi, Fukuoka, 819–0395 Japan
E-mail: †{yuma,yosimura,yasuura}@c.csce.kyushu-u.ac.jp

Abstract　There is a potential that the secret information on an encryption LSI is leaked from a scan chain. There are many countermeasures against scan based attack. When we design a circuit, we need to evaluate a security of the circuit applied these countermeasures quantitatively and choose the best one. However, it is not discussed a quantitative security evaluation against scan based attack so much. In this paper, we propose a quantitative security evaluation method. In this method, we evaluate security using a mutual information between the obtained information which an attacker can obtain and the secret information which an attacker wants to get as an evaluation index. We evaluate securities of DES circuits with different configurations using the proposed method and show quantitatively that the security of a circuit depends on its configuration.

Key words　scan based attack，security，mutual information，DES，BIST

1. はじめに

セキュリティ対策，著作権保護などの要求から，現在様々なデジタル製品には暗号 LSI が搭載されている．暗号 LSI 上では暗号化・復号化に用いる秘密鍵などの秘密情報が扱われる．暗号 LSI に対する攻撃法はサイドチャネル攻撃 [1] など様々なものが考案されており，暗号 LSI は悪意ある第三者からの攻撃の脅威にさらされている．このため，攻撃及び攻撃に対する防御法に対する関心が高まっている．

暗号 LSI を含む現在のほとんどの LSI には，テストを効率的に行うためにテスト容易化設計が用いられている．最も一般的なテスト容易化設計にスキャン設計がある [2]．スキャン設計では，LSI 中のフリップフロップ (FF) を数珠つなぎに接続し，シフトレジスタとして構成する．これにより LSI 中の FF を LSI の外部から直接制御・観測することが可能になり，LSI のテストを効率的に行える．また，スキャンチェーンは LSI が故障した際の故障診断にも用いることができる．このため，製品出荷後もスキャンチェーンは使用できる状態であることが多い．

しかしながら，スキャン設計を悪用し，暗号 LSI 上の秘密情報を特定する攻撃の危険性が指摘されている．文献 [3], [4] において，Yang らは共通鍵暗号である DES(Data Encryption Standard) 及び AES(Advanced Encryption Standard) に対するスキャンベース攻撃を提案している．一般的な共通鍵暗号では，ラウンドと呼ばれる処理を複数回繰り返すことで暗号化を行う．Yang らの攻撃法では，暗号 LSI のレジスタに保持されているラウンド処理の結果をスキャンチェーンを介して取得し，秘密情報を推測している．

スキャンベース攻撃に対する防御法には，高いテスト容易性とセキュリティを両立させることが求められる．また，面積などのオーバーヘッドも許容範囲内に抑える必要がある．現在までにスキャンベース攻撃に対する防御法は様々な手法が提案されている [4]〜[8]．しかしながら，これらの多くは元の回路に対してテスト容易性の低下や面積の増加を招くなどの問題がある．よって，実際にスキャンベース攻撃を考慮して回路の設計を行う際には，セキュリティ，テスト容易性，面積などのバランスを考慮して最適な防御法を選択する必要がある．そのためには，セキュリティ，テスト容易性，面積などについて定量的な評価を行う必要がある．テスト容易性は，故障検出率などの指標を用いて定量的な評価を行うことが可能である．また，面積もゲート数などによって定量的に評価することが可能である．しかしながら，セキュリティに関する定量的な評価についてあまり議論されておらず，スキャンベース攻撃に対する回路の定量的なセキュリティ評価が難しい．

そこで，本稿ではスキャンベース攻撃に対する暗号回路のセキュリティの定量的な評価について議論を行う．スキャンベース攻撃では，攻撃者はスキャンチェーンを悪用し，暗号回路から得た暗号化の中間結果などからラウンドキーなどの秘密情報を推測する．そこで本稿では，評価対象の暗号回路から攻撃者が取得できる取得情報が，秘密情報に関してどれほどの情報量を持つか，つまり取得情報と秘密情報との相互情報量を評価することで，スキャンベース攻撃に対する暗号回路のセキュリティを定量的に評価する．本稿の評価手法では，まず暗号回路を取得情報や秘密情報及びそれらを関連付ける関数によってモデル化する．さらに，このモデル上の関数における入出力間の確率分布を解析し，得られた確率分布から取得情報と秘密情報との相互情報量を求める．

さらに，フルスキャン設計及び，BIST(Built In Self Test) を適用した DES 暗号回路を例にセキュリティ評価を行う．評価結果より，回路構成によってセキュリティが変化することを定量的に示す．

本稿の構成は以下の通りである．まず，第 2 章でスキャンベース攻撃について述べる．第 3 章でセキュリティ評価手法について述べ，第 4 章で回路構成の異なる DES 暗号回路でのセキュリティ評価について述べる．最後に第 5 章で本稿をまとめる．

2. スキャンベース攻撃

本章では，文献 [3] で Yang らが提案した DES(Data Encryption Standard) に対するスキャンベース攻撃の概要を説明する．

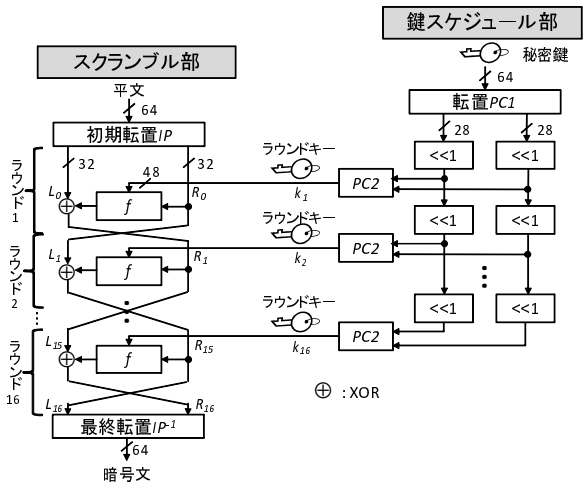

図 1　DES の基本構造

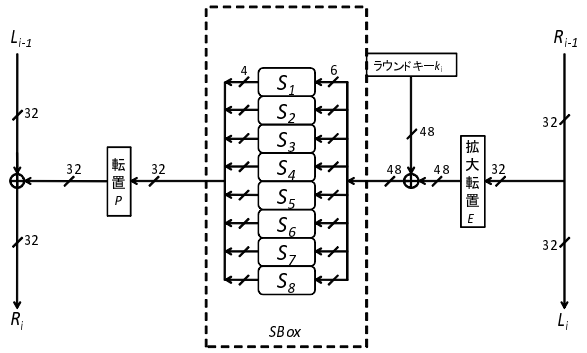

図 2　DES のラウンド関数 f

2.1 DES(Data Encryption Standard)

DES(Data Encryption Standard) は，1977 年にアメリカ合衆国の連邦情報処理標準規格（FIPS）に採用された共通鍵暗号である [9]．DES は 64bit の平文を 56bit の秘密鍵を用いて 64bit の暗号文に暗号化する．

図 1 に DES の基本構造を示す．64bit の平文を左右 32bit（L_i と R_i）に分け，左右のデータを交互にラウンド関数 f に入力し，f による処理を 16 ラウンド繰り返す．ラウンド i では，そのラウンドに対応した 48bit のラウンドキー K_i を用いる．ラウンドキー K_i は，鍵スケジュール部で転置やシフト処理を行い生成される．

暗号化処理は，まず初期転置 IP によって 64bit の平文を並べ換え，ラウンド処理を 16 回繰り返し，最後に IP の逆変換である最終転置 IP^{-1} を行う．ラウンド処理における関数 f の構成を図 2 に示す．関数 f ではまずビット重複を許して 32bit のデータを 48bit に並べ替える拡大転置 E を行う．次に，48bit のラウンドキーとの XOR を行い，その後，出力 48 bit は 6bit ずつ 8 個に分割される．分割された出力はそれぞれ，$SBox$ と呼ばれる 6bit 入力 4bit 出力の 8 個のランダムな置換テーブル（S_1〜S_8）に入力され，4bit 出力となる．最後に 8 個の 4bit 出力をまとめ，32bit 転置 P を行う．

表 1 に $SBox$ の置換表の例として S_1 の置換表（10 進数で表記）を示す．S_1 では入力の最上位ビットと最下位ビットの 2bit

表 1　$SBox(S_1)$ の置換表

Address	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

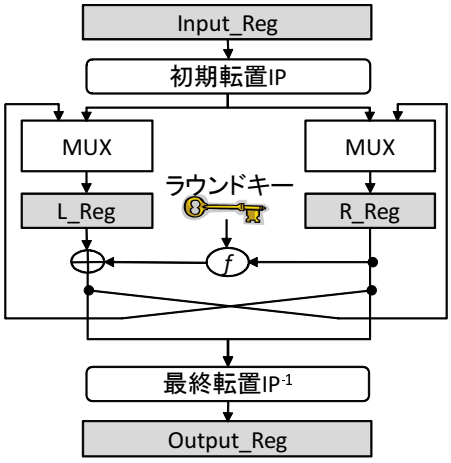

図 3　DES の実装例

で置換表の行を，残りの 4bit で列を指定し，出力が決定される．表 1 から分かるように任意の出力となる入力は 4 つある．S_2〜S_8 も同様に任意の出力となる入力が 4 つあり，出力から入力が一意に決定できないという性質を持つ．

DES の実装例を図 3 に示す．Input_Reg に平文が保持される．R_Reg，L_Reg には各ラウンド終了後の処理結果が保持される．16 ラウンドの暗号化処理の後，暗号文が Output_Reg に保持される．

2.2　攻撃の概要

図 3 に示す DES の実装例を用いて文献 [3] で提案されている DES に対するスキャンベース攻撃の概要を説明する．

スキャンチェーンを利用して DES の秘密鍵を特定する際の手順は大きく分けて 3 つある．以下にその 3 つの手順を示す．

手順 1 スキャンチェーンの構造を特定する．

手順 2 ラウンドキーを特定する．

手順 3 ラウンドキーから秘密鍵を求める．

手順 1 では，まず，1bit ずつ異なる既知の平文を入力し，クロックを進め，スキャンチェーン中の位置を特定したいレジスタに平文を保持させる．次にテストモードでスキャンチェーンよりビット列を読み出す．これらのビット列を比較することで，スキャンチェーン中での FF の位置を特定することができる．**手順 2** では，**手順 1** で特定したスキャンチェーンの構造を用いて，R_Reg と L_Reg に保持される DES の 1 ラウンド目の処理結果を読み出す．1 ラウンド目の処理結果より，$Sbox$ の出力を特定することができる．さらに，特定のビットが異なる 3 つの平文を入力することで $Sbox$ の出力から $Sbox$ の入力を求め，ラウンドキーを特定することができる．最後に**手順 3** で，ラウンドキーより秘密鍵を特定する．ラウンドキー K_1 より秘密鍵 56bit 中の 48bit は特定できる．さらに，**手順 2** と同様にラウンドキー K_2，K_3 を求め，これらより秘密鍵の残り 8bit を特定する．

3.　セキュリティ評価手法

本章では，スキャンベース攻撃に対する暗号回路の定量的なセキュリティ評価手法について説明する．2 章で述べたように，攻撃者はレジスタに保持されている暗号化の中間結果をスキャンチェーンを介して取得し，この値から 1 ラウンド目のラウンドキーの候補を絞り込む．この時，回路構成によっては，ラウンドキーの候補数や，それぞれの候補である確率に偏りがある場合も考えられる．よって，評価を行う際には，評価対象の回路において，攻撃者が入手できる取得情報から秘密情報の候補数をどれほど絞り込めるのか，及びそれらの候補ごとの確率的な偏りも考慮できる評価が適当である．そこで本稿では，攻撃者が入手できる取得情報と秘密情報との相互情報量を評価指標として，暗号回路のセキュリティを定量的に評価する．本稿では，取得情報と秘密情報との相互情報量を求めるために，まず暗号回路を取得情報や秘密情報及びそれらを関連付ける関数によってモデル化する．さらに，このモデル上の関数における入出力間の確率分布を解析し，得られた確率分布から取得情報と秘密情報との相互情報量を求める．

なお，本稿では，暗号回路に実装されている暗号は共通鍵暗号と仮定する．共通鍵暗号は，ラウンド関数での処理を複数回繰り返すことで暗号化を行う．本稿で想定する暗号回路では，各ラウンドごとの中間結果がレジスタに保持されるものとする．また，攻撃者はスキャンチェーンを含む暗号回路の構造を知っているものと仮定する．よって攻撃者は，秘密情報に依存する値以外を保持するレジスタの値を知っており，スキャンチェーンから得られたビット列と回路中の FF との対応を知っている．

3.1　相互情報量

本節では，本稿でセキュリティの評価指標として用いる相互情報量 [10] について説明する．相互情報量は，二つの確率変数について，一方の確率変数を知ることでもう一方の確率変数についてどれだけ推測できるようになるかを表す量である．

2 つの確率変数 X, Y に対して相互情報量 $I(X;Y)$ は式 (1) で定義される．

$$I(X;Y) = H(X) - H(X|Y)[\text{bit}] \qquad (1)$$

$H(X)$ は X の平均情報量あるいはエントロピーと呼ばれ，元々の X の曖昧さを表す量であり，$H(X|Y)$ は条件付き情報量あるいは条件付きエントロピーと呼ばれ Y を知ったあとで残る X の曖昧さを表す量である．つまり，相互情報量は Y を知ることにより減る X の曖昧さの量を表す．よって，相互情報量が大きいほど X と Y は関連性が高く，一方を知った時に他方について多くの情報を得られることになる．特に，相互情報量が 0 だった場合は，X と Y にはまったく関連性がない，つまり独立であることを意味する．逆に相互情報量が $H(X)$ と等しいとき，つまり $H(X|Y) = 0$ のとき，X と Y は全く同じであり，一方を知れば，他方を完全に推測できることを意味する．

$H(X)$，$H(X|Y)$ は，それぞれ式 (2)，(3) で定義される．な

お，$P_X(x)$ は確率変数 X が実現値 x をとる確率であり，X の周辺確率を表す．同様に $P_Y(y)$ 及び $P_{X|Y}(x|y)$ はそれぞれ Y の周辺確率，Y で条件を付けた X の条件付き確率を表す．また，対数の底は 2 である．

$$H(X) = -\sum_x P_X(x) \log P_X(x)[\text{bit}] \tag{2}$$

$$H(X|Y) = -\sum_y P_Y(y) \sum_x P_{X|Y}(x|y) \log P_{X|Y}(x|y)[\text{bit}] \tag{3}$$

また，$P_{X|Y}(x|y)$ は X と Y の結合確率 $P_{XY}(x,y)$ を用いて式 (4) より求められる．よって，X と Y の結合確率分布が分かれば相互情報量を求めることができる．

$$P_{X|Y}(x|y) = \frac{P_{XY}(x,y)}{P_Y(y)} \tag{4}$$

3.2 評 価 手 法

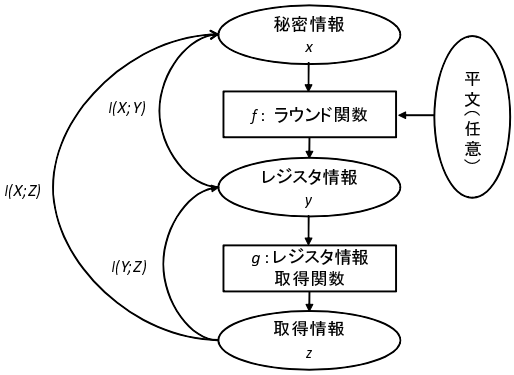

図 4　共通鍵暗号回路モデル

図 4 に本稿で評価対象とする共通鍵暗号回路モデルを示す．回路モデルは以下から成る．

- ラウンド関数 f : ラウンド処理を行う関数
- レジスタ情報取得関数 g : レジスタの値を外部に出力する関数

また，ラウンド関数 f の入力 $x \in V_X$ を**秘密情報**，レジスタ情報取得関数 g の入力（ラウンド関数 f の出力）$y \in V_Y$ を**レジスタ情報**，レジスタ情報取得関数の出力 $z \in V_Z$ を**取得情報**と呼ぶ．なお，集合 V_X, V_Y, V_Z はそれぞれ秘密情報集合，レジスタ情報集合，取得情報集合である．秘密情報はラウンドキーなどの攻撃者が特定したい情報，レジスタ情報はレジスタに保持されるラウンド関数 f の処理結果，取得情報はスキャンチェーンなどを介して攻撃者が取得できる情報に対応する．

V_X, V_Y, V_Z 上の確率変数をそれぞれ X, Y, Z とする．本稿では攻撃者は任意の平文を回路に与えられると仮定する．よって，Y や Z は，X の確率分布，及び関数 f, g の性質によってその確率分布が決まる．本稿では，X は V_X 上の一様分布に従うものとする．

以上の確率変数を考えた場合，相互情報量 $I(X;Y)$ は，レジスタ情報を知ることで得られる秘密情報の情報量を表し，相互情報量 $I(Y;Z)$ は，取得情報を知ることで得られるレジスタ情報の情報量を表し，相互情報量 $I(X;Z)$ は，取得情報を知ることで得られる秘密情報の情報量を表す．攻撃者は取得情報から秘密情報を推測するので，回路のセキュリティは取得情報と秘密情報との相互情報量 $I(X;Z)$ で評価できる．相互情報量 $I(X;Z)$ が小さいほど取得情報から秘密情報を推測することが難しく，セキュリティが高いことを意味する．

以下では，相互情報量 $I(X;Z)$ の求め方について述べる．相互情報量 $I(X;Z)$ を求めるには，X と Z の結合確率分布を求める必要がある．そこで，まず回路モデル上のラウンド関数 f の入出力として関連付けられている X と Y，及びレジスタ情報取得関数 g の入出力として関連付けられている Y と Z の結合確率分布 $P_{XY}(x,y)$，$P_{YZ}(y,z)$ をこれらの関数の入出力表より求める．これらの確率分布から X と Z の結合確率分布 $P_{XZ}(x,z)$ を求め，その後，$P_{XZ}(x,z)$ から定義に従って相互情報量を求める．

4. 評 価 結 果

本章では，フルスキャン設計，及び BIST を適用した DES 回路を例に回路のセキュリティを評価する．

4.1 フルスキャン設計 DES 回路

DES ではラウンドキーは 48bit，f 関数の出力は 32bit なので $V_X = \{0,1\}^{48}$，$V_Y = \{0,1\}^{32}$ である．またフルスキャン設計回路では，レジスタの値がスキャンチェーンを介して外部にそのまま出力されるので，$V_Z = \{0,1\}^{32}$ である．評価対象回路は以下から成る．

- $f : \{0,1\}^{48} \times \{0,1\}^{32} \to \{0,1\}^{32}$
- $g : \{0,1\}^{32} \to \{0,1\}^{32}$

DES のラウンド関数において，秘密情報を特定する際に問題になるのは，$SBox$ の出力から入力を一意に特定できないことである．ラウンド関数の他の部分については出力から入力を一意に特定することが可能である．よって本稿では，簡単のためラウンド関数 f は $SBox$ のみで構成されているとする．また，フルスキャン設計回路では，レジスタ情報取得関数 g は入力をそのまま出力する関数である．よって，フルスキャン設計回路では式 (5) が成り立つ．

$$I(X;Z) = I(X;Y) \tag{5}$$

以下，$SBox$ の入出力間の確率分布を解析し，$I(X;Y)$ を求める．まず，$SBox$ 中の S_1 に着目する．$V_{X_1} = \{0,1\}^6, V_{Y_1} = \{0,1\}^4$ をそれぞれ S_1 の入力集合と出力集合とし，V_{X_1}, V_{Y_1} 上の確率変数を X_1, Y_1 とする．X_1 は V_{X_1} 上の一様分布に従うとする．X_1 と Y_1 の結合確率分布 $P_{X_1Y_1}(x,y)$ は表 1 に示す S_1 の入出力表から求めることができる．表 2 に $P_{X_1Y_1}(x,y)$ を示す．式 (4) を用いて求めた条件付き確率分布 $P_{X_1|Y_1}(x|y)$ を表 3 に示す．表 3 から任意の出力に対して入力の候補数は 2^2 であり，それぞれの条件付き確率は $1/2^2$ であることが分かる．よって，$H(X_1|Y_1)$ は式 (6) のように求められる．

$$H(X_1|Y_1) = \frac{1}{2^4}(-\frac{1}{2^2}\log\frac{1}{2^2} \cdot 2^2) \cdot 2^4 = 2[\text{bit}] \tag{6}$$

S_2〜S_8 においても同様の結果が得られる．S_1〜S_8 はそれぞれ

表 2　S_1 における入力 X_1 と出力 Y_1 の結合確率分布

		Y_1					
$P_{X_1Y_1}(x,y)$		0000	0001	$\cdots$	1110	1111	$P_{X_1}(x)$
X_1	000000	0	0	0	$\frac{1}{2^6}$	0	$\frac{1}{2^6}$
	$\vdots$	$\vdots$	0	$\cdots$	$\vdots$	$\vdots$	$\vdots$
	000110	0	$\frac{1}{2^6}$	0	0	0	$\frac{1}{2^6}$
	$\vdots$	$\vdots$	0	$\cdots$	$\vdots$	$\vdots$	$\vdots$
	001111	0	$\frac{1}{2^6}$	0	0	0	$\frac{1}{2^6}$
	$\vdots$	$\vdots$	0	$\cdots$	$\vdots$	$\vdots$	$\vdots$
	100010	0	$\frac{1}{2^6}$	0	0	0	$\frac{1}{2^6}$
	$\vdots$	$\vdots$	0	$\cdots$	$\vdots$	$\vdots$	$\vdots$
	101101	0	$\frac{1}{2^6}$	0	0	0	$\frac{1}{2^6}$
	$\vdots$	$\vdots$	0	$\cdots$	$\vdots$	$\vdots$	$\vdots$
	111111	0	0	$\cdots$	0	0	$\frac{1}{2^6}$
$P_{Y_1}(y)$		$\frac{1}{2^4}$	$\frac{1}{2^4}$	$\cdots$	$\frac{1}{2^4}$	$\frac{1}{2^4}$	

表 3　S_1 における出力 Y_1 で条件を付けた入力 X_1 の条件付き確率分布

		Y_1				
$P_{X_1\|Y_1}(x\|y)$		0000	0001	$\cdots$	1110	1111
X_1	000000	0	0	0	$\frac{1}{2^2}$	0
	$\vdots$	$\vdots$	0	$\cdots$	$\vdots$	$\vdots$
	000110	0	$\frac{1}{2^2}$	0	0	0
	$\vdots$	$\vdots$	0	$\cdots$	$\vdots$	$\vdots$
	001111	0	$\frac{1}{2^2}$	0	0	0
	$\vdots$	$\vdots$	0	$\cdots$	$\vdots$	$\vdots$
	100010	0	$\frac{1}{2^2}$	0	0	0
	$\vdots$	$\vdots$	0	$\cdots$	$\vdots$	$\vdots$
	101101	0	$\frac{1}{2^2}$	0	0	0
	$\vdots$	$\vdots$	0	$\cdots$	$\vdots$	$\vdots$
	111111	0	0	$\cdots$	0	0

独立に処理を行うので，$SBox$ 全体での条件付きエントロピー $H(X|Y)$ は $2 \times 8 = 16$[bit] である．つまり，任意のレジスタ情報に対して，秘密情報の候補数は 2^{16} であり，それぞれの条件付き確率は $1/2^{16}$ である．また，X が $\{0,1\}^{48}$ 上の一様分布に従うため，$H(X) = -(\frac{1}{2^{48}} \log \frac{1}{2^{48}}) \cdot 2^{48} = 48$[bit] である．

以上より，相互情報量 $I(X;Z)$ は，式 (7) のように計算される．

$$\begin{aligned} I(X;Z) &= I(X;Y) \\ &= H(X) - H(X|Y) \\ &= 48 - 16 = 32[\text{bit}] \end{aligned} \tag{7}$$

4.2　BIST を適用した DES 回路

本節では，BIST(Built In Self Test) を適用した DES 回路についてセキュリティの評価を行う．BIST では回路からの出力は，SISR(Single Input Shift Resister)(図 5) や MISR(Multi Input Shift Resister)(図 6) などの LFSR(Linear Feedback Shift Resister) で圧縮される．本節では，レジスタ情報取得関数 g として，図 5 や図 6 のような 16 段の LFSR を仮定する．また，簡単のため，LFSR に対してレジスタ情報が直接入力されるものとする．取得情報は，レジスタ情報がすべて LFSR に入力され終わったときの LFSR の内容とする．32bit のレジスタ情報が 16bit の取得情報に圧縮されるため，取得情報と秘密情報との相互情報量 $I(X;Z)$ は，フルスキャン設計に比べて低下する，つまりセキュリティが向上することが予想される．

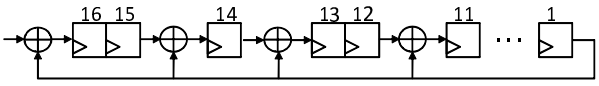

図 5　16 段 SISR の例

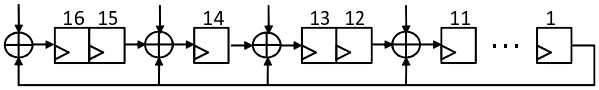

図 6　16 段 MISR の例

フルスキャン設計の DES 回路と異なるのは，レジスタ情報取得関数 g とその出力である取得情報である．よって，V_X，V_Y は 4.1 節と同様である．また，取得情報は LFSR によって 16bit に圧縮されるため，$V_Z = \{0,1\}^{16}$ である．評価対象回路は以下から成る．

- $f : \{0,1\}^{48} \times \{0,1\}^{32} \to \{0,1\}^{32}$
- $g : \{0,1\}^{32} \to \{0,1\}^{16}$

4.1 節で述べたように，ラウンド関数 f の入出力において任意の出力に対して，入力の候補数は 2^{16} であり，それぞれの条件付き確率は $1/2^{16}$ である．また，レジスタ情報取得関数 g において，任意の出力に対して，入力の候補数は 2^{16} であり，それぞれの条件付き確率は $1/2^{16}$ である．ラウンド関数 f や，レジスタ情報取得関数 g は，関数であるため任意の入力に対してその出力は一意に決まる．言い換えると，異なる出力から推測

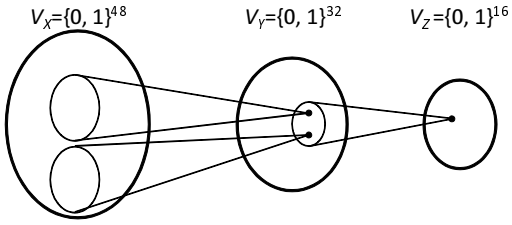

図 7　BIST を適用した DES 回路での情報の関係

できる入力の候補集合は重なることはない．よって，図 7 に示すように，任意の取得情報に対するレジスタ情報の候補集合の各元から考えられる秘密情報の候補集合はすべて異なる．この時，任意の取得情報に対して，秘密情報の候補数は 2^{32} であり，それぞれの条件付き確率は $1/2^{32}$ である．よって，$H(X|Z)$ は式 (8) のように求められる．

$$H(X|Z) = \frac{1}{2^{32}}(-\frac{1}{2^{32}} \log \frac{1}{2^{32}} \cdot 2^{32}) \cdot 2^{32} = 32[\text{bit}] \tag{8}$$

以上より，相互情報量 $I(X;Z)$ は，式 (9) のように計算される．

$$\begin{aligned} I(X;Z) &= H(X) - H(X|Z) \\ &= 48 - 32 = 16[\text{bit}] \end{aligned} \tag{9}$$

4.3 考　　察

まず，評価結果について考察する．フルスキャン設計の DES 回路においては取得情報と秘密情報との相互情報量 $I(X;Z)$ は 32bit であった．一方，BIST を適用した DES 回路における相互情報量 $I(X;Z)$ は 16bit であった．この結果から，BIST によって回路のセキュリティは向上すると言える．

次に，相互情報量 $I(X;Z)$ を最小とする関数について考察する．関数では，任意の入力に対してその出力が一意に決定される．言い換えると，異なる出力から推測できる入力の候補集合が重なることはない．よって $I(X;Z)$ を最小とするには，$I(X;Y)$ と $I(Y;Z)$ をそれぞれ最小にするようなラウンド関数 f，及びレジスタ情報取得関数 g を用いればよい．

ここで，関数 $h : \{0,1\}^m \rightarrow \{0,1\}^n$ を考える．ただし $m > n$ とする．$\{0,1\}^m$, $\{0,1\}^n$ 上の確率変数をそれぞれ A，B とする．式 (1) より，$I(A;B)$ を最小にするには，条件付きエントロピー $H(A|B)$ を最大にすればよい．$H(A|B)$ が最大になるのは，任意の出力 $b \in \{0,1\}^n$ に対して，$b = h(a)$ を満たす入力 $a \in \{0,1\}^m$ の数が 2^{m-n} 個であり，それぞれの条件付き確率が $1/2^{m-n}$ となる場合である．本章で評価した DES の $SBox$ や LFSR はこのような性質を満たしており，16bit の取得情報と 48bit の秘密情報を考えた場合，相互情報量 $I(X;Z)$ は最小となっている．

5. おわりに

本稿では，スキャンベース攻撃に対する暗号回路のセキュリティ評価手法を提案した．提案したセキュリティ評価手法では，取得情報と秘密情報の相互情報量を評価指標として，暗号回路のセキュリティを定量的に評価した．また，フルスキャン設計の DES 回路と BIST を適用した DES 回路を例に，セキュリティ評価を行った．その結果，BIST を適用した回路では，フルスキャン設計の回路に比べ，セキュリティが向上することが定量的に示された．

今後の課題としては，公開鍵暗号などの他の暗号回路に対しても評価を行えるようにモデルの拡張を行うことが挙げられる．

謝　　辞

本研究の一部は，科学技術振興機構 (JST) の戦略的創造研究推進事業 (CREST-DVLSI)「統合的高信頼化設計のためのモデル化と検出・訂正・回復技術」，及び科学研究費補助金・基盤 A(No.19200004)，科学研究費補助金・若手研究 B(No.20700050) の支援による．

文　　献

[1] YongBin Zhou, DengGuo Feng, “Side-Channel Attacks: Ten Years After Its Publication and the Impacts on Cryptographic Module Security Testing”, Cryptology ePrint Archive, Report 2005/388.

[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，東京，2004.

[3] Bo Yang, Kaijie Wu, Ramesh Karri, “Scan Based Side Channel Attack on Dedicated Hardware Implementations of Data Encryption Standard”, Test Conference, 2004. Proceedings. ITC 2004. International, pp.339–344, 2004.

[4] Bo Yang, Kaijie Wu, Ramesh Karri, “Secure Scan: A Design-for-Test Architecture for Crypto Chips”, Annual ACM IEEE Design Automation Conference, pp.135–140, 2005.

[5] 伊藤侑磨，吉村正義，安浦寛人，“スキャンパス攻撃を考慮した暗号 LSI のテスタビリティ評価”，信学技報 Vol.107 No.482，pp.57–62，2008.

[6] 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”，信学技報 Vol.107 No.482，pp.39–44，2008.

[7] M. Doulcier, M.-L. Flottes, B. Rouzeyre, “AES-Based BIST: Self-Test, Test Pattern Generation and Signature Analysis,” 4th IEEE International Symposium on Electronic Design, Test and Applications (delta 2008), delta,pp.314-321, 2008.

[8] J. Lee, M. Tehranipoor, J. Plusquellic, “Securing Designs against Scan-Based Side-Channel Attacks”, IEEE transactions on dependable and secure computing, Volume 4, Issue 4, 2007.

[9] “FIPS 46-3,Data Encryption Standard(DES)”,NIST, http://csrc.nist.gov/publications/fips/fip s46-3/fips46-3.pdf，1999.

[10] 今井秀樹，情報・符号・暗号の理論，コロナ社，東京，2004.