**报告十五： 2021.4.16： New efficient constructions of verifiable data streaming with accountability(IEEE Annals of Telecommunications 2019) 报告人：李佳薇 记录者：李佳薇**

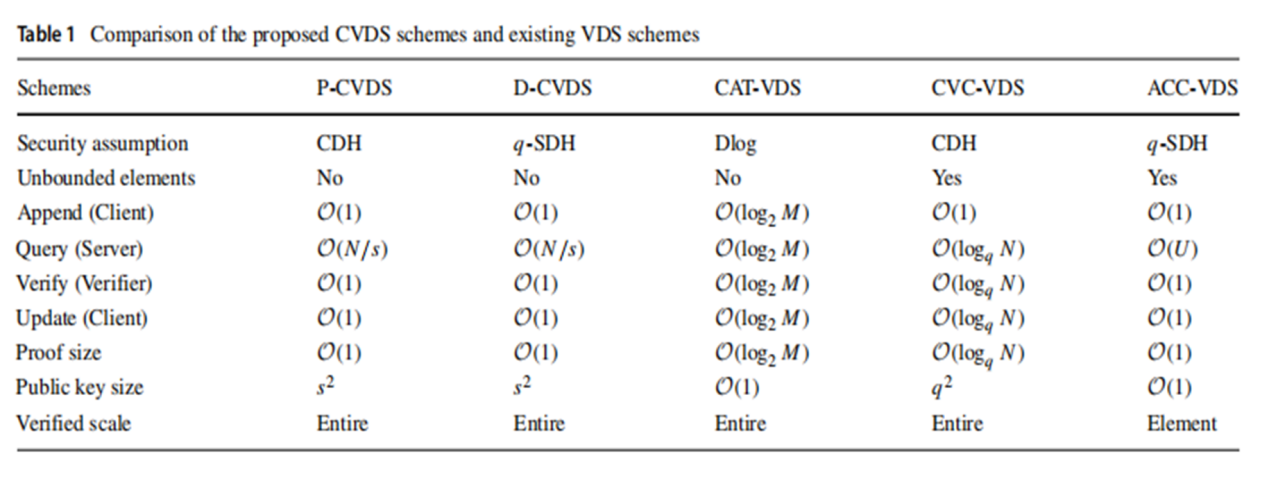
1. **报告内容**

**背景**

1、数据流方案中的问题：①树结构的复杂性 ②向量承诺的公共参数爆炸性③缺乏问责制

2、问责制：当验证结果失败时，验证者能够判断服务器或客户端的伪造。

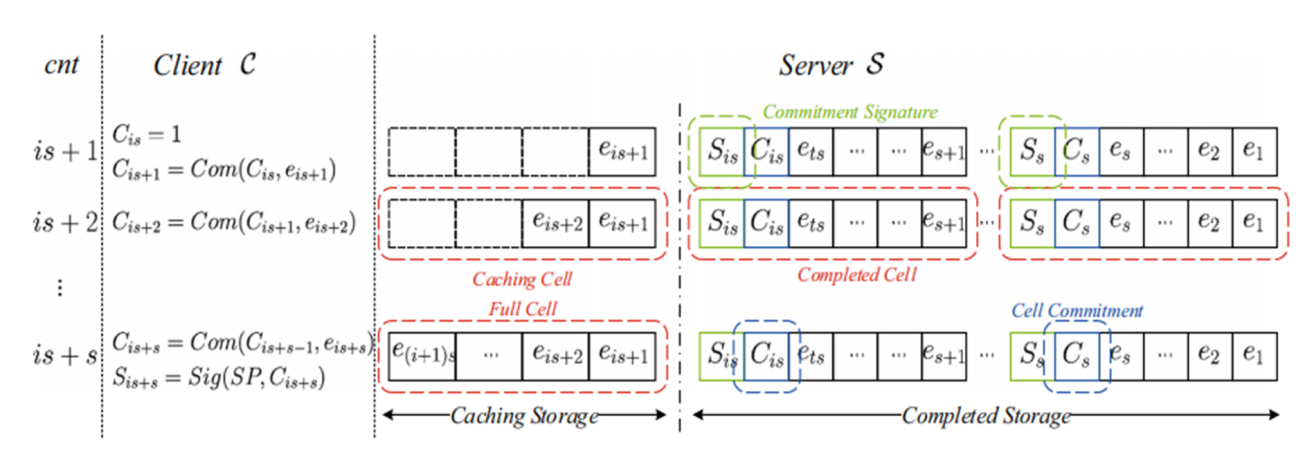
3、基于CVC的VDS方案的方案缺点：只能验证单个数据的正确性，而不是整个数据流的正确性。



**论文内容**

1、增维向量承诺(DIVC)

每个新到达的元素与单元格中之前的元素都按时间顺序提交，只有在元素的数量到达单元格容量的上限之前，才能确定单元格的承诺。此外，这些单元格共享一组关键参数，这直接减少了整个数据流过程的参数数量，并避免了使用基于树的结构。



1. 基于计数布隆过滤器P-CVDS和动态累加器的D-CVDS

DIVC可用于验证已完成的单元格的完整性，而布隆过滤器和累加器可确保所有的单元格承诺都是正确的。

**2、总结**

本篇论文提出融合问责制和验证整个数据流的VDS方案，但存在以下问题：

1. 问责制中，证据分解为服务器证据和客户端证据，无法确切证明服务器或客户端伪造。
2. 规定了数据的数量，不符合流数据的特性。
3. 完整单元格和缓存单元格中验证单个数据的承诺有什么区别？缓存单元格中的数据承诺存在哪里？
4. 针对大量流数据可以采用批处理技术验证吗？