计算机工程 2006 32 (23): 156-158,170 ISSN: 1000-3428 CN: 31-1289/TP

安全技术

基于FPGA的有限域求逆算法的改进及实现

鲍可进，宋永刚

（江苏大学计算机学院，镇江 212013）

收稿日期 修回日期 网络版发布日期 2006-11-23 接受日期

摘要 介绍了椭圆曲线密码和超椭圆曲线密码算法中一个重要的模块——求逆模块。分析并比较了现有的3种求逆算法，提出了针对FPGA快速实现的改进算法。根据改进的算法设计了求逆的硬件框图，并用VHDL实现了该设计。该设计使用Altera公司的Quartus II软件在EP1S10F780C6上进行编译、综合、布局布线。实验结果证明，该改进的算法无论在速度上还是在芯片面积上都具有比以往的算法更优秀的性能。

关键词 FPGA 椭圆曲线密码 超椭圆曲线密码 有限域 逆

分类号

DOI:

通讯作者:

作者个人主页: 鲍可进;宋永刚