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　元 年　 ６ 月 １１ 日現在

機関番号：１２６１２
研究種目：基盤研究(A)（一般）
研究期間：2015～2018
課題番号：１５Ｈ０１６８８

研究課題名（和文）レーザーフォールト攻撃による情報漏洩を防ぐ耐タンパー技術の総合的研究

研究課題名（英文）Comprehensive study on anti-tamper techniques to prevent information leakage by laser fault injection attacks

研究代表者

崎山　一男（Sakiyama, Kazuo）

電気通信大学・大学院情報理工学研究科・教授

研究者番号：８０５０８８３８

交付決定額（研究期間全体）：（直接経費）　　30,100,000円

研究成果の概要（和文）：本研究では、レーザー光を用いて暗号回路に故意にソフトエラーを誘発させ、秘密情報の取得を試みるレーザーフォールト攻撃に対する抜本的対策技術を確立した。具体的には、(1)レーザーフォールト攻撃の評価環境の構築、(2)レーザー照射時の基板電位変動の実測と攻撃検知手法の開発、(3)検知に基づく暗号アルゴリズムレベルの対策技術の開発、及び(4)対策技術の安全性評価を行った。物理的・数理的観点からレーザーフォールト攻撃における情報漏洩メカニズムの理解を深め、プロトタイプICチップを用いて対策技術の実現可能性を明らかにした。

研究成果の学術的意義や社会的意義
暗号学、集積回路工学、環境電磁工学等の分野横断型の研究体制で取り組み、レーザーフォールト攻撃の物理的・数理的メカニズムを解明することができた。また、暗号回路の安全性向上に繋がる新規研究分野を開拓することができた。本研究を通じて開発した技術は、暗号回路に対する物理的攻撃に対して効率の良い対策技術を実現するものである。社会の安心・安全を実現する高セキュリティ暗号ICチップの耐タンパー性の向上に繋がるものである。

研究成果の概要（英文）：In this research, we have established fundamental countermeasure techniques against laser fault injection attacks, where an attacker intentionally induces soft errors in a cryptographic circuit to retrieve secret information. Specifically, we have conducted four research items; (1) construction of evaluation environment of laser fault injection attacks, (2) measurement of substrate potential fluctuation at laser irradiation and development of attack detection method, (3) development of countermeasure techniques for cryptographic-algorithm level based on detection, and (4) safety evaluation of countermeasure technology. We have deepened our understandings of the information leakage mechanism in the laser fault injection attack from physical and mathematical viewpoints and clarified the feasibility of countermeasure techniques using a prototype IC chip.

研究分野：情報セキュリティ

キーワード：暗号・認証等　電子デバイス・機器　計算機システム

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９、ＣＫ－１９（共通）

１．研究開始当初の背景

これまでの大規模集積回路におけるソフトエラーに対する研究の目的は、以下の２つに大別される。１)情報システムの安定性の確保：放射線などによる回路の誤動作を早期に検知し、可能であれば正常動作に回復することを目的とする研究。２)暗号回路の安全性の担保：暗号回路に故意にソフトエラーを誘発させ、秘密情報の取得を試みる攻撃（フォールト攻撃）を扱う研究。上記１）に対しては、効果的な対策回路がすでに提案されているが、それらは２）の対策技術としては不十分である。事実、2010 年に発表された故障感度解析を用いたフォールト攻撃は、１）の対策技術で防ぐことができない。最初に提案されたフォールト攻撃は、暗号回路の処理中に攻撃者が故意にソフトエラーを誘発し、その際に出力される誤り暗号文を解析することで暗号内部の秘密情報を取得するものである。“On the Importance of Checking Cryptographic Protocols for Faults,” Boneh, DeMillo, and Lipton, Eurocrypt'97 で、公開鍵暗号 RSA に対する最初のフォールト攻撃手法が発見され、 “Differential Fault Analysis of Secret Key Cryptosystems,” Biham, Shamir, CRYPTO'97 で、共通鍵暗号 DES に対する攻撃が提案された。その後、フォールト攻撃研究はさらに進化し、高度な統計を用いた解析手法とソフトエラー誘発手法に関する実践的研究が世界中で取り組まれている。中でもレーザー照射によるフォールト攻撃（レーザーフォールト攻撃）は、もっとも深刻な攻撃の脅威とされている。回路故障をビット単位で誘発させることができる上に、ソフトエラー誘発のタイミングを高い精度で制御することができるためである。これまで、フォトディテクターの利用により攻撃を予防する対策が考えられてきたが、誘発された（ソフト）エラーを検知するわけではないことや、フォトンの入射条件により検知可能な範囲は制限的となることなどから、フォールト攻撃の抜本的対策技術とはいえない。なぜならば、フォトディテクターをいかに回路上に配置したとしても、回路設計手法や暗号アルゴリズムへの展開に向けた学術的議論は難しく、体系的な対策技術の確立に繋がらないためである。一方、これまでの暗号研究者によるアルゴリズムでのフォールト攻撃対策は、アルゴリズム記述が可能なものに限られていた。フォールト攻撃対策技術を開発するためには、物理レイヤからアルゴリズムレイヤに至るまでの総合的なフォールト攻撃の理解が不可欠であり、暗号解析、集積回路工学、環境電磁工学等の分野横断型の研究体制による研究の推進が強く求められている。

２．研究の目的

本研究は、暗号回路に故意にソフトエラーを誘発させ、秘密情報の取得を試みるフォールト攻撃への抜本的対策技術の確立を目的とする。現在、最も強力なフォールト攻撃の一つとして知られるレーザーフォールト攻撃に焦点を絞り、ソフトエラーの発生を正確に検知するセンサを開発する。さらに、暗号アルゴリズムと連動した対策技術の構築を狙う。開発した技術は、耐タンパー暗号回路の設計自動化に貢献し、暗号 IC チップの耐タンパー性の向上に繋げる。分野横断型の研究体制で取り組み、レーザーフォールト攻撃の物理的・数理的メカニズムを解明し、暗号回路の安全性向上に繋がる新規研究分野を開拓する。

３．研究の方法

以下の 4 つの研究項目に対して、レーザーフォールト攻撃に対する物理的・数理的観点からのメカニズムの理解と対策技術の実現可能性を明らかにする。

(1) レーザーフォールト攻撃の評価環境の構築：レーザー照射により生じる基板電位変動の測定と攻撃の検知が可能となる評価環境を構築する。また、どのようなエラーが誘発されたかを明らかにするために、評価実験により得られた出力信号の解析環境を構築する。

(2) レーザー照射時の基板電位変動の実測と攻撃検知手法の開発：IC チップの基板電位変動の分布を測定し、レーザー照射によるシリコン基板応答の物理特性を明らかにする。また、電位変動測定によりレーザー照射の検知手法を開発し、暗号アルゴリズムレベルの対策に用いる。

(3) 検知に基づく暗号アルゴリズムレベルの対策技術の開発：レーザー照射検知信号をアルゴリズムレベルでの対策として利用する。暗号アルゴリズムとして、AES 暗号あるいは AES 暗号のラウンド関数を用いる。

(4) 対策技術の安全性評価：レーザーの検知から対策処理までの時間における情報漏洩のリスクについて、定量的に評価し、検知感度の調整や検知信号レベルの閾値の決定を行う。また、解析ツールとして故障感度解析をはじめとする最新の解析手法を取り入れる。

具体的な研究の方法は、次のとおりである。1)レーザー制御部と検知部に分けて、レーザーフォールト攻撃に対する安全性評価環境を構築する。2)レーザー照射時の基板電位変動の実測と検知手法の開発に向けて、センサ回路の物理的配置の条件を実験により明らかにし、レーザー光に対する基板応答モデルを構築する。また、フォールト検知センサを開発する。3)検知に基づく暗号アルゴリズムレベルの対策技術の開発に必要となる入力パラメータを整理し、情報

漏洩量をトータルで最小化できるアルゴリズムを開発する。4)対策技術の安全性評価として、作製したテスト IC チップの安全性を評価する技術を確立し、レーザーフォールト攻撃への耐性を評価する。

４．研究成果

4 つの研究項目に対して以下の成果が得られた。図 1 は、フォールト攻撃対策回路(レーザー検知センサ回路と電源遮断回路)で保護された AES 暗号を搭載したプロトタイプ IC チップである。

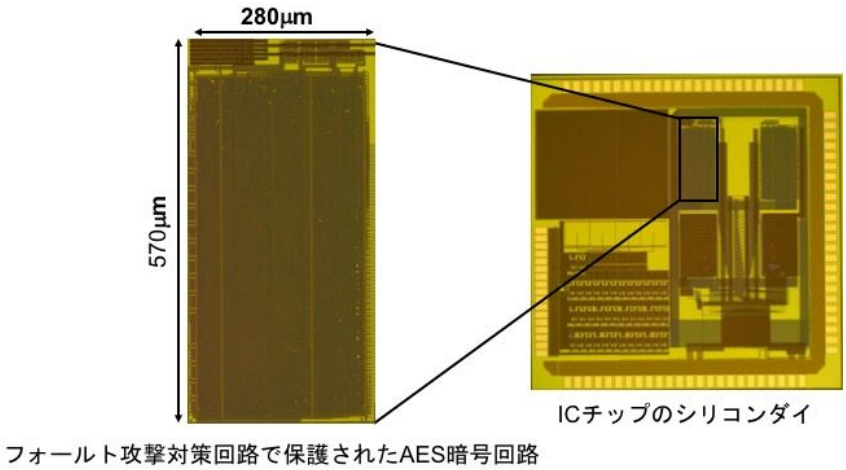

図 1 試作したプロトタイプ IC チップ

(1) レーザーフォールト攻撃の評価環境の構築：レーザー制御部とレーザー検知部を自動的に相互制御できる統合制御プログラムを開発した。この制御プログラムを用いて、レーザー制御部とレーザー検知部を同期・連動させ、レーザー照射時の基板電位変動分布データを収集した。用いたレーザー制御部の時空間分解能は 100 ピコ秒、1 マイクロメートルであった。さらに、プロトタイプ IC チップに対して、実際の攻撃を想定した実験が可能となる環境を構築した。これにより、情報漏えいの有無を定量的に評価できる解析環境を構築することができた。

(2) レーザー照射時の基板電位変動の実測と攻撃検知手法の開発：回路のレイアウト情報から情報漏洩量をシミュレートできる基板応答モデルを構築し、センサ配置位置の安全性に対する影響を評価した。項目(1)で構築した評価環境で得られた実測データに基づき、レーザー検知センサ回路の配置条件を明らかにした。基板応答モデルの妥当性と設計手法の最適性は、プロトタイプ IC チップに対するフォールト攻撃実験で確認することができた。

(3), (4) 検知に基づく暗号アルゴリズムレベルの対策技術の開発／対策技術の安全性評価：暗号回路の電源領域を独立させ、センサ回路による検知信号により電源遮断を行うことで、効果的な情報漏洩対策(暗号回路の中間値データを強制的に瞬時に揮発させる)が可能となる回路を開発し、プロトタイプ IC チップに搭載した。これにより、データの瞬時無効化を前提とする新しい暗号アルゴリズムが構築できるようになった。項目(1)において構築した評価環境を用いてプロトタイプ IC チップを評価した結果、当初の予想どおり、数ナノ秒程度で AES 回路の中間データが完全に無効化されていることが観測できた。従来の対策と比べて極めて短時間であり、情報漏洩対策として有効であることが実証できた。また、電源遮断時に漏洩する電磁波サイドチャネル情報を調べた結果、レーザー攻撃対策による副作用は見られなかった。

５．主な発表論文等

〔雑誌論文〕（計９件）

① Kohei Matsuda, Tatsuya Fujii, Natsu Shoji, Takeshi Sugawara, Kazuo Sakiyama, Yu-ichi Hayashi, Makoto Nagata, and Noriyuki Miura, “A 286 F²/Cell Distributed Bulk-Current Sensor and Secure Flush Code Eraser against Laser Fault Injection Attack on Cryptographic Processor,” IEEE Journal of Solid-State Circuits, Vol.53, No.11, pp. 3174-3182, 2018. (査読有).
DOI: 10.1109/JSSC.2018.2869142.

② Kohei Matsuda, Tatsuya Fujii, Natsu Shoji, Takeshi Sugawara, Kazuo Sakiyama, Yu-ichi Hayashi, Makoto Nagata, and Noriyuki Miura, “A 286F²/Cell Distributed Bulk-Current Sensor and Secure Flush Code Eraser Against Laser Fault Injection Attack,” Dig. Tech. Papers, 2018 IEEE Intl. Solid-State Circuits Conference (ISSCC’18), #21.5, pp.352-354, 2018. (査読有).

DOI: 10.1109/ISSCC.2018.8310329.

③ Takeshi Sugawara, Natsu Shoji, Kazuo Sakiyama, Kohei Matsuda, Noriyuki Miura, and Makoto Nagata, “Exploiting Bitflip Detector for Non-Invasive Probing and its Application to Ineffective Fault Analysis,” Proc. Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC’17), pp.49-56, 2017. (査読有).
DOI: 10.1109/FDTC.2017.17.

④ Kohei Matsuda, Noriyuki Miura, Makoto Nagata, Yu-ichi Hayashi, Tatsuya Fujii, and Kazuo Sakiyama, “On-Chip Substrate-Bounce Monitoring for Laser-Fault Countermeasure,” Proc. 2016 IEEE Asian Hardware-Oriented Security and Trust (AsianHOST'16), pp.1-6, 2016 (査読有).
DOI: 10.1109/AsianHOST.2016.7835565.

⑤ Yu-ichi Hayashi and Jong-Gwan Yook, “Introduction to a Special Session on EMC and Information Security,” Proc. URSI Asia-Pacific Radio Science Conference (URSI AP-RASC’16), pp.1275-1276, 2016 (査読有).
DOI: 10.1109/URSIAP-RASC.2016.7601329.

⑥ Kazuo Sakiyama, Reina Yagasaki, Takanori Machida, Tatsuya Fujii, Noriyuki Miura, and Yu-ichi Hayashi, “Circuit-Level Information Leakage Prevention for Fault Detection,” Proc. URSI Asia-Pacific Radio Science Conference (URSI AP-RASC’16), pp.1-4, 2016 (査読有).
DOI: 10.1109/URSIAP-RASC.2016.7601328.

⑦ Yu-ichi Hayashi, “State-of-the-art research on electromagnetic information security,” Radio Science, Vol.41, pp.1213-1219, 2016 (査読有).
DOI: 10.1002/2016RS006034.

⑧ Shugo Mikami, Dai Watanabe, and Kazuo Sakiyama, “A Performance Evaluation of Cryptographic Algorithms on FPGA and ASIC on RFID Design Flow,” Proc. International Conference on Information and Communication Technology (ICoICT’16), pp.1-6, 2016 (査読有).
DOI: 10.1109/ICoICT.2016.7571944.

⑨ Kazuo Sakiyama, Arisa Matsubara, and Takanori Machida, “Advanced fault analysis techniques on AES,” Proc. Joint IEEE International Symposium on Electromagnetic Compatibility and EMC Europe (EMC’15), pp.230-234, 2015 (査読有).
DOI: 10.1109/ISEMC.2015.7256164.

〔学会発表〕（計１８件）

① 菅原健, 庄司奈津, 崎山一男, 松田航平, 三浦典之, 永田真, “フォルト検出センサを悪用した非侵襲プロービング攻撃,” 2018 年暗号と情報セキュリティシンポジウム, 2018.

② 庄司奈津, 菅原健, 岩本貢, 崎山一男, “ブロック暗号へのプロービング攻撃における鍵復元効率の正確な評価モデル,” 2018 年暗号と情報セキュリティシンポジウム, 2018.

③ 郡義弘, 藤本大介, 林優一, 崎山一男, 三浦典之, 永田真, “IC 内部の回路構成変更が秘密鍵の取得性に与える影響の評価,” 情報・システムソサエティ特別企画学生ポスターセッション, 2018.

④ 郡義弘, 藤本大介, 林優一, 三浦典之, 永田真, 崎山一男, “レーザーフォールト攻撃対策である電源遮断回路実装時のサイドチャネル耐性評価,” ハードウェアセキュリティ研究会, 2018.

⑤ Natsu Shoji, Ryuga Matsumura, Takeshi Sugawara, and Kazuo Sakiyama, “An Evaluation of Ineffective Fault Analysis on AES using Single-Bit Bit-Set/Reset Faults,” The 12th International Workshop on Security (IWSEC'17) Poster Session, 2017.

⑥ Kohei Matsuda, Noriyuki Miura, Makoto Nagata, “Laser fault injection attack countermeasure by abnormal substrate potential bounce monitoring,” The 16th International Conference on Computers, Communications, and Systems (ICCCS 2017), 2017.

⑦ 庄司奈津, 松村竜我, 菅原 健, 崎山一男, “ 誤り暗号文を使わない AES への故障利用攻撃, ” ハードウェアセキュリティ研究会, 2017.

⑧ Kazuo Sakiyama, “Who Will Fault Sensors be Helpful for? ” COSIC Seminar (招待講演), 2017.

⑨ 菅原健, “サイドチャネル攻撃と対策,” 2017 年電子情報通信学会ソサイエティ大会・チュートリアルセッション(招待講演), 2017.

⑩ 松田航平, 三浦典之, 永田真, 林優一, 藤井達哉, 崎山一男, “基板電流検知回路を用いたレーザーフォールト注入攻撃対策のオーバヘッド推定,” 電子情報通信学会総合大会, 2017.

⑪ 三上修吾, 崎山一男, “プライバシ保護可能な認証プロトコルの RFID タグ実装と性能評価,” ハードウェアセキュリティフォーラム 2016, 2016.

⑫ 松田航平, 三浦典之, 永田真, 林優一, 藤井達哉, 崎山一男, “基板電位変動モニタリングによるレーザーフォールト注入攻撃対策,” 電子情報通信学会ソサイエティ大会, 2016.

⑬ 松田航平, 三浦典之, 永田真, 林優一, 藤井達哉, 矢ヶ崎玲奈, 崎山一男, “基板電位変動モニタリングによるレーザーフォールト注入攻撃対策,” LSI とシステムのワークショップ 2016, 2016.
⑭ Kazuo Sakiyama, “Foundations of Secure Scaling -- Double Arbiter PUF and Security Evaluation Using Deep Learning,” Dagstuhl Seminar 16342 (招待講演), 2016.
⑮ 松田航平, 三浦典之, 永田真, 林優一, 藤井達哉, 矢ヶ崎玲奈, 崎山一男, “レーザーフォールト注入時の IC 基板電位変動のオンチップ測定,” 2016 年暗号と情報セキュリティシンポジウム (SCIS2016), 2016.
⑯ 林優一, 本間尚文, 青木孝文, 曽根秀昭, “漏えい電磁波を用いたタブレット端末における入力キーの取得とその対策,” 第 38 回情報理論とその応用シンポジウム (SITA2015), 2015.
⑰ Yang Li and Kazuo Sakiyama, “Review Fault Attacks on ECC Implementations with Fault Sensitivity Analysis,” IEEE Asian Solid-State Circuits Conference 2015, (A-SSCC ’15) (招待講演), 2015.
⑱ Yu-ichi Hayashi, “Introduction to on EM Information Leakage from Information and Communication Devices,” URSI-Japan Radio Science Meeting (招待講演), 2015.

〔図書〕（計２件）
① 一般社団法人 電気学会・電気システムセキュリティ特別技術委員会, “IoT 時代の電磁波セキュリティ ~21 世紀の社会インフラを電磁波攻撃から守るには~, 分担執筆, 崎山一男, 林優一, 付録 B 暗号モジュールを搭載したハードウェアからの情報漏えいの可能性の検討,” pp.302-309, 科学情報出版, 2018.
ISBN 978-1-118-66001-0.
② Kazuo Sakiyama, Yu Sasaki, Yang Li, “Security of Block Ciphers: From Algorithm Design to Hardware Implementation,” 320 pages, Wiley, 2015.
ISBN 978-1-118-66001-0.

〔産業財産権〕
○出願状況（計０件）

○取得状況（計０件）

〔その他〕
ホームページ等
http://sakiyama-lab.jp/study/

６．研究組織

(1)研究分担者
研究分担者氏名：林 優一
ローマ字氏名：(HAYASHI, Yu-ichi)
所属研究機関名：奈良先端科学技術大学院大学
部局名：先端科学技術研究科
職名：教授
研究者番号（8 桁）：６０５５１９１８

研究分担者氏名：三浦 典之
ローマ字氏名：(MIURA, Noriyuki)
所属研究機関名：神戸大学
部局名：システム情報学研究科
職名：准教授
研究者番号（8 桁）：７０６５０５５５

研究分担者氏名：菅原 健
ローマ字氏名：(SUGAWARA, Takeshi)
所属研究機関名：電気通信大学
部局名：大学院情報理工学研究科

職名：准教授
研究者番号（8桁）：６０７８５２３６

研究分担者氏名：李 陽
ローマ字氏名：(LI, Yang)
所属研究機関名：電気通信大学
部局名：大学院情報理工学研究科
職名：准教授
研究者番号（8桁）：２０８２１８１２

(2)研究協力者
研究協力者氏名：フェルバーウェーデ イングリッド
ローマ字氏名：(VERBAUWHEDE, Ingrid)

研究協力者氏名：ダンジェ ジャンルック
ローマ字氏名：(DANGER, Jean-Luc)

研究協力者氏名：バシーン シバム
ローマ字氏名：(BHASIN, Shivam)