(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 111211910 B
(45)授权公告日 2023.04.14

(21)申请号 201911395270.6
(22)申请日 2019.12.30
(65)同一申请的已公布的文献号
申请公布号 CN 111211910 A
(43)申请公布日 2020.05.29
(73)专利权人 南京如般量子科技有限公司
地址 211100 江苏省南京市江宁区麒麟高新技术产业开发区
专利权人 如般量子科技有限公司
(72)发明人 富尧 钟一民 余秋炜 刘骄
(74)专利代理机构 南京睿之博知识产权代理有限公司 32296
专利代理师 刘菊兰
(51)Int.Cl.
H04L 9/32(2006.01)
H04L 9/30(2006.01)
H04L 9/08(2006.01)
审查员 朱华慧

权利要求书2页 说明书7页 附图2页

(54)发明名称

基于秘密共享公钥池的抗量子计算CA及证书颁发系统及其颁发和验证方法

(57)摘要

本发明公开了一种基于秘密共享公钥池的抗量子计算CA及证书颁发系统及其颁发和验证方法，系统包括位于同一群组内拥有同一公钥池的CA服务器和用户，公钥池存有若干公钥单元，各个公钥单元包括用于表征用户公钥信息的公钥单元指针随机数、公钥指针函数、用户公钥秘密碎片一和公钥算法，用户密钥卡内还存有CA公钥、用户公钥秘密碎片二、公钥单元指针随机数等。本发明使用公钥单元指针随机数和用户公钥秘密碎片代替了公钥，使得数字证书中公钥不公开，因此量子计算机无法通过公钥去破解相应的私钥，且对数字证书中仅需要对敌方无法获知的证书实际内容进行签名，减轻计算压力，同时提高了数字证书的抗量子计算安全性与可靠性。

CN 111211910 B

1.一种基于秘密共享公钥池的抗量子计算CA及证书颁发方法,应用于基于秘密共享公钥池的抗量子计算CA及证书颁发系统,所述系统包括位于同一群组内的CA服务器和用户,CA服务器和各用户均配置内部存有相同公钥池和各自公私钥对的密钥卡,由CA服务器颁发密钥卡和数字证书,CA服务器对每个用户公钥以秘密共享方式得到用户公钥秘密碎片一和用户公钥秘密碎片二;

所述公钥池存有与群组内用户数量对应的公钥单元,各个公钥单元包括用于表征用户公钥信息的公钥单元指针随机数、公钥指针函数、用户公钥秘密碎片一和公钥算法;

所述用户密钥卡内还存有CA公钥、用户公钥秘密碎片二、公钥单元指针随机数;

所述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;

当数字证书的颁发者和持有者均为CA服务器时,CA服务器自签名生成抗量子证书作为CA根证书,持有者信息包括持有者名称、持有者公钥算法和CA公钥的哈希值;当数字证书的颁发者和持有者不相同时,CA服务器生成的抗量子证书作为普通数字证书,持有者信息包括持有者名称、持有者公钥算法、公钥单元指针随机数和公钥秘密碎片二;

所述公钥指针函数包括公钥指针函数算法ID和内部参数,以公钥单元指针随机数为输入量计算获得公钥单元的位置指针值;

数字证书颁发步骤为:

生成证书信息,包括版本号、序列号和有效期;

生成颁发者信息,包括颁发者名称;

生成持有者信息,包括持有者名称、持有者公钥算法、持有者的公钥单元指针随机数和持有者公钥经过(2,2)秘密共享后的持有者的公钥秘密碎片二;

生成CA数字签名,CA服务器在进行数字签名之前通过持有者的公钥单元指针随机数找到对应的公钥秘密碎片一,结合持有者公开的持有者公钥秘密碎片二进行秘密恢复计算得到持有者公钥,并得到实际持有者信息,实际持有者信息包括持有者名称、持有者公钥算法、持有者的公钥单元指针随机数、持有者的公钥;

将证书信息、颁发者信息和实际持有者信息作为证书实际内容,利用CA私钥对证书实际内容行数字签名计算,得到数字签名;

将签名后的抗量子证书发送给对应用户。

2.一种基于秘密共享公钥池的抗量子计算CA及证书验证方法,应用于基于秘密共享公钥池的抗量子计算CA及证书颁发系统,所述系统包括位于同一群组内的CA服务器和用户,CA服务器和各用户均配置内部存有相同公钥池和各自公私钥对的密钥卡,由CA服务器颁发密钥卡和数字证书,CA服务器对每个用户公钥以秘密共享方式得到用户公钥秘密碎片一和用户公钥秘密碎片二;

所述公钥池存有与群组内用户数量对应的公钥单元,各个公钥单元包括用于表征用户公钥信息的公钥单元指针随机数、公钥指针函数、用户公钥秘密碎片一和公钥算法;

所述用户密钥卡内还存有CA公钥、用户公钥秘密碎片二、公钥单元指针随机数;

所述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;

当数字证书的颁发者和持有者均为CA服务器时,CA服务器自签名生成抗量子证书作为CA根证书,持有者信息包括持有者名称、持有者公钥算法和CA公钥的哈希值;当数字证书的颁发者和持有者不相同时,CA服务器生成的抗量子证书作为普通数字证书,持有者信息包

括持有者名称、持有者公钥算法、公钥单元指针随机数和公钥秘密碎片二；

所述公钥指针函数包括公钥指针函数算法ID和内部参数，以公钥单元指针随机数为输入量计算获得公钥单元的位置指针值；

CA根证书验证的方法为：

用户取出存储在密钥卡内部的CA公钥，将对CA公钥进行哈希运算得到的哈希值与数字证书中的哈希值进行对比，如果相同进入下一步，反之流程结束；

用户采用CA公钥对根证书中的颁发者数字签名进行验证，验证通过进入下一步，反之流程结束；

用户检查数字证书的有效期，如果在有效期内，则根证书验证成功，存储于根证书集合中，反之根证书认证失败。

3.根据权利要求2所述的基于秘密共享公钥池的抗量子计算CA及证书验证方法，其特征在于，抗量子数字证书验证步骤为：

用户验证抗量子数字证书的持有者是否为颁发者CA服务器，如是，则进入CA根证书的验证流程；如否，则进入下一步普通数字证书验证流程；

在进行数字签名验证之前，用户根据公钥单元指针随机数在公钥池中寻找到匹配的公钥单元；

用户取出匹配的公钥单元中的秘密碎片一，结合数字证书中对应的秘密碎片二进行秘密恢复计算得到持有者公钥，并得到实际持有者信息，将证书信息、颁发者信息和实际持有者信息作为证书实际内容；

用户采用CA公钥并利用证书实际内容对数字证书中的颁发者数字签名进行验证，验证通过进入下一步，反之流程结束；

用户检查数字证书的有效期，如果在有效期内，则数字证书验证成功，反之，数字证书验证失败。

4.根据权利要求3所述的基于秘密共享公钥池的抗量子计算CA及证书验证方法，其特征在于：用户寻找到匹配的公钥单元步骤为：用户根据公钥单元指针随机数在公钥池中寻找具有相同公钥单元指针随机数的公钥单元，如未找到，则验证失败，流程结束；如果找到，再根据匹配的公钥单元中的公钥指针函数对该公钥单元指针随机数进行计算，计算得到公钥单元的位置指针值与该公钥单元的位置指针进行比较；如果相同，则验证通过，该单元为匹配的公钥单元。

基于秘密共享公钥池的抗量子计算CA及证书颁发系统及其颁发和验证方法

技术领域

[0001] 本发明涉及非对称密码体系和数字证书体系技术领域,尤其涉及一种基于秘密共享公钥池的抗量子计算CA及证书颁发系统及其颁发和验证方法。

背景技术

[0002] 数字签名,又称公钥数字签名、电子签名等,是一种使用公钥加密技术、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。数字签名就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。

[0003] 一般来说,所谓数字签名就是附加在数据单元上的一些数据,或是对数据单元所做的密码变换。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。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)。

[0004] 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。而数字证书是基于非对称密码体系实现的。

[0005] 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。

[0006] 为解决上述抗量子计算的问题,同时减少数字证书的计算量、减轻密钥卡的负担,需要对现有的数字证书的颁发系统和方法进行改进降低了证书颁发的效率以及证书验证的效率。

发明内容

[0007] 发明目的:针对现有技术中的缺陷,本发明公开了一种基于秘密共享公钥池的抗量子计算CA及证书颁发系统及其颁发和验证方法,通过对用户公钥进行秘密共享的方式,在不影响密钥生成效率的前提下,使数字证书具有了抗量子计算的安全性与可靠性。

[0008] 技术方案:为实现上述技术目的,本发明采用了如下技术方案:

[0009] 一种基于秘密共享公钥池的抗量子计算CA及证书颁发系统,其特征在于:包括位于同一群组内的CA服务器和用户,CA服务器和各用户均配置内部存有相同公钥池和各自公

私钥对的密钥卡，由CA服务器颁发密钥卡和数字证书，CA服务器对每个用户公钥以秘密共享方式得到用户公钥秘密碎片一和用户公钥秘密碎片二；

[0010] 所述公钥池存有与群组内用户数量对应的公钥单元，各个公钥单元包括用于表征用户公钥信息的公钥单元指针随机数、公钥指针函数、用户公钥秘密碎片一和公钥算法；

[0011] 所述用户密钥卡内还存有CA公钥、用户公钥秘密碎片二、公钥单元指针随机数；

[0012] 所述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。

[0013] 优选地，当数字证书的颁发者和持有者均为CA服务器时，CA服务器自签名生成抗量子证书作为CA根证书，持有者信息包括持有者名称、持有者公钥算法和CA公钥的哈希值；当数字证书的颁发者和持有者不相同时，CA服务器生成的抗量子证书作为普通数字证书，持有者信息包括持有者名称、持有者公钥算法、公钥单元指针随机数和公钥秘密碎片二。

[0014] 优选地，所述公钥指针函数包括公钥指针函数算法ID和内部参数，以公钥单元指针随机数为输入量计算获得公钥单元的位置指针值。

[0015] 一种基于秘密共享公钥池的抗量子计算CA及证书颁发方法，其特征在于，数字证书颁发步骤为：

[0016] 生成证书信息，包括版本号、序列号和有效期；

[0017] 生成颁发者信息，包括颁发者名称；

[0018] 生成持有者信息，包括持有者名称、持有者公钥算法、持有者的公钥单元指针随机数和持有者公钥经过(2,2)秘密共享后的持有者的公钥秘密碎片二；

[0019] 生成CA数字签名，CA服务器在进行数字签名之前通过持有者的公钥单元指针随机数找到对应的公钥秘密碎片一，结合持有者公开的持有者公钥秘密碎片二进行秘密恢复计算得到持有者公钥，并得到实际持有者信息，实际持有者信息包括持有者名称、持有者公钥算法、持有者的公钥单元指针随机数、持有者的公钥；

[0020] 将证书信息、颁发者信息和实际持有者信息作为证书实际内容，利用CA私钥对证书实际内容行数字签名计算，得到数字签名；

[0021] 将签名后的抗量子证书发送给对应用户。

[0022] 一种基于秘密共享公钥池的抗量子计算CA及证书验证方法，其特征在于，所述CA根证书验证的方法为：

[0023] 用户取出存储在密钥卡内部的CA公钥，将对CA公钥进行哈希运算得到的哈希值与数字证书中的哈希值进行对比，如果相同进入下一步，反之流程结束；

[0024] 用户采用CA公钥对根证书中的颁发者数字签名进行验证，验证通过进入下一步，反之流程结束；

[0025] 用户检查数字证书的有效期，如果在有效期内，则根证书验证成功，存储于根证书集合中，反之根证书认证失败。

[0026] 一种基于秘密共享公钥池的抗量子计算CA及证书验证方法，其特征在于，抗量子数字证书验证步骤为：

[0027] 用户验证抗量子数字证书的持有者是否为颁发者CA服务器，如是，则进入CA根证书的验证流程；如否，则进入下一步普通数字证书验证流程；

[0028] 在进行数字签名验证之前，用户根据证书中的公钥单元指针随机数在公钥池中寻找到匹配的公钥单元；

[0029] 用户取出匹配的公钥单元中的秘密碎片一，结合数字证书中对应的秘密碎片二进行秘密恢复计算得到持有者公钥，并得到实际持有者信息，将证书信息、颁发者信息和实际持有者信息作为证书实际内容；

[0030] 用户采用CA公钥并利用证书实际内容对数字证书中的颁发者数字签名进行验证，验证通过进入下一步，反之流程结束；

[0031] 用户检查数字证书的有效期，如果在有效期内，则数字证书验证成功，反之，数字证书验证失败。

[0032] 优选地，用户寻找到匹配的公钥单元步骤为：用户根据公钥单元指针随机数在公钥池中寻找具有相同公钥单元指针随机数的公钥单元，如未找到，则验证失败，流程结束；如果找到，再根据匹配的公钥单元中的公钥指针函数对该公钥单元指针随机数进行计算，计算得到公钥单元的位置指针值与该公钥单元的位置指针进行比较；如果相同，则验证通过，该单元为匹配的公钥单元。

[0033] 有益效果：由于采用了上述技术方案，本发明具有如下技术效果：

[0034] (1)、本发明中使用公钥单元指针随机数和对公钥池中的用户公钥进行秘密共享得到的秘密碎片代替了公钥，使得数字证书中公钥不公开，因此量子计算机无法通过公钥去破解相应的私钥；这样的方案确保了CA服务器和持有者的非对称算法系统的安全，从而使得证书拥有着抵抗量子计算的能力。

[0035] (2)、本发明对数字证书中签名的保护不需要额外的加密步骤，仅需要对敌方无法获知的证书实际内容进行签名，就可以使得该签名可以实现抗量子计算，不增加CA服务器和用户对数字证书签名和验证的计算压力；其原理是，由于CA服务器签名的公钥、私钥均未公开，且数字签名的输入未公开，因此公开数字签名的输出并不会导致公钥、私钥及数字签名的输入中的任意一者被量子计算机破解。

[0036] (3)、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服务器内生成，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。

附图说明

[0037] 图1为本发明的CA密钥卡的密钥区分布图；

[0038] 图2为本发明的用户密钥卡的密钥区分布图；

[0039] 图3为本发明的数字证书的结构图。

具体实施方式

[0040] 下面结合附图对本方案做进一步的说明。

[0041] 如附图1所示为本发明的基于秘密共享公钥池的抗量子计算CA及证书颁发系统的一个实施例的结构示意图，本发明实现一种基于秘密共享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的成员组成的群组。群组中的CA服务器拥有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。

[0042] 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。

[0043] 与申请号为“201610843210.6”的专利相比,密钥卡的颁发机制有所不同。本发明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。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。

[0044] 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。

[0045] 系统说明

[0046] 1.PK单元

[0047] 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用户成员的个数。PK单元是由PKR、FPOS信息、(x1,PK1)和PK算法四个部分组成,PK单元结构如下所示。其中PKR为公钥单元指针随机数(公钥的存储位置参数),FPOS为公钥指针函数,(x1,PK1)为公钥PK经过(2,2)秘密共享后得到的秘密碎片,PK算法即公钥算法,包含有签名算法编号及相关算法参数。

[0048] 秘密共享算法的原理如下所示:

[0049] 从素数阶q的有限域GF(q)中随机选取n个不同的非零元素x1,x2,…,xn,分成n组秘密碎片,表示为Pi(i=1,2,…,n)。设共享的秘密信息为M,从GF(q)中选取t-1个元素a1,a2,…,a(t-1),构造多项式$f(x)=M+\sum_{j=1}^{t-1}aj*xj)$,则有Mi=f(xi)(1≤i≤n)。(xi,Mi)作为秘密碎片Pi。

[0050] 从n个秘密碎片中获取任意t个秘密碎片可以得到共享秘密信息M,具体步骤如下:根据公式$\lambda i=\prod_{j=1,j\neq i}^{j=t}(\frac{-xj}{xi-xj})$,可以求得t个拉格朗日参数λi,因而可以根据公式M=f(0)=∑λi*Mi求得M。

[0051] 在CA服务器对每个PK进行(2,2)的秘密共享计算后得到秘密碎片(x1,PK1)和(x2,PK2)。假设PK是基于ECC算法生成的,即为椭圆曲线点(x,y)的模式,则以x和y的拼接作为一个秘密进行共享。秘密碎片(x1,PK1)存放在公钥池的PK单元中。其他用户得到相应公钥需

要凑齐2组秘密可以恢复初始PK,具体的恢复步骤为:

[0052] 2组秘密求得拉格朗日参数:

[0053] λ1＝(-x2)/(x1-x2)

[0054] λ2＝(-x1)/(x2-x1)

[0055] 求得PK＝λ1*PK1+λ2*PK2＝(x1*PK2-x2*PK1)/(x1-x2)

[0056] PK单元:

[0057]

PKR	FPOS信息	(x1,PK1)	PK算法

[0058] 其中FPOS信息包括FPOS算法ID和内部参数,如下所示。

[0059] FPOS信息:

[0060]

FPOS算法ID	内部参数

[0061] 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。

[0062] 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。

[0063] 2.密钥卡

[0064] 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密钥卡包括公钥池和CA公私钥对;用户密钥卡包括公钥池、用户公私钥对、用户公钥秘密碎片(x2,PK2)、公钥单元指针随机数和CA公钥。CA密钥卡的公钥池和用户密钥卡中的公钥池相同。密钥卡的分布结构如图1和图2。

[0065] 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,表示为PKv/SKv,v∈[1,N]。并对公钥PKv进行(2,2)秘密共享计算得到(x1,PK1)v、(x2,PK2)v,v∈[1,N]。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为公钥单元的位置指针。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、(x1,PK1)v和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。

[0066] CA服务器生成一对基于RSA算法的公私钥对PKCA/SKCA作为CA服务器的密钥。以颁发的第一个密钥卡为CA密钥卡,将CA公私钥对PKCA/SKCA和公钥池通过安全的方式发送到CA密钥卡中。后续颁发的密钥卡为用户密钥卡,将CA公钥和公钥池通过安全的方式发送到用户密钥卡中,并从CA服务器的公钥池或私钥池中找到未分配的公钥单元或私钥,将对应的公私钥对PKv/SKv以及相对应的公钥单元指针随机数、公钥秘密碎片(x2,PK2)v颁发给用户密钥卡。

[0067] 安全发送的方法可以是以下6种情况的任一种:

[0068] (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;

[0069] (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;

[0070] (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;

[0071] (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;

[0072] (5)通过安全存储介质,将信息直接拷贝到用户密钥卡内;

[0073] (6)其他未提及的安全发送手段。

[0074] 实施例一

[0075] 1.1数字证书生成

[0076] 数字证书的结构如图3所示。

[0077] 本实施例中,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、持有者公钥算法、持有者的公钥单元指针随机数和持有者公钥PKv经过(2,2)秘密共享后的(x2,PK2)v;颁发者数字签名包括CA数字签名。

[0078] CA数字签名的生成如下所述:

[0079] CA服务器在进行数字签名之前先通过持有者的公钥单元指针随机数找到对应的秘密碎片(x1,PK1),结合持有者公开的秘密碎片(x2,PK2)进行秘密恢复计算得到持有者公钥PKv,并得到实际持有者信息。实际持有者信息包括持有者名称、持有者公钥算法、持有者的公钥单元指针随机数和持有者公钥PKv。

[0080] 将证书信息、颁发者信息和实际持有者信息总称为证书实际内容,命名为PCERT3,CA服务器利用自身私钥SKCA对PCERT3进行RSA算法的签名计算,得到签名SIGCA＝HASH(PCERT3)^SKCAmod n,其中,HASH()表示为RSA算法中使用的计算哈希值的哈希算法;n为RSA算法的参数,即2个大素数的乘积。

[0081] 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。根证书与普通数字证书的主要区别在于根证书持有者信息为:持有者名称、公钥算法、CA公钥的哈希值HASH(PKCA)。

[0082] 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。

[0083] 1.2.数字证书验证

[0084] 1.2.1普通数字证书的验证

[0085] 经典的数字证书的生成是含有持有者公钥的,而本实施例中的数字证书中没有公钥,只有公钥单元指针随机数和公钥PKv经过(2,2)秘密共享生成的(x2,PK2)v。因而敌方不可能通过数字证书破解相应的私钥,包括用户私钥和CA服务器的私钥。保证了数字证书的安全性。

[0086] 在进行数字证书验证之前,用户先根据公钥单元指针随机数PKR在公钥池中进行匹配,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。取出PK单元中的秘密碎片(x1,PK1)v,结合数字证书中对应

的秘密碎片(x2,PK2)v进行秘密恢复计算得到持有者公钥PKv。之后进行对数字签名的验证。

[0087] 首先用户取出存储在密钥卡内部的CA公钥PKCA并利用PCERT3(证书信息、颁发者信息和实际持有者信息)对数字证书中的颁发者数字签名进行验证。如果签名验证失败,则说明数字证书为假。反之,则验证数字证书的有效期,如果在有效期内,则数字证书验证成功。反之,数字证书验证失败。

[0088] 1.2.2根证书的验证

[0089] 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。

[0090] 根证书验证的具体流程如下:

[0091] 首先用户取出存储在密钥卡内部的CA公钥PKCA,对公钥PKCA进行哈希运算得到HASH(PKCA)',将HASH(PKCA)'与数字证书中的哈希值HASH(PKCA)进行对比,如果不同,则数字证书验证失败,流程结束。反之,则进行下一步验证。利用公钥PKCA对根证书中的颁发者数字签名进行验证。如果签名验证失败,则说明数字证书为假。反之,则进行进一步验证。检查数字证书的有效期,验证证书是否位于有效期内。如果在有效期内,则根证书验证成功,可存储于根证书集合中。反之,根证书认证失败。

[0092] 1.3.数字证书验证后续实例

[0093] 用户在验证持有者的数字证书并得到数字证书持有者的公钥。假如持有者的公私钥对是基于ECDSA算法,则通过私钥计算得到的签名可表示为{r,s}。由于签名中的r容易被量子计算机破解,从而导致私钥泄露,因此需要对r进行偏移量计算,偏移量的协商可以通过公钥池实现。例,取签名者的公钥单元的秘密碎片(x1,PK1)v,结合签名中的s参数,对其进行哈希值算法计算得到HASH((x1,PK1)v||s),利用哈希值对r进行偏移量计算得到r+HASH((x1,PK1)v||s),最终签名表示为(r+HASH((x1,PK1)v||s),s)。由于HASH((x1,PK1)v||s)无法被敌方所知,因此r无法被敌方所知,因此可以防止量子计算机对r的破解。

[0094] 综上所述可知,本发明通过对用户公钥进行秘密共享的方式,在不影响生成效率的前提下,使数字证书具有了抗量子计算的安全性与可靠性。

[0095] 以上所述仅是本发明的优选实施方式,应当指出:对于本技术领域的普通技术人员来说,在不脱离本发明原理的前提下,还可以做出若干改进和润饰,这些改进和润饰也应视为本发明的保护范围。


密钥区（CA密钥卡）
公钥池
CA公私钥对

图1

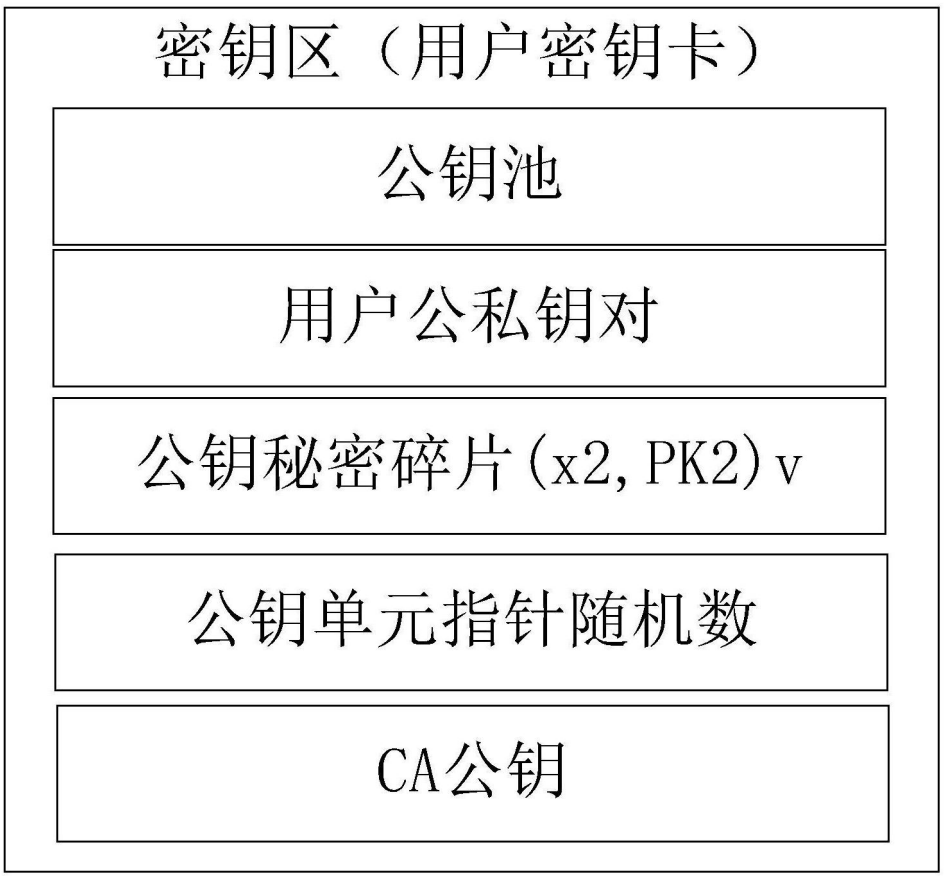
密钥区（用户密钥卡）
公钥池
用户公私钥对
公钥秘密碎片(x2,PK2)v
公钥单元指针随机数
CA公钥

图2

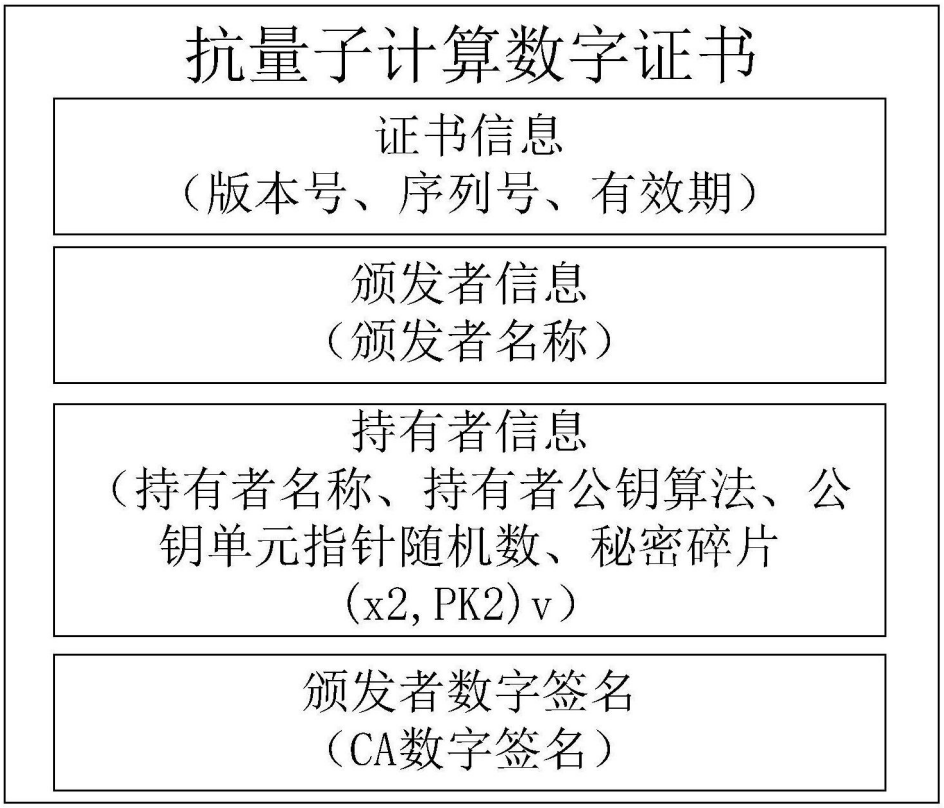
抗量子计算数字证书
证书信息
（版本号、序列号、有效期）
颁发者信息
（颁发者名称）
持有者信息
（持有者名称、持有者公钥算法、公钥单元指针随机数、秘密碎片
(x2,PK2)v）
颁发者数字签名
（CA数字签名）

图3