ISSN 2186-5647

2-35

IP 保護のための論理暗号化の評価

日大生産工(学部)　○橋立　英実　日大生産工　細川　利典
京都産業大　吉村　正義

1　はじめに

近年，超大規模集積回路(Very Large Scale Integrated circuits: VLSI)は，社会情報基盤技術や，機密情報に関する情報を保持するシステムにおいて使用されている．このため，VLSI の信頼性が社会に与える影響は大きくなっている[1]．また，VLSI は大規模化や高集積化のため，回路規模が増大している．VLSI の設計は，人件費や設計コストの削減のため，外部から IP コア(Intellectual Property core)を購入するケースが増加している[2]．自社ですべての機能ブロックの設計を行うよりも，IP ベンダから IP コアを購入し，VLSI の一部の機能ブロックを実現することにより，設計コストの削減を図っている．しかしながら，その結果として VLSI の著作権侵害による信頼性の低下が懸念されている[3]．具体例として，マスクの窃盗や，工場が許可していない過剰な数の VLSI を生産による VLSI の信頼性の低下が挙げられる．最近の研究では，VLSI の著作権侵害は電子産業や防御産業において主要な攻撃となっている[3].

これに対し EPIC(Ending Piracy of Integrated Circuits)[10]は，IP 権利保有者のみが生成することができる外部鍵を用いて，各チップを機能動作させることができる．ここで，鍵は複製できないものと仮定する．EPIC は(1)自動チップ ID 生成器，(2)組合せ論理暗号化，(3)公開鍵暗号[4]の仕様に基づいて VLSI の著作権侵害に対抗する回路を設計する．本論文において，論理暗号化とは論理回路を暗号化することで，暗号化とは正しい鍵を入力しない限り，通常の機能動作を行わないようにすることと定義する．また，活性化とは，回路に対して正しい鍵を入力することにより，元の回路と同等の機能を有する状態と定義する．EPIC は，論理暗号化のオーバーヘッドによる回路の遅延や消費電力が小さく，検証のための標準設計フローやテスト方式を変更する必要がない．網羅的なプロトコル解析により，EPIC は様々な著作権侵害の試みに対して驚異的な対抗策であることが示された[9]. しかしながら, EPIC では，ランダムに論理暗号化を行う信号線を決定するので，間違った鍵を印加しても，通常の機能動作を有することがある，という課題を有していた．その課題を解決するために，ランダムパターン故障シミュレーションを用いて，故障が外部出力に伝搬されやすい信号線に論理暗号化回路を挿入する方法が提案されている(FLE：Fault analysis based Logic Encryption) [6]．本論文では，さらに FLE を拡張して故障が検出される外部出力数が多い故障箇所の信号線に論理暗号化回路を挿入する方法を提案する．

第 2 章では，EPIC による暗号化フローを説明する．第 3 章では，既存の設計フローに論理暗号化を追加したフローを説明する．第 4 章では，論理暗号化が施された VLSI の製造フロー及びテストフローについて説明する．第 5 章では，組合せ回路の論理暗号化の鍵探索問題を定式化して考察する．第 6 章では，故障シミュレーションを用いた論理暗号化箇所決定アルゴリズムを説明し，第 7 章に実験結果を示す. 第 8 章で本論文をまとめ, 今後の課題を挙げる．

2　論理暗号化フロー

この章では EPIC による論理暗号化のフローを説明する．図 1 に, 既存の VLSI の設計/製造フローに新しいプロトコルを追加したフローを示す. まず始めに VLSI 設計者はチップ ID を生成する[7]. VLSI 設計者は IP ベンダに対してチップ ID を送信する．IP ベンダは，チップ ID と公開鍵暗号方式[4]を用いて, マスターの公開鍵と秘密鍵を生成し, マスターの公開鍵を VLSI 設計者に送信する．VLSI 設計者はマスターの秘密鍵と乱数生成器を IP コアに埋め込み, 論理合成を行う．その後，組合せ論理暗号化を行う．論理暗号化を行うことによって, 共通鍵が生成される. VLSI 設計者は共通鍵を IP ベンダに送信しなければならない．VLSI 設計者が暗号化されたマスクを生成し，それを製造ベンダに送る．製造ベンダは，暗号化されたマスクを用いて，VLSI を製造する．ただし，論理暗号化された回路は活性化されてテストを行う必要がある．そのため，製造ベンダは IP ベンダから論理暗号化された回路を活性化するための鍵(入力鍵)を送信してもらわなければならない．製造ベンダは，初回起動時に乱数生成器を用いて，ランダムチップの公開鍵と秘密鍵を生成する．乱数生成器は最初の起動時のみしか動作しない．このとき，製造ベンダで生成されたランダムチップの秘密鍵は VLSI の中に焼き付けられる．製造ベンダは IP ベンダにランダムチップの公開鍵を送信する．IP ベンダは，公開鍵暗号方式を用いて，共通鍵をマスターの秘密鍵とランダムチップの公開鍵で暗号化し，その結果として入力鍵を生成する．IP ベンダは入力鍵を製造ベンダに送信する．製造ベンダが製造した VLSI の状態を図 2 に示す．EPIC を用いて暗号化設計された回路は活性化された状態でテストされなければならない．製造ベンダは，入力鍵を用いて回路を活性化させ，テストにパスした回路を市場に出荷する．

Evaluation of logic Encryption for IP Protection

Hidemi HASHIDATE, Toshinori HOSOKAWA and Masayoshi YOSHIMURA

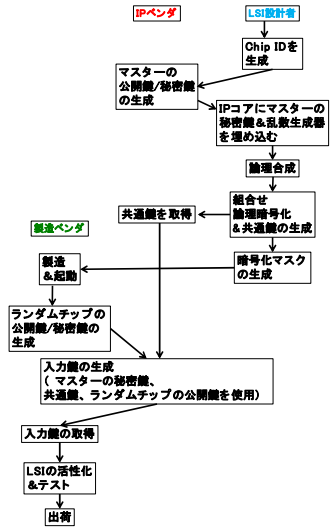

図 1. EPIC の論理暗号化フロー

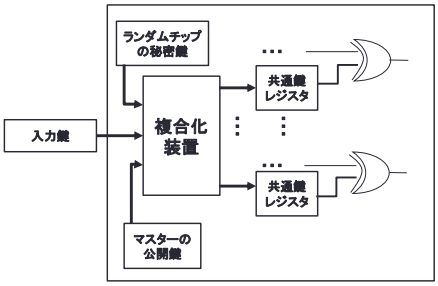

図 2. 復号化システム

3 論理暗号化を組み込んだ設計フロー

通常の設計フローに合わせて，論理合成によってレジスタ転送レベル(Register Transfer Level：RTL)からゲートレベルネットリストを生成する．組合せ論理回路はクリティカルパスに影響が及ばないように XOR ゲートや XNOR ゲートを挿入し，共通鍵レジスタと接続する(図 2)．共通鍵レジスタとは，暗号化された入力鍵を複合化したときの値を保存するレジスタである．共通鍵レジスタに正しい鍵が入力されたとき，その回路はオリジナル回路と同等の機能を有する．間違った共通鍵が入力されれば，挿入された信号線はインバータに置き換わる．論理暗号化のための XOR や XNOR が挿入される信号線はランダムに決定される．上記の設計を施すことで共通鍵レジスタは正しい鍵が入力された時のみ，元の回路と同等の機能動作を果たすことから，共通鍵は IP ベンダへ安全に送信される必要がある．

4 製造フロー

VLSI の製造とテストを行う企業は同一であると仮定する．製造されたチップは，テストされる前に活性化されなければいけない．なぜなら，活性化しなければチップは暗号化によって予期せぬ結果を出力するからである．最初の電源起動時に，ランダムチップの秘密鍵と公開鍵を生成し，ランダムチップの秘密鍵を電気的なプログラム用フューズに焼き付ける．一方，チップを活性化させるために，製造ベンダは IP ベンダにランダムチップ鍵の公開鍵を渡さなければならない．IP ベンダはマスターの秘密鍵とランダムチップの公開鍵を用いて共通鍵を暗号化し，入力鍵として工場に送らなければならない．入力鍵が盗まれたとしても，ランダムチップの公開鍵を用いて共通鍵をマスターの秘密鍵と一緒に暗号化したことは，マスターの秘密鍵に対する解読をより難しくする．回路に入力鍵を入力したとき，入力鍵は回路内にあるランダムチップの秘密鍵とマスターの公開鍵を用いて複合化される(図 2)．複合化されたものは共通鍵として生成され回路を活性化させる．その後，製造テストを行う．

5 組合せ回路の論理暗号化の鍵探索問題

図 4 に図 3 の回路の信号線w_iを論理暗号化した回路を示す．k ビット長の鍵で組合せ回路$C(\vec{x})$を暗号化するために，EPIC では k 個のゲートを用いたて暗号化する($\vec{x}$は外部入力ベクトルである)．k 個の信号線$w_i(1 \le i \le k)$を選択し鍵ビットのy_iと対応させる．選択された信号線w_i(図 3)は XOR ゲート$w'_i = w_i \oplus y_i$または XNOR$w'_i = \overline{w_i \oplus y_i}$として挿入される(図 5)．鍵ビットの$y_i$が 0 ならば$w'_i = w_i \oplus y_i$を用いることができ，それ以外ならば$w'_i = \overline{w_i \oplus y_i}$を適用できる． 本論文では，論理暗号化された組合せ回路を$C(\vec{x},\vec{y})$と表現する．全ての鍵を探索する問題を定式化すると下記のようになる．

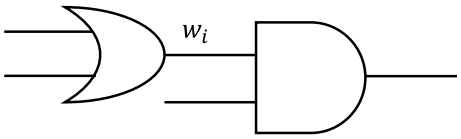

図 3. 論理回路

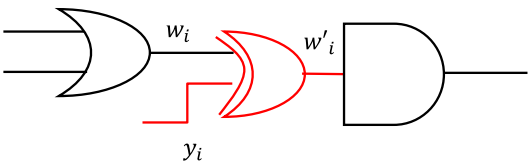

図 4. 論理暗号化回路

$$\exists \vec{y} \forall \vec{x} \;\; C(\vec{x},\vec{y}) = C(\vec{x}) \qquad (1)$$

式(1)はブール方程式であり，この式を解くことで鍵の組合せを探索できる．しかしながら，この問題は NP 困難である．現実的な時間において SAT (Satisfiability problem)を解くことで，十分な長さの鍵の組合せを探索することは困難である．もし攻撃者が製造ベンダで$C(\vec{x},\vec{y})$と$C(\vec{x})$が入手可能ならば，攻撃者が共通鍵を発見することを手助けすることになる．信頼性を説明する上で次の定義，定理を述べる．

定義 1

論理暗号化された組合せ回路$C(\vec{x},\vec{y})$の効果的な鍵の長さL($\vec{y}$)は，総当たり攻撃で予想される鍵の組合せの対数(log_2)である．

定理 1

組合せ回路 C($\vec{x},\vec{y}$)は，n 個の独立したテスト可能なモジュールごとに暗号化されている．鍵$k_j(1 \le j \le n)$はモジュール j を暗号化している．モジュール j の復号化の全ての鍵は，2^{kj}の組合せの中でG_j個ある．鍵k_jの長さL($\vec{y}$)は以下の式(2)で与えられる．

$$L(\vec{y}) \le log_2\left(\sum_{j=1}^{n}\frac{2^{k_j}}{G_j}\right) - 1 \qquad (2)$$

鍵は総当たり攻撃に耐えるための十分な長さを十分に持たなければならない．いくつかの鍵の組合せを持っていることは有益である．鍵の長さは 64 以上が推奨されている[5].

6　縮退故障シミュレーションを用いた論理暗号化挿入箇所の決定

EPIC ではランダムに論理暗号化を行う信号線を選択する.そのため, 暗号化された値が他の信号線によってマスクされてしまう可能性がある.その具体例を図 5 に示す．図 5 は信号線 a に対して論理暗号化を行った回路図である．(a,b,c,d,i)=(0,0,0,0,1)を印加した場合, 論理暗号化の影響を受けず外部出力には通常動作と同等の値 0 が出力されている．これは信号線 b によって論理暗号化の効果がマスクされているからである．その課題を解決するために，縮退故障シミュレーションを用いた論理暗号化挿入箇所決定アルゴリズムが提案されている(FLE) [6].

効率よく論理暗号化を行うために，縮退故障モデルと論理暗号化回路の関連付けを行う．縮退故障には 0 縮退故障と 1 縮退故障がある.信号線 f の 0 縮退故障モデルの具体例を図 6 に示す．(a,b,c,d)=(0,0,0,0)を印加した場合，外部出力線 h には 0/1(正常値/異常値)が出力される．通常では外部出力 h に 0 が出力されるが，信号線 f が 0 縮退故障を起こしていると仮定したとき，h は 1 を出力する．次に，図 6 の回路の信号線 f に XOR を挿入した論理暗号化回路を図 7 に示す．鍵となる信号線 i に 1 を入力する．このとき，(a,b,c,d)=(0,0,0,0)を入力した場合，外部出力は通常の回路の期待値とは違う 1 という値が出力される．これは，信号線 f が 0 縮退故障したと仮定した場合と同等の振る舞いをする．この性質を利用し，論理暗号化を行う前に故障シミュレーションを実行する. FLE で提案されている論理暗号化挿入箇所は下記の式で故障ポイントが高い箇所に挿入する．

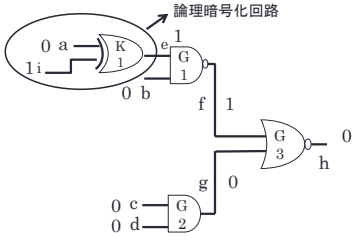

図 5．EPIC の課題点

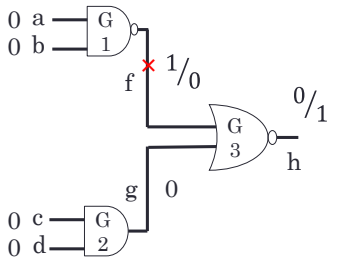

図 6．信号線 f の 0 縮退故障

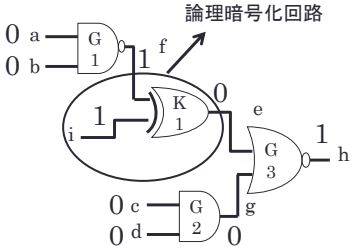

図 7．論理暗号化モデル

故障ポイント　＝（信号線 n の 0 縮退故障の検出回数×信号線 n の 0 縮退故障の検出外部出力数）＋（信号線 n の 1 縮退故障の検出回数×信号線 n の 1 縮退故障の検出外部出力数）　(3)

本論文では，各信号線の縮退故障を検出した外部出力数の総和を計算し，総和が多い信号線に対して論理暗号化を行うアルゴリズムを提案する．提案手法の論理暗号化挿入箇所は下記の式で論理暗号化ポイントが高い箇所に挿入する．

論理暗号化ポイント　＝　信号線 n の 0 縮退故障の検出外部出力数+信号線 n の 1 縮退故障の検出外部出力数　(4)

	信号線1	ポイント(1)	信号線2	ポイント(2)
提案手法	G11_stem	320	G14	176
EPIC	G6	56	G3	32

表 1．論理暗号化ポイント

回路名	提案手法(%)	EPIC[5](%)
s27_C	96.8	17.1

表 2．実験結果

また，FLE との実験結果を比較することにより，どちらが効率よく論理暗号化を行っているかを評価する．評価関数は下記の式（5）で評価する．

$$\text{評価関数} \quad = \quad \frac{1}{M\times 2^N}\times\sum_{j=1}^{M}\sum_{i=1}^{N} a_{i,j} \qquad (5)$$

7　実験結果

本章では, 6 章で提案した手法に対する評価に関する実験について述べる. 実験として, 組合せ回路に対してランダムに論理暗号化を行う信号線を決定する EPIC と，故障シミュレーションを行って論理暗号化を論理暗号化ポイントの高い箇所の信号線に決定する提案手法について比較した．対象回路は ISCAS‘89 ベンチマーク回路の s27_C(外部入力線数は 7 本，外部出力線数は 4 本)，対象故障モデルは単一縮退故障としている．故障シミュレーションは 128 個の全数テストパターンを使用した. EPIC では，論理暗号化ポイントが一番低い信号線の箇所に論理暗号化を行い, 提案手法では, 論理暗号化ポイントの高い信号線の箇所に論理暗号化を行った. また, それぞれ二つの論理暗号化回路を挿入した．表 1 に上記の実験結果を示す. ”提案手法”は故障シミュレーションを実行し，論理暗号化ポイントが高い箇所を選択，”EPIC”は故障シミュレーションを実行し，論理暗号化ポイントが低い箇所を選択していることを示している．また，”EPIC”ではクリティカルパスは論理暗号化の対象にしていない．”信号線 1”と”信号線 2”は論理暗号化した信号線名で，”ポイント(1)”と”ポイント(2)”は, それぞれ”信号線 1”と”信号線 2”の論理暗号化ポイントを示している．今回行った実験は下記の式で評価した.

$$\frac{\text{選択した論理暗号化ポイントの総和}}{\text{外部出力線数}\times 2^{\text{外部入力線数}}}\times 100 \qquad (6)$$

式(6)の”外部入力線数”は，論理暗号化した時の鍵の入力線数を含まない．表 1 に上記の実験結果を示す．”回路名”は実験対象とした回路名, ”提案手法”と”EPIC[5]”は故障シミュレーションを使用して論理暗号化を行った時の式(6)の値を示している.

実験結果より, EPIC による論理暗号化よりも故障シミュレーションを用いれば，より効率的に論理暗号化が可能と考えられる.

8　おわりに

本論文では，ランダムに論理暗号化を行う EPIC が制御地にマスクされてしまうという課題点を挙げ，その課題を解決するために，縮退故障シミュレーションに着目し，各信号線の縮退故障を検出した外部出力数の総和を計算し，総和が多い信号線に対して論理暗号化を行うアルゴリズムを提案した．今後の課題として，論理暗号化は間違った鍵を印加したときに値を反転して伝搬させる機能を持っているが，間違った鍵同士で 2 度値が反転すれば正常値に戻ってしまうという課題がある．その解決策として，論理暗号化箇所決定アルゴリズムに，論理暗号化を決定した信号線の影響を受けない箇所について論理暗号化箇所を決定すれば，より効率的に論理暗号化ができると推測する.

参考文献

[1] 木村雅秀，Phil Keys, 内田泰，″その電子部品，ホンモノですか？ ″ 日経エレクトロニクス， pp.29-50, Apr 2010.

[2] M.Yasin and S.M.Saeed, J.V.Rajendran, O.Sinanoglu, “Activation of Logic Encrypted Chips: Pre-Test or Post-Test?” Design, Automation and Test in Europe, pp.139-144 Mar 2016.

[3] W. Schneider, Jr. “Defense Science Board (DSB) study on High Performance Microchip Supply,” Office of the Under Secretary of Defense For Acquisition, Technology, and Logistics Washington Feb 2005.

[4] N.Ferguson and B. Schneier, “Practical Cryptography,” John Wiley and Sons, in 2003.

[5] J. Roy, F. Koushanfar, and I. Markov, “EPIC: Ending Piracy of Integrated Circuits,” Design, Automation and Test in Europe, pp. 1069-1074, in 2008.

[6] J.Rajendran, Y.Pino, O.Sinanoglu, and R.Karri, “Logic Encryption: A Fault Analysis Perspective,” Design, Automation Test in Europe, pp.953-958, 2012.

[7] Y.Alkabani and F. Koushanfar. Active hardware metering for intellectual property protection and security, in USENIX Security , pp.291-306 , 2007.