计算机工程与应用 2007 43 (2期): 157 ISSN: 1002-8331 CN: 11-2127/TP

网络、通信与安全

公钥密码中指数运算乘积的快速实现算法

史建红, 金晨辉

解放军信息工程大学电子技术学院201教研室

收稿日期 2006-1-25 修回日期 网络版发布日期 接受日期

摘要 多个指数运算的乘积是公钥密码学中的一种重要运算。该文针对求逆元素的运算量较大的情形,提出了两种有效实现该运算的算法:在基固定和基不固定两种情况下,分别将多个指数表示成联合稀疏形和串代换形式,然后利用快速Shamir算法进行计算。分析表明,算法有效降低了快速Shamir算法的运算次数。

关键词 公钥密码,数字签名,指数运算乘积,联合稀疏形

分类号

Fast Algorithms for Multi-exponentiation in Public Key Cryptography

,

解放军信息工程大学电子技术学院201教研室

Abstract

Multi-exponentiation is one of the important operation for public key cryptography. This paper presents two effective algorithms for multi-exponentiation when the inverse element is not easy to compute. First, transferring the exponents to joint sparse form and string-replacement form for fixed-base and unfixed-base multi-exponentiation separately; and then using the fast Shamir algorithm to obtain the result. The new algorithms reduce the operation number of fast Shamir algorithm effectively.

Key words public key cryptography digital signature multi-exponentiation joint sparse form

DOI:

通讯作者 史建红 shijianhong shijianhong2005@yahoo.com.cn