计算机工程与应用 2007 43 (4期): 96-98 ISSN: 1002-8331 CN: 11-2127/TP

产品、研发、测试

基于智能卡的RSA与ECC算法的比较与实现

刘淳 张凤元 张其善

北京航空航天大学202教研室 北京航空航天大学 电子工程系

收稿日期 2006-1-12 修回日期 网络版发布日期 2007-1-23 接受日期

摘要 智能卡上的常用公钥算法为RSA和ECC算法。本文分别阐述了两者在带有加密协处理器的智能卡平台上的实现过程，包括RSA算法中模幂运算、模乘运算的实现；ECC算法中基域的选择、坐标系的选择、标量乘法和域算术运算的实现。并在Infineon的SLE66CLX系列智能卡芯片上实现了多种密钥长度的RSA和ECC算法，对两种算法的时间和空间效率进行了比较，根据比较结果指出了两者的优劣。

关键词 智能卡 RSA ECC

分类号

The comparing and implementation of ECC and RSA algorithms on smart card

Abstract

RSA and ECC are two public-key algorithms generally used on smart card. The implementation processes of those two algorithms on smart card with cryptographic coprocessor are explained separately. The implementation process of RSA includes modular exponentiation and modular multiplication. The process of ECC includes the selection of base field and coordinates, scalar multiplication and field operation. Later, according to the implementation of RSA and ECC algorithms with multiple key length on Infineon SLE66CLX320P smart card, time and space efficiency of these two algorithms is compared. And advantages and disadvantages are presented.

Key words smart card RSA Elliptic Curve Cryptography(ECC)

DOI:

通讯作者 刘淳 shniu@sohu.com