

刘文菊,张俊伟,马建峰,杨超,李兴华.基于身份密钥交换的安全模型[J].通信学报,2010,(3):89-94

基于身份密钥交换的安全模型

DOI:

中文关键词:

英文关键词:

基金项目:

作者

单位

[刘文菊](#)

[张俊伟](#)

[马建峰](#)

[杨超](#)

[李兴华](#)

摘要点击次数: 378

全文下载次数: 382

中文摘要:

研究了基于身份的密钥交换协议的可证明安全问题。在通用可组合安全框架下,提出了基于身份密钥交换协议的模型。在攻击模型中,添加了攻陷密钥生成中心的能力。根据基于身份密钥交换的特点,设计了基于身份密钥交换的理想函数。在新的攻击模型和理想函数下,提出的模型既保证了基于身份密钥交换的通用可组合安全性,又保证了一个重要的安全属性——密钥生成中心前向保密性。此外,带有密钥确认属性的Chen-Kudla协议可以安全实现基于身份密钥交换的理想函数。

英文摘要:

[查看全文](#) [查看/发表评论](#) [下载PDF阅读器](#)

[关闭](#)

版权所有: 通信学报

地址: 北京东城区广渠门内大街80号通正国际大厦6层602室 电话: 010-67110006-869/878/915/917 电子邮件: xuebao@ptpress.com.cn

技术支持: 北京勤云科技发展有限公司