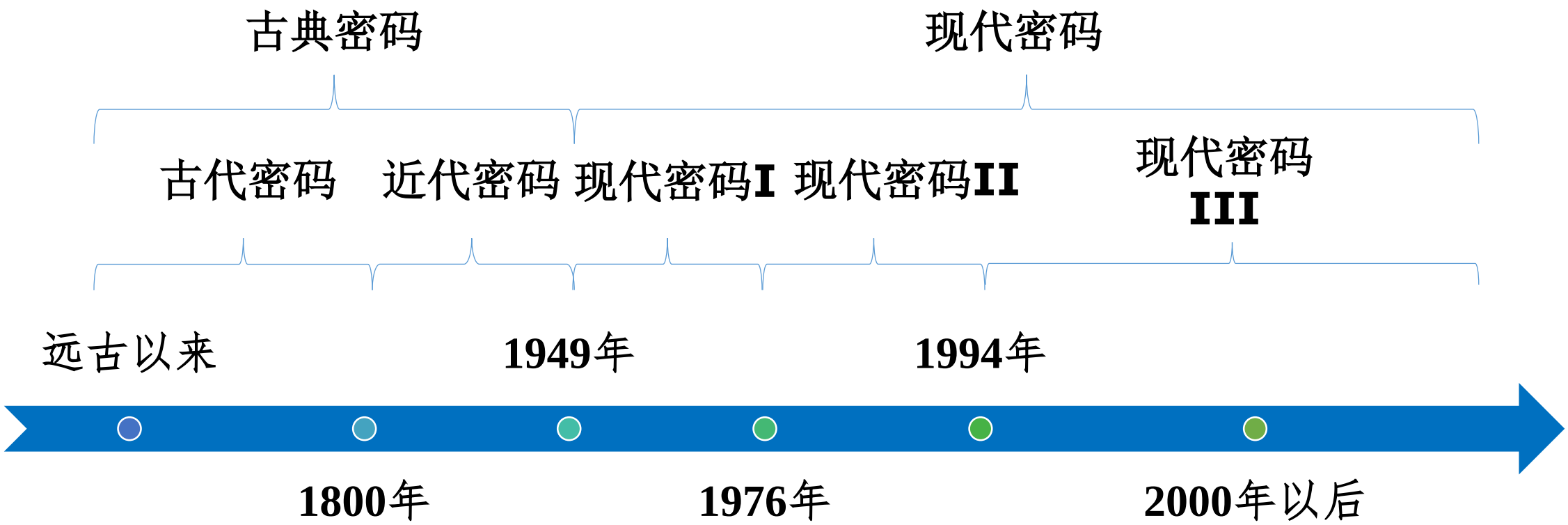
现代密码学

第四讲 密码学发展简史

信息与软件工程学院

密码学发展时间轴


古典密码
现代密码
古代密码
近代密码
现代密码I
现代密码II
现代密码
III
远古以来
1949年
1994年
1800年
1976年
2000年以后

第四讲 密码学发展简史

- 古代密码
- 近代密码
- 现代密码
- 未来展望

古代密码

- 时间区域：从由人类以来到1800年
- 密码设计与分析被当作一门艺术
- 这一时期的密码学专家常常是凭直觉和信念来进行密码设计和分析，而不是靠推理证明
- 数据的保密基于加密算法的保密
- 密码工作者多为语言学家、猜谜高手等

古代密码（续）

- 著名密码算法：
  - 500 B.C.，古斯巴达“天书”密码（置换密码）
  - 205-123 B.C.，古希腊人棋盘密码（代替密码）
  - 50 B.C.，古罗马恺撒密码（代替密码）
  - 16世纪，维吉尼亚（Vigenère）的密码（代替密码）

第四讲 密码学发展简史

- 古代密码
- 近代密码
- 现代密码
- 未来展望

近代密码

- 时间区域：从1800到1949年
- 密码机的迅速发展
- 越来越多的数学家加入密码队伍

著名的密码机

- **1795年，杰弗逊圆盘（Jefferson disk）**
- **1914年，美陆军和海军的M-138-T4**
- **1918年，德国的Enigma密码机**
- **1926年，Kryha密码机**
- **1936年，瑞典的哈格林发明的Haglin密码机，C-36**
- **英国TYPEX打字密码机**

古典密码阶段

- 时间：
  - 1949年之前：古典密码
- 特点：
  - 密码学还不是科学，而是艺术
  - 出现一些密码算法和加密设备
  - 出现密码算法设计的基本手段(代替法 & 置换法)
- 保密性：
  - 数据的保密基于加密算法的保密

古典密码阶段

- 里程碑事件
  - 1883年Kerckhoffs第一次明确提出了密码编码的原则：

    加密算法应建立在算法的公开不影响明文和密钥的安全，即密码算法的安全性仅依赖于对密钥的保密。

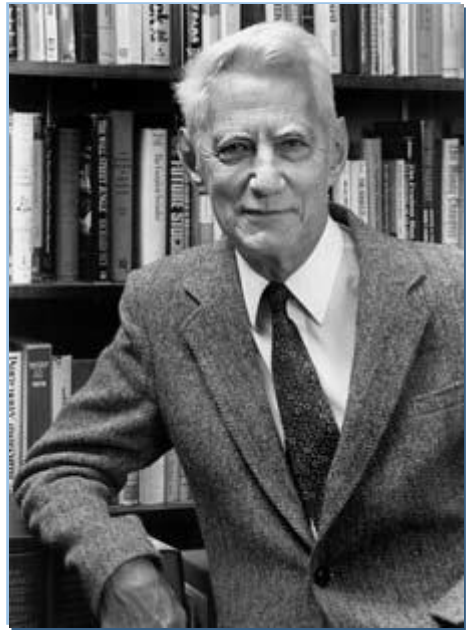
  - 这一原则已得到普遍承认，成为判定密码强度的衡量标准，也成为古典密码和现代密码的分界线之一。

第四讲 密码学发展简史

- 古代密码
- 近代密码
- 现代密码
- 未来展望

现代密码I阶段

时间跨度：1949年-1976年



1949年：

Shannon发表“The Communication Theory of Secret Systems”

- 定义理论安全性，提出扩散和混淆原则
- 奠定了密码学的理论基础
- 艺术→科学

现代密码I阶段特点

- 里程碑事件：
  - 1949年Shannon的“保密系统的信息理论”
  - 1967年Kahn的“The Codebreakers”
  - 1971-73年IBM的Feistel等的几篇技术报告
  - Lucifer ➔ DES
- 保密性：
  - 数据的安全基于密钥而不是算法的保密

现代密码II阶段

时间跨度：1976年-1994年

- **1976 年 Diffie & Hellman 的“New Directions in Cryptography”提出了公钥密码的概念**
- **1977年Rivest, Shamir & Adleman提出了RSA公钥算法**
- **1977年，DES成为了第一代公开的、完全说明细节的商业级密码标准**
- **90年代逐步出现椭圆曲线等其他公钥算法**

2015年图灵奖

公钥密码部分解决了对称密钥密码算法密钥共享和密钥管理困难的问题！

现代密码II阶段特点

- 对称密钥加密算法进一步发展，加密算法更加复杂，以DES为代表的加密算法正式成为行业标准
- 第二把加密密钥“公钥”开始出现，以RSA加密算法为代表的公开密钥加密算法开始流行
- 以Hash算法为代表的解决数据完整性的数据摘要算法也开始出现

第四讲 密码学发展简史

- 古代密码
- 近代密码
- 现代密码
- 未来展望

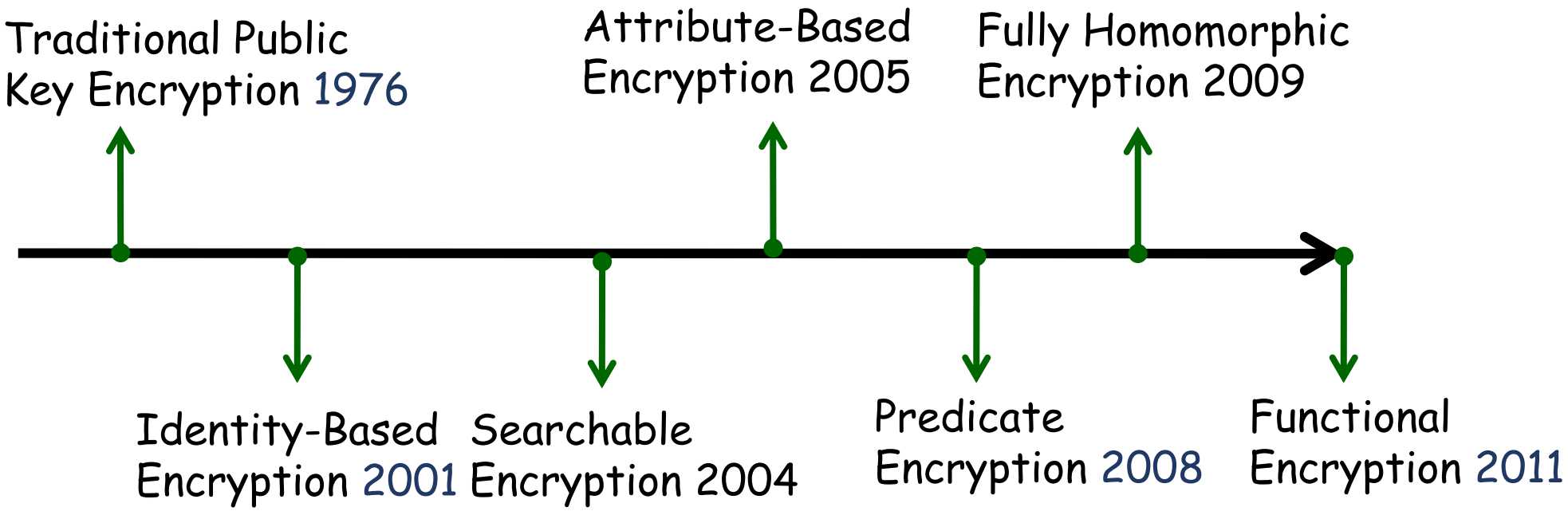
现代密码III阶段

- 时间区域：1994年至未来
  - 1994年，Shor提出量子计算机模型下分解大整数和求解离散对数的多项式时间算法
  - 2000年，AES正式取代DES成为了新的加密标准
  - 2006年，第一届后量子密码学国际研讨会召开
  - 2017年，NIST开始征集后量子密码标准

公钥密码未来发展——后量子公钥密码

- 后量子密码
  - 基于编码的公钥密码
  - 基于格的公钥密码
  - 基于HASH的公钥密码
  - 多变量公钥密码

公钥密码未来发展阶段


Traditional Public Key Encryption 1976
Identity-Based Encryption 2001
Searchable Encryption 2004
Attribute-Based Encryption 2005
Predicate Encryption 2008
Fully Homomorphic Encryption 2009
Functional Encryption 2011

感 谢 聆 听!

xynie@uestc.edu.cn