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　 ６ 月　 ４ 日現在

機関番号：１３７０１
研究種目：若手研究(B)
研究期間：2012～2014
課題番号：２４７６０２７４

研究課題名（和文）セキュアかつ低消費電力な断熱的論理回路の設計

研究課題名（英文）LSI design of secure and low-power adiabatic logic

研究代表者
高橋　康宏（Takahashi, Yasuhiro）

岐阜大学・工学部・准教授

研究者番号：００４０２２１４

交付決定額（研究期間全体）：（直接経費）　　2,700,000円

研究成果の概要（和文）：高セキュリティな断熱的論理回路は、差動入力論理が電流ばらつきが少なくなることが分かった。この結果をふまえ、新しい断熱的論理回路CSSALを提案した。提案した論理回路CSSALを使用し、暗号回路で良く使用されるガロア体乗算器とSboxを集積回路実装したところ、提案回路による集積回路は、従来回路よりも1/10の低電力特性を示し、電流ばらつきは1/5となった。これらのことより、提案回路は暗号用論理回路として有望な回路であるといえる。

研究成果の概要（英文）：This research proposes a new adiabatic logic which is named as Charge Sharing Symmetric Adiabatic logic (CSSAL). The comparison results of individual logics have shown that the proposed CSSAL circuit exhibits low and uniform peak supply current traces for all dual-input transistors, which performs its logic immunity for side-channel attacks. The designed Galois field multiplier and 8bit-Sbox LSIs have ultra low-power dissipation characteristics compared with the conventional LSIs. From the basis of the simulation and measurement results, we assures that the proposed logic has potential applicability for low-power and secure low frequency devices, such as in IC card, RFID tags, and/or wireless sensors.

研究分野：集積回路設計

キーワード：断熱的論理　セキュア　AES

１．研究開始当初の背景

非接触 IC カードなどのスマートカードは、その利便性から電子決済・個人認証手段として拡がりを見せている。一方で、利便性と安全性を両立させるためは、セキュリティ強化が重要な技術課題となる。スマートカード用にハードウェア実装された IC への攻撃手法のひとつに、処理時間、消費電力、電磁波などから漏れ出た情報を読み取るサイドチャネル攻撃がある。IC が内部情報を暴露する要因は、暗号回路に用いられる論理回路の電流値が変動するためである。したがって、論理演算をマスクする素子を用いて電流変動を抑える、ノイズを付加し変動を見えにくくする、などの対策が考えられる。しかし、これらの対策は回路規模と消費電力の増大を招くことから、電源供給が限られているスマートカードでは実現的といえない。そこで、電流変動が極めて少ない論理回路を設計すれば、攻撃に強い論理回路として普及し、より高セキュリティなスマートカードとなる。この電流変動が少ない論理回路の候補のひとつが、断熱的論理回路であり、研究代表者は以前より研究を進めてきた。断熱的論理回路は、低電力化の回路構成法「断熱充電理論」に基づく。具体的には、(a)一定の傾きで増減を繰り返す電圧を用いて回路を駆動し、オン抵抗の熱的損失を抑える。(b)電圧保持容量の充放電を緩やかにし、電荷を電源に再充電することでエネルギーの再利用を行う、技術のことで、極めて低消費電力の論理動作が実現できる。

２．研究の目的

本研究は、断熱的論理回路は周期波電源で駆動することから、ワイヤレス給電の交流電力に着目し、スマートカード内の IC を直接駆動することで、従来必要としていた交流/直流変換回路を省き、より低消費電力なワイヤレス給電システムを構築できると考えた。よって、この研究課題では、以下のことを明らかにすることを目的とした。

(1) 従来の断熱的論理回路群の電流変動について、シミュレーションにて評価する。
(2) 回路構造の違いにより、電流変動にどのような影響があるかを明らかにする。
(3) 高セキュリティな断熱的論理回路を提案、暗号回路を実装してその電流変動の様子を明らかにする。

３．研究の方法

(1) 回路構造と消費電力の相関関係の解析：断熱的論理回路の回路構造には、シングルエンド入力と差動入力とに分類される。回路構造によって、シングルエンド入力、差動入力回路は、消費エネルギーに差が生じる。そこで、回路構造と消費電力にはどのような相関関係があるのかを回路シミュレーションより解析し、その要因を明らかにする。
(2) 周期波電源の違いによる消費電力評価：台形波、三角波、正弦波などの波形形状により、断熱的論理回路の消費電力が異なることから、シミュレーションにより消費電力を解析し、最も適した電源波形を決定する。
(3) 差分電力解析による回路構造評価：差分電力解析は、消費電力を繰り返し測定し統計処理することで、秘密情報を推測する手法である。これは、入力が変化する時の論理回路の消費電力ばらつきが主要因である。そこで、論理回路の回路構造が消費電力ばらつきにどのように影響するかを回路シミュレーションにて解析する。
(4) ピーク電流と電源の相関関係：入力遷移と電源の周期タイミングは断熱的論理回路の動作に重要な要因であり、タイミングがずれると大きなピーク電流が回路に流れる。そこで、ピーク電流と電源にはどのような相関関係があるのかを回路シミュレーションより確認する。
(5) 0.18 μmCMOS プロセスによる回路設計：暗号回路を本研究で提案するセキュア断熱的論理回路を用いて集積回路の設計を設計・計測し、提案型セキュア断熱的論理回路の有用性を確認する。

４．研究成果

(1) 回路構造の違いによる電流変動を回路シミュレーションにより確認したところ、差動入力回路が電流変動の少ない回路であることがわかった。この結果をふまえ、図 1 に示す新しい回路(Charge Sharing Symmetric Adiabatic logic、CSSAL)を提案した。この回路は、従来の差動論理回路で使用されている MP2 および MN2 からなるインバータと MP3 と MN1 からなるインバータで構成されるフリップフロップ回路と差動入力を制御するための NMOS スイッチ MN5 および MN6 に電源を制御するための PMOS スイッチ MP1、グランド信号を制御するための NMOS スイッチ MN8, すべての節点の等価負荷容量を均一化するための NMOS スイッチ MN7 からなる。この回路において、低消費電力化は Eval 信号により、入力信号遷移時の電流変動の均一化は、Disch 信号により達成できる。
(2) 図 2 は、従来の暗号用断熱的差動論理回路群(2N-2N2P、ECRL、SAL、および、SyAL)と本提案回路の電流変動の回路シミュレーション比較を示したものである。図より、本提案回路は、電流のピーク値が従来回路よりも低く、また、電流の変動も少ないことが分かる。一般に, 断熱論理回路のピーク電流は、従来の CMOS 論理回路のそれよりも低くなる。よって、暗号モジュールでよく利用される TDPL

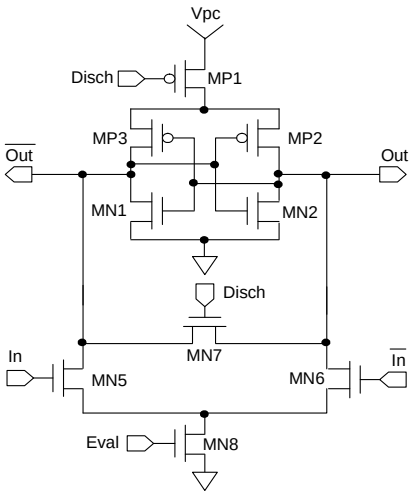

図 1 提案回路 CSSAL

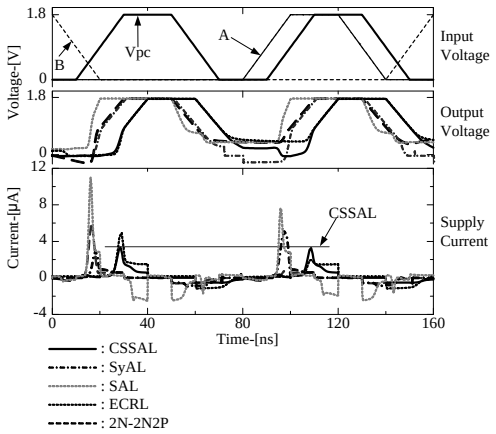

図 2 提案回路と従来回路の
電流変動の様子

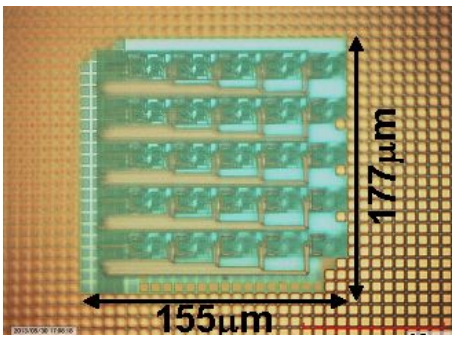

図 3 CSSAL 乗算器 LSI のチップ写真

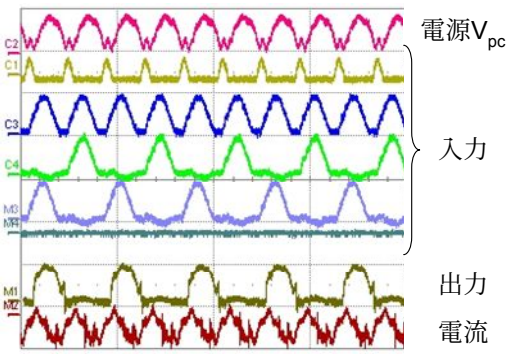

図 4 測定結果(1.25 MHz 動作時)

や WDDL よりも本提案回路は著しい電流ピーク低減を達成できる。

(3) IC 試作した乗算回路(図 3)は、4MHz の周波数で動作することを確認し、また消費電力は 1.13μW であった。これは、従来の論理回路と比較した場合、1/10 以下の電力であることがわかった。また、提案回路の電流ピークは均一性を示し、従来回路よりも 1/5 以下の変動であることを確認した。これらのことより、提案回路は高セキュリティな回路であるといえる。

5．主な発表論文等

〔雑誌論文〕（計６件）

① C. Monteiro, Y. Takahashi, and T. Sekine, Low-power secure S-Box circuit using CSSAL for AES hardware design, IET Circuits, Devices & Systems, 2015 (採録決定).

② C. Monteiro, Y. Takahashi, and T. Sekine, Low power bit-parallel cellular multiplier implementation in secure dual-rail adiabatic logic, IACSIT International J. Modeling and Optimization, vol.3, no.4, pp.329-332, Aug. 2013.

③ C. Monteiro, Y. Takahashi, and T. Sekine, Charge-sharing symmetric adiabatic logic in countermeasure against power analysis attacks at cell level, Microelectronics Journal, vol.44, no.6, pp.496-503, June 2013.

④ 高橋康宏, 佐藤比佐夫, オフチップ共振回路を用いた断熱的論理用低消費電力電源回路, 電気学会論文誌 C, vol.133, no.2, pp.250-255, Feb. 2013.

⑤ N.A. Nayan, Y. Takahashi, and T. Sekine, The ramped-step voltage in adiabatic logic circuits: analysis of parameters to further reduce power dissipation, Research J. of Applied Sciences, Engineering and Technology, vol.5, no.1, pp.114-117, Jan. 2013.

⑥ N.A. Nayan, Y. Takahashi, and T. Sekine, LSI implementation of a low-power 4×4-bit array two-phase clocked adiabatic static CMOS logic multiplier, Microelectronics Journal, vol.43, no.4, pp.244-249, April 2012.

〔学会発表〕（計２０件）

① C. Monteiro, 高橋康宏, 関根敏和, Security evaluation of CSSAL countermeasure against side-channel attacks using frequency spectrum analysis, 信学技報, vol.114, no.381, EMCJ2014-82, pp.75-80, 2014 年 12 月 19 日, 静岡大学, 浜松市.

② C. Monteiro, Y. Takahashi, and T.

Sekine, Effectiveness of dual-rail CSSAL against power analysis attack under CMOS process variation, Proc. IEEE APCCAS 2014, pp.121-124, 2014年11月17-20日, 石垣島, 沖縄市.

③ C. Monteiro, Y. Takahashi, and T. Sekine, Process variation verification of low-power secure CSSAL AES S-box, Proc. IEEE MWSCAS 2014, pp.21-24, 2014年8月3-6日, テキサス, アメリカ.

④ C. Monteiro, Y. Takahashi, and T. Sekine, An LSI implementation of a bit-parallel cellular multiplier over GF(2^4) using secure charge-sharing symmetric adiabatic logic, Proc. IEEE ISCAS 2014, pp.826-829, 2014年6月1-5日, メルボルン,オーストラリア.

⑤ C. Monteiro, 高橋康宏, 関根敏和, Measurement of CSSAL Multiplier over GF(24) LSI Implemented in 0.18 μm CMOS Technology, 2014年電子情報通信学会総合大会講演論文集, vol.2014, p.2 (A-1-2), 2014年3月18-21日, 新潟大学, 新潟市.

⑥ Y. Takahashi, H. Sato, and T. Sekine, Design and reliability analysis of voltage reference circuit in 180 nm CMOS process, Proc. IEEE IMPACT-IAAC 2013, pp.480-483, 2013年10月22-25日, 台北市, 台湾.

⑦ 高橋康宏, C. Monteiro, 関根敏和, 負荷容量均一化対称構造断熱的論理回路CSSAL ～論理回路設計と暗号回路設計の事例～, 信学技報, vol.113, no.224, CAS2013-49, pp.71-75, 2013年9月27日, 岐阜大学, 岐阜市.

⑧ C. Monteiro, 高橋康宏, 関根敏和, LSI implementation of a secure low-power CSSAL cellular multiplier, 信学技報, vol.113, no.224, CAS2013-52, pp.89-94, 2013年9月27日, 岐阜大学, 岐阜市.

⑨ C. Monteiro, 高橋康宏, 関根敏和, LSI implementation of a bit-parallel cellular multiplier over GF(24) using charge-sharing symmetric adiabatic logic, 2013年電子情報通信学会ソサイエティ大会講演論文集, vol.2013, p.101 (C-12-41), 2013年9月17-21日, 福岡工業大学, 福岡市.

⑩ C. Monteiro, Y. Takahashi, and T. Sekine, Low power secure CSSAL bit-parallel multiplier over GF(2^4) in 0.18 μm CMOS technology, Proc. IEEE ECCTD 2013, Digital Circuit Design (USB), 4pages, 2013年9月8-12日, ドレスデン, ドイツ.

⑪ C. Monteiro, Y. Takahashi, and T. Sekine, Low power bit-parallel cellular multiplier implementation in secure dual-rail adiabatic logic, Proc. IACSIT ICCSS 2013, pp.329-332, 2013年8月10-11日, バルセロナ, スペイン.

⑫ C. Monteiro, Y. Takahashi, and T. Sekine, Robust secure charge-sharing symmetric adiabatic logic against side-channel attacks, Proc. IEEE TSP 2013, pp.732-736, 2013年7月2-4日, ローマ, イタリア.

⑬ C. Monteiro, Y. Takahashi, and T. Sekine, Low power secure AES S-box using adiabatic logic circuit, Proc. IEEE FTFC 2013, Regular session 3 (USB), 4pages, 2013年6月20-21日, パリ, フランス.

⑭ C. Monteiro, Y. Takahashi, and T. Sekine, DPA resistance of charge-sharing symmetric adiabatic logic, Proc. IEEE ISCAS 2013, pp.2581-2584, 2013年5月19-23日, 北京, 中国.

⑮ C. Monteiro, Y. Takahashi, and T. Sekine, Low power bit-parallel multiplier over GF(2^4) using CSSAL for cryptographic hardware implementation, Proc. IEEE Coolchips XVI, Poster session, 1page, 2013年4月17-19日, 横浜コンベンションセンター, 横浜市.

⑯ C. Monteiro, 高橋康宏, 関根敏和, Low power CSSAL bit-parallel multiplier over GF(2^4) in 0.18 μm CMOS technology, 信学技報, vol.113, no.2, EMCJ2013-3, pp.13-18, 2013年4月12日, 岡山大学, 岡山市.

⑰ C. Monteiro, Y. Takahashi, and T. Sekine, Secure charge-sharing symmetric adiabatic logic implementation in AES S-Box architecture for smart card, Proc. IEEE ICEIC 2013, pp.304-305, 2013年1月30日-2月2日, バリ, インドネシア.

⑱ C. Monteiro, 高橋康宏, 関根敏和, Survey on secure adiabatic logic for countermeasure against side-channel attacks, 信学技報, vol.112, no.361, EMCJ2012-100, pp.95-100, 2012年12月14日, 岐阜大学, 岐阜市.

⑲ Y. Takahashi, Z. Luo, T. Sekine, N.A. Nayan, and M. Yokoyama, 2PCDAL: Two-phase clocking dual-rail adiabatic logic, Proc. IEEE APCCAS 2012, pp.124-127, 2012年12月2-5日, 高雄市, 台湾.

⑳ Y. Takahashi, T. Sekine, N.A. Nayan, and M. Yokoyama, Power-saving analysis of adiabatic logic in subthreshold region, Proc. IEEE ISPACS 2012, pp.590-594, 2012年11月4-7日, 淡水市, 台湾.

〔図書〕（計０件）

〔産業財産権〕
○出願状況（計１件）
名称：差動論理によりサイドチャネル攻撃から保護される暗号回路
発明者：高橋康宏，モンテイロカンシオ，関根敏和
権利者：同上
種類：特許
番号：特許願 2012-274909 号
出願年月日：平成２５年１２月１７日
国内外の別： 国内

○取得状況（計０件）

〔その他〕
ホームページ等
http://www1.gifu-u.ac.jp/~yasut/

６．研究組織
(1)研究代表者
高橋 康宏（TAKAHASHI, Yasuhiro）
岐阜大学・工学部・准教授
研究者番号：00402214

(2)研究分担者
なし

(3)連携研究者
関根敏和（SEKINE, Toshikazu）
岐阜大学・工学部・准教授
研究者番号：00108060

横山道央（YOKOYAMA, Michio）
山形大学・大学院理工学研究科・准教授
研究者番号：40261573

(4)研究協力者
加藤和成（SEKINE, Toshikazu）
モンテイロ カンシオ（MONTEIRO, Cancio）