特別研究報告書

高速乗算器の TEG 設計及び特性評価

Design and Characteristic Analysis
of High Speed Multipliers

指 導 教 員

矢野 政顯　教授

報 告 者

学籍番号：1065008

氏名：石川 純平

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なってきた高速乗算器の試作チップ設計および特性評価に関する研究成果をまとめたものである。

近年、我々の日常生活において、携帯電話・ディジタルカメラをはじめとする様々なディジタル電化製品の急激な普及が進むにつれ、マイクロプロセッサおよびディジタル信号処理プロセッサ（Digital Signal Processor；DSP）という言葉を頻繁に耳にするようになってきた。これらは論理 LSI の代表的なものであり、その集積度および処理性能は飛躍的な発展を遂げている。DSP などの代表的な論理 LSI に使用されているのが乗算器である。このような乗算器はディジタル信号処理で繰り返し用いられる積和演算をより高速に処理するために高速性が要求される。

このような要請に応えるため、本研究は 8 ビット×8 ビットの高速乗算器の設計および特性評価を目的とした。高速乗算器の設計に必要な設計データを得るために、N-MOSFET、P-MOSFET および CMOS インバータを設計評価した。この設計にはチャンネル長が 0.18 μm、有効電圧は 1.8V の VDEC 日立の設計ルールを使用した。この経験をもとに続いて高速乗算器を設計評価した。設計にはチャンネル長が 0.35 μm、有効電圧 3.3V の設計ルールを使用し、レイアウトツールとして Layout Plus4.4.6 を用いた。試作は VDEC を通じて行い、試作品を入手して評価した結果マニュアル設計の部分でいくつかのレイアウト設計ミスがあったが当初の目的をほぼ達成した。

本論文は第 1 章で、この研究の目的および背景について述べる。第 2 章では CMOS インバーターライブラリの基礎的な設計技術および設計について述べる。第 3 章では MOSFET および CMOS インバータの設計と特性評価について触れる。また、第 4 章では、高速乗算器の設計について説明する。第 5 章では、高速乗算器試作チップの評価について述べる。最後に第 6 章で本研究の成果のまとめと今後の課題について述べる。

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、株式会社日立製作所、ローム株式会社、ケイデンス株式会社の協力で行われたものである。

A communicative field exchange with information to study, however communicate to information; moreover it depend on importance of information, however defend information from except transmitter and receiver. These matters relating that information is valuable in present society called an advanced information society. The encryption technology is penetrating through a general life because informational worth became high. Cipher is using for information secrecy and authentication. There is electronic signature as an example of authentication using cipher. Thus, cipher is active in various cases; moreover it can roughly classify into two kinds. One is a “common key cryptography” which performs encryption and decryption using a common key. Another is a “public key cryptography” which using two keys called secret key and public key. Then, the “public key cryptography” is used in communication now

However, “public key cryptography” must do complicated operation. Therefore, high speed processing is necessary to communication using encryption. Accordingly, in this paper suggest that “multiplier using Redundant Binary System” as the circuit so as to do “index calculation and surplus calculation” at high speed. So, I compared “multiplier using Redundant Binary System” with two kinds of “multipliers using Full-Adder” with regard to “Data arrival time”, “The number of Gate” and “Power”. As a result of suggestion, “multiplier using Redundant Binary System” increase degrees of three times than “multipliers using Full-Adder” with regard to “The number of Gate” and “Power”. But, a result is obtained that “multiplier using Redundant Binary System” is more rapidly than “multipliers using Full-Adder”, and It was the result that the rate of increase of “Data arrival time” by the increase in the number of input bits was small. Moreover, improvement in the speed is further expectant by applying “Booth-decoder” to “AND-circuit” equivalent to partial product generation. As a future subject, it is performing reduction of “The number of Gate” and “Power”, maintaining rapidity of “multiplier using Redundant Binary System”.

Chapter 1 of this paper describes a research background and the purpose and Chapter 2 explains the operation method of RSA code and usual. Chapter 3 suggests “multiplier using Redundant Binary System”. Chapter 4 describes about the finding of the research of “Data arrival time”, “The number of Gate” and “Power”. Lastly, Chapter 5 describes a future subject on the basis of the result of this research.