

安全技术

基于RSA的同态密钥协商

向广利<sup>1</sup>, 朱平<sup>2</sup>, 张俊红<sup>2</sup>, 马捷<sup>2</sup>

(1. 武汉理工大学计算机学院, 武汉 430070; 2. 武汉大学计算机学院, 武汉 430072)

收稿日期 修回日期 网络版发布日期 2007-9-28 接受日期

摘要

回顾了密钥管理的基本内容, 介绍了RSA公钥密码体制和整数环上的同态加密机制, 提出了基于RSA的同态密钥协商。该协议主要利用RSA的公钥和同态加密机制建立一个会话密钥。与Diffie-Hellman以及基于口令的密钥协商协议相比, 它分别有更快的运算速度和较好的安全性。利用BAN逻辑证明了该协议的安全性。

关键词 [同态加密; 密钥协商; BAN逻辑](#)

分类号 [TP393](#)

DOI:

对应的英文版文章: [19-43](#)

通讯作者:

作者个人主页: [向广利<sup>1</sup>](#); [朱平<sup>2</sup>](#); [张俊红<sup>2</sup>](#); [马捷<sup>2</sup>](#)

扩展功能

本文信息

▶ [Supporting info](#)

▶ [PDF](#) (166KB)

▶ [\[HTML全文\]](#) (0KB)

▶ [参考文献\[PDF\]](#)

▶ [参考文献](#)

服务与反馈

▶ [把本文推荐给朋友](#)

▶ [加入我的书架](#)

▶ [加入引用管理器](#)

▶ [引用本文](#)

▶ [Email Alert](#)

▶ [文章反馈](#)

▶ [浏览反馈信息](#)

相关信息

▶ [本刊中 包含“同态加密; 密钥协商; BAN逻辑” 的相关文章](#)

▶ 本文作者相关文章

· [向广利](#)

· [朱平](#)

· [张俊红](#)

· [马捷](#)