计算机工程 2009 35 (22): 224-226 ISSN: 1000-3428 CN: 31-1289/TP 首页 当期目录 上一期

工程应用技术与实现

基于Montgomery的RSA高速低成本实现

王 辉，刘宏伟，张慧敏

(北京科技大学信息工程学院，北京 100083)

收稿日期 修回日期 网络版发布日期 接受日期

摘要 给出一种支持多种位数RSA算法加密芯片的完整设计方案。采用改进的Montgomery模乘算法和LR模幂算法，根据大数运算的特点和降低资源消耗的需要改进主要运算电路的结构，并采用全定制IC的设计流程进行实现。实验结果表明，该方案结构简单，节省了面积，且能达到较高的性能。

关键词 RSA算法；模乘；模幂；进位保留加法器；Booth编码；超前进位加法器

分类号 TP301.6

DOI:

通讯作者:

作者个人主页: 王 辉;刘宏伟;张慧敏