様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

令和　３ 年　 ８ 月 １８ 日現在

機関番号：１７１０２
研究種目：基盤研究(C)（一般）
研究期間：2018～2020
課題番号：１８Ｋ１１２１９

研究課題名（和文）論理IPの盗用を防ぐ堅牢な論理暗号化アルゴリズムの研究

研究課題名（英文）Developing robust algorithms for logic encryption protecting against piracy of logic IP

研究代表者
松永　裕介（Matsunaga, Yusuke）

九州大学・システム情報科学研究院・准教授

研究者番号：００３３６０５９

交付決定額（研究期間全体）：（直接経費）　　3,400,000円

研究成果の概要（和文）：LSIの設計図である論理IPを盗用や剽窃から守る手法である「論理暗号化」に関して，より堅牢なアルゴリズムを開発するための指標として，暗号化された回路の脆弱性を様々な角度から検討を行った．
まず，「SAT攻撃」と呼ばれる既存の暗号化に対する解析アルゴリズムを改良し，高速化および省メモリ化を達成した．また，様々な攻撃に対する評価尺度として「攻撃耐性」と「施錠強度」という2つの評価指標を提案し，それらの指標をランダムサンプリング手法を用いて統計的に導出するアルゴリズムを提案した．

研究成果の学術的意義や社会的意義
本研究では論理暗号化に対する基本的な攻撃手法である「SAT攻撃」のアルゴリズムの効率化を行った．これは暗号化された回路の攻撃耐性を効率よく評価する際に役立つものと思われる．
また，最近では「SAT攻撃」に耐性を持つ論理暗号化手法も提案されているが，これに対しては多くの場合に正しく動く近似鍵を求めるという「近似解攻撃」という攻撃手法も知られている．このような状況を踏まえ，攻撃に対する耐性と強度の2つの側面から暗号化の堅牢性を評価する指標を提案することで，ある程度攻撃手法を限定せずに汎用的に堅牢な暗号化の条件を数値化することが可能になったと思われる．

研究成果の概要（英文）：In this research project, we focus on "logic encryption" algorithms,which protect against piracy of logic IP(Intellectual Property). To develop robust encryption algorithms, evaluation of robustness or weakness of encrypted circuits is very important.
First, we developed an improved "SAT-attack" algorithm, which is a decryption algorithm for logic encryption. Our improved algorithm runs much faster than existing algorithms with fewer memory footprint. Second, we proposed evaluation metrics called "Attack Resilience" and "Lock Strength", which evaluate how encrypted circuits are robust against various attacking methods.We also proposed estimation algorithms for these metrics using random sampling.

研究分野：計算機工学

キーワード：論理暗号化　SAT　LSI設計　セキュリティ

1　研究開始当初の背景

大規模な LSI をゼロから設計することは極めて稀であり，多くの場合は IP(Intellectual Property) と呼ばれるすでに設計された部品を組み合わせ，足りない部分だけを新規設計する手法が用いられている．IP にはマスクパタンからゲート回路，RTL 回路などさまざまな種類があるが，特に論理 IP と呼ばれるゲート回路や RTL 回路の IP は剽窃や盗用，改変などの著作権侵害が容易に行えるという欠点を持つ．そのため，悪意のある半導体メーカー (あるいは半導体設計者) が他社から論理 IP を取得し，それをあたかも自分の知財であるかのように装って販売もしくは提供することが可能である．また，論理 IP を改変し秘密情報を取得するためのバックドアを追加する事例も報告されている．

このようなゲートレベルあるいは RT レベルの論理 IP に対する著作権保護の一手法として論理暗号化 (logic enctyption) 手法が提案されている [1]．論理暗号化とは元の論理回路に「鍵入力」と呼ばれる外部入力信号線を追加し，鍵入力に正しい値が与えられた時のみ回路全体が正しく動作するように回路を改変する手法のことである．この論理 IP を入手したとしても鍵入力の正しい値を知らなければ論理 IP を動作させることはできないため，鍵入力を適切に管理することで論理 IP を保護することが可能となる．

その後，いくつかの論理暗号化手法が提案された [1, 2, 3]．

論理暗号化が提案された当初は暗号化の鍵を探索するアルゴリズムが未知であったため，暗号化の堅牢性を定量的に表す適切な尺度がなかった．その後いくつかの攻撃方法が提案され，特に文献 [4] で提案されている SAT ソルバを用いた攻撃アルゴリズムを用いると既存の暗号化手法の殆どが脆弱であり暗号鍵が容易に特定できることが示された．

その後，この SAT 攻撃に耐性を持つ論理暗号化手法が提案されている [3]．この手法では SAT 攻撃を用いてもほとんどの場合に，鍵入力のビット数の指数に比例した回数の繰り返しを必要とすることがわかっている．

一見，この TTLock は優れた手法の様に思われるがいくつか問題点もある．一つがその回路の構造から秘密鍵が特定されやすいということである．また，例え鍵入力の値として誤ったものを与えたとしても出力に誤った値が現れる確率が極めて低いという特徴を持つ．これは正確に動作するかを 0 か 1 かで判断したら誤動作と言えるが，実用上はほぼ正常に動作していると見なせてしまうことになる．つまり鍵を解錠することができなくてもドアに隙間が空いているようなものである．

このように論理暗号化の技術は提案されてまだ日が浅く，実用的に十分と言える手法が確立してはいない．

2　研究の目的

本研究では堅牢な論理暗号化手法の開発を最終目的として，そのために暗号化された回路の耐性や強度を評価する手法に対する検討を行なう．

3　研究の方法

本研究では大きく分けて以下の 2 テーマに関して研究を行った．

3.1 SAT 攻撃の効率化

現時点で最も強力な攻撃手法である SAT 攻撃のアルゴリズムについて，計算時間やメモリ使用量の改善を行った改良型のアルゴリズムの開発を行なう．

3.2 暗号化手法の耐性・強度の評価指標

SAT 攻撃は重要な攻撃手法だが，それ以外にも暗号化された回路の構造から鍵の情報を推定する手法などさまざまな攻撃手法が提案されている．しかし，いちいち個別の攻撃手法に対する耐性・強度の評価を行なうことは現実的ではない．そこで，攻撃手法を限定しない汎用の評価指標を提案し，その評価アルゴリズムの開発を行なう．

4 研究成果

4.1 SAT 攻撃の効率化

SAT 攻撃で扱っている SAT 問題は以下の通りである．

$$F(k_1) \wedge F(k_2) \wedge \mathcal{C}_{enc}(x_i, k_1, y_1) \wedge \mathcal{C}_{enc}(x_i, k_2, y_2) \wedge (y_1 \neq y_2) \tag{1}$$

前述の様に SAT 攻撃のアルゴリズムで時間を要する原因は繰り返し回数が増える毎に鍵入力の条件 F が複雑になってゆくことにある．ここではこの F を表す CNF 式の生成方法について述べる．F は新しい入力値 x_i と出力値 y_i が与えられた時に式 (2) の様に更新される．

$$F \leftarrow F \wedge \mathcal{C}_{enc}(x_i, k, y_i) \tag{2}$$

もちろん，x_i, y_i の値が異なる場合の $\mathcal{C}_{enc}(x_i, k, y_i)$ は互いに異なる関数となるため単純にはそれぞれ別個の変数を用いて符号化を行う必要があるが, 実際には元となっている回路が同一であり, そこから符号化された元の CNF 式も同じ形をしている. 2 つの入力値 x_{i1} と x_{i2} の値によっては $\mathcal{C}_{enc}(x_{i1}, ky_{i1})$ と $\mathcal{C}_{enc}(x_{i2}, ky_{i2})$ の部分回路が論理的に等価である場合もあり得る. そこで, 回路構造の同形性のみを用いて等価なゲートを判定する簡易な等価検証を行うことで等価なゲートを見つけ，重複した CNF 節の生成を行わない改良型の鍵条件生成アルゴリズムを開発した．アルゴリズムの概略は以下のようになっている．

1. 鍵条件回路を空で初期化する．$L \leftarrow \emptyset$
2. 入力 x_i を暗号化された回路に適用した結果の論理回路を生成する．
3. その際に L にすでに等価なゲートが存在している場合には新規のゲートを作らずに既存のゲートを用いる．新規のゲートは L に追加する．
4. 鍵を求める SAT ソルバ，差分入力を求める SAT ソルバのそれぞれに対して直前の回路生成の際に新規に作られたゲートに対してのみ Tseitin の符号化を用いて CNF 式を生成する．

前述のようにここではゲートの等価性判定をゲートの種類が同じで，同じファンインを持つかどうかだけで行っているのでハッシュ関数を用いれば高速に判定を行うことが可能である．もともと同じ暗号化回路から生成される回路なので論理的に等価なゲートは構造的にも等価な場合が多いため有効かつ効率的と思われる．この手法の欠点は鍵条件を表す CNF 式を作る際に式だけでなく回路構造まで作成し，かつその回路構造を最後

まで保持しておかなければならないということである．繰り返し回数の多い時には使用メモリ量が増えるという問題点がある．しかし，実験によれば等価ゲートを見つけて生成する CNF 式を少なくする効果の方が勝っている場合が多い．

4.2 暗号化手法の耐性・強度の評価指標

4.2.1 評価指標の定義

SAT 攻撃は多くの場合，有効な攻撃手法であり，SAT 攻撃で鍵が推定されてしまう暗号化手法は実用的ではないと言える．しかし，SAT 攻撃以外にも攻撃手段は存在し，また，SAT 攻撃で解けないと思われる回路に対しては SAT 攻撃は莫大な計算時間を費やすため，SAT 攻撃のみを評価指標として用いることも現実的ではない．

そこで，攻撃手法を限定せず，暗号化された回路の情報から暗号化の耐性・強度を指標化する検討を行った．単純には暗号化に対する指標は 1 次元でよいように思われるが実はそうではない．前述したように論理暗号化をドアの施錠に例えると，鍵穴にピックを差し込んで解錠することがしやすいかどうかという観点とは別に鍵のかかったドアをそのままこじ開けることができるかどうかという観点も必要である．そこで，前者を「攻撃耐性」，後者を「暗号化強度」と呼ぶことにする．具体的には以下の様に定義される．

攻撃耐性　1 つの外部入力の値に対して誤った出力を生成する鍵入力の値の数の平均値.
暗号化強度　1 つの鍵入力の値に対して誤った出力を生成する外部入力の値の数の平均値.

まず，攻撃耐性であるが，この値が大きいときには，SAT 攻撃の 1 回の繰り返しで候補から取り除かれる鍵入力の値が多いことを意味する．つまり，全体としての繰り返し回数が少なくなることが予想され，SAT 攻撃で解を求めることが容易になると思われる．そこで，一般にはこの値が小さいことが SAT 攻撃で解を求められる可能性を低くすることにつながると考えられる．

一方，暗号化強度に関しては，逆にこの値が大きいということは適当な鍵入力の値を用いた時に暗号化された回路が誤動作する確率が高くなることを意味する．そこで，この値が大きな暗号化ほど正解以外の鍵を用いた時の暗号化の効果（強度）が高いということになる．

4.2.2 評価指標の算定方法

さて，前述のように評価指標を定義したわけだが，実際にはこれらの指標を正確に計算することは困難である．そこで，ランダムサンプリングを用いた手法と SAT 問題の Model Counting を用いた手法を提案した．

ランダムサンプリングを用いた手法では外部入力あるいは鍵入力の値をランダムに与えて結果を計算する．大数の法則にしたがってランダムサンプリングを用いた平均値は真の平均値に収束することが知られているので十分な数のサンプルを用いればよい近似となると思われる．

ランダムサンプリングによる手法では予想される値がある程度大きい場合にはよい近似となるが，結果の値が極めて小さい場合，推定精度の問題がある．例えば実際の値が $\frac{1}{10^{10}}$ であるような場合にはたかだか 10^3〜10^5 程度のサンプル数で真値を推測することは不可能である．実際，SAT 攻撃に耐性を持つ暗号化手法の場合，予想される攻撃耐性は極めて小さな値になるのでここで述べたような状況となる．そこで，別の手法として SAT 問題の Model Counting を用いた手法を提案する．

Model Counting とは SAT 問題を充足する解の個数を数える問題のことである．そもそも解があるかないかを判定するだけの SAT 問題が $\mathcal{NP}$ 問題であるので，当然のことながら Model Counting はより難しい問

題となっている．そこで，実用的には MCMC(Markov Chain Mote Calro) を用いた手法 [7] や XOR 制約を用いた手法 [8] のような近似手法が用いられている．そこで，ここでは XOR 制約を用いた手法を提案する．XOR 制約を用いた手法の基本的なアイデアは，解が存在するブール空間をランダムに 2^l 個の部分空間に分割し，その 1 つの部分空間に対して SAT 問題を解いた結果，ただ一つの解が存在したならば，全ブール空間上には約 2^l 個の解が存在すると推測する，というものである．今，ブール空間を分割するには k 個の変数 $x_1, x_2, \ldots, x_k$ をランダムに選び，それらを排他的論理和 (XOR) で結合した論理式 $(x_1 \oplus x_2 \oplus \cdots x_k)$ を作る．その式が 0 か 1 のどちらかに等しいという制約を l 回追加することで，結果として解空間を 2^l に分割することになる．

これらの評価指標の算出方法を評価するために，あらかじめ真値がわかっている暗号化回路を用意し測定を行った結果，予想通り，攻撃耐性に関しては Model Counting を用いた手法が高い推定精度を得ることができた．一方，暗号強度に対してはランダムサンプリング手法が計算時間，精度ともに良い結果となった．

4.3 回路構造に基づく攻撃耐性の評価

今までのアプローチとは別に構造的特徴による SAT 攻撃への耐性についての検討を行なった．SAT 攻撃に耐性がある論理暗号化手法である SARLock や Anti-SAT に対して，論理暗号化後の回路の特徴に基づいた removbale attack による攻撃に脆弱であることが文献などで示されている．そこで，removbale attack への脆弱性が示されていない TTLock に対して構造的特徴による耐性に関して研究を行った．その結果，TTLock 手法における元々の論理回路 (LC) から修正された論理回路 (MLC) の生成の際に，単なる再論理合成を用いた生成方法では，MLC 中に脆弱性となる構造的特徴が存在することがわかった．本研究では，この構造的特徴を特定し，構造的特徴から秘密鍵を導出する手法を開発した．

参考文献

[1] J.A. Roy, F. Koushanfar, and I.L. Markov, “Ending piracy of integrated circuits,” Computer, vol.43, no.10, pp.30–38, Oct 2010.

[2] J. Rajendran, H. Zhang, C. Zhang, G. Rose, Y. Pino, O. Sinanoglu, and R. Karri, “Fault analysis-based logic encryption,” vol.64, no.2, pp.410–424, 2015.

[3] M. Yasin, A. Sengupta, B.C. Schafer, Y. Makris, O. Sinanoglu, and J. Rajendran, “What to lock? functional and parametric locking,” Great Lake Symposium on VLSI, pp.351–356, May 2017.

[4] P. Subramanyan, S. Ray, and S. Malik, “Evaluating the security of logic encryption algorithms,” 2015 IEEE International Symposium on Hardware Oriented Security and Trust (HOST), pp.137–143, May 2015.

[5] G. Tseitin, “On the complexity of proofs in propositional logics,” In Automation of Reasoning: Classical Papers in Computational Logic 1967 – 1970, volume 2, Springer, 1970.

[6] T. Larrabee, “Test pattern generation using Boolean satisfiability,” IEEE Trans. Computer-Aided Design, vol.11, no.1, pp.4–15, 1992.

[7] A. Biere, M. Heule, H. van Maaren, and T. Walsh, Handbook of Satisfiability, IOS Press, 2009.

[8] C.P. Gomes, A. Sabharwal, and B. Selman, “Near-uniform sampling of combinatorial spaces using xor constraints,” NIPS, pp.481–488, 2006.

５．主な発表論文等

〔雑誌論文〕　計0件

〔学会発表〕　計11件（うち招待講演　0件／うち国際学会　1件）

１．発表者名 Yusuke Matsunaga and Masayoshi Yoshimura
２．発表標題 An Efficient SAT-Attack Algorithm Against Logic Encryption
３．学会等名 IOLTS2019（国際学会）
４．発表年 2019年

１．発表者名 松永　裕介
２．発表標題 誤り修正論理合成を用いた論理暗号化手法について
３．学会等名 FTC研究会
４．発表年 2019年

１．発表者名 松永　裕介
２．発表標題 誤り修正論理合成を用いた論理暗号化手法
３．学会等名 情報処理学会DAシンポジウム
４．発表年 2019年

１．発表者名 松永　裕介
２．発表標題 アフィン変換を用いた論理暗号化手法について
３．学会等名 電子情報通信学会VLD研究会
４．発表年 2019年～2020年

１．発表者名
松永　裕介

２．発表標題
アフィン変換を用いた論理暗号化手法の評価

３．学会等名
電子情報通信学会VLD研究会

４．発表年
2019年～2020年

１．発表者名
松永　裕介

２．発表標題
テストセット最小化問題の両立集合被覆問題への定式化とその解法

３．学会等名
情報処理学会DAシンポジウム

４．発表年
2018年

１．発表者名
松永　裕介

２．発表標題
組合せ最適化問題としてのテストセット最小化問題

３．学会等名
FTC研究会

４．発表年
2018年

１．発表者名
松永　裕介,　吉村　正義

２．発表標題
論理暗号化に対するSAT攻撃の効率的なアルゴリズムについて

３．学会等名
電子情報通信学会VLD研究会（デザインガイア）

４．発表年
2018年

１．発表者名
松永　裕介,　吉村　正義

２．発表標題
論理暗号化に対するSAT攻撃アルゴリズムの高速化

３．学会等名
FTC研究会

４．発表年
2019年

１．発表者名
松永　裕介,　吉村　正義

２．発表標題
論理暗号化に対する効率的なSAT攻撃アルゴリズムの評価

３．学会等名
電子情報通信学会VLD研究会

４．発表年
2019年

１．発表者名
南　周作，松永　裕介

２．発表標題
論理施錠の施錠強度と攻撃耐性についての新たな評価の手法

３．学会等名
電子情報通信学会VLD研究会

４．発表年
2020年～2021年

〔図書〕　計0件

〔産業財産権〕

〔その他〕

―

６．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考
研究分担者	吉村　正義 (Yoshimura Masayoshi) (90452820)	京都産業大学・情報理工学部・准教授 (34304)	

７．科研費を使用して開催した国際研究集会

〔国際研究集会〕　計0件

８．本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関