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

张兴兰,张 振.双向匿名的基于属性的密钥隔离签密[J].通信学报,2013,(11):48~50

双向匿名的基于属性的密钥隔离签密

Attribute-based key-insulated signcryptionwith bidirectional anonymity

投稿时间： 2013-06-17

DOI：10.3969/j.issn.1000-436x.2013.11.006

中文关键词：基于属性签密 属性基 密钥隔离 密钥泄露 双向匿名

英文关键词:attribute-based signcryption attribute based key insulated key exposure bidirectional anonymity

基金项目:国家自然科学基金资助项目(61272044)

作者	单位
张兴兰，张 振	北京工业大学 计算机学院，北京 100124

中文摘要:

为解决发送者和接收者都具有匿名性的基于属性签密方案中密钥泄露的问题，将密钥隔离机制引入到基于属性签密方案中，给出了基于属性密钥隔离签密的形式化定义和安全模型，构建了随机预言模型下安全的基于属性的密钥隔离签密方案。改进后的方案不仅没有失去原有的双向匿名性，而且满足前向安全性和后向安全性的要求，减轻了密钥泄露带来的危害。最后在安全模型的基础上，给出了双向匿名的基于属性的密钥隔离签密的机密性、认证性和匿名性的安全性证明。

英文摘要:

To solve exposure of secret key in attribute-based signcryption with anonymity for both sender and receiver, key-insulation mechanism to attribute-based signcryption was untroduced. Given the formal definition and security notions, the scheme of attribute-based key-insulated signcryption was proposed, which is provably secure under the random oracle model. The improved scheme not only satisfies the requirement of bidirectional anonymity, but also achieves forward security and afterward security, consequently reduced the hazard of key exposure. Finally, confidentiality, authentication and anonymity in attribute-based key-insulated signcryption scheme were proved based on given security notions.

查看全文 查看/发表评论 下载PDF阅读器

关闭