(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 109918888 A
(43)申请公布日 2019.06.21

(21)申请号 201910034536.8

(22)申请日 2019.01.15

(71)申请人 如般量子科技有限公司
地址 312030 浙江省绍兴市柯桥区柯岩街道余渚村1幢

(72)发明人 富尧 钟一民 余秋炜

(74)专利代理机构 杭州君度专利代理事务所（特殊普通合伙）33240
代理人 解明铠 刘静静

(51)Int.Cl.
G06F 21/33(2013.01)
H04L 9/08(2006.01)
H04L 9/06(2006.01)
H04L 9/32(2006.01)

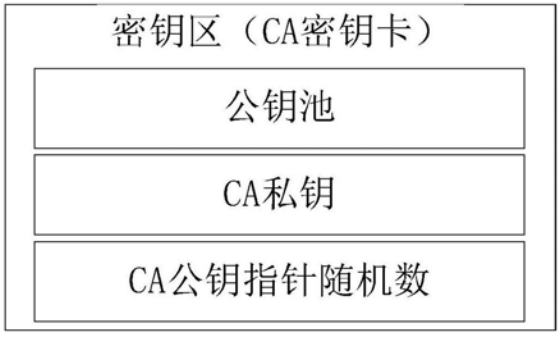
权利要求书2页 说明书9页 附图2页

(54)发明名称

基于公钥池的抗量子证书颁发方法及颁发系统

(57)摘要

本发明涉及一种基于公钥池的抗量子证书颁发方法和颁发系统，参与方包括证书授权中心和用户，各参与方均配置有密钥卡，各密钥卡内均存储有公钥池、私钥、证书授权中心的公钥指针随机数，用户的密钥卡内还存储有用户公钥指针随机数，所述抗量子证书颁发方法包括：生成抗量子证书的版本号、序列号和有效期；生成持有者名称、公钥算法和持有者公钥指针随机数；利用证书授权中心的私钥对抗量子证书进行数字签名；生成一个真随机数，利用真随机数对所述数字签名进行加密；利用证书授权中心的私钥对所述真随机数进行加密；将抗量子证书安全发送至对应用户。所述抗量子证书不会被量子计算机破解。



CN 109918888 A

1.基于公钥池的抗量子证书颁发方法，参与方包括证书授权中心和用户，各参与方均配置有密钥卡，各密钥卡内均存储有公钥池、私钥、证书授权中心的公钥指针随机数，用户的密钥卡内还存储有用户公钥指针随机数，其特征在于，所述抗量子证书颁发方法包括在所述证书授权中心进行的如下步骤：

生成抗量子证书的版本号、序列号和有效期；

生成持有者名称、公钥算法和持有者公钥指针随机数；

利用证书授权中心的私钥对抗量子证书进行数字签名；

生成一个真随机数，利用真随机数对所述数字签名进行加密；

利用证书授权中心的私钥对所述真随机数进行加密；

将抗量子证书安全发送至对应用户。

2.如权利要求1所述的基于公钥池的抗量子证书颁发方法，其特征在于，所述公钥池中存储有若干个公钥单元，每个参与方对应其中一个公钥单元，每个公钥单元包括：公钥指针随机数、公钥指针函数、公钥和公钥算法；

所述抗量子证书中还记载有证书授权中心的公钥指针随机数，所述抗量子证书颁发方法还包括在用户端进行所述抗量子证书的验证，抗量子证书验证包括如下步骤：

依据接收的抗量子证书中的持有者公钥指针随机数在公钥池中寻找对应的公钥单元，若找到对应的公钥单元，则进行下一步；

根据对应的公钥单元中的公钥指针函数对持有者公钥指针随机数进行计算，若得到的公钥指针与公钥单元的公钥指针相同，则进行下一步；

在公钥池和受信任的根证书列表中寻找接收的抗量子证书中记载的证书授权中心的公钥指针随机数，若找到，则进行下一步；

依据证书授权中心的公钥指针随机数从公钥池中取出证书授权中心的公钥；

利用证书授权中心的公钥解密得到真随机数；

利用真随机数解密得到数字签名；

利用证书授权中心的公钥解密数字签名得到抗量子证书的原文摘要，若该原文摘要与根据抗量子证书记载信息计算得到的原文摘要一致，则进行下一步；

验证抗量子证书是否在有效期内。

3.如权利要求2所述的基于公钥池的抗量子证书颁发方法，其特征在于，还包括在抗量子证书验证之前进行的抗量子证书种类鉴别步骤，该种类鉴别步骤包括在用户端进行的：

判断接收的抗量子证书中的持有者公钥指针随机数是否与证书授权中心的公钥指针随机数相同：

若不相同，则进行抗量子证书的验证过程；

若相同，则进行抗量子证书的验证过程，若验证通过，将该抗量子根证书加入受信任的根证书列表。

4.基于公钥池的抗量子证书颁发系统，参与方包括证书授权中心和用户，各参与方均配置有密钥卡，各密钥卡内均存储有公钥池、私钥、证书授权中心的公钥指针随机数，用户的密钥卡内还存储有用户公钥指针随机数，其特征在于，所述抗量子证书颁发方法包括设置在所述证书授权中心的：

第一模块，用于生成抗量子证书的版本号、序列号和有效期；

第二模块，用于生成持有者名称、公钥算法和持有者公钥指针随机数；

第三模块，用于利用证书授权中心的私钥对抗量子证书进行数字签名；

第四模块，用于生成一个真随机数，利用真随机数对所述数字签名进行加密；

第五模块，用于利用证书授权中心的私钥对所述真随机数进行加密；

第六模块，用于将抗量子证书安全发送至对应用户。

5.如权利要求4所述的基于公钥池的抗量子证书颁发系统，其特征在于，所述公钥池中存储有若干个公钥单元，每个参与方对应其中一个公钥单元，每个公钥单元包括：公钥指针随机数、公钥指针函数、公钥和公钥算法；

所述抗量子证书中还记载有证书授权中心的公钥指针随机数，所述抗量子证书颁发系统还包括设置在用户端的抗量子证书验证模块，该抗量子证书验证模块包括：

第一子模块，用于依据接收的抗量子证书中的持有者公钥指针随机数在公钥池中寻找对应的公钥单元；

第二子模块，用于根据对应的公钥单元中的公钥指针函数对持有者公钥指针随机数进行计算，并判断得到的公钥指针与公钥单元的公钥指针是否相同；

第三子模块，用于在公钥池和受信任的根证书列表中寻找接收的抗量子证书中记载的证书授权中心的公钥指针随机数；

第四子模块，用于依据证书授权中心的公钥指针随机数从公钥池中取出证书授权中心的公钥；

第五子模块，用于利用证书授权中心的公钥解密得到真随机数；

第六子模块，用于利用真随机数解密得到数字签名；

第七子模块，用于利用证书授权中心的公钥解密数字签名得到抗量子证书的原文摘要，判断该原文摘要与根据抗量子证书记载信息计算得到的原文摘要是否一致；

第八子模块，用于验证抗量子证书是否在有效期内。

6.如权利要求5所述的基于公钥池的抗量子证书颁发系统，其特征在于，还包括设置在用户端的抗量子证书种类鉴别模块，该抗量子证书种类鉴别模块用于在抗量子证书验证之前进行的抗量子证书种类鉴别，所述抗量子证书种类鉴别模块用于判断接收的抗量子证书中的持有者公钥指针随机数是否与证书授权中心的公钥指针随机数相同：

若不相同，则进行抗量子证书的验证过程；

若相同，则进行抗量子证书的验证过程，若验证通过，将该抗量子根证书加入受信任的根证书列表。

7.基于公钥池的抗量子证书颁发系统，其特征在于，参与方包括证书授权中心和用户，各参与方均配置有密钥卡，各密钥卡内均存储有公钥池、私钥、证书授权中心的公钥指针随机数，用户的密钥卡内还存储有用户公钥指针随机数；

各参与方包括存储器和处理器，存储器中存储有计算机程序，该处理器执行计算机程序时实现权利要求1～3任一项所述的基于公钥池的抗量子证书颁发方法。

基于公钥池的抗量子证书颁发方法及颁发系统

技术领域

[0001] 本发明涉及安全通信领域，尤其是一种基于公钥池的抗量子证书颁发方法及颁发系统。

背景技术

[0002] 数字签名(又称公钥数字签名、电子签名等)在理念上是一种类似写在纸上的普通的物理签名，但是使用了公钥加密领域的技术实现，用于鉴别数字信息的方法。一套数字签名通常定义两种互补的运算，一个用于签名，另一个用于验证。

[0003] 数字签名，就是只有信息的发送者才能产生的别人无法伪造的一段数字串，这段数字串同时也是对信息的发送者发送信息真实性的一个有效证明。

[0004] 数字签名的文件的完整性是很容易验证的(不需要骑缝章，骑缝签名，也不需要笔迹专家)，而且数字签名具有不可抵赖性(不可否认性)。

[0005] 简单地说，所谓数字签名就是附加在数据单元上的一些数据，或是对数据单元所作的密码变换。这种数据或变换允许数据单元的接收者用以确认数据单元的来源和数据单元的完整性并保护数据，防止被人(例如接收者)进行伪造。它是对电子形式的消息进行签名的一种方法，一个签名消息能在一个通信网络中传输。基于公钥密码体制和私钥密码体制都可以获得数字签名，主要是基于公钥密码体制的数字签名，包括普通数字签名和特殊数字签名。普通数字签名算法有RSA、ElGamal、Fiat-Shamir、Guillou-Quisquarter、Schnorr、Ong-Schnorr-Shamir数字签名算法、DSA，椭圆曲线数字签名算法和有限自动机数字签名算法等。特殊数字签名有盲签名、代理签名、群签名、不可否认签名、公平盲签名、门限签名、具有消息恢复功能的签名等，它与具体应用环境密切相关。显然，数字签名的应用涉及到法律问题，美国联邦政府基于有限域上的离散对数问题制定了自己的数字签名标准(DSS)。

[0006] 在如今的密码学领域中，主要有两种密码系统，一是对称密钥密码系统，即加密密钥和解密密钥使用同一个；另一个是公开密钥密码系统，即加密密钥和解密密钥不同，其中一个可以公开，而数字证书正好是基于非对称密码体系实现的。

[0007] 但是随着量子计算机的发展，经典非对称密钥加密算法将不再安全，无论加解密、数字签名还是密钥交换方法，量子计算机都可以通过公钥计算得到私钥，因此目前经典的数字证书将在量子时代变得不堪一击。

发明内容

[0008] 本发明提供一种基于公钥池的抗量子证书颁发方法及颁发系统，防止抗量子证书被量子计算机破解。

[0009] 基于公钥池的抗量子证书颁发方法，参与方包括证书授权中心和用户，各参与方均配置有密钥卡，各密钥卡内均存储有公钥池、私钥、证书授权中心的公钥指针随机数，用户的密钥卡内还存储有用户公钥指针随机数，所述抗量子证书颁发方法包括在所述证书授

权中心进行的如下步骤：

[0010] 生成抗量子证书的版本号、序列号和有效期；

[0011] 生成持有者名称、公钥算法和持有者公钥指针随机数；

[0012] 利用证书授权中心的私钥对抗量子证书进行数字签名；

[0013] 生成一个真随机数，利用真随机数对所述数字签名进行加密；

[0014] 利用证书授权中心的私钥对所述真随机数进行加密；

[0015] 将抗量子证书安全发送至对应用户。

[0016] 以下还提供了若干可选方式，但并不作为对上述总体方案的额外限定，仅仅是进一步的增补或优选，在没有技术或逻辑矛盾的前提下，各可选方式可单独针对上述总体方案进行组合，还可以是多个可选方式之间进行组合。

[0017] 可选地，所述公钥池中存储有若干个公钥单元，每个参与方对应其中一个公钥单元，每个公钥单元包括：公钥指针随机数、公钥指针函数、公钥和公钥算法；

[0018] 所述抗量子证书中还记载有证书授权中心的公钥指针随机数，所述抗量子证书颁发方法还包括在用户端进行所述抗量子证书的验证，抗量子证书验证包括如下步骤：

[0019] 依据接收的抗量子证书中的持有者公钥指针随机数在公钥池中寻找对应的公钥单元，若找到对应的公钥单元，则进行下一步；

[0020] 根据对应的公钥单元中的公钥指针函数对持有者公钥指针随机数进行计算，若得到的公钥指针与公钥单元的公钥指针相同，则进行下一步；

[0021] 在公钥池和受信任的根证书列表中寻找接收的抗量子证书中记载的证书授权中心的公钥指针随机数，若找到，则进行下一步；

[0022] 依据证书授权中心的公钥指针随机数从公钥池中取出证书授权中心的公钥；

[0023] 利用证书授权中心的公钥解密得到真随机数；

[0024] 利用真随机数解密得到数字签名；

[0025] 利用证书授权中心的公钥解密数字签名得到抗量子证书的原文摘要，若该原文摘要与根据抗量子证书记载信息计算得到的原文摘要一致，则进行下一步；

[0026] 验证抗量子证书是否在有效期内。

[0027] 可选地，还包括在抗量子证书验证之前进行的抗量子证书种类鉴别步骤，该种类鉴别步骤包括在用户端进行的：

[0028] 判断接收的抗量子证书中的持有者公钥指针随机数是否与证书授权中心的公钥指针随机数相同：

[0029] 若不相同，则进行抗量子证书的验证过程；

[0030] 若相同，则进行抗量子证书的验证过程，若验证通过，将该抗量子根证书加入受信任的根证书列表。

[0031] 本发明还提供了一种基于公钥池的抗量子证书颁发系统，参与方包括证书授权中心和用户，各参与方均配置有密钥卡，各密钥卡内均存储有公钥池、私钥、证书授权中心的公钥指针随机数，用户的密钥卡内还存储有用户公钥指针随机数，所述抗量子证书颁发方法包括设置在所述证书授权中心的：

[0032] 第一模块，用于生成抗量子证书的版本号、序列号和有效期；

[0033] 第二模块，用于生成持有者名称、公钥算法和持有者公钥指针随机数；

[0034] 第三模块，用于利用证书授权中心的私钥对抗量子证书进行数字签名；

[0035] 第四模块，用于生成一个真随机数，利用真随机数对所述数字签名进行加密；

[0036] 第五模块，用于利用证书授权中心的私钥对所述真随机数进行加密；

[0037] 第六模块，用于将抗量子证书安全发送至对应用户。

[0038] 以下还提供了若干可选方式，但并不作为对上述总体方案的额外限定，仅仅是进一步的增补或优选，在没有技术或逻辑矛盾的前提下，各可选方式可单独针对上述总体方案进行组合，还可以是多个可选方式之间进行组合。

[0039] 可选地，所述公钥池中存储有若干个公钥单元，每个参与方对应其中一个公钥单元，每个公钥单元包括：公钥指针随机数、公钥指针函数、公钥和公钥算法；

[0040] 所述抗量子证书中还记载有证书授权中心的公钥指针随机数，所述抗量子证书颁发系统还包括设置在用户端的抗量子证书验证模块，该抗量子证书验证模块包括：

[0041] 第一子模块，用于依据接收的抗量子证书中的持有者公钥指针随机数在公钥池中寻找对应的公钥单元；

[0042] 第二子模块，用于根据对应的公钥单元中的公钥指针函数对持有者公钥指针随机数进行计算，并判断得到的公钥指针与公钥单元的公钥指针是否相同；

[0043] 第三子模块，用于在公钥池和受信任的根证书列表中寻找接收的抗量子证书中记载的证书授权中心的公钥指针随机数；

[0044] 第四子模块，用于依据证书授权中心的公钥指针随机数从公钥池中取出证书授权中心的公钥；

[0045] 第五子模块，用于利用证书授权中心的公钥解密得到真随机数；

[0046] 第六子模块，用于利用真随机数解密得到数字签名；

[0047] 第七子模块，用于利用证书授权中心的公钥解密数字签名得到抗量子证书的原文摘要，判断该原文摘要与根据抗量子证书记载信息计算得到的原文摘要是否一致；

[0048] 第八子模块，用于验证抗量子证书是否在有效期内。

[0049] 可选地，还包括设置在用户端的抗量子证书种类鉴别模块，该抗量子证书种类鉴别模块用于在抗量子证书验证之前进行的抗量子证书种类鉴别，所述抗量子证书种类鉴别模块用于判断接收的抗量子证书中的持有者公钥指针随机数是否与证书授权中心的公钥指针随机数相同：

[0050] 若不相同，则进行抗量子证书的验证过程；

[0051] 若相同，则进行抗量子证书的验证过程，若验证通过，将该抗量子根证书加入受信任的根证书列表。

[0052] 本发明还提供了基于公钥池的抗量子证书颁发系统，参与方包括证书授权中心和用户，各参与方均配置有密钥卡，各密钥卡内均存储有公钥池、私钥、证书授权中心的公钥指针随机数，用户的密钥卡内还存储有用户公钥指针随机数，

[0053] 各参与方包括存储器和处理器，存储器中存储有计算机程序，该处理器执行计算机程序时实现权利要求1～3任一项所述的基于公钥池的抗量子证书颁发方法。

[0054] 本发明中，使用的密钥卡是独立的硬件隔离设备，公钥、私钥和真随机数等其他相关参数均在CA内(即证书授权中心)生成，密钥分发后在密钥卡中存储，用户使用时被恶意软件或恶意操作窃取密钥的可能性大大降低，也不会被量子计算机获取并破解。本发明的

数字证书体系所使用的所有非对称算法中的公钥以及相关算法参数均不参与网络传输，所以通信双方的公私钥被窃取破解的可能性较低。本发明中使用公钥指针随机数代替了公钥，增加了证书验证的准确度，也保证了公钥的安全。另外，数字证书中基于公私钥的数字签名被随机数进一步加密，形成加密的数字签名。即使在量子计算机存在的情况下，也难以被推导出私钥。综上所述，本发明保障了数字证书系统的公私钥及证书的安全。

附图说明

[0055] 图1为本发明的CA密钥卡密钥区的分布图；

[0056] 图2为本发明的用户密钥卡密钥区的分布图；

[0057] 图3为本发明的数字证书的结构图。

具体实施方式

[0058] 下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅仅是本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都属于本发明保护的范围。

[0059] 为了更好地描述和说明本申请的实施例，可参考一幅或多幅附图，但用于描述附图的附加细节或示例不应当被认为是对本申请的发明创造、目前所描述的实施例或优选方式中任何一者的范围的限制。

[0060] 应该理解的是，除非本文中有明确的说明，各步骤的执行并没有严格的顺序限制，这些步骤可以以其它的顺序执行。而且，至少一部分步骤可以包括多个子步骤或者多个阶段，这些子步骤或者阶段并不必然是在同一时刻执行完成，而是可以在不同的时刻执行，这些子步骤或者阶段的执行顺序也不必然是依次进行，而是可以与其它步骤或者其它步骤的子步骤或者阶段的至少一部分轮流或者交替地执行。

[0061] 本发明实现一种基于公钥池的抗量子计算的数字证书体系。本发明所实现的场景为一个拥有同一公钥池成员组成的群组。群组中的CA拥有CA密钥卡，而其他成员均拥有用户密钥卡。本发明中的密钥卡不仅可以存储大量的数据，还具有处理信息的能力。本发明中，所有密钥卡都存在相应需求的算法。

[0062] 密钥卡的描述可见申请号为“201610843210.6”的专利。当为移动终端时，密钥卡优选为密钥SD卡；当为固定终端时，密钥卡优选为密钥USBkey或主机密钥板卡。

[0063] 与申请号为“201610843210.6”的专利相比，密钥卡的颁发机制有所不同。本专利的密钥卡颁发方为密钥卡的主管方，一般为群组的管理部门，例如某企业或事业单位的管理部门；密钥卡被颁发方为密钥卡的主管方所管理的成员，一般为某企业或事业单位的各级员工。用户端首先到密钥卡的主管方申请开户。当用户端进行注册登记获批后，将得到密钥卡(具有唯一的密钥卡ID)。密钥卡存储了客户注册登记信息。密钥卡中的用户侧密钥都下载自CA服务站，且对同一个密钥卡的主管方来说，其颁发的每个密钥卡中存储的密钥池是完全一致的。优选为，密钥卡中存储的密钥池大小可以是1G、2G、4G、8G、16G、32G、64G、128G、256G、512G、1024G、2048G、4096G等等。

[0064] 密钥卡从智能卡技术上发展而来，是结合了真随机数发生器(优选为量子随机数

发生器)、密码学技术、硬件安全隔离技术的身份认证和加解密产品。密钥卡的内嵌芯片和操作系统可以提供密钥的安全存储和密码算法等功能。由于其具有独立的数据处理能力和良好的安全性,密钥卡成为私钥和密钥池的安全载体。每一个密钥卡都有硬件PIN码保护,PIN码和硬件构成了用户使用密钥卡的两个必要因素。即所谓“双因子认证”,用户只有同时取得保存了相关认证信息的密钥卡和用户PIN码,才可以登录系统。即使用户的PIN码被泄露,只要用户持有的密钥卡不被盗取,合法用户的身份就不会被仿冒;如果用户的密钥卡遗失,拾到者由于不知道用户PIN码,也无法仿冒合法用户的身份。

[0065] 基于公钥池的抗量子证书颁发方法,参与方包括证书授权中心和用户,各参与方均配置有密钥卡,各密钥卡内均存储有公钥池、私钥、证书授权中心的公钥指针随机数,用户的密钥卡内还存储有用户公钥指针随机数,所述抗量子证书颁发方法包括在所述证书授权中心进行的如下步骤:

[0066] 生成抗量子证书的版本号、序列号和有效期;

[0067] 生成持有者名称、公钥算法和持有者公钥指针随机数;

[0068] 利用证书授权中心的私钥对抗量子证书进行数字签名;

[0069] 生成一个真随机数,利用真随机数对所述数字签名进行加密;

[0070] 利用证书授权中心的私钥对所述真随机数进行加密;

[0071] 将抗量子证书安全发送至对应用户。

[0072] 在其中一个实施例中,所述公钥池中存储有若干个公钥单元,每个参与方对应其中一个公钥单元,每个公钥单元包括:公钥指针随机数、公钥指针函数、公钥和公钥算法;

[0073] 所述抗量子证书中还记载有证书授权中心的公钥指针随机数,所述抗量子证书颁发方法还包括在用户端进行所述抗量子证书的验证,抗量子证书验证包括如下步骤:

[0074] 依据接收的抗量子证书中的持有者公钥指针随机数在公钥池中寻找对应的公钥单元,若找到对应的公钥单元,则进行下一步;

[0075] 根据对应的公钥单元中的公钥指针函数对持有者公钥指针随机数进行计算,若得到的公钥指针与公钥单元的公钥指针相同,则进行下一步;

[0076] 在公钥池和受信任的根证书列表中寻找接收的抗量子证书中记载的证书授权中心的公钥指针随机数,若找到,则进行下一步;

[0077] 依据证书授权中心的公钥指针随机数从公钥池中取出证书授权中心的公钥;

[0078] 利用证书授权中心的公钥解密得到真随机数;

[0079] 利用真随机数解密得到数字签名;

[0080] 利用证书授权中心的公钥解密数字签名得到抗量子证书的原文摘要,若该原文摘要与根据抗量子证书记载信息计算得到的原文摘要一致,则进行下一步;

[0081] 验证抗量子证书是否在有效期内。

[0082] 在其中一个实施例中,还包括在抗量子证书验证之前进行的抗量子证书种类鉴别步骤,该种类鉴别步骤包括在用户端进行的:

[0083] 判断接收的抗量子证书中的持有者公钥指针随机数是否与证书授权中心的公钥指针随机数相同:

[0084] 若不相同,则进行抗量子证书的验证过程;

[0085] 若相同,则进行抗量子证书的验证过程,若验证通过,将该抗量子根证书加入受信

任的根证书列表。

[0086] 结合图示，对抗量子证书颁发过程详述如下：

[0087] 1.PK单元

[0088] 公钥池是由n个PK单元组成，PK单元即公钥单元，n的个数为群组内所有成员的个数，包括CA(即证书授权中心)和其他用户。PK单元是由PKR、FPOS信息、PK和PK算法四个部分组成，如表1所示。其中PKR为公钥指针随机数(即公钥的存储位置参数)，FPOS为公钥指针函数，PK为公钥。

[0089] 表1

[0090]

PKR	FPOS信息	PK	PK算法	

[0091] 其中FPOS信息包括FPOS算法ID和内部参数，FPOS信息如表2所示。

[0092] 表2

[0093]

FPOS算法ID	内部参数

[0094] FPOS的算法可以有多种计算方式，例如，FPOS(PKR)＝(a*PKR+b)％n。其中％为取模运算；PKR为输入变量；n(PK单元的个数)为外部参数；a、b为内部参数。或FPOS(PKR)＝(PKR^c)*d％n；其中^为乘方运算，％为取模运算；PKR为输入变量；n(PK单元的个数)为外部参数；c、d为内部参数。上述两种算法仅作为参考，本发明并不受限于该两种计算方式。

[0095] PK算法指具体的公钥算法(非对称密码算法)，可以有多种公钥算法，例如RSA/DSA/ECC等。

[0096] 2.密钥卡

[0097] 本发明中密钥卡分为两种密钥卡，一种是用于CA系统的CA密钥卡，还有一种是用户密钥卡。CA密钥卡包括公钥池、CA私钥和CA公钥指针随机数；用户密钥卡包括公钥池、用户私钥、用户公钥指针随机数和CA公钥指针随机数。CA密钥卡的公钥池和用户密钥卡中的密钥池相同。密钥池的结构分别如图1和图2。

[0098] CA服务器在颁发密钥卡之前会创建一个至少有n*sp大小的公钥池文件和一个至少有n*ss大小的私钥池文件。sp为1个PK单元的大小，ss为1个SK的大小，SK为私钥。CA服务器将生成n个PK/SK对。CA服务器可以提供多种非对称算法，生成每个PK/SK对时，CA服务器会选择一种非对称算法。CA服务器生成PKR，PKR为真随机数，优选为量子随机数。CA服务器随机生成FPOS算法ID和FPOS内部参数，计算得到PKPOS，PKPOS为公钥位置指针。CA服务器对公钥池文件PKPOS所在位置进行赋值，即写入PKR、FPOS信息、PK、PK算法。CA服务器对私钥池文件PKPOS所在位置进行赋值，即写入SK。假如PKPOS所在位置已经被赋值，则更换PKR、FPOS算法ID、FPOS内部参数中的1个或多个，重新执行本流程，直到找到未被赋值的位置。

[0099] CA服务器从公钥池文件随机选取一个PK单元，将该PK单元的公钥作为CA公钥，即PK_{CA}，并将该PK单元的PKR作为CA公钥指针随机数，即PKR_{CA}。同时取出在私钥池文件同位置的私钥，即SK_{CA}。CA的公钥/私钥对可以是1个或多个，如为多个，则多次执行前述流程。CA服务器通过安全发送方式把公钥池文件、私钥和CA公钥指针随机数发送给CA密钥卡，CA密钥卡将相关密钥存储到CA密钥卡内部。CA通过安全发送方式把PKR、PKR_{CA}、PKR对应的私钥、公钥池文件发送给用户密钥卡，用户密钥卡将相关密钥存储到用户密钥卡内部。

[0100] 安全发送的方法可能是：

[0101] (1)用户密钥卡通过USB或网络接口等，直接连接至CA密钥卡，并由CA密钥卡传输信息；

[0102] (2)用户密钥卡和CA密钥卡均通过USB或网络接口等，连接到CA认可的某台安全主机，由主机中转信息；

[0103] (3)CA密钥卡与用户密钥卡分配有预共享密钥，CA密钥卡用预共享密钥对信息进行加密，网络传输至用户密钥卡后被用户密钥卡解密；

[0104] (4)CA密钥卡与用户密钥卡之间有量子密钥分发网络，CA密钥卡用量子密钥分发的密钥对信息进行加密，传输至用户密钥卡后被用户密钥卡解密；

[0105] (5)通过安全存储介质，将信息直接拷贝到用户密钥卡内；

[0106] (6)其他未提及的安全发送手段。

[0107] 3.数字证书生成

[0108] 数字证书的结构如图3所示。

[0109] 数字证书包括证书信息、颁发者信息、持有者信息和颁发者数字签名四个部分。其中证书信息包括版本号、序列号和有效期；颁发者信息为颁发者名称；持有者信息包括持有者名称、公钥算法和持有者的公钥指针随机数；颁发者数字签名包括签名算法和加密的CA数字签名。其中CA数字签名的加密如下所述：设数字证书的证书信息、颁发者信息和持有者信息为M，M的摘要为MD，CA服务器利用私钥SK_{CA}签名MD得到签名MS＝{MD}SK_{CA}。CA服务器产生一个真随机数R，利用R对签名MS加密得到{MS}R。CA服务器再利用私钥SK_{CA}加密R得到{R}SK_{CA}。最终加密签名为PKR_{CA}||{MS}R||{R}SK_{CA}。

[0110] 特别地，抗量子计算根证书是CA自签名证书：颁发者即为持有者，即CA服务器。

[0111] 用户在使用普通数字证书前，一般已事先下载安装了CA根证书，验证了其有效性，并设置为受信任证书。CA根证书用于验证其他数字证书。

[0112] 4.数字证书验证

[0113] 4.1普通数字证书的验证

[0114] 首先用户先根据持有者信息中的持有者公钥指针随机数PKR去密钥卡公钥池中进行匹配，是否能找到具有相同PKR的PK单元，如果没有找到，则验证失败，流程结束。如果找到，再根据匹配的PK单元中的FPOS信息对该PKR进行计算，得到的值与该PK单元的PKPOS进行比较。如果相同，则PKR验证通过。然后用户根据加密的CA数字签名中的CA公钥指针随机数PKR_{CA}，验证其是否位于密钥卡中的CA公钥指针随机数区域；如果不是，则查找PKR_{CA}是否位于受信任的根证书列表中的某个根证书内；如果仍没有找到PKR_{CA}，则验证失败，流程结束。如找到PKR_{CA}，则从密钥卡公钥池中取出CA公钥PK_{CA}。用户利用PK_{CA}将数字证书的颁发者数字签名中的{R}SK_{CA}解密得到R。用户利用R解密{MS}R得到MS，用PK_{CA}解密MS得到MD。用户取出数字证书的证书信息、颁发者信息和持有者信息为M’，对M’进行摘要计算得到MD’。对比MD和MD’，如相等则说明证书的数字签名合法，即该证书确实来自CA。最后验证证书是否位于有效期内。

[0115] 4.2根证书的验证

[0116] 如用户验证某数字证书时，发现该证书的颁发者即为持有者，则进入根证书的验证流程。

[0117] 根证书的验证类似上述的用户证书验证。具体流程如下：

[0118] 首先用户先根据根证书中的公钥指针随机数去密钥卡中的CA公钥指针随机数区域进行匹配，是否能找到具有相同的PKR_{CA}值。如不存在相等的PKR_{CA}值，则执行4.1的流程，如果流程执行成功，则说明该证书为合法根证书，可存储于根证书集合中；如存在相等的PKR值，则继续下文流程。用户根据匹配的PK单元中的FPOS信息对该PKR_{CA}进行计算，得到的值与该PK单元的PKPOS进行比较。如果相同，则PKR_{CA}验证通过。然后用户根据PKR_{CA}，从密钥卡公钥池中取出CA公钥PK_{CA}。用户利用PK_{CA}将数字证书的颁发者数字签名中的$\{R\}SK_{CA}$解密得到R。用户利用R解密{MS}R得到MS，用PK_{CA}解密MS得到MD。用户取出数字证书的证书信息、颁发者信息和持有者信息为M'，对M'进行摘要计算得到MD'。对比MD和MD'，如相等则说明证书的数字签名合法。最后验证证书是否位于有效期内。

[0119] 在其中一个实施例中，提供一种基于公钥池的抗量子证书颁发系统，参与方包括证书授权中心和用户，各参与方均配置有密钥卡，各密钥卡内均存储有公钥池、私钥、证书授权中心的公钥指针随机数，用户的密钥卡内还存储有用户公钥指针随机数，所述抗量子证书颁发方法包括设置在所述证书授权中心的：

[0120] 第一模块，用于生成抗量子证书的版本号、序列号和有效期；

[0121] 第二模块，用于生成持有者名称、公钥算法和持有者公钥指针随机数；

[0122] 第三模块，用于利用证书授权中心的私钥对抗量子证书进行数字签名；

[0123] 第四模块，用于生成一个真随机数，利用真随机数对所述数字签名进行加密；

[0124] 第五模块，用于利用证书授权中心的私钥对所述真随机数进行加密；

[0125] 第六模块，用于将抗量子证书安全发送至对应用户。

[0126] 在其中一个实施例中，所述公钥池中存储有若干个公钥单元，每个参与方对应其中一个公钥单元，每个公钥单元包括：公钥指针随机数、公钥指针函数、公钥和公钥算法；

[0127] 所述抗量子证书中还记载有证书授权中心的公钥指针随机数，所述抗量子证书颁发系统还包括设置在用户端的抗量子证书验证模块，该抗量子证书验证模块包括：

[0128] 第一子模块，用于依据接收的抗量子证书中的持有者公钥指针随机数在公钥池中寻找对应的公钥单元；

[0129] 第二子模块，用于根据对应的公钥单元中的公钥指针函数对持有者公钥指针随机数进行计算，并判断得到的公钥指针与公钥单元的公钥指针是否相同；

[0130] 第三子模块，用于在公钥池和受信任的根证书列表中寻找接收的抗量子证书中记载的证书授权中心的公钥指针随机数；

[0131] 第四子模块，用于依据证书授权中心的公钥指针随机数从公钥池中取出证书授权中心的公钥；

[0132] 第五子模块，用于利用证书授权中心的公钥解密得到真随机数；

[0133] 第六子模块，用于利用真随机数解密得到数字签名；

[0134] 第七子模块，用于利用证书授权中心的公钥解密数字签名得到抗量子证书的原文摘要，判断该原文摘要与根据抗量子证书记载信息计算得到的原文摘要是否一致；

[0135] 第八子模块，用于验证抗量子证书是否在有效期内。

[0136] 在其中一个实施例中，抗量子证书颁发系统还包括设置在用户端的抗量子证书种类鉴别模块，该抗量子证书种类鉴别模块用于在抗量子证书验证之前进行的抗量子证书种

类鉴别，所述抗量子证书种类鉴别模块用于判断接收的抗量子证书中的持有者公钥指针随机数是否与证书授权中心的公钥指针随机数相同：

[0137] 若不相同，则进行抗量子证书的验证过程；

[0138] 若相同，则进行抗量子证书的验证过程，若验证通过，将该抗量子根证书加入受信任的根证书列表。

[0139] 关于抗量子证书颁发系统的具体限定可以参见上文中对于抗量子证书颁发系统的限定，在此不再赘述。上述各个模块可全部或部分通过软件、硬件及其组合来实现。上述各模块可以硬件形式内嵌于或独立于计算机设备中的处理器中，也可以以软件形式存储于计算机设备中的存储器中，以便于处理器调用执行以上各个模块对应的操作。

[0140] 在一个实施例中，提供了一种计算机设备，即一种抗量子证书颁发系统，该计算机设备可以是终端，其内部结构可以包括通过系统总线连接的处理器、存储器、网络接口、显示屏和输入装置。其中，该计算机设备的处理器用于提供计算和控制能力。该计算机设备的存储器包括非易失性存储介质、内存储器。该非易失性存储介质存储有操作系统和计算机程序。该内存储器为非易失性存储介质中的操作系统和计算机程序的运行提供环境。该计算机设备的网络接口用于与外部的终端通过网络连接通信。该计算机程序被处理器执行时以实现抗量子证书颁发系统。该计算机设备的显示屏可以是液晶显示屏或者电子墨水显示屏，该计算机设备的输入装置可以是显示屏上覆盖的触摸层，也可以是计算机设备外壳上设置的按键、轨迹球或触控板，还可以是外接的键盘、触控板或鼠标等。

[0141] 在其中一个实施例中，还提供基于公钥池的抗量子证书颁发系统，参与方包括证书授权中心和用户，各参与方均配置有密钥卡，各密钥卡内均存储有公钥池、私钥、证书授权中心的公钥指针随机数，用户的密钥卡内还存储有用户公钥指针随机数，

[0142] 各参与方包括存储器和处理器，存储器中存储有计算机程序，该处理器执行计算机程序时实现所述的基于公钥池的抗量子证书颁发方法。

[0143] 以上所述实施例的各技术特征可以进行任意的组合，为使描述简洁，未对上述实施例中的各个技术特征所有可能的组合都进行描述，然而，只要这些技术特征的组合不存在矛盾，都应当认为是本说明书记载的范围。

[0144] 以上所述实施例仅表达了本发明的几种实施方式，其描述较为具体和详细，但并不能因此而理解为对发明范围的限制。应当指出的是，对于本领域的普通技术人员来说，在不脱离本发明构思的前提下，还可以做出若干变形和改进，这些都属于本发明的保护范围。因此，本发明的保护范围应以所附权利要求为准。

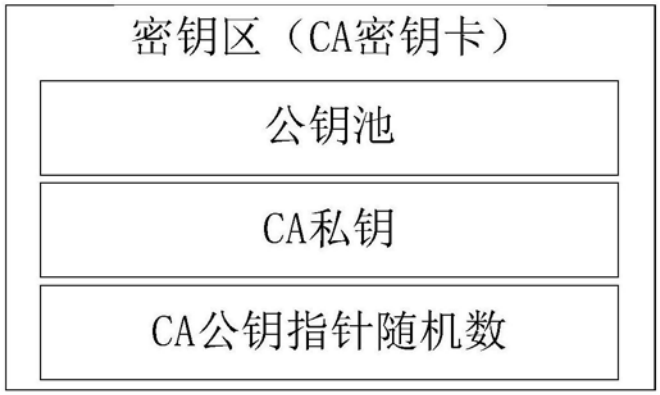

密钥区（CA密钥卡）
公钥池
CA私钥
CA公钥指针随机数

图1

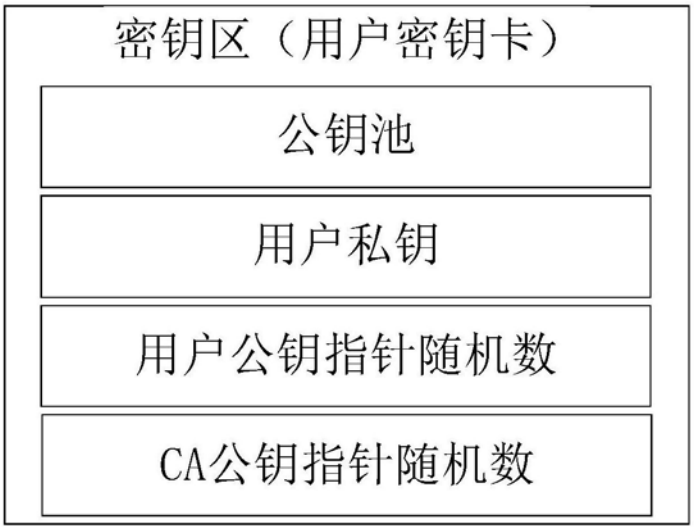

密钥区（用户密钥卡）
公钥池
用户私钥
用户公钥指针随机数
CA公钥指针随机数

图2

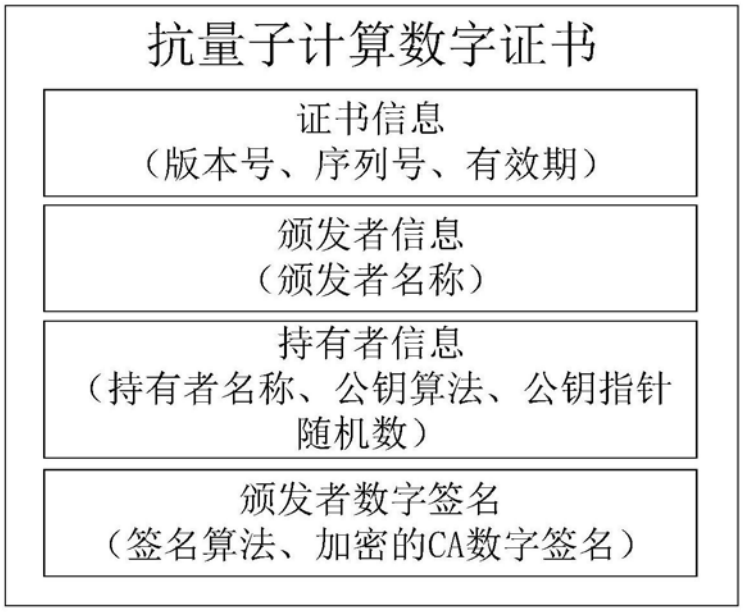

抗量子计算数字证书
证书信息
（版本号、序列号、有效期）
颁发者信息
（颁发者名称）
持有者信息
（持有者名称、公钥算法、公钥指针
随机数）
颁发者数字签名
（签名算法、加密的CA数字签名）

图3