(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 117395000 A
(43)申请公布日 2024.01.12

(21)申请号 202311659788.2

(22)申请日 2023.12.06

(71)申请人 鼎铉商用密码测评技术(深圳)有限公司
地址 518000 广东省深圳市坪山新区坪山街道行政二路4号招商花园城9栋

(72)发明人 陈磊 胡迎春

(74)专利代理机构 深圳市世纪恒程知识产权代理事务所 44287
专利代理师 鲁叶

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

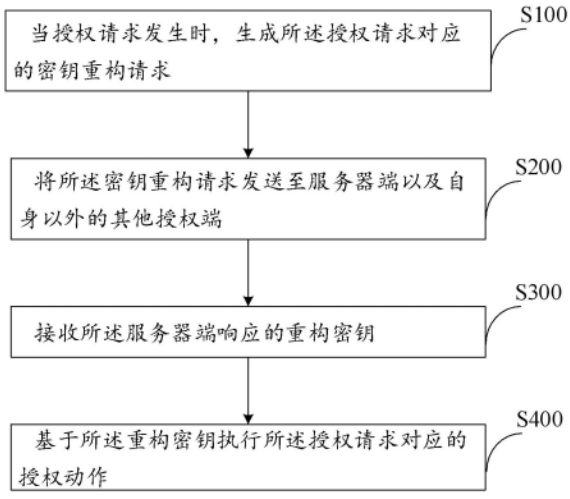
权利要求书2页 说明书9页 附图3页

(54)发明名称

多方授权方法、多方授权设备以及可读存储介质

(57)摘要

本发明涉及数字信息的传输技术领域,尤其涉及一种多方授权方法、多方授权设备以及可读存储介质。通过当授权请求发生时,生成所述授权请求对应的密钥重构请求;将所述密钥重构请求发送至服务器端以及自身以外的其他授权端;接收所述服务器端响应的重构密钥;基于所述重构密钥执行所述授权请求对应的授权动作。增强了授权密钥的安全性和管理,提高整体系统的安全性,并能够更好地适应多方参与的复杂场景,为动态的协作提供支持。



CN 117395000 A

1.一种多方授权方法,其特征在于,应用于授权端,所述多方授权方法包括:

当授权请求发生时,生成所述授权请求对应的密钥重构请求;

将所述密钥重构请求发送至服务器端以及自身以外的其他授权端;

接收所述服务器端响应的重构密钥;

基于所述重构密钥执行所述授权请求对应的授权动作。

2.如权利要求1所述的多方授权方法,其特征在于,所述多方授权方法,还包括:

生成所述授权动作对应的授权密钥;

根据授权端的数量,对所述授权密钥进行密钥分割处理,生成所述数量对应份额的密钥片段;

基于随机分配算法,确定所述授权端与所述密钥片段之间的对应关系;

根据所述对应关系,向所述其他授权端分发所述密钥片段。

3.如权利要求2所述的多方授权方法,其特征在于,所述基于所述重构密钥执行所述授权请求对应的授权动作的步骤之后,还包括:

在所述授权动作执行结束后,执行所述生成所述授权动作对应的授权密钥的步骤。

4.如权利要求2所述的多方授权方法,其特征在于,所述基于所述重构密钥执行所述授权请求对应的授权动作的步骤之前,还包括:

基于所述重构密钥对预设密文执行解密操作;

在解密成功时,执行所述基于所述重构密钥执行所述授权请求对应的授权动作的步骤;

否则,丢弃所述重构密钥,并执行所述生成所述授权请求对应的密钥重构请求的步骤。

5.如权利要求4所述的多方授权方法,其特征在于,所述生成所述授权动作对应的授权密钥的步骤之后,还包括:

基于随机数生成算法,生成随机数;

根据所述授权密钥加密所述随机数,生成所述预设密文。

6.如权利要求2所述的多方授权方法,其特征在于,所述多方授权方法还包括:

接收所述其他授权端发送的所述密钥重构请求;

确定所述密钥重构请求对应的所述密钥片段;

将所述密钥片段发送至所述服务器端。

7.如权利要求6所述的多方授权方法,其特征在于,所述接收所述其他授权端发送的所述密钥重构请求的步骤之后,还包括:

读取所述密钥重构请求中的密钥片段;

对所述密钥重构请求中的密钥片段进行一致性验证;

当所述密钥重构请求中的密钥片段通过一致性验证之后,执行所述确定所述密钥重构请求对应的所述密钥片段的步骤;

若所述密钥重构请求中的密钥片段未通过一致性验证,发送密钥片段验证未通过的响应信息至所述密钥重构请求的发送端。

8.一种多方授权方法,其特征在于,应用于服务器端,所述多方授权方法包括:

接收授权端发送的密钥重构请求,以及密钥片段;

根据所述密钥片段生成所述密钥重构请求对应的重构密钥;

将所述重构密钥作为所述密钥重构请求的响应信息,发送至所述密钥重构请求的发送端。

9.一种多方授权设备,其特征在于,所述多方授权设备包括:存储器、处理器及存储在所述存储器上并可在所述处理器上运行的多方授权程序,所述多方授权程序配置为实现如权利要求1至7中任一项,或者实现如权利要求8所述的多方授权方法的步骤。

10.一种可读存储介质,其特征在于,所述可读存储介质上存储有多方授权程序,所述多方授权程序被处理器执行时实现如权利要求1至8任一项所述的多方授权方法的步骤。

多方授权方法、多方授权设备以及可读存储介质

技术领域

[0001] 本发明涉及数字信息的传输技术领域,尤其涉及一种多方授权方法、多方授权设备以及可读存储介质。

背景技术

[0002] 授权机制是确保数据和资源访问安全、隐私保护以及合规性的关键因素。在传统的授权机制中,通常由一个授权机构或者实体来负责授予访问权限。但是,这种集中式授权由于密钥都由单一授权方管理,如果该机构或实体受到黑客攻击或内部泄密,用户和其他参与方的敏感数据和隐私信息可能面临被泄露、篡改或滥用的风险。因此,传统的授权机制存在安全性不足的缺陷。

[0003] 上述内容仅用于辅助理解本发明的技术方案,并不代表承认上述内容是现有技术。

发明内容

[0004] 本发明的主要目的在于提供一种多方授权方法,旨在解决传统的授权机制存在安全性不足的问题。

[0005] 为实现上述目的,本发明提供的一种多方授权方法,应用于授权端,所述多方授权方法包括以下步骤:

当授权请求发生时,生成所述授权请求对应的密钥重构请求;

将所述密钥重构请求发送至服务器端以及自身以外的其他授权端;

接收所述服务器端响应的重构密钥;

基于所述重构密钥执行所述授权请求对应的授权动作。

[0006] 可选地,所述多方授权方法,还包括:

生成所述授权动作对应的授权密钥;

根据授权端的数量,对所述授权密钥进行密钥分割处理,生成所述数量对应份额的密钥片段;

基于随机分配算法,确定所述授权端与所述密钥片段之间的对应关系;

根据所述对应关系,向所述其他授权端分发所述密钥片段。

[0007] 可选地,所述基于所述重构密钥执行所述授权请求对应的授权动作的步骤之后,还包括:

在所述授权动作执行结束后,执行所述生成所述授权动作对应的授权密钥的步骤。

[0008] 可选地,所述基于所述重构密钥执行所述授权请求对应的授权动作的步骤之前,还包括:

基于所述重构密钥对预设密文执行解密操作;

在解密成功时,执行所述基于所述重构密钥执行所述授权请求对应的授权动作的

步骤；

否则，丢弃所述重构密钥，并执行所述生成所述授权请求对应的密钥重构请求的步骤。

[0009] 可选地，所述生成所述授权动作对应的授权密钥的步骤之后，还包括：

基于随机数生成算法，生成随机数；

根据所述授权密钥加密所述随机数，生成所述预设密文。

[0010] 可选地，所述多方授权方法还包括：

接收所述其他授权端发送的所述密钥重构请求；

确定所述密钥重构请求对应的所述密钥片段；

将所述密钥片段发送至所述服务器端。

[0011] 可选地，所述接收所述其他授权端发送的所述密钥重构请求的步骤之后，还包括：

读取所述密钥重构请求中的密钥片段；

对所述密钥重构请求中的密钥片段进行一致性验证；

当所述密钥重构请求中的密钥片段通过一致性验证之后，执行所述确定所述密钥重构请求对应的所述密钥片段的步骤；

若所述密钥重构请求中的密钥片段未通过一致性验证，发送密钥片段验证未通过的响应信息至所述密钥重构请求的发送端。

[0012] 可选地，应用于服务器端，所述多方授权方法包括：

接收授权端发送的密钥重构请求，以及密钥片段；

根据所述密钥片段生成所述密钥重构请求对应的重构密钥；

将所述重构密钥作为所述密钥重构请求的响应信息，发送至所述密钥重构请求的发送端。

[0013] 此外，为实现上述目的，本发明还提供一种多方授权设备，所述多方授权设备包括存储器、处理器及存储在所述存储器上并可在所述处理器上运行的多方授权程序，所述多方授权程序被所述处理器执行时实现如上所述的多方授权方法的步骤。

[0014] 此外，为实现上述目的，本发明还提供一种计算机可读存储介质，所述计算机可读存储介质上存储有多方授权程序，所述多方授权程序被处理器执行时实现如上所述的多方授权方法的步骤。

[0015] 本发明实施例提供一种多方授权方法，通过生成密钥重构请求并将其发送至服务器端以及其他授权端，实现了多方参与的密钥管理，可以避免单一授权端承担所有密钥管理的风险和负担；此外，将密钥的生成和存储分散到多个参与方，提高了密钥的安全性。通过每次授权请求都生成新的密钥重构请求，并将其发送给其他授权端，使得系统可以动态地适应不同的授权请求和参与方。这种灵活性和动态协作使系统能够适应多方参与的复杂场景，并在实时性和安全性上得到提高。因此，通过分散密钥管理和动态协作支持，可以增强授权密钥的安全性和管理，提高整体系统的安全性，并能够更好地适应多方参与的复杂场景，为动态的协作提供支持。

附图说明

[0016] 此处的附图被并入说明书中并构成本说明书的一部分，示出了符合本发明的实施

例,并与说明书一起用于解释本发明的原理。为了更清楚地说明本发明实施例的技术方案,下面将对实施例描述中所需要使用的附图作简单地介绍,显而易见地,对于本领域普通技术人员而言,在不付出创造性劳动性的前提下,还可以根据这些附图获得其他的附图。

[0017] 图1为本发明实施例涉及的多方授权设备的硬件运行环境的架构示意图;

图2为本发明多方授权方法的第一实施例的流程示意图;

图3为本发明多方授权方法的第二实施例的流程示意图;

图4为本发明多方授权方法的第三实施例的流程示意图。

[0018] 图5为本发明多方授权方法的一示例的流程示意图。

[0019] 本发明目的的实现、功能特点及优点将结合实施例,参照附图作进一步说明。

具体实施方式

[0020] 本申请一种多方授权方法,通过当授权请求发生时,生成所述授权请求对应的密钥重构请求;将所述密钥重构请求发送至服务器端以及自身以外的其他授权端;接收所述服务器端响应的重构密钥;基于所述重构密钥执行所述授权请求对应的授权动作。增强了授权密钥的安全性和管理,提高整体系统的安全性,并能够更好地适应多方参与的复杂场景,为动态的协作提供支持。

[0021] 为了更好地理解上述技术方案,下面将参照附图更详细地描述本公开的示例性实施例。虽然附图中显示了本公开的示例性实施例,然而应当理解,可以以各种形式实现本公开而不应被这里阐述的实施例所限制。相反,提供这些实施例是为了能够更透彻地理解本公开,并且能够将本公开的范围完整地传达给本领域的技术人员。

[0022] 作为一种实现方案,图1为本发明实施例方案涉及的多方授权设备的硬件运行环境的架构示意图。

[0023] 如图1所示,该多方授权设备可以包括:处理器101,例如中央处理器(Central Processing Unit,CPU),存储器102,通信总线103。其中,存储器102可以是高速的随机存取存储器(Random Access Memory,RAM)存储器,也可以是稳定的非易失性存储器(Non-Volatile Memory,NVM),例如磁盘存储器。存储器102可选的还可以是独立于前述处理器101的存储装置。通信总线103用于实现这些组件之间的连接通信。

[0024] 本领域技术人员可以理解,图1中示出的结构并不构成对多方授权设备的限定,可以包括比图示更多或更少的部件,或者组合某些部件,或者不同的部件布置。

[0025] 如图1所示,作为一种计算机可读存储介质的存储器102中可以包括操作系统、数据存储模块、网络通信模块、用户接口模块以及多方授权程序。

[0026] 在图1所示的多方授权设备中,处理器101、存储器102可以设置在多方授权设备中,所述多方授权设备通过处理器101调用存储器102中存储的多方授权程序,并执行以下操作:

当授权请求发生时,生成所述授权请求对应的密钥重构请求;

将所述密钥重构请求发送至服务器端以及自身以外的其他授权端;

接收所述服务器端响应的重构密钥;

基于所述重构密钥执行所述授权请求对应的授权动作。

[0027] 在一实施例中,处理器101可以用于调用存储器102中存储的多方授权程序,并执

行以下操作：

生成所述授权动作对应的授权密钥；

根据授权端的数量，对所述授权密钥进行密钥分割处理，生成所述数量对应份额的密钥片段；

基于随机分配算法，确定所述授权端与所述密钥片段之间的对应关系；

根据所述对应关系，向所述其他授权端分发所述密钥片段。

[0028] 在一实施例中，处理器101可以用于调用存储器102中存储的多方授权程序，并执行以下操作：

在所述授权动作执行结束后，执行所述生成所述授权动作对应的授权密钥的步骤。

[0029] 在一实施例中，处理器101可以用于调用存储器102中存储的多方授权程序，并执行以下操作：

基于所述重构密钥对预设密文执行解密操作；

在解密成功时，执行所述基于所述重构密钥执行所述授权请求对应的授权动作的步骤；

否则，丢弃所述重构密钥，并执行所述生成所述授权请求对应的密钥重构请求的步骤。

[0030] 在一实施例中，处理器101可以用于调用存储器102中存储的多方授权程序，并执行以下操作：

基于随机数生成算法，生成随机数；

根据所述授权密钥加密所述随机数，生成所述预设密文。

[0031] 在一实施例中，处理器101可以用于调用存储器102中存储的多方授权程序，并执行以下操作：

接收所述其他授权端发送的所述密钥重构请求；

确定所述密钥重构请求对应的所述密钥片段；

将所述密钥片段发送至所述服务器端。

[0032] 在一实施例中，处理器101可以用于调用存储器102中存储的多方授权程序，并执行以下操作：

读取所述密钥重构请求中的密钥片段；

对所述密钥重构请求中的密钥片段进行一致性验证；

当所述密钥重构请求中的密钥片段通过一致性验证之后，执行所述确定所述密钥重构请求对应的所述密钥片段的步骤；

若所述密钥重构请求中的密钥片段未通过一致性验证，发送密钥片段验证未通过的响应信息至所述密钥重构请求的发送端。

[0033] 在一实施例中，处理器101可以用于调用存储器102中存储的多方授权程序，并执行以下操作：

接收授权端发送的密钥重构请求，以及密钥片段；

根据所述密钥片段生成所述密钥重构请求对应的重构密钥；

将所述重构密钥作为所述密钥重构请求的响应信息，发送至所述密钥重构请求的

发送端。

[0034] 基于上述多方授权设备的硬件架构,提出本发明多方授权方法的实施例。

[0035] 参照图2,在第一实施例中,所述多方授权方法应用于授权端,所述多方授权方法包括以下步骤:

步骤S100:当授权请求发生时,生成所述授权请求对应的密钥重构请求。

[0036] 在本实施例中,在授权端有授权请求发生的时候,根据授权请求所对应的授权动作,生成授权请求对应的密钥重构请求。需要说明的是,这里的密钥重构请求,用于请求获取执行授权请求对应的授权动作所需要的授权密钥。可以理解的是,密钥重构请求的响应信息在本实施例中称为重构密钥,而重构密钥不一定相当于授权请求对应的授权密钥,只有在重构密钥可以用于执行授权请求对应的授权动作的时候,重构密钥才相当于授权密钥。

[0037] 可选地,密钥重构请求包括授权请求,或者包括授权请求和授权密钥的一个密钥片段。需要说明的是,授权请求用于确定授权动作所需要的目标授权密钥所对应的密钥片段。对属于同一个授权密钥的密钥片段进行密钥重构操作,可以获得重构密钥。

[0038] 步骤S200:将所述密钥重构请求发送至服务器端以及自身以外的其他授权端。

[0039] 在本实施例中,授权端在生成密钥重构请求之后,将密钥重构请求发送至服务器端以及自身以外的其他授权端。需要说明的是,这里的其他授权端,都保存有生成重构密钥所需要的密钥片段。

[0040] 可选地,在将密钥重构请求发送至其他授权端之前,可以根据其他授权端的数量,确定密钥重构请求发送的份额;然后根据密钥重构请求发送的份额,于其他授权端中选取相应数量的目标授权端发送密钥重构请求。需要说明的是,只有在拥有一定数量的同一个授权密钥的密钥片段时,才能够进行密钥重构操作。

[0041] 作为一种可选的实施方式,假设密钥重构请求中仅包括授权请求。当授权端一共有5个时,选取的目标授权端的数量至少为3个;当授权端一共有7个时,选取的目标授权端的数量至少为5个。

[0042] 作为另一种可选的实施方式,假设密钥重构请求中包括授权请求和密钥片段。当授权端一共有5个时,选取的目标授权端的数量至少为2个;当授权端一共有7个时,选取的目标授权端的数量至少为4个。

[0043] 步骤S300:接收所述服务器端响应的重构密钥。

[0044] 步骤S400:基于所述重构密钥执行所述授权请求对应的授权动作。

[0045] 在本实施例中,在将密钥重构请求发送至服务器端和其他授权端之后,接收服务器端响应密钥重构请求生成的重构密钥。可以理解的是,基于密钥重构操作生成重构密钥的步骤在服务器端执行。

[0046] 在接收到服务器端发送的重构密钥之后,基于重构密钥执行授权请求对应的授权动作。

[0047] 进一步地,所述多方授权方法,还包括:

步骤S510:生成所述授权动作对应的授权密钥;

步骤S520:根据授权端的数量,对所述授权密钥进行密钥分割处理,生成所述数量对应份额的密钥片段;

步骤S530:基于随机分配算法,确定所述授权端与所述密钥片段之间的对应关系;

步骤S540:根据所述对应关系,向所述其他授权端分发所述密钥片段。

[0048] 在本实施例中,每个授权动作对应有授权密钥,授权密钥在授权请求发生之前便在授权端生成。授权端在生成授权动作对应的授权密钥之后,并不对授权密钥进行保存,而是根据授权端的数量,对授权密钥进行密钥分割处理,生成与授权端的数量对应份额的密钥片段。然后,在保存其中一个密钥片段之后,基于随机分配算法,确定自身以外的其他授权端与剩余的密钥片段之间的对应关系,并根据对应关系,将剩余的密钥片段分发至自身以外的其他授权端。可以理解的是,经过上述过程,每个授权端都保存有该授权动作对应的授权密钥的一个密钥片段。

[0049] 通过授权密钥的生成、分割和分配,使授权请求对应的授权动作,需要由多个授权端合作完成。这样做的目的在于增强授权过程的安全性和可靠性。

[0050] 可选地,在所述授权动作执行结束后,执行所述生成所述授权动作对应的授权密钥的步骤,以实现授权动作对应的授权密钥的更新。此外,执行所述生成所述授权动作对应的授权密钥的步骤的条件,还可以是在授权端的数量发生变更的时候,或者是在密钥片段或授权密钥发生泄漏的时候。

[0051] 在授权动作执行结束后执行生成授权动作对应的授权密钥的步骤,可以确保每次授权动作都使用一个新的授权密钥。进而增强授权动作的安全性,防止潜在的密钥泄露或密钥失效对系统安全造成的风险。此外,授权端的数量变需要重新生成和分配授权密钥和密钥片段,以确保新的授权端可以获得密钥重构操作所需的密钥片段,并且使原有的授权端不再具有执行授权动作的权限。如果密钥片段或授权密钥发生泄漏,为了保护系统的安全性,需要生成新的授权密钥,并重新分配密钥片段,以确保未经授权的人或实体无法获取有效的授权密钥或者密钥片段。这样做的目的在于,通过在适当的时机生成授权动作对应的授权密钥,确保授权过程的安全性和可靠性,并及时应对潜在的安全风险。

[0052] 可选地,授权端在接收到服务器发送的重构密钥之后,需要先对重构密钥进行验证,并在重构密钥验证通过之后,才基于重构密钥执行授权请求对应的授权动作。具体地,重构密钥的验证步骤包括,基于所述重构密钥对预设密文执行解密操作;在解密成功时,执行所述基于所述重构密钥执行所述授权请求对应的授权动作的步骤;否则,丢弃所述重构密钥,并执行所述生成所述授权请求对应的密钥重构请求的步骤。可以理解的是,若重构密钥能够成功对预设密文进行解密操作,则可以确定重构密文相当于授权动作对应的授权密钥,可用于执行授权动作。

[0053] 进一步地,预设密文是授权端在生成授权密钥的时候,生成并保存在授权端中的。具体地,授权端在生成授权密钥之后,基于随机数生成算法,生成随机数;然后采用授权密钥对随机数进行加密操作,生成预设密文。可以理解的,预设密文是用于验证重构密钥的有效性。

[0054] 在本实施例提供的技术方案中,通过生成密钥重构请求并将其发送至服务器端以及其他授权端,实现了多方参与的密钥管理,可以避免单一授权端承担所有密钥管理的风险和负担;此外,将密钥的生成和存储分散到多个参与方,提高了密钥的安全性。通过每次授权请求都生成新的密钥重构请求,并将其发送给其他授权端,使得系统可以动态地适应不同的授权请求和参与方。这种灵活性和动态协作使系统能够适应多方参与的复杂场景,

并在实时性和安全性上得到提高。因此,通过分散密钥管理和动态协作支持,可以增强授权密钥的安全性和管理,提高整体系统的安全性,并能够更好地适应多方参与的复杂场景,为动态的协作提供支持。

[0055] 参照图3,基于上述实施例,在第二实施例中,所述多方授权方法还包括:

步骤S600:接收所述其他授权端发送的所述密钥重构请求;

步骤S700:确定所述密钥重构请求对应的所述密钥片段;

步骤S800:将所述密钥片段发送至所述服务器端。

[0056] 在本实施例中,当授权端接收到其他授权端发送的密钥重构请求时,根据密钥重构请求,确定所要进行重构的授权密钥;然后从保存的各个授权密钥对应的密钥片段中,该授权密钥所对应的密钥片段。可以理解的是,最后确定的这个授权密钥所对应的密钥片段,即密钥重构请求对应的密钥片段。进一步地,在确定密钥重构请求对应的密钥片段之后,将该密钥片段发送至服务器端,以供服务器端生成重构密钥。

[0057] 进一步地,授权端在接收到密钥重构请求之后,对密钥重构请求进行验证,当重构请求验证通过之后,才调用密钥对应的密钥片段发送至服务器端;否则,发送密钥重构请求验证未通过的响应信息至密钥重构请求的发送端。

[0058] 通过对密钥重构请求进行验证,可以防止来自未授权的发送端或者恶意攻击者的非法请求对系统安全的威胁。只有在请求验证通过后,授权端才会将对应的密钥片段发送至服务器端,从而保护了授权密钥的机密性和完整性。因此,通过对密钥重构请求进行验证,可以有效地防止非法请求,保护授权密钥的安全性,进而达到提高系统安全性的目的。

[0059] 在一实施例中,密钥重构请求包括密钥片段。通过读取所述密钥重构请求中的密钥片段,并对所述密钥重构请求中的密钥片段进行一致性验证。当所述密钥重构请求中的密钥片段通过一致性验证之后,执行所述确定所述密钥重构请求对应的所述密钥片段的步骤;若所述密钥重构请求中的密钥片段未通过一致性验证,发送密钥片段验证未通过的响应信息至所述密钥重构请求的发送端。

[0060] 在另一实施例中,密钥重构请求包括密钥片段以及该密钥片段的MAC值。通过读取所述密钥重构请求中的MAC值,并基于HMAC算法,获取密钥重构请求中的密钥片段的MAC值;然后,验证所述密钥片段的MAC值,与所述密钥重构请求中的MAC值的一致性;并在所述密钥片段的MAC值通过一致性验证时,执行所述确定所述密钥重构请求对应的所述密钥片段的步骤。

[0061] 在本实施例提供的技术方案中,通过根据密钥重构请求确定对应的密钥片段,并将确定的密钥片段发送至服务器端进行密钥重构。实现多方参与、分散管理和多方授权,进而达到提高密钥的安全性和系统的安全性的目的。

[0062] 参照图4,基于上述实施例,在第三实施例中,所述多方授权方法应用于服务器端,所述多方授权方法包括:

步骤S910:接收授权端发送的密钥重构请求,以及密钥片段;

步骤S920:根据所述密钥片段生成所述密钥重构请求对应的重构密钥;

步骤S930:将所述重构密钥作为所述密钥重构请求的响应信息,发送至所述密钥重构请求的发送端。

[0063] 在本实施例中,服务器端在接收到授权端发送的密钥重构请求以及密钥片段之

后,基于密钥片段,执行密钥重构操作,生成所述密钥重构请求对应的重构密钥,并将所述重构密钥作为所述密钥重构请求的响应信息,发送至所述密钥重构请求的发送端。

[0064] 可选地,服务器端在基于密钥片段,执行密钥重构操作的步骤之前,需要根据接收到的密钥片段的份额和授权端的数量,判断是否符合密钥重构条件;并在密钥片段的份额符合密钥重构条件时,才进行密钥重构操作。示例性地,当授权端的数量为5时,至少需要3个密钥片段才符合密钥重构条件;当授权端的数量为7时,至少需要5个密钥片段才符合密钥重构条件。

[0065] 示例性地,如图5所示,假设一共有5个授权端,分别为授权端A、授权端B、授权端C、授权端D和授权端E。首先,授权端A针对授权动作,生成对应的授权密钥,并基于授权密钥对一随机数进行加密操作,生成并保存预设密文。然后,根据授权端的数量,对授权密钥进行密钥分割处理,生成5个密钥片段,分别为片段1、片段2、片段3、片段4和片段5。然后,授权端A将片段1保存,并将片段2、片段3、片段4和片段5随机分发至授权端B、授权端C、授权端D和授权端E。

[0066] 假设授权端B接收到的是片段2,授权端C接收到的是片段3,授权端D接收到的是片段4,授权端E接收到的是片段5。当授权端E接收到请求方发送的授权请求时,授权端E基于授权请求生成密钥重构请求。然后基于授权端的数量为5,于自身以外的其他授权端中选取3个目标授权端。

[0067] 假设选取的目标授权端为授权端B、授权端C和授权端D。授权端B、授权端C和授权端D在接收到密钥重构请求之后,根据密钥重构请求,对应地将片段2、片段3以及片段4发送至服务器端。服务器端根据接收到的片段2、片段3以及片段4,进行密钥重构操作,生成重构密钥,并将重构密钥发送至授权端E。

[0068] 授权端E在接收到重构密钥之后,基于重构密钥,响应端的授权请求,对请求端进行授权操作。

[0069] 在本实施例提供的技术方案中,由于服务器端具有更强的安全性能和防护机制,可以确保密钥重构的安全性,防止重要信息被泄露。因此通过将密钥重构请求和密钥片段发送至服务器端,可以在相对安全的环境下完成密钥重构的过程。通过在服务器端完成密钥重构的过程,可以简化密钥管理的流程。授权端只需发送密钥重构请求和密钥片段至服务器端,而无需实际进行密钥重构的计算过程,减轻了授权端的计算负担,提高了系统的效率和响应速度。

[0070] 此外,本领域普通技术人员可以理解的是实现上述实施例的方法中的全部或部分流程,是可以通过计算机程序来指令相关的硬件来完成。该计算机程序包括程序指令,计算机程序可以存储于一存储介质中,该存储介质为计算机可读存储介质。该程序指令被多方授权设备中的至少一个处理器执行,以实现上述方法的实施例的流程步骤。

[0071] 因此,本发明还提供一种计算机可读存储介质,所述计算机可读存储介质存储有多方授权程序,所述多方授权程序被处理器执行时实现如上实施例所述的多方授权方法的各个步骤。

[0072] 其中,所述计算机可读存储介质可以是U盘、移动硬盘、只读存储器(Read-Only Memory,ROM)、磁碟或者光盘等各种可以存储程序代码的计算机可读存储介质。

[0073] 需要说明的是,由于本申请实施例提供的存储介质,为实施本申请实施例的方法

所采用的存储介质,故而基于本申请实施例所介绍的方法,本领域所属人员能够了解该存储介质的具体结构及变形,故而在此不再赘述。凡是本申请实施例的方法所采用的存储介质都属于本申请所欲保护的范围。

[0074] 本领域内的技术人员应明白,本发明的实施例可提供为方法、系统或计算机程序产品。因此,本发明可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且,本发明可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质(包括但不限于磁盘存储器、CD-ROM、光学存储器等)上实施的计算机程序产品的形式。

[0075] 本发明是参照根据本发明实施例的方法、设备(系统)、和计算机程序产品的流程图和/或方框图来描述的。应理解可由计算机程序指令实现流程图和/或方框图中的每一流程和/或方框、以及流程图和/或方框图中的流程和/或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器,使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的装置。

[0076] 这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中,使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品,该指令装置实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能。

[0077] 这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上,使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理,从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的步骤。

[0078] 应当注意的是,在权利要求中,不应将位于括号之间的任何参考符号构造成对权利要求的限制。单词“包含”不排除存在未列在权利要求中的部件或步骤。位于部件之前的单词“一”或“一个”不排除存在多个这样的部件。本发明可以借助于包括有若干不同部件的硬件以及借助于适当编程的计算机来实现。在列举了若干装置的单元权利要求中,这些装置中的若干个可以是通过同一个硬件项来具体体现。单词第一、第二以及第三等的使用不表示任何顺序。可将这些单词解释为名称。

[0079] 尽管已描述了本发明的优选实施例,但本领域内的技术人员一旦得知了基本创造性概念,则可对这些实施例做出另外的变更和修改。所以,所附权利要求意欲解释为包括优选实施例以及落入本发明范围的所有变更和修改。

[0080] 显然,本领域的技术人员可以对本发明进行各种改动和变型而不脱离本发明的精神和范围。这样,倘若本发明的这些修改和变型属于本发明权利要求及其等同技术的范围之内,则本发明也意图包含这些改动和变型在内。

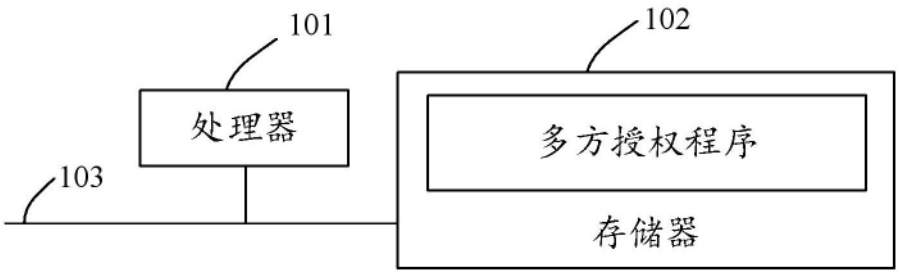

101
处理器
102
多方授权程序
103
存储器

图1

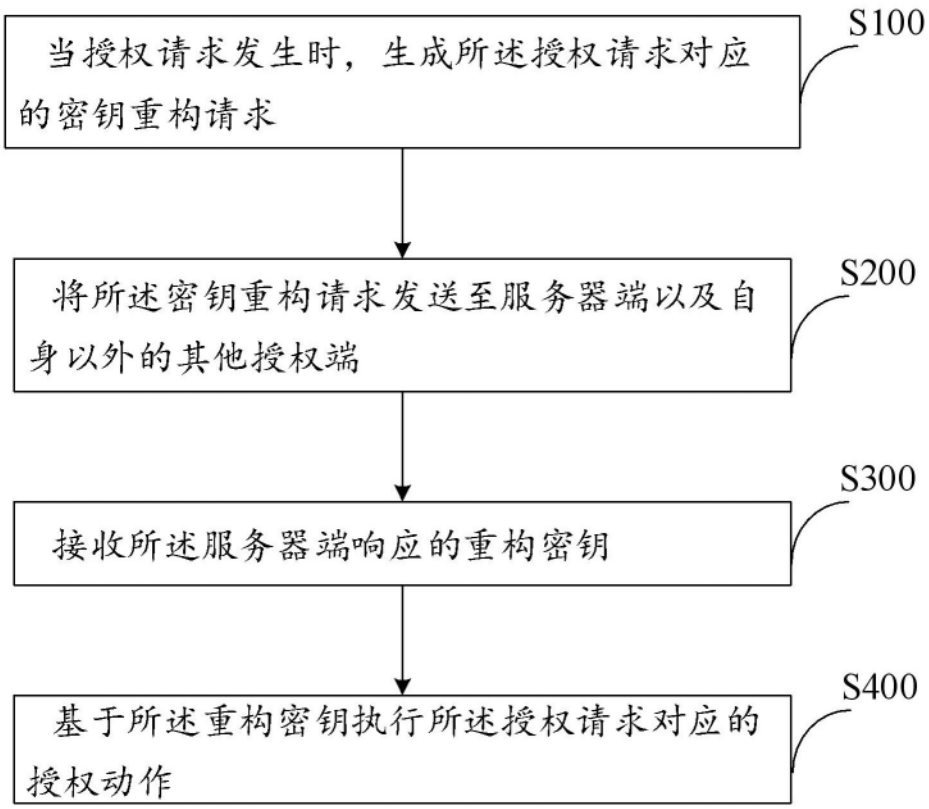

当授权请求发生时，生成所述授权请求对应的密钥重构请求
S100
将所述密钥重构请求发送至服务器端以及自身以外的其他授权端
S200
接收所述服务器端响应的重构密钥
S300
基于所述重构密钥执行所述授权请求对应的授权动作
S400

图2

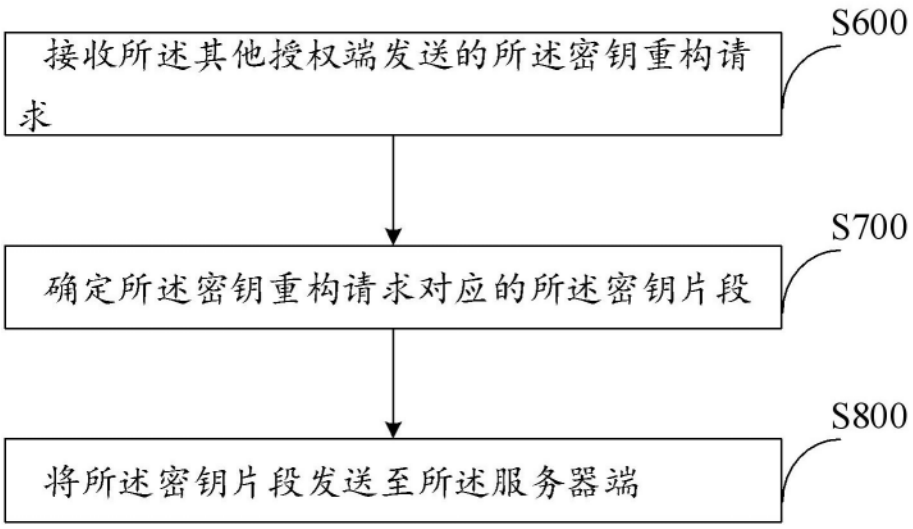

S600
接收所述其他授权端发送的所述密钥重构请求
S700
确定所述密钥重构请求对应的所述密钥片段
S800
将所述密钥片段发送至所述服务器端

图3

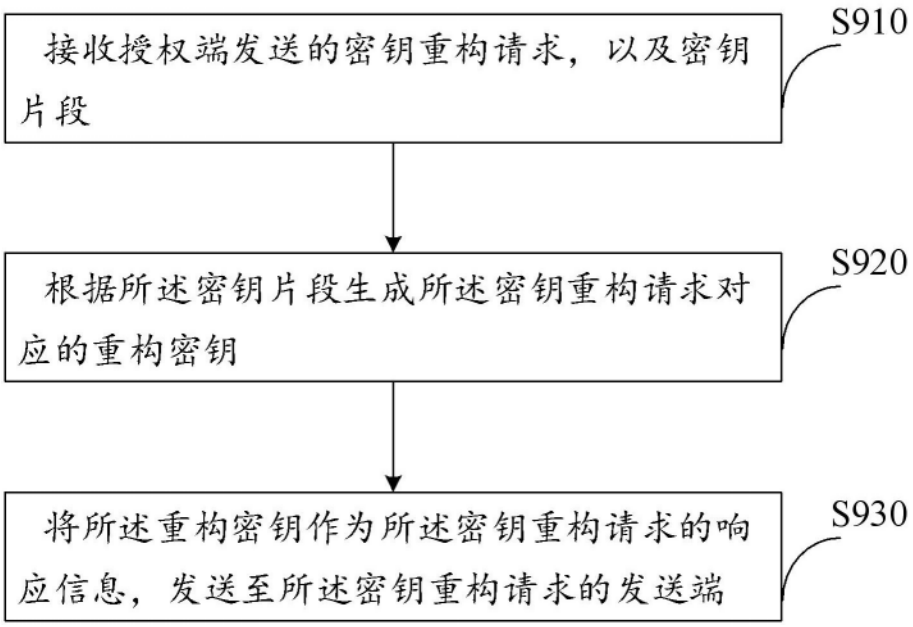

S910
接收授权端发送的密钥重构请求，以及密钥片段
S920
根据所述密钥片段生成所述密钥重构请求对应的重构密钥
S930
将所述重构密钥作为所述密钥重构请求的响应信息，发送至所述密钥重构请求的发送端

图4

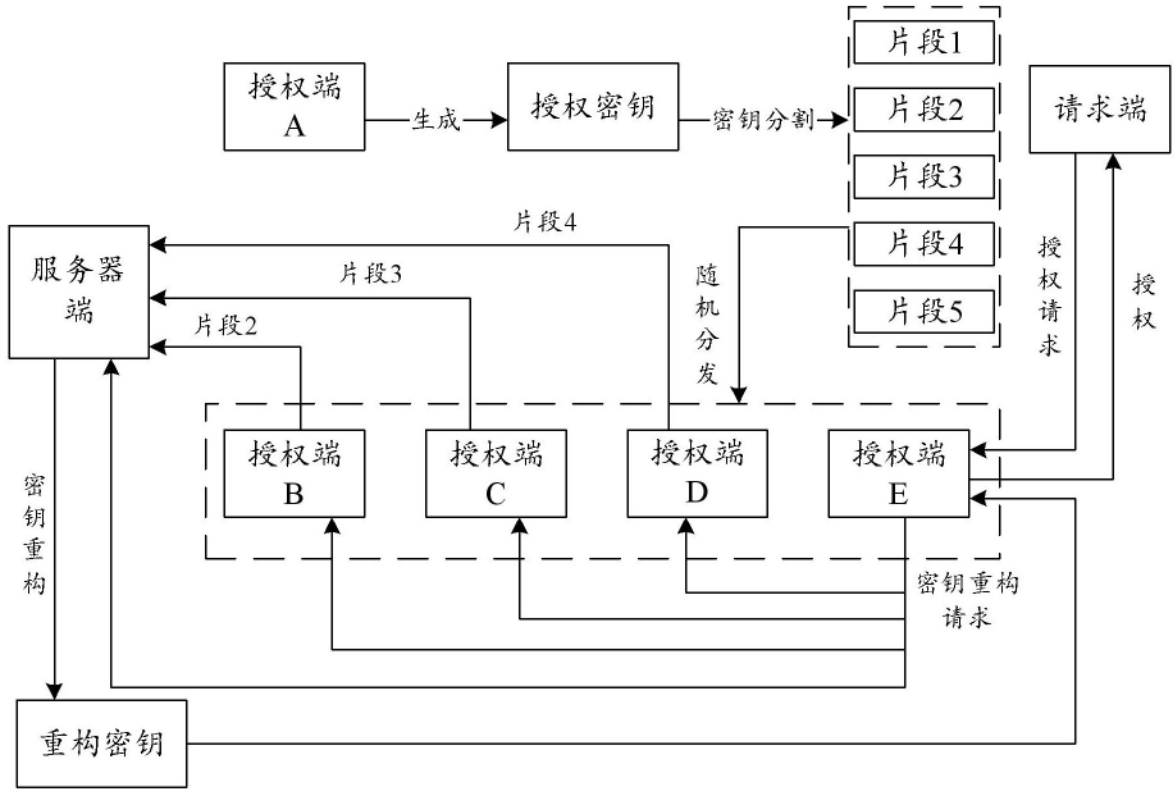

授权端
A
生成
授权密钥
密钥分割
片段1
片段2
片段3
片段4
片段5
请求端
服务器
端
片段4
片段3
片段2
随机分发
授权请求
授权
密钥重构
授权端
B
授权端
C
授权端
D
授权端
E
密钥重构
请求
重构密钥

图5