计算机工程 2007 33 (24): 175-176 ISSN: 1000-3428 CN: 31-1289/TP

安全技术

基于GF(2n)上椭圆曲线标量乘的快速实现

杨先文，李 峥

解放军信息工程大学电子技术学院，郑州 450004

收稿日期 修回日期 网络版发布日期 2007-12-14 接受日期

摘要 椭圆曲线密码体制是一种基于代数曲线的公开密码体制，其曲线的标量乘速度决定了该密码体制的速度。正规基表示基域元素虽然利于硬件实现，但当n较大时会消耗大量的硬件资源。该文通过对椭圆曲线密码体制不同层次的算法进行分析，给出了具体的快速实现方案，并完成了与8位CPU的接口设计。FPGA实现结果表明，硬件消耗为14 544个逻辑单元，在频率为53.70 MHz时钟驱动下，运算速度为每秒40.71次。

关键词 多项式基 椭圆曲线 标量乘法

分类号 TP309

DOI:

通讯作者:

作者个人主页: 杨先文;李 峥