计算机应用 2006 26 (11): 2576-2577 ISSN: 1001-9081 CN: 51-1307/TP

信息安全

基于加同态公钥密码体制的两方安全议价协议

赵洋[1];蓝天[2];马新新[2];张凤荔[2];[2]

电子科技大学[1]

收稿日期 2006-8-28 修回日期 网络版发布日期 2007-11-14 接受日期

摘要 安全多方计算及其应用是目前密码学领域的一个重要研究方向。在不需要第三方参与且保证安全的前提下，如何完成多方的协作运算是其研究的核心。基于加同态公钥加密算法的议价协议，是安全多方计算应用的一个具体实现，通过协议的执行，参与方可以进行商品价格的协商，并保障输入的私密性和结果的正确性。协议的执行过程中不需要第三方的参与，协议的安全性基于所采用的同态公钥加密算法。

Abstract Secure multi party computation with its applications is an important direction in current cryptography research field. The research focuses on how to accomplish the secure cooperative computation among multi party without the participation of the third party. The two party bargaining protocol, based on homomorphic public key cryptosystem, was an example of secure multi party computation s applications. One participant can make a bargain with the other by implementing the protocol. During the implementation of protocol, the privacy of input and the correctness of output could be preserved. The protocol can be implemented without the participation of the third party and its security was based on additive homomorphic public key cryptosystem.

关键词 安全多方计算 百万富翁问题 同态密码体制 议价

Key words secure multi-party computation;millionaires' problem;homomorphic public key cryptosystem;bargainin

分类号

DOI:

通讯作者:
赵洋 zhaoyang@uestc.edu.cn

作者个人主页: 赵洋 蓝天 马新新 张凤荔