电子与信息学报 2005 27 (11): 1745-1749 ISSN: 1009-5896 CN: 11-4494/TN

论文

基于新型秘密共享方法的高效RSA门限签名方案

张文芳[*] [**], 何大可[*] [**], 王小敏[*],郑 宇[***]

[*]西南交通大学计算机与通信工程学院 成都 610031;[**]西南交通大学信息安全与国家计算网格省重点实验室 成都 610031

收稿日期 2004-5-31 修回日期 2004-11-19 网络版发布日期 2007-12-27 接受日期

摘要

针对传统的门限RSA签名体制中需对剩余环$Z_{\varphi(N)}$中元素求逆(而环中元素未必有逆)的问题，该文首先提出一种改进的Shamir秘密共享方法。 该方法通过在整数矩阵中的一系列运算来恢复共享密钥。由于其中涉及的参数均为整数，因此避免了传统方案中由Lagrange插值公式产生的分数而引起的环$Z_{\varphi(N)}$中的求逆运算。然后基于该改进的秘密共享方法给出了一个新型的门限RSA Rivest Shanair Atleman签名方案。由于该方案无须在任何代数结构(比如$Z_{\varphi(N)}$)中对任何元素求逆，也无须进行代数扩张，因此在实际应用中更为方便、有效。

关键词 秘密共享 门限群签名 RSA 子密钥(密钥影子) 可信任中心

分类号 TN918

A New RSA Threshold Group Signature Scheme Based on Modified Shamir's Secret Sharing Solution

Zhang Wen-fang[*] [**], He Da-ke[*] [**], Wang Xiao-min[*], Zheng Yu[*] [**]

[*]School of Computer and Communications Engineering, Southwest Jiaotong University, Chengdu 610031, China;[**]Laboratory of Information Security and National Computing Grid, Southwest Jiaotong University, Chengdu 610031, China

Abstract

In order to avoid computing elements' inverses in the ring $Z_{\varphi(N)}$ since they may not exit, a new RSA threshold group signature scheme based on modified Shamir's secret sharing solution is proposed. Differing from the old schemes based on Lagrange interpolation solution in which fraction arithmetic operations leading to the computation of elements' inverses in $Z_{\varphi(N)}$ should be handled, this new scheme reconstructs its group secret key through series of integer arithmetic operations in integral matrixes, by which it can efficiently avoid the computation of any element's inverse in any algebraic structure (such as $Z_{\varphi(N)}$), and can further avoid algebraic extensions. Therefore, this new scheme is more efficient and convenient than the old ones.

Key words Secret sharing Threshold group signature RSA Sub-key (shadow) Trusted party

DOI:

通讯作者

作者个人主页 张文芳[*] [**]; 何大可[*] [**]; 王小敏[*];郑 宇[***]