算術演算LSIの高水準設計技術とその応用に関する研究

安全・安心な社会を担う算術演算LSIの統一的な設計技術を目指して

本間 尚文
東北大学　大学院情報科学研究科
准教授

研究の背景

情報化社会の深化により、身の回りのあらゆる機器にVLSIシステムが搭載されつつある。システムの性能を左右する算術演算回路（データパス）の性能は、デバイスレベルや論理レベル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。これまで、2進数に基づく算術アルゴリズムだけでなく、多進数系や冗長数系を用いた算術アルゴリズムも盛んに研究されており、それらが高い性能を発揮することも示されている。近年では、暗号処理やエラー訂正処理を行うアプリケーションが急速に拡大しており、そこで用いられるガロア体に基づく算術アルゴリズムの重要性も高まっている。今後もLSIシステムの応用の多様化に伴い、算術アルゴリズムを用途に応じて適切に設計する必要性はますます高まると予想される。

一方で、現在のVLSI設計技術は論理回路の合成手法を基本として発展しており、複雑化する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るとは言えない。現在、回路設計に一般的に用いられるハードウェア記述言語HDL（Hardware Description Language）は、非2進数系やガロア体上の演算を扱うための高水準なデータ構造や記法を持たない。このため、2進数系以外の算術アルゴリズムを設計する場合、2値論理信号を用いたおよそ直観的ではない低水準な記述を強いられる。また、一般に多入力多出力な算術演算回路では、その機能を計算機シミュレーションで検証するために膨大な時間が必要となる。現代の暗号処理では128ビット以上の入力となるため、計算機シミュレーションによる完全な検証はそもそも現実的に不可能である。暗号理論の分野では、暗号処理を実行する算術演算回路のバグを利用して秘密情報を奪う攻撃も報告されており、算術アルゴリズムを高速かつ完全に検証することは検証時間の面だけでなくセキュリティの面からも強く望まれている。

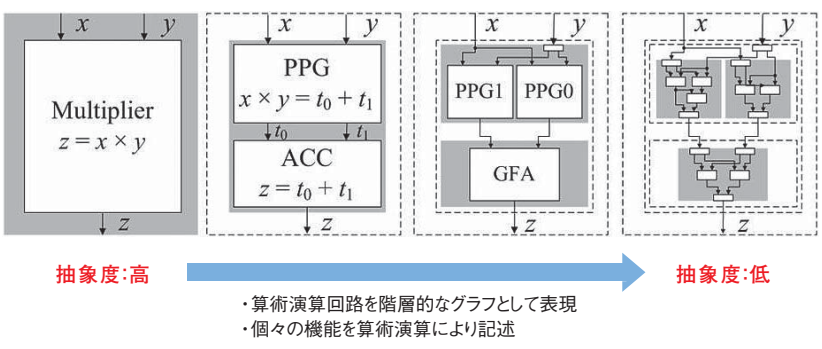
研究の成果

本研究では、上記のVLSIデータパスの設計問題を解決する新しい設計パラダイムとして、算術アルゴリズムの高水準な記述・検証・合成技術を開発してきた。

1. 算術アルゴリズムの形式的設計・検証手法の発案

本研究では、数系・数式に基づく算術アルゴリズムの統一的な表現手法を発案し、それに基づく設計技術を開発してきた。提案手法は、①算術アルゴリズムを算術的な方程式（整数方程式やガロア体方程式）により形式的に記述可能、②任意の重み数系・ガロア体を記述可能、③アルゴリズムの正当性を数式処理により静的かつ高速に検証可能、④正当性の証明された算術アルゴリズムを従来の論理式に等価変換可能などの特長を有する[1]。提案手法では、算術演算回路がしばしばそれ自身も算術演算機能を有する部分回路の組み合わせにより表現されることに着目し、部分回路の演算すべてをある数系上の変数による算術演算と見なして階層的に設計する（図1）。このとき、各回路の演算機能がその内部構造（部分回路の演算の組み合わせ）によって実現されるかどうかを調べる等価性判定により、算術演算回路の機能の正しさを検証することができる。本研究では、任意の重み数系の算術演算回路が提案手法により統一的に設計できることを明らかにするとともに、グレブナー基底を用いた多項式簡約アルゴリズムによる等価性判定を用いることで、128ビット以上の入力を持つ算術演算回路でも現実的な時間で完全な検証が可能となることを示した[2, 3]。

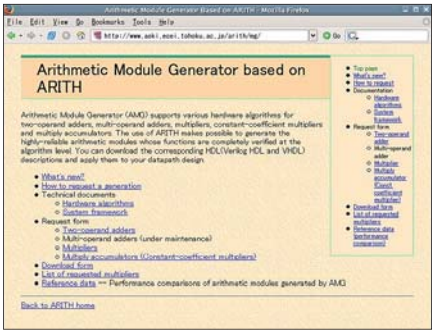
図1　算術演算回路記述（算術演算グラフ）の例



2. 算術演算モジュールジェネレータの開発

本研究では、上記の手法に基づく算術演算回路の合成・検証システム（モジュールジェネレータ）を開発し、インターネット上で公開した（図2）[4]。同システムは従来の論理合成では不可能だった1000種類以上の算術演算回路の合成を実現している。同合成・検証システムは、世界でも他に類を見ない規模と高い信頼性を備えており、欧米を中心に世界中から利用されている。2004年の公開以降、算術演算回路のダウンロード数は1万件、合成データへのアクセス数は33万件に達しており、最先端の製品開発から学術・教育用途まで幅広く応用されている。また、同検証システムは、グレブナー基底を用いた検証手法により、64ビットの算術演算回路であっても数分で検証を完了する。これは、従来の検証時間を100～1000分の1にまで削減している。

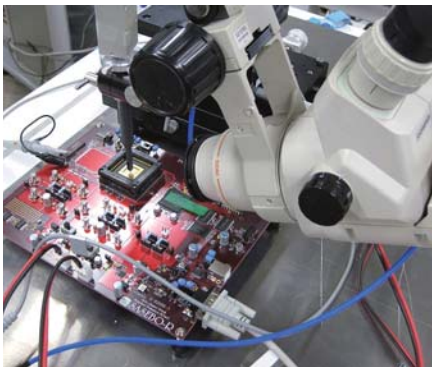
図2 公開中の算術演算モジュールジェネレータ



3. 暗号処理LSIの設計・検証への応用

本研究では、上記の手法を発展させ、暗号処理LSIの設計・検証技術にも応用してきた。例えば、公開鍵暗号として最もよく利用されているRSA暗号プロセッサの系統的な設計手法を開発するとともに、上記の検証手法を拡張することで国際標準共通鍵暗号の一つであるAES（Advanced Encryption Standard）の128ビットデータパスを完全に検証できることを実証している[5, 6]。また、産業技術総合研究所と共同で開発した暗号処理LSIの設計・評価用プラットフォーム（図3）は、NIST（米国国立標準技術研究所）をはじめとする国内外の多数の企業・大学・研究機関で採用されており、事実上の世界標準となっている。RSA暗号発明者のAdi Shamir教授（ワイツマン科学研究所）らと実施した共同研究では、多様なRSA暗号プロセッサ設計に有効な安全性検証手法を開発している[7]。

図3 暗号処理LSIの
設計・評価用プラットフォームによる評価の様子



将来の展望

本研究の手法は、実装するデバイスや回路技術に依らない汎用的な手法であり、次世代デバイス（単電子デバイス、分子デバイス、スピントロニクスデバイス等）の算術演算回路設計技術を確立する上でも重要な基盤技術になると考えられ、今後ますますの発展が期待される。

また、暗号処理LSI設計への応用では、近年脅威が指摘されている各種の物理攻撃への対策も含めて機能を完全に保証する暗号処理LSIの設計技術への展開が期待される。

本研究は、東北大学大学院情報科学研究科計算機構論分野を中心とした多くの共同研究者との共同研究に基づくものである。ここにあらためて関係各位に深く感謝する。

補足説明

ガロア体
有限の要素からなる四則演算（加減乗除）に閉じている集合である。暗号処理やエラー訂正処理では、主に素数2を法とする集合から得られた拡大体が利用される。

形式的検証
ハードウェアおよびソフトウェアのシステムにおいて、シミュレーションを用いずに仕様と実装が正しい（もしくは正しくない）ことを数学的に証明することで行う検証である。

グレブナー基底
多変数多項式の簡約化を一意に行える多項式の集合である。多変数の連立代数方程式の求解に利用される。

References（参考文献）

【1】Naofumi Homma, Yuki Watanabe, Takafumi Aoki, and Tatsuo Higuchi, “Formal Design of arithmetic circuits based on arithmetic description language,” IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Vol. E89-A, No. 12, pp. 3500–3509, December 2006.

【2】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, Dec 2008.

【3】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.

【4】Naofumi Homma, Yuki Watanabe, Kazuya Ishida, Takafumi Aoki, and Tatsuo Higuchi, “A multiplier module generator based on arithmetic description language,” Proceedings of the IP Based SoC Design Conference & Exhibition, pp. 207–212, December 2005.

【5】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.

【6】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.

【7】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, Jun 2010.