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　　８　月　　２　日現在

機関番号：　１４５０１
研究種目：　基盤研究(A)（一般）
研究期間：　2014～2016
課題番号：　２６２４０００５

研究課題名（和文）暗号ＶＬＳＩの電磁波セキュリティを確保するサイドチャネル攻撃センサの構成法と実証

研究課題名（英文）Development of Side-Channel Attack Sensing Techniques and Prototyping toward Electromagnetic Security of Cryptographic VLSI Circuits

研究代表者

永田　真（Nagata, Makoto）

神戸大学・科学技術イノベーション研究科・教授

研究者番号：４０２７４１３８

交付決定額（研究期間全体）：（直接経費）　　32,700,000円

研究成果の概要（和文）：サイドチャネル攻撃への耐性を有し、高度に電磁波セキュリティを保証する暗号VLSI技術を確立した。具体的には、(1)暗号コア近傍に接近する電磁界マイクロプローブをオンチップで検知するサイドチャネル攻撃センサの回路技術、(2)暗号コア近傍における電磁界マイクロプローブとサイドチャネル攻撃センサの結合の電磁界シミュレーション及びセンサ回路の動作シミュレーション手法、(3)暗号コアから漏洩するサイドチャネル情報を用いて暗号コアを認証・真正性を確認する技術の開発に成功した。また、半導体集積回路の試作チップを用いたプロトタイプシステムを構築し、研究成果の効果を実証した。

研究成果の概要（英文）：Cryptographic VLSI techniques have been established for assuring electromagnetic security with remarkably high tamper resistance against side-channel attacks. Three research items include: (1) On-chip detection of the proximate placement and approach of electromagnetic micro probes as the side-channel attack sensing technique, (2) integrated simulation techniques of electromagnetic coupling between the electromagnetic micro probe and on-chip side-channel sensors and also circuit operations, (3) positive usage of side-channel information for the authentication of cryptographic cores. These research items have been successfully completed and demonstrated with the fabricated integrated-circuit (IC) chips and prototype systems.

研究分野：　集積回路設計工学

キーワード：　サイドチャネル攻撃センサ　サイドチャネル攻撃無効化　サイドチャネル攻撃耐性　電磁波セキュリティ　ハードウェアセキュリティ　暗号モジュール　ICカード　情報漏えい

１．研究開始当初の背景

近年、個人情報の保護や高信頼な電子商取引への要求に伴い、暗号モジュール（暗号処理を実行する LSI 回路）の応用が急速に拡大しており、携帯電話の SIM カードや RFID など演算リソースの制限された組込み機器では暗号処理のハードウェア化による高速化・省電力化が強く求められている。一方、暗号モジュールの実装の脆弱性を利用して秘密情報を奪う実装攻撃の脅威が指摘されている。 特に演算中の消費電力や放射電磁波といった漏洩情報を観察することで秘密情報を奪うサイドチャネル攻撃は、その攻撃能力の高さと実現の容易さから、現実的な脅威と言われている。しかし、現状ではサイドチャネル攻撃に対して汎用的かつ低オーバーヘッドで効果を発揮する決定的な対策技術は確立していない。一般に、対策技術は乱数によって中間値を遮蔽するマスキングと中間値を隠ぺいするハイディングが基本とされ、これまでアルゴリズムやロジックレベルで数多く提案されているが、効果があると確認された従来対策は、少なくとも回路規模にして数倍程度増加することが知られている。そのため、回路面積や消費電力が厳しく制限される組込み機器には向いていない。さらに近年、スタンダードセルの動作の非対称性を利用した従来対策を全て無効化する局所的な電磁波解析攻撃の可能性が報告されており、そうした攻撃への耐性を有する組込み用途向け暗号モジュールの設計技術の確立が世界的に急務となっている。

２．研究の目的

電磁波解析攻撃時にマイクロプローブを対象に接近させると、不可避的に回路近傍の電磁界が乱れるという環境電磁工学的な着想から、これまでに培ってきた上記技術を融合・深化し、LSI 近傍の電磁界をオンチップで高感度に計測可能なサイドチャネル攻撃センサを開発する（図 1）。さらに、暗号工学の知見に基づき、多様なサイドチャネル攻撃シナリオに対応できる、同センサを核とした対策技術を開拓する。

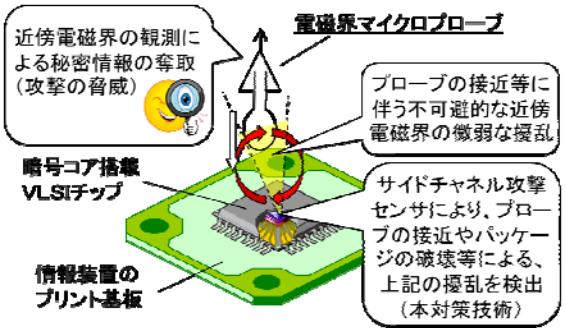

図 1: サイドチャネル攻撃センサによる攻撃検知と対策の概念図。

３．研究の方法

本研究では、サイドチャネル攻撃への耐性を有する暗号 VLSI 技術の確立を目指し、集積回路工学、環境電磁工学、暗号工学の学際連携のもとで以下の 3 つの研究項目を推進する。すなわち、

(1) サイドチャネル攻撃センシング手法の開発
(2) 電磁波セキュリティ対策技術の開発
(3) 多様なサイドチャネル攻撃シナリオに対応した対策技術の開発

である。

環境電磁工学的には電磁波解析攻撃による電磁界の乱れから攻撃を検知できるという着想に基づき、従来に無い対策手法として、サイドチャネル攻撃センサを開発する。誘導結合型 LC 発振器を基本要素とした小型かつデジタル処理との親和性の高いセンサ回路構成により、局所的な電磁波解析攻撃を検出・無効化できるだけでなく、 暗号コアに対してわずか数パーセントの面積・電力オーバーヘッドで実現することを狙う。従来のアルゴリズム・ロジックレベルの対策（少なくとも消費電力 4 倍程度）を大きく上回る効率になると予想され、これまでの対策方式を根本から置き換えるほどの優位性を有する。

研究項目(1)では、サイドチャネル攻撃センサを具体する集積回路を研究開発し、プロトタイプシステムを構築する。

研究項目(2)では、サイドチャネル攻撃センサと電磁波解析攻撃の物理的な相互作用を集積回路チップ及びその近傍の電磁界シミュレーションにより解析し、電磁波セキュリティ対策の方針と有効性を確認する。

研究項目(3)では、サイドチャネル攻撃の多様性を暗号工学の立場から検証し、本研究の成果を最大に活用するべく、検知と防御および応用のシナリオを構築する。

本研究の実施体制についてまとめる。

研究代表者（神戸大学）のグループは、VLSI システムにおける電源ノイズおよび電磁ノイズの発生・伝搬・干渉に関する体系的な研究成果を有しており、高分解能のオンチップ・ノイズセンサ技術や高精度のノイズシミュレーション技術を本研究の基盤とする。

研究分担者（東北大学）のグループは、暗号 VLSI における電磁環境両立性(EMC)に関して、実験と理論の両面から研究を推進し、これまでに近傍および遠方の電磁界変動（電磁ノイズ）に秘密鍵などの暗号情報が重畳していることを明らかにしている。

研究分担者（電気通信大学）のグループは、暗号アルゴリズムの VLSI 実装により生ずる物理的な脆弱性の解明について暗号理論に立脚した研究を推進しており、これまでに暗号コアのサイドチャネル攻撃やフォールト注入攻撃の理論モデルの構築と実験実証の成果を有している。

加えて、暗号学分野で歴史のある仏国にお

いて、暗号実装と VLSI 設計技術について顕著な研究実績を有する Telecom Paristech の研究者と研究協力体制を構築し、当該分野の世界的な研究開発動向における本研究の取組みおよび研究成果の優位性について議論するとともに、大学院生等の人材交流を進める。

４．研究成果

本研究における三つの研究課題に関する研究成果概要を、下記にまとめる。なお、本研究課題による研究成果をエレクトロニクス分野の英文専門誌にレビュー論文としてまとめ、オープンアクセスにより広く周知した（主な発表論文等・雑誌論文の①）

(1) サイドチャネル攻撃センシング手法の開発

LC 発振回路を用いたセンサ設計指針を導出し、初期のプロトタイプチップを開発した。サイドチャネル攻撃の実験環境を構築し、電磁界マイクロプローブが暗号コアから 0.1 mm 以内に接近した場合に、LC 発振回路の周波数が 1%以上変化することにより有意に検知できることを示した。開封された状態の IC チップにおけるサイドチャネル攻撃を検知できることから、例えば IC カードにおける秘密情報の不正な覗き見を防止できると考えられる。サイドチャネル攻撃センサのイメージを図 2 に示す。

本研究初期のプロトタイプシステム（図 3）による測定結果を図 4 に示す。攻撃者によるマイクロプローブが集積回路チップ上の暗号コアのおよそ 0.1 mm 程度まで近接した場合に、センサ出力信号の発振周波数が数%と大きく変化し、これにより攻撃を検知している。

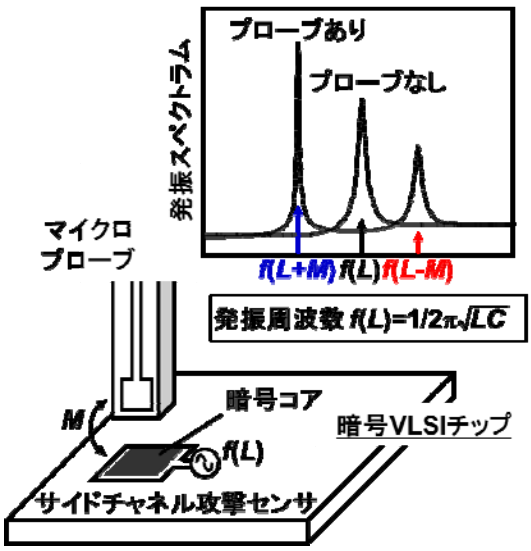

図 2: サイドチャネル攻撃センサの基本構成と攻撃検知における応答（イメージ）。

これらの研究成果について、当該分野において最重要と位置づけられる国際会議*1 で発表し、また最優秀論文賞*2 を受賞した。

*1 IEEE Symposium on VLSI Circuits 2014.

*2 IACR CHES 2014 Best paper award.

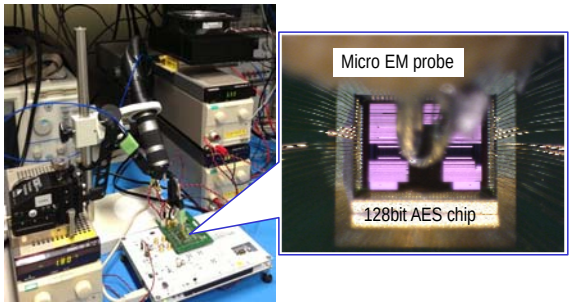

図 3: プロトタイプシステム（写真）

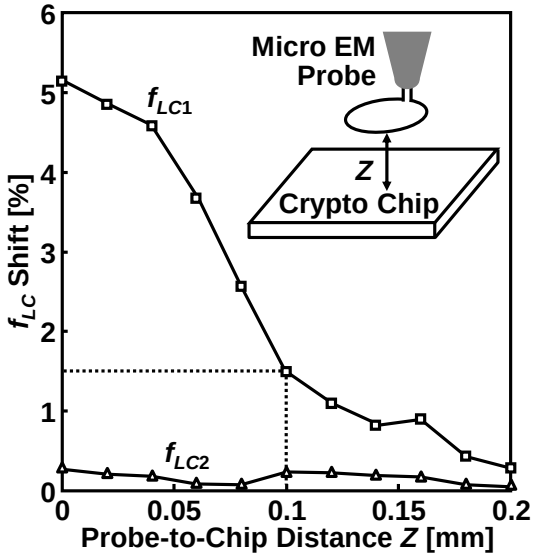

図 4: サイドチャネル攻撃センサの攻撃検知特性（プロトタイプシステムによる実測）。

続いて、サイドチャネル攻撃センサ基本回路を利用して、攻撃者が暗号 VLSI に接近させるマイクロプローブの検知距離を 0.5 mm 程度まで延伸する（前項に比べて 5 倍の遠距離に相当する）センサ信号処理法を考案し、プロトタイプシステムにより実証した。

さらに、サイドチャネル攻撃センシングの検知性能の向上に向けた基本構造の再検討も進めた。すなわち、金属探知機の原理をマイクロスケールに縮小応用することで、誘導平衡状態の二つの発振器方コイルを具備する新しいセンサ回路を考案・具体化し、攻撃者によるマイクロプローブの検知距離を 0.5 mm 程度まで延伸できることを確認した。基本回路に比べて 5 倍程度大きく、またセンサ信号処理による手法と同等以上の効果を達成した。

(2) 電磁波セキュリティ対策技術の開発

本センサを核とした電磁波セキュリティ対策技術について、AES 暗号コアを例題とし

た攻撃検出シナリオと暗号無効化アルゴリズム、および IC チップ上での温度やデバイスばらつきに対するセンサ検知特性の較正方法について考察した。また、本センサと周辺磁界との相互作用について、電磁界シミュレーション環境を構築し、解析を進めた。センサの検知コイルと攻撃者のマイクロプローブの形状や空間相対位置などが検知性能に及ぼす大局的な影響について考察し、プロトタイプシステムに搭載されたテストチップの設計データを例題としてシミュレーションにより確認するとともに、検知性能を改善するための設計指針について研究を進めた。サイドチャネル攻撃シナリオに関して、暗号分野で世界的に権威のある学術論文誌*3 に掲載決定した。

センサ基本回路を核として、マイクロプローブによるセンサ近傍の磁界の擾乱を解析する電磁界シミュレーション手法及び検知回路の動作シミュレーション手法を確立した。暗号コアとセンサ回路を並列動作することにより、マイクロプローブの接近検知にかかる遅延時間を大幅に短縮する動作モードの可能性を、検知性能の視点から見出し、また暗号コアにより攻撃を早期無効化するシナリオを検証した。

*3 IACR Journal of Cryptology.

(3) 多様なサイドチャネル攻撃シナリオに対応した対策技術の開発

多様なサイドチャネル攻撃シナリオに対応した対策技術の開発について、暗号工学の立場から暗号コアに対する攻撃検出シナリオを一般化した。とりわけ、AES 暗号コアを例題として、暗号コアそのものの存在や動作がサイドチャネル攻撃センシングには大きく影響しないことを明らかにした。さらに、暗号 VLSI システムのサイドチャネル漏洩を低減する電源回路の構成法やサイドチャネル情報を利用することでセキュリティ性能を向上する暗号利用法について研究を進めた。また、暗号コアから漏洩するサイドチャネル情報を用いて暗号コアを認証する「サイドチャネル認証システム」を新たに提案し、暗号コアの計算処理に伴うサイドチャネル情報を用いることにおり、暗号コアを搭載するセキュリティ VLSI チップの真正性を高精度に確認できることを示した。

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２１件（うち査読有２０件））

① Daisuke Ishihata, Naofumi Homma, Yu-ichi Hayashi, Noriyuki Miura, Daisuke Fujimoto, Makoto Nagata, Takafumi Aoki, “Enhancing Reactive Countermeasure against EM Attacks with Low Overhead,” in Proc. The 2017 IEEE International Symposium on Electromagnetic Compatibility (EMC 2017), accepted.（査読有）

② Makoto Nagata, Daisuke Fujimoto, Noriyuki Miura, Naofumi Homma, Yu-ichi Hayashi, Kazuo Sakiyama, "Protecting cryptographic integrated circuits with side-channel information (Review paper)," IEICE Electronics Express(ELEX), Vol. 14 No. 2 pp. 1-13, Feb. 2017.（査読有）
DOI: 10.1587/elex.14.20162005.

③ Wei He, Jakub Breier, Shivam Bhasin, Noriyuki Miura, Makoto Nagata, "Ring Oscillator Under Laser: Potential of PLL Based Countermeasure Against Laser Fault Injection," Proc. IEEE 2016 Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC 2016), #4.2, pp. 102-113, Aug. 2016.（査読有）
DOI: 10.1109/FDTC.2016.13.

④ Yu-Ichi Hayashi, “State-of-the-art research on electromagnetic information security (Invited),” Radio Science, Vol. 41, pp. 1213-1219, July 2016.（査読有）
DOI: 10.1002/2016RS006034.

⑤ Noriyuki Miura, Zakaria Najm, Wei He, Shivam Bhasin, Xuan Thuy Ngo, Makoto Nagata, Jean-Luc Danger, "PLL to the Rescue: A Novel EM Fault Countermeasure," Proc. 2016 53rd ACM/EDAC/IEEE Design Automation Conference (DAC 2016), #57.5, pp. 1-6, June 2016.（査読有）
DOI: 10.1145/2897937.2898065.

⑥ Kazuo Sakiyama, Momoka Kasuya, Takanori Machida, Arisa Matsubara, Yunfeng Kuai, Yu-Ichi Hayashi, Takaaki Mizuki, Noriyuki Miura, Makoto Nagata, "Physical Authentication Using Side-Channel Information," Proc. IEEE International Conference on Information and Communication Technology (ICoICT 2016), May 2016.（査読有）
DOI: 10.1109/ICoICT.2016.7571953.

⑦ Naofumi Homma, Yu-ichi Hayashi, Takafumi Aoki, Noriyuki Miura, Daisuke Fujimoto, Makoto Nagata, "Design Methodology and Validity Verification for a Reactive Countermeasure Against EM Attacks," IACR Journal of Cryptology, pp. 1-19, Online, Dec. 2015.（査読有）
DOI: 10.1007/s00145-015-9223-3.

⑧ Noriyuki Miura, Daisuke Fujimoto, Makoto Nagata, "Proactive and Reactive Protection Circuit Techniques Against EM Leakage and Injection," Proc. Joint IEEE International Symposium on Electromagnetic Compatibility and EMC Europe (EMC 2015), #SS-1-7, pp. 252-257,

Aug. 2015.（査読有）
DOI: 10.1109/ISEMC.2015.7256168.

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

⑩ Noriyuki Miura, Daisuke Fujimoto, Makoto Nagata, Naofumi Homma, Yuichi Hayashi, Takafumi Aoki, "EM Attack Sensor: Concept, Circuit, and Design-Automation Methodology (Invited)," Proc. ACM Design Automation Conference 2015 (DAC 2015), #69.2, pp. 1-6, June 2015.（査読有）
DOI: 10.1145/2744769.2747923.

⑪ Kohki Taniguchi, Noriyuki Miura, Taisuke Hayashi, Makoto Nagata, "At-Product-Test Dedicated Adaptive Supply-Resonance Suppression," Proc. 2015 IEEE 33rd VLSI Test Symposium (VTS 2015), #06A-1, pp. 127-130, May. 2015.（査読有）
DOI: 10.1109/VTS.2015.7116273.

⑫ 永田真, "IC チップの真正性の確保と対策 -ハードウェアセキュリティの根源的課題に向き合う-," IEICE Fundamentals Review, Vol. 8 No. 3 pp. 177-182, Jan. 2015.
DOI:10.1587/ESSFR.8.177.（査読無）

⑬ Naofumi Homma, Yu-ichi Hayashi, Noriyuki Miura, Daisuke Fujimoto, Daichi Tanaka, Makoto Nagata, Takafumi Aoki, "EM Attack Is Non-Invasive? -- Design Methodology and Validity Verification of EM Attack Sensor," IACR Workshop on Cryptographic Hardware and Embedded Systems 2014 (CHES 2014), #1-1, LNCS 8731, pp. 1-16, Sep. 2014.（査読有）
DOI: 10.1007/978-3-662-44709-3_1.

⑭ Noriyuki Miura, Daisuke Fujimoto, Yu-ichi Hayashi, Naofumi Homma, Takafumi Aoki, Makoto Nagata, "Integrated-Circuit Countermeasures Against Information Leakage Through EM Radiation," Proc. 2014 IEEE Intl. Symp. on Electromagnetic Compatibility, #TH-AM-3-3, pp. 748-751, Aug. 2014.（査読有）
DOI: 10.1109/ISEMC.2014.6899068.

⑮ Noriyuki Miura, Daisuke Fujimoto, Daichi Tanaka, Yu-ichi Hayashi, Naofumi Homma, Takafumi Aoki, Makoto Nagata, "A Local EM-Analysis Attack Resistant Cryptographic Engine with Fully-Digital Oscillator-Based Tamper-Access Sensor," IEEE 2014 Symposium on VLSI Circuits, Dig. Tech. Papers, #16.4, pp. 172-173, June 2014. 査読有）
DOI: 10.1109/VLSIC.2014.6858423.

⑯ Daisuke Fujimoto, Daichi Tanaka, Noriyuki Miura, Makoto Nagata, Yu-ichi Hayashi, Naofumi Homma, Shivam Bhasin, Jean-Luc Danger, “Side-Channel Leakage on Silicon Substrate of CMOS Cryptographic Chip,” in Proceedings of the 2014 IEEE International Symposium on Hardware-Oriented Security and Trust (HOST 2014), pp. 32-37, May 2014.（査読有）
DOI: 10.1109/HST.2014.6855564.

〔学会発表〕（計３１件（うち招待１１件））

① 永田真、「IC チップのハードウェアセキュリティ：真正性の確保と攻撃への対策（招待講演）」、2016 IEEE Metro Area Workshop in Kansai, 2016.8.3.

② Naofumi Homma, “Side-Channel-Aware Circuit Design: Prevention and Detection of Side-Channel Attacks (Invited),” 2016 IEEE Intl. Solid-State Circuits Conference (ISSCC 2016), Forum, 2016.1.31.

③ Naofumi Homma, “Recent Topics on Hardware Security (Invited),” 2015 Intl. Workshop on Information and Communication Security, 2015.12.9.

④ Yang Li, Kazuo Sakiyama, “Review Fault Attacks on ECC Implementation with Fault Sensitivity Analysis (Invited),” IEEE Asian Solid-State Circuits Conference 2015 (A-SSCC 2015), 2015.11.10.

⑤ Makoto Nagata, "IC Chips to be Dependable, Secure, and Robust (Plenary)," International Technical Conference on Circuits/Systems, Computers and Communications 2015 (ITC-CSCC 2015), 2015.7.1

⑥ Makoto Nagata, "Securing Cryptographic Engines ? Circuit Techniques against EM Attacks (Invited)," International Symposium on IoT Enabling Chips, 2015.6.20.

⑦ Makoto Nagata, "IC Chips to Be Dependable, Secure, and Robust (Invited)," VirginiaTech, CESCA Day 2015, 2015.5.2.

⑧ Makoto Nagata, "Side Channel Leakage in Cryptographic Modules: Introduction to Physical Origins and Attack Models (Tutorial)," 20th Asia and South Pacific Design Automation Conference (ASP-DAC 2015), 2015.1.19.

⑨ Kazuo Sakiyama, “Fault Analysis for Cryptosystems: Introduction to Differential Fault Analysis and Fault Sensitivity Analysis (Tutorial)," 20th Asia and South Pacific Design Automation Conference (ASP-DAC 2015), 2015.1.19.

〔図書〕（計１件）

① Kazuo Sakiyama, Yu Sasaki, Yang Li, “Security of Block Ciphers: From Algorithm Design to Hardware

Implementation,” 320 pages, Wiley, 2015.

〔産業財産権〕
なし

〔その他〕
なし

６．研究組織
(1)研究代表者
永田　真 (NAGATA, Makoto)
神戸大学・大学院科学技術イノベーション研究科・教授
研究者番号：４０２７４１３８

(2)研究分担者
三浦　典之 (MIURA, Noriyuki)
神戸大学・システム情報学研究科・准教授
研究者番号：７０６５０５５５

本間　尚文 (HOMMA, Naofumi)
東北大学・電気通信研究所・教授
研究者番号：００３４３０６２

林　優一 (HAYASHI, Yu-ichi)
東北学院大学・工学部・准教授
研究者番号：６０５５１９１８

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

(3)連携研究者
なし

(4)研究協力者
Jean-Luc Danger
Telecom Paristech, Professor