(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 112104453 B
(45)授权公告日 2022.08.09

(21)申请号 202010781236.9

(22)申请日 2020.08.06

(65)同一申请的已公布的文献号
申请公布号 CN 112104453 A

(43)申请公布日 2020.12.18

(73)专利权人 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
专利权人 南京如般量子科技有限公司

(72)发明人 富尧 钟一民 杨羽成

(74)专利代理机构 南京中盟科创知识产权代理事务所(特殊普通合伙) 32279
专利代理师 张靖尧

(51)Int.Cl.
H04L 9/08(2006.01)
H04L 9/32(2006.01)
H04L 9/40(2022.01)

(56)对比文件
CN 110557367 A,2019.12.10
CN 110768781 A,2020.02.07
US 9660978 B1,2017.05.23
富尧.量子通信若干理论研究.《中国博士学位论文电子期刊网》.2016,全文.

审查员 章鹏

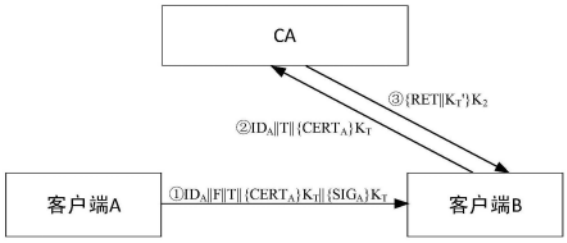
权利要求书2页 说明书7页 附图1页

(54)发明名称

一种基于数字证书的抗量子计算数字签名系统及签名方法

(57)摘要

本发明提出一种基于数字证书的抗量子计算数字签名系统及签名方法,所述系统包括客户端和部署有密钥管理服务器的CA机构;密钥管理服务器基于ID密码学为CA机构和客户端分配密钥,以使在根证书和数字证书颁发阶段和数字签名阶段中,客户端和CA机构都能根据分配到的密钥基于ID密码学与所通信的对象之间进行密钥协商,以实现整个数字签名过程的抗量子计算保密通信。本发明能够在不改变传统CA及基于数字证书的数字签名系统的整体流程和数据结构、不需要在客户端存储密钥池的前提下,实现数字签名过程中的抗量子计算保密通信。基于ID密码学的密钥颁发服务器对每个不同用户的系统公私钥均不同,提高了系统安全性。



CN 112104453 B

1.一种基于数字证书的抗量子计算数字签名系统,包括:CA机构和客户端,其特征在于:

所述CA机构部署有密钥管理服务器,密钥管理服务器为CA机构和客户端分别生成一个唯一的ID,并为CA机构和客户端配置密钥数据,包括:CA机构的系统公私钥、客户端的系统公私钥、CA机构的公私钥、客户端的公私钥;所述各公私钥遵循ID密码学,客户端与CA机构之间能够根据所持有的公私钥计算出彼此间的对称密钥;

密钥管理服务器保存CA机构的系统公私钥和客户端的系统私钥,将CA机构的公私钥和ID颁发给CA机构,将客户端的公私钥和ID颁发给客户端;

在根证书和数字证书颁发阶段:客户端与CA机构根据自己分配到的ID和公私钥进行对称密钥计算,并根据计算出的对称密钥进行保密通信;

在签名阶段:签名方客户端首先用自己的证书私钥对待发送的原始文件和数字证书进行加密,得到数字签名;然后计算与CA机构的第一对称密钥,用计算出的第一对称密钥分别加密数字签名和数字证书,最后将签名方客户端ID、原始文件、加密后的数字签名、加密后的数字证书一起作为签名文件公开;

签名认证方客户端接收到公开的签名文件后,将签名方客户端ID、自己的ID和加密后的数字证书一并发送给CA机构;

CA机构接收到来自签名认证方客户端的消息后,根据消息中携带的签名方客户端ID计算出与签名方客户端之间的第一对称密钥,用计算出的第一对称密钥对加密后的数字证书进行解密,得到签名方客户端的数字证书;CA机构对签名方客户端的数字证书进行证书有效验证,得到验证结果;CA机构计算与签名认证方客户端的第二对称密钥,并用计算出的第二对称密钥加密第一对称密钥和验证结果,将加密后的消息返回给签名认证方客户端;

签名认证方客户端接收到CA机构的反馈消息后,计算出与CA机构之间的第二对称密钥以解密反馈消息,得到第一对称密钥和验证结果;若验证结果为证书失效,则签名验证失败;若验证结果为证书有效,则签名认证方客户端用第一对称密钥解密公开的签名文件中加密的数字证书和数字签名,然后用根证书验证数字证书、用数字证书中的证书公钥验证数字签名,验证通过后,信任签名方客户端发来的原始文件。

2.根据权利要求1所述的一种基于数字证书的抗量子计算数字签名系统,其特征在于:所述CA机构的系统公私钥、客户端的系统公私钥、CA机构的公私钥、客户端的公私钥的生成方式如下:

CA机构的系统私钥为密钥管理服务器随机生成,CA机构的系统公钥由相应系统私钥与一个加法循环群的生成元进行计算得到;客户端的系统私钥由CA机构的系统私钥加密客户端ID得到,客户端的系统公钥由客户端的系统私钥与所述生成元进行计算得到;CA机构和客户端的公钥由哈希函数计算相应ID得到,CA机构和客户端的私钥由自己的公钥与自己的系统私钥计算得到。

3.根据权利要求2所述的一种基于数字证书的抗量子计算数字签名系统,其特征在于:

所述客户端计算与所述CA机构之间的对称密钥的步骤为:客户端采用哈希函数计算CA机构ID,得到CA机构的公钥,再将自己的私钥与CA机构的公钥进行计算,得到对称密钥;

所述CA机构计算与所述客户端之间的对称密钥的步骤为:根据客户端ID计算客户端的公钥,再通过密钥管理服务器提供的客户端系统私钥与CA机构的公钥进行计算,将计算结

果再与客户端的公钥进行计算,得到与客户端的对称密钥。

4.根据权利要求3所述的一种基于数字证书的抗量子计算数字签名系统,其特征在于:在所述在根证书和数字证书颁发阶段和签名阶段中,客户端与CA机构间通过计算对称密钥进行保密通信时,还通过计算消息认证码保证信息的完整性并完成通信双方的身份校验。

5.根据权利要求3所述的一种基于数字证书的抗量子计算数字签名系统,其特征在于:

在所述在根证书和数字证书颁发阶段和签名阶段中,数据发送方将协商好的对称密钥作为根密钥,然后随机生成一个明文消息,用对称密钥加密所述明文消息,得到最终密钥,用最终密钥对待发送的内容进行加密,然后将加密数据和明文消息发送给数据接收方;

数据接收方接收到来自数据发送方的数据后,根据协商好的对称密钥和接收到的明文消息计算最终密钥,用计算出的最终密钥解密加密数据,得到加密内容。

6.根据权利要求5所述的一种基于数字证书的抗量子计算数字签名系统,其特征在于:所述明文消息为数据发送方实时生成的时间戳,所述时间戳用于记录数据发送方发送数据的时间。

7.根据权利要求1所述的一种基于数字证书的抗量子计算数字签名系统,其特征在于:

所述CA机构配置有本地抗量子计算装置,而所述密钥管理服务器部署在本地抗量子计算装置中。

8.根据权利要求1所述的一种基于数字证书的抗量子计算数字签名系统,其特征在于:所述客户端配置有客户端抗量子计算装置,所述密钥管理服务器生成客户端公私钥和ID后,将公私钥和ID存储在客户端抗量子计算装置中颁发给客户端。

9.根据权利要求7或8所述的一种基于数字证书的抗量子计算数字签名系统,其特征在于:所述抗量子计算装置包括密钥卡、移动终端、密码机、网关。

10.一种基于数字证书的抗量子计算数字签名方法,其特征在于,所述方法基于权利要求1至9任意一项所述的基于数字证书的抗量子计算数字签名系统实现两个客户端之间的数字签名认证。

一种基于数字证书的抗量子计算数字签名系统及签名方法

技术领域

[0001] 本发明涉及数字证书领域，尤其涉及基于数字证书的抗量子计算数字签名系统及签名方法。

背景技术

[0002] CA(Certification Authority)是证书的签发机构，它是公钥基础设施(Public Key Infrastructure,PKI)的核心。CA是负责签发证书、认证证书、管理已颁发证书的机关。CA拥有一个证书(内含CA公钥)。网上的公众用户通过验证CA的签字从而信任CA，任何人都可以得到CA的证书，用以验证它所签发的证书。证书的格式和验证方法普遍遵循X.509国际标准。

[0003] 数字签名又称公钥数字签名，是只有信息的发送者才能产生的别人无法伪造的数字串，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。现有的数字签名在信息传输过程中往往使用的都是基于数学算法复杂度的加密方式，如当今主流的非对称加密算法，如RSA加密算法，大多数都是基于大整数的因式分解或者有限域上的离散对数的计算这两个数学难题。他们的破解难度也就依赖于解决这些问题的效率。传统计算机上，要求解这两个数学难题，花费时间为指数时间(即破解时间随着公钥长度的增长以指数级增长)，这在实际应用中是无法接受的。而为量子计算机量身定做的秀尔算法可以在多项式时间内(即破解时间随着公钥长度的增长以k次方的速度增长，其中k为与公钥长度无关的常数)进行整数因式分解或者离散对数计算，从而为RSA、离散对数加密算法的破解提供可能。

[0004] 为了使数字签名系统能够抗量子计算，行业内提出了基于量子保密通信的抗量子计算数字签名系统，如专利CN109861813A提出一种基于非对称密钥池的抗量子计算HTTPS通信方法和系统，并具体公开了一种通信方法，该方法的参与方包括服务器、证书授权中心及客户端，客户端配置密钥卡，密钥卡内存储有非对称密钥池；所述抗量子计算HTTPS通信方法，包括以下步骤：服务器端获取证书授权中心颁发的数字证书，并向客户端发送该数字证书，所述数字证书中记载有服务器的公钥指针随机数；客户端获取证书授权中心颁发的与所述数字证书相匹配的根数字证书，依据所述根数字证书对服务器发送的数字证书进行验证，根据验证通过的数字证书中记载的服务器的公钥指针随机数，在所述非对称密钥池中获取服务器公钥；利用服务器公钥对随机生成的共享密钥进行加密，向服务器发送加密结果以进行密钥协商；与服务器利用所述共享密钥进行HTTPS通信。

[0005] 专利CN109861813A提出的方案虽然能够实现基于量子保密通信的抗量子计算，但是存在以下缺陷：

[0006] 1、专利CN109861813A所提出的技术方案中，客户端需要配置存储了所有成员的公钥的量子密钥卡，增加了客户端密钥卡的存储成本和操作工作量，且用户端密钥管理工作较为复杂；

[0007] 2、专利CN109861813A所提出的技术方案中，改变了传统CA及基于数字证书的数字

签名系统的整体流程和数据结构，例如导致数字证书的格式和使用方式的改变，导致CA及用户应用系统切换到抗量子计算方案的成本过高。

发明内容

[0008] 发明目的：为克服现有技术的缺陷，本发明提出一种基于数字证书的抗量子计算数字签名系统及签名方法，能够在不改变传统CA及基于数字证书的数字签名系统的整体流程和数据结构、不需要在客户端存储密钥池的前提下，实现数字签名过程中的抗量子计算保密通信。

[0009] 发明内容：为实现上述目的，本发明一方面提出一种基于数字证书的抗量子计算数字签名系统，包括CA机构和客户端；所述CA机构部署有密钥管理服务器，密钥管理服务器为CA机构和客户端分别生成一个唯一的ID，并为CA机构和客户端配置密钥数据，包括：CA机构的系统公私钥、客户端的系统公私钥、CA机构的公私钥、客户端的公私钥；所述各公私钥遵循ID密码学，客户端与CA机构之间能够根据所持有的公私钥计算出彼此间的对称密钥；

[0010] 密钥管理服务器保存CA机构的系统公私钥和客户端的系统私钥，将CA机构的公私钥和ID颁发给CA机构，将客户端的公私钥和ID颁发给客户端；

[0011] 在根证书和数字证书颁发阶段：客户端与CA机构根据自己分配到的ID和公私钥进行对称密钥计算，并根据计算出的对称密钥进行保密通信；

[0012] 在签名阶段：签名方客户端首先用自己的证书私钥对待发送的原始文件和数字证书进行加密，得到数字签名；然后计算与CA机构的第一对称密钥，用计算出的第一对称密钥分别加密数字签名和数字证书，最后将签名方客户端ID、原始文件、加密后的数字签名、加密后的数字证书一起作为签名文件公开；

[0013] 签名认证方客户端接收到公开的签名文件后，将签名方客户端ID、自己的ID和加密后的数字证书一并发送给CA机构；

[0014] CA机构接收到来自签名认证方客户端的消息后，根据消息中携带的签名方客户端ID计算出与签名方客户端之间的第一对称密钥，用计算出的第一对称密钥对加密后的数字证书进行解密，得到签名方客户端的数字证书；CA机构对签名方客户端的数字证书进行证书有效验证，得到验证结果；CA机构计算与签名认证方客户端的第二对称密钥，并用计算出的第二对称密钥加密第一对称密钥和验证结果，将加密后的消息返回给签名认证方客户端；

[0015] 签名认证方客户端接收到CA机构的反馈消息后，计算出与CA机构之间的第二对称密钥以解密反馈消息，得到第一对称密钥和验证结果；若验证结果为证书失效，则签名验证失败；若验证结果为证书有效，则签名认证方客户端用第一对称密钥解密公开的签名文件中加密的数字证书和数字签名，然后用根证书验证数字证书、用数字证书中的证书公钥验证数字签名，验证通过后，信任签名方客户端发来的原始文件。

[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] 可选的，所述CA机构的系统公私钥、客户端的系统公私钥、CA机构的公私钥、客户端的公私钥的生成方式如下：CA机构的系统私钥为密钥管理服务器随机生成，CA机构的系

统公钥由相应系统私钥与一个加法循环群的生成元进行计算得到;客户端的系统私钥由CA机构的系统私钥加密客户端ID得到,客户端的系统公钥由客户端的系统私钥与所述生成元进行计算得到;CA机构和客户端的公钥由哈希函数计算相应ID得到,CA机构和客户端的私钥由自己的公钥与自己的系统私钥计算得到。

[0018] 可选的,所述客户端计算与所述CA机构之间的对称密钥的步骤为:客户端采用哈希函数计算CA机构ID,得到CA机构的公钥,再将自己的私钥与CA机构的公钥进行计算,得到对称密钥;所述CA机构计算与所述客户端之间的对称密钥的步骤为:根据客户端ID计算客户端的公钥,再通过密钥管理服务器提供的客户端系统私钥与CA机构的公钥进行计算,将计算结果再与客户端的公钥进行计算,得到与客户端的对称密钥。

[0019] 可选的,在所述在根证书和数字证书颁发阶段和签名阶段中,客户端与CA机构间通过计算对称密钥进行保密通信时,还通过计算消息认证码保证信息的完整性并完成通信双方的身份校验,以确保正在通信的对象就是所要通信的对象。

[0020] 可选的,在所述在根证书和数字证书颁发阶段和签名阶段中,数据发送方将协商好的对称密钥作为根密钥,然后随机生成一个明文消息,用对称密钥加密所述明文消息,得到最终密钥,用最终密钥对待发送的内容进行加密,然后将加密数据和明文消息发送给数据接收方;数据接收方接收到来自数据发送方的数据后,根据协商好的对称密钥和接收到的明文消息计算最终密钥,用计算出的最终密钥解密加密数据,得到加密内容。

[0021] 通过以对称密钥作为根密钥,用根密钥结合随机生成的明文消息计算出最终密钥的方式,可以避免在两个通信对象间需要多次传输数据时对称密钥一直不变的情况。发送方每次生成的明文消息都不同,所以这个消息认证码每次也都不同。而明文消息是一并发送的,所以接收方也可以计算出这个消息认证码。通过这样的方式,发送方和接收方可以保证每次交互数据时的最终密钥都跟上一次不一样,大大降低了密钥被破解的可能。

[0022] 可选的,所述明文消息为数据发送方实时生成的时间戳,所述时间戳用于记录数据发送方发送数据的时间。通过设置时间戳,CA机构和客户端进性保密通信时,可以判断数据发送方发送数据的时间在不在数字证书的有效范围,方便验证数据发送方的数字证书是否有效。

[0023] 可选的,所述CA机构配置有本地抗量子计算装置,而所述密钥管理服务器部署在本地抗量子计算装置中。

[0024] 可选的,所述客户端配置有客户端抗量子计算装置,所述密钥管理服务器生成客户端公私钥和ID后,将公私钥和ID存储在客户端抗量子计算装置中颁发给客户端。

[0025] 可选的,所述抗量子计算装置包括密钥卡、移动终端、密码机、网关。

[0026] 本发明还提出一种基于数字证书的抗量子计算数字签名方法,该方法基于所述的基于数字证书的抗量子计算数字签名系统实现两个客户端之间的数字签名认证。

[0027] 有益效果:

[0028] 1.本发明可以实现抗量子计算的基于数字证书的数字签名;

[0029] 2.本发明中所使用的对称密钥均基于ID密码学实时计算生成,不需要进行对称密钥提前存储,对用户来说成本低、不存在对称密钥管理和存储问题;

[0030] 3.本发明没有改变传统CA及基于数字证书的数字签名系统的整体流程和数据结构,因此CA及用户应用系统切换到抗量子计算方案的成本不高;

[0031] 4.本发明中,基于ID密码学的密钥颁发服务器对每个不同用户的系统公私钥均不同,即使某个用户的系统公钥丢失导致系统私钥被量子计算机破解,也不会危及到CA和其他用户的系统公私钥。

附图说明

[0032] 图1为本发明实施例中涉及的步骤流程图。

具体实施方式

[0033] 下面将结合附图和具体实施例对本发明作更进一步的说明。但应当理解的是,本发明可以以各种形式实施,以下在附图中出示并且在下文中描述的一些示例性和非限制性实施例,并不意图将本发明限制于所说明的具体实施例。

[0034] 应当理解的是,在技术上可行的情况下,以上针对不同实施例所列举的技术特征可以相互组合,从而形成本发明范围内的另外的实施例。此外,本发明所述的特定示例和实施例是非限制性的,并且可以对以上所阐述的结构、步骤、顺序做出相应修改而不脱离本发明的保护范围。

[0035] 本发明旨在提供一种能够在不改变传统CA及基于数字证书的数字签名系统的整体流程和数据结构、不需要在客户端存储密钥池的前提下,实现数字签名过程中的抗量子计算保密通信的技术方案。

[0036] 有鉴于此,本发明提出一种基于数字证书的抗量子计算数字签名系统及签名方法。下面通过具体实施例加以说明。

[0037] 实施例:

[0038] 本实施例提出一种基于数字证书的抗量子计算数字签名系统,由用户端以及证书权威机构CA组成,用户端可分为签名者A、签名认证者B。

[0039] CA具有抗量子计算装置T_{CA},T_{CA}中部署有基于ID密码学的密钥管理服务器KMS。

[0040] KMS为A和B颁发抗量子计算装置T_A、T_B。抗量子计算装置可以是密钥卡、移动终端、密码机、网关等,可与CA机构或各个用户端分别进行主板接口通信、近距离无线通信、可控的内网通信等,可保证通信范围内不会被量子计算机窃取信息,例如抗量子计算装置可以是密钥卡插接在CA机构的主机主板上,或者抗量子计算装置可以是移动终端与同样是移动终端的双方进行NFC通信,或者抗量子计算装置是密码机或网关与同一内网的PC主机双方进行安全的内网通信。

[0041] KMS为某个成员颁发公私钥时,首先需要建立一套基于ID密钥学的系统参数,步骤如下:

[0042] (1)G_1,G_2是阶为q的GDH(Diffie-Hellman群)群,q是一个大素数,G_1是由椭圆曲线上的点构成的加法循环群,P是群G_1的生成元;G_2是一个乘法循环群;双线性映射$e:G_1\times G_1\rightarrow G_2$。

[0043] (2)随机地取$SK_{MS}\in Z_p^*$作为CA的系统私钥,SK_{MS}仅保存在KMS的抗量子计算装置中,计算CA的系统公钥$PK_{MS}=SK_{MS}*P$,PK_{MS}保存在CA的抗量子计算装置T_{CA}。KMS对每个不同用户的系统公私钥均不同,对于用户端A,KMS会生成唯一编码作为ID_A,A的系统私钥为$SK_{MSA}=MAC(ID_A,SK_{MS})$(MAC(m,k)为使用密钥k对消息m计算消息认证码),A的系统公钥为$PK_{MSA}=SK_{MSA}*$

P;对于用户端B,KMS会生成唯一编码作为ID_B,B的系统私钥为$SK_{MSB}=MAC(ID_B,SK_{MS})$,B的系统公钥为$PK_{MSB}=SK_{MSB}*P$;系统私钥保存在KMS的抗量子计算装置中,系统公钥保存在对应用户端的抗量子计算装置中,即PK_{MSA}保存在T_A中,PK_{MSB}保存在T_B中。

[0044] (3)选择哈希函数$H_1:\{0,1\}^*\rightarrow G_1$,$H_2:G_2\rightarrow\{0,1\}^*$。

[0045] (4)系统参数为$\{q,G_1,G_2,e,n,P,H_1,H_2\}$。

[0046] KMS为CA颁发公私钥时,生成唯一编码作为ID_{CA},调用哈希函数H_1计算公钥$PK_{CA}=H_1(ID_{CA})$,再根据公钥PK_{CA}计算私钥$SK_{CA}=SK_{MS}*PK_{CA}$,将CA的ID和公私钥即ID_{CA}、PK_{CA}、SK_{CA}存储于CA的抗量子计算装置T_{CA}。T_{CA}中还存储有CA根证书$CERT_{CA}$,$CERT_{CA}$中包括证书的版本号、序列号、有效期以及CA的证书公钥PK_{CERTCA}和证书签名,其中证书公钥和证书签名可以基于RSA、ECC、离散对数、ID密码学等多种非对称密码算法。

[0047] KMS为用户端A颁发公私钥时,调用哈希函数H_1计算公钥$PK_A=H_1(ID_A)$,再根据公钥PK_A计算私钥$SK_A=SK_{MSA}*PK_A$,将A的ID和公私钥即ID_A、PK_A、SK_A存储于A的抗量子计算装置T_A。

[0048] KMS为用户端B颁发公私钥时,调用哈希函数H_1计算公钥$PK_B=H_1(ID_B)$,再根据公钥PK_B计算私钥$SK_B=SK_{MSB}*PK_B$,将B的ID和公私钥即ID_B、PK_B、SK_B存储于B的抗量子计算装置T_B。

[0049] 步骤1:颁发根证书

[0050] CA机构为所有客户端颁发根证书,此处以客户端A为例详述颁发过程:

[0051] (1)A→CA

[0052] 用户端A根据ID_{CA}计算得到$PK_{CA}=H_1(ID_{CA})$,进一步计算与CA之间的对称密钥$K_{A-CA}=e(SK_A,PK_{CA})$。获取时间戳T_1,使用K_{A-CA}对T_1加密,得到最终密钥$K_1=MAC(T1,K_{A-CA})$。

[0053] 使用K_1对A的身份信息AINFO加密得到$\{AINFO\}K_1$,使用K_1对T_1和AINFO计算消息认证码得到$MAC(T_1||AINFO,K_1)$,连同ID_A、ID_{CA}以及T_1一起发送至CA,发送的消息可表示为$ID_A||ID_{CA}||T_1||\{AINFO\}K_1||MAC(T_1||AINFO,K_1)$。

[0054] (2)CA→A

[0055] CA中的KMS计算A的系统私钥为$SK_{MSA}=MAC(ID_A,SK_{MS})$,根据$PK_{CA}=H_1(ID_{CA})$得到$SK_{CAA}=SK_{MSA}*PK_{CA}$。进一步得到CA与A之间的对称密钥$K_{CA-A}=e(SK_{CAA},PK_A)$。根据ID密码学可得:$K_{A-CA}=e(SK_A,PK_{CA})=e(SK_{MSA}*PK_A,PK_{CA})=e(PK_A,SK_{MSA}*PK_{CA})=e(PK_A,SK_{CAA})=e(SK_{CAA},PK_A)=K_{CA-A}$。使用$K_{CA-A}$对$T_1$计算消息认证码得到$K'_1=MAC(T_1,K_{CA-A})$。使用$K'_1$解密并验证消息认证码,得到A的身份信息AINFO。

[0056] CA取出CA根证书$CERT_{CA}$,获取时间戳T_2,使用K_{CA-A}对T_2加密计算得到最终密钥$K_2=MAC(T_2,K_{CA-A})$。使用K_2对$CERT_{CA}$加密得到$\{CERT_{CA}\}K_2$,使用K_2对T_2和$CERT_{CA}$计算消息认证码得到$MAC(T_2||CERT_{CA},K_2)$,连同ID_{CA}、ID_A以及T_2一起发送至A,发送的消息可表示为$ID_{CA}||ID_A||T_2||\{CERT_{CA}\}K_2||MAC(T_2||CERT_{CA},K_2)$。

[0057] A收到消息后,使用K_{A-CA}对T_2加密计算得到最终密钥$K'_2=MAC(T_2,K_{A-CA})$。使用K'_2解密并验证消息认证码,得到CA根证书$CERT_{CA}$,A对其进行验证后,存入本地抗量子计算装置T_A内。

[0058] 用户端B也与CA进行如上相同步骤,获得CA根证书$CERT_{CA}$,存入本地抗量子计算装置T_B内。

[0059] 步骤2:颁发证书

[0060] (1)A→CA

[0061] 用户端A计算与CA之间的对称密钥$K_{A-CA}=e(SK_A,PK_{CA})$。获取时间戳T_3，使用K_{A-CA}对T_3加密计算得到最终密钥$K_3=MAC(T_3,K_{A-CA})$。

[0062] A生成证书公私钥对PK_{CERTA}、SK_{CERTA}，可以基于RSA、ECC、离散对数、ID密码学等多种非对称密码算法。使用K_3对A的身份信息AINFO和A的证书公钥PK_{CERTA}加密得到$\{AINFO||PK_{CERTA}\}K_3$，使用K_3对T_3、AINFO以及PK_{CERTA}计算消息认证码得到$MAC(T_3||AINFO||PK_A,K_3)$，连同$ID_A$、$ID_{CA}$以及$T_3$一起发送至CA，发送的消息可表示为$ID_A||ID_{CA}||T_3||\{AINFO||PK_{CERTA}\}K_3||MAC(T_3||AINFO||PK_{CERTA},K_3)$。

[0063] (2)CA→A

[0064] CA中的KMS计算A的系统私钥为$SK_{MSA}=MAC(ID_A,SK_{MS})$，根据$PK_{CA}=H_1(ID_{CA})$得到$SK_{CAA}=SK_{MSA}*PK_{CA}$。进一步得到CA与A之间的对称密钥$K_{CA-A}=e(SK_{CAA},PK_A)$。根据ID密码学可得：$K_{A-C_A}=e(SK_A,PK_{CA})=e(SK_{MSA}*PK_A,PK_{CA})=e(PK_A,SK_{MSA}*PK_{CA})=e(PK_A,SK_{CAA})=e(SK_{CAA},PK_A)=K_{CA-A}$。使用$K_{CA-A}$对$T_3$加密计算得到最终密钥$K'_3=MAC(T_1,K_{CA-A})$。使用$K'_3$解密并验证消息认证码，得到A的身份信息AINFO和用于计算$CERT_A$的PK_{CERTA}。

[0065] CA制作A的证书$CERT_A$。然后CA获取时间戳T_4，使用K_{CA-A}对T_4加密计算得到最终密钥$K_4=MAC(T_4,K_{CA-A})$。使用K_4对$CERT_A$加密得到$\{CERT_A\}K_4$，使用K_4对T_4和$CERT_A$计算消息认证码得到$MAC(T_4||CERT_A,K_4)$，连同ID_{CA}、ID_A以及T_4一起发送至A，发送的消息可表示为$ID_{CA}||ID_A||T_4||\{CERT_A\}K_4||MAC(T_4||CERT_A,K_4)$。

[0066] A收到消息后，使用K_{A-CA}对T_4加密计算得到$K'_4=MAC(T_4,K_{A-CA})$。使用K'_4解密并验证消息认证码，得到自己的证书$CERT_A$，A对其进行验证后，存入本地抗量子计算装置T_A内。

[0067] 用户端B生成证书公私钥对PK_{CERTB}、SK_{CERTB}，也与CA进行如上相同步骤，获得自己的证书$CERT_B$。B对$CERT_B$进行验证后，存入本地抗量子计算装置T_B内。

[0068] 步骤3：数字签名

[0069] (1)A签名得到签名文件并广播

[0070] 令原始文件为F，签名时间为T。

[0071] 用户端A计算与CA之间的对称密钥$K_{A-CA}=e(SK_A,PK_{CA})$。使用K_{A-CA}对T加密计算得到最终密钥$K_T=MAC(T,K_{A-CA})$。使用A的证书私钥SK_{CERTA}对F、T以及$CERT_A$计算签名得到$SIG_A=SIGN(F||T||CERT_A,SK_{CERTA})$。使用$K_T$对$CERT_A$和$SIG_A$分别加密得到$\{CERT_A\}K_T$和$\{SIG_A\}K_T$。使用$K_T$对$ID_A$、F、T、$CERT_A$以及$SIG_A$计算消息认证码得到$MAC(ID_A||F||T||CERT_A||SIG_A,K_T)$。连同$ID_A$、F、T、$\{CERT_A\}K_T$和$\{SIG_A\}K_T$一起作为签名文件FS公开，公开的签名文件可表示为

[0072] $FS=ID_A||F||T||\{CERT_A\}K_T||\{SIG_A\}K_T||MAC(ID_A||F||T||CERT_A||SIG_A,K_T)$。

[0073] (2)B→CA

[0074] B收到FS后，计算与CA之间的对称密钥$K_{B-CA}=e(SK_B,PK_{CA})$。获取时间戳T_5，使用K_{B-CA}对T_5加密计算得到$K_5=MAC(T_5,K_{B-CA})$。使用K_5对T_5、ID_A、T以及$\{CERT_A\}K_T$计算消息认证码得到$MAC(T_5||ID_A||T||\{CERT_A\}K_T,K_5)$。连同$ID_A$、$ID_B$、$ID_{CA}$、$T_5$、T、以及$\{CERT_A\}K_T$一起发送至CA，发送的消息可表示为

[0075] $M_1=ID_B||ID_{CA}||T_5||ID_A||T||\{CERT_A\}K_T||MAC(T_5||ID_A||T||\{CERT_A\}K_T,K_5)$。

[0076] (3)CA→B

[0077] CA收到消息后，CA中的KMS计算B的系统私钥为$SK_{MSB}=MAC(ID_B,SK_{MS})$，根据$PK_{CA}=H_1(ID_{CA})$计算得到$SK'_{CA}=SK_{MSB}*PK_{CA}$。进一步根据$PK_B=H_1(ID_B)$得到CA与B之间的对称密钥$K_{CA-B}$

$=e(SK'_{CA},PK_B)$。根据ID密码学可得:$K_{B-CA}=e(SK_B,PK_{CA})=e(SK_{MSB}*PK_B,PK_{CA})=e(PK_B,SK_{MSB}*PK_{CA})=e(PK_B,SK'_{CA})=e(SK'_{CA},PK_B)=K_{CA-B}$。CA使用$K_{CA-B}$对$T_5$加密计算得到$K'_5=MAC(T_1,K_{CA-B})$。使用$K'_5$解密$M_1$并验证消息认证码,证实消息来自于B。

[0078] CA中的KMS计算A的系统私钥为$SK_{MSA}=MAC(ID_A,SK_{MS})$,计算得到$SK_{CAA}=SK_{MSA}*PK_{CA}$。进一步根据$PK_A=H_1(ID_A)$得到CA与A之间的对称密钥$K_{CA-A}=e(SK_{CAA},PK_A)$。根据ID密码学可得:$K_{A-CA}=e(SK_A,PK_{CA})=e(SK_{MSA}*PK_A,PK_{CA})=e(PK_A,SK_{MSA}*PK_{CA})=e(PK_A,SK_{CAA})=e(SK_{CAA},PK_A)=K_{CA-A}$。

[0079] CA使用K_{CA-A}对T加密计算得到$K'_T=MAC(T,K_{CA-A})$。使用K'_T解密$\{CERT_A\}K_T$得到$CERT_A$。判断$CERT_A$是否在证书撤销列表中,判断结果记为RET。

[0080] CA获取时间戳T_6,使用K_{CA-B}对T_6加密计算得到$K_6=MAC(T_6,K_{CA-B})$。使用K_6加密RET和K'_T得到$\{RET||K'_T\}K_6$,使用K_6对T_6、RET和K'_T计算消息认证码得到$MAC(T_6||RET||K'_T,K_6)$。连同ID_{CA}、ID_B、T_6以及$\{RET||K'_T\}K_6$一起发送至B,发送的消息可表示为$M_2=ID_{CA}||ID_B||T_6||\{RET||K'_T\}K_6||MAC(T_6||RET||K'_T,K_6)$。

[0081] (4)B

[0082] B收到M_2后,使用K_{B-CA}对T_6加密计算得到$K'_6=MAC(T_6,K_{B-CA})$。使用K'_6解密$\{RET||K'_T\}K_6$得到RET和K'_T。如果RET为失败,则文件签名验证失败,流程结束;否则继续。使用K'_T解密FS中的$\{CERT_A\}K_T$和$\{SIG_A\}K_T$得到$CERT_A$和SIG_A。使用$CERT_{CA}$中的PK_{CERTCA}验证A的证书$CERT_A$,验证通过后,使用PK_{CERTA}验证SIG_A,验证通过后,信任F是来自A的文件。

[0083] 本实施例还提出一种基于上述系统实现的基于数字证书的抗量子计算数字签名方法,该方法在两个客户端A和B之间实现基于数字证书的抗量子计算数字签名,签名流程如图1所示。

[0084] 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。

[0085] 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专利范围的限制。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,本发明专利的保护范围应以所附权利要求为准。

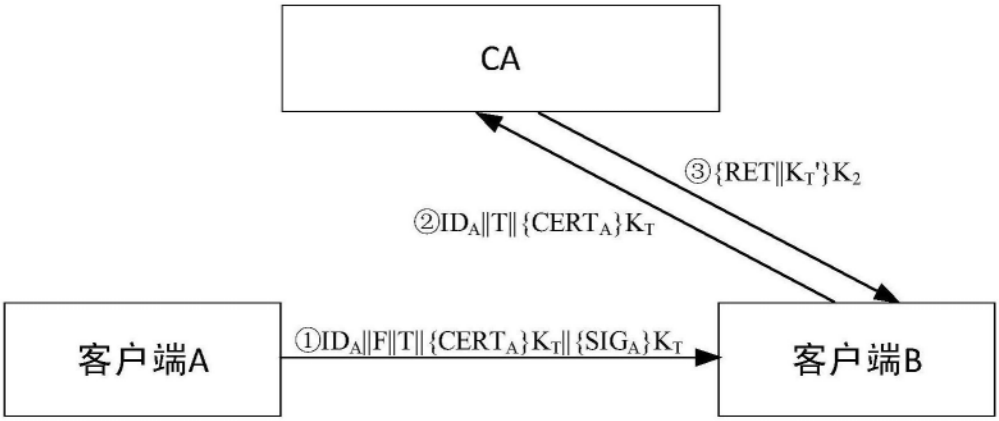


图1