ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 2, March 2016

A Parallel Algorithm for Design of Hybrid Modular Parallel Prefix Adder

M.GOMATHI-PG Student

M.E in VLSI design, second year,
Department of E.C.E, Maha Barathi Engineering College. Chinnasalem.

***Abstract*—In this brief, the implementation of hybrid modular parallel prefix adder with effective prefix structure is analyzed. The prefix structure used in this is Han Carlson prefix structure. The proposed results show a significant delay reduction and area × time^2 improvements over adder with other prefix structure, all this at the cost of higher power consumption, which is the main reason preventing the use of parallel-prefix adders to achieve high-speed reverse converters in nowadays systems. Hence, to solve the high power consumption problem, novel specific hybrid parallel-prefix-based adder components that provide better tradeoff between delay and power consumption are herein presented to design reverse converters. A methodology is also described to design reverse converters based on different kinds of prefix adders. This methodology helps the designer for design and implementation of portable devices.**

***Index Terms*—carry look ahead adder, prefix structure, parallel-prefix adder, residue number system (RNS), reverse converter.**

I. INTRODUCTION

IN the world of battery-based and portable devices, the residue number system (RNS) can play a significant role due to its low-power features and competitive delay. The RNS can provide carry-free and fully parallel arithmetic operations for several applications, including digital signal processing and cryptography. However, its real usage requires forward and reverse converters to be integrated in the existing digital systems. The reverse conversion, i.e., residue to binary conversion, is a hard and time-consuming operation.

Hence, the problem of designing high-performance reverse converters has motivated continuous research using two main approaches to improve the performance of the converters: 1) investigate new algorithms and novel arithmetic formulations to achieve simplified conversion formulas and 2) introduce new moduli sets, which can lead to more simple formulations. Thereafter, given the final simplified conversion equations, they are computed using well-known adder architectures, such as carry-save adders (CSAs) and ripple-carry architectures, to implement carry-propagate adders (CPAs) and, more seldom, fast and expensive adders such as the ones with carry-look ahead or parallel-prefix architectures. In this brief, for the first time, we present a comprehensive methodology to wisely employ parallel-prefix adders in carefully selected positions in order to design fast reverse converters. The collected experimental results based on area, delay, and power consumption show that, as expected, the usage of the parallel-prefix adders to implement converters highly increases the speed at the expense of additional area and remarkable increase of power consumption. The significant growing of power consumption makes the reverse converter not competitive. Two power-efficient and low-area hybrid parallel-prefix adders are presented in this brief to tackle with these performance limitations, leading to significant reduction of the power delay product (PDP) metric and considerable improvements in the area-time2 product (AT2*)* in comparison with the original converters without using parallel-prefix adders.

The adders with the large complex gates will be too slow for VLSI, so the design is modularized by breaking it into trees of smaller and faster adders which are more readily implemented. For large adders the delay of passing the carry through the look-ahead stages becomes dominated and therefore tree adders or parallel prefix adders are used. High speed adders depends on the previous carry to generate the present sum. In integer addition any decrease in delay will directly relate to an increase in throughput. In nanometer range, it is very important

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 2, March 2016

to develop addition algorithm that provide high performance while reducing power. Parallel prefix adders are suitable for VLSI implementation since they rely on the use of simple cells and maintain regular connection between them. We can define each prefix structures in terms of logic levels, fanout and wiring tracks. Zero or more inverters are added to each prefix cell output to minimize the delay based on this model, buffers are individually sized to minimize the delay, buffers are used to minimize the fanout and loading on gates since high fanout causes poor performance. A modified Han-Carlson adder uses fewer number of prefix operations by adjusting the number of stages amongst Kogge-Stone and Brent-kung adder and thus reduces the area required by the adder circuitry. There are three stages in performing prefix computation as shown in "Fig.1" below. First is the pre-processing stage to calculate generate and propagate bit, second stage is the carry computation stage to compute the carry bit and the third stage is the post-processing stage to compute the sum bit.

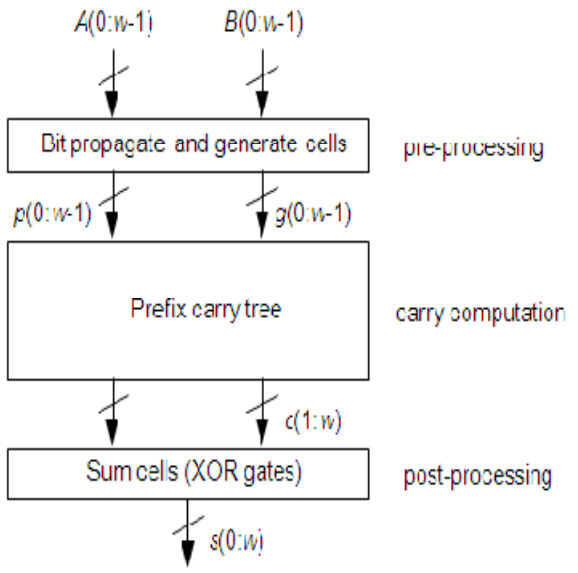


Fig.1 Parallel Prefix Adder Structure

The graph representation of Hybrid Han-Carlson Adder is shown in Fig.2 below

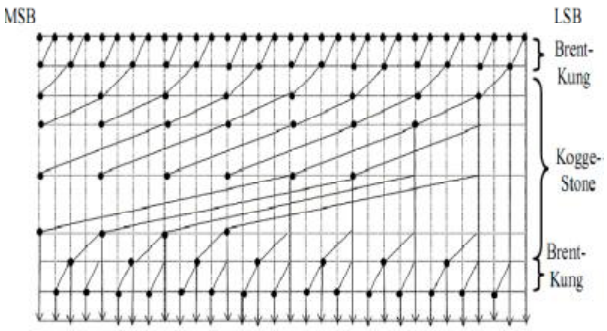


Fig. 2: Graph representation of 32-bit Hybrid Han-Carlson Adder

II. BACKGROUND

The forward converter, modulo arithmetic units, and reverse converter are the main parts of the RNS. In contrast to other parts, reverse converter consists of a complex and nonmodular structure. Therefore, more attention should be directed to its design to prevent slow operation and compromise the benefits of the RNS. Both the characteristics of the moduli set and conversion algorithm have significant effects on the reverse converter performance. Hence, distinct moduli sets have been introduced. In addition to the moduli set, hardware components selection is a key to the RNS performance. For instance, parallel-prefix adders are known as unsuitable structures for complex reverse converters because of their high power consumption. However, parallel-prefix adders with its high-speed feature have been used in the RNS modular arithmetic channels. This performance gain is due to parallel carry computation structures, which is based on different algorithms. Each of these structures has distinct characteristics, such as Sklansky (SK), and Kogge–Stone (KS) have the maximum and minimum fan-out, respectively, both providing minimal logic depth. Minimum fan-out comes at the expense of more circuit area. Therefore, hardware components selection should be undertaken carefully.

III. NEW PARALLEL-PREFIX-BASED COMPONENTS

The Chinese remainder theorem, or other related improved approaches and techniques underlie the RNS reverse conversion, whose formulation can be directly mapped to ripple-carry adders (RCA). However, this leads to significant speed degradation,

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 2, March 2016

due to the linear increase of the delay in the RCA with the number of bits. Parallel-prefix adders can be used in the RNS reverse converters to bind the delay to logarithmic growth. However, in reverse converters, several parallel-prefix adders are usually required. Even when only one adder is used, the bit length of this adder is quite large. Consequently, this results in high power consumption notwithstanding its high speed. Therefore, in this section, two approaches that take advantage of the delay properties of the parallel prefix adders with competitive power consumption are introduced.

A. *Proposed Work*

It's describes design of Parallel Prefix Hybrid Han-Carlson Adder. It differs from other adder in that it can be used for large word sizes. The proposed design reduces the number of prefix operation by using more number of Brent-Kung stages and lesser number of Kogge-Stone stages. This also reduces the complexity, silicon area and power consumption significantly.

B. *Implementation*

The designing of proposed adder architecture is done using Xilinx ISE 13.1 Tool and the complete source code for 32 bit implementation of proposed adder is done. Christo Ananth et al. [4] proposed a system which contributes the complex parallelism mechanism to protect the information by using Advanced Encryption Standard (AES) Technique. AES is an encryption algorithm which uses 128 bit as a data and generates a secured data. In Encryption, when cipher key is inserted, the plain text is converted into cipher text by using complex parallelism. Similarly, in decryption, the cipher text is converted into original one by removing a cipher key. The complex parallelism technique involves the process of Substitution Byte, Shift Row, Mix Column and Add Round Key. The above four techniques are used to involve the process of shuffling the message. The complex parallelism is highly secured and the information is not broken by any other intruder.

g= a and b & p= a xor b

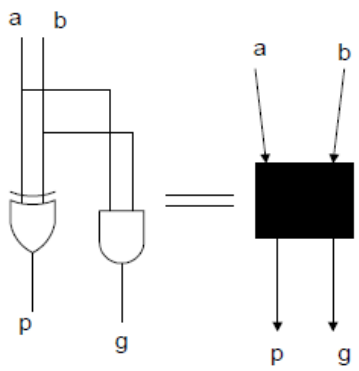


Fig 3: square cell

Circular cells: for computation of prefix operation (gi. pi) ○ (gj. pj)=(gi+ pi.gj,pi. pj) The main reason for the high power consumption and area overhead of these adders is the recursive effect of generating and propagating signals at each prefix level.

An optimized approach is proposed in, which uses an extra prefix level to add the output carry. However, this method suffers from high fan-out, which can make it usable only for small width operands.

However, we could address this problem by eliminating the additional prefix level and using a modified excess-one unit instead. In contrast to the BEC, this modified unit is able to perform a conditional increment based on control signals as shown in Fig. 2, and the resulted hybrid modular parallel-prefix excess-one (HMPE) adder is depicted in Fig. 3. Summarizing, the HMPE is highly flexible, since it can be used with every prefix networks. Hence, the circuit performance metrics such as area, delay, and power-consumption can be adjusted by selecting the desired prefix structure. It improves speed to a considerable level.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 2, March 2016

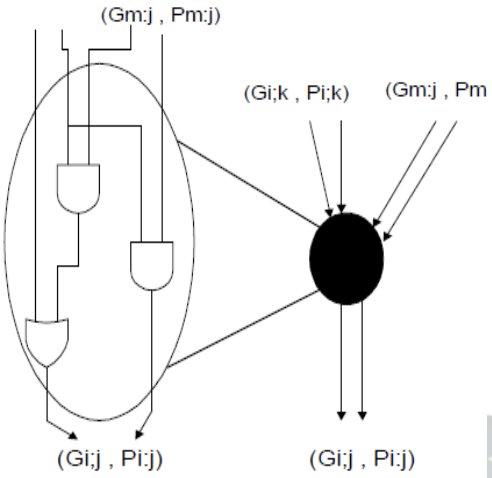


Fig 4:circular cell

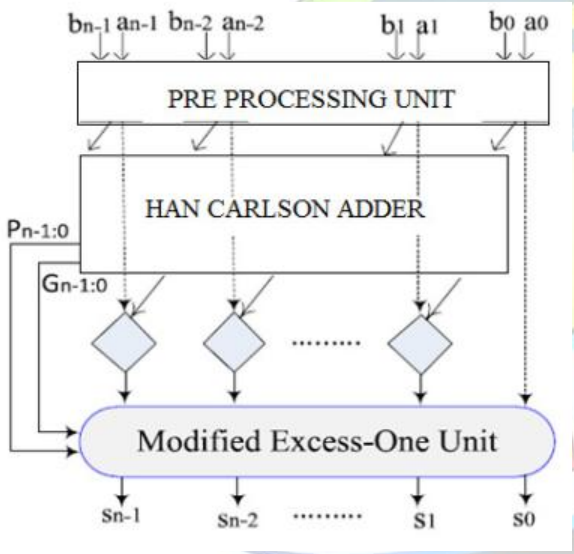


Fig 5: block diagram representation of hybrid parallel adder

. On the other hand, the HRPX avoids the usage of a large size parallel-prefix adder with high power consumption, and also does not have the penalty of using the long carry-propagation chain of a RCA.

IV. REVERSE CONVERTER DESIGN METHODOLOGY

In this section, the methodology of reverse converter design is described. In the following, a method employing distinct components in the architecture of the reverse converter will be presented. Several reverse converters for different moduli sets have been introduced which can be classified into three classes. The first class consists of converters with a tree of CSAs with EAC followed by a two-operand modulo $2k - 1$ CPA. A second class includes more complex reverse converters, which have several CSAs and CPAs with EACs followed by a final regular subtractor with two operands of different size. The implementation of this subtractor using regular binary-adder results in one operand with some constant bits.

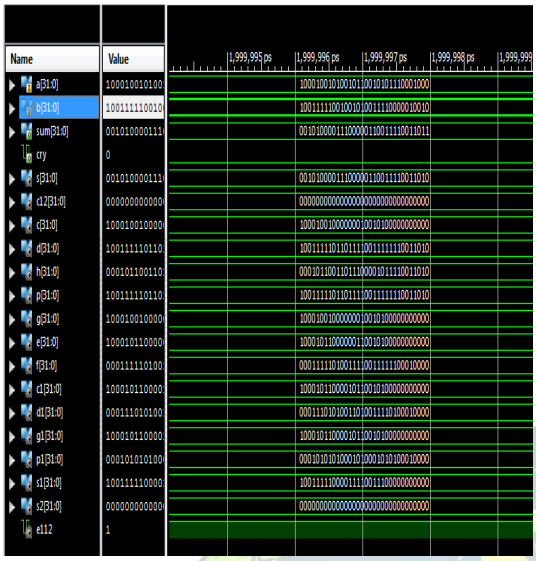
The third class covers the reverse converters that have been designed for moduli sets with moduli other than the popular $2n$ and $2n \pm 1$. The suggested method for applying the HMPE and HRPX in the reverse converter is shown in Fig. 4. First of all, it is relevant to decide about the required performance metrics based on the specified application. If it is just important to achieve the least power consumption and hardware cost without considering speed, no prefix adder is needed. On the other hand, if high speed is the designer goal, the CPAs with EAC and the regular CPAs should be replaced by traditional parallel prefix modulo $2n - 1$ adder and regular parallel-prefix adders, respectively.

BRENT KUNG ADDER	HAN CARLSON ADDER
Carry Stages: log2 n;	Carry Stages: log2 n+1;
The number of cells: (n/2).log2n;	The number of cells: (n/2);
Maximum fan-out: n/2.	Maximum fan-out: 2.

V. RESULT

From the above work, it is seen that the Han-Carlson adder presented a reduction in the complexity and hence provides a tradeoffs for the construction of large adders. These wide adders are useful in applications like cryptography for security purpose, global unique identifiers used as an identifier in computer software and this wide adder also provides good speed.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 2, March 2016



REFERENCES

[1] Azadeh, "Reverse Converter Design via Parallel-Prefix Adders: Novel Components, Methodology, and Implementations" *IEEE Tran Very Large 2015.*

[2] C. H. Vun, A. B. Premkumar, and W. Zhang, "A new RNS based DA approach for inner product computation," *IEEE Trans. Circuits Syst. I, Reg. Papers, vol. 60, no. 8, pp. 2139–2152, Aug. 2013.*

[3] J. Chen and J. Hu, "Energy-efficient digital signal processing via voltage over scaling-based residue number system," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst., vol. 21, no. 7, pp. 1322–1332, Jul. 2013.*

[4] Christo Ananth, H.Anusuya Baby, "High Efficient Complex Parallelism for Cryptography", IOSR Journal of Computer Engineering (IOSR-JCE), Volume 16, Issue 2, Ver. III (Mar-Apr. 2014), PP 01-07

[5] P. R. Brent and H. T. Kung, "A regular layout for parallel adders," *IEEE Trans. Comput.*, vol. 31, no. 3, pp. 260–264, Mar. 1982.

[6] P. M. Kogge and H. S. Stone, "A parallel algorithm for the efficient solution of a general class of recurrence equations," *IEEE Trans. Comput.*, vol. 22, no. 8, pp. 783–791, Aug. 1973.

[7] Ramkumar.P and H. M. Kittur, "Low power and area efficient carry select adder," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 20, no. 2, pp. 371–375, Feb. 2012.

[8] R. Zimmermann, "Efficient VLSI implementation of modulo ($2n\pm1$) addition and multiplication," in *Proc. 14th IEEE Int. Symp. Comput. Arithmetic*, Apr. 1999, pp. 158–167.

[9] S. J. Piestrak, "A high speed realization of a residue to binary converter," *IEEE Trans. Circuits Syst. II, Analog Digit. Signal Process.*, vol. 42,no. 10, pp. 661–663, Oct. 1995.

[10] H. Kunz and R. Zimmermann, "High-performance adder circuit generators in parameterized structural VHDL," Integr. Syst. Lab., ETH Zürich Univ., Zürich, Switzerland, Tech. Rep. 96/7, 1996.