电子与信息学报 2008 30 (9): 2246-2249 ISSN: 1009-5896 CN: 11-4494/TN

论文

一个高效的基于身份和RSA的紧致多重数字签名方案

张亚玲 张 璟 王晓峰

西安理工大学计算机科学与工程学院 西安 710048

收稿日期 2007-12-28 修回日期 2008-6-10 网络版发布日期 接受日期

摘要
紧致多重数字签名是指多个用户对同一个消息进行多重签名，所得多重签名的长度和单个用户签名的长度相当。该文提出一个高效的基于身份和RSA的紧致多重签名方案。签名和验证的效率比Bellare和Neven的多重签名方案提高了接近50%，多重签名的长度和单个RSA签名长度相当，因为使用了基于身份的公钥密码，新方案很好地实现了多重签名的紧致性目标。在随机预言模型和RSA假设下证明了方案的安全性。

关键词 数字签名；紧致多重数字签名；公钥密码；RSA密码体制

分类号 TP309

An Efficient Identity Based Compact Multi-signature From RSA

Zhang Ya-ling Zhang Jing Wang Xiao-feng

the School of Computer Science and Engineering, Xi'an Univ. of Tech., Xi'an 710048, China

Abstract
A compact multi-signature is a special digital signature that allows multiple signers to generate a signature on the same message with the property that the length of the signature is almost same as that of an individual signature. An efficient identity based compact multi-signature scheme from RSA is proposed in this paper. The efficiency of the new scheme is improved by 50% than that of Bellare and Neven's scheme. The signature length of the new scheme is almost same as that of a single RSA signature, as the identity based public key is used, the goal to design a compact multi-signature is nearly achieved. The security of the new scheme is proved under the assumption of RSA in the random oracle model.

Key words Digital signature Compact multi-signature Public key RSA cryptography

DOI:

通讯作者 张亚玲

作者个人主页 张亚玲 张 璟 王晓峰