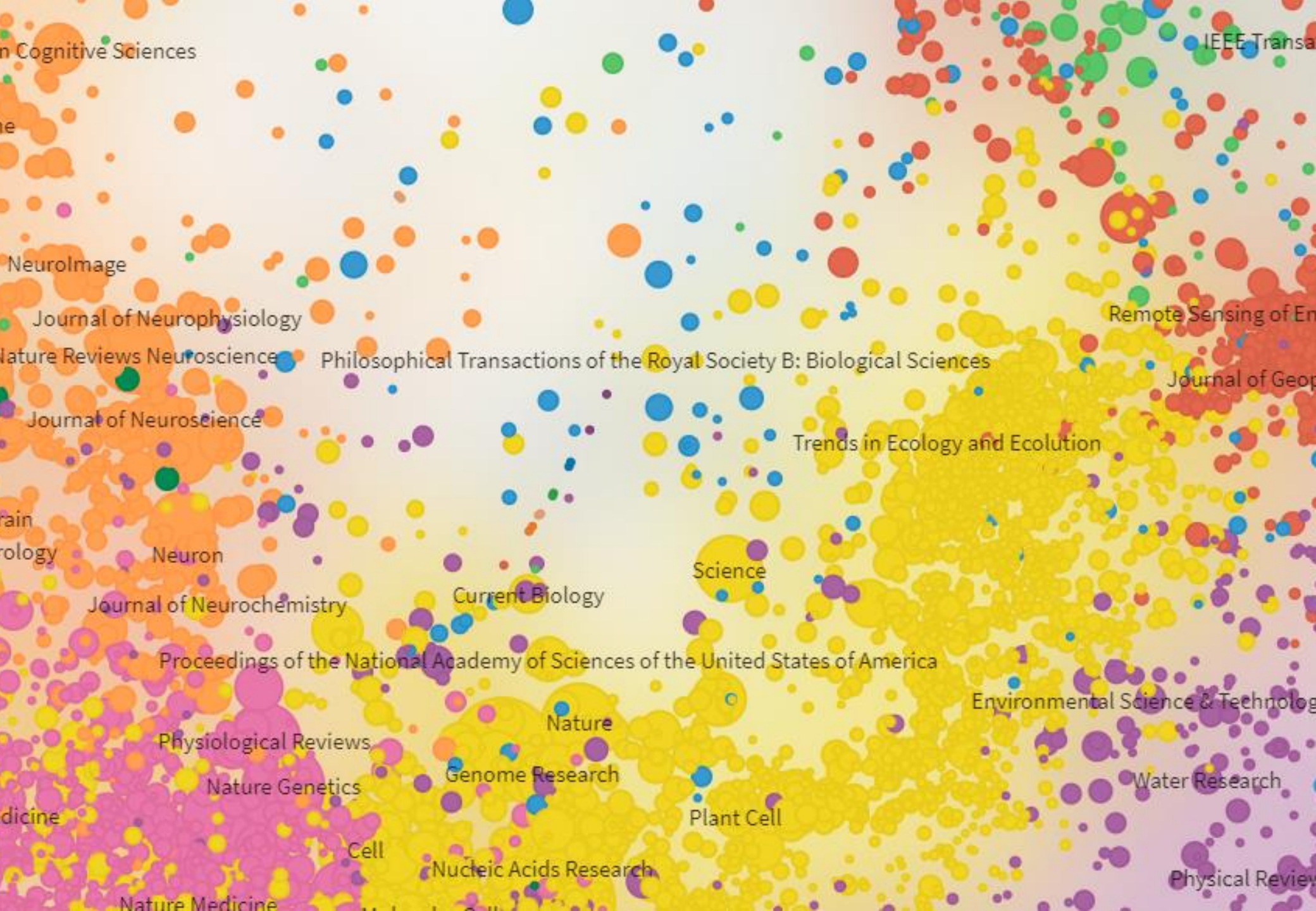




赋能科研175年

Empowering Science for 175 years

SPRINGER NATURE






生物技术和应用微生物学领域排名第一的研究型期刊，收录范围涵盖生物学、生物医学、农业及环境科学领域相关的商业、政治、伦理、法律和社会等方面的研究。

- 超分辨率成像
- 介绍ANNA-PALM，一种使用人工神经网络快速定位宽视野图像重建超分辨率视图的计算策略.

<https://www.nature.com/nbt/>

An aerial photograph of the Five-hundred-meter Aperture Spherical radio Telescope (FAST) nestled in a lush, green mountainous region. The large, circular dish of the telescope is the central focus, surrounded by dense vegetation and steep hills. In the background, more mountains are visible under a blue sky with scattered white clouds. A semi-transparent black banner is overlaid across the middle of the image, containing white text.

FAST正式投用后，获得的数据量将大幅增长，由每天20TB至80TB增长到500TB左右。数据量激增意味着工作量也成倍增长。

关于 Springer Nature

1.0



A WEEKLY ILLUSTRATED JOURNAL OF SCIENCE

"To the solid ground
Of Nature trusts the mind that builds for aye." - WORDSWORTH

见证近 150 年来 人类历史上的重大科学突破

1880：指纹用于刑侦技术

1896：首次发现 X 射线

1903：发现镭的放射性衰变

1925：发现非洲类人猿——人类的起源

1927：发现电子的波动性——电子显微镜的基石

1932：破解原子由质子、中子和电子组成——原子能时代的开端

1953：发现DNA的双螺旋结构——开启生物学的黄金时代

1958：首次确定蛋白质结构——蛋白质组学

1961：破解DNA到蛋白质的编码过程

1963：利用地磁证据证明大陆板块漂移学说

1978：合成第一个单克隆抗体——癌症的靶向治疗

1983：发现艾滋病病毒

1985：在南极上空发现臭氧空洞——引发全球对环境问题的关注

1991：纳米碳管的合成——开启新材料时代

1992：发现30万年前的尼安德特人头骨残骸

1994：首次合成强力抗癌新药——紫杉醇

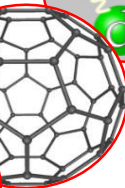
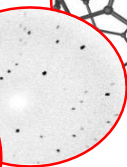
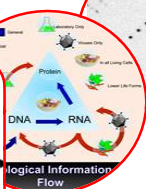
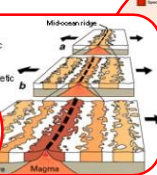
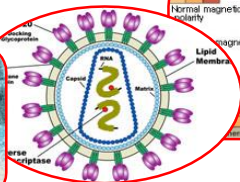
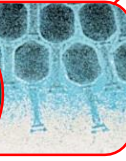
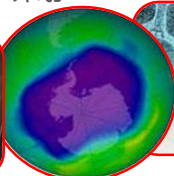
1995：首次发现太阳系外的行星

1997：克隆羊多莉诞生

2001：人类基因组计划

2006：破解安提基特拉机械装置

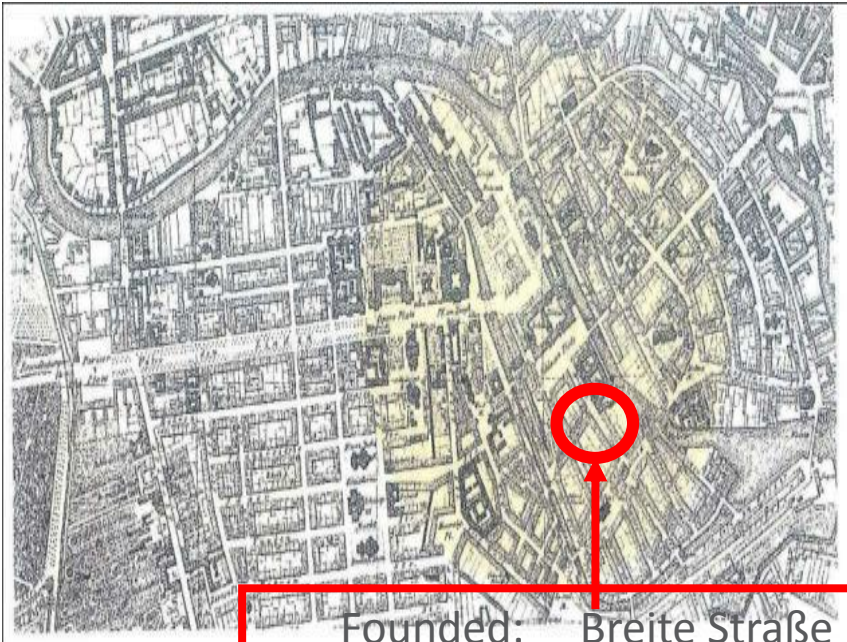
2012：ENCODE计划



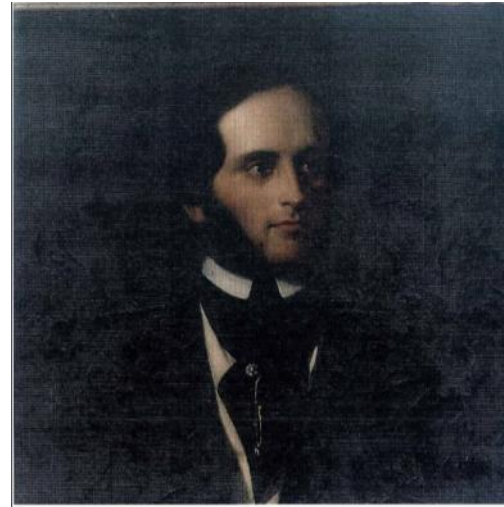
SPRINGER NATURE

出版社简介

Springer 于1842年始建于柏林，拥有175年的历史.....



Founded: Breite Straße
Today: Heidelberger Platz



SPRINGER NATURE



施普林格（Springer）创立于1842年，是全球领先的科学、技术和医学出版机构，公司以创新的信息产品和服务让学术界、科研机构和企业研发部门的科研人员享有高品质的内容。施普林格拥有世界上最重要的科学、技术和医学类电子书数据库和回溯图书档案文库之一，以及种类全面的开放获取期刊。

nature

《自然》杂志（*Nature*）创刊于1869年，是全球被引用最多的科学期刊，年引用量超过50万次。作为全球首屈一指的多学科科学期刊，其影响因子高达41.456。《自然》的读者包括了数百万科学家和学生，遍及世界各地4000余家机构，每月有350万名独立用户在其网站上浏览超过800万页的内容。



麦克米伦教育（Macmillan Education）是全球第三大英语教材和课程资料出版机构，也是本地K12基础教育出版商，此外还通过帕尔格雷夫（Palgrave）出版和销售久负盛名的高等教育图书。他们共同服务于50个市场的客户，并为遍及全球120个国家的客户提供高质量的内容和创新的数字产品与服务。



BioMed Central是全球最大的开放获取出版机构，出版超过286种经同行评审的开放获取刊物，涉及生物学、生物医学和医学等领域。其注册用户超过180万，因而能够有针对性地为各种专长、职称和学科的人士带来机会。

Apress®

Apress是一家致力于满足IT专业人士、软件开发者及程序员需求的技术出版机构。Apress以纸本和电子版形式出版1500余种图书，是全球IT专业人士、软件开发者和商业领袖的权威信息来源。

SCIENTIFIC
AMERICAN

《科学美国人》（*Scientific American*）创刊于1845年，是美国持续出版历史最悠久的杂志，也是大众读者获取科技信息及政策的重要权威来源。其纸本在全球有350万读者，网站ScientificAmerican.com月平均浏览量达550万人次。

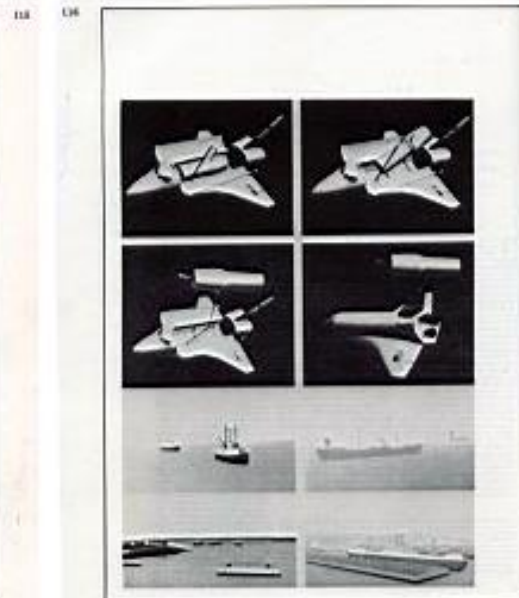
palgrave
macmillan

帕尔格雷夫·麦克米伦（Palgrave Macmillan）是一家面向人文及社会科学（HSS）的全球性学术与商业出版机构。作为首家不设边界的HSS出版机构，其出版篇幅不限，覆盖各种业务模式，让读者和作者从其一家出版机构就能获得最佳的专业学习和学术资料。

A Decade of Research @ Xerox PARC
reprint of
Sept 1977 Scientific American Article on Xerox Alto
"Microelectronics and the Personal Computer"
pp. 230-244, by Alan Kay



alto-1.jpg



alto-2.jpg



alto-3.jpg

CRISPR-baby scientist fails to satisfy critics

He Jiankui gives talk about controversial genome-edited baby claim, but ethical questions remain.



News Feature | 28 November 2018

Does science have a bullying problem?

A spate of bullying allegations have rocked several high-profile science institutions. Here's how researchers... [show more](#)

Holly Else



World View | 27 November 2018

First law of leadership: be human first, scientist second

Want to get the best research from your team? Take these six steps to invest in stronger relationships, urges Alison Antes.

Alison Antes



Current Issue | 29 November 2018



News & Views | 28 November 2018

A glimpse into the heart



Nature Briefing | 28 November 2018

Daily briefing: The



SPRINGER NATURE

10000+

New Books every year

2016年出版约2700种英文期刊和超过10000本新书，5大出版领域包括：科学、技术、医学、商业和交通

eBook Collection with more than 200,000 titles available

电子图书文库拥有超过20万种图书

Largest open access portfolio worldwide, with over 500 open access journals

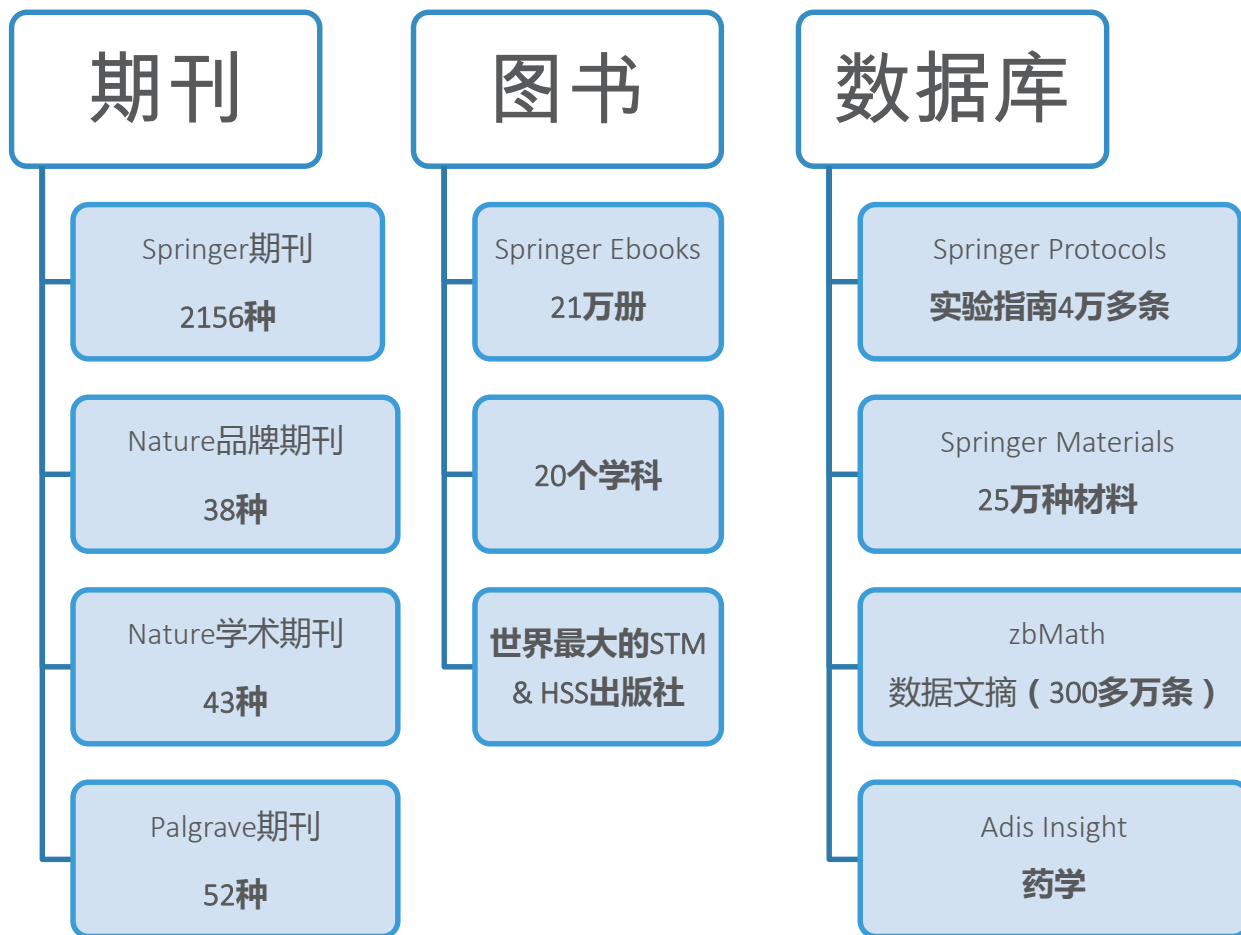
全球最大的开放获取期刊库，拥有超过500种开放获取期刊

SPRINGER NATURE

Springer Nature产品简介

2.0

Springer Nature产品



Springer电子期刊

- Springer SLCC期刊数据库收录期刊1700多种
- 60%以上被SCI和SSCI收录
- 随时出版，随时更新
- IP控制，无并发用户限制
- 与Springer所有电子资源整合，充分实现链接功能
- 涵盖11个学科，部分期刊在相关学科有较高排名

Springer电子期刊—学科分类

学科组合	子学科	
Science, Technology and Engineering (STE) 科技工程专辑	Chemistry and Materials Science	化学和材料科学
	Computer Science	计算机科学
	Earth and Environmental Science	地球环境科学
	Engineering	工程学
	Mathematics and Statistics	数学和统计学
	Physics and Astronomy	物理学和天文学
Medicine and Life Science 生物医学专辑	Biomedical and Life Sciences	生物医学和生命科学
	Medicine	医学
Social Science and Humanities 人文社科专辑	Behavioral Science	行为科学
	Business and Economics	商学和经济学
	Humanities, Social Sciences and Law	人文社科和法律

SpringerLink平台使用简介

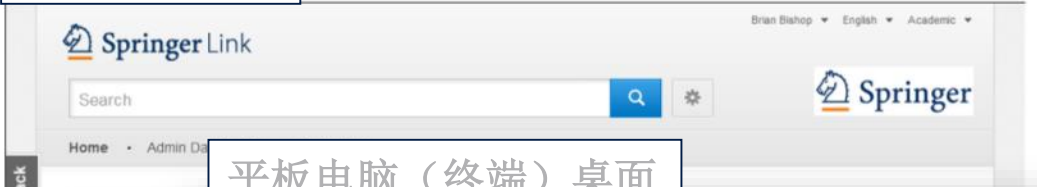
3.0

SpringerLink平台访问

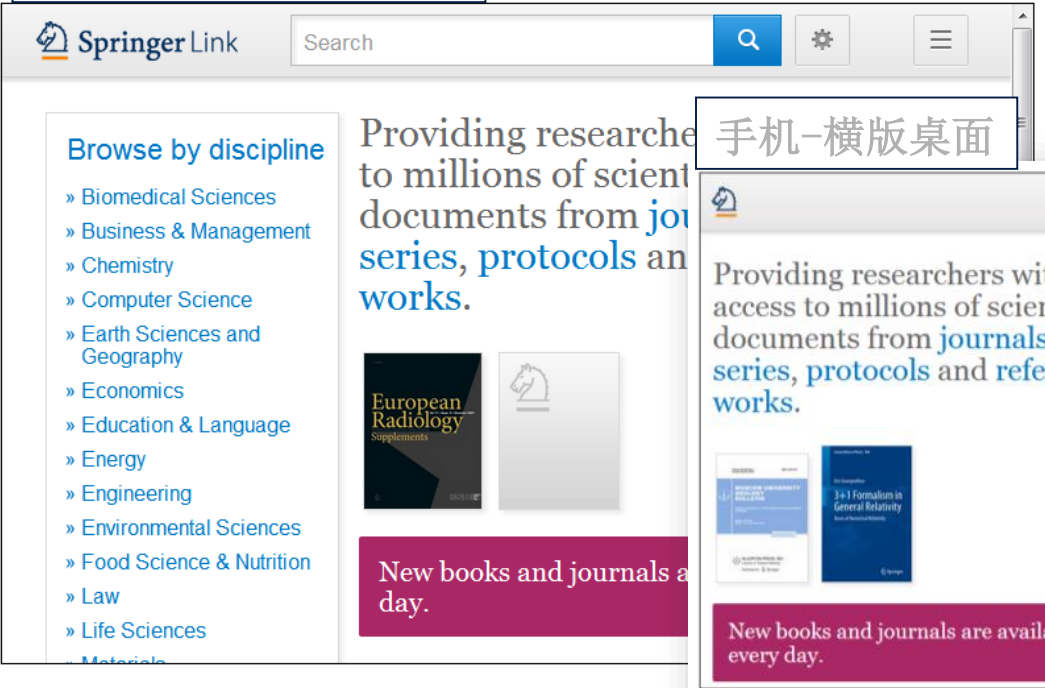
新平台适应各种移动终端、智能手机

平台访问网址: **link.springer.com** (IP控制)

普通电脑桌面



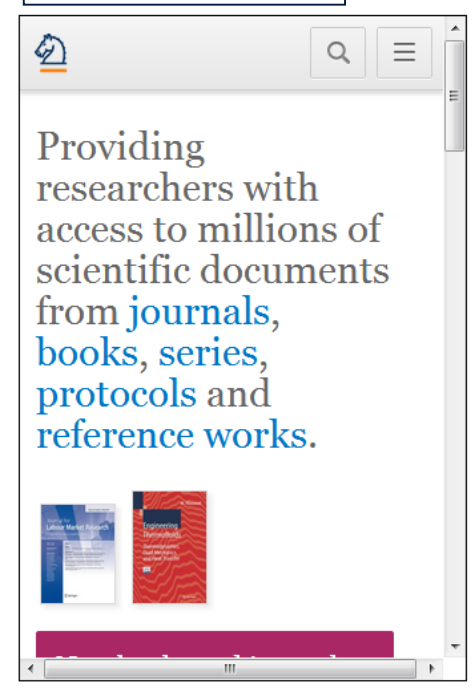
平板电脑（终端）桌面



手机-横版桌面



手机-竖版桌面



SpringerLink平台界面

The screenshot shows the SpringerLink homepage. A red box highlights the search bar at the top left, with a red arrow pointing to it from the label "检索" (Search). Another red box highlights the "Sign up / Log in" link at the top right, with a red arrow pointing to it from the label "注册, 免费推送" (Register, free delivery). A third red box highlights the "Browse by discipline" list on the left, with a red arrow pointing to it from the label "学科浏览" (Subject browsing). The main content area features a large banner with the text "Providing researchers with access to millions of scientific documents from journals, books, series, protocols and reference works." Below this are sections for "Featured Journals" and "Featured Books", each displaying several book covers. A purple box on the right side of the banner states "New books and journals are available every day."

检索

注册, 免费推送

学科浏览

Browse by discipline

- » Architecture & Design
- » Astronomy
- » Biomedical Sciences
- » Business & Management
- » Chemistry
- » **Computer Science**
- » Earth Sciences & Geography
- » Economics
- » Education & Language
- » Energy
- » Engineering
- » Environmental Sciences
- » Food Science & Nutrition
- » Law
- » Life Sciences
- » Materials
- » Mathematics
- » Medicine
- » Philosophy
- » Physics
- » Psychology
- » Public Health
- » Social Sciences
- » Statistics

Browse 9,290,088 resources

Articles	5,507,835
Chapters	3,258,726
Reference Work Entries	483,313
Protocols	40,214

Providing researchers with access to millions of scientific documents from journals, books, series, protocols and reference works.

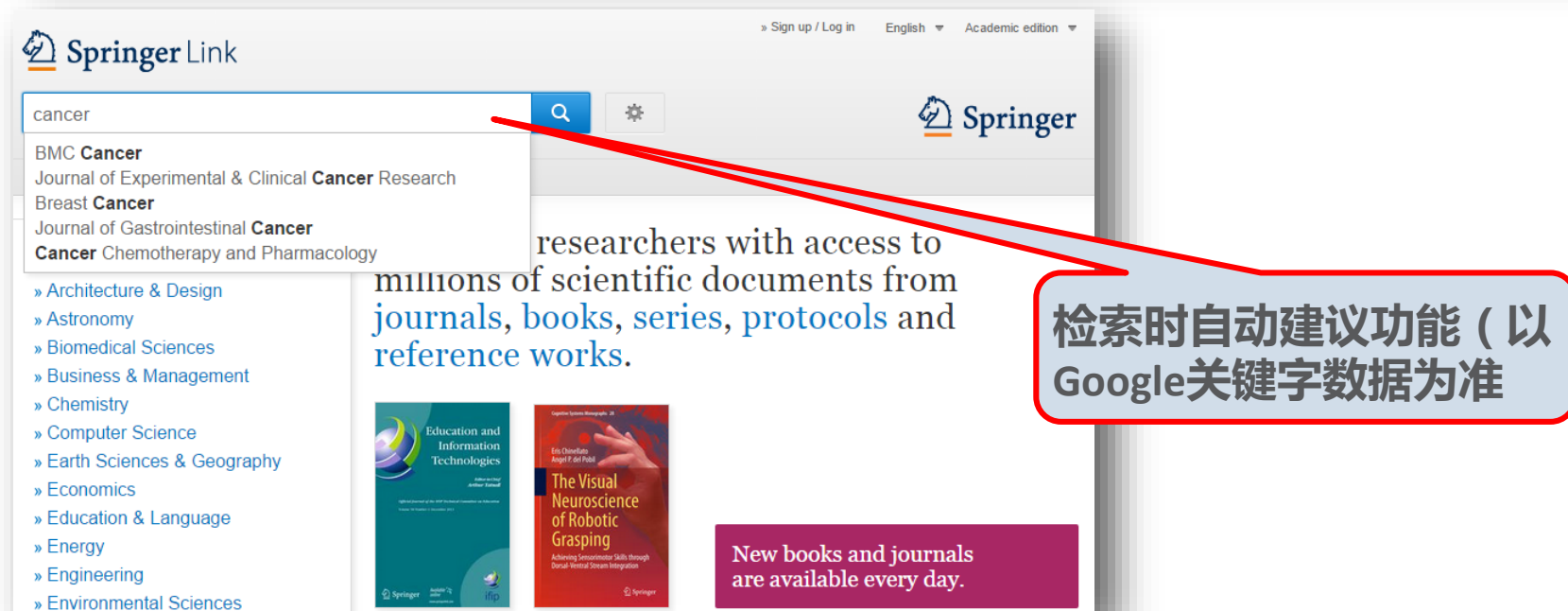
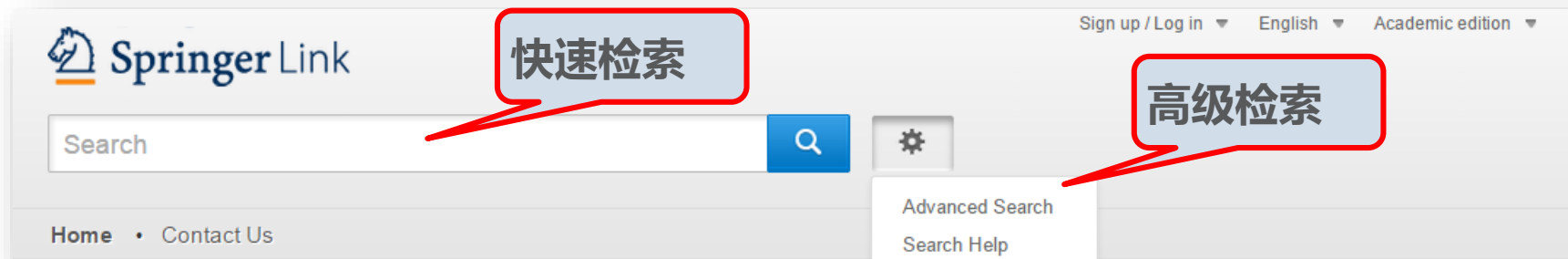
New books and journals are available every day.

Featured Journals

Featured Books

JRE

SpringerLink平台检索：快速检索



SpringerLink平台检索：快速检索续

预览选项

内容类型

学科

分支学科

语言

cryptology

New Search

Springer

Home • Contact Us

Include Preview-Only content

72,137 Result(s) for 'cryptology'

Sort By

Relevance

Newest First

Oldest First

is

between

1955

and

201

Page 1 of 3,607

Refine Your Search

Content Type

Chapter	43,436
Article	25,576
Reference Work Entry	1,675
Book	1,427
Journal	23
Reference Work	2

Discipline

see all

Computer Science	70,945
Mathematics	13,938
Engineering	5,380
Business & Management	3,041
Physics	2,775

Subdiscipline

see all

Security and Cryptology	67,083
Theoretical Computer Science	36,295
Communication Networks	28,788
SWE	24,870
Database Management & Information Retrieval	21,018

Language

English	66,921
German	5,093
Italian	64
French	58

cryptology

This one-of-a-kind reference is unmatched in the breadth and scope of its coverage and serves as the primary reference for students and professionals in computer science and communications. The Dictionary feat...

Computer Science and Communications Dictionary (2001)

» Download PDF (1243 KB)

cryptology

Friedrich L. Bauer in Encyclopedia of Cryptography and Security (2005)

» Download PDF (2864 KB)

Black-Box Models of Comput

Tibor Jager (2012)

An Introduction to Cryptolog

Henk C. A. van Tilborg in The Kluwer Internati

(1988)

cryptology

New Search

Springer

Home • Contact Us

Include Preview-Only content

72,108 Result(s) for 'cryptology'

Sort By

Relevance

Date Published

Page 1 of 3,606

Refine Your Search

Content Type

Chapter	43,409
Article	25,576
Reference Work Entry	1,675
Book	1,425
Journal	23
Reference Work	2

Your search also matched 29 preview-only results, e.g.

Les virus informatiques: théorie, pratique et applications

» Include preview-only content

cryptology

This one-of-a-kind reference is unmatched in the breadth and scope of its coverage and serves as the primary reference for students and professionals in computer science and communications. The Dictionary feat...

Computer Science and Communications Dictionary (2001)

检索结果数量

检索结果导出一次最多导1000条

排序：相关度，时间

选择出版物时间

直接下载

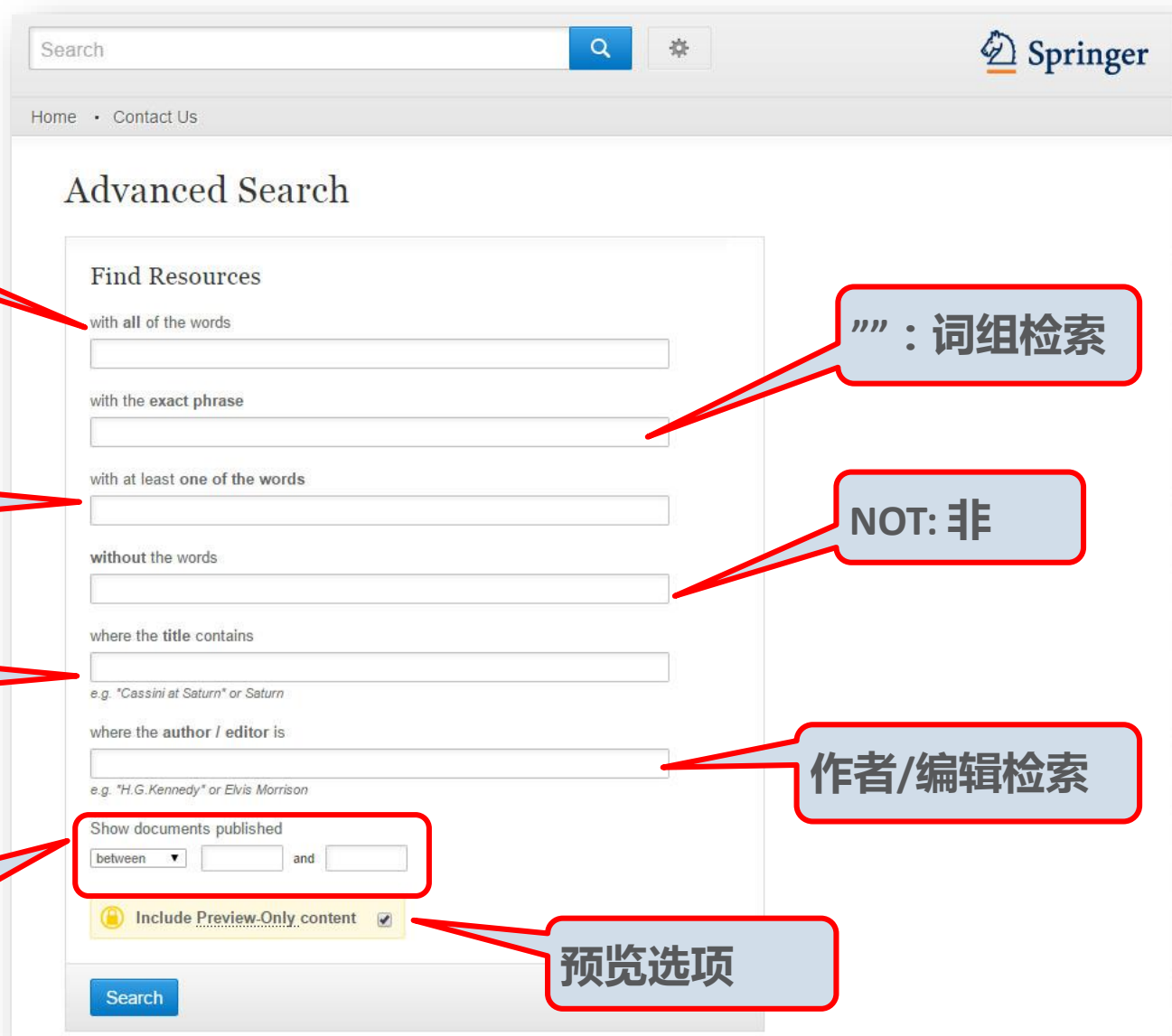
SpringerLink平台检索：高级检索

AND: 与

OR: 或

标题检索

选择出版日期



The image shows the SpringerLink Advanced Search interface. At the top, there is a search bar with a magnifying glass icon and a settings gear icon. Below the search bar, there are links for "Home" and "Contact Us". The main section is titled "Advanced Search" and contains a "Find Resources" form. The form has several input fields with labels: "with all of the words", "with the exact phrase", "with at least one of the words", "without the words", "where the title contains", and "where the author / editor is". Each field has a corresponding example text below it. There are also checkboxes for "Show documents published" (with a dropdown menu for "between" and "and") and "Include Preview Only content". A "Search" button is at the bottom left. Red callout boxes with Chinese text point to specific features: "AND: 与" points to the "with all of the words" field; "OR: 或" points to the "with at least one of the words" field; "标题检索" points to the "where the title contains" field; "选择出版日期" points to the "Show documents published" section; "预览选项" points to the "Include Preview Only content" checkbox; "作者/编辑检索" points to the "where the author / editor is" field; and "词组检索" points to the "with the exact phrase" field.

Search

Home • Contact Us

Advanced Search

Find Resources

with all of the words

with the exact phrase

with at least one of the words

without the words

where the title contains

e.g. "Cassini at Saturn" or Saturn

where the author / editor is

e.g. "H.G. Kennedy" or Elvis Morrison

Show documents published

between and

Include Preview Only content

Search

词组检索

NOT: 非


作者/编辑检索

预览选项

PCD and Strychnine

✕ New Search


[Home](#) • [Contact Us](#)

 Include Preview-Only content ☒

Refine Your Search

Content Type

Article 

Discipline

Biomedicine	9
Medicine & Public Health	3
Life Sciences	1
Psychology	1

Subdiscipline

[see all](#)

Neurology	8
-----------	---

14 Result(s) for 'PCD and Strychnine'


within **Article** 

Sort By

Newest First ▼




Date Published

 Article

Does D-Cycloserine Augmentation of CBT Improve Therapeutic Homework Compliance for Pediatric Obsessive–Compulsive Disorder?

Clinical studies in adults and children with obsessive–compulsive disorder (OCD) have shown that d-cycloserine (DCS) can improve treatment response by enhancing fear extinction learning during exposure-based psyc...

Jennifer M. Park, Brent J. Small, Daniel A. Geller... in *Journal of Child and Family Studies* (2014)

 Article

Browse by discipline

- » Biomedicine
- » Business and Management
- » Chemistry
- » Computer Science
- » Earth Sciences
- » Economics
- » Education
- » Engineering
- » Environment
- » Geography
- » History
- » Law
- » Life Sciences
- » Literature
- » Materials Science
- » Mathematics
- » Medicine & Public Health
- » Pharmacy
- » Philosophy
- » Physics
- » Political Science and International Relations



Discipline	
Medicine & Public Health ×	
Subdiscipline see all	
Internal Medicine	303,138
Medicine/Public Health, general	283,721
Oncology	270,326
Pharmacology/Toxicology	221,584
Cardiology	163,418



Discipline

Medicine & Public Health

Subdiscipline

see all

Internal Medicine	303,138
Medicine/Public Health, general	283,721
Oncology	270,326
Pharmacology/Toxicology	221,584
Cardiology	163,418



Refine by Subdiscipline

Close

Page 1 of 34

Internal Medicine	303,138
Medicine/Public Health, general	283,721
Oncology	270,326
Pharmacology/Toxicology	221,584
Cardiology	163,418
Surgery	162,075
Drug Safety and Pharmacovigilance	160,779
Pediatrics	152,596
Imaging / Radiology	148,354
Neurology	146,325
Gastroenterology	134,311
General Practice / Family Medicine	131,058
Orthopedics	121,757
Public Health	121,484
Psychiatry	118,004
Gynecology	111,490
Intensive / Critical Care Medicine	107,808
Pathology	100,775
Neurosurgery	100,437
Abdominal Surgery	87,296



Include Preview-Only
content ☒

121,556 Result(s)

within English ☒ Computer Science ☒ Algorithm Analysis and Problem Complexity ☒
Conference Paper ☒



Refine Your Search

Content Type

Conference Paper ☒

Chapter 121,556

Discipline

Computer Science ☒

Subdiscipline

see all

Algorithm Analysis and Problem
Complexity ☒

Artificial Intelligence (incl.
Robotics) 54,276

Computer Communication
Networks 47,988

Information Systems
Applications (incl. Internet) 38,019

Computation by Abstract
Devices 36,334

Language

English ☒

Sort By

Newest First ▼

► Date Published



Page

1

of 6,078



Chapter and Conference Paper

Early Performance Evaluation of the Hybrid Cluster with Torus Interconnect Aimed at Molecular-Dynamics Simulations

In this paper, we describe the Desmos cluster that consists of 32 hybrid nodes connected by a low-latency high-bandwidth torus interconnect. This cluster is aimed at cost-effective classical molecular dynamics...

Vladimir Stegailov, Alexander Agarkov... in *Parallel Processing and Applied Mathematics* (2018)



Chapter and Conference Paper

Automatic Creation of a Large and Polished Training Set for Sentiment Analysis on Twitter

Within the field of sentiment analysis and emotion detection applied to tweets, one of the main problems related to the construction of an automatic classifier is the lack of suitable training sets. Considerin...

Stefano Cagnoni, Paolo Fornacciari... in *Machine Learning, Optimization, and Big Da...* (2018)



Chapter and Conference Paper

Using Differential Evolution with a Simple Hybrid Feature for Personalized Recommendation




[International Workshop on Machine Learning, Optimization, and Big Data](#)

..... MOD 2017: [Machine Learning, Optimization, and Big Data](#) pp 146-157 | [Cite as](#)

Automatic Creation of a Large and Polished Training Set for Sentiment Analysis on Twitter

Authors

[Authors and affiliations](#)

Stefano Cagnoni, Paolo Fornacciari, Juxhino Kavaja, Monica Mordonini, Agostino Poggi, Alex Solimeo,
Michele Tomaiuolo 

Conference paper

First Online: 21 December 2017

5

Readers

740

Downloads

Part of the [Lecture Notes in Computer Science](#) book series (LNCS, volume 10710)

SpringerLink平台检索：高级检索续

示例：美国或英国量子密码理论和
技术（非BB84）

**theory AND technology AND
"quantum cryptography" AND (USA
OR England) AND NOT (BB84)**

多个检索框之间的关系为"AND"

优先级：NOT>OR>AND

布尔逻辑运算符不分大小写

如非指定，快速检索框中词与词之间的默认关系为"AND"

Advanced Search

Find Resources

with all of the words

theory technology

SpringerLink

theory AND technology AND "quantum crypt...

Home • Contact Us

648 Result(s) for 'theory AND technology AND "quantum cryptography" AND (USA OR England) AND NOT (BB84)'

Sort By: Relevance | Date Published | Page 1 of 33

Content Type

Chapter	526
Article	115
Reference Work Entry	7

Discipline

Computer Science	484
Physics	200
Mathematics	161
Engineering	86
Materials	40

Subdiscipline

Theoretical Computer Science	350
Security and Cryptology	331
SWE	246
Communication Networks	200
Quantum Physics	107

Language

English	646
German	2

Chapter

An Update on Quantum Cryptography

Although written about fifteen years ago, Wiesner's seminal paper, to which the origin of quantum cryptography must be traced back, did not appear in print until the spring of 1983 [W83]. The first published account... Charles H. Bennett, Gilles Brassard in *Advances in Cryptology* (1985)

» Download PDF (341 KB)

Chapter

Post-quantum Cryptography: Code-Based Signatures

This survey provides a comparative overview of code-based signature schemes with respect to security and performance. Furthermore, we explicitly describe several code-based signature schemes with additional p... Pierre-Louis Cayrel, Mohammed Mezziani in *Advances in Computer Science and Information Security* (2010)

» Download PDF (317 KB)

Chapter

13 Quantum Cryptography

In this final short chapter, we will present the fundamental idea of quantum cryptography. This is not the same thing as quantum computing treated in Chapter 3. There, quantum computers are used to cryptanalyze... Daniel Neuenhauer in *Probabilistic and Statistical Methods in Cryptology* (2004)

» Download PDF (99 KB)

Chapter

On the Power of Two-Party Quantum Cryptography

SpringerLink-期刊的浏览

The screenshot shows the SpringerLink interface for the Journal of Cryptology. The page includes a navigation bar, a journal description, a list of latest articles, a table of journal statistics, and a search section for volumes and issues. Red callout boxes with arrows point to specific features, explaining their functions in Chinese.

Journal of Cryptology
ISSN: 0933-2790 (Print) 1432-1378 (Online)

Description
The Journal of Cryptology is a forum for original results in all areas of modern information security. Both cryptography and cryptanalysis are covered, including information theoretic and complexity theoretic perspectives as well as implementation, application, and standards issues. Coverage includes such topics as public key and conventional algorithms and their implementations, cryptanalytic attacks, pseudo-random sequences ... [show all](#)

[Browse Volumes & Issues](#)

Latest Articles

OriginalPaper
New Second-Preimage Attacks on Hash Functions
Elena Andreeva, Charles Bouillaguet, Orr Dunkelman... (October 2016)
[» Download PDF \(981KB\)](#) [» View Article](#)

OriginalPaper
Cryptanalysis of Full RIPEMD-128
Franck Landelle, Thomas Peyrin (October 2016)
[» Download PDF \(943KB\)](#) [» View Article](#)

OriginalPaper
Bug Attacks
Eli Biham, Yaniv Carmeli, Adi Shamir (October 2016)
[» Download PDF \(593KB\)](#) [» View Article](#)

[» See all articles](#)

Journal Statistics

Impact Factor	Available
1.617	1989 - 2016
Volumes	Issues
29	111
Articles	Open Access
539	4 Articles

Stay up to Date

- [Article abstracts by RSS](#)
- [Register for journal updates](#)

Find a Volume or Issue

Volume Issue

Share

[f](#) [t](#) [in](#)

Annotations:

- 浏览所有卷期, 期刊内检索** (Browse all volumes and issues, search within the journal)
- 期刊简要信息** (Journal brief information)
- 影响因子, 文章数量, 卷期数, 年限等** (Impact factor, number of articles, number of volumes/issues, years, etc.)
- RSS订阅和期刊更新注册提醒** (RSS subscription and journal update registration reminder)
- 查找卷期** (Find volume and issue)
- 最新发表的文章** (Latest published articles)

SpringerLink-期刊的浏览

The screenshot shows the 'About this Journal' page for the 'Journal of Cryptology'. The page is divided into several sections: Journal Title, Coverage, Print ISSN, Online ISSN, Publisher, Topics, Industry Sectors, and Additional Links. Red boxes highlight specific sections, and red arrows point from these boxes to Chinese labels in blue boxes on the right.

About this Journal

Journal Title
Journal of Cryptology

Coverage
Volume 1 / 1989 - Volume 29 / 2016

Print ISSN
0933-2790

Online ISSN
1432-1378

Publisher
Springer US

Topics

- » Coding and Information Theory
- » Computational Mathematics and Numerical Analysis
- » Combinatorics
- » Probability Theory and Stochastic Processes
- » Communications Engineering, Networks

Industry Sectors

- » Aerospace
- » Electronics
- » IT & Software
- » Telecommunications

Additional Links

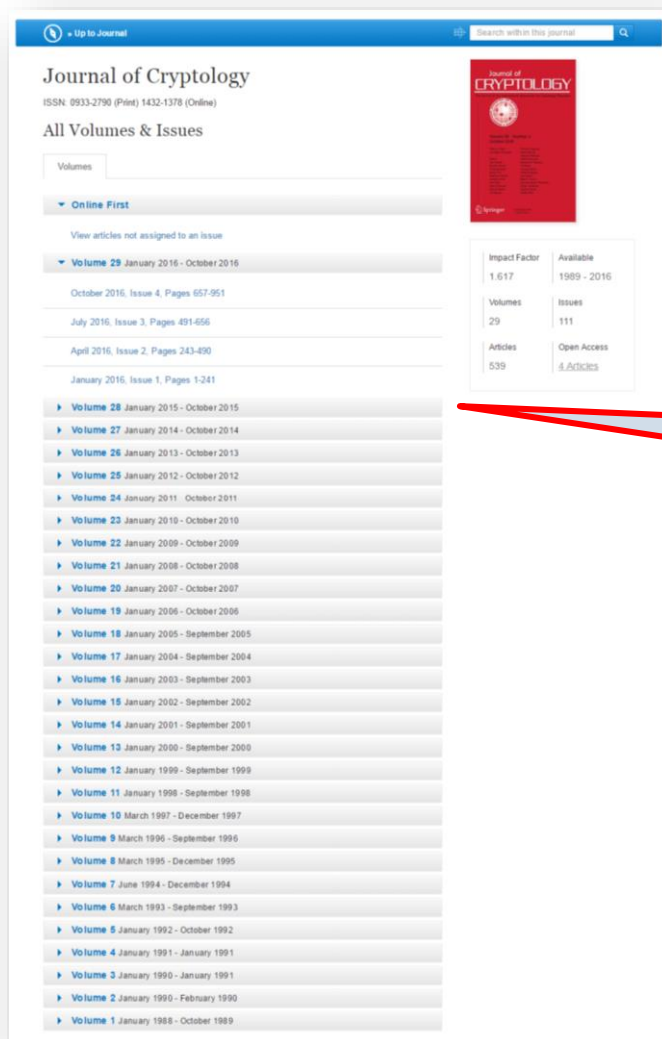
- » Register for Journal Updates
- » Editorial Board
- » About This Journal
- » Manuscript Submission

所属主题分类

所属行业分类

其他链接

SpringerLink-期刊的浏览



可以浏览该期刊所有卷期刊
点击相应链接就可以查年到
到某卷某期的所有内容

SpringerLink-期刊的浏览：查看文章

The screenshot shows the SpringerLink interface for the article "New Second-Preimage Attacks on Hash Functions" from the Journal of Cryptology. The page is annotated with red callouts pointing to specific features:

- 下载PDF** (Download PDF): Points to the "Download PDF" button in the top right sidebar.
- 文章信息：标题，作者，摘要** (Article information: title, author, abstract): Points to the article title, author list, and abstract section.
- 论文快速定位** (Quick navigation): Points to the table of contents on the right sidebar.
- 导出引文** (Export citation): Points to the "Export citation" dropdown menu, which is open, showing options like .RIS, .ENW, and .BIB.

Article Details:

Journal of Cryptology
October 2016, Volume 29, Issue 4, pp 657–696

New Second-Preimage Attacks on Hash Functions

Elena Andreeva, Charles Bouillaguet, Orr Dunkelman, Pierre-Alain Fouque, Jonathan Hoch, John Kelsey, Adi Shamir, Sébastien Zimmer

Article
First Online: 23 June 2015
DOI: 10.1007/s00145-015-9206-4

Cite this article as:
Andreeva, E., Bouillaguet, C., Dunkelman, O. et al. J Cryptol (2016) 29: 657. doi:10.1007/s00145-015-9206-4

Abstract

In this work, we present several new generic second-preimage attacks on hash functions. Our first attack is based on the herding attack and applies to various Merkle–Damgård-based iterative hash functions. Compared to the previously known long-message second-preimage attacks, our attack offers more flexibility in choosing the second-preimage message at the cost of a small computational overhead. More concretely, our attack allows the adversary to replace only a few blocks in the original target message to obtain the second preimage. As a result, our new attack is applicable to constructions previously believed to be immune to such second-preimage attacks. Among others, these include the dithered hash proposal of Rivest, Shoup's UOWHF, and the ROX constructions. In addition, we also suggest several time-memory-data tradeoff attack variants, allowing for a faster online phase, and even finding second preimages for shorter messages. We further extend our attack to sequences stronger than the ones suggested in Rivest's proposal. To this end we introduce the *kite generator* as a new tool to attack any dithering sequence over a small alphabet. Additionally, we analyse the second-preimage security of the basic *tree hash* construction. Here we also propose several second-preimage attacks and their time-memory-data tradeoff variants. Finally, we show how both our new and the previous second-preimage attacks can be applied even more efficiently when multiple short messages, rather than a single long target message, are available.

Keywords

Cryptanalysis Hash function Dithering sequence Second-preimage attack Herding attack Kite Generator

Communicated by Antoine Joux.

A preliminary version of this paper appeared in [2].

Table of Contents:

- Article
- Abstract
- 1 Introduction
- 2 A New Generic Second-Pr...
- 3 Time-Memory-Data Trade...
- 4 Time-Memory-Data Trade...
- 5 Dithered Hashing
- 6 Second-Preimage Attacks ...
- 7 Dealing with High-Comple...
- 8 Matching the Security Bo...
- 9 Second-Preimage Attack ...
- Acknowledgments
- Appendix: A Suffix-Friendly ...
- References
- Copyright information
- About this article

Export citation

- .RIS
- .ENW
- .BIB





Papers
Reference Manager
RefWorks
Zotero

EndNote

BibTeX
JabRef
Mendeley

SpringerLink-期刊的浏览：查看文章

References

1. J.P. Allouche, Sur la complexité des suites infinies. *Bull. Belg. Math. Soc.* **1**, 133–143 (1994).
citeseer.ist.psu.edu/allouche94sur.html 
2. E. Andreeva, C. Bouillaguet, P. Fouque, J.J. Hoch, J. Kelsey, A. Shamir, S. Zúñiga, Preimage attacks on dithered hash functions, in ed. by N.P. Smart. *Advances in Cryptology EUROCRYPT 2008, 27th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Istanbul, Turkey, April 13–17, 2008. Proceedings.* Lecture Notes in Computer Science, vol. 4965 (Springer, 2008), pp. 270–288. doi:[10.1007/978-3-540-78967-3_16](https://doi.org/10.1007/978-3-540-78967-3_16) 
3. E. Andreeva, B. Mennink, Provable chosen-target-forced-midfix preimage resistance, in eds. by A. Miri, S. Vaudenay. *Selected Areas in Cryptography—18th International Workshop, SAC 2011, Toronto, ON, Canada, August 11–12, 2011. Revised Selected Papers.* Lecture Notes in Computer Science, vol. 7118 (Springer, 2011), pp. 37–54. doi:[10.1007/978-3-642-28496-0_3](https://doi.org/10.1007/978-3-642-28496-0_3) 
4. E. Andreeva, G. Neven, B. Preneel, T. Shrimpton, Seven-property-preserving iterated hashing: ROX, in ed. by K. Kurosawa. *ASIACRYPT'07. Lecture Notes in Computer Science*, vol. 4833 (Springer, 2007), pp. 130–146
5. J.P. Aumasson, L. Henzen, W. Meier, R.C.W. Phan, SHA-3 proposal BLAKE. Submission to NIST (2008). <http://131002.net/blake/blake.pdf> 

提供直接链接服务

SpringerLink-图书主页：图书主页介绍

The screenshot shows the SpringerLink page for the book "Advances in Cryptology – CRYPTO 2016". The page includes a top navigation bar with a search box and a "Download Book (PDF, 17286 KB)" button. The main content area displays the book title, conference details, and editors. A "Table of contents" section lists chapters with download links. A "Book Metrics" section shows citations, mentions, readers, and downloads. A "MyCopy" section offers a softcover edition for purchase. The page is annotated with red boxes and callouts: a box around the top download button, a box around the bottom download buttons, a box around the "Table of contents" section, a box around the "Book Metrics" section, and a box around the "Look Inside" button.

Download Book (PDF, 17286 KB)

Search within this book

Book
Lecture Notes in Computer Science
Volume 9814 2016

Advances in Cryptology – CRYPTO 2016

36th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2016, Proceedings, Part I

Editors: Matthew Robshaw, Jonathan Katz
ISBN: 978-3-662-53017-7 (Print) 978-3-662-53018-4 (Online)

Download Book (PDF, 17286 KB) **Download Book (ePub, 13926 KB)**

Table of contents (24)

Front Matter
» [Download PDF \(109KB\)](#) Pages I-XIII

Provable Security for Symmetric Cryptography

Front Matter
» [Download PDF \(21KB\)](#) Pages 1-1

Chapter
Key-Alternating Ciphers and Key-Length Extension: Exact Bounds and Multi-user Security
Viet Tung Hoang, Stefano Tessaro
» [Download PDF \(918KB\)](#) » [View Chapter](#) Pages 3-32

Chapter
Counter-in-Tweak: Authenticated Encryption Modes for Tweakable Block Ciphers
Thomas Peyrin, Yannick Seurin
» [Download PDF \(829KB\)](#) » [View Chapter](#) Pages 33-63

Book Metrics

Citations	2
Mentions	38
Readers	53
Downloads	591

Provided by Bookmetrix

MyCopy Softcover Edition
24.99
EUR/USD/GBP/CHF
[Buy Now](#)

Other actions

» [About this Book](#)

Share

[f](#) [t](#) [in](#)

图书内检索
Look Inside

图书计量信息

下载整本图书

SpringerLink-图书主页续

▼ About this Book

Book Title

Advances in Cryptology – CRYPTO 2016

Book Subtitle

36th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2016, Proceedings, Part I

Copyright

2016

DOI

10.1007/978-3-662-53018-4

Print ISBN

978-3-662-53017-7

Online ISBN

978-3-662-53018-4

Series Title

» [Lecture Notes in Computer Science](#)

Series Volume

9814

Series ISSN

0302-9743

Publisher

Springer Berlin Heidelberg

Copyright Holder

International Association for Cryptologic Research

Additional Links

» [About this Book](#)

Topics

» [Data Encryption](#)
 » [Systems and Data Security](#)
 » [Algorithm Analysis and Problem Complexity](#)
 » [Management of Computing and Information Systems](#)
 » [Discrete Mathematics in Computer Science](#)

Industry Sectors

» [Telecommunications](#)
 » [Automotive](#)
 » [IT & Software](#)

eBook Packages

» [Computer Science](#)

Editors

[Matthew Robshaw](#) ⁽¹³⁾

[Jonathan Katz](#) ⁽¹⁴⁾

Editor Affiliations

13. Impinj, Inc.

14. University of Maryland

图书信息

图书分类信息

作者信息

SpringerLink-图书章节

Download Book (PDF, 17286 KB) Download Chapter (918 KB)

Chapter

Advances in Cryptology – CRYPTO 2016

Volume 9814 of the series Lecture Notes in Computer Science pp 3-32

Date: 21 July 2016

Key-Alternating Ciphers and Key-Length Extension: Exact Bounds and Multi-user Security

Viet Tung Hoang, Stefano Tessaro

Download Book (PDF, 17286 KB)

Download Chapter (918 KB)

Abstract

The best existing bounds on the concrete security of key-alternating ciphers (Chen and Steinberger, EUROCRYPT '14) are only *asymptotically* tight, and the quantitative gap with the best existing attacks remains numerically substantial for concrete parameters. Here, we prove exact bounds on the security of key-alternating ciphers and extend them to XOR cascades, the most efficient construction for key-length extension. Our bounds essentially match, for any possible query regime, the advantage achieved by the best existing attack.

Our treatment also extends to the multi-user regime. We show that the multi-user security of key-alternating ciphers and XOR cascades is very close to the single-user case, i.e., given enough rounds, it does not substantially decrease as the number of users increases. On the way, we also provide the first explicit treatment of multi-user security for key-length extension, which is particularly relevant given the significant security loss of block ciphers (even if ideal) in the multi-user setting.

The common denominator behind our results are new techniques for information-theoretic indistinguishability proofs that both extend and refine existing proof techniques like the H-coefficient method.

Keywords

Symmetric cryptography – Block ciphers – Provable security – Tightness – Multi-user security



Chapter Metrics

Readers	2
Downloads	24

Provided by Bookmetrix

MyCopy Softcover Edition

24.99

EUR/USD/GBP/CHF

Buy Now

View Chapter

Reference tools

Export citation

Add to Papers

Other actions

About this Book

Reprints and Permissions

Share



下载统计

查看HTML格式全文

导出引文
关于本书
版权信息等

SPRINGER NATURE

下载

SpringerLink-图书章节续

► Supplementary Material (0)

► References (26)

▼ About this Chapter

Title

Key-Alternating Ciphers and Key-Length Extension: Exact Bounds and Multi-user Security

Book Title

► Advances in Cryptology – CRYPTO 2016

Book Subtitle

36th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2016, Proceedings, Part I

Pages

pp 3-32

Copyright

2016

DOI

10.1007/978-3-662-53018-4_1

Print ISBN

978-3-662-53017-7

Online ISBN

978-3-662-53018-4

Series Title

► Lecture Notes in Computer Science

Series Volume

9814

Series ISSN

0302-9743

Publisher

Springer Berlin Heidelberg

Topics

► Data Encryption
► Systems and Data Security
► Algorithm Analysis and Problem Complexity
► Management of Computing and Information Systems
► Discrete Mathematics in Computer Science

Keywords

Symmetric cryptography
Block ciphers
Provable security
Tightness
Multi-user security

Industry Sectors

► Telecommunications
► Automotive
► IT & Software

eBook Packages

► Computer Science

Editors

Matthew Robshaw⁽¹³⁾

Jonathan Katz⁽¹⁴⁾

Editor Affiliations

13. Impinj, Inc.

14. University of Maryland

Authors

Viet Tun

Stefano

Author Affiliations

15. Department of Computer Science

University of California, Santa Barbara

16. Department of Computer Science

University of California, Santa Barbara

17. Department of Computer Science

University of California, Santa Barbara

18. Department of Computer Science

University of California, Santa Barbara

19. Department of Computer Science

University of California, Santa Barbara

20. Department of Computer Science

University of California, Santa Barbara

21. Department of Computer Science

University of California, Santa Barbara

22. Department of Computer Science

University of California, Santa Barbara

23. Department of Computer Science

University of California, Santa Barbara

24. Department of Computer Science

University of California, Santa Barbara

25. Department of Computer Science

University of California, Santa Barbara

26. Department of Computer Science

University of California, Santa Barbara

27. Department of Computer Science

University of California, Santa Barbara

28. Department of Computer Science

University of California, Santa Barbara

29. Department of Computer Science

University of California, Santa Barbara

30. Department of Computer Science

University of California, Santa Barbara

作者或编辑信息

分类信息

章节信息

1. Andreeva, E., Bogdanov, A., Dodis, Y., Mennink, B., Steinberger, J.P.: On the indistinguishability of key-alternating ciphers. In: Canetti, R., Garay, J.A. (eds.) CRYPTO 2013, Part I. LNCS, vol. 8042, pp. 531–550. Springer, Heidelberg (2013) » CrossRef
2. Bellare, M., Boldyreva, A., Micali, S.: Public-key encryption in a multi-user setting: security proofs and improvements. In: Preneel, B. (ed.) EUROCRYPT 2000. LNCS, vol. 1807, pp. 259–274. Springer, Heidelberg (2000) » CrossRef
3. Bellare, M., Ristenpart, T., Rogaway, P., Stegers, T.: Format-preserving encryption. In: Jacobson Jr., M.J., Rijmen, V., Safavi-Naini, R. (eds.) SAC 2009. LNCS, vol. 5867, pp. 295–312. Springer, Heidelberg (2009) » CrossRef
4. Bellare, M., Rogaway, P.: The security of triple encryption and a framework for code-based game-playing proofs. In: Vaudenay, S. (ed.) EUROCRYPT 2006. LNCS, vol. 4004, pp. 409–426. Springer, Heidelberg (2006) » CrossRef
5. Bernstein, D.J.: How to stretch random functions: the security of protected counter sums. J. Cryptol. **12**(3), 185–192 (1999) » MathSciNet » CrossRef » MATH
6. Bernstein, D.J.: Break a dozen secret keys, get a million more for free (2015). » <http://blog.cryp.to/20151120-batchattacks.html>
7. Bogdanov, A., Knudsen, L.R., Leander, G., Standaert, F.-X., Steinberger, J., Tischhauser, E.: Key-alternating ciphers in a provable setting: encryption using a small number of public permutations. In: Pointcheval, D., Johansson, T. (eds.) EUROCRYPT 2012. LNCS, vol. 7237, pp. 45–62. Springer, Heidelberg (2012) » CrossRef
8. Chen, S., Lampe, R., Lee, J., Seurin, Y., Steinberger, J.: Minimizing the two-round even-mansour cipher. In: Garay, J.A., Gennaro, R. (eds.) CRYPTO 2014, Part I. LNCS, vol. 8616, pp. 39–56. Springer, Heidelberg (2014) » CrossRef
9. Chen, S., Steinberger, J.: Tight security bounds for key-alternating ciphers. In: Nguyen, P.Q., Oswald, E. (eds.) EUROCRYPT 2014. LNCS, vol. 8441, pp. 327–350. Springer, Heidelberg (2014) » CrossRef
10. Dai, Y., Lee, J., Mennink, B., Steinberger, J.: The security of multiple encryption in the ideal cipher model. In: Garay, J.A., Gennaro, R. (eds.) CRYPTO 2014, Part I. LNCS, vol. 8616, pp. 20–38. Springer, Heidelberg (2014) » CrossRef
11. Dunkelman, O., Keller, N., Shamir, A.: Minimalism in cryptography: the even-mansour scheme revisited. In: Pointcheval, D., Johansson, T. (eds.) EUROCRYPT 2012. LNCS, vol. 7237, pp. 336–354. Springer, Heidelberg (2012) » CrossRef
12. Even, S., Mansour, Y.: A construction of a cipher from a single pseudorandom permutation. In: Imai, H., Rivest, R.L., Matsumoto, T. (eds.) ASIACRYPT 1991. LNCS, vol. 739, pp. 210–224. Springer, Heidelberg (1993)
13. Even, S., Mansour, Y.: A construction of a cipher from a single pseudorandom permutation. J. Cryptol. **10**(3), 151–162 (1997) » MathSciNet » CrossRef » MATH
14. Gaži, P.: Plain versus randomized cascading-based key-length extension for block ciphers. In: Canetti, R., Garay, J.A. (eds.) CRYPTO 2013, Part I. LNCS, vol. 8042, pp. 551–570. Springer, Heidelberg (2013) » CrossRef
15. Gaži, P., Lee, J., Seurin, Y., Steinberger, J., Tessaro, S.: Relaxing full-codebook security: a refined analysis of key-length extension schemes. In: Leander, G. (ed.) FSE 2015. LNCS, vol. 9054, pp. 319–341. Springer, Heidelberg (2015) » CrossRef
16. Gaži, P., Maurer, U.: Cascade encryption revisited. In: Matsui, M. (ed.) ASIACRYPT 2009. LNCS, vol. 5912, pp. 37–51. Springer, Heidelberg (2009) » CrossRef

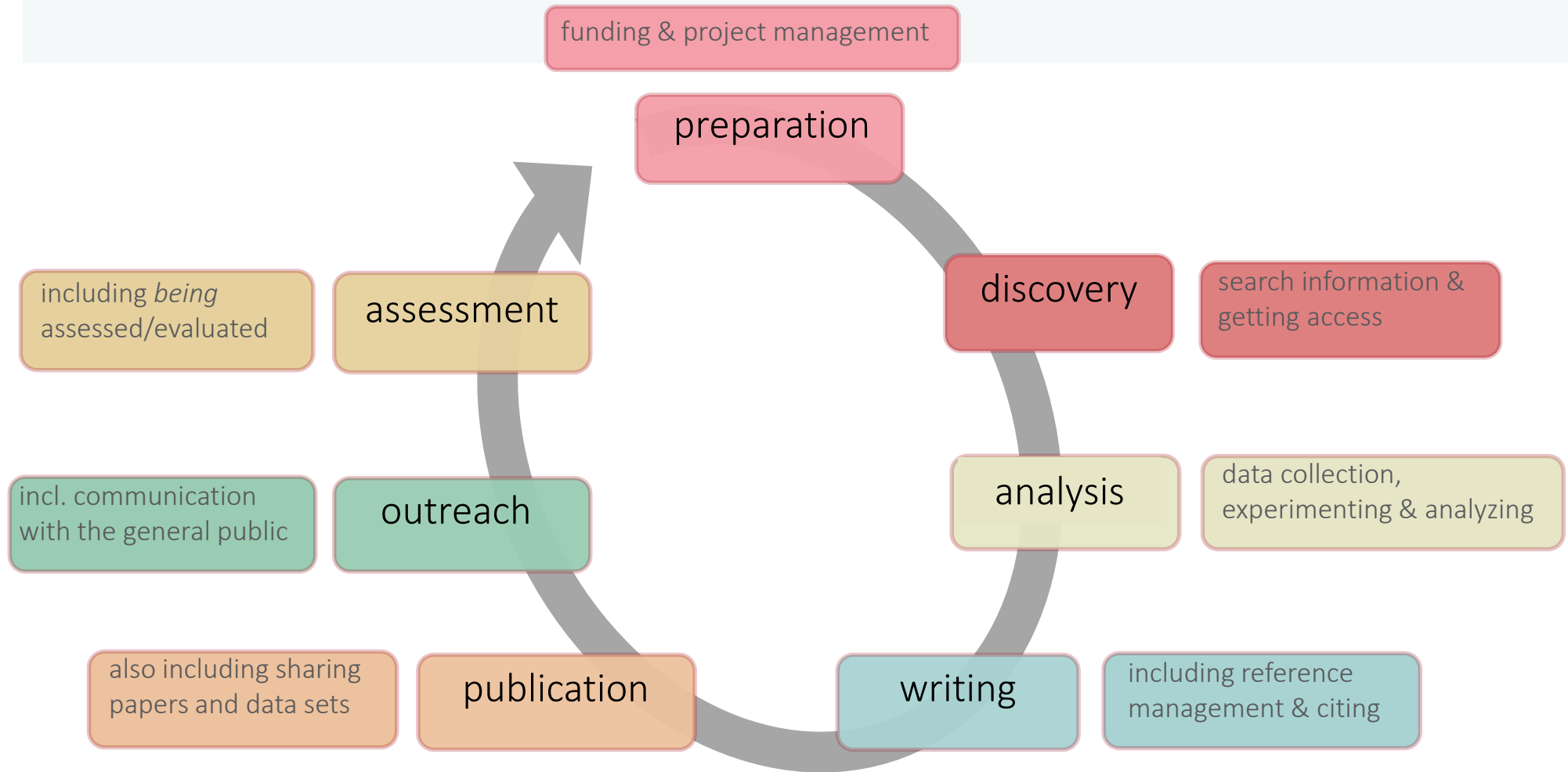
期刊论文投稿简介

4.0

Cycle of Academic Research

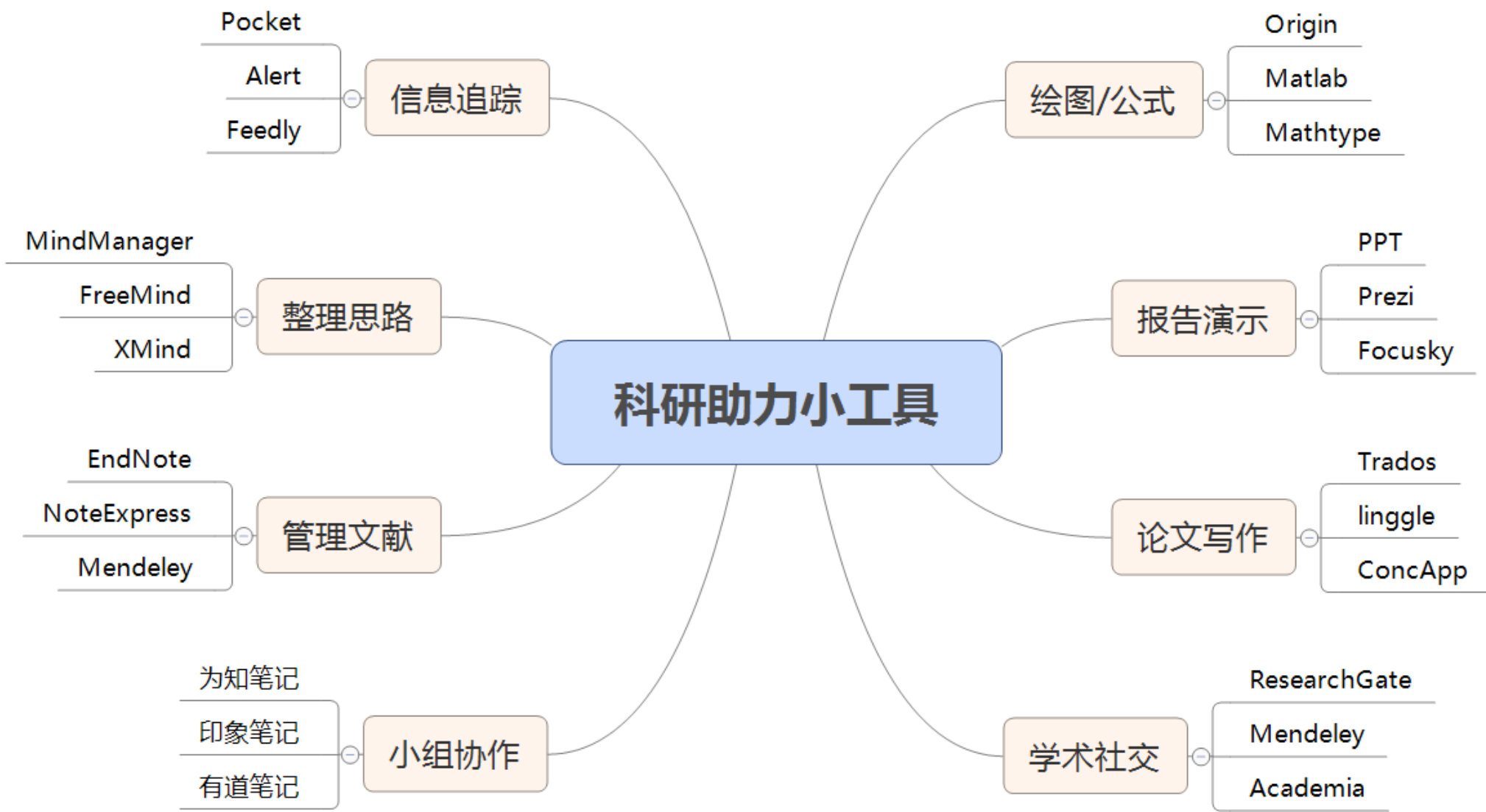


A model of the research workflow



Changing research workflows





[Home](#)[About](#)[Get](#)[LaTeX3](#)[Publications](#)[Help](#)[News](#)



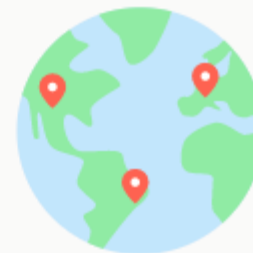
Read and discuss publications

Find the research you need to help your work and join open discussions with the authors and other experts.



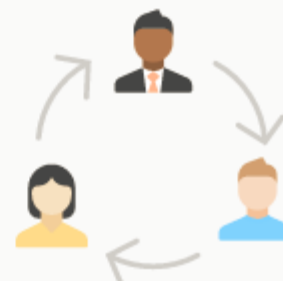
Get stats on your research

See in-depth stats on who's been reading your work and keep track of your citations.



Create exposure for your work

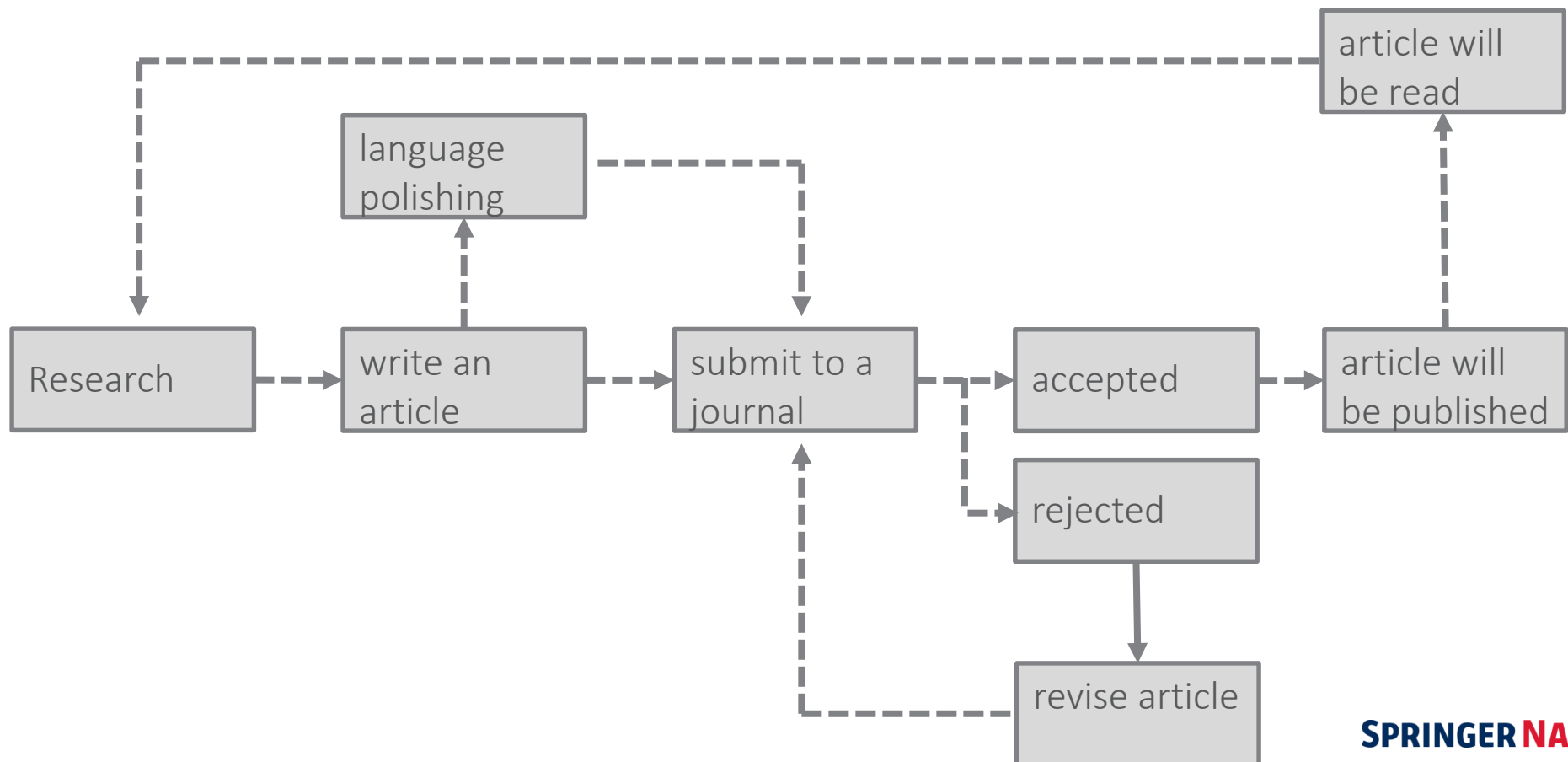
Share your work from any stage of the research cycle to gain visibility and citations.



Connect with your colleagues

Connect and collaborate with researchers from around the world in all scientific disciplines.

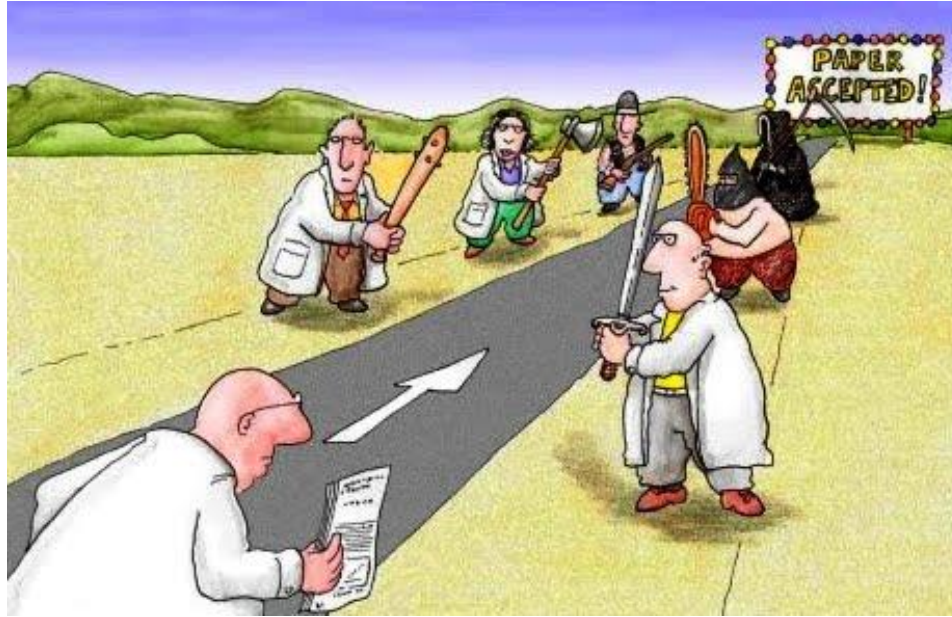
The Life of a Journal Article Submission



A medium shot of Sheldon Cooper from the TV show 'The Big Bang Theory'. He is wearing a purple t-shirt and looking slightly to his left with a serious expression. Behind him is a whiteboard with some hand-drawn diagrams and mathematical symbols. The quote is overlaid on a dark grey semi-transparent box at the bottom of the frame.

"Peers?, I have no peers."

Peer review



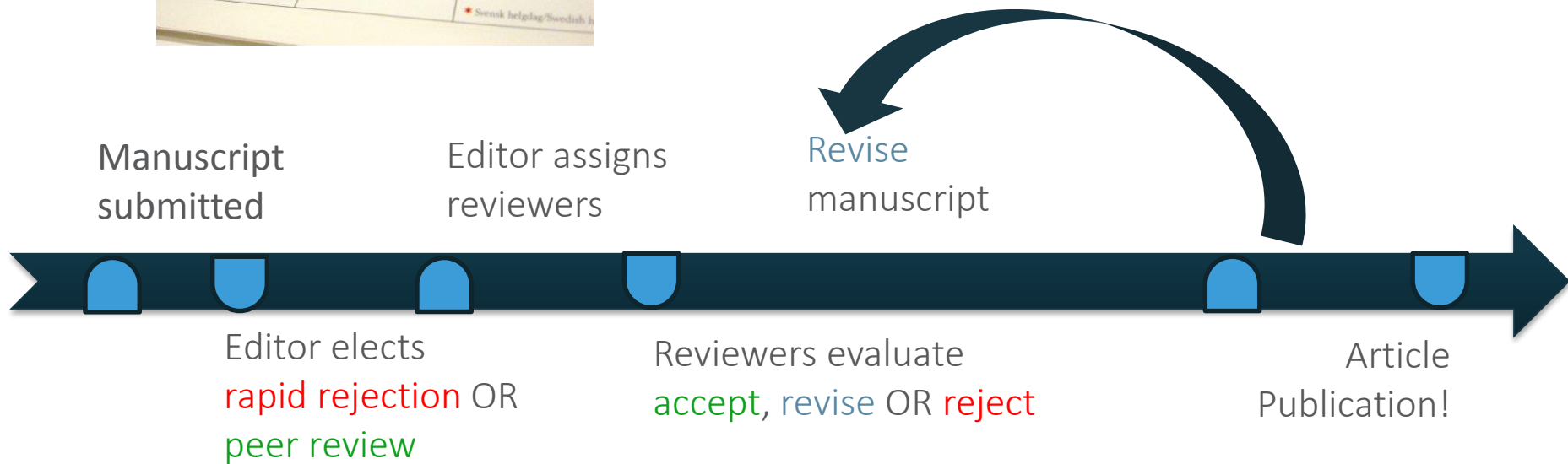
NATURE

Peer review

Journal publishing timelines can vary depending on editor and reviewer



Submission to publication
3 months – 12 months



Peer review

Article Tracking – track the status of your article during production



Article Tracking

If you would like to keep track of your articles as they move through production – this is the right tool for you. Springer's Article Tracking informs you of your article's current status in 8 stages. You can also opt for receiving an email alert once a new stage has been reached.

ARTICLE TRACKING - MY ACCEPTED ARTICLES (1)

Sort Articles by ☒ Publication Stage ☐ Title ascending

1 > 2 > **3** > 4 > 5 > 6 > 7

Investigating the candidate for the invasive meningococcal glycoconjugates with glycoconjugate

Journal: Glycoconjugate Journal

Article proofs sent to author

The proofs of your typeset article have been sent to you by email. Please return your corrections to us as soon as possible.

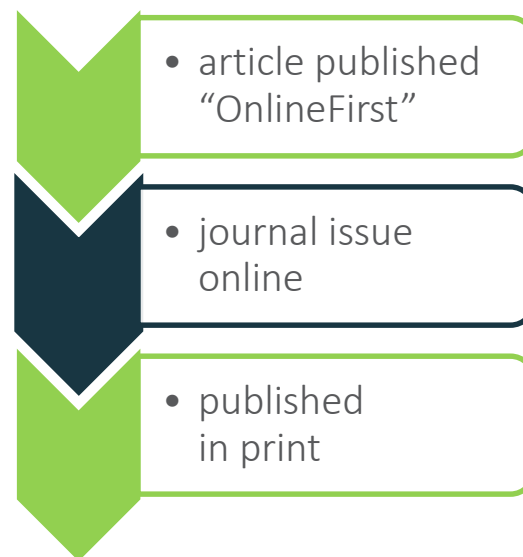
You have ordered 0 offprints [CHANGE YOUR ORDER](#)

☒ Contact your production editor

☐ Send me an email notification for each stage that my article reaches

ARTICLE TRACKING - MY PUBLISHED ARTICLES (0)

[TOP](#)



Congratulations

SPRINGER NATURE

期刊选择：作者和审稿人分别最关注什么？

- 作者最关注的因素：
 - 期刊的声誉
 - 目标读者群
 - 同行评审速度
 - 是否开放获取
- 审稿人需要何种稿件：
 - 与期刊主题相符
 - 科学合理性
 - 有何新发现
 - 该成果的进展是否能引起目标读者的兴趣

Springer

HOME | MY SPRINGER | SUBJECTS | SERVICES | IMPRINTS & PUBLISHERS | ABOUT US

» *Journal Authors*

CONTACT US

Check out what is read and downloaded!

Find trending topics and popular keywords
Live and in real-time - realtime.springer.com

INFORMATION FOR JOURNAL AUTHORS

Manuscript Guidelines
How to prepare and submit articles; templates and artwork guidelines

Resources for Journal Authors
All you need to know: from article preparation to its worldwide distribution

The 'MyPublication' Process
Easily manage all administrative tasks of your article's production

Springer and Open Access
Choose from different publishing options

AuthorZone: RT @Zona_Springer: Felicitaciones a la Universidad del Salvador en Argentina quienes hoy empiezan su prueba de Springer #eBooks! #biblioteca, <http://twitter.com/AuthorZone/statuses/650962955761131>
Mon May 02 15:52:20 CEST 2011

AuthorZone: Did you know? #AOCs members receive a 25% discount on all English-language books from Springer. [#AM2011](http://ow.ly/4L9eC), <http://twitter.com/AuthorZone/statuses/650543218715688>
Mon May 02 15:05:32 CEST 2011

AuthorZone: Want to give your Springer book or journal article a face? Upload a video about your research here <http://ow.ly/4YNN>, <http://twitter.com/AuthorZone/statuses/6503809660918169>
Mon May 02 15:01:05 CEST 2011

» SUBSCRIBE TO THIS FEED

NAVIGATE TO...

- Journal Author Home
- How to publish your journal article
- Book Author Home
- How to publish your book

FIND ANSWERS ABOUT...

Turning your manuscript into a Springer journal article

- » Selecting a journal
- » Manuscript preparation
- » Electronic submission
- » Reviewing and acceptance
- » MyPublication
- » Copyediting and language polishing
- » Data processing and typesetting
- » Checking the article: proofing procedure
- » Publishing your article: OnlineFirst
- » Publishing your article in a journal issue

Abstracting & Indexing, Impact Factors

Open Access

E-Access via SpringerLink.com

Copyright, Rights & Licensing

Book discount & invoice information

Marketing: greatest possible visibility for your work

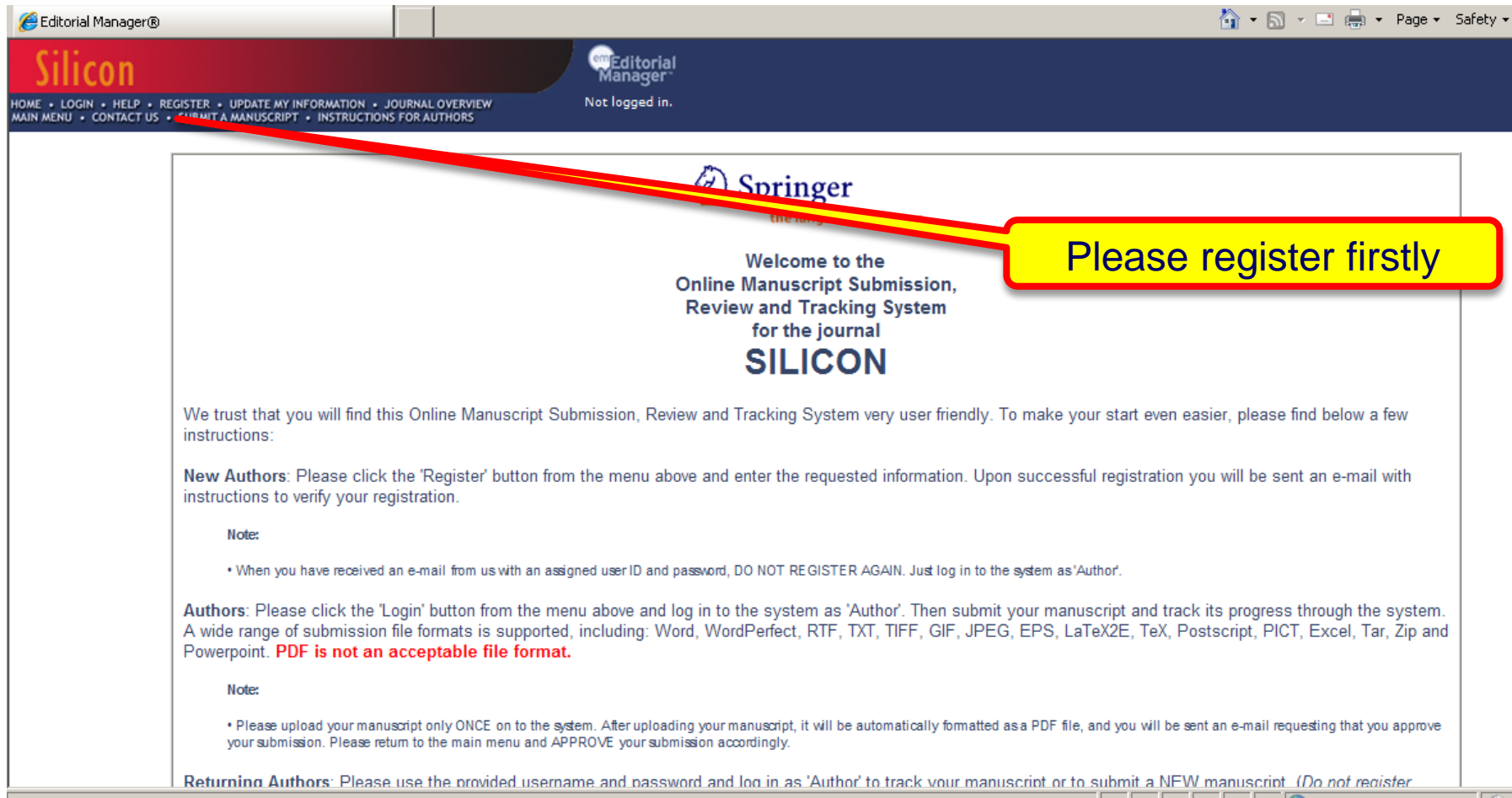
Submitting

Electronic submission

Electronic submission substantially reduces the editorial processing and reviewing times and shortens overall publication times



Submitting



Editorial Manager®

Silicon

HOME • LOGIN • HELP • REGISTER • UPDATE MY INFORMATION • JOURNAL OVERVIEW
MAIN MENU • CONTACT US • **• SUBMIT A MANUSCRIPT •** INSTRUCTIONS FOR AUTHORS

Not logged in.

Springer
the journal

Welcome to the
Online Manuscript Submission,
Review and Tracking System
for the journal
SILICON

We trust that you will find this Online Manuscript Submission, Review and Tracking System very user friendly. To make your start even easier, please find below a few instructions:

New Authors: Please click the 'Register' button from the menu above and enter the requested information. Upon successful registration you will be sent an e-mail with instructions to verify your registration.

Note:

- When you have received an e-mail from us with an assigned user ID and password, DO NOT REGISTER AGAIN. Just log in to the system as 'Author'.

Authors: Please click the 'Login' button from the menu above and log in to the system as 'Author'. Then submit your manuscript and track its progress through the system. A wide range of submission file formats is supported, including: Word, WordPerfect, RTF, TXT, TIFF, GIF, JPEG, EPS, LaTeX2E, TeX, Postscript, PICT, Excel, Tar, Zip and Powerpoint. **PDF is not an acceptable file format.**

Note:

- Please upload your manuscript only ONCE on to the system. After uploading your manuscript, it will be automatically formatted as a PDF file, and you will be sent an e-mail requesting that you approve your submission. Please return to the main menu and APPROVE your submission accordingly.

Returning Authors: Please use the provided username and password and log in as 'Author' to track your manuscript or to submit a NEW manuscript. *(Do not register*

Submitting

Author Main Menu

[Alternate Contact Information](#)

[Unavailable Dates](#)

New Submissions

[Submit New Manuscript](#)

Submissions Sent Back to Author (0)

Incomplete Submissions (0)

Submissions Waiting for Author's Approval (0)

Submissions Being Processed (0)

Please click
here to start
your
submission

Revisions

Submissions Needing Revision (0)

Revisions Sent Back to Author (0)

Incomplete Submissions Being Revised (0)

Revisions Waiting for Author's Approval (0)

Revisions Being Processed (0)

Declined Revisions (0)

Completed

Submissions with a Decision (0)

Submitting

Frequently Asked Questions

- ✓
- ✓
-
- ✓
- ✓
- ✓
-
- ✓
- ✓
-
-
- ➔

Required **Items** are marked with a *. When all **Items** have been attached, click **Next** at the bottom of the page.

PLEASE NOTE THAT THIS JOURNAL FOLLOWS A DOUBLE BLIND REVIEW PROCEDURE. PLEASE REMOVE YOUR NAME FROM ALL THE FILES YOU UPLOAD!!

Item

*Manuscript (excluding authors' names and affiliations) ▼

Enter a **Description** and then click the **Browse** button to select the file you wish to upload, then click the **Attach This File** button.

Description

Manuscript (excluding authors' names and

File Name:

浏览...

Attach This File



No items have yet been attached for this submission.

Successful

Previous

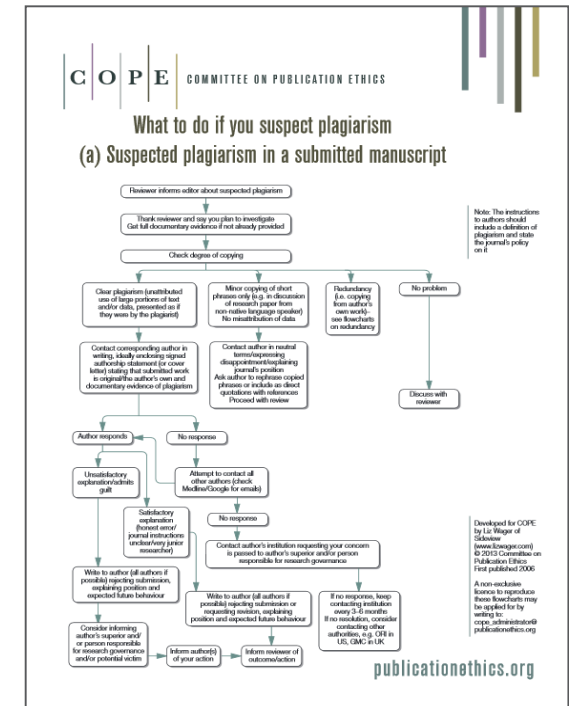
Next

How do Editors deal with plagiarism? 编辑如何处理抄袭

- Use plagiarism detection software 使用抄袭检查软件

- During submission 投稿过程中发现抄袭
- Ask authors for explanation 要求作者解释
- Authors may be allowed to re-write 重写
- Manuscript may be **rejected** 拒稿
- Editor may contact authors' institution
- 报告学校

- After publication 发表后发现抄袭
- May publish **retraction or correction** 撤稿或修正



How do Editors deal with plagiarism? 编辑如何处理抄袭

FAT STUDIES
https://doi.org/10.1080/21604851.2018.1453622

 **Routledge**
Taylor & Francis Group

 Check for updates

RETRACTED ARTICLE: Who are they to judge? Overcoming anthropometry through fat bodybuilding

Richard Baldwin

Department of History, Gulf Coast State College, Panama City, Florida, USA

ABSTRACT

While fat activism has disrupted many dominant discourses that causally contribute to negative judgments about fat bodies, it has not yet penetrated the realm of competitive bodybuilding. The author introduces fat bodybuilding as a means of challenging the prevailing assumptions of maximally fat-exclusionary (sports) cultures while raising fundamental ontological questions about what it means to “build a body.” Specifically, he advocates for imagining a new classification within bodybuilding, termed *fat bodybuilding*, as a fat-inclusive politicized performance and a new culture to be embedded within bodybuilding.

KEYWORDS

Fat activism; fat bodybuilding; sport; anthropometry

People who inhabit fat bodies are constantly judged—morally, aesthetically, physically, emotionally, economically, and in other ways that undermine their dignity. Most of all, people inhabiting fat bodies are judged for visual and superficial reasons: for the bodies they inhabit. Fat activism stands in opposition to the social stigma associated with fat, and, more generally, fatphobic attitudes throughout culture, and it has had considerable successes even though these attitudes are hegemonic and entrenched.

Particularly, anthropometric (body measuring) and ever more refined judgments of bodies and forms of physicality are commonplace in sports, reaching their zenith in the cultural space of competitive bodybuilding. Within the bodybuilding arena, bodies defy the “thin” ideals of anthropometry, yet they are respected because of their association with strength, fitness, and health. A paradox of anthropometry thus arises: bodybuilders’ bodies exist outside anthropometric expectations yet are still afforded social

8 Tips for writing a good paper

Before you begin

Research topics can be identified by exploiting opportunities



一开始时，你可以查阅本领域的文献。最初可以先看一些大家都感兴趣的期刊，看一些优秀的综述；当然，不要把自己的关注点局限在期刊里，看一本该领域内的书籍也是很有必要的，可以让你对该课题的历史及发展状况做一个全面的了解。



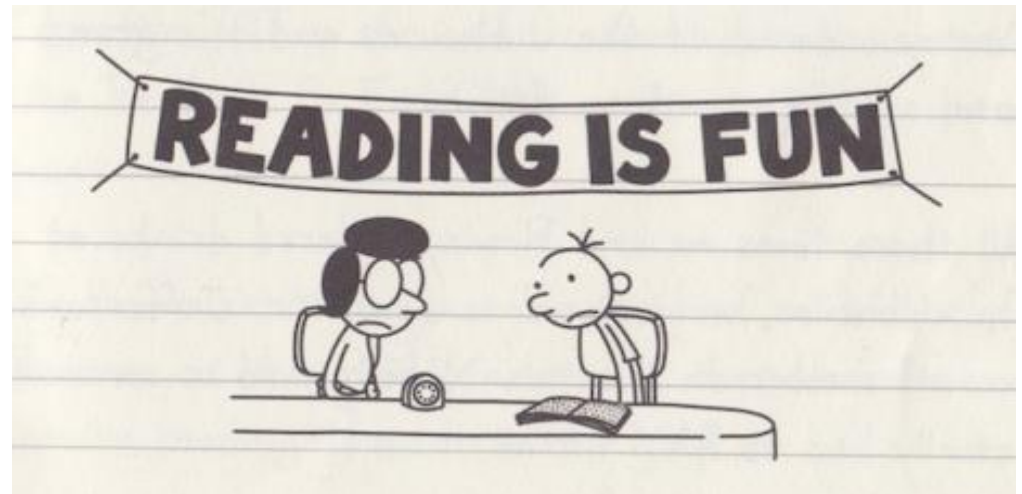
随着知识的积累，开始寻找一些令人困惑的现象，关于世界的未解之谜，新技术，亟需更佳解决方案的问题等。



带着准备好的问题与导师，师兄师姐交流，更可以参加一些学术会议，与该领域内某篇重要文献的作者直接进行交流。

Tip 1

- **Read many papers 多读文章**
- Know the field
- Join a journal club
- Read outside of your area to develop broad scope – think about quality of work
阅读自己研究领域以外的文献，拓宽知识面——注重研究质量
- Be aware of reporting guidelines



Tip 2

- Be objective about your work
客观对待自己的研究



.....Editors and reviewers will be 😊

Tip 3

- **Write in good English 用英语好好写**
- Complex language is not needed. Best science is where complex ideas are expressed in a way that people not in that field can understand
用非专业人士也能看懂的方式来表述复杂的想法
- Poorly written manuscripts get rejected – reviewers or editors lose patience or can't 'see' the results or advance
表述不明的文章会被拒稿——审稿人和编辑会对该研究的结果丧失兴趣
- Use a professional copy-editing service

The ABC of writing style



accurate



brief



clear

Be accurate (准确)

- **Tell your readers what they need to know**

Original

Of the 16.9-fold genome coverage, the majority was from 454 sequencing by synthesis of paired and unpaired reads, with the remaining coverage from Sanger dye primer sequencing of paired reads.

Improved

Of the 16.9-fold genome coverage, 74% was from 454 sequencing by synthesis of paired and unpaired reads. Sanger dye primer sequencing of paired reads was used for the remaining 26% (Supplementary Table 1 and Supplementary Note).

Be brief (简要)

- Keep to the point
- Avoid redundancy

Original

Based on these results, we hypothesized that vaccinated control individuals would show similar cytokine profiles to those treated with compound X. To assess this hypothesis, we compared the cytokine profiles of the vaccinated control individuals with those of treated patients. We found a higher frequency of...

Improved

Based on these results, we hypothesized that vaccinated control individuals would show similar cytokine profiles to those treated with compound X. By contrast, we found a higher frequency of...

Brevity (简短)

Difficulty was experienced in obtaining the isolate in an extremely purified state.

The isolate was difficult to purify completely.

Be clear (清晰)

- Break up long sentences
- Put closely related ideas together

Original

Whereas chimpanzees are widespread across equatorial Africa, bonobos, which have a relatively small and remote habitat, which also meant that they were the last ape species to be described, live only south of the Congo River (Fig. 1a) and are the rarest of all apes in captivity.

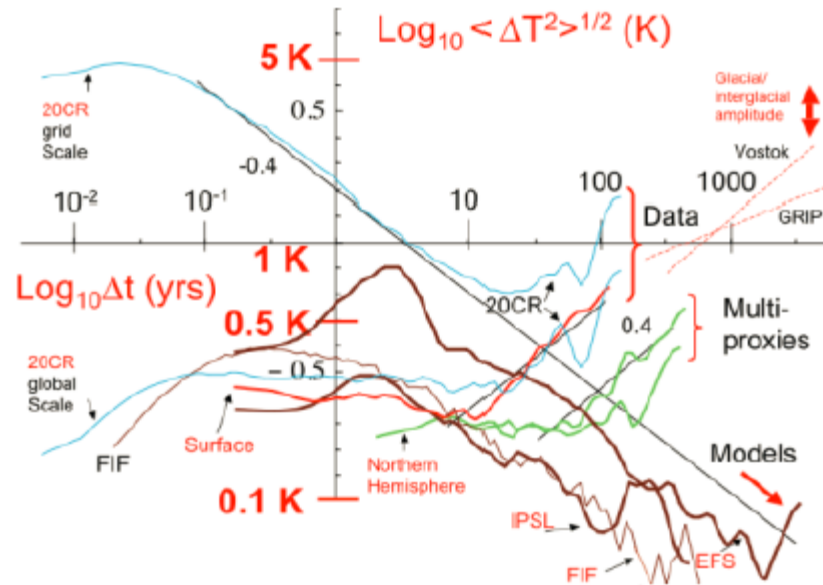
Improved

Whereas chimpanzees are widespread across equatorial Africa, bonobos live only south of the Congo River (Fig. 1a). As a result of their relatively small and remote habitat, bonobos were the last ape species to be described and are the rarest of all apes in captivity.

Be clear (清晰)

- Use simple words (but be specific)
-
- ✗ We found that the technique that we utilized had a relatively high accuracy in comparison with absorption spectroscopy (fig. 2).
 - ✓ Our technique was more accurate than absorption spectroscopy (fig. 2).

Be clear (清晰)



Earth Syst. Dynam. Discuss., 3, 1259-1286, 2012

- Too much information!
- Difficult to pull the main claim of the paper out from the jumble of information provided. We need to be able to glance at the figures and understand them
- The axes labels of this graph can't be understood without referring to the text
- Trend lines: add more information to an already busy graphic
- Reference to a previous graphic ('Vostock' and 'GRIP')

Tip 4

Decide early on where to publish 提前决定投哪本期刊

- This will help shape your study, based on the goals needed for publication in your target journal. Will help define the form of study and advance required.

针对期刊对文章的要求进行研究，有助于把握研究方向和创新性。

- Look at journal's aims and scopes page

仔细阅读该期刊所涵盖领域及对文章的要求

- Think about how you will structure your papers when you design your experiment

在设计实验时就开始思考文章架构

- What controls and statistical tests are needed?

设置哪些对照组，使用何种统计方法

- What collaborators / co authors should you work with to complete study?

需要和哪些共同作者合作才能完成该研究

- What is your aim with study? What are you trying to show / prove?

研究目的是什么？想要表现或证明什么？

Tip 5

Quality is everything 质量决定一切

- Try to publish in as high a quality journal as you can.
尽可能发表在质量最高的期刊上
- One great study is better than several lesser quality ones
一篇高质量的文章 > 多篇内容相似的一般文章
- Avoid trying to publish lots of research papers that provide small amounts of new data from a single research project.
切勿将一项完整的研究分割成若干篇文章发表

Tip 6

Become a reviewer! 珍惜审稿的机会！

- Get used to how to critically assess science – it will help you to assess your own study

了解如何批判地评估科研成果，有助于准确评估自己的工作

- Ask your supervisor if you can help with the next review they do

向导师申请帮其完成下一次的审稿工作

- You' ll become familiar with issues that reviewers raise as you see other reports

看别人的审稿报告，熟悉审稿人如何提问



Tip 7

• Respond to reviewers and editors 如何回复编辑和审稿人

- Ensure you understand what reviewers and editors are asking for (if unsure make an informal query to the editor prior to submitting your response).

明白评审和编辑提出什么要求

- Provide a full, and concise point-by-point response to the reviewers and editors.

提交完整的回复，将评审和编辑的要求逐点说明

- If you disagree with an issue, provide a clear rationale for your argument within the response. Back up with references where possible.

如果对评审提出的问题有异议，需在回复中提供详细的论证，最好附有参考文献

- Give clear indication where revisions in the manuscript have been made (tracked changes, highlighted etc).

指明对文章的哪些部分进行了修改

We thank the reviewers for their detailed and insightful evaluations of our submitted manuscript. We address these point by point.

Reviewer 1

The primary outcome measure is described as both 'proportion corrected severe anaemia in <24 hr' AND time to correction. One is a straightforward comparison to two proportions and the second a more complex time-dependent function. Since sampling was 'only' 8 hourly, do we really gain much from using the more complex analyses? Suggest separating out the two ways of describing this end point in the text and table 3.

In the protocol the primary outcome is "Correction of severe anaemia (to a Hb > than 6g/dl) at 24 hours"; before analysis was done, a decision was made to analyse this using time-to-event methods because of the potential for a child to abscond from hospital before 24 hours and for missing Hb measurements at 24 hours to lead to censored observations. The analysis of time from randomisation also indicates when this correction most commonly occurred. We have amended the main text to make this clearer. Because the decision was made on this primary analysis method before starting the analysis, we do not think that this should be changed now. (Note: Figure 3(a) presents the mean haemoglobin at 24 hours in children still alive in each group.)

A related issue is given that sampling Hb values was 8 hourly - how can figure 2 have been generated in which the probability of Hb correction is described as a continuous variable?

Although measurements were 8 hourly in the protocol there was some variation around this in practice. Figure 2 does show 'jumps' clearly indicating the 8 hourly measurements but it also provides additional information about when correction occurred as some jumps are larger than others. The title and y axis label have been changed to clarify that this shows the time to the first haemoglobin measurement >6g/dl.

Typos: methods Extra full stop 1st sentence in screened procedure and extra underscore from penultimate paragraph; "Furthermore, there is evidence indicating SMA has a"

We thank the reviewer for noting the grammatical errors- in the revised manuscript these have been corrected.

Reviewer 2

1. Provide comment on baseline differences particularly the greater proportion on patients in T30 with sickle cell anaemia and convulsions compared to T20; and the greater proportion of patients with "prostration" in the T20 group.

Tip 8

Learn to live with rejection! 正确看待被拒稿

- All scientific careers are faced with rejection
被拒稿是每个研究人员的必经之路
- Take reviewers advice and improve the study / manuscript
根据审稿人的意见进行修改
- If you are invited to resubmit, do the revisions that the reviewers request.
Don' t argue for the sake of it
如果有重投的机会，一定要根据审稿人的意见进行修改，切勿进行过多争论
- There are other journals
选择其他期刊
- Try not to resent negative comments
不要给出负面回应和评论
 - You can appeal If there has been an error 如果有事实错误可以申诉
 - If you have new data to support your findings 用新数据来支持发现



翻拍自河出书房新社一九九三年的
《新文艺读本：寺山修司》

多忙の日々。1969年頃

Thank you

乔昆鹏

Kunpeng.Qiao@springernature.com

SPRINGER NATURE



扫码下载PPT