A Study on Soft Core Processor Configurations for Embedded Applications

Ben Kueffler, Christopher Cole, Rafi Meguerdijian, Vlad Cretu, Sasoun Torousian
California State Polytechnic University, Pomona

Abstract

Field Programmable Gate Array (FPGA) designs have become widely adopted with their flexibility in accelerating performance of specific applications at a low power cost. This flexibility comes with the desire to also have customizable designs to suit the application. In this survey, we will perform tests on the Xilinx MicroBlaze processor within a 7-Series FPGA. Each of these tests enables some features on the processor while disabling others. Minimum area, high performance, maximum frequency, and frequency optimized implementations will be produced in order to survey tradeoffs that exist within these various architectures. The application that will be chosen to survey these tradeoffs will be an encryption and decryption algorithm. Our tests will demonstrate the tradeoff of power and area for performance, with an emphasis on tradeoffs for embedded cryptography applications.

Purpose

In order to analyze the effect and realize the advantage of soft processor implementations, six different MicroBlaze configurations will be produced. These implementations will be tested alongside a software algorithm designed to take advantage of certain hardware acceleration that is found in some of the configurations.

Implementations

- Three Stage Pipeline
- Three Stage Pipeline with Multiplier & Divider
- Five Stage Pipeline with Multiplier
- Five Stage Pipeline with Multiplier & Divider
- Five Stage Pipeline with Multiplier, Divider, & Branch Target Buffer

System Architecture

The system architecture consists of a typical FPGA design utilizing a soft processor such as the MicroBlaze. The MicroBlaze system, along with many other designs, utilizes AMBA AXI as the bus. The processor acts a master in order to control peripherals and access memory. The data and instruction memory lies on block RAM acting as a slave on the AXI bus. Additional slaves utilized for the purpose of testing include the AXI Uartlite and AXI timer submodules.

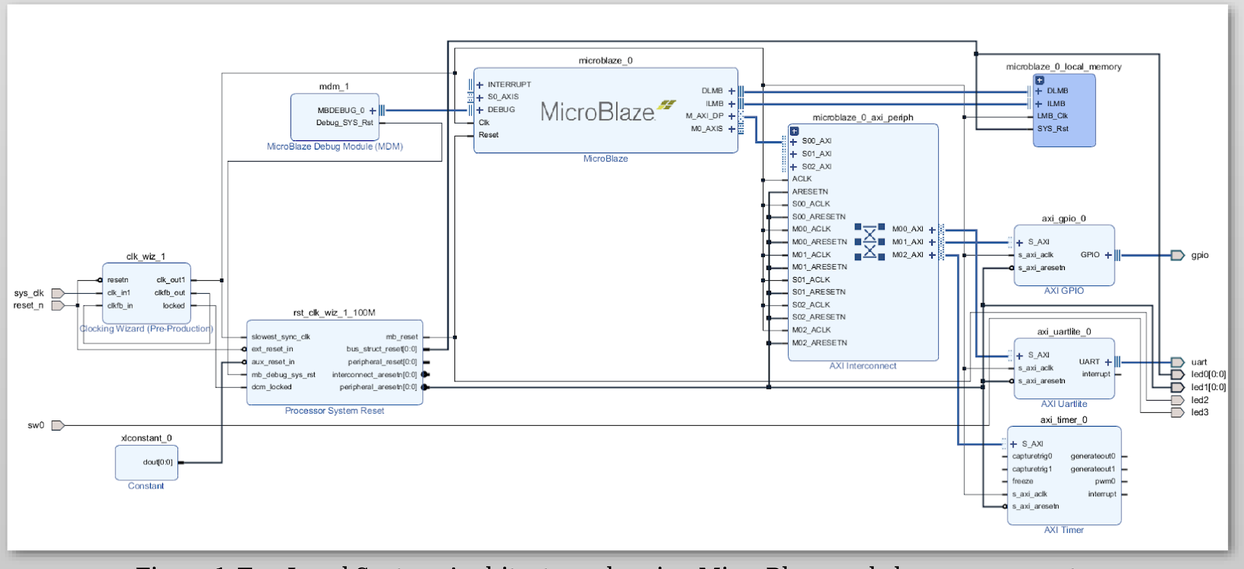

Figure 1: Top Level System Architecture showing MicroBlaze and slave components

Software and Test

In order to test the performance of the six processor implementations in a use case common for embedded applications, RSA encryption and decryption was chosen. The test consists of sending two 32kB files to be encrypted, followed by decryption. A hardware timer keeps the cycle count to determine the execution time.

```
Select a file 32kB or less to encrypt
Starting Encrypt/Decrypt on file...
Encrypted Message is : ¥||KKL9
                                  u╤b╤b6b||╪i||`
                                                ||bb6g||
                                                        u6
                                                          buLhK%LK16>>||6i6U
                                                                          ||↓bh╪╪||bbUhK%||╪i1>
                                                                                              ?g2
Decrypted Message is : Hello, this is a secret message that should only appear after successful decrypting!
Total cycles: 1378684
The execution time was 0 hours, 0 minutes, and 0.13 seconds!
```

Figure 2: Output after RSA encryption and Decryption

Results

The results indicate that the MicroBlaze implementations that utilize hardware acceleration in the form of multipliers and dividers improve the best in terms of performance. However, not all increases in hardware correspond to a an increase in performance, as shown with the five stage implementation of the branch target buffer. In general, hardware that targets the applications needs the best will see the greatest performance benefit. In analyzing the power data, the same trend can be seen, as the hardware more accurately targets the applications, performance per Watt increases.

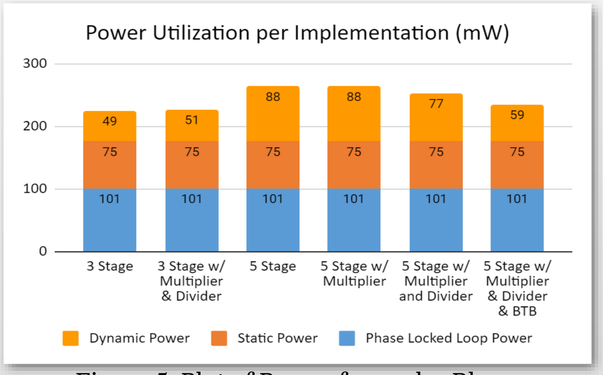

Figure 5: Plot of Power for each uBlaze

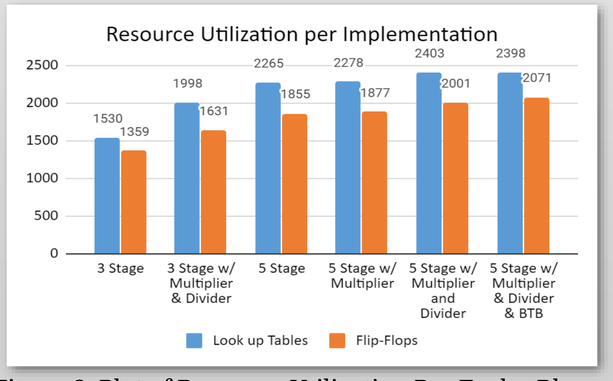

Figure 3: Plot of Resource Utilization Per Each uBlaze

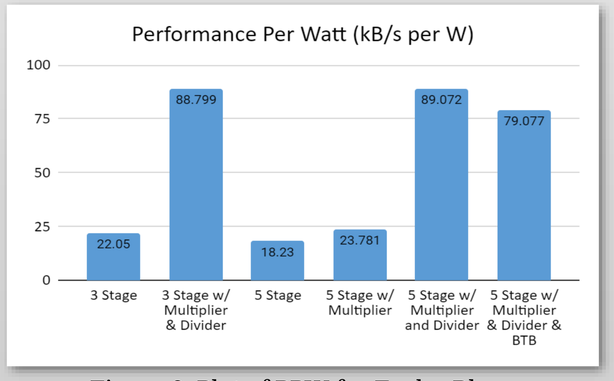

Figure 6: Plot of PPW for Each uBlaze

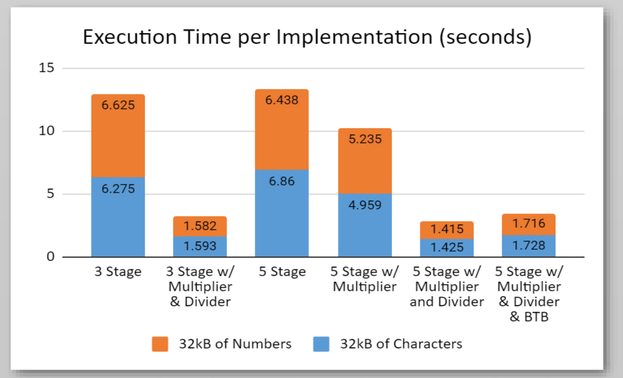

Figure 4: Plot of Execution Time Per Each uBlaze

Conclusion

The MicroBlaze system demonstrates the effectiveness of soft-core processors when targeting a specific application. The ability to reconfigure and optimize the processor allows for performance and cost competitive with the alternative of off-chip and hard-core solutions.

Acknowledgements

For support during this undertaking, thanks to Dr. Mohamed El-Hadedy. Additional thanks to Md Mohsin for a starting point on RSA encryption implementation in C