(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 117411642 A
(43)申请公布日 2024.01.16

(21)申请号 202311564275.3

(22)申请日 2023.11.22

(71)申请人 北京富算科技有限公司
地址 100070 北京市丰台区南四环西路188号十六区18号楼1至15层101内7层701-8

(72)发明人 孙小超 陈立峰 李腾飞 赵华宇 卫骞 杜浩 尤志强 卞阳 张伟奇

(74)专利代理机构 北京慧加伦知识产权代理有限公司 16035
专利代理师 李永敏

(51)Int.Cl.
H04L 9/32(2006.01)
H04L 9/30(2006.01)
H04L 9/08(2006.01)
H04L 9/40(2022.01)

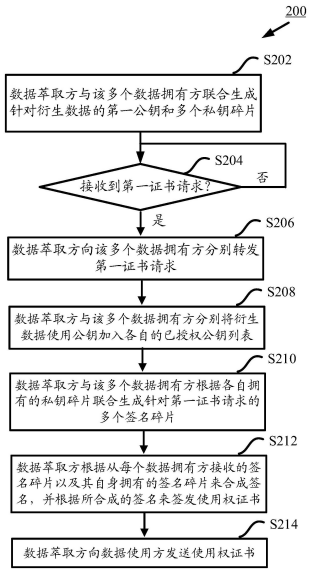
权利要求书2页 说明书7页 附图7页

(54)发明名称

针对多方联合生成的衍生数据的访问控制方法及装置

(57)摘要

本公开的实施例提供一种针对多方联合生成的衍生数据的访问控制方法及装置。多方包括数据萃取方和多个数据拥有方。数据萃取方和该多个数据拥有方各自拥有一个衍生数据碎片。方法包括:数据萃取方与该多个数据拥有方联合生成针对衍生数据的第一公钥和多个私钥碎片;响应于数据萃取方接收到数据使用方对衍生数据的第一证书请求:数据萃取方向该多个数据拥有方分别转发第一证书请求;数据萃取方与该多个数据拥有方根据各自拥有的私钥碎片联合生成针对第一证书请求的多个签名碎片;数据萃取方根据从每个数据拥有方接收的签名碎片以及其自身拥有的签名碎片来合成签名,并根据所合成的签名来签发使用权证书;以及数据萃取方向数据使用方发送使用权证书。



CN 117411642 A

1.一种针对多方联合生成的衍生数据的访问控制方法,其特征在于,所述多方包括数据萃取方和多个数据拥有方,所述衍生数据被表征为多个衍生数据碎片,所述数据萃取方和所述多个数据拥有方各自拥有一个衍生数据碎片,所述访问控制方法包括:

所述数据萃取方与所述多个数据拥有方联合生成针对所述衍生数据的第一公钥和与所述第一公钥对应的私钥的多个私钥碎片,其中,所述数据萃取方和所述多个数据拥有方各自拥有所述第一公钥和一个不同的私钥碎片;

响应于所述数据萃取方接收到数据使用方对所述衍生数据的第一证书请求:

所述数据萃取方向所述多个数据拥有方分别转发所述第一证书请求,所述第一证书请求附带所述数据使用方的衍生数据使用公钥;

所述数据萃取方与所述多个数据拥有方分别将所述衍生数据使用公钥加入各自的已授权公钥列表;

所述数据萃取方与所述多个数据拥有方根据各自拥有的私钥碎片联合生成针对所述第一证书请求的多个签名碎片,其中,所述数据萃取方和所述多个数据拥有方各自拥有一个签名碎片;

所述数据萃取方根据从每个数据拥有方接收的签名碎片以及其自身拥有的签名碎片来合成签名,并根据所合成的签名来签发使用权证书,其中,所述使用权证书包括所述衍生数据使用公钥;以及

所述数据萃取方向所述数据使用方发送所述使用权证书。

2.根据权利要求1所述的访问控制方法,其特征在于,所述访问控制方法还包括响应于所述数据萃取方接收到所述数据使用方对所述衍生数据的第一使用请求:

所述数据萃取方向所述多个数据拥有方分别转发所述第一使用请求,所述第一使用请求附带所述使用权证书中的所述衍生数据使用公钥和经衍生数据使用私钥所作的签名;

所述数据萃取方与所述多个数据拥有方分别对所述第一使用请求进行验证;以及

响应于所述数据萃取方与所述多个数据拥有方中的任何一方对所述第一使用请求的验证不通过,拒绝所述第一使用请求。

3.根据权利要求2所述的访问控制方法,其特征在于,所述访问控制方法还包括:

响应于所述数据萃取方与所述多个数据拥有方中的每一方对所述第一使用请求的验证均通过,所述数据萃取方与所述多个数据拥有方以及所述数据使用方联合使用所述多个衍生数据碎片来执行所述数据使用方的目标任务。

4.根据权利要求2或3所述的访问控制方法,其特征在于,对所述第一使用请求进行验证包括:

验证所述第一使用请求中的所述衍生数据使用公钥是否在所述已授权公钥列表中;

验证针对所述衍生数据使用公钥的授权是否过期;以及

使用所述衍生数据使用公钥来对所述第一使用请求中的签名进行验签。

5.根据权利要求1至3中任一项所述的访问控制方法,其特征在于,所述多个衍生数据碎片通过以下操作来生成:

所述数据萃取方获得每个数据拥有方的数据使用证书;

所述数据萃取方根据每个数据拥有方的数据使用证书生成与该数据拥有方相对应的使用凭证;

所述数据萃取方向每个数据拥有方发送与该数据拥有方相对应的使用凭证;以及

响应于每个数据拥有方对与其相对应的使用凭证的验证均通过,所述数据萃取方和所述多个数据拥有方对所述多个数据拥有方各自拥有的原始数据进行联合萃取以生成所述多个衍生数据碎片。

6.根据权利要求5所述的访问控制方法,其特征在于,在生成所述多个衍生数据碎片的过程中,如果任一数据拥有方对与其相对应的使用凭证的验证不通过,则停止生成所述多个衍生数据碎片。

7.根据权利要求5所述的访问控制方法,其特征在于,所述数据萃取方获得每个数据拥有方的数据使用证书包括将每个数据拥有方作为目标数据拥有方并执行以下操作:

所述数据萃取方向所述目标数据拥有方发送第二证书请求,其中,所述第二证书请求附带所述数据萃取方的第二公钥;以及

所述数据萃取方从所述目标数据拥有方接收所述目标数据拥有方的数据使用证书,其中,所述目标数据拥有方的所述数据使用证书由所述目标数据拥有方使用所述目标数据拥有方的第一私钥来签发,所述目标数据拥有方的所述数据使用证书包括所述第二公钥,并且所述第二公钥被加入所述目标数据拥有方的已授权公钥列表。

8.根据权利要求7所述的访问控制方法,其特征在于,所述数据萃取方根据每个数据拥有方的数据使用证书生成与该数据拥有方相对应的使用凭证包括将每个数据拥有方作为目标数据拥有方并执行以下操作:

所述数据萃取方从所述目标数据拥有方的所述数据使用证书中取出所述第二公钥;

所述数据萃取方使用与所述第二公钥相对应的第二私钥对第二使用请求进行签名,其中,所述第二使用请求包括使用所述目标数据拥有方的指定数据的请求;以及

所述数据萃取方根据所述第二公钥和签名后的第二使用请求来生成所述使用凭证。

9.一种针对多方联合生成的衍生数据的访问控制装置,其特征在于,所述多方包括数据萃取方和多个数据拥有方,所述衍生数据被表征为多个衍生数据碎片,所述数据萃取方和所述多个数据拥有方各自拥有一个衍生数据碎片,所述访问控制装置包括:

至少一个处理器;以及

存储有计算机程序的至少一个存储器;

其中,当所述计算机程序由所述至少一个处理器执行时,使得所述访问控制装置执行根据权利要求1至8中任一项所述的访问控制方法的步骤。

10.一种存储有计算机程序的计算机可读存储介质,其特征在于,所述计算机程序在由处理器执行时实现根据权利要求1至8中任一项所述的访问控制方法的步骤。

针对多方联合生成的衍生数据的访问控制方法及装置

技术领域

[0001] 本公开的实施例涉及计算机技术领域,具体地,涉及针对多方联合生成的衍生数据的访问控制方法及装置。

背景技术

[0002] 在需要进行数据共享的场景中(例如数联网中)存在多种角色,其中存在一种数据商——数据萃取方,它本身不具有任何原始数据的所有权,它所具有的是数据价值提取技术(或称为数据价值萃取技术)。数据萃取方可以联合多方的原始数据作为原料数据产生出新的数据,这一新的数据称之为多方联合衍生数据(集),简称衍生数据。由于衍生数据在某些应用场景下具有优于原料数据的特点,因此衍生数据也可作为新的数据集参与到数联网的运作过程中。由于数据萃取方及多个原料数据的提供方均参与了数据萃取过程,因此萃取出的衍生数据实际应该是多方共有。并且多方联合衍生数据并不应单独完整存在于任何一个参与方的存储空间内(理想状况是衍生数据以多方碎片的形式存在于各方的存储空间内)。在实际访问衍生数据之前,需要对访问者是否具有对衍生数据的访问权限进行鉴定。在实际使用衍生数据时需要访问各个参与方的存储空间,当完成对各方数据的访问后,才能完成对衍生数据的访问。可以看出对于衍生数据的访问是对全体参与方的访问。因此,需要制定针对衍生数据的访问控制方法。

发明内容

[0003] 本文中描述的实施例提供了一种针对多方联合生成的衍生数据的访问控制方法、访问控制装置以及存储有计算机程序的计算机可读存储介质。

[0004] 根据本公开的第一方面,提供了一种针对多方联合生成的衍生数据的访问控制方法。多方包括数据萃取方和多个数据拥有方。衍生数据被表征为多个衍生数据碎片。数据萃取方和该多个数据拥有方各自拥有一个衍生数据碎片。访问控制方法包括:数据萃取方与该多个数据拥有方联合生成针对衍生数据的第一公钥和与第一公钥对应的私钥的多个私钥碎片,其中,数据萃取方和该多个数据拥有方各自拥有第一公钥和一个不同的私钥碎片;响应于数据萃取方接收到数据使用方对衍生数据的第一证书请求:数据萃取方向该多个数据拥有方分别转发第一证书请求,第一证书请求附带数据使用方的衍生数据使用公钥;数据萃取方与该多个数据拥有方分别将衍生数据使用公钥加入各自的已授权公钥列表;数据萃取方与该多个数据拥有方根据各自拥有的私钥碎片联合生成针对第一证书请求的多个签名碎片,其中,数据萃取方和该多个数据拥有方各自拥有一个签名碎片;数据萃取方根据从每个数据拥有方接收的签名碎片以及其自身拥有的签名碎片来合成签名,并根据所合成的签名来签发使用权证书,其中,使用权证书包括衍生数据使用公钥;以及数据萃取方向数据使用方发送使用权证书。

[0005] 在本公开的一些实施例中,访问控制方法还包括响应于数据萃取方接收到数据使用方对衍生数据的第一使用请求:数据萃取方向该多个数据拥有方分别转发第一使用请

求,第一使用请求附带使用权证书中的衍生数据使用公钥和经衍生数据使用私钥所作的签名;数据萃取方与该多个数据拥有方分别对第一使用请求进行验证;以及响应于数据萃取方与该多个数据拥有方中的任何一方对第一使用请求的验证不通过,拒绝第一使用请求。

[0006] 在本公开的一些实施例中,访问控制方法还包括:响应于数据萃取方与该多个数据拥有方中的每一方对第一使用请求的验证均通过,数据萃取方与该多个数据拥有方以及数据使用方联合使用该多个衍生数据碎片来执行数据使用方的目标任务。

[0007] 在本公开的一些实施例中,对第一使用请求进行验证包括:验证第一使用请求中的衍生数据使用公钥是否在已授权公钥列表中;验证针对衍生数据使用公钥的授权是否过期;以及使用衍生数据使用公钥来对第一使用请求中的签名进行验签。

[0008] 在本公开的一些实施例中,多个衍生数据碎片通过以下操作来生成:数据萃取方获得每个数据拥有方的数据使用证书;数据萃取方根据每个数据拥有方的数据使用证书生成与该数据拥有方相对应的使用凭证;数据萃取方向每个数据拥有方发送与该数据拥有方相对应的使用凭证;以及响应于每个数据拥有方对与其相对应的使用凭证的验证均通过,数据萃取方和多个数据拥有方对多个数据拥有方各自拥有的原始数据进行联合萃取以生成多个衍生数据碎片。

[0009] 在本公开的一些实施例中,在生成多个衍生数据碎片的过程中,如果任一数据拥有方对与其相对应的使用凭证的验证不通过,则停止生成多个衍生数据碎片。

[0010] 在本公开的一些实施例中,数据萃取方获得每个数据拥有方的数据使用证书包括将每个数据拥有方作为目标数据拥有方并执行以下操作:数据萃取方向目标数据拥有方发送第二证书请求,其中,第二证书请求附带数据萃取方的第二公钥;以及数据萃取方从目标数据拥有方接收目标数据拥有方的数据使用证书,其中,目标数据拥有方的数据使用证书由目标数据拥有方使用目标数据拥有方的第一私钥来签发,目标数据拥有方的数据使用证书包括第二公钥,并且第二公钥被加入目标数据拥有方的已授权公钥列表。

[0011] 在本公开的一些实施例中,数据萃取方根据每个数据拥有方的数据使用证书生成与该数据拥有方相对应的使用凭证包括将每个数据拥有方作为目标数据拥有方并执行以下操作:数据萃取方从目标数据拥有方的数据使用证书中取出第二公钥;数据萃取方使用与第二公钥相对应的第二私钥对第二使用请求进行签名,其中,第二使用请求包括使用目标数据拥有方的指定数据的请求;以及数据萃取方根据第二公钥和签名后的第二使用请求来生成使用凭证。

[0012] 根据本公开的第二方面,提供了一种针对多方联合生成的衍生数据的访问控制装置。该访问控制装置包括至少一个处理器;以及存储有计算机程序的至少一个存储器。当计算机程序由至少一个处理器执行时,使得访问控制装置执行根据本公开的第一方面所述的访问控制方法的步骤。

[0013] 根据本公开的第三方面,提供了一种存储有计算机程序的计算机可读存储介质,其中,计算机程序在由处理器执行时实现根据本公开的第一方面所述的访问控制方法的步骤。

附图说明

[0014] 为了更清楚地说明本公开的实施例的技术方案,下面将对实施例的附图进行简要

说明,应当知道,以下描述的附图仅仅涉及本公开的一些实施例,而非对本公开的限制,其中:

[0015] 图1是数联网的示意性拓扑图;

[0016] 图2是根据本公开的实施例的针对多方联合生成的衍生数据的访问控制方法的示意性流程图;

[0017] 图3是根据本公开的实施例的数据萃取方与多个数据拥有方联合生成衍生数据的示意性流程图和信令方案;

[0018] 图4是根据本公开的实施例的数据萃取方与多个数据拥有方联合生成针对衍生数据的第一公钥和多个私钥碎片的示意性流程图和信令方案;

[0019] 图5是根据本公开的实施例的数据萃取方与多个数据拥有方联合生成使用权证书的示意性流程图和信令方案;

[0020] 图6是根据本公开的实施例的数据萃取方与多个数据拥有方及数据使用方联合使用衍生数据的示意性流程图和信令方案;

[0021] 图7是根据本公开的实施例的针对多方联合生成的衍生数据的访问控制装置的示意性框图。

[0022] 在附图中,最后两位数字相同的标记对应于相同的元素。需要注意的是,附图中的元素是示意性的,没有按比例绘制。

具体实施方式

[0023] 为了使本公开的实施例的目的、技术方案和优点更加清楚,下面将结合附图,对本公开的实施例的技术方案进行清楚、完整的描述。显然,所描述的实施例是本公开的一部分实施例,而不是全部的实施例。基于所描述的本公开的实施例,本领域技术人员在无需创造性劳动的前提下所获得的所有其它实施例,也都属于本公开保护的范围。

[0024] 除非另外定义,否则在此使用的所有术语(包括技术和科学术语)具有与本公开主题所属领域的技术人员所通常理解的相同含义。进一步将理解的是,诸如在通常使用的词典中定义的那些的术语应解释为具有与说明书上下文和相关技术中它们的含义一致的含义,并且将不以理想化或过于正式的形式来解释,除非在此另外明确定义。另外,诸如“第一”和“第二”的术语仅用于将一个部件(或部件的一部分)与另一个部件(或部件的另一部分)区分开。

[0025] 图1示出数联网的示意性拓扑图。数联网可包括多个子网10。每个子网10包括枢纽节点11和与枢纽节点直接连接的多个参与节点12。该多个子网10中的枢纽节点11相互直接连接。枢纽节点11与枢纽节点11之间可以通过专网进行互联。枢纽节点11承担对参与节点12进行信息聚合、寻址导航等功能。参与节点12可以是各类政务主体、行业主体、公司主体、机构主体等。直接连接到同一个枢纽节点11的参与节点12通过该枢纽节点11进行通信。直接连接到不同枢纽节点11的参与节点12通过它们各自直接连接的枢纽节点11进行通信。也就是说,参与节点12只与其直接连接的枢纽节点11直接通信,枢纽节点11之间可直接通信,而参与节点12之间需经由相应的枢纽节点11进行通信。

[0026] 在数联网中可能存在多种角色,包括数据商——数据萃取方。数据萃取方可以联合多个参与节点12的原始数据作为原料数据产生出衍生数据。图2示出根据本公开的实施

例的针对多方联合生成的衍生数据的访问控制方法的示意性流程图。在这里,衍生数据被表征为多个衍生数据碎片。数据萃取方和该多个数据拥有方各自拥有一个衍生数据碎片。图3示出根据本公开的实施例的数据萃取方与多个数据拥有方联合生成衍生数据的示意性流程图和信令方案。假设有3个数据拥有方P1、P2和P3。数据拥有方P1拥有原始数据D1。数据拥有方P2拥有原始数据D2。数据拥有方P3拥有原始数据D3。数据萃取方R希望从原始数据D1、D2和D3中萃取出衍生数据。

[0027] 在生成衍生数据的过程中,如图3所示,数据萃取方R获得每个数据拥有方的数据使用证书(即,D1、D2和D3的数据使用证书)。在动作302,数据萃取方R根据每个数据拥有方的数据使用证书生成与该数据拥有方相对应的使用凭证。例如,数据萃取方R根据数据拥有方P1的针对D1的数据使用证书生成针对D1的使用凭证。数据萃取方R根据数据拥有方P2的针对D2的数据使用证书生成针对D2的使用凭证。数据萃取方R根据数据拥有方P3的针对D3的数据使用证书生成针对D3的使用凭证。然后,在动作304,数据萃取方R向每个数据拥有方发送与该数据拥有方相对应的使用凭证。如果每个数据拥有方对与其相对应的使用凭证的验证均通过(P1对D1的凭证的验证通过,P2对D2的凭证的验证通过,P3对D3的凭证的验证通过),则在动作306数据萃取方R和多个数据拥有方P1、P2和P3对多个数据拥有方P1、P2和P3各自拥有的原始数据D1、D2和D3进行联合萃取以生成多个衍生数据碎片G0、G1、G2和G3。数据萃取方R拥有衍生数据碎片G0。数据拥有方P1拥有衍生数据碎片G1。数据拥有方P2拥有衍生数据碎片G2。数据拥有方P3拥有衍生数据碎片G3。

[0028] 在本公开的一些实施例中,在生成多个衍生数据碎片的过程中,如果任一数据拥有方对与其相对应的使用凭证的验证不通过,则停止生成多个衍生数据碎片。

[0029] 在本公开的一些实施例中,数据萃取方获得每个数据拥有方的数据使用证书包括将每个数据拥有方作为目标数据拥有方并执行以下操作:数据萃取方向目标数据拥有方发送第二证书请求,其中,第二证书请求附带数据萃取方的第二公钥,第二证书请求包括获得目标数据拥有方的指定数据使用权限的请求;以及数据萃取方从目标数据拥有方接收目标数据拥有方的数据使用证书。其中,目标数据拥有方的数据使用证书由目标数据拥有方使用目标数据拥有方的第一私钥来签发,目标数据拥有方的数据使用证书包括第二公钥,并且第二公钥被加入目标数据拥有方的已授权公钥列表。

[0030] 在本公开的一些实施例中,数据萃取方根据每个数据拥有方的数据使用证书生成与该数据拥有方相对应的使用凭证包括将每个数据拥有方作为目标数据拥有方并执行以下操作:数据萃取方从目标数据拥有方的数据使用证书中取出第二公钥;数据萃取方使用与第二公钥相对应的第二私钥对第二使用请求进行签名,其中,第二使用请求包括使用目标数据拥有方的指定数据的请求;以及数据萃取方根据第二公钥和签名后的第二使用请求来生成使用凭证。也就是说,使用凭证包括第二公钥和签名后的第二使用请求。

[0031] 回到图2,在框S202处,数据萃取方与该多个数据拥有方联合生成针对衍生数据的第一公钥和与第一公钥对应的私钥的多个私钥碎片(相当于对衍生数据的访问控制凭证)。其中,数据萃取方和该多个数据拥有方各自拥有第一公钥和一个不同的私钥碎片。图4示出根据本公开的实施例的数据萃取方与多个数据拥有方联合生成针对衍生数据的第一公钥和多个私钥碎片的示意性流程图和信令方案。假设有3个数据拥有方P1、P2和P3。数据萃取方R与数据拥有方P1、P2和P3在动作402处联合生成针对衍生数据的第一公钥GPK和多个私

钥碎片GSK0、GSK1、GSK2、GSK3。其中,数据萃取方R拥有第零私钥碎片GSK0和第一公钥GPK。数据拥有方P1拥有第一私钥碎片GSK1和第一公钥GPK。数据拥有方P2拥有第二私钥碎片GSK2和第一公钥GPK。数据拥有方P3拥有第三私钥碎片GSK1和第一公钥GPK。

[0032] 回到图2,在框S204处,确定数据萃取方是否接收到数据使用方对衍生数据的第一证书请求。第一证书请求附带数据使用方的衍生数据使用公钥。第一证书请求包括获得衍生数据使用权限的请求。

[0033] 如果数据萃取方接收到数据使用方对衍生数据的第一证书请求(在框S204处为“是”),则在框S206处数据萃取方向该多个数据拥有方分别转发第一证书请求。在框S208处,数据萃取方与该多个数据拥有方分别将衍生数据使用公钥加入各自的已授权公钥列表。在框S210处,数据萃取方与该多个数据拥有方根据各自拥有的私钥碎片联合生成针对第一证书请求的多个签名碎片。其中,数据萃取方和该多个数据拥有方各自拥有一个签名碎片。在框S212处,数据萃取方根据从每个数据拥有方接收的签名碎片以及其自身拥有的签名碎片来合成签名,并根据所合成的签名来签发使用权证书。其中,使用权证书包括衍生数据使用公钥。在框S214处,数据萃取方向数据使用方发送使用权证书。

[0034] 图5示出根据本公开的实施例的数据萃取方与多个数据拥有方联合生成使用权证书的示意性流程图和信令方案。数据使用方U拥有成对的衍生数据使用公钥UPK和衍生数据使用私钥USK。数据使用方U在动作502处向数据萃取方R发送第一证书请求Q。第一证书请求Q附带数据使用方的衍生数据使用公钥UPK。数据萃取方R在接收到第一证书请求Q之后,在动作504分别向数据拥有方P1、P2和P3转发第一证书请求Q。然后,在动作505,数据萃取方R与数据拥有方P1、P2和P3联合生成针对第一证书请求的多个签名碎片。数据萃取方R拥有签名碎片S0。数据拥有方P1拥有签名碎片S1。数据拥有方P2拥有签名碎片S2。数据拥有方P3拥有签名碎片S3。数据拥有方P1在动作506向数据萃取方R发送签名碎片S1。数据拥有方P2在动作507向数据萃取方R发送签名碎片S2。数据拥有方P3在动作508向数据萃取方R发送签名碎片S3。在动作510,数据萃取方R从签名碎片S0、S1、S2、S3恢复出签名,并将该签名潜入进使用权证书。然后,数据萃取方R在动作512向数据使用方U发送使用权证书。

[0035] 数据使用方U获得使用权证书之后相当于获得了对衍生数据的使用权限。图6示出根据本公开的实施例的数据萃取方与多个数据拥有方及数据使用方联合使用衍生数据的示意性流程图和信令方案。在数据使用方U需要实际使用衍生数据的情况下,数据使用方U在动作602向数据萃取方R发送对衍生数据的第一使用请求UQ。数据萃取方在动作604向该多个数据拥有方P1、P2、P3分别转发第一使用请求UQ。第一使用请求UQ附带使用权证书中的衍生数据使用公钥UPK和经衍生数据使用私钥USK所作的签名。数据萃取方R与该多个数据拥有方P1、P2、P3分别对第一使用请求UQ进行验证。如果数据萃取方R与该多个数据拥有方P1、P2、P3中的任何一方对第一使用请求UQ的验证不通过,则第一使用请求UQ会被拒绝。

[0036] 在图6的示例中,数据萃取方R在动作606处对第一使用请求UQ进行验证。如果验证通过,则数据萃取方R引用衍生数据碎片G0,否则终止联合使用该多个衍生数据碎片的过程。数据拥有方P1在动作607处对第一使用请求UQ进行验证。如果验证通过,则数据萃取方R引用衍生数据碎片G1,否则终止联合使用该多个衍生数据碎片的过程。数据拥有方P2在动作608处对第一使用请求UQ进行验证。如果验证通过,则数据萃取方R引用衍生数据碎片G2,否则终止联合使用该多个衍生数据碎片的过程。数据拥有方P3在动作609处对第一使用请

求UQ进行验证。如果验证通过,则数据萃取方R引用衍生数据碎片G3,否则终止联合使用该多个衍生数据碎片的过程。

[0037] 如果数据萃取方R与该多个数据拥有方P1、P2、P3中的每一方对第一使用请求UQ的验证均通过,则在动作610处数据萃取方R与该多个数据拥有方P1、P2、P3以及数据使用方U联合使用该多个衍生数据碎片G0、G1、G2、G3来执行数据使用方U的目标任务。

[0038] 在本公开的一些实施例中,对第一使用请求UQ进行验证包括:验证第一使用请求UQ中的衍生数据使用公钥UPK是否在已授权公钥列表中;验证针对衍生数据使用公钥UPK的授权是否过期;以及使用衍生数据使用公钥UPK来对第一使用请求UQ中的签名进行验签。

[0039] 图7是根据本公开的实施例的针对多方联合生成的衍生数据的访问控制装置700的示意性框图。多方包括数据萃取方和多个数据拥有方。衍生数据被表征为多个衍生数据碎片。数据萃取方和该多个数据拥有方各自拥有一个衍生数据碎片。如图7所示,该访问控制装置700可包括处理器710和存储有计算机程序的存储器720。当计算机程序由处理器710执行时,使得访问控制装置700可执行如图2所示的方法200的步骤。在一个示例中,访问控制装置700可以是计算机设备或云计算节点。访问控制装置700可位于数据萃取方处。访问控制装置700可与多个数据拥有方联合生成针对衍生数据的第一公钥和与第一公钥对应的私钥的多个私钥碎片,其中,访问控制装置700和该多个数据拥有方各自拥有第一公钥和一个不同的私钥碎片。响应于访问控制装置700接收到数据使用方对衍生数据的第一证书请求:访问控制装置700可向该多个数据拥有方分别转发第一证书请求,第一证书请求附带数据使用方的衍生数据使用公钥;访问控制装置700可与该多个数据拥有方分别将衍生数据使用公钥加入各自的已授权公钥列表;访问控制装置700可与该多个数据拥有方根据各自拥有的私钥碎片联合生成针对第一证书请求的多个签名碎片,其中,访问控制装置700和该多个数据拥有方各自拥有一个签名碎片;访问控制装置700可根据从每个数据拥有方接收的签名碎片以及其自身拥有的签名碎片来合成签名,并根据所合成的签名来签发使用权证书,其中,使用权证书包括衍生数据使用公钥;以及访问控制装置700可向数据使用方发送使用权证书。

[0040] 在本公开的实施例中,处理器710可以是例如中央处理单元(CPU)、微处理器、数字信号处理器(DSP)、基于多核的处理器架构的处理器等。存储器720可以是使用数据存储技术实现的任何类型的存储器,包括但不限于随机存取存储器、只读存储器、基于半导体的存储器、闪存、磁盘存储器等。

[0041] 此外,在本公开的实施例中,访问控制装置700也可包括输入设备730,例如键盘、鼠标等,用于输入数据萃取指令等。另外,访问控制装置700还可包括输出设备740,例如显示器等,用于输出联合使用衍生数据的执行结果等。

[0042] 在本公开的其它实施例中,还提供了一种存储有计算机程序的计算机可读存储介质,其中,计算机程序在由处理器执行时能够实现如图2所示的方法的步骤。

[0043] 综上所述,根据本公开的实施例的针对多方联合生成的衍生数据的访问控制方法将衍生数据的所有权归属给各个原料数据方(数据拥有方)以及数据萃取方,为后续访问该衍生数据提供了很好的访问控制逻辑。对于数据使用方来说,使用衍生数据的流程与使用原始数据的流程是相同的。数据使用方可以像使用原始数据一样使用衍生数据。在使用衍生数据的过程中,数据使用方只需像使用原始数据一样,向数据萃取方(或者衍生数据代理

方)提供使用凭证即可。由于衍生数据是以碎片态的形式被使用,因此不会暴露衍生数据的隐私信息。此外,衍生数据的使用还为原始数据提供任意层次萃取的可能性。例如,可以从原始数据生成一级衍生数据,再从一级衍生数据生成二级衍生数据,以此类推。

[0044] 附图中的流程图和框图显示了根据本公开的多个实施例的装置和方法的可能实现的体系架构、功能和操作。在这点上,流程图或框图中的每个方框可以代表一个模块、程序段或指令的一部分,所述模块、程序段或指令的一部分包含一个或多个用于实现规定的逻辑功能的可执行指令。在有些作为替换的实现中,方框中所标注的功能也可以以不同于附图中所标注的顺序发生。例如,两个连续的方框实际上可以基本并行地执行,它们有时也可以按相反的顺序执行,这依所涉及的功能而定。也要注意的是,框图和/或流程图中的每个方框、以及框图和/或流程图中的方框的组合,可以用执行规定的功能或动作的专用的基于硬件的系统来实现,或者可以用专用硬件与计算机指令的组合来实现。

[0045] 除非上下文中另外明确地指出,否则在本文和所附权利要求中所使用的词语的单数形式包括复数,反之亦然。因而,当提及单数时,通常包括相应术语的复数。相似地,措辞“包含”和“包括”将解释为包含在内而不是独占性地。同样地,术语“包括”和“或”应当解释为包括在内的,除非本文中明确禁止这样的解释。在本文中使用术语“示例”之处,特别是当其位于一组术语之后时,所述“示例”仅仅是示例性的和阐述性的,且不应当被认为是独占性的或广泛性的。

[0046] 适应性的进一步的方面和范围从本文中提供的描述变得明显。应当理解,本申请的各个方面可以单独或者与一个或多个其它方面组合实施。还应当理解,本文中的描述和特定实施例旨在仅说明的目的并不旨在限制本申请的范围。

[0047] 以上对本公开的若干实施例进行了详细描述,但显然,本领域技术人员可以在不脱离本公开的精神和范围的情况下对本公开的实施例进行各种修改和变型。本公开的保护范围由所附的权利要求限定。

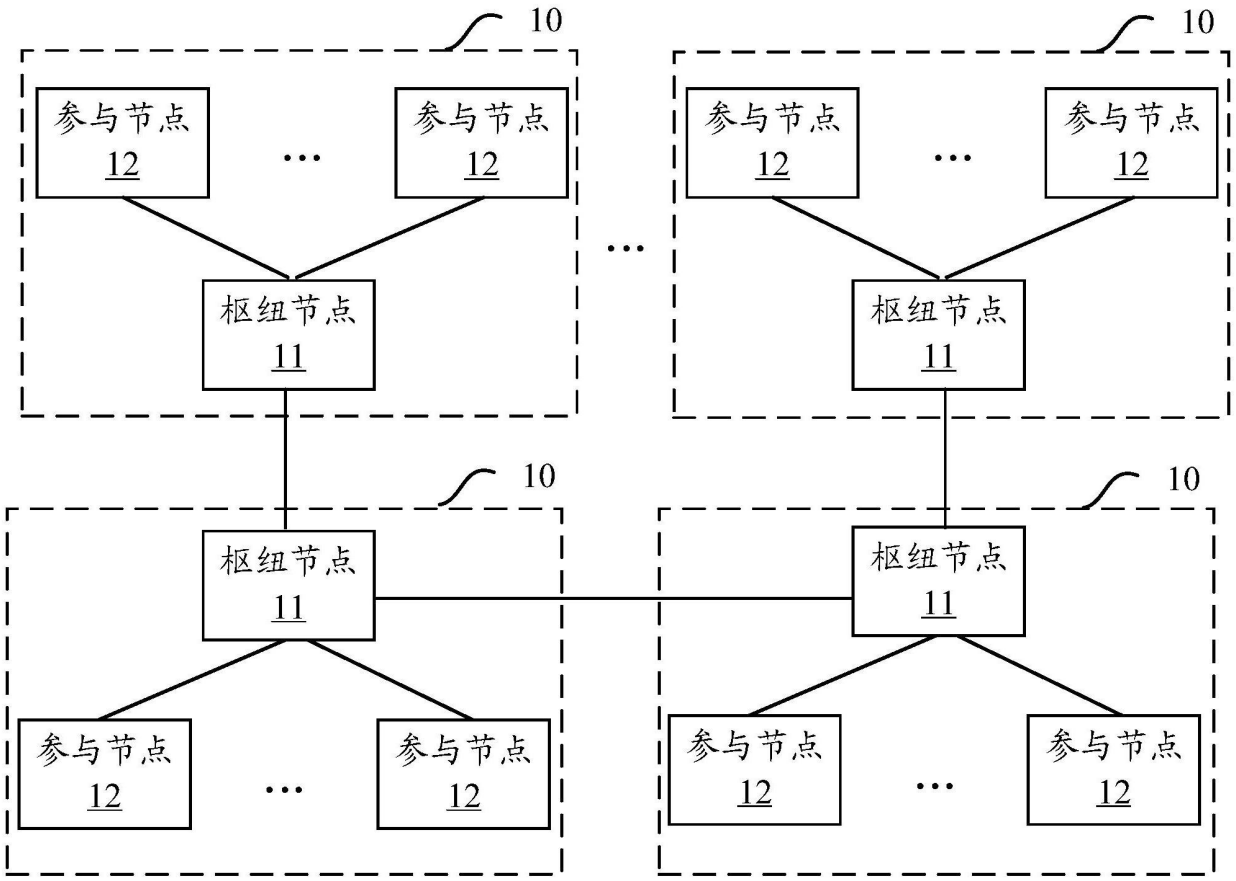

10
参与节点
12
参与节点
12
枢纽节点
11
10
参与节点
12
参与节点
12
枢纽节点
11
10
枢纽节点
11
参与节点
12
参与节点
12
10
枢纽节点
11
参与节点
12
参与节点
12

图1

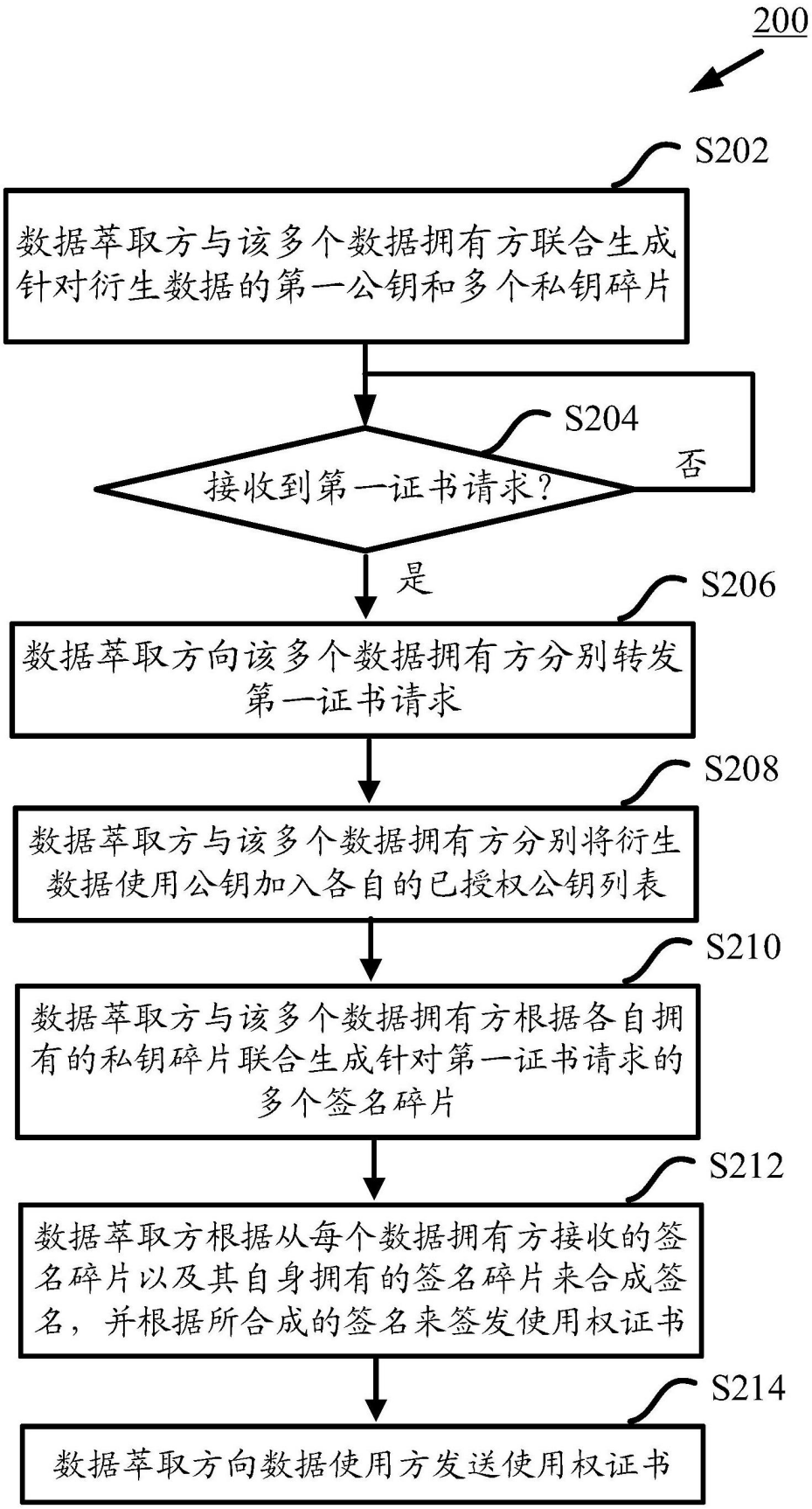

200
S202
数据萃取方与该多个数据拥有方联合生成针对衍生数据的第一公钥和多个私钥碎片
S204
接收到第一证书请求?
否
是
S206
数据萃取方向该多个数据拥有方分别转发第一证书请求
S208
数据萃取方与该多个数据拥有方分别将衍生数据使用公钥加入各自的已授权公钥列表
S210
数据萃取方与该多个数据拥有方根据各自拥有的私钥碎片联合生成针对第一证书请求的多个签名碎片
S212
数据萃取方根据从每个数据拥有方接收的签名碎片以及其自身拥有的签名碎片来合成签名，并根据所合成的签名来签发使用权证书
S214
数据萃取方向数据使用方发送使用权证书

图2

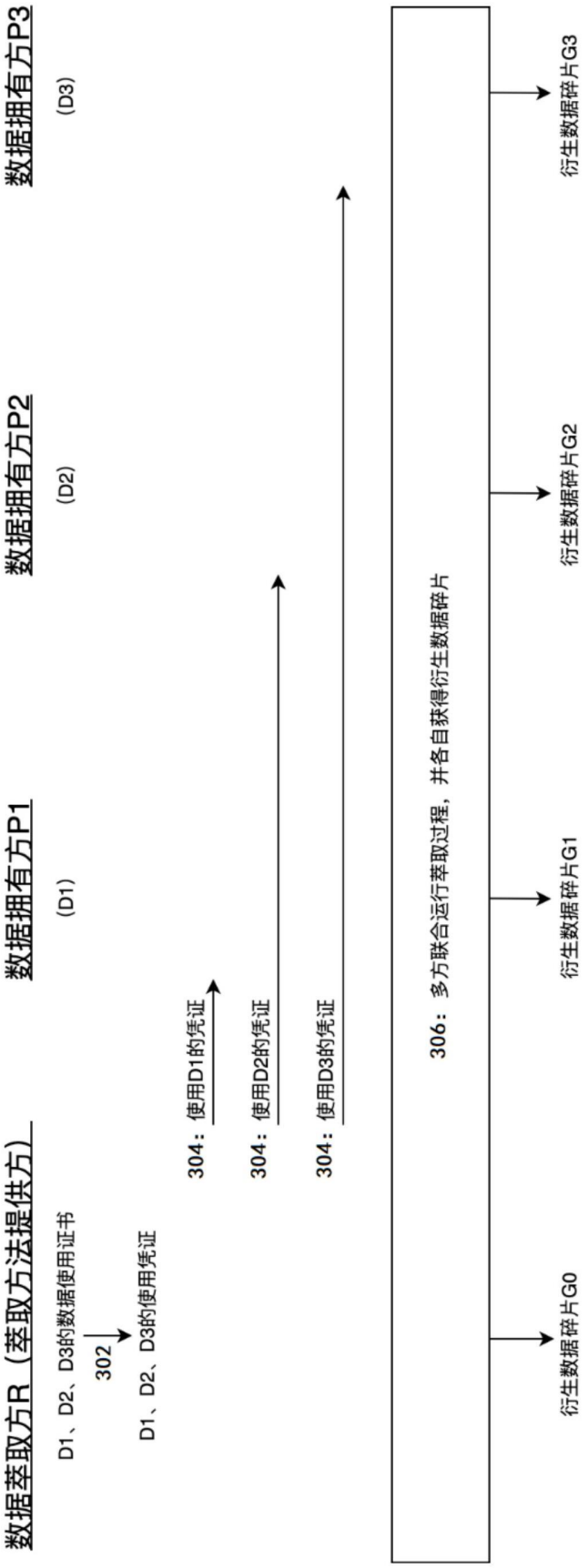

数据萃取方R（萃取方法提供方）
数据拥有方P1
(D1)
数据拥有方P2
(D2)
数据拥有方P3
(D3)
D1、D2、D3的数据使用证书
302
D1、D2、D3的使用凭证
304：使用D1的凭证
304：使用D2的凭证
304：使用D3的凭证
306：多方联合运行萃取过程，并各自获得衍生数据碎片
衍生数据碎片G0
衍生数据碎片G1
衍生数据碎片G2
衍生数据碎片G3

图3

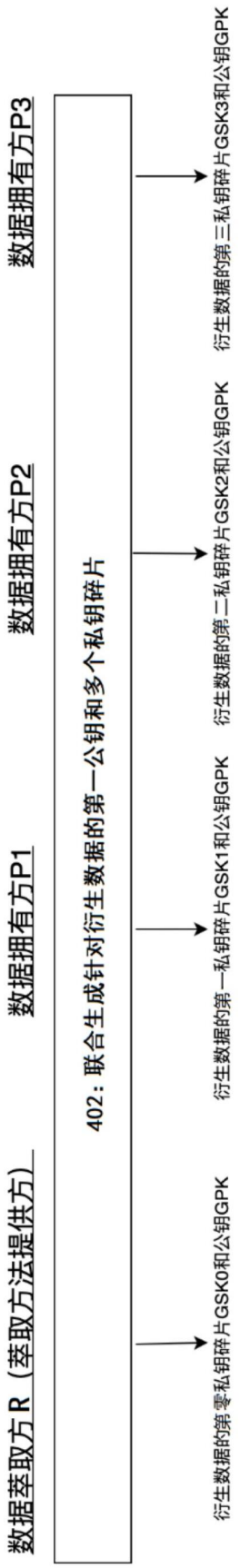

数据萃取方R（萃取方法提供方）
数据拥有方P1
数据拥有方P2
数据拥有方P3
402：联合生成针对衍生数据的第一公钥和多个私钥碎片
衍生数据的第零私钥碎片GSK0和公钥GPK
衍生数据的第一私钥碎片GSK1和公钥GPK
衍生数据的第二私钥碎片GSK2和公钥GPK
衍生数据的第三私钥碎片GSK3和公钥GPK

图4

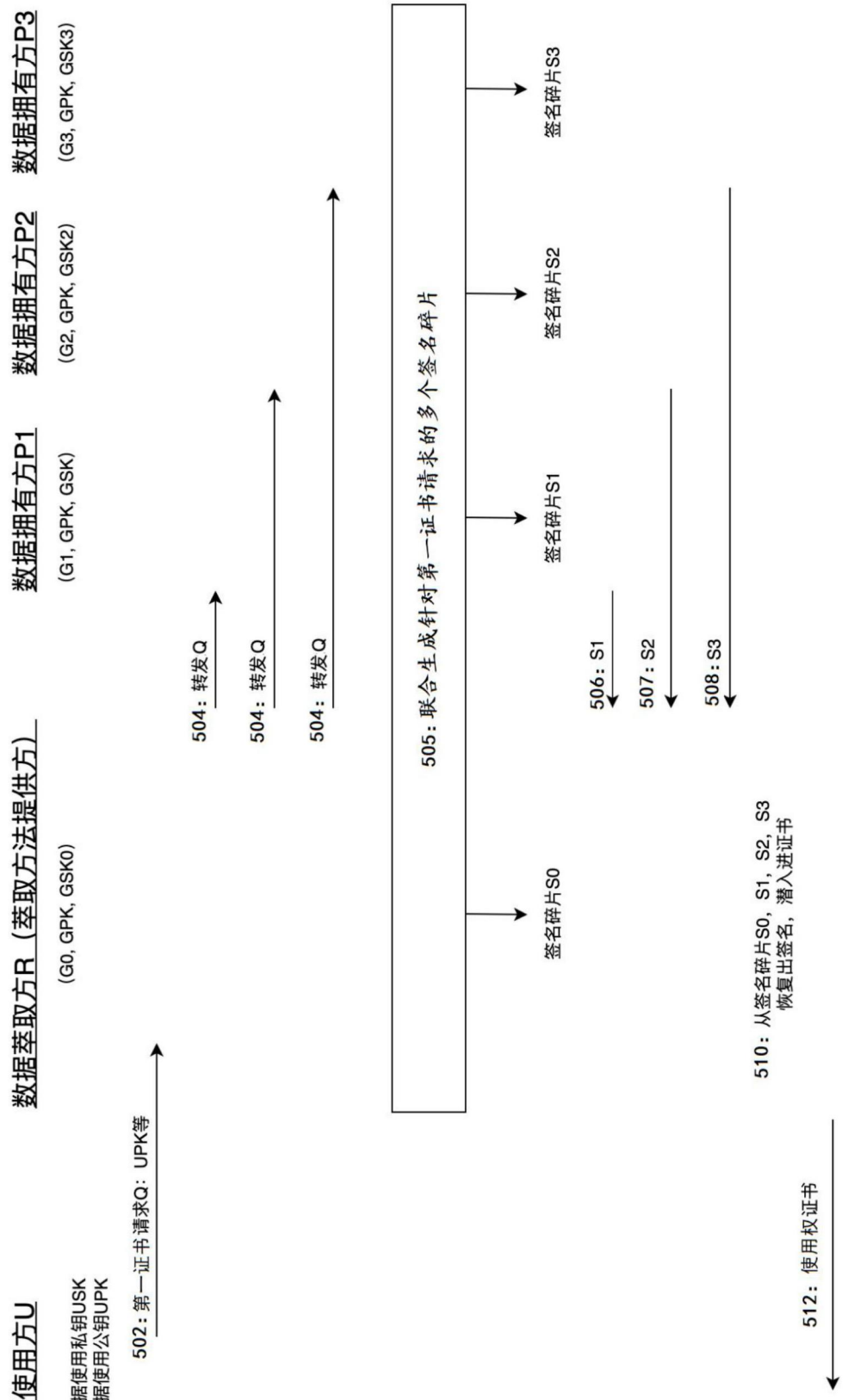

数据使用方U
数据萃取方R（萃取方法提供方）
(G0, GPK, GSK0)
数据拥有方P1
(G1, GPK, GSK)
数据拥有方P2
(G2, GPK, GSK2)
数据拥有方P3
(G3, GPK, GSK3)
衍生数据使用私钥USK
衍生数据使用公钥UPK
502：第一证书请求Q：UPK等
504：转发Q
504：转发Q
504：转发Q
505：联合生成针对第一证书请求的多个签名碎片
签名碎片S0
签名碎片S1
签名碎片S2
签名碎片S3
506：S1
507：S2
508：S3
510：从签名碎片S0，S1，S2，S3
恢复出签名，潜入进证书
512：使用权证书

图5

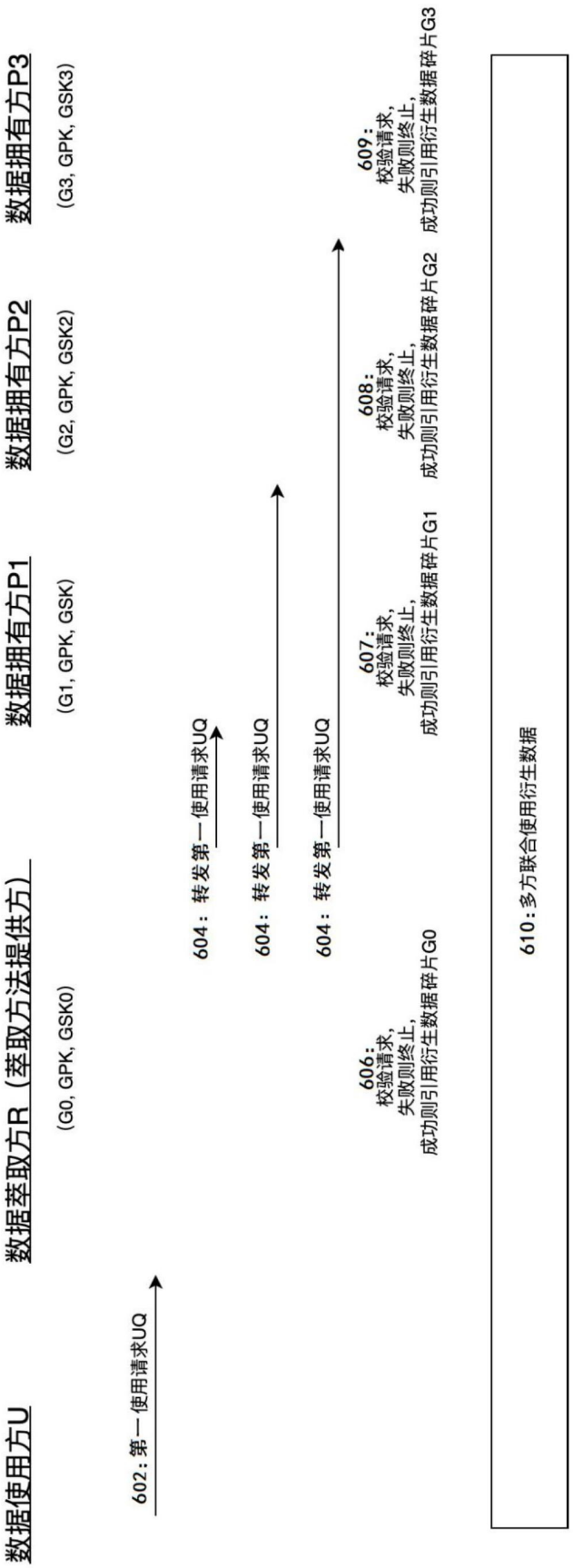

数据使用方U
数据萃取方R（萃取方法提供方）
(G0, GPK, GSK0)
数据拥有方P1
(G1, GPK, GSK)
数据拥有方P2
(G2, GPK, GSK2)
数据拥有方P3
(G3, GPK, GSK3)
602：第一使用请求UQ
604：转发第一使用请求UQ
604：转发第一使用请求UQ
604：转发第一使用请求UQ
606：
校验请求，
失败则终止，
成功则引用衍生数据碎片G0
607：
校验请求，
失败则终止，
成功则引用衍生数据碎片G1
608：
校验请求，
失败则终止，
成功则引用衍生数据碎片G2
609：
校验请求，
失败则终止，
成功则引用衍生数据碎片G3
610：多方联合使用衍生数据

图6

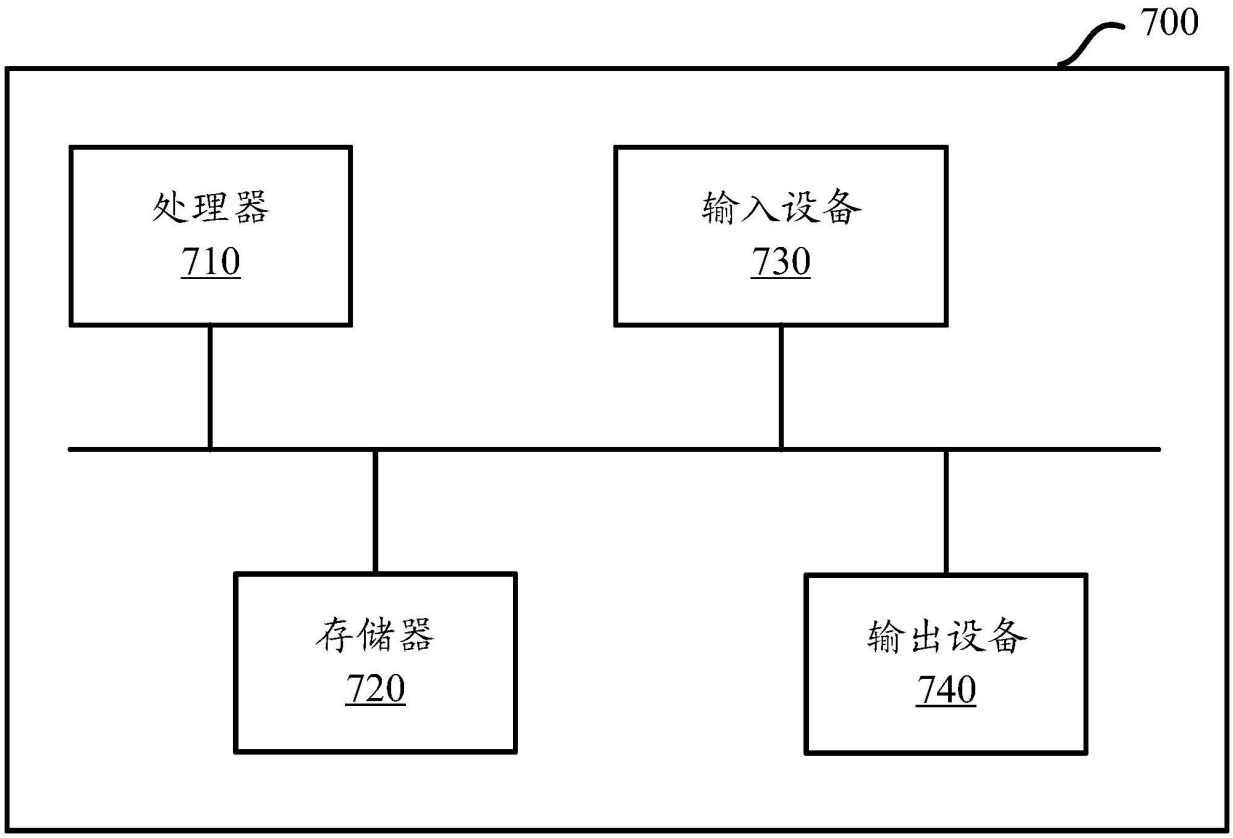


图7