计算机工程 2012, 38(2) 132-134 DOI: 10.3969/j.issn.1000-3428.2012.02.042 ISSN: 1000-3428 CN: 31-1289/TP

安全技术

基于身份的签密方案分析与改进

周才学，周 顽，胡日新，江永和

(九江学院信息科学与技术学院，江西 九江 332005)

摘要： 分析3种基于身份的签密方案，使用不可区分性选择明文攻击(IND-CPA)方法对前2种方案进行攻击，使用IND-CPA和伪造攻击方法对第3种方案进行攻击，并分别给出改进方案。分析结果表明，这3种改进方案的运算效率较高，且具有机密性、不可伪造性、不可否认性、公开验证性和前向安全性。

关键词： 签密 基于身份的签密 语义安全性 不可伪造性 公开验证性 前向安全性

Analysis and Improvement of Identity-based Signcryption Schemes

ZHOU Cai-xue, ZHOU Wan, HU Ri-xin, JIANG Yong-he

(School of Information Science and Technology, Jiujiang University, Jiujiang 332005, China)

Abstract: This paper analyzes three identity-based signcryption schemes, attacks the first two schemes using Indistinguishability under Chosen Ciphertext Attack(IND-CPA), attacks the last one using IND-CPA and forgery attacks method and provides improved schemes respectively. Analysis results show that the improved schemes maintain higher efficiency while satisfying confidentiality, unforgeability, nonrepudiation, public verification and forward security.

Keywords: signcryption identity-based signcryption semantic security unforgeability public verifiability forward security

收稿日期 2011-04-21 **修回日期** **网络版发布日期** 2012-01-20

DOI: 10.3969/j.issn.1000-3428.2012.02.042

基金项目:

通讯作者:

作者简介: 周才学(1966－)，男，副教授、硕士、CCF会员，主研方向：网络与信息安全，密码学；周 顽、胡日新，副教授、硕士；江永和，讲师、硕士

通讯作者E-mail: charlesjjjx@126.com

扩展功能

本文信息

Supporting info

PDF(327KB)

[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

签密

基于身份的签密

语义安全性

不可伪造性

公开验证性

前向安全性

本文作者相关文章

周才学

周顽

胡日新

江永和

PubMed

Article by Zhou, C. H.

Article by Zhou, K.

Article by Hu, R. X.

Article by Jiang, Y. H.

参考文献：

[2] Malone-Lee J. Identity-based Signcryption[EB/OL]. (2002-07-09).

http://eprint.iacr.org/2002/098.

[3] Divya N, Reddy K C. Signcryption Scheme for Identity-based Cryptosystems[EB/OL]. (2003-05-07). http://eprint.iacr.org/2003/ 066.pdf.

[9] 李 顺, 曾 超, 李 军. 一种基于身份的签密方案[J].计算机工程.2010, 36(8):135-137 浏览

本刊中的类似文章

1. 李方伟, 万丽, 闫少军.基于椭圆曲线的盲代理盲签名方案[J]. 计算机工程, 2012,38(3): 139-140,144
2. 邓宇乔.一种前向安全的代理重签名方案[J]. 计算机工程, 2012,38(2): 144-145
3. 周莹莹, 张建中.一种有代理门限签名方案的密码分析与改进[J]. 计算机工程, 2012,38(01): 120-121,124
4. 宋明明, 张彰, 谢文坚.一种无证书签密方案的安全性分析[J]. 计算机工程, 2011,37(9): 163-164
5. 魏靓, 张串绒, 郑连清.一种基于身份的广义签密方案[J]. 计算机工程, 2011,37(8): 4-6
6. 孙静, 廖凯宁, 王伟 .一个可证明安全的短环签密方案[J]. 计算机工程, 2011,37(8): 140-142
7. 肖鸿飞, 刘长江.一种基于身份的改进高效签密方案[J]. 计算机工程, 2011,37(24): 126-128
8. 张建中, 张艳丽.一种子秘密可更新的动态多秘密共享方案[J]. 计算机工程, 2011,37(20): 117-119
9. 王琴.一种基于身份的代理签密体制[J]. 计算机工程, 2011,37(19): 120-121,125
10. 冀会芳, 韩文报, 刘连东.标准模型中基于身份的多PKG签密方案[J]. 计算机工程, 2011,37(18): 22-24

文章评论

反馈人		邮箱地址	
反馈标题		验证码	6293