VIII-P-2.4

THỰC HIỆN THUẬT TOÁN MÃ HÓA RSA TRÊN PHẦN CỨNG FPGA

Trần Hoàng Đạt, Lưu Xuân Vỹ
Khoa Điện tử - Viễn thông, Trường ĐH KHTN, ĐHQG-HCM

Tóm tắt

Ngày nay, bảo mật là một vấn đề vô cùng quan trọng trong việc truyền dẫn dữ liệu. Và RSA là một phương pháp mã hóa dữ liệu phổ biến và hiện quả cao. Trong thiết kế chúng tôi đề xuất sử dụng thuật toán Montgomery. Và để tối ưu tài nguyên hệ thống, chúng tôi đã tiến hành thay thế phép nhân số học 1024-bits trong thuật toán Montgomery bằng phép cộng số học và bộ dem. Thiết kế đã được kiểm tra thành công và đáp ứng được thời gian thực trên board DE2-115 của Altera với chip Cyclone® IV 4CE115 FPGA.

A LOW-COST FPGA-BASED IMPLEMENTATION USING RSA ALGORITHM

Abstract

This paper presents the FPGA implementation of RSA public-key cryptography based on the Montgomery's algorithm. By deeply analyzing, the authors replace the 1024-bit modular multiplication in the algorithm by only adders and buffers in order to reduce the resource costs. A completed real-time system have been built and tested successfully on DE2-115 Altera board with Cyclone IV FPGA chip so as to verify the operation of the implementation.

Email liên hệ: ***thdat@fetel.hcmus.edu.vn***