算術演算LSIの統一的な設計・検証技術の確立を目指して

東北大学　大学院情報科学研究科　准教授
本間　尚文

研究の背景

クレジットカードや家電製品など身の回りの様々な機器にLSI（大規模集積回路）がどんどん搭載されています。このLSIシステムの性能は、データを処理する算術演算回路のハードウェアアルゴリズム（算術アルゴリズム）に大きく左右されます。近年では、個人情報の保護や高信頼な電子商取引のために暗号処理やエラー訂正処理を行うLSIの応用が急速に拡大しており、そこで多用されるガロア体（有限体）上の算術アルゴリズムの重要性も高まっています。一方で、従来の回路設計手法は、ガロア体などを扱う高水準なデータ構造や記法を持たないため、その算術アルゴリズムの設計に直観的ではない膨大な2値論理記述が必要でした。また、算術演算回路は一般に多入力・多出力なため、従来の計算機シミュレーションで機能を完全に検証することは困難でした。こうした背景から、算術アルゴリズムの高水準な設計技術および高速・完全な検証技術の開発が強く望まれていました。

研究の成果

これまでの研究で、私は、任意の算術アルゴリズムがそれ自身も算術演算となる部分アルゴリズムの組み合わせによって階層的に構成できることに着目し、算術式表現に基づく算術アルゴリズムの統一的な設計理論を構築してきました。特に、設計した算術アルゴリズムと仕様として与えた機能との等価性を代数的な計算により判定することで、任意の算術アルゴリズムの機能を高速かつ完全に検証できることを示しました。また、提案した理論を応用して、従来は困難とされていた算術演算回路の自動合成・検証システムを開発しました（図1）。開発したシステムは、現在インターネット上で公開されており（http://www.aoki.ecei.tohoku.ac.jp/arith/）、これまで欧米を中心に学術・教育用途から最先端の製品開発にまで広く利用されています。近年では、同システムをガロア体上の算術アルゴリズムに拡張し、最もよく利用される国際標準暗号の1つであるAES（Advanced Encryption Standard）の算術アルゴリズムの完全な検証に世界で初めて成功しました。

今後の展望

本研究の手法は、実装するデバイスや回路技術によらない汎用的な手法です。そこで今後は、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など）の算術演算回路設計・検証にもこの提案手法を応用したいと考えています。また、暗号処理LSI設計への応用では、近年その脅威が指摘されている各種攻撃への対策も含めて、機能を完全に保証する設計技術の開発に取り組んでいきます（図2）。

関連する科研費

平成22-24年度　若手研究（A）「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」
平成25-28年度　基盤研究（A）「ガロア体算術演算に基づくVLSIデータパスの形式的設計技術の開拓」

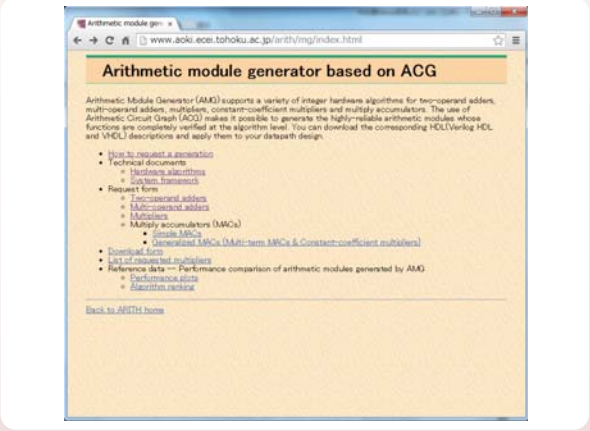

図1　公開中の算術演算モジュールジェネレータ

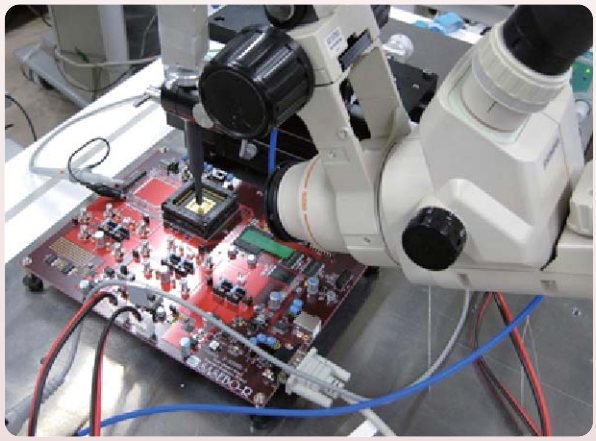

図2　設計したAES回路の安全性評価実験の様子