一个前向安全的基于签密的密钥协商协议

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

安全有效地传递信息是计算机安全通信研究领域的主要目标。借鉴Zheng和张串绒将签密技术运用到密钥协商协议中的思想，利用基于身份的签密方案，提出一种具有前向安全性的密钥协商协议。该协议在具有基于身份的公钥密码体制特点的同时，又拥有签密技术的优点。与已有的方案相比，该密钥协商协议除了具有机密性、认证性、还具有前向安全性的特点。

存档文本