様式 C-19

科学研究費補助金研究成果報告書

平成２２年　５月　２１日現在

研究種目：若手研究（B）
研究期間：2008～2009
課題番号：20700041
研究課題名（和文）　計算機代数に基づく高性能 VLSI データパスの形式的設計技術の開発

研究課題名（英文）　Formal design method of high-performance VLSI datapaths based on computer algebra

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

研究成果の概要（和文）：本研究では，算術アルゴリズムの高水準設計技術の開発を目指し，計算機代数に基づく算術アルゴリズムの形式的検証手法を開発した．また，その応用として算術演算モジュールジェネレータを開発した．特に，開発するジェネレータでは，セキュリティシステム応用で多用される演算（べき乗剰余演算）アルゴリズムの生成を可能にした．生成されるアルゴリズムは，全て本研究で開発された形式的手法により完全に検証される．

研究成果の概要（英文）：This research project aimed to develop high-level design methodology for arithmetic algorithms, and developed formal verification method of arithmetic algorithms based on computer algebra and its application to arithmetic module generator.　In particular, the newly-developed generator can generate typical operations in security systems such as modular exponentiation operations.　The generated algorithms can be verified completely by the formal verification method.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
2008 年度	1,600,000	480,000	2,080,000
2009 年度	1,600,000	480,000	2,080,000
年度			
年度			
年度			
総　計	3,200,000	960,000	4,160,000

研究分野：計算機科学
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：(1)計算機システム，(2)システムオンチップ，(3)VLSI 設計技術，(4)算術アルゴリズム，(5)形式的設計，(6)，計算機代数，(7)データパス，(8)グレブナー基底

１．研究開始当初の背景

身の回りのあらゆる機器に VLSI システムが搭載されるユビキタス社会においては，システムの性能を左右するデータパスを用途に応じて適切に設計する必要がある．特にデータパスの大部分を占める算術演算回路の性能は，デバイスレベルや論理レベルでの最適化のみならず，算術演算のハードウェアアルゴリズム（算術アルゴリズム）に大きく依存する．しかし，現在の EDA（Electronic Design Automation）技術は論理回路の記述や検証を基本として発展しており，算術アル

ゴリズムの設計に対して十分な設計環境が整っていない．従来のハードウェア記述言語（HDL: Hardware Description Language）では論理式によって回路を記述するため，算術演算を基本とする算術アルゴリズムを直接記述することは難しい．特に 2 進数系以外（2 の補数表現，冗長数系，多進数系など）の算術アルゴリズムを HDL で記述するためには，2 値論理信号に基づいた低水準の構造記述が必要となる．また，一般に多入力多出力となる算術演算回路を論理シミュレーションにより検証するには膨大な計算時間が必要となる．

このような問題を根本的に解決するため，本申請者は算術アルゴリズムの記述・検証・合成に特化した算術アルゴリズム記述言語 ARITH とその言語処理系を提案してきた．ARITH は，①算術演算回路のアルゴリズムを整数方程式に基づいて形式的に記述可能，②非 2 進数系を含む任意の重み数系を記述可能，③アルゴリズムの正当性を数式処理等により静的に検証可能，④正当性の証明された算術アルゴリズムを従来の HDL に変換可能という特長を有する．

２．研究の目的

本研究では,以下の 2 項目を研究目的とする．

(1) 計算機代数に基づく形式的検証手法の開発：提案する算術アルゴリズム記述の高速な検証手法として，計算機代数（多項式リダクションとグレブナー基底）を応用した形式的検証手法を開発する．また，従来の形式的検証手法（ワードレベルの決定グラフや二分モーメントグラフ）との比較により，その性能を評価する．

(2) 算術演算モジュールジェネレータの開発：ARITH を演算器ライブラリのデータ形式に用いたデータパスモジュールジェネレータを開発する．特に，セキュリティシステム応用で多用される演算に特化したジェネレータを構築する．

３．研究の方法

本研究では,下記 2 項目を並行して実施する．

(1) 計算機代数に基づく算術アルゴリズムの形式的検証手法の開発

(2) 暗号処理向けデータパスモジュールジェネレータの開発

平成 20 年度は上記(1) および (2) に対応して以下の 2 項目について研究を行う．

(1) 任意の整数方程式の組み合わせで記述される算術アルゴリズムに適用可能な形式的検証手法を開発する．本申請者らがこれまでに開発してきた検証手法は，多項式リダクションのみを用いており，検証対象が線形整数方程式の組み合わせで記述される算術アルゴリズムに限定されていた．そこで，これまでの検証手法を拡張し，検証対象となる機能（整数方程式）の正当性を判定する問題を多項式イデアル所属問題に帰着させることで，任意の多項式からなる算術アルゴリズムを取り扱い可能とする．拡張した手法では，等価性判定に用いる内部回路記述（多項式集合）をグレブナー基底へと変換し，得られたグレブナー基底に多項式リダクションを実行することにより，検証対象の機能が多項式集合により導出できるかどうかを判定する．本研究では，以上の形式的検証手法を定式化するとともに，そのプロトタイプソフトウェアを開発する．開発においては必要に応じて数値計算ライブラリを利用する．

(2) モジュールジェネレータで生成するべき乗剰余演算アルゴリズムの基本設計を行う．本研究では特に左バイナリ法による設計を検討する．乗剰余算と自乗剰余算は，モンゴメリ乗算アルゴリズムにより，除算を用いることなく加算とシフト演算のみで実現する．これにより，回路面積や演算速度で大幅な性能向上が図る．なお，モンゴメリ乗算の計算過程で使用する乗算アルゴリズムには，本申請者らの開発したジェネレータで生成する 352 種類のアルゴリズムを適用する予定である．また，演算語長は 4 ビットから 128 ビットまで網羅的に設計する．

平成 21 年度は上記 (1) および (2) に対応して以下の 2 項目について研究を行う．

(1) 前年度に開発した検証手法の性能評価を行う．まず，比較のため，従来の形式的検証手法（ワードレベルの決定グラフや二分モーメントグラフ）を実装する．従来手法で用いるグラフ構造は，ARITH に新たな記述を追加することなく実現できる見通しを得ている．その上で，いくつかの回路機能の検証を通して提案手法の性能を比較・評価する．具体的には，従来手法が有利な例として並列プリフィックス加算器，提案手法が有利な例として Wallace 加算木をそれぞれ検証する予定である．開発した手法は，論理演算を含む任意の機能を原理的に検証可能であるが，検証の複雑さは対象となる数式の数と次数に依存するため，算術演算を論理レベルで最適化したアルゴリズムに適用した場合には検証時間が増大すると予想される．評価結果から従来手法と提案手法の最適な組み合わせを検討し，より大規模な算術アルゴリズムにも適用可能な形式的検証手法の確立を目指す．

(2) べき乗剰余算アルゴリズムを生成可能なモジュールジェネレータを開発する．まず，前年度に設計したアルゴリズムを ARITH でライブラリ化する．次に，回路設計用ソフトウェア（Design Compiler および Astro）によりその性能を概算する．特に優れた性能が期待できるモジュールについては,ASIC や FPGA によるプロトタイプを試作する．また，本ジ

ェネレータはWeb上に公開する予定である．それと並行して，モジュール検証の高速化のため，前年度に開発した検証手法をジェネレータに実装する．公開鍵暗号や共通鍵暗号モジュールを自動生成するための拡張についても合わせて検討する予定である．

４．研究成果

平成 20 年度は，上記の(1)および(2)に対応して以下の研究成果を得た．

(1) 任意の整数方程式の組み合わせで記述される算術アルゴリズムに適用可能な形式的検証手法を開発した．本申請者らがこれまでに開発してきた検証手法は，多項式リダクションのみを用いており，線形整数方程式の組み合わせで記述される算術アルゴリズムに対象が限定されていた．そこで，これまでの検証手法を拡張し，検証対象となる機能（整数方程式）の正当性を判定する問題を多項式イデアル所属問題に帰着させることで，任意の多項式からなる算術アルゴリズムを取り扱い可能とした．拡張した手法では，等価性判定に用いる内部回路記述（多項式集合）をグレブナー基底へと変換し，得られたグレブナー基底に多項式リダクションを実行することにより，検証対象の機能が多項式集合により導出できるかどうかを判定した．本研究では，以上の形式的検証手法を定式化するとともに，そのプロトタイプソフトウェアを開発した．開発においては数値計算ライブラリを利用した．

(2) モジュールジェネレータで生成するべき乗剰余演算アルゴリズムの基本設計を行った．本研究では特に左バイナリ法による設計を検討した．乗剰余算と自乗剰余算は，モンゴメリ乗算アルゴリズムにより，除算を用いることなく加算とシフト演算のみで実現した．これにより，回路面積や演算速度で大幅な性能向上を実現した．なお，モンゴメリ乗算の計算過程で使用する乗算アルゴリズムには，本申請者らの開発したジェネレータが生成した242種類のアルゴリズムを用いた．また，演算語長は4ビットから128ビットまで網羅的に設計した．

平成 21 年度は，上記の (1) および (2) に対応して以下の研究成果を得た．

(1) 前年度に開発した検証手法の性能評価を行った．まず，比較のため，従来の形式的検証手法（ワードレベルの決定グラフや二分モーメントグラフ）を実装した．従来手法で用いるグラフ構造は，ARITH に新たな記述を追加することなく実現した．その上で，いくつかの回路機能の検証を通して提案手法の性能を比較・評価した．具体的には，従来手法が有利な例として並列プリフィックス加算器，提案手法が有利な例としてWallace加算木をそれぞれ検証した．開発した手法は，論理演算を含む任意の機能を原理的に検証可能であるが，検証の複雑さは対象となる数式の数と次数に依存するため，算術演算を論理レベルで最適化したアルゴリズムに適用した場合には検証時間が増大した．評価結果から従来手法と提案手法の最適な組み合わせを考案するとともに，より大規模な算術アルゴリズムにも適用可能な形式的検証手法を検討した．

(2) べき乗剰余算アルゴリズムを生成可能なモジュールジェネレータを開発した．まず，前年度に設計したアルゴリズムをARITHでライブラリ化した．次に，回路設計用ソフトウェア（Design Compiler および Astro）によりその性能を概算した．特に優れた性能が期待できるモジュールについては，FPGAによるプロトタイプを試作した．また，それと並行して，モジュール検証の高速化のため，前年度に開発した検証手法をジェネレータに実装した．公開鍵暗号や共通鍵暗号モジュールを自動生成するための拡張についても合わせて検討した．

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 27 件）

(1) Yongdae Kim, Takeshi Sugawara, Naofumi Homma, Takafumi Aoki, Akashi Satoh, ″Biasing power traces to improve correlation in power analysis attacks,″ International Workshop on Constructive Side-Channel Analysis and Secure Design 2010, pp. 77--80, February 2010.査読有

(2) 本間尚文，青木孝文，佐藤証，“暗号モジュールへのサイドチャネル攻撃とその安全性評価の動向,” 電子情報通信学会論文誌A, Vol. J93-A, No. 2, pp. 42--51, February 2010.査読無（招待）

(3) 宮本篤志，本間尚文，青木孝文，佐藤証“RSA暗号プロセッサのFPGA実装に対する平文選択型SPAの評価,” 電子情報通信学会論文誌D, Vol.J92-D,No.12,pp. 2168--2180, December. 2009. 査読有

(4) 菅原健，本間尚文，青木孝文，佐藤証，“ハッシュ関数Whirlpoolの高スケーラブル回路アーキテクチャ,” 情報処理学会論文誌，Vol. 50, No. 11, pp. 2618--2632, November 2009. 査読有

(5) Takeshi Sugawara, Yu-ichi Hayashi, Naofumi Homma, Takaaki Mizuki, Takafumi Aoki, Hideaki Sone, and Akashi Satoh, ″Mechanism behind Information Leakage in Electromagnetic Analysis of

Cryptographic Modules," Workshop on Information Security Applications - WISA 2009, Lecture Notes in Computer Science 5932, pp. 66--78, Springer-Verlag, 2009. 査読有

(6) Naofumi Homma, Yuki Watanabe, Katsuhiko Degawa, Takafumi Aoki, Tatsuo Higuchi, "Systematic approach to designing multiple-valued arithmetic circuits based on arithmetic description language," Journal of Multiple-Valued Logic and Soft Computing, Vol. 15, No. 4, pp. 329-340, 2009. 査読有

(7) Masahiro Yamaguchi, Hideki, Toriduka, Shoichi Kobayashi, Takeshi Sugawara, Naofumi Homma, Akashi Satoh, Takafumi Aoki, "Side Channel Attack to Magnetic Near Field of Cryptographic LSI and Its Protection by Magnetic Thin Film," Soft Magnetic Materials 19, A3-11, September 2009. 査読有

(8) Toshihiro Katashita, Akashi Satoh, Takeshi Sugawara, Naofumi Homma, and Takafumi Aoki, "Development of Side-Channel Attack Standard Evaluation Environment," European Conference on Circuit Theory and Design 2009, pp. 403--408, August 2009. 査読有

(9) Takeshi Sugawara, Naofumi Homma, Takafumi Aoki, and Akashi Satoh, "Differential Power Analysis of AES ASIC Implementations with Various S-box Circuits," European Conference on Circuit Theory and Design 2009, pp. 395--398, August 2009. 査読有

(10) Takeshi Sugawara, Yu-ichi Hayashi, Naofumi Homma, Takaaki Mizuki, Takafumi Aoki, Hideaki Sone, and Akashi Satoh, "Spectrum Analysis on Cryptographic Modules to Counteract Side-Channel Attacks," Proceedings of the 2009 International Symposium on Electromagnetic Compatibility, pp. 21--24, July 2009. 査読有

(11) Yu-ichi Hayashi, Takeshi Sugawara, Yoshiki Kayano, Naofumi Homma, Takaaki Mizuki, Akashi Satoh, Takafumi Aoki, Shigeki Minegishi, Hideaki Sone, and Hiroshi Inoue, "An Analysis of Information Leakage from a Cryptographic Hardware via Common-Mode Current," Proceedings of the 2009 International Symposium on Electromagnetic Compatibility, pp. 17--20, July 2009. 査読有

(12) Atsushi Miyamoto, Naofumi Homma, Takafumi Aoki, and Akashi Satoh, "Evaluation of Simple/Comparative Power Analysis Against an RSA ASIC Implementation", Proceedings of the 2009 IEEE International Symposium on Circuits and Systems, pp. 2918--2921, May 2009. 査読有

(13) Yuichi Baba, Atsushi Miyamoto, Naofumi Homma, Takafumi Aoki, "Multiple-Valued Constant-Power Adder for Cryptographic Processor," Proceedings of the 39th International Symposium on Multiple Valued Logic, pp. 239--244, May 2009. 査読有

(14) Atsushi Miyamoto, Naofumi Homma, Takafumi Aoki, and Akashi Satoh, "An experimental comparison of power analysis attacks against RSA processors on ASIC and FPGA," Proceedings of the 15th Workshop on Synthesis And System Integration of Mixed Information technologies, pp. 58--63, March 2009. 査読有

(15) Takeshi Sugawara, Naofumi Homma, Takafumi Aoki, and Akashi Satoh, "Compact ASIC Architectures for the 512-bit Hash Function Whirlpool," Workshop on Information Security Applications - WISA 2008, Lecture Notes in Computer Science 5379, pp. 28--40, Springer-Verlag, 2009. 査読有

(16) Toshihiro Katashita, Akashi Satoh, Takeshi Sugawara, Naofumi Homma and Takafumi Aoki, "Enhanced Correlation Power Analysis using Key Screening Techniques," 2008 International Conference on ReConFigurable Computing and FPGAs, pp. 403--408, December 2008. 査読有

(17) Naofumi Homma, Takafumi Aoki, and Tatsuo Higuchi, "A Systematic Approach for Designing Redundant Arithmetic Adders Based on Counter Tree Diagrams," IEEE Transactions on Computers, Vol. 57, No. 12, pp. 1633-1646, December 2008. 査読有

(18) Atsushi Miyamoto, Naofumi Homma, Takafumi Aoki, and Akashi Satoh, "Systematic design of high-radix Montgomery multipliers for RSA processors," Proceedings of the 26th IEEE International Conference of Computer Design, pp. 416--421, October 2008. 査読有

(19) Yuki Watanabe, Naofumi Homma,

Takafumi Aoki, and Tatsuo Higuchi, “Arithmetic Circuit Verification Based on Symbolic Computer Algebra,” IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Vol. E91-A, No. 10, pp. 3038-3046, October 2008. 査読有
(20) Atsushi Miyamoto, Naofumi Homma, Takafumi Aoki, and Akashi Satoh, ″Chosen-message SPA attacks against FPGA-based RSA hardware implementations,″ Proceedings of the 2008 International Conference on Field Programmable Logic and Applications, pp. 35--40, September 2008. 査読有
(21) Akashi Satoh, Takeshi Sugawara, Naofumi Homma, and Takafumi Aoki, ″High-performance concurrent error detection scheme for AES hardware,″ Cryptographic Hardware and Embedded Systems - CHES 2008, Lecture Notes in Computer Science 5154, pp. 100--112, Springer-Verlag, August 2008. 査読有
(22) Naofumi Homma, Atsushi Miyamoto, Takafumi Aoki, Akashi Satoh, and Adi Shamir, ″Collision-based power analysis of modular exponentiation using chosen-message pairs,″ Cryptographic Hardware and Embedded Systems - CHES 2008, Lecture Notes in Computer Science 5154, pp. 15--29, Springer-Verlag, August 2008. 査読有
(23) Naofumi Homma, Atsushi Miyamoto, Takafumi Aoki, and Akashi Satoh, ″Power analysis of RSA processors with high-radix Montgomery multipliers,″ Proceedings of 17th International Workshop on Post-Binary ULSI Systems, pp. 21--24, May 2008. 査読有
(24) Yuki Watanabe, Naofumi Homma, Katsuhiko Degawa, Takafumi Aoki, and Tatsuo Higuchi, ″High-level design of multiple-valued arithmetic circuits based on arithmetic description language,″ Proceedings of the 38th IEEE International Symposium on Multiple-Valued Logic, No. 31, pp. 112--117, May 2008. 査読有
(25) Atsushi Miyamoto, Naofumi Homma, Takafumi Aoki, and Akashi Satoh, ″Enhanced power analysis attack using chosen message against RSA hardware implementations,″ Proceedings of the 2008 IEEE International Symposium on Circuits and Systems, pp. 3282--3285, May 2008. 査読有
(26) Takeshi Sugawara, Naofumi Homma, Takafumi Aoki, and Akashi Satoh, ″High-performance ASIC implementations of the 128-bit block cipher CLEFIA,″ Proceedings of the 2008 IEEE International Symposium on Circuits and Systems, pp. 2925--2928, May 2008. 査読有
(27) Yuki Watanabe, Naofumi Homma, Takafumi Aoki, and Tatsuo Higuchi, ″Arithmetic module generator with algorithm optimization capability,″ Proceedings of the 2008 IEEE International Symposium on Circuits and Systems, pp. 1796--1799, May 2008. 査読有

〔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