特別研究報告書

題　　目

冗長二進数を用いたRSA用乗算器の高速化

High-Speed Multiplication for RSA Code
using Redundant Binary System

指 導 教 員

矢野　政顕　　教授

報 告 者

学籍番号：1065085

氏名：松村　暢也

平成 16 年　2 月　16 日

高知工科大学　電子･光システム工学コース

内容梗概

本論文は著者が高知工科大学大学院工学研究コース修士課程在学中に行ってきた冗長二進数を用いた RSA 用乗算器の高速化に関する研究成果をまとめたものである。

情報をやりとりする通信の分野では、いかにして情報を伝達するか、また情報の重要度によっては、いかにして送信者、受信者以外の第三者から情報を守るかといったことが研究され続けている。このことは、高度情報化社会いわれる現在の社会で、いかに情報に価値があるかということを物語っている。情報の価値が高くなったことで、一般の生活にまで暗号化技術が浸透している。暗号は情報の秘匿と認証に用いられている。暗号を用いる認証の例には電子署名がある。このようにさまざまな面で活用されている暗号には、大きく分けて二つの種類がある。一つは共通の鍵を使用して暗号化、復号化を行う「共通鍵暗号」、もう一つは秘密鍵と公開鍵という二種類の鍵を用いる「公開鍵暗号」である。公開鍵暗号を用いた方が鍵数を少なくできるため、現在、通信等では公開鍵暗号が広く用いられている。

しかし、公開鍵暗号は暗号化する際に複雑な演算を行わなければならない。そのため、通信などで暗号化が用いられるためには高速な処理が必要となる。そこで、本論文では乗算剰余演算を高速に行うための回路として冗長二進数を用いた乗算器を提案する。そして、FA を用いた二種類の乗算器との演算時間とゲート数の比較を行った。比較を行った結果、演算速度については入力のビット数が増加した場合、冗長二進数を用いた乗算器が FA を用いたものより高速であり、入力ビット数増加による演算時間の増加率も小さいという結果が得られた。また、部分積生成にあたる AND 回路に Booth デコーダを適用することで更に高速化が期待できる。しかし、ゲート数に関しては冗長二進数を用いた乗算器が FA を用いたものと比べて三倍程度増加した。これは、FA の入力ビット数に対して冗長二進加算器の入力ビット数が二倍になることに関係し、そのため回路規模が大きくなってしまう。今後の課題としては、冗長二進数を用いた乗算器の高速性を維持しつつ回路規模を低減させることである。

本論文の第 1 章では研究の背景、目的について述べ、第 2 章では RSA 暗号の演算方法と従来の乗算方法について説明する。第 3 章では冗長二進数を用いた乗算器について提案する。第 4 章では従来手法の乗算器と提案手法の乗算器について演算速度と面積についての比較・検討結果について述べる。最後に第 5 章では本研究で得られた成果を要約し、今後に残された課題について述べ、結論とする。

なお、本研究は東京大学大規模集積システム設計教育研究センターを通し、シノプシス株式会社の協力で行われたものである。

This paper summarizes High-Speed Multiplication for RSA Code using Redundant Binary System, which is performed for the degree of Master at the Graduate School of Engineering, the Kochi University of Technology.

In the communication field, many researches have been carried out into encryption, which is used to protect communication from unauthorized transmitter and receiver. This means that the information becomes more and more valuable in modern society; so-called an advanced information society. The encryption technology becomes popular in a daily life because the value of information is recognized higher and higher. Cipher is used for information secrecy and authentication. The electronic signature is one example of authentication using cipher. The cipher is classified into two types. The one is common key cryptography, which perfumes encryption and decryption using a common key. The other is public key cryptography, which uses two keys; a secret key and a public key. Recently, the public key cryptography is used in communication area, because of its small number of keys comparing to the common key cryptography.

The public key cryptography, however, requires complicated arithmetic operation for encryption and decryption. Therefore, high speed arithmetic processing is necessary in transmitters and receivers'. This paper proposes a multiplier using Redundant Binary System (RBS) as a circuit that performs index and surplus calculations at high speed. We compared the multiplier using RBS with two kinds of multipliers using Full-Adder (FA), with regard to data arrival time and gate count. As for data arrival time, the multiplier using RBS is faster than the multipliers using FA, and this tendency is grown when the number of input data bits is increased. Improvement in the speed is expected when Booth decoder is applied to the partial product generation. As for gate count, the multiplier using RBS requires more gates than the multipliers using FA. Future researches should focus on the reduction of gate count.

This paper consists of 5 Chapters. The first Chapter describes background and purpose of this research. Chapter 2 explains the arithmetic operation method of RSA code comparing with ordinary ones. In Chapter 3, we propose the multiplier using RBS, and Chapter4 shows the comparison results of multipliers regarding to data arrival time and gate count. Finally, Chapter 5 summarizes this paper suggesting future research subjects.

This work is supported by VLSI Design and Education Center (VDEC), the University of Tokyo in collaboration with Rohm Corporation and Synopsys, Inc.