



信息安全专业概述

|  |  |
| --- | --- |
| **专 业** | **信息安全** |
| **姓 名** | **李骏成** |
| **日 期** | **2022/9/8** |

**摘 要**

随着计算机技术与网络通信技术的广泛应用，社会对计算机的依赖越来越大，而计算机系统的安全一旦受到破坏，不仅会导致严重的社会混乱，也会带来巨大的经济损失。因此信息安全已成为信息科学的热点课题，信息安全专业也受到了社会各界的普遍关注。

信息安全学科是由数学、计算机科学与技术、信息与通信工程和电子科学与技术等学科交叉而成的一门综合性学科。目前主要研究领域涉及现代密码学、计算机系统安全、计算机与通信网络安全、信息系统安全、电子商务、电子政务系统安全等。

目前信息安全方面的人才还十分稀少，尤其是政府、国防、金融、公安和商业等部门对信息安全人才的需求很大。目前国内从事信息安全的专业人才人数并不多，并且大多分布在高校和研究院所，按照目前信息化发展的状况，社会对信息安全专业的人才需求量达几十万人。要解决供需矛盾，必须加快信息安全人才的培养。

本文将重点进行专业研究内容介绍、专业主要课程介绍、专业学习建议和指导、目前专业前沿研究方向介绍、专业本科毕业生去向介绍，全面阐述信息安全专业相关信息，对信息安全专业产生全面、正确的认知。

**目 录**

[**第1章 专业研究内容介绍** - 1 -](#_Toc113560648)

[1.1 信息安全方向 - 1 -](#_Toc113560649)

[1.1.1 操作系统安全 - 1 -](#_Toc113560650)

[1.1.2 数据库安全 - 1 -](#_Toc113560651)

[1.1.3 物理安全 - 2 -](#_Toc113560652)

[1.2 网络空间安全方向 - 2 -](#_Toc113560653)

[第二章 专业主要课程内容 - 3 -](#_Toc113560654)

[2.1 总体框架 - 3 -](#_Toc113560655)

[2.2 理论课程 - 3 -](#_Toc113560656)

[2.2.1 通识类知识 - 3 -](#_Toc113560657)

[2.2.2 学科基础知识 - 3 -](#_Toc113560658)

[2.2.3 专业知识 - 3 -](#_Toc113560659)

[2.3 实践教学 - 4 -](#_Toc113560660)

[第三章 专业学习建议与指导 - 4 -](#_Toc113560661)

[第四章 目前专业的前沿研究方向 - 4 -](#_Toc113560662)

[4.1 隐私计算 - 4 -](#_Toc113560663)

[4.2 公钥密码学 - 5 -](#_Toc113560664)

[4.2.1 传统公钥体制 - 5 -](#_Toc113560665)

[4.2.2 函数加密 - 5 -](#_Toc113560666)

[4.3 AI安全 - 5 -](#_Toc113560667)

[4.4 量子密码 - 6 -](#_Toc113560668)

[第五章 专业本科毕业生去向 - 6 -](#_Toc113560669)

[**结 论** - 7 -](#_Toc113560670)

[**参考文献** - 8 -](#_Toc113560671)

**第1章 专业研究内容介绍**

## 1.1 信息安全方向

在哈尔滨工业大学计算学部下设的信息安全学院中，还分为两个方向，一个是信息安全方向，一个是网络空间安全方向，这一部分中主要介绍信息安全方向。

信息安全专业是一门普通高等学校本科专业，属于计算机类专业，基本修业年限为四年，授予管理学或理学或工学学士学位。该专业是计算机、通信、数学、物理、法律、管理等学科的交叉学科，主要研究确保信息安全的科学与技术。培养能够从事计算机、通信、电子商务、电子政务、电子金融等领域的信息安全高级专门人才。

信息安全包括网络安全，信息安全还包括操作系统安全，数据库安全，硬件设备和设施安全，物理安全，人员安全，软件开发，应用安全等。信息安全侧重于计算机数据和信息的安全。

### 1.1.1 操作系统安全

操作系统作为计算机系统的基础软件是用来管理计算机资源的，它直接利用计算机硬件并为用户提供使用和编程接口。各种应用软件均建立在操作系统提供的系统软件平台之上，上层的应用软件要想获得运行的高可靠性和信息的完整性、保密性，必须依赖于操作系统提供的系统软件基础，任何想象中的、脱离操作系统的应用软件的高安全性，就如同幻想在沙滩上建立堡垒一样，毫无根基可言。不难想象，在网络环境中，网络系统的安全性依赖于网络中各主机系统的安全性，而主机系统的安全性正是由其操作系统的安全性所决定的，没有安全的操作系统的支持，网络安全也毫无根基可言。所以，操作系统安全是计算机网络系统安全的基础。

### 1.1.2 数据库安全

数据库安全包含两层含义：第一层是指系统运行安全，系统运行安全通常受到的威胁如下，一些网络不法分子通过网络，局域网等途径通过入侵电脑使系统无法正常启动，或超负荷让机子运行大量算法，并关闭cpu风扇，使cpu过热烧坏等破坏性活动； 第二层是指系统信息安全，系统安全通常受到的威胁如下，黑客对数据库入侵，并盗取想要的资料。数据库系统的安全特性主要是针对数据而言的，包括数据独立性、数据安全性、数据完整性、并发控制、故障恢复等几个方面。

数据库安全的防护技术有：数据库加密（核心数据存储加密）、数据库防火墙（防漏洞、防攻击）、数据脱敏（敏感数据匿名化）等。

### 1.1.3 物理安全

物理安全描述了旨在拒绝未经授权访问设施、设备和资源并保护人员和财产免受损害或伤害的安全措施。物理安全涉及使用多层相互依赖的系统，包括闭路电视监控、保安、防护屏障、锁、访问控制、周界入侵检测、威慑系统、消防，以及其他旨在保护人员和财产的系统。

受保护设施的物理安全系统通常旨在：

* 阻止潜在的入侵者（例如警告标志、安全照明和周边标记）；
* 检测入侵并监控/记录入侵者（例如入侵者警报和闭路电视系统）；和
* 触发适当的事件响应（例如由保安和警察）。

安全设计人员、架构师和分析师需要平衡安全控制与风险，同时考虑指定、开发、测试、实施、使用、管理、监控和维护控制的成本，以及更广泛的问题，如美学、人权利、健康和安全以及社会规范或公约。适合高度戒备监狱或军事场所的物理访问安全措施可能不适用于办公室、家庭或车辆，尽管原则相似。

## 1.2 网络空间安全方向

网络空间安全是一门普通高等学校本科专业，属计算机类专业，基本修业年限为四年，授予工学学士学位。

该专业培养德、智、体等全面发展，掌握网络空间安全理论基础和专业知识，熟悉相关领域发展动态，具有强的工程实践和系统开发能力，具有独立从事网络与信息系统的安全分析、设计、集成、开发、测试、维护等的能力，能够独立的解决工程应用领域的技术难题，具备较强的工程实践创新能力；具有强的工程项目的组织与管理能力、技术创新和系统集成能力；具备网络空间安全领域科学研究、技术开发和工程应用服务工作能力的行业骨干和领军人才。

# 第二章 专业主要课程内容

## 2.1 总体框架

信息安全专业的知识体系包括通识类知识、学科基础知识、专业知识和实践性教学等。课程体系须支持各项毕业要求的有效达成，进而保证专业培养目标的有效实现。人文社会科学类课程约占15%，数学和自然科学类课程约占15%，实践约占20%，学科基础知识和专业知识课程约占30%。

人文社会科学类教育能够使学生在从事工程设计时考虑经济、环境、法律、伦理等各种制约因素。

数学和自然科学类教育能够使学生掌握理论和实验方法，为学生表述工程问题、选择恰当数学模型、进行分析推理奠定基础。

学科基础类课程包括学科的基础内容，能体现数学和自然科学在该专业中应用能力的培养；专业类课程、实践环节能够体现系统设计和实现能力的培养。

课程体系的设置有企业或行业专家有效参与。

## 2.2 理论课程

### 2.2.1 通识类知识

通识类知识包括人文社会科学类、数学和自然科学类两部分。人文社会科学类知识包括经济、环境、法律、伦理等基本内容；数学和自然科学类知识包括高等工程数学、概率论与数理统计、离散结构、力学、电磁学、光学与现代物理的基本内容。

### 2.2.2 学科基础知识

学科基础知识被视为专业类基础知识，培养学生计算思维、程序设计与实现、算法分析与设计、系统能力等专业基本能力，能够解决实际问题。

建议教学内容覆盖以下知识领域的核心内容：程序设计、数据结构、计算机组成、操作系统、计算机网络、信息管理，包括核心概念、基本原理以及相关的基本技术和方法，并让学生了解学科发展历史和现状。

### 2.2.3 专业知识

培养学生将基本原理与技术运用于信息安全科学研究、技术开发和应用服务等工作的能力。建议教学内容包含信息科学基础、信息安全基础、密码学、网络安全、信息系统安全、信息内容安全等知识领域的基本内容。以下为核心课程体系示例：

信息安全导论、信息安全数学基础、模数电路与逻辑、程序设计、数据结构与算法、计算机组成与系统结构、EDA技术及应用、操作系统原理及安全、编译原理、信号与系统、通信原理、密码学、计算机网络、网络与通信安全、软件安全、逆向工程、可靠性技术、嵌入式系统安全、数据库原理及安全、取证技术、信息内容安全。

## 2.3 实践教学

具有满足教学需要的完备实践教学体系。主要包括实验课程、课程设计、实习、毕业设计（论文），4年总的实验当量不少于2万行代码。积极开展科技创新、社会实践等多种形式的实践活动，到各类工程单位实习或工作，取得工程经验，基本了解本行业状况。

# 第三章 专业学习建议与指导

学习需要一个良好的学习习惯，建议刚开始一定要精通一项程序语言，学习其他的就会一通百通。过程中是按步骤学习，绝不半途看见苹果丢了梨，一定要强迫自己抵制新鲜技术的诱惑。信息安全其实是个广而深的领域，可以细分为操作系统安全、数据库安全、网络爬虫、web安全、渗透测试、自动化运维、代码审计、应急响应等等，至于学什么，就需要看你自己对哪方面感兴趣，正所谓兴趣是最好的老师，注重技术的积累。

实时关注一些比赛信息，例如：CTF大赛、强网杯、网鼎杯、天府杯、长安杯等，都是相关的比赛项目，平时的话可以自己在靶场挖挖漏洞，练习一下。信息安全行业最注重实践，靶场练习是必不可少的，靶场有很多大牛，还可以定向练习，技术提升了也可以增加秋招成功的几率。

同时也不能过于注重比赛，还是要以学校的学习成绩放在主位的，学校中学习的内容是一切的基础，一定要将基础打牢，这样才能从根本提高自身对于技术的认知深度，否则不理解根本原理，一切都是流于表面，真正有深度的技术是无法真正地灵活使用的。

# 第四章 目前专业的前沿研究方向

## 4.1 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。对此，数牍科技副总裁张迎春提出：隐私计算是破解数据安全和数据要素价值发挥矛盾的“技术解”。国际咨询机构IDC中国日前发布的《隐私计算全景研究》报告也对隐私计算的发展潜力作出了数据解读：2021年中国隐私计算市场规模突破8.6亿元。

今年的政府工作报告也首度将“数字经济治理”写入其中，目的是在数据市场的快速发展的当下，平衡数据安全与开放利用之间的关系。采取的具体措施包括《个人信息法》《数据安全法》的颁布以及各种行政管理办法的出台。

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。

## 4.2 公钥密码学

### 4.2.1 传统公钥体制

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。这一领域的祖师爷是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。因为这个名词还没有权威的翻译，我也不敢乱翻了。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。

### 4.2.2 函数加密

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。

## 4.3 AI安全

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 (adversarial robustness), 在训练过程大家研究数据投毒 (data poisoning)、后门攻击 (backdoor attack)等。

## 4.4 量子密码

加密是保障信息安全的重要手段之一。当前最常用的加密技术是用复杂的数学算法来改变原始信息。这种方法虽然安全性较高，但存在被破译的可能，并非绝对可靠。而量子密码术是一种截然不同的加密方法。

量子密码就像一个物体一样，当陌生人想要复制它或者是破解它，必然会刺激到量子，这时它就会在原来的基础上发生改变，这就导致陌生人破解的量子不再是原来的量子，所以别人想要复制或者是破解它，都是没有意义的存在，正因为这种特殊的性质让量子密码技术变得神秘且不可能破解，从而能够更有效地保证信息数据的安全，所以说量子密码技术是“牢不可破的密码系统”。所以任何想测算和破译密钥的人，都会因改变量子状态而得到无意义的信息，而信息合法接收者也可以从量子态的改变而知道密钥曾被截获过。从理论上来说，用量子密码加密的通信不可能被窃听，安全程度极高。世界上第一个量子密码通信网络2004年6月3日在美国马萨诸塞州剑桥城正式投入运行。

# 第五章 专业本科毕业生去向

1.信息安全专业的毕业生可以做网络警察，网络警察是以网络技术为主要手段，集打击犯罪、管理防范等于一体的综合性实战警种。除了侦破案件外，还肩负着监控公共信息、参与互联网有害信息专项清理整治工作，协调有关部门，删除网站有害信息、加强公安科技建设等。

2.运维类岗位也是信息安全专业的一个就业方向，目前很多安全类专业的毕业生会从事运维类岗位，这就要求信息安全专业的学生要具有较强的动手实践能力。运维类岗位往往需要具备三大块知识基础，其一是计算机网络知识;其二是操作系统知识;其三是存储知识。

3.网络工程师也是信息安全专业的一个就业方向，主要负责对网络障碍的分析，及时处理和解决网络中出现的问题。负责机房线路的布置和协议的规范工作。负责计算机间的网络联接及网络共享，并负责网络间安全性的设置。负责系统网络的拓扑图的建立和完善，并做好系统路由的解析和资料的整理。

信息是社会发展的重要战略资源。在网络信息技术高速发展的今天，信息安全专业可谓是最受人重视的。毕业生可在政府机关、国家安全部门、银行、金融、证券、通信领域从事各类信息安全系统、计算机安全系统的研究、设计、开发和管理工作，也可在IT领域从事计算机应用工作。

**结 论**

信息安全专业，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。

信息是社会发展的重要战略资源。国际上围绕信息的获取、使用和控制的斗争愈演愈烈，信息安全成为维护国家安全和社会稳定的一个焦点，各国都给以极大的关注和投入。网络信息安全已成为亟待解决、影响国家大局和长远利益的重大关键问题，它不但是发挥信息革命带来的高效率、高效益的有力保证，而且是抵御信息侵略的重要屏障，信息安全保障能力是21世纪综合国力、经济竞争实力和生存能力的重要组成部分，是世纪之交世界各国都在奋力攀登的制高点。信息安全问题全方位地影响我国的政治、军事、经济、文化、社会生活的各个方面，如果解决不好将使国家处于信息战和高度经济金融风险的威胁之中。总之，在网络信息技术高速发展的今天，信息安全已变得至关重要，信息安全已成为信息科学的热点课题。目前我国在信息安全技术方面的起点还较低，国内只有极少数高等院校开设信息安全专业，信息安全技术人才奇缺。本专业毕业生可在政府机关、国家安全部门、银行、金融、证券、通信领域从事各类信息安全系统、计算机安全系统的研究、设计、开发和管理工作，也可在IT领域从事计算机应用工作。我们应充分认识信息安全在网络信息时代的重要性和其具有的极其广阔的市场前景，适应时代，抓住机遇!

**参考文献**

[1] 杜晓玉,李辉,张磊,周毅.新工科的信息安全专业建设规划研究[J].计算机时代,2022(09):127-131.DOI:10.16644/j.cnki.cn33-1094/tp.2022.09.029.

[2] 肖蓉,崔晓晖.网络空间安全专业人才能力培养模式探索[J].软件导刊,2021,20(07):187-191.

[3] 信息安全专业就业前景(百度文库): https://wenku.baidu.com/view/b87dee9e8462caaedd3383c4bb4cf7ec4bfeb65f.html?fr=income1-wk\_app\_search\_ctr-search

[4] 信息安全专业介绍(百度文库): https://wenku.baidu.com/view/df1e1f7801f69e3143329426.html?fr=income2-doc-search