

RTLにおけるコントローラの論理暗号化手法

吉村 正義^{1,a)} 橋立 英実² 辻川 敦也² 細川 利典²

概要: 近年 IP コアを用いた VLSI 設計が盛んであるが、IP コアの複製や過剰生産といった著作権侵害が問題となっている。IP コアを用いた VLSI の過剰生産を防ぐ手法の 1 つの方法として、論理暗号化手法が提案されている。論理暗号化手法とは IP コアである論理回路に対して鍵入力を追加し、鍵入力値が特定の入力値が印加されたときのみ、正しく機能動作し外部出力応答を行う設計手法である。しかしながら、正しい鍵入力値を容易に特定できる SAT 攻撃が近年提案された。一方、SAT 攻撃に対して耐性のある論理暗号化手法がいくつか提案されている。この SAT 攻撃に耐性のある論理暗号化手法は適用された回路の構造的特徴を利用した攻撃などの脆弱性が指摘されている。そこで本論文では、SAT 攻撃に耐性があり、脆弱性となる構造的特徴を持たない論理暗号化手法を提案する。提案した論理暗号化手法は、RTL の設計段階のコントローラに適用する。SAT 攻撃への耐性は、既存の SAT 攻撃への耐性のある論理暗号化手法を応用し、コントローラ拡大を用いることで、鍵入力ビット数を変更できるようにする。MCNC ベンチマーク回路を用いて、提案する論理暗号化法を適用し、回路面積を評価した。

A Logic Encryption Method for Contoroller on RTL

MASAYOSHI YOSHIMUA^{1,a)} HIDEMI HASHIDATE² ATSUYA TSUJIKAWA² TOSHINORI HOSOKAWA²

Abstract: In recent years, IP cores has been used on VLSI designs. However, there are piracies of IP core such as duplication and overproduction. Logic encryption method is proposed as one of the methods to prevent overproduction of VLSI with IP cores. The logic encryption method is a design method that adds key inputs to a logic circuit, and that circuit has functions correctly output only when a correct key input value is applied. However, SAT attack method has been proposed. SAT attack method can easily identify the correct key input value. On the other hand, several logic encryption methods resistant to SAT attacks have been proposed. Those logic encryption methods have vulnerable such as an attack that utilizes the features of circuit structure of the applied circuits. In this paper, we propose a logic encryption method that is resistant to SAT attack and has no feature of circuit structure that makes it vulnerable. The proposed method is applied to the controller on the RTL design. We applied the proposed logic encryption method using the MCNC benchmark circuit and evaluated the number of key bits and the circuit area.

1. はじめに

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) の高機能化や高集積化が進んでおり、VLSI の設計規模が増大し、VLSI 設計における人件費や設計/製造などのコストが増加している。この課題を解決するために、一部の機能を実装した

回路である IP コア (Intellectual Property core) を用いる設計の水平分業が広く取り入れられている。IP ベンダが主に提供する IP コアは、RTL (Resister Transfer Level) 回路記述 (Soft core)、論理回路記述 (Firm core)、レイアウト回路記述 (Hard core) の 3 種類のレベルがある。IP コアを使用することにより、人件費や設計期間の削減を図る。

しかしながら、IP コアに対する著作権侵害の恐れが指摘されている。著作権侵害の例として、IP コアの不正な再利用、マスクの窃盗や、IP ベンダが許可した数を越える過剰な VLSI の生産などがある [1]。LSI の過剰生産防御法の 1 つとして、論理暗号化を用いた EPIC (Ending Piracy

¹ 京都産業大学
Kyoto Sangyo University, Kita, Kyoto 603-8555, Japan

² 日本大学
Nihon University, Narashino, Chiba 275-7575, Japan

^{a)} yoshimura.masayoshi@cc.kyoto-su.ac.jp

of Integrated Circuits)[2] という仕組みが提案されている。EPIC を適用された VLSI を正常に機能動作させるためには、IP ベンダのみが生成できる鍵入力が必要となる。EPIC は、(1) チップ固有の ID 生成、(2) IP の論理暗号化、(3) IP ベンダによる公開鍵暗号方式によるチップごとの鍵入力生成で構成されている。EPIC において、IP コアの論理暗号化は論理ゲートの追加によって行われる。このため、設計フローやテスト方式の大幅な変更は必要がない。

これに対して、様々な論理暗号化手法に対して、鍵入力を特定できる SAT 攻撃 [3] が提案された。SAT 攻撃は、効率良く鍵探索空間を狭める外部入力値を繰り返し求めながら、鍵入力を特定する手法である。SAT 攻撃は 2 つのフェーズに分かれる。1 つ目のフェーズは、異なる鍵入力に対して、外部出力値が誤る外部入力値を求めるフェーズである。2 つ目のフェーズは、1 つ目のフェーズで求めた外部入力値を用いて、正常な外部出力値を求め、鍵入力の新たな制約条件とするフェーズである。この 2 つのフェーズを繰り返し行うことで、鍵入力の候補を絞り込む。EPIC や従来の論理暗号化手法は、ある外部入力値が誤った外部出力値を出力する鍵入力は一般に複数存在している。1 度の 2 つのフェーズの繰り返しによって、これらの複数の鍵入力を正常な鍵入力候補から除去することができる。

この SAT 攻撃に対する防御手法 [4-6] がいくつか提案されている。文献 [4-6] は、2 つ目のフェーズでの効率を落とすことを狙っている。ある外部入力値が誤った外部出力値を出力する鍵入力を 1 通りとしている。1 度の 2 つのフェーズの繰り返しによって、一つのみ鍵入力を正常な鍵入力候補から除去されるため、SAT 攻撃の探索効率が著しく低下する。一方、文献 [4-6] は論理暗号化手法は、ある外部入力値が誤った外部出力値を出力する鍵入力を 1 通りとする論理構造であり、巨大なデコーダ回路となっている。これらの構造的特徴を特定され、鍵入力を特定される恐れがある。

そこで本論文では、SAT 攻撃の 2 つ目のフェーズの効率を落としつつ、構造的特徴を持たない論理暗号化法を提案する。文献 [4,5] はどちらもゲートレベルでの論理暗号化手法である。本論文では RTL 記述のコントローラ部を変更することで、論理暗号化手法を行う。RTL 記述のコントローラは、論理合成によって、デコーダ回路となりやすい。そこで、RTL 記述のコントローラをに対して論理暗号化を行い、論理合成を行う。論理合成されたゲートレベルの回路は、元々のコントローラによるデコーダ構造と論理暗号化によるデコーダ構造の両方をもつ。よって、いずれの構造的特徴がわかりにくい論理暗号化された回路となる。

2. 過剰生産の防止手法

本章では、論理暗号化による VLSI の過剰生産の防止方法 [2] について説明する。

論理暗号化された IP コアをもちいて、複数のチップを生成する。しかし、同一の設計データを用いると論理暗号化された回路を正常動作させる鍵入力はすべて共通のものとなる。そこで、すべてのチップに対して共通の鍵入力をチップ固有の ID を鍵として暗号化する。これによって、チップ固有の ID が異なる場合、全てのチップごとに異なる正常動作させる入力となる。

EPIC において、公開鍵暗号方式によって、鍵入力を暗号化している。チップ固有の ID を用いることで、あるチップに対する正常動作させる入力が漏洩しても、その他のチップでは正常動作しない。よって、チップ固有の ID ごとにあるチップに対する正常動作させる入力を生成する必要がある。この仕組みによって、過剰生産を防ぐことができる。

3. SAT 攻撃とその対策手法

3.1 SAT 攻撃

本章では、SAT 攻撃について説明する [3]。SAT 攻撃の入力は、論理暗号化済みのゲートレベルのネットリスト C と、正常な鍵入力で活性化されたチップ V の 2 つである。ネットリスト C は IP ベンダから提供されたネットリストである。チップ V の鍵入力は耐タンパ性のあるメモリに格納されており、外部から鍵入力は特定できないものとする。またチップ V に対して、外部入力値 I を入力することによって、正常な外部出力 O を得ることができる。

SAT 攻撃アルゴリズムについて説明する。入力は C と V である。出力は正常な鍵入力 K_c である。初めに、カウンタ i を 1 に初期化する。次に、論理暗号化回路された回路を 2 つ用意し、外部入力 X を共通化した CNF 式 $F_i = C(X, K_1, Y_1) \wedge C(X, K_2, Y_2)$ を作成する。 F_i に、2 つの回路の外部出力値 Y_1, Y_2 が異なる外部入力値 X と鍵入力 X_1, X_2 という条件を加え、SAT ソルバを用いて、 X, K_1, K_2, Y_1, Y_2 を求める。もし求められた場合、その外部入力値 X を X_i^d として保存する。次に、 V に X_i^d を入力し、その外部出力値 Y_i^d を得る。取得した X_i^d と Y_i^d に基づいた制約式 $C(X_i^d, K_1, Y_i^d) \wedge C(X_i^d, K_2, Y_i^d)$ を F_i に追加する。 i を 1 加算し、SAT ソルバで F_i を適用する。これを SAT ソルバで解が得られなくなるまで繰り返す。SAT ソルバで解が得られない場合は、 F_i のみを SAT ソルバに適用し、正常な鍵入力 K_c を得る。

SAT 攻撃は、識別入力と呼ばれる X_i^d を繰り返し求め、誤った鍵入力の等価クラスを鍵候補から削除することによって、正常な鍵入力を求める。よって、SAT 攻撃に耐性のある論理暗号化手法は、識別入力を求める時間を増加さ

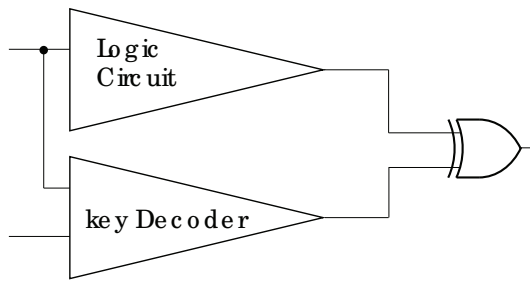


図 1 SAT 攻撃への対策手法

せるか、一つの識別入力により削除される鍵入力を削減することに基づいている。

3.2 SAT 攻撃への対策手法

本節では、SAT 攻撃への耐性がある論理暗号化手法を説明する。文献 [4]-[6] の論理暗号化手法は、一つの識別入力により削除される鍵入力を削減することに基づいている。ある外部入力値に対して、誤った外部出力値となる誤った鍵入力を一つにしている。これによって、SAT 攻撃の繰り返し回数を増加させ、SAT 攻撃への耐性を高めている。

文献 [4,5] では、外部入力値と鍵入力値を入力とし、誤った外部出力を反転させるか否かを示す信号を出力するデコーダ回路を追加する。図 1 に概要を示す。このデコーダ回路によって、どの外部入力値と鍵入力値が入力されると、外部出力値が誤るか否かを制御する。このデコーダはある外部入力値に対して、誤った外部出力値となる誤った鍵入力を一つにするよう構成することで、SAT 攻撃への耐性を高める。

このデコーダの構造は SAT 攻撃への耐性を高める一方で、構造的な構造に対する攻撃への脆弱性を有している。外部出力値が誤っている時における信号線の 0 である確率と 1 である確率を求めることで、外部出力値が誤るか否かを制御する Key Decoder の出力信号線を特定することができる。そしてこのデコーダ回路を解析することで、どの鍵入力の時に外部出力値が反転するか否かを特定することができる。

この構造的な欠点に対して、文献 [6] では、デコーダ回路を $X = K$ であるかを判定する回路とし、暗号化前の論理回路の出力を正しい鍵入力と等しい外部入力値が入力されたときに出力が反転している回路に変更する TT-Lock という論理暗号化手法を提案している。この TT-Lock の回路構成を図 2 に示す。

図 2 の Modified Logic Circuit(以下 MLC) は、暗号化前の論理回路に対して、外部入力値 $X = K_c$ である時のみ出力が誤るよう変更されている。これにより、デコーダ部を特定および解析されても、正しい鍵入力を特定できない。MLC 部は特定可能であるが、MLC がどの外部入力値に対して、出力が誤るよう設計変更されたのかを特定する必要

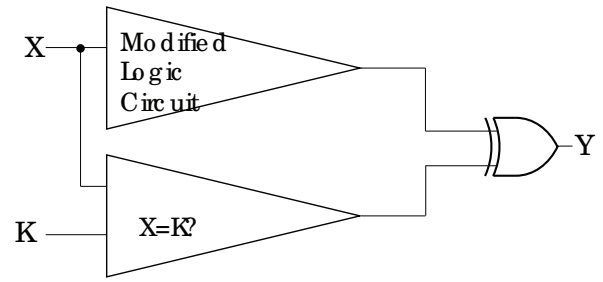


図 2 SAT 攻撃への対策手法

がある。

TT-Lock では、MLC をどのように生成するかが課題である。TT-Lock は暗号化前の論理回路に $X = K_c$ である時のみ出力が誤るよう変更する回路を追加している。この回路 $X = K_c?$ 判定部を特定されると、正しい鍵入力 K_c を特定される。文献 [6] では、再論理合成を行うことで、 $X = K_c?$ 判定部を特定されにくくしている。

4. 提案手法

本節では SAT 攻撃と構造的特徴に基づく攻撃手法に耐性のある論理暗号化手法を提案する。提案手法は、文献 [4-6] と同様に、誤った外部出力値となる誤った鍵入力を一つとすることで SAT 攻撃への耐性を高める。一方、回路構造に基づく攻撃への耐性は、TT-Lock[6] を 2 つの手法で改良することで耐性を高める。具体的には、(1)RTL における TT-Lock における別の MLC 部の追加と、(2) コントローラ拡大による鍵入力数の増加である。

まず RTL における TT-Lock における MLC 部の追加について述べる。

本論文の対象とする RTL 回路はコントローラ部とデータパス部から構成されており、データパス部とコントローラ部は互いに信号線で接続している。コントローラ部からデータパス部への信号線はコントロール信号であり、データパスからコントローラへの信号線は状態信号である。コントローラ部は現状態と外部入力値に基づいて、次状態とコントロール信号を生成する。

論理暗号化される前のコントローラ部の入力、現状態と外部入力値のペアである。現状態と外部入力のペアに対して、次状態とコントロール信号となる状態遷移の記述がされていたとする。このコントローラ部の入力に鍵入力を追加し、論理暗号化を行う。

まず、コントローラ部の入力ごとに異なる鍵入力を割り当てる。ここでは、コントローラ部の現状態と外部入力値の一部分もしくは全部を割り当てられた鍵入力として説明を行う。次に、現状態と外部入力値のペアに対して、割り当てられた鍵入力と一致しているかを判定する。もし割り当てられた鍵入力であるならば、論理暗号化前と異なる次状態とコントロール信号を出力する。もし割り当てられた

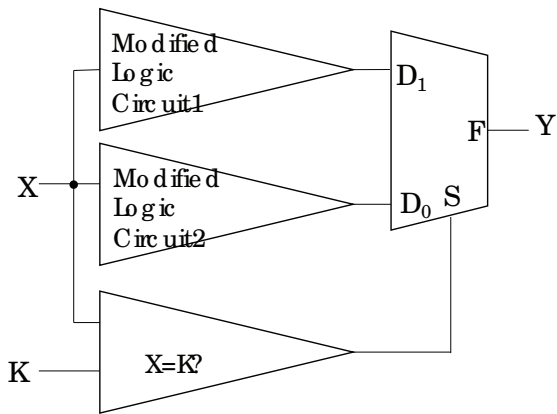


図 3 提案手法の論理構造

鍵入力でないならば、論理暗号化前と同じ次状態とコントロール信号を出力する。ただし、割り当てられた鍵入力が正しい鍵入力の場合のみ、正しい鍵入力に対しては、論理暗号化前と同じ次状態とコントロール信号を出力し、正しい鍵入力でない場合、論理暗号化前と異なる次状態とコントロール信号を出力する。

このように RTL においてコントローラ部の記述を変更することで、すべての状態遷移の記述中に、現状態と外部入力値のペアと鍵入力値との比較部があり、一致した場合の出力と異なる場合の出力部がある。この論理構造を図 3 に示す。図 3 では、一致した場合の出力を Modified Logic Circuit 1(MLC1) とし、一致しなかった場合の出力を Modified Logic Circuit 2(MLC2) としている。

次にコントローラ拡大による鍵入力数の増加手法について述べる。SAT 攻撃への耐性を高めるために、鍵入力はコントローラの入力ごとに割り当てられる。つまり、コントローラの入力数が鍵入力数の上限となる。鍵入力数は、SAT 攻撃をはじめとする攻撃への耐性の指標の一つである。論理暗号化する設計者が必要とする耐性に基づいて、鍵入力数を決定できるべきである。そこで本論文では、コントローラ拡大を用いて状態数を増加させることで、コントローラの入力数および鍵入力数を増加させる。本論文で用いるコントローラ拡大は、拡大前後の入力と出力は同一であり、内部の状態のみ異なり、コントローラ拡大前後で順序回路として等価な回路である。必要な鍵入力数は指数的に増えるため、鍵入力数の bit 数に応じてスケラブルにコントローラを変更できる必要がある。またリセット状態からの到達不能状態は鍵入力特定に利用できるため、リセット状態からの到達不能状態をなくす。

これらの要求を満たすため、コントローラ拡大を次のような手順で実施した。(1) 個々の状態ではなくコントローラ全体を複製し、状態数を増加させる。(2) 複製したコントローラごとに固有のグループ ID をつける。(3) 元のコントローラから定義済みの状態と外部入力のペアを一つ選

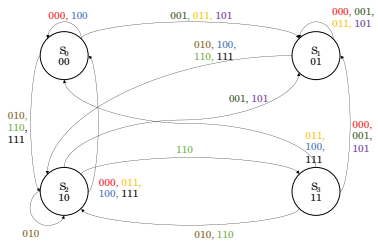


図 4 コントローラの状態遷移図

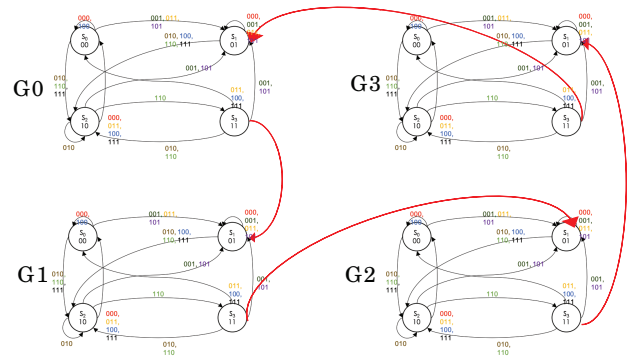


図 5 コントローラ拡大後の状態遷移図

択する。(4) (3) で選択された状態と外部入力のペアに対する状態遷移先を、グループ ID が次のグループの状態遷移先に変更する。ただし、グループ ID が最大の場合、次のグループが存在しないため、最小のグループ ID の状態遷移先に変更する。

このコントローラ拡大手法を図 4 に示すコントローラの状態遷移図を例にとって、説明する。このコントローラは外部入力ビット数が 3、状態数が 4 であり、状態のビット数の最小は 2 である。このコントローラに対して、提案する論理暗号化手法を鍵入力の bit 数を 7 で適用することを考える。元々の外部入力ビット数が 3、状態のビット数は 2 であるため、状態の bit 数を 2 増やす必要がある。状態の bit 数を 2 増やすため、コントローラを $4 (= 2^2)$ 個コピーする。4 つのコントローラにそれぞれグループ IDG0, G1, G2, G3 をつける。次に元のコントローラから定義済みの状態と外部入力のペアを一つ選択する。今回は、状態 S_3 かつ外部入力値 000 の時に次状態が S_1 である状態を選択したとする。選択された状態遷移を次のグループの状態となるように変更する。グループ G0 の状態 S_3 かつ外部入力値 000 の時に次状態をグループ G1 の S_1 となるように変更する。これをすべてのグループに対して次状態を変更する。これによってコントローラ拡大された状態遷移図を図 5 に示す。図 5 は、状態数が 16 になっており、すべての状態が到達可能状態となっている。

5. 実験結果

本論文ではコントローラのベンチマーク回路である MCNC ベンチマーク回路の一部の回路と自作の 32bit デー

表 1 実験対象回路

Circuits	#In	#Out	#States	#bits
dk15	3	5	4	2
beecount	3	5	7	3

タパスを用いて鍵入力の bit 数と論理暗号化による回路面積について評価実験を行った。提案する論理暗号化手法は C++言語で実装した。論理合成は synpsys 社の Design-Compiler を用いた。

評価対象のコントローラ回路は、dk15, beecount の 2 つの RTL 回路である。表 1 に評価対象の回路のデータを示す。「#In」はコントローラの外部入力数を、「#Out」は外部出力数を、「#States」は状態数を、「#bits」は状態の bit 数をそれぞれ示す。

データパス回路は bit 幅が 32bit で 5 入力、1 出力であり、内部に 3 つの比較器と、1 つの加算器、減算器、および乗算器を含んでいる。このデータパス回路はコントローラの種類や鍵入力ビット数に依存せず共通のものを用いている。

実験では、RTL のネットリストに対して、鍵入力ビット数を変化させた。実験結果を表 2 に示す。「#keybits」は暗号化時の鍵入力のビット数を、area は論理合成後の面積を、「org」は暗号化していないコントローラとデータパスの回路を、「area」は論理合成後の面積を、「ratio」は暗号化前と暗号化後の面積比 (%) を示す。また dk15 の鍵入力ビット数 5, beecount の鍵入力ビット数 6 の実験結果はコントローラ拡大を用いていない。また dk15 の鍵入力ビット数 6 以上, beecount の鍵入力ビット数 7 以上の実験結果はコントローラ拡大を適用した。

表 2 は鍵入力の bit 数が増加するにつれ、面積が増加していることがわかる。一方、コントローラ拡大がない場合は、dk15 で 2%, beecount で 4%と面積の増加割合は小さかった。コントローラ拡大をした場合、特に鍵入力の bit 数 16 の場合、dk15 で約 50 倍、beecount で約 40 倍と大幅に増加した。また鍵入力ビット数が増加すると、鍵の入力ビット数が 1 増加するごとに、面積が約 2 倍に増加した。これはデータパスの面積は鍵入力ビット数によって変化しないが、コントローラ部は鍵入力ビット数によって変化するためである。鍵入力ビット数が 12 以上の場合は、コントローラの面積が支配的になっていることがわかる。

6. おわりに

本論文では、IP コアを用いた VLSI の過剰生産を防ぐ論理暗号化手法を提案した。提案手法は、SAT 攻撃に耐性があり、脆弱性となる構造的特徴を持たない論理暗号化手法である。RTL の設計段階のコントローラに適用し、コントローラの状態遷移記述を鍵入力によって次状態を変化させることで SAT 攻撃に耐性があり、構造的特徴を持たない

表 2 鍵の bit 数と論理合成後の面積

#keybits	dk15		beecount	
	area	ratio	area	ratio
org	10,175	100	10,104	100
5	10,384	102	—	—
6	10,646	105	10,462	104
8	11,625	114	11,638	115
10	14,622	144	15,161	150
12	37,403	368	33,360	330
14	140,642	1382	106,773	1057
16	518,212	5093	398,500	3944

論理暗号化である。またコントローラ拡大により鍵入力のビット数を制御することも示した。提案手法を MCNC ベンチマーク回路に適用した。鍵入力ビット数と回路面積の関係を調べた。鍵入力ビット数が小さいうちは面積の増加率は低かった。一方、鍵入力ビット数が増加するにつれて、回路面積が指数的に増大した。

今後の課題は、鍵入力ビット数が増加に伴う回路面積増加率を抑制することと、SAT 攻撃や回路の構造的特徴を利用した攻撃手法に対する耐性評価である。

謝辞 本研究の一部は日本学術振興会科学技術研究補助金基盤 (C)(課題番号 18K11219) の研究助成による。

参考文献

- [1] W. Schneider, F. Chairman, “Defense Science Board Task Force On High Performance Microchip Supply,” 2005,
- [2] J. Roy, F. Koushanfar, and I. Markov, “Ending Piracy of Integrated Circuits,” Computer, vol. 43, no. 10, pp30-38, 2010.
- [3] P. Subramanyan, S. Ray, and S. Malik, “Evaluating the Security of Logic Encryption Algorithms,” in Proc. IEEE International Symposium on Hardware Oriented Security and Trust, pp.137-143, 2015.
- [4] M. Yasin, B. Mazumdar, J. Rajendran, o. Sinanoglu, “SARLock: SAT Attack Resistant Logic Locking,” in Proc. IEEE International Symposium on Hardware Oriented Security and Trust, pp236-241, 2016.
- [5] Y. Xie, A. Srivastava, “Anti-SAT: Mitigating SAT Attack on Logic Locking,” IEEE Trans. Comput. Aided Design Integr. Circuits Syst (Early Access). 2018.
- [6] M. Yasin, A. Sengupta, B. C. Schafer, Y. Makris, O. Sinanoglu, and J. V. Rajendran. “What to lock?: Functional and parametric locking,” In Proceedings of the on Great Lakes Symposium on VLSI 2017, 2017.