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

电子与信息学报 » 2010, Vol. 32 » Issue (8) :1948-1952 DOI: 10.3724/SP.J.1146.2009.00824

通用可组合的三方口令认证密钥交换协议

邓淼磊① 王玉磊② 周利华①*

①(西安电子科技大学计算机学院 西安 710071)
②(南阳理工学院网络中心 南阳 473004)

Universally Composable Three Party Password-authenticated Key Exchange Protocol

Deng Miao-lei① Wang Yu-lei② Zhou Li-hua①*

①(College of Computer Science, Xidian University, Xi'an 710071, China)
②(Network Information Center, Nanyang Institute of Technology, Nanyang 473004, China)

摘要 现有的许多三方口令认证密钥交换(3PAKE)协议都被发现是不安全的。该文基于通用可组合(UC)模型，定义了3PAKE理想函数。在两方口令认证密钥交换理想函数辅助的混合模型下，构造了一个实现3PAKE理想函数的3PAKE协议。新的协议由中间密钥生成、消息认证传输和会话密钥生成3个阶段构成。该协议是UC安全的，并且结构简单。

关键词： 密码学 安全协议 口令认证密钥交换 通用可组合

Abstract： Many existing three Party Password-Authenticated Key Exchange (3PAKE) protocols are found insecure. An ideal functionality of 3PAKE is defined in the universal composability model，and a 3PAKE protocol is constructed to realize the 3PAKE ideal functionality in the hybrid model which aided by two party password-authenticated key exchange ideal functionality. The new protocol comprises of three phases: intermediate key generation, message authentication transmission and session key generation. The protocol is UC-secure, and has simpler structure.

Keywords： Cryptography Security protocol Password-Authenticated Key Exchange (PAKE) Universal composition

Received 2009-06-03;

本文基金:

河南省科技攻关计划项目(102102210432)资助课题

通讯作者: 邓淼磊 Email: zhyhyx@163.com

引用本文:
邓淼磊, 王玉磊, 周利华.通用可组合的三方口令认证密钥交换协议[J] 电子与信息学报, 2010,V32(8): 1948-1952

Deng Miao-Lei, Wang Yu-Lei, Zhou Li-Hua.Universally Composable Three Party Password-authenticated Key Exchange Protocol[J] , 2010,V32(8): 1948-1952
链接本文:

http://jeit.ie.ac.cn/CN/10.3724/SP.J.1146.2009.00824 或 http://jeit.ie.ac.cn/CN/Y2010/V32/I8/1948