様　式　Ｃ－１９、Ｆ－１９、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成 ２７ 年　 ５ 月 １８ 日現在

機関番号：３４３０４
研究種目：挑戦的萌芽研究
研究期間：2013～2014
課題番号：２５５４００２０

研究課題名（和文）秘密情報の秘匿性と製造検査容易性の両立をはかるLSI設計手法の研究

研究課題名（英文）Study on LSI design methods for security and testability

研究代表者
吉村　正義（YOSHIMURA, Masayoshi）

京都産業大学・コンピュータ理工学部・准教授

研究者番号：９０４５２８２０

交付決定額（研究期間全体）：（直接経費）　　2,900,000円

研究成果の概要（和文）：本研究は、LSIの設計情報が漏洩したとしても、秘密情報が搭載されたLSIに対して、LSIの内部に格納された秘密情報を秘匿しつつ、LSIの内部に製造時に故障が発生していないかを容易に検査できる設計技術を開発することである。従来、LSIの設計を工夫し、その設計情報を秘匿することで、安全性は保たれていた。しかしLSI の設計情報はLSIの設計に携わる多数の人が知りうる情報であり、完全な秘匿は困難である。そこで本研究はLSI の設計情報に依存せずに安全性を保つ設計手法および設計支援技術を開発した。秘密情報の漏洩度合いを相互情報量によって評価し、提案手法の安全性を定量的に示した。

研究成果の概要（英文）：The scan design method makes it possible to increase testability. Scan-based Attacks with scan design decrease security for confidential information on LSIs. Conventional methods provide assurance of security with complicated scan designs. If information about complicated scan designs, attackers could obtain confidential information on LSIs by using scan-based attacks. Complicated scan designs is a novel confidential information.
We proposed a design method with both testability and security without depending on complicated scan designs. The proposed method is a design method which ensures testability on behavior level testability without scan design. Several designs were applied to the proposed methods. We measured quantitatively the security for the designs applied to the proposed method. The measure for security evaluation is mutual information.

研究分野：情報工学

キーワード：安全　信頼性　LSI設計技術　暗号LSI　製造テスト　テストパタン生成　テスト容易化設計

１．研究開始当初の背景

価値や信用に関する情報を保護するために，様々なデジタル製品に暗号LSIが搭載されている．暗号 LSI とは暗号化・復号化の処理を行う LSI である．暗号 LSI は暗号化・復号化に用いる秘密鍵を用いて，第三者に秘匿したい情報を処理する．暗号 LSI に対する攻撃法はサイドチャネル攻撃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．

暗号 LSI を含む多くの LSI には，製造テストのためにスキャンチェインが挿入されている．スキャン設計とは LSI のテスト容易化設計として一般的に用いられる手法の一つである．スキャンチェインによって，LSI の可制御性と可観測性が向上し，LSI のテストを容易にする．スキャン設計は LSI が故障した際の故障診断にも使用される．このため，製品出荷後もスキャンチェインは使用できる状態であることが多い．

しかしながら，Yang らはスキャンチェインを通して暗号 LSI 内部にある暗号化・復号化に用いる秘密鍵などの秘密情報を特定される危険性が指摘した．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示し，秘密鍵が特定可能であることを示した．

このスキャンベース攻撃に対する防御法には，高いテスタビリティ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．しかしながら，これらの多くは元の回路に対してテスタビリティの低下や面積の増加を招く，防御法を適用した回路構成情報が新たな保護する対象となってしまうなどの問題がある．つまり，テスタビリティが低下せず，面積の増加も少なく，新たな秘密情報が発生しない防御手法が求められている．

２．研究の目的

スキャンベース攻撃に対して，最も効果的な防御法は，暗号 LSI を暗号 LSI 中のすべての FF にスキャンチェインを挿入しないノンスキャン設計にすることである．しかしながら，暗号 LSI 中のすべての FF をノンスキャン FF で構成した場合，暗号 LSI のテスタビリティは著しく低下する．そこで，スキャンチェインの構成を変えることによるテスタビリティとセキュリティのトレードオフの関係を明らかにすることは重要である．これがこの研究の第一の目的である．

第二の目的は，スキャンベース攻撃を防ぎ，テスタビリティや面積などのオーバーヘッドが少ないテスト手法を開発することである．

３．研究の方法

まず既存の防御手法の定量的な評価を行った．本研究では安全性の定量的な評価尺度として相互情報量を用いて，漏洩する秘密情報の安全性を評価した．既存の防御手法は，手法 1 と手法 2 の 2 つに分類される．手法 1 は検査容易化するための回路に種々の工夫を施し，その工夫を秘密とすることで，秘密情報を安全にする手法である．手法 2 は観測結果の情報を LSI 内で圧縮し出力し，その圧縮手法を秘密にすることで，秘密情報を安全にする手法である．手法 1 は LSI の設計情報が漏洩すると，秘密情報は全て漏洩する．そのため手法 2 の手法に対して，安全性の評価を実施し，既存手法の評価を実施した．評価尺度に相互情報量を用いた．相互情報量は，2 つの情報の相互依存度を評価するものである．つまり，攻撃者が入手可能な情報から秘匿されている情報をどの程度特定できるかを示す尺度である．攻撃者が入手可能な情報は LSI の回路情報や LSI の出力応答であり，秘匿されている情報は LSI に搭載されている秘密情報である．この二つの情報に対する相互情報量を安全性の評価尺度として，評価を実施した．

次に評価結果に基づき，新たな秘密情報を持たない防御手法について，研究を実施した．手法 2 は，LSI の応答を観測した結果をどのように圧縮するかによって，漏洩する秘密情報の相互情報量が決定される．この圧縮方法は，次の 3 つの要素技術から構成される．1 つ目は，LSI にどのような入力を与え，どのような応答を得るかである．2 つ目は，どの応答結果を観測するかである．3 つ目は，観測した情報をどのように圧縮するかである．これら 3 つの要素技術について検討を行った．

最後に開発した防御手法をさまざまな暗号回路に適用して，安全性やテスト容易性，面積などの項目の評価を行った．

４．研究成果

設計データが漏えいした場合，圧縮回路が出力するデータに含まれる秘密情報に関する相互情報量について計測した．計測した結果，圧縮回路が出力するビット数と相互情報量はほぼ等しいことがわかった．この結果は，入力するデータや圧縮回路に依存しなかった．これにより，圧縮回路の構成を工夫しても，漏えいする情報量が変化しないことを示す．

この結果を受け，設計データが漏えいしても，秘密情報が漏えいしない防御方法に関して，検討を行った．その結果，スキャン設計を採用せず，テスト容易性を高める方針を採用した．設計方針の検討と検証実験によって，設計の初期段階でテスト容易化設計を実施することで，スキャン設計と同等のテスト容易性を確保できることがわかった．

最後に開発した設計手法を DES 暗号回路や AES 暗号回路に対して適用し，テスト容易性や面積オーバーヘッドなどについて評価を実施した．その結果，スキャン設計とほぼ同等のテスト容易性があることがわかった．この成果は 2015 年 2 月に開催されたディペンダブルコンピューティング研究会にて報告した(学会発表②)．

５．主な発表論文等
（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計　5 件）

① 安浦寛人，松永裕介，吉村正義，杉原真，"設計自動化技術," 日本信頼性学会誌, 査読有, Vol.35, No.8, p.430, 2013.

② 堀洋平, 鈴木大輔, 吉村正義, 吉川雅弥, 藤野毅, "セキュリティ LSI に対するタンパリングの手法," 日本信頼性学会誌，査読有, Vol.35, No.8, p.492, 2013.

③ 吉村正義, "スキャンベース攻撃への対策," 日本信頼性学会誌，査読有，Vol.35, No.8, p.496, 2013.

④ Hiroshi Yamazaki, Motohiro Wakazono, Toshinori Hosokawa, and Masayoshi Yoshimura, "A Test Compaction Oriented Don't Care Identification Method Based on X-bit Distribution," IEICE Transactions on Information and Systems, 査読有, Vol. E96-D, No. 9, pp.1994-2002, 2013.

⑤ Taiga Takata, Masayoshi Yoshimura, and Yusuke Matsunaga, "Efficient Fault Simulation Algorithms for Analyzing Soft Error Propagation in Sequential Circuits," IPSJ Transactions on System LSI Design Methodology, 査読有, Vol.6, August issue, pp.127-134, 2013.

〔学会発表〕（計　11 件）

① Hiroshi Yamazaki, Jun Nishimaki, Toshinori Hosokawa and Masayoshi Yoshimura, "A Multi Cycle Capture Test Generation Method for Low Capture Power Dissipation," Designing with Uncertainty - Opportunities & Challenges, 査読有, Grenoble(France), March 13th, 2015.

② 吉村 正義, 西間木 淳, 細川 利典, “スキャンベース攻撃を考慮した暗号 LSI のテスト手法,” 信学技報, 査読なし, vol. 114, no. 446, DC2014-82, pp. 25-30, 機械振興会館（東京), 2015 年 2 月 13 日.

③ 坊屋鋪 知拓, 細川 利典, 吉村 正義, “信号非遷移情報に基づくトロイ回路検出法,” 信学技報, 査読なし,vol. 114, no. 446, DC2014-81, 機械振興会館（東京), pp. 19-24, 2015 年 2 月 13 日.

④ 山崎 紘史, 西間木 淳, 細川 利典, 吉村正義, “キャプチャ消費電力削減のためのマルチサイクルキャプチャテスト生成法,” 信学技報, 査読なし,vol. 114, no. 329, ビーコンプラザ（大分県・別府市), DC2014-54, pp. 191-196, 2014 年 11 月 28 日.

⑤ 高橋 慶安, 山崎 紘史, 細川 利典, 吉村正義, “キャプチャ消費電力削減のためのテストポイント挿入法,”信学技報, 査読なし,vol. 114, no. 329, DC2014-53, pp. 185-190, ビーコンプラザ（大分県・別府市), 2014 年 11 月 28 日.

⑥ 山崎紘史, 川連裕斗, 西間木淳, 平井淳士, 細川利典, 吉村正義, 山崎浩二, “マルチサイクルキャプチャテスト生成を用いた低消費電力指向遷移故障テスト生成法,” 信学技報, 査読なし, vol. 113, no. 430, DC2013-89, pp. 61-66, 機械振興会館（東京), 2014 年 2 月 10 日.

⑦ 田中まりか, 山崎紘史, 細川利典, 吉村正義, 新井雅之, “BAST におけるシフトデータ量削減法,” 信学技報, 査読なし,vol. 113, no. 430, DC2013-87, pp. 49-54, 機械振興会館（東京), 2014 年 2 月 10 日.

⑧ 高橋慶安, 山崎紘史, 細川利典, 吉村正義, “SAT を用いた低キャプチャ電力指向ドントケア割当て法,”信学技報, 査読なし, vol. 113, no. 430, DC2013-83, pp. 25-30, 機械振興会館（東京), 2014 年 2 月 10 日.

⑨ 田中まりか, 山崎紘史, 細川利典, 吉村正義, 新井雅之, 中尾教伸, “BAST におけるテストデータ量削減のためのインバータブロック構成法,”信学技報, 査読なし, vol. 113, no. 321, DC2013-51, 鹿児

島県文化センター (鹿児島県・鹿児島市), pp. 171-176, 2013 年 11 月 28 日.

⑩ Masayoshi Yoshimura, Amy Ogita, and Toshinori Hosokawa, "A Smart Trojan Circuit and Smart Attack Method in AES Encryption Circuits," 16th IEEE Symposium Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT2013), 査読有, New York (USA), pp.278-283, October 4, 2013.

⑪ Hiroshi Yamazaki, Motohiro Wakazono, Toshinori Hosokawa, and Masayoshi Yoshimura, "A don't care identification method for test compaction", 2013 IEEE 16th International Symposium on Design and Diagnostics of Electronic Circuits & Systems (DDECS), Karlovy Vary (Czech Republic), pp.215-218, April 8, 2013.

〔その他〕
ホームページ等
http://www.cc.kyoto-su.ac.jp/~myoshi

６．研究組織
(1)研究代表者
吉村　正義 (YOSHIMURA, Masayoshi)
京都産業大学・コンピュータ理工部・准教授
研究者番号：90452820