中国矿业大学计算机学院

2017 级本科生课程报告

课程名称 文献检索与学术写作

报告时间 2019.10.9

学生姓名 袁孝健

学　　号 06172151

专　　业 信息安全

任课教师 张风荣

任课教师评语

任课教师评语

考查点	18-20	16-17	14-15	12-13	0-11	得分
文献检索的方法、步骤；检索的有效性(20分)	熟悉4种以上数据库文献检索的方法、步骤；能正确提取检索的作者；充分检索了相关文献并进行了相应的分析	较为熟悉4种以上数据库文献检索的方法、步骤；能正确提取检索的关键词和作者；较为充分检索了相关文献	较为熟悉3种以上数据库文献检索的方法、步骤；检索相关文献不够充分	文献检索的方法、步骤不够熟悉，存在缺陷；检索的相关文献不够充分，存在较大片面性	文献检索的方法、步骤不熟悉；检索的相关文献较少	
在各种中英文数据库的熟练使用基础上，能对检索结果进行有效分析（20分）	在信息检索的基础上，给出的文献重要性和作者重要性，理由合理；格式规范	在信息检索的基础上，给出的文献重要性和作者重要性，理由较为合理；格式规范	在信息检索的基础上，给出的文献重要性和作者重要性理由基本合理；格式规范	在信息检索的基础上，给出的文献重要性和作者重要性理由不够合理	不能正确使用各种中英文数据库；给出的文献重要性和作者重要性理由不合理、牵强	
总分（40分）						

Information Retrieval

Task 1:

Try to retrieve and analyze Chinese literature from CNKI and Wanfang databases. Find a researcher from the list of the members of Chinese Association for Cryptographic Research and retrieve her/ his published papers. If the published papers of the researcher are less than 10, then find out 15 Chinese documents published in the past three years.

要查询的学者:

吴文玲	中国科学院软件研究所	副理事长

1、中国知网:

(1) 首先要想使用中国矿业大学图书馆的资源需要链接 VPN，然后打开矿大图书馆首页 (http://lib.cumt.edu.cn/)，并选择【中文数据库】中的“中国知网”。

(2) 在搜索框左边的下拉框中选择作者一项并输入“吴文玲”，可以看到共有 162 篇文献被 CNKI 收录。但是可以明显看到其中某些文献的领域与要搜索的学者领域有很大差别，判断存在同名作者，于是进入高级搜索。

(3) 在高级检索中，首先将检索条件中作者项精确匹配“吴文玲”，根据了解可知该学者研究领域为密码学方向，于是可以通过全文匹配关键词“密码”，进行检索。

搜索结果如下，可以看到该学者有 87 篇文献被 CNKI 收录，其中以第一作者身份被收录 38 篇。

(4) 点击该学者的一篇文献后，即可进行下载。

(5) 也可以点击上述图片中作者的名字从而进入其个人主页，如下

(6) 在作者个人主页上可以看到她被 CNKI 检索的全部文献，以及关注的领域、合作作者、获得支持基金等相关信息。

2、万方数据资源系统

(1) 在图书馆【中文数据库】分类下选择进入“万方数据资源系统”，如下:

(2) 同样先直接按作者姓名搜索“吴文玲”如下，可以看到共检索 228 篇文献，很明显知道存在同名情况。与 CNKI 不同，在万方的搜索结果下面会直接按 H 指数列出同名作者。

可以直接点击第一个吴文玲（中国科学院），进入该作者个人主页。

可以看到该学者，总文献量为 96 篇，核心发文量为 68 篇，同时还对其研究兴趣以及发文趋势进行了可视化展示，下拉可以看到该作者的具体发表文献：

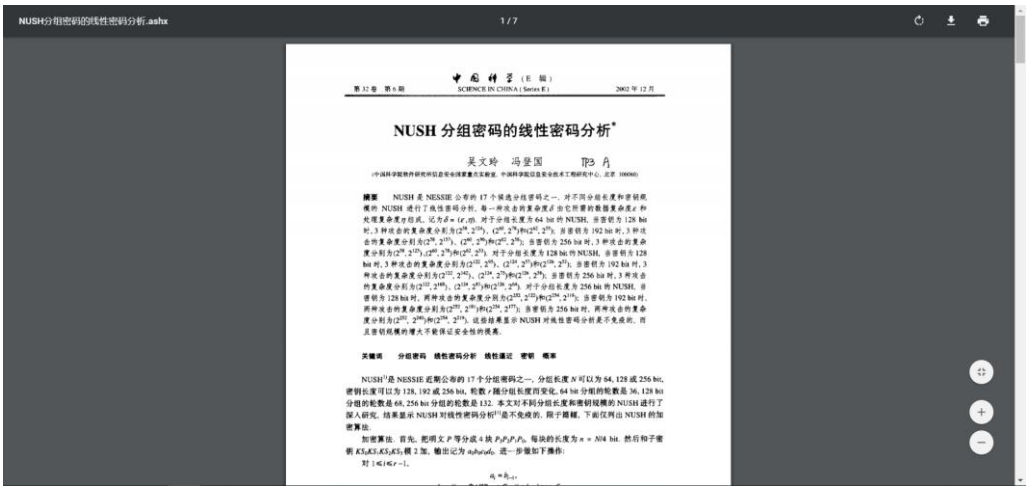
(3) 除此之外，我们继续尝试使用万方数据库的高级检索功能：

①文献类型选择期刊论文、学位论文、会议论文，作者姓名精确匹配“吴文玲”，关键词模糊匹配“密码”，可看到共检索 68 篇文献。

②文献类型选择期刊论文、学位论文、会议论文，作者姓名精确匹配“吴文玲”，=作者单位模糊匹配“中国科学院”，可看到共检索 68 篇文献。

(4) 选择一篇文献点击后，可选择在线阅读、下载、导出、收藏等:

尝试在线阅读，如下：

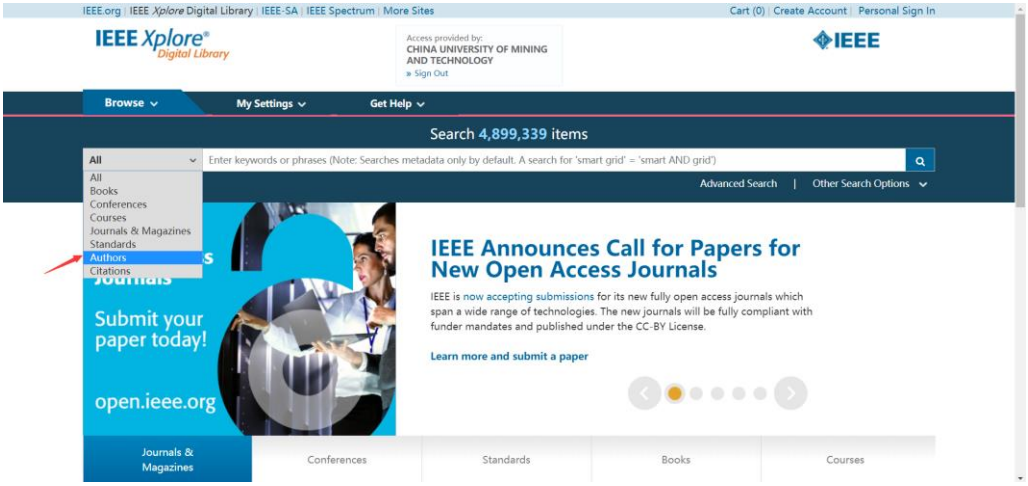


Task 2:

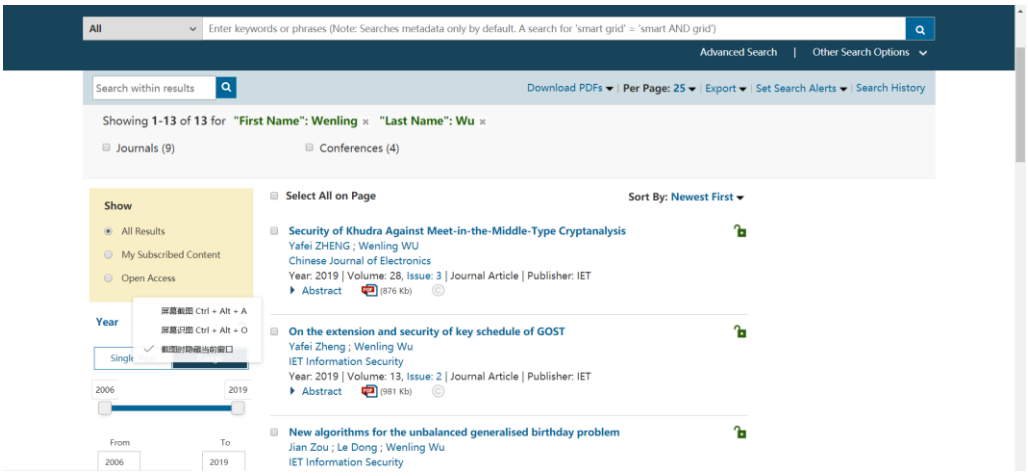
Retrieve and analyze English literature and index from IEEE database, Springer database, EI database and SCI database. Try to find out 15 important English documents published in the past three years, and give the reasons why you think it is important.

1、IEEE Xplore Digital Library (IEEE database)

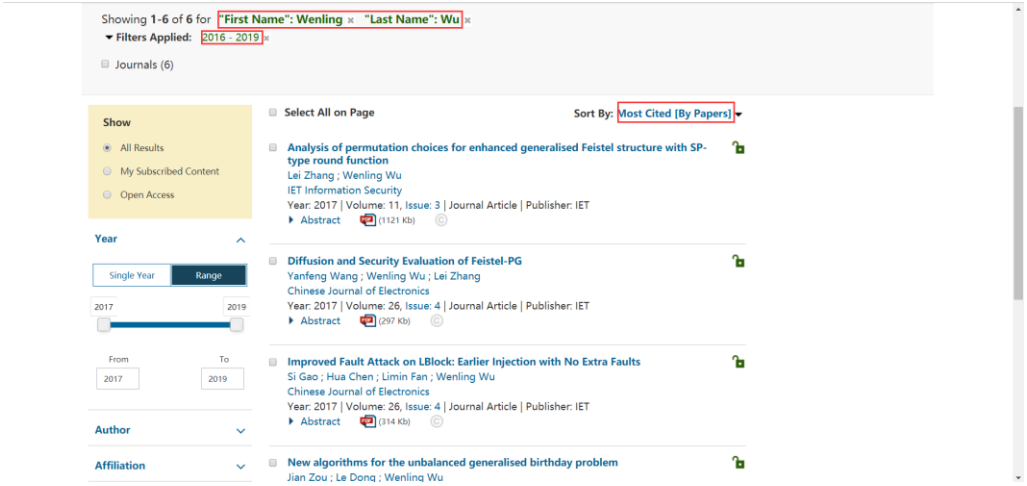
(1) 在图书馆【外文数据库】分类下进入 IEL(IEEE/IET) (美国电气电子工程师学会/英国工程技术学会)，并在搜索栏左侧下拉框中选择 Author 一项。



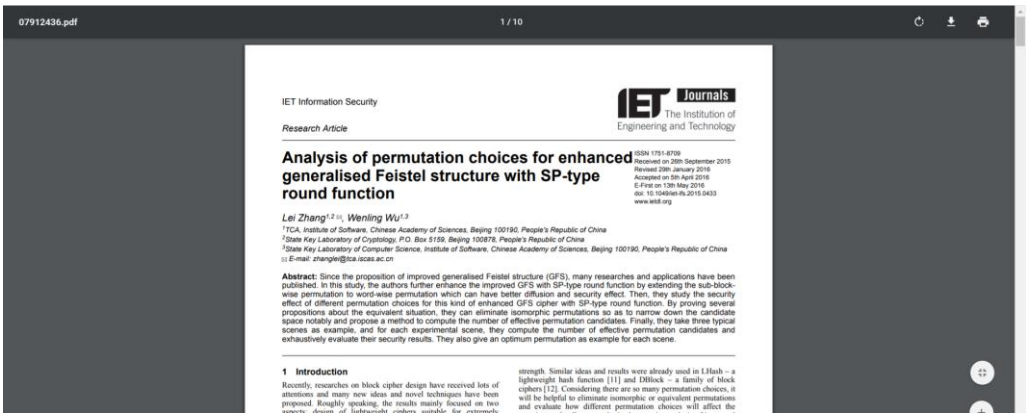
(2) 在 Authors 搜索中，输入 First Name 为 Wenling、Family Name 为 Wu，得到如下检索，可以看到共有 13 篇文献被 IEEE 检索。



(3) 因为要求搜索近三年的文献，因此在左侧栏的 Year 条件中，将年份筛选为 From 2016 To 2019，同时按被引用的次数进行排序，得到检索结果如下，共有 6 篇文献被检索，但是可以看到该学者近三年 IEEE 检索的论文并没有被其他论文所引用。

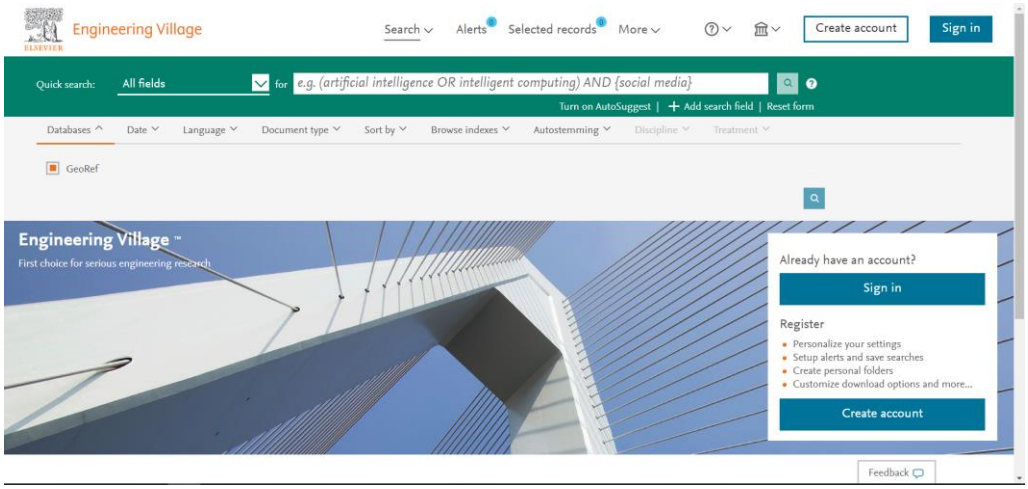


(4) 我们点击第一篇文献，进入后可以选择下载 PDF，即可进行下载或阅读:

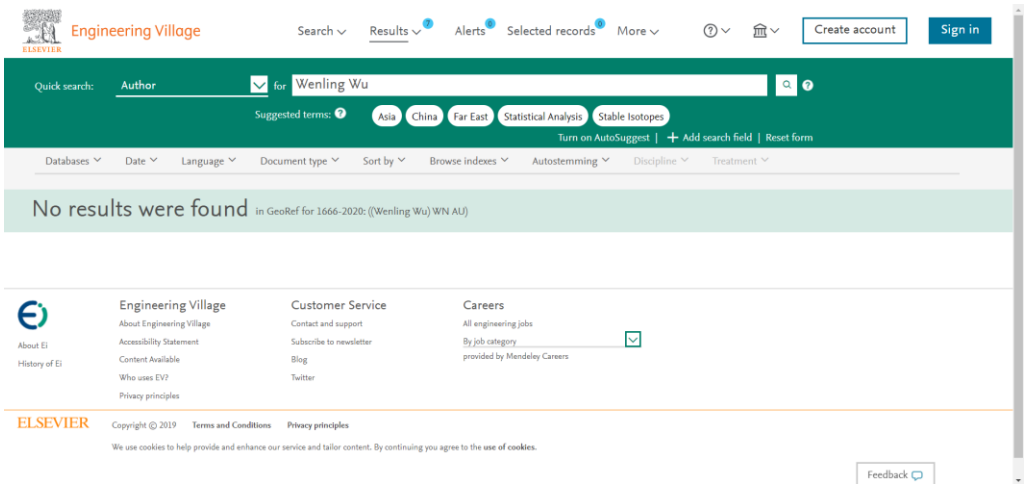


2、Engineering Village (EI database)

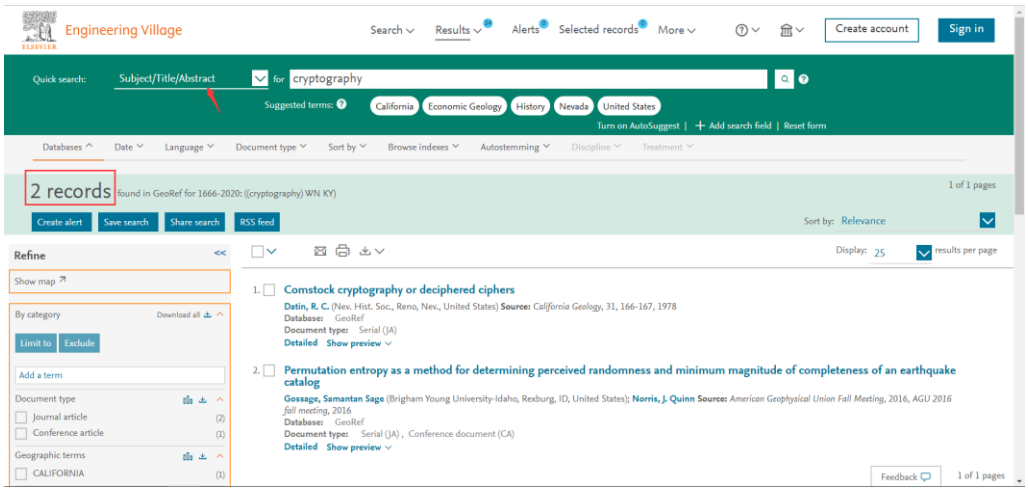
(1) 在图书馆【外文数据库】分类中进入 Engineering Village 平台 (EI)，如下:



(2) 在搜索栏左侧下拉框中，选择 Author 进行条件检索，但是尝试检索“Wenling Wu”和“Wu Wenling”，均未能找到该学者所发表的文献，判断该学者并无文献被 EI 检索。

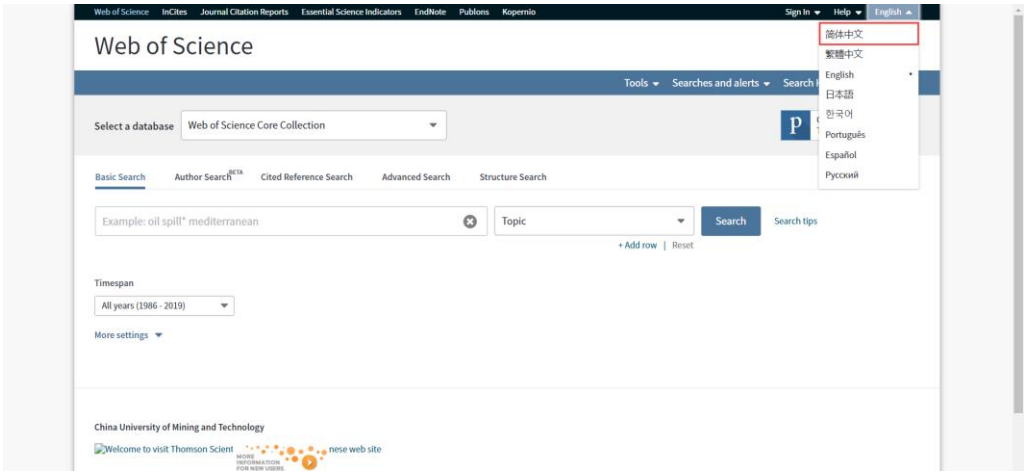


(3) 于是尝试检索主题为密码学的文献，选择 Subject/Title/Abstract 并以关键词 cryptography 进行检索，发现只有两篇密码学文章被检索。经检索知，Engineering Village 平台大多为工程类文献。



3、 Web of Science (SCI database)

(1) 在图书馆【外文数据库】分类中进入 Web of Science，发现该数据库支持简体中文语言:

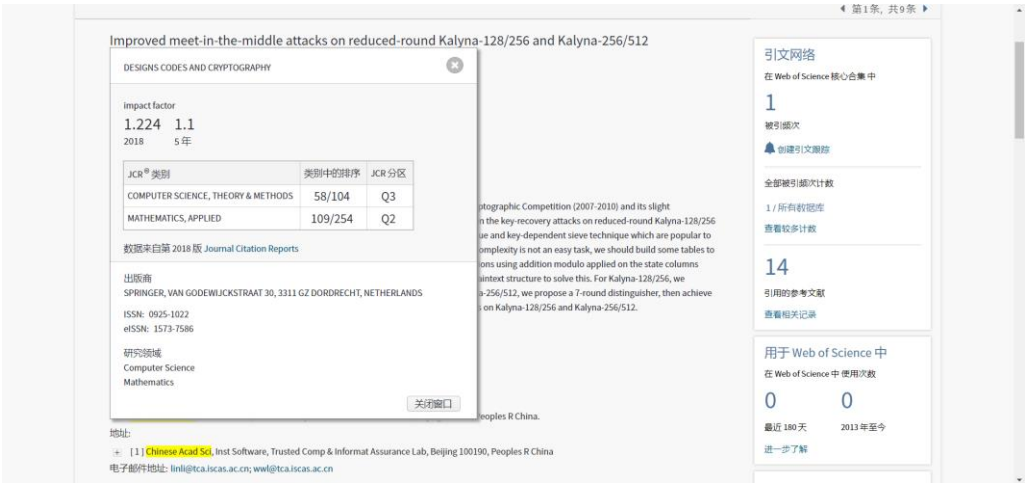


(2) 在搜索条件中设置如下：

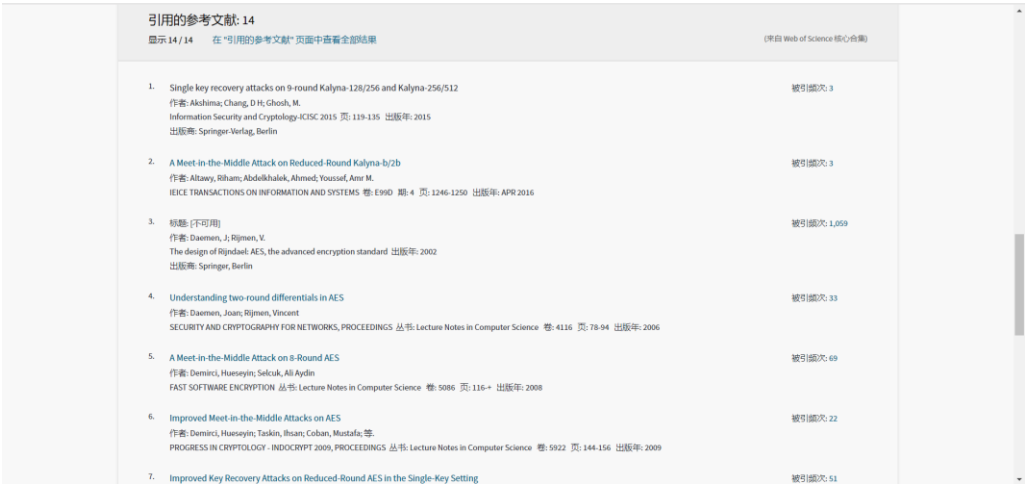
作者：Wu Wenling；机构扩展：Chinese Acad Sci；自定义年份：2016 至 2019；更多设置：勾仅选 Science Citation Index Expanded (SCI-EXPANDED) --2000 年至今

(3) 按上述条件检索并按被引次数排序可得，该作者近三年被 SCI 收录文献 9 篇。

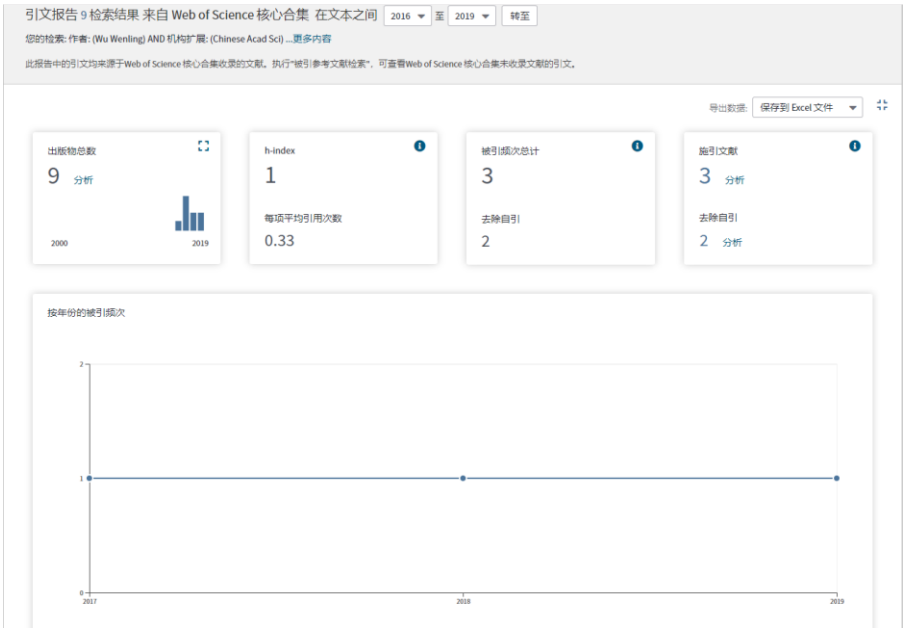
(4) 选择第一篇文献进入，可以看到此文献的详细信息，包括所发表期刊的影响因子。



(5) 除此之外，还能看到该文献所引用的其他文献及其被引用的次数，方便了我们寻找优秀的文献;

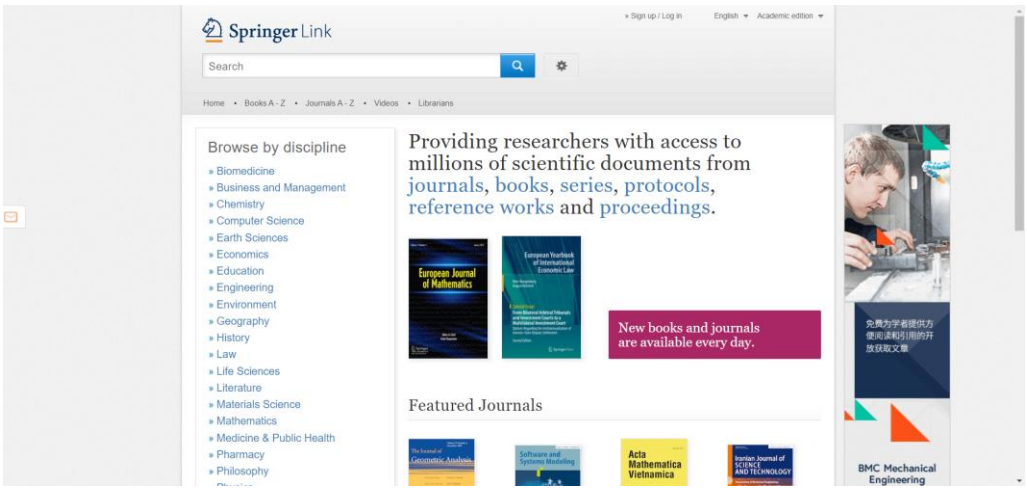


(6) 该网站还能自动生成引文报告，吴文玲学者最近 3 年的 SCI 引文报告如下，方便进行分析，

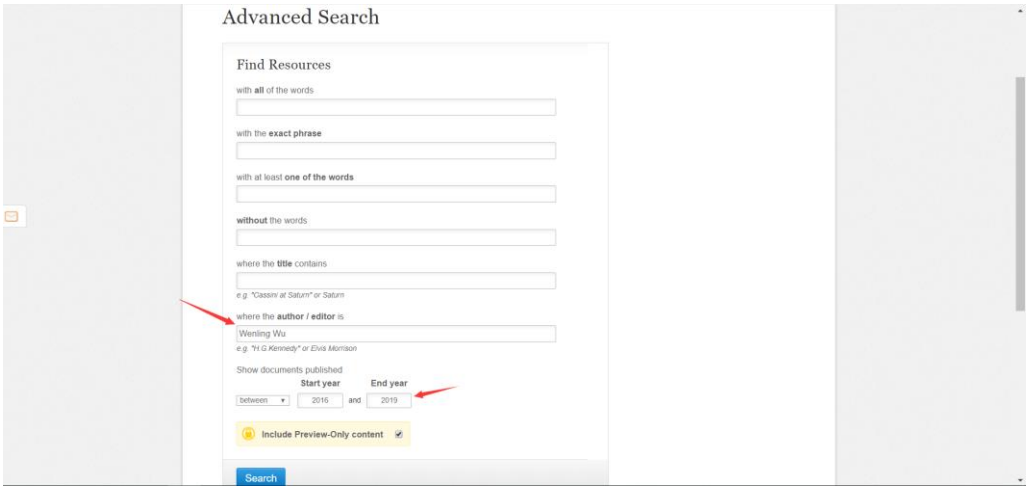


4、 Springer Link (Springer database)

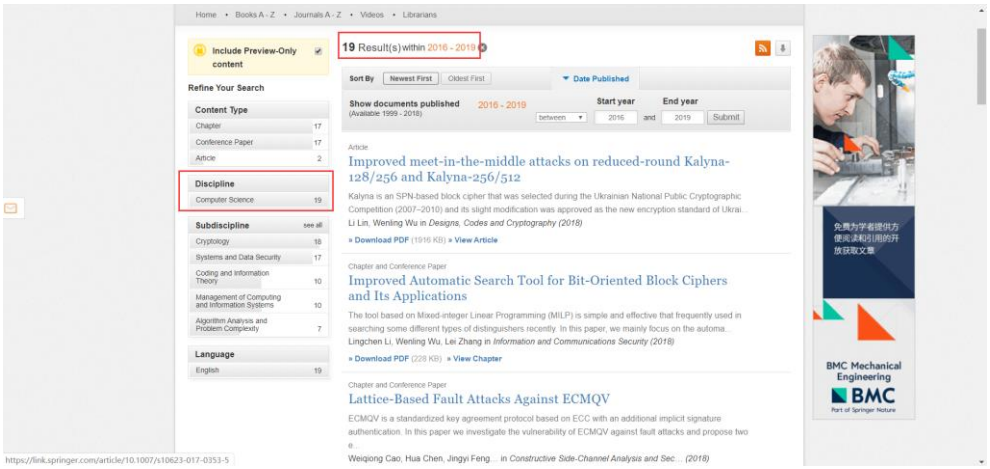
(1) 在图书馆【外文数据库】分类中进入 Springer Link:



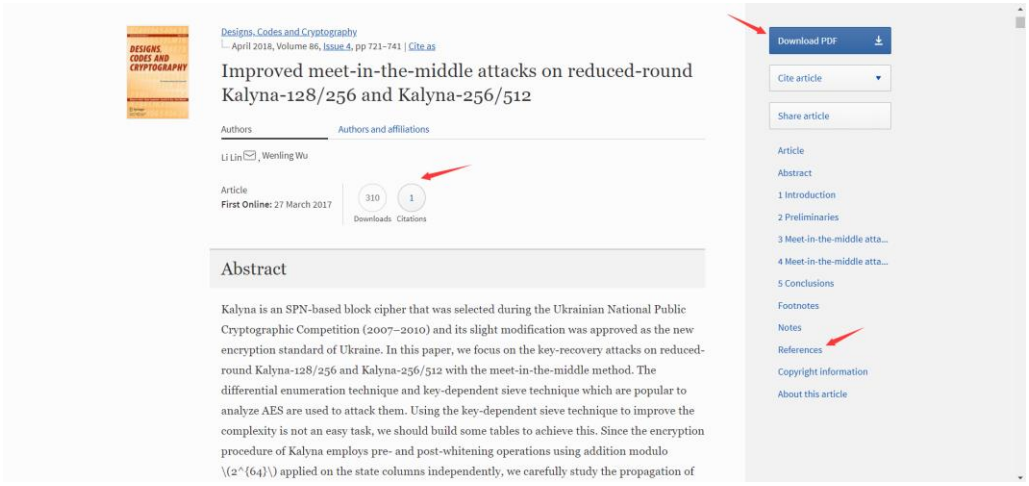
(2) 点击搜索框右侧齿轮按钮选择进入高级搜索，设置作者为“Wenling Wu”，且出版年份限定为近三年内(2016-2019)



(3) 搜索结果如下，可以看到所属学科均为 Computer Science，该学者 2016 年-2019 年期间共被 Springer Link 收录文献 19 篇。



(4) 点击进入一篇文章，会显示下载次数、引用次数、参考文献等相关信息，还可以点击右上角的 Download PDF 进行下载或者 Share article 进行分享。



5、Result

上述以检索中国密码协会副理事长吴文玲教授的文献为例，分别记录了 IEEE、EI、SCI、Springer 四种外文数据库的初步检索过程，在检索的过程中我选取了相关领域以下 15 篇文献作为最终结果，并认为其较为重要：

(1) Lossless and Reversible Data Hiding in Encrypted Images With Public-Key Cryptography

Reason：IEEE 检索，74 Paper Citations、3383 Full Text Views，该文针对由具有概率和同态性质的公钥密码系统加密的密文图像，提出了一种无损，可逆和组合的数据隐藏方案。

(2) Investigating Cube Attacks on the Authenticated Encryption Stream Cipher ACORN

Cite this paper as: Salam M.I., Bartlett H., Dawson E., Pieprzyk J., Simpson L., Wong K.KH. (2016) Investigating Cube Attacks on the Authenticated Encryption Stream Cipher ACORN. In: Batten L., Li G. (eds) Applications and Techniques in Information Security. ATIS 2016. Communications in Computer and Information Science, vol 651. Springer, Singapore

Reason：Springer 检索，10 次引用，419 次下载，其是将多维数据集攻击应用于 ACORN 的简化版本，这是 CAESAR 密码竞赛中的候选密码设计

(3) Espresso: A stream cipher for 5G wireless communication systems

Cite this article as: Dubrova, E. & Hell, M. Cryptogr. Commun. (2017) 9: 273. https://doi.org/10.1007/s12095-015-0173-2

Reason：Springer 检索，引用 3 次，下载 667 次，与最新的 5G 技术联系，结合了 NLFSRs 和 Galois 的优点，提出了新的流密码方案。

(4) Automatic Search for the Best Trails in ARX: Application to Block Cipher Speck

Cite this paper as: Biryukov A., Velichkov V., Le Corre Y. (2016) Automatic Search for the Best Trails in ARX: Application to Block Cipher Speck. In: Peyrin T. (eds) Fast Software Encryption. FSE 2016. Lecture Notes in Computer Science, vol 9783. Springer, Berlin, Heidelberg

Reason：Springer 检索，引用 5 次，下载 1.1k 次，报告了 Speck32，Speck48，Speck64，Speck96 和 Speck128 的多达 10、9、8、7 和 7 轮最佳差分轨迹的概率以及具有最高概率的差分路径的确切数量。

(5) Blockchains and Smart Contracts for the Internet of Things

Reason：IEEE 检索，617 Paper Citations、103736 Full Text Views，研究了物联网与区块链这两个热门领域的组合，并得出结论此组合可以在多个行业中引起重大变革，从而为新的业务模型和新颖的分布式应用程序铺平道路。

(6) ZMAC: A Fast Tweakable Block Cipher Mode for Highly Secure Message Authentication

Cite this paper as: Iwata T., Minematsu K., Peyrin T., Seurin Y. (2017) ZMAC: A Fast Tweakable Block Cipher Mode for Highly Secure Message Authentication. In: Katz J., Shacham H. (eds) Advances in Cryptology – CRYPTO 2017. CRYPTO 2017. Lecture Notes in Computer Science, vol 10403. Springer, Cham

Reason：Springer 检索，引用 7 次，下载 1.8k 次，提出了一种新的模式 ZMAC，允许根据可调整的分组密码(TBC)构造消息身份验证代码(MAC)。

(7) Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts

Reason：IEEE 检索，308 Paper Citations、41389 Full Text Views， Hawk 是一种去中心化的智能合约系统，它不会在区块链上以明文形式存储金融交易，且 Hawk 程序员无需实施加密，其编译器会自动生成一个高效的加密协议，合同方可以使用零知识证明等加密原语与区块链进行交互。

(8) An image encryption scheme based on chaotic tent map

Reason：SCI 检索，57 次引用，Journal Impact Factor 为 4.604，近年来，图像加密已经成为有吸引力的研究领域，该文提出了一种基于混沌帐篷图的图像加密方案，基于这种地图的图像加密系统可以表现出更好的性能。

(9) A Realistic Lightweight Anonymous Authentication Protocol for Securing Real-Time Application Data Access in Wireless Sensor Networks

Reason：IEEE 检索，61 Paper Citations、1287 Full Text Views，为 WSN 提出了一种现实的身份

验证协议，该协议可以确保各种命令性安全属性，例如用户匿名性，不可追溯性，前向/后向保密性，完美的前向保密性等。

(10) Extended Generalized Feistel Networks Using Matrix Representation to Propose a New Lightweight Block Cipher: Lilliput

Reason：IEEE 检索，16Paper Citations、557 Full Text Views，提出新的轻量级分组密码：Lilliput。

(11) An image encryption algorithm based on chaotic system and compressive sensing

Reason：SCI 检索，30 次引用，Journal Impact Factor 为 4.086，提出了一种基于忆阻混沌系统，基本元胞自动机（ECA）和压缩感知（CS）的图像加密算法

(12) RoadRunneR: A Small and Fast Bitslice Block Cipher for Low Cost 8-Bit Processors

Cite this paper as: Baysal A., Şahin S. (2016) RoadRunneR: A Small and Fast Bitslice Block Cipher for Low Cost 8-Bit Processors. In: Güneysu T., Leander G., Moradi A. (eds) Lightweight Cryptography for Security and Privacy. LightSec 2015. Lecture Notes in Computer Science, vol 9542. Springer, Cham

Reason：Springer 检索、7 次引用，582 次下载，提出了 RoadRunneR，即 8 位软件中的一种高效分组密码，其安全性可证明可抵抗差分和线性攻击，此外，还提出了一种新的度量标准，以公平地比较分组密码。

(13) A novel chaos-based image encryption using DNA sequence operation and Secure Hash Algorithm SHA-2

Reason：SCI 检索，72 次引用，Journal Impact Factor 为 4.604，提出了一种基于脱氧核糖核酸（DNA）掩蔽，安全哈希算法 SHA-2 和 Lorenz 系统的混合模型的新型图像加密算法。

(14)Entropic uncertainty relations and their applications

Resason：SCI 检索，引用 110 次，Impact Factor 为 38.296，熵不确定性关系已成为几乎所有量子密码协议（例如量子密钥分发和两方量子密码术）的安全性分析的中心要素，该文章调查了熵不确定性关系，对不确定性原理进行各种最新的更一般的表述。最后，讨论了各种应用，从纠缠见证到波粒对偶再到量子密码学。

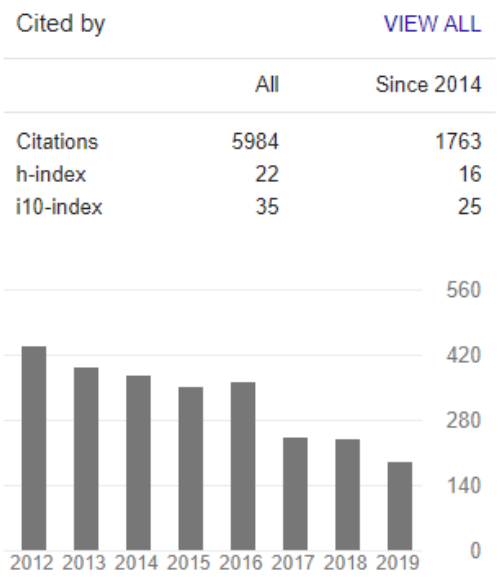
(15)An improved and provably secure privacy preserving authentication protocol for SIP

Reason：SCI 检索，引用 85 次，提出了一种基于 ECC 的隐私保护改进认证方案，该方案提供了相互认证，并抵抗 Tu 等人和 Farash 提到的所有已知攻击。

Task 3:

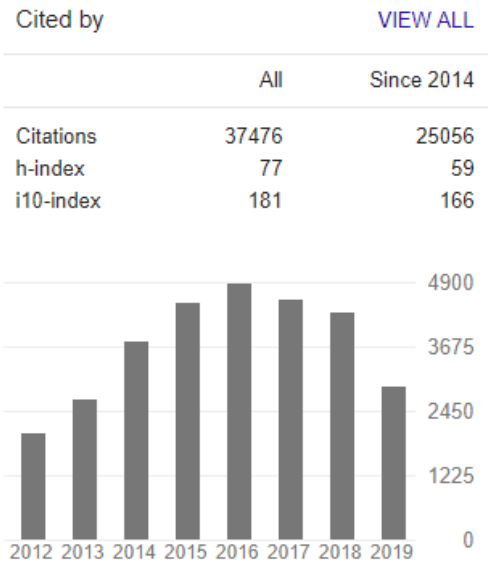
By synthesizing Chinese and English literatures, try to find 5 important authors in this field and introduce their research contents briefly.

(1) Xiaoyun Wang



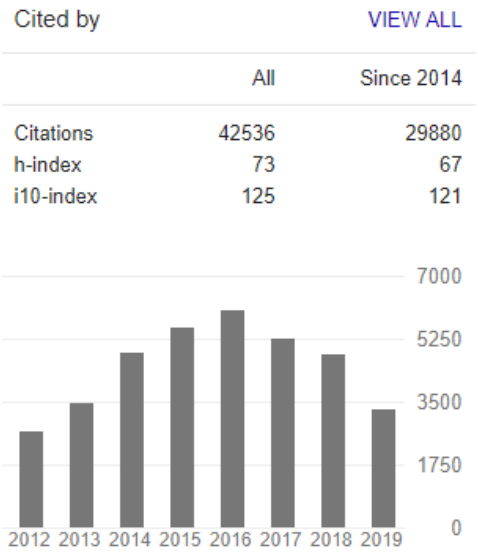
从事密码理论与密码数学问题研究，提出了密码哈希函数的碰撞攻击理论，即模差分比特分析法，提高了破解了包括 MD5、SHA-1 在内的 5 个国际通用哈希函数算法的概率；给出了系列消息认证码 MD5-MAC 等的子密钥恢复攻击和 HMAC-MD5 的区分攻击；提出了格最短向量求解的启发式算法二重筛法；设计了中国哈希函数标准 SM3，该算法在金融、国家电网、交通等国家重要经济领域广泛使用。

(2) Amit Sahai



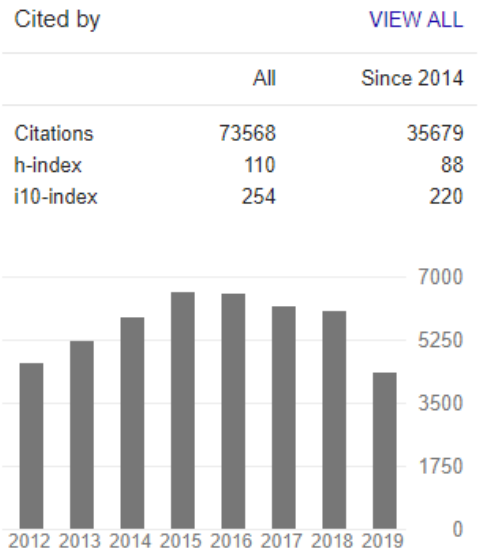
主要研究方向:计算机安全与密码学基础，包括信息论、密码证明、安全多方计算、软件安全和保护。他是基于属性加密、功能加密和模糊不可分辨加密的联合发明人，在 STOC、CRYPTO 和 ACM 杂志上发表了 100 多篇原创技术研究论文。

(3) Brent Waters



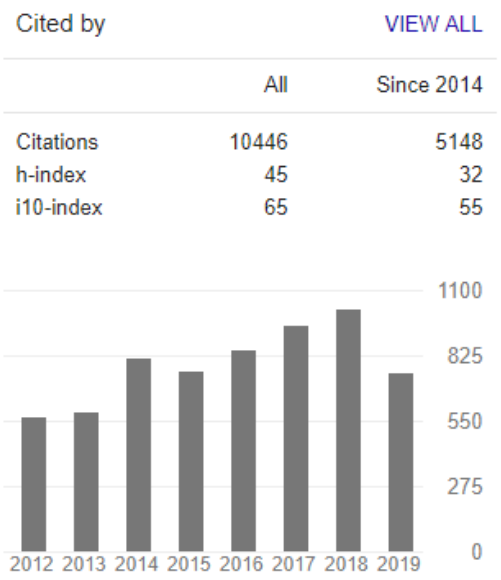
主要研究领域是密码学和计算机安全，2005 年，Waters 与 Amit Sahai 首次提出了基于属性的加密和功能加密的概念。2013 年，Waters 与 Amit Sahai, Sanjam Garg, Craig Gentry, Shai Halevi，和 Mariana Raykova 一起发表了一篇论文，证明了混淆原语的不可分辨性

(4) Dan Boneh



主要研究领域是密码学、计算机安全以及计算机科学理论。Boneh 与加州大学戴维斯分校的 Matt Franklin 一起，是 Weil 对基于配对的密码学发展的主要贡献者之一。

(5) Daniele Micciancio



主要研究领域有：点阵和编码问题的算法、复杂性和密码学应用；密码协议的符号分析(计算机和网络安全的正式方法)；密码学中的许多其他主题(例如，零知识证明、具有特殊属性的密码原语)