密码学

第一讲　信息安全概论

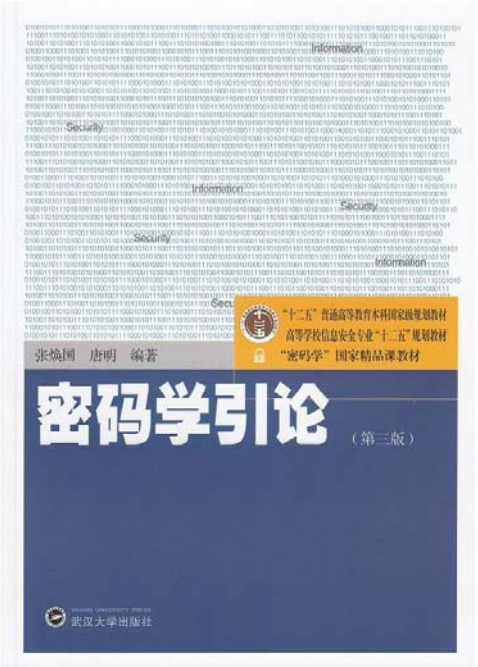
王后珍
whz@whu.edu.cn
13437279329

武汉大学国家网络安全学院
空天信息安全与可信计算教育部重点实验室

教材

- 普通高等教育“十二五”国家规划教材
- 高等学校信息安全专业规划教材
- 《密码学引论》第3版
- 张焕国 唐明 编著
- 武汉大学出版社
- 国家精品课程

  http://www.icourses.cn



武漢大学

教材

- **教材：**
  - 张焕国、唐明，《密码学引论》第三版，武汉大学出版社，2015。

- **参考书：**
  - 王后珍、李莉、杜瑞颖等译，张焕国 审校，《密码学与网络安全》第七版，电子工业出版社，2017。
  - 杨波，《现代密码学》，清华大学出版社，2003。
  - 张焕国、覃中平 等著，《演化密码引论》，武汉大学出版社，2010。

课程介绍

- 理论课
  - 课程中文名称：《密码学》
  - 课程英文名称：Cryptology
  - 时间：周一上午**3-5**节（**9:50-12:15**）
  - 地点：**3区1-616**
  - 课程类型：必修课程
  - 课程学分数：3
  - 课程学时数：54学时(1-18周*每周3学时)
  - 授课对象：信息安全专业本科学生

课程介绍

- 实验课
  - 课程名称：《密码学课程设计》
  - 时间：待定
  - 地点：待定
  - 课程类型：必修课程
  - 课程学时数：36学时
  - 授课对象：信息安全专业本科学生

目 录

目 录

实验课内容

教学内容	学时	实验内容	学时
1、密码学的基本概念	3		
2、古典密码	3	古典密码的编程实现	实验：4
3、数据加密标准(DES)	3	DES的编程实现	实验：4
4、高级数据加密标准(AES)	3	AES密码的编程实现	实验：4
5、我国商用密码SMS4	3	SMS4密码的编程实现	实验：4
6、分组密码的应用技术	3		
7、序列密码	4	序列密码的编程实现	实验：4
8、复习：对称密码	4		

实验课内容

教学内容	学时	实验内容	学时
9、公开密钥密码	6	RSA算法的实现	实验：4
10、数字签名	4		
11、HASH函数	3		
12、认证	4		
13、密钥管理	4	公钥系统的使用	实验：4
14、PKI技术	3		
15、复习：公钥密码	4		
		综合实验 文件加密软件系统	8

武漢大学

Dependences

- 先修课程
  - 高等数学、线性代数、离散数学、概率论与数理统计、信息安全数学基础
  - 高级语言程序设计、数据结构、算法设计与分析
  - 电路与电子技术、数字逻辑、计算机组成原理
- 后续课程
  - 网络安全、电子商务。。。

教学目的

- 密码学由密码编制学和密码分析学组成。密码编制学研究编制高质量密码的理论与技术，密码分析学研究分析和破译密码的理论和技术。这两者相辅相成，共同组成密码学。
- 密码学是信息安全学科的重要组成部分，密码技术是信息安全领域的关键技术。密码学的知识和实践能力是《信息安全专业指导性专业规范》中规定的必修内容。因此，《密码学》在信息安全专业中是必修课程。
- 通过《密码学课程》的教学，使学生掌握密码学的基本知识、基本理论和基本技术。通过配套的实验课程《密码学课程设计》的教学，使学生掌握密码学的基本实践能力。为今后的工作和学习，奠定密码学的基础。

教学要求

- 通过本课程的教学，要求学生掌握密码学的基本知识、基本理论和基本技术。通过配套的实验课程《密码学课程设计》的教学，要求学生掌握密码学的基本实践能力。为今后的工作和进一步学习，奠定密码学的基础。

考核方式

- 平时成绩30%
  - 课堂
  - 作业
- 期末成绩70%

密码学

第一讲　信息安全概论

王后珍

武汉大学计算机学院

空天信息安全与可信计算教育部重点实验室

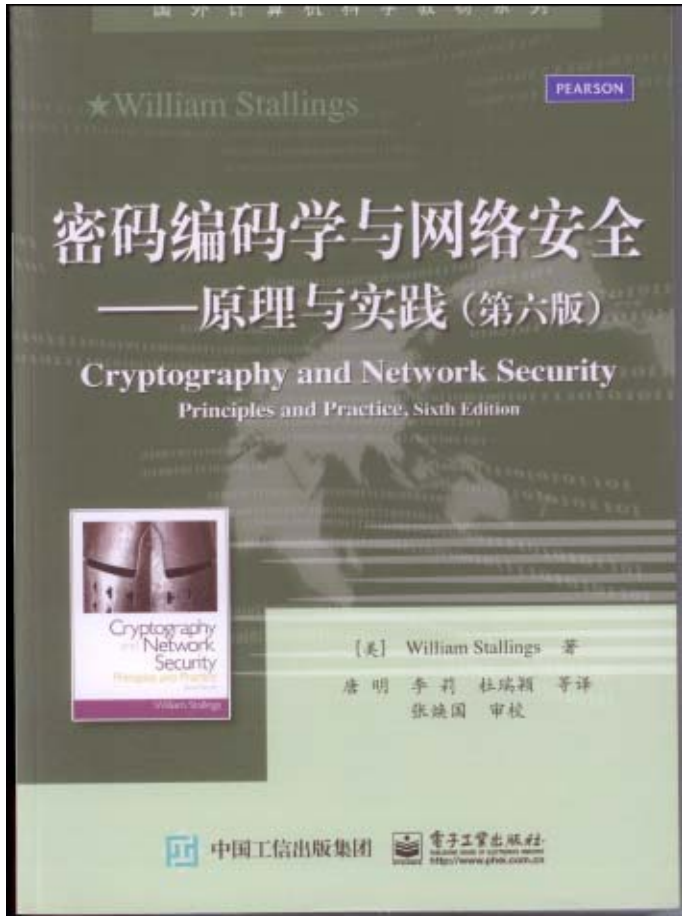
目 录

目 录

教材与主要参考书

教材

参考书



本讲内容

一、二十一世纪是信息的时代

二、信息安全形势严峻

三、网络空间安全学科概论

四、武汉大学的网络空间安全学科

一、二十一世纪是信息的时代

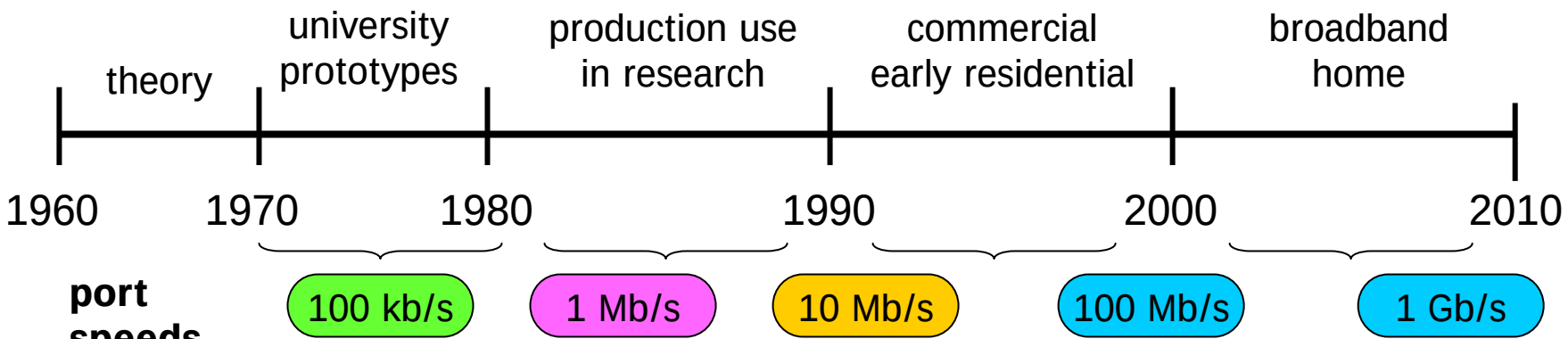
1、二十一世纪是信息时代

- 人类社会在经历了机械化、电气化之后，进入了一个崭新的信息化时代。
- 信息产业超过钢铁、机械、石油、汽车、电力等传统产业，成为世界第一大产业。
- 信息和信息技术改变着人类的生活和工作方式。离开计算机、网络、电视和手机等电子信息设备，人们将无法生活和工作。
- 信息成为重要的战略资源。信息的获取、存储、传输、处理和安全保障能力成为综合国力和经济竞争力的重要组成部分。

一、二十一世纪是信息的时代

1、二十一世纪是信息时代

- 信息社会正按新摩尔定律、吉尔德定律、千倍定律高速发展：
  - 新摩尔定律：芯片集成度、CPU处理能力，每18个月翻一番。INTERNET网络的发展速度每6个月翻一番。IT行业的人才每18个月换一茬。
  - 千倍定律：高性能计算能力每10年提高1000倍。
  - 吉尔德定理律：干网通信带宽每6个月翻一翻。



武漢大学

一、二十一世纪是信息的时代

2、信息技术与产业空前繁荣

- 信息技术与产业的发展，为社会创造了巨大财富。
- 比尔盖茨连续13年世界首富，08年退休，把自己的580亿美元资产全部捐献给以他命名的慈善基金会。
- 2011年6月美国Apple公司的资产世界第一，相当于165个国家GDP之和。
- 2013年比尔盖茨又重新回到世界首富的位置上。
- 中国电信、中国移动、华为、联想等企业上升为世五百强。

一、二十一世纪是信息的时代

3、我国成为世界信息产业大国

- 我国因特网用户量，居世界第一。
- 我国手机拥有量，居世界第一。
- 我国电话机拥有量，居世界第一。
- 我国有线电视机拥有量，居世界第一。
- 大多数中低档电子产品，我国都居世界第一。

- 但是，我国在高档和基础性IT技术方面尚落后：
  - 集成电路（CPU，专用电路）、高级电子仪器
  - 系统软件（OS，DB）、行业应用软件

一、二十一世纪是信息的时代

3、我国成为世界信息产业大国

●我国的电子计算机

■我国的PC机产量和拥有量都是世界第一。

■2009年1月8日宣布,国防科大研制出天河-1号超级计算机，2570万亿次/秒，世界第一。

■2009年的世界前三位最快计算机：

♣第一中国“天河”，第二美国“黑豹”，第三中国“曙光”

■2013年国防科大研制处天河-2号，重回世界第一。

■2016年国家并行计算机工程中心研制出“神威.太湖之光”12.5亿亿次/秒，目前已三连冠。

注：2017年6月19日，全球超级计算机500强名单公布，第三次夺冠。

一、二十一世纪是信息的时代

4、新型计算机已经出现

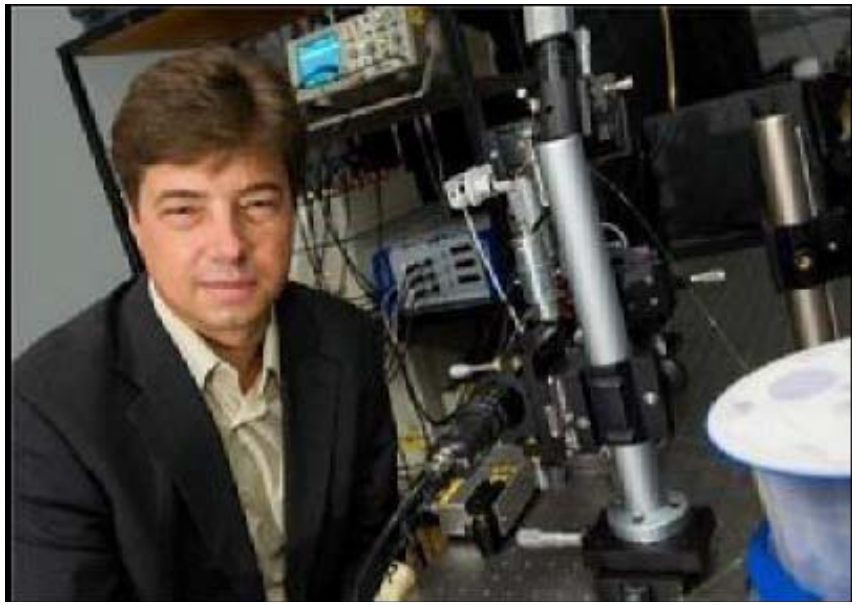
①光计算机

- 光通信技术已经十分成熟，得到广泛应用。
- 光存储
  - 光的只读存储技术已十分成熟，得到广泛应用。
  - 光的随机存储技术，尚待提高。
- 光计算尚需研究
  - 模拟光计算主要的缺点是计算精度不高。
  - 数字光计算的关键技术尚待攻克。

一、二十一世纪是信息的时代

4、新型计算机已经出现

①光计算机



一、二十一世纪是信息的时代

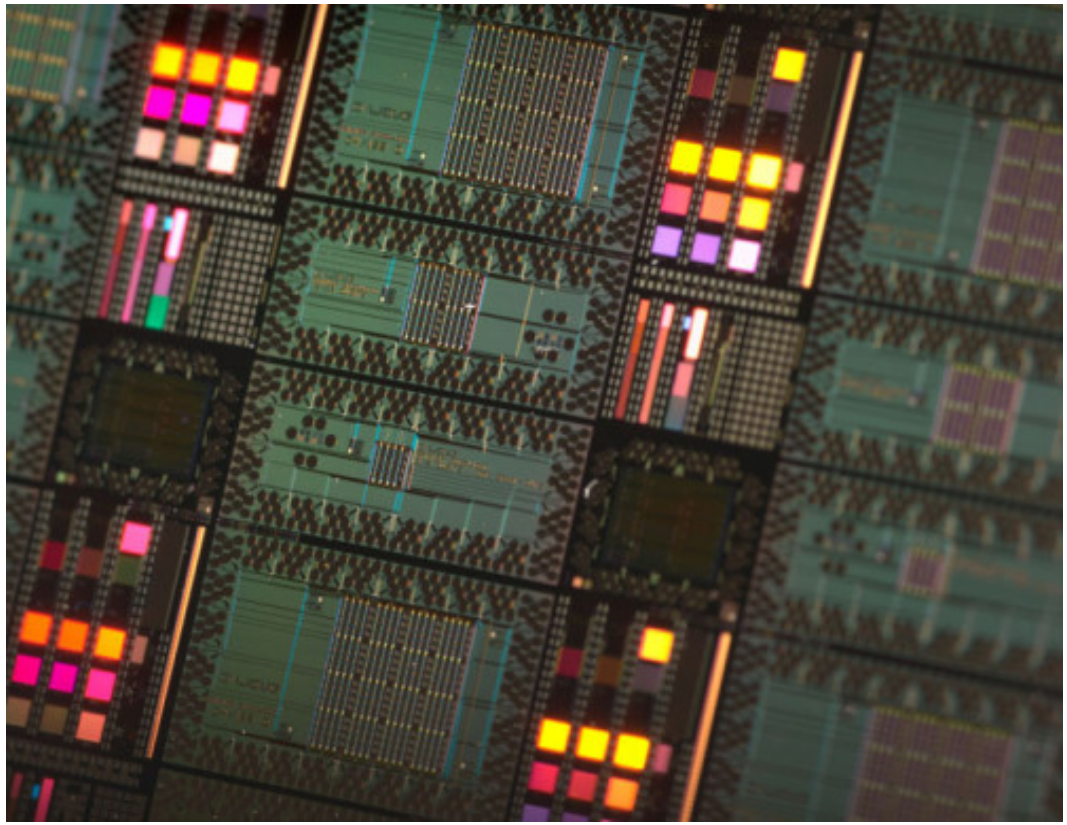
4、新型计算机已经出现

②量子计算机：

- 加拿大的量子计算机：
  - 2007年2月加拿大的D-Wave System公司宣布研制出世界上一台商用16量子位的量子计算机。
  - 2008年5月提高到48量子位。
  - 2011年5月30日，提高到128量子位，以1000万$一台出售。洛克希德马丁公司购买，用于F35战机等新式武器的研制。
  - 2013年初，又提高到512量子位， 1500万$一台。谷歌公司购买，用于提高信息搜索速度和研究人工智能。
- 加拿大的量子计算机的发展速度是惊人的，但它是专用型量子计算机，不是通用型量子计算机。

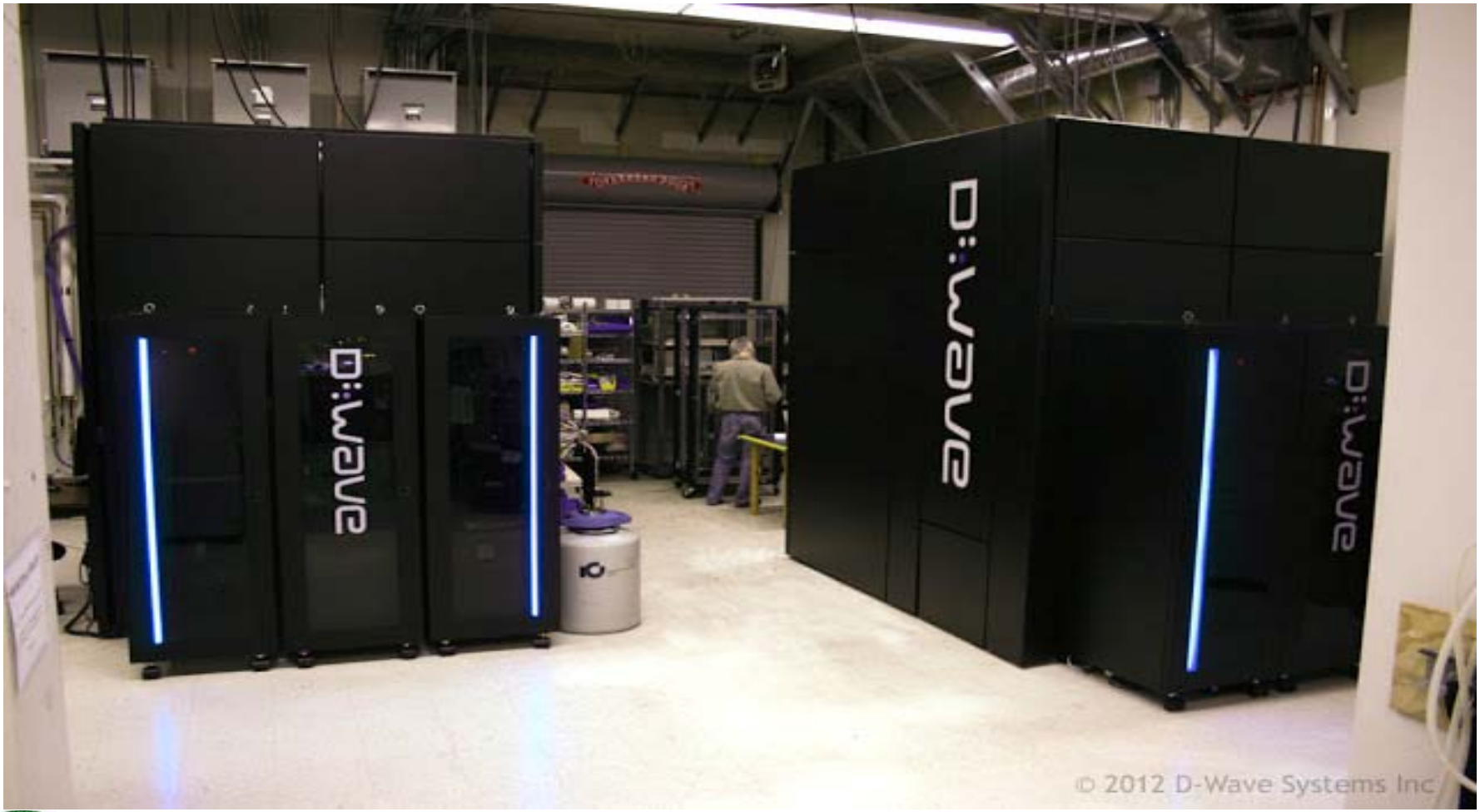
加拿大D-Wave System公司的量子计算机

128qbit量子计算机



处理器阵列

加拿大D-Wave System公司的量子计算机



512qbit量子计算机

一、二十一世纪是信息的时代

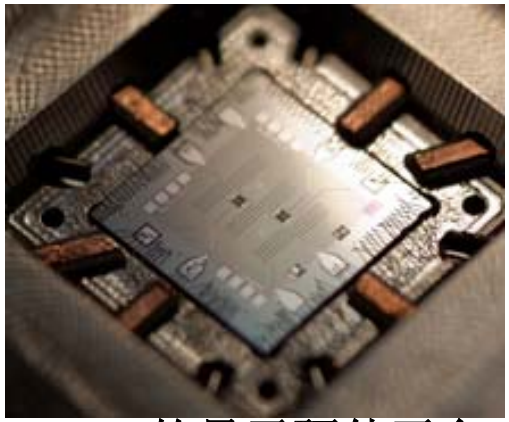
4、新型计算机已经出现

②量子计算机：

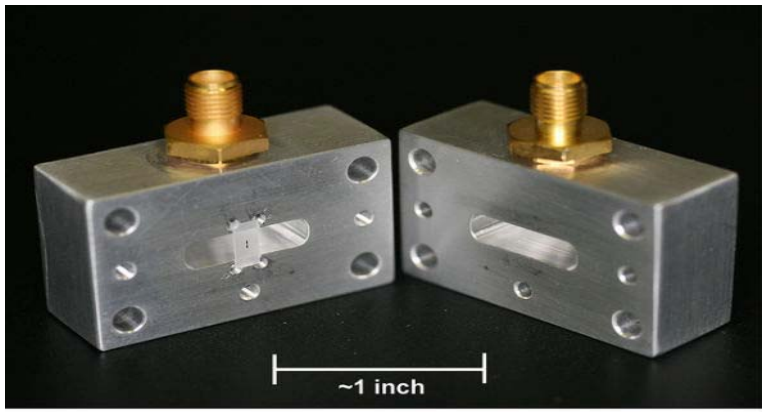
- 美国的量子计算机：
  - 2001年 IMB公司研制出世界上第一台7量子位的示例型量子计算机。宣告量子计算机原理的正确性和可行性。
  - 美国政府和军方执行着5个量子计算研究计划，但具体展却密而不宣。
  - 2011年9月，UCSB制出9量子位冯诺依曼量子计算机。
  - 2012年9月，UCSB宣布利用该硬件平台完成因子分解的Shor算法量子电路实验。
  - 通用量子计算机还没有突破，但技术进展却日新月异。

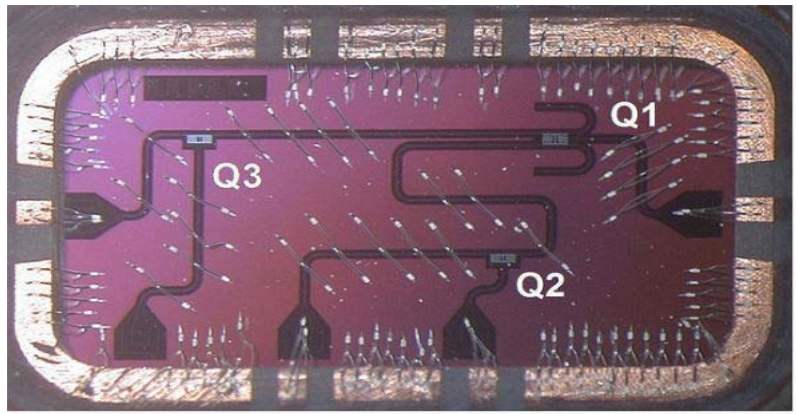
一、二十一世纪是信息的时代

美国的量子计算机技术



UCSB的量子硬件平台





IBM提升量子计算机规模的关键技术

一、二十一世纪是信息的时代

③DNA计算机

●1994年美国南加州大学的L.Adleman提出DNA计算的思想，并在试管液体中进行实验。

●DNA计算的基本思想：

以DNA碱基序列为信息编码的载体，利用现代分子生物学技术，在控制酶的作用下，进行DNA序列反应。反应前的DNA编码为输入，反应后的DNA编码为输出。

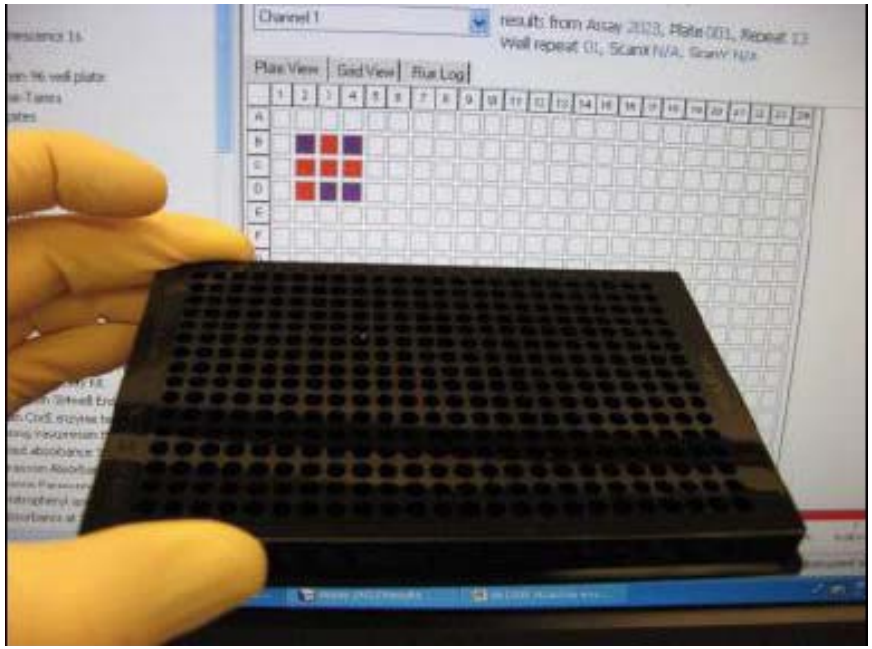
一、二十一世纪是信息的时代

③ DNA计算机

- **DNA计算的特点：**
  - 并行：运算速度快，可达1.2×10^{18}次/s，比目前最快的电子计算机快得多。
  - 节能：能耗是目前超级计算机的$1/10^{18}$。
  - 存储密度高:每$(纳米)^3$1bit，存储密度是现在存储器的2^9倍。
  - 2003年以色列研制出可人机交互的DNA计算机
- 2012.2.8美国加州斯克里普斯研究院和以色列理工学院开发出一种生物计算机，可破译DNA芯片中的加密图像。
- **DNA计算机是并行的，因此与量子计算机一样，将对现有密码构成严重威胁！**

一、二十一世纪是信息的时代

③ DNA计算机



武漢大学

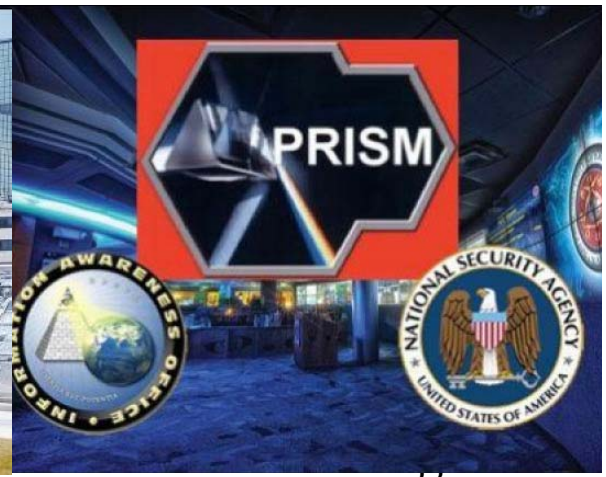
二、信息安全形势严峻

由于信息是重要的战略资源，计算机系统集中管理着国家和企业的政治、军事、金融、商务等重要信息，因此计算机系统成为不法分子的主要攻击目标。又由于计算机系统本身的脆弱性和网络的开放性，使得信息安全成为世人关注的社会问题。当前，信息安全的形势是严峻的。

二、信息安全形势严峻

1、敌对势力的破坏

- 2002年在江泽民主席的767专机上查出27个窃听器。
- 美国国务卿奥尔布赖特说：有了因特网，对付中国就有办法了。
- 2013美国棱镜计划曝光，美国中情局对中国等许多国家进行信、邮件的信息监控。



二、信息安全形势严峻

2、敌对势力的破坏

- 2013年4月14日，美国“华盛顿自由灯塔”网站诬蔑武汉大学计算机学院空天信息安全与可信计算教育部重点实验室是中国秘密网络战的研究中心和攻击中心。
- 美国官员诬蔑说，该实验室是武汉大学顶尖的信息安全和网络战中心之一。还称，武汉大学计算机学院过去培养的760多名毕业生目前在中国军队和政府工作。

二、信息安全形势严峻

3、黑客入侵

●黑客入侵已经成为一种经常性、多发性的信息安全事件

●2001年5月1日前后，发生了一场网上“ 中美黑客大战”，双方互相攻击对方的网站，双方都有很大损失。这场网上大战，给我们留下深刻的思考。

●2010年，美国和以色列黑客利用APT(Advanced Persistent Threaten)攻击，物理摧毁了伊朗纳坦兹核工厂的上千台铀浓缩离心机，重创了伊朗的核计划。这一事件表明：黑客攻击已从过去的窃取信息为主的“软打击”，上升到毁坏硬件设备的“硬摧毁”阶段。这给关系到国计民生的工业控制系统安全敲响了警钟。

二、信息安全形势严峻

4、利用计算机进行经济犯罪

●利用计算机进行经济犯罪超过普通经济犯罪

- 电信诈骗
- 银行卡诈骗
- QQ诈骗

●我国的发案率每年高速度递增

5、计算机病毒

●计算机病毒已超过 几万种，而且还在继续增加

●病毒新趋势

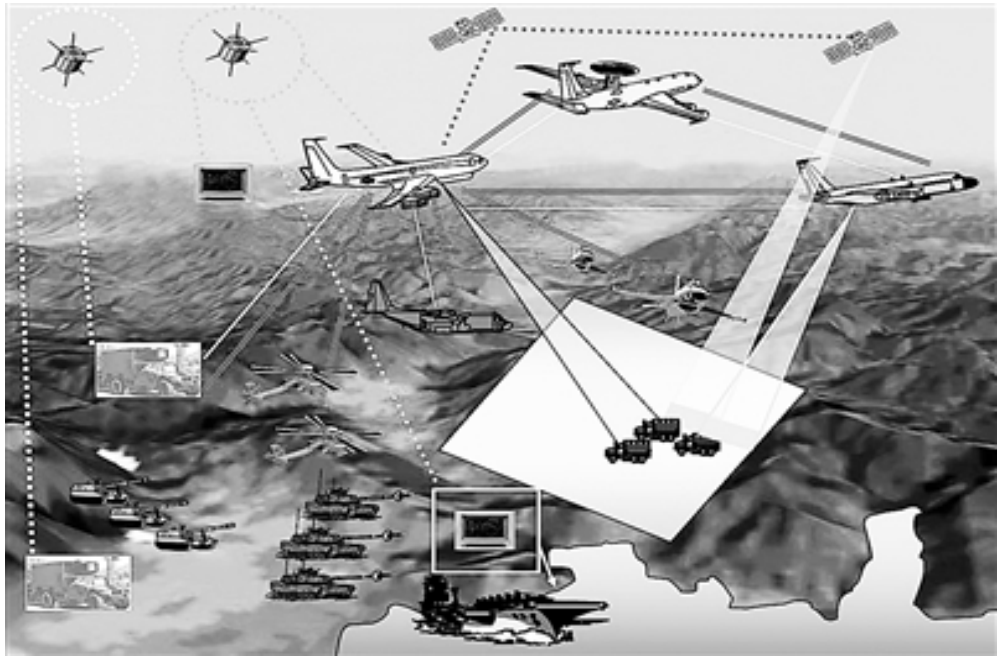
- 追求经济和政治利益
- 团体作案，形成地下产业链

二、信息安全形势严峻

6、信息战

●信息技术的发展促进了军事革命，信息战、网络战成为重要作战形式。

- 1995年美国提出信息作战的概念，并成立信息作战指导委员会



二、信息安全形势严峻

6、信息战

●信息技术的发展促进了军事革命，信息战、网络战成为重要作战形式。

- 两次海湾战争中，美国都成功实施了信息战
- 2007年美国成立网络作战司令部
- 2011.5.16美国公布“网络空间国际战略”，7.14公布“网络空间作战战略”。提出“陆、海、空、天、网络”5维一体的美国国家安全概念
- 2012年1月5日美国宣布把战略重心放到亚太地区
- 美国和以色列黑客利用APT攻击，物理摧毁了伊朗纳坦兹核工厂的上千台铀浓缩离心机。
- 伊朗利用电子对抗技术捕获了美国的无人侦察机

二、信息安全形势严峻

7、我国基础信息技术与产品受控于国外

- **CPU等集成电路芯片依赖进口**

  在集成电路中植入病毒、后门、窃听器是容易的。

- **操作系统等基础软件依赖国外**
  - 操作系统、数据库、**BIOS**、应用软件都有漏洞
  - 平均**1000**行代码就可能有一个**BUG**。
- **漏洞和后门被对手利用实施攻击，可造成严重后果**

二、信息安全形势严峻

8、信息技术进步对信息安全提出新挑战

- 量子计算机规模进一步提高，将攻破现有许多密码。
  - 1448位的量子计算机可以攻破256位的ECC密码
    - 我国二代身份证采用了256位的ECC密码
  - 2048位的量子计算机可以攻破1024位的RSA密码
    - 国际电子商务网络采用了1024位的RSA密码
- DNA计算机的发展同样对现有密码构成威胁。
  - DNA计算机也是并行的
  - 强大的计算能力可攻破许多密码

二、信息安全形势严峻

9、确保我国信息安全是我国的国家战略

●党的十六大文件明确：信息安全是国家安全的组成部分。

●党的十八大文件明确指出“高度关注海洋、太空、网络空间安全”。

●2013年底中央成立“网络安全与信息化领导小组”，习主席任组长。统一领导我国网络安全与信息化工作。

●2014年2月习近平指出：没有网络安全，就没有国家安全。没有信息化，就没有现代化。

●加快国家信息安全保障体系建设，确保我国的信息安全，已经成为我国的国家战略。

三、网络空间安全学科概论

国务院学位委员会和教育部学位[2015]11号文件

国务院学位委员会
教育部 文件

学位〔2015〕11号

国务院学位委员会 教育部
关于增设网络空间安全一级学科的通知

各省、自治区、直辖市学位委员会、教育厅（教委），新疆生产建设兵团教育局，有关部门（单位）教育（人事）司（局），中国人民解放军学位委员会，中共中央党校学位评定委员会，各学位授予单位：

为实施国家安全战略，加快网络空间安全高层次人才培养，根据《学位授予和人才培养学科目录设置与管理办法》的规定和程序，经专家论证，国务院学位委员会学科评议组评议，报国务院学位委员会批准，决定在“工学”门类下增设“网络空间安全”一级学科，学科代码为“0839”，授予“工学”学位。请各单位加强“网络空间安全”的学科建设，做好人才培养工作。

（此页无正文）

国务院学位委员会　　教育部

2015年6月11日

抄送：教育部有关司局

三、网络空间安全学科概论

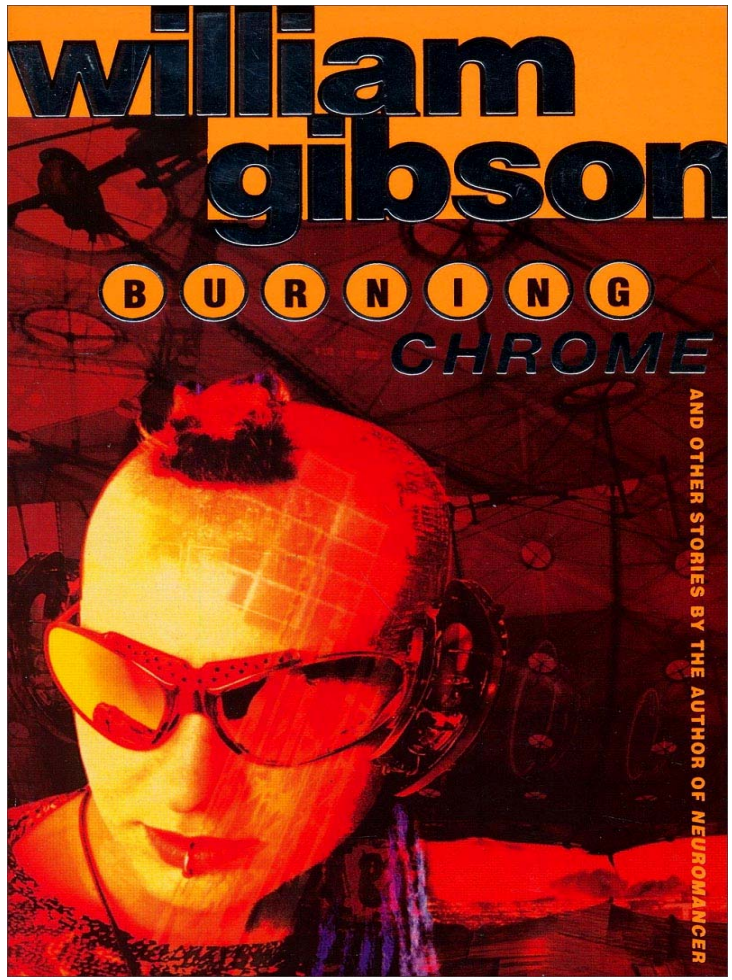
1. 社会信息化产生了三元信息世界观

- 信息技术与产业的发展和应用，使社会进入信息化时代
- 在信息化时代，人们生活和工作在物理世界、人类社会和信息空间（**Cyberspace**）组成的三元世界中。
- 为了描述人们生活和工作的信息空间，创造了**Cyberspace**一词。
- 在国内**Cyberspace**有多种翻译：信息空间、网络空间、网电空间、数字世界等。甚至译音：赛博空间

三、网络空间安全学科概论

1. 社会信息化产生了三元信息世界观

   - 1982年，加拿大作家威廉•吉布森在其短篇科幻小说《燃烧的铬》中创造了“Cyberspace”一词，意指由计算机创建的虚拟信息空间。



三、网络空间安全学科概论

1. 社会信息化产生了三元信息世界观

- 2008年美国第54号总统令对赛博空间进行了定义：

  “赛博空间是信息环境中的一个全球域，由独立且互相依存的IT基础设施网络组成，包括互联网、电信网、计算机系统，以及嵌入式处理器和控制器。”

Cyberspace

三、网络空间安全学科概论

1. 社会信息化产生了三元信息世界观

- 我们的观点：
  - **Cyberspace 是信息时代人类赖以生存的信息环境，是所有信息系统的集合。**
  - 它以计算机和网络系统实现的信息化为特征。
  - **因此把Cyberspace翻译成信息空间或网络空间是比较好的。**
    - 信息空间突出了信息化的特征和核心内涵是信息
    - 网络空间突出了网络化的特征

三、网络空间安全学科概论

2. 网络空间安全的核心内涵仍是信息安全

- 信息安全是信息的影子，哪里有信息那里就存在信息安全问题。
- 从信息论角度来看，系统是载体，信息是内涵。
- 网络空间是所有信息系统的集合，是一种复杂巨系统。因此，网络空间存在更加严峻的信息安全问题。
- 网络空间安全的核心内涵仍是信息安全。没有信息安全，就没有网络空间安全。

三、网络空间安全学科概论

3、网络空间的信息系统安全观

- 能源、材料、信息是支撑现代社会大厦的支柱！
  - 能源、材料是物质的、具体的
  - 信息是逻辑的、抽象的
  - 信息不能脱离信息系统而独立存在！
- 因此，不能脱离信息系统孤立地谈论信息安全！
- 信息系统安全立体（纵向）视角，四个层面的安全：

  设备安全，数据安全，内容安全，行为安全

  中文词安全＝Security + Safety
  - Security是指阻止人为恶意地对安全的危害。
  - Safety是指阻止非人为对安全的危害，或人为但非恶意。

三、网络空间安全学科概论

①设备安全的概念

- 设备是系统的物质基础
- 信息设备的安全是信息系统安全的首要问题
  - 设备的稳定性(Stability)

    设备在一定时间内不出故障的概率。
  - 设备的可靠性(Reliability)

    设备能在一个给定时间内正常执行任务的概率。
  - 设备的可用性(Availabity)

    设备随时可以正常使用的概率。

三、网络空间安全学科概论

②数据安全

- 采取措施确保数据免受未授权的泄露、篡改和毁坏。
  - ■数据的秘密性(Secrecy)

    数据不被未授权者知晓的属性
  - ■数据的完整性(Integrity)。

    数据是正确的、真实的、未被篡改的、无缺失的属性
  - ■数据的可用性(Availabity)

    数据是随时可以使用的属性
- 传统的信息安全主要指数据安全

三、网络空间安全学科概论

③内容安全

- 内容安全是信息安全在法律、政治、道德层次上的要求。
  - ■信息内容在政治上是健康的
  - ■信息内容符合我国法律法规
  - ■信息内容符合中华民族优良的道德规范
- 广义的内容安全还包括：
  - ■信息隐藏
  - ■隐私保护
  - ■知识产权保护

三、网络空间安全学科概论

④行为安全

- 行为安全从主体的行为考察是否能够确保信息安全。
- 符合哲学上实践是检验真理的唯一标准的原理。
  - 行为的秘密性：行为不能危害数据秘密性，必要时行为本身也应是秘密的
  - 行为的完整性：行为不能危害数据完整性，行为的过程和目标是预期的
  - 行为的可控性：当行为的过程出现偏离预期时，能够发现、控制或纠正

三、网络空间安全学科概论

2、信息安全措施

- 信息安全措施＝{法律措施，教育措施，管理措施，技术措施，…}

注意：

- 决不能低估法律、教育、管理的作用，许多时候它们的作用大于技术。
- 信息安全界的行话：“三分技术，七分管理”
- 确保信息安全是一个系统工程，必须综合采取各种措施才能奏效。

三、网络空间安全学科概论

- 信息安全的技术措施

  信息安全技术措施＝{硬件系统安全、操作系统安全、密码技术、网络安全技术、软件安全技术、病毒防治技术，信息内容安全技术，信息隐藏技术，信息对抗技术，数字取证技术，容错技术，…}。

- 注意
  - 信息系统的硬件系统安全和操作系统安全是信息系统安全的基础，密码技术、网络安全技术等是关键技术。

三、网络空间安全学科概论

- 信息安全的管理措施
  - 信息安全管理措施既包括信息设备、机房的安全管理、信息管理，又包括对人的安全管理，其中对人的管理是最主要的。
  - 行话：“三分技术，七分管理。”

- 信息安全的法律措施
  - 法律是武器。
  - 我国政府制定了关于信息安全的各种法律法规。

三、网络空间安全学科概论

- 信息安全的教育措施
  - 对人的思想品德教育、安全意识教育、安全法律法规的教育等。
  - 国内外的计算机犯罪事件都是人的思想品德出问题造成的。

确保信息安全是一个系统工程必须综合采取各种措施才能奏效！

三、网络空间安全学科概论

3、网络空间安全学科内涵

- 网络空间安全学科是研究信息获取、信息存储、信息传输和信息处理领域中信息安全保障问题的一门新兴学科。
- 网络空间安全学科是计算机、通信、电子、数学、物理、生物、管理、法律和教育等学科交叉融合而形成的一门新型学科。它与这些学科既有紧密的联系，又有本质的不同。信息安全学科已经形成了自己的内涵、理论、技术和应用，并服务于信息社会，从而构成一个独立的一级学科（工学类学科）。

三、网络空间安全学科概论

4、网络空间安全学科的研究方向与内容

①密码学

- 密码学由密码编码学和密码分析学组成。其中密码编码学主要研究对信息进行编码以实现信息隐蔽，而密码分析学主要研究通过密文获取对应的明文信息。
  - 对称密码
  - 公钥密码
  - Hash函数
  - 密码协议
  - 新型密码：生物密码，量子密码等
  - 密码应用

三、网络空间安全学科概论

4、网络空间安全学科的研究方向与内容

②网络安全

- 网络安全的基本思想是在网络的各个层次和范围内采取防护措施，以便能对各种网络安全威胁进行检测和发现，并采取相应的响应措施，确保网络环境的信息安全。
  - 通信安全
  - 协议安全
  - 网络防护
  - 入侵检测
  - 入侵响应
  - 可信网络

三、网络空间安全学科概论

4、网络空间安全学科的研究方向与内容

③信息系统安全

- 信息系统是信息的载体，是直接面对用户的服务系统。信息系统安全的特点是从系统级的整体上考虑安全威胁与防护。
  - 硬件系统安全
  - 软件系统安全
  - 访问控制
  - 可信计算
  - 信息系统安全测评认证
  - 信息系统安全等级保护

三、网络空间安全学科概论

4、网络空间安全学科的研究方向与内容

④信息内容安全

- 信息内容安全是信息安全在政治、法律、道德层次上的要求。我们要求信息内容是安全的，就是要求信息内容在政治上是健康的， 在法律上是符合国家法律法规的，在道德上符合中华民族优良的道德规范的。
  - ■信息内容的获取
  - ■信息内容的分析与识别
  - ■信息内容的管理和控制
  - ■信息内容安全的法律保障

三、网络空间安全学科概论

4、网络空间安全学科的研究方向与内容

⑤信息对抗

- 信息对抗是，为消弱、破坏对方电子信息设备和信息的使用效能，保障己方电子信息设备和信息正常发挥效能而采取的综合技术措施，其实质是斗争双方利用电磁波和信息的作用来争夺电磁频谱和信息的有效使用和控制权。
- 主要研究内容：
  - 通信对抗；
  - 雷达对抗；
  - 光电对抗；
  - 计算机网络对抗。

四、武汉大学的信息安全学科

- 2001年武汉大学创建了全国第一个信息安全本科专业
- 2001-2003年武汉大学建立了：

  信息安全硕士点、博士点、博士后产业基地

  形成了信息安全人才培养的完整体系。
- 2005年“信息安全本科专业教学体系与人才培养研究”获湖北省教学成果奖一等奖
- 2006年武汉大学信息安全专业获湖北省“品牌专业”
- 2007年武汉大学信息安全专业获“国家特色专业建设点”
- 2008年武汉大学建立“空天信息安全与可信计算“教育部重点实验室。

四、武汉大学的信息安全学科

- 2009年武汉大学的“密码学课程“被评为”国家精品课程”。
- 2012年武汉大学牵头制定出我国“信息安全专业规范”
- 2012年“坚持特色办学思想，建设信息安全专业”获湖北省教学成果一等奖。
- 2014年“创建信息安全专业培养体系，引领信息安全专业建设”获国家教学成果奖一等奖。
- 2014年获批“网络安全国家虚拟仿真实验教学中心”
- 武汉大学承担完成了大批国家和企业的重要科研项目，获得了一些有影响的科研成果。
- 武汉大学已成为我国信息安全科学研究和人才培养的重要基地！

谢　谢！