基于余数系统 RSA 密码算法快速实现

莫一奉，李树国

（清华大学 微电子学研究所，北京 100084）

摘　要：本文基于余数系统实现了 RSA 密码算法.为每一个计算单元选择形式相近的四个模，基于这四个模的约减单元比常规方法选模对应的约减单元所需要面积更小，延时而更短.按照本文提出的方法选模，选了 7 组共 28 个位宽为 74 的模，应用这些模基于 Cox-Rower 结构设计了余数系统蒙哥马利模乘器，实现 RSA 密码算法.在 SMIC 0.13 μm 标准单元库下进行综合，设计的 RSA 电路最高频率 278 MHz.在该频率下，中国剩余定理模式下的 1 024、2 048 位 RSA 以及常规模式下 1 024 位 RSA 解密分别需要 710 μs、99 μs、350 μs，快于已发表的同类设计.

Fast Implementation of RSA Algorithm Based on RNS

MO Yi-feng，LI Shu-guo

(Institute of Microelectronics, Tsinghua University, Beijing 100084, China)

Abstract：In this paper, we implement RSA cryptographic using Residue number system (RNS). We choose four modulo similar in the form for every computational unit. The reduction unit supports these four modulo is smaller and shorter than the required reduction unit corresponding to the conventional method selection. According to our proposed method, we select seven groups of modulo with a width of 74, and design a RNS Montgomery multiplier based on Cox-Rower architecture to implement RSA cryptography. In the SMIC 0.13 μm standard cell library, clock frequency reaches up to 278 MHz. At this frequency, 1 024, 2 048-bit RSA decryption in Chinese Remainder Theorem (CRT) mode and 1 024-bit RSA decryption require 710 μs, 99 μs, 350 μs, respectively, faster than the published related designs.

Key words：residue number system; RSA; fast implementation; montgomery multiplier

作者简介：

莫一奉　男，(1990-)，硕士研究生.研究方向为信息安全算法的大规模数字集成电路设计与实现.E-mail:873087176@qq.com.

李树国　男，(1963-)，教授，博士生导师.研究方向为信息安全算法的大规模数字集成电路设计与实现.