计算机应用 2008 28 (02): 432-433,436 ISSN: 1001-9081 CN: 51-1307/TP

信息安全

不使用对的基于身份的广播加密

张新方[1];徐秋亮[1]

山东大学计算机科学与技术学院[1]

收稿日期 2007-9-3 修回日期 网络版发布日期 2008-1-30 接受日期

摘要 基于身份的加密方案和基于身份的广播加密方案一般都是使用椭圆曲线上的双线性映射(也称为对)来实现的。提出一个不使用双线性映射的基于身份的广播加密方案，基于二次剩余假设，在Random Oracle模型下是可证安全的。

Abstract Identity Based Encryption(IBE) schemes and Identity Based Broadcast Encryption (IBBE) schemes are often constructed by using bilinear maps (a.k.a. parings) on elliptic curves. In this paper, an Identity Based Broadcast Encryption scheme without pairings was given. It is secure in Random Oracle according to the Quadratic Residuosity assumption.

关键词 广播加密 基于身份的加密 基于身份的广播加密 二次剩余

Key words broadcast encryption;identity based encryption;identity based broadcast encryption;quadratic residuosity

分类号

DOI:

通讯作者:
张新方 cindy1130@126.com

作者个人主页: 张新方 徐秋亮