计算机工程与应用 2007 43 (7期): 163-166 ISSN: 1002-8331 CN: 11-2127/TP

网络、通信与安全

基于椭圆曲线密码体制的XML盲签名方案

程艳 傅鹂 陈承源 向宏 胡海波

重庆大学软件学院

收稿日期 2006-3-27 修回日期 网络版发布日期 2007-2-14 接受日期

摘要 通过将XML数字签名技术延伸到盲签名，并在实现中使用椭圆曲线公钥密码算法，提出了基于椭圆曲线密码体制的XML盲签名方案，用实例阐述了该方案的实施流程，并分析了其安全性。该方案结合椭圆曲线密码体制和XML数字签名的优势，在实现保护用户匿名性的同时，扩大了XML数字签名在受限环境中的应用范围，提高了网络环境中信息交换的效率。

关键词 盲签名 XML数字签名 椭圆曲线密码体制

分类号

XML Blind Signature Scheme Based on Elliptic Curve Cryptography

Yan Cheng

Abstract

This paper proposes an XML blind signature scheme based on Elliptic Curve Cryptography, uses an example to explain how to implement the scheme, and analyses its security. This scheme has increased the applications in limited environment, which need XML digital signature, and has improved the efficiency of information exchange on the Internet. At the same time, it has protected people’s anonymity.

Key words blind signature xml digital signature elliptic curve cryptography

DOI:

通讯作者 程艳 dennie_cheng@163.com