Research of Data Security for Erasure-coded Storage Clusters

蔡颖　黄建忠　曹强　谢长生

武汉光电国家实验室

引言

为应对容量可扩展性和I/O高并发性等存储需求，集群存储系统不断被企业采用，并成为一种行之有效的存储方式。但是，

- 集群存储系统采用开放式网络存储架构，潜在地存在安全隐患；
- 集群存储系统是将独立的存储节点结合在一起来实现集群存储的，增加存储节点可以提升整个存储集群性能，同时也会增大存储节点失效的概率。

因此，必须采用合适的数据存储方案来增强存储集群中数据的机密性和可靠性。结合加密技术和纠删码技术，提供一种新的数据安全可靠存储方案，该方案可达到高数据机密性和存储可靠性，并通过对加密环节的改进使本方案在性能和空间利用率上都具有优势。

方法

加密模块中引入一异或因子nonce，让加密后的nonce和数据块进行异或运算，以达到加密数据块的效果，即对数据块进行间接加密取代直接加密，这将会大大降低加密过程的计算开销。此外，将nonce附在数据块后一起存储起来，可避免对nonce进行管理。具体过程见图1。

需要注意的是，为了避免明文攻击，对不同数据块必须采用不同的异或因子。在这，将使用数据块的哈希值作为该数据块对应的异或因子nonce。

由于最终的数据存储方案主要是应用XOR操作和RS编码技术，将其简称为XOR-RS存储方案。

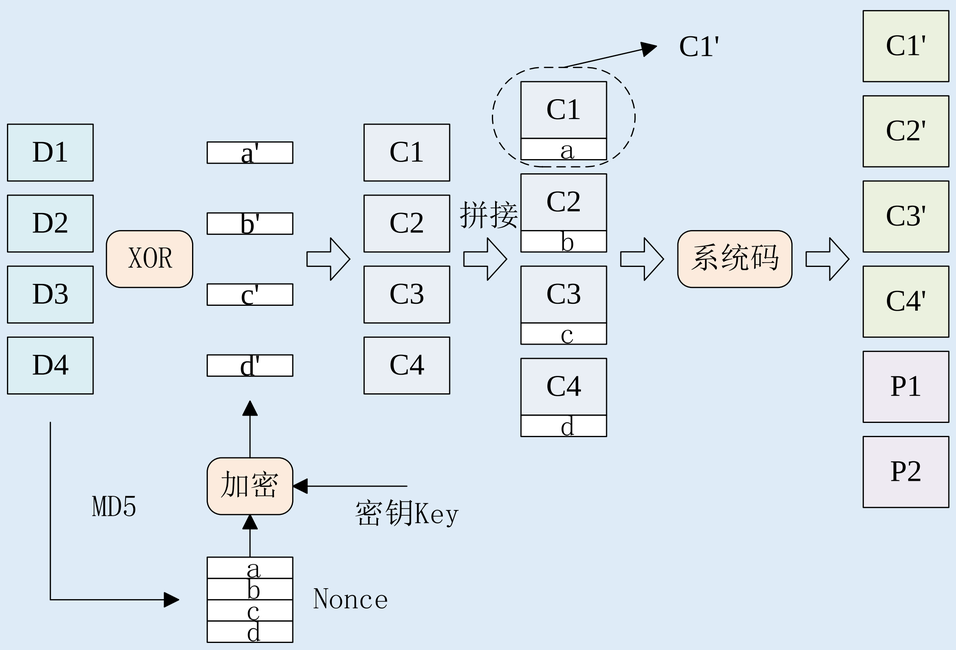


图1 纠删码异或加密，数据块对应的异或因子不同

XOR-RS方案的读写流程概述如下：

1）写数据，包括加密、编码、磁盘写三个环节；

2）正常数据读，包括磁盘读、解密两个环节；

3）失效数据读，包括磁盘读、解码、解密三个环节。

可以看出，数据读写包括多种不同环节，若按同步方式进行，必须等前一环节结束才能开始下一环节。但是由于编码使用的是系统码，写过程和失效读过程中，第一环节得到的加密数据块可以跳过编解码环节直接进行第三环节，同步运行会产生不必要的等待。因此，将各环节按流水线方式进行组织，以提高读写性能，如图2为写数据的流水线图。

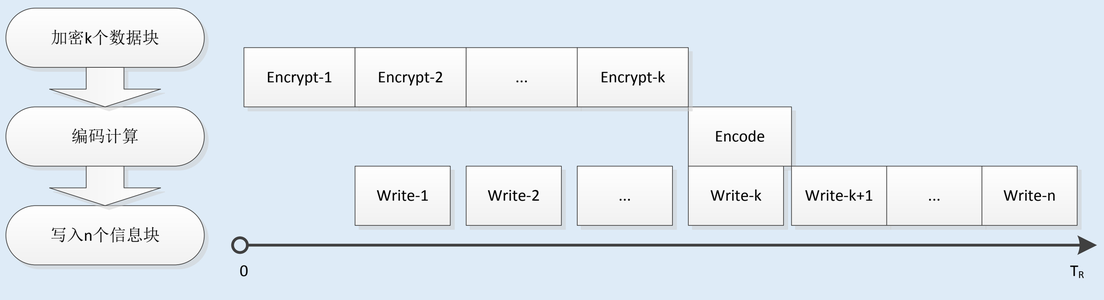


图2 写数据的流水线图

结果

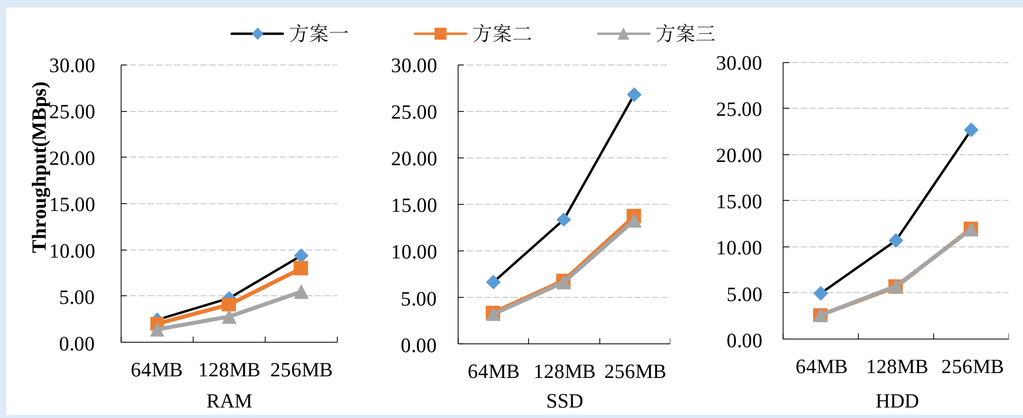
加密技术和两种冗余机制（副本和纠删码技术）分别结合组成两种基准方案，加密三副本方案和加密纠删码方案。这两种方案和XOR-RS在三种存储介质中分别对不同大小的数据进行测试。测试使用的加密方法为对称加密，纠删码采用RS编码。

表1为读/写功能中需要测试的时间开销。

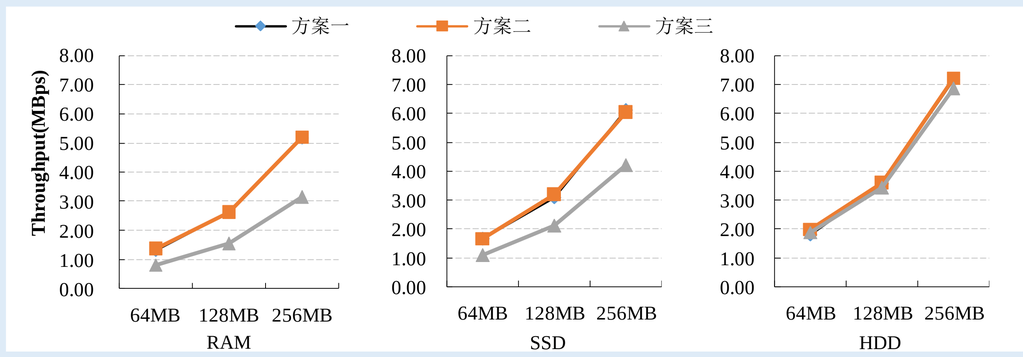
表1. 各功能需测试的时间开销

写数据	数据在内存，编码+加密+传输+写入
读数据	读取+传输（只传k块）+解码+解密

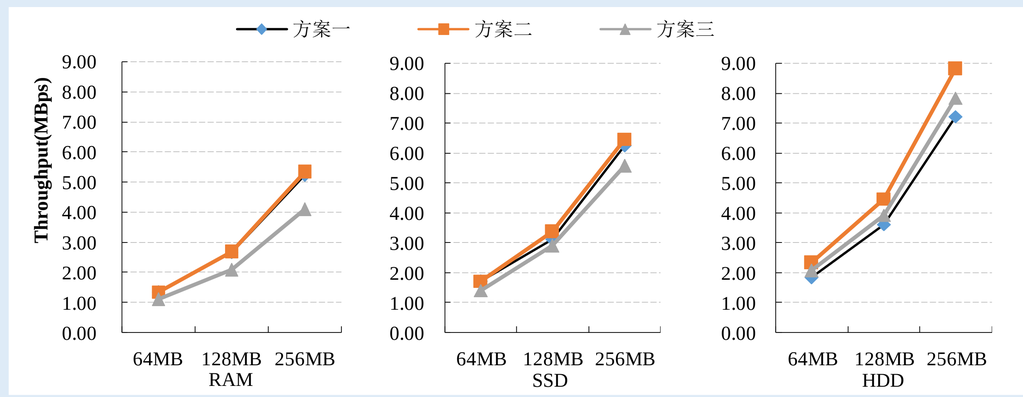
图3展示了在不同存储介质中不同方案的写性能和读性能。



a)写数据



b)正常读



c)缺块读

图3 不同存储介质RAM, SSD和HDD的写性能和读性能，a)写数据；b)正常读；c)缺块读

结论

新数据安全可靠存储方案（XOR-RS）的特点为：

- 使用加密的异或因子和数据进行异或操作，间接加密数据。异或因子的数据量比数据更小，异或操作又是一种高效运算，因而本方案具有更高的加密性能；
- 对比副本机制，纠删码技术可以在没有增加过量存储空间开销的基础上保证存储的高可靠性。

因此，本方案在性能和空间利用率上都具有优势。但是，本文仍存在一定的缺陷：

- 虽然本方案的加密性能变高，但加密强度可能会有一定程度的降低，在本文中并未探讨这一问题，将会加强对安全强度的研究
- 在此探究的安全性主要是围绕数据的机密性，将进一步对数据的完整性进行研究。

主要参考文献

[1] Weatherspoon H, Kubiatowicz J D. Erasure coding vs. replication: A quantitative comparison[M]//Peer-to-Peer Systems. Springer Berlin Heidelberg, 2002: 328-337.

[2] Diesburg S M, Wang A I A. A survey of confidential data storage and deletion methods[J]. ACM Computing Surveys (CSUR), 2010, 43(1): 2.