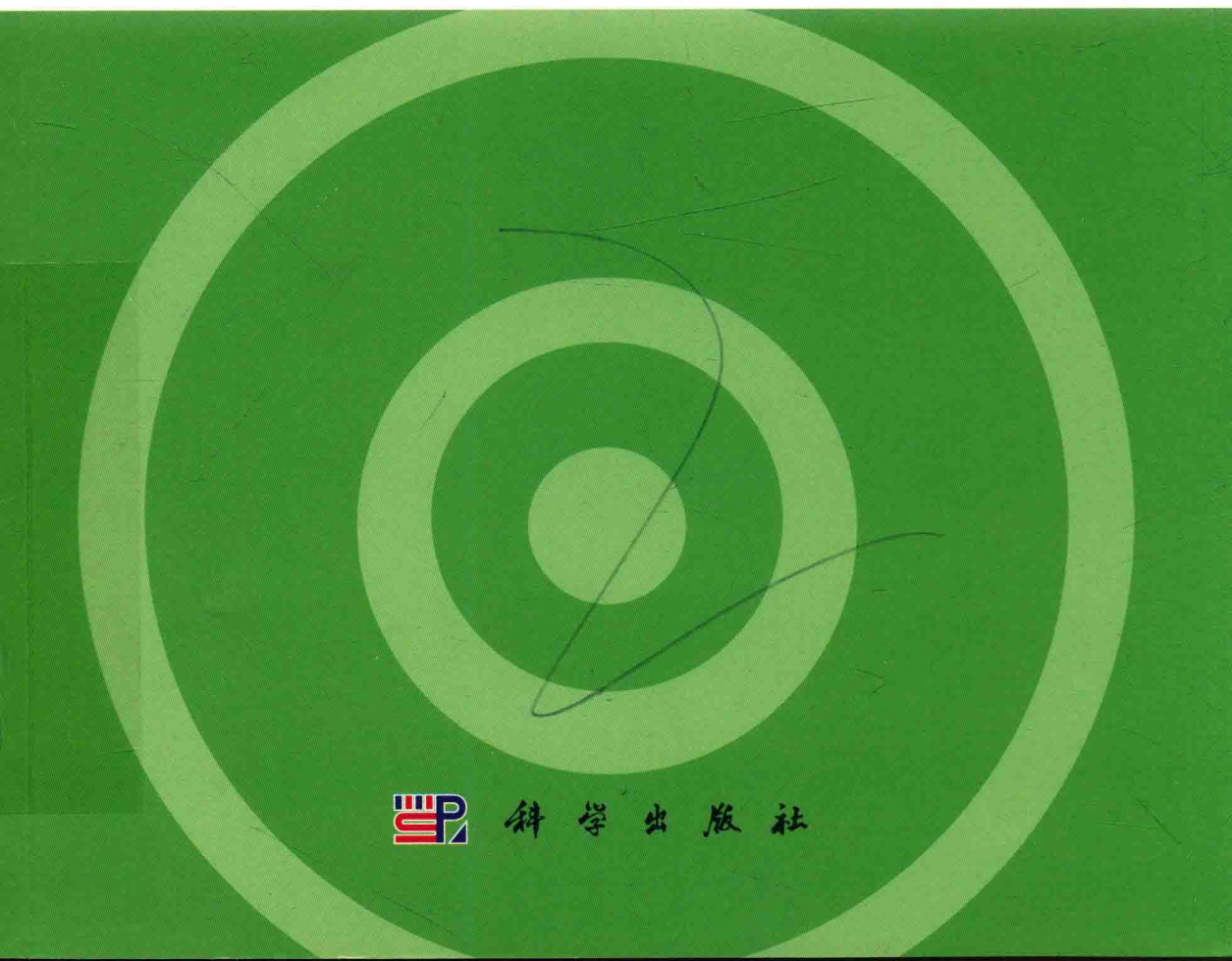
信息科学技术学术著作丛书

云存储安全服务

许 力 黄欣沂 王 峰 著



科学出版社

国家科学技术学术著作出版基金资助出版

信息科学技术学术著作丛书

云存储安全服务

许　力　黄欣沂　王　峰　著

科学出版社

北京

内 容 简 介

本书围绕近年来新兴的云存储安全的研究热点和难点，以密码学的应用为主线，重点介绍和分析了公钥密码学在云存储数据隐私和身份隐私、数据完整性审计、身份认证等方面的具体应用。全书分为云存储安全和密码学、隐私保护、数据完整性审计、访问控制服务四个部分。其中，第一部分是对云存储安全和密码学相关知识的综述；第二部分在私有云、公有云及混合云模型下，从用户的数据隐私和身份隐私两个方面分析了密码学在云存储隐私保护方面的应用；第三部分针对不同的云存储应用环境，设计了多种数据完整性审计方案；第四部分描述和分析了如何利用数字签名技术进行有效的身份认证，以保障访问控制服务安全。

本书可供计算机网络与信息安全、密码学、通信与信息系统、计算机科学、信息科学等专业研究人员、高校教师、研究生及高年级本科生参考，也可作为相关领域工程技术人员的参考书。

图书在版编目（CIP）数据

云存储安全服务/许力，黄欣沂，王峰著. —北京：科学出版社，2019.8
(信息科学技术学术著作丛书)
ISBN 978-7-03-060226-8

Ⅰ. ①云… Ⅱ. ①许… ②黄… ③王… Ⅲ. ①计算机网络-信息存贮-信息安全-研究 Ⅳ. ①TP393.071

中国版本图书馆 CIP 数据核字（2018）第 292280 号

责任编辑：裴 育 张海娜 纪四稳 / 责任校对：彭珍珍
责任印制：吴兆东 / 封面设计：蓝正设计

科学出版社 出版
北京东黄城根北街 16 号
邮政编码：100717
http://www.sciencep.com
北京中石油彩色印刷有限责任公司 印刷

科学出版社发行 各地新华书店经销

*

2019 年 8 月第 一 版 开本：720×1000 B5
2019 年 8 月第一次印刷 印张：13 1/4
字数：265 000

定价：95.00 元

（如有印装质量问题，我社负责调换）

《信息科学技术学术著作丛书》序

21 世纪是信息科学技术发生深刻变革的时代，一场以网络科学、高性能计算和仿真、智能科学、计算思维为特征的信息科学革命正在兴起。信息科学技术正在逐步融入各个应用领域并与生物、纳米、认知等交织在一起，悄然改变着我们的生活方式。信息科学技术已经成为人类社会进步过程中发展最快、交叉渗透性最强、应用面最广的关键技术。

如何进一步推动我国信息科学技术的研究与发展；如何将信息技术发展的新理论、新方法与研究成果转化为社会发展的推动力；如何抓住信息技术深刻发展变革的机遇，提升我国自主创新和可持续发展的能力？这些问题的解答都离不开我国科技工作者和工程技术人员的求索和艰辛付出。为这些科技工作者和工程技术人员提供一个良好的出版环境和平台，将这些科技成就迅速转化为智力成果，将对我国信息科学技术的发展起到重要的推动作用。

《信息科学技术学术著作丛书》是科学出版社在广泛征求专家意见的基础上，经过长期考察、反复论证之后组织出版的。这套丛书旨在传播网络科学和未来网络技术，微电子、光电子和量子信息技术、超级计算机、软件和信息存储技术、数据知识化和基于知识处理的未来信息服务业、低成本信息化和用信息技术提升传统产业，智能与认知科学、生物信息学、社会信息学等前沿交叉科学，信息科学基础理论，信息安全等几个未来信息科学技术重点发展领域的优秀科研成果。丛书力争起点高、内容新、导向性强，具有一定的原创性，体现出科学出版社“高层次、高水平、高质量”的特色和“严肃、严密、严格”的优良作风。

希望这套丛书的出版，能为我国信息科学技术的发展、创新和突破带来一些启迪和帮助。同时，欢迎广大读者提出好的建议，以促进和完善丛书的出版工作。

中国工程院院士
原中国科学院计算技术研究所所长
李国杰

前　言

云计算作为一种新兴的服务模型，自 2006 年提出便受到了工业界、学术界的广泛关注。各大信息技术公司，如国外的谷歌、微软、IBM、亚马逊以及国内的百度、阿里巴巴、腾讯等都纷纷推出各自的云服务平台。然而，随着云计算技术的不断发展，云计算所带来的安全问题也日益突出。用户将数据存储在云服务器上，便失去了对数据的绝对控制权。云环境的开放性，导致用户的隐私容易遭到泄露。为了更好地保护用户数据的安全和隐私，越来越多的研究理论、方法和工具被提出，密码学方法便是其中一种有效而直接的方法，并逐步得到广大研究人员和工程技术人员的认可。

本书围绕近年来新兴的云存储安全研究的热点和难点，以密码学的应用为主线，基于作者在云计算安全、网络与信息安全和数据隐私保护等方面课题的研究成果，并结合国内外相关领域的研究成果展开详细的阐述和分析，全书分为四个部分，共 15 章。

第一部分是对云存储安全和密码学相关知识的综述。其中，第 1 章比较详细地介绍云计算的发展历程和相关云服务平台，以及目前存在的一些安全挑战，并介绍后续章节的安排；第 2 章介绍密码学的基础知识，针对几种关键机制进行深入的分析。

第二部分在私有云、公有云及混合云模型下，从用户的数据隐私和身份隐私两个方面分析密码学在云存储隐私保护方面的应用。其中，第 3 章介绍支持数据隐私和可用性的分布式云存储协议，结合分布式编码方式，设计出使用门限加密的分布式云存储系统，利用公钥加密和同态性实现隐私保护；第 4 章介绍基于属性加密的私有云分布式云存储协议，利用分布式纠删码技术，将分块编码处理后的密文数据存储在若干个云服务器中，提高模型的鲁棒性；第 5 章介绍基于属性加密的混合云分布式云存储协议，去除绝对可信中心的干预，实现各属性服务器完全独立式工作，提高数据的安全性；第 6 章介绍具有身份隐私保护功能的基于属性加密的分布式云存储协议，通过对加密者的身份信息进行预处理以及对访问结构中的属性信息进行隐藏，有效解决数据内容、身份信息、访问结构三方面的隐私问题。

第三部分针对不同的云存储应用环境，设计多种数据完整性审计方案。其中，第 7 章在第 3 章的基础上，设计实现一种分布式云存储环境下的数据完整性审计

协议；第 8 章针对以智能手机为代表的移动设备，设计一种基于隐私保护的支持公众审计的数据完整性审计方案；第 9 章基于数据完整性审计模型，为云用户存储数据提出一个安全存储协议；第 10 章构造门限结构的支持群体协作的基于属性加密(GO-ABE)方案，并提出利用 GO-ABE 方案构造的适用于医疗云环境的支持远程数据完整性审计的安全存储协议；第 11 章在假定存在恶意用户的前提下，利用改进的动态云存储的存储结构，构造基于身份的不可否认的动态数据完整性审计方案。

第四部分描述和分析如何利用数字签名技术进行有效的身份认证，以保障访问控制服务安全。其中，第 12 章设计一种安全认证签名，保障在软件即服务(SaaS)模型中的安全性和公平性，防止参与者不诚实行为的发生；第 13 章利用模糊控制，设计安全访问策略，提供可变的访问决策来控制云计算资源的利用；第 14 章基于 M2SDH 困难假设，构造一种高效的无向无状态的传递签名方案；第 15 章提出广义指定验证者传递签名，并以此为基础设计两个能够实现云存储中图状大数据的安全认证方案。

作者在密码理论、云计算安全、网络与信息安全和数据隐私保护等领域展开了多年的研究，书中大部分内容是这些研究的成果，其中许多内容来自相应的原创论文；作者及所在的福建省网络安全与密码技术重点实验室和异构网络安全通信福建省高校科研创新团队在相关领域承担过许多科研项目，相关的研究成果也在本书中得以引用。

本书的撰写得到福建师范大学数学与信息学院、福建省网络安全与密码技术重点实验室的领导和同仁的支持和帮助，在此表示感谢。国家自然科学基金面上项目(61771140、61472083)、国家科学技术学术著作出版基金项目、国家自然科学基金海峡联合基金项目(U1405255)、福建省杰出青年科学基金项目(2016J06013)、福建师范大学创新团队建设计划(IRTL1207)、福建省科技计划高校产学研合作项目(2017H6005)、福建省自然科学基金面上项目(2016J01277)为本书相关的研究工作提供了资助。林昌露、陈兰香、周赵斌、林丽美老师以及曾雅丽、姚川、吴胜艳、曹夕、李梦婷、林超、赵陈斌、赖启超、张欣欣、翟亚飞等研究生协助进行书稿的整理工作，在此一并表示感谢。

由于云存储技术发展迅速，许多安全问题尚无定论，加之作者水平有限，书中难免存在不妥之处，敬请同行及读者批评指正。

作　者

2019 年 1 月

目　录

第二部分 隐 私 保 护

第三部分　数据完整性审计

第一部分　云存储安全和密码学

云计算作为一种新兴的服务模型，自2006年提出，便受到了工业界、学术界的广泛关注。各大信息技术公司，如国外的谷歌、微软、IBM、亚马逊以及国内的百度、阿里巴巴、腾讯等都纷纷推出各自的云服务平台。然而，随着云计算技术的不断发展，云计算所带来的安全问题也日益突出。为了更好地保护用户数据的安全和隐私，越来越多的研究理论、方法和工具被提出，密码学方法便是其中一种有效而直接的方法。

本部分主要介绍相关的云计算和密码学知识。其中，第1章比较详细地介绍云计算的发展历程和相关云服务平台，以及目前存在的一些安全挑战，并介绍后续章节的安排；第2章介绍密码学的基础知识，针对几种关键机制进行深入的分析。

第 1 章　云计算概述

云计算是当前信息技术领域的热门话题之一，是学术界、产业界等各界关注的焦点。本章首先从云计算的定义及发展历程对云计算进行概述；其次通过云安全事件来说明云计算存在的安全挑战。

1.1　云　计　算

“云计算”(cloud computing)一词，自 2006 年提出便在产业界和学术界掀起了波澜[1]，而后，云计算便成为当前信息技术(information technology, IT)行业最热的一个技术名词。云计算的出现并非偶然，早在 20 世纪 60 年代，麦卡锡就提出了把计算能力作为一种像水和电一样的公用事业提供给用户的理念，这成为云计算思想的起源。在 20 世纪 80 年代网格计算、90 年代公用计算，以及 21 世纪初虚拟化技术、面向服务的架构(service-oriented architecture, SOA)、软件即服务(software-as-a-service, SaaS)等应用的支撑下，云计算作为一种新兴的资源使用和交付模式逐渐为学术界和产业界所认知。云计算的诸多优势，如便利性、实用性以及可扩展性等，使企业无须再背负基础设备管理及维护的沉重负担，因此云计算被寄望成为继水、气、电力、电话之后的第五大公共服务[2]。Gartner 公司早在 2011 年 1 月发布的《IT 行业十大战略技术报告》中就将云计算技术列为十大战略技术之首[3]。

然而，云计算发展至今，仍然没有一个统一的定义。李开复认为云和钱庄是同一个意思。以前没有钱庄，人们只能把钱放在枕头底下，后来有了钱庄，大家觉得还很安全，就把钱存进去，不过兑现起来比较麻烦。现在钱庄发展为银行，实现了可以到任何一个网点取钱，或者通过自动取款机(automatic teller machine, ATM)取钱，就像我们日常用电不需要家家装备发电机，直接从电力公司购买一样[4]。Vaquero 等[5]列举了二十几种不同阶段的云计算定义，目前被广泛接受的是美国国家标准与技术研究院(National Institute of Standards and Technology, NIST)提出的关于云计算的定义[6]。该定义认为云计算是一种模型，这个模型可以随时随地地、便利地、按需地从可配置计算资源共享池中获取所需的资源(包括网络、服务器、存储、应用和服务)，这些资源能够以最小的管理工作量或与服务器最少