IEEE TRANSACTIONS ON

VERY LARGE SCALE INTEGRATION (VLSI) SYSTEMS

A JOINT PUBLICATION OF THE IEEE CIRCUITS AND SYSTEMS SOCIETY
THE IEEE COMPUTER SOCIETY
THE IEEE SOLID-STATE CIRCUITS SOCIETY

JUNE 1997 VOLUME 5 NUMBER 2 IEVSE9 (ISSN 1063–8210)

PAPERS

TRANSACTIONS BRIEFS

CALLS FOR PAPERS

INFORMATION FOR AUTHORS

The IEEE TRANSACTIONS ON VERY LARGE SCALE INTEGRATION (VLSI) SYSTEMS is published quarterly. Contributed papers may be of a tutorial nature. Transactions Briefs include contributions of the following nature: corrections; rebuttals of previous briefs; comments on published results; discussion of experiences using published results; conjectures; posing of new problems; announcement of new results and other contributions written in the format of a correspondence. Research papers must be of original contributions and must not duplicate descriptions or derivations available elsewhere. The author should limit paper length whenever this can be done without impairing quality.

If a contribution is of sufficient general interest to the entire IEEE membership, it will be recommended for publication in the PROCEEDINGS OF THE IEEE. Submission of a manuscript manifests the fact that it has been neither coprighted, published, nor submitted for publication elsewhere, unless otherwise so stated by the author.

To avoid delay, please be guided by the following suggestions.

A. Process for Submission of a Technical Paper

1) Send to the Editor-in-Chief a postscript version of your manuscript to (http://microsys6.engr.utk.edu/~tvlsi), seven copies of y manuscript, each copy complete with illustrations, abstract, and indexterms.
2) Enclose a signed copyright form with your manuscript. (You may reproduce the copyright form.)
3) Enclosed with each manuscript, on a separate page five to ten index terms (key phrases). These terms should be alphabetized, relative , independent (coordinate index terms), and as a group should optimally characterize the paper.
4) Enclose originals for the illustrations (including tables) in the style described below. Alternatively, good quality copies may be sent initially, with the originals ready to be sent immediately upon acceptance of the paper.
5) Enclose a separate page giving your preferred address for correspondence and return of page proofs.
6) Enclose a technical biography and photograph of each author for a paper (not a Transactions Brief), or be ready to supply these upon acceptance of a paper.
7) The referee process assumes the anonymity of the reviewers of your paper. It is also possible to provide a review in which the author's identity is also kept from the reviewers. Should you wish to take advantage of this provision, please make your desires explicit in this regard in your cover letter to the Editor-in-Chief. In this case, make sure that your name appears only on a removable cover page.
8) If the manuscript has been presented, published, or submitted for publication elsewhere, please so inform the Editor-in-Chief. Our primary objective is to publish technical material not available elsewhere, but on occasion we publish papers of unusual merit that have appeared or will appear before other audiences.

B. Style for Manuscript

1) The manuscript should be typewritten or printed double-spaced, one side only, using a font size of 11 points or larger. (Good office-duplicated copies are acceptable.)
2) Provide an informative 100-250 word abstract, at the head of the manuscript, to appear with the paper.
3) Provide a separate double-spaced sheet using all footnotes, beginning with "Manuscript received _______________" continuing with an "Acknowledgment of financial support" and "Affiliation of author."
4) References must appear as a separate bibliography at the end of the paper, with items referred to by numerals in square brackets, e.g., [12]. References should be complete and in IEEE style (see item 6).
   Style for papers: Author, first initials followed by last name, title, volume, inclusive page numbers, month, year.
   Style for books: Author, title, location of publisher, year, chapter, or page numbers (if desired).
5) Provide a separate sheet listing all figure captions, in proper IEEE style, e.g., "Fig. 6. The final 32-bit adder design."
6) For further information, see the booklet, *Information for IEEE Transactions and Journal Authors*, available from the IEEE Operations Center, Transactions/Journal Department, 445 Hoes Lane, P.O. Box 1331, Piscataway, NJ 08855-1331.

C. Style for Illustrations

1) Originals for illustrations should be sharp, noise-free, and of good contrast. We regret we cannot provide drafting or art service.
2) Line drawings should be in India ink or drafting cloth, paper, or board. Use only 8-1/2 in by 11-in size sheets, to simplify handling of the manuscript.
3) On graphs, show only the coordinate axes, or at most the major grid lines, to avoid a dense hard-to-read result.
4) All lettering should be large enough to permit legible reduction of the figure to column width, perhaps as much as 4:1. Typing on figures is not acceptable.
5) Photographs should be glossy prints, of good contrast and gradation, and any reasonable size.
6) Identify each original on the back, or at the bottom of front, and indicate the author's name.
7) Note B-5) above. Captions lettered on figures will be blocked out in reproduction, in favor of typeset captions.

D. Final Manuscripts in Electronic Form

If a manuscript is accepted for publication, the author will be asked to supply an electronic or magnetic form of the manuscript via email disk, or tape, and two matching hard copies. The IEEE can process most software, but not page layout programs. Do not send postscript files

E. Page Charges

After a manuscript has been accepted for publication, the author's company or institution will be approached with a request to pay a charge of $110 per page. Payment of page charges for this IEEE TRANSACTIONS is not obligatory; nor is it a prerequisite for publication. The author will receive 100 reprints (without covers) free only if the page charge is honored. Detailed instructions will accompany the page proofs.

F. Copyright

It is the policy of the IEEE to own the copyright to the technical contributions it publishes on behalf of the interests of the IEEE, its authors, and their employers, and to facilitate the appropriate reuse of this material by others. To comply with the U.S. Copyright Law, authors are required to sign an IEEE copyright transfer form before publication. This form, a copy of which appears in the March 1997 issue of this TRANSACTIONS returns to authors and their employers full rights to reuse their material for their purposes. Authors must submit a signed copy of this form with their manuscript.

IEEE TRANSACTIONS ON VERY LARGE SCALE INTEGRATION (VLSI) SYSTEMS

The Circuits and Systems Society is an association of IEEE members with professional interest in the field of circuits and systems theory. All members of the IEEE are eligible for membership in the Society upon payment of the annual Society membership fee of $7.00. The Computer Society is an association of people with professional interest in the field of computers. All members of the IEEE are eligible for membership in the Computer Society upon payment of the annual Society membership fee of $29.00. For information on joining, write to the IEEE Computer Society, 1730 Massachusetts Avenue, NW, Washington, DC 20036-1903. The annual subscription fee for members of either society is $18.00. For information on joining, write to the IEEE at the address below. *Member copies of Transactions/Journals are for personal use only.*

IEEE TRANSACTIONS ON VERY LARGE SCALE INTEGRATION (VLSI) SYSTEMS (ISSN 1063–8210) is published quarterly by The Institute of Electrical and Electronics Engineers, Inc. Responsibility for the contents rests upon the authors and not upon the IEEE, the Society/Council, or its members. **IEEE Corporate Office:** 345 East 47 Street, New York, NY 10017-2394. **IEEE Operations Center:** 445 Hoes Lane, P.O. Box 1331, Piscataway, NJ 08855-1331. **NJ Telephone:** 908-981-0060. **Price/Publication Information:** Individual copies: IEEE Members $10.00 (first copy only), nonmembers $20.00 per copy. (Note: Add $4.00 postage and handling charge to any order from $1.00 to $50.00, including prepaid orders.) Member and nonmember subscription prices available upon request. Available in microfiche and microfilm. **Copyright and Reprint Permissions:** Abstracting is permitted with credit to the source. Libraries are permitted to photocopy for private use of patrons, provided the per-copy fee indicated in the code at the bottom of the first page is paid through the Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923. For all other copying, reprint, or republication permission, write to Copyrights and Permissions Department, IEEE Publications Administration, 445 Hoes Lane, P.O. Box 1331, Piscataway, NJ 08855-1331. Copyright © 1997 by The Institute of Electrical and Electronics Engineers, Inc. All rights reserved. Periodicals Postage Paid at New York, NY and at additional mailing offices. **Postmaster:** Send address changes to IEEE TRANSACTIONS ON VERY LARGE SCALE INTEGRATION (VLSI) SYSTEMS, IEEE, 445 Hoes Lane, P.O. Box 1331, Piscataway, NJ 08855-1331.

Pipelined H-Trees for High-Speed Clocking of Large Integrated Systems in Presence of Process Variations

Mohamed Nekili, Guy Bois, and Yvon Savaria, *Member, IEEE*

***Abstract*—This paper addresses the problem of clocking large high-speed digital systems, as well as deterministic skew modeling, a related problem. A conventional method for clocking a large digital system is to use a set of metallic lines organized as a tree. This method is limited by the bandwidth of the clock network. Another limitation of existing solutions is that available skew models do not directly take into account process variations. In order to provide a reliable skew model, and to avoid the frequency limitation, we propose a novel approach that distributes the clock with an H-tree, whose branches are composed of minimum-sized inverters rather than metal. With such a structure, we obtain the highest clocking rate achievable with a given technology. Indeed, clock rates around 1 GHz are possible with a 1.2 μm CMOS technology. From the skew modeling standpoint, we derive an analytic expression of the skew between two leaves of the H-tree, which we consider to be the difference in root-to-leaf delay pairs. The skew upper bound obtained has an order of complexity which, with respect to the H-tree size D, is the same as the one that may be derived from the Fisher and Kung model for both side-to-side and neighbor-to-neighbor communications, i.e., a $\Omega(D^2)$, whereas, the Steiglitz and Kugelmass probabilistic model predicts $\Theta(D \times \sqrt{\mathrm{Log}\, D})$. In an H-tree implemented with metallic lines, the leaf-to-leaf skew is obviously bounded by the delay between the root and the leaves. However, with the logic based H-tree proposed in this paper, we arrive at a nonobvious result, which states that the leaf-to-leaf skew grows faster than the root-to-leaf delay in presence of a uniform transistor time constant gradient. This paper also proposes generalizations of the skew model to 1) the case of chips in a wafer subject to a smooth, but nonuniform gradient and 2) the case of H-tree configurations mixing logic and interconnections; in this respect, this paper covers the H-tree configurations based on the combination of logic and interconnections.**

***Index Terms*—H-tree, high-speed clocking, pipelining, process variations, skew.**

I. Introduction

THE evolution of VLSI chips toward larger die sizes and faster clock speeds makes clock design an increasingly important issue. A striking example of what can be accomplished with aggressive clock design is the DEC alpha chip [1], designed to operate at more than 200 MHz. At such speeds, clock skew becomes a very significant problem. Available literature dealing with skew [2]–[8], [10], [11] approaches the problem both from deterministic and probabilistic standpoints.

In the deterministic approaches, Friedmann and Powell [6] emphasize the use of a hierarchical clock distribution, while others [2], [3], [8], [11] suggest the length equalization of the different paths followed by the clock throughout the circuit. Shoji [5] suggests an approach that guarantees a symmetry between paths that contribute to propagate "0" and "1." This symmetry ensures proper operation despite some types of process variations [5]. Except for the work of Fisher and Kung [4], which provides bounds on skew, the other authors do not deal with the analytic modeling of system skew.

In the probabilistic approaches, Kugelmass and Steiglitz [7] consider the delay of a clock signal along a given path as a sum of delays along path segments, each of these segments behaving according to a probabilistic law. Then, by assuming independence between these delays, the total delay, as well as the skew, can then be described by a normal law. By assuming independence and the linearity of delay with line length, their approach becomes an oversimplification of the reality. Other authors [10] consider the skew as a dispersion in the physical parameters of a circuit (e.g., geometrical dimensions) and in the process (e.g., sensitivity to temperature).

The work that is most directly related to that presented in this paper is the work of Fisher and Kung [4]. These authors have developed two deterministic skew models (the difference model and the summation model), from which they determined bounds on skew. However, these models do not directly refer to a process variation model. The difference model tends to be unrealistically optimistic, whereas, under the summation model, Fisher and Kung reached a pessimistic result which states that, from a skew standpoint, synchronous systems are not feasible with large two-dimensional arrays.

In order to avoid the frequency limitation when using metallic lines, we propose a logic-based H-tree structure that provides the highest clocking rate achievable with a given technology in Section II. To provide a reliable skew model, Section III suggests a model based on delay differences combined with a model of electrical variations in the process parameters. Under this model, we derive an analytic expression of the skew between any leaf pair, which we consider to be the difference in root-to-leaf delay pairs. Even though the model of electrical variations described in this paper assumes

Manuscript received March 24, 1994; revised September 22, 1995. This work was supported by the INI (Institut National de formation en Informatique) in Algiers, CIDA (Canadian International Development Agency), and strategic grant and operating grants from the Natural Sciences and Engineering Research Council of Canada.

The authors are with the Department of Electrical Engineering, Ecole Polytechnique of Montréal, Station "Centre-Ville," Montréal, P.Q. H3C 3A7, Canada.

Publisher Item Identifier S 1063-8210(97)01949-5.

VLSI Array Algorithms and Architectures for RSA Modular Multiplication

Yong-Jin Jeong, *Member, IEEE,* and Wayne P. Burleson, *Member, IEEE*

***Abstract*—We present two novel iterative algorithms and their array structures for integer modular multiplication. The algorithms are designed for Rivest–Shamir–Adelman (RSA) cryptography and are based on the familiar iterative *Horner's* rule, but use precalculated complements of the modulus. The problem of deciding which multiples of the modulus to subtract in intermediate iteration stages has been simplified using simple look-up of precalculated complement numbers, thus allowing a finer-grain pipeline. Both algorithms use a carry save adder scheme with modulo reduction performed on each intermediate partial product which results in an output in carry-save format. Regularity and local connections make both algorithms suitable for high-performance array implementation in FPGA's or deep submicron VLSI. The processing nodes consist of just one or two full adders and a simple multiplexor. The stored complement numbers need to be precalculated only when the modulus is changed, thus not affecting the performance of the main computation. In both cases, there exists a bit-level systolic schedule, which means the array can be fully pipelined for high performance and can also easily be mapped to linear arrays for various space/time tradeoffs.**

***Index Terms*— Cryptography, modular multiplication, RSA, systolic arrays, VLSI.**

I. Introduction

CRYPTOGRAPHY systems have been growing in importance recently as a method for improving data security. *Public key cryptography* (PKC) systems are generally preferred to traditional *secret key cryptography* systems like the *data encryption standard* due to the safety of key distribution [3]. The Rivest–Shamir–Adelman (RSA) [10] system is one of the most widely used public key cryptography systems, and its core arithmetic is modular multiplication over a positive integer. Modular multiplication is also a major computation of *residue number systems* [13] as well as other cryptography systems (e.g., *international data encryption algorithm* [8], [16], Diffie–Hellman key exchange [3]). In this paper, we develop an array modular multiplier with applications to, but not restricted to, RSA systems.

In RSA, the modulus is a product of two large prime numbers, usually more than 500 bits, and should be changeable for security reasons. But, since the modulus (or key) is not changed very often, we can use precomputation and look-up in our array modular multipliers. We are not aware of anyone who has utilized this special property of *multirate input data* in the RSA algorithm, that is, the *input message* changes rapidly while the *key* remains unchanged for a long period. In practice, the key is updated infrequently, for example, a few months, weeks, or days, depending on the security requirements. In order to satisfy the ever growing security requirements of high-speed communications, such as personal communication services and wireless local area networks, a *dedicated* VLSI hardware solution is needed because of 1) high throughput requirements, 2) low-power requirements, 3) a high-volume market, 4) the computation is poorly suited to microprocessors or DSP's, and 5) the problem size is expected to continue to grow rather than saturate.

Modular multiplication is generally considered a complicated arithmetic operation because of the inherent multiplication and division operations. There are two main approaches to computing modular multiplication: 1) perform the modulo operation *after* multiplication or 2) *during* multiplication. The modulo operation is accomplished by integer division in which only the remainder is needed for further computation. The first approach requires a $n \times n$ bit multiplier with a $2n$-bit register followed by a $2n \times n$ bit divider. In the second approach, the modulo operation occurs in each iteration step of integer multiplication. Therefore the first approach requires more hardware while the second requires more addition/subtraction computations due to $O(n)$ modulo reduction steps. In both cases, most previous research has focused on the fast calculation of a long carry chain. Redundant number systems and a higher radix carry-save form are some of the different number representations that have been used for this purpose [12], [14]. A carry prediction technique has also been used for fast calculation of modular multiplication [1].

Since PKC was introduced, many algorithms and hardware structures have been proposed for modular multiplication, and [4] contains a good review on this topic. Several array structures suited for VLSI implementation have been discussed in [4], [5], [14], and [15]. In [14], Vandemeulebroecke *et al.*, use a *modulo after multiplication* approach using a *signed digit* number representation. It consists of two arrays: one for multiplication and the other for integer division. In [5], Koc and Hung apply Blakley's algorithm [2] and use a sign-estimation method by looking at the five most significant bits in each iteration stage. Although they derive a bit-level systolic array structure, the latency and clock cycle are relatively long due to the control node which estimates the sign of the intermediate result in each stage. In [4] and [15], Eldridge and

Manuscript received November 21, 1994; revised January 26, 1996. This work was supported in part by NSF Grant MIP-9108086.

Y. Jeong is with Samsung Electronics, Co., Seoul, Korea.

W. Burleson is with the Department of Electrical and Computer Engineer-

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.

WHAT WILL YOU BUILD? | **sales@docketalarm.com** | **1-866-77-FASTCASE**

fastcase®
Smarter legal research.