科学研究費助成事業　　研究成果報告書

平成 ２６ 年　 ６ 月　 ４ 日現在

機関番号：１１３０１
研究種目：若手研究(A)
研究期間：2010～2013
課題番号：２２６８０００３

研究課題名（和文）耐タンパー性を有する超高性能公開鍵暗号プロセッサの開発

研究課題名（英文）Development of high-performance public-key cryptographic processors with tamper resistance

研究代表者
本間　尚文（Homma, Naofumi）

東北大学・情報科学研究科・准教授

研究者番号：００３４３０６２

交付決定額（研究期間全体）：（直接経費）　10,300,000円、（間接経費）　3,090,000円

研究成果の概要（和文）：本研究は，世界最高水準の耐タンパー性と高い演算性能を兼ね備えた暗号プロセッサおよびその設計技術を開発した．具体的には，公開鍵暗号の中心的な演算である冪乗剰余演算に特化したプロセッサアーキテクチャを設計し，サイドチャネル攻撃に対する高い耐性を備えるRSA暗号プロセッサを開発した．また，開発したプロセッサのプロトタイプ実装に対して，サイドチャネル攻撃（入力選択型電力・電磁波解析攻撃および故障利用攻撃）実験を網羅的に実施し，その耐性を実証した．さらに，それと並行して，多様な設計要求に応じて当該RSA 暗号プロセッサを自動生成するジェネレータを開発した．

研究成果の概要（英文）：This research project developed a high-performance cryptographic processor with a state-of-the-art tamper resistance capability and its design methodology. More precisely, we designed a processor architecture specified for exponentiation operation which is an integral part of public-key cryptographic operation, and developed an RSA processor highly resistant to side-channel attacks. In addition, we demonstrated the validity of the developed processor through an exhaustive set of experiments on side-channel attacks (i.e., chosen-message power/EM analysis attacks and fault injection attacks) against a prototype implementation of the developed processor. Moreover, we developed an automatic generator which generates RSA processors depending on various design specifications.

研究分野：総合領域

科研費の分科・細目：情報学・計算機システム・ネットワーク

キーワード：計算機システム　システムオンチップ　VLSI設計技術　暗号プロセッサ　耐タンパー性

１．研究開始当初の背景

近年，暗号モジュール（暗号処理を実行するLSI 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，現実的な脅威となりつつある．しかし現状では，暗号モジュールに対する最新のセキュリティ要件であるISO/IEC19790 においても，その対策は含まれていない．今後の情報化社会では，個人情報の保護や高信頼な電子商取引が必須であり，サイドチャネル攻撃に耐性を有する暗号モジュールとその設計技術の確立が急務である．特に，RSA 暗号に代表される公開鍵暗号では，冪乗剰余演算を中心とした膨大な多倍長計算を必要とするため，計算能力の限られた組込みシステム向けのハードウェア設計が強く求められている．

本申請者は，産業技術総合研究所と共同で，サイドチャネル攻撃標準評価ボード（SASEBO）や ISO/IEC 国際標準暗号のハードウェア IP を開発するなど，暗号モジュールに対するサイドチャネル攻撃とその防御に関する研究を先導してきた．SASEBO は，現在，米国国立標準技術研究所（NIST）を含む国内外の研究機関や企業で広く利用され，本分野のデファクトスタンダードとなっている．また，公開鍵暗号へのサイドチャネル攻撃に関する研究では，暗号研究の第一人者である Adi Shamir 教授 （RSA 暗号発明者の一人） と共同研究を実施し，主要な学術誌および国際会議で共著論文を発表している．特に，二つの電力波形の比較から鍵を推定する比較電力解析に世界で初めて成功するなど，その波形解析技術が高く評価されている．一方で，本申請者は，これまで非 2 進数系や多値論理に基づく新しい原理の計算機構の研究を行い，従来の 2 進 2 値論理方式にとらわれずに，デバイス物理に応じて最適な論理方式を選択することによりシステムの超高性能化を実現できることを実証してきた．従来，サイドチャネル攻撃対策では，その安全性に重点があり，安全性と演算性能を両立させた対策はほとんど報告されていないが，本申請者は，これまで培ってきた新原理に基づく演算アルゴリズムと回路実装技術を応用することで，それらを両立する公開鍵暗号プロセッサを実現できるとの着想に至った．

２．研究の目的

本研究では，世界最高水準の耐タンパー性と演算性能を兼ね備えた暗号プロセッサとその設計技術の確立を目指し，アーキテクチャの設計から自動生成システムの開発までの下記 4 項目を目的とする．

(1) 高基数モンゴメリ乗算に基づく冪乗剰余演算プロセッサアーキテクチャの設計：RSA 暗号や ElGamal 暗号といった公開鍵暗号の中心的な演算である冪乗剰余演算に特化したプロセッサアーキテクチャを設計する．特に，乗剰余演算と自乗剰余演算に高基数モンゴメリ乗算アルゴリズムを採用することで，高いスケーラビリティと回路効率を実現できることを明らかにする．

(2) 電流モード論理回路に基づく RSA 暗号プロセッサの開発：上記(1)のアーキテクチャに基づく RSA 暗号プロセッサを電流モード論理回路を用いて実現する．特に，プロセッサの性能を左右するデータパスを多値電流モード論理に基づく冗長数系演算器で実装することで，従来の CMOS 回路に匹敵する高い演算性能が得られることを明らかにする．

(3) ASIC によるプロトタイプ実装を用いたサイドチャネル攻撃耐性の評価：上記 RSA 暗号プロセッサのプロトタイプを ASIC で実装し，そのサイドチャネル攻撃耐性を実証する．具体的には，実装した ASIC を SASEBO 上に搭載し，現在最も強力な攻撃である平文選択型電力・電磁波解析攻撃と故障利用攻撃を網羅的に実施し，その耐性を定量的に評価する．特に，電磁波解析攻撃では，高空間分解能マイクロ磁界プローブを用いた詳細な漏洩電磁波計測を ASIC 全体に渡って実施し，得られた漏洩電磁波の強度マップから，その対策の効果と限界を解明する．

(4) RSA 暗号プロセッサジェネレータの開発：上記 RSA 暗号プロセッサのジェネレータを開発する．本ジェネレータは，設計仕様（アーキテクチャ・基数・算術演算アルゴリズム）に応じて， 100 種類以上のプロセッサの HDL 記述を生成可能とする．また，内部の検証系により，生成する HDL 記述の機能をアルゴリズムレベルで完全に保証する．代表的な設計仕様をジェネレータで生成し，その性能評価を実施する．

３．研究の方法

本研究では，上述の研究目的を当初の予定を繰り上げて 3 年間で達成した．平成 22 年度は，RSA 暗号プロセッサの中心となる冪乗剰余演算プロセッサアーキテクチャを設計するとともに，多値電流モード論理（MV-CML）と従来の CMOS が混載した回路の設計環境を構築する．平成 23 年度は，前年度に開発したアーキテクチャを基本とした MV-CML/CMOS 混載回路による RSA 暗号プロセッサを開発するとともに，その演算性能を評価する．平成 24 年度は，当該 RSA 暗号プロセッサへのサイドチャネル攻撃実験と RSA 暗号プロセッサジェネレータの開発を並行して進める．サイドチャネル攻撃実験では，ASIC 実装した RSA 暗号プロセッサを SASEBO 上に搭載し，電力・電磁波解析攻撃実験および故障利用攻撃実験を実施する．一方，ジェネレータ開発では，これまでのインタフェースやパーサーを拡

張して暗号プロセッサ向けの生成系を構築するとともに，高基数モンゴメリ乗算アルゴリズムに対応する検証系を新たに開発する．

４．研究成果

(1) 平成 22 年度は下記 2 項目の研究を実施した．

① 冪乗剰余演算プロセッサアーキテクチャの設計：

RSA 暗号の中心的な演算である冪乗剰余演算に特化したプロセッサアーキテクチャを設計した．冪乗剰余演算アルゴリズムには，小面積で効率的な実装が可能なバイナリ法を用いた．また，各乗剰余算と自乗剰余算には除算を用いることなく加算とシフト演算のみで同演算を実現可能なモンゴメリ乗算アルゴリズムを採用した．特に，入力が 1024 ビット以上となる RSA 暗号のため，入力語長を 8～128 ビットのワードに分割する高基数モンゴメリ乗算に基づくプロセッサアーキテクチャを設計した．これにより，スケーラビリティと回路効率の大幅な向上を図った．また，設計したアーキテクチャの演算性能を明らかにするため，従来の CMOS セルライブラリを用いた合成を実施し，その演算速度や消費電力を評価した．

② MV-CML/CMOS 混載回路の設計フロー開発：

開発する暗号プロセッサでは，主要コンポーネントとなる演算回路部分を MV-CML 回路で構成し，それ以外の部分を従来の CMOS 回路で構成する．本年度は，このような MV-CML/CMOS 混載回路を 2 値・多値融合論理システムととらえ，その設計ツールを開発した．まず，本申請者らが提案するハードウェアアルゴリズム記述言語 ARITH および合成用データ構造 CTD（Counter Tree Diagram）を用いた上位設計フローを開発した．さらに，下位設計のため，MV-CML 回路の物理モデルとセルレイアウトを組み込んだライブラリを開発した．それらを統合することで回路設計フローを開発した．

(2) 平成 23 年度は下記 2 項目の研究を実施した．

① MV-CML/CMOS 混載回路による RSA 暗号プロセッサの開発：

前年度に開発した冪乗剰余演算プロセッサアーキテクチャを元に MV-CML/CMOS 混載回路による RSA 暗号プロセッサを開発した．RSA 暗号の暗号化・復号は冪乗剰余演算そのものであるため，シーケンサやメモリ部分は同アーキテクチャの軽微な拡張や変更により実現した．一方，データパス部分は，MV-CML 回路で高性能に実装するため，演算器を非 2 進数演算アルゴリズムにより実現した．本研究では，特に冗長 2 進数系による高速加算アルゴリズムの使用を検討した．前年度に開発した設計フローを用いて，設計した RSA 暗号プロセッサの回路合成を実施するとともに，その演算性能を評価した．

② RSA 暗号プロセッサに対するサイドチャネル攻撃実験環境の構築：

本研究で開発した RSA 暗号プロセッサのサイドチャネル攻撃耐性を評価するために実験環境を構築した．具体的には，CMOS 回路で開発した RSA 暗号プロセッサのプロトタイプを ASIC で実装し，そのサイドチャネル情報（消費電力や放射電磁波）を測定するためのシステムを構築した．本実験では，本申請者が開発したサイドチャネル攻撃標準評価ボード SASEBO-R に ASIC を搭載し，マイクロ磁界プローブ等を用いて消費電力や放射電磁波を詳細に測定すること検討した．また，Xilinx FPGA のディジタルクロック制御機能を利用して意図的にクロック信号にグリッチを発生させ，故障利用攻撃を実施するための回路を設計した．

(3) 平成 24 年度は下記 2 項目の研究を実施した．

① 前年度に開発した暗号プロセッサ実装に対するサイドチャネル攻撃実験の実施：

前年度に開発した RSA 暗号プロセッサのプロトタイプ実装に対するサイドチャネル攻撃実験を網羅的に実施した．実験には，同じく前年度に構築したサイドチャネル情報（消費電力および放射電磁波）測定システムを利用した．具体的には現在 RSA 暗号に対して最も強力な受動的電力・電磁波解析攻撃の一つとされる入力選択型の攻撃を実施し，その耐タンパー性を評価した．放射電磁波は上記測定システムとマイクロ磁界プローブを組み合わせることで測定した．一方，能動的攻撃実験として，前年度に開発したクロックグリッチ発生回路をサイドチャネル攻撃標準評価ボードの FPGA 上に実装して故障利用攻撃実験を実施した．具体的には RSA 暗号に対する攻撃の一つである Safe-error 攻撃を実施した．故障注入のタイミングをナノ秒単位で制御することでその耐タンパー性を評価した．

② RSA 暗号プロセッサジェネレータの開発：

本研究で開発した RSA 暗号プロセッサの HDL（ハードウェア記述言語）記述を設計仕様に応じて自動生成するジェネレータを開発した．具体的には，RSA 暗号プロセッサデータパスの中心的な演算であるべき乗剰余演算を可能な積和演算器の自動生成を実現するシステムを開発した．入力する設計仕様としては，入力語長に加えて，100 種類を越える積和演算アルゴリズムを選択可能とした．

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 12 件）

1. Miroslav Knezevic, Kazuyuki Kobayashi, Jun Ikegami, Shin’ichiro Matsuo, Akashi Satoh, Unal Kocabas, Junfeng Fan, Toshiro Katashita, Takeshi

Sugawara, Kazuo Sakiyama, Ingrid Verbauwhede, Kazuo Ohta, Naofumi Homma, Takafumi Aoki, “Fair and Consistent Hardware Evaluation of Fourteen Round Two SHA-3 Candidates,” IEEE Transactions on Very Large Scale Integration Systems, Vol.20, No.5, pp.827–840, May 2012. 査読有.

2. Kazuya Saito, Naofumi Homma, and Takafumi Aoki, “A Formal Approach to Designing Arithmetic Circuits over Galois Fields Using Symbolic Computer Algebra,” Proceedings of the 17th Workshop on Synthesis And System Integration of Mixed Information technologies, pp. 153-158, March 2012. 査読有.
3. Naofumi Homma, Kazuya Saito, and Takafumi Aoki, “A Formal Approach to Designing Cryptographic Processors Based on GF(2^m) Arithmetic Circuits,” IEEE Transactions on Information Forensics & Security, Vol. 7, No. 1, pp. 3-13, February 2012. 査読有.
4. 林優一, 本間尚文, 水木敬明, 青木孝文, 曽根秀昭, “暗号モジュールに対するサイドチャネル攻撃とその対策技術の研究動向,”電気学会論文誌 A, vol. 132 (2012), no. 1, pp.9-12, January 2012. 査読有.
5. Takeshi Sugawara, Naofumi Homma, Takafumi Aoki, and Akashi Satoh, “High-performance Architecture for Concurrent Error Detection for AES Processors,” IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Vol. E94-A, No.10, pp. 1971–1980, October 2011. 査読有.
6. Atsushi Miyamoto, Naofumi Homma, Takafumi Aoki, and Akashi Satoh, “Systematic design of RSA processors based on high-radix Montgomery multipliers,” IEEE Transactions on Very Large Scale Integration Systems, Vol. 19, No. 7, pp. 1136-1146, July 2011. 査読有.
7. Kazuya Saito, Naofumi Homma and Takafumi Aoki, “A Graph-Based Approach to Designing Multiple-Valued Arithmetic Algorithms,” Proceedings of the 41st International Symposium on Multiple Valued Logic, pp. 27-32, May 2011. 巻数無し. 査読有.
8. 馬場祐一, 宮本篤志, 本間尚文, 青木孝文, 佐藤証, “RSA 暗号プロセッサ自動生成システムの設計と評価,” 情報処理学会論文誌, Vol. 51, No. 9, pp. 1847–1858, September 2010. 査読有. (推薦論文)
9. Takeshi Sugawara, Naofumi Homma, Takafumi Aoki, and Akashi Satoh, “Profiling attack using multivariate regression analysis,” IEICE Electronics Express, Vol. 7, No. 15, pp. 1139-1144, August 2010. 査読有.
10. Naofumi Homma, Yuichi Baba, Atsushi Miyamoto, and Takafumi Aoki, “Multiple-Valued Constant-Power Adder and Its Application to Cryptographic Processor,” IEICE Transactions on Information and Systems, Vol.E93-D, No.8, pp.2117-2125, August 2010. 査読有.
11. Naofumi Homma, Atsushi Miyamoto, Takafumi Aoki, Akashi Satoh, and Adi Shamir, “Comparative Power Analysis of Modular Exponentiation Algorithms,” IEEE Transactions on Computers, Vol. 59, No. 6, pp. 795–807, June 2010. 査読有.
12. Yuichi Baba, Naofumi Homma, Atsushi Miyamoto, Takafumi Aoki, “Design of tamper-resistant registers for multiple-valued cryptographic processors,” Proceedings of the 40th International Symposium on Multiple Valued Logic, pp. 67-72, May 2010. 巻数無し. 査読有.

〔学会発表〕(計 15 件)

1. 岡本広太郎, 本間尚文, 青木孝文, “ガロア体上の乗算器モジュールジェネレータの構築,” 第 75 回情報処理学会全国大会, 3K-8, 1-135–1-136, March 7, 2013. 仙台.
2. Naofumi Homma, “Security Evaluation of Cryptographic Systems against Physical Attacks,” 2012 Bilateral Workshop between Tohoku University and National Tsing Hua University, December 12, 2012. 仙台. (招待講演)
3. 岡本広太郎, 本間尚文, 青木孝文, “正規基底表現されたガロア体上の算術演算回路の形式的設計に関する検討,” 第 35 回多値論理フォーラム, No. 7, pp. 7-1-7-6, September 15, 2012. 富山.
4. Naofumi Homma, “Toward Formal Design of Cryptographic Processors Based on Galois Field Arithmetic,” PROOFS (Security Proofs for Embedded Systems) Workshop, September 13, 2012. ルーベン, ベルギー. (招待講演)
5. 岡本広太郎, 本間尚文, 青木孝文, “ガロア体上の算術演算回路の自動生成システムの構築,” 平成 24 年度 電気関係学会東北支部連合大会, No. 1I03, pp. 115, August 30, 2012. 本庄.

6. Naofumi Homma, “What are going to be the key MVL innovations over the next 10 years?” Special Panel Session on Upcoming Advances in MVL, the 42nd International Symposium on Multiple-Valued Logic, May 14, 2012. ヴィクトリア, カナダ. (招待講演)
7. 齋藤和也, 本間尚文, 青木孝文, “ガロア体上の算術演算回路の形式的設計とその AES 暗号プロセッサへの応用,” 2012 年暗号と情報セキュリティシンポジウム, Vol. 4C1-4, pp.1-8, February 2, 2012. 金沢.
8. 齋藤和也, 本間尚文, 青木孝文, “ガロア体上の算術演算回路の形式的表現に関する検討,” 第 25 回多値論理とその応用研究会, No. 8, pp. 38-44, January 7 2012. 宮崎.
9. 齋藤和也, 本間尚文, 青木孝文, “算術回路グラフの暗号プロセッサ設計への応用,” 第 34 回多値論理フォーラム, No. 11, pp. 11-1-11-6, September 18, 2011. 筑波.
10. Sho Endo, Naofumi Homma and Takafumi Aoki, “Efficient countermeasure against fault injection attacks on modular,” 平成 23 年度 電気関係学会東北支部連合大会, No. 1A03, pp. 3, August 25, 2011. 多賀城.
11. Naofumi Homma, “DPA Contest V3 and SASEBO-W for V4,” International Workshop on Constructive Side-Channel Analysis and Secure Design, February 24, 2011. ダルムシュタット, ドイツ. (招待講演)
12. 齋藤和也, 本間尚文, 青木孝文, “算術回路グラフに基づく算術演算回路の形式的設計に関する検討,” 第 24 回多値論理とその応用研究会, No. 8, pp. 8-1−8-6, January 8 2011. 仙台.
13. 齋藤和也, 本間尚文, 青木孝文, “多値算術演算回路向け算術アルゴリズムの形式的表現と検証に関する検討,” 第 33 回多値論理フォーラム, No. 8, pp. 8-1-8-6, September 2010. 広島.
14. 齋藤和也, 菅原健, 本間尚文, 青木孝文, 佐藤証, “楕円曲線暗号ハードウェアの電力解析による安全性評価,” 平成 22 年度 電気関係学会東北支部連合大会, No. 1E08, p. 143, August 2010. 八戸.
15. 本間尚文, “暗号 LSI の設計技術,” 日本学術振興会 シリコン超集積化システム第 165 委員会, April 16, 2010. 東京. (招待講演)

〔図書〕(計 1 件)
1. 本間尚文, 青木孝文, “サイドチャネル攻撃,” 映像情報メディア学会, 映像情報メディア学会誌, Vol. 64, No. 11, pp. 1576-1579, November 2010.

〔その他〕
ホームページ等
http://www.aoki.ecei.tohoku.ac.jp/arith/mg/index.html

６．研究組織
(1)研究代表者
本間　尚文 (HOMMA NAOFUMI)
東北大学・大学院情報科学研究科・准教授
研究者番号：00343062