様　式　Ｃ－１９、Ｆ－１９、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成 ２７ 年　 ９ 月 １７ 日現在

機関番号：１２３０１
研究種目：基盤研究(C)（一般）
研究期間：2011～2014
課題番号：２３５０００５７

研究課題名（和文）最小ＳＤ数表現を用いた長い語長の剰余べき乗演算システムの研究

研究課題名（英文）Arithmetic system using minimal signed-digit number representation for residue exponential operations with long word length

研究代表者
魏　書剛（Wei, Shugang）

群馬大学・大学院理工学府・教授

研究者番号：１０２５１１２５

交付決定額（研究期間全体）：（直接経費）　　2,400,000円

研究成果の概要（和文）：長い語長を持つ剰余演算アルゴリズムの提案および剰余演算システムの設計評価を実施した。ＳＤ数表現の符号化を検討し、遅延時間の最適な剰余加算回路構成を考察した。そして、長い語長の剰余乗算について、新しい符号化を使用した直列型剰余乗算回路を構築した。最小ＳＤ数表現を用いることにより、ハードウェア規模と動作周波数との両方においても性能が大幅に改善された。これらの演算回路を用いた長い語長の剰余べき乗演算のＲＳＡ暗号化処理回路を設計した。計算回数を有効に減らすアルゴリズムを開発するため、ＳＤ数表現を最小ＳＤ数表現へ変換する回路の改良方法も行った。設計評価により提案の演算システムの高速性が確認できた。

研究成果の概要（英文）：New algorithms using minimal signed-digit (SD) number representation for the residue exponential operations with long word length were presented. A binary recoding method for the SD number is used for implementing the residue additions. By applying the recoding and the minimal signed-digit number representation, the residue addition circuit performance was modified. The proposed residue arithmetic circuits can be applied for the implementation of the RSA encryption with very long word length. To reduce the complexity of the residue operations, an efficient algorithm has been also proposed to obtain the minimal signed-digit number representations.
The design and simulation results show that high-speed exponential operations can be implemented by the proposed method.

研究分野：情報工学

キーワード：最小ＳＤ数表現　ＶＬＳＩシステム　算術演算システム　剰余演算

１．研究開始当初の背景

剰余演算および剰余数系における算術演算は、現在信号処理、データ通信、暗号処理、情報セキュリティなどの分野において応用され、その高速化が、ますます重要な研究課題となってきている。

剰余数系における剰余数演算について、様々な方法が提案されている。それらの方法が従来の２進数演算に依存するため、回路システムアーキテクチャのみを工夫することが多い。例えば、High-speed parallel-prefix VLSI ling adders, Giorgos Dimitrakopoulos and Dimitris Nikolos, IEEE Trans. on Computers, Vol. 54, no. 2, 225-231 (2005)、**Efficient diminished-1 modulo 2^n+1 multipliers,** Costas Efstathiou 他, IEEE Trans. on Computers, Vol. 54, no. 4, 491-496(2005) による研究結果によりも、２進数加算を用いたため、高速化の回路構成においては、剰余部分積の剰余加算回路部分は非常に複雑な構成になってしまう。

暗号による情報保護の応用分野において、語長が極めて長い剰余演算に基づく公開鍵暗号が主流となり、コンピュータ通信などで幅広く利用されている。しかし、安全性のため、2048 ビット長の鍵を使うことが必要とされており、暗号化処理の速度がますます重要な課題とされている。我々は、剰余数の冗長な数表現を定義することにより、符号桁付き（Signed-Digit,ＳＤ）数表現を剰余演算に導入するという新しい概念を提案した。従来の非冗長な剰余数系には適用できないため、我々は、ＳＤ数演算の優れた演算性質を冗長な剰余数系に適用できる概念に基づき、定数の剰余加算時間で語長に依存しない剰余加算アルゴリズムを提案した。

提案のアルゴリズムにより、剰余加算の演算数の語長が長くなっても、剰余演算が一段のＳＤ数加算により実現される。この剰余加算回路を暗号処理の剰余演算に使うことにより、高速な暗号処理につながる。

２．研究の目的

本研究では、冗長な数表現、SD(Signed-Digit)数を剰余数演算に適用することにより高速剰余演算を実現することを着目し、特に語長が極めて長い公開鍵暗号のための高速剰余演算アルゴリズムの提案を目的とする。ＲＳＡ暗号方式が広く使われている現在、暗号の安全性を保証するために、2048ビット長の鍵が必要とされている。法の補数を用いて剰余加算演算を行うことにより、剰余演算が簡単に行われる。また、鍵とした整数を最小SD数表現で表現し剰余乗算および剰余加算の回数を大きく減らし、並列な演算ができる処理回路を開発したい。また、剰余数系による並列演算を暗号処理に導入することを挑戦し、より高速暗号処理システムを実現する。

３．研究方法

いままでの剰余べき乗演算の方法について調査を行った。数学の手法による解析および実験による考察などを実施することにより、それらの方法による高速処理の問題点を明確にした。そして、現在考えている最小ＳＤ数表現を用いた方法について、計算量などを検討し、どれだけの高速化を達成する可能か、解析を行った。アルゴリズムの詳細について、具体的な回路設計を行う前提で、基本的な演算アルゴリズムやアーキテクチャを構築した。また、剰余数系における算術演算を用いて、語長の長い演算をいくつかの語長の短い演算により実現することを考えた。本研究の一部として、理論的な性質を究明することを行った。そのなか、関係の数表現間の変換処理アルゴリズムの高速化、並列なアーキテクチャの構築、さらにメモリや演算回路の詳細設計も重要な検討課題とした。

アルゴリズムをＶＬＳＩに実装するため、暗号化処理システムの評価を行った。具体的に、各演算の機能ブロックについて回路設計について、高性能を重視した詳細設計も実施した。指導している博士後期課程学生（２名）および修士学生（数名）が本研究に参加し、アルゴリズムの詳細や回路設計・性能評価などを担当する。

４．研究成果

長い語長を持つ剰余演算アルゴリズムおよび剰余演算システムの高速化について、Signed-Digit（ＳＤ）数による演算回路の高速化、演算回数の最小化および演算の並列化を実現するため、アルゴリズム詳細の解析や実装を行い、問題点を解析した。まず、ＳＤ数表現の剰余加算の高速化のため、符号化などを検討し、回路コストと遅延時間の最適な剰余加算回路構成を考察した。具体的に、２進ＳＤ数の３値を２値符号の２ビットで表現することについて、すべての符号化可能な組み合わせ（２４通り）を行い、ハードウェア記述言語ＶＨＤＬによる回路設計と性能評価を実施した。剰余加算時間は、２つのＳＤ数加算時間より短くなり、以前提案したＳＤ数を用いた剰余加算回路より70%に短縮された。そして、長い語長の剰余乗算について、高速なＳＤ数剰余加算アルゴリズムを用いることにより、新しい符号化を使用した直列型剰余乗算回路を構築した。従来の剰余加算回路の一部を使った構造となったため、ハードウェア規模と動作周波数との両方においても性能が大幅に改善された。さらに、これらの演算アルゴリズムおよび演算回路を用いた長い語長の剰余べき乗演算のＲＳＡ暗号化処理回路を設計した。２つの直列型剰余乗算を用いた回路構成を提案し、２０２４ビットの語長でも、高速に暗号化処理を可能にし、１つのＶＬＳＩチップに実装できることが分かった。また、ＳＤ数表現から最小ＳＤ数を求めるアルゴリズムを提案し、改良のアルゴリズムを用いる回路構成を考察した。ＳＤ数表現を最小ＳＤ数表現へ変換する回路の改良方法も行った。長い語長をもつ演算システムに、最小ＳＤ数表現を有効に利用できることを明らかにしている。

また、長い語長を有する算術演算を語長の短い剰余演算により実現することを考案している。剰余数系の数表現と重み数表現との相互変換について、関連の研究成果として、最小ＳＤ数演算の符号化を用いて高速変換手法を提案した。また、最小ＳＤ数表現を用いて並列剰余乗算や平方演算の高速アルゴリズムの提案および回路実装による評価を行った。

これらの研究結果は、学術雑誌、ワークショップおよび国際会議にて発表された。

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　16 件）

1. Conversions between RNS and Mixed-Radix Numbers Using Signed-Digit Arithmetic, Wei S. 査読有 IEEE Proceedings of ISIC-2014, 600-603 Dec. 2014.
2. Residue Checker Using Optimal Signed-Digit Adder Tree for Error Detection of Arithmetic Circuits, Wei S., 査読有 IEEE Proceedings of TENCON2014, Paper ID: 00439, PID00439, Oct. 2014.
3. Efficient Squaring Circuit Using Canonical Signed-Digit Number Representation, Tanaka Y. Wei S., 査読有 IEICE Electronics Express, Vol.11, No.2, 1-9, 2014.

4. An Advanced Implementation of Canonical Signed-Digit Recoding Circuit, Tanaka Y., Wei S., 查読有 Journal of Communication and Computer, Vol.10, No.11,1396-1402 2013.
5. Efficient Implementations of Canonical Signed-Digit Recoding Algorithm, Tanaka Y., Zhang Y., Wei S., 查読有 Proceedings of ICDV2013, 67-72, Nov. 2013.
6. Recoding Algorithms for Minimal Signed-Digit Numbers in Residue Number System, Zhang Y., Tanaka Y. and Wei S., 查読有 IEEE Proceedings of TENCON2013, Paper ID: 422, Oct.2013.
7. Residue-Weighted Number Conversion Using Signed-Digit Number for Moduli Set $\{2^{2n}-1, 2^{2n+1}+1, 2^n\}$, Jiang C., Wei S., 査読有 Analog Integrated Circuits and Signal Processing, Vol. 77, no.2, 105-112, 2013.
8. High-Speed Modular multipliers Based on a New Binary Signed-Digit Adder Tree Structure, Zhang M., Wei S., 査読有 Journal of Circuits, Systems, and Computers, Vol. 22, no.6, pp.1350043(18 pages) (DOI: 10.1142/S0218126613500436) 2013.
9. New Binary Modular Adder Tree Structure for Arithmetic of Error Checker of Arithmetic, Zhang M., Wei S., 査読有 Journal of Communication and Computer, Vol.10,No.3, 295-300, 2013.
10. Residue-Weighted Number Conversion for Moduli Set $\{2^n-1, 2^n+1, 2^{2n}+1, 2^n\}$ Using Signed-Digit Number, Jiang C. Wei S., 査読有 Journal of Circuits, Systems, and Computers, Vol. 22, no.1, pp.1250070(17 pages) (DOI: 10.1142/S0218126612500703) 2013.
11. Residue-Binary Number Conversion Using Signed-Digit Arithmetic for a Three-Moduli Set, Wei S., 査読有 IEEE Proceedings of TENCON2012, 371-374, 2012.
12. An RSA encryption Implementation Method Using Signed-Digit Arithmetic Circuits, Wei S., 査読有 IEEE Proceedings of 5th International Conference on Biomedical Engineering and Informatics, 1337-1341, 2012.
13. Sequential Modular Multipliers Using Residue Signed-Digit Additions, Journal of Communication and Computer, Wei S., 査読有 Vol. 9, No.8, 872-878, 2012.
14. Residue Signed-Digit Arithmetic and the Conversion between Residue and Binary Numbers for a Four-Moduli Set, Proceedings of 11th International Symposium on

Distributed Computing and Applications to Business, Engineering and Science, Wei S., and Jiang C., 査読有 436-440, 2012.

15. A Sequential Modular Multiplication Algorithm Using Signed-Digit Additions, IEEE Proceedings of TENCON2011, Wei S., 査読有 370-374, 2011.
16. Efficient Residue Checker Using New Binary Modular Adder Tree Structure for Arithmetic of Error Detection, Proceedings of Eighth International Conference on Fuzzy Systems and Knowledge Discovery, Zhang M., Wei S., 査読有 2481-2485, 2011.

〔学会発表〕（計 6 件）

1. 剰余ＳＤ数演算回路を用いた算術演算誤り検出，根間，田中，茂木，魏，電子情報通信学会研究報告，VLD2014-136,, 151-156, 2014.
2. 剰余ＳＤ数の非零桁数を削減する変換アルゴリズム，田中，魏，第２５回回路とシステムワークショップ論文集，156-159, 2013.
3. ＳＤ数の２値符号化による算術演算回路の最適化設計と性能評価，小林，茂木，魏，信学技報，115，39-44，2013.
4. ＳＤ数演算を用いたＲＳＡ暗号処理回路の設計の性能評価，浅岡，田中，魏，信学技報，115，45-50，2012.
5. ＳＤ数演算を剰余数系一重み数系変換アルゴリズム，新井，田中，魏，電子情報通信学会研究報告，VLD2011-110，111-116，2012.
6. ２分木構造の剰余ＳＤ数演算を用いた算術演算エラー検出回路，劉，茂木，魏，電子情報通信学会研究報告，VLD2011-110，117-121，2012.

〔図書〕（計 0 件）

〔産業財産権〕
○出願状況（計 0 件）

名称：
発明者：
権利者：
種類：
番号：
出願年月日：
国内外の別：

○取得状況（計 0 件）

名称：
発明者：
権利者：
種類：
番号：
出願年月日：
取得年月日：
国内外の別：

〔その他〕
ホームページ等

６．研究組織
(1)研究代表者
魏 書剛（Wei Shugang）
群馬大学・大学院理工学府・教授
研究者番号：10251125

(2)研究分担者
（ ）
研究者番号：

(3)連携研究者
（ ）
研究者番号：