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

电子与信息学报 » 2011, Vol. 33 » Issue (7) :1582-1588 DOI: 10.3724/SP.J.1146.2010.01346

基于身份的同时生效签密体制研究

刘文琦* 顾宏 杨建华*

大连理工大学电信学部 大连 116023

Identity-based Concurrent Signcryption Scheme

Liu Wen-qi Gu Hong Yang Jian-hua*

Faculty of Electronic Information and Electrical Engineering, Dalian University of Technology, Dalian 116023, China

摘要 签密体制能够在一个逻辑步骤内完成数字签名和加密两项功能。某些场合下，通信双方存在利益冲突，同时生效签名体制可以在不需要可信第三方的条件下提供签名交换的公平性。基于此，该文提出同时生效签密概念及其安全模型，并利用双线性对建立了一个基于身份的同时生效签密方案，证明了在BDH问题及Co-CDH是困难的假设下，方案是安全的。

关键词： 签密 同时生效签名 双线性对 随机预言模型

Abstract： Signcryption is a cryptographic primitive that combines both the function of digital signature and encryption in a logical single step. However, in some occasion there are conflicts of interest between the two entities, so concurrent signature is proposed to ensure fair exchange of the signature without special trusted third party. The notion of concurrent signcryption is defined and the security model is proposed in this paper. And an identity-based concurrent signcryption scheme is established using bilinear based on the framework. The scheme is proved to be secure assuming Bilinear Diffie-Hellman problem and Computational Co-Diffie-Hellman problem are hard in the bilinear context.

Keywords： Signcryption Concurrent signature Bilinear pairing Random oracle model

Received 2010-12-06;

通讯作者: 刘文琦 Email: wqliu@dlut.edu.cn

引用本文:

刘文琦, 顾宏, 杨建华.基于身份的同时生效签密体制研究[J] 电子与信息学报, 2011,V33(7): 1582-1588

Liu Wen-Qi, Gu Hong, Yang Jian-Hua.Identity-based Concurrent Signcryption Scheme[J] , 2011,V33(7): 1582-1588

链接本文:

http://jeit.ie.ac.cn/CN/10.3724/SP.J.1146.2010.01346 **或** http://jeit.ie.ac.cn/CN/Y2011/V33/I7/1582