



《信息安全专业概况》

**（黑体2号字）**

|  |  |
| --- | --- |
| **专 业** | **信息安全** |
| **姓 名** | **亢赋洲** |
| **日 期** | **2022/9/9** |

**摘 要**

信息安全专业是管理[网络安全](https://baike.so.com/"/doc/1276211-1349506.html/"" \t "https://baike.so.com/doc/\\"_blank\\")的一个专业。根据教育部《普通高等学校本科专业目录 》，专业代码为080904K，属于计算机类(0809)。具有全面的信息安全专业知识，使得学生有较宽的知识面和进一步发展的基本能力。

关键词：信息安全、专业简介、研究内容、就业方向

**目 录**

[第1章 信息安全专业简介 - 4 -](#_Toc14478)

[1.1 专业概述 - 4 -](#_Toc8865)

[1.2 培养目标 - 4 -](#_Toc8865)

[1.3 研究内容 - 4 -](#_Toc8865)

[第2章 信息安全课程内容 - 5 -](#_Toc14478)

[2.1 主要课程 - 5 -](#_Toc8865)

[2.1.1 密码学 - 5 -](#_Toc23216)

[2.1.2计算机网络 - 6 -](#_Toc22557)

[第3章 研究前沿 - 7 -](#_Toc14478)

[3. 1 隐私计算 - 7 -](#_Toc8865)

[3.2 公钥密码 - 7 -](#_Toc8865)

[3.3 AI Security - 8 -](#_Toc8865)

[第4章 就业去向 - 9 -](#_Toc14478)

[4. 1 工作需求 - 9 -](#_Toc8865)

[4. 2 就业方向 - 9 -](#_Toc8865)

[4. 3 就业前景 - 9 -](#_Toc8865)

[结 论 - 11 -](#_Toc5560)

[参考文献 - 12 -](#_Toc1841)

**第1章 信息安全专业简介**

## 1.1 专业概述

信息安全专业是管理[网络安全](https://baike.so.com/"/doc/1276211-1349506.html/"" \t "https://baike.so.com/doc/\\"_blank\\")的一个专业。根据教育部《普通高等学校本科专业目录 》，专业代码为080904K，属于计算机类(0809)。具有全面的信息安全专业知识，使得学生有较宽的知识面和进一步发展的基本能力.

加强学科所要求的基本修养，使学生具有本学科科学研究所需的基本素质，为学生今后的发展、创新打下良好的基础;使学生具有较强的应用能力，具有应用已掌握的基本知识解决实际应用问题的能力，不断增强系统的应用、开发以及不断获取新知识的能力。努力使学生既有扎实的理论基础，又有较强的应用能力;既可以承担实际系统的开发，又可进行科学研究。

## 1.2 培养目标

本专业是[计算机](https://baike.so.com/doc/3435270-3615253.html" \t "https://baike.so.com/doc/_blank)、[通信](https://baike.so.com/doc/5725670-5938407.html" \t "https://baike.so.com/doc/_blank)、[数学](https://baike.so.com/doc/5343249-5578692.html" \t "https://baike.so.com/doc/_blank)、[物理](https://baike.so.com/doc/1004722-1062202.html" \t "https://baike.so.com/doc/_blank)、[法律](https://baike.so.com/doc/1296429-1370714.html" \t "https://baike.so.com/doc/_blank)、[管理](https://baike.so.com/doc/1462322-1546098.html" \t "https://baike.so.com/doc/_blank)等学科的[交叉学科](https://baike.so.com/doc/6336902-6550515.html" \t "https://baike.so.com/doc/_blank)，主要研究确保[信息安全](https://baike.so.com/doc/5397333-5634634.html" \t "https://baike.so.com/doc/_blank)的科学与技术。培养能够从事计算机、通信、电子商务、[电子政务](https://baike.so.com/doc/5346917-5582364.html" \t "https://baike.so.com/doc/_blank)、电子金融等领域的信息安全高级专门人才。信息安全的概念在本世纪经历了一个漫长的历史阶段，90年代以来得到了深化。进入21世纪，随着信息技术的不断发展，信息安全问题也日显突出。如何确保信息系统的安全已成为全社会关注的问题。国际上对于信息安全的研究起步较早，投入力度大，已取得了许多成果，并得以推广应用。目前国内已有一批专门从事信息安全基础研究、技术开发与技术服务工作的研究机构与高科技企业，形成了我国信息安全产业的雏形，但由于国内专门从事信息安全工作技术人才严重短缺，阻碍了我国信息安全事业的发展。信息安全专业是十分具有发展前途的专业。

## 1.3 研究内容

信息安全专业主要学习内容有：信息安全、网络与通讯安全、数据库与信息安全 、  
软件与系统权架构安全等。可以发现，不论信息安全、网络安全，还是系统安全，或是研究数据的安全性、或是网络协议的安全性、或是加密解密技术，虽然分支研究的侧重点不同，但很多分支不可避免的属于交叉的分支。

**第2章 信息安全课程内容**

## 2.1主要课程

根据哈尔滨工业大学对信息安全本科生的培养方案，设置的主要课程如下：  
 1. 数学与自然科学基础。包括微积分、代数与几何、概率论与数理统计等数学基础知识，以及物理、生命科学等自然科学基础知识。

1. 人文社会科学类知识。包括人文与社会、经济与管理、科学与工程等方面的基础知识。
2. 大类专业基础知识：（1）离散结构，（2）算法与复杂性，（3）计算机组织与结构，（4）操作系统，（5）程序设计语言，（6）系统基础，（7）软件开发基础，（8）软件工程，（9）网络与通信，（10）信息管理，（11）人工智能，（12）信息保障与安全，（13）社会问题与专业实践等知识领域。
3. 专业核心知识：（1）密码学，（2）信息系统安全，（3）网络安全，（4）信息内容安全(含多媒体安全)，（5）逆向分析，（6）云安全，（7）舆情分析。

可以发现，信息安全专业四年中学习的课程内容还是很多的。本文受限与篇幅无法一一介绍，只会着重挑选出其中比较重要的几门课程进行详细地介绍。

## 2.1.1 密码学

密码学是研究编制密码和破译密码的技术科学。研究密码变化的客观规律，应用于编制密码以保守通信秘密的，称为编码学；应用于破译密码以获取通信情报的，称为破译学。总称密码学。

密码学（在西欧语文中，源于希腊语kryptós“隐藏的”，和gráphein“书写”）是研究如何隐密地传递信息的[学科](https://baike.so.com/doc/5422096.html" \t "https://baike.so.com/doc/_blank)。在现代特别指对信息以及其传输的数学性研究，常被认为是数学和计算机科学的分支，和信息论也密切相关。著名的密码学者Ron Rivest解释道：“密码学是关于如何在敌人存在的环境中通讯”，自[工程学](https://baike.so.com/doc/6117077.html" \t "https://baike.so.com/doc/_blank)的角度，这相当于密码学与纯数学的异同。密码学是信息安全等相关议题，如认证、访问控制的核心。密码学的首要目的是隐藏信息的[涵义](https://baike.so.com/doc/6941321.html" \t "https://baike.so.com/doc/_blank)，并不是隐藏信息的存在。密码学也促进了计算机科学，特别是在于电脑与网络安全所使用的技术，如访问控制与信息的机密性。密码学已被应用在日常生活：包括自动柜员机的[芯片卡](https://baike.so.com/doc/4014765.html" \t "https://baike.so.com/doc/_blank)、电脑使用者存取密码、[电子商务](https://baike.so.com/doc/5333306.html" \t "https://baike.so.com/doc/_blank)等等。

密码是通信双方按约定的法则进行信息特殊变换的一种重要保密手段。依照这些法则，变明文为[密文](https://baike.so.com/doc/5568274.html" \t "https://baike.so.com/doc/_blank)，称为加密变换；变密文为[明文](https://baike.so.com/doc/415176.html" \t "https://baike.so.com/doc/_blank)，称为脱密变换。密码在早期仅对文字或数码进行加、脱密变换，随着通信技术的发展，对语音、图像、数据等都可实施加、脱密变换。

哈工大此课程使用的教材是《现代密码学 原理与协议》，是世界上密码学最权威的教材之一。

## 2.1.2 计算机网络

计算机网络是指将[地理](https://baike.baidu.com/item/%E5%9C%B0%E7%90%86?fromModule=lemma_inlink" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%BD%91%E7%BB%9C/_blank)位置不同的具有独立功能的多台[计算机](https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA/140338?fromModule=lemma_inlink" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%BD%91%E7%BB%9C/_blank)及其外部设备，通过通信线路连接起来，在[网络操作系统](https://baike.baidu.com/item/%E7%BD%91%E7%BB%9C%E6%93%8D%E4%BD%9C%E7%B3%BB%E7%BB%9F/3997?fromModule=lemma_inlink" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%BD%91%E7%BB%9C/_blank)，[网络管理软件](https://baike.baidu.com/item/%E7%BD%91%E7%BB%9C%E7%AE%A1%E7%90%86%E8%BD%AF%E4%BB%B6/6579078?fromModule=lemma_inlink" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%BD%91%E7%BB%9C/_blank)及[网络通信协议](https://baike.baidu.com/item/%E7%BD%91%E7%BB%9C%E9%80%9A%E4%BF%A1%E5%8D%8F%E8%AE%AE/4438611?fromModule=lemma_inlink" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%BD%91%E7%BB%9C/_blank)的管理和协调下，实现[资源共享](https://baike.baidu.com/item/%E8%B5%84%E6%BA%90%E5%85%B1%E4%BA%AB/233480?fromModule=lemma_inlink" \t "https://baike.baidu.com/item/%E8%AE%A1%E7%AE%97%E6%9C%BA%E7%BD%91%E7%BB%9C/_blank)和信息传递的计算机系统。 [1]

计算机网络主要是由一些通用的、可编程的硬件互连而成的，而这些硬件并非专门用来实现某一特定目的（例如，传送数据或视频信号）。这些可编程的硬件能够用来传送多种不同类型的数据，并能支持广泛的和日益增长的应用。

哈工大使用的教材为《计算机网络 自顶向下方法》，作者是(美)库罗斯。是当前世界上最为流行的计算机网络教科书之一，讲解以[因特网](https://baike.so.com/doc/2011565-2128705.html" \t "https://baike.so.com/doc/_blank)为例，学以致用。

**第3章 研究前沿**

## 3.1 隐私计算

对于企业而言，数据需要尽可能的高速流通才能创造更多的价值。而面对流通过程中如此海量用户数据的安全和隐私，难免变得畏手畏脚、桎梏重重。

隐私计算是多方安全计算、联邦学习、可信任执行环境等技术子项所组成的技术的统称，目的是为了让多个数据拥有者，在不暴露数据本身的前提下，实现数据的互通、共享和计算，发挥出数据本身的最大价值，同时保证数据不会泄露。

我们可以借助[姚期智](https://www.zhihu.com/search?q=%E5%A7%9A%E6%9C%9F%E6%99%BA&search_source=Entity&hybrid_search_source=Entity&hybrid_search_extra={"sourceType":"answer","sourceId":2557968617}" \t "_blank)提出的“百万富翁问题”来理解：有两个百万富翁想比比谁更有钱，但又不想让对方知道自己到底拥有多少财富。那么，隐私计算就可以在不借助第三方的情况下，让他们知道到底谁更有钱。

另外，在隐私计算中，多方安全计算技术是传输、处理数据很关键的一环。其本质上就是对数据进行加密，让数据的参与方可以使用数据却看不见具体信息。

提到数据加密，目前国际范围内认可的、保密性最强的数据传输技术之一：端对端加密技术已经有着成熟的应用市场。

使用该技术的通讯软件只有参与通讯的用户可以读取信息内容，可以很好的防止潜在的窃听者窃取、篡改、和拦截聊天信息。

## 3.2 公钥密码

传统公钥密码体制，即我们知道的RSA，ElGamal加密和签名，已经是三十年前的研究成果了。传统公钥密码学现在的研究内容，主要集中在选择密文安全(chosen ciphertext security)的加密方案构造。这一领域的开创者是Cramer和Shoup。随后，各种各样满足这样的安全方案被提了出来。近期，大约是2007年开始，学者们的方向是selective opening security的公钥加密方案。这一个领域的权威是Bellare。值得注意的是，在这个领域，中国的学者Junzuo Lai在EUROCRYPT 2014上发表了论文，这是国内密码学界很值得庆祝的一个事情。

接下来是函数加密(Functional Encryption)。函数加密以前的基础是双线应对(bilinear map)，现在已经扩展了。函数加密的领导者是斯坦福大学的Boneh教授。Boneh基本统领了公钥密码学，后面的很多代表人物都是他的学生或者是学生的学生。他首先提出了身份基加密(identity-based encryption)，随后他和他的学生一起研究了很多具有多种功能的加密方案，最终将他们统一起来，定义为了函数加密。在函数加密中，有一种有趣的加密方案是属性基加密(attribute-based encryption)，这是一个在现有[云存储](https://www.zhihu.com/search?q=%E4%BA%91%E5%AD%98%E5%82%A8&search_source=Entity&hybrid_search_source=Entity&hybrid_search_extra={"sourceType":"answer","sourceId":30108599}" \t "_blank)安全中比较实用的一类加密方案，因此单独列举出来。这个子领域的代表人物是Waters。

随后是同态加密。这是一个可能会改变计算机发展的加密模式。同态加密的提出者是Gentry，他是Boneh的学生之一。同态加密现在的基础是格密码学(lattice based cryptography)。现在，研究者一方面进一步构造效率更高的同态加密方案，另一方面也转向了演化而来的新密码学工具：多线性对(multilinear map)的构造和应用中。这个是公钥密码学现在最热的研究方向。

如果想了解所有的[密码学](https://www.zhihu.com/search?q=%E5%AF%86%E7%A0%81%E5%AD%A6&search_source=Entity&hybrid_search_source=Entity&hybrid_search_extra={"sourceType":"answer","sourceId":30108599}" \t "https://www.zhihu.com/question/25024086/answer/_blank)最新研究进展，可以参考中国计算机学会(CCF)推荐的顶级会议和期刊中，网络与信息安全部分对应的会议和期刊论文。

3.3 AI Security

AI Security主要包括两个方面: (1) AI for security 和 (2) security of AI。 前者是利用新的技术来更好的解决传统网络安全问题，后者是研究新的技术带来的新安全隐患（而这些安全隐患是传统网络安全技术所无法解决的）。

基本上来说，这个领域主要研究两个主要的部分：模型的安全性和数据安全性。

相对而言，数据安全性与传统的安全研究领域更密切相关。例如，大家会关心数据的隐私性问题（e.g., 差分隐私、加密、水印）和数据的偏见问题 (e.g., 数据的标记给模型带来的偏见，例如一个[超分](https://www.zhihu.com/search?q=%E8%B6%85%E5%88%86&search_source=Entity&hybrid_search_source=Entity&hybrid_search_extra={"sourceType":"answer","sourceId":1733966674}" \t "_blank)的模型更容易把特别模糊的黑人超分为白人)。前者是安全领域一直以来的研究问题，而后者是更加新兴的（也许也是更具潜力的）研究问题。

相反，模型的安全性与传统网络安全领域的研究就存在有较大的差别。基本上这个领域围绕AI模型从训练到部署到预测的各个阶段可能存在的安全性问题展开。例如，在测试阶段，大家研究模型的对抗[鲁棒性](https://www.zhihu.com/search?q=%E9%B2%81%E6%A3%92%E6%80%A7&search_source=Entity&hybrid_search_source=Entity&hybrid_search_extra={"sourceType":"answer","sourceId":1733966674}" \t "_blank) (adversarial robustness), 在训练过程大家研究数据投毒 (data poisoning)、后门攻击 (backdoor attack)等。

1. **就业去向**

4.1 工作需求

安全研发：主要是研发一些安全产品或者安全工具。

安全渗透：为了证明网络防御按照预期计划正常运行而提供的一种机制。不妨假设，你的公司定期更新安全策略和程序，时时给系统打补丁，并采用了[漏洞扫描器](https://www.zhihu.com/search?q=%E6%BC%8F%E6%B4%9E%E6%89%AB%E6%8F%8F%E5%99%A8&search_source=Entity&hybrid_search_source=Entity&hybrid_search_extra={"sourceType":"answer","sourceId":2460023629}" \t "_blank)等工具，以确保所有补丁都已打上。

安全运维：负责维护并确保整个服务的高可用性，同时不断优化系统架构提升部署效率、优化资源利用率提高整体的ROI。

安服：可以理解为售后阶段，像是一些重大节日的网络安全保卫也属于这个阶段的服务内容。

安全实施：在做完安全体系架构设计的基础上做网络安全硬件实施以及相应硬件设备的设置等。

代码审计：检查源代码中的安全缺陷，检查程序源代码是否存在安全隐患，或者有编码不规范的地方，通过自动化工具或者人工审查的方式，对[程序源代码](https://www.zhihu.com/search?q=%E7%A8%8B%E5%BA%8F%E6%BA%90%E4%BB%A3%E7%A0%81&search_source=Entity&hybrid_search_source=Entity&hybrid_search_extra={"sourceType":"answer","sourceId":2460023629}" \t "_blank)逐条进行检查和分析，发现这些源代码缺陷引发的安全漏洞，并提供代码修订措施和建议。

4.2 就业方向

毕业后主要在[新能源](https://www.zhihu.com/search?q=%E6%96%B0%E8%83%BD%E6%BA%90&search_source=Entity&hybrid_search_source=Entity&hybrid_search_extra={"sourceType":"answer","sourceId":1676139510}" \t "https://www.zhihu.com/question/_blank)、互联网、计算机软件等行业工作，大致如下：

1 新能源

2 互联网/电子商务

3 计算机软件

4 房地产

5 贸易/进出口

毕业后主要从事项目经理、[网络工程师](https://www.zhihu.com/search?q=%E7%BD%91%E7%BB%9C%E5%B7%A5%E7%A8%8B%E5%B8%88&search_source=Entity&hybrid_search_source=Entity&hybrid_search_extra={"sourceType":"answer","sourceId":1676139510}" \t "https://www.zhihu.com/question/_blank)、网络管理员等工作，大致如下：

1 项目经理

2 网络工程师

3 网络管理员

4.3 就业前景

（1）国家政策支持

2021年3月9日，《[信息安全技术信息系统密码应用基本要求](https://www.zhihu.com/search?q=%E4%BF%A1%E6%81%AF%E5%AE%89%E5%85%A8%E6%8A%80%E6%9C%AF%E4%BF%A1%E6%81%AF%E7%B3%BB%E7%BB%9F%E5%AF%86%E7%A0%81%E5%BA%94%E7%94%A8%E5%9F%BA%E6%9C%AC%E8%A6%81%E6%B1%82&search_source=Entity&hybrid_search_source=Entity&hybrid_search_extra={"sourceType":"answer","sourceId":2460023629}" \t "_blank)》（GB/T39786-2021）正式发布，并于2021年10月1日起实施。

2021年4月2日，工信部新闻发言人表示将发布《[App个人信息保护管理暂行规定](https://www.zhihu.com/search?q=App%E4%B8%AA%E4%BA%BA%E4%BF%A1%E6%81%AF%E4%BF%9D%E6%8A%A4%E7%AE%A1%E7%90%86%E6%9A%82%E8%A1%8C%E8%A7%84%E5%AE%9A&search_source=Entity&hybrid_search_source=Entity&hybrid_search_extra={"sourceType":"answer","sourceId":2460023629}" \t "_blank)》等系列行业标准。

2021年6月10日，《中华人民共和国数据安全法》正式发布，2021年9月1日起实施。

2021年8月17日，《[关键信息基础设施安全保护条例](https://www.zhihu.com/search?q=%E5%85%B3%E9%94%AE%E4%BF%A1%E6%81%AF%E5%9F%BA%E7%A1%80%E8%AE%BE%E6%96%BD%E5%AE%89%E5%85%A8%E4%BF%9D%E6%8A%A4%E6%9D%A1%E4%BE%8B&search_source=Entity&hybrid_search_source=Entity&hybrid_search_extra={"sourceType":"answer","sourceId":2460023629}" \t "_blank)》正式发布，并于2021年9月1日起施行。

2021年8月20日，十三届全国人大常委会第三十次会议表决通过《[中华人民共和国个人信息保护法](https://www.zhihu.com/search?q=%E4%B8%AD%E5%8D%8E%E4%BA%BA%E6%B0%91%E5%85%B1%E5%92%8C%E5%9B%BD%E4%B8%AA%E4%BA%BA%E4%BF%A1%E6%81%AF%E4%BF%9D%E6%8A%A4%E6%B3%95&search_source=Entity&hybrid_search_source=Entity&hybrid_search_extra={"sourceType":"answer","sourceId":2460023629}" \t "_blank)》，并于2021年11月1日起正式施行。

2021年9月1日，《网络产品安全漏洞管理规定》（以下简称《规定》）施行。

2021年10月19日，第十三届全国人大常委会第三十一次会议对《中华人民共和国反电信网络诈骗法（草案）》进行了初次审议，这是我国首次对打击治理电信网络诈骗进行专门立法，并已在[中国人大](https://www.zhihu.com/search?q=%E4%B8%AD%E5%9B%BD%E4%BA%BA%E5%A4%A7&search_source=Entity&hybrid_search_source=Entity&hybrid_search_extra={"sourceType":"answer","sourceId":2460023629}" \t "_blank)网公布，面向社会公众征求意见。

2021年11月14日，国家网信办发布了《网络数据安全管理条例（征求意见稿）》公开征求意见。

2021年12月，中央网络安全和信息化委员会印发《“十四五”国家信息化规划》（以下简称《规划》），对我国“十四五”时期信息化发展作出部署安排。

2021年，公安部部署全国公安机关深入推进“净网2021”专项行动，各地公安网安部门紧密结合党史学习教育和队伍教育整顿，聚焦人民群众关切的网络违法犯罪和网络乱象，持续深化网络违法犯罪打击、网络生态治理和秩序整治。

（2）网络安全市场规模

随着数字经济的发展，网络安全作为必要保障，其投入将持续增加。数据显示，中国网络安全市场从2016年的269.5亿元增长至2020年的531.9亿元，预计在2022年底将达到704.3亿元。

（3）人才缺口

据2021年网络安全宣传周的白皮书显示，网络安全产业人才需求高速增长，目前网络安全行业存在巨大人才缺口，平均供求比约为1：2，存在资深人才储备不足、新人培养和育留难度大等挑战。

从上面三点足以看出信息安全行业发展前景相当可观。

**结 论**

信息安全的概念在二十世纪经历了一个漫长的历史阶段，90年代以来得到了深化。进入21世纪，随着互联网的发展，传统的网络边界不复存在，给未来的互联网应用和业务带来巨大改变，给信息安全也带来了新挑战。融合开放是互联网发展的特点之一，网络安全也因此变得正在向分布化、规模化、复杂化和间接化等方向发展，信息安全产业也将在融合开放的大安全环境中探寻发展。国际上对于信息安全的研究起步较早，投入力度大，已取得了许多成果，并得以推广应用。中国已有一批专门从事信息安全基础研究、技术开发与技术服务工作的研究机构与高科技企业，形成了中国信息安全产业的雏形，但由于中国专门从事信息安全工作技术人才严重短缺，阻碍了中国信息安全事业的发展。[信息安全专业](https://baike.so.com/doc/1764470-1865853.html" \t "https://baike.so.com/doc/_blank)是十分具有发展前途的专业。我们需要充分认识到当今社会信息安全的重要性，把握住时代的风口，为各行各业作出贡献。

**参考文献**

[1] 钟志永 姚珺．大学计算机应用基础．重庆：重庆大学出版社，2012：144-146 [[2] 赵立坚：美议员贼喊捉贼，中国人民很生气](https://baike.baidu.com/reference/339810/beeb2wWrJyArDA36jWgo89xsAD0JpSvdN_eHOzfJCpxw0FSNWgEpj_xWgQPpFqpgdYG69AKDef1VQ7i05KY0YRhKnA67hyTKasNjupRqv7yWbF40nucKDbZ8jwB7jgy_0dhS" \t "https://baike.baidu.com/item/%E4%BF%A1%E6%81%AF%E5%AE%89%E5%85%A8/_blank) ．百家号[引用日期2021-09-11

[3] [发展我国信息安全产业的对策](https://baike.baidu.com/reference/339810/a7d4xPeSlfTvfUdmqbJpIStvH0ah6rFX4gMHBOjByZdbHCXT9GvyN_khmPmspDlny48YokxSjxnLs1Vm91IrR8vXNgamEOWXgIFpMovlSmWGS3wuZjKcj0cjjPlHZU1JREXNujWkLB7XDImKuHjkWnAJBWwbqqMobjDKcHNyfTQ1Uc2fD7f6GsF1rRc_P8jdamr2I4HBmwiA0U7ruw8uoTC9QW5ju6UHU5LAbT25LDULGbcphecQc5QFhIPShyyhpwZWztspFKQB95xE5XZh39luaGebW0s" \t "https://baike.baidu.com/item/%E4%BF%A1%E6%81%AF%E5%AE%89%E5%85%A8/_blank) ．中国知网[引用日期2020-03-06]

[4] [信息安全与加密技术](https://baike.baidu.com/reference/339810/69dfyfFQlckgp03Dmsprv_knIVRXi5TvzMmoyMv9fu7GAsWYQC2UXAFHT4BfjP4f9UG2VQgTGlNICHYoX2NqQDHjUwCgbZ6AMep2CT07-rZkc9fMTLUvAHoJgd1Me6Iyl72TARRKCi6_" \t "https://baike.baidu.com/item/%E4%BF%A1%E6%81%AF%E5%AE%89%E5%85%A8/_blank) ．万方数据知识服务平台[引用日期2019-10-18]

[5] [网络环境下的信息安全](https://baike.baidu.com/reference/339810/10b1T1kN20WZqZ3lEquMQUzsQP9RXT6NP3A1Bk12jSorj6JdcfCrNvuXqqxHbDRCp6DiCKVyuJRUl152qO-dQY0pXbRssVq10ipfkAJ-W9gzSEhw8iR0qrsvM8DeizK2qn5lZog10mLx" \t "https://baike.baidu.com/item/%E4%BF%A1%E6%81%AF%E5%AE%89%E5%85%A8/_blank) ．万方数据知识服务平台[引用日期2019-10-18]

[6] [大数据时代的个人信息安全问题与对策](https://baike.baidu.com/reference/339810/de66MT7gl444lDp2h_sJB1r9ZKCHyOv0j_GgFd3hS7MONVPdYE6TsROORQbv8eddlLXSRhGQssJytdGnugHuljoZ8MINKaWDe7lH4V8R1VjvGJlRTEcLomjyeWNzjNj8MMwbuOAalISW" \t "https://baike.baidu.com/item/%E4%BF%A1%E6%81%AF%E5%AE%89%E5%85%A8/_blank) ．万方数据知识服务平台[引用日期2019-10-18]