通信学报
Journal on Communications
主管单位：中国科学技术协会
主办单位：中国通信学会

谭鹏许1,陈越1,兰巨龙2,贾洪勇1.用于云存储的安全容错编码[J].通信学报,2014,(3):109~115

用于云存储的安全容错编码

Secure fault-tolerant code for cloud storage

投稿时间： 2012-12-27

DOI：10.3969/j.issn.1000-436x.2014.3.012

中文关键词：RC编码 容错技术 云计算 云存储 基于公钥的门限体制 判定性BDHE假设

英文关键词:regenerating codes fault-tolerant cloud computing cloud storage threshold public-key encryption decisional BDHE assumption

基金项目:国家科技支撑计划基金资助项目(2008BAH37B03)

作者	单位
谭鹏许1，陈越1，兰巨龙2，贾洪勇1	1. 解放军信息工程大学 网络空间安全学院，河南 郑州 450004；2. 国家数字交换系统工程技术研究中心，河南 郑州 450002

中文摘要:

针对当前基于RC编码的容错技术的安全缺陷，提出了一种安全编码——SRCS编码，以保证在云计算以及云存储这种高度开放环境下，存储系统容错过程中数据的安全性。该编码将门限体制引入到了传统的RC编码当中，利用基于公钥的门限体制保护编码矩阵，在确保基于传统RC编码的容错技术高效、低冗余优势的前提下，解决了其在开放环境下编码矩阵存在的安全问题。最后利用判定性BDHE假设，在部分适应性攻击模型下证明了SRCS编码的安全性。

英文摘要:

A secure regenerating code, called SRCS was proposed to solve the security problem during the process of the fault-tolerant of storage systems, especially the storage system in an extremely open environment such as cloud computing and cloud storage. SRCS achieves the security of the encoding matrix in the regenerating code using the threshold public-key encryption with low redundancy and high efficiency. It is proven that SRCS is secure in the semi-adaptive model using decisional BDHE assumption.

查看全文 查看/发表评论 下载PDF阅读器

关闭