Design of FIR Filter Using Modified Montgomery Multiplier with Pipelining Technique

Shobana.J¹, Ms.P.Kavipriya², Sarojini.K³

¹Department of ECE, M.Tech VLSI Design, Sathyabama University, Tamilnadu, India
²Department of ECE, Senior Lecturer, Sathyabama University, Tamilnadu, India
³Department of ECE, M.Tech VLSI Design, Sathyabama University, Tamilnadu, India

Abstract: This paper implements the FIR filter by using Montgomery multiplier. The main objective of this paper is used to reduce the area, delay and analyze the performance of the Montgomery multiplier. It performs the fastest multiplication of modular operation. Add the pipelining in Montgomery multiplier, it will improve the speed of the operation. The main application of the Montgomery multiplier is cryptography for encryption/decryption purpose.

Keywords: Montgomery multiplier, FIR filter, Pipelining, Replication, VLSI.

I. INTRODUCTION

Multipliers are one of the key components in digital signal processing applications such as frequency domain filtering, frequency transformations etc. Montgomery multiplier is one of the modular multiplier. It performs modular multiplication operation. Peter Montgomery have been achieved a way to speed up arithmetic operation in which the modulus [3] is used for a long running computation. These methods have been explored as a hardware operation. It is particularly suitable for implementation on general purpose computers like signal processors or microprocessors. However Montgomery multiplication is easier to solve the side-channel attacks, so in some circumstances the Montgomery technique may be preferable.

The main objective is to design a FIR filter based on this Montgomery multiplication. Because FIR filters consist of multiplier, adder and unit delay. It is represented as finite impulse response and it is used to remove the unwanted frequencies from the original signal. The FIR filters mainly used for digital signal processors. To design Montgomery multiplier by using adders and shift registers and to include the pipelining, it will improve the speed of the operation. Because, the pipelining is used to improve the throughput of the design. We show the parametric design using pipelining and replication. The main advantage of the parametric design is their scalability and reusability. By replicating the design, it will increase the latency. Because, replication used to measure the latency and pipelining used to measure the throughput of the design. Modular multiplication is mainly used in encryption/decryption, authentication, cryptography, key distribution and many other applications. Montgomery multiplication also may be used for the basis for Montgomery exponentials.

This paper describes as follows, Section I implements the introduction, section II introduce the previous work and section III describes the pipelining. Section IV employs the Montgomery multiplication. Section V describes the design of FIR filter and section VI introduces results and discussions. Finally section VII concludes this paper.

II. EXISTING METHOD

In our works are represented in Montgomery multiplier with pipelining and replication features. It shows how a general algorithms consisting of a loop dependencies carried from one iteration to the next can be automatically mapped to a parametric hardware designs with pipelining and replication features [1]. In this model used to predict the area taken by the designs with less than 5% of error and their frequencies and throughputs with less than 22% of error. They are developing a Montgomery multiplier with carry save adder based design. In this method number of clock cycles is reduced, so it is mainly improve the speed of the design. But, it covers more space in the design space exploration.

III. PIPELINING

Pipelining is an important technique used in several applications such as DSP systems, microprocessors etc. It originates from the idea of a water pipe with continuous water sent in without waiting for the water in the pipe to come out. Accordingly, it provides the results in speed enhancement for the critical path in most DSP
Design of FIR Filter Using Modified Montgomery Multiplier with Pipelining Technique

systems. For example, it can either increase the clock speed or reduce the power consumption at the same speed in a DSP system. It has an several techniques, like, dynamic scheduling, loop unrolling, software pipelining etc.

Dynamic scheduling is the hardware re-arranging instruction execution to reduce the stalls while maintaining dataflow exception behavior. It is used to simplify the compiler of the operation. The operations over which the compiler has complete control when operations are executed. It eliminates the need for complex circuitry in the CPU, which frees up space and power for the functions including additional execution resources.

IV. MONTGOMERY MULTIPLICATION

The Montgomery multiplication is an efficient method for performing modular multiplications with an odd modulus. It replaced costly division operation with simple shifts [2]. This algorithm is mainly suitable for the implementations on general purpose computers.

Given two integers \( A, B \) with odd modulus \( M \). The Montgomery multiplication \( Y \) can be represented as, [2]

\[
Y = \text{montmulti} (A, B) = A \times B \times R^{-1} \mod M
\]

Given \( A, B < M \) and \( R \) is represented as,

\[
gcd(R, M) = 1. \text{ Where } R = 2^n \text{ and } M \text{ is an integer in the range } 2^{n+1} < M < 2^n, \text{ since } R, \text{ it is sufficient that the modulus } M \text{ is an integer. Since Montgomery multiplication is not an ordinary multiplication, there is a process of conversion between the ordinary domain and the Montgomery domain. The conversion between the ordinary domain and the Montgomery domain is given by the relation}
\]

\[
A \leftrightarrow A' \text{ with } A' = A \times 2^{-n} \mod M.
\]

This conversion is represented as in Table I.

<table>
<thead>
<tr>
<th>ORDINARY DOMAIN</th>
<th>MONTGOMERY DOMAIN</th>
</tr>
</thead>
<tbody>
<tr>
<td>( A )</td>
<td>( A' = A \times 2^{-n} \mod M )</td>
</tr>
<tr>
<td>( B )</td>
<td>( B' = B \times 2^{-n} \mod M )</td>
</tr>
<tr>
<td>( AB )</td>
<td>( (A \times B') = A \times B \times 2^{-n} \mod M )</td>
</tr>
</tbody>
</table>

The Montgomery multiplication provides the reduced product using a series of additions. Montgomery multiplication is particularly used in implementations of the RSA cryptosystem or other cryptosystems based on modular arithmetic.

Proposed Work:

To implement the pipelining and replication technique of our design, it is used to improve the speed of the operation. To replicate the block, the delay will be increase. So we add the pipelining in our block, it improve the speed and reduce the number of clock cycles. The 32-bit Montgomery multiplier can be represented in Fig. 1.

To design a new architecture of Montgomery multiplier with pipelining technique, which is used to multiply the two number representations with modulo \( M \), we introduce a pipelining technique in our internal architecture which gives fast operation of our design. To use Montgomery multiplication, we must have the multiplicand \( (A) \) and multipliers \( (B) \) must be less than modulo \( M \).
The cost of the modular multiplication is equal to the three integer multiplications plus cost of conversion to or from the Montgomery domain. But the cost of conversion is negligible compared to number of multiplications executed in the Montgomery domain. The internal structure of Montgomery multiplier is represented as shown in Fig. 2.

- The modulo M is to be a prime to the radix, (i.e.,) there exists no common divisor for M and radix.
- The multiplicand and the multiplier (A, B) must be lesser than M.

Montgomery multiplication mainly used for encryption/decryption, cryptography, key distribution, authentication and many other applications. Montgomery multiplication also used for the Montgomery exponentials.

V. FIR FILTER

Digital filters are mainly used for Digital Signal Processor. It has two main uses, signal separation and signal restoration.
- Signal separation is needed when the signals have been contaminated with noise or other signals.
- Signal restoration is needed when the signal is distorted in some way.
The filters can be represented as in equation,
\[ Y[n] = x[n] \ast f[n] = \sum_{k=0}^{\infty} f(k) x(n-k) = \sum_{k=0}^{\infty} x(k) f(n-k). \]

Digital filters having two types and it is represented as FIR filter and IIR filter.

- FIR filter is represented as Finite Impulse Response, whose impulse response or response to any finite length input of finite duration, because it settles to zero in finite time.
- IIR filter is represented as Infinite Impulse Response, whose impulse response is infinite duration.

Design of FIR filter:
FIR filters requires three basic building blocks in multiplication, addition and unit delay.
- DSP system of multiplication must be fast and must have sufficient to support the desired application.
- Signal addition is a very basic DSP function. In an FIR filter additions are required in combination with multiplications.
- The unit delay provides a one sample signal delay. A sample value is stored in a memory slot for one sample clock cycle.

Proposed Work:
To design a FIR filter by using our Montgomery multiplier architecture. We have to design a 8-tap FIR filter. In this filter gives better performance of the filter operation. The FIR filters can be represented as shown in Fig. 3.

FIR filters have some properties over IIR filter. It has require no feedback and it is inherently stable. They can be easily designed to be linear phase by making the coefficient sequence symmetric.

The main disadvantage of FIR filters is that considerably more computation power in a general purpose processor is required compared to an IIR filter with similar sharpness or selectivity, especially when low frequency cutoffs are needed. Many digital signal processors gives specialized hardware features to make FIR filters approximately as efficient as IIR for many applications.

VI. RESULTS AND DISCUSSIONS

Proposed Method:
Montgomery Multiplier:
The simulation results and device utilization summary of modified 32-bit Montgomery multiplier as shown in Fig. 4 & Fig. 5.
Design of FIR Filter Using Modified Montgomery Multiplier with Pipelining Technique

Fig. 4: simulation results of Montgomery multiplier.

<table>
<thead>
<tr>
<th>Device Utilization Summary (estimated values)</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Logic Utilization</td>
<td></td>
</tr>
<tr>
<td>number of Slice Resources</td>
<td>194</td>
</tr>
<tr>
<td>number of Slice LUTs</td>
<td>210</td>
</tr>
<tr>
<td>number of FF used and LUT FF open</td>
<td>116</td>
</tr>
<tr>
<td>number of dedicated LUTs</td>
<td>120</td>
</tr>
<tr>
<td>number of FLs</td>
<td>1</td>
</tr>
<tr>
<td>number of FOTLs</td>
<td>1</td>
</tr>
</tbody>
</table>

Fig. 5: Device Utilization Summary

The RTL schematic and synthesis report of modified Montgomery multiplier as shown in Fig. 6, Fig. 7 & Fig. 8.

Fig. 6: RTL schematic

Fig. 7: Internal structure of RTL schematic
Design of FIR Filter Using Modified Montgomery Multiplier with Pipelining Technique

Internal architecture of Montgomery multiplier:

The simulation results and device utilization summary of internal architecture of modified 16-bit Montgomery multiplier as shown in Fig. 9 & Fig. 10.

Fig. 9: Montgomery multiplier

Fig. 10: Device Utilization Summary

The RTL schematic and synthesis report of internal structure of 16-bit modified Montgomery multiplier as shown in Fig. 11, Fig. 12 & Fig. 13.

Fig. 11: RTL schematic
Design of FIR Filter Using Modified Montgomery Multiplier with Pipelining Technique

Fig. 12: Internal structure of RTL schematic

Fig. 13: Synthesis Report

FIR Filter:
The simulation results and device utilization summary of FIR filter as shown in Fig. 14 & Fig. 15.

Fig. 14: Simulation results of FIR filter

Fig. 15: Device Utilization Summary

<table>
<thead>
<tr>
<th>Device Utilization Summary (estimated values)</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Logic Utilization</td>
<td>Li</td>
</tr>
<tr>
<td>Number of Site Registers</td>
<td>596</td>
</tr>
<tr>
<td>Number of Site LUs</td>
<td>392</td>
</tr>
<tr>
<td>Number of FU/OD/ADD/LUT/FF gates</td>
<td>574</td>
</tr>
<tr>
<td>Number of R policentric blocks</td>
<td>18</td>
</tr>
<tr>
<td>Number of LV/LSHA/SCA/SHA/PLA3e</td>
<td>1</td>
</tr>
<tr>
<td>Number of FPGA 8Ls</td>
<td>0</td>
</tr>
</tbody>
</table>
The RTL schematic diagram and synthesis report of FIR filter as shown in Fig. 16, Fig. 17 & Fig. 18.

**Fig. 16: RTL schematic**

**Fig. 17: Internal structure of RTL schematic**

**Fig. 18: Synthesis Report**

### COMPARISON TABLE:

**Montgomery Multiplier**

To compare the Montgomery multipliers of existing and proposed method as shown in Table II.

**Table II: comparison table of existing and proposed Montgomery multiplier.**

<table>
<thead>
<tr>
<th>METHOD</th>
<th>Number of Slice Registers</th>
<th>Number of Slice LUTs</th>
<th>Maximum Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>Existing Method</td>
<td>USED: 160</td>
<td>Available: 129803</td>
<td>USED: 256</td>
</tr>
<tr>
<td>Proposed Method</td>
<td>144</td>
<td>129803</td>
<td>190</td>
</tr>
</tbody>
</table>

### VII. CONCLUSION

The Montgomery multiplication algorithm is an efficient method for modular multiplication with an arbitrary modulus, particularly suitable for implementation on general-purpose computers like signal processors or microprocessors. The proposed system of Montgomery multiplier used to reduce the area and usage of time is less. To implement the pipelining into the Montgomery multiplier architecture, it gives better performance. However many digital signal processors provide specialized hardware features to make FIR filters
Design of FIR Filter Using Modified Montgomery Multiplier with Pipelining Technique

approximately as efficient as IIR for many applications. In this proposed multiplier is applied to the 8-tap FIR filter used for fast computation. In this process are implemented by using Xilinx Artix 7.

Future Work:
To implement the Montgomery multiplier can be applied to N number of bits and to design the N-tap FIR filter. The main application of Montgomery multiplier is cryptography like RSA and ECC algorithms etc…. Further the design is implemented in many applications.

REFERENCES


