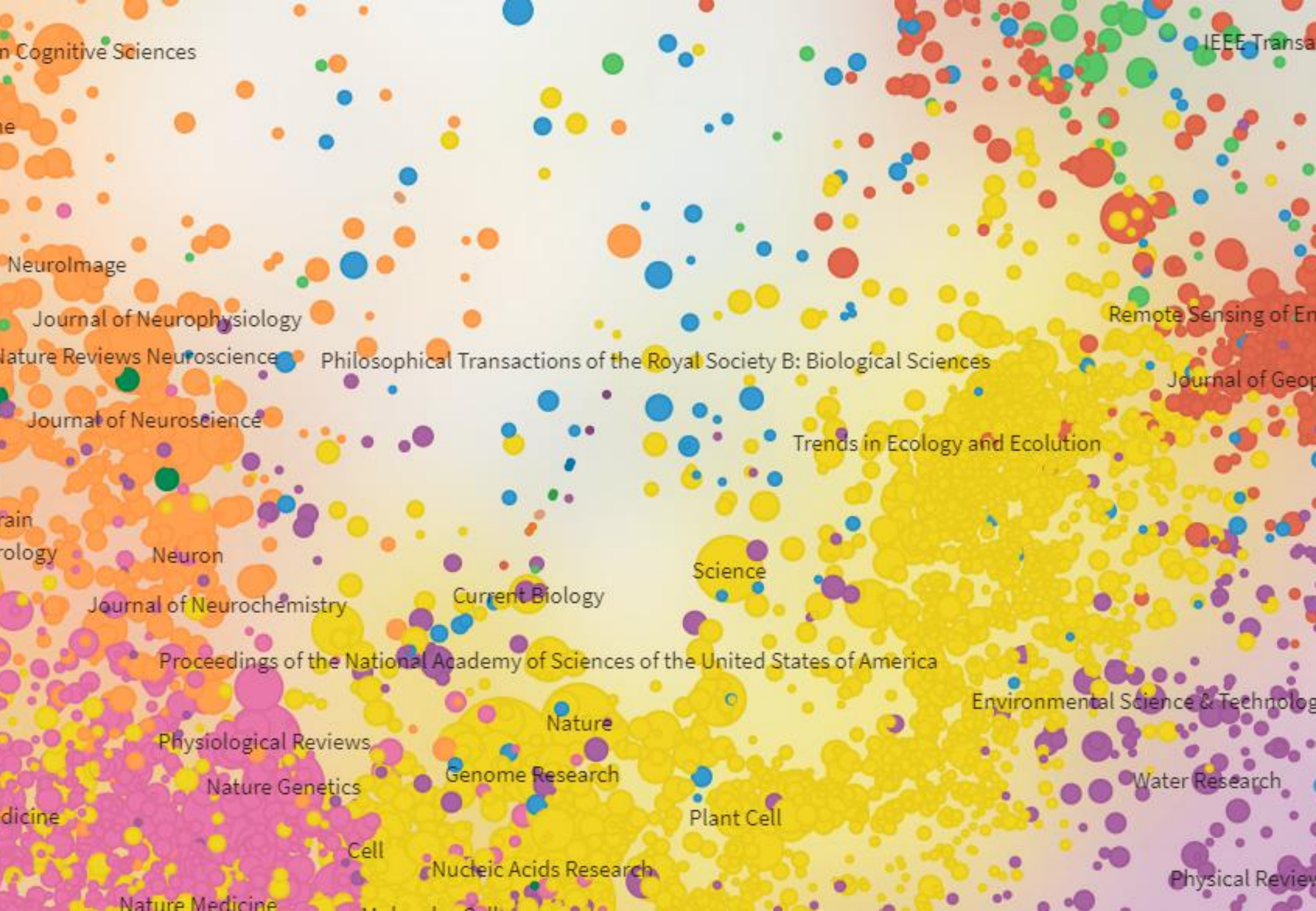
赋能科研175年

Empowering Science for 175 years

SPRINGER NATURE


n Cognitive Sciences
IEEE Transa
NeuroImage
Journal of Neurophysiology
Remote Sensing of En
Nature Reviews Neuroscience
Philosophical Transactions of the Royal Society B: Biological Sciences
Journal of Geop
Journal of Neuroscience
Trends in Ecology and Ecolution
rain
rology
Neuron
Science
Current Biology
Journal of Neurochemistry
Proceedings of the National Academy of Sciences of the United States of America
Environmental Science & Technolog
Nature
Physiological Reviews
Genome Research
Nature Genetics
Water Research
dicine
Plant Cell
Cell
Nucleic Acids Research
Physical Review
Nature Medicine

SpringerNature公司介绍

1.0

"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

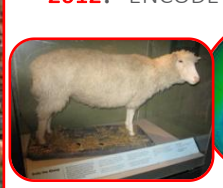
1995：首次发现太阳系外的行星

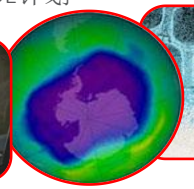
1997：克隆羊多莉诞生

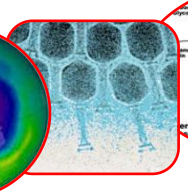
2001：人类基因组计划

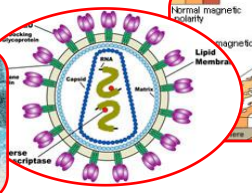
2006：破解安提基特拉机械装置

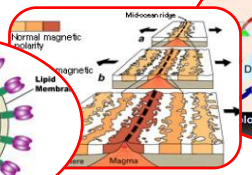
2012：ENCODE计划

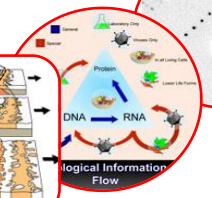


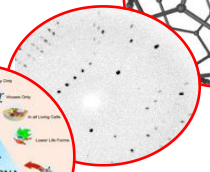


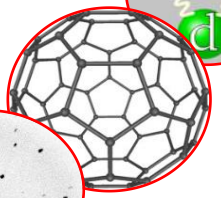








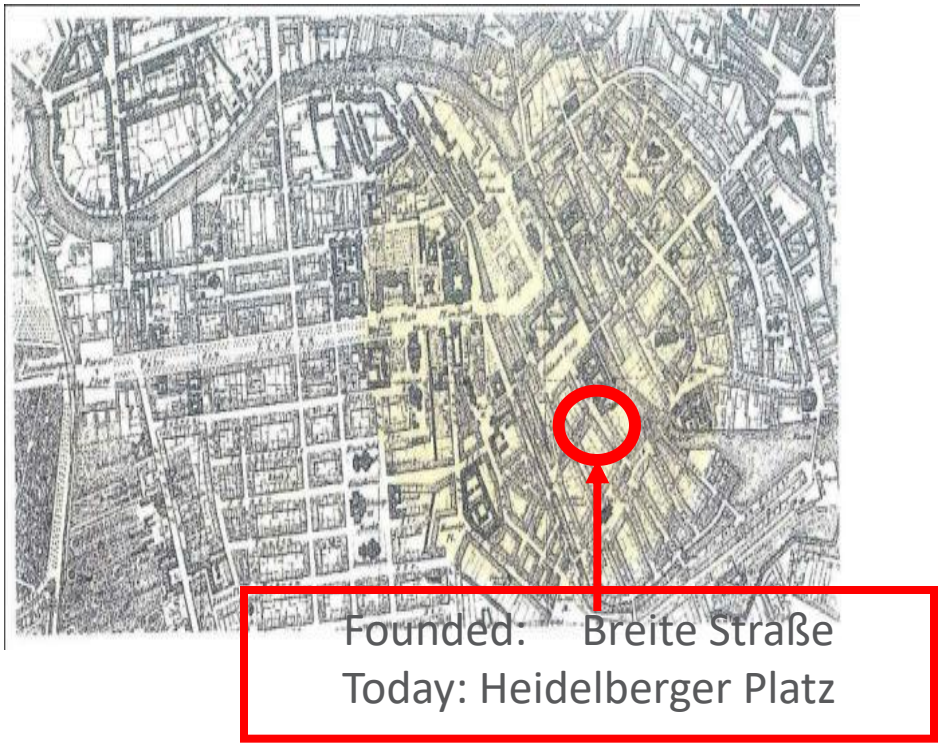




SPRINGER NATURE

出版社简介

Springer 于1842年始建于柏林，拥有175年的历史……



Springer	nature	macmillan education
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、技术和医学类电子图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。	《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阅览超过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 The Open Access Publisher	Apress®	SCIENTIFIC AMERICAN	palgrave macmillan
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。	《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月平均阅览量达550万人次。	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。

http://www.digibarn.com/collections/books/xerox-parc-1970-80/alto-article/

A Decade of Research @ Xerox PARC

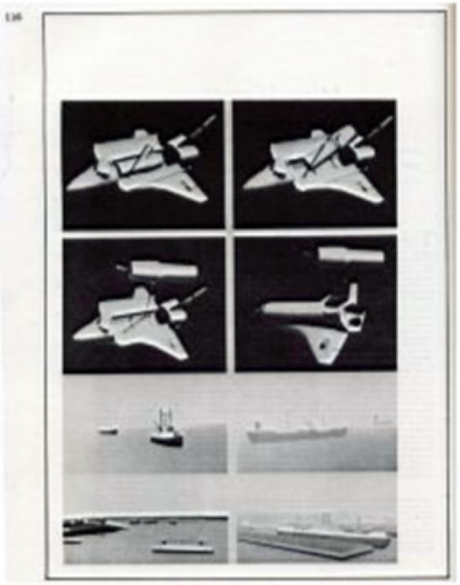
reprint of

Sept 1977 Scientific American Article on Xerox Alto "Microelectronics and the Personal Computer"

pp. 230-244, by Alan Kay

Note: All contents on these pages are copyright Scientific American unless otherwise noted. This article is reproduced here for historical reference only and can only be used by reference for scientific and other research purposes.

alto-1.jpg



alto-2.jpg

alto-3.jpg

SPRINGER NATURE

A leading global scientific, technical and medical publisher…
全球领先的科学、技术、医学、人文社科出版社

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产品简介

2.0

Springer Nature产品

期刊

- Springer期刊
  2156种
- Nature品牌期刊
  38种
- Nature学术期刊
  43种
- Palgrave期刊
  52种

图书

- Springer Ebooks
  21万册
- 20个学科
- 世界最大的STM & HSS出版社

数据库

- Springer Protocols
  实验指南4万多条
- Springer Materials
  25万种材料
- zbMath
  数据文摘（300多万条）
- Adis Insight
  药学

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

部分学科专辑SCI收录比例

Behavioral Science	56%
Biomedical and Life Science	89%
Business and Economics	50%
Chemistry and Materials Science	82%
Computer Science	65%
Earth and Environmental Science	75%
Engineering	52%
Humanities, Social Science & Law	39%
Mathematics and Statistics	72%
Medicine	57%
Physics and Astronomy	89%

SPRINGER NATURE

重点期刊推荐 – Nature品牌期刊

图书馆已订购	
Nature	《自然》周刊
Nature Biotechnology	《自然 · 生物技术》
Nature Climate Change	《自然 · 气候变化》
Nature Genetics	《自然 · 遗传学》
Nature Geoscience	《自然 · 地理科学》
Nature Methods	《自然 · 方法》
Nature Plants	《自然 · 植物》
Nature Protocols	《自然 · 实验室指南》

重点期刊推荐 – Nature品牌期刊

This Week

Editorial

Editorial | 17 April 2018

Military work threatens science and security

In an uncertain world, more governments are asking universities to help develop weapons. That's a threat to the culture and conscience of researchers.

Editorial | 18 April 2018

Checklists work to improve science

Nature authors say a reproducibility checklist is a step in the right direction, but more needs to be done.

Editorial | 18 April 2018

A welcome framework for research in Africa

A new set of ethics principles should help researchers and funders do justice to the interests of those involved with Africa's genomics research.

重点期刊推荐 – Nature品牌期刊

World View

World View | 18 April 2018

Science must rise up to support people like me

Institutions could do more to support researchers who have disabilities, says Aaron Schaal.

Aaron Schaal

Science must rise up to support people like me

Institutions could do more to support researchers who have disabilities, says Aaron Schaal.

Aaron Schaal

重点期刊推荐 – Nature品牌期刊

Research Highlights

Research Highlight | 10 April 2018

Gentle 'slow slip' earthquakes belie hidden danger

Fluid build-up after a slow quake raises the risk of massive rupture.

Research Highlight | 12 April 2018

Why fit fathers sire smarter offspring

Mice that hit the running wheel have brainier pups than sedentary rodents do.

Research Highlight | 13 April 2018

Laser-beam 'tweezers' guide two atoms to collide

A carefully manipulated crash shows what happens when atoms collide in the cold.

Research Highlight | 12 April 2018

Deadly tumours are often born of childhood mutations

Early chromosomal disruption can set the stage for kidney cancer decades later.

NGER NATURE

重点期刊推荐 – Nature品牌期刊

This Week

Editorial

Editorial | 17 April 2018

Military work threatens science and security

In an uncertain world, more governments are asking universities to help develop weapons. That's a threat to the culture and conscience of researchers.

Editorial | 18 April 2018

Checklists work to improve science

Nature authors say a reproducibility checklist is a step in the right direction, but more needs to be done.

Editorial | 18 April 2018

A welcome framework for research in Africa

A new set of ethics principles should help researchers and funders do justice to the interests of those involved with Africa's genomics research.

重点期刊推荐 – 《自然·生物技术》

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

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。

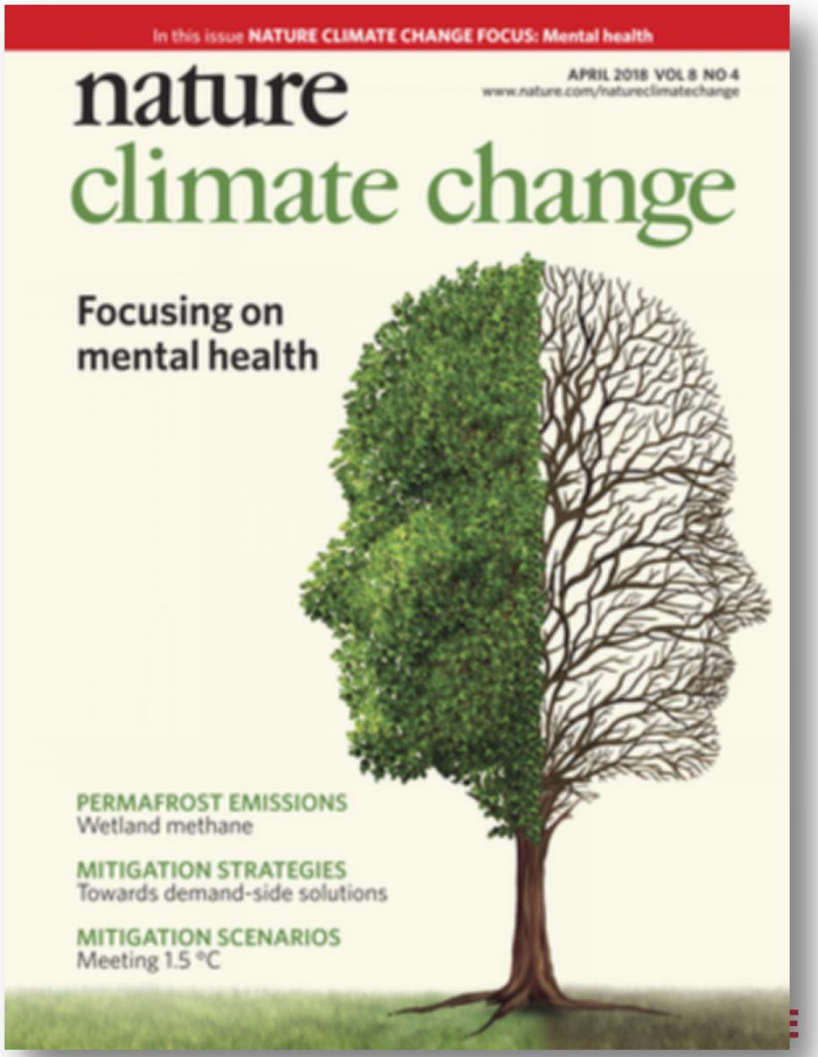
超分辨率成像

重点期刊推荐 — 《自然·气候变化》

https://www.nature.com/nclimate/

致力于发表有关全球气候变化成因、效应以及更大范围潜在影响的最前沿和最重要的高质量研究成果。

在“巴黎协定”中，各国致力于制定更加雄心勃勃的气候政策目标，旨在将全球变暖限制在1.5°C而不是比工业化前水平高出2°C。 气候模型现在表明，实现1.5°C的目标将对北极海冰产生重大影响。

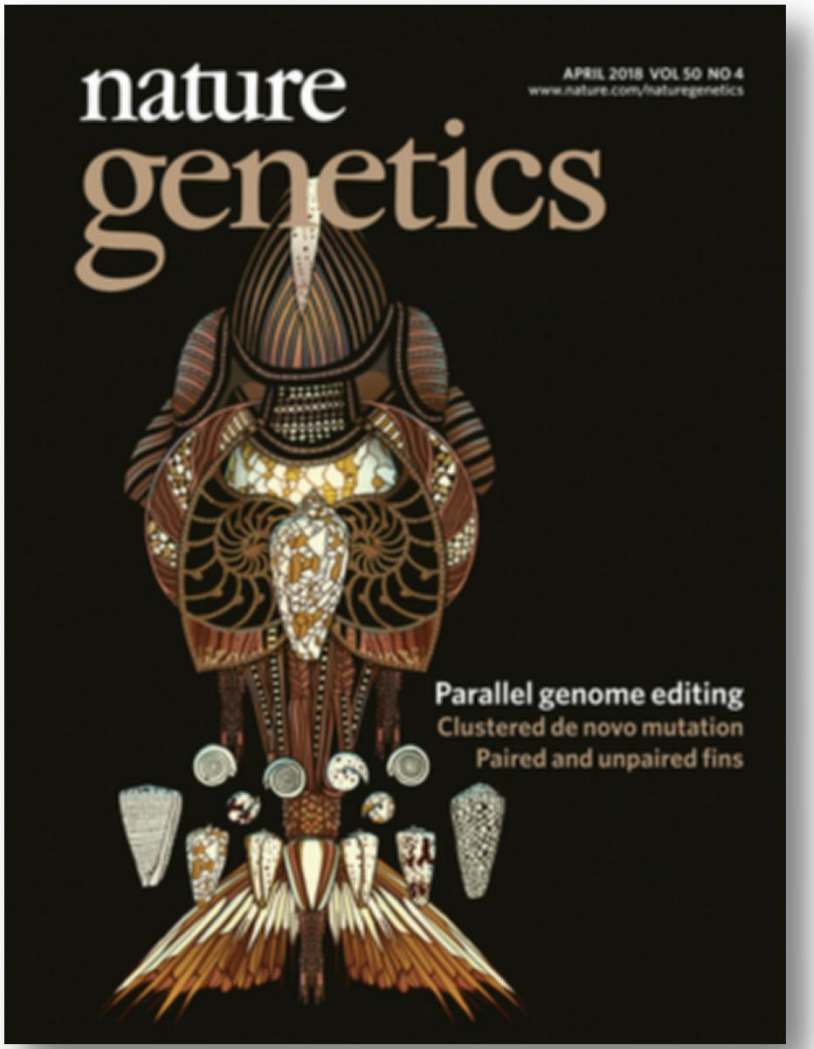


重点期刊推荐 — 《自然·遗传学》

https://www.nature.com/ng/

遗传学领域内排名第一的基础研究型期刊，发表遗传学领域内最高品质的研究论文。期刊收录范围涵盖人类基因及基因组、实验胚胎学、癌症、染色体生物学及基因技术。此外，本刊还发表该领域内的新资讯、新观点，报导发表在其他期刊上的重要研究亮点，专题概述与讨论遗传学发展的相关议题，主题涵盖范围甚广。

了解DNA序列变异的功能效应对于基础生物学，进化和医学遗传学的研究至关重要。然而，以高通量方式测量这些效应是一个重大挑战。一个有希望的途径是用CRISPR-Cas9系统进行精确编辑，该系统允许在与引导RNA（gRNA）的靶向序列相匹配的基因组位点处产生DNA双链断裂（DSB）。



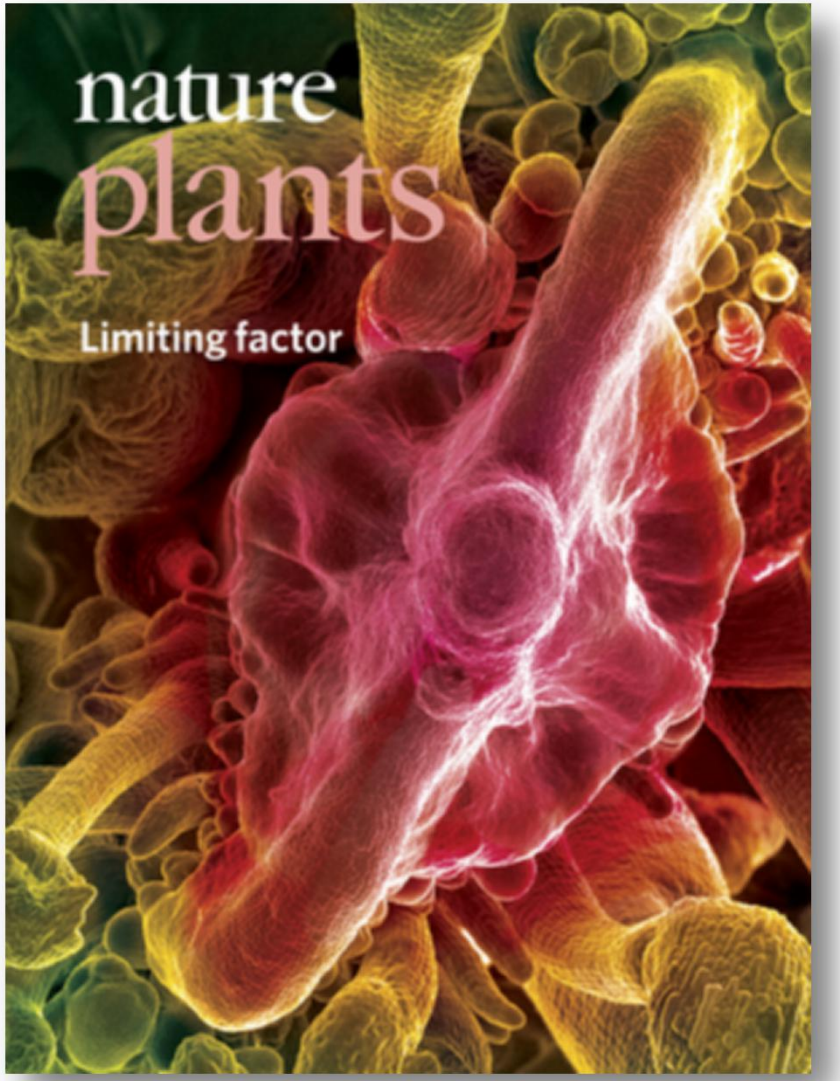
重点期刊推荐 — 《自然 · 植物》

https://www.nature.com/nplants/

专注发表植物科学领域最前沿的基础和应用研究成果，涵盖植物学的各个方面：植物的进化，植物的生长发育、新陈代谢，植物与环境的相互关系及其对人类社会的重要意义。此外，本刊也将关注植物的遗传学、细胞生物学、生态学和进化过程，以及植物王国与人类的相互关系。

只要有必要，福利一直在政治上引起争议。 现代工业化国家的福利使用各种机制，例如食物，服务或现金，为贫困公民提供援助。

虽然不同的社会对福利有不同的态度和态度，但在美国和英国，那些依赖这种“伸手乞讨”的人常常被认为不值得被救济。福利受益者经常被用作政治替罪羊，同时试图生存并使自己和家人摆脱贫困，在一些世界上最富有的国家，通常非常微薄的福利。



Springer重点期刊推荐《GENOME BIOLOGY》

Open Access

IF：11.908

https://genomebiology.biomedcentral.com/

基因表达的多层面控制需要调控机制在转录水平和转录后水平的紧密协调。 在这里，我们通过全长mRNA测序研究了单个mRNA分子上的转录起始，剪接和聚腺苷酸化事件的相互依赖性。

Springer重点期刊推荐《PRECISION AGRICULTURE》

IF:2.012

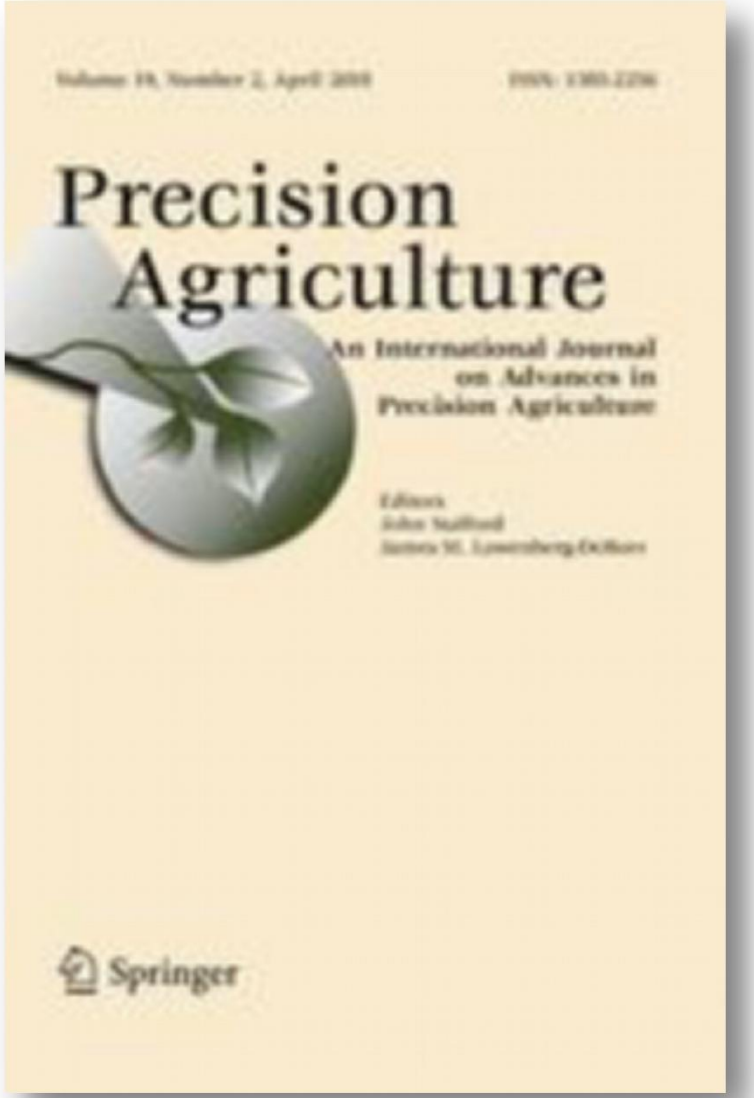
https://link.springer.com/journal/11119

讨论的主题包括：

自然资源变异性，包括土壤和作物变异性和特征

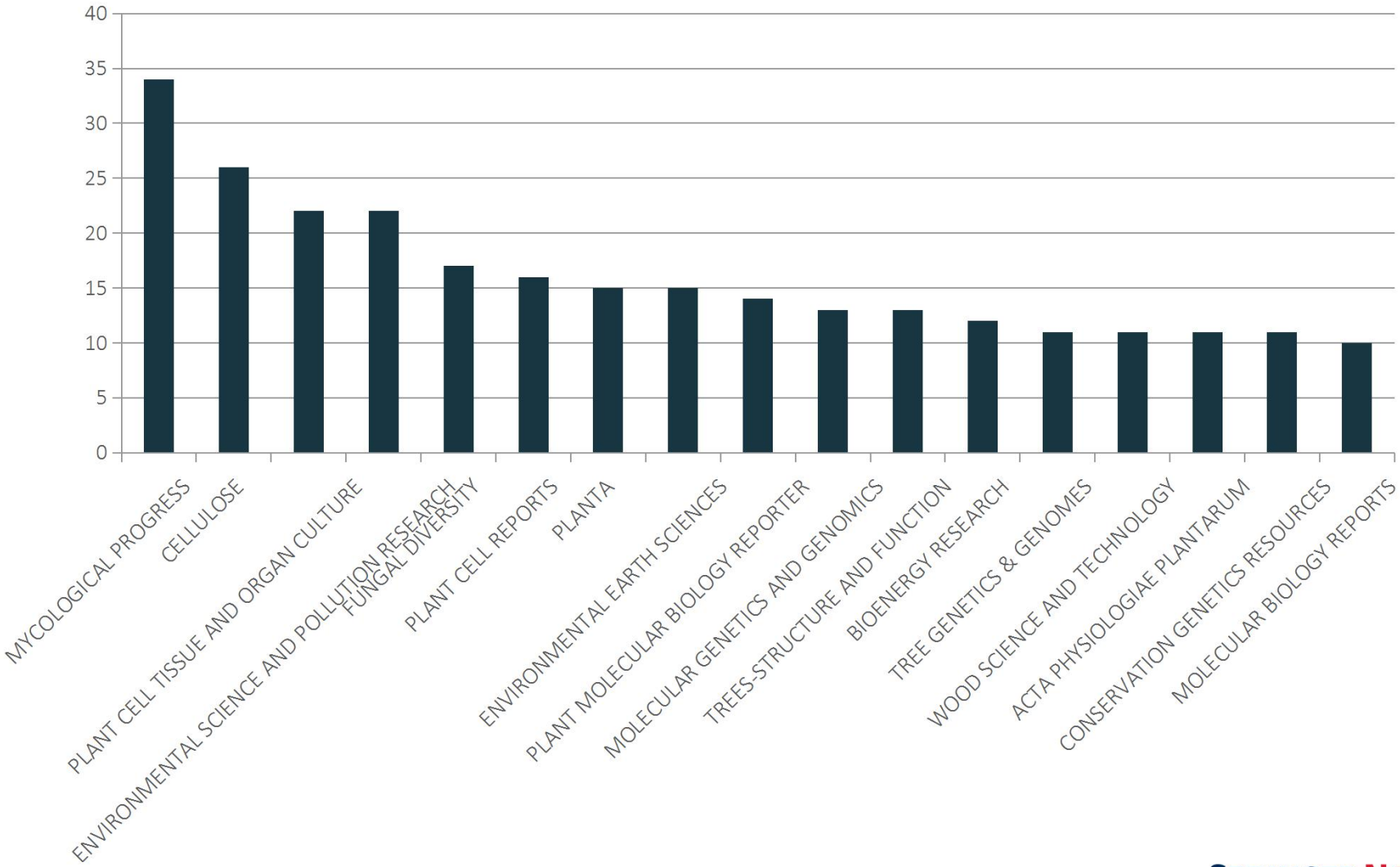
管理变异性，包括采样技术和方法，营养和作物保护化学品推荐和作物质量

工程技术，专注于传感器系统，计算技术，定位系统和用于特定场地应用的控制系统



北京林业大学作者发文领域分布

北京林业大学作者发文期刊分布



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

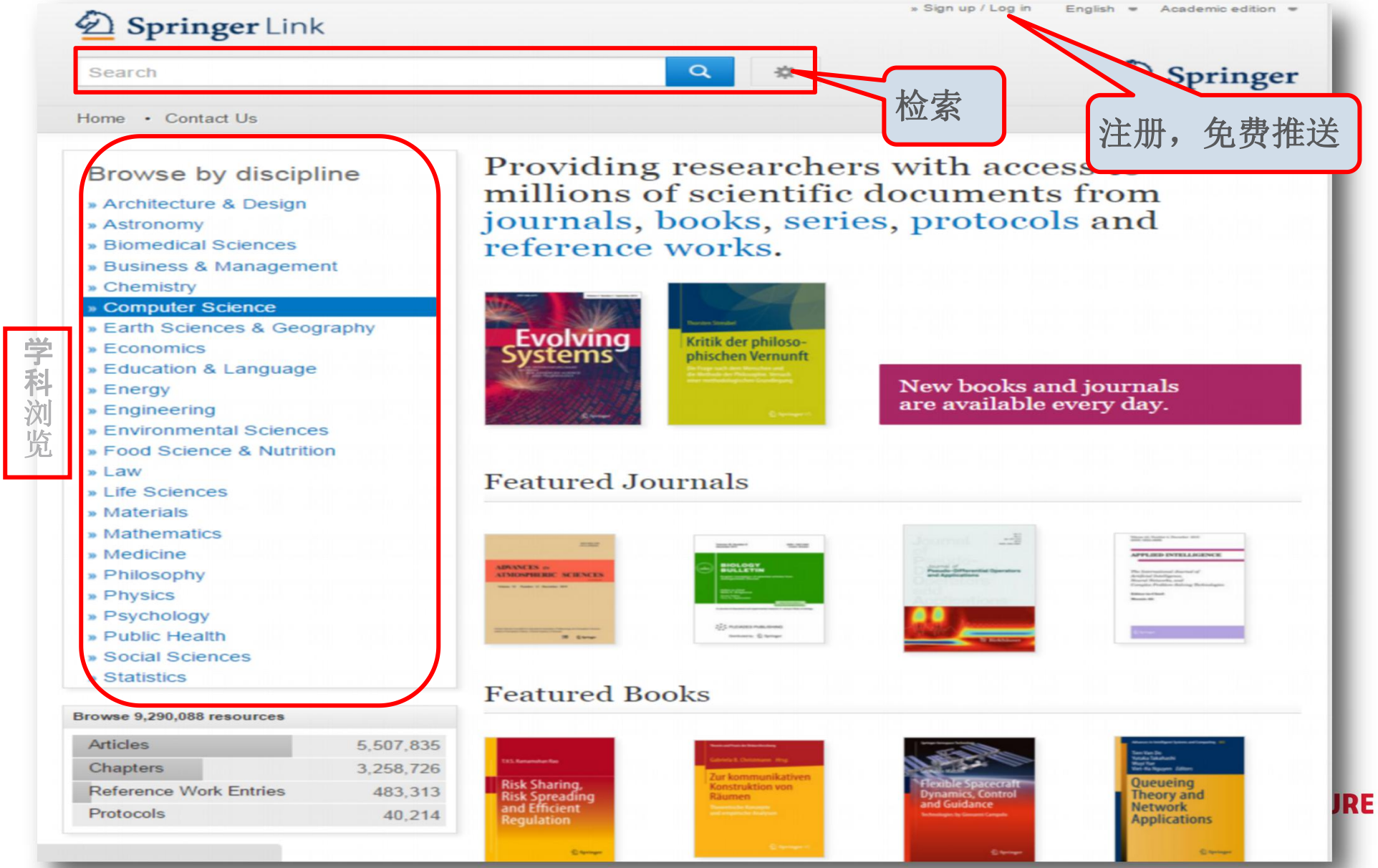
平板电脑（终端）桌面

手机-横版桌面

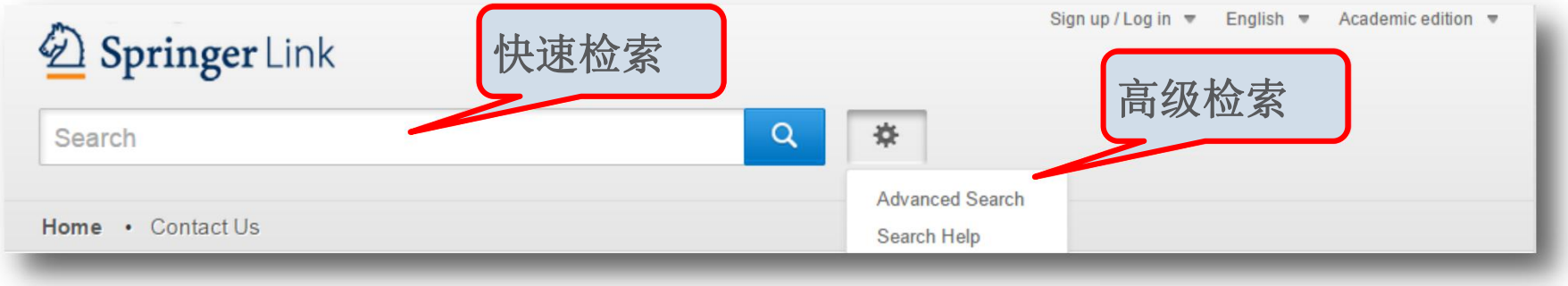
手机-竖版桌面

SPRINGER NATURE

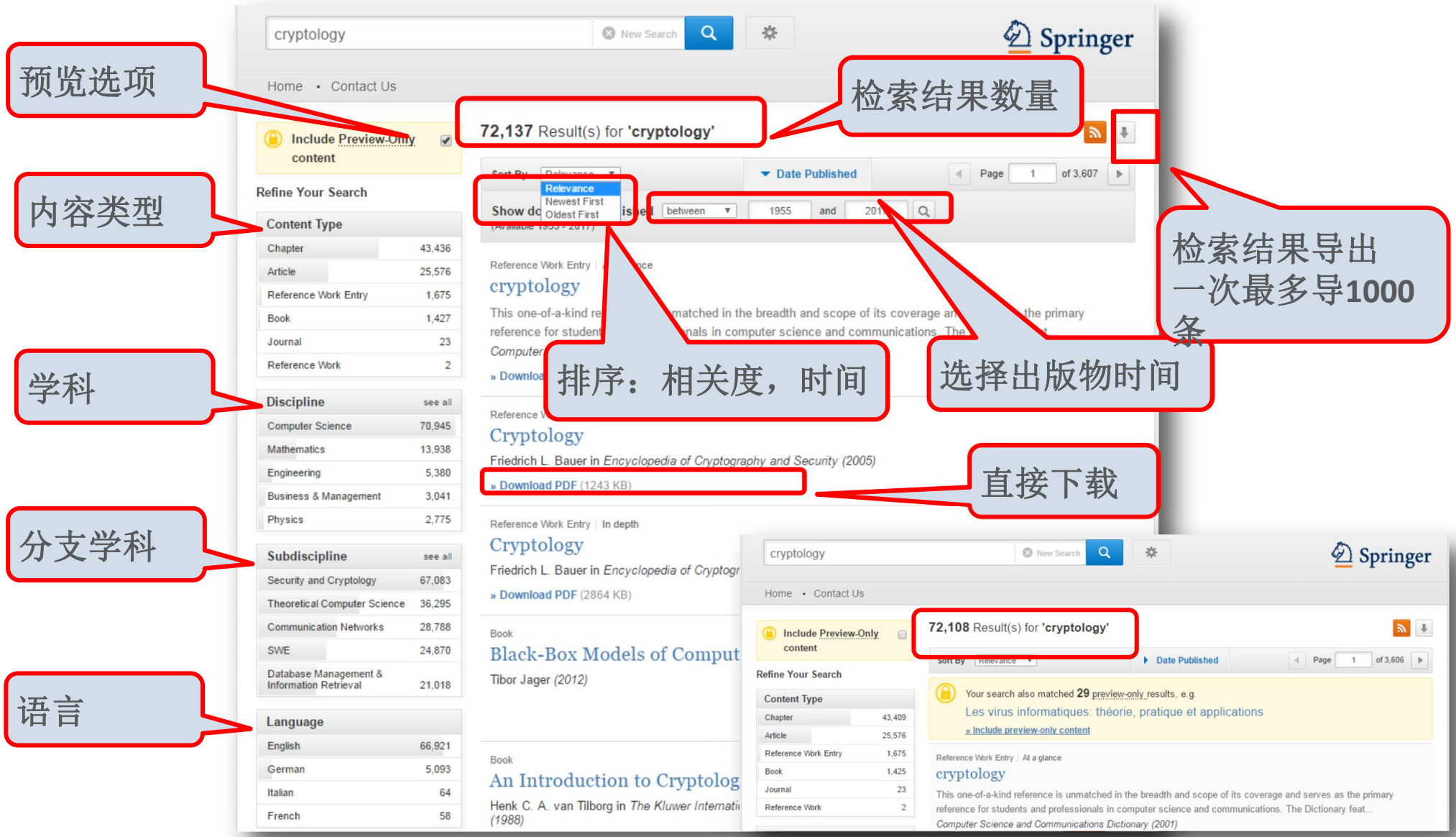
SpringerLink平台界面



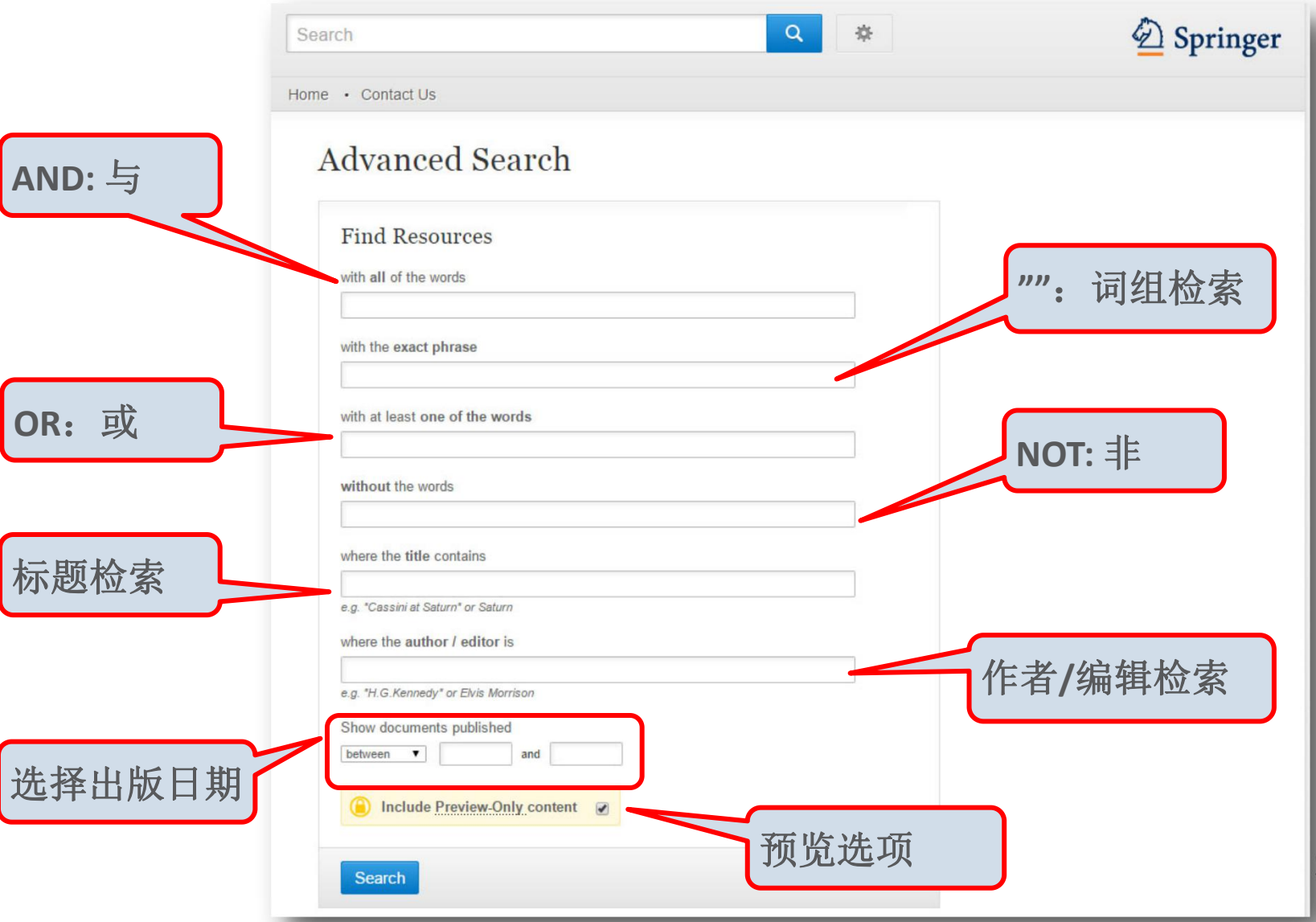
SpringerLink平台检索：快速检索



SpringerLink平台检索：快速检索续



SpringerLink平台检索：高级检索



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

follow this link to go to Law

Refine by Subdiscipline

- Private International Law, International & Foreign Law, Comparative L
- Civil Law
- Medical Law
- Commercial Law
- Public International Law
- Law, general
- Administrative Law
- Theories of Law, Philosophy of Law, Legal History
- Fundamentals of Law
- European Law
- Medicine/Public Health, general
- Criminal Law
- Constitutional Law
- Philosophy of Law
- Public Law
- Environmental Law/Policy/Ecojustice
- Labour Law/Social Law
- Financial Law/Fiscal Law
- Human Rights
- International Economic Law, Trade Law

SpringerLink平台检索：高级检索续

social respo

New Search

schaefer's position on shareholders and **social responsibility**

conflicts between corporate strategy and ethical and **social responsibilities**

corporate **social responsibility** theories

the impact of board diversity and gender composition on corporate **social responsibility**

81 Result(s) for **'"social respo*"'**

within Law Commercial Law English

Sort By Relevance Date Published Page 1 of 5

Book

Globalisation of Corporate Social Responsibility and its Impact on Corporate Governance

Prof. Jean J. du Plessis... *(2018)*

Chapter

Corporate Social Responsibility and the Corporate Board: Assessing the Indian Experiment

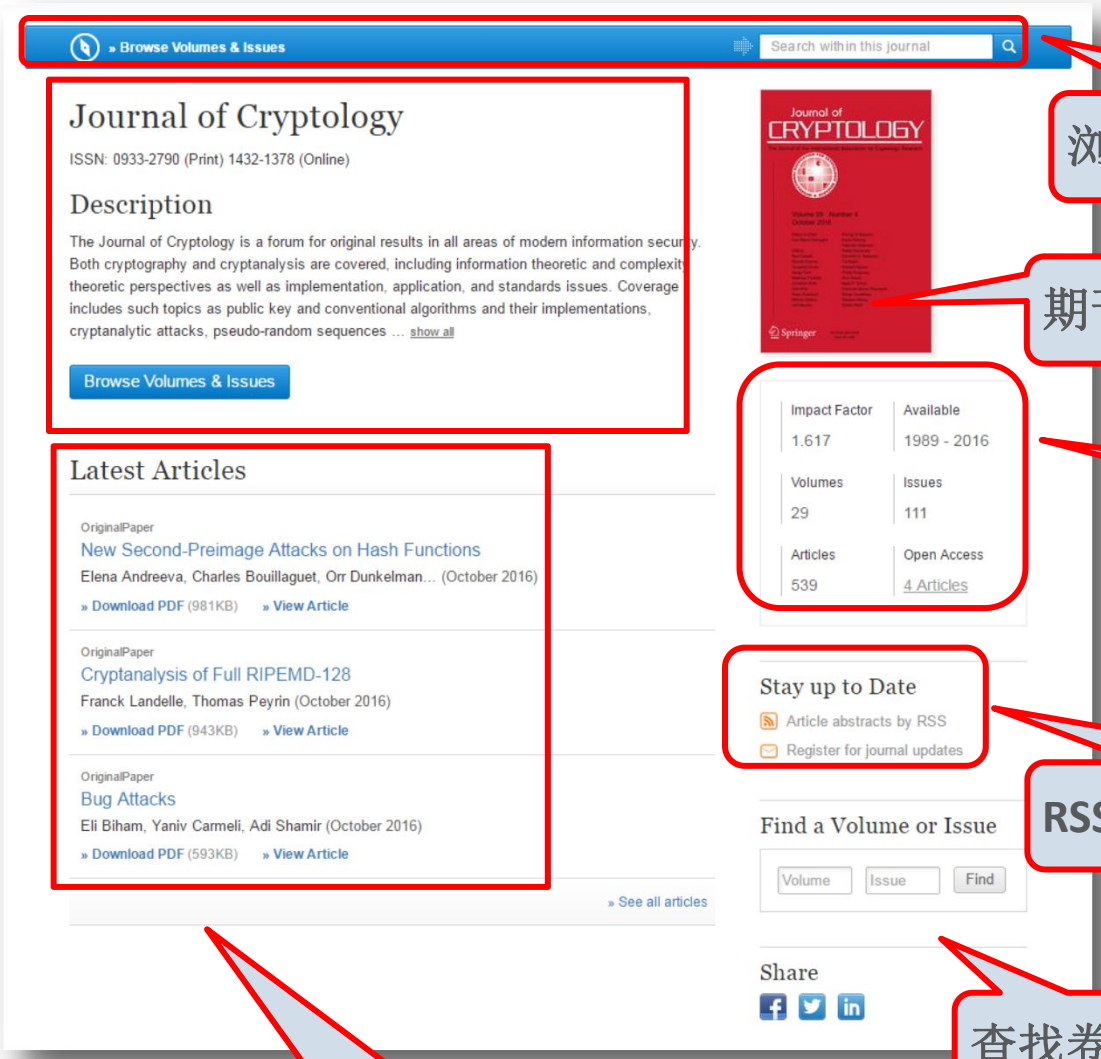
Corporate social responsibility (CSR) has received significant attention from...

Afra Afsharipour in *Globalisation of Corporate Social Responsi... (2018)*

» Download PDF (429 KB) » View Chapter

SpringerLink-期刊的浏览

期刊主页介绍



浏览所有卷期, 期刊内检索

期刊简要信息

影响因子，文章数量，卷期数，年限等

RSS订阅和期刊更新注册提醒

查找卷期

最新发表的文章

SPRINGER NATURE

SpringerLink-期刊的浏览

期刊主页–续

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

Additional Links
» Register for Journal Updates
» Editorial Board
» About This Journal
» Manuscript Submission

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

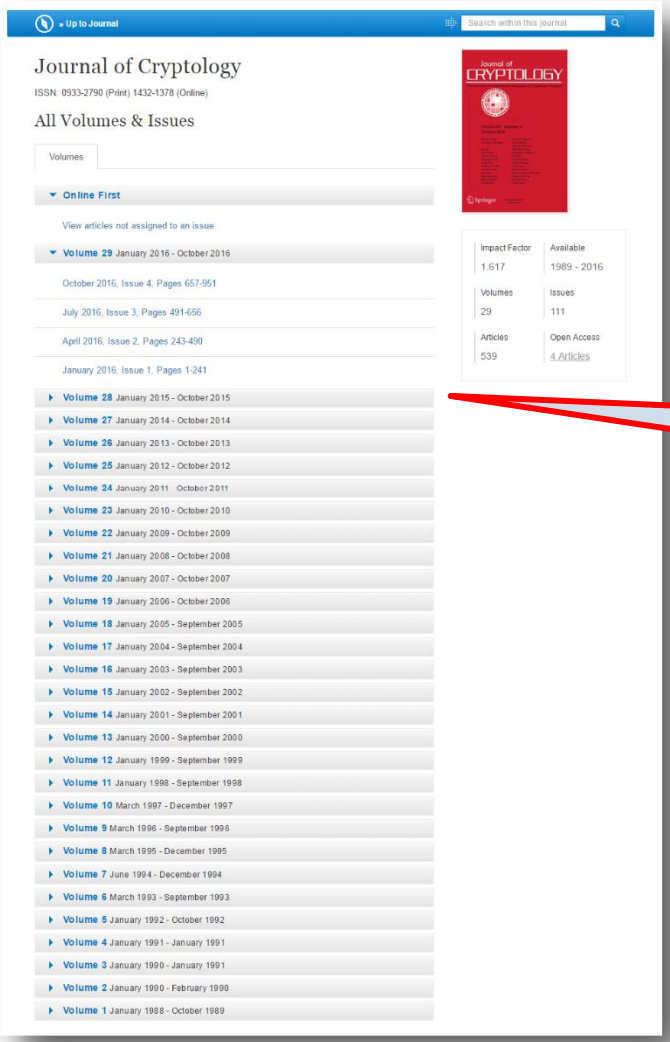
所属主题分类

所属行业分类

其他链接

SpringerLink-期刊的浏览

浏览所有卷期



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

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

192 Views

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].

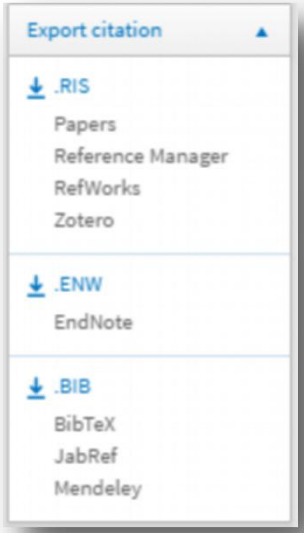
Download PDF
Export citation
Share article

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

下载PDF

文章信息：标题，作者，摘要

论文快速定位



Export citation

.RIS
Papers
Reference Manager
RefWorks
Zotero

.ENW
EndNote

.BIB
BibTeX
JabRef
Mendeley

导出引文

SpringerLink-期刊的浏览
查看文章-续

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. Zimmer, [illegible] 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

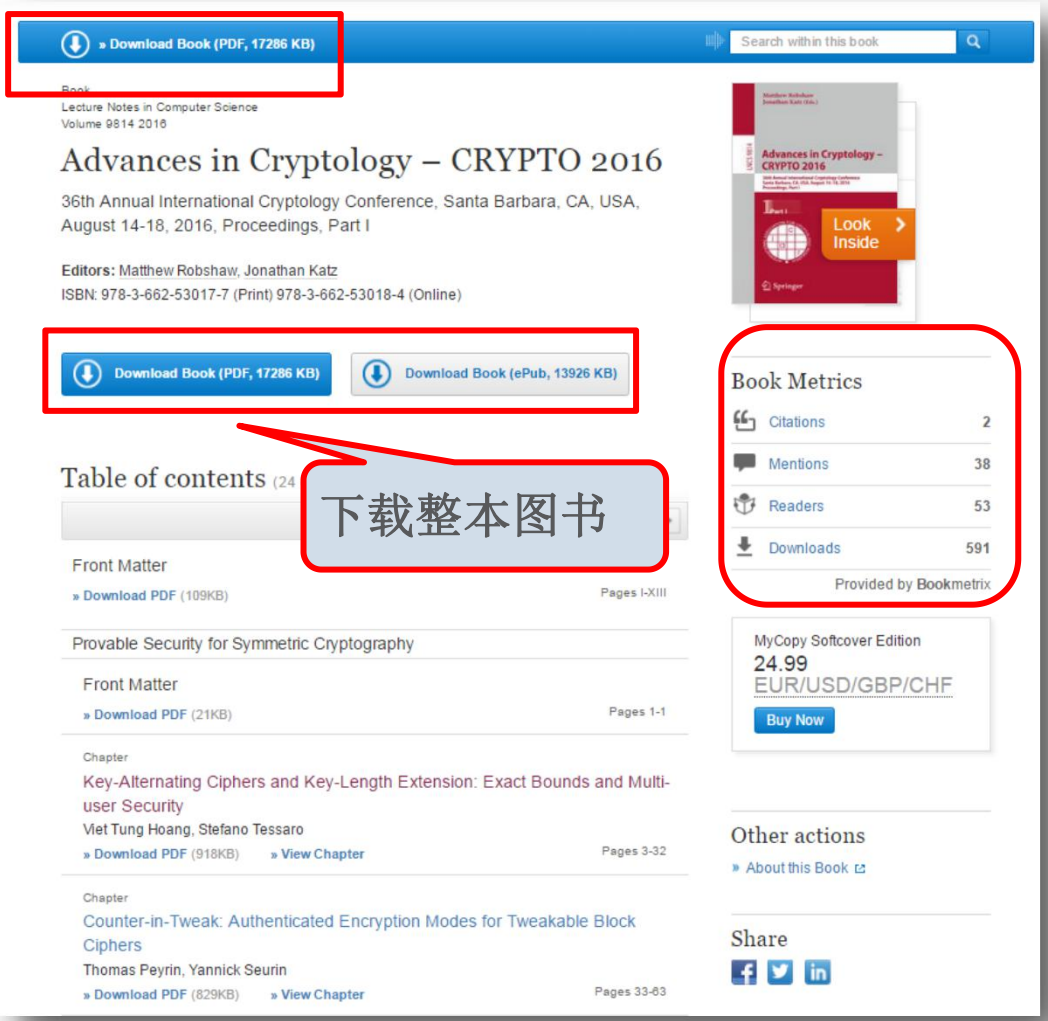
3. E. Andreeva, B. Mennink, Provable chosen-target-forced-midfix preimage resistance, in eds. by A. Miri, S. Vaudenay. *Selected Areas in Cryptography—18th International Workshop, SAC 2011, Toronto, ON, Canada, August 11–12, 2011.* Revised Selected Papers. Lecture Notes in Computer Science, vol. 7118 (Springer, 2011), pp. 37–54. doi:10.1007/978-3-642-28496-0_3

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



图书内检索
Look Inside

图书计量信息

SPRINGER NATURE

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-图书章节续

图书章节介绍

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. Univ

Authors
Viet Tun
Stefano

Author A
15. Depa
Universit
Santa Ba

作者或编辑信息

分类信息

章节信息

References (26)

1.Andreeva, E., Bogdanov, A., Dodis, Y., Mennink, B., Steinberger, J.P.: On the indifferentiability 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.cr.yp.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

SpringerLink-图书章节

图书章节介绍

» 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

Look Inside

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

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

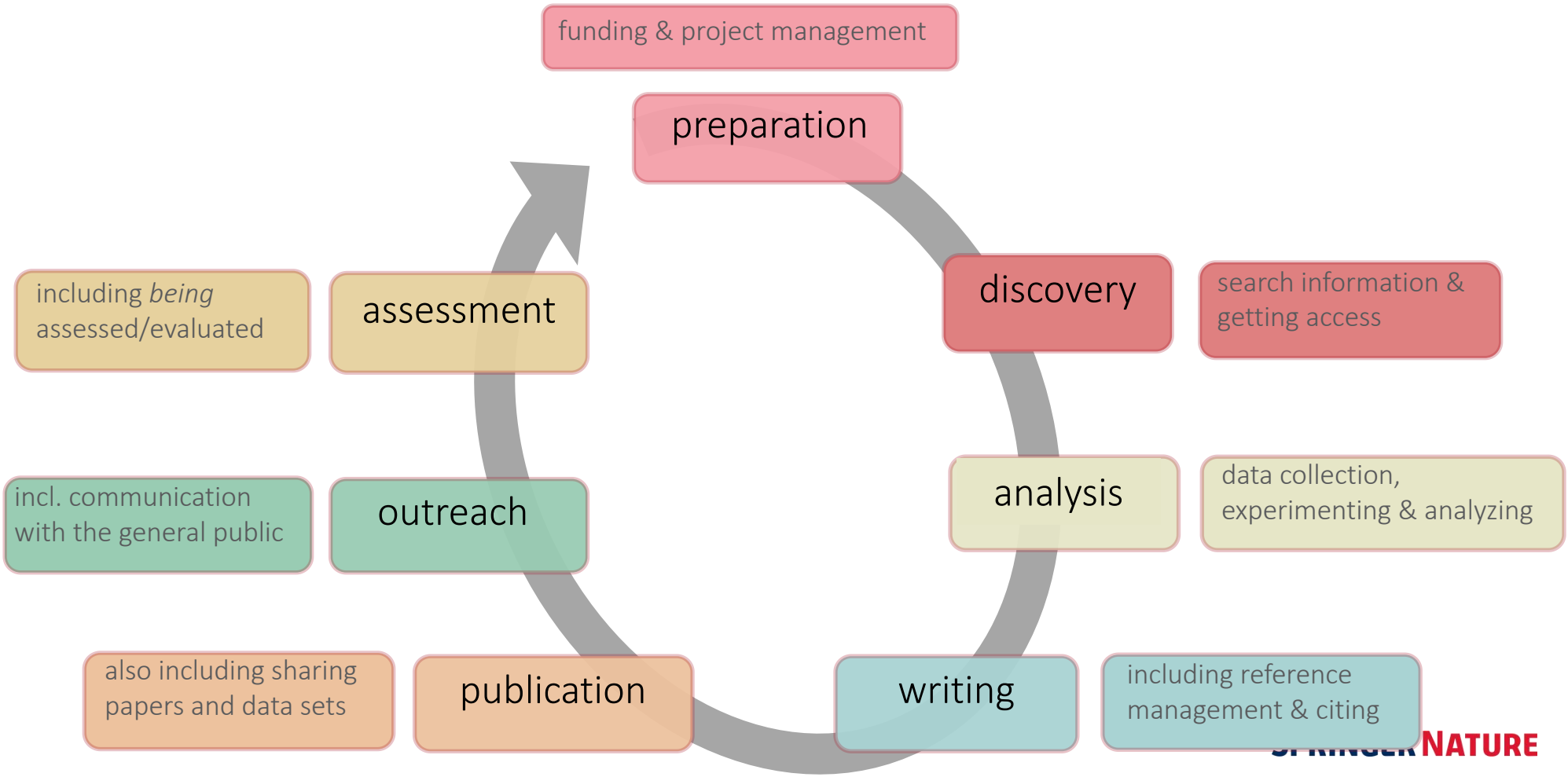
期刊论文投稿简介

4.0

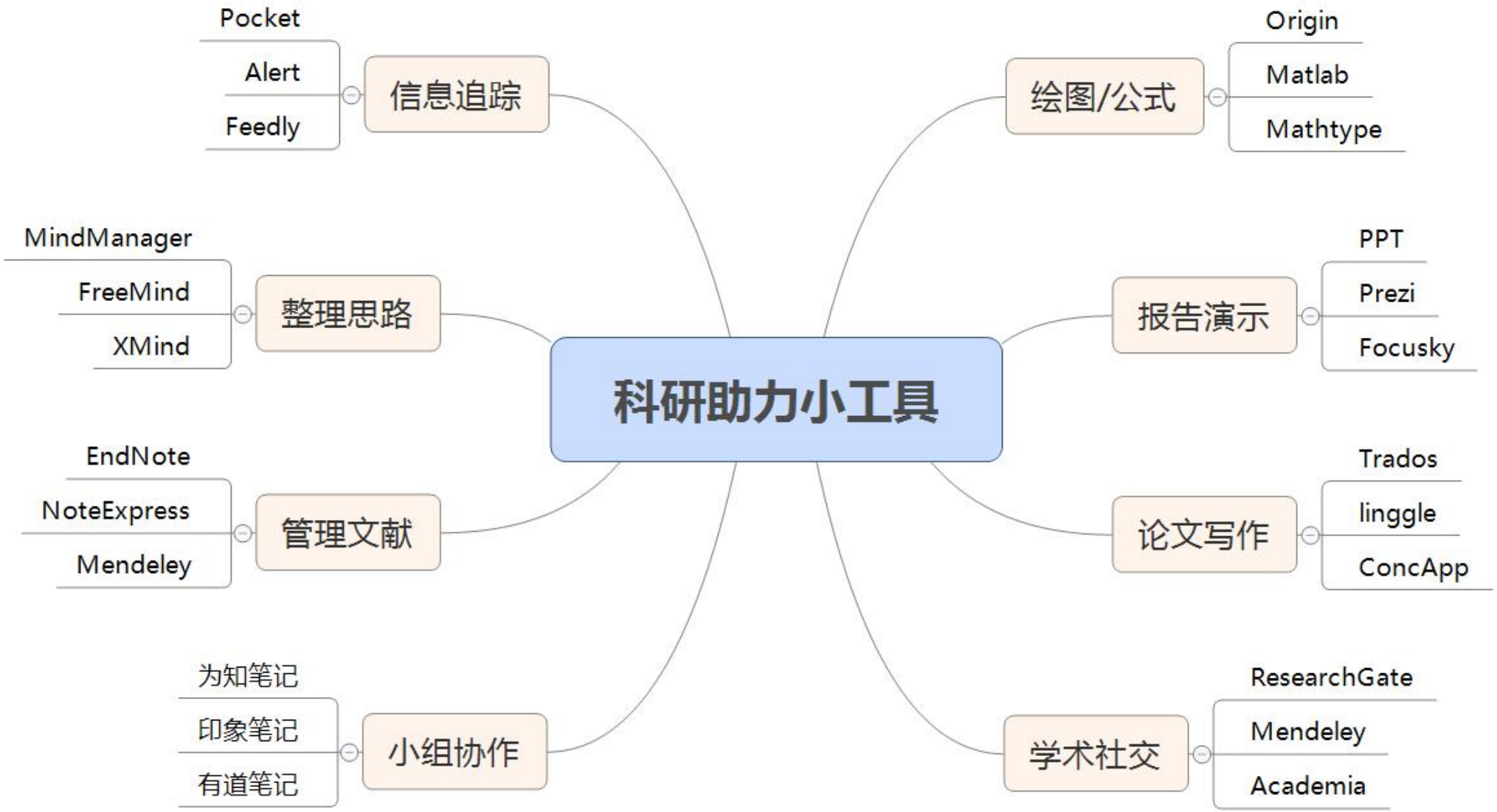
Cycle of Academic Research

SPRINGER NATURE

A model of the research workflow



Changing research workflows


科研助力小工具
信息追踪
Pocket
Alert
Feedly
整理思路
MindManager
FreeMind
XMind
管理文献
EndNote
NoteExpress
Mendeley
小组协作
为知笔记
印象笔记
有道笔记
绘图/公式
Origin
Matlab
Mathtype
报告演示
PPT
Prezi
Focusky
论文写作
Trados
linggle
ConcApp
学术社交
ResearchGate
Mendeley
Academia


The LaTeX Project
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.

Create exposure for your work

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

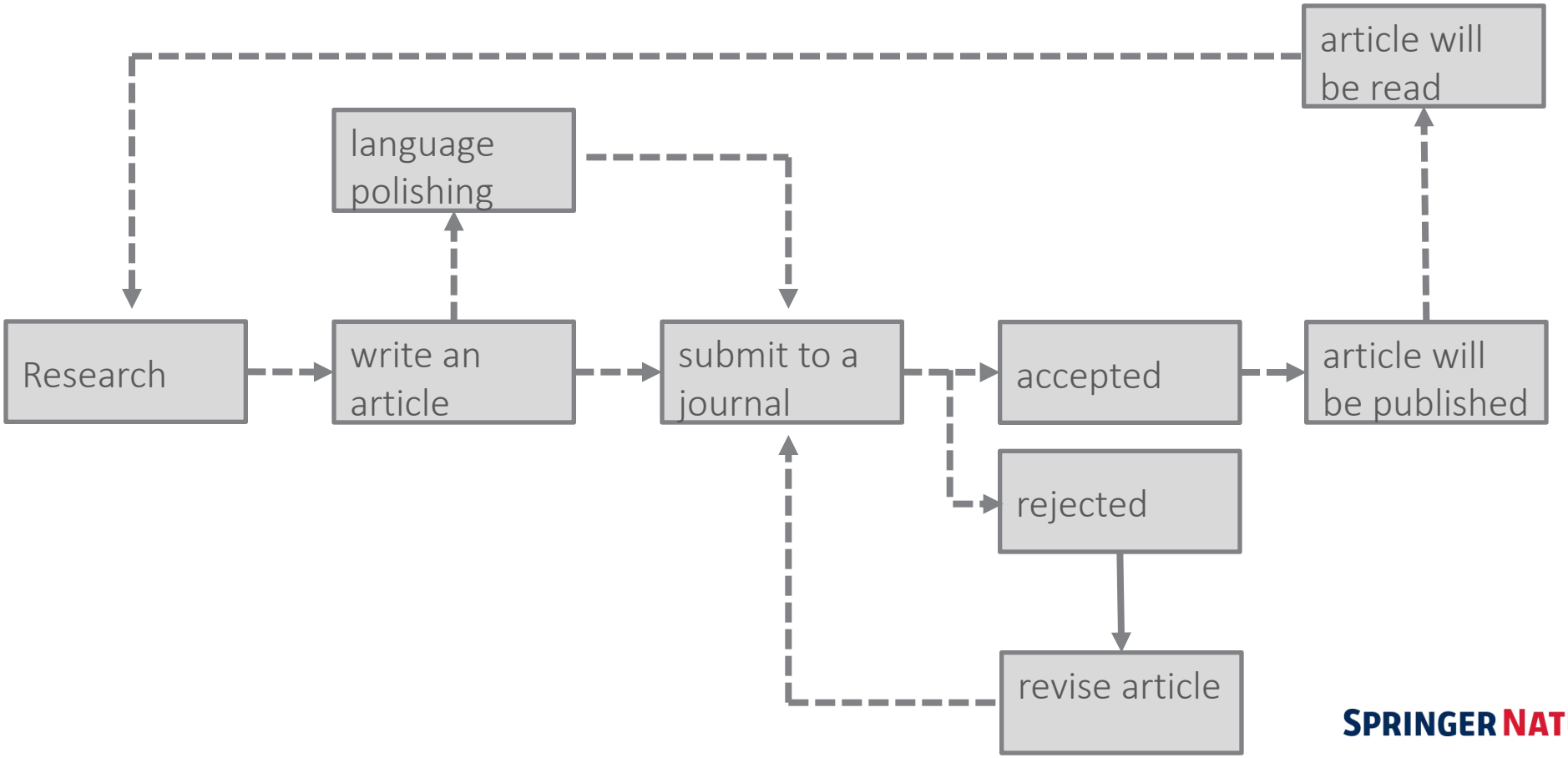
Get stats on your research

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

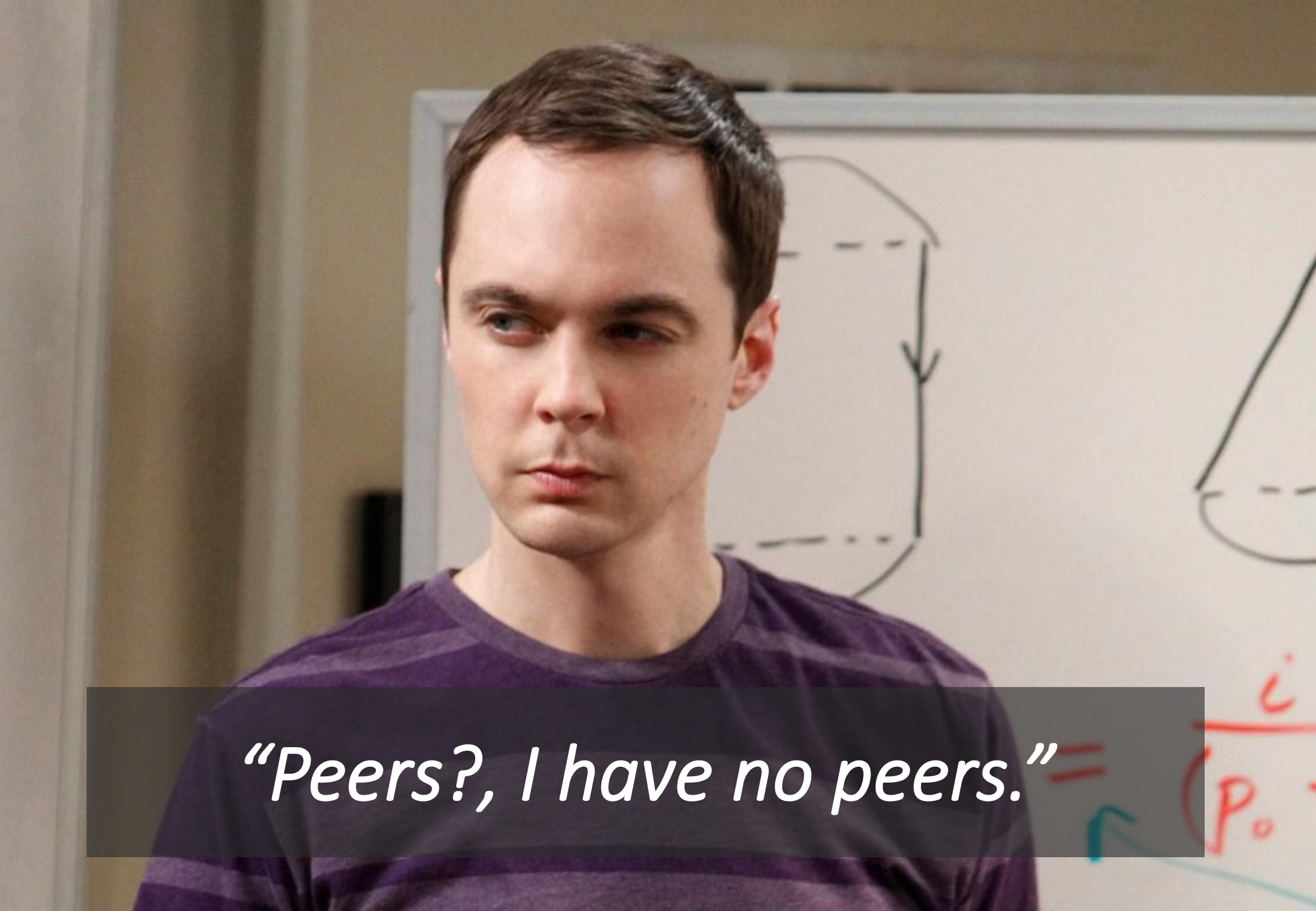
Connect with your colleagues

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

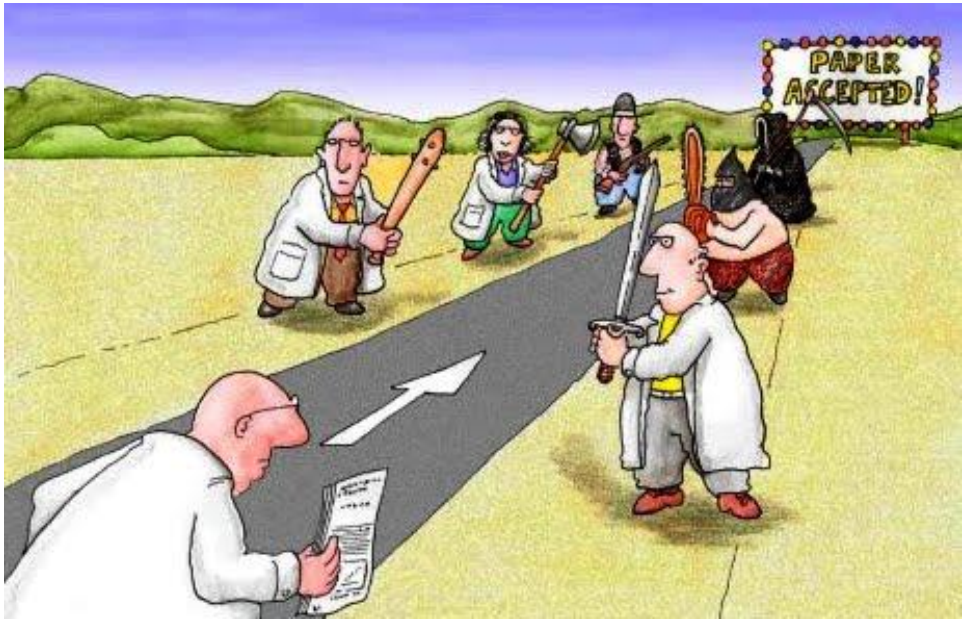
The Life of a Journal Article Submission



SPRINGER NATURE


“Peers?, I have no peers.”

Peer review

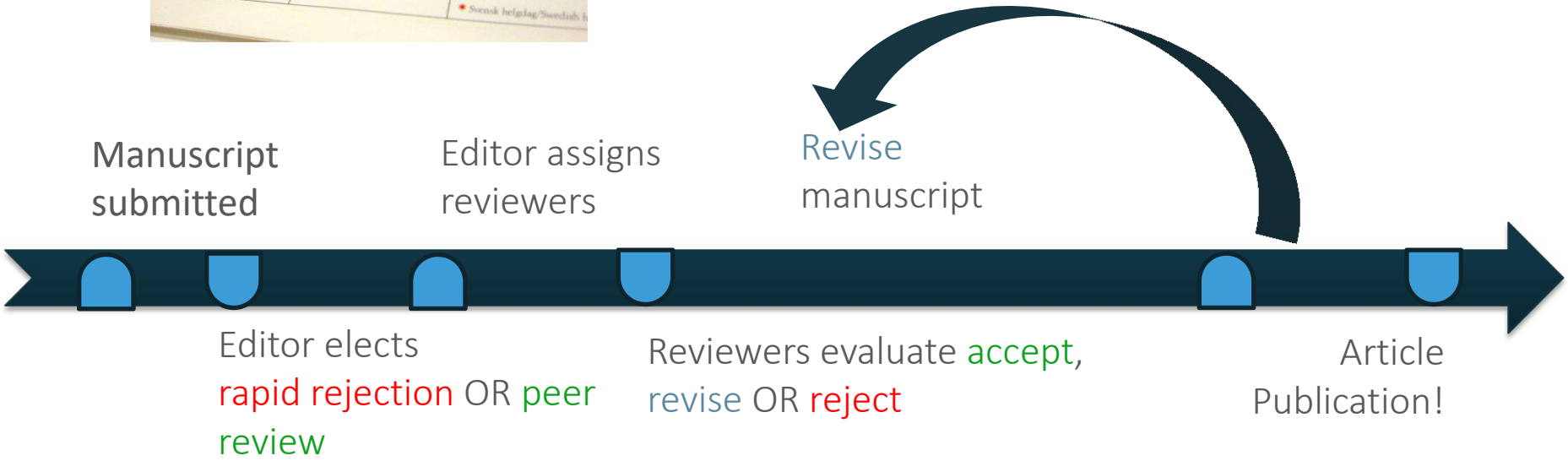


NATURE

Peer review

Journal publishing timelines can vary depending on editor and reviewer

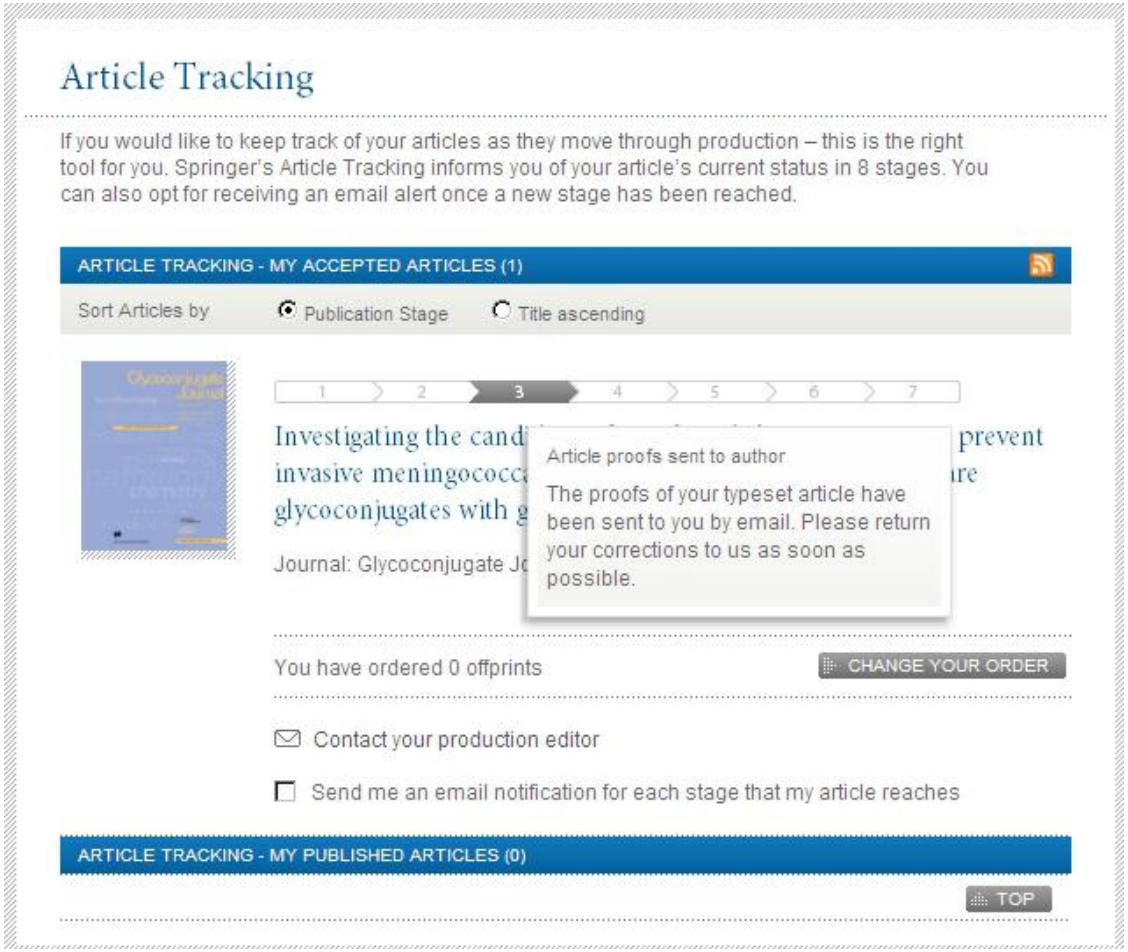
Submission to publication
3 months – 12 months



Peer review

Article Tracking – track the status of your article during production

receipt + MyPublication → type-setting → proofs to author → corrected proofs



- article published "OnlineFirst"
- journal issue online
- published in print

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

Home > Authors > 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 'My Publication' Process

Easily manage all administrative tasks of your article's production

Springer and Open Access

Choose from different publishing options

@AUTHORZONE

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

AuthorZone: Did you know? #AOCS members receive a 25% discount on all English-language books from Springer. http://ow.ly/4L9eC #AM2011, http://twitter.com/AuthorZone/statuses/650543218715688

AuthorZone: Want to give your Springer book or journal article a face? Upload a video about your research here http://ow.ly/4JYNN, http://twitter.com/AuthorZone/statuses/650380966091816 9

» 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

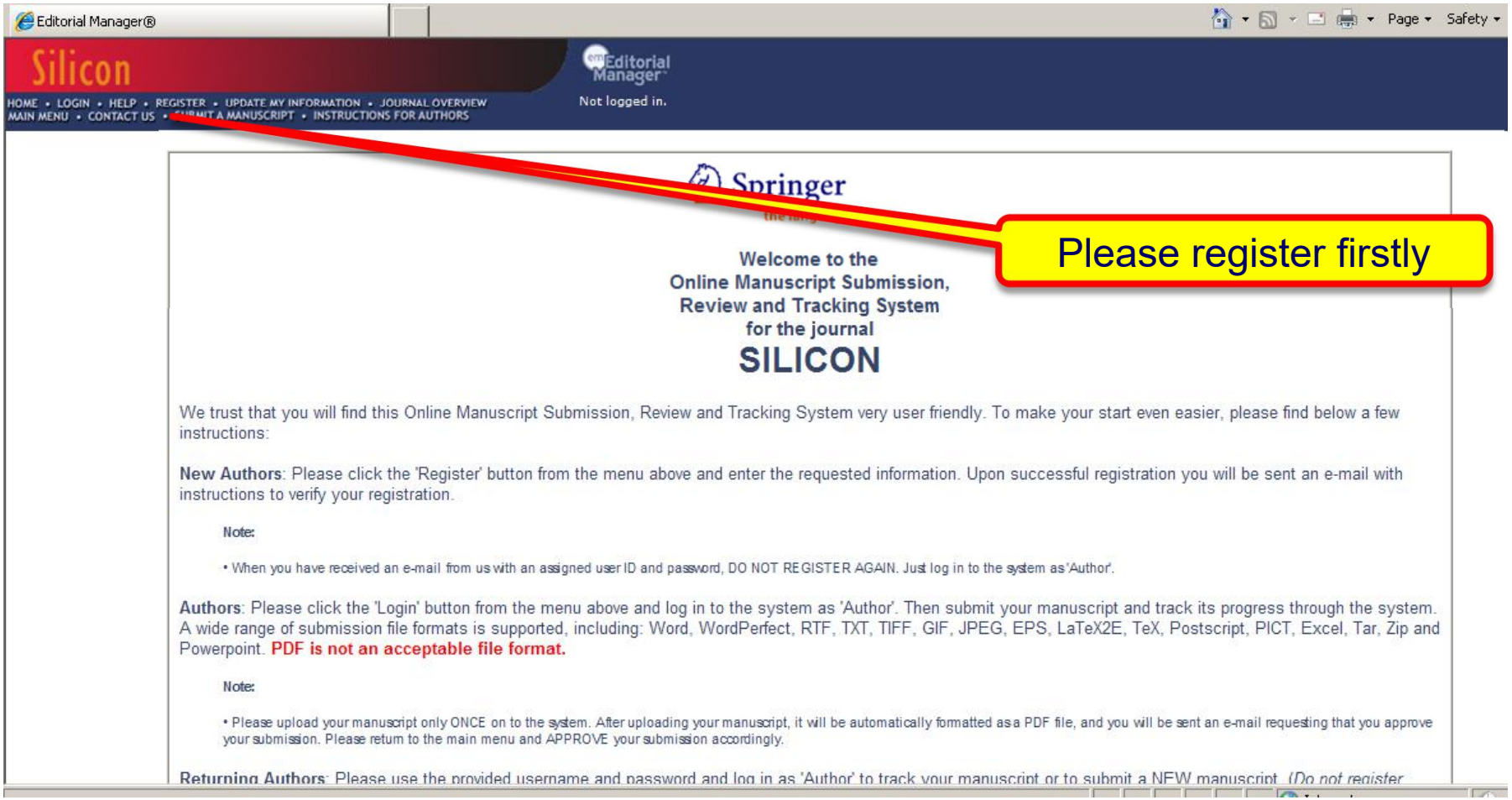
RE

Submitting

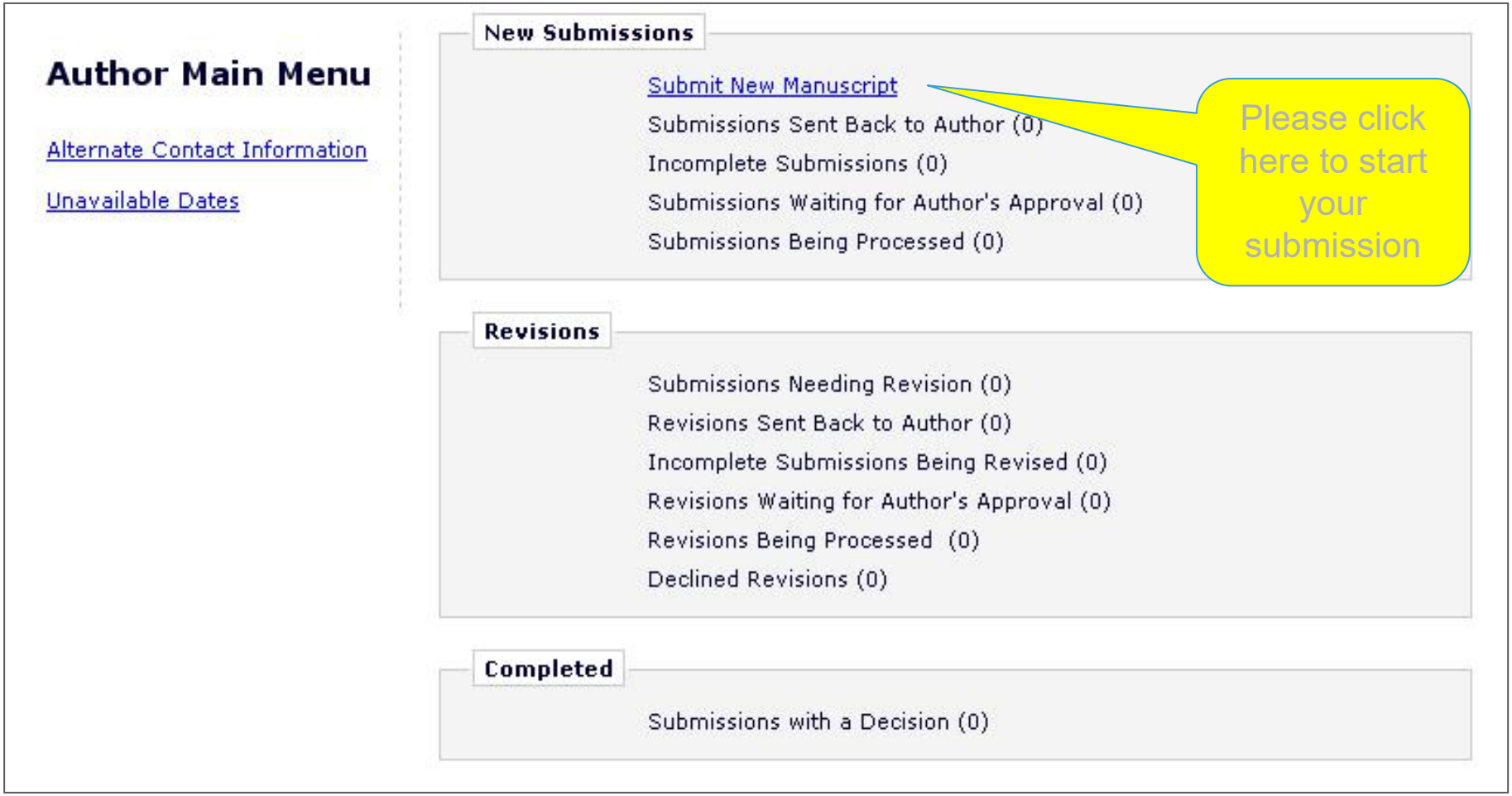
Electronic submission

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

Submitting


Editorial Manager®
Page
Safety
Silicon
Editorial Manager
Not logged in.
HOME • LOGIN • HELP • REGISTER • UPDATE MY INFORMATION • JOURNAL OVERVIEW
MAIN MENU • CONTACT US • SUBMIT A MANUSCRIPT • INSTRUCTIONS FOR AUTHORS
Springer
Please register firstly
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

- ✓ Select Article Type
- ✓ Enter Title
- Add/Edit/Remove Authors
- ✓ Select Section/Category
- ✓ Submit Abstract
- ✓ Enter Keywords
- Select Classifications
- ✓ Additional Information
- ✓ Enter Comments
- Suggest Reviewers
- Request Editor
- ➡ Attach Files

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.

Previous Next

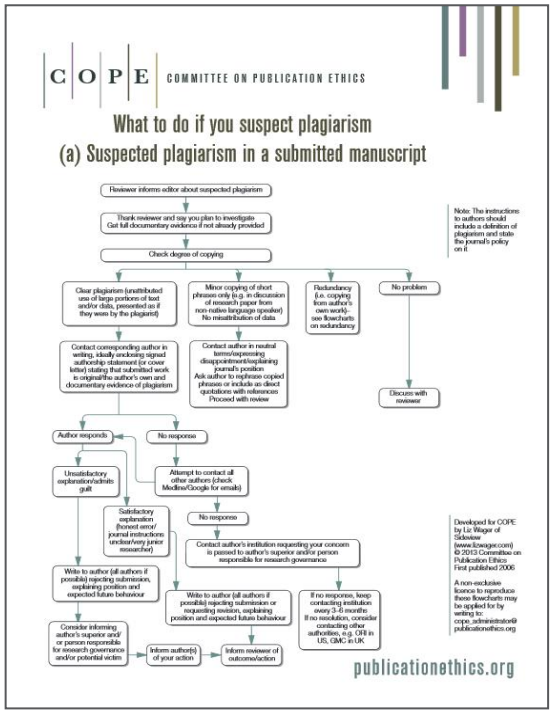
Successful

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



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。

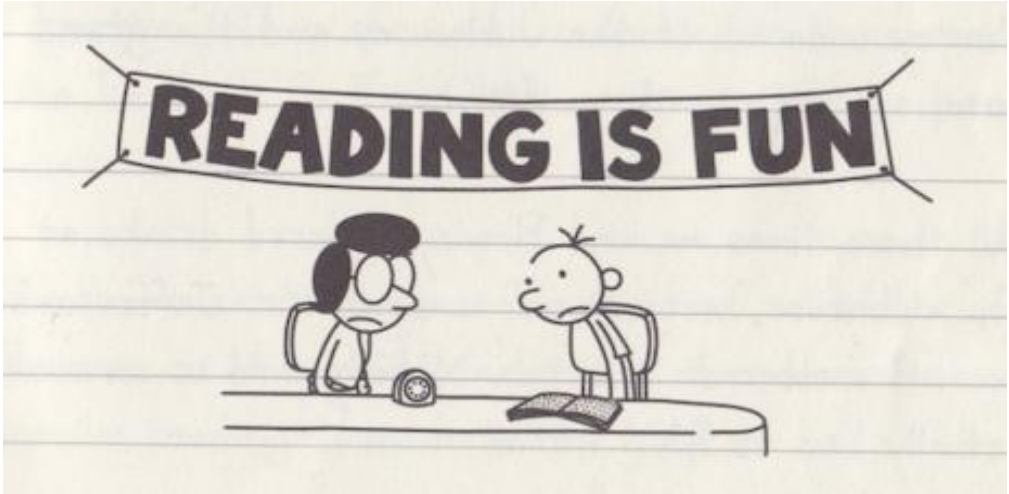
随着知识的积累，开始寻找一些令人困惑的现象，关于世界的未解之谜，新技术，亟需更佳解决方案的问题等。

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

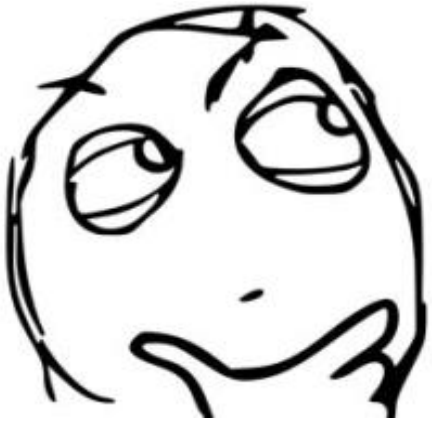
- Read many papers 多读文章

- 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

a

accurate

b

brief

c

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.

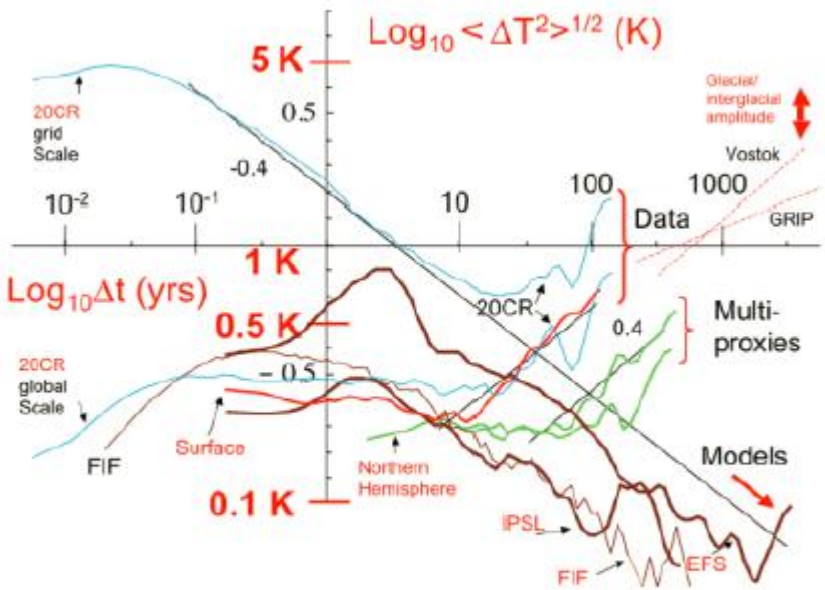
Be clear (清晰)

- 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 experimen

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

Springer电子期刊共收录多少种？共有几个子学科？请说出任三个子学科。

1700余种，11个学科。

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

What is the ABC of writing style ?

The ABC of writing style

a

accurate

b

brief

c

clear

编辑如何处理抄袭？

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