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

平成　２９　年　　６　月　１５　日現在

機関番号：　３３９１９
研究種目：　基盤研究(C)（一般）
研究期間：　2013～2016
課題番号：　２５３３０１６２

研究課題名（和文）セキュリティLSIに対するハードウェアトロイの対策と検出に関する研究

研究課題名（英文）Countermeasures and Detection Techniques for Hardware Trojans on Security Modules

研究代表者

吉川　雅弥（Yoshikawa, Masaya）

名城大学・理工学部・教授

研究者番号：５０３７３０９８

交付決定額（研究期間全体）：（直接経費）　　3,900,000円

研究成果の概要（和文）：リバースエンジニアリングの技術の進歩に伴い，ハードウェアトロイの脅威が顕在化してきた。ハードウェアトロイとは，予め定めた発動条件を満たした場合，不正な動作を行うハードウェアウイルスのことである。一方，機密情報は，理論的に安全性が保障されているアルゴリズムを用いて，データを暗号化している。しかし，暗号化は回路で行われるため，その回路動作時の消費電力等を測定することで，不正に内部の秘密情報を解析する攻撃が研究されている。そのため，最近では暗号回路を対象に，いくつかの不正防止回路が開発されている。そこで本研究では不正防止回路も含めた暗号回路に対するハードウェアトロイの対策・検出手法を開発した。

研究成果の概要（英文）：With advancements of reverse engineering technologies, Hardware Trojans are a new threat that is emerging in many countries. In Hardware Trojans, a hidden function is activated and extensive damage occurs when predetermined conditions specified by an attacker are satisfied. Confidential information is protected using the encryption standard used which is theoretically secured. However, although an encryption algorithm is theoretically secured, a secret key for an encryption device can be revealed by analyzing side-channel information such as power consumption. Therefore, several countermeasures are proposed. This study developed detection techniques for Hardware Trojans which are incorporated into cryptographic circuits including countermeasures.

研究分野：　総合領域

キーワード：　ハードウェアトロイ　検出技術　セキュリティ

１．研究開始当初の背景

半導体集積回路は，携帯電話やパソコンなど様々な電子機器に搭載されている。しかし，リバースエンジニアリングの技術の進歩に伴い，現在，半導体市場の 5%が模倣品であると言われている。米国では，兵器など軍用の半導体・電子部品での模倣品被害の深刻さを報告している。このような模倣品の集積回路にハードウェアトロイが組み込まれる危険性が指摘されている。ハードウェアトロイとは，あらかじめ定めた発症条件をトリガとして，ユーザに気づかれずにシステムの停止や重要情報の流出などの破壊工作を行うハードウェアウイルスのことである。

一方で，クレジットカードやキャッシュカードのように，集積回路を利用して金銭情報や個人情報を保管するシステムが社会基盤として広く普及している。このような集積回路には機密情報保持のために暗号回路が用いられており，使用される標準暗号は，計算量的にその安全性が保障されている。
しかし，計算量的に安全な暗号アルゴリズムであっても，回路としてハードウェア実装された場合，暗号化の処理時に生じる消費電力や電磁波などの暗号アルゴリズムとは直接関係のない 2 次的な情報を解析することで，暗号化での秘密鍵を推定できることが報告されている。そのため，そのような不正な解析を防止する対策回路がいくつか提案されている。

２．研究の目的

ハードウェアトロイは物理的に LSI 内に組み込まれているため，外部からは気付きにくく，ソフトウェアトロイと異なり取り除くことができない。そのため，米国では現実的な脅威として，ハードウェアトロイを懸念しているが，現在までにハードウェアトロイの対策・検出技術について，学会レベルの動作原理に関する発表がいくつかある程度で，まだ確立されていない。そのような状況の中で，情報セキュリティーの要であるセキュリティーモジュールである暗号回路に対するハードウェアトロイの対策・検出技術は，安全・安心に生活するための最も重要な技術の１つである。そこで申請研究では，不正防止回路も含めたセキュリティーモジュールに対するハードウェアトロイの対策と検出方法を確立する。これにより，セキュリティーの要である暗号回路の安全性を保障する。

３．研究の方法

本研究では，4 年間の研究期間において，不正防止回路も含めたセキュリティーモジュールに対するハードウェアトロイの対策と検出方法を開発した。

対策手法と検出手法のそれぞれについて，サブテーマを数か月単位で設定して研究を進めた。対策手法と検出手法については，それぞれの検討を行う前に，様々なトロイの評価・検証を行った。ここでは，複数のトリガー，複数の実装方法，複数のセキュリティモジュールに対して定量的に評価をした。次にセキュリティモジュール単体ではなく，アプリケーションも含めて，その特性を評価することで対策手法と検出手法の検討を行った。

４．研究成果

全体として当初の目標をおおむね達成することができた。まず，対策技術に関して，トロイの実装方法についての検討を行った。特に，省面積実装を指向した方法について，トロイトリガーに着目して，複数の実装方法について FPGA を用いた評価実験により検証した。また, 標準暗号 AES の回路だけでなく，組込システムで期待が高まっている軽量暗号や楕円暗号についてもトロイの実装方法について検討を行った。さらに，実用的なアプリケーションとして車載 ECU を対象としたトロイに関してもその実装方法や対策についても検討を行った。処理時間が問題になる車載システムについて, CAN を実装したモックアップを用いた評価実験により，その有効性を検討した。

一方，検出技術に関しては，まず，これまで開発を進めてきたサイドチャネル攻撃対策用のトロイを対象に評価・検証を行った。このサイドチャネル攻撃対策用のトロイは，トロイトリガーが発動すると対策を無効化するトロイであるため，一般的な機能テストでの検出が難しいことを，FPGA を用いた評価実験により実証した。また，トロイトリガーに関して，これまで発表されているような条件を満たせば必ず発動するトリガーではなく，再現性が無いトロイトリガーを開発することによって，トロイの検出困難性を検討した。さらに，一般的な入力信号をトリガーとするのではなく，リセット信号をトリガーとする新しいトロイも新たに開発して，検出に必要な技術の基本検討を行った。消費電力等のサイドチャネル情報を利用した検出方法の基本検討を行った。この検出方法では，サポートベクターマシーンを使ってトロイのモデル化を行った。また，複数の種類のトロイを FPGA に実装して評価実験を行い，その有効性を検証した。さらに，より高精度な検出を実現するために必要な漏洩電磁波等のサイドチャネル情報について，分析・考察を行った。そして，これまで検討してきた消費電力等のサイドチャネル情報を利用したサポートベクターマシーンを用いた検出方法について，新たに回路のスタンバイ状態に着目した検出方法を考案し，トリガーや動作の異なった複数のトロイを，種類の違う複数

の FPGA に実装して評価実験を行い，その有効性を検証した。さらに，トロイの FPGA への実装方法による違いについても，面積や消費電力について，分析・考察を行った。これらの成果については，関連する国内研究会や国際会議で発表するだけでなく，学術論文誌でも発表した。

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 2 件）

① **野崎佑典，藤野毅，吉川雅弥，**“**軽量暗号 TWINE に対する周波数領域での電力解析とその評価，**”**電子情報通信学会論文誌 B，査読有，** vol.J99-B，no.10，pp.881–892，**2016 年 10 月**
DOI：10.14923/transcomj.2016IAP0003

〔学会発表〕（計 25 件）

① H.Nagata, Y.Ikezaki, Y.Nozaki, M.Yoshikawa, “Hardware Trojan Detection Method based on Deep Learning,” Proc. of RISP International Workshop on Nonlinear Circuits, Communications and Signal Processing, pp.53–56, March 2017.(U.S.A)

② **岩瀬貴都，野崎佑典，吉川雅弥「センサトリガを用いたハードウェアトロイの実装と評価」電子情報通信学会技術研究報告,** vol.116, no.315, CAS2016-58, pp.1-6, **2016 年 11 月.(兵庫県)**

③ Y.Nozaki, Y.Ikezaki, M.Yoshikawa, "Hardware Trojan for an Authenticated Encryption Minalpher," Proc. of IEEE 5th Global Conference on Consumer Electronics, pp.455-456, Oct. 2016. (Kyoto, Japan)

④ **岩瀬貴都，吉川雅弥「モデルの差異によるハードウェアトロイ検出率への影響評価」第 41 回東海ファジィ研究会講演論文集,** no.8，pp.1-4，**2016 年 8 月.(愛知県)**

⑤ **岩瀬貴都，吉川雅弥「スタンバイ状態に着目したハードウェアトロイの検出手法」第 13 回情報学ワークショップ** WiNF2015 **講演論文集,** pp.25-29, **2015 年 12 月.(愛知県)**

⑥ **池崎良哉**, **吉川雅弥「ハードウェアトロイのトリガ条件と実装面積の考察」平成 27 年度電気・電子・情報関係学会東海支部連合大会講演論文集**, D2-1, **2015 年 9 月.(愛知県)**

⑦ **岩瀬貴都**, **吉川雅弥「モデル化を必要としないハードウェアトロイの検出手法とその評価」平成 27 年度電気・電子・情報関係学会東海支部連合大会講演論文集**, D2-3, **2015 年 9 月.(愛知県)**

⑧ **池崎良哉**, **吉川雅弥「小面積を指向したハードウェアトロイとその実装評価」平成 27 年度電気関係学会北陸支部連合大会**, F1-22, **2015 年 9 月.（石川県）**

⑨ **岩瀬貴都**, **吉川雅弥「異なる FPGA ボードにおけるハードウェアトロイの検出評価」第 39 回東海ファジィ研究会講演論文集**, no.6, pp.1-5, **2015 年 8 月.(愛知県)**

⑩ M.Yoshikawa, Y.Hayashi, Y.Nozaki, K.Asahi, "Secure automotive embedded system using a lightweight block cipher against malicious Trojan attack", Proc. of 21st ISSAT International Conference on Reliability & Quality in Design, pp.218-221, Aug. 2015.(U.S.A)

⑪ R.Matsuhisa, Y.Nozaki, K.Nohara, K.Asahi, M.Yoshikawa, "A Hardware Trojan Architecture for Elliptic Curve Cryptography", Proc. of International Conference on Electrical Engineering, 15A-167, pp.1-6, July 2015.

⑫ M.Yoshikawa, K.Sugioka, Y.Nozaki, K.Asahi, "Secure in-vehicle systems against Trojan attacks", Proc. of International Conference on Computer and Information Science, pp.29-33, June 2015. (U.S.A)

⑬ **松久僚真，吉川雅弥「楕円曲線暗号に対するハードウェアトロイの考察」第 38 回東海ファジィ研究会講演論文集,** No24**,** pp.1-4，**2015 年 2 月.(愛知県)**

⑭ K.Nohara, K.Asahi, M.Yoshikawa, "Study of threat for automotive embedded system by Trojan virus", IEEE 3rd Global Conference on Consumer Electronics, pp.405-406, Oct. 2014.(Chiba, Japan)

⑮ **野原康平，吉川雅弥,**「ECU **のトロイ混入による危険性についての一考察」，電子情報通信学会，信学技報**, vol.114, no.123, VLD2014-52, pp.231-236, **2014 年 7 月.(北海道)**

⑯ M.Yoshikawa, T.Tsukadaira, "Implementation and detection tests for countermeasure-annulled hardware trojan on FPGA", Proc. of International

Conference on Micro Nano Devices, Structure Computing Systems, pp.268-273, March 2014. (Singapore)

⑰ M.Yoshikawa, Y.Mori, T.Kumaki, "Implementation aware Hardware Trojan Trigger", Proc. of International Conference on Industrial Electronics and Applications , pp.482-486, Feb. 2014.(Hong Kong)

〔図書〕（計 0 件）

〔産業財産権〕

○出願状況（計 0 件）

○取得状況（計 0 件）

〔その他〕

６．研究組織

(1) 研究代表者
吉川　雅弥（Masaya Yoshikawa）
名城大学・理工学部・教授
研究者番号：50373098