计算机工程 2012, 38(3) 134-136 DOI: 10.3969/j.issn.1000-3428.2012.03.045 ISSN: 1000-3428 CN: 31-1289/TP



安全技术

# 基于身份的P2PSIP可认证密钥协商方案

蒋 华[1,2]，贾永兴[1,2]，汪良辰[1,2]，杨庆锐[1,2]

(1. 北京电子科技学院通信工程系，北京 100070；2. 西安电子科技大学通信工程学院，西安 710071)

**摘要：** 为解决点对点会话初始协议(P2PSIP)的安全性问题，根据其分布式特点，结合身份公钥密码，提出一种可认证密钥协商方案。分析其安全性、运算效率和密钥托管等问题。该方案可以实现P2PSIP呼叫过程的双向身份认证和密钥协商，抵抗中间人攻击、重放攻击和离线密码攻击，防止消息体篡改、会话劫持和身份欺骗。

**关键词：** 点对点会话初始协议 身份 认证 密钥协商 双线性 密钥托管

# Authenticable Key Agreement Scheme for P2PSIP Based on Identity

JIANG Hua [1,2], JIA Yong-xing [1,2], WANG Liang-chen [1,2], YANG Qing-rui [1,2]

(1. Department of Telecommunications Engineering, Beijing Electronic Science and Technology Institute, Beijing 100070, China; 2. School of Telecommunications Engineering, Xidian University, Xi'an 710071, China)

Abstract: In order to fit with the Peer to Peer Session Initiation Protocol(P2PSIP) security issues and its distributed characteristics, this paper proposes an authenticable key agreement scheme for P2PSIP by using identity-based cryptography, and analyzes its security, efficiency and key escrow problem. This scheme provides mutual-authentication and key agreement in the process of P2PSIP call, ensuring the security of P2PSIP communication, and avoiding the disadvantage of Public Key Infrastructure (PKI).

Keywords: Peer to Peer Session Initiation Protocol(P2PSIP) identity authentication key agreement bilinear key escrow

**收稿日期** 2011-07-08 **修回日期** **网络版发布日期** 2012-02-05

DOI: 10.3969/j.issn.1000-3428.2012.03.045

**基金项目**:

中央办公厅信息安全与保密重点实验室开放基金资助项目(YZDJ0804)；北京市教育委员会共建专项基金资助项目

**通讯作者**:

**作者简介**: 蒋 华(1962－)，男，教授，主研方向：信息论与编码，密码通信；贾永兴、汪良辰、杨庆锐，硕士研究生

**通讯作者**E-mail: wlc8571@163.com

扩展功能

本文信息

Supporting info

PDF(284KB)

[HTML] 下载

参考文献[PDF]

参考文献

服务与反馈

把本文推荐给朋友

加入我的书架

加入引用管理器

引用本文

Email Alert

文章反馈

浏览反馈信息

本文关键词相关文章

点对点会话初始协议

身份

认证

密钥协商

双线性

密钥托管

本文作者相关文章

蒋华

贾永兴

汪良辰

杨庆锐

PubMed

Article by Jiang, H.

Article by Gu, Y. X.

Article by Hong, L. C.

Article by Yang, Q. D.

**参考文献：**

[1] Jennings C, Lowekamp B, Rescorla E, et al. Resource Location and Discovery(RELOAD) [EB/OL]. (2008-07-23). http://www. p2psip.org/drafts/draft-ietf-p2psip-reload-00.txt.

[2] 马 骥, 周晓光, 辛 阳, 等. 基于信任域的SIP认证机制[J].计算机工程.2009, 35(12):131-132 浏览

[3] Song H, Jiang X, Matuszewski M, et al. Security Requirements in Peer-to-Peer Session Initiation Protocol[EB/OL]. (2008-07-23). http://www.p2psip.org/drafts/draft-matuszewski-p2psip-security-

[4] requirements-03.txt.

[5] Song Yongchao, Zhao Ben, Jiang Xingfeng, et al. P2PSIP Security Analysis and Evaluation[EB/OL]. (2008-07-23). http://www. p2psip.org/drafts/draft-song-p2psip-security-eval-00.txt.

[7] Smart N P. An ID-based Authenticated Key Agreement Protocol Based on the Weil Pairing[J].Electron. Lett.2002, 38(13):630-

[8] Chen L, Cheng Z, Smart N P. Identity-based Key Agreement Protocols from Pairings [EB/OL]. (2010-03-12). http://grouper.ieee. org/groups/1363/IBC/submissions/Chen-IBE.pdf.

[10] 李晓霞, 宋茂强. 基于SIP的安全通信机制的研究[D]. 北京: 北京邮电大学, 2007.

## 本刊中的类似文章

1. 曹源, 杨林, 付宗波, 喻波, 徐小青.一种通用的身份模型及其构建流程[J]. 计算机工程, 2012,38(3): 119-120,123

2. 轩秀巍, 滕建辅, 白煜.基于二次剩余的增强型RFID认证协议[J]. 计算机工程, 2012,38(3): 124-125,129

3. 江琼希, 周南润.分簇式传感器网络多项式密钥预分配改进方案[J]. 计算机工程, 2012,38(3): 116-118

4. 张韶远, 卢建朱.基于生物特征的鲁棒远程用户认证方案[J]. 计算机工程, 2012,38(3): 137-138

5. 曹素珍, 王彩芬, 陈小云, 吕浩音.一种不含双线性对的可截取签名方案[J]. 计算机工程, 2012,38(3): 110-112

6. 丁清, 朱敏, 闫二辉.一种安全高效的WAPI改进策略[J]. 计算机工程, 2012,38(3): 153-155

7. 马巧梅, 王尚平.一个超轻量级的RFID认证协议[J]. 计算机工程, 2012,38(2): 151-152

8. 周才学, 周顽, 胡日新, 江永和.基于身份的签密方案分析与改进[J]. 计算机工程, 2012,38(2): 132-134

9. 牛淑芬, 王彩芬.多源线性网络编码的同态签名算法[J]. 计算机工程, 2012,38(2): 126-128

10. 谷宗运, 吕皖丽, 罗斌, 韩成美.基于特征点的抗几何变换图像被动认证算法[J]. 计算机工程, 2012,38(2): 229-230

## 文章评论

| | | | |
|---|---|---|---|
| 反馈人 | | 邮箱地址 | |
| 反馈标题 | | 验证码 | 7038 |
| | | | |