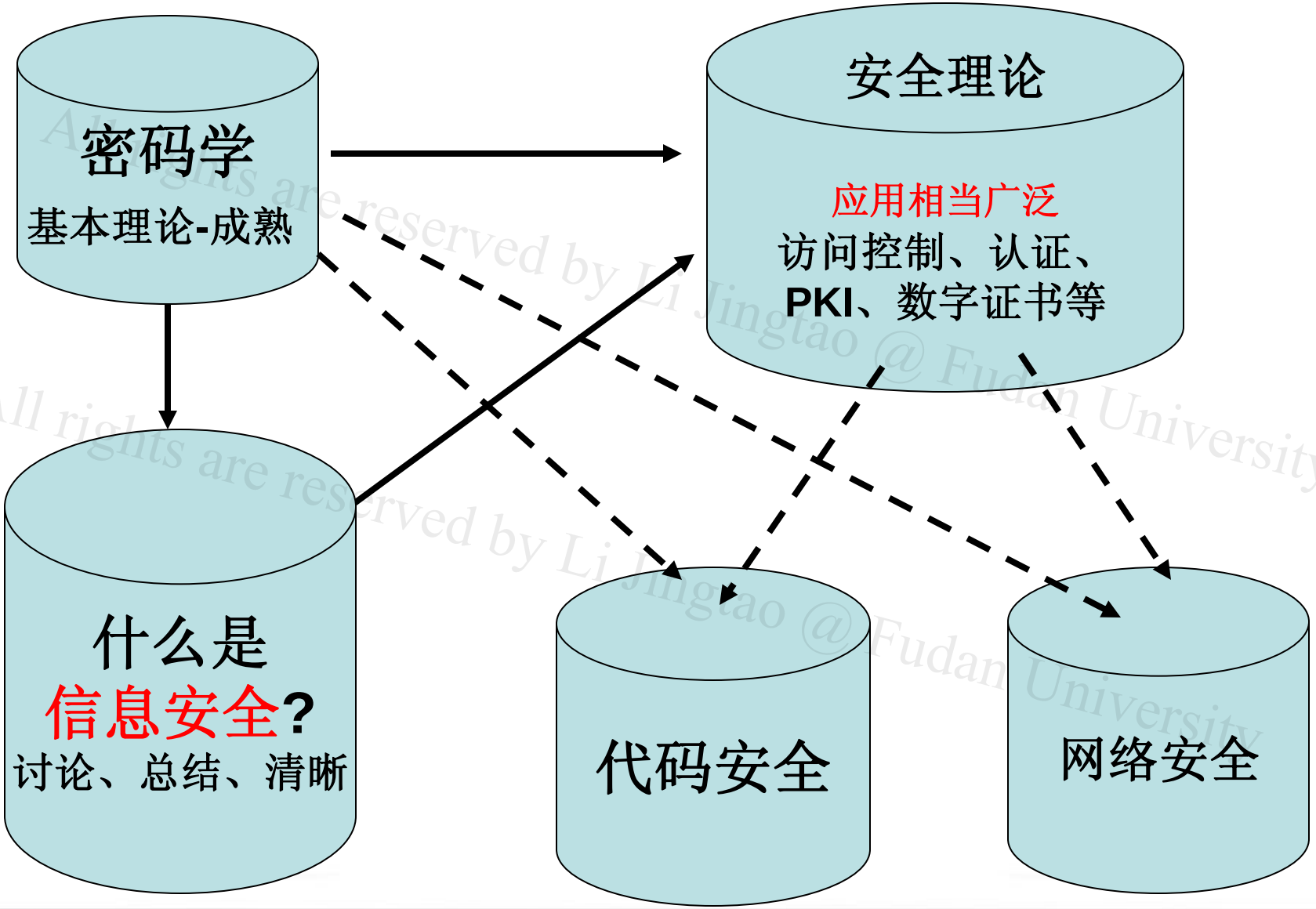
信息安全（07）

PKI (Public Key Infrastructure)

公钥基础设施

——公钥技术的应用

内容间的联系

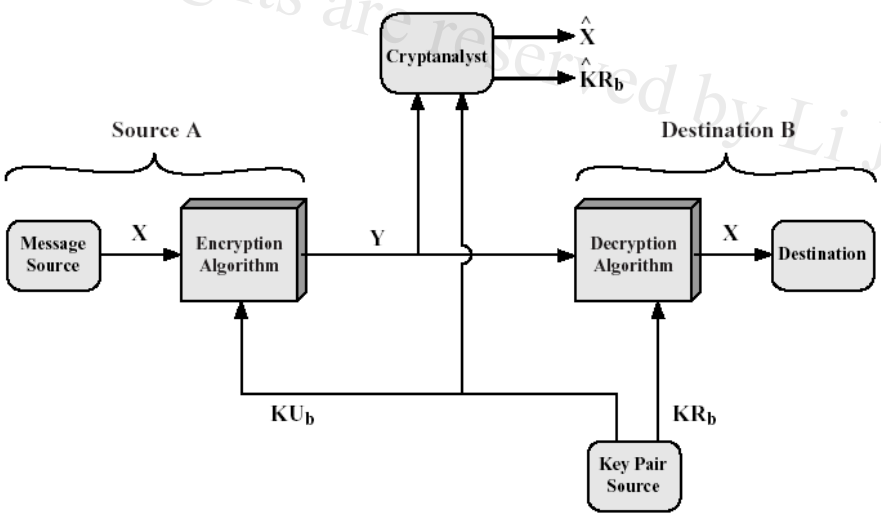


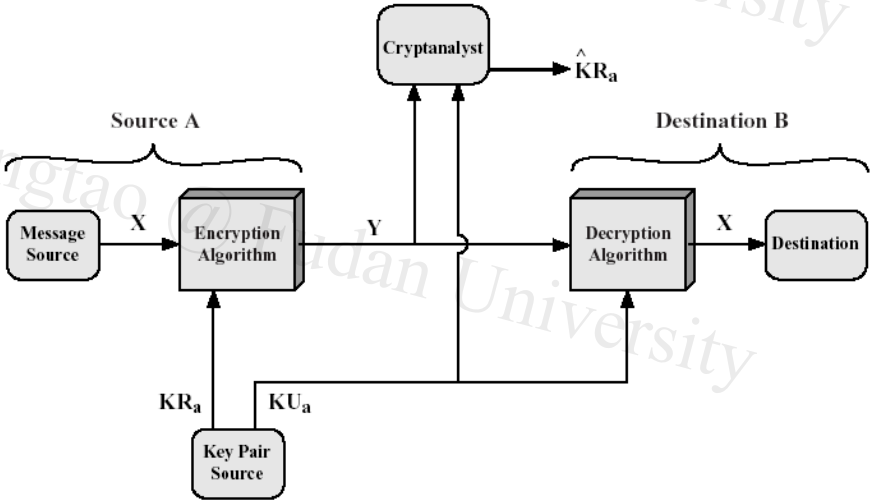
内容提要

- 公钥技术回顾
- PKI之动机
- 数字证书格式
- PKI的组成
- PKI信任关系
- PKI的应用

回顾：公钥技术

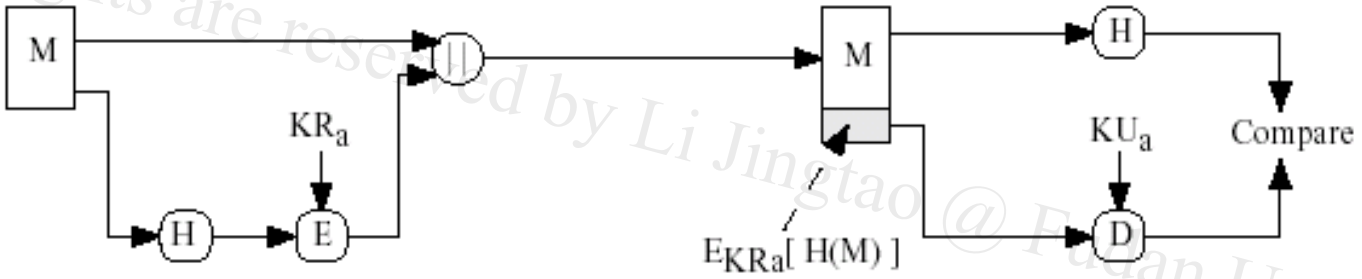
- 公钥技术
  - 建立在非对称密码算法基础上
  - 公钥和私钥对
  - 服务：保密性、完整性、认证和抗抵赖



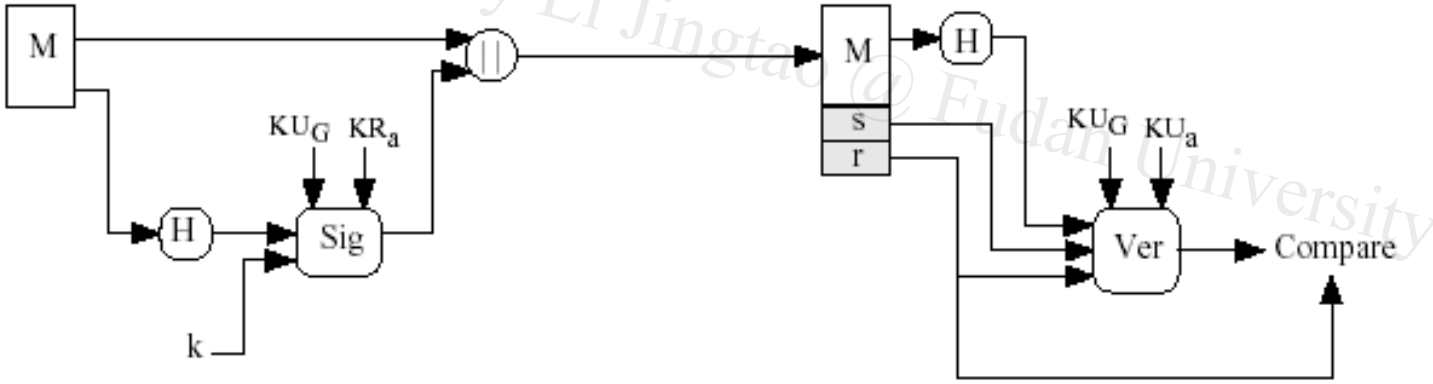


回顾：数字签名

- 两种数字签名方案



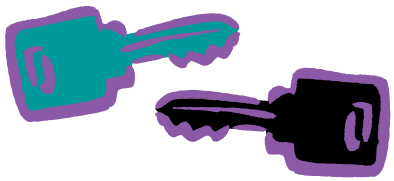
(a) RSA Approach



(b) DSS Approach

密钥对的用法

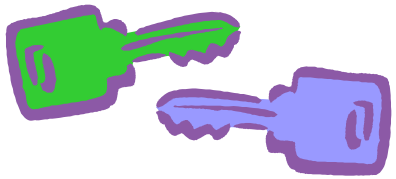
- 用于加密的密钥对



用公钥加密

用私钥解密

- 用于签名的密钥对



用私钥签名

用公钥验证

内容提要

- 公钥技术回顾
- PKI之动机
- 数字证书格式
- PKI的组成
- PKI的应用

PKI之动机

- 公钥技术
  - 如何提供数字签名功能
  - 如何实现不可否认服务
  - 公钥和身份如何建立联系
    - 为什么要相信这是某个人的公钥
    - 公钥的权限
  - 公钥如何管理
- 方案：引入证书(certificate)
  - 通过证书把公钥和身份关联起来

More details

- 思路和我们现实世界的解决方案一致
  - 证书：身份证、学位证、驾照……
  - 具有公信力的第三方

More details

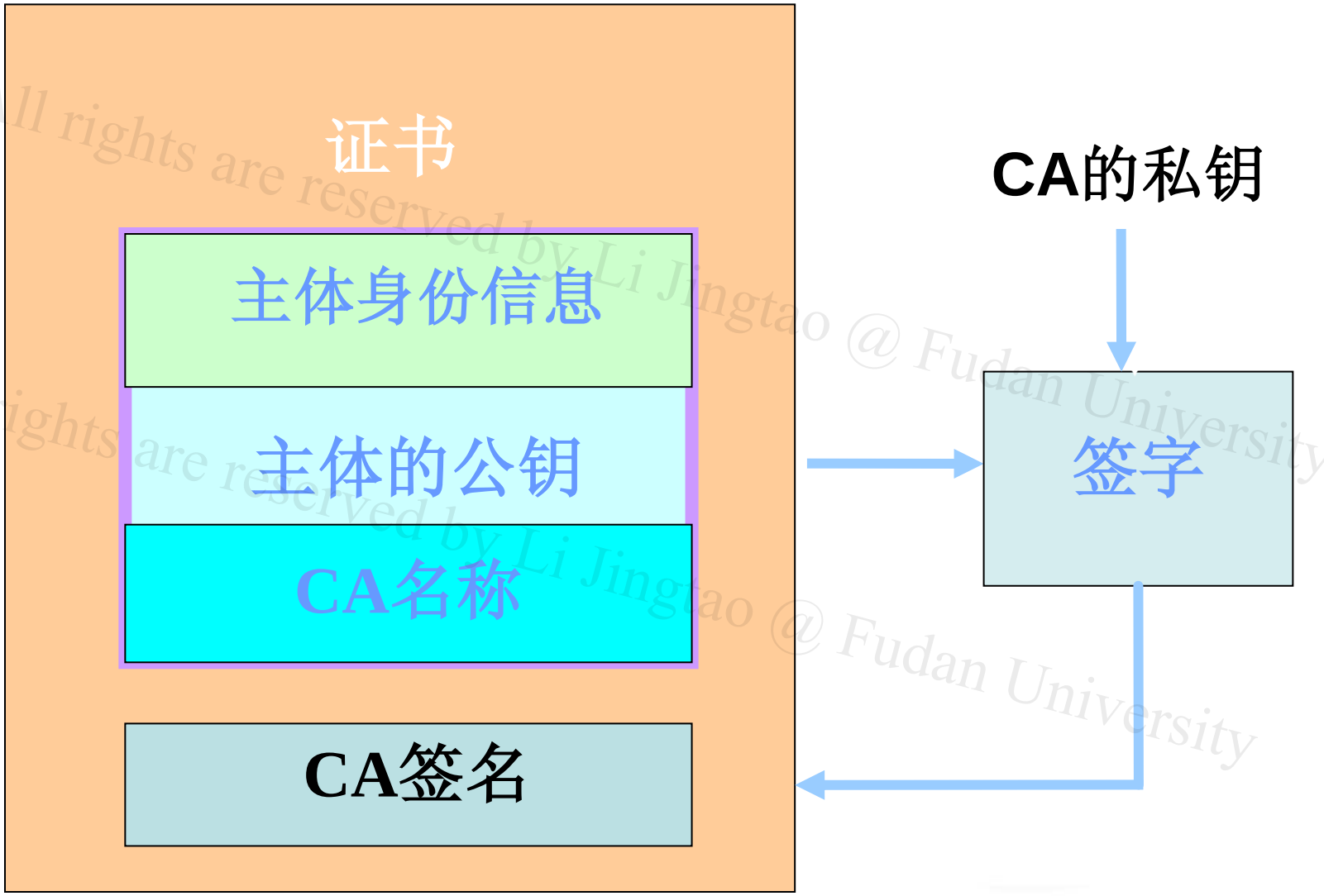
- 思路和我们现实世界的解决方案一致
  - 证书：身份证、学位证、驾照……
  - 具有公信力的第三方
- PKI方案：
  - 数字证书（Digital certificate）
  - CA （Certification Authority）

More details

- 思路和我们现实世界的解决方案一致
  - 证书：身份证、学位证、驾照……
  - 具有公信力的第三方
- PKI方案：
  - 数字证书（Digital certificate）
  - CA （Certification Authority）

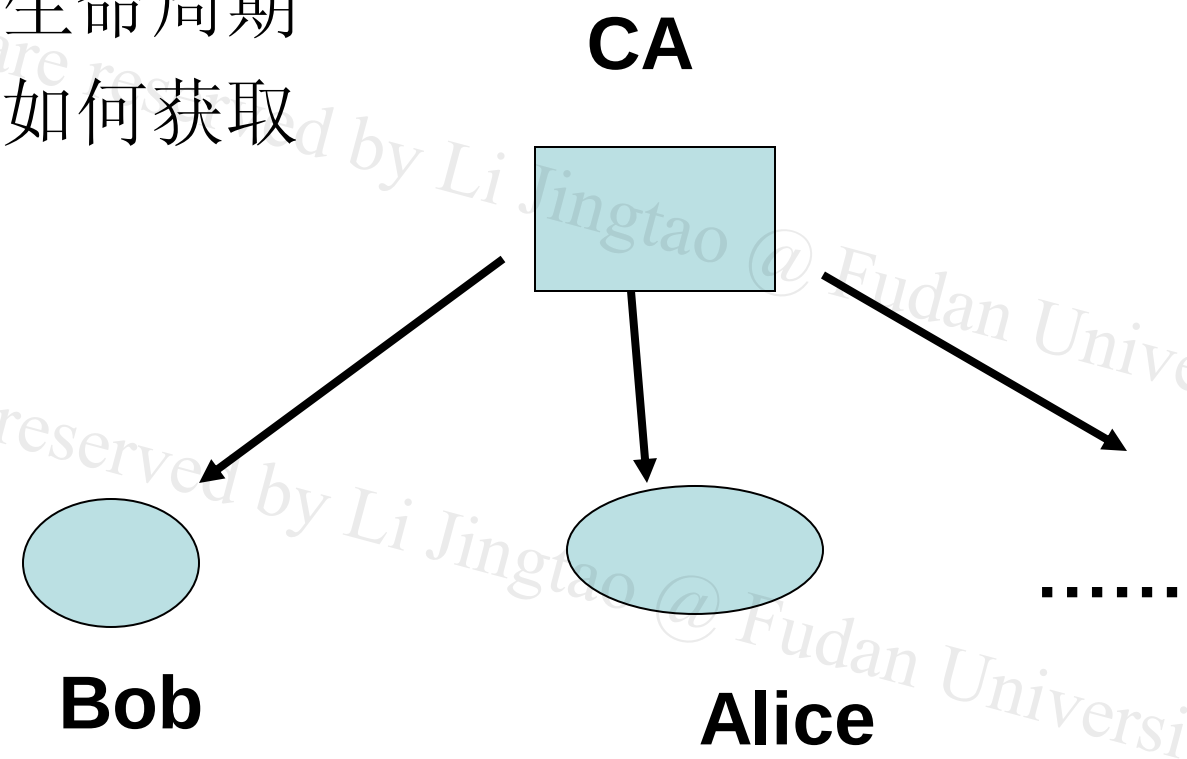
- Q：其他思路？

数字证书的结构

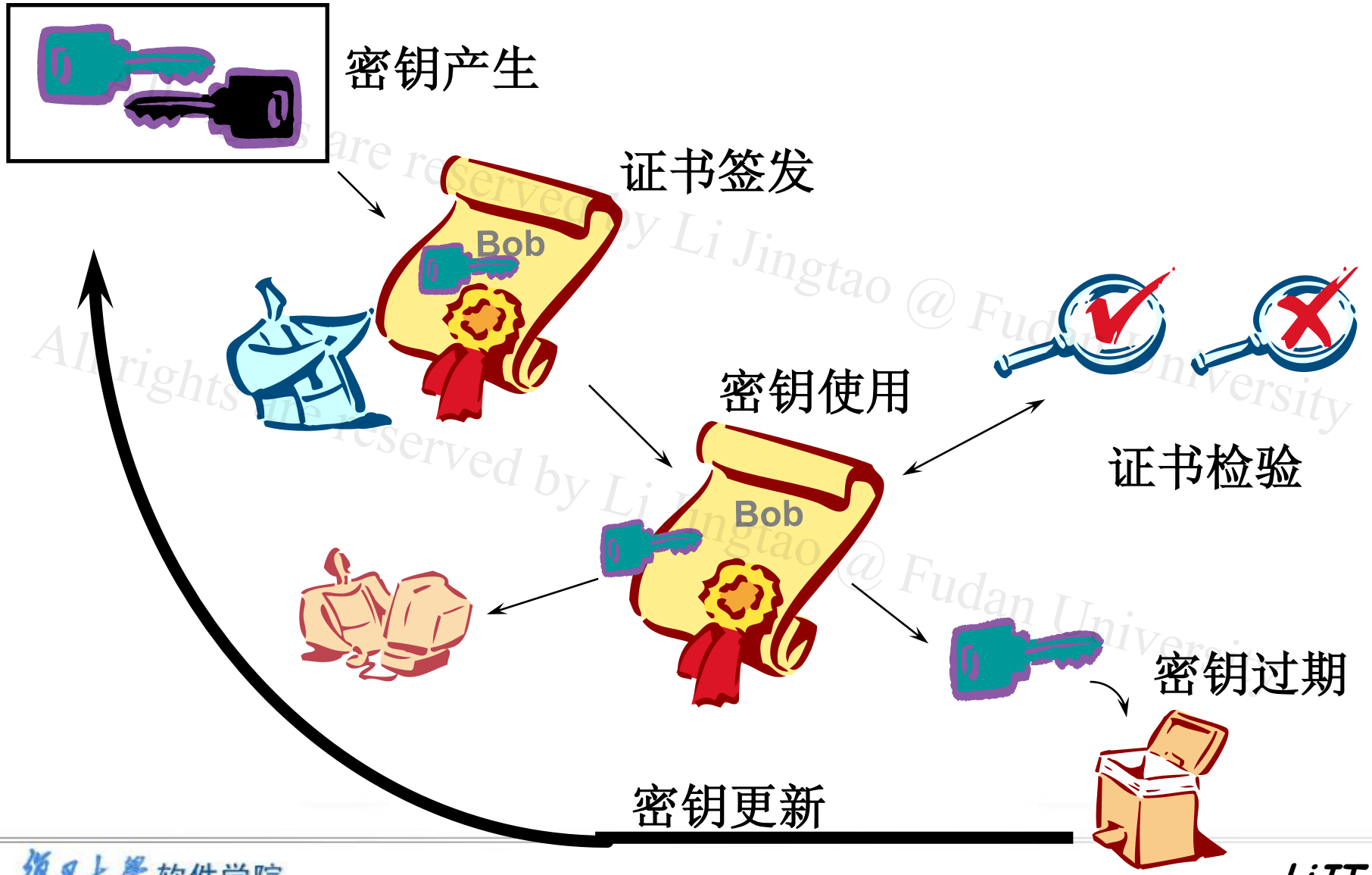


考虑一种最简单的情况：单CA模型

- 问题？
  - 密钥生命周期
  - 密钥如何获取
  - ……



密钥生命周期



PKI (Public Key Infrastructure)

- 定义：
  - 用公钥原理和技术实施和提供安全服务的具有普适性的安全基础设施
- 一个完整的PKI应该包括
  - 证书授权中心(CA)
  - 证书库
  - 证书注销
  - 密钥备份和恢复
  - 自动密钥更新
  - 密钥历史档案
  - 交叉认证
  - 支持不可否认
  - 时间戳
  - 客户端软件

内容提要

- 公钥技术回顾
- PKI之动机
- 数字证书格式
- PKI的组成
- PKI的应用

PKI中的证书

- 证书(certificate)，有时候简称为cert
- PKI适用于异构环境中，所以证书的格式在所使用的范围内必须统一
- 证书是一个机构颁发给一个安全主体的证明，所以证书的权威性取决于该机构的权威性
- 一个证书中，最重要的信息是主体名字、主体的公钥、机构的签名、算法和用途
- 签名证书和加密证书分开
- 最常用的证书格式为X.509 v3

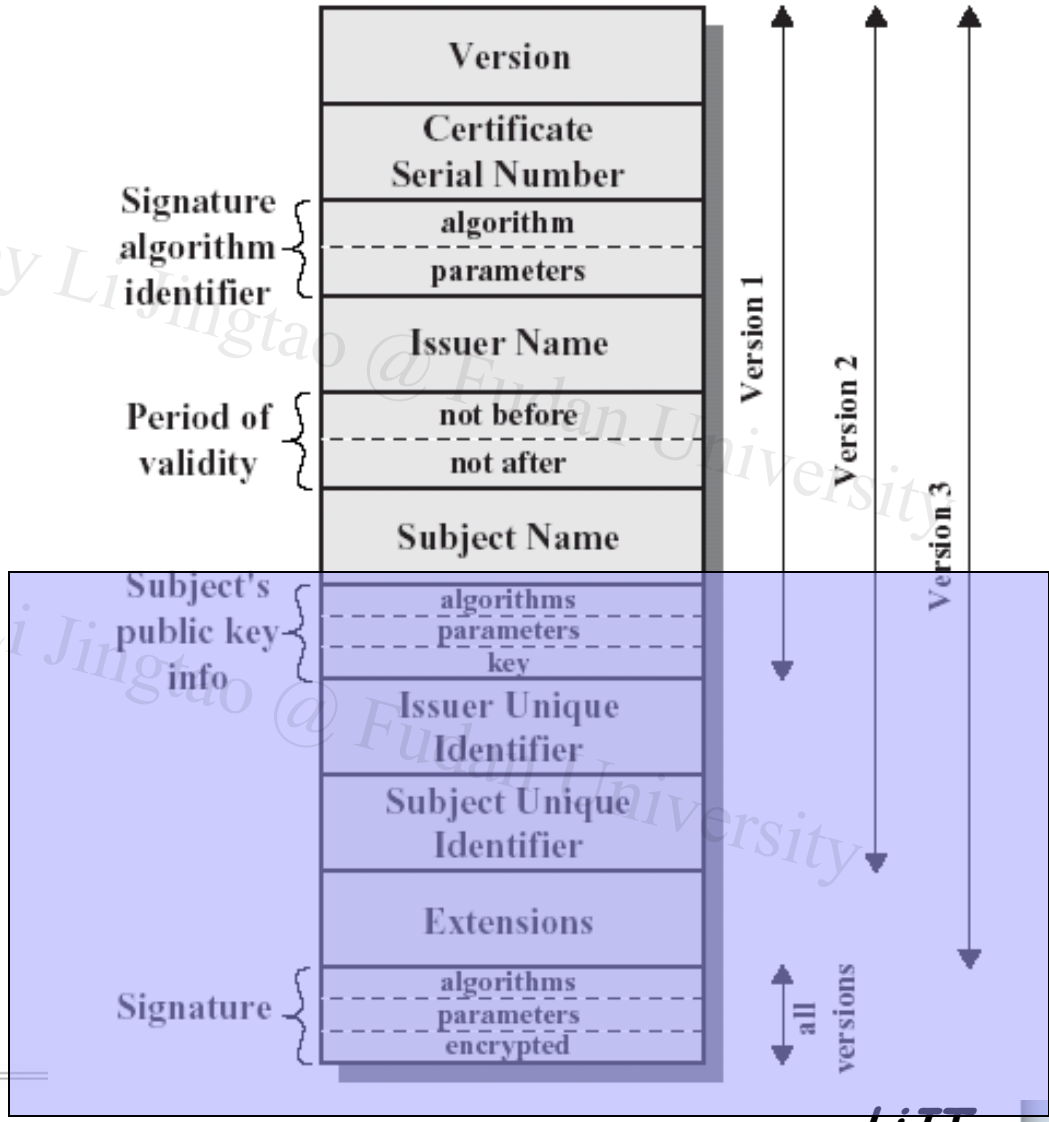
证书（续）

- 证书格式遵循 X.509国际标准
  - 实际是X.500系列标准的一个
- 证书的内容还应表明证书的有效性：
- —证书没有过期
  —密钥没有修改
  —用户仍然有权使用这个密钥
  —CA负责回收证书，发行无效证书清单
- 证书使用

  证书帮助证实个人身份，你的证书和你的密钥就是你是谁的证据

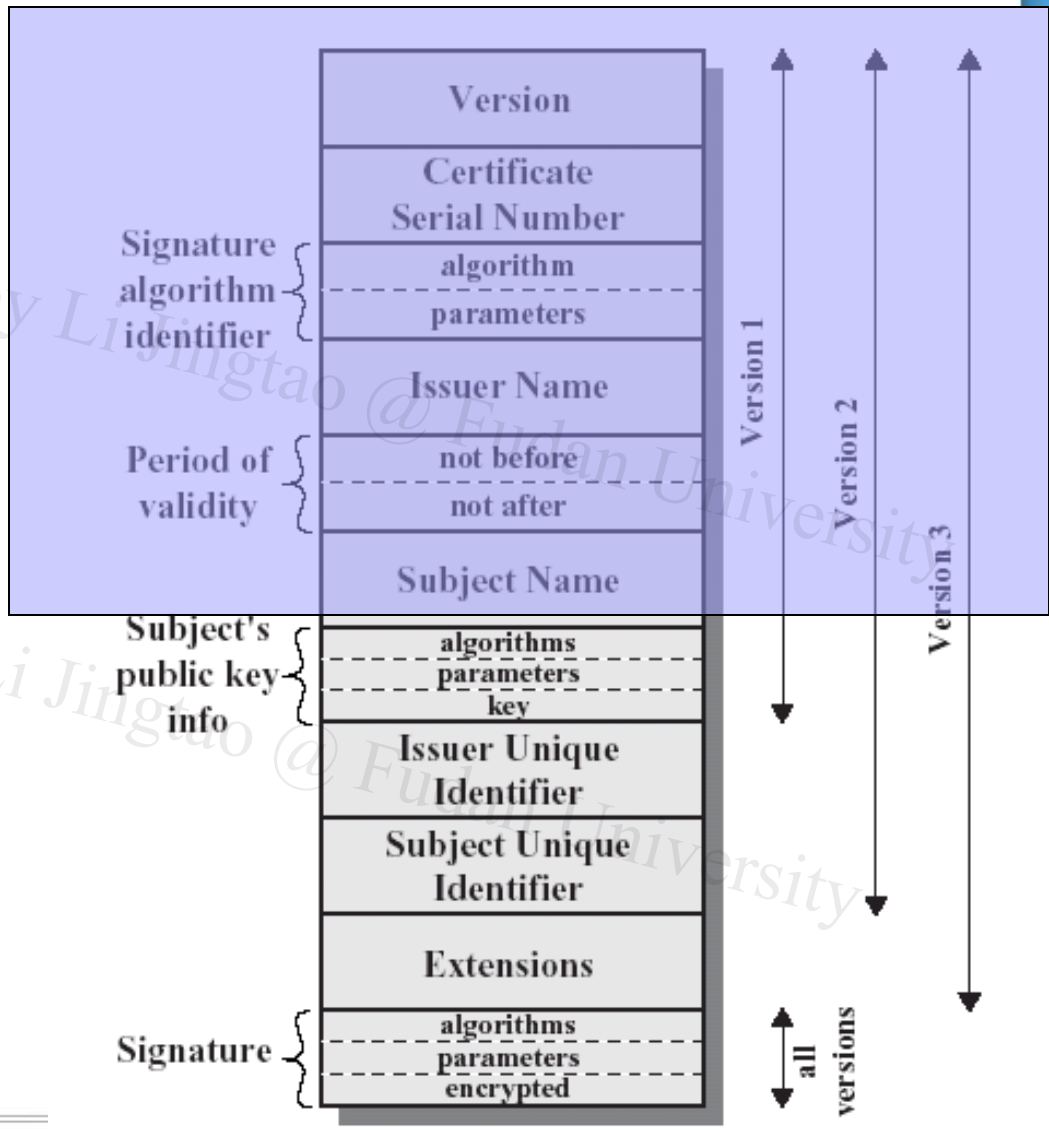
X.509证书格式

- 版本1、2、3
- 序列号
  - 在CA内部唯一
- 签名算法标识符
  - 指该证书中的签名算法
- 签发人名字
  - CA的名字
- 有效时间
  - 起始和终止时间
- 主体名字



X.509证书格式(续)

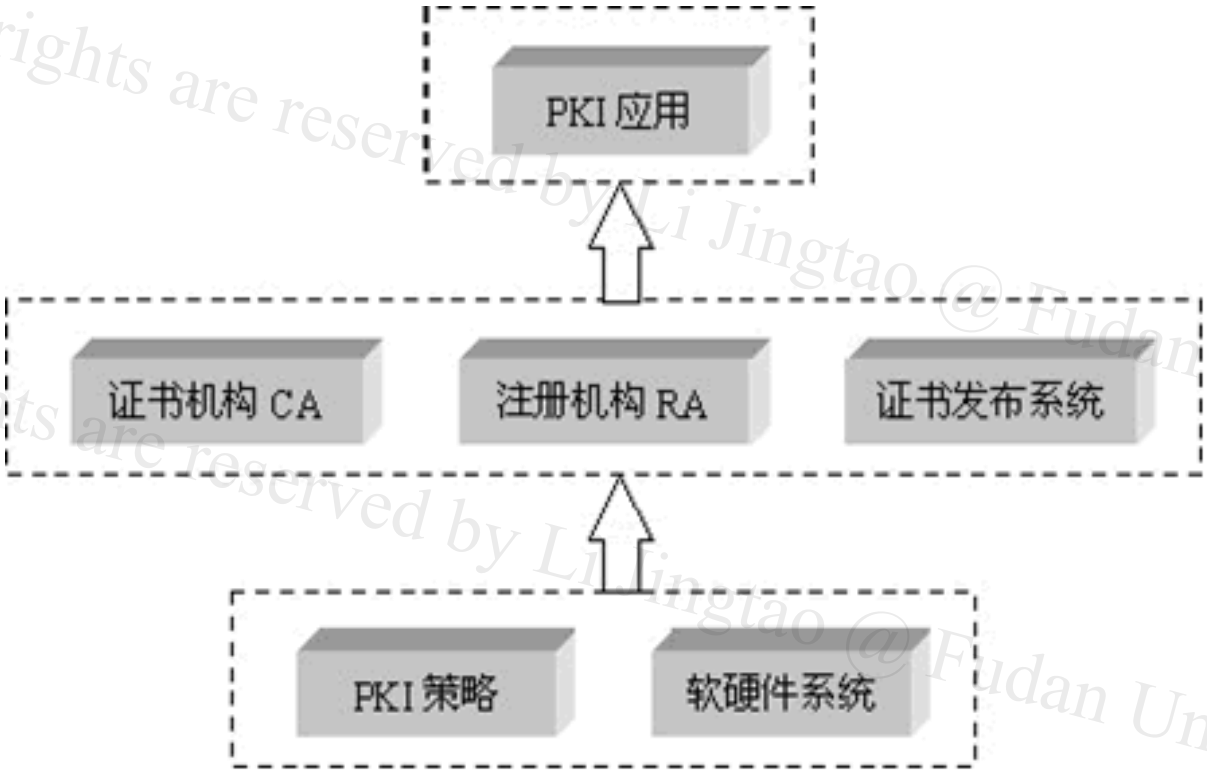
- 主体的公钥信息
  - 算法
  - 参数
  - 密钥
- 签发人唯一标识符
- 主体唯一标识符
- 扩展域
- 签名



PKI (Public Key Infrastructure)

- 复杂系统：
  - 一个简单视图
- 一个完整的PKI应该包括
  - 证书授权中心(CA)
  - 证书库
  - 证书注销
  - 密钥备份和恢复
  - 自动密钥更新
  - 密钥历史档案
  - 交叉认证
  - 支持不可否认
  - 时间戳
  - 客户端软件

PKI组成（1）



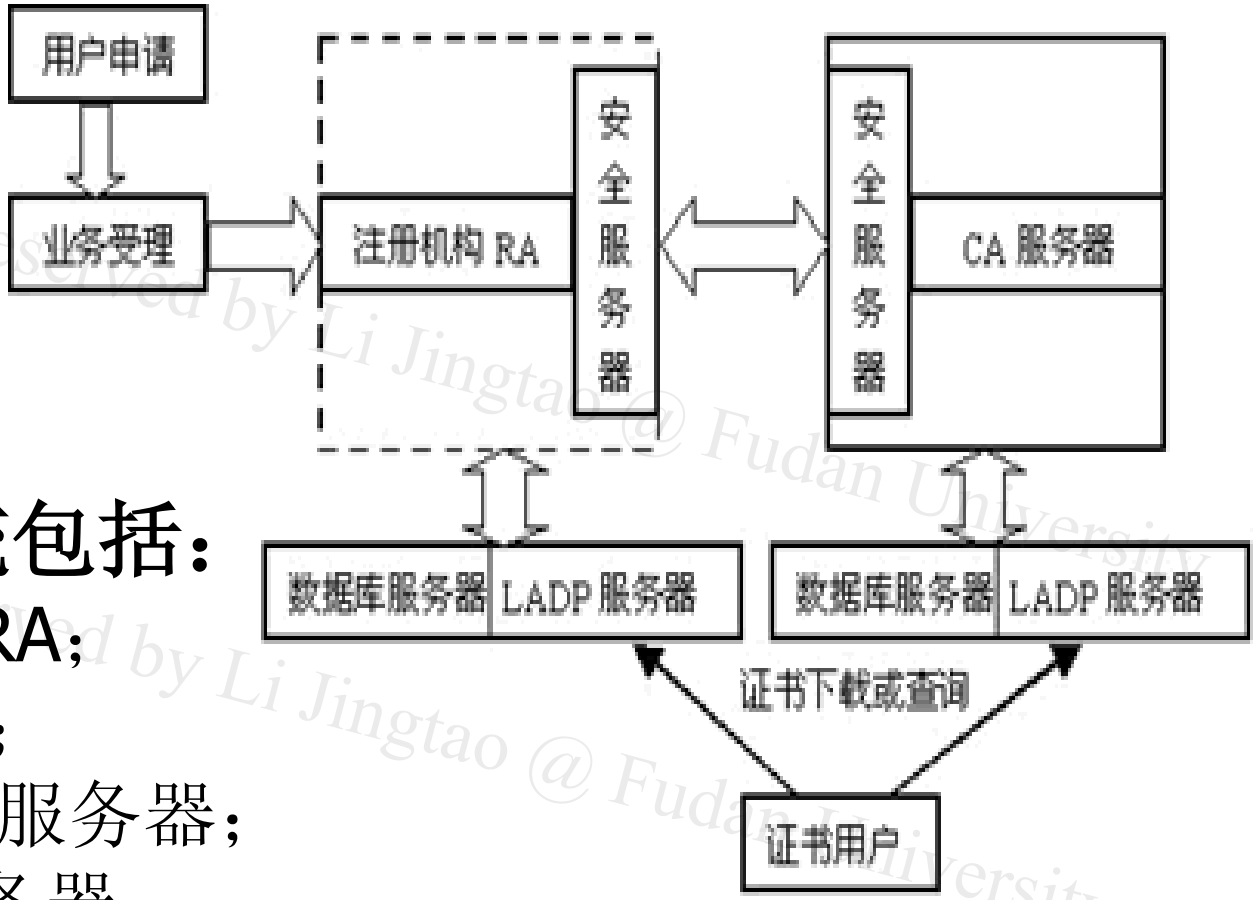
PKI组成（2）

- 软硬件系统
  支撑整个PKI信息系统运行的各种基础软硬件环境，如操作系统，网络环境。
- PKI策略
  PKI安全策略建立和定义了一个组织信息安全方面的指导方针，同时也定义了密码系统使用的处理方法和原则。它包括一个组织怎样处理密钥和有价值的信息，根据风险的级别定义安全控制的级别。一般情况下，在PKI中有两种类型的策略：
  - 一是证书策略，用于管理证书的使用，比如，可以确认某一CA是在Internet上的公有CA，还是某一企业内部的私有CA；
  - 另外一个就是CPS（Certificate Practice Statement）。一些由商业证书发放机构（CCA）或者可信的第三方操作的PKI系统需要制订CPS。这是一个包含如何在实践中增强和支持安全策略的一些操作过程的详细文档。它包括CA是如何建立和运作的，证书是如何发行、接收和废除的，密钥是如何产生、注册的，以及密钥是如何存储的，用户是如何得到它的等等。

CA(Certificate Authority)

- 职责
  - 接受用户的请求
  - (由RA负责对用户的身份信息进行验证)
  - 用自己的私钥签发证书
  - 提供证书查询
  - 接受证书注销请求
  - 提供证书注销表
- 各个组件和功能示意图

CA系统



典型的CA系统包括：

- 注册机构RA；
- CA服务器；
- LDAP目录服务器；
- 数据库服务器；
- 安全服务器

CA系统基本组件

- RA(Registration Authority)
  - 把用户的身份和它的密钥绑定起来——建立信任关系
- CA(Certificate Authority)
  - 发证
- 证书库/目录
  - 保存证书，供公开访问

注册机构RA

注册机构RA提供用户和CA之间的一个接口，在CA体系结构中起承上启下的作用，注册机构并不给用户签发证书，而只是一方面，接受用户的注册申请，收集用户信息和确认用户身份，对用户进行资格审查，决定是否同意CA给其签发数字证书并向CA提出证书请求；另一方面向LDAP服务器和安全服务器转发CA颁发的数字证书和证书撤消列表。对于一个规模较小的PKI应用系统来说，可把注册管理的职能由认证中心CA来完成，而不设立独立运行的RA。但这并不是取消了PKI的注册功能，而只是将其作为CA的一项功能而已。PKI国际标准推荐由一个独立的RA来完成注册管理的任务，可以增强应用系统的安全。

CA服务器

CA服务器使整个证书机构的核心，负责证书的签发。CA首先产生自身的私钥和公钥（密钥长度至少为1024位），然后生成数字证书，并且将数字证书传输给安全服务器。CA还负责为操作员、安全服务器以及注册机构服务器生成数字证书。CA服务器是整个结构中最为重要的部分，存有CA的私钥以及发行证书的脚本文件，出于安全的考虑，应将CA服务器与其他服务器隔离，任何通信采用人工干预的方式，确保认证中心的安全。

LDAP服务器

LDAP服务器提供目录浏览服务，负责将注册机构服务器传输过来的用户信息以及数字证书加入到服务器上。这样其他用户通过访问LDAP服务器就能够得到其他用户的数字证书。

数据库服务器

数据库服务器是认证机构中的核心部分，用于认证机构中数据（如密钥和用户信息等）、日志合统计信息的存储和管理。实际的的数据库系统应采用多种措施，如磁盘阵列、双机备份和多处理器等方式，以维护数据库系统的安全性、稳定性、可伸缩性和高性能。

安全服务器

安全服务器面向普通用户，用于提供证书申请、浏览、证书撤消列表以及证书下载等安全服务。安全服务器与用户的的通信采取安全信道方式（如SSL的方式，不需要对用户进行身份认证）。用户首先得到安全服务器的证书（该证书由CA颁发），然后用户与服务器之间的所有通信，包括用户填写的申请信息以及浏览器生成的公钥均以安全服务器的密钥进行加密传输，只有安全服务器利用自己的私钥解密才能得到明文，这样可以防止其他人通过窃听得到明文。从而保证了证书申请和传输过程中的信息安全性。

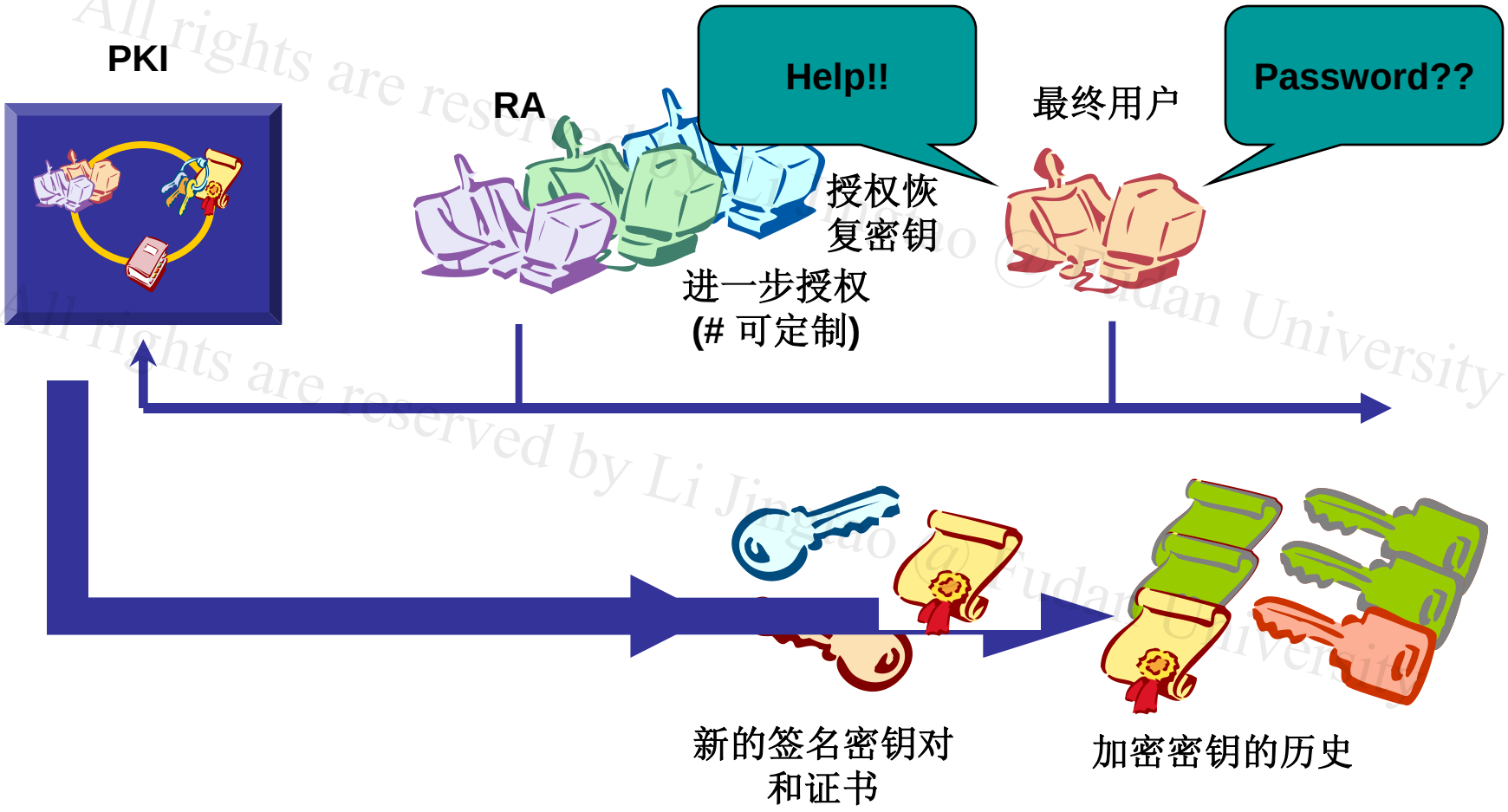
证书的撤销机制

- 由于各种原因，证书需要被撤销
  - 比如，私钥泄漏、密钥更换、用户变化
- PKI中注销的方法
  - CA维护一个CRL(Certificate Revocation List)

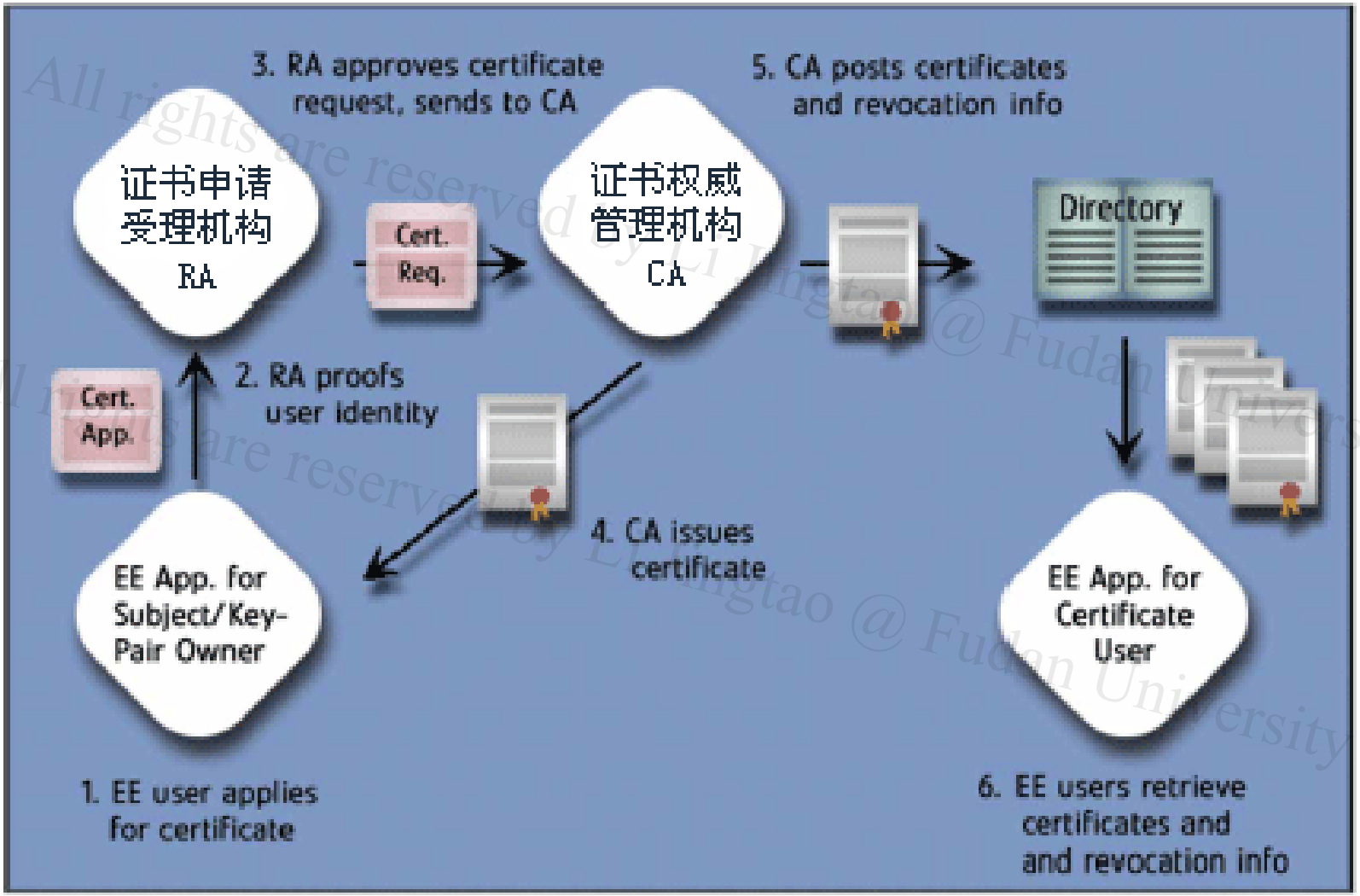
CRL

- CRL格式
  - X.509 V2 CRL
  - 分段CRL、增量CRL
  - CRL支持LDAP，HTTP等发布方式
  - 每XX小时一次发布一次
- 基于Web的CRL服务
  - 检查CRL的URL应该内嵌在用户的证书中
  - 可以提供安全途径(SSL)访问URL
  - 返回注销状态信息
  - 其他的用法由浏览器决定

密钥备份和恢复



PKI的运作过程

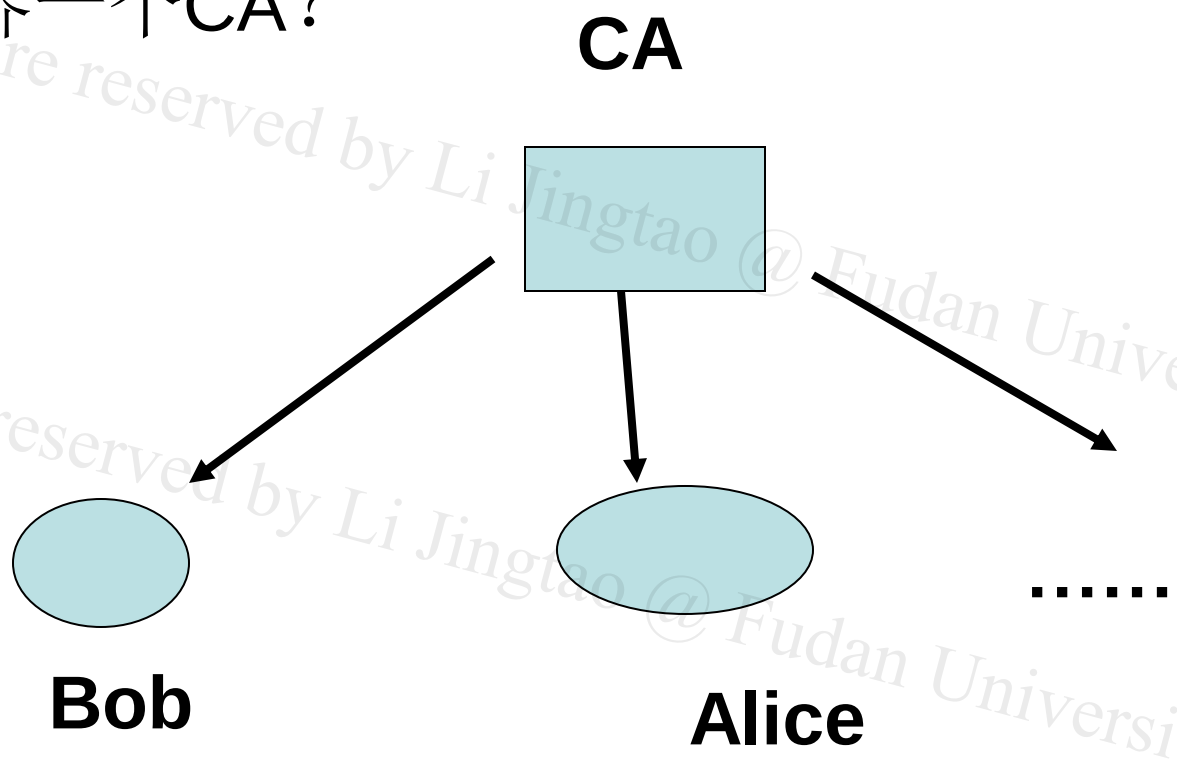


内容提要

- 公钥技术回顾
- PKI之动机
- 数字证书格式
- PKI的组成
- PKI信任关系
- PKI的应用

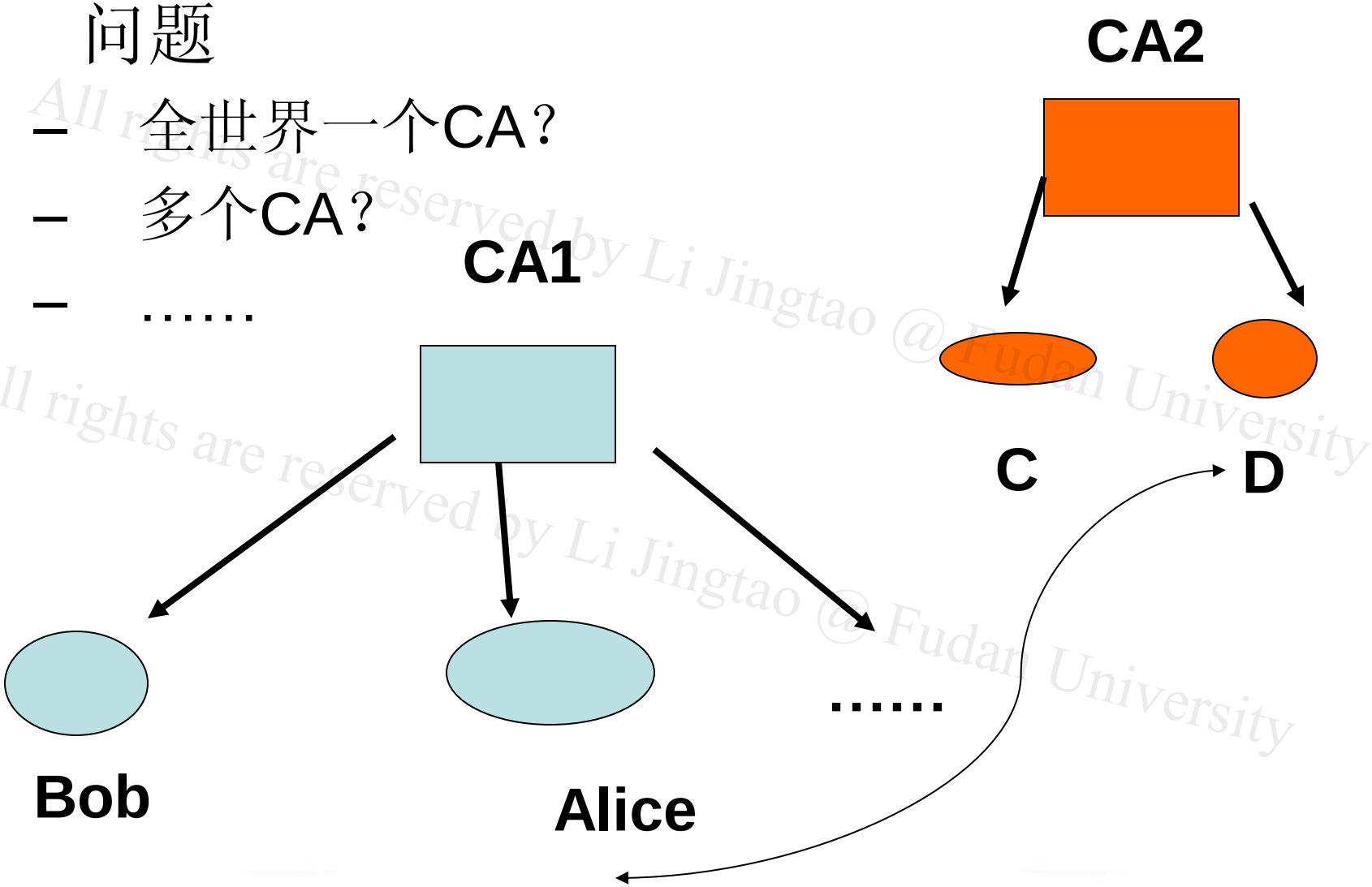
单CA模型

- 问题
  - 全世界一个CA?



单CA模型

- 问题
  - 全世界一个CA?
  - 多个CA?
  - ……

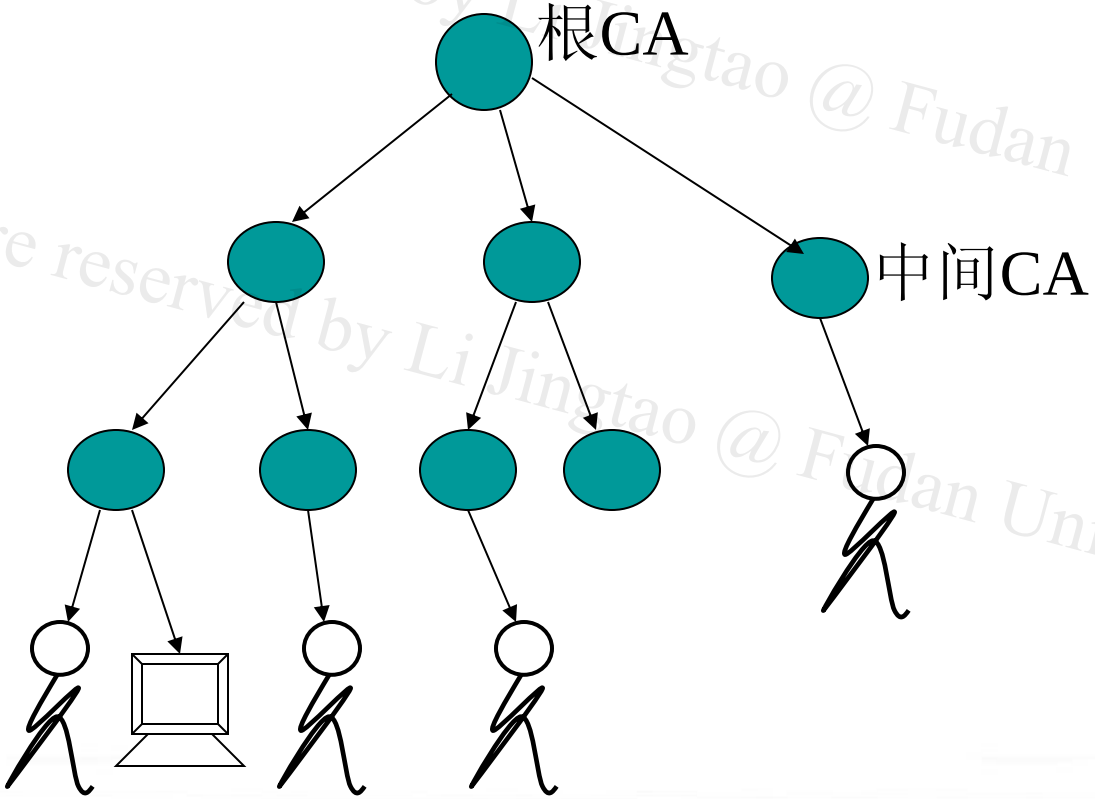


CA信任关系

- 当一个安全主体看到另一个安全主体出示的证书时，他是否信任此证书？
  - 信任难以度量，总是与风险联系在一起
- 可信CA
  - 如果一个主体假设CA能够建立并维持一个准确的“主体-公钥属性”之间的绑定，则他可以信任该CA，该CA为可信CA
- 信任模型
  - 基于层次结构的信任模型
  - 交叉认证

CA层次结构

- 对于一个运行CA的大型权威机构而言，签发证书的工作不能仅仅由一个CA来完成
- 它可以建立一个CA层次结构



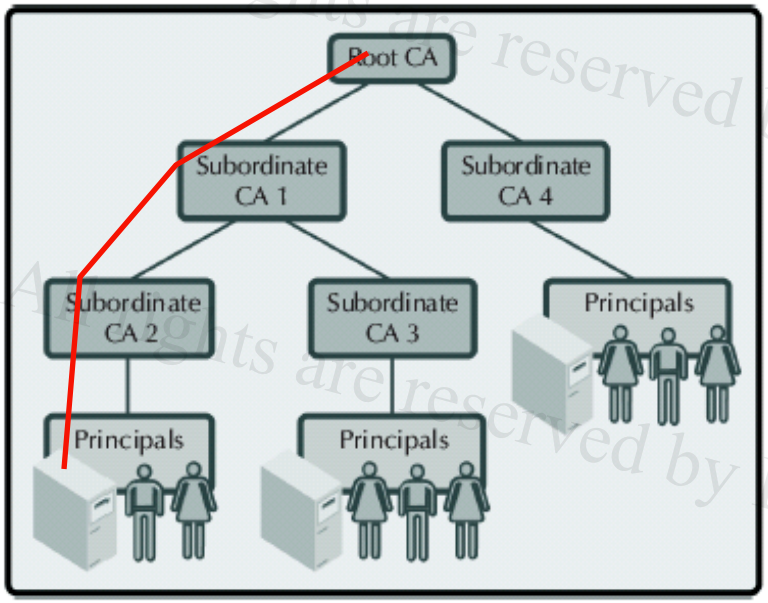
CA层次结构的建立

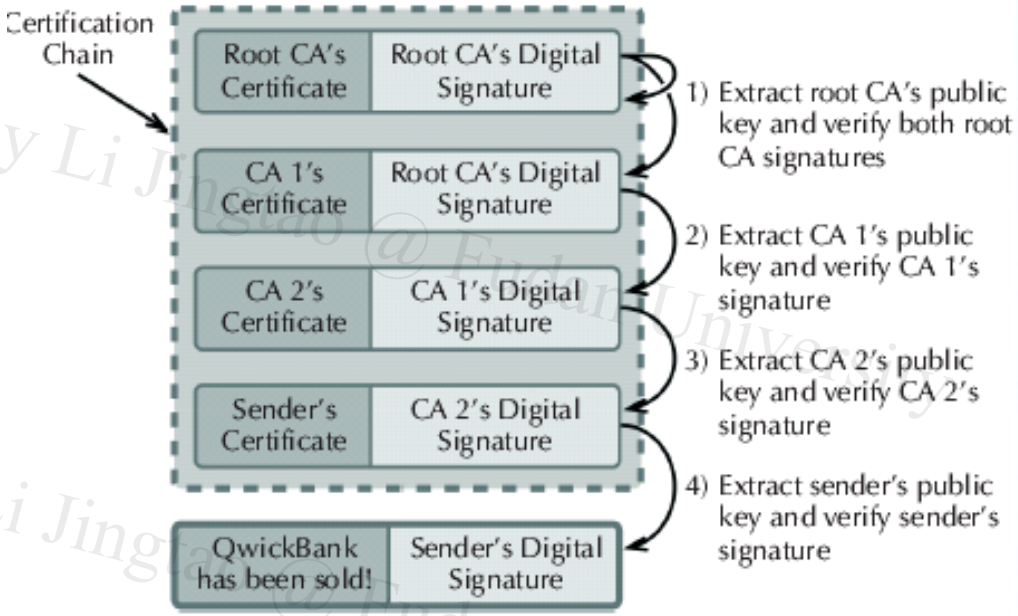
- 根CA具有一个自签名的证书
- 根CA依次对它下面的CA进行签名
- 层次结构中叶子节点上的CA用于对安全主体进行签名
- 对于主体而言，它需要信任根CA，中间的CA可以不必关心(透明的)；同时它的证书是由底层的CA签发的
- 在CA的机构中，要维护这棵树
  - 在每个节点CA上，需要保存两种cert
    (1) Forward Certificates: 其他CA发给它的certs
    (2) Reverse Certificates: 它发给其他CA的certs

层次结构CA中证书的验证

- 假设主体A看到B的一个证书
- B的证书中含有签发该证书的CA的信息
- 沿着层次树往上找，可以构成一条证书链，直到根证书
- 验证过程：
  - 沿相反的方向，从根证书开始，依次往下验证每一个证书中的签名。其中，根证书是自签名的，用它自己的公钥进行验证
  - 一直到验证B的证书中的签名
  - 如果所有的签名验证都通过，则A可以确定所有的证书都是正确的，如果他信任根CA，则他可以相信B的证书和公钥
- 问题：证书链如何获得？

证书链的验证示例





交叉认证

- 两个不同的CA层次结构之间可以建立信任关系
  - 单向交叉认证
    - 一个CA可以承认另一个CA在一定名字空间范围内的所有被授权签发的证书
  - 双向交叉认证
- 交叉认证的约束
  - 名字约束
  - 路径长度约束
  - 策略约束

交叉认证

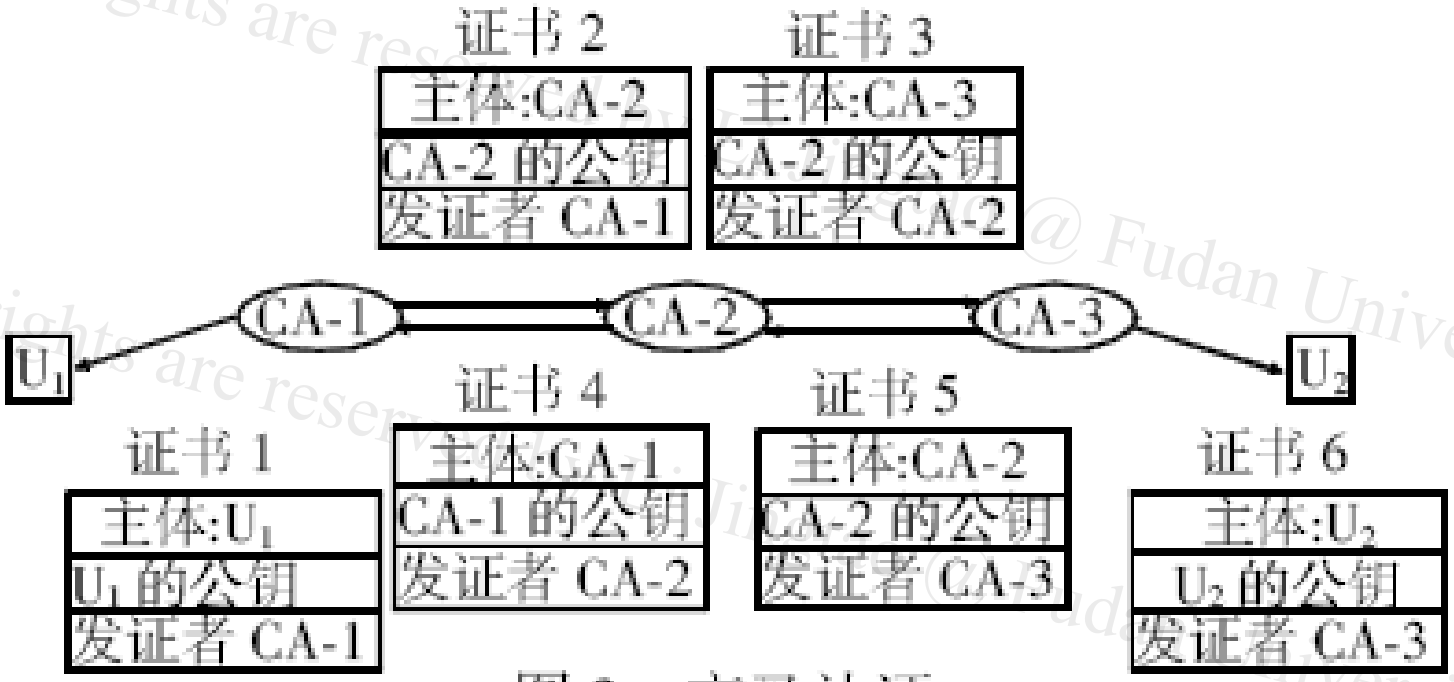


图 2　交叉认证

桥CA （BCA）

- 不同于交叉认证结构的PKI, BCA 不直接向用户发放证书;
- BCA 不作为一个可信任点供PKI中的用户使用, 这一点也不同于层次结构中的根CA。
- BCA 与不同的用户群体建立对等的可信任关系, 允许用户保持原有的可信任点。
- 这些关系被结合起来形成“信任桥”，使得来自不同用户群体的用户通过指定信任级别的BCA 相互作用。

桥CA （BCA）

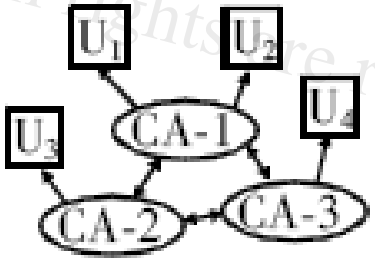


图 3 网状结构的 PKI 认证体系

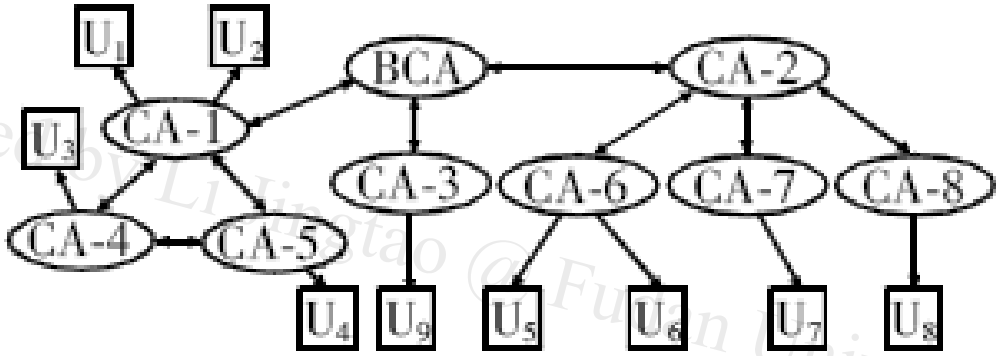


图 4 桥 CA 认证体系

与PKI有关的标准情况

- Certificates —— X.509 v.3
- 交叉认证 —— PKIX group in IETF(RFC 2459)
- 智能卡/硬件插件 PKCS #11
- PKCS系列
- 目录服务LDAP

PKCS系列标准

PKCS是由RSA公司及其合作伙伴制定的一组公钥密码学标准，其中包括证书申请、证书更新、证书撤销列表发布、扩展证书内容以及数字签名、数字信封的格式等方面的一系列相关协议。

- PKCS #1
  - RSA Encryption Standard
- PKCS #3
  - Diffie-Hellman Key-Agreement Standard
- PKCS # 5
  - Password-Based Encryption Standard
- PKCS #6
  - Extended-Certificate Syntax Standard

PKCS系列标准(续)

- PKCS #7
  - Cryptographic Message Syntax Standard
- PKCS #8
  - Private-Key Information Syntax Standard
- PKCS #9
  - Selected Attribute Types
- PKCS #10
  - Certification Request Syntax Standard
- PKCS #11
  - Cryptographic Token Interface Standard
- PKCS #12
  - Personal Information Exchange Standard
- PKCS #13
  - Elliptic Curve Cryptography Standard
- PKCS #15
  - Cryptographic Token Information Format Standard

PKI提供的基本服务

- 认证
  - 采用数字签名技术，签名作用于相应的数据之上
    - 被认证的数据 —— 数据源认证服务
    - 用户发送的远程请求 —— 身份认证服务
    - 远程设备生成的challenge信息 —— 身份认证
- 完整性
  - PKI采用了两种技术
    - 数字签名：既可以是实体认证，也可以是数据完整性
    - MAC(消息认证码)：如DES-CBC-MAC或者HMAC-MD5
- 保密性
  - 用公钥分发随机密钥，然后用随机密钥对数据加密
- 不可否认
  - 发送方的不可否认 —— 数字签名
  - 接受方的不可否认 —— 收条 + 数字签名

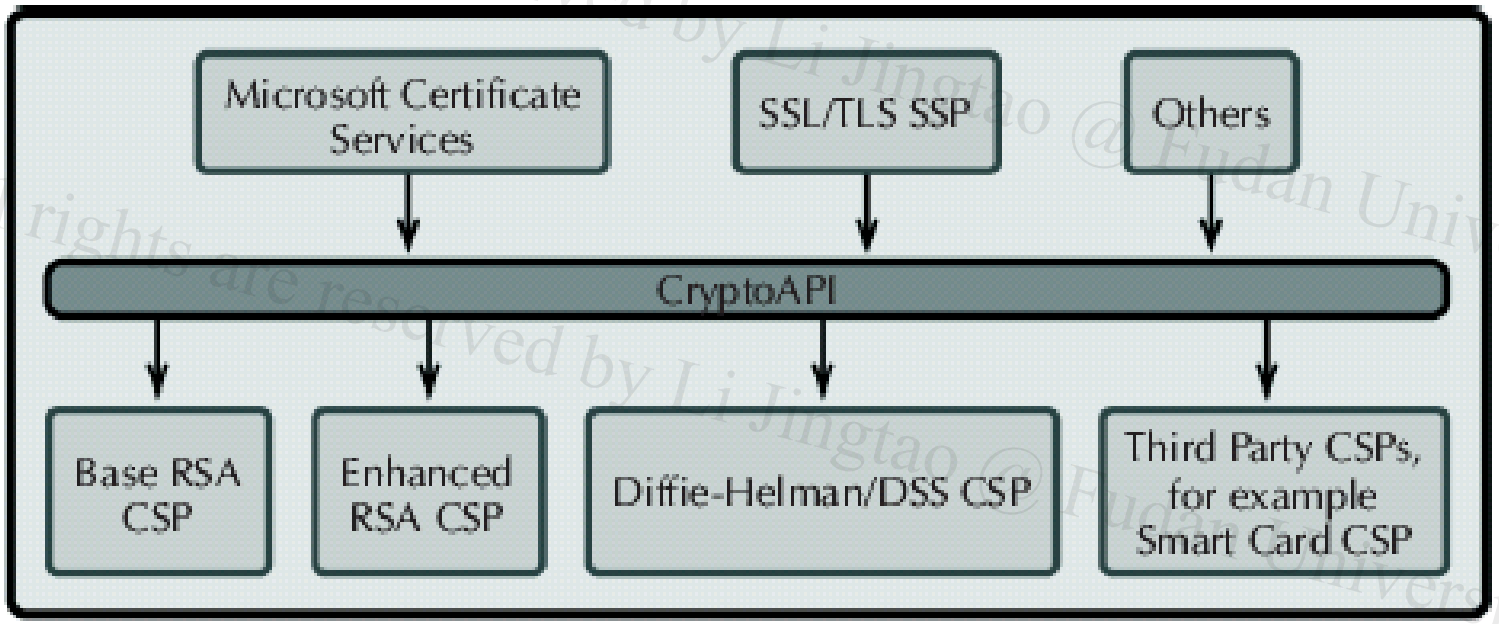
PKI应用

- 基本的应用
  - 文件保护
  - E-mail
  - Web应用
- 其他
  - VPN
  - SSL/TLS
  - XML/e-business
  - WAP

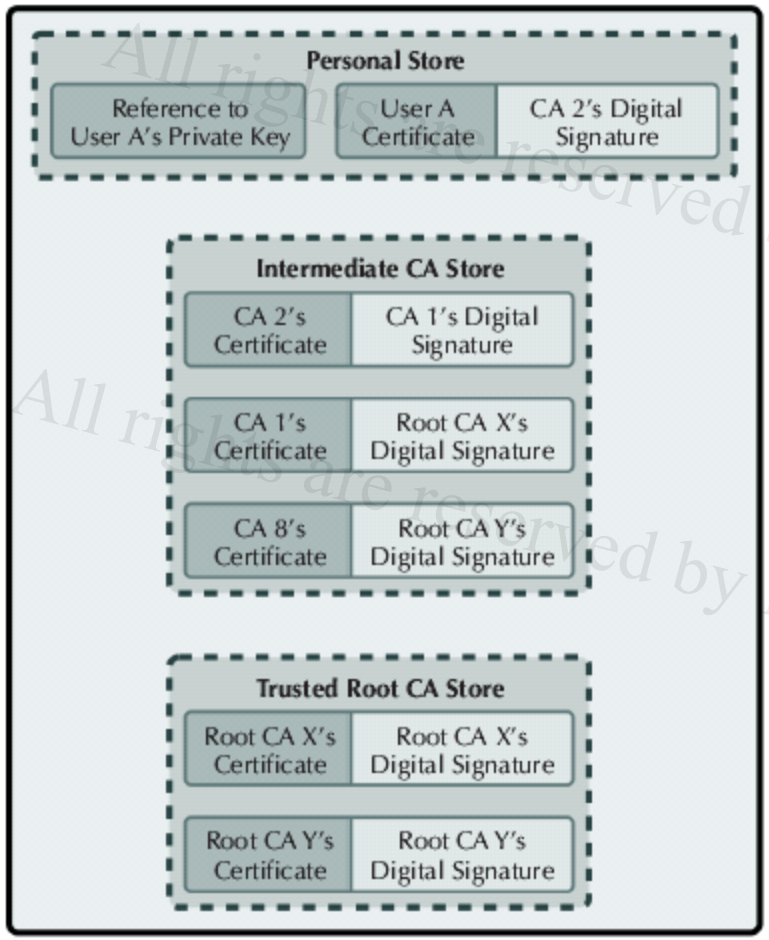
- Microsoft CryptoAPI
- ……

Windows 2000中的PKI

- Windows 2000中的安全模块示意图



Windows 2000中的证书存储区



内容提要

- 公钥技术回顾
- PKI之动机
- 数字证书格式
- PKI的组成
- PKI信任关系
- PKI的应用

PKI实现的选择

- 建立自己的PKI
- 购买一个PKI
- 从第三方购买PKI服务
- 等待一个政府PKI
- PKI和应用联合开发，相互协作

国内CA发展状况简介

- 1998年成立第一家CA，已有100多家
- 分类：区域类、行业类、商业类、内部自用类

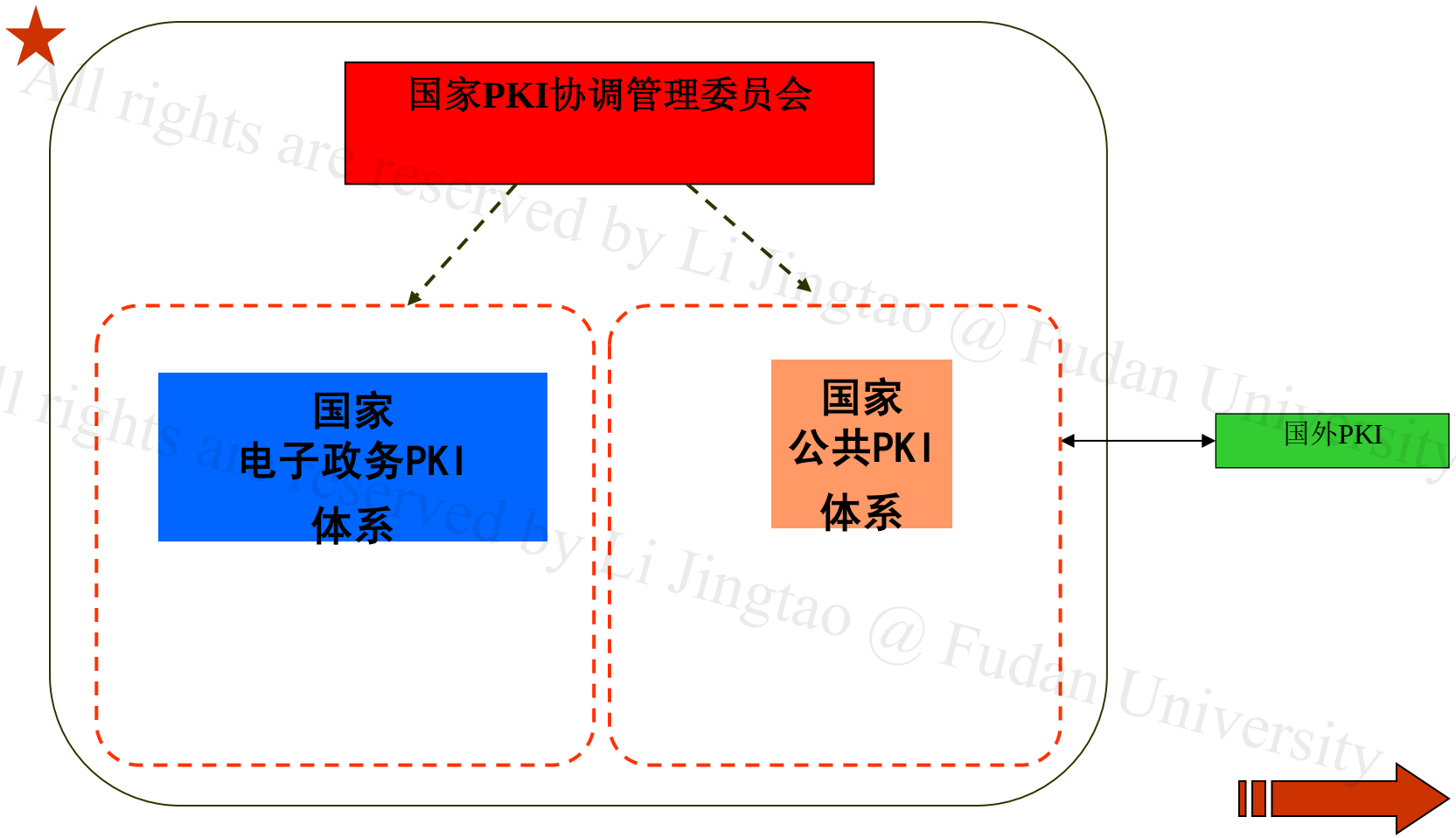
上海的CA简介

- 上海主要的CA
  - 上海CA中心
  - 公务网CA中心
  - 上海证券交易所CA
  - 工商CA
  - 其他行业内部CA
  - 企业内部CA

A Case Study-国家PKI发展规划

- 统一领导、统一规划、统一标准，由政府主管部门实行授权管理；
- 坚持独立自主的原则，积极支持民族产业和信息安全服务业；
- 高度重视PKI体系自身安全的建设；
- 在统筹规划下，充分发挥各行业、各地区的积极性，分工合作，积极探索与实验、稳步推进

国家PKI体系的构成



国家PKI协调管理委员会

- 是国家的PKI政策管理机构,负责制定国家PKI管理政策、国家PKI体系发展规划，监督、指导国家电子政务PKI体系和国家公共PKI体系的建设、运行和应用，具体负责审批CA机构的成立和撤消

国家电子政务PKI体系

- 是服务于国家各级机构、组织和部门的内部电子政务业务（如公文流转）的PKI体系
- 负责向参与这些业务的各实体（包括人员、机构和设备）提供信任和安全服务
- 采用严格的层次结构信任模型，由政务根中心（GRCA）、政务认证中心（GCA）和注册机构（RA）组成

国家公共PKI体系的信任模型

- 国家公共PKI体系采用网状信任模型，由国家桥中心（NBCA）、地区桥中心（LBCA）、公众服务认证中心（SCA）和注册机构（RA）组成
- 国家桥中心NBCA是沟通各地方、各行业建立的CA认证中心的桥梁，它只与CA进行交叉认证，不向最终用户发放证书
- 地区桥中心LBCA功能与NBCA类似，但它是自发组织的机构，代表一批CA与NBCA交叉认证；

公开密钥基础设施的应用

- ✓ 随着互联网技术的推广和普及，各种网络应用如电子商务、电子政务、网上银行、网上证券交易等也迅猛发展。但如何保障这些应用的安全性，已成为发展网络通信需要解决的重要任务。
- ✓ 在公开密钥加密技术基础上发展起来的PKI（Public Key Infrastructure，公钥基础设施）很好地适应了互联网的特点，可为互联网以及网络应用提供全面的安全服务如认证、密钥管理、数据完整性检验和不可否认性保证等。今天互联网的安全应用，已经离不开PKI的支持了。

立法情况

- ✓电子签名法
  - ✓美国，2000年，克林顿
  - ✓中国，2004年，个别应用有限制