別紙様式第１３号（論文内容の要旨及び論文審査の結果の要旨）

氏名（本籍）	CANCIO　MONTEIRO（東ティモール民主共和国）
学位の種類	博　士（工学）
学位授与番号	甲第　４７６　　号
学位授与日付	平成　２７　年　３　月　２５　　日
専攻	電子情報システム工学専攻
学位論文題目	Charge-sharing symmetric adiabatic logic: Comparative analysis, application and LSI implementation for cryptographic hardware design （負荷容量均一化対称構造断熱的論理回路　～暗号ハードウェア設計のための比較解析、応用および LSI 実装～）
学位論文審査委員	（主　査）教授　木村　宏 （副　査）教授　中村　隆　　准教授　關根　敏和

論文内容の要旨

In this dissertation, the research study on low-power secure logic design using adiabatic logic techniques, and its implementation for cryptographic devices that require low-power, low frequency speed, and high security demands are summarized as follows:

1. The initial preliminary study was, researching and investigating all novel and well-known existing conventional secure logic styles, analyzing their CMOS cell structures from the point view of internal equivalent RC models, conducting some comparison study on the logic's ability for counteracting power analysis attacks by investigating the instantaneous peak supply current values and transitional energy fluctuation using SPICE simulator.
2. The results of preliminary study revealed that the existing secure logic styles are vulnerable for resistance against side-channel analysis attacks, and extremely power consuming, specifically, the implementation in the low-power and low frequency devices, such as IC-card, RFID tags and secure wireless sensors. Hence, I have designed, simulated, and investigated the Charge-Sharing Symmetric Adiabatic Logic (CSSAL) circuits. The comparison results of individual logics have shown that my proposed CSSAL circuits exhibits low and uniform peak supply current traces for all possible dual-input transitions, which performs its logic immunity for side-channel attacks.
3. Two LSIs have been implemented and fabricated using 0.18 um, 1.8-V CMOS process technology, with transistor size of wide (W)/length (L) = 0.6 μm / 0.18 μm for all PMOS and NMOS transistors.
    a. The first LSI was a bit-parallel cellular multiplier over GF(2^4), where, in the same chip, I have implemented two multiplier logic circuits, such as CSSAL multiplier and the conventional three-phase dual-rail pre-charged logic (TDPL) multiplier for my measurement comparison. The full custom layout was designed in cadence virtuoso IC6.1 with the chip size of 172 x 155 μm^2 and the global energy dissipation of 14 pJ at 12.5 MHz for the CSSAL multiplier has achieved, while TDPL has 183 x 173 μm^2 of the chip size, and the global energy dissipation is 122.6 pJ, which is nine time higher than the proposed CSSAL multiplier at the post layout simulation level. The CSSAL multiplier logic speed in the pre-layout simulation was tested from 1.25 MHz—125 MHz, however, the maximum speed was degraded to 50 MHz in the post layout simulation.

b. Second LSI was an 8-bit AES S-box circuit using positive polarity Reed-Muller (PPRM) representation with a composite field technique. In the pre-layout simulation level, I carefully investigated the CSSAL and other conventional dual-rail adiabatic logic styles from the view point of the transitional power fluctuation and the peak current traces in the 8-bit S-box in order to compare their resistance against side-channel attacks. A method to eliminate unwanted glitch current, the author applied triple-power clock to each respective inversion block; thus, the CSSAL S-box circuit performs uniform peak current traces and it has significant power reduction compare to the conventional logic style in the S-box circuit. The full custom layout was designed in same process as the multiplier above, with the chip are is 795 x 614 μm^2.

4. The fabricated LSIs were measured to check the input-output functionalities, to verify that the measurement results of output signals are same as the simulation results or not. Moreover, I have conducted further measurement of the supply current transition for power analysis attacks investigation. On the basis of the simulation and measurement results, I assure that the proposed CSSAL logic has potential applicability for low power and secure low frequency devices, such as in IC-card, RFID tags and/or secure wireless sensors.

論文審査結果の要旨

本研究は、差分電力解析などの攻撃に対して安全な CMOS 論理回路を提案している。一般に、CMOS 論理回路は，内部状態の遷移時に電源から電流が流れ、その波形が内部処理に依存するので、逆にこの波形から内部の処理を推定されるおそれがある。本研究で新たに提案する負荷容量均一化対称構造断熱的論理回路は、電源電流波形が内部処理に依存しないように工夫されている。また，断熱的原理を用いて電源から回路に流入する電流を小さくして低消費電力にしている。その詳細な消費電力解析を行って最適な動作条件を見出すと共に、基本論理回路やそれらを組み合わせた暗号処理回路への応用を系統的に検討しており、学術的に新規性のある多くの知見を得ている。また、LSI への実装を行い、提案回路および消費電力解析の有効性を確かめている。

この研究の結果を基にまとめられた学位論文、論文内容の要旨、学位論文の基礎となる発表論文に基づく審査の結果、学位論文として十分と判断し、合格とする。

最終試験結果の要旨

論文提出者は、在学中の３年間において、勉学・研究活動に精勤し、所定の講義の単位を取得するとともに、学位申請論文としての研究内容を３編の学術論文と９編の国際会議論文として公表した.

これらの結果を確認して、学位認定に伴う最終試験の結果を合格と判定する。

発表論文（論文名、著者、掲載誌名、巻号、ページ）

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

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

3. Low power secure S-Box circuit using CSSAL for AES hardware design, C. Monteiro, Y. Takahashi, and T. Sekine, IET Circuits, Devices & Systems(in print).

4. A comparison of cellular multiplier cell using secure adiabatic logics, C. Monteiro, Y. Takahashi, and T. Sekine, Proc. The 27th International Technical Conference on Circuits/Systems, Computer and Communications (ITC–CSCC) 2012, Hokkaido, Japan, July 2012, E–M2–03 (CD-ROM), 4pages.

5. Secure charge-sharing symmetric adiabatic logic implementation in AES S-Box architecture for smart card, C. Monteiro, Y. Takahashi, and T. Sekine, Proc. The IEEE International Conference on Electronics, Information and Communication (ICEIC) 2013, Bali, Indonesia, Jan. 2013, pp.306–305.

6. DPA resistance of charge-sharing symmetric adiabatic logic, C. Monteiro, Y. Takahashi, and T. Sekine, Proc. The IEEE International Symposium on Circuits and Systems (ISCAS) 2013, Beijing, China, May 2013, pp. 2581–2584.

7. Low power secure AES S-box using adiabatic logic circuit, C. Monteiro, Y. Takahashi, and T. Sekine, Proc. The IEEE Faible Tension Faible Consommation (FTTC) 2013, Paris, France, June 2013, 4pages.

8. Robust secure charge-sharing symmetric adiabatic logic against side-channel attacks, C. Monteiro, Y. Takahashi, and T. Sekine, Proc. The IEEE 36th International Conference on Telecommunications and Signal Processing (TSP) 2013, Rome, Italy, July 2013, pp. 732–736.

9. Low power secure CSSAL bit-parallel multiplier over GF(2^4) in 0.18 μm CMOS technology, C. Monteiro, Y. Takahashi, and T. Sekine, Proc. The IEEE European Conference on Circuit Theory and Design (ECCTD) 2013, Dresden, Germany, Sept. 2013, 4pages.

10. An LSI implementation of a bit-parallel cellular multiplier over GF(2^4) using secure charge-sharing symmetric adiabatic logic, C. Monteiro, Y. Takahashi, and T. Sekine, Proc. The IEEE ISCAS 2014, Melbourne, Australia, June 2014, pp. 826–829.

11. Process variation verification of low-power secure CSSAL AES S-box, C. Monteiro, Y. Takahashi, and T. Sekine, Proc. The 57th IEEE International Midwest Symposium on Circuits and Systems 2014, College Station, TX, Aug. 2014, pp. 21–24.

12. Effectiveness of dual-rail CSSAL against power analysis attack under CMOS process variation, C. Monteiro, Y. Takahashi, and T. Sekine, Proc. IEEE Asia Pacific Conference on Circuits and Systems (APCCAS) 2014, Okinawa, Japan, Nov. 2014, pp. 121-124.