计算机应用 2006 26 (09): 2131-2133 ISSN: 1001-9081 CN: 51-1307/TP

信息安全

椭圆曲线点乘IP核的设计与实现

邹候文[1]; 王锋[2]; 唐屹[2];[2]

广州大学数学与信息科学学院[1]

收稿日期 2006-3-21 修回日期 网络版发布日期 2006-8-31 接受日期

摘要 基于NIST推荐的GF(2^163)上的Koblitz曲线，根据López改进Montgomery点乘算法，提出一种有限状态机控制的ECC点乘实现方案，设计了ECC点乘IP核。用QuartusⅡ5.0在EP2S90F1508C3器件中综合仿真，整个IP核消耗逻辑资源14502个ALUTs，最高主频166MHz,点乘运算速度可达12835次/s。

关键词 椭圆曲线 点乘 IP核

分类号

DOI:

对应的英文版文章:6031434

通讯作者:
邹候文 zouhw@163.com
作者个人主页: 邹候文 王锋 唐屹