电子与信息学报 2009 31 (10): 2392-2396 ISSN: 1009-5896 CN: 11-4494/TN

论文

原始签名人匿名的代理环签名研究

鲍皖苏, 隗 云, 钟普查

解放军信息工程大学电子技术学院 郑州 450004

收稿日期 2008-9-22 修回日期 2009-6-18 网络版发布日期 2009-9-29 接受日期

摘要
环签名是一种新的匿名签名技术，能保证签名用户的无条件匿名性。代理环签名是将代理签名和环签名相结合产生的一种签名。已有的代理环签名方案都是利用环签名的思想实现代理签名人的身份匿名性，但原始签名人的身份始终是公开的。该文基于RSA问题的难解性提出了一种新的代理环签名方案，在保证代理签名人身份匿名性的同时，还能保证原始签名人身份匿名性，并证明该方案在随机预言模型下能抵抗适应性选择消息攻击。

关键词 环签名 代理环签名 身份匿名性

分类号 TN918.1

Research on Proxy Ring Signature with Anonymity of the Original Signer

Bao Wan-su, Wei Yun, Zhong Pu-cha

Institute of Electronic Technology, the PLA Information Engineering University, Zhengzhou 450004, China

Abstract
Ring signature is a new kind of anonymous signature which can provide unconditional anonymity of the signer. Proxy ring signature is the combination of proxy signature and ring signature. Previous proxy ring signature schemes are constructed based on the idea of ring signature to provide the privacy protection for the proxy signer while the identity of the original signer is public. A new proxy ring signature scheme based on the difficulty of RSA problem is proposed in this paper, which can provide the privacy protection for both the proxy signer and the original signer. It proves that the proposed scheme can resist the adaptive chosen-message attack in the random oracle model.

Key words Ring signature Proxy ring signature Privacy protection

DOI:

通讯作者

作者个人主页 鲍皖苏; 隗 云; 钟普查