

面向分布式存储的高性能可重构加密方案

冯志华, 张宇轩, 罗重, 王佳宁

(北京计算机技术及应用研究所, 北京 100854)

摘要: 全球进入以数字经济为主导的信息社会, 数据成为关键生产要素, 当今越来越多的数据被收集、处理和存储, 分布式存储系统作为一种高效的存储架构在各数据领域得到广泛应用。然而, 随着数据存储规模的不断扩大, 分布式存储面临着信息泄露、数据破坏等更深层次的安全风险挑战。这些挑战将推动大数据分布式存储安全技术的创新变革, 促进了国产密码技术和计算存储技术的融合。针对分布式存储节点数据信息泄露等安全问题, 考虑到分布式存储加密性能与灵活性等需求, 提出一种动态可重构加密存储解决方案。该方案设计了基于 bio 映射框架的高性能可重构密码模块, 在此基础上构建多个配用不同密码算法的存储池, 实现高性能硬盘数据加解密操作和存储池密码算法动态切换, 并开发了具有密码算法和密钥远程在线加载功能的密码协议, 满足各存储节点可重构密码模块统一管理与便捷安全更新需求, 实现基于密码重构技术的数据细粒度加密保护和逻辑安全隔离功能。实验结果表明, 该方案对存储数据进行加密保护与安全隔离的性能损耗约 10%, 可为分布式存储系统达到 GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》第三级及以上在设备和计算安全、应用和数据安全等方面提出的密码应用技术要求提供技术途径。

关键词: 分布式存储加密; 可重构加密技术; 块设备加密; 算法在线加载; 逻辑安全隔离

中图分类号: TP309

文献标志码: A

DOI: 10.11959/j.issn.2096-109x.2023072

High-performance reconfigurable encryption scheme for distributed storage

FENG Zhihua, ZHANG Yuxuan, LUO Chong, WANG Jianing

Beijing Institute of Computer Technology and Applications, Beijing 100854, China

Abstract: As the world embraces the digital economy and enters an information society, data has emerged as a critical production factor. The collection, processing, and storage of data have become increasingly prevalent. Distributed storage systems, known for their efficiency, are widely used in various data fields. However, as the scale of data storage continues to expand, distributed storage faces more significant security risks, such as information leakage and data

收稿日期: 2022-12-06; 修回日期: 2023-03-21

通信作者: 张宇轩, 759464216@qq.com

基金项目: 国家重点研发计划 (2018YFB220030); 山东省重点研发计划 (2022CXGC010108)

Foundation Items: The National Key R&D Program of China (2018YFB220030), Key R&D Program of Shandong Province, China(2022CXGC010108)

引用格式: 冯志华, 张宇轩, 罗重, 等. 面向分布式存储的高性能可重构加密方案[J]. 网络与信息安全学报, 2023, 9(5): 59-70.

Citation Format: FENG Z H, ZHANG Y X, LUO C, et al. High-performance reconfigurable encryption scheme for distributed storage[J]. Chinese Journal of Network and Information Security, 2023, 9(5): 59-70.

destruction. These challenges drive the need for innovative advancements in big data distributed storage security technology and foster the integration of domestic cryptographic technology with computing storage technology. This work focused on addressing security issues, particularly information leakage, in distributed storage nodes. A dynamic and reconfigurable encryption storage solution was proposed, which considered the requirements for encryption performance and flexibility. A high-performance reconfigurable cryptographic module was designed based on the bio mapping framework. Based on this module, multiple storage pools equipped with different cryptographic algorithms were constructed to facilitate high-performance encryption and decryption operations on hard disk data. The scheme also enabled dynamic switching of cryptographic algorithms within the storage pools. A cryptographic protocol with remote online loading functions for cryptographic algorithms and keys was developed to meet the unified management and convenient security update requirements of reconfigurable cryptographic modules in various storage nodes. Furthermore, the scheme implemented fine-grained data encryption protection and logical security isolation functions based on cryptographic reconstruction technology. Experimental results demonstrate that the performance loss of this scheme for encryption protection and security isolation of stored data is approximately 10%. It provides a technical approach for distributed storage systems to meet the cryptographic application technology requirements outlined in GB/T 39786-2021 "Information Security Technology-Basic Requirements for Cryptography Applications" Level 3 and above in terms of device and computing security, application and data security.

Keywords: distributed storage encryption, reconfigurable encryption technology, block device encryption, algorithm online loading, logical safety isolation

0 引言

作为云存储中使用的重要技术之一, 分布式存储技术通过存储即服务模型实现了大批量数据的远程存储^[1-2], 使用此技术的分布式存储系统的可靠性、可用性和存取效率得到了提升, 并易于扩展。然而, 当前的分布式存储系统在安全方面仍存在问题, 在医疗、金融等重要领域中都曾出现数据泄露事件, 造成重大经济损失和不良社会影响。如何同时兼顾分布式存储系统的安全与性能, 确保存储数据不可泄露与安全隔离是当前亟待解决的问题^[3]。

在分布式存储环境下, 保证数据存储的安全性主要是保证数据自身的隐私性、机密性、完整性和可用性, 针对这些方面, 使用密码技术对数据存储安全进行保障是最合适且满足要求的方法。为对应用密码技术的分布式存储系统进行定性分析, 标准 GB/T 39786—2021《信息安全技术 信息系统密码应用基本要求》从物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全 4 个方面提出了密码应用技术要求, 标准 GB/T 37939—2019《信息安全技术 网络存储安全技术要求》从访问安全、系统安全、数据安全及管理

安全等方面对网络存储提出了安全功能要求和安全保障要求。根据以上需求, 结合分布式存储系统 in 应用场景及性能等方面对数据存储安全的需求, 具体总结如下。

1) 海量数据安全存储对高性能密码运算的需求。随着近些年数据量的不断增长, 大量数据的高性能计算和存储对分布式存储的性能提出了超高需求。同时, 标准 GB/T 40879-2021《数据中心能效限定值及能效等级》提出了对数据中心能效等级的技术要求, 随着绿色计算被业界广泛提及与推广, 对分布式存储系统提出了高性能、低功耗、低时延的需求, 数据的安全存储对高性能密码运算提出了需求。

2) 不同安全等级、不同用户对云端数据存储安全隔离需求。为了确保数据存储安全, 标准 GB/T 37973—2019《信息安全技术 大数据安全管理指南》中提出在系统安全性设计时需要考虑将不同类别和级别的数据分开存储, 采取物理或逻辑隔离机制。并且, 分布式存储系统需要为多种用户提供数据存储服务, 需要使用多种密码算法来保障不同用户数据和业务数据的安全隔离, 这对密码算法的快速灵活切换提出了需求。

3) 密码资源(密码算法参数及密钥等)统一

管理、便捷更新^[4]需求。部分涉及国家安全的重要领域，往往对密码算法有特殊需求，会使用区别于标准算法的非公开特定密码算法。这种背景下算法更新和升级的速度快，需要对算法信息等关键密码资源进行统一管控，保证其本地存储及外部配置的保密性和安全性。

有许多学者对分布式存储系统的数据安全性提升问题进行了研究。文献[5]提出一种应用于云计算场景的轻量级加密算法，用以提升安全性和降低性能损耗；文献[6]对 Ceph 分布式存储系统进行了改进，提出将加解密操作放置于各个客户端的网关，从而缓解加解密操作带来的性能瓶颈；文献[7]提出将存储文件数据分为两部分，每部分进行混淆加密后分割存储，可以实现更低的存储开销；文献[8]基于遗传算法，提出了一种应用于分布式存储系统的隐私数据保护框架；文献[9]提出一种加密数据的云存储方案，在封闭计算环境中对数据安全加密后再存储至分布式文件系统。以上提出的安全存储方案中均采用密钥变更的方式对数据进行保护，且没有做到对密码资源的统一管理和配置更新。

针对以上分布式存储系统的数据存储安全问题与需求，本文提出一种动态可重构加密存储解决方案，对存储节点数据进行细粒度加密和安全隔离。本文方案将存储空间划分为配用不同加密算法的存储池，采用可重构密码模块为存储池灵活快速地切换密码算法，提供数据细粒度加解密服务，并使用密钥管理系统为可重构密码模块提供密码算法和密钥远程在线加载配置和管理，实

现对密码资源的统一管理与便捷更新。

1 可重构密码芯片

相较于使用通用处理器架构以及专用集成电路架构的密码芯片，可重构密码芯片具有较高灵活性和性能，并且可以将算法信息进行隔离，在设计制造过程中不包含密码算法的信息，具有“安全白片”的特征^[10]。

本文使用的可重构密码芯片架构为粗粒度可重构架构（CGRA，coarse-grained reconfigurable architecture），其对称加密算法性能可达 25 Gbit/s，符合大规模数据的加解密性能要求。此芯片支持外部配置算法资源，算法及协议配置信息可通过映射工具编译完成后外部配置到可重构密码芯片中^[4]。不同密码芯片的性能对比如表 1 所示，测试算法为 AES（advanced encryption standard）对称加密算法。相较于其他架构的密码芯片，本文使用的密码芯片灵活性高，可以灵活快速配置和切换算法，与同架构的密码芯片相比，本文使用的密码芯片功耗较低，可以较好地满足高性能和低功耗的使用需求。

同时，可重构密码芯片作为一个独立的功能模块集成在系统中，可重构计算通路的重构功能由其配置通路完成，其功能实现和规模不受主控处理器的影响，具有较高的灵活度^[18]。并且，此可重构密码芯片支持物理不可复制函数（PUF，physical unclonable function），依据 PUF 对配置信息及密钥等进行保护，可以做到配置信息明文不出芯片、密码运算不出芯片，保证外部配置过程的安全性。

表 1 不同密码芯片的性能对比
Table 1 Comparison of performance of different cryptographic chips

类型	架构型号	工艺/nm	峰值性能/Gbit·s ⁻¹	实测性能/Gbit·s ⁻¹	功耗/W	能量效率/Gbit/(s·W) ⁻¹
CGRA	本文	28	25	9.37	3.50	7.14
	Cryptoratorpor ^[11]	45	128	—	6.18	20.72
FPGA	Virtex-5 ^[12]	65	58.75	—	1.40	42.02
	zedboard ^[13]	—	—	0.564	2.18	—
	Virtex-7 ^[14]	—	49.66	—	—	—
ASIC	定制设计 ^[15]	45	53	—	0.16	341.94
	定制设计 ^[16]	130	25.60	—	0.04	627.14
GPU	Gtx295 ^[17]	55	59.6	—	288.96	0.21

注：文献中未说明的密码芯片的相关数据在表格中用“—”标明。

2 动态可重构加密存储系统方案设计

2.1 设计原则

根据前文对分布式存储系统存储数据的加密需求分析, 本文设计一种面向分布式存储的动态可重构加密存储模型, 通过使用支持多种算法灵活重构的可重构密码芯片来实现可重构密码模块, 为存储数据提供密码服务和安全保障, 并使用密钥管理系统为可重构密码模块提供密码资源的安全配置和安全更新, 满足标准 GB/T 39786—2021《信息安全技术 信息系统密码应用基本要求》第三级及以上对应用密码技术的分布式加密存储系统的部分要求: 首先, 使用密码技术对登录设备的用户进行身份鉴别, 保证用户身份的真实性; 其次, 在远程管理设备时应采用密码技术建立安全的信息传输通道; 最后, 采用密码技术保证重要数据在传输和存储过程中的机密性。根据以上设计原则, 本文主要研究内容分为以下3点。

1) 本文选择在存储服务器端调用可重构密码模块对块存储数据进行加解密, 此过程对上层用户是无感知的, 用户不必考虑如何管理数据加密相关的密钥及算法信息, 并且为上层用户提供不同安全等级的数据资源读写, 实现数据安全隔离, 本文设计使用不同算法的加密存储池, 并实现与用户的绑定, 后续如果考虑应用系统细粒度安全需求, 可以增加应用层安全防护措施。

2) 在服务器端调用可重构密码模块对数据进行加解密操作需要考虑降低数据加解密所带来的性能损耗问题, 而在服务器端的应用层进行加解密, 数据需要从应用层流转至可重构密码芯片中进行加解密, 在流转时的损耗较大, 会影响到最终的整体性能。因此, 为实现对数据的较高性能加密存储, 减少数据传输损耗, 本文选择在服务器端文件系统级做改进, 通过在块设备层更改数据流传输, 调用可重构密码芯片对数据做加解密操作。

3) 为了对密码资源进行统一配置管理, 本文使用密钥管理系统对密码资源进行管理, 并设计对应的密码资源远程在线加载协议, 实现安全远程配置密码资源。

2.2 系统架构

本文所设计的分布式加密存储系统层次架构如图1所示。图中安全层功能的主要实现形式为存储网关, 不在本文的研究范围内, 本文主要在分布式存储的存储资源层进行研究, 增加了可重构加密存储服务, 包括可重构密码模块和加密存储池, 为用户提供数据高性能加密存储和逻辑安全隔离服务, 并在当前通用的密钥管理系统上增加了算法配置管理功能, 用于对可重构密码模块中的密码资源进行统一安全配置和管理。

根据以上层次框架, 本文提出分布式加密存储系统架构如图2所示。

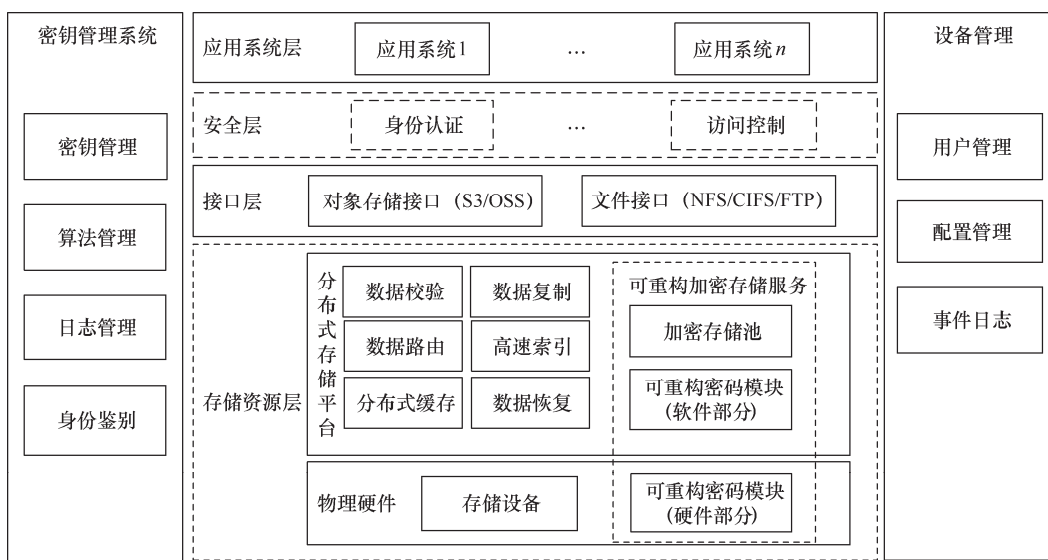


图1 分布式加密存储系统层次架构
Figure 1 Distributed encrypted storage system hierarchy architecture

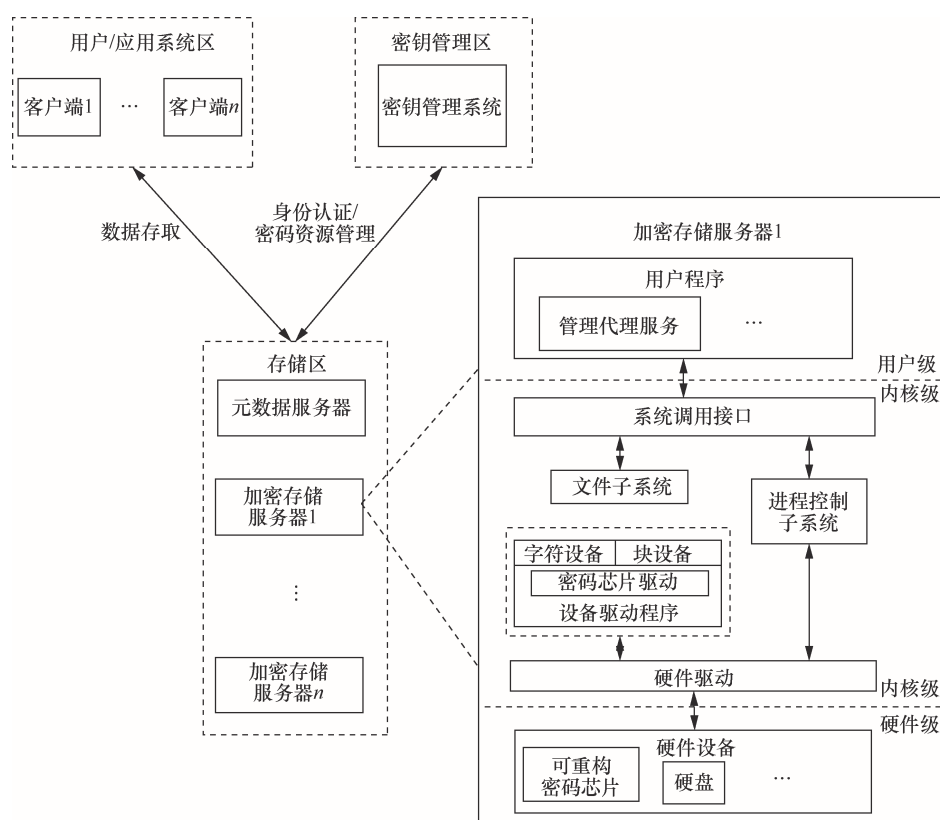


图2 分布式加密存储系统架构
Figure 2 Distributed encrypted storage system architecture

其中，可重构密码芯片部署在加密存储服务器中，可以对加密算法进行快速、灵活地重构，满足方案中需要灵活切换密码算法的需求。它可以通过部署于应用层的管理代理服务与密钥管理系统进行双向认证，构建安全会话通路，并向密钥管理系统发起请求进行密码资源的更新配置，之后可以依据存储池的划分重构得到对应的密码算法和加密密钥对数据进行加解密操作。

管理代理服务软件部署在加密存储服务器的用户层中，可以通过调用可重构密码模块，实现与密钥管理系统间的双向认证、密钥协商、密码资源下发配置及更新等功能。

密钥管理系统支持对称及非对称密码算法，对密码资源进行安全存储与统一管理，基于多级密钥管理体系对密钥的生成、激活、撤销、轮换、销毁、归档、恢复等全生命周期进行管理。在方案中，与管理代理服务建立安全会话通道后，系统为可重构密码模块使用的密码资源进行统一配置管理，底层使用硬件安全模块来确保密码资源

的保密性、完整性和可用性。

2.3 可重构密码模块设计

可重构密码模块的实现主要基于 Device Mapper (Device Mapper 是 Linux 系统内核中用来将块设备映射到虚拟块设备的架构) 下的 dm-crypt 加密模块，将设备映射模块定义在 Linux 内核 I/O 体系结构中的通用块层和 I/O 调度层之间，对于 bio 读写请求进行重定向处理。

在 Linux 数据读写架构中，内核层中的通用块层起到承上启下的作用，包含一系列与硬盘数据读写紧密相关的结构体，如请求 (request)、请求队列 (request_queue)、硬盘 (gendisk) 等^[19]。其中，bio 为通用块层的关键数据结构，它在 Linux 数据读写模型中承担着实际文件数据的逻辑地址和物理地址的映射与传输作用，描述了读写操作中硬盘数据的定位 (硬盘中起始扇区号和扇区数)。

在 Device Mapper 架构下，可以将实际的物理设备抽象为统一的逻辑设备后向系统内核提供

服务^[20],而在逻辑设备内部,则可根据需求构建原设备所不具有的功能,如磁盘阵列(raid)、加密(dm-crypt)、镜像(mirror)、快照(snapshot)等^[21]。其中,Device Mapper架构的加密功能通过虚拟出一个块设备,对转发的bio请求进行数据加密。因此,为实现较高性能的数据安全加密存储,在减少对操作系统内核修改的设计背景下,通过对Device Mapper架构下的dm-crypt模块进行设计,改变bio的传输流,即可实现主机、可重构密码芯片与存储硬盘三者之间数据的传输。

可重构密码模块设计如图3所示,图中密钥管理系统主要对可重构密码模块中的密码资源进行远程配置管理。在常规块设备读写体系下,bio请求到达通用块层时,已经建立起底层存储设备扇区与内存页之间的映射关系,通用块层根据bio中存储设备信息寻找与之对应的请求队列,并根据队列信息传递bio请求。在通用块层和I/O调

度层间建立起加密模块后,映射设备会作为虚拟块设备取代实际物理块设备来接收通用块层传来的bio,并将bio传递至映射设备虚拟块设备的请求队列,映射设备的虚拟块设备会向内核申请必要的内存资源以完成读写操作。目标驱动负责具体的读写调度操作,当接收到映射设备转发来的bio后,会确定实际目标设备扇区物理地址和bio读写信息,并根据读写请求调用驱动,将相应数据及地址信息转发至可重构密码芯片,可重构密码芯片调用相应加密算法,选择对应的加密密钥分量,并与地址信息进行异或计算组合得到数据块对应的加密密钥,实现对数据的细粒度加解密操作。

相较于原Device Mapper架构,本文可重构密码模块设计主要在dm-crypt模块下对bio的转发流程进行了修改,在目标驱动中解析bio并将数据转发至可重构密码芯片进行加解密操作。可重构密码模块读/写请求处理流程如图4所示,当

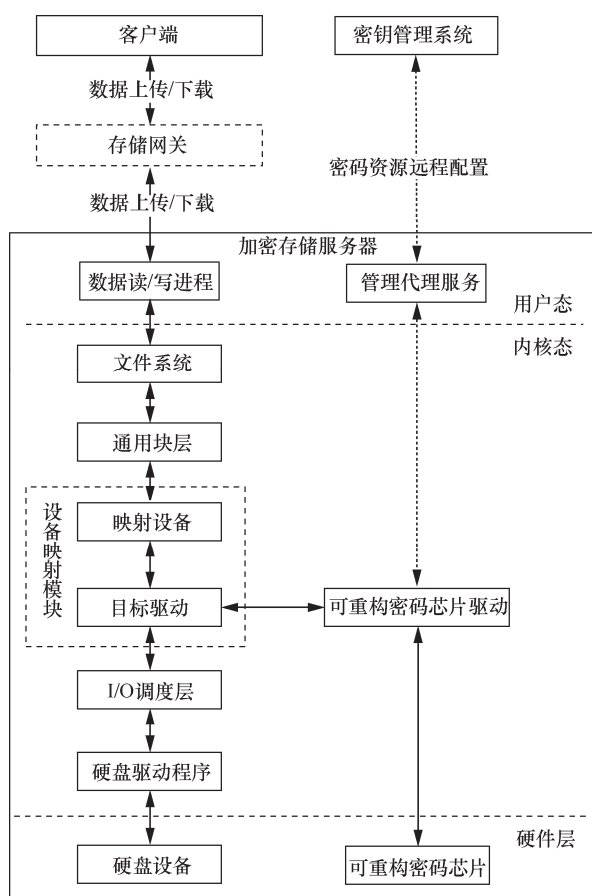


图3 可重构密码模块设计

Figure 3 Design of reconfigurable encryption module

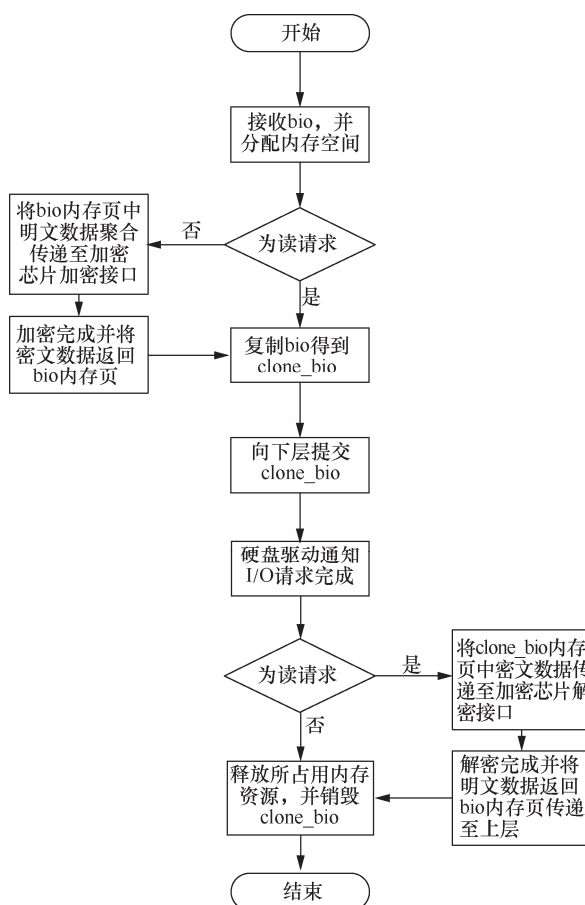


图4 可重构密码模块读/写请求处理流程

Figure 4 Reconfigurable encryption module read/write request processing

目标驱动接收到映射设备转发来的 bio 后, 会根据 bio 结构体确定实际目标设备扇区物理地址和 bio 读写信息, 并为 bio 的重定向与转发操作申请对应的内存资源。目标驱动根据 bio 是否为读/写请求, 调用可重构密码芯片来对数据进行解密读出或加密存储操作。

方案中设计的可重构密码模块主体在操作系统内核的块设备层实现, 通过使用 Device Mapper 架构, 可以使此模块较为便捷地应用到其他 Linux 系统中, 具有较高的可移植性。与 Linux 内核中已存在的 dm-crypt 加密模块相比, 方案重新定义了加解密模块的映射表, 调用可重构密码芯片实现更为高性能的数据加解密。

2.4 密码资源远程在线加载协议

为实现对密码资源(加密算法参数及密钥等)的统一管理, 满足对密码资源的更新配置操作, 本文方案基于可重构密码芯片的可动态配置特性, 设计了密钥管理系统与可重构密码模块间的算法资源远程在线加载协议。密钥管理系统安全

保存对应可重构密码芯片使用的算法资源数据(包括加密密钥及算法配置参数等), 密码资源远程在线加载流程如图 5 所示, 包括如下步骤。

1) 存储服务器启动后, 管理代理服务调用可重构密码模块与密钥管理系统进行安全认证和密钥协商, 身份认证与密钥协商过程遵循 GM/T 0050—2016《密码设备管理 设备管理技术规范》, 在密钥协商完成后构建安全会话通道, 通道传输的数据使用协商的会话密钥 key_{sess} 和对称加密算法 SM4 进行保护。

2) 双向认证成功并构建安全会话通路后, 管理代理服务调用可重构密码模块对应 API 接口得到需要进行参数及密钥配置的密码算法标识 alg_i , 并通过安全会话通路向密钥管理系统发送配置请求, 请求分发对应的密码资源。

3) 密钥管理系统接收解析密码算法标识 alg_i , 并从存储库中查询是否存在对应算法标识 alg_i 的密码资源信息 c , 若存在, 则与管理代理服务协商对密码资源信息 c 进行保护的一次性的分

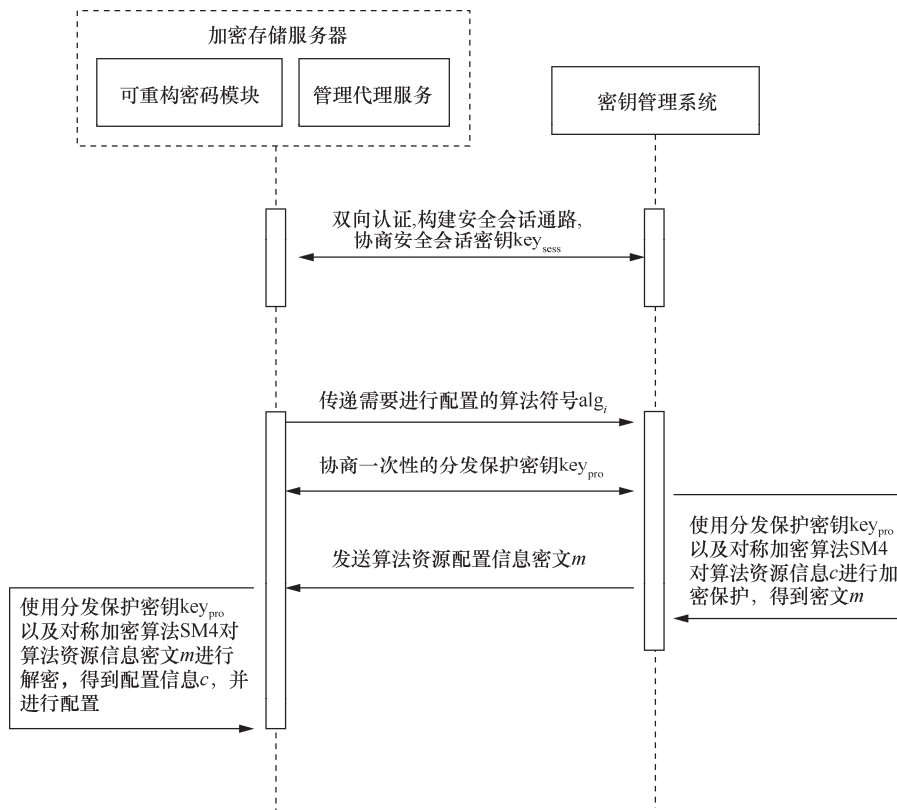


图5 密码资源远程在线加载流程
Figure 5 Remote online loading process of cryptographic resources

发保护密钥 key_{pro} , 协商分发保护密钥过程与数据结构遵循 GM/T 0051—2016《密码设备管理 对称密钥管理技术规范》。

4) 密钥管理系统利用协商的分发保护密钥 key_{pro} 以及对称加密算法 SM4 对密码资源信息 c 进行加密保护, 得到密文 m 后通过安全会话通道传输给管理代理服务。

5) 管理代理服务调用可重构密码模块, 使用分发保护密钥 key_{pro} 以及对称加密算法 SM4 解密密文 m 得到密码资源信息 c , 将密码资源信息 c 安全配置到模块内。

2.5 加密存储池设计

存储池是分布式存储系统和云平台的主要构成部分, 分布式存储系统管理员可以为特定数据类型创建存储池, 或者使用存储池将一组用户与另一组用户隔离。存储池需要在系统进行实施时对节点数量、磁盘配比以及用户角色划分等进行良好的规划, 以更好地支撑业务发展。

在设计实现可重构密码模块后, 每台加密存储服务器可在操作系统内核的块设备层调用可重构密码芯片对存储数据进行加密保护, 并且将对数据进行加密的加密密钥与数据块的块地址相关联, 实现对数据的细粒度加密保护。然而, 在当前分布式存储系统中, 服务需求差异较大、业务范围复杂、用户类型繁杂, 具有对不同用户、不同业务存储数据进行安全隔离的需求, 需要考虑将该加密模块应用于以下场景。

1) 系统中用户类型繁杂, 分为多种安全等级, 需要对不同等级的用户存储数据进行安全隔离。

2) 系统中业务范围多, 数据分为不同安全等级, 需要将不同安全等级的数据进行隔离存储。

为了对数据进行安全隔离, 保障数据的安全性, 本文依据所设计高性能可重构密码模块的算法可快速切换、动态重构特性, 结合分布式存储系统的存储池设计一种存储数据逻辑隔离方法。通过定义配用不同加密算法的可重构加密存储池, 对用户或业务存储数据时进行隔离约束, 保证不同等级数据的安全隔离存储。

为了将存储服务器上的数据隔离应用至整个分布式存储系统, 为不同等级的用户或业务

提供服务, 需要在分布式存储系统中提出加密存储池的概念, 即分布式存储系统为一组用户分配的存储区域, 包括其自身存储数据及所占有的存储资源, 多个用户可以将数据存储于同一个加密存储池, 但用户只能对自身存储区域进行访问。

根据以上规则结合可重构密码模块进行加密存储池设计, 如图 6 所示, 本文并未深入研究存储网关, 后续可通过网关实现用户身份认证和访问控制等功能。将每台加密存储服务器的存储空间进行划分后, 得到多个加密存储分区, 并规定存储服务器中划分的多个存储分区使用不同的对称加密算法和加密密钥对存储数据进行加密保护。在加密存储分区划分完成后, 为在分布式存储系统中对其进行统一管理, 本文方案设计将多台存储服务器使用同一种加密算法的存储分区进行划分映射, 规划得到多个加密硬盘域, 每个加密硬盘域由多个存储分区组成, 并且使用同一种加密算法对数据进行保护, 这样就能够将不同硬盘域的故障、存储资源进行隔离。最终基于加密硬盘域设计得到对应的加密存储池, 每个加密存储池内部规定使用多副本方式或纠删码方式对数据进行保护, 并为对应的一组用户提供数据安全存储服务, 可以实现不同等级用户的数据安全隔离。

3 系统安全性分析与实验测试

3.1 密码应用合规性分析

本节对所设计的分布式加密存储系统的安全性进行分析, 系统的安全性应满足标准 GB/T 39786—2021《信息安全技术 信息系统密码应用基本要求》中提出的 4 个基本安全要求: 机密性、完整性、真实性以及不可否认性。机密性指只有授权用户可以获取信息; 完整性指信息在输入和传输的过程中, 不被非法授权修改和破坏, 保证数据的一致性; 真实性指保证合法用户对信息和资源的使用不会被不正当地拒绝; 不可否认性指通信双方在信息交互过程中, 确信参与者本身, 以及参与者所提供信息的真实同一性, 即所有参与者都不可能否认或抵赖本人的真实身份。

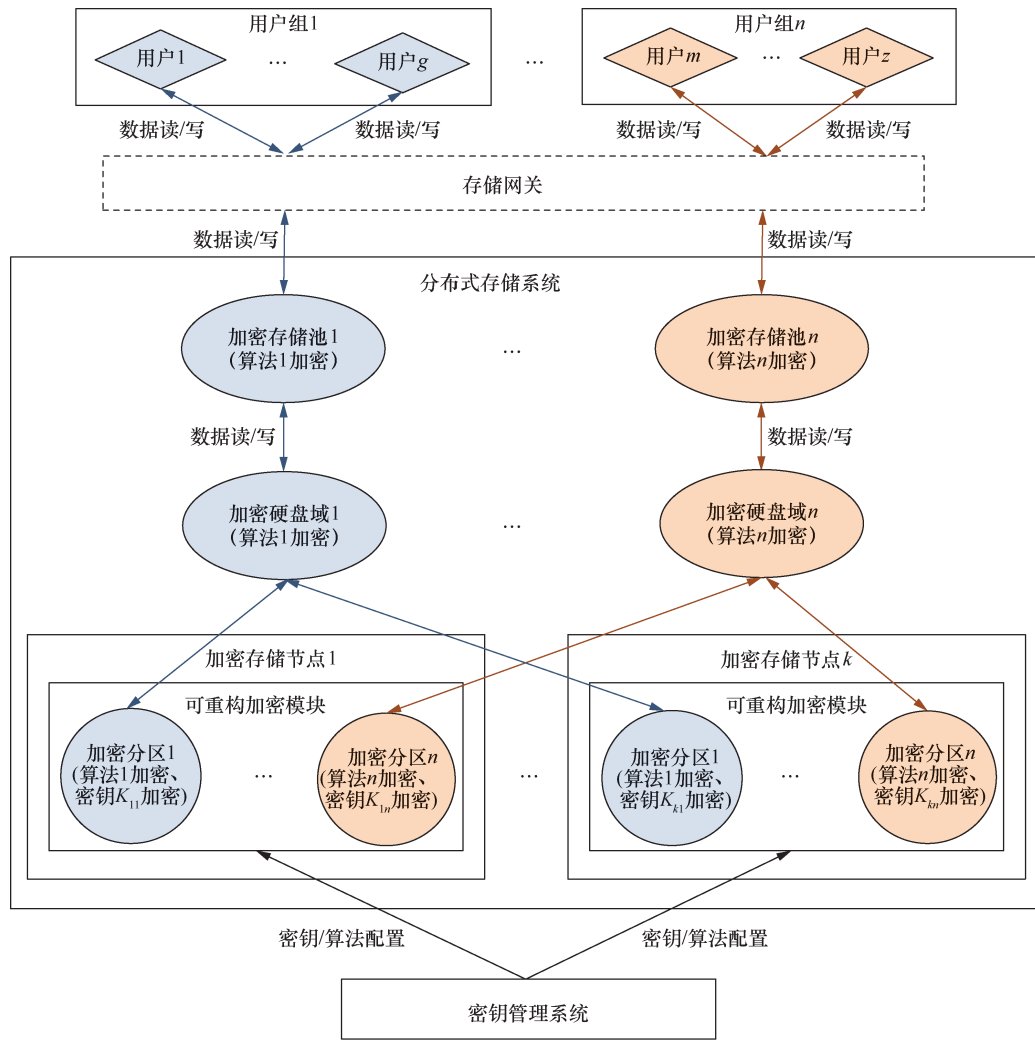


图6 加密存储池设计
Figure 6 Encrypted storage pool design

根据以上4个基本安全要求对所设计的分布式加密存储系统进行分析。

1) 系统的机密性：系统中的用户需要与加密存储池进行绑定，通过访问对应的加密存储池来上传或获取对应的数据，此时只有授权的系统用户才能访问使用对应加密存储池中的数据，保障系统中数据的机密性。

2) 系统的完整性：分布式存储系统都会使用完整性保护措施来保证数据传递和存储的完整性，且系统中所涉及密钥及算法传输的信息都会使用对应密钥进行加密保护，防止被攻击者获取或破坏，保障系统中数据和密码资源的完整性。

3) 系统的真实性：一方面，用户通过存储网

关才能获得访问存储系统的权限；另一方面，只有加密存储服务器通过与密钥管理系统间的双向认证，密钥管理系统才能正常进行密码模块密码资源的下发配置，进而为用户提供密码服务，保障系统的真实性。

4) 系统的不可否认性：本文主要集中在存储服务器上的数据加密存储研究，计划下一步在系统中使用数字签名和时间戳等技术来保证用户与存储系统间通信行为的不可抵赖性。

在对系统的整体安全性进行分析后，还需对系统中的密码资源安全进行分析。在本文方案中，密钥及算法参数的存储基于三级密钥保护体制，由密钥管理系统的硬件安全模块及可重构加密卡进行安全存储。所设计的密码资源

远程在线加载协议具体数据结构等规则遵循 GM/T 0050—2016《密码设备管理 设备管理技术规范》以及 GM/T 0051—2016《密码设备管理 对称密钥管理技术规范》，在将密钥或算法参数通过网络通道进行通信传输时需要先协商一次性的分发保护密钥来对其进行安全保护，实现通信过程的机密性，保障密钥及算法参数传输过程的安全性。

因此，本文方案在数据安全和密码资源安全两方面都提供了可靠的安全性保护。

3.2 系统性能测试

为验证可行性，本节将所设计方案应用于 Ceph 分布式存储系统，并且基于实现的系统完成相关性能测试。系统架构如 2.2 节所述，每台服务器配置好软硬件后，需要对存储空间进行划分，每个分区使用不同的算法对数据进行加密。本文系统中将整体存储空间划分为使用 SM4 算法、AES 算法以及 TEA (tiny encryption algorithm) 加解密的加密存储池。

系统部署如图 7 所示，测试环境中服务器型号为 t1800-24s，CPU 型号为 Intel Pentium CPU D1508 @ 2.20 GHz，硬盘为 HGST 960 G SSD，Ceph 存储系统的存储节点为 3 台物理机，并部署独立的可重构密码模块（考虑到存储加密容错需求，可以每台物理机部署多个密码模块进行冗余设计），物理机部署的操作系统为 Linux 系统，同时配置对应的密钥管理系统。

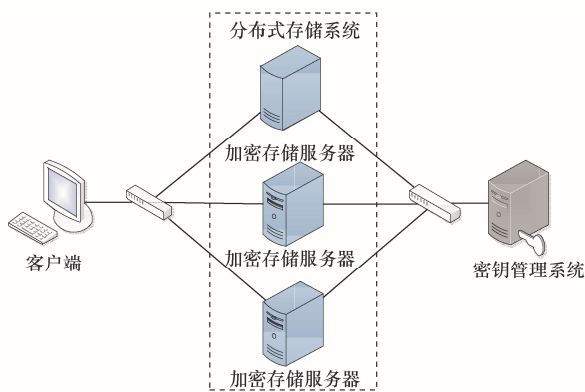


图 7 系统部署
Figure 7 System deployment

使用 fio 工具以及 vdbench 工具^[22]对应用本文方案实现的加密 Ceph 分布式存储系统以

及未应用本文方案的 Ceph 分布式存储系统的性能进行测试，测试中选择测试数据块大小为 4 kB 到 1 MB 之间，测试其 I/O 时延以及读写性能。

测试 I/O 时延统计结果如图 8 所示，加密系统的一次 I/O 任务被划分为数据加密时延、数据 I/O 时延和其他 3 部分操作。

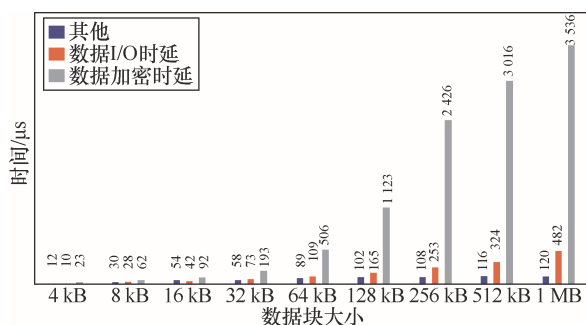


图 8 时延统计结果
Figure 8 Delay statistics result

根据前文设计以及测试结果分析，引入可重构密码模块后，增加的系统开销主要来源为：数据转发开销、加解密开销以及算法重构开销等。其中，数据转发开销主要为在系统内核解析数据并将其转发至可重构密码芯片的时延开销；加解密开销则是密码模块的主要性能损耗因素；算法重构开销是可重构密码芯片一次动态切换加密算法导致的开销，实际使用时可以忽略不计。

对系统的读、写性能测试结果如图 9 与图 10 所示，由测试结果可知，引入可重构密码模块后系统的读写性能有所下降，分布式存储系统单个存储节点的读写性能在原系统读性能的 90% 左右。

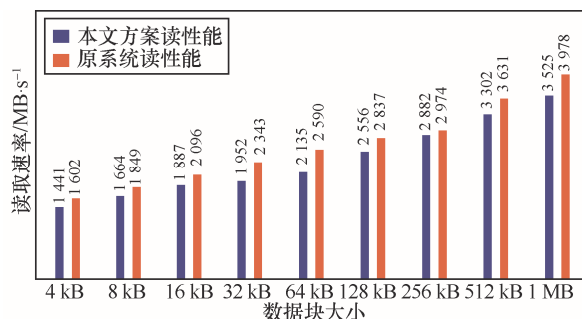


图 9 读性能测试结果
Figure 9 Read performance test result

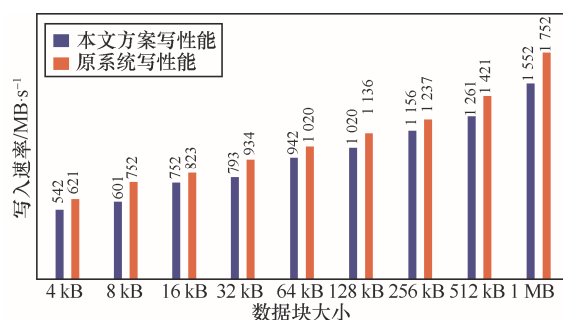


图10 写性能测试结果

Figure 10 Write performance test result

4 结束语

为提升分布式存储系统的安全性，完成对存储数据的高性能加密保护和安全隔离，本文提出一种动态可重构加密存储解决方案。方案基于 bio 映射框架，设计了具有较高可移植性和高性能的可重构密码模块，并在此基础上构建多个配用不同密码算法的存储池，实现高性能硬盘数据加解密操作和存储池密码算法动态切换；本文还设计了具有密码算法和密钥远程在线加载功能的密码协议，满足各存储节点可重构密码模块统一管理与便捷安全更新需求，实现基于密码重构技术的数据细粒度加密保护和逻辑安全隔离功能，并对每台存储服务器中嵌入高性能可重构密码模块的分布式存储系统进行测试，加密后性能满足预期需求。该方法可为分布式存储系统达到 GB/T 39786—2021《信息安全技术 信息系统密码应用基本要求》第三级及以上在设备和计算安全、应用和数据安全等方面提出的密码应用技术要求提供技术途径。

参考文献：

- [1] LI Y. Intelligent cryptography approach for secure distributed big data storage in cloud computing[J]. Information Ences, 2016: 103-115.
- [2] KAPUSTA K, MEMMI G. Enhancing data protection in a distributed storage environment using structure-wise fragmentation and dispersal of encrypted data[C]//IEEE International Conference on Big Data Science and Engineering; IEEE International Conference on Trust, Security and Privacy In Computing and Communications. 2017.
- [3] 桑杰, 许雪姣, 刘硕, 等. 基于国密算法的分布式加密存储研究[J]. 数据通信, 2020, (1): 4.
SANG J, XU X J, LIU S, et al. Research on distributed encrypted storage based on national security algorithm[J]. Data Commun, 2020, (1): 4.
- [4] 杨锦江. 基于可重构计算的密码处理器关键技术研究[D]. 南京: 东南大学, 2018.
YANG J J. Research on key technologies of reconfigurable cryptographic processors[D]. Nanjing: Southeast University, 2018.
- [5] FT A, ASA B, AA C, et al. A new lightweight cryptographic algorithm for enhancing data security in cloud computing-sciencedirect[J]. Global Transitions Proceedings, 2021.
- [6] SMITH A, RILEY J, SYED M, et al. Exploring untrusted distributed storage for high performance computing[C]//The Practice and Experience in Advanced Research Computing. 2019.
- [7] ABDEL-KADER R F, EL-SHERIF S H, RIZK R Y. Efficient two-stage cryptography scheme for secure distributed data storage in cloud computing[J]. International Journal of Electrical and Computer Engineering, 2020(3).
- [8] MARYAM K, SHAHZAD A, FARIA F, et al. Privacy-aware genetic algorithm based data security framework for distributed cloud storage[J]. Microprocessors and Microsystems, 2022(94).
- [9] 杜瑞忠, 王少泓, 田俊峰. 基于封闭环境加密的云存储方案[J]. 通信学报, 2017, 38(7): 10.
DU R Z, WANG S X, TIAN J F. Cloud storage scheme based on closed-box encryption[J]. Journal on Communications, 2017, 38(7): 10.
- [10] 袁航. 动态可重构密码芯片关键技术研究[D]. 北京: 清华大学, 2019.
YUAN H. Research on key technologies of dynamic reconfigurable cryptographic chip[D]. Beijing: Tsinghua University, 2019.
- [11] SAYILAR G, CHIOU D. Cryptoraptor: high throughput reconfigurable cryptographic processor[C]//IEEE/ACM International Conference on Computer-aided Design. 2014.
- [12] BULENS P, STANDAERT F X, QUISQUATER J J, et al. Implementation of the AES-128 on Virtex-5 FPGAs[C]//DBLP. 2008.
- [13] LI X, CAO C, LI P, et al. Energy-efficient hardware implementation of LUKS PBKDF2 with AES on FPGA[C]//Trustcom/Bigdataase/Ispa. 2017.
- [14] SMEKAL D, HAJNY J, MARTINASEK Z. Comparative analysis of different implementations of encryption algorithms on FPGA network cards[C]//IFAC Conference on Programmable Devices and Embedded Systems. 2018.
- [15] NISHIKAWA N, IWAI K, KUROKAWA T. High-performance symmetric block ciphers on multicore CPU and GPU[J]. International Journal of Networking & Computing, 2012, 2(2): 251-268.
- [16] RAHIMUNNISA K, KARTHIGAIAKUMAR P, CHRISTY N, et al. PSP: parallel sub-pipelined architecture for high throughput AES on FPGA and ASIC[J]. Central European Journal of Computer Science, 2013, 3(4):173-186.
- [17] BOS J W, OSVIK D A, STEFAN D. Fast implementations of AES on various platforms[J]. IACR Cryptology Eprint Archive, 2009: 501.
- [18] 王博. 高效可重构密码芯片架构及其抗物理攻击技术研究[D]. 北京: 清华大学, 2018.
WANG B. Energy efficient architecture and physical attack countermeasures for reconfigurable cryptographic processors[D]. Beijing: Tsinghua University, 2018.
- [19] 张包铨. 内核态时序数据存储服务设计与实现[D]. 成都: 电子科技大学, 2022.

ZHANG B S. Design and implementation of time series data storage system in kernel space [D]. Chengdu: University of Electronic Science and Technology of China, 2022.

- [20] 赵南雨, 陈莉君. 一种面向 Hadoop 中间数据存储的混合存储系统[J]. 信息技术, 2017(11): 161-166.

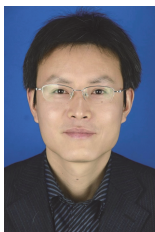
ZHAO N Y, CHEN L J. Hybrid storage system focus on Hadoop intermediate storing[J]. Information Technology, 2017(11): 161-166.

- [21] 周山东, 宋新芳, 金波, 等. 基于 TCM 的全盘加密系统的研究与实现[J]. 计算机工程与设计, 2012, 33(9): 6.

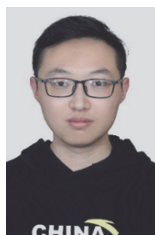
ZHOU S D, SONG X F, JIN B, et al. Research and implementation of trusted full disk encryption system based on TCM[J]. Computer Engineering and Design, 2012, 33(9): 6.

- [22] BERRYMAN A, CALYAM P, HONIGFORD M, et al. VDBench: a benchmarking toolkit for thin-client based virtual desktop environments[C]//IEEE Second International Conference on Cloud Computing Technology & Science. 2010.

[作者简介]



冯志华 (1979-), 男, 湖北孝感人, 博士, 北京计算机技术及应用研究所研究员, 主要研究方向为计算机及信息系统安全。



张宇轩 (1998-), 男, 河北石家庄人, 北京计算机技术及应用研究所助理工程师, 主要研究方向为计算机应用技术。



罗重 (1994-), 男, 湖北孝感人, 北京计算机技术及应用研究所工程师, 主要研究方向为计算机应用技术。



王佳宁 (1980-), 男, 河北安平人, 北京计算机技术及应用研究所高级工程师, 主要研究方向为密码管理理论、密码应用理论、密码工程。