ISSN 2186-5647

2-7

IP コアの論理暗号化法の復号化鍵数の評価

日大生産工(院)　○橋立 英実　日大生産工　細川 利典

京都産大　吉村 正義

1. まえがき

近年の半導体微細化技術の進歩に伴って，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増大している．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．これにより VLSI 設計には人件費や設計/製造コストなどの開発コストの増加が起きている．

この課題を解決するために，VLSI の設計は，開発コスト削減のしている，外部から IP コア(Intellectual Property core)を購入する．具体的には，自社ですべての VLSI 上の機能ブロックの設計を行うのではなく，IP ベンダから IP コアを購入し，IP コアを用いて 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 IP コアの著作権侵害が懸念されている．具体例として，IP コアの無断再利用，マスクの窃盗や，IP ベンダが許可していない過剰な数の VLSI の生産などが挙げられる．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[1].

これに対し EPIC(Ending Piracy of Integrated Circuits)[2]は，VLSI を論理暗号化することにより VLSI の過剰生産を防ぐことを提案している．VLSI を機能動作させるためには，IP ベンダのみが生成することができる入力鍵が必要となる．EPIC の手法は(1)チップ ID 生成器，(2)組合せ論理暗号化，(3)公開鍵暗号の仕様に基づいている．この手法によって VLSI の過剰生産に対抗する VLSI を設計する． EPIC は，論理暗号化のオーバーヘッドによる VLSI の遅延や消費電力の増加が小さく，その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．また，プロトコル解析により，EPIC は過剰生産に対して頑強な対抗策であることが示された．

EPIC は (Exclusive OR)XOR ゲートや (Exclusive NOR)XNOR ゲートなどを回路に挿入することで論理暗号化を行っている．XOR ゲートや XNOR ゲートを挿入することで誤った鍵を印加したときに，誤った値が外部出力まで伝搬する．

しかしながら，EPIC ではランダムに信号線を選択し論理暗号化を行うので，鍵を印加しても誤った外部出力が護ることが少ない，または，ない場合がある．誤った外部出力が少ないと解析されやすいという課題を EPIC は有る．

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を行う方法が提案されている．故障が外部出力に伝搬されやすい信号線は論理暗号化の影響が受けやすい信号線である．FLE(Fault analysis Based Logic Encryption: FLE)はランダムパターン故障シミュレーションの結果から生成される故障辞書から，故障が外部出力に伝搬しやすい信号線を特定し，その信号線に対して論理暗号化を行っている．FLE では暗号化した VLSI にランダムパターンを入力した場合に誤った外部出力と正しい外部出力のハミング距離が評価尺度として提案されている．ランダムパターン集合に対してハミング距離が平均して 50%であるなら攻撃者から解析されにくいとされている．なぜなら，ランダムパターンを入力したときに外部出力結果が期待値と比較して，ハミング距離が低くなることは，ほとんどの鍵に対して正しい鍵が入力されている可能性が高いからである．反対に，ハミング距離が 100%に近づくほど誤った鍵を入力していることになり，その出力の反転した値は，ほぼ期待値に近づくと考えられるからである．したがって，ハミング距離が低い値を参考にして解析を行えば，鍵が特定できる．それゆえ，出力値を反転してもハミング距離が変わらない 50%が良いとされている．しかしながら，この考えは EPIC の暗号化設計に対して有効ではない．EPIC は IP コアに復号化回路を内蔵する設計になっており，入力した値は直接論理暗号化に到達せず，その復号化回路を通り論理暗号化回路に到達する仕組みになっている．1 つのテストパタンを入力したときに得られるハミング距離から，少しずつ 0%に近づけていくことは困難である．それゆえ，新たに論理暗号化の強度を示す複合化鍵数を指標として提案する．この評価尺度はランダムパターン攻撃を想定している．復号化鍵数が多ければランダムパターンで鍵が特定されてしまうが，復号化鍵数が少なければ特定されにくくなる．

第 2 章では IP コア，鍵の種類の定義を行い，また，強度の指標として用いられるハミング距離による指標と復号鍵数による指標の定義を行う．第 3 章では入力

An Evaluation for the Number of Decoding key for Logic Encryption Methods for IP Core

Hidemi HASHIDATE, Toshinori HOSOKAWA, Masayoshi YOSHIMURA

鍵を生成するための論理暗号化の鍵生成フローの説明，論理暗号化を組込んだ設計/製造フローの説明と入力鍵を印加したときの復号化フローの流れを説明する．第 4 章ではハミング距離における論理暗号化評価尺度と手法と第 5 章で復号化鍵数を用いた論理暗号化評価尺度と評価尺度を計算するための手法の説明を行う．第 6 章では評価回路と評価基準を述べ，実験結果を示し，結果に対する考察/解析を述べる．第 7 章では結論として提案内容と得られた結果のまとめを述べたあと，今後の課題を記す．

2. 論理暗号化

論理暗号化とは，論理回路を暗号化することであり，暗号化とは正しい鍵を入力しない限り，論理回路が機能動作を行わないようにする技術である．論理暗号化は論理ゲートを用いて実現される．論理暗号化は XOR ゲートや XNOR ゲートなどを回路に追加することによって，その機能を隠すことができる．図 2.3-1 と表 2.3-1 に組合せ回路とその真理値表をそれぞれ示す．また，図 2.3-2 に図 2.3-1 の回路の信号線 c に対して論理暗号化を行った暗号化回路を示す．表 2.3-2，表 2.3-3 に図 2.3-2 の回路図の真理値表を示す．次に，暗号化回路について，それぞれの役割を示す．図 2.3-2 にある XOR ゲートが「錠」となり，信号線 x が「鍵」となる．この二つが暗号化部分となる．先に，正しい鍵の例を示すと，信号線 x の正しい鍵は’0’であり，誤った鍵は’1’となる．次に鍵が鍵として機能していることを示す．表 2.3-2 と表 2.3-3 から信号線 x に正しい鍵’0’を印加しても，外部出力に影響がないことがわかる．また，誤った鍵’1’は外部出力において値が反転していることがわかる．鍵の影響が外部出力まで伝搬している入力を値で示す．XNOR ゲートは鍵の値が反転するだけで，錠としての役割は XOR ゲートと同じである．このことから，XOR ゲートや XNOR ゲートが論理暗号化に適用できる．

FLE では暗号化の強度として暗号化回路にランダムパターン集合を入力したときの外部出力値と期待値を比較してそのハミング距離の値でその強度を測ることを提案している．FLE ではハミング距離が 50%に近づくほど強度が強いことが示されている．1 つのランダムパターンに対して 50%を保証しているわけではなく，パターン集合の平均が 50%に近ければいいと考えられている．しかしながら，ハミング距離が 50%より大きく離れた値であるランダムパターンがパターン集合にあった場合には，暗号化した信号線が容易に解析されてしまうことが示されている．本論文では，復号鍵数による指標を提案する．復号化鍵数が少なければ，暗号化強度が高いと考えられる．なぜなら，攻撃者が探索しなければならない鍵空間が増えるからである．

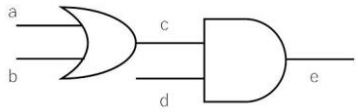

図 2.3-1 通常回路

表 2.3-1 通常回路の真理値表

a	b	d	e
0	0	0	0
0	0	1	0
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	1
1	1	0	0
1	1	1	1

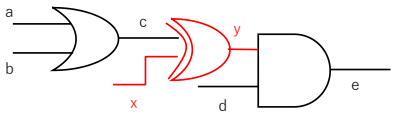

図 2.3-2 暗号化回路

表 2.3-2 暗号化回路の真理値表(正しい鍵)

a	b	d	x	e
0	0	0	0	0
0	0	1	0	0
0	1	0	0	0
0	1	1	0	1
1	0	0	0	0
1	0	1	0	1
1	1	0	0	0
1	1	1	0	1

表 2.3-3 暗号化回路の真理値表(誤った鍵)

a	b	d	x	e
0	0	0	1	0
0	0	1	1	1
0	1	0	1	0
0	1	1	1	0
1	0	0	1	0
1	0	1	1	0
1	1	0	1	0
1	1	1	1	0

2.4 論理暗号化と公開鍵暗号を用いた過剰生産防御法

本節では，文献[2]で提案されている論理暗号化と公開鍵暗号を用いた過剰生産に対する防御法を述べる．図 2.4-1 に IP ベンダが提供する論理

暗号化 IP コアを含んだ設計データを示す. K は論理暗号化回路の復号鍵を示し，CK とは復号鍵 K をチップ ID の公開鍵で暗号化した鍵である. PUF によって鍵生成部が生成され，チップ ID の公開鍵と秘密鍵を外部出力する.

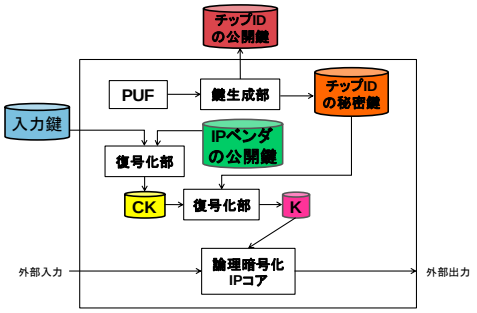

図 2.4-1 公開鍵暗号を用いた暗号化回路

3. 論理暗号化の設計/製造フローと鍵生成フロー

本章では，論理暗号化の鍵生成フロー，文献[2]の設計/製造フローについて説明する. 図 3.1 に論理暗号化の鍵生成フローの図を示す. 図 3.1 では、まず始めに IP ベンダが論理暗号化された回路を復号化する IP コアをチップ鍵の公開鍵で暗号化する. 暗号化された IP コアの復号化鍵 K'をマスター鍵の秘密鍵で暗号化する. これが最終的に回路に印加する入力鍵となる.

図 3.2 に文献[2]の設計/製造フローの図を示す. IP ベンダは IP コアを論理暗号化する. そのとき，IP コアの復号化鍵 K を生成する. また PUF と鍵生成部，マスター鍵の公開鍵，二つの復号化部を IP コアに追加する. VLSI 設計者は IP ベンダが論理暗号化した回路を受け取り，マスクを生成する. 生成したチップは鍵生成部を用いてチップ ID を生成する. そのうち，秘密鍵は回路に記憶され，公開鍵は外部に出力する. 工場は IP ベンダにチップ鍵の公開鍵を送信する. 工場は製造テストを行い製造した回路を出荷する.

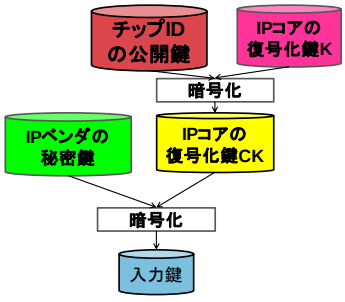

図 3.1 入力鍵生成フロー

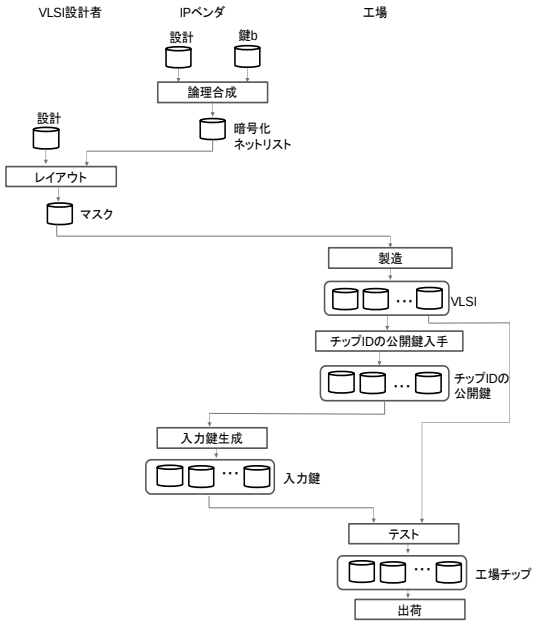

図 3.2 設計/製造フロー

4. ハミング距離を用いた論理暗号化評価尺度

本章では，文献[3]で提案されているハミング距離による論理暗号化評価尺度について説明する. パターンN_{Pt}，外部出力ビット数N_{Po}，ランダムパターン c を印加した時の暗号化回路の外部出力値と通常回路の期待値と異なる外部出力の数をD_iとすると，文献[2]で提案されている暗号化評価尺度E_{Po}は下記の式(1)で表される.

$$E_{Po} = \frac{1}{N_{Po} \times N_{Pt}} \sum_i^{N_{pt}} D_i \qquad (1)$$

この式(1)は，暗号化回路に対してパターンを印加した時にどれくらいの確率で誤った値が外部出力されるかを表している. 式(1)は 50%に近づくほど暗号化強度が高いことが示されている[3].

5. 復号化鍵数を用いた論理暗号化評価尺度

本章では，本論文で提案する復号化鍵数を用いた論理暗号化評価尺度を提案する. 鍵ビット数を n，通常回路と全く同じ動作をするときの鍵(復号化鍵)の数をD_nとし，D_nを論理暗号化評価尺度とする.

Dn の値が小さくなると暗号化強度が強固になる. その理由としては，鍵の個数が小さくなると，ランダムに鍵を選択したときにその鍵が復号鍵である確率が低くなるからである. 図 5.1 に論理シミュレーションによる鍵候補探索の入出力設

計図を示す．はじめに、鍵が n 個の論理暗号化回路の鍵候補を探索する．探索空間する鍵候補数は 2^n 個あり，その鍵候補に対して論理シミュレーションを行い，その外部出力と正しい外部出力応答との比較により，復号化鍵候補として外部出力が一致した鍵候補の集合を求める．

図 5.2 に等価性検証を用いた鍵の特定用回路を示す．復号化鍵候補を K1 に制約と OR ゲートの出力を 1 に設定する制約値を与え，その制約を満たす，すなわち外部出力が一致しない外部入力 PI が存在するか否かを判定する．この制約を満足する場合，K1 に設定された鍵は誤った鍵として判定され，制約を満足しない場合は，K1 に設定された鍵は正しい鍵として判定される．図 5.1 に鍵候補探索のフローチャートを示す.これは，n 個の論理暗号化ゲートを入れた回路に対して，論理暗号化回路が元の回路と一致するかをシミュレーションするためのフローチャートである.ランダムパターンを 5 個入力したときに，論理暗号化回路と元の正しい回路の出力結果を比較し，5 個すべての出力結果が正しいとき，鍵候補として出力される.図 5.2 に鍵特定モデルを示す．これは，鍵候補を制約としたときに，元の回路と等価であるかどうかを判定するモデルである．この鍵特定モデルを CNF(Conjunctive Normal Form)式で表し，SAT(Satisfiability problem) で解くことで等価性検証を行っている．

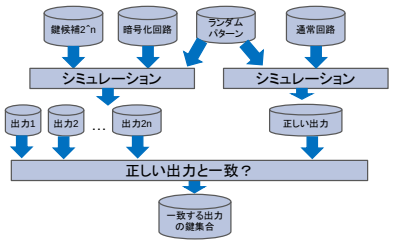

図 5.1 鍵候補探索

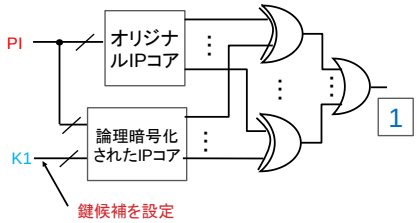

図 5.2 鍵特定モデル

6. 実験結果

本章では，ISCAS’85 ベンチマーク回路において，EPIC[2]と FLE[3]の両方の暗号化を行い，ハミング距離に基づく論理暗号化評価尺度と復号化鍵数に基づく論理暗号化評価尺度とを用いて評価を行った．論理暗号化する鍵ビット数はそれぞれ 26 ビットで論理暗号化を行った.表 6.1 に EPIC の実験結果,表 6.2 に FLE の実験結果を示す．EPIC の手法で論理暗号化を行った回路では,復号化鍵数が最大 2 個であるのに対して，FLE の手法で論理暗号化を行った回路では，4096 個である．この原因は，故障辞書を基に論理暗号化を行っている FLE では,すでに論理暗号化された信号線の近傍の信号線に論理暗号化されやすい傾向があるためである．それゆえ，鍵の影響が互いに干渉しあいマスクしていると考えられる．

表 6.1 EPIC の復号化鍵数とハミング距離

回路名	復号化鍵候補	復号化鍵数	EVA1
c880	32	2	19.23
c1355	432	1	10.77
c1908	128	2	12.43
c2670	512	1	2.97
c3540	4096	1	20.97
c5315	256	1	3.89
c6288	8	1	30.10
c7552	448	1	7.22

表 6.2 FLE の復号化鍵数とハミング距離

回路名	復号化鍵候補	復号化鍵数	EVA1
c880	2	1	45.13
c1355	262144	4096	25.22
c1908	32	32	41.35
c2670	4	1	10.88
c3540	2	1	30.52
c5315	1	1	9.23
c6288	2	1	35.03
c7552	1	1	16.97

7. 結論

本論文では，論理暗号化のセキュリティの新しい評価尺度として，復号化鍵数をセキュリティの評価尺度として提案した. ISCAS’85 ベンチマーク回路を用いて，故障解析に基づく論理暗号化法を評価した結果，c1355 と c1908 の回路において，復号化鍵数はそれぞれ 4096 個と 32 個であることがわかった．

参考文献

[1] W. Schneider, F. Chairman, “Defense Science Koard Task Force On High Performance Microchip Supply.” Office of the Under Secretary of Defense For Acquistion, Technology, and Logistics, in Washington, in 2005.

[2] J. Roy, F. Koushanfar, and I. Markov, “EPIC: Ending Piracy of Integrated Ciruits.” Design, Automation and Test in Europe in 2008.

[3] J. Rajendran, Y. Pino and O.Sinanoglu, “Logic Encryption: A Fault Analysis Perspective” Design, Automation and Test in 2012.