基于无证书密码学的可认证三方密钥协商协议

http://www.firstlight.cn 2010-05-01

为了使密钥协商协议能够抵抗主动攻击，提出了一个可认证的无证书三方密钥协商协议。首先分析现有密钥协商协议的特点，然后以无证书密码学理论为基础设计一个安全的三方密钥协商协议。该协议只需要一轮消息交换就可以建立起安全的三方会话密钥，有效地克服了密钥托管问题，提供完善的前向安全性。通过性能分析表明，该协议具有较高的安全性和运行效率。

存档文本