(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 109787758 A
(43)申请公布日 2019.05.21

(21)申请号 201910049038.0

(22)申请日 2019.01.18

(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.
H04L 9/08(2006.01)

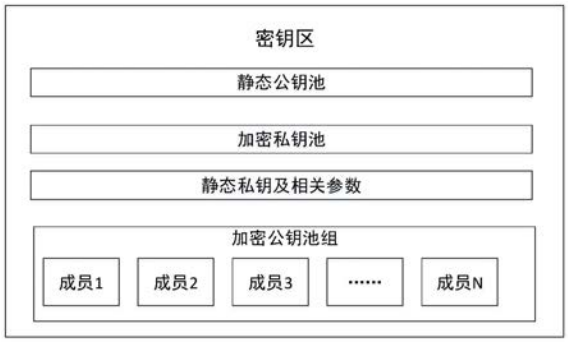
权利要求书3页 说明书10页 附图3页

(54)发明名称

基于私钥池和Elgamal的抗量子计算MQV密钥协商方法和系统

(57)摘要

本发明涉及一种基于私钥池和Elgamal的抗量子计算MQV密钥协商方法，参与方配置有密钥卡，实施所述抗量子计算MQV密钥协商方法时，包括：在己方生成相应的临时公钥和临时私钥，用加密私钥和对方的加密公钥生成共享密钥，并利用共享密钥加密己方的临时公钥得到密文；将所述密文，用于得到对方加密公钥的真随机数，和己方的静态公钥指针地址以密文形式发送给对方；接收方利用己方的加密私钥和对方的加密公钥生成共享密钥，利用共享密钥解密所述密文得到对方的临时公钥，利用所述静态公钥指针地址得到对方的静态公钥，并利用对方的临时公钥、静态公钥，和己方临时私钥、临时公钥、静态私钥以及算法参数生成协商密钥。



CN 109787758 A

1.基于私钥池和Elgamal的抗量子计算MQV密钥协商方法，其特征在于，参与方配置有密钥卡，密钥卡内存储有静态公钥池、加密私钥池、加密公钥池组以及静态私钥和算法参数，所述加密私钥池存储有加密私钥，所述加密公钥池组包括数量与密钥卡数量相对应的加密公钥池，各加密公钥池中存储有与所述加密私钥相对应的加密公钥，所述静态公钥池中存储有与所述静态私钥相对应的静态公钥；

实施所述抗量子计算MQV密钥协商方法时，包括：

在己方生成相应的临时公钥和临时私钥，用加密私钥和对方的加密公钥生成共享密钥，并利用共享密钥加密己方的临时公钥得到密文；将所述密文，用于得到对方加密公钥的真随机数，和己方的静态公钥指针地址以密文形式发送给对方；

接收来自对方的所述密文，所述真随机数，和所述静态公钥指针地址，利用所述真随机数得到对方的加密公钥和己方的加密私钥，利用己方的加密私钥和对方的加密公钥生成共享密钥，利用共享密钥解密所述密文得到对方的临时公钥，利用所述静态公钥指针地址得到对方的静态公钥，并利用对方的临时公钥、静态公钥，和己方临时私钥、临时公钥、静态私钥以及算法参数生成协商密钥。

2.如权利要求1所述的基于私钥池和Elgamal的抗量子计算MQV密钥协商方法，其特征在于，所述参与方包括发起方和响应方，在所述发起方包括：

生成第一真随机数，利用第一真随机数生成第一临时公钥和第一临时私钥；

生成第二真随机数，利用第二真随机数从所述密钥卡中得到己方的第一加密私钥和对方的第一加密公钥；

将己方的第一加密私钥和对方的第一加密公钥进行运算得到第一共享密钥，并利用第一共享密钥加密所述第一临时公钥得到第一密文；

将所述第一密文，第二真随机数，己方的静态公钥指针地址和己方的加密公钥池编号以密文形式发送给响应方。

3.如权利要求2所述的基于私钥池和Elgamal的抗量子计算MQV密钥协商方法，其特征在于，在所述响应方包括：

利用接收的第二真随机数从所述密钥卡中得到己方的第一加密私钥和对方的第一加密公钥；

将己方的第一加密私钥和对方的第一加密公钥进行运算得到第一共享密钥，并利用第一共享密钥解密所述第一密文得到对方的第一临时公钥；

利用接收的静态公钥指针地址从所述密钥卡中得到对方的第一静态公钥；

生成第三真随机数，利用第三真随机数生成第二临时公钥和第二临时私钥；

从密钥卡中得到己方的第二静态私钥，并相应计算出协商密钥；

生成第四真随机数，利用第四真随机数从所述密钥卡中得到己方的第二加密私钥和对方的第二加密公钥；

将己方的第二加密私钥和对方的第二加密公钥进行运算得到第二共享密钥，并利用第二共享密钥加密所述第二临时公钥得到第二密文；

将所述第二密文，第四真随机数，己方的静态公钥指针地址以密文形式发送给发起方。

4.如权利要求3所述的基于私钥池和Elgamal的抗量子计算MQV密钥协商方法，其特征在于，在所述响应方，计算出协商密钥的方式为：

协商密钥为K且$K = h \cdot Sb(Ka' + \overline{Ka'}A)$;其中：

h为密钥卡中的所述算法参数；

$$Sb = kb + (\overline{Kb})b;$$

kb为响应方的第二临时私钥；

Kb为响应方的第二临时公钥；

b为响应方的第二静态私钥；

Ka'为发起方的第一临时公钥；

A为发起方的第一静态公钥。

5.如权利要求3所述的基于私钥池和Elgamal的抗量子计算MQV密钥协商方法，其特征在于，在所述发起方还包括：

利用接收的第四真随机数从所述密钥卡中得到己方的第二加密私钥和对方的第二加密公钥；

将己方的第二加密私钥和对方的第二加密公钥进行运算得到第二共享密钥，并利用第二共享密钥解密所述第二密文得到对方的第二临时公钥；

利用接收的静态公钥指针地址从所述密钥卡中得到对方的第二静态公钥；

从密钥卡中得到己方的第一静态私钥，相应计算出协商密钥。

6.如权利要求5所述的基于私钥池和Elgamal的抗量子计算MQV密钥协商方法，其特征在于，在所述发起方，计算出协商密钥的方式为：

协商密钥为K'且$K' = h \cdot Sa(Kb' + \overline{Kb'}B)$;其中：

h为密钥卡中的所述算法参数；

$$Sa = ka + (\overline{Ka})a;$$

ka为发起方的第一临时私钥；

Ka为发起方的第一临时公钥；

a为发起方的第一静态私钥；

Kb'为响应方的第二临时公钥；

B为响应方的第二静态公钥。

7.基于私钥池和Elgamal的抗量子计算MQV密钥协商系统，其特征在于，参与方配置有密钥卡，密钥卡内存储有静态公钥池、加密私钥池、加密公钥池组以及静态私钥和算法参数，所述加密私钥池存储有加密私钥，所述加密公钥池组包括数量与密钥卡数量相对应的加密公钥池，各加密公钥池中存储有与所述加密私钥相对应的加密公钥，所述静态公钥池中存储有与所述静态私钥相对应的静态公钥；

所述抗量子计算MQV密钥协商系统，包括：

第一模块，用于在己方生成相应的临时公钥和临时私钥，用加密私钥和对方的加密公钥生成共享密钥，并利用共享密钥加密己方的临时公钥得到密文；将所述密文，用于得到对方加密公钥的真随机数，和己方的静态公钥指针地址以密文形式发送给对方；

第二模块，用于接收来自对方的所述密文，所述真随机数，和所述静态公钥指针地址，利用所述真随机数得到对方的加密公钥和己方的加密私钥，利用己方的加密私钥和对方的

加密公钥生成共享密钥，利用共享密钥解密所述密文得到对方的临时公钥，利用所述静态公钥指针地址得到对方的静态公钥，并利用对方的临时公钥、静态公钥，和己方临时私钥、临时公钥、静态私钥以及算法参数生成协商密钥。

8.基于私钥池和Elgamal的抗量子计算MQV密钥协商系统，其特征在于，参与方配置有密钥卡，密钥卡内存储有静态公钥池、加密私钥池、加密公钥池组以及静态私钥和算法参数，所述加密私钥池存储有加密私钥，所述加密公钥池组包括数量与密钥卡数量相对应的加密公钥池，各加密公钥池中存储有与所述加密私钥相对应的加密公钥，所述静态公钥池中存储有与所述静态私钥相对应的静态公钥；

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1～6任一项所述的基于私钥池和Elgamal的抗量子计算MQV密钥协商方法。

基于私钥池和Elgamal的抗量子计算MQV密钥协商方法和系统

技术领域

[0001] 本发明涉及公钥密码体制和私钥池技术，具体涉及群组内通信双方间的密钥交换技术。

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] 当前保证网络信息安全的关键技术就是密码技术，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。

[0004] 对称密钥密码系统的安全性依赖以下两个因素。第一，加密算法必须是足够强的，仅仅基于密文本身去解密信息在实践上是不可能的；第二，加密方法的安全性来自于密钥的秘密性，而不是算法的秘密性。对称加密系统最大的问题是密钥的分发和管理非常复杂、代价高昂。对称加密算法另一个缺点是不容易实现数字签名。所以，在当今的移动电子商务领域中的加密算法实现主要是依赖于公开密钥体制。

[0005] 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。

[0006] 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。根据所基于的数学难题来分类，有以下三类系统目前被认为是安全和有效的：大整数因子分解系统(代表性的有RSA)、离散对数系统(代表性的有DSA)和椭圆离散对数系统(ECC)。

[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。

发明内容

[0008] 本发明提供一种安全性更高的基于私钥池和Elgamal的抗量子计算MQV密钥协商方法和系统。

[0009] 本发明基于私钥池和Elgamal的抗量子计算MQV密钥协商方法，参与方配置有密钥卡，密钥卡内存储有静态公钥池、加密私钥池、加密公钥池组以及静态私钥和算法参数，所述加密私钥池存储有加密私钥，所述加密公钥池组包括数量与密钥卡数量相对应的加密公钥池，各加密公钥池中存储有与所述加密私钥相对应的加密公钥，所述静态公钥池中存储有与所述静态私钥相对应的静态公钥；

[0010] 实施所述抗量子计算MQV密钥协商方法时，包括：

[0011] 在己方生成相应的临时公钥和临时私钥，用加密私钥和对方的加密公钥生成共享密钥，并利用共享密钥加密己方的临时公钥得到密文；将所述密文，用于得到对方加密公钥的真随机数，和己方的静态公钥指针地址以密文形式发送给对方；

[0012] 接收来自对方的所述密文，所述真随机数，和所述静态公钥指针地址，利用所述真随机数得到对方的加密公钥和己方的加密私钥，利用己方的加密私钥和对方的加密公钥生成共享密钥，利用共享密钥解密所述密文得到对方的临时公钥，利用所述静态公钥指针地址得到对方的静态公钥，并利用对方的临时公钥、静态公钥，和己方临时私钥、临时公钥、静态私钥以及算法参数生成协商密钥。

[0013] 可选的，所述参与方包括发起方和响应方，在所述发起方包括：

[0014] 生成第一真随机数，利用第一真随机数生成第一临时公钥和第一临时私钥；

[0015] 生成第二真随机数，利用第二真随机数从所述密钥卡中得到己方的第一加密私钥和对方的第一加密公钥；

[0016] 将己方的第一加密私钥和对方的第一加密公钥进行运算得到第一共享密钥，并利用第一共享密钥加密所述第一临时公钥得到第一密文；

[0017] 将所述第一密文，第二真随机数，己方的静态公钥指针地址和己方的加密公钥池编号以密文形式发送给响应方。

[0018] 可选的，在所述响应方包括：

[0019] 利用接收的第二真随机数从所述密钥卡中得到己方的第一加密私钥和对方的第一加密公钥；

[0020] 将己方的第一加密私钥和对方的第一加密公钥进行运算得到第一共享密钥，并利用第一共享密钥解密所述第一密文得到对方的第一临时公钥；

[0021] 利用接收的静态公钥指针地址从所述密钥卡中得到对方的第一静态公钥；

[0022] 生成第三真随机数，利用第三真随机数生成第二临时公钥和第二临时私钥；

[0023] 从密钥卡中得到己方的第二静态私钥，并相应计算出协商密钥；

[0024] 生成第四真随机数，利用第四真随机数从所述密钥卡中得到己方的第二加密私钥和对方的第二加密公钥；

[0025] 将己方的第二加密私钥和对方的第二加密公钥进行运算得到第二共享密钥，并利用第二共享密钥加密所述第二临时公钥得到第二密文；

[0026] 将所述第二密文，第四真随机数，己方的静态公钥指针地址以密文形式发送给发起方。

[0027] 可选的，在所述响应方，计算出协商密钥的方式为：

[0028] 协商密钥为K且$K = h \cdot Sb(Ka' + \overline{Ka'}A)$；其中：

[0029] h为密钥卡中的所述算法参数；

[0030] $Sb = kb + (\overline{Kb})b$；

[0031] kb为响应方的第二临时私钥；

[0032] Kb为响应方的第二临时公钥；

[0033] b为响应方的第二静态私钥；

[0034] Ka'为发起方的第一临时公钥；

[0035] A为发起方的第一静态公钥。

[0036] 可选的，在所述发起方还包括：

[0037] 利用接收的第四真随机数从所述密钥卡中得到己方的第二加密私钥和对方的第二加密公钥；

[0038] 将己方的第二加密私钥和对方的第二加密公钥进行运算得到第二共享密钥，并利用第二共享密钥解密所述第二密文得到对方的第二临时公钥；

[0039] 利用接收的静态公钥指针地址从所述密钥卡中得到对方的第二静态公钥；

[0040] 从密钥卡中得到己方的第一静态私钥，相应计算出协商密钥。

[0041] 可选的，在所述发起方，计算出协商密钥的方式为：

[0042] 协商密钥为K'且$K' = h \cdot Sa(Kb' + \overline{Kb'}B)$；其中：

[0043] h为密钥卡中的所述算法参数；

[0044] $Sa = ka + (\overline{Ka})a$；

[0045] ka为发起方的第一临时私钥；

[0046] Ka为发起方的第一临时公钥；

[0047] a为发起方的第一静态私钥；

[0048] Kb'为响应方的第二临时公钥；

[0049] B为响应方的第二静态公钥。

[0050] 本发明还提供一种基于私钥池和Elgamal的抗量子计算MQV密钥协商系统，参与方配置有密钥卡，密钥卡内存储有静态公钥池、加密私钥池、加密公钥池组以及静态私钥和算法参数，所述加密私钥池存储有加密私钥，所述加密公钥池组包括数量与密钥卡数量相对应的加密公钥池，各加密公钥池中存储有与所述加密私钥相对应的加密公钥，所述静态公钥池中存储有与所述静态私钥相对应的静态公钥；

[0051] 所述抗量子计算MQV密钥协商系统，包括：

[0052] 第一模块，用于在己方生成相应的临时公钥和临时私钥，用加密私钥和对方的加密公钥生成共享密钥，并利用共享密钥加密己方的临时公钥得到密文；将所述密文，用于得到对方加密公钥的真随机数，和己方的静态公钥指针地址以密文形式发送给对方；

[0053] 第二模块，用于接收来自对方的所述密文，所述真随机数，和所述静态公钥指针地址，利用所述真随机数得到对方的加密公钥和己方的加密私钥，利用己方的加密私钥和对方的加密公钥生成共享密钥，利用共享密钥解密所述密文得到对方的临时公钥，利用所述静态公钥指针地址得到对方的静态公钥，并利用对方的临时公钥、静态公钥，和己方临时私钥、临时公钥、静态私钥以及算法参数生成协商密钥。

[0054] 本发明还提供一种基于私钥池和Elgamal的抗量子计算MQV密钥协商系统，参与方配置有密钥卡，密钥卡内存储有静态公钥池、加密私钥池、加密公钥池组以及静态私钥和算法参数，所述加密私钥池存储有加密私钥，所述加密公钥池组包括数量与密钥卡数量相对应的加密公钥池，各加密公钥池中存储有与所述加密私钥相对应的加密公钥，所述静态公钥池中存储有与所述静态私钥相对应的静态公钥；

[0055] 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私钥池和Elgamal的抗量子计算MQV密钥协商方法。

[0056] 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服务器内生成，再分配给密钥卡，相应的密钥池和私钥及参数均存储在指定安全区域，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。由于在网络中传输的公钥只有临时公钥，且临时公钥是被加密传输的，加密所用的公私钥是从非对称密钥池组中选取的，外界无法获得，因此该公钥被破解的概率极低。在网络中传输的其他数据仅是密钥位置相关的参数，无法独立计算得到密钥，因此本发明的密钥协商方法的安全性相对经典的ECMQV密钥协商方法要高很多。也保证了后续的通信双方的消息的安全性。

附图说明

[0057] 图1为本发明中密钥池的分布示意图；

[0058] 图2为实施例的密钥协商流程图；

[0059] 图3为计算私钥和公钥的流程示意图。

具体实施方式

[0060] 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。

[0061] 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。

[0062] 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。

[0063] 本发明实现场景为在一个非对称密码体系的群组中的任意两个对象甲、乙。本发明中的群组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。群组中每个密钥卡具有多个密钥池，分别是静态公钥池、加密私钥池和加密公钥池组以及静态私钥和相关参数。加密公钥池组的个数为群组内所有成员的个数，加密公钥池组即群组内各成员对应的加密公钥池的集合。具体密钥卡内的分布如图1所示。本发明中，对象甲和对象乙的本地系统中都存在相应需求的算法。

[0064] 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。

[0065] 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同一个密钥管理服务站，且对同一群组密钥卡的主管方来说，其颁发的每个密钥卡中存储的公钥密钥池组是完全一致的。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。

[0066] 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。

[0067] 密钥卡在充值密钥池时，密钥管理服务器会指定密钥卡一个群组身份，并给予群组内的ID。服务器在创建一个群组时会定义一个素数p，p满足p>3。并且生成两个小于p的非负整数，参数α和参数β，用于构建一个椭圆曲线E：$\gamma^2=x^3+\alpha x+\beta$。另外设椭圆曲线的阶为n，以及假设h为辅助因子，该椭圆曲线的元点即基点为Q。设群组成员个数为N。服务器会产生N个真随机数作为静态私钥，并计算得到相应的公钥，将这些公钥写入到同一个文件内组成静态公钥文件，即静态公钥池。上述所得公私钥用于作为ECMQV算法的静态公私钥。服务器会再利用生成元g产生一个q阶循环群G的有效描述。该循环群需要满足一定的安全性质。同时产生大数据量的处于{1,…,q-1}范围的随机数作为加密私钥，并组成加密私钥池，所产生的加密私钥池个数为N。并根据加密私钥计算得到相应的加密公钥，并组成对应的加密公钥池。每个加密公钥池内加密公钥的位置都与对应加密私钥池内对应加密私钥的位置相同。

[0068] 在密钥卡注册时，服务器会将静态公钥文件、未分配的加密私钥池以及加密公钥池组一并存储在密钥卡内。同时将未分配的静态私钥中随机选取一个分配给该密钥卡并将对应的静态公钥指针地址存储在密钥卡内，静态公钥指针地址用于查找与静态私钥成对的公钥。另外，密钥卡内还存放有己方加密公钥池编号，以及相关的算法参数椭圆曲线域参数{p,α,β,Q,n,h}和{g,q,G}。

[0069] 设本系统密钥协商的对象分别为对象甲和对象乙。对象甲为密钥协商的主动方(发起方)，对象乙为密钥协商的配合方(响应方)。设对象甲对应的静态公私钥对为(A,a)，公钥为A，私钥为a；设对象乙对应的静态公私钥对为(B,b)，公钥为B，私钥为b；设对象甲的加密非对称密钥池所对应的加密公私钥对为(Ki,ki)，公钥为Ki，私钥为ki，公钥Ki的计算方式为$Ki=g^{ki} \bmod q$；设对象乙的加密非对称密钥池所对应的加密公私钥对为(Kj,kj)，公钥为Kj，私钥为kj，公钥Kj的计算方式为$Kj=g^{kj} \bmod q$。本发明中，加密算法为Elgamal加密算法。

[0070] 其中一实施例中，提供一种基于私钥池和Elgamal的抗量子计算MQV密钥协商方法，参与方配置有密钥卡，密钥卡内存储有静态公钥池、加密私钥池、加密公钥池组以及静态私钥和算法参数，所述加密私钥池存储有加密私钥，所述加密公钥池组包括数量与密钥

卡数量相对应的加密公钥池，各加密公钥池中存储有与所述加密私钥相对应的加密公钥，所述静态公钥池中存储有与所述静态私钥相对应的静态公钥；

[0071] 实施所述抗量子计算MQV密钥协商方法时，包括：

[0072] 在己方生成相应的临时公钥和临时私钥，用加密私钥和对方的加密公钥生成共享密钥，并利用共享密钥加密己方的临时公钥得到密文；将所述密文，用于得到对方加密公钥的真随机数，和己方的静态公钥指针地址以密文形式发送给对方；

[0073] 接收来自对方的所述密文，所述真随机数，和所述静态公钥指针地址，利用所述真随机数得到对方的加密公钥和己方的加密私钥，利用己方的加密私钥和对方的加密公钥生成共享密钥，利用共享密钥解密所述密文得到对方的临时公钥，利用所述静态公钥指针地址得到对方的静态公钥，并利用对方的临时公钥、静态公钥，和己方临时私钥、临时公钥、静态私钥以及算法参数生成协商密钥。

[0074] 所述参与方包括发起方和响应方，协商密钥的具体流程主要分三个阶段。

[0075] 第一阶段，在所述发起方包括：

[0076] 生成第一真随机数，利用第一真随机数生成第一临时公钥和第一临时私钥；

[0077] 生成第二真随机数，利用第二真随机数从所述密钥卡中得到己方的第一加密私钥和对方的第一加密公钥；

[0078] 将第一加密私钥和对方的第一加密公钥进行运算得到第一共享密钥，并利用第一共享密钥加密所述第一临时公钥得到第一密文；

[0079] 将所述第一密文，第二真随机数，己方的静态公钥指针地址和己方的加密公钥池编号以密文形式发送给响应方。

[0080] 第二阶段，在所述响应方包括：

[0081] 利用接收的第二真随机数从所述密钥卡中得到己方的第一加密私钥和对方的第一加密公钥；

[0082] 将第一加密私钥和对方的第一加密公钥进行运算得到第一共享密钥，并利用第一共享密钥解密所述第一密文得到对方的第一临时公钥；

[0083] 利用接收的静态公钥指针地址从所述密钥卡中得到对方的第一静态公钥；

[0084] 生成第三真随机数，利用第三真随机数生成第二临时公钥和第二临时私钥；

[0085] 从密钥卡中得到己方的第二静态私钥，并相应计算出协商密钥，计算出协商密钥的方式为：

[0086] 协商密钥为K且$K = h \cdot Sb(Ka' + \overline{Ka'}A)$；其中：

[0087] h为密钥卡中的所述算法参数；

[0088] $Sb = kb + (\overline{Kb})b$；

[0089] kb为响应方的第二临时私钥；

[0090] Kb为响应方的第二临时公钥；

[0091] b为响应方的第二静态私钥；

[0092] Ka’为发起方的第一临时公钥；

[0093] A为发起方的第一静态公钥；

[0094] 生成第四真随机数，利用第四真随机数从所述密钥卡中得到己方的第二加密私钥

和对方的第二加密公钥；

[0095] 将第二加密私钥和对方的第二加密公钥进行运算得到第二共享密钥，并利用第二共享密钥加密所述第二临时公钥得到第二密文；

[0096] 将所述第二密文，第四真随机数，己方的静态公钥指针地址以密文形式发送给发起方。

[0097] 第三阶段，在所述发起方还包括：

[0098] 利用接收的第四真随机数从所述密钥卡中得到己方的第二加密私钥和对方的第二加密公钥；

[0099] 将第二加密私钥和对方的第二加密公钥进行运算得到第二共享密钥，并利用第二共享密钥解密所述第二密文得到对方的第二临时公钥；

[0100] 利用接收的静态公钥指针地址从所述密钥卡中得到对方的第二静态公钥；

[0101] 从密钥卡中得到己方的第一静态私钥，相应计算出协商密钥，计算出协商密钥的方式为：

[0102] 协商密钥为K’且$K' = h \cdot Sa(Kb' + \overline{Kb'}B)$;其中：

[0103] h为密钥卡中的所述算法参数；

[0104] $Sa = ka + (\overline{Ka})a$;

[0105] ka为发起方的第一临时私钥；

[0106] Ka为发起方的第一临时公钥；

[0107] a为发起方的第一静态私钥；

[0108] Kb’为响应方的第二临时公钥；

[0109] B为响应方的第二静态公钥。

[0110] 以下结合附图2～图3，提供另一实施例，基于私钥池和Elgamal的抗量子计算MQV密钥协商方法，包括：

[0111] 步骤1:对象甲生成临时公私钥并将相关参数发送至对象乙

[0112] 1.1对象甲生成临时私钥:对象甲随机生成一个真随机数ka(第一真随机数)作为本次密钥协商的临时私钥ka(第一临时私钥)，并计算得到临时公钥Ka＝(ka)Q(第一临时公钥)，Q为椭圆曲线域参数之一。

[0113] 1.2对象甲取加密私钥和乙方加密公钥:对象甲产生一个真随机数r1(第二真随机数)。对象甲将随机数r1通过指定算法拆分成ri1和rj1。对象甲将ri1通过密钥指针算法fkp得到加密私钥指针地址kpi1。对象甲根据加密私钥指针地址kpi1从本地系统的加密私钥池中取出相应的加密私钥ki1(甲方的第一加密私钥)。

[0114] 同时，对象甲将rj1通过非对称密钥指针函数fkp计算得到对象乙的加密公钥指针地址kpj1。对象甲根据加密公钥指针地址kpj1和对象乙的加密公钥池编号Pj，从本地系统中的加密公钥密钥池组中取出乙方加密公钥Kj1(乙方的第一加密公钥)。对象乙的加密公钥池编号Pj是通过访问服务器或者向对象乙直接请求得到的。

[0115] 1.3对象甲加密临时公钥:对象甲生成共享密钥s1＝Kj1^ki1(第一共享密钥)。对象甲对临时公钥Ka加密后得到第一密文c1＝{Ka}·s1。

[0116] 1.4对象甲将密钥协商消息发送到对象乙:对象甲将临时公钥密文c1、随机数r1、

对象甲的静态公钥指针地址ra和对象甲的加密公钥池编号Pi加密发送到对象乙。

[0117] 步骤2:对象乙解密解析消息,计算得到协商密钥并将相关参数发送至对象甲

[0118] 2.1对象乙接收消息并解密解析:对象乙接收到来自对象甲的消息,对其进行解密解析得到对象甲的静态公钥指针地址ra'、对象甲的加密公钥池编号Pi'、随机数r1'和临时公钥密文c1'。

[0119] 2.2对象乙取得加密私钥和甲方加密公钥:对象乙将随机数r1'通过指定算法拆分成ri1'和rj1'。对象乙将rj1'通过密钥指针算法fkp得到加密私钥指针地址kpj1'。对象乙根据加密私钥指针地址kpj1'从本地系统的加密私钥池中取出相应的加密私钥kj1(乙方的第一加密私钥)。

[0120] 同时,对象乙将ri1'通过非对称密钥指针函数fkp计算得到对象甲的加密公钥指针地址kpi1'。对象乙根据加密公钥指针地址kpi1'和对象甲的加密公钥池编号Pi'从本地系统中的加密公钥密钥池组中取出甲方公钥Ki1(甲方的第一加密公钥)。

[0121] 2.3对象乙解密得到甲方临时公钥并取出甲方静态公钥:对象乙计算共享密钥s1'=Ki1^kj1。对象乙利用共享密钥s1'对临时公钥密文c1'解密得到甲方第一临时公钥Ka'=c1'·s1'-1。s1-1是s1在循环群G上的逆元。对象乙利用对象甲的静态公钥指针地址ra'从静态公钥池中取出对象甲的静态公钥A(第一静态公钥)。

[0122] 2.4对象乙生成临时私钥并取出自身静态私钥:对象乙随机生成一个真随机数kb(第三真随机数)作为本次密钥协商的临时私钥,计算得到临时公钥Kb=(kb)Q(第二临时公钥)。对象乙取出自身静态私钥b(第二静态私钥)。

[0123] 2.5对象乙计算得到协商密钥:对象乙利用已有的参数计算得到$Sb = kb + (\overline{Kb})b$。其中$\overline{Kb} = (kb \bmod 2^L) + 2^L$,且$L = \left\lceil \frac{\lfloor \log_2 n \rfloor + 1}{2} \right\rceil$。对象乙通过计算得到协商密钥$K = h \cdot Sb(Ka' + \overline{Ka'}A)$。

[0124] 2.6对象乙取得加密私钥和甲方加密公钥:对象乙产生一个真随机数r2(第四真随机数)。对象乙将随机数r2通过指定算法拆分成ri2和rj2。对象乙将rj2通过密钥指针算法fkp得到加密私钥指针地址kpj2。对象乙根据加密私钥指针地址kpj2从本地系统的加密私钥池中取出相应的加密私钥kj2(乙方的第二加密私钥)。

[0125] 同时,对象乙将ri2通过非对称密钥指针函数fkp计算得到对象甲的加密公钥指针地址kpi2。对象乙根据加密公钥指针地址kpi2和对象甲的公钥池编号Pi'从本地系统中的加密公钥密钥池组中取出甲方公钥Ki2(甲方的第二加密公钥)。

[0126] 2.6对象乙加密临时公钥:对象乙生成共享密钥s2=Ki2^kj2(第二共享密钥)。对象乙对临时公钥Kb加密后得到第二密文c2={Kb}·s2。

[0127] 2.7对象乙将密钥协商消息发送到对象甲:对象乙将临时公钥密文c2、随机数r2和对象乙的公钥指针地址rb加密发送到对象甲。

[0128] 步骤3:对象甲解密解析消息并计算协商密钥

[0129] 3.1对象甲接收消息并解密解析:对象甲接收到来自对象乙的消息,对其进行解密解析得到对象乙的公钥指针地址rb'、随机数r2'和临时公钥密文c2'。

[0130] 3.2对象甲取得加密私钥和乙方加密公钥:对象甲将随机数r2'通过指定算法拆分

成ri2’和rj2’。对象甲将ri2’通过密钥指针算法fkp得到加密私钥指针地址kpi2’。对象甲根据加密私钥指针地址kpi2’从本地系统的加密私钥池中取出相应的加密私钥ki2(甲方的第二加密私钥)。

[0131] 同时,对象甲将rj2’通过非对称密钥指针函数fkp计算得到对象乙的加密公钥指针地址kpj2’。对象甲根据加密公钥指针地址kpj2’和对象乙的公钥池编号Pj从本地系统中的加密公钥密钥池组中取出乙方公钥Kj2(乙方的第二加密公钥)。

[0132] 3.3对象甲解密得到乙方临时公钥并取出乙方静态公钥:对象乙计算共享密钥s2’=Kj2^ki2。对象甲利用共享密钥s2’对临时公钥密文c2’解密得到Kb’=c2’·s2’-1。s2-1是s2在循环群G上的逆元。对象甲利用对象乙的公钥指针地址rb’从静态公钥池中取出对象乙的静态公钥B(第二静态公钥)。

[0133] 3.4对象甲计算得到协商密钥:对象甲取出自身静态私钥a(第一静态私钥)。对象甲利用已有的参数计算得到$Sa = ka + (\overline{Ka})a$。其中$\overline{Ka} = (ka \bmod 2^L) + 2^L$,且$L = \left\lceil \frac{\lfloor \log_2 n \rfloor + 1}{2} \right\rceil$。对象甲通过计算得到协商密钥:$K' = h \cdot Sa(Kb' + \overline{Kb}'B)$。

[0134] 对象甲的协商密钥演变得到:

[0135]
$$K' = h \cdot Sa\left(Kb' + \overline{Kb}'B\right) = h \cdot Sa\left(kbQ + \overline{Kb}'bQ\right) = h \cdot Sa\left(kb + \overline{Kb}'b\right)Q$$
$$= h \cdot SaSbQ$$

[0136] 对象乙的协商密钥演变得到:

[0137]
$$K = h \cdot Sb\left(Ka' + \overline{Ka}'A\right) = h \cdot Sb\left(kaQ + \overline{Ka}'aQ\right) = h \cdot Sa\left(ka + \overline{Ka}'a\right)Q = h \cdot SbSaQ$$

[0138] 所以对象甲和对象乙得到的协商密钥相同,密钥协商成功。

[0139] 其中一实施例中,提供一种基于私钥池和Elgamal的抗量子计算MQV密钥协商系统,参与方配置有密钥卡,密钥卡内存储有静态公钥池、加密私钥池、加密公钥池组以及静态私钥和算法参数,所述加密私钥池存储有加密私钥,所述加密公钥池组包括数量与密钥卡数量相对应的加密公钥池,各加密公钥池中存储有与所述加密私钥相对应的加密公钥,所述静态公钥池中存储有与所述静态私钥相对应的静态公钥;

[0140] 所述抗量子计算MQV密钥协商系统,包括:

[0141] 第一模块,用于在己方生成相应的临时公钥和临时私钥,用加密私钥和对方的加密公钥生成共享密钥,并利用共享密钥加密己方的临时公钥得到密文;将所述密文,用于得到对方加密公钥的真随机数,和己方的静态公钥指针地址以密文形式发送给对方;

[0142] 第二模块,用于接收来自对方的所述密文,所述真随机数,和所述静态公钥指针地址,利用所述真随机数得到对方的加密公钥和己方的加密私钥,利用己方的加密私钥和对方的加密公钥生成共享密钥,利用共享密钥解密所述密文得到对方的临时公钥,利用所述静态公钥指针地址得到对方的静态公钥,并利用对方的临时公钥、静态公钥,和己方临时私钥、临时公钥、静态私钥以及算法参数生成协商密钥。

[0143] 关于抗量子计算MQV密钥协商系统的具体限定可以参见上文中对于抗量子计算MQV密钥协商系统的限定,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。

[0144] 在一个实施例中，提供了一种计算机设备，即一种基于私钥池和Elgamal的抗量子计算MQV密钥协商系统，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上述抗量子计算MQV密钥协商方法，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。

[0145] 其中一实施例中，提供一种基于私钥池和Elgamal的抗量子计算MQV密钥协商系统，参与方配置有密钥卡，密钥卡内存储有静态公钥池、加密私钥池、加密公钥池组以及静态私钥和算法参数，所述加密私钥池存储有加密私钥，所述加密公钥池组包括数量与密钥卡数量相对应的加密公钥池，各加密公钥池中存储有与所述加密私钥相对应的加密公钥，所述静态公钥池中存储有与所述静态私钥相对应的静态公钥；

[0146] 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私钥池和Elgamal的抗量子计算MQV密钥协商方法。

[0147] 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。

[0148] 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。

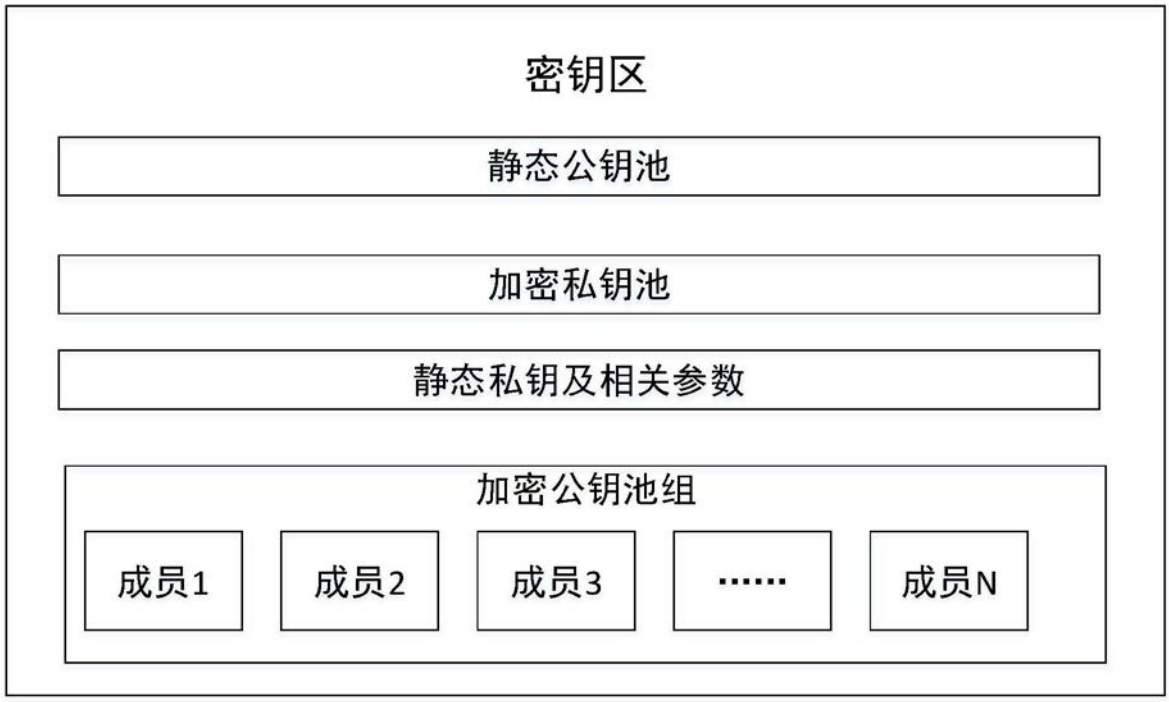


图1

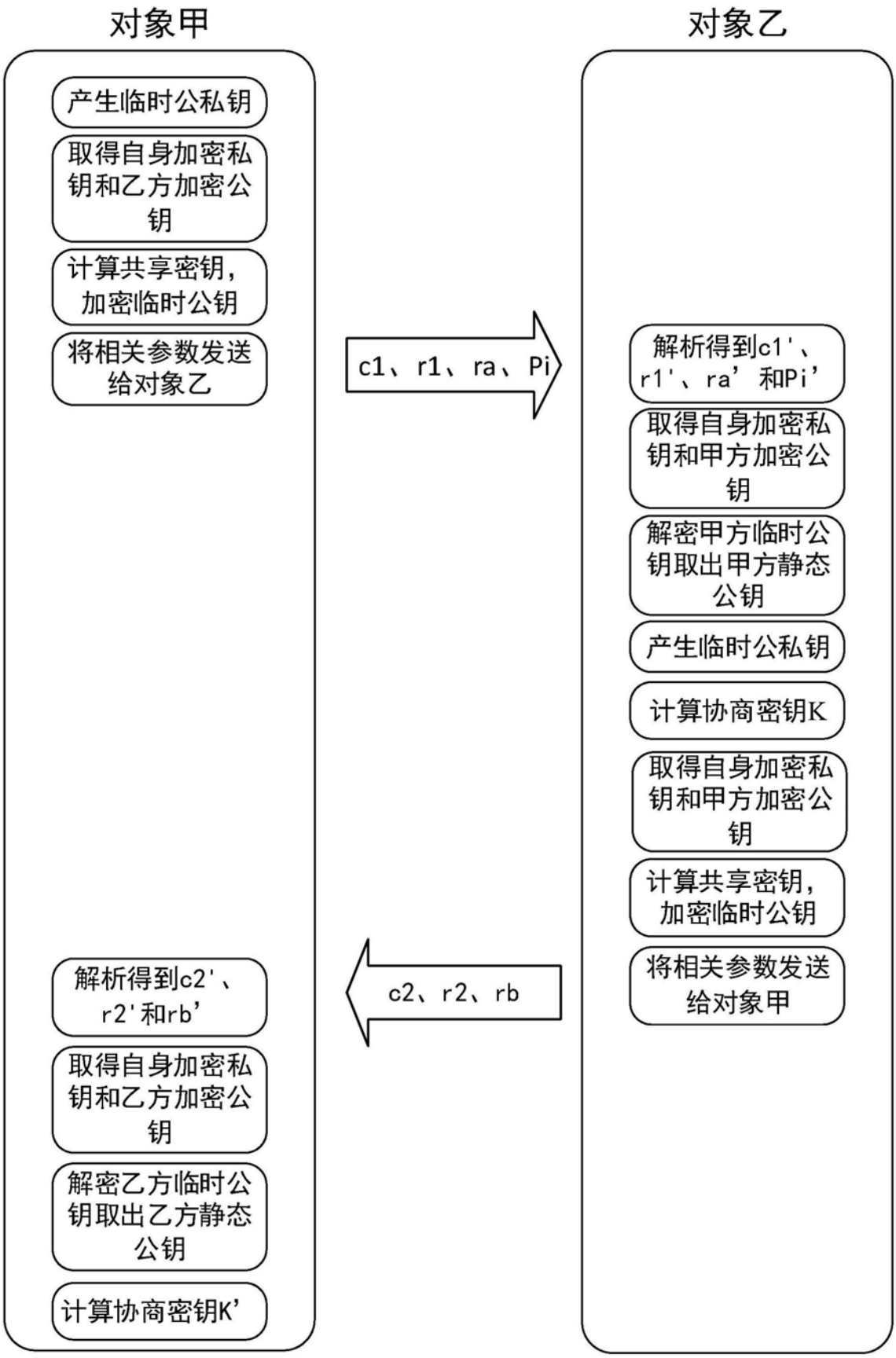

对象甲
对象乙
产生临时公私钥
取得自身加密私钥和乙方加密公钥
计算共享密钥，加密临时公钥
将相关参数发送给对象乙
c1、r1、ra、Pi
解析得到c1'、r1'、ra'和Pi'
取得自身加密私钥和甲方加密公钥
解密甲方临时公钥取出甲方静态公钥
产生临时公私钥
计算协商密钥K
取得自身加密私钥和甲方加密公钥
计算共享密钥，加密临时公钥
将相关参数发送给对象甲
c2、r2、rb
解析得到c2'、r2'和rb'
取得自身加密私钥和乙方加密公钥
解密乙方临时公钥取出乙方静态公钥
计算协商密钥K'

图2

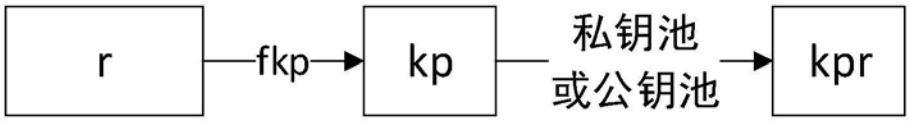


图3