Abstract

This paper presents hardware implementation of multistage trapdoor knapsack public key cryptosystem which is primarily based on Merkle-Hellman scheme. So far, multistage knapsack is not broken and there has not been known a specific attack against this system. Modular multiplier is the critical and fundamental part of the hardware implementation. In this paper, Montgomery’s multiplication algorithm is modified with great hardware reduction. An efficient and optimized architecture for modular multiplication is proposed. Three stages knapsack public cryptosystem are implemented on DE2-115 FPGA development kit. The either implemented stages (encryption or decryption) take