KARATSUBA MULTIPLIER USING TSPC

Harshith Reddy Surakanti
Deptartment of Electrical Engineering
Purdue University, Indianapolis, IN
harshith.surakanti@gmail.com

***Abstract* —** This paper presents an efficient 8x8 multiplier utilizing the Karatsuba algorithm. Large integer multiplications are a fundamental requirement in digital signal processing (DSP) algorithms, media applications, cryptographic systems, and other computational fields. The Karatsuba-like multiplication technique is recognized as one of the most efficient algorithms for large number multiplication.

In this work, we propose an optimized hardware architecture for the Karatsuba multiplier, leveraging TSPC logic to achieve improved trade-offs between area, delay, and power consumption. The proposed design requires 4,486 transistors, of which 1,733 are PMOS and 2,752 are NMOS. While this increases the overall power dissipation, the design efficiently operates at clock frequencies ranging from 1 GHz to 4 GHz, with a data period of 5 ns. Below 500Mhz, we get error outputs, due to degradation of stored currents. The power dissipation is theoretically predicted to be approximately 288 μW, and the delay is estimated around 429 pSec for 1 Ghz operation. This makes the architecture suitable for high-performance, resource-constrained applications, balancing resource usage with computational speed.

Keywords — Karatsuba multiplication, large integer multiplication, divide and conquer, cryptography, digital signal processing, true single phase logic.

I. INTRODUCTION

In modern VLSI design, efficient arithmetic operations are crucial for enhancing computational performance, particularly in systems requiring rapid and accurate large-number multiplications. The Karatsuba multiplication algorithm is a well-known fast multiplication technique that reduces computational complexity compared to the traditional schoolbook method. It leverages a divide-and-conquer approach to break large multiplications into smaller subproblems, making it highly efficient for large integer arithmetic.

The Karatsuba algorithm is particularly beneficial in cryptographic systems**,** media processing, and digital signal processing, where operations on large integers are common. Its lower time complexity of O ($n^{1.58}$}), compared to the $O(n^2)$ complexity of traditional multiplication, allows for significant improvements in both speed and resource utilization. Despite these advantages, hardware implementations of Karatsuba multipliers face challenges related to area efficiency, clocking overhead, and power consumption, which are critical factors in VLSI systems.

This paper introduces a novel implementation of Karatsuba multiplication using True Single-Phase Clocking (TSPC) logic, a technique known for its efficiency in reducing the complexity of clock distribution and power consumption in digital circuits. TSPC logic, with its reduced transistor count and single-phase clocking, presents an ideal platform for implementing the Karatsuba algorithm in VLSI designs, where minimizing both delay and area are paramount.

II. TSPC LOGIC

This article delves into the True Single-Phase Clock (TSPC) logic, a technique introduced to address challenges in high-speed digital CMOS circuit design. Initially developed to minimize power consumption and area, TSPC logic became an attractive solution for simplifying clock distribution in complex chips, where clock skews and long interconnects posed significant problems. By eliminating the need for nonoverlapping clock phases, TSPC allowed faster operation and reduced complexity compared to other methods such as C2MOS and NORA logic.

The main concept behind TSPC logic is to use a single clock phase to control dynamic latches composed of NMOS and PMOS transistors in alternating stages. This design avoids the race conditions found in traditional dynamic logic circuits like Domino logic. While Domino and NORA circuits often suffer from charge-sharing issues, TSPC addresses these concerns, enabling more efficient and reliable operation.

TSPC was applied in various high-performance systems, such as frequency dividers and phase detectors, due to its reduced hardware and power requirements. True single-phase clock (TSPC) logic has several advantages that make it a preferred choice for high-performance processors and memory circuits.

Despite its advantages, TSPC faces challenges at lower clock frequencies, where leakage currents can degrade the stored state, especially at high temperatures. In our design we face challenges below 500Mhz Therefore, designers must carefully balance speed, power, and reliability when using TSPC logic in digital circuits.

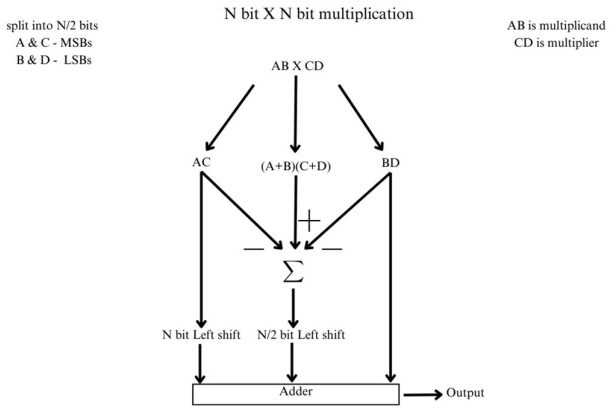
In conclusion, TSPC logic has significantly contributed to high-speed, low-power digital design, offering simpler and more efficient circuits compared to multi-phase clocking methods. Its versatility and impact on modern chip design remain notable, especially in the context of power-sensitive and high-performance applications.

III. KARATSUBA

Karatsuba multiplication is a divide-and-conquer algorithm that significantly optimizes the multiplication of large numbers compared to traditional methods like the grade-school multiplication, which runs in $O(n^2)$. Anatolii

Karatsuba introduced this algorithm in 1962, which operates in $O(n\log_2 3) \approx O(n^{1.585})$, improving the efficiency of multiplying large numbers.

A. Working Principle of Karatsuba



Tree Diagram of Karatsuba Implementation

Given two large n-bit numbers X and Y, Karatsuba splits them into two halves, represented as:

$$X = 2^{n/2}A+B$$
$$Y = 2^{n/2}C+D$$

Where A, B, C, and D represent the most significant and least significant halves of the numbers.

The product X×Y can be computed as:

$$XY=2^{n}AC+2^{n/2}(AD+BC) +BD$$

$$XY=2^{n}AC+2^{n/2[}(A+B)(C+D) – AC-AD] +BD$$

Instead of directly calculating all four terms (AC, AD, BC, and BD), Karatsuba reduces the number of multiplications by cleverly reusing subproducts. The algorithm requires only three multiplications and multiple additions and subtractions, as follows:

1. $P1 = A\times C$
2. $P2 = B\times D$
3. $P3 = (A+B) \times (C+D)$
4. $AD + BC = P3-P1-P2$

By reducing the number of recursive multiplications from four to three, Karatsuba achieves a time complexity of $O(n^{1.585})$. For large numbers, this results in significant performance improvements.

B. Recursive Application

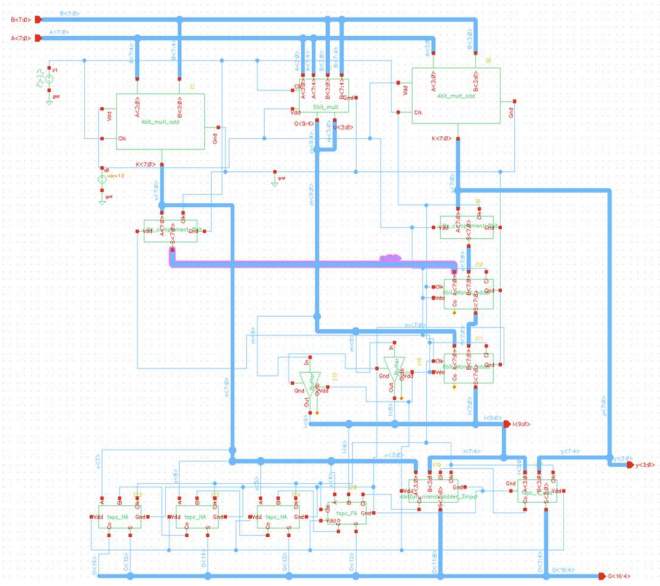
Karatsuba's method can be recursively applied, further splitting the numbers as needed for very large digit multiplications. Its recursive nature and ability to break down large-digit multiplications into simpler operations make it a powerful tool in computational mathematics and cryptography, where large numbers are frequently encountered.

C. Performance Analysis

The Karatsuba algorithm shines for large-digit multiplications, particularly for numbers that exceed a few hundred bits. While the cost of multiplication is generally higher than that of addition and subtraction operations, the reduction in the number of multiplicative steps ensures overall time savings. According to Dwivedi (2013), performance gains become more pronounced as the bit length increases, making Karatsuba a preferred choice for cryptographic and large-number computations.

For smaller numbers, Karatsuba may not outperform simpler algorithms due to the overhead of recursive calls. However, as the input size grows, its efficiency becomes apparent, especially when compared to $O(n^2)$ methods.

IV. Karatsuba using TSPC



Schematic of Karatsuba Multiplier

Combining Karatsuba multiplication with True Single-Phase Clock (TSPC) logic significantly enhances the efficiency and performance of digital designs, particularly in high-speed and low-power applications. Karatsuba, when paired with TSPC logic, which simplifies clock distribution and minimizes power consumption through a single-phase clocking mechanism, the result is a highly efficient and streamlined design.

This integration leads to faster multipliers with reduced hardware complexity, lower power consumption, and improved clocking stability. It is especially beneficial in applications like signal processing and cryptography, where high-speed, low-power multiplication is essential. Moreover, TSPC's smaller area footprint complements Karatsuba's reduced computational steps, yielding a design that is both compact and power-efficient, ideal for modern VLSI systems and portable devices.

Implementation:

To implement the Karatsuba multiplication using True Single-Phase Clock (TSPC) logic, several key steps were taken to optimize both speed and power efficiency. The

design begins with the creation of basic gates like AND and XOR, using TSPC logic. These gates form the building blocks for higher-order operations like partial product generation and addition.

For the addition of partial products, dynamic Manchester carry generators were built. These dynamic adders enable parallel addition of partial products, improving speed and reducing the complexity associated with traditional ripple carry adders. The partial products were derived by dividing the 8-bit inputs into two 4-bit segments: least significant 4 bits (LSB) and most significant 4 bits (MSB). Multiplication was performed on both segments using two 4-bit multiplier blocks (4bit_mult), yielding intermediate results.

The middle multiplication block, which computes (A+B)(C+D), was implemented as a recursive multiplication involving an additional 4-bit multiplication (5bit_mult block). The result of this middle block was then subtracted from the results of the LSB and MSB multiplications to complete the Karatsuba multiplication process.

To handle negative results and perform subtraction efficiently, 8-bit two's complement blocks were created. These blocks handle the complement operation in 2 bits and feed into dynamic Manchester adders. Shifting operations were incorporated to correctly align the partial products before final addition. This design combines the recursive nature of Karatsuba multiplication with the high-speed, low-power benefits of TSPC logic. The integration of dynamic adders and recursive multiplication blocks enables efficient computation, while TSPC logic ensures minimal power consumption and area utilization, making it suitable for high-performance VLSI systems and portable devices.

V. RESULTS

Test cases at 500 ps clock period and 8nSec data rate

TABLE I.

	CADENCE	
Frequency	**Power dissipation**	**Propagation delay**
500 Mhz	220.894u	335.846p
1 Ghz	242.556u	796.886p
2 Ghz	278.737u	926.474p
4Ghz	334.07u	882.432p

Power dissipation and propagation delay table

Theoretical Calculations:

Propagation delay for TSPC AND gate = 0.69 $R_{on}C_l$

Considering worst path delay = 3 NMOS + 2 NMOS
Tp=0.69(3R)(3Cl) +0.69 (2R) (2Cl) = 3.29pSec
TSPC XOR = 2 Tpand + T_{inv}=7.59 pSec
Total delay = 5 bit multiplication + 3 (8-bit adders)
= 429 pSec

Static Power dissipation:
Leakage currents = PMOS Count * $Ip_{leakage}$ + NMOS Count * $In_{leakage}$
Leakage Currents=1733*993x10-12 + 2753*1*10-9 = 1.72u + 2.75 u = 4.47 uA
Pstatic=Ileakage * Vdd * No. of inputs
Pstatic =4.47u *1.2*10 = 53.64uW

Pdynamic = Vdd^2 * f *C_l activity factor=1, at 1 Ghz
= 1.2^2 * 1* 10^9 * 320f F
= 230uW
Total power = Pstatic + Pdynamic = 230uW+53.64uW
= 288.64uW

VI. FUTURE SCOPE

This work can be further extended by exploring pipelining and parallelism to enhance throughput and performance of the Karatsuba multiplier. Implementing low-power techniques such as clock gating, dynamic voltage scaling, and pass transistor logic can reduce power consumption, making the design more suitable for resource-constrained applications. Additionally, adopting advanced technology nodes like FinFET or 3D IC integration could improve area, delay, and power trade-offs. Future work could also focus on integrating error-detection and fault-tolerance mechanisms to enhance reliability, especially for cryptographic and DSP applications that require robust performance under varying conditions.

REFERENCES

[1] B. Kang and H. Cho, "FlexKA: A Flexible Karatsuba Multiplier Hardware Architecture for Variable-Sized Large Integers," in IEEE Access, vol. 11, pp. 55212-55222, 2023, doi: 10.1109/ACCESS.2023.3282646.

[2] A. Mehta, C. B. Bidhul, S. Joseph and P. Jayakrishnan, "Implementation of single precision floating point multiplier using Karatsuba algorithm," 2013 International Conference on Green Computing, Communication and Conservation of Energy (ICGCE), Chennai, India, 2013, pp. 254-256, doi: 10.1109/ICGCE.2013.6823439.

[3] A.A. Karatsuba (1995). "The Complexity of Computations" . *Proceedings of the Steklov Institute of Mathematics*. **211**: 169–183.

[4] M. V. Krishna, M. A. Do, K. S. Yeo, C. C. Boon and W. M. Lim, "Design and Analysis of Ultra Low Power True Single Phase Clock CMOS 2/3 Prescaler," in IEEE Transactions on Circuits and Systems I: Regular Papers, vol. 57, no. 1, pp. 72-82, Jan. 2010, doi: 10.1109/TCSI.2009.2016183.

[5] Performance Analysis of Karatsuba Multiplication Algorithm for Different Bit Lengths, Procedia - Social and Behavioral Sciences,Volume 195, 2015, Pages 1860-1864, ISSN 1877-0428, https://doi.org/10.1016/j.sbspro.2015.06.420. Fifth International Conference on Advances in Recent Technologies in Communication and Computing (ARTCom), 20-21 Sept, Bangalore IET, ISBN: 978-1-84919-842-4 (2013), pp. 223-228