计算机工程 2011, 37(24) 126-128 DOI: 10.3969/j.issn.1000-3428.2011.24.042 ISSN: 1000-3428 CN: 31-1289/TP

安全技术

一种基于身份的改进高效签密方案

肖鸿飞，刘长江

(解放军信息工程大学电子技术学院，郑州 450004)

摘要： 分析一种基于身份的高效签密方案S-IDSC的安全特性，指出其不满足前向安全性和公开验证性。为此，提出一种改进的基于身份的高效签密方案E-IBSC。安全性分析表明，改进方案能满足签密方案的一般安全要求。性能分析表明，改进方案保持了与原方案相当的计算复杂度，增加的通信负载在可接受的范围内。

关键词： 基于身份 签密 双线性对 前向安全性 公开验证性

Improved Efficient Identity-based Signcryption Scheme

XIAO Hong-fei, LIU Chang-jiang

(Institute of Electronic Technology, PLA Information Engineering University, Zhengzhou 450004, China)

Abstract: This paper analyzes the security issues of an efficient identity-based signcryption scheme S-IDSC. It indicates its lack of the security characteristics of forward security and public verifiability. An improved signcryption scheme E-IBSC is proposed. Security analysis shows that E-IBSC can satisfy the generic security requirements of signcryption schemes. Performance analysis shows that E-IBSC maintains the equivalent computational overheads with only additional acceptable communication load.

Keywords: identity-based signcryption bilinear parings forward security public verifiability

收稿日期 2011-06-29 **修回日期** **网络版发布日期** 2011-12-20

DOI: 10.3969/j.issn.1000-3428.2011.24.042

基金项目:

肖鸿飞(1984－)，男，硕士研究生，主研方向：网络安全，密码学；刘长江，高级工程师

通讯作者:

作者简介:

通讯作者E-mail: fieey1984@yahoo.com.cn

参考文献：

[2] Malone-Lee J. Identity-based Signcryption[EB/OL]. (2009-01-22). http://eprint.iacr.org/2002/098.

[4] 李 虓, 何明星, 罗大文. 基于身份的签密方案[J].计算机工程.2009, 35(22):144-146 浏览

本刊中的类似文章

1. 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

2. 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
3. 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
4. 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
5. 杨路.无对运算的无证书隐式认证及密钥协商协议[J]. 计算机工程, 2012,38(2): 138-140
6. 张建中, 马冬兰.一种高效的门限部分盲签名方案[J]. 计算机工程, 2012,38(01): 130-131,134
7. 高欢欢, 张建中.一种基于身份的门限代理签名方案[J]. 计算机工程, 2012,38(01): 132-134
8. 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
9. 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
10. 张玉磊.高效的无证书紧致有序多重签名方案[J]. 计算机工程, 2011,37(8): 108-111

文章评论

反馈人		邮箱地址	
反馈标题		验证码	2756