通信学报
Journal on Communications
主管单位：中国科学技术协会
主办单位：中国通信学会

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	

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：