



SpringerLink/ Nature.com平台内容与  
功能介绍

客户发展经理 乔昆鹏

2018年3月

**SPRINGER NATURE**

# SpringerNature公司介绍

# 1.0

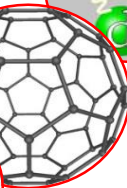
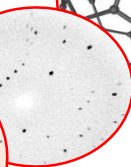
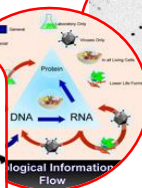
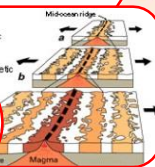
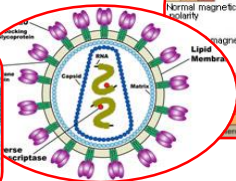
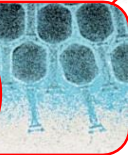
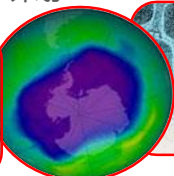


A WEEKLY ILLUSTRATED JOURNAL OF SCIENCE

"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

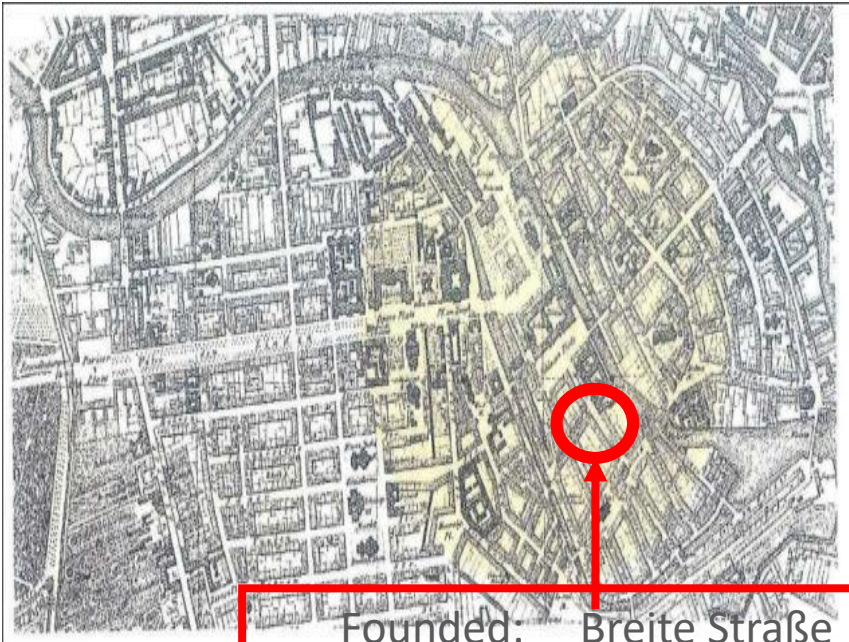
- 1880: 指纹用于刑侦技术
- 1896: 首次发现 X 射线
- 1903: 发现镭的放射性衰变
- 1925: 发现非洲类人猿——人类的起源
- 1927: 发现电子的波动性——电子显微镜的基石
- 1932: 破解原子由质子、中子和电子组成——原子能时代的开端
- 1953: 发现 DNA 的双螺旋结构——开启生物学的黄金时代
- 1958: 首次确定蛋白质结构——蛋白质组学
- 1961: 破解 DNA 到蛋白质的编码过程
- 1963: 利用地磁证据证明大陆板块漂移学说
- 1978: 合成第一个单克隆抗体——癌症的靶向治疗
- 1983: 发现艾滋病毒
- 1985: 在南极上空发现臭氧空洞——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



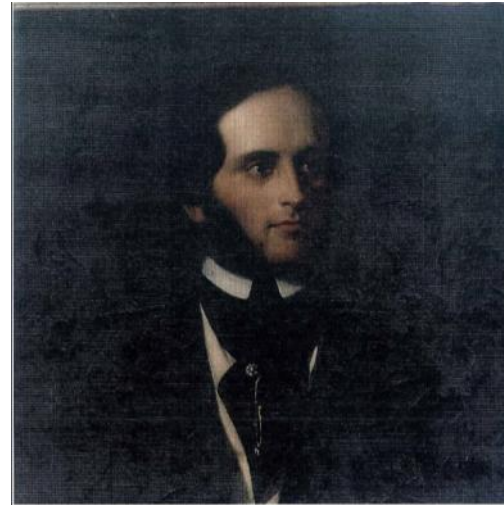
SPRINGER NATURE

# 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

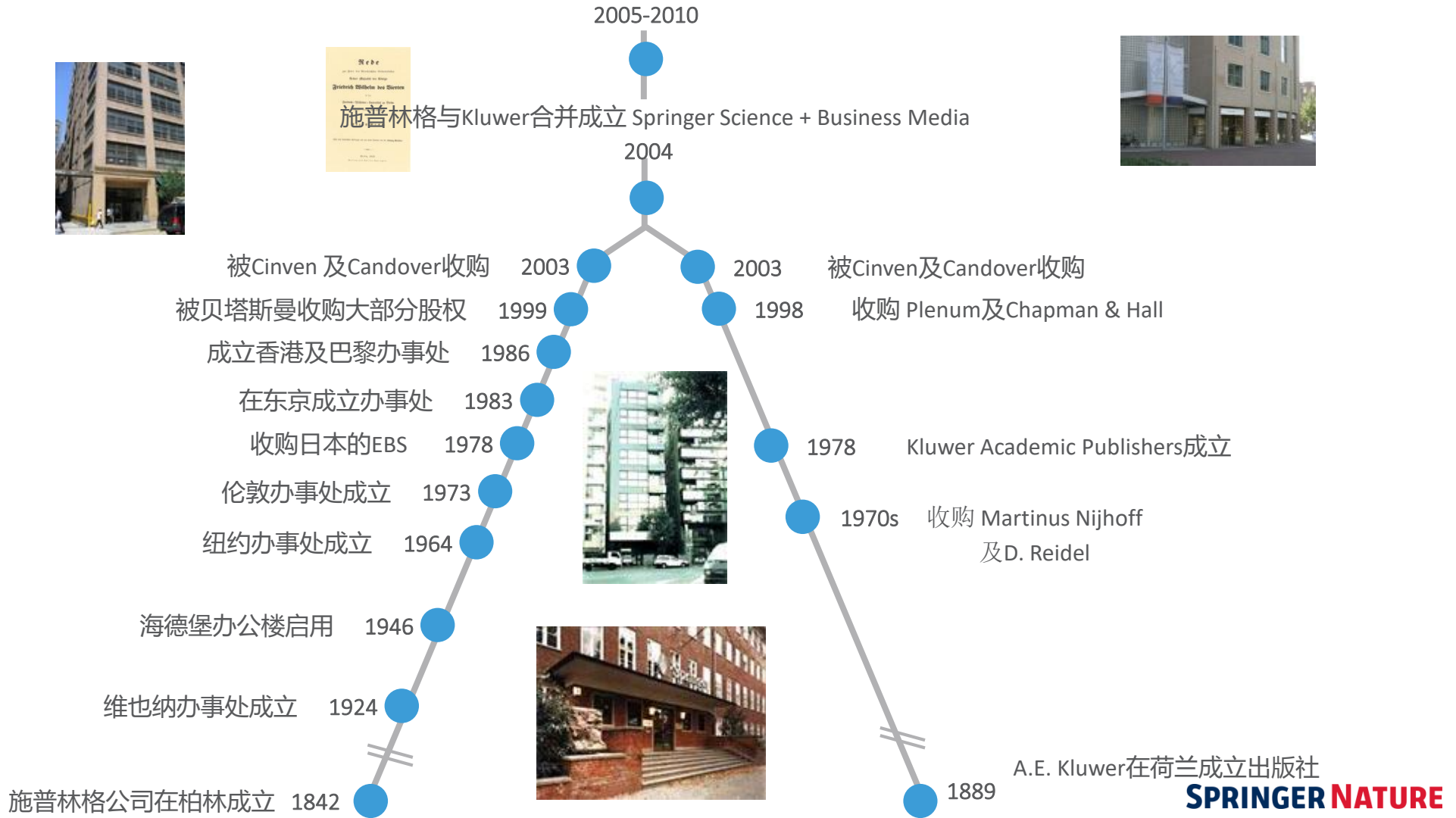


**SPRINGER NATURE**



# 历史沿革

Springer 收购: Current Medicine Group, Humana Press, Bohn Stafleu van Loghum 和 BioMed Central.



**SPRINGER NATURE**

# 我们的领先品牌

			
<p>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。</p>	<p>《自然》杂志 (<i>Nature</i>) 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。</p>	<p>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。</p>	
			
<p>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。</p>	<p>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。</p>	<p>《科学美国人》 (<i>Scientific American</i>) 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。</p>	<p>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。</p>

# 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

More than **13,000** employees worldwide

在全球拥有超过**13000**名员工

# 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	
<b>Science, Technology and Engineering (STE)</b> 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
<b>Medicine and Life Science</b> 生物医学专辑	Biomedical and Life Sciences	生物医学和生命科学
	Medicine	医学
<b>Social Science and Humanities</b> 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

Search

✕ New Search


[Home](#) • [Admin Dashboard](#) • [Contact Us](#)
 **Include Preview-Only content**
**5,174,028** Result(s)within **Article** ✕

## Refine Your Search

## Content Type

**Article** ✕

## Discipline

[see all](#)

Medicine & Public Health	1,237,719
Life Sciences	710,978
Chemistry	648,260
Physics	429,879
Biomedicine	395,409

## Subdiscipline

[see all](#)

Physical Chemistry	337,410
Biochemistry, general	314,957
Plant Sciences	269,760
Analytical Chemistry	238,527

Sort By

Newest First ▾

**Date Published**

Page

1

of 258,702

Your search also matched **995,707** [preview-only](#) results, e.g.

[Efficient flush-reload cache attack on scalar multiplication based signature algorithm](#)

» [Include preview-only content](#)

Article

**Foreword**Roger Fosdick in *Journal of Elasticity* (2017)

» [Download PDF](#) (495 KB) » [View Article](#)

Article

**Erratum to: Low-temperature creep in pure metals and alloys**M. E. Kassner, K. K. Smith, C. S. Campbell in *Journal of Materials Science* (2017)

» [Download PDF](#) (1052 KB) » [View Article](#)

# SpringerLink平台使用简介

# 3.0



# SpringerLink平台访问

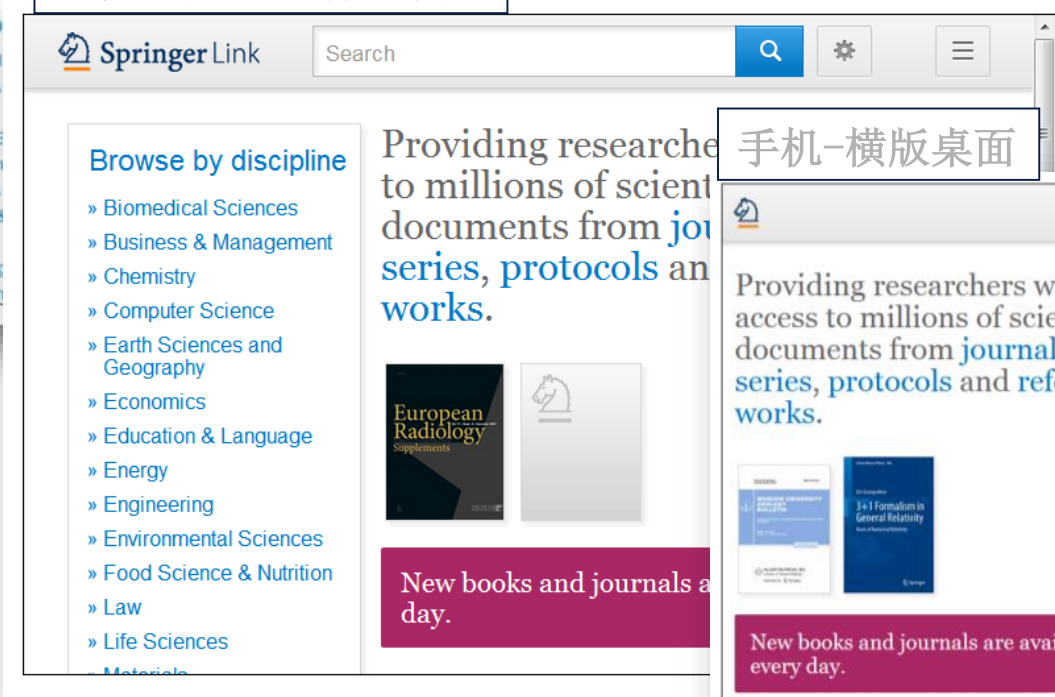
新平台适应各种移动终端、智能手机

平台访问网址: **link.springer.com** (IP控制)

普通电脑桌面



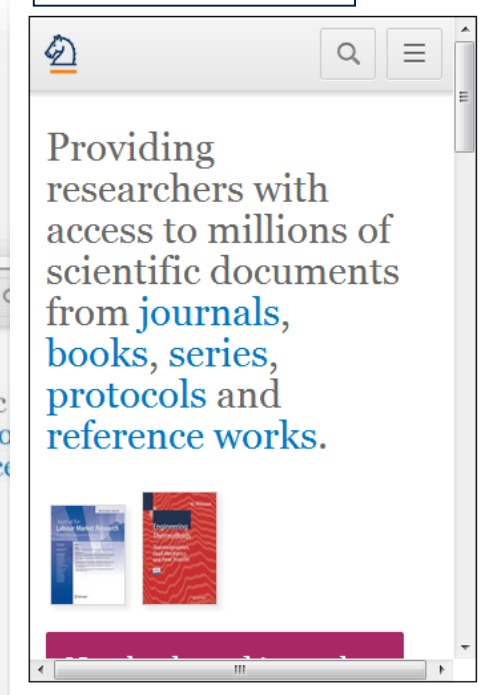
平板电脑（终端）桌面



手机-横版桌面



手机-竖版桌面



**SPRINGER NATURE**

# SpringerLink平台界面

Springer Link

Search

Sign up / Log in English Academic edition

Home • Contact Us

**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

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

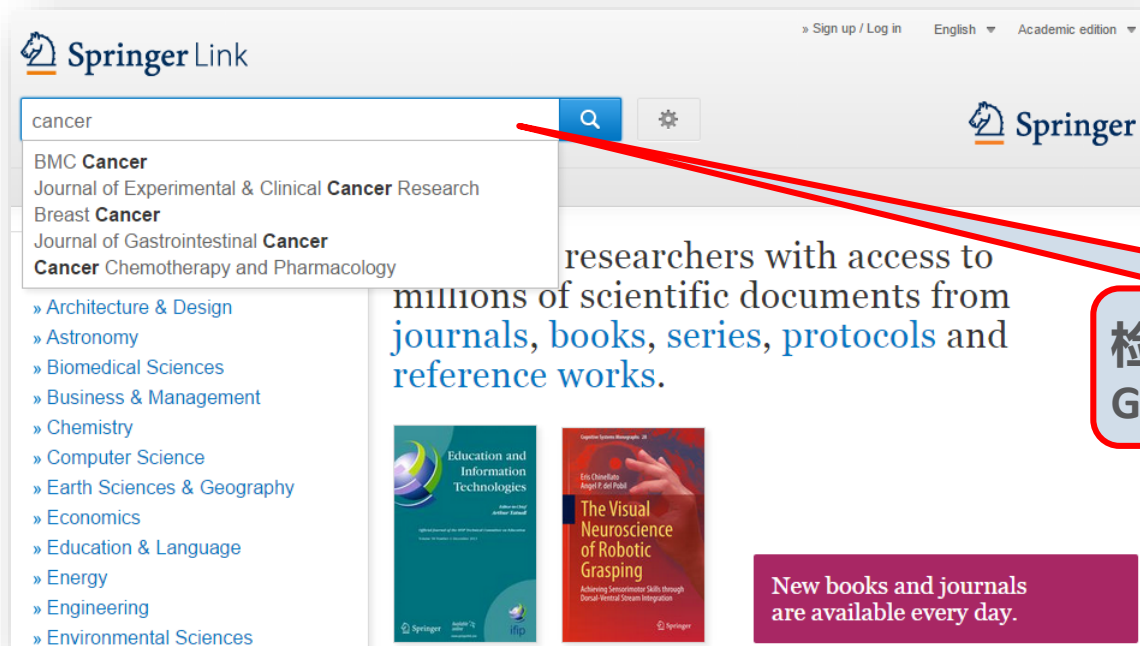
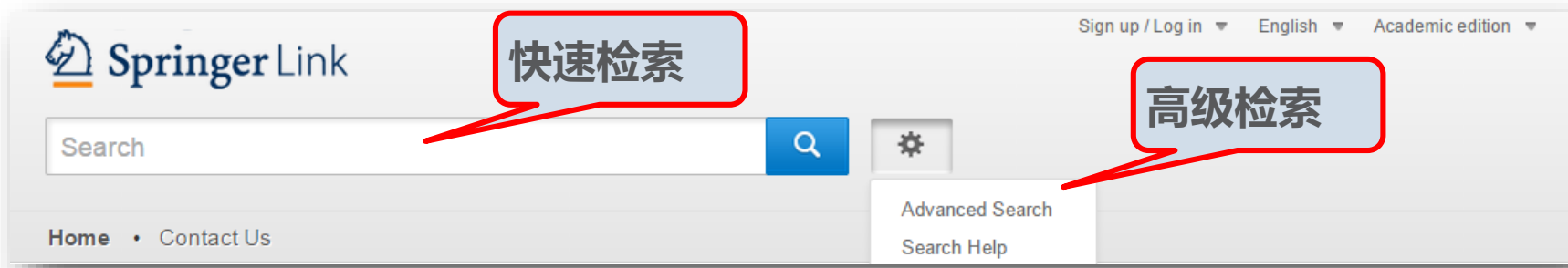
Featured Books

Browse 9,290,088 resources

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

**JRE**

# SpringerLink平台检索：快速检索



# SpringerLink平台检索：快速检索续

The image shows a screenshot of the SpringerLink search interface for the query 'cryptology'. The interface includes a search bar, navigation links, and a 'Refine Your Search' section with various filters. Annotations in red callouts point to specific features and results.

**Annotations:**

- 预览选项** (Preview options): Points to the 'Include Preview-Only content' checkbox.
- 内容类型** (Content type): Points to the 'Content Type' filter table.
- 学科** (Discipline): Points to the 'Discipline' filter table.
- 分支学科** (Subdiscipline): Points to the 'Subdiscipline' filter table.
- 语言** (Language): Points to the 'Language' filter table.
- 检索结果数量** (Search results count): Points to the '72,137 Result(s) for 'cryptology'' text.
- 排序：相关度，时间** (Sort by: Relevance, Date Published): Points to the 'Sort By' dropdown menu.
- 选择出版物时间** (Select publication time): Points to the date range filter 'between 1955 and 2011'.
- 检索结果导出一次最多导1000条** (Export search results, up to 1000 at a time): Points to the export icon.
- 直接下载** (Download directly): Points to the 'Download PDF' link for a result.

**Search Results Summary:**

72,137 Result(s) for 'cryptology'

Sort By: Relevance (selected), Newest First, Oldest First

Content Type Filter:

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

Discipline Filter:

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

Subdiscipline Filter:

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

Language Filter:

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

Search Results:

Reference Work Entry | In depth  
**Cryptology**  
Friedrich L. Bauer in *Encyclopedia of Cryptography and Security* (2005)  
» Download PDF (1243 KB)

Reference Work Entry | In depth  
**Cryptology**  
Friedrich L. Bauer in *Encyclopedia of Cryptology*  
» Download PDF (2864 KB)

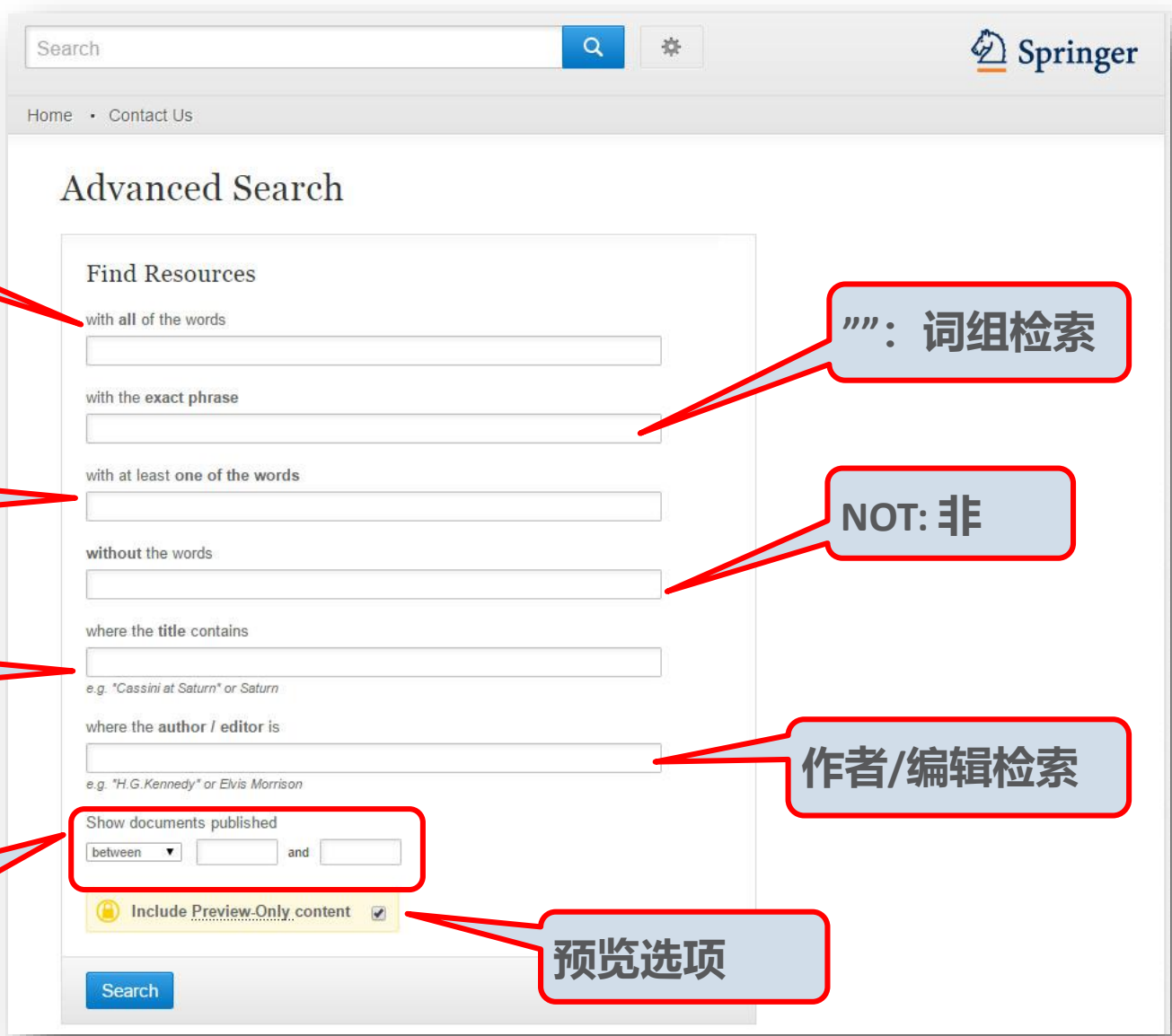
Book  
**Black-Box Models of Comput**  
Tibor Jager (2012)

Book  
**An Introduction to Cryptolog**  
Henk C. A. van Tilborg in *The Kluwer Internati* (1988)

72,108 Result(s) for 'cryptology'

Your search also matched 29 preview-only results, e.g. Les virus informatiques: théorie, pratique et applications  
» Include preview-only content

# SpringerLink平台检索：高级检索



AND: 与

OR: 或

标题检索

选择出版日期

"": 词组检索

NOT: 非

作者/编辑检索

预览选项



# 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”

The screenshot displays the SpringerLink 'Advanced Search' interface. At the top, the search query is entered: 'theory AND technology AND "quantum cryptography" AND (USA OR England) AND NOT (BB84)'. The search results show 648 results. The first result is a chapter titled 'An Update on Quantum Cryptography' by Charles H. Bennett and Gilles Brassard, published in 1985. The second result is a chapter titled 'Post-quantum Cryptography: Code-Based Signatures' by Pierre-Louis Cayrel and Mohammed Mezziani, published in 2010. The third result is a chapter titled '13 Quantum Cryptography' by Daniel Neuenschwander, published in 2004. The fourth result is a chapter titled 'On the Power of Two-Party Quantum Cryptography'.

**Advanced Search**

Find Resources

with all of the words

theory technology

SpringerLink

theory AND technology AND "quantum crypt

Springer

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 [WB3]. 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 Informati... (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 cryptanalyz...  
Daniel Neuenschwander 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

## 期刊主页介绍

The screenshot shows the SpringerLink homepage for the 'Journal of Cryptology'. The page includes a search bar at the top, a journal description, a list of latest articles, a table of journal statistics, an RSS subscription section, and a volume/issue search form. Red callout boxes with arrows point to these features, providing Chinese annotations.

**Callout 1:** 浏览所有卷期, 期刊内检索 (Browse all volumes and issues, search within the journal)

**Callout 2:** 期刊简要信息 (Journal summary information)

**Callout 3:** 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.)

**Callout 4:** RSS订阅和期刊更新注册提醒 (RSS subscription and journal update registration reminder)

**Callout 5:** 查找卷期 (Find volume/issue)

**Callout 6:** 最新发表的文章 (Latest published articles)

# SpringerLink-期刊的浏览

## 期刊主页-续

The image shows a screenshot of a SpringerLink journal page for 'Journal of Cryptology'. The page is annotated with red callout boxes and labels. The callout boxes highlight the 'Topics', 'Industry Sectors', and 'Additional Links' sections. The labels, which are blue rounded rectangles with white text, are: '所属主题分类' (Subject Classification) pointing to the Topics section, '所属行业分类' (Industry Classification) pointing to the Industry Sectors section, and '其他链接' (Other Links) pointing to the Additional Links section.

**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

## 浏览所有卷期

The screenshot shows the SpringerLink interface for the Journal of Cryptology. The page title is "Journal of Cryptology" with ISSN 0933-2790 (Print) and 1432-1378 (Online). Below the title, it says "All Volumes & Issues". There is a search bar at the top right. A red callout box points to the list of volumes, indicating that users can browse all volumes and click on links to view content from a specific year to a specific issue.

Impact Factor	Available
1.617	1989 - 2016

Volumes	Issues
29	111

Articles	Open Access
539	4 Articles

Volume 29 January 2016 - October 2016

October 2016, Issue 4, Pages 657-951

July 2016, Issue 3, Pages 491-656

April 2016, Issue 2, Pages 243-490

January 2016, Issue 1, Pages 1-241

Volume 28 January 2015 - October 2015

Volume 27 January 2014 - October 2014

Volume 26 January 2013 - October 2013

Volume 25 January 2012 - October 2012

Volume 24 January 2011 - October 2011

Volume 23 January 2010 - October 2010

Volume 22 January 2009 - October 2009

Volume 21 January 2008 - October 2008

Volume 20 January 2007 - October 2007

Volume 19 January 2006 - October 2006

Volume 18 January 2005 - September 2005

Volume 17 January 2004 - September 2004

Volume 16 January 2003 - September 2003

Volume 15 January 2002 - September 2002

Volume 14 January 2001 - September 2001

Volume 13 January 2000 - September 2000

Volume 12 January 1999 - September 1999

Volume 11 January 1998 - September 1998

Volume 10 March 1997 - December 1997

Volume 9 March 1996 - September 1996

Volume 8 March 1995 - December 1995

Volume 7 June 1994 - December 1994

Volume 6 March 1993 - September 1993

Volume 5 January 1992 - October 1992

Volume 4 January 1991 - January 1991

Volume 3 January 1990 - January 1991

Volume 2 January 1990 - February 1990

Volume 1 January 1988 - October 1989

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 Boullaguet, 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., Boullaguet, 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].

下载PDF

文章信息：标题，作者，摘要





论文快速定位

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](http://citeseer.ist.psu.edu/allouche94sur.html) 
2. E. Andreeva, C. Bouillaguet, P. Fouque, J.J. Hoch, J. Kelsey, A. Shamir, S. Zimmerman, Improved 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

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)

Search within this book

Download Book (PDF, 17286 KB)

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](#) <sup>(13)</sup>  
[Jonathan Katz](#) <sup>(14)</sup>

### 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

作者或编辑信息

分类信息

章节信息

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](#)<sup>(13)</sup>  
[Jonathan Katz](#)<sup>(14)</sup>

### Editor Affiliations

13. Impinj, Inc.  
 14. University of Maryland

### Authors

[Viet Tun](#)  
[Stefano](#)

### Author Affiliations

15. Department of Mathematics, University of California, Santa Barbara

### References (26)

- 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](#) » [Eprint](#)
- 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](#) » [Eprint](#)
- 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](#) » [Eprint](#)
- 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](#) » [Eprint](#)
- Bernstein, D.J.: How to stretch random functions: the security of protected counter sums. *J. Cryptol.* **12**(3), 185–192 (1999) » [MathSciNet](#) » [CrossRef](#) » [MATH](#) » [Eprint](#)
- Bernstein, D.J.: Break a dozen secret keys, get a million more for free (2015). » <http://blog.cryp.to/20151120-batchattacks.html>
- 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](#) » [Eprint](#)
- 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](#) » [Eprint](#)
- 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](#) » [Eprint](#)
- 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](#) » [Eprint](#)
- 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](#) » [Eprint](#)
- 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)
- Even, S., Mansour, Y.: A construction of a cipher from a single pseudorandom permutation. *J. Cryptol.* **10**(3), 151–162 (1997) » [MathSciNet](#) » [CrossRef](#) » [MATH](#) » [Eprint](#)
- 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](#) » [Eprint](#)
- 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](#) » [Eprint](#)
- Gaži, P., Maurer, U.: Cascade encryption revisited. In: Matsui, M. (ed.) ASIACRYPT 2009. LNCS, vol. 5912, pp. 37–51. Springer, Heidelberg (2009) » [CrossRef](#) » [Eprint](#)

# SpringerLink-图书章节

## 图书章节介绍

下载

The screenshot shows a SpringerLink page for a chapter. At the top, there are two download buttons: 'Download Book (PDF, 17286 KB)' and 'Download Chapter (918 KB)'. Below this, the chapter title is 'Key-Alternating Ciphers and Key-Length Extension: Exact Bounds and Multi-user Security' by Viet Tung Hoang and Stefano Tessaro. There are more download buttons for the book and chapter. The abstract discusses security bounds for key-alternating ciphers. On the right, there is a book cover image, 'Chapter Metrics' (Readers: 2, Downloads: 24), a 'MyCopy Softcover Edition' priced at 24.99, and a 'Buy Now' button. At the bottom, there are 'Reference tools' (Export citation, Add to Papers), 'Other actions' (About this Book, Reprints and Permissions), and 'Share' options (Facebook, Twitter, LinkedIn).

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

# Nature电子期刊访问平台

[www.nature.com](http://www.nature.com)

# Nature电子期刊访问平台


► [Publications A-Z index](#) ► [Browse by subject](#)

[Subscribe](#) [Register](#) [Submit Manuscript](#) [My account](#)  
[Login](#) [Cart](#)

# nature.com

[Advanced search](#)

21 April 2016



MACMILLAN AUSTRALIA

### Warming brings better weather to the US — for now


The weather experienced by the majority of the US population has become more pleasant over the past 40 years, owing to climate change, a *Nature* paper reports.

#### Latest news

- [Monkey kingdom](#)
- [Peer review: Troubled from the start](#)
- [UK government pulls back from rule 'gagging' researchers](#)

► [More news from Nature](#)

### Nature journal



ENDLESS SUMMER

[► Contents 21 Apr 16](#)  
[► Podcasts](#) ► [Videos](#)

### Inside nature.com

- [Publications A-Z](#)  
browse the nature.com publications index
- [Nature.com regions](#)  
► [Asia-Pacific](#)  
► [Nature India](#)  
► [Nature Middle East](#)  
[see more](#) ►
- [naturejobs.com](#)  
► [Post a Science job now!](#)
- [Launchpad](#)  
► [Mobile](#)  
► [Projects](#)  
[see more](#) ►
- [Multimedia](#)  
► [Nature Videos](#)  
► [Nature Podcast](#)  
► [More podcasts](#)  
► [Webcasts](#)

### Latest research

- [The collection of MicroED data for macromolecular crystallography](#)  
**FREE**  
*Nature Protocols*
- [Pharmacogenomics in diabetes mellitus: insights into drug action and drug discovery](#)

### Explore nature.com

- [Introducing Nature Index](#)
- [Nature Outlooks](#)

查询方式:  
简单检索  
高级检索  
字顺浏览  
学科浏览

# Nature电子期刊访问平台—浏览

The screenshot displays the Nature.com A-Z index page. At the top, there is a dark red header with the text "nature.com A-Z index" and links for "Login" and "Cart". Below the header is a search bar with a "go" button and a link to "Advanced search". The main content area is divided into two columns: "Publications A - M" and "Publications N - Z". The "Publications A - M" column lists journals such as "Acta Pharmacologica Sinica" and "American Journal of Gastroenterology Supplements". The "Publications N - Z" column lists journals such as "Nature", "Nature Arabic Edition", "Nature Astronomy", "Nature Biomedical Engineering", "Nature Biotechnology", and "Nature Cell Biology". To the right of these columns is a section for "RSS Web Feeds" and "Gateways and databases", which includes links to "Application Notes", "Bioentrepreneur", "BioPharma Dealmakers", and "Nature Index". A "CLOSE ^" button is visible on the left side of the page. At the bottom, there is a navigation bar with the "nature.com" logo and a "Login / Sign up" button. The footer contains a grid of links for "Journals A-Z", "All Subjects", "nature.com", "Subscriptions", "Authors & Referees", "Librarians", "Advertisers", "Press", "About", "Nature", "Nature Communications", "Nature Protocols", "Review journals", "Scientific Reports", "View all »", "Biological Sciences", "Earth & Environmental Sciences", "Health Sciences", "Physical Sciences", "Scientific Community & Society", and "View all »".



# Nature电子期刊访问平台—检索

## Advanced Search

Find Articles...

that contain

where the li

where the

Refine your results by...

publication **date**

Year ▼ to Year ▼

**journal(s)**

Find a Journal



**volume**

**start page / article no.**

Search

# Latest News

## Latest News

News | 07 November 2016

### Illegal ivory mostly from recent elephant killings

Carbon-dating study suggests governments are not fuelling trade by selling off old tusks.

News | 03 November 2016

### Scientists can publish their best work at any age

New equation also suggests way to predict a researcher's potential to produce top work.

News | 04 November 2016

### Hard work, little reward: *Nature* readers reveal working hours and research challenges

In an online poll, almost two-thirds of readers say they have considered quitting research.

News | 02 November 2016

### Ant genomes rewrite history of Panama land bridge

Genetic analysis suggests connection between the Americas emerged millions of years earlier than previously thought.

News | 03 November 2016

### Tracker flags up failures to report clinical trials

Computerized search of trial registry lists worst offenders.

News | 02 November 2016

### Axion alert! Exotic-particle detector may miss out on dark matter

Supercomputer calculation suggests hypothesized particle may be heavier than thought.

[All News >>](#)

# Latest Research Highlights

## Latest Research Highlights

Research Highlights | 07 November 2016

### Bacterial pathogenesis: *Rickettsia* releases the tension



This study shows that the bacterial effector Sca4 promotes intercellular spread of the obligate intracellular pathogen *Rickettsia parkeri*... [show more](#)

Ursula Hofer

*Nature Reviews Microbiology*

Research Highlights | 07 November 2016

### Archaeal biology: Masters of methane



Three new studies investigate the metabolic pathways that anaerobic archaea use to produce hydrocarbons such as methane and butane.

Ursula Hofer

*Nature Reviews Microbiology*

Research Highlights | 07 November 2016

### Microbiome: Complexity at the sub-genus level

Andrea Du Toit

*Nature Reviews Microbiology*

Research Highlights | 07 November 2016

### Acute kidney injury: Loss of PKC- $\epsilon$ protects against IRI

Andrea Aguilar

*Nature Reviews Nephrology*

Research Highlights | 07 November 2016

### Viral infection: Rabies virus causes stress

Andrea Du Toit

*Nature Reviews Microbiology*

Research Highlights | 07 November 2016

### Fungal biology: A key regulator of secondary metabolites

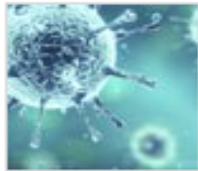
Andrea Du Toit

*Nature Reviews Microbiology*

[All Research Highlights >>](#)

# 按学科进行浏览

## Browse by subject



### Biological sciences

Biological sciences encompasses all the divisions of natural sciences examining various aspects of vital processes. The concept includes... [show more](#)

[Biotechnology](#)
[Genetics](#)
[Immunology](#)
[Neuroscience](#)


### Earth and environmental sciences

Earth and environmental sciences cover all aspects of Earth and planetary sciences, and broadly encompasses solid Earth processes, surface... [show more](#)

[Climate sciences](#)
[Ecology](#)
[Environmental sciences](#)
[Solid Earth sciences](#)


### Health sciences

The health sciences study all aspects of health, disease and healthcare. This field of study aims to develop knowledge, interventions and... [show more](#)

[Endocrinology](#)
[Gastroenterology](#)
[Neurology](#)
[Oncology](#)

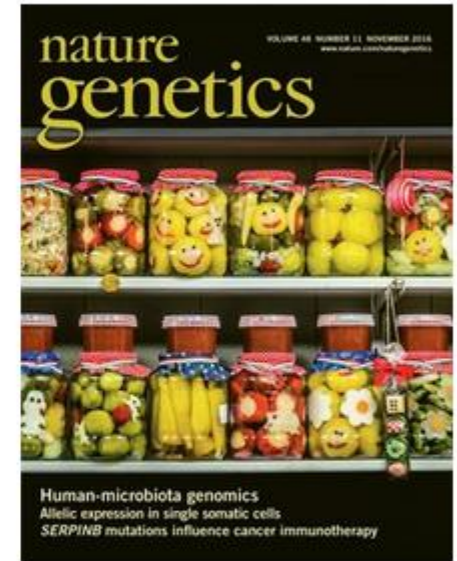
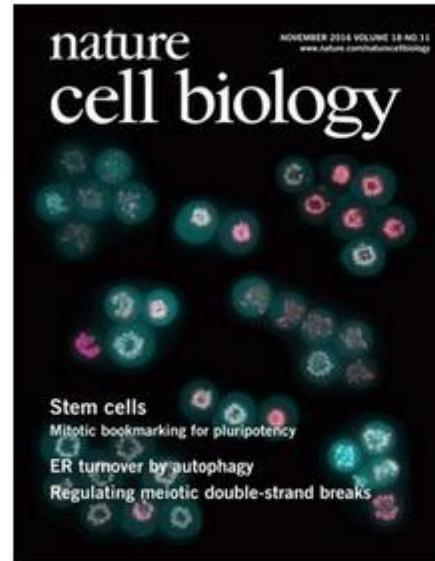

### Physical sciences

Physical sciences are those academic disciplines that aim to uncover the underlying laws of nature - often written in the language of... [show more](#)

[Chemistry](#)
[Materials science](#)
[Nanoscience and technology](#)
[Physics](#)
[All subjects >>](#)

# 按出版物进行浏览

## Publications



[All publications >>](#)


# Go beyond the article

nature.com 不仅仅提供文字上的内容,每星期发放的多媒体内容,让你比以往任何时候都更接近科学。




nature.com podcasts Login

Search  go [Advanced search](#)






### Nature Podcast




[nature podcast](#)

This week, we examine Egyptian archaeology after the Arab Spring, hear how the immune system helps keep us warm, and dig out the missing elements from the Earth's innards. Plus, the best of the rest from this week's *Nature*.








Bio International Convention




AJH Podcast



Bio International Convention



BrainPod



Cancer Podcast

Nature Podcasts  
 可以下载免费的音频节目，  
 这里包含有自然科学及系列刊  
 的每周重点

可以免费观看在线的串流影片  
 及同时可以与科学家们分析  
 和讨论分享他们的发现，  
 (请注意最新的串流影片  
 存放在Youtube网站).

nature.com [Publications A-Z index](#) [Browse by subject](#)

[Subscribe](#) [Register](#) [Submit manuscript](#) [My account](#)

nature Login

International weekly journal of science

Search  go [Advanced search](#)

Journal home > [Videoarchive index](#) > [Supergene controls butterfly mimicry](#)

Supergene controls butterfly mimicry - by Natur... naturevideo





**FOR AUTHORS AND REFEREES**[Guide to Authors](#)[Guide to Referees](#)[Editorial policies](#)[Language editing](#)[Scientific editing](#)[Reprints & permissions](#)**FOR READERS**[Journals A-Z](#)[Subject Pages](#)[Protocol Exchange](#)[Blogs](#)[Podcasts](#)[Webcasts](#)[Subscriptions](#)[Mobile apps](#)[RSS](#)**FOR LIBRARIANS**[Account administration](#)[Site licenses](#)[Catalogs](#)[Print subscriptions](#)[Pay per view](#)[Open access](#)[Promotion tools](#)[Public interfaces](#)[User guides](#)[Library relations](#)[Publisher collaborations](#)**CAREERS AND EVENTS**[Natureconferences](#)[Natureevents](#)[Naturejobs.com](#)

What

Description or keyword

Where

Country, city or postal code

[Find Jobs](#)

Post a job

Reach thousands of  
science jobseekers

Upload your CV

Apply for science jobs  
quickly and easily[Jobs](#)[News and Blog](#)[Career Expo](#)[For employers](#)Popular Science Jobs: [Biomedical Science](#) | [Environmental Science](#) | [Science Technician](#) | [Food Science](#) | [Forensic Science](#)

## Jobs of the Week

FEATURED

### Positions at Center for Precision Medicine, The First Affiliated Hospital of Wenzhou Medical University

The First Affiliated Hospital of Wenzhou Medical University · Wenzhou, China · 8 days ago

Bioinformaticians, Laboratory Manager and Research Assistants, Center for Precision Medicine, The First Affiliated Hospital of Wenzhou Medical University The First Affiliated Hospital of Wenzhou Medical University was founded in 1919. The hospital is located in the beautiful coastal city of Wenz...



FEATURED

### Excellent scholars, East China University of Science and Technology (ECUST)

East China University of Science and Technology (ECUST) · Shanghai, China · 13 days ago

East China University of Science and Technology (ECUST) is located in Shanghai, a cosmopolitan



## Featured Employers

**TECHNISCHE  
UNIVERSITÄT  
DRESDEN****TU Dresden**TU Dresden, excellence comes  
from the heart**華東理工大學****East China University of  
Science and ...****同濟大學**

TONGJI UNIVERSITY

**Tongji University**Institute for Advanced Study  
of Tongji University**LUDWIG-  
MAXIMILIANS-  
UNIVERSITÄT  
MÜNCHEN****Ludwig-Maximilians-  
Universität (LMU) ...**Ludwig-Maximilians-Universität  
(LMU) in Munich**Advanced Study (IAS) of**

# natureconferences

 Search  [go](#) [Advanced search](#)

## About Natureconferences

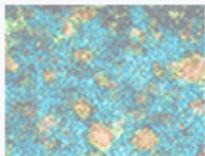
Nature Publishing Group is distinguished by its scientific excellence, breadth of coverage, timeliness of topics, and commitment to clear scientific communication. In keeping with this tradition, *Natureconferences* are aimed at the international scientific community, with the goal of fostering and facilitating communication and collaboration between scientists.

We are proud to present these unique events (some in concert with specific institutions) that will become essential resources for the researchers of today and tomorrow.

For more information on upcoming events from *Natureconferences*, [sign up](#) to receive our monthly email alert

Follow us on Twitter: [@NatureConf](#)

## Calendar 2017



### **Nature Conference on Environmental and Human Microbiomes: Drivers of Future Sustainability**

**February 12-17, 2017**

Venue: Nanyang Executive Centre, Singapore

Organizers: Staffan Normark (Karolinska Institutet, Sweden), Yehuda Cohen (Singapore Centre for Environmental Life Sciences Engineering (SCELSE), Singapore), Alexander Zehnder (Nanyang Technological University, Singapore), Staffan Kjellberg (Singapore Centre for Environmental Life Sciences Engineering (SCELSE), Singapore), Nico Fanget (Nature Research, UK)

# nature events directory

[home](#)
[event seekers](#)
[event organizers](#)
[calendar](#)
[about us](#)


## Search science events




Science  
EVENTS of the week

### [SPIE LASE 2017 - Part of SPIE Photonics West](#)

28th January - 2nd February 2017

Moscone Center, 747 Howard St, San Francisco, United States

### [11th Annual Primary Care Spring Conference Session I](#)

27th March 2017 at 08:00 - 31st March 2017 at 12:15 (GMT-05:00) Eastern Time (US & Canada)

Hammock Beach Resort, 200 Ocean Crest Dr, Palm Coast, United States

### [The Multi-Channel Patient Engagement Course](#)

28th - 29th September 2017  
TBC, London, United Kingdom

### [The Pharma Business Development Course - An Overview Course](#)

12th - 13th December 2017  
TBC, London, United Kingdom

## Events by Date



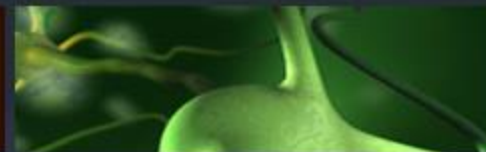
- ❖ November 2016 (282 events)
- ❖ December 2016 (188 events)
- ❖ January 2017 (104 events)
- ❖ February 2017 (135 events)
- ❖ March 2017 (150 events)
- ❖ April 2017 (126 events)
- ❖ Search more dates

## Events by Country



- ❖ United States (165 events)
- ❖ United Kingdom (132 events)
- ❖ China (99 events)
- ❖ Germany (67 events)
- ❖ United Arab Emirates (56 events)
- ❖ Greece (50 events)
- ❖ Search more countries

## Events by Area



- ❖ Life Sciences (598 events)
- ❖ Others (262 events)
- ❖ Engineering (244 events)
- ❖ Chemical Sciences (93 events)
- ❖ Earth and Environ.Sciences (61 events)
- ❖ Physical Sciences (42 events)
- ❖ Search more areas

# 期刊论文投稿简介

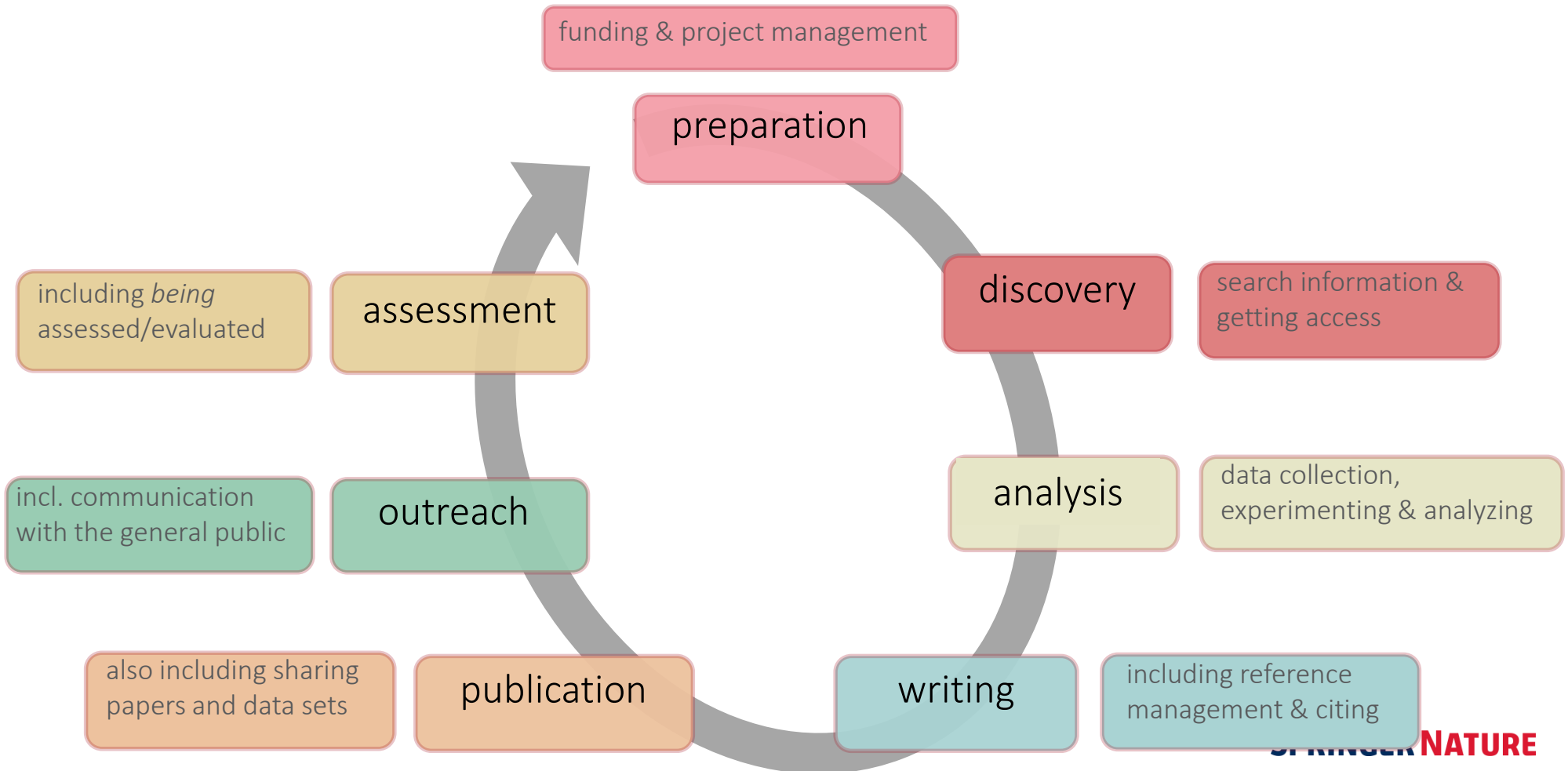
# 4.0



# Cycle of Academic Research



# A model of the research workflow





# Changing research workflows



# 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。

# Before you begin

i.e. : Reading Resources from Springer

SpringerLink

Search

Home - Contact Us

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

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.

Recent Activity

What's being read within your organisation

Case Report  
Repeated occurrence of slow flow phenomenon during and late after sinusitis-eluting stent implantation  
Heart and Vessels, January 2014  
1 min ago

Original Article  
Pulse wave analysis of the aortic pressure waveform in patients with vasovagal syncope  
5 mins ago

Database

Springer

LIFE SCIENCES

Theoretical and Applied Genetics

Visit us at [springer.com](http://springer.com)

Free Trial Access to Top Downloaded Articles

Theoretical and Applied Genetics invites you to read a selection of top downloaded articles for free.

- Determination of genetic structure of germplasm collections: are traditional hierarchical clustering methods appropriate for molecular marker data? - T. L. Odong, J. van Heerwaarden, J. Jansen, T. J. L. van Hintum, and F. A. van Eeuwijk
- A genome-wide genetic map of NLR disease resistance loci in potato - E. Bakker, T. Born, P. Prins, et al.
- A high-density microsatellite consensus map for bread wheat (*Triticum aestivum* L.) - D. J. Somers, P. Isaac, and K. Edwards
- High-throughput SNP discovery and genotyping in durum wheat (*Triticum durum* Desf.) - D. Trebbi, M. Maccaferri, P. de Heer, et al.
- Genome based prediction of testcross value in

Impact Factor: 3.264

Theoretical and Applied Genetics

Editor-in-Chief:  
Albrecht E. Melchinger,  
Stuttgart, Germany

Reviews Editor:  
Rajeev K. Varshney,  
Greater Hyderabad, India

E-newsletter

SpringerLink

New Issue Alert

Wednesday, September 7

Dear Leo Jiang,

We are pleased to deliver your requested table of contents alert for *Heilberufe*. Good news: now you will find quick links to the full text of the article in PDF or HTML. Choose your preferred format and access the article with only one click!

Volume 63 Number 9 is now available on [SpringerLink](http://SpringerLink)

Sign up for **SpringerAlerts** Register for Springer's email services providing you with info on the latest books in your field. [More!](#)

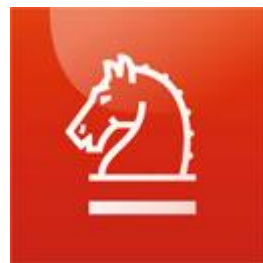
In this issue:

Pflege Praxis  
Nahrungskarenz nach Darm-OP ist obsolet  
Jana Andr a & Arved Weimann

[Abstract](#) [Full text HTML](#) [Full text PDF](#)

Pflege Praxis

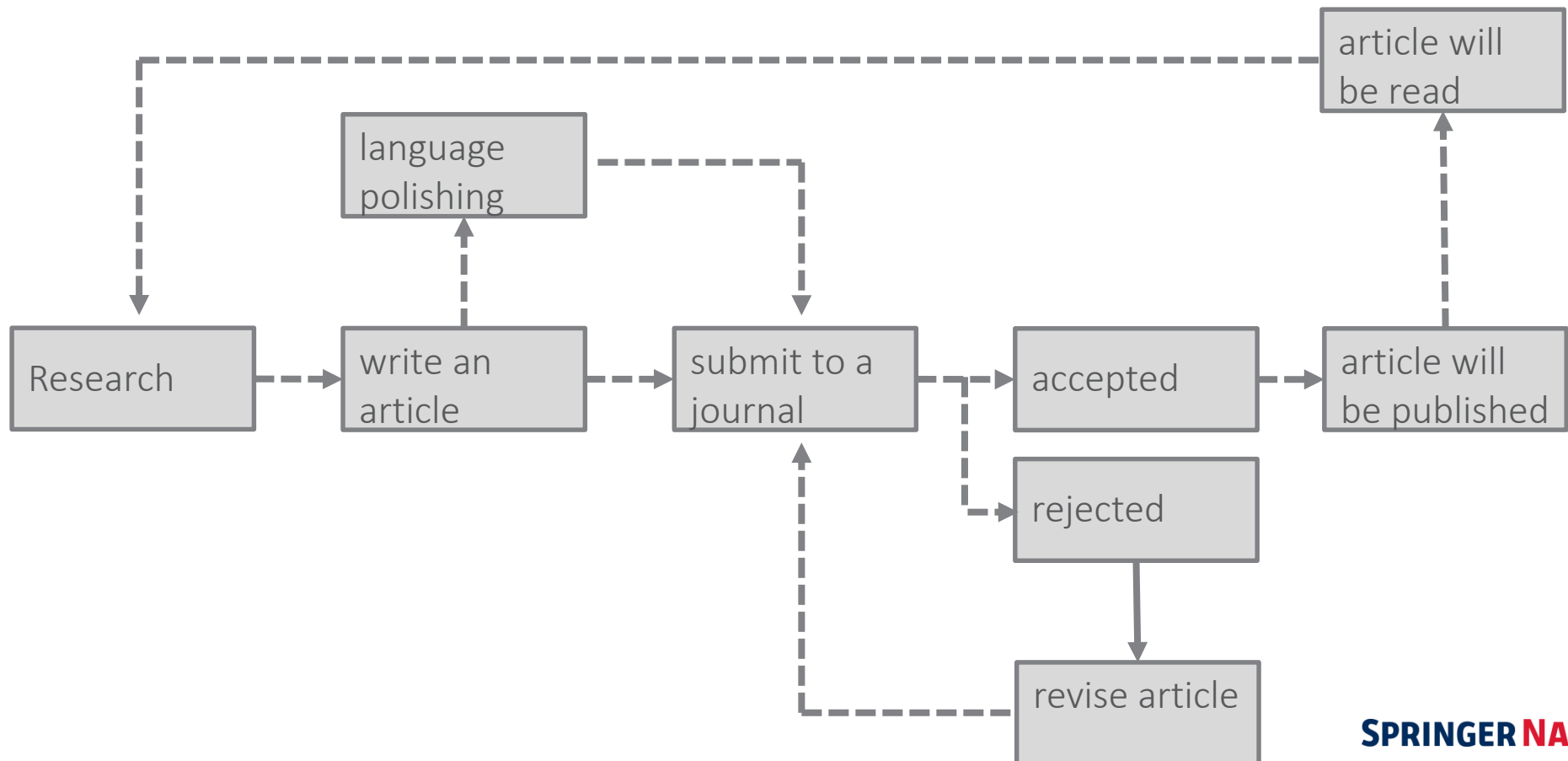
Table of Content



<http://weibo.com/springerchina>

SPRINGER NATURE

# The Life of a Journal Article Submission



# 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 'MyPublication' 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>  
Mon May 02 15:02:20 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/4JYNN>, <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 &amp; Indexing, Impact Factors

## Open Access

## E-Access via SpringerLink.com

## Copyright, Rights &amp; Licensing

## Book discount &amp; invoice information

## Marketing: greatest possible visibility for your work

# Submitting

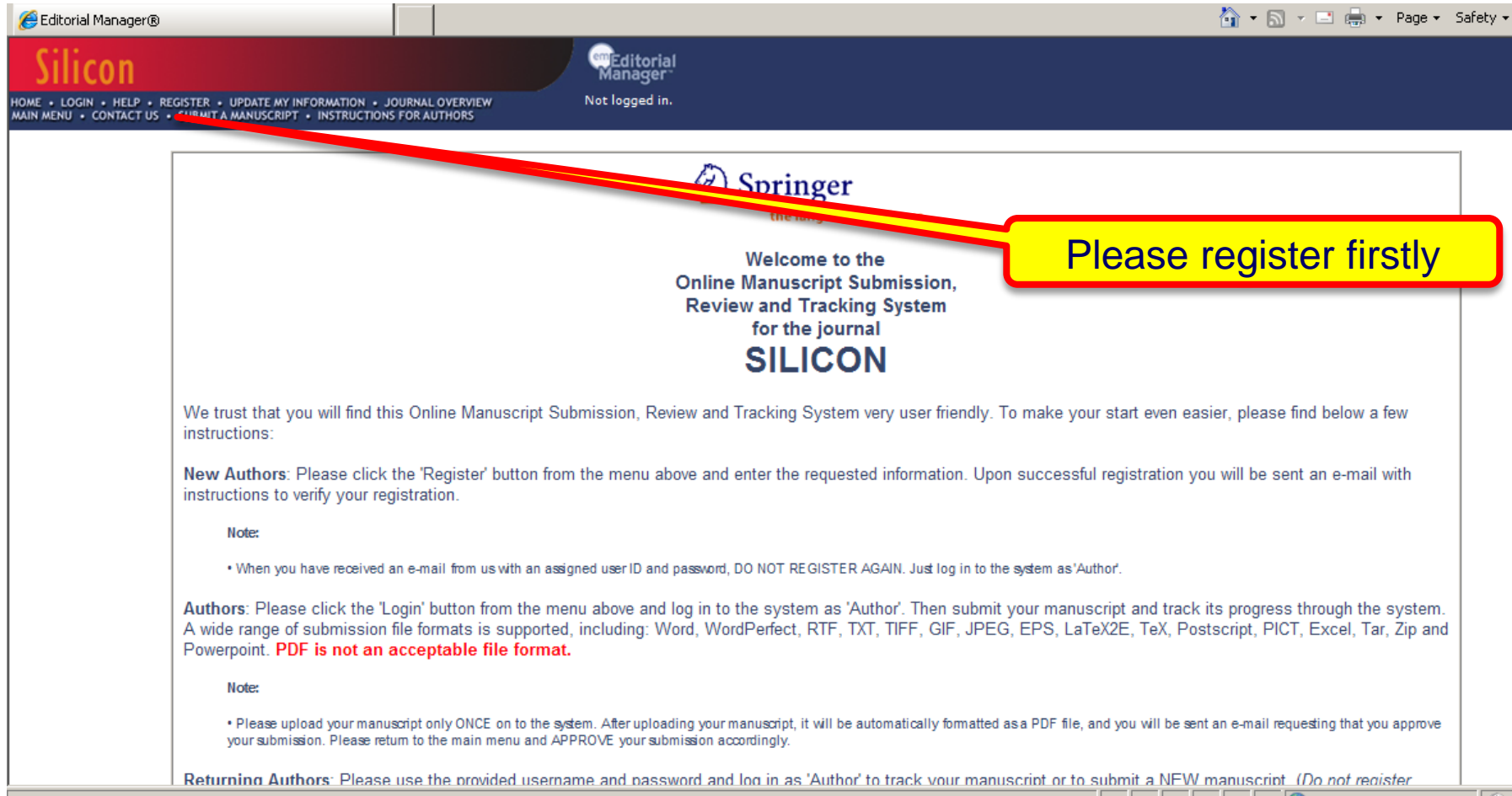
## Electronic submission

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

The screenshot displays the journal's homepage for 'Aesthetic Plastic Surgery'. The page features a navigation bar at the top with categories like 'SUBDISCIPLINES', 'JOURNALS', 'BOOKS', 'TEXTBOOKS', and 'SERIES'. Below the navigation, there is a section for the journal's cover image and title, along with details such as the Editor-in-Chief (Henry Spornik), ISSN numbers, and the publisher (Springer New York). A prominent orange 'Springer Link Read online' button is visible. On the right side, there are several orange buttons for 'Online First Articles', 'Read Current Issue', and 'Free Electronic Sample Copy'. Below these, a section titled 'FOR AUTHORS AND EDITORS' contains a list of links: 'Aims and Scope', 'Submit Online', 'Instructions for Authors', 'Conflict of Interest Statement (pdf, 28 k...', and 'Conflict of Interest Form (doc, 36 ...'. The 'Submit Online' link is highlighted in blue, and a hand cursor is pointing at it. A magnified inset box shows the 'Submit Online' and 'Instructions for Authors' links in more detail, with a hand cursor pointing at the 'Submit Online' link.



# Submitting



Editorial Manager®

**Silicon**

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

Not logged in.

**Springer**  
the logo

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*

Please register firstly

# 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  ▾

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

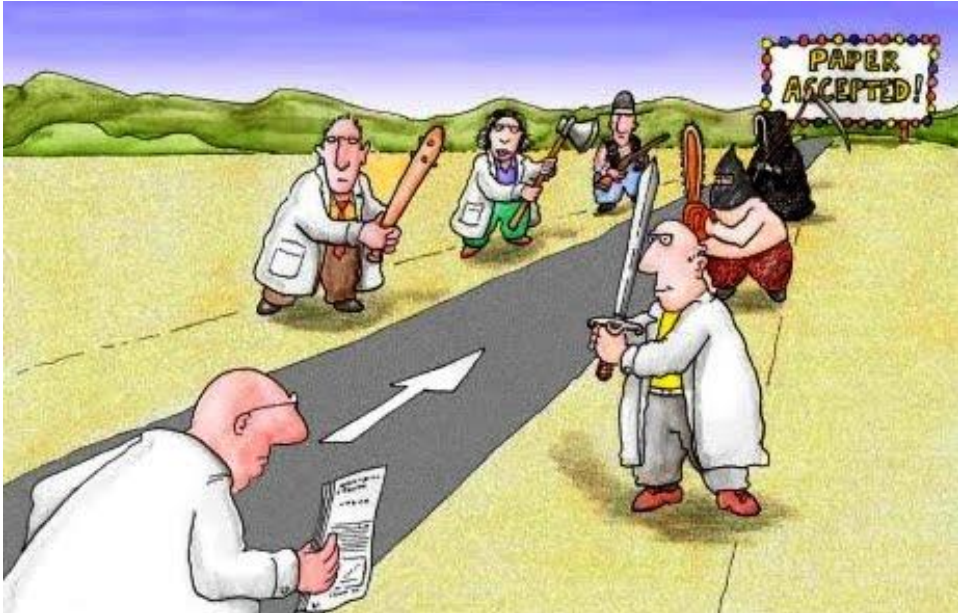
Description

File Name:

 No items have yet been attached for this submission.

# Successful

# Peer review

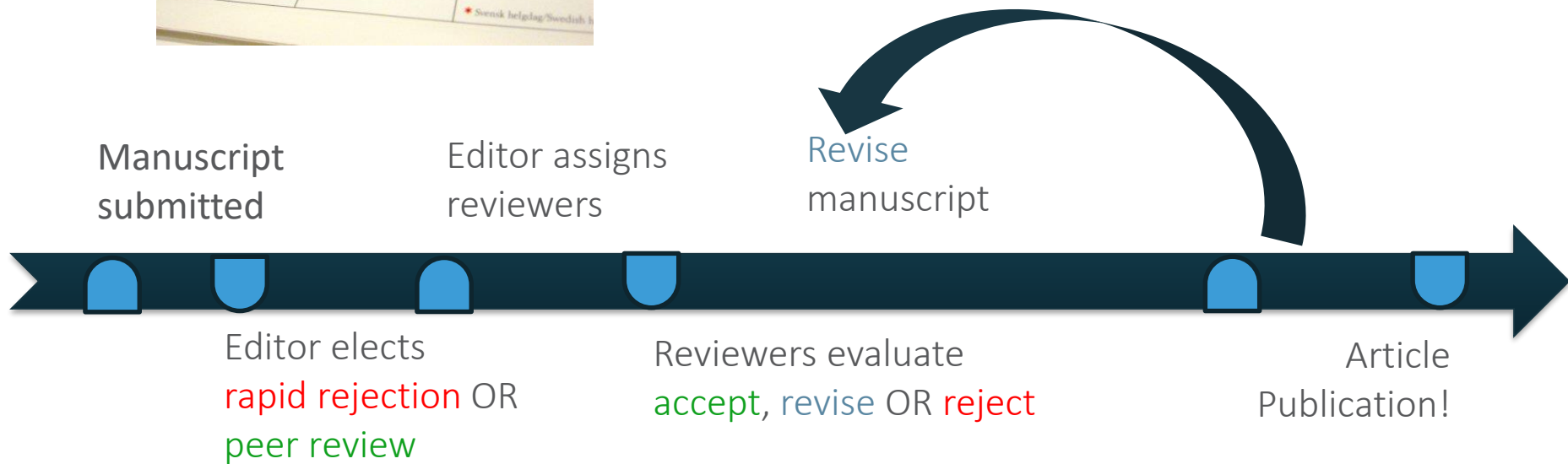


## Peer review

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 causative agent of invasive meningococcal disease: glycoconjugates with glycosaminoglycans  
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](#)

- article published "OnlineFirst"

- journal issue online

- published in print

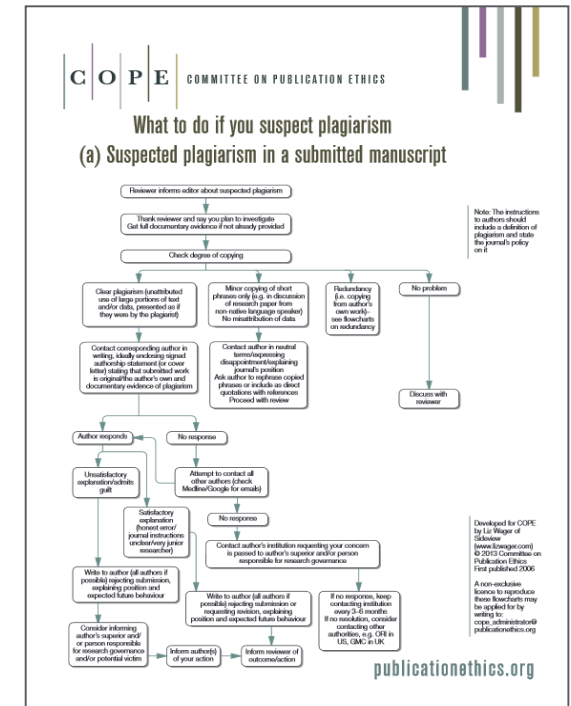
**Congratulations**  
CONGRATULATIONS

**SPRINGER NATURE**



# 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

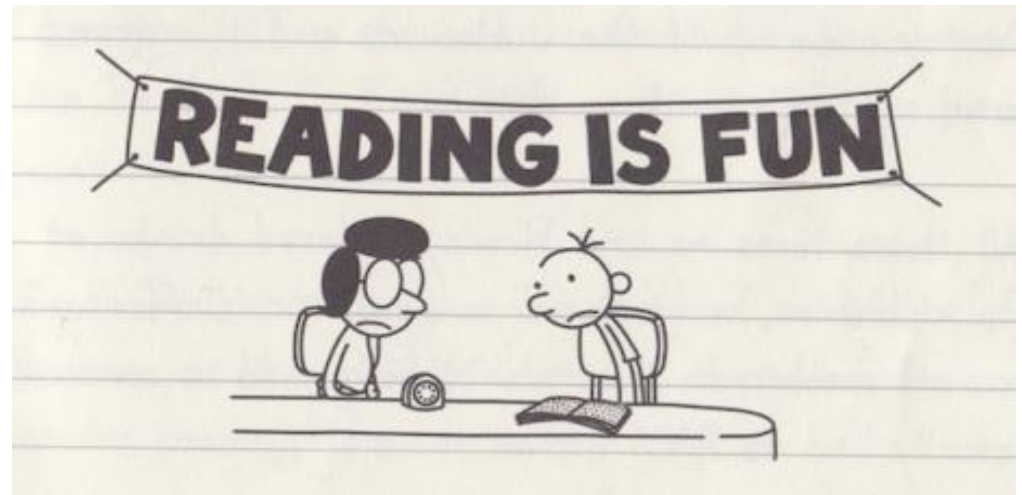




# 8 Tips for writing a good paper

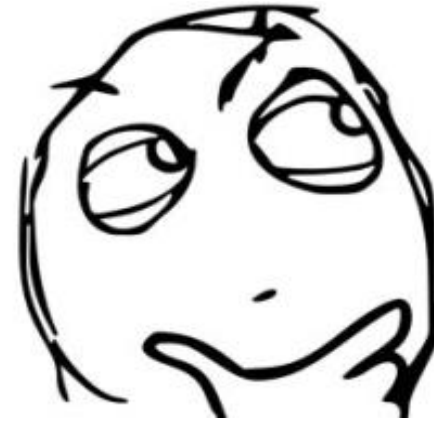
# Tip 1

- **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.

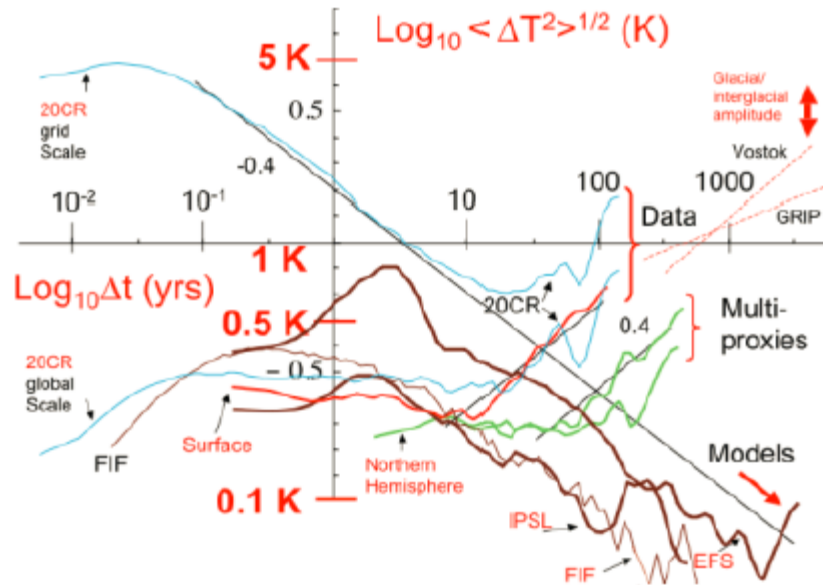
### Improved

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

# Thank you

乔昆鹏

Kunpeng.Qiao@springernature.com

**SPRINGER NATURE**