计算机工程与应用 2010 46 (8): 1-4 ISSN: 1002-8331 CN: 11-2127/TP

博士论坛

构建无证书的两方认证密钥协商协议

侯孟波，徐秋亮，蒋 瀚

山东大学 计算机科学与技术学院，济南 250101

收稿日期 2009-11-26 修回日期 2010-1-13 网络版发布日期 2010-3-11 接受日期

摘要 基于无证书的认证密钥协商方案相比基于PKI的方案具有身份管理的简单性，同时相比基于身份的方案具有无密钥托管性。基于可证安全的无证书加密方案提出了一个两方认证密钥协商方案. 通过与其他方案在安全性和有效性方面的比较，该方案满足更多的安全属性要求，如完美前向安全性，PKG前向安全性，已知会话相关临时秘密信息安全性和无密钥托管等安全特性，同时具有良好的计算有效性。

关键词 认证密钥协商 无证书加密 完美前向安全 私钥生成中心（PKG）前向安全 密钥托管

分类号 TN918.1

Constructing certificateless-based two-party authenticated key agreement protocol

HOU Meng-bo，XU Qiu-liang，JIANG Han

School of Computer Science and Technology，Shandong University，Jinan 250101，China

Abstract

The certificateless-based authenticated key agreement protocols have the advantages of simplicity of managing identities compared to the PKI-based schemes，as well as avoiding the key escrow issues inherited in the identity-based schemes.This paper proposes a two-party certificateless-based authenticated key agreement scheme based on a provably secure certificateless-based public key encryption scheme.The comparisons with other comparable schemes in security and efficiency show that，the new scheme achieves more of the desired security attributes，such as perfect forward secrecy，PKG forward secrecy，known session-specific temporary information secrecy and key escrowless.Meanwhile it keeps the nice computational efficiency.

Key words authenticated key agreement certificateless-based encryption perfect forward secrecy Private Key Generator（PKG） forward secrecy key escrow

DOI: 10.3778/j.issn.1002-8331.2010.08.001

通讯作者 侯孟波 houmb@sdu.edu.cn