

# ACM Digital Library 简介和使用指南

May 2022

# Today's Research Driving Tomorrow's Technology



## Contents

- 01 认识ACM
- 02 ACM DL资源内容介绍
- 03 ACM DL资源内容的品质
- 04 ACM DL 的使用



# 01 认识ACM



# A.M. 图灵奖



图灵奖是ACM(美国计算机协会)于1966年设立,对获奖者的要求极高,评奖程序极严,只授予对计算机领域带来深远影响的科学家。

--计算机界的“诺贝尔奖”



艾伦·麦席森·图灵 (Alan Mathison Turing, 1912 - 1954), 英国数学家、逻辑学家, 被称为**计算机之父, 人工智能之父**。ACM设立这个奖项就是为了纪念这位伟大的科学家。



# ACM程序设计大赛

-- “程序设计的奥林匹克”



ACM程序设计大赛是大学级别最高的脑力竞赛。大赛至今已有近40年的历史，是世界范围内历史最悠久、规模最大的程序设计竞赛。

比赛对参赛学生的逻辑分析能力、策略制定和脑力方面具有极大的挑战性。大赛提倡在压力较大的情况下，培养学生的创造力、团队合作精神以解决竞赛的问题，从而挑选和发掘世界上最优秀的程序设计人才。







ACM DIGITAL LIBRARY | 3

# 关于ACM出版社

ACM(Association for Computing Machinery)

**美国计算机学会**创立于1947年， 是全球历史最悠久和最大的计算机教育科研机构。

目前拥有会员**10万**多名， 遍布全球**100**多个国家。

**Journals&Transactions:** 出版计算机领域最权威和前瞻的文献。

**Conference** --每年主办200多场会议， 每场会议都会出版相关会议录。

**Special Interest Groups** -- 根据计算机领域的每项专业设有37个特别兴趣组(SIGs)， 针对其不同的研究方向有相应的出版物。



# 02 ACM DL 内容介绍





# 1999年开始提供在线数据库服务

期刊、杂志和汇刊  
53种



超过4000  
卷会议录



“在线计算机  
文献指南”数  
据库



37种SIG时  
事通讯



ACM附属  
机构出版  
物



ACM口述  
历史访谈  
录

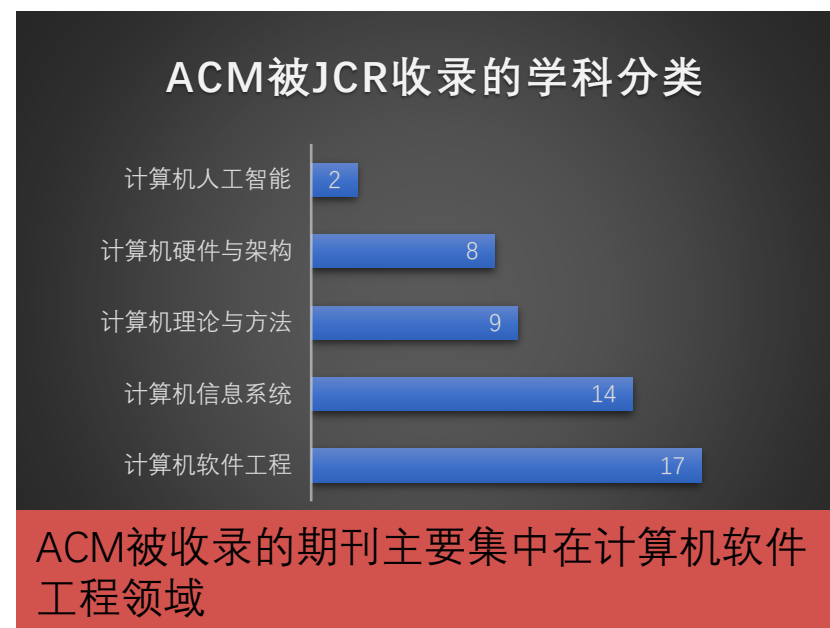
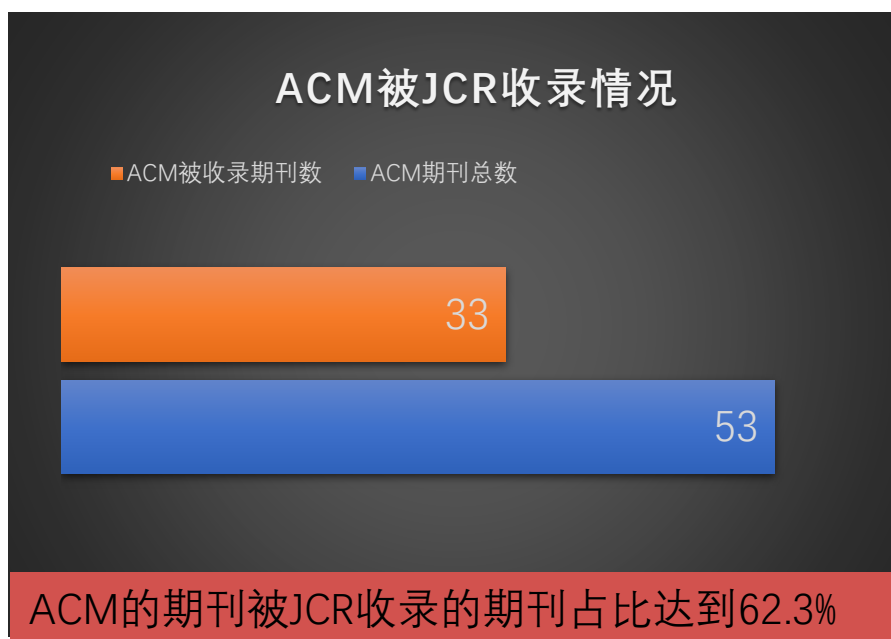




# 03 ACM DL 内容品质



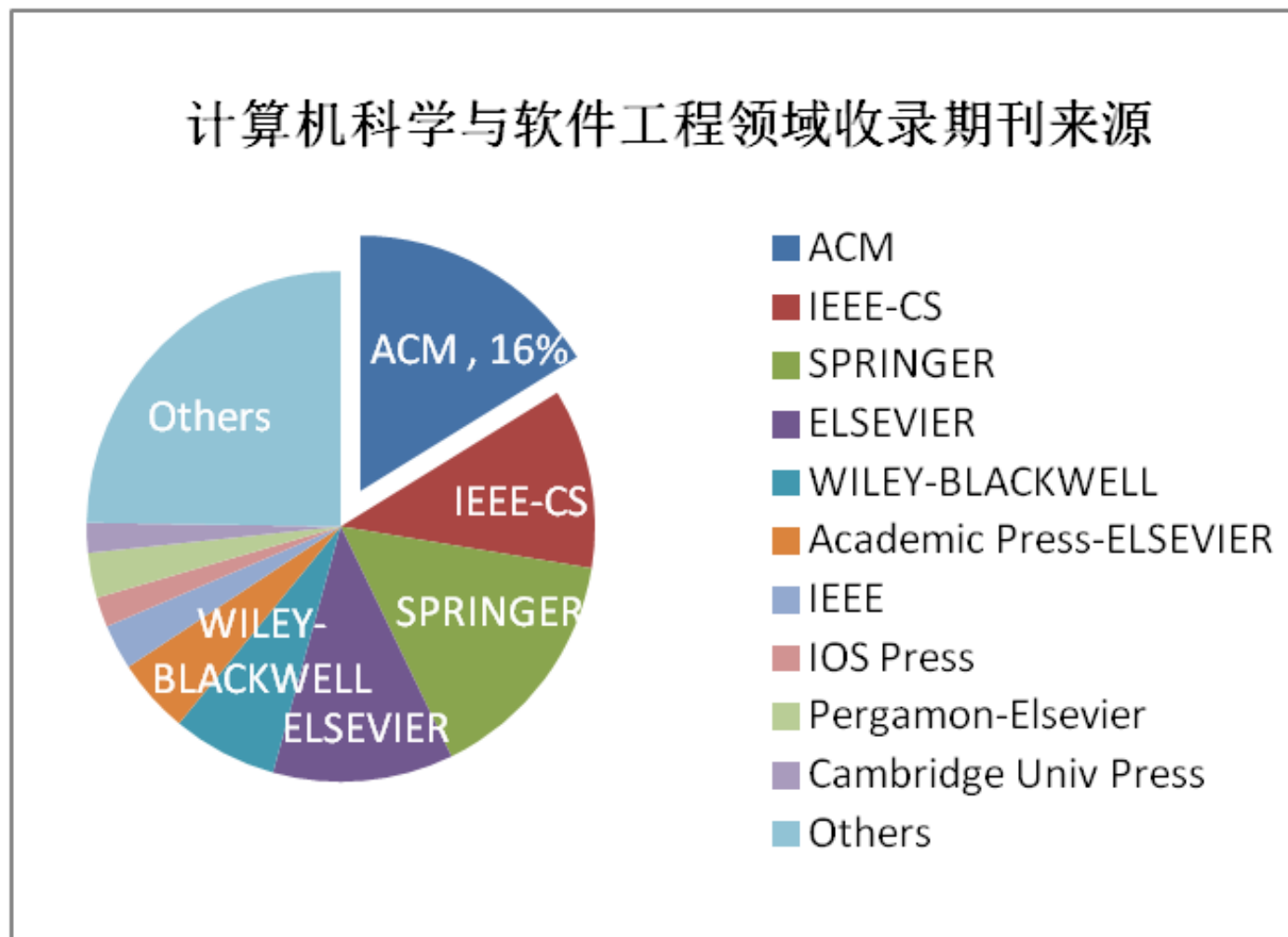
## 3.1 ACM期刊被JCR收录概况



数据来源：2016JCR报告

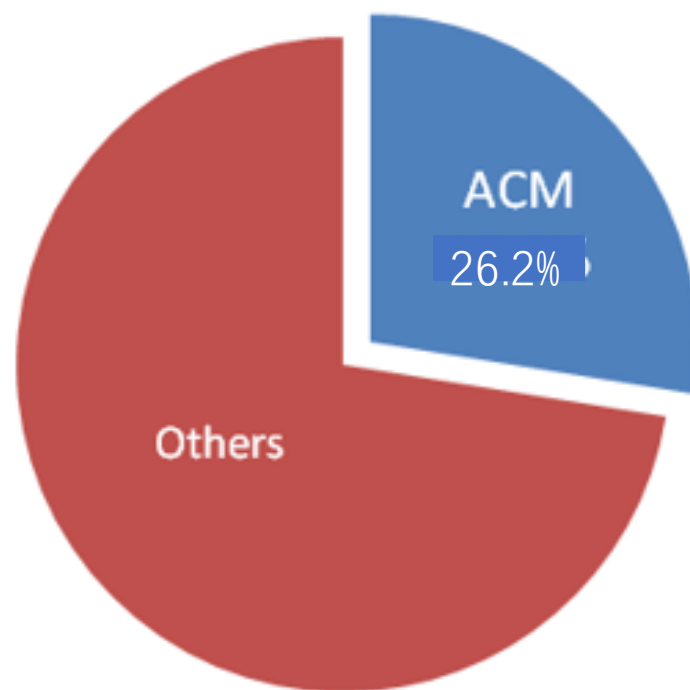


### 3.2 ACM是软件工程领域最大的期刊来源



数据来源：2016JCR报告

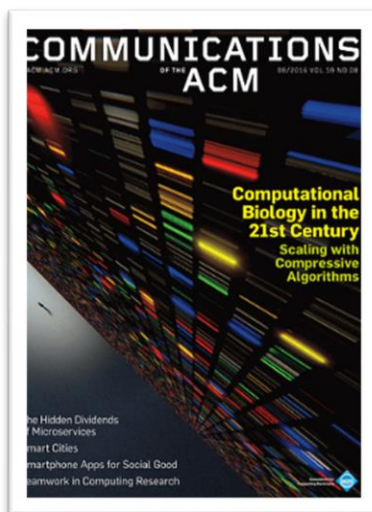
### 3.3 ACM软件工程领域期刊被引量(达到55,555次)



数据来源：2016JCR报告



## 3.4 ACM 高引用量期刊举例



### Communications of the ACM(CACM)

被引用总量：18,535， 影响因子：4.027

在计算机软件工程、计算机硬件与架构、计算机理论与方法学科领域总引用量均排名第1

### Journal of the ACM (JACM)

被引用总量：6,947 影响因子：1.855

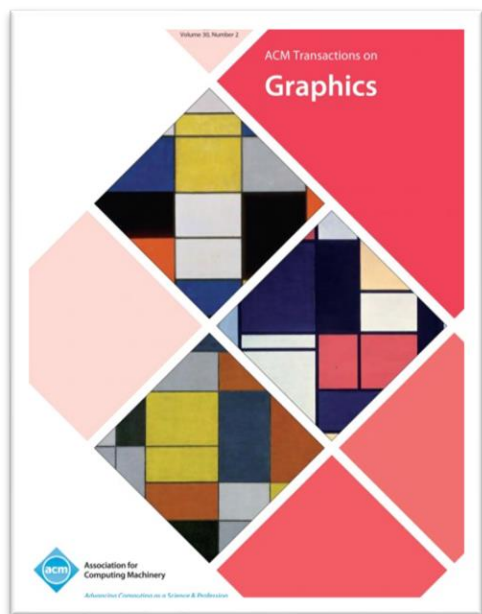
在计算机工程学科领域总引用量排名第5

数据来源：2016JCR报告





## 3.4 ACM高影响因子期刊举例



### ACM Transactions on Graphics (TOG)

被引用总量: 14,180 影响因子: 4.088

在计算机科学与软件工程学科领域影响因子排名第1



### ACM Computing Surveys(CSUR)

被引用总量: 6,629 影响因子: 6.748

在计算机科学理论和方法学科领域影响因子排名第2

数据来源: 2016JCR报告



## 3.5 ACM 会议录

- ACM和其旗下的SIG（37个特别兴趣小组）每年主办会议170余次，每年新增500多卷，目前共**4500**多卷。
- 在在计算机领域，ACM是会议、研讨会和专题论坛的最大举办机构。
- 在传播最新科研成果和技术手段方面，相较于期刊，会议录更具备博采众长、新颖、快速的特点。
- 对于计算机等工业领域，会议录被阅读参考的机会大于期刊



## 3.6 ACM 主办的顶级会议（列举）

会议英文名称	会议英文名称缩写	会议中文名称
Design Automation Conference	DAC	国际设计自动化会议
Annual International ACM SIGIR Conference on Research and Development in Information Retrieval	SIGIR	国际信息检索研发年会
ACM Annual International Conference on Mobile Computing and Networking	Mobicom, ACM	国际移动计算和网络会议
ACM International Symposium on Mobile Ad Hoc Networking and Computing	MobiHoc, ACM	国际移动自组织网络和计算会议
ACM Symposium on Theory of Computing	STOC	ACM计算理论年会
ACM Conference on Management of Data	SIGMOD	ACM数据管理国际会议
ACM Knowledge Discovery and Data Mining	<b>SIGKDD</b>	知识发现与数据挖掘国际会议
Special Interest Group on Data Communication	SIGCOMM	ACM数据通讯国际会议
Special Interest Group on Mobility of Systems, Users, Data and Computing	MOBICOM	ACM 移动通信会议
ACM Conference on Computer and Communications Security	CCS	ACM计算机与通信安全会议
ACM SIGGRAPH/SIGGRAPH Asia	<b>SIGGRAPH</b>	ACM 计算机图形与交互技术会议
ACM International Conference on Multimedia	Multimedia	ACM 多媒体国际会议
ACM SIG CHI	SIGCHI	ACM 人机交互会议
ACM Conference on the Foundations of Software Engineering (inc: ESEC-FSE when held jointly)	FSE	ACM软件工程基础会议
ACM SIGPLAN - SIGACT Symposium on Principles of Programming Languages	POPL	程序设计语言原理会议



## SIG newsletter



ACM SIGMIS Database: the  
DATABASE for Advances in  
Information Systems

被2016JCR收录



ACM SIGMOD Record

被2016JCR收录



ACM SIGPLAN Notices

被2016JCR收录



# 04 ACM DL 使用平台





# 登陆 <http://dl.acm.org/>



**ACM DL DIGITAL LIBRARY**

The **ACM Digital Library** is a research, discovery and networking platform containing:

- The **Full-Text Collection** of all ACM publications, including journals, conference proceedings, technical magazines, newsletters and books.
- A collection of curated and **hosted full-text** publications from select publishers.
- The **ACM Guide to Computing Literature**, a comprehensive bibliographic database focused exclusively on the field of computing.
- A richly interlinked set of **connections** among authors, works, institutions, and specialized communities.

[Using the ACM Digital Library](#)

[For Consortia Administrators](#)

---

**Announcements**

**Digital Library Training Sessions**

Join us for our [DL Weekly Online Training Sessions](#)

[My Binders](#) [SIGN OUT: igroups](#)

**Advanced Search** 高级检索区

**Browse the ACM Publications:**

- [Journals/Transactions](#)
- [Magazines](#)
- [Proceedings](#)
- [ACM Books](#)

**Browse the Special Interest Groups (SIGs)** 按照出版物不同类别分类浏览

- [Special Interest Groups \(SIGs\)](#)

**Browse the Conferences:**

- [Recent and Upcoming Conferences](#)
- [Conference Listing](#)

**Browse the Special Collections:** 浏览兴趣小组 newsletter

- [eBooks](#) available to ACM Members
- [ACM International Conference Proceeding Series \(ICPS\)](#)
- [Classic Book Series](#)
- [ACM Oral History interviews](#)
- [ACM Curricula Recommendations](#)
- [NSF Workshop Reports](#)

**Browse the Hosted Content**



# 快速检索—ACM DL



My Binders   SIGN OUT: **igroupsin**

cryptography   **SEARCH**

输入关键字  
cryptography,  
点击search

Searched for *cryptography* [new search] [edit/save query]

Searched The ACM Full-Text Collection: 444,662 records [Expand your search to The ACM Guide to Computing Literature: 2,573,063 records] ?

6,716 results found   全文检索结果数量   Export Results: [bibtex](#) | [endnote](#) | [acmref](#) | [csv](#)

**Refine by People**  
Names ▶  
Institutions ▶  
Authors ▶  
Editors ▶  
Reviewers ▶

**Refine by Publications**  
Publication Names ▼  
[Journal of the ACM \(JACM\) \(302\)](#)  
[Communications of the ACM \(195\)](#)  
[IEEE/ACM Transactions on Networking \(TON\) \(152\)](#)  
[ACM SIGACT News \(137\)](#)  
[ACM SIGOPS Operating Systems Review \(81\)](#)  
[ACM Transactions on Information and System Security \(TISSEC\) \(81\)](#)  
[ACM SIGPLAN Notices \(67\)](#)

Result 1 – 20 of 6,716

Result page: [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#) [10](#) >>

Sort by: [relevance](#)

检索结果可按不同要求显示

1



[Verification of a Cryptographic Primitive: SHA-256](#)  
[Andrew W. Appel](#)  
April 2015   ACM Transactions on Programming Languages and Systems (TOPLAS): Volume 37 Issue 2, April 2015  
**Publisher:** ACM  
**Bibliometrics:** Citation Count: 3  
Downloads (6 Weeks): 22, Downloads (12 Months): 215, Downloads (Overall): 318  
Full text available:  [PDF](#)   点击PDF,直接浏览全文  
This article presents a full formal machine-checked verification of a C program: the OpenSSL implementation of SHA-256. This is an interactive proof of functional correctness in the Coq proof assistant, using the Verifiable C program logic. Verifiable C is a separation logic for the C language, proved sound with respect ...  
**Keywords:** Cryptography  
[\[result highlights\]](#)  
**CCS:**  
Computational complexity and **cryptography**  
**Cryptography**

文章所在的期刊卷期信息

文摘信息



# PDF直接浏览、下载、打印

## Verification of a Cryptographic Primitive: SHA-256

ANDREW W. APPEL, Princeton University

This article presents a full formal machine-checked verification of a C program: the OpenSSL implementation of SHA-256. This is an interactive proof of functional correctness in the Coq proof assistant, using the Verifiable C program logic. Verifiable C is a separation logic for the C language, proved sound with respect to the operational semantics for C, connected to the CompCert verified optimizing C compiler.

Categories and Subject Descriptors: D.2.4 [Software/Program Verification]: Correctness Proofs; E.3 [Data Encryption]: Standards; F.3.1 [Specifying and Verifying and Reasoning about Programs]

General Terms: Verification

Additional Key Words and Phrases: Cryptography

### ACM Reference Format:

Andrew W. Appel. 2015. Verification of a cryptographic primitive: SHA-256. ACM Trans. Program. Lang. Syst. 37, 2, Article 7 (April 2015), 31 pages.  
DOI: <http://dx.doi.org/10.1145/2701415>

### 1. INTRODUCTION

*[C]ryptography is hard to do right, and the only way to know if something was done right is to be able to examine it. ... This argues very strongly for open source cryptographic algorithms. ... [But] simply publishing the code does not automatically mean that people will examine it for security flaws.*  
Bruce Schneier [1999]

*Be suspicious of commercial encryption software. ... [because of] back doors. ... Try to use public-domain encryption that has to be compatible with other implementations. ...*

Bruce Schneier [2013]

Schneier is saying to use widely used, well-examined open-source implementations of widely published, nonproprietary, widely used, well-examined, standard algorithms—“many eyes make all bugs shallow” works only if there are many eyes paying attention.


To this I add: use implementations that are *formally verified with machine-checked proofs of functional correctness, of side-channel resistance, of information-flow prop-*

7

下载 打印



# 快速检索—ACM “在线计算机文献指南数据库”



My Binders   SIGN OUT: **igroupsin**

cryptography   **SEARCH**

Searched for *cryptography* [new search] [edit/save query] [advanced search]

Searched The ACM Full-Text Collection: 444,662 records [Expand your search to The ACM Guide to Computing Literature: 2,573,063 records] ?

6,716 results found   Export Results: [bibtex](#) | [ref](#) | [csv](#)

**Refine by People**  
Names ▶  
Institutions ▶  
Authors ▶  
Editors ▶  
Reviewers ▶



**Refine by Publications**  
Publication Names ▶  
[Journal of the ACM \(JACM\) \(302\)](#)  
[Communications of the ACM \(195\)](#)  
[IEEE/ACM Transactions on Networking \(TON\) \(152\)](#)  
[ACM SIGACT News \(137\)](#)  
[ACM SIGOPS Operating Systems Review \(81\)](#)  
[ACM Transactions on Information and System Security \(TISSEC\) \(81\)](#)  
[ACM SIGPLAN Notices \(67\)](#)

Result 1 – 20 of 6,716

Result page: [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#) [10](#) >>

Sort by: [relevance](#) ▼

1

[Verification of a Cryptographic Primitive: SHA-256](#)  
[Andrew W. Appel](#)  
April 2015   ACM Transactions on Programming Languages and Systems (TOPLAS): Volume 37 Issue 2, April 2015  
**Publisher:** ACM  
**Bibliometrics:** Citation Count: 3  
Downloads (6 Weeks): 22, Downloads (12 Months): 215, Downloads (Overall): 318  
Full text available:  [PDF](#)  
This article presents a full formal machine-checked verification of a C program: the OpenSSL implementation of SHA-256. This is an interactive proof of functional correctness in the Coq proof assistant, using the Verifiable C program logic. Verifiable C is a separation logic for the C language, proved sound with respect ...  
**Keywords:** Cryptography  
[\[result highlights\]](#)  
**CCS:**  
Computational complexity and **cryptography**  
**Cryptography**

点击，直接  
扩展到文摘  
库检索 **SLab**

# ACM” 在线计算机文献指南数据库” 检索结果



My Binders   SIGN OUT: **igroupsin**

cryptography   **SEARCH**

Searched for *cryptography* [new search] [edit/save query] [advanced search]

Searched The ACM Guide to Computing Literature: 2,573,397 records [Limit your search to The ACM Full-Text Collection: 444,690 records] ?

**41,687** results found   文摘检索数量   Export Results: bibtex | endnote | acmref | csv

**Refine by People**  
Names ▶  
Institutions ▶  
Authors ▶  
Editors ▶  
Advisors ▶  
Reviewers ▶

**Refine by Publications**  
Publication Names ▶  
ACM Publications ▶  
All Publications ▶  
Content Formats ▶  
Publishers ▶

**Refine by Conferences**  
Sponsors ▶  
Events ▶  
Proceeding Series ▶

**Refine by Publication Year**

Result 1 – 20 of 41,687

Result page: 1 2 3 4 5 6 7 8 9 10 >>  
Sort by: relevance ▼

1

[Cryptography](#)  
[Andre Langie](#)  
February 2008  
**Bibliometrics:** Citation Count: 0  
[\[result highlights\]](#)

2

[Cryptography](#)  
[Patrick Horster](#)  
July 1986  
**Bibliometrics:** Citation Count: 0  
[\[result highlights\]](#)


3

[Cryptography](#)





# 搜索结果按出版物分类



My Binders   SIGN OUT: **igroupsin**

cryptography   **SEARCH**

Searched for *cryptography* [new search] [edit/save query] [advanced search]

Searched The ACM Full-Text Collection: 444,662 records [Expand your search to The ACM Guide to Computing Literature: 2,573,063 records] ?

6,716 results found   Export Results: bibtex | endnote | acmref | csv



**Refine by People**  
Names ▶  
Institutions ▶  
Authors ▶  
Editors ▶  
Reviewers ▶

**Refine by Publications**  
Publication Names ▼  
[Journal of the ACM \(JACM\) \(302\)](#)  
[Communications of the ACM \(195\)](#)  
[IEEE/ACM Transactions on Networking \(TON\) \(152\)](#)  
[ACM SIGACT News \(137\)](#)  
[ACM SIGOPS Operating Systems Review \(81\)](#)  
[ACM Transactions on Information and System Security \(TISSEC\) \(81\)](#)  
[ACM SIGPLAN Notices \(67\)](#)

Result 1 – 20 of 6,716

Result page: 1 2 3 4 5 6 7 8 9 10 >>  
Sort by: relevance ▼

1

[Verification of a Cryptographic Primitive: SHA-256](#)  
[Andrew W. Appel](#)  
April 2015   ACM Transactions on Programming Languages and Systems (TOPLAS): Volume 37 Issue 2, April 2015  
**Publisher:** ACM  
**Bibliometrics:** Citation Count: 3  
Downloads (6 Weeks): 22, Downloads (12 Months): 215, Downloads (Overall): 318  
Full text available:  [PDF](#)  
This article presents a full formal machine-checked verification of a C program: the OpenSSL implementation of SHA-256. This is an interactive proof of functional correctness in the Coq proof assistant, using the VeriC program logic. Verifiable C is a separation logic for the C language, proved sound with respect to the semantics of C. Cryptography  
[Rights]  
**CCS:**  
Computational complexity and cryptography  
Cryptography

检索结果按照出版物名称分类



# 搜索结果按兴趣小组赞助方分类



My Binders   SIGN OUT: **igroupsin**

cryptography   **SEARCH**

Searched for *cryptography* [new search] [edit/save query] [advanced search]

Searched The ACM Full-Text Collection: 444,690 records [Expand your search to The ACM Guide to Computing Literature: 2,573,397 records] ?

6,717 results found   Export Results: [bibtex](#) | [endnote](#) | [acmref](#) | [csv](#)

**Refine by People**  
Names ▶  
Institutions ▶  
Authors ▶  
Editors ▶  
Reviewers ▶

**Refine by Publications**  
Publication Names ▶  
ACM Publications ▶  
All Publications ▶  
Content Formats ▶  
Publishers ▶

**Refine by Conferences**  
Sponsors ▼  
[SIGACT \(1629\)](#)  
[SIGSAC \(1161\)](#)  
[ACM \(876\)](#)  
[SIGDA \(307\)](#)  
[SIGAI \(259\)](#)  
[SIGOPS \(243\)](#)  
[SIGARCH \(169\)](#)  
[SIGMOBILE \(167\)](#)  
[SIGPLAN \(150\)](#)

Result 1 – 20 of 6,717

Result page: [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#) [10](#) >>  
Sort by: [relevance](#) ▼

1

 [Verification of a Cryptographic Primitive: SHA-256](#)  
[Andrew W. Appel](#)  
April 2015   ACM Transactions on Programming Languages and Systems (TOPLAS): Volume 37 Issue 2, April 2015  
**Publisher:** ACM  
**Bibliometrics:** Citation Count: 3  
Downloads (6 Weeks): 20, Downloads (12 Months): 216, Downloads (Overall): 319  
Full text available:  [PDF](#)  
This article presents a full formal machine-checked verification of a C program: the OpenSSL implementation of SHA-256. This is an interactive proof of functional correctness in the Coq proof assistant, using the Verifiable C program logic. Verifiable C is a separation logic for the C language, proved sound with respect ...  
**Keywords:** Cryptography  
[\[highlights\]](#)  
[s in cryptography with weak, correlated and leaky sources](#)  
[Vichs](#)  
2013   ITCS '13: Proceedings of the 4th conference on Innovations in Theoretical Computer Science  
**er:** ACM

2016年8月

检索结果按照会议兴趣小组赞助方分类



# ACM DL高级检索界面

ACM DL DIGITAL LIBRARY

My Binders SIGN OUT: igroupsin

## Advanced Search

Select items from The ACM Full-Text Collection ?

Where Any field matches all of the following words or phrases: information security - +

Where Common Fields matches all of the following words or phrases: - +

Any field

Title

Author

Abstract

Publication Year

Full-text

Additional Fields

Author Affiliation

Author Keyword

Conference Location

Conference Sponsor

Name (all roles)

Publisher

Codes

ISBN/ISSN

DOI

Classification

Primary CCS

CCS

SEARCH

[save]

ntax]

Saved

No save

限定检索范围

Digital Library is published by the Association for Computing Machinery. Copyright © 2016 ACM, Inc.

[Terms of Usage](#) [Privacy Policy](#) [Code of Ethics](#) [Contact Us](#)



## 以“信息安全 (information security)”为例

ACM DL DIGITAL LIBRARY [My Binders](#) [SIGN OUT: igroups](#)

**Advanced Search**

Select items from  ?

Where  matches any of the following words or phrases:  - +

Where  is in the range  to  - +

以“文摘，出版年限”限定做高级检索

登录个人账户后，可以保存检索式

# 高级检索—搜索结果



My Binders   SIGN OUT: **igroupsin**

recordAbstract:(information sec)

Searched for *recordAbstract:(information security)* [new search] [edit/save query] [advanced search]

Searched The ACM Full-Text Collection: 444,690 records [Expand your search to The ACM Guide to Computing Literature: 2,573,397 records] ?

**Refinements** [remove all] *click each refinement below to remove*

Published since: 1947  
Published before: 2016

82,409 results found

全文数量

Export Results: [bibtex](#) | [endnote](#) | [acmref](#) | [csv](#)

**Refine by People**  
Names ▶  
Institutions ▶  
Authors ▶  
Editors ▶  
Advisors ▶  
Reviewers ▶

Result 1 – 20 of 82,409

Result page: [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#) [10](#) >>  
Sort by: [relevance](#) ▼

**Refine by Publications**  
Publication Names ▼  
[ACM SIGPLAN Notices \(1171\)](#)  
[Communications of the ACM \(800\)](#)  
[Journal of Computing Sciences in Colleges \(725\)](#)  
[ACM SIGCSE Bulletin \(617\)](#)  
[ACM SIGSOFT Software Engineering Notes \(527\)](#)  
[ACM SIGCOMM Computer Communication Review \(512\)](#)  
[ACM SIGMOD Record \(404\)](#)

**1** [Information security control in the application of grid security](#)  
 [Yuan Jia-bin, Gu Kai-kai](#)  
November 2007   CHINA HPC '07: Proceedings of the 2007 Asian technology information program's (ATIP's) 3rd workshop on High performance computing in China: solution approaches to impediments for high performance computing  
**Publisher:** ACM  
**Bibliometrics:** Citation Count: 0  
Downloads (6 Weeks): 5, Downloads (12 Months): 13, Downloads (Overall): 279  
Full text available:  [PDF](#)  
To improve the security of the information system, the information security control theory is studied. This paper introduces information security and automatic control theory, presents the information security control theory, traverses the characteristic of the information security control theory. This paper also analyses the security grid technology, introduces the information ...  
**Keywords:** security control, grid security, information security, grid  
[result highlights]

出版物分类





## “信息安全” 为检索词全文数量最多的出版物（前十）

出版物名称	全文数量
ACM SIGPLAN Notices	1171
Communications of the ACM	800
Journal of Computing Sciences in Colleges	725
ACM SIGCSE Bulletin	617
ACM SIGSOFT Software Engineering Notes	527
ACM SIGCOMM Computer Communication Review	512
ACM SIGMOD Record	494
IEEE/ACM Transactions on Networking (TON)	408
ACM SIGIR Forum	401
Personal and Ubiquitous Computing	396



## “信息安全” 领域发文最多的ACM专题兴趣小组



ACM程序设计语言专题兴趣小组



ACM计算机人机交互专题兴趣小组



ACM信息检索专题兴趣小组



ACM超文本、超媒体和网络专题兴趣小组



ACM人工智能专题兴趣小组



# Thanks.

