电子与信息学报 2010 32 (3): 693-699 ISSN: 1009-5896 CN: 11-4494/TN

论文

一种基于DAA的强匿名性门限签名方案

甄鸿鹄[①②], 陈 越[①], 郭渊博[①]

[①]解放军信息工程大学电子技术学院 郑州 450004; [②]解放军63612部队 瓜州 736100

收稿日期 2009-3-9 修回日期 2009-10-26 网络版发布日期 2010-3-4 接受日期

摘要
针对目前大多数门限签名方案不能实现签名成员匿名或匿名效果比弱的问题，该文提出了一种带有子密钥分发中心的强匿名性(*n*, *t*)门限签名方案。方案主要基于可信计算组织在其v1.2标准中采用的直接匿名认证(Direct Anonymous Attestation, DAA)方案，以及零知识证明和Feldman门限秘密共享等技术实现。相较已有方案，该方案即使在签名验证者和子密钥分发中心串通的情况下，也能够实现子签名的不可追踪性，也即可确保子签名成员的强匿名性。分析显示，方案除具有强匿名性外还具备签名子密钥不可伪造、子签名可验证以及一定的鲁棒性等特征。该方案在“匿名表决”等一些对匿名性要求较高的场合中有着重大的应用价值。

关键词 门限签名 匿名表决 直接匿名认证(DAA) 零知识证明 秘密共享

分类号 TP309

A Strong Anonymity Threshold Signature Scheme Based on DAA

Zhen Hong-hu[①②], Chen Yue[①], Guo Yuan-bo[①]

[①]Institute of Electronic Technology, the PLA Information Engineering University, Henan Zhengzhou 450004, China; [②]PLA NO. 63612 Unit, Guazhou 736100, China

Abstract
For most present threshold signature schemes, sub-sign member can not sign a message anonymously or theirs anonymity is very weak. To improve their anonymity, a strong anonymity (*n*, *t*) threshold signature scheme based on DAA (Direct Anonymous Attestation), which is adopted by Trusted Computing Group v1.2 specifications, is proposed. Compared with the others, the scheme colligates DAA, zero-knowledge proof and Feldman verifiable secret sharing technique to achieve untraceable sub-sign and insure strong anonymity of signers, even the verifier and the dealer are colluded. Besides strong anonymity, analysis shows the scheme also has the property of unforgeable share, verifiable sub-sign, and robustness etc. It can be used in the situations which desire high-level anonymity such as “anonymous voting”.

Key words Threshold signature Anonymous voting Direct Anonymous Attestation (DAA) Zero-knowledge proof Secret sharing

DOI: 10.3724/SP.J.1146.2009.00287

通讯作者 甄鸿鹄 xtwjngn@126.com

作者个人主页 甄鸿鹄[①②]; 陈 越[①]; 郭渊博[①]