(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 110519226 B
(45)授权公告日 2021.12.07

(21)申请号 201910642481.9
(22)申请日 2019.07.16
(65)同一申请的已公布的文献号
申请公布号 CN 110519226 A
(43)申请公布日 2019.11.29
(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 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.
H04L 29/06(2006.01)
H04L 9/06(2006.01)
H04L 9/08(2006.01)

(56)对比文件
CN 109756500 A,2019.05.14
CN 109981255 A,2019.07.05
CN 109672537 A,2019.04.23
CN 109818756 A,2019.05.28
US 2014122865 A1,2014.05.01

审查员 肖敬伟

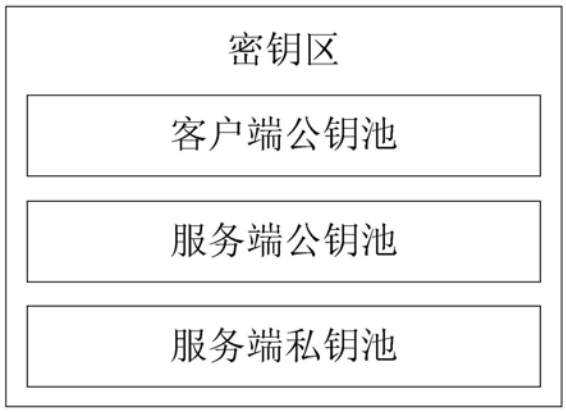
权利要求书3页 说明书12页 附图2页

(54)发明名称

基于非对称密钥池和隐式证书的量子通信服务端保密通信方法和系统

(57)摘要

本申请涉及一种基于非对称密钥池和隐式证书的量子通信服务端保密通信方法和系统,本专利对基于隐式证书的保密通信方法,使用隐式证书隐式地对公钥的可信度进行证明,使用非对称密钥和数字签名对用户的身份进行证明,保密通信的收发双方都能明确对方的身份,其他任何人均无法对保密通信进行干预或仿冒。由于非对称密钥均未公开,而公开的用户信息中无法获取密钥,因此本文的非对称密钥使用方式具有抗量子计算的特性。



CN 110519226 B

1.基于非对称密钥池和隐式证书的量子通信服务端保密通信方法，其特征在于，所述量子通信服务端保密通信方法包括密钥颁发过程和通信过程，所述密钥颁发过程如下：

颁发服务器生成第一随机数、第二随机数、接受密钥端A公钥和接受密钥端A私钥，其中接受密钥端A公钥是利用基点生成元和所述接受密钥端A私钥生成，利用所述第一随机数从自身存储中取出第一颁发服务器公钥和第一颁发服务器私钥，利用所述第一颁发服务器公钥和所述接受密钥端A公钥生成隐式证书参数，利用所述隐式证书参数和接受密钥端A设备信息生成隐式证书；利用所述隐式证书进行哈希计算得到第一哈希值；利用所述第二随机数从自身存储中取出第二颁发服务器公钥和第二颁发服务器私钥，利用所述第一哈希值，第一颁发服务器私钥以及第二颁发服务器私钥生成私钥参数；将颁发服务器公钥池、所述第一随机数、所述第二随机数、所述接受密钥端A私钥以及私钥参数写入接受密钥端A密钥卡内；

所述接受密钥端A从接受密钥端A密钥卡中读取颁发服务器公钥池、第一随机数、第二随机数、接受密钥端A私钥以及私钥参数；利用所述接受密钥端A私钥和基点生成元得到接受密钥端A公钥，利用所述第一随机数、第二随机数分别从所述颁发服务器公钥池得到第一颁发服务器公钥和第二颁发服务器公钥，利用所述隐式证书参数，第一颁发服务器公钥，接受密钥端A设备信息得到所述第一哈希值；利用所述第一哈希值、接受密钥端A私钥以及私钥参数生成工作私钥，利用所述第一哈希值、隐式证书参数以及第二颁发服务器公钥生成密钥信息，所述密钥信息包括接受密钥端A设备信息，隐式证书参数以及所述第二随机数；

接受密钥端B获取接受密钥端A发送的密钥信息，所述密钥信息包括接受密钥端A设备信息，隐式证书参数以及第二随机数；利用所述接受密钥端A设备信息，隐式证书参数生成隐式证书，对所述隐式证书进行哈希计算得到第一哈希值，利用所述第二随机数从接受密钥端B密钥卡中的服务端公钥池中取得第二服务端公钥，利用所述第一哈希值、隐式证书参数以及第二服务端公钥计算得到接受密钥端A公钥；

所述接受密钥端A公钥用于接受密钥端A和接受密钥端B之间的通信加密；

所述通信过程如下：

客户端A生成第一密钥随机数，利用所述第一密钥随机数从自身密钥卡中的服务端公钥池中得到第一服务端公钥和第二服务端公钥，生成第一密钥计算随机数，利用所述第一密钥计算随机数，基点生成元以及第一服务端公钥生成第一密钥，利用所述第一密钥计算随机数和第二服务端公钥生成第二密钥，生成第一消息，所述第一消息包括通信内容，客户端A密钥信息以及客户端B密钥信息，利用自身私钥对所述第一消息签名得到第一签名，利用所述第二密钥对所述第一消息和第一签名得到第一加密包，将所述第一加密包、第一密钥随机数，以及第一密钥发送至服务端QA；

所述服务端QA获取所述第一加密包、第一密钥随机数，以及第一密钥后，利用所述第一密钥随机数根据预设算法得到所述第一服务端公钥以及第二服务端私钥，利用所述第一密钥，第一服务端公钥以及第二服务端私钥以及基点生成元计算得到所述第二密钥，利用所述第二密钥解密所述第一加密包得到所述第一消息和第一签名，利用所述客户端A密钥信息计算得到客户端A公钥验证所述第一签名；与服务端QB加密通信将所述第一消息发送至所述服务端QB；

所述服务端QB获取、解密后获取所述第一消息，生成第二密钥随机数，利用所述第二密

钥随机数从自身密钥卡中得到第三服务端公钥和第四服务端私钥,生成第二密钥计算随机数,利用所述第二密钥计算随机数,基点生成元以及所述第三服务端公钥生成第三密钥,利用所述第二密钥计算随机数和客户端B公钥生成第四密钥,利用所述第四服务端私钥对所述第一消息签名得到第二签名,利用所述第四密钥加密所述第一消息和第二签名生成第二加密包;向所述客户端B发送所述第二密钥随机数,第三密钥以及第二加密包;

所述客户端B获取所述第二加密包,第二密钥随机数以及第三密钥后,利用利用所述第二密钥随机数根据预设算法得到所述第三服务端公钥以及第四服务端公钥,利用所述第二密钥随机数,第三服务端公钥以及客户端B私钥以及基点生成元计算得到所述第四密钥,利用所述第四密钥解密所述第二加密包得到所述第一消息和第二签名,利用所述第四服务端公钥验证所述第一签名;验证通过后信任并接受所述第一消息。

2.如权利要求1所述的量子通信服务端保密通信方法,其特征在于,当客户端A和客户端B均为服务端Q的下位设备时:

所述服务端Q获取所述第一加密包、第一密钥随机数,以及第一密钥后,利用所述第一密钥随机数根据预设算法得到所述第一服务端公钥以及第二服务端私钥,利用所述第一密钥,第一服务端公钥以及第二服务端私钥以及基点生成元计算得到所述第二密钥,利用所述第二密钥解密所述第一加密包得到所述第一消息和第一签名,利用所述客户端A密钥信息计算得到客户端A公钥验证所述第一签名;

生成第二密钥随机数,利用所述第二密钥随机数与不同的计算函数得到第三密钥指针和第四密钥指针,利用所述第三密钥指针和第四密钥指针从自身密钥卡中的服务端公钥池中得到第三服务端公钥和第四服务端私钥,生成第二密钥计算随机数,利用所述第二密钥计算随机数,基点生成元以及所述第三服务端公钥生成第三密钥,利用所述第二密钥计算随机数和客户端B公钥生成第四密钥,利用所述第四服务端私钥对所述第一消息签名得到第二签名,利用所述第四密钥加密所述第一消息和第二签名生成第二加密包;向所述客户端B发送所述第二密钥随机数,第三密钥以及第二加密包。

3.如权利要求1所述的量子通信服务端保密通信方法,其特征在于,所述客户端A利用所述第一密钥随机数与不同的计算函数得到第一密钥指针和第二密钥指针,利用所述第一密钥指针和第二密钥指针从自身密钥卡中的服务端公钥池中得到第一服务端公钥和第二服务端公钥。

4.如权利要求1所述的量子通信服务端保密通信方法,其特征在于,所述服务端QB利用所述第二密钥随机数与不同的计算函数得到第三密钥指针和第四密钥指针,利用所述第三密钥指针和第四密钥指针从自身密钥卡中的服务端公钥池中得到第三服务端公钥、从服务端私钥池中第四服务端私钥。

5.一种客户端A设备,包括存储器和处理器,所述存储器存储有计算机程序,其特征在于,所述处理器执行所述计算机程序时实现权利要求1中所述量子通信服务端保密通信方法的中的客户端A的步骤。

6.一种客户端B设备,包括存储器和处理器,所述存储器存储有计算机程序,其特征在于,所述处理器执行所述计算机程序时实现权利要求1中所述量子通信服务端保密通信方法的中的客户端B的步骤。

7.一种服务端设备,包括存储器和处理器,所述存储器存储有计算机程序,其特征在

于,所述处理器执行所述计算机程序时实现权利要求1中所述量子通信服务端保密通信方法的中的服务端QA的步骤。

8.一种服务端设备,包括存储器和处理器,所述存储器存储有计算机程序,其特征在于,所述处理器执行所述计算机程序时实现权利要求1中所述量子通信服务端保密通信方法的中的服务端QB的步骤。

9.一种服务端设备,包括存储器和处理器,所述存储器存储有计算机程序,其特征在于,所述处理器执行所述计算机程序时实现权利要求2中所述量子通信服务端保密通信方法的中的服务端Q的步骤。

10.基于非对称密钥池和隐式证书的量子通信服务端保密通信系统,其特征在于,包括设有客户端,服务端以及通信网络;所述客户端配置有客户端密钥卡,所述客户端密钥卡内存储有服务端公钥池和客户端私钥;所述服务端配置有服务端密钥卡,所述服务端密钥卡内存储有服务端私钥池,客户端公钥池以及服务端公钥池;

所述客户端,服务端通过所述通信网络实现权利要求1中所述量子通信服务端保密通信方法的步骤。

基于非对称密钥池和隐式证书的量子通信服务端保密通信方法和系统

技术领域

[0001] 本申请涉及安全通信技术领域，特别是涉及基于非对称密钥池和隐式证书的量子通信服务端保密通信方法和系统。

背景技术

[0002] 迅速发展的Internet给人们的生活、工作带来了巨大的方便，人们可以坐在家里通过Internet收发电子邮件、打电话、进行网上购物、银行转账等活动。同时网络信息安全也逐渐成为一个潜在的巨大问题。一般来说网络信息面临着以下几种安全隐患：网络信息被窃取、信息被篡改、攻击者假冒信息、恶意破坏等。

[0003] 其中保密通信是其中一种保护人们网络信息的手段，一般通过密码学加密的方法来实现，加密之前通信双方需要共享保密通信密钥。而当前进行保密通信主要是依靠密码技术，而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。目前大部分的保密通信使用算法时，一般先依靠公钥密码体系获取共享对称密钥，然后使用对称密钥对消息进行加密。

[0004] 公开密钥加密系统采用的加密钥匙(公钥)和解密钥匙(私钥)是不同的。由于加密钥匙是公开的，密钥的分配和管理就很简单，公开密钥加密系统还能够很容易地实现数字签名。

[0005] 自公钥加密问世以来，学者们提出了许多种公钥加密方法，它们的安全性都是基于复杂的数学难题。但是在传统的公钥密码学中，公钥是与身份无关的字符串，存在如何确认公钥真实性的问题。公钥基础设施PKI运用可信任第三方——认证中心(Certification Authority，CA)颁发公钥证书的方式来绑定公钥和身份信息。但是PKI证书办理复杂，需搭建复杂的CA系统，证书发布、吊销、验证和保存需求占用较多资源，这就限制PKI在实时和低带宽环境中的广泛应用。

[0006] 基于ECQV(Elliptic Curve Qu-Vanstone)自签名隐式证书机制设计了一种双向认证密钥协商协议，该ECQV隐式证书的生成基于ECC算法，它的证书更小，计算速度更快，可以显著提高认证效率。传统证书中，公钥和数字签名是分开的，而在ECQV自签名隐式证书中，数字签名是嵌入到公钥中的，这也是“自签名”的含义，接收方可以从中提取公钥来验证其身份。

[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，因此目前常用的非对称密钥将在量子时代变得不堪一击。

[0008] 由于量子计算机的潜在威胁，现有基于对称密钥池进行保密通信的方案，利用服务端与客户端之间的对称密钥池进行保密通信，放弃使用公钥密码学，以避免保密通信系统被量子计算机破解。

[0009] 现有技术存在的问题：

[0010] 1.现有基于对称密钥池进行保密通信的方案，服务端与客户端之间使用对称密钥池，其容量巨大，对服务端的密钥存储带来压力；

[0011] 2.现有基于对称密钥池进行保密通信的方案，由于对称密钥池密钥容量巨大，服务端不得不将密钥加密存储于普通存储介质例如硬盘内，而无法存储于服务端的密钥卡内；

[0012] 3.现有基于对称密钥池进行保密通信的方案，由于对称密钥池密钥容量巨大，给密钥的在线更新造成麻烦。

发明内容

[0013] 基于此，有必要针对上述技术问题，提供一种能够减少服务端存储数据量的基于非对称密钥池和隐式证书的量子通信服务端保密通信方法。

[0014] 本申请公开了基于非对称密钥池和隐式证书的量子通信服务端保密通信方法，所述量子通信服务端保密通信方法包括密钥颁发过程和通信过程，所述密钥颁发过程如下：

[0015] 颁发服务器生成第一随机数、第二随机数、接受密钥端A公钥和接受密钥端A私钥，其中接受密钥端A公钥是利用基点生成元和所述接受密钥端A私钥生成，利用所述第一随机数从自身存储中取出第一颁发服务器公钥和第一颁发服务器私钥，利用所述第一颁发服务器公钥和所述接受密钥端A公钥生成隐式证书参数，利用所述隐式证书参数和接受密钥端A设备信息生成隐式证书；利用所述隐式证书进行哈希计算得到第一哈希值；利用所述第二随机数从自身存储中取出第二颁发服务器公钥和第二颁发服务器私钥，利用所述第一哈希值，第一颁发服务器私钥以及第二颁发服务器私钥生成私钥参数；将颁发服务器公钥池、所述第一随机数、所述第二随机数、所述接受密钥端A私钥以及私钥参数写入接受密钥端A密钥卡内；

[0016] 所述接受密钥端A从接受密钥端A密钥卡中读取颁发服务器公钥池、第一随机数、第二随机数、接受密钥端A私钥以及私钥参数；利用所述接受密钥端A私钥和基点生成元得到接受密钥端A公钥，利用所述第一随机数、第二随机数分别从所述颁发服务器公钥池得到第一颁发服务器公钥和第二颁发服务器公钥，利用所述隐式证书参数，第一颁发服务器公钥，接受密钥端A设备信息得到所述第一哈希值；利用所述第一哈希值、接受密钥端A私钥以及私钥参数生成工作私钥，利用所述第一哈希值、隐式证书参数以及第二颁发服务器公钥生成密钥信息，所述密钥信息包括接受密钥端A设备信息，隐式证书参数以及所述第二随机数；

[0017] 接受密钥端B获取接受密钥端A发送的密钥信息，所述密钥信息包括接受密钥端A设备信息，隐式证书参数以及第二随机数；利用所述接受密钥端A设备信息，隐式证书参数生成隐式证书，对所述隐式证书进行哈希计算得到第一哈希值，利用所述第二随机数从接受密钥端B密钥卡中的服务端公钥池中取得第二服务端公钥，利用所述第一哈希值、隐式证书参数以及第二服务端公钥生成接受密钥端A公钥；

[0018] 所述接受密钥端A公钥用于接受密钥端A和接受密钥端B之间的通信加密；

[0019] 所述通信过程如下：

[0020] 客户端A生成第一密钥随机数，利用所述第一密钥随机数从自身密钥卡中的服务

端公钥池中得到第一服务端公钥和第二服务端公钥，生成第一密钥计算随机数，利用所述第一密钥计算随机数，基点生成元以及第一服务端公钥生成第一密钥，利用所述第一密钥计算随机数和第二服务端公钥生成第二密钥，生成第一消息，所述第一消息包括通信内容，客户端A密钥信息以及客户端B密钥信息，利用自身私钥对所述第一消息签名得到第一签名，利用所述第二密钥对所述第一消息和第一签名得到第一加密包，将所述第一加密包、第一密钥随机数，以及第一密钥发送至服务端QA；

[0021] 所述服务端QA获取所述第一加密包、第一密钥随机数，以及第一密钥后，利用所述第一密钥随机数根据预设算法得到所述第一服务端公钥以及第二服务端私钥，利用所述第一密钥，第一服务端公钥以及第二服务端私钥以及基点生成元计算得到所述第二密钥，利用所述第二密钥解密所述第一加密包得到所述第一消息和第一签名，利用所述客户端A密钥信息计算得到客户端A公钥验证所述第一签名；与服务端QB加密通信将所述第一消息发送至所述服务端QB；

[0022] 所述服务端QB获取、解密后获取所述第一消息，生成第二密钥随机数，利用所述第二密钥随机数从自身密钥卡中得到第三服务端公钥和第四服务端私钥，生成第二密钥计算随机数，利用所述第二密钥计算随机数，基点生成元以及所述第三服务端公钥生成第三密钥，利用所述第二密钥计算随机数和客户端B公钥生成第四密钥，利用所述第四服务端私钥对所述第一消息签名得到第二签名，利用所述第四密钥加密所述第一消息和第二签名生成第二加密包；向所述客户端B发送所述第二密钥随机数，第三密钥以及第二加密包；

[0023] 所述客户端B获取所述第二加密包，第二密钥随机数以及第三密钥后，利用利用所述第二密钥随机数根据预设算法得到所述第三服务端公钥以及第四服务端公钥，利用所述第二密钥随机数，第三服务端公钥以及客户端B私钥以及基点生成元计算得到所述第四密钥，利用所述第四密钥解密所述第二加密包得到所述第一消息和第二签名，利用所述第四服务端公钥验证所述第一签名；验证通过后信任并接受所述第一消息。

[0024] 优选的，当客户端A和客户端B均为服务端Q的下位设备时：

[0025] 所述服务端Q获取所述第一加密包、第一密钥随机数，以及第一密钥后，利用所述第一密钥随机数根据预设算法得到所述第一服务端公钥以及第二服务端私钥，利用所述第一密钥，第一服务端公钥以及第二服务端私钥以及基点生成元计算得到所述第二密钥，利用所述第二密钥解密所述第一加密包得到所述第一消息和第一签名，利用所述客户端A密钥信息计算得到客户端A公钥验证所述第一签名；

[0026] 生成第二密钥随机数，利用所述第二密钥随机数与不同的计算函数得到第三密钥指针和第四密钥指针，利用所述第三密钥指针和第四密钥指针从自身密钥卡中的服务端公钥池中得到第三服务端公钥和第四服务端私钥，生成第二密钥计算随机数，利用所述第二密钥计算随机数，基点生成元以及所述第三服务端公钥生成第三密钥，利用所述第二密钥计算随机数和客户端B公钥生成第四密钥，利用所述第四服务端私钥对所述第一消息签名得到第二签名，利用所述第四密钥加密所述第一消息和第二签名生成第二加密包；向所述客户端B发送所述第二密钥随机数，第三密钥以及第二加密包。

[0027] 优选的，所述客户端A利用所述第一密钥随机数与不同的计算函数得到第一密钥指针和第二密钥指针，利用所述第一密钥指针和第二密钥指针从自身密钥卡中的服务端公钥池中得到第一服务端公钥和第二服务端公钥，

[0028] 优选的，所述服务端QB利用所述第二密钥随机数与不同的计算函数得到第三密钥指针和第四密钥指针，利用所述第三密钥指针和第四密钥指针从自身密钥卡中的服务端公钥池中得到第三服务端公钥、从服务端私钥池中第四服务端私钥。

[0029] 本申请公开了一种客户端A设备，包括存储器和处理器，所述存储器存储有计算机程序，所述处理器执行所述计算机程序时实现上述技术方案中所述量子通信服务端保密通信方法的中的客户端A的步骤。

[0030] 本申请公开了一种客户端B设备，包括存储器和处理器，所述存储器存储有计算机程序，所述处理器执行所述计算机程序时实现上述技术方案中所述量子通信服务端保密通信方法的中的客户端B的步骤。

[0031] 本申请公开了一种服务端设备，包括存储器和处理器，所述存储器存储有计算机程序，所述处理器执行所述计算机程序时实现上述技术方案中所述量子通信服务端保密通信方法的中的服务端QA的步骤。

[0032] 本申请公开了一种服务端设备，包括存储器和处理器，所述存储器存储有计算机程序，所述处理器执行所述计算机程序时实现上述技术方案中所述量子通信服务端保密通信方法的中的服务端QB的步骤。

[0033] 本申请公开了一种服务端设备，包括存储器和处理器，所述存储器存储有计算机程序，所述处理器执行所述计算机程序时实现上述技术方案中所述量子通信服务端保密通信方法的中的服务端Q的步骤。

[0034] 本申请公开了基于非对称密钥池和隐式证书的量子通信服务端保密通信系统，包括设有客户端，服务端以及通信网络；所述客户端配置有客户端密钥卡，所述客户端密钥卡内存储有服务端公钥池和客户端私钥；所述服务端配置有服务端密钥卡，所述服务端密钥卡内存储有服务端私钥池，客户端公钥池以及服务端公钥池；

[0035] 所述客户端，服务端通过所述通信网络实现上述技术方案中所述量子通信服务端保密通信方法的步骤。

[0036] 本发明中，使用的密钥卡是独立的硬件隔离设备。公钥、私钥和其他相关参数均存储在密钥卡中的数据安全区，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。由于在经典网络中均无涉及公私钥及算法参数的明文传递，因此非对称密钥被破解的风险很低。密钥卡保障了通信双方的通信安全，也极大的提高了身份认证的安全性。同时非对称密钥池解决了对称密钥池给服务端带来密钥存储压力，降低了存储成本。例如，原先用户的对称密钥池大小均为1G，用户个数为N，则服务端需要存储NG的密钥池；而如果存储非对称密钥池，客户端存储服务端公钥池大小为1G，服务端同样只需要存储1G大小的服务端私钥池。由于密钥量大大下降，所有密钥可以存储在安全性更高的密钥卡内，且给密钥备份提供了便利。

[0037] 另外，由于用户的个人密钥由原先的对称密钥池改为非对称密钥，因此给密钥更新带来便利。如本专利实施例所示，用户可以通过实施例中的保密通信方法，以本地更新的密钥为消息，与服务端进行保密通信，从而快速在线更新个人密钥，解决了对称密钥池由于容量过大而无法快速在线更新的不便。

[0038] 同时，本专利对基于隐式证书的保密通信方法，使用隐式证书隐式地对公钥的可信度进行证明，使用非对称密钥和数字签名对用户的身份进行证明，保密通信的收发双方

都能明确对方的身份，其他任何人均无法对保密通信进行干预或仿冒。由于非对称密钥均未公开，而公开的用户信息中无法获取密钥，因此本文的非对称密钥使用方式具有抗量子计算的特性。

[0039] 最后，本专利对非对称密码学加密流程进行改进，对容易被量子计算机破解的密文参数(k*G)进行偏移量计算(例如：RAQ＝k*G-PKQA1)，该偏移量只能被基于加密者群组的服务端公钥池中的密钥进行偏移量恢复，即使量子计算机也无法得到k，即本文的非对称密码学加密流程具有抗量子计算的特性。而常规做法是，对密文参数进行对称加密计算，其计算量大大高于本专利的偏移量计算。因此本专利的偏移量计算是一种更优的抗量子计算方式。

附图说明

[0040] 图1为本发明中服务端密钥卡的密钥池分布示意图；

[0041] 图2为本发明中客户端密钥卡的密钥池分布示意图；

[0042] 图3为本发明中实施例1的结构示意图；

[0043] 图4为本发明中实施例2的结构示意图。

具体实施方式

[0044] 为了使本申请的目的、技术方案及优点更加清楚明白，以下结合附图及实施例，对本申请进行进一步详细说明。应当理解，此处描述的具体实施例仅仅用以解释本申请，并不用于限定本申请。其中本申请中的服务端在未做特殊说明的情况下均为量子通信服务端，本申请中的各名称以字母和数字组合为准，例如Q，服务端Q，服务端在下文表示同一含义，即服务端Q；再例如第一密钥KR1，KR1，真随机数KR1，第一密钥在下文中表示同一含义，即第一密钥KR1，其余名称同理。

[0045] 本申请公开了基于非对称密钥池和隐式证书的量子通信服务端保密通信方法，所述量子通信服务端保密通信方法包括密钥颁发过程和通信过程，所述密钥颁发过程如下：

[0046] 颁发服务器生成第一随机数、第二随机数、接受密钥端A公钥和接受密钥端A私钥，其中接受密钥端A公钥是利用基点生成元和所述接受密钥端A私钥生成，利用所述第一随机数从自身存储中取出第一颁发服务器公钥和第一颁发服务器私钥，利用所述第一颁发服务器公钥和所述接受密钥端A公钥生成隐式证书参数，利用所述隐式证书参数和接受密钥端A设备信息生成隐式证书；利用所述隐式证书进行哈希计算得到第一哈希值；利用所述第二随机数从自身存储中取出第二颁发服务器公钥和第二颁发服务器私钥，利用所述第一哈希值，第一颁发服务器私钥以及第二颁发服务器私钥生成私钥参数；将颁发服务器公钥池、所述第一随机数、所述第二随机数、所述接受密钥端A私钥以及私钥参数写入接受密钥端A密钥卡内；

[0047] 所述接受密钥端A从接受密钥端A密钥卡中读取颁发服务器公钥池、第一随机数、第二随机数、接受密钥端A私钥以及私钥参数；利用所述接受密钥端A私钥和基点生成元得到接受密钥端A公钥，利用所述第一随机数、第二随机数分别从所述颁发服务器公钥池得到第一颁发服务器公钥和第二颁发服务器公钥，利用所述隐式证书参数，第一颁发服务器公钥，接受密钥端A设备信息得到所述第一哈希值；利用所述第一哈希值、接受密钥端A私钥以

及私钥参数生成工作私钥，利用所述第一哈希值、隐式证书参数以及第二颁发服务器公钥生成密钥信息，所述密钥信息包括接受密钥端A设备信息，隐式证书参数以及所述第二随机数；

[0048] 接受密钥端B获取接受密钥端A发送的密钥信息，所述密钥信息包括接受密钥端A设备信息，隐式证书参数以及第二随机数；利用所述接受密钥端A设备信息，隐式证书参数生成隐式证书，对所述隐式证书进行哈希计算得到第一哈希值，利用所述第二随机数从接受密钥端B密钥卡中的服务端公钥池中取得第二服务端公钥，利用所述第一哈希值、隐式证书参数以及第二服务端公钥生成接受密钥端A公钥；

[0049] 所述接受密钥端A公钥用于接受密钥端A和接受密钥端B之间的通信加密；

[0050] 所述通信过程如下：

[0051] 客户端A生成第一密钥随机数，利用所述第一密钥随机数从自身密钥卡中的服务端公钥池中得到第一服务端公钥和第二服务端公钥，生成第一密钥计算随机数，利用所述第一密钥计算随机数，基点生成元以及第一服务端公钥生成第一密钥，利用所述第一密钥计算随机数和第二服务端公钥生成第二密钥，生成第一消息，所述第一消息包括通信内容，客户端A密钥信息以及客户端B密钥信息，利用自身私钥对所述第一消息签名得到第一签名，利用所述第二密钥对所述第一消息和第一签名得到第一加密包，将所述第一加密包、第一密钥随机数，以及第一密钥发送至服务端QA；

[0052] 所述服务端QA获取所述第一加密包、第一密钥随机数，以及第一密钥后，利用所述第一密钥随机数根据预设算法得到所述第一服务端公钥以及第二服务端私钥，利用所述第一密钥，第一服务端公钥以及第二服务端私钥以及基点生成元计算得到所述第二密钥，利用所述第二密钥解密所述第一加密包得到所述第一消息和第一签名，利用所述客户端A密钥信息计算得到客户端A公钥验证所述第一签名；与服务端QB加密通信将所述第一消息发送至所述服务端QB；

[0053] 所述服务端QB获取、解密后获取所述第一消息，生成第二密钥随机数，利用所述第二密钥随机数从自身密钥卡中得到第三服务端公钥和第四服务端私钥，生成第二密钥计算随机数，利用所述第二密钥计算随机数，基点生成元以及所述第三服务端公钥生成第三密钥，利用所述第二密钥计算随机数和客户端B公钥生成第四密钥，利用所述第四服务端私钥对所述第一消息签名得到第二签名，利用所述第四密钥加密所述第一消息和第二签名生成第二加密包；向所述客户端B发送所述第二密钥随机数，第三密钥以及第二加密包；

[0054] 所述客户端B获取所述第二加密包，第二密钥随机数以及第三密钥后，利用利用所述第二密钥随机数根据预设算法得到所述第三服务端公钥以及第四服务端公钥，利用所述第二密钥随机数，第三服务端公钥以及客户端B私钥以及基点生成元计算得到所述第四密钥，利用所述第四密钥解密所述第二加密包得到所述第一消息和第二签名，利用所述第四服务端公钥验证所述第一签名；验证通过后信任并接受所述第一消息。

[0055] 优选的，当客户端A和客户端B均为服务端Q的下位设备时：

[0056] 所述服务端Q获取所述第一加密包、第一密钥随机数，以及第一密钥后，利用所述第一密钥随机数根据预设算法得到所述第一服务端公钥以及第二服务端私钥，利用所述第一密钥，第一服务端公钥以及第二服务端私钥以及基点生成元计算得到所述第二密钥，利用所述第二密钥解密所述第一加密包得到所述第一消息和第一签名，利用所述客户端A密

钥信息计算得到客户端A公钥验证所述第一签名；

[0057] 生成第二密钥随机数，利用所述第二密钥随机数与不同的计算函数得到第三密钥指针和第四密钥指针，利用所述第三密钥指针和第四密钥指针从自身密钥卡中的服务端公钥池中得到第三服务端公钥和第四服务端私钥，生成第二密钥计算随机数，利用所述第二密钥计算随机数，基点生成元以及所述第三服务端公钥生成第三密钥，利用所述第二密钥计算随机数和客户端B公钥生成第四密钥，利用所述第四服务端私钥对所述第一消息签名得到第二签名，利用所述第四密钥加密所述第一消息和第二签名生成第二加密包；向所述客户端B发送所述第二密钥随机数，第三密钥以及第二加密包。

[0058] 优选的，所述客户端A利用所述第一密钥随机数与不同的计算函数得到第一密钥指针和第二密钥指针，利用所述第一密钥指针和第二密钥指针从自身密钥卡中的服务端公钥池中得到第一服务端公钥和第二服务端公钥，

[0059] 优选的，所述服务端QB利用所述第二密钥随机数与不同的计算函数得到第三密钥指针和第四密钥指针，利用所述第三密钥指针和第四密钥指针从自身密钥卡中的服务端公钥池中得到第三服务端公钥、从服务端私钥池中第四服务端私钥。

[0060] 本申请公开了一种客户端A设备，包括存储器和处理器，所述存储器存储有计算机程序，所述处理器执行所述计算机程序时实现上述技术方案中所述量子通信服务端保密通信方法的中的客户端A的步骤。

[0061] 本申请公开了一种客户端B设备，包括存储器和处理器，所述存储器存储有计算机程序，所述处理器执行所述计算机程序时实现上述技术方案中所述量子通信服务端保密通信方法的中的客户端B的步骤。

[0062] 本申请公开了一种服务端设备，包括存储器和处理器，所述存储器存储有计算机程序，所述处理器执行所述计算机程序时实现上述技术方案中所述量子通信服务端保密通信方法的中的服务端QA的步骤。

[0063] 本申请公开了一种服务端设备，包括存储器和处理器，所述存储器存储有计算机程序，所述处理器执行所述计算机程序时实现上述技术方案中所述量子通信服务端保密通信方法的中的服务端QB的步骤。

[0064] 本申请公开了一种服务端设备，包括存储器和处理器，所述存储器存储有计算机程序，所述处理器执行所述计算机程序时实现上述技术方案中所述量子通信服务端保密通信方法的中的服务端Q的步骤。

[0065] 本申请公开了基于非对称密钥池和隐式证书的量子通信服务端保密通信系统，包括设有客户端，服务端以及通信网络；所述客户端配置有客户端密钥卡，所述客户端密钥卡内存储有服务端公钥池和客户端私钥；所述服务端配置有服务端密钥卡，所述服务端密钥卡内存储有服务端私钥池，客户端公钥池以及服务端公钥池；

[0066] 所述客户端，服务端通过所述通信网络实现上述技术方案中所述量子通信服务端保密通信方法的步骤。

[0067] 系统说明

[0068] 本发明在一个基于非对称密钥池体系中，对任意1个用户端与另一个用户端之间进行通信。下文中量子通信服务站简称为服务端。本发明的密钥池体系中每个对象都具有密钥卡，可存储大数据量的密钥，也具备处理信息的能力。本发明中，用户端和服务端的本

地系统中都存在相应需求的算法。

[0069] 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。

[0070] 密钥卡从智能卡技术上发展而来，是结合了密码学技术、硬件安全隔离技术、量子物理学技术(搭载量子随机数发生器的情况下)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。总之，密钥卡使得密钥等绝密信息不以明文形式出现在主机的磁盘及内存中，从而能有效保证绝密信息的安全。

[0071] 本发明中，密钥卡分为服务端密钥卡和客户端密钥卡。服务端密钥卡密钥区结构如图1所示，主要存储有客户端公钥池、服务端公钥池和服务端私钥池。客户端密钥卡密钥区结构如图2所示，主要存储有服务端公钥池、客户端公钥指针随机数、客户端私钥以及私钥参数。所述密钥卡均由服务端颁发。

[0072] 服务端在密钥卡注册时，先由服务端选择椭圆曲线的域参数包含q，a，b，G和n。q代表有限域Fq的大小；变量a和b是椭圆曲线$y^2=x^3+ax+b$的系数，这里$4a^3+27b^2\neq 0$；G是基点生成元。服务端生成椭圆曲线后，选择基点生成元G，满足它的阶是整数n。服务端生成的私钥sk和公钥pk满足pk＝sk*G。

[0073] 除了将服务端公钥池和服务端私钥池写入密钥卡的密钥区外，还会将身份私钥以及对应的身份公钥的指针地址和算法的相关参数{q,a,b,G,n}写入到密钥卡指定区域。

[0074] 非对称密钥颁发：

[0075] 非对称密钥颁发即密钥卡颁发，此流程全部在服务端进行。

[0076] 设ID为U的客户端为客户端CU，客户端CU的密钥卡内客户端私钥为kU。设客户端CU对应的服务端为SU，则U内包含SU的信息，代表CU的密钥卡由SU颁发。服务端根据匹配的密钥卡内的随机数发生器生成客户端公钥指针随机数rkU/rkSU。

[0077] 根据客户端私钥kU以及G计算得到RU＝kU*G。

[0078] 将rkU结合指针函数frk得到指针rkpU，通过rkpU在服务端公钥池中取出公钥pkU，在服务端私钥池中取出私钥skU。

[0079] 计算PU＝RU+pkU。

[0080] 根据PU和U得到客户端CU的隐式证书CertU＝Encode(PU,U)。Encode(*)是指一种包括了*信息的证书的组成和实际编码方式，具体根据应用而定。再对CertU进行哈希计算得到eU＝H(CertU)。

[0081] 将rkSU结合指针函数frk得到指针rkpSU，通过rkpSU在服务端公钥池中取出公钥pkSU，在服务端私钥池中取出私钥skSU。

[0082] 计算私钥参数rU＝eU*skU+skSU(mod n)。

[0083] 将服务端公钥池、客户端公钥指针随机数rkU/rkSU、客户端私钥kU以及私钥参数rU存入客户端密钥卡的对应存储区，完成对客户端的非对称密钥颁发即密钥卡颁发。

[0084] 客户端获取非对称密钥：

[0085] 客户端根据密钥卡内客户端私钥kU以及G计算得到RU＝kU*G。

[0086] 客户端提取卡内公钥指针随机数rkU，将rkU结合指针函数frk得到指针rkpU，通过rkpU在服务端公钥池中取出公钥pkU。

[0087] 计算PU＝RU+pkU。

[0088] 根据PU和U得到客户端CU的隐式证书CertU＝Encode(PU,U)。再对CertU进行哈希计算得到eU＝H(CertU)。

[0089] 计算得到实际的私钥dU＝eU*kU+rU(mod n)

[0090] 客户端提取卡内公钥指针随机数rkSU，将rkSU结合指针函数frk得到指针rkpSU，通过rkpSU在服务端公钥池中取出公钥pkSU。

[0091] 计算得到实际的公钥QU＝eU*PU+pkSU。也可以用QU＝dU*G计算得到实际的公钥QU。

[0092] 客户端将U、PU以及rkSU作为UINFO公布，UINFO可表示为U||PU||rkSU。U和rkSU不含有密码相关信息；由于PU＝RU+pkU，敌方无法获取RU或pkU任意一者的信息。因此UINFO无需加密即可抵抗量子计算。

[0093] 其他客户端获取公钥：

[0094] 其他客户端可根据UINFO中U和PU得到客户端CU的隐式证书CertU＝Encode(PU,U)。再对CertU进行哈希计算得到eU＝H(CertU)。

[0095] 根据UINFO中的rkSU结合指针函数frk得到指针rkpSU，通过rkpSU在服务端公钥池中取出公钥pkSU。

[0096] 计算得到实际公钥QU＝eU*PU+pkSU。

[0097] 实施例1

[0098] 系统说明

[0099] 本实施例包括客户端A、客户端B、服务端QA和服务端QB，结构如图3所示。QA和QB分别带有各自的密钥管理服务器。QA和QB有QKD通道。客户端A和客户端B配有客户端密钥卡，服务端QA和服务端QB配有服务端密钥卡。上述客户端A归属于服务端QA，即A的密钥卡由QA的密钥管理服务器所颁发，客户端A与服务端QA共享非对称密钥池对。客户端B归属于服务端QB，即B的密钥卡由QB的密钥管理服务器所颁发，客户端B与服务端QB共享非对称密钥池对。

[0100] 步骤1：

[0101] 客户端A根据匹配的密钥卡内的随机数发生器生成随机数RA，随机数RA结合指针函数f1得到指针PA1，通过PA1在服务端公钥池中取出公钥PKQA1。随机数RA结合指针函数f2得到指针PA2，通过PA2在服务端公钥池中取出公钥PKQA2。

[0102] 计算RAQ＝k*G-PKQA1，KAQ＝k*PKQA2。k为随机数。

[0103] 设待传输的消息为M，包括客户端A的信息AINFO、客户端B的信息BINFO以及消息内容MSG。M可表示为AINFO||BINFO||MSG。

[0104] 使用客户端A的私钥SKA对M进行签名得到SIGNAQ＝SIGN(M,SKA)，SIGN为一种ECC签名算法。

[0105] 使用KAQ对M和SIGNAQ加密得到CAQ＝ENC(M||SIGNAQ,KAQ)。ENC(m,K)表示使用K对

m进行对称加密。

[0106] 将RA、RAQ以及CAQ发送至服务端QA。

[0107] 步骤2：

[0108] 服务端QA收到RA||RAQ||CAQ后，根据随机数RA结合指针函数f1得到指针PA1，通过PA1在服务端公钥池中取出公钥PKQA1。根据随机数RA结合指针函数f2得到指针PA2，通过PA2在服务端私钥池中取出私钥SKQA2。

[0109] 计算RAQ'＝RAQ+PKQA1。由于PKQA2＝SKQA2*G，可计算KAQ＝SKQA2*RAQ'。

[0110] 使用KAQ对CAQ进行解密得到M和SIGNAQ。

[0111] 根据AINFO得到A的公钥PKA，使用PKA对SIGNAQ进行验证。

[0112] 验证通过后，使用与服务端QB通过QKD协商获得的密钥KQ对M进行加密及消息认证后发送至服务端QB。

[0113] 步骤3：

[0114] 服务端QB收到后，使用KQ对M进行解密，完成消息认证后，进行下一步。

[0115] 服务端QB根据匹配的密钥卡内的随机数发生器生成随机数RQ，随机数RQ结合指针函数f1得到指针PQ1，通过PQ1在服务端公钥池中取出公钥PKQB1。随机数RQ结合指针函数f2得到指针PQ2，通过PQ2在服务端私钥池中取出私钥SKQB2。

[0116] 计算RQB＝kQ*G-PKQB1，KQB＝kQ*PKB。kQ为随机数。

[0117] 使用SKQB2对M进行签名得到SIGNQB＝SIGN(M,SKQB2)。

[0118] 使用KQB对M和SIGNQB加密得到CQB＝ENC(M||SIGNQB,KQB)。

[0119] 将RQ、RQB以及CQB发送至客户端B。

[0120] 步骤4：

[0121] 客户端B收到RQ||RQB||CQB后，根据随机数RQ结合指针函数f1得到指针PQ1，通过PQ1在服务端公钥池中取出公钥PKQB1。根据随机数RQ结合指针函数f2得到指针PQ2，通过PQ2在服务端公钥池中取出公钥PKQB2。

[0122] 计算RQB'＝RQB+PKQB1，由于PKB＝SKB*G，计算KQB＝SKB*RQB'。

[0123] 使用KQB对CQB进行解密得到M和SIGNQB。

[0124] 使用PKQB2对SIGNQB进行验证。

[0125] 验证通过后，客户端B得到并信任客户端A发送的消息MSG。

[0126] 实施例2

[0127] 本实施例包括客户端A、客户端B和服务端Q，结构如图4所示。服务端Q带有密钥管理服务器。客户端A和客户端B配有客户端密钥卡，服务端Q配有服务端密钥卡。上述客户端A和客户端B都归属于服务端Q，即客户端A和客户端B的密钥卡都由服务端Q的密钥管理服务器所颁发，客户端A与服务端Q共享非对称密钥池对，客户端B与服务端Q也共享非对称密钥池对。

[0128] 步骤1：

[0129] 客户端A根据匹配的密钥卡内的随机数发生器生成随机数RA，随机数RA结合指针函数f1得到指针PA1，通过PA1在服务端公钥池中取出公钥PKQA1。随机数RA结合指针函数f2得到指针PA2，通过PA2在服务端公钥池中取出公钥PKQA2。

[0130] 计算RAQ＝k*G-PKQA1，KAQ＝k*PKQA2。

[0131] 设待传输的消息为M,包括客户端A的信息AINFO、客户端B的信息BINFO以及消息内容MSG。M可表示为AINFO||BINFO||MSG。

[0132] 使用客户端A的私钥SKA对M进行签名得到SIGNAQ＝SIGN(M,SKA),SIGN为一种ECC签名算法。

[0133] 使用KAQ对M和SIGNAQ加密得到CAQ＝ENC(M||SIGNAQ,KAQ)。

[0134] 将RA、RAQ以及CAQ发送至服务端Q。

[0135] 步骤2：

[0136] 服务端Q收到RA||RAQ||CAQ后,根据随机数RA结合指针函数f1得到指针PA1,通过PA1在服务端公钥池中取出公钥PKQA1。根据随机数RA结合指针函数f2得到指针PA2,通过PA2在服务端私钥池中取出私钥SKQA2。

[0137] 计算RAQ'＝RAQ+PKQA1。由于PKQA2＝SKQA2*G,可计算KAQ＝SKQA2*RAQ'。

[0138] 使用KAQ对CAQ进行解密得到M和SIGNAQ。

[0139] 根据AINFO得到A的公钥PKA,使用PKA对SIGNAQ进行验证。

[0140] 验证通过后,服务端Q根据根据匹配的密钥卡内的随机数发生器生成随机数RQ,随机数RQ结合指针函数f1得到指针PQ1,通过PQ1在服务端公钥池中取出公钥PKQB1。随机数RQ结合指针函数f2得到指针PQ2,通过PQ2在服务端私钥池中取出私钥SKQB2。

[0141] 计算RQB＝kQ*G-PKQB1,KQB＝kQ*PKB。kQ为随机数。

[0142] 使用SKQB2对M进行签名得到SIGNQB＝SIGN(M,SKQB2)。

[0143] 使用KQB对M和SIGNQB加密得到CQB＝ENC(M||SIGNQB,KQB)。

[0144] 将RQ、RQB以及CQB发送至客户端B。

[0145] 步骤3：

[0146] 客户端B收到RQ||RQB||CQB后,根据随机数RQ结合指针函数f1得到指针PQ1,通过PQ1在服务端公钥池中取出公钥PKQB1。根据随机数RQ结合指针函数f2得到指针PQ2,通过PQ2在服务端公钥池中取出公钥PKQB2。

[0147] 计算RQB'＝RQB+PKQB1,由于PKB＝SKB*G,计算KQB＝SKB*RQB'。

[0148] 使用KQB对CQB进行解密得到M和SIGNQB。

[0149] 使用PKQB2对SIGNQB进行验证。

[0150] 验证通过后,客户端B得到并信任客户端A发送的消息MSG。

[0151] 结论

[0152] 本发明中,使用的密钥卡是独立的硬件隔离设备。公钥、私钥和其他相关参数均存储在密钥卡中的数据安全区,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。由于在经典网络中均无涉及公私钥及算法参数的明文传递,因此非对称密钥被破解的风险很低。密钥卡保障了通信双方的通信安全,也极大的提高了身份认证的安全性。同时非对称密钥池解决了对称密钥池给服务端带来密钥存储压力,降低了存储成本。例如,原先用户的对称密钥池大小均为1G,用户个数为N,则服务端需要存储NG的密钥池;而如果存储非对称密钥池,客户端存储服务端公钥池大小为1G,服务端同样只需要存储1G大小的服务端私钥池。由于密钥量大大下降,所有密钥可以存储在安全性更高的密钥卡内,且给密钥备份提供了便利。

[0153] 另外,由于用户的个人密钥由原先的对称密钥池改为非对称密钥,因此给密钥更

新带来便利。如本专利实施例所示，用户可以通过实施例中的保密通信方法，以本地更新的密钥为消息，与服务端进行保密通信，从而快速在线更新个人密钥，解决了对称密钥池由于容量过大而无法快速在线更新的不便。

[0154] 同时，本专利对基于隐式证书的保密通信方法，使用隐式证书隐式地对公钥的可信度进行证明，使用非对称密钥和数字签名对用户的身份进行证明，保密通信的收发双方都能明确对方的身份，其他任何人均无法对保密通信进行干预或仿冒。由于非对称密钥均未公开，而公开的用户信息中无法获取密钥，因此本文的非对称密钥使用方式具有抗量子计算的特性。

[0155] 最后，本专利对非对称密码学加密流程进行改进，对容易被量子计算机破解的密文参数(k*G)进行偏移量计算(例如:RAQ＝k*G-PKQA1)，该偏移量只能被基于加密者群组的服务端公钥池中的密钥进行偏移量恢复，即使量子计算机也无法得到k，即本文的非对称密码学加密流程具有抗量子计算的特性。而常规做法是，对密文参数进行对称加密计算，其计算量大大高于本专利的偏移量计算。因此本专利的偏移量计算是一种更优的抗量子计算方式。

[0156] 以上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。

[0157] 以上所述实施例仅表达了本申请的几种实施方式，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，在不脱离本申请构思的前提下，还可以做出若干变形和改进，这些都属于本申请的保护范围。因此，本申请专利的保护范围应以所附权利要求为准。

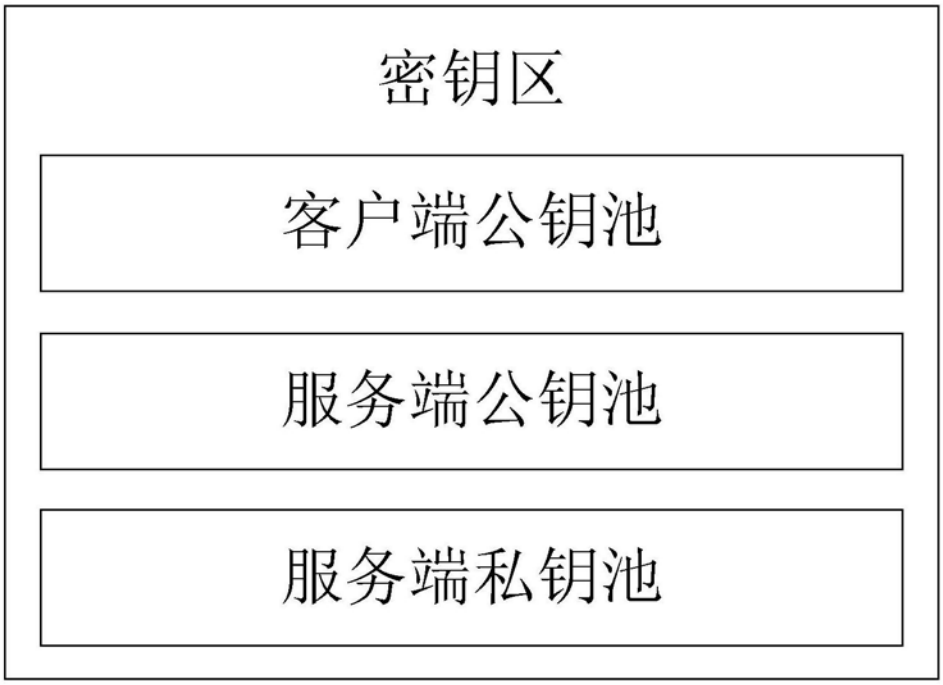


图1

图2

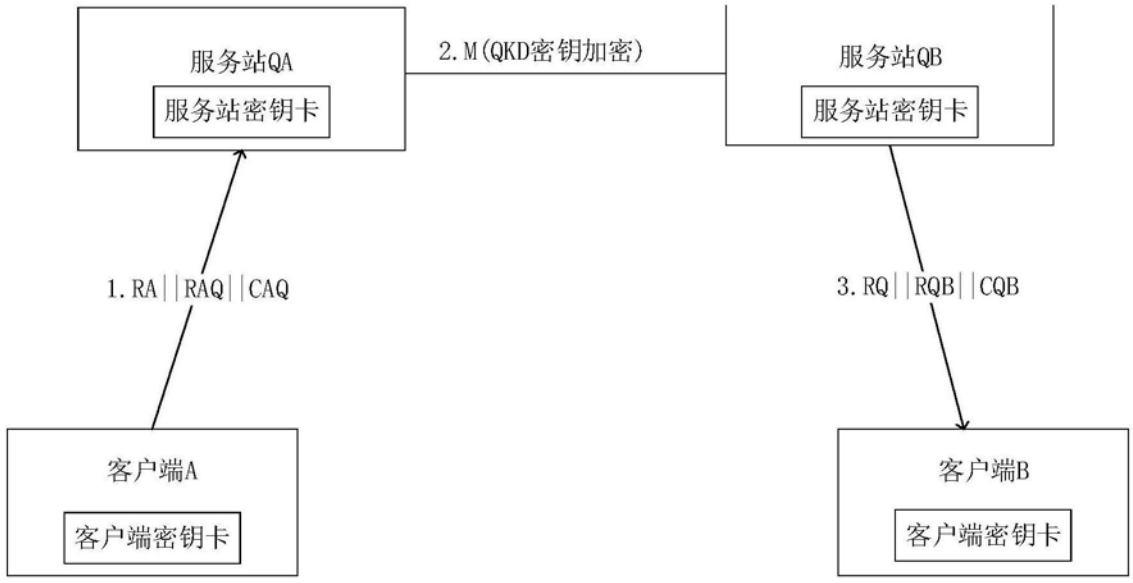

服务站QA
服务站密钥卡
2.M(QKD密钥加密)
服务站QB
服务站密钥卡
1.RA||RAQ||CAQ
3.RQ||RQB||CQB
客户端A
客户端密钥卡
客户端B
客户端密钥卡

图3

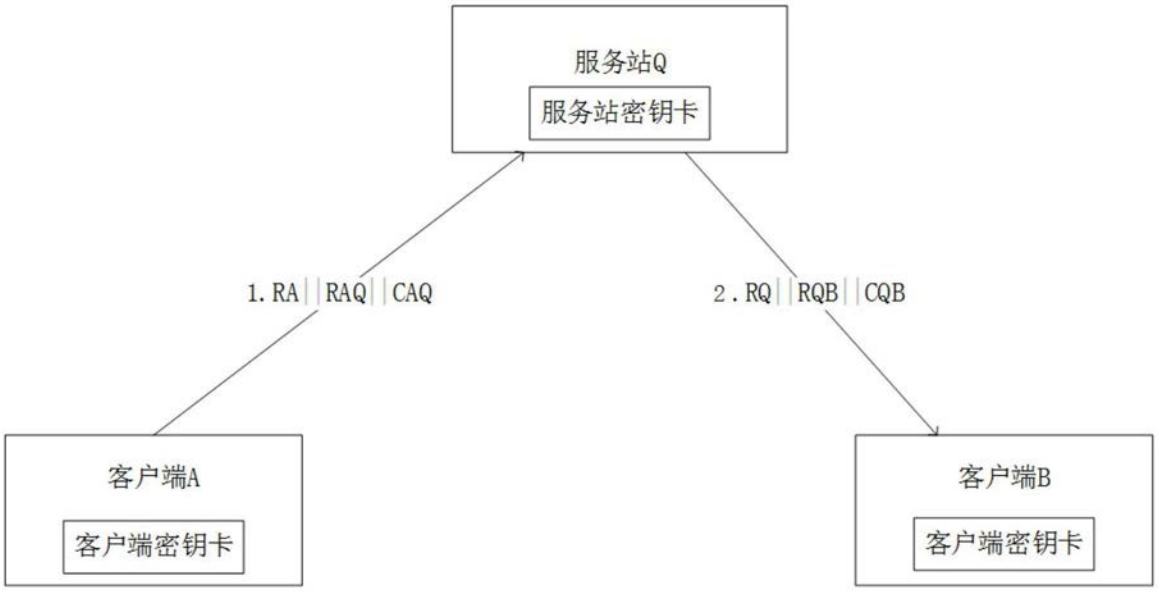

服务站Q
服务站密钥卡
1.RA||RAQ||CAQ
2.RQ||RQB||CQB
客户端A
客户端密钥卡
客户端B
客户端密钥卡

图4