计算机工程与应用 2010 46 (7): 25-28 ISSN: 1002-8331 CN: 11-2127/TP

博士论坛

身份基认证密钥协商协议的分析与改进

侯孟波，徐秋亮

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 2010-1-14 网络版发布日期 2010-3-2 接受日期

摘要 对三个标准模型下可证明安全的身份基认证密钥协商协议进行了安全属性缺陷分析，在原方案基础上提出了一个安全增强的新方案。新方案满足目前已知的绝大多数安全属性要求，包括已知会话密钥安全性、抗密钥泄露伪装、抗未知密钥共享、无密钥控制以及消息独立性，特别是满足完美前向安全性、PKG前向安全性、已知会话相关临时秘密信息安全性，同时保持了良好的计算效率。

关键词 身份基认证密钥协商 安全属性 PKG前向安全性 已知会话相关临时秘密信息安全性

分类号 TN918.1

Analysis and improvement of ID-based authenticated key agreement protocols

HOU Meng-bo，XU Qiu-liang

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

Abstract

The security attributes of three provable secure ID-based authenticated key agreement protocols are analyzed，and an enhanced ID-based authenticated key agreement protocol is presented based on the previous work.The new scheme achieves most of the known security attributes，such as known-key secrecy，key-compromise impersonation resilience，unknown key-share resilience，no-key control and message independence，especially the PKG-forward secrecy and known session-specific temporary information secrecy attributes，meanwhile keeping with the nice efficiency.

Key words ID-based authenticated key agreement security attributes PKG-forward secrecy known session-specific temporary information secrecy

DOI: 10.3778/j.issn.1002-8331.2010.07.008

通讯作者 侯孟波 houmb@sdu.edu.cn