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

冯 超,张 权,唐朝京.计算可靠的Diffie-Hellman密钥交换协议自动证明[J].通信学报,2011,(10):118~126

计算可靠的Diffie-Hellman密钥交换协议自动证明

DOI：

中文关键词：

英文关键词：

基金项目：

作者 **单位**

冯 超，张 权，唐朝京

中文摘要：

针对Diffie-Hellman密钥交换协议，提出了采用观测等价关系的建模方法，证明了该方法的可靠性，并利用该方法扩展了自动工具CryptoVerif的验证能力。发现了对公钥Kerberos协议自动证明中敌手能力模型的缺陷，并提出了修正方法。利用扩展的CryptoVerif自动证明了基于Diffie-Hellman的Kerberos协议的安全性，验证了该扩展方法的有效性。与现有大部分证明方法不同的是，该证明方法既保留了自动证明工具的易用性，又保证了计算模型下的强可靠性。

英文摘要：

查看全文 查看/发表评论 下载PDF阅读器

关闭