结题报告：数据挖掘中的双方隐私保护——多方安全计算（SMC）问题探究

侯柏韬 齐风腾

摘要：该项目学习并总结了数据挖掘过程中的常用挖掘方式方法，根据其在对数字数据处理具有计算性的基础上，通过对多种常用方安全计算算法的学习和分析，提出了多方安全求和计算的协议方案。同时根据数据库联合计算的需求，改进了多方安全求和方案，并落于实施，通过对1500个模拟数据进行测试，验证了该协议算法的可行性和安全性。结果表明该算法可以在多个数据库进行联合计算时有效保证隐私数据的安全性。

作者、摘要、关键词、英文题名、英文摘要、英文关键词、正文、参考文献、附录和致谢

信息技术的快速发展使得信息数据库作为21世纪新的重要资源而得到了人们的重视，每个数据库中含有的信息就是数据库的核心所在，也是数据拥有者的资本。但单个数据库的存储量终究受限于存储条件、成本、信息源。因此信息资源共享成为新技术的必要手段。但是各个数据库的拥有者都要求本身私有信息的不可泄露或知识版权等问题，在资源共享过程中完成公共查询要求并不泄露自身的保密数据，这正是安全多方计算绝佳的应用场景。