**主要内容：**

随着全球数据总量的指数级增长，大规模数据的存储安全和隐私保护成为重要研究挑战。针对云存储场景的大量分析和统计发现存在大量冗余数据，数据去重技术被广泛应用进来检测并识别云存储系统中的共有重复数据以节省存储成本和网络带宽。

然而基于数据去重的云存储系统面临着数据隐私保护风险及其解决方法带来的性能问题，例如数据去重加密方法的机密性与时间开销，文件上传和文件访问中的隐私保护与计算开销，以及共享数据的可用性保障与存储开销等问题。因此，如何构建安全且高效的基于数据去重的云存储系统是目前亟待解决的问题。

**关键问题：**

在基于数据去重的云存储系统的文件数据访问过程中，多用户对共享数据采用访问控制以及收敛加密等方法方法来保护数据隐私性，但是也还面临诸多的挑战。具体而言，基于数据去重存储系统目前不可避免地面临着非法入侵、越权操作和设备故障等数据隐私保护的安全风险问题：首先，攻击者通过暴力破解攻击尝试获取数据的明文信息。其次，在文件上传和下载过程中攻击者通过两种方式破坏数据隐私性；具体而言，在文件上传中，攻击者实施哈希证明攻击来欺骗存储服务端并下载隐私数据；而在文件访问中，攻击者访问未授权的去重后数据。

**主要技术：**

1. 针对现有的数据去重加密方法面临的暴力破解攻击带来的数据隐私保护问题，研究一种基于用户语义感知的哈希摘要收敛加密方法，并研究用户间文件级基于服务器协助的加盐加密算法，结合研究用户内的数据块级别的基于用户协助加密算法生成随机安全密钥，以抵抗暴力破解攻击和减少整体加密过程中的时间开销；
2. 针对现有的所有权证明方法存在误判导致的数据隐私泄露和数据更新开销大的问题，研究一种基于两级验证和高效数据更新的所有权证明方法，研究结合快速索引验证策略和代数签名验证的挑战应答协议，来抵抗哈希证明攻击和避免隐私泄露，同时通过准确定位和部分更新的方法减少更新开销，以达到高效隐私保护的目标。
3. 针对现有的隐私保护中的访问控制方法存在对小文件计算开销大且不支持灵活用户撤销的问题，研究一种基于用户语义加密去重的访问控制方法，聚合小文件成段并利用传统数据去重中的相似性语义生成密钥加密数据来减少计算开销，同时利用基于代理的属性加密管理文件元数据以实现灵活用户撤销和减少元数据开销。

**技术就绪度：**

发表论文6篇，含CC推荐A类一篇，B类两篇， SCI（JCR一区）两篇；

1. Wen Xia, Hong Jiang, Dan Feng, Fred Douglis, Philip Shilane, Yu Hua, Min Fu, Yucheng Zhang, and Yukun Zhou. A Comprehensive Study of the Past, Present, and Future of Data Deduplication, Proceedings of the IEEE (PIEEE), Vol.104, No.9, 2016, pages 1681-1710. (中国计算机学会CCF推荐的A类期刊，影响因子：9.107)
2. Pengfei Zuo, Yu Hua, Cong Wang, Wen Xia, Shunde Cao, Yukun Zhou, and Yuanyuan Sun. Mitigating Traffic-based Side Channel Attacks in Bandwidth-efficient Cloud Storage, in Proceedings of the 32th IEEE International Parallel & Distributed Processing Symposium (IPDPS’18), Vancouver, British Columbia CANADA, May 21-25, 2018. (中国计算机学会CCF推荐的B 类会议)
3. Yukun Zhou, Dan Feng, Yu Hua, Wen Xia, Min Fu, Fangting Huang, and Yucheng Zhang, A Similarity-aware Encrypted Deduplication Scheme with Flexible Access Control in the Cloud. Future Generation Computer Systems (FGCS), Vol.84, pages: 177-189, 2017, Elsevier (SCI 索引, JCR1 区A 类期刊，影响因子：4.639)；
4. Yukun Zhou, Dan Feng, Wen Xia, Min Fu, Fangting Huang, Yucheng Zhang, and Chunguang Li, SecDep: A User-Aware Efficient Fine-Grained Secure Deduplication Scheme with Multi-Level Key Management. Proceedings of the 31st International Conference on Massive Storage Systems and Technology (MSST’15), Santa Clara, CA, USA, June, 2015, pages 1-14. (中国计算机学会CCF推荐的B类会议)
5. 周玉坤, 冯丹, 夏文, 付忞. 面向数据去重的基于二次哈希的收敛加密策略. 计算 机工程与科学, 第38 卷第9 期, 第1755-1762 页, 2016 年9 月.（中文核心期刊）
6. Pengfei Zuo, Yu Hua, Cong Wang, Wen Xia, Shunde Cao, Yukun Zhou, Yuanyuan Sun, “Mitigating Traffic-based Side Channel Attacks in Bandwidth-efficient Cloud Storage”, in Proceedings of ACM Symposium on Cloud Computing (SoCC), 2017. (Abstract Only).

专利和软著（四项）：

1. 一种适用于备份系统的安全数据去重方法和系统. 中国国家发明专利, 授权号: ZL201310301670.2, 日期: 2016.03.02. （已授 权）
2. 一种基于用户感知的高效安全数据去重方法及系统. 中国国家发明专利, 授权号: ZL201510257654.7, 日期: 2017.11.10. （已授权）
3. 一种相似性感知的安全数据去重方法. 中国国家发明专利, 申请号：201710963426.0, 日期：2017.10.09
4. 基于高效安全数据去重的备份系统, 中国计算机软件 著作权, 申请号: No.2015SR179323, 日期: 2015.09.15.

**拟产出成果：**

拟计划未来三年研究基于上述核心技术以及具体解决方案，发表学术论文2-4篇，申请专利软著2-4项等；