电子与信息学报
JOURNAL OF ELECTRONICS & INFORMATION TECHNOLOGY

电子与信息学报 » 2011, Vol. 33 » Issue (5) :1204-1210 DOI: 10.3724/SP.J.1146.2010.01031

标准模型下多个PKG的基于身份广义签密

冀会芳* 韩文报 刘连东*

信息工程大学 郑州 450002

Identity Based Generalized Signcryption Scheme for Multiple PKGs in Standard Model

Ji Hui-fang Han Wen-bao Liu Lian-dong*

Information Engineering University, Zhengzhou 450002, China

摘要 广义签密是指除了能实现签密功能，还可单独实现加密和认证功能的密码机制。该文定义了不同PKG环境下基于身份的广义签密方案较为全面的安全模型，并提出一个具体方案，进而在标准模型下证明了方案的安全性。和已有的不同PKG环境下基于身份签密方案相比，文中方案的效率较高，且应用范围更为广泛。

关键词： 基于身份密码 广义签密 不同PKG环境 双线性对 标准模型

Abstract： Generalized signcryption is a cryptographic primitive which could not only realize signcryption but also provide encryption and authentication alone. In this paper, the formal definition and a complete security notion of identity based generalized signcryption for multiple PKGs is defined. A concrete scheme is also proposed with security proof in standard model. Compared with several existing identity based signcryption schemes for multiple PKGs, the new scheme is more efficient and flexible.

Keywords： Identity based cryptosystem Generalized signcryption Multiple PKG environments Bilinear pairings Standard model

Received 2010-09-21;

本文基金:

国家973计划项目(2007CB807902)，新世纪优秀人才计划(NCET-07-0384)和全国优秀博士学位论文作者专项基金(FANEDD-2007B74)资助课题

通讯作者: 冀会芳 Email: huifangji@126.com

引用本文:

冀会芳, 韩文报, 刘连东.标准模型下多个PKG的基于身份广义签密[J] 电子与信息学报, 2011,V33(5): 1204-1210

Ji Hui-Fang, Han Wen-Bao, Liu Lian-Dong.Identity Based Generalized Signcryption Scheme for Multiple PKGs in Standard Model[J] , 2011,V33(5): 1204-1210

链接本文:

http://jeit.ie.ac.cn/CN/10.3724/SP.J.1146.2010.01031 或 http://jeit.ie.ac.cn/CN/Y2011/V33/I5/1204