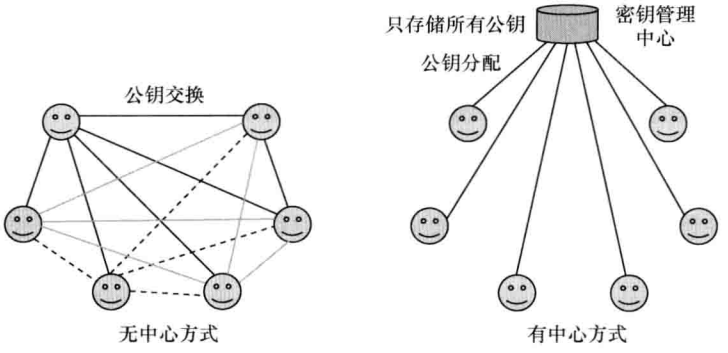

图 1-3　非对称密钥管理技术的两种模式

1．无中心模式

每对用户通过交换获得对方公钥。当两个用户之间需要保密通信时，可以直接使用对方的公钥对数据加密，对方收到密文后用自己的私钥即可解密；也可以随机产生一个对称密钥，使用对称密钥对数据加密，再使用对方的公钥加密对称密钥，对方收到密文后，先用自己的私钥解密获得对称密钥，然后再使用该对称密钥解密数据。

无中心模式具有以下特点：

（1）公钥交换次数随用户数目呈指数增长。N 个用户时，共需要公钥交换次数为 $N(N-1)/2$。如，N=6 时为 15 次交换，N=1000 时为 500 000 次交换。

（2）每个用户需保存所有用户的公钥。N 个用户时，每个用户需保管 $N-1$ 个公钥。

由于公钥交换次数随用户数目呈指数增长，且每个用户都需要管理所有用户的公钥，因此该模式只适合用于小规模用户场合。

该模式目前比较成熟的应用是 PGP 模式，在互联网上有很多独立的个人群体内部使用。

2．有中心模式

存在一个独立的密钥管理中心，每个用户均信任该中心。密钥管理中心为每个用户分配一个公钥，并负责存储和管理所有的用户公钥。在进行密钥分配时，可由用户自己产生公钥和私钥，只把公钥提交给密钥管理中心；也可以由密钥管理中心为用户产生公钥和私钥，把公钥和私钥均安全传递给用户，但只保存公钥。当某用户的私钥泄露后，密钥管理中心将该用户的公钥标记为失效。

当两个用户之间需要保密通信时，需要通过密钥管理中心动态验证对方公钥的合法性：（1）该公钥是否失效；（2）该公钥是否是当前用户的。

有中心模式具有以下特点：

（1）公钥分配次数与用户数目呈线性关系。N 个用户时，公钥分配次数为 N，且每个用户只需保管 1 个私钥和公钥。

（2）由于公钥是随机产生的，无法判断属于哪个用户，因此密钥管理中心需保存公钥与用户的映射关系，存在映射关系被篡改的安全风险。

（3）用户之间进行保密通信时，需要通过密钥管理中心动态验证对方公钥的合法性，既无法实现脱机保密通信，又容易导致密钥管理中心成为性能瓶颈。

由于密钥管理中心需存储所有公钥与用户的映射关系，且需在线验证公钥的合法性，因

此该模式不适合于大规模的公众服务领域。

1.3 PKI 本质是把非对称密钥管理标准化

由于非对称密钥管理的无中心模式只适合用于小规模用户场合，很难适应公众普遍参与的信息时代，已经逐渐被边缘化；在信息时代，非对称密钥管理的有中心模式已经成为主流。

非对称密钥管理模式，尽管很好地解决了密钥协商或分配时密钥容易泄露的难题，但并没有解决好密钥与用户映射关系容易被篡改的问题，依然通过密钥管理中心集中存储公钥与用户的映射关系。

PKI 通过引入 CA、数字证书、LDAP、CRL、OCSP 等技术并制定相应标准，有效地解决了公钥与用户映射关系、集中服务性能瓶颈、脱机状态查询等问题；同时为促进并提高证书应用的规范性，还制定了很多与证书应用相关的各种标准。

1. CA 和数字证书

为有效解决公钥与用户映射关系容易被篡改的问题，PKI 引入“CA”和“数字证书”技术。

（1）CA 为证书权威，是 Certificate Authority 的缩写，也称作 CA 中心或证书认证中心，是一种特殊的密钥管理中心，拥有自己的公钥和私钥，负责给用户签发数字证书，即使用 CA 中心私钥对用户身份信息和公钥信息进行加密处理（签名）后形成数字证书。

（2）数字证书是一种特殊的文件格式，包含用户身份信息、用户公钥信息和 CA 中心私钥的签名。用户身份信息包括姓名或名称、单位、城市、国家等。

当获得数字证书后，使用 CA 中心的公钥对数字证书中私钥的签名进行解密处理后，就可验证该数字证书是否被篡改，从而确认公钥与用户身份的映射关系。只要保证 CA 中心私钥的安全性，就能保证数字证书很难被篡改，从而保证了公钥与用户映射关系很难被篡改。

用户在验证数字证书是否被篡改时，必须首先获得 CA 中心的公钥。为方便用户识别 CA 中心的公钥，CA 中心也为自己签发数字证书，该证书包含 CA 中心公钥、CA 中心身份信息和 CA 中心私钥的签名。

数字证书实际上是把用户公钥、公钥与用户的绑定关系以公开形式发布出去，方便信息时代大规模用户使用。

2. LDAP

CA 中心存储着所有[illegible]字证书，为方便用户快速获得交易对方的数字证书，避免 CA 中心成为性能瓶颈，PKI 又引入了 LDAP 技术，通过 LDAP 方式对外提供证书查询或下载服务。LDAP 为轻量目录访问协议，是 Light-weight Directory Access Protocol 的缩写。

专业的关系型数据库管理系统（如 Oracle、DB2 等），专门对结构化数据进行管理，应用系统只需通过 SQL 语句（报文协议）发送各种数据管理指令，而具体管理工作完全由数据库管理系统负责。尽管这种数据管理方式大大简化了应用系统的复杂度，但由于其读写功能相对均衡，很难满足高性能的查询服务。为获得高性能的查询服务，需要对数据管理的读取功能进行特殊优化，于是出现了目录服务技术（DAP）。目录服务技术对查询功能进行优化，比修改操作快 10 倍以上，适合快速响应和大容量查询服务。DAP 技术通过目录树方式对数

据进行管理，应用系统只需通过 X.500 协议就能对数据进行快速查询。

由于 X.500 协议过于复杂，实现成本很高，于是国际组织对 X.500 进行了简化，形成 LDAP 标准，而且 LDAP 支持 TCP/IP 协议，更适合于互联网领域使用。

由于数字证书是可以公开的，CA 中心也可以将其签发的数字证书存储到其他地方，供用户查询或下载。

3．CRL 和 OCSP

当用户私钥泄露后，CA 中心有责任将该用户的证书标记为失效。但用户如何获得对方证书是否失效的状态呢？为方便用户获得证书状态，PKI 引入了 CRL 和 OCSP 技术。

（1）CRL（Certificate Revocation List）。

CRL 为证书作废列表，是 Certificate Revocation List 的缩写，也称作证书黑名单，是一种特殊的文件格式，包含所有失效的证书清单、下次 CRL 生成时间和 CA 中心私钥的签名。

CA 中心定期生成 CRL，并将下次生成时间写入 CRL 中，方便用户按时定期下载 CRL。跟数字证书类似，CRL 也是通过 CA 中心私钥的签名来保证 CRL 无法被篡改的。用户只需定期获取 CRL 后，就可在本地脱机验证证书是否失效，在下次 CRL 生成时间之前无需联系 CA 中心。

由于 CRL 是可以公开的，CA 中心也可以将其签发的 CRL 存储到其他地方，供用户查询或下载。

（2）OCSP（Online Certificate Status Protocol）。

当 CA 中心将私钥已泄露的用户证书标记为失效后，如果还未到下次 CRL 生成时间，此时其他用户通过最新 CRL 并不知道该用户证书已经失效，依然将该用户当作有效用户继续进行各种保密通信和合法交易，可能会造成一定的损失。

为解决 CRL 滞后的缺陷，避免给高实时性或高风险交易造成重大损失，PKI 引入了 OCSP，对用户提供实时的证书状态查询服务。

OCSP 为在线证书状态协议，是 Online Certificate Status Protocol 的缩写，当用户需要实时查询对方证书是否有效时，可通过 OCSP 协议实时访问 CA 中心获得对方证书的当前状态。

4．其他 PKI 标准

除与 CA 直接相关的上述标准外，PKI 还包括其他很多标准，如密码相关标准、证书应用标准、证书存储标准、证书访问标准、CA 运营标准等。

密码相关标准包括 ASN.1、DER、HMAC、DES、AES、RSA、ECC 等。

证书应用标准包括 SSL/TLS、SET、WAP、IPSec、TSP、PMI 等。

证书存储标准包括 PKCS 系列标准、ISO 7816 系列标准等。

证书访问标准包括 PKCS 11、CryptoAPI、JCE、PC/SC 等。

CA 运营标准包括 CP、CPS 等。

1.4　私钥专有性使人联想到手写签名

CA 中心为每个用户签发包含用户公钥的数字证书，而用户私钥只由用户自己保管，CA 中心及每个用户都不知道其他任何用户的私钥。

如果采用各种管理手段和技术手段能够确保不发生以下操作，则在网络上由用户私钥进行的任何加解密操作行为，均可以看作是该用户的正常行为：

（1）用户私钥不会被泄露，任何其他人都无法获得该私钥。

（2）用户私钥不会被劫持，任何其他人都不能在违背该用户主观意愿下使用该私钥随意进行加解密操作。

显然，私钥属于用户专有，这种特性很容易让人联想到手写签名。私钥由计算机随机产生，相同的概率很低，具有唯一性；使用私钥对数据进行加解密操作，可看作是“签名动作”（事实上，只有私钥加密属于签名范畴，具体原理可参考后续章节的内容）。使用私钥对电子文档进行加密操作后的结果称作数字签名或电子签名。

尽管电子签名与手写签名具有很高的相似性，但本质上还是存在很多区别的：

（1）电子签名仅表现为一组代码，需要计算机系统进行鉴别，无法仅凭视觉来进行辨认。

（2）电子签名是一种数据，无法以原件形式提交。这对传统的法律证据规则提出了挑战。

（3）电子签名可通过计算机网络在线签署，可以节省当事人的时间、提高交易效率。

（4）电子签名需要特殊电子认证方式以确定其真实性。需要经过资质信誉良好的认证机构按照一定的标准，通过计算机系统的核查对电子签名的真实性与有效性予以确认。

（5）电子签名容易被改动，且修改后不易被发现，可能给电子签名的签署者在电子交易中带来很大的损失。

1.5 电子签名法赋予电子签名与认证法律地位

如果电子文档是一份商务合同，那么用户私钥签署电子签名后是否就成为电子合同呢？如果电子签名没有法律效力，该文档还是一个普通的电子文档，并不是真正意义上的电子合同。可喜的是，期盼已久的《中国人民共和国电子签名法》（以下简称《电子签名法》）终于于 2005 年 4 月 1 日正式施行，该法给电子签名与认证赋予了法律效力，大大增强了电子交易的安全性，保障网上交易者的信心，建立良好的网络信用机制和高效的网上交易途径，对我国电子商务的发展以及网络经济繁荣起到极其重要的促进作用。

《电子签名法》主要规定了电子签名及其相关定义、满足法律法规规定的数据电文、可靠的电子签名和电子认证服务等。需要特别注意的是，并不是所有的电子签名都具有法律效力，只有可靠的电子签名才具有法律效力。

1. 电子签名及相关定义

电子签名，是指数据电文中以电子形式所含、所附用于识别签名人身份并表明签名人认可其中内容的数据。

数据电文，是指以电子、光学、磁或者类似手段生成、发送、接收或者储存的信息。

电子签名人，是指持有电子签名制作数据并以本人身份或者以其所代表的人的名义实施电子签名的人。

电子签名依赖方，是指基于对电子签名认证证书或者电子签名的信赖从事有关活动的人。

电子签名认证证书，是指可证实电子签名人与电子签名制作数据有联系的数据电文或者其他电子记录。

电子签名制作数据，是指在电子签名过程中使用的，将电子签名与电子签名人可靠地联

系起来的字符、编码等数据。

电子签名验证数据，是指用于验证电子签名的数据，包括代码、口令、算法或者公钥等。

2．满足法律法规规定的数据电文

能够有形地表现所载内容，并可以随时调取查用的数据电文，视为符合法律、法规要求的书面形式。

符合下列条件的数据电文，视为满足法律、法规规定的原件形式要求：

（1）能够有效地表现所载内容并可供随时调取查用。

（2）能够可靠地保证自最终形成时起，内容保持完整、未被更改。但是，在数据电文上增加背书以及数据交换、储存和显示过程中发生的形式变化不影响数据电文的完整性。

符合下列条件的数据电文，视为满足法律、法规规定的文件保存要求：

（1）能够有效地表现所载内容并可供随时调取查用。

（2）数据电文的格式与其生成、发送或者接收时的格式相同，或者格式不相同但是能够准确表现原来生成、发送或者接收的内容。

（3）能够识别数据电文的发件人、收件人以及发送、接收的时间。

数据电文有下列情形之一的，视为发件人发送：

（1）经发件人授权发送的。

（2）发件人的信息系统自动发送的。

（3）收件人按照发件人认可的方法对数据电文进行验证后结果相符的。

法律、行政法规规定或者当事人约定数据电文需要确认收讫的，应当确认收讫。发件人收到收件人的收讫确认时，数据电文视为已经收到。

3．可靠的电子签名

电子签名同时符合下列条件的，视为可靠的电子签名：

（1）电子签名制作数据用于电子签名时，属于电子签名人专有。

（2）签署时电子签名制作数据仅由电子签名人控制。

（3）签署后对电子签名的任何改动能够被发现。

（4）签署后对数据电文内容和形式的任何改动能够被发现。

可靠的电子签名与手写签名或者盖章具有同等的法律效力。

4．电子认证服务

电子签名需要第三方认证的，由依法设立的电子认证服务提供者提供认证服务。

提供电子认证服务，应当具备下列条件：

（1）具有与提供电子认证服务相适应的专业技术人员和管理人员。

（2）具有与提供电子认证服务相适应的资金和经营场所。

（3）具有符合国家安全标准的技术和设备。

（4）具有国家密码管理机构同意使用密码的证明文件。

（5）法律、行政法规规定的其他条件。

从事电子认证服务，应当向国务院信息产业主管部门提出申请，并提交相关材料。国务院信息产业主管部门接到申请后经依法审查，征求国务院商务主管部门等有关部门的意见后，予以许可的，颁发电子认证许可证书；不予许可的，应当书面通知申请人并告知理由。