Abstract

Some applications such as RSA encryption/decryption need integer arithmetic operations with many bits. However, such operations cannot be performed directly by conventional CPUs, because their instruction supports integers with fixed bits, say, 64 bits. Since the CPUs need to repeat arithmetic operations to numbers with fixed bits, they have considerably overhead to execute applications involving integer arithmetic with many bits. On the other hand, This paper implements hardware algorithms for such applications in the FPGAs for further acceleration. However, the implementation of hardware algorithm is usually very complicated and debugging of hardware is too hard. The main contribution of this paper is to present an intermediate approach of software and hardware using FPGAs. More specifically, this paper presents a processor based on FDFM (Few DSP slices and Few Memory blocks) approach that supports arithmetic operations with flexibly many bits, and implement it in the FPGA. To show the potentiality of designed processor, 128-bit RSA encryption/decryption is implemented and compare with soft processor "MicroBlaze" in FPGA. The resulting processor uses only one DSP48E1 slice and four Block RAMs (BRAMs), and RSA encryption software on it runs in 0.42ms. However, MicroBlaze uses three DSP48E1 slices and 170 Block RAMs.
RSA Cryptography using our Designed Processor and MicroBlaze Soft Processor in FPGAs

(BRAMs) and runs in 152.28ms. Hence, the proposed designed processor is significantly efficient in terms of resource used and time complexity in comparison to soft processor "MicroBlaze" in FPGAs. Also the proposed processor can be used efficiently for longer bit arithmetic operation such as 2048-bit without further modifications and hence it is more flexible.

References

- VIRTEX-6 FPGA Memory Resources (V1.5), Xilinx Inc., 2010.
- VIRTEX 6 ML605 Hardware USER GUIDE (V1.2.1), Xilinx Inc., 2010.
- VIRTEX-6 FPGA DSP48E1 SLICE USER GUIDE (V1.3), Xilinx Inc., 2011.
- VIRTEX-6 FPGA DSP48E1 SLICE USER GUIDE (V1.2), Xilinx Inc., 2009.
- S. Bo, K. Kawakami, K. Nakano, and Y. Ito, "An RSA encryption hardware algorithm using a single DSP Block and single Block RAM on the FPGA," International


Index Terms

- Computer Science
- Security

Keywords

- Multiple-Length-Arithmetic
- MicroBlaze
- Soft Processor
- Montgomery Modular
- Multiplication in RSA
- FPGA
- DSP Slices
- Block RAMs