第二章 密码学基础
第三节 密码学新进展及研究方向

主讲人：李建华 张全海
网络空间安全技术研究院

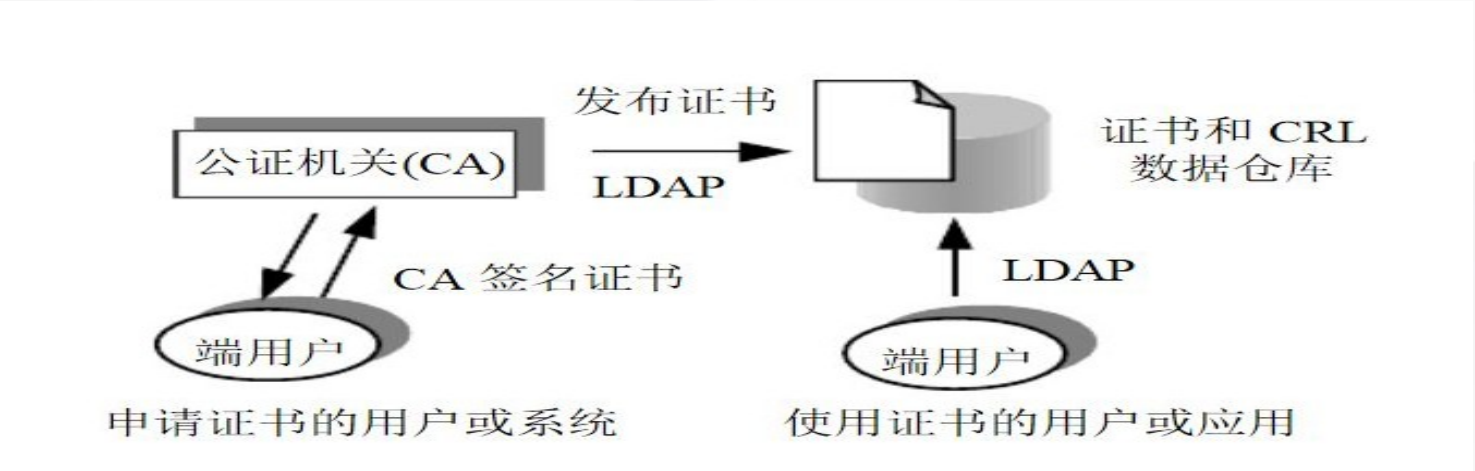
2024 年 11 月

上海交通大學
SHANGHAI JIAO TONG UNIVERSITY

目 录

公钥基础设施

- 公钥基础设施（ Public Key Infrastructure ， PKI ）是一个用公钥概念与技术来实施和提供安全服务的具有普适性的安全基础设施。
- PKI 是生成、管理、存储、分发和吊销基于公钥密码学的公钥证书所需要的硬件、软件、人员、策略和规程的总和，其最基本的元素是数字证书。
- PKI 中证书权威（ Certificate Authority CA), 对用户证书带来了复杂的管理问题，是否有办法可以简化这种密钥的管理？



公钥证书（数字证书）

- 公钥证书由证书管理机构 CA (Certificate Authority) 为用户建立，其中的数据项包括与该用户的秘密钥相匹配的公开钥及用户的身份和时间戳等，所有的数据项经 CA 用自己的秘密钥签字后就形成证书。

- 证书的形式为 $C_A = E_{SK_{CA}}[T, ID_A, PK_A]$，其中 ID_A 是用户 A 的身份标识，PK_A 是 A 的公钥，T 是当前时间戳，SK_{CA} 是 CA 的密钥。

- 公钥证书是用来绑定实体姓名以及该实体的其它相关属性和相应公钥的凭证。s 是网络环境中的一种身份证，用于证明某一用户的身份及其公开密钥的合法性。

- 使用 X.509 协议，广泛应用在网络安全设施： IP 安全协议、 SSL 、 SET 和 S/MIME

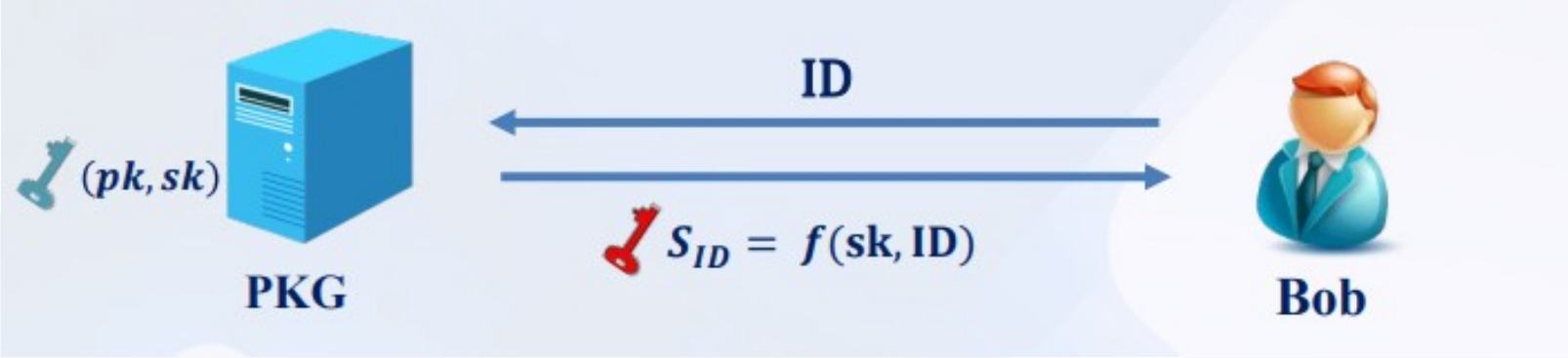
身份基公钥密码

RSA 加密系统发明者之一 Shamir 于 1984 年首次提出了**身份基公钥密码**(IdentityBasedCryptograph ， IBC) ，**使用能唯一标识用户身份的信息作为公钥**，例如**电话号码或 Email 地址**等，简化了传统公钥密码体系中的用户证书管理。

在身份基公钥密码中，用户公钥可以为任意的比特串。用户私钥通过可信第三方，即 PKG 生成。

- (pk, sk) ：用户的公私钥对
- ID ：用户的公钥身份字符串
- PKG ：私钥生成中心（PrivateKeyGenerator ）

身份基公钥密码密钥生成过程：



身份基加密机制框架


PKG
认证并申请对应
标识Bob@b.com
的私钥
安全地分发
Bob@b.com的私钥
Alice用Bob@b.com加密
Bob用私钥解密
Alice@a.com
Bob@b.com
明文

身份基加密

一个身份基加密方案包含四个算法：

① 系统建立算法： PKG 生成系统公开参数和主密钥；

② 密钥提取算法：用户将 ID 提交给 PKG ， PKG 生成 ID 对应的私钥；

③ 加密算法：利用用户身份 ID 加密消息，生成加密密文；

④ 解密算法：利用身份 ID 对应的私钥解密密文，得到明文消息。

身份基加密方案扩展了身份基公钥密码体制，能够较好地解决 PKI 证书管理复杂问题，被广泛应用于安全电子邮件、 AdHoc 网络密钥管理等应用场景。

身份基签名

一个身份基签名方案包含四个算法：

① 系统建立算法： PKG 生成系统公开参数和主密钥；

② 密钥提取算法：用户将 ID 提交给 PKG ， PKG 生成 ID 对应的私钥；

③ 签名算法：给定用户身份 ID 的私钥和消息，生成消息的签名；

④ 验证算法：给定用户身份 ID 、签名和消息，验证签名是否正确。

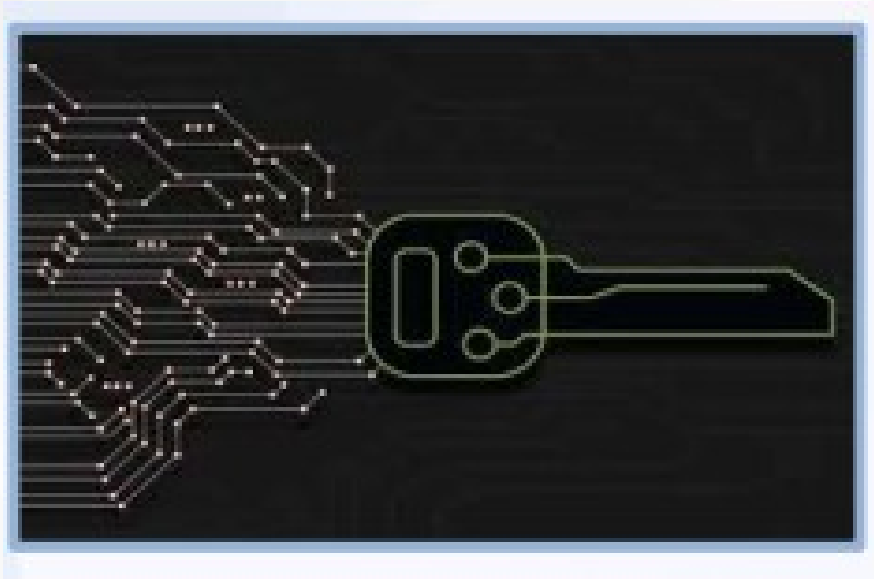
身份基签名方案扩展了身份基公钥密码体制，但一般的身份基签名方案与传统的公钥签名方案相比并没有非常明显的优点，其主要原因在于传统公钥签名本身也同样能实现基于身份签名的功能。

身份基公钥密码优缺点

优点：

① 无需公钥证书，加密或签名验证不需要知道除身份外的其他信息；

② 无需证书机构，存在可信第三方私钥生成中心 (PKG) 向用户提供服务；



缺点：

① 密钥托管问题：恶意的 PKG 可能存储用户私钥的副本，使其有能力解密任何一个用户发送给用户 ID 的密文或伪造用户 ID 的数字签名。

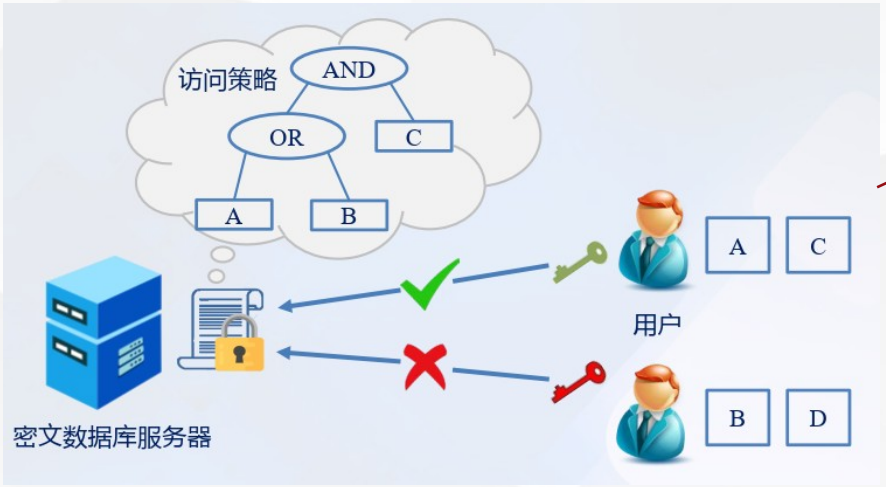
属性基公钥密码（ ABE)

在传统的 IBE 体制中，通信过程是一对一的，然而现实世界中更多的是一对多的通信模式。尽管可以通过**多次的一对一模式**来多现**多对一通信模式**，但是当接收方人数很多时，这种方法无疑非常低效。 ABE 方式：数据拥有者根据用户的属性来加密数据，并且只有当用户拥有特定属性组合时才能解密数据，这种加密方式为数据共享和访问控制提供了**一种细粒度的控制机制**。

在属性基加密中，密钥和密文都与**一组属性**相关联，属性集合表示用户身份。加密者根据将要加密的消息和接收者的属性构造一个加密策略，当**属性满足加密策略**时，解密者才能够解密。

基于属性的集合比基于身份加密的唯一标识符*具有更强更丰富的表达能力*。

属性基加密机制



在属性基加密中，系统的**每个权限**都可以用**一个属性**来表示。系统中存在一个**属性权威（ Attribute Authority ， AA)** ，属性权威对每个用户的属性进行认证，并颁发相应密钥。

应用场合：医疗保健、企业数据管理、云存储服务、教育和学术研究

密钥策略属性基加密

密钥策略属性基加密
（ Key Policy Attribute-Based Encryption, KP-ABE ）

密文策略属性基加密

密文策略属性基加密
（ Ciphertext Policy Attribute-Based Encryption, CP-ABE ）

属性基签名

①属性基签名（ Attribute-Based Signature ， ABS ）是由**模糊身份签名**发展而来的；

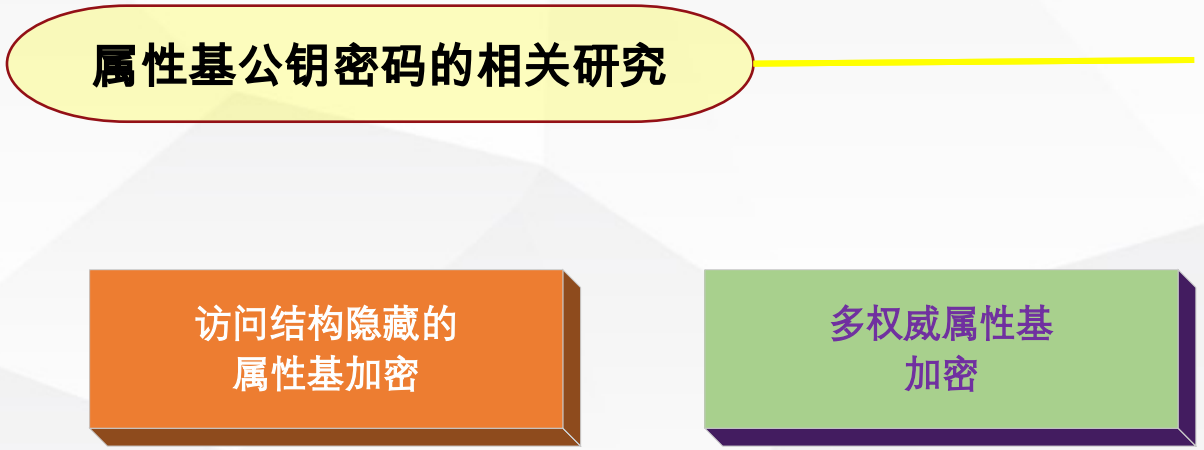
②根据签名的生成过程分为：密钥策略属性基签名（ KP-ABS ）、签名策略属性基签名（ SP-ABS ）；

③**当且仅当属性集合满足访问结构时，签名者可以对消息生成合法签名**；

④属性基签名特点是**匿名性**。

属性基公钥密码的相关研究

- 属性基公钥密码拥有许多良好的性质，能够有效实现非交互式的**细粒度访问控制**，并且在加密数据库、物联网和云计算等诸多领域都有良好的应用前景。



上海交通大學
SHANGHAI JIAO TONG UNIVERSITY

目 录

同态密码

随着云计算的普及与应用，由数据存储和计算服务外包带来的数据安全和隐私保护问题愈加受到关注。同态密码可以在不泄露敏感信息的前提下完成对密文的处理，成为保护**数据安全**，提高**密文处理分析能力**的关键技术。

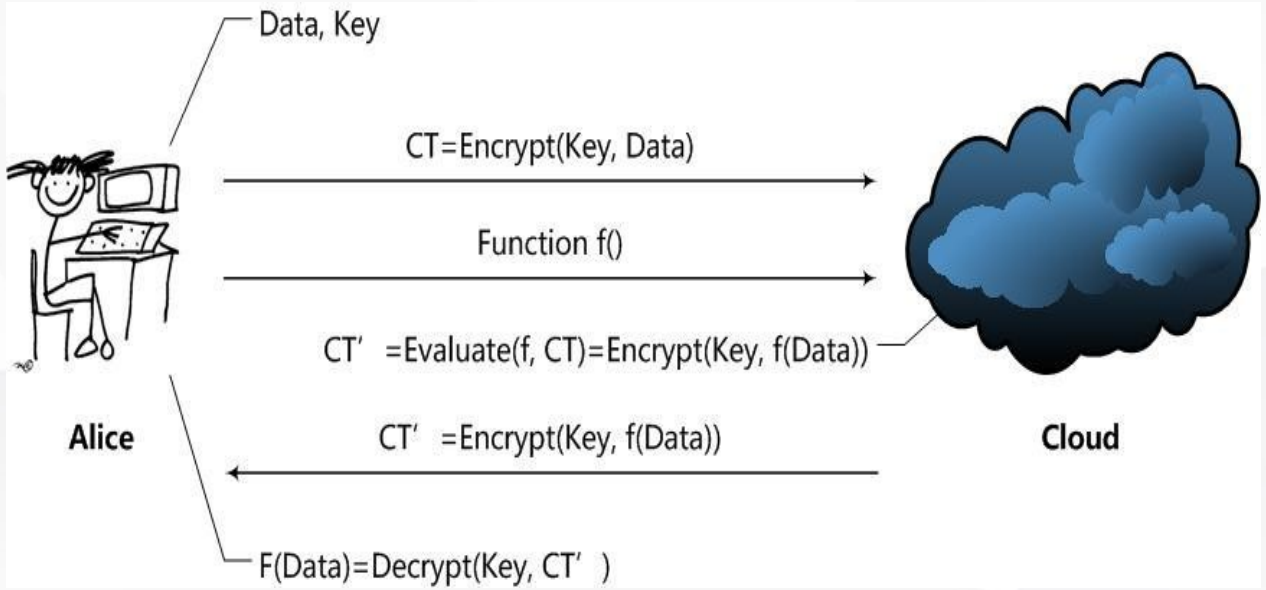
同态密码的概念最初是由 Rivest 、Adleman 和 Dertouzos 于 1978 年在题为 On databanks and privacy homomorphic 的论文中提出的隐私同态（ Privacy Homomorphic ）概念

同态加密思想的三个重要发展时期

1. 1978-1999 部分同态加密的繁荣发展时期
2. 1996-2009 部分同态加密与浅同态加密的交织发展时期
3. 2009年以后 全同态加密的繁荣发展时期

同态密码

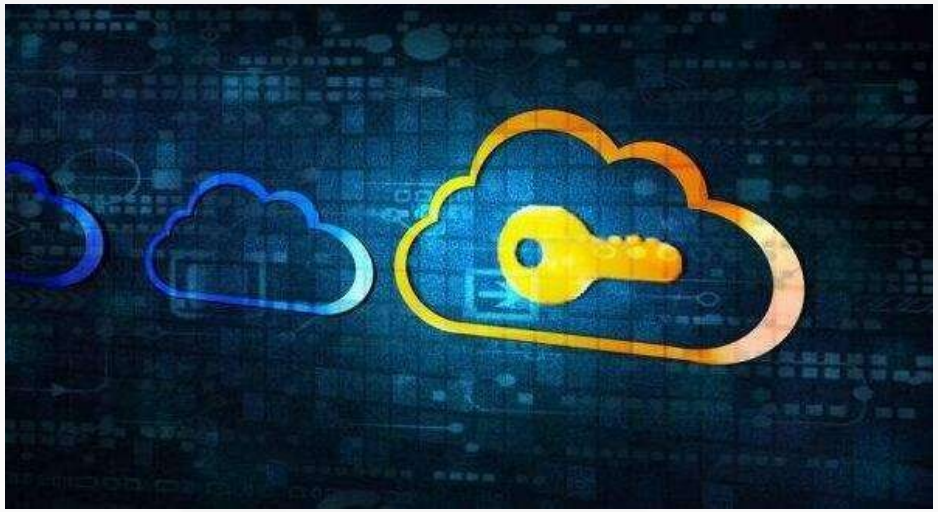
- 同态是一个数学概念，如果 **E(f(a ， b)) = f(E(a) ， E(b))** ，则 **E(.) 是一个同态映射**。
- 假设加密操作为 E(.) ，明文为 m ，密文为 e ，如果针对明文的操作 f ，可以根据 E 构造出 f ，使得 E(f(m)) = f(e) 。 那么 E 就是一个针对 f 的同态加密算法。
- 同态加密是指在不知道解密算法和密钥情况下，可以**对密文直接进行特定运算，而其运算结果解密后与用明文进行相同运算所得的结果一致**。



同态密码技术的应用

安全云计算与委托计算

例如，医疗机构委托有较强数据处理能力的第三方，在同态加密技术的支持下实现数据处理同时保护隐私。



远程文件存储

用户可以将自己的数据加密后存储在不信任的远程服务器上，而远程服务器却对这些信息的具体内容一无所知。

同态密码技术的优缺点

优点：

①无密钥方的计算处理，既可以减少通信代价，又可以避免每一个密文解密后再计算而花费高昂的计算代价。

缺点：

①只能实现单比特加密，效率较低；

②困难性假设未论证，寻找可论证的困难问题是个难题；

③需要额外的消除噪音算法，依然不是自然同态。

上海交通大學
SHANGHAI JIAO TONG UNIVERSITY

目 录

抗量子密码

基于量子物理学的量子密码

- 主要集中在量子密钥分配、量子秘密共享、量子认证、量子密码算法和量子密码算法的安全性等方面的研究；
- 安全性是基于**量子物理设备**的。

基于生物学的 DNA 密码

- 是随着**基因工程**和**生物计算**的发展而诞生的；
- 安全性是建立在生物困难问题上的。

基于数学的抗量子计算密码

- 基于量子计算机不擅长计算的**数学困难问题**构造的；
- 研究方向主要有：基于格的密码、基于 Hash 的数字签名、基于纠错编码的密码和基于多变量的密码。

抗量子密码

- NIST PQC 标准征集工作与 2016 年正式启动。 NIST 主要聚焦于以下 3 类抗量子密码算法的征集：加密、密钥交换、数字签名。截至 2017.11.30 提交截止， NIST 共收到 82 个算法草案。在进行初步筛选后， NIST 公布了 69 个“完整且适合”的草案。在 69 个候选草案中，主要包括以下 4 种数学方法构造的抗量子密码算法：
  - **格 (Lattice-based)**：最早出现于 1996 年，主要用于构造加密、数字签名、密钥交换，以及众多高级密码学应用，如：**属性加密 (Attribute-based encryption)**、陷门函数 (Trapdoor functions)、伪随机函数 (Pseudorandom functions)、同态加密 (Homomorphic Encryption) 等。代表算法： NTRU 系列、 NewHope 、一系列同态加密算法 (BGV 、 GSW 、 FV 等)。由于其计算速度快、通信开销较小，且能被用于构造各类密码学算法和应用，因此被认为是**最有希望的抗量子密码技术**
  - **编码 (Code-based)**：最早出现于 1978 年，主要用于构造加密算法。代表算法： McEliece
  - **多变量 (Multivariate-based)**：最早出现于 1988 年，主要用于构造数字签名、加密、密钥交换等。代表算法： HFE (Hidden Field Equations)、 Rainbow (Unbalanced Oil and Vinegar (UOV) 方法)、 HFEv- 等
  - **哈希 (Hash-based)**：最早出现于 1979 年，主要用于构造数字签名。代表算法： **Merkle 哈希树签名**、 XMSS 、 Lamport 签名等

上海交通大學
SHANGHAI JIAO TONG UNIVERSITY

目 录

轻量级密码概述

轻量密码的特性

- 目标：为资源受限的设备定制专属的密码解决方案；
- 特点：对吞吐率的要求比普通密码算法低；
- 实用性：部分轻量密码采用机器内置密钥。

轻量密码的设计方法实现

- 设计要求：存储计算开销小、能耗低、安全性；
- 第一种方法：在现有的密码方案上进行轻量化改进；
- 第二种方法：设计一个全新的轻量密码方案。

轻量密码的性能评估

- 硬件开销：延迟、功耗、吞吐率
- 软件开销：寄存器、 RAM 、 ROM 的空间使用

轻量级密码的研究现状

1994 年提出
Tiny Encryption
Algorithm

2004 年欧洲成立
ECRYPT 项目

2012 年 IEC 发布
29192《轻量级密码》标准

2012 年 IEC 发布
29167 系列标准并扩展至今

2013 年 NIST 启动
轻量密码研究项目

2013 年
CRYPTREC 启动
轻量密码研究项目

2017 年 NIST 发布
NISTIR8114 轻量密码
调查报告

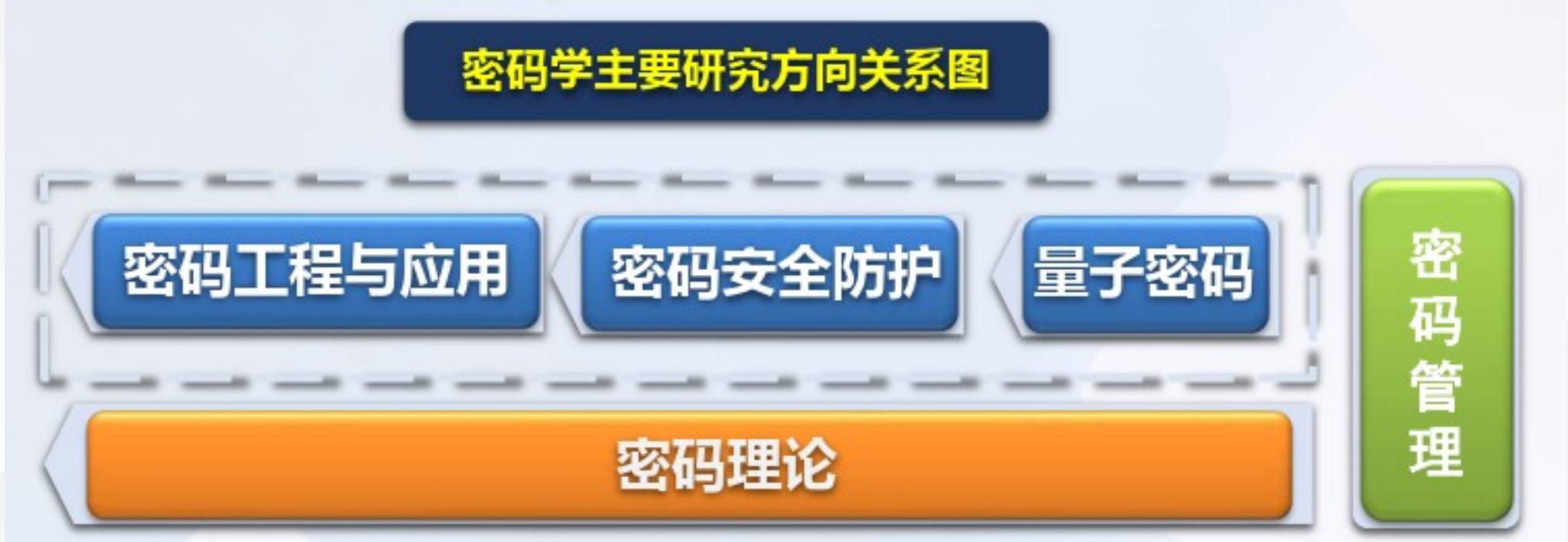
2018 年
NIST 发布
NISTIR 轻量
密码算法征集
需求和评估标
准通知

上海交通大學
SHANGHAI JIAO TONG UNIVERSITY

目 录

研究方向

密码学是研究密码编码、密码分析、密码工程、密码应用、密码管理、密码安全防护等问题的一门科学，是数学、计算机科学与技术、信息与通信工程、电子科学与技术、管理科学与工程等多个学科融合形成的交叉学科。



研究方向

1. 密码基础理论、对称密码设计与分析（**序列密码、分组密码、消息认证码（ MAC ）、散列（ Hash)**）
   公钥密码设计与分析、密码协议设计与分析（**密钥协商、身份认证协议、群签名协议、安全多方计算、电子投票和电子货币**）
   新型密码设计
2. 密码芯片设计（密码芯片架构）
   密码模块设计
   密码技术应用
3. 密码系统安全防护、抗攻击
   安全防护、密码系统测评
4. 量子计算、量子密码分配、
   量子密码协议
5. 密码管理理论与方法、
   密码管理工程与技术、
   密码管理政策与法治

上海交通大學

SHANGHAI JIAO TONG UNIVERSITY

谢谢！

饮水思源 爱国荣校