11.11-12.16工作汇报

董一林 2022 .12.19

2022.11.11-2022.12.16工作概括

根据毕业设计题目以及老师、师兄要求，主要针对以下三个模块进行学习:

① In-storage Computing架构
② Encrypted Deduplication去重技术
③ 同态加密技术（特别是全同态加密方案CKKS）

1.In-storage Computing(ISC)架构学习

相关论文阅读：

①SSD In-Storage Computing for List Intersection. 2016.6

在三星Smart SSDs中实验，通过ISC架构加速List Intersaction操作，通过实验验证ISC架构的优越性，并为如何制造和利用Smart SSDs提供建议。

②Insider: Designing In-Storage Computing System for Emerging High-Performance Drive. 2019.1

推出INSIDER，一种经过重新设计的全栈存储系统，帮助用户通过适度的编程工作利用In-storage computing架构。

③EISC— An FPGA-Based System-Level Emulation Platform. 2019.11

构建一个完整的基于FPGA的ISC仿真系统，使用此系统评估12个常见应用程序，从结果中得到选择ISC友好型应用程序的基本标准，并且通过假设一个通用的驱动程序结构，建立一个能够准确定量分析的分析模型。


论文阅读：SSD In-Storage Computing for List Intersection

DYL 2022/11/15

Abstract

in-storage computing/smart ssds：利用SSD离荷兰，在ssd内部计算.

list intersaction：在搜索引擎和分析查询中很重要的操作.

研究通过smart ssds加速list intersaction，降低能耗.

Tips：按住ctrl并单击论文标题可阅读对应MarkDown笔记

1.In-storage Computing总结

1. In-Storage Computing架构的特点：
将计算卸载到存储驱动器中，使计算直接在驱动器内部进行

2. In-Storage Computing架构的优点：

（1）节省驱动器到主机的互连带宽；
（2）节省主机到驱动器的互联带宽；
（3）最终充分利用新兴存储器的高性能；

3. 适合In-Storage Computing的任务：

（1）具有低操作强度；
（2）具有较高的相对数据比率；
（3）I/O密集型操作；

采取In-Storage Computing架构，将应用程序卸载到存储驱动器内之后应关注的重点：
设计准确定量分析模型，实验ISC架构的优越性

2.Encrypted Deduplication(E-Dedup)学习

相关论文阅读：

①Revisiting Frequency Analysis against Encrypted Deduplication via Statistical Distribution. 2022.5

通过分布性重新审视频率分析导致的安全漏洞，表明E-Dedup技术在利用底层存储工作负载特性的复杂频率分析攻击面前更加脆弱。

②Secure and Lightweight Deduplicated Storage via Shielded Deduplication-Before-Encryption.2022.11

传统DaE方式：先对数据执行Encrypt，在对加密数据进行Deduplication

研究DbE方式：先进行Deduplication,再Encrypt非重复的数据。

③Tunable Encrypted Deduplication with Attack-resilient Key Management. 2022.11

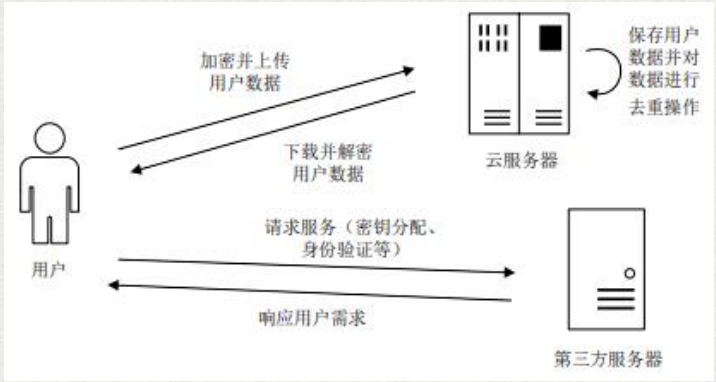
设计TED可调节机制，平衡存储效率和数据保密性之间的权衡，

通过配置存储膨胀因子放松MLE确定性性质，用于防御频率分析。

2.Encrypted Deduplication总结

1. Deduplication：

（1）一种粗粒度压缩技术，消除存储中的重复数据副本；
（2）仅存储复制块的一个副本，其他复制块引用指针；
（3）在备份、虚拟机映像、文件系统快照、云服务中应用广泛；



2. Encrypted deduplication：

（1）传统的加密通过MLE对称密钥原语实现；
（2）保留从加密数据块中进行重复数据删除的有效性；

3. Frequency analysis：

原始的加密方法建立在确定性加密基础上，不可避免泄露块的频率，以此进行攻击、去重

研究前景：加密和去重有时存在冲突，寻找合适的算法，同时实现安全性和存储高效率，
针对其计算资源、内存资源、带宽资源进行分析，研究可卸载到SSD内的操作，
与In-storage computing架构相结合。

3.同态加密&全同态加密方案CKKS学习

同态加密基础学习：

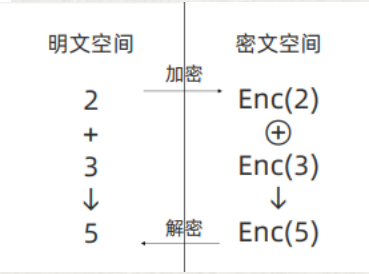
阿里安全双子座实验室《隐私计算基础理论：同态加密》

01 同态加密技术概览

02 半同态加密技术介绍

03 全同态加密技术介绍

04 同态加密的应用



CKKS相关论文阅读：

①Homomorphic Encryption for Arithmetic of Approximate Numbers.2017.12

构建近似算数的同态加密方案CKKS，支持加密信息的近似加法和乘法。

②A Full RNS Variant of Approximate Homomorphic Encryption.2018.8

在CKKS算法的基础上使用RNS(Residue Number System)和NTT(Number Theoretic Transformation)技术以加速原有CKKS算法。

③Better Bootstrapping for Approximate Homomorphic Encryption.2019.7

实现近似同态加密方案CKKS的Full-RNS变体的引导工作Bootstrapping。

3.同态加密&CKKS总结

1. 同态加密的特点：
   将原始数据经过同态加密后，对得到的密文进行特定的运算，然后将计算结果再进行同态解密后得到的明文等价于原始明文数据直接进行相同计算所得到的数据结果。

2. 同态加密的应用：
   （1）安全向量内积；
   （2）安全数据库；
   （3）安全聚合Secure aggregation；

3. CKKS的特点：
   针对实数或复数的浮点数加法和乘法同态运算，得到的计算结果为近似值，
   适用于机器学习模型训练等不需要精确结果的场景，可全同态加密。

4.研究前景：
   （1）针对CKKS的操作同态乘、同态加、Rescale、Relinearization、Rotation等，
   对NTT、KeySwitch进行优化，使用FPGA加速CKKS；
   （2）使用搭载FPGA的三星二代Smart SSDs，将CKKS卸载到ssd内部，
   通过In-storage computing架构加速CKKS算法。

End