(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 117688588 A
(43)申请公布日 2024.03.12

(21)申请号 202311760492.X

(22)申请日 2023.12.20

(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 石代蒙

(51)Int.Cl.
G06F 21/60(2013.01)
G06F 16/22(2019.01)
G06F 16/245(2019.01)
G06F 7/58(2006.01)

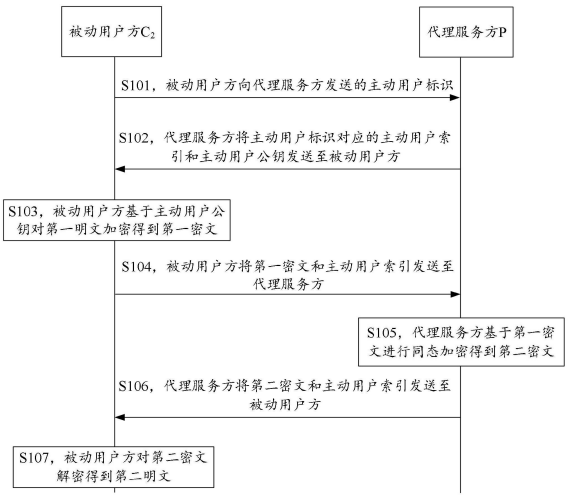
权利要求书3页 说明书11页 附图5页

(54)发明名称

相关随机性的生成方法及装置

(57)摘要

本公开的实施例提供一种相关随机性的生成方法及装置。该方法由代理服务方执行,包括:接收被动用户方发送的主动用户标识;将主动用户标识对应的主动用户公钥发送至被动用户方,以使被动用户方基于主动用户公钥对第一明文加密得到第一密文;接收被动用户方发送的第一密文;基于第一密文进行同态加密得到第二密文,并将第二密文发送至被动用户方,以使被动用户方对第二密文解密得到第二明文;其中,被动用户方拥有的第一明文碎片与主动用户方拥有的第二明文碎片构成一组相关随机性关系,第一明文碎片包括第一明文和第二明文。该方法不仅可以避免线上资源的浪费,解决用户不友好的问题,而且可以加速线上的计算,从而提升用户体验。



CN 117688588 A

1.一种相关随机性的生成方法,其特征在于,应用于相关随机性的生成系统,所述相关随机性的生成系统包括代理服务方、主动用户方和被动用户方,所述方法由所述代理服务方执行;所述方法包括:

接收所述被动用户方发送的主动用户标识;

将所述主动用户标识对应的主动用户索引和主动用户公钥发送至所述被动用户方,以使所述被动用户方基于所述主动用户公钥对第一明文加密得到第一密文;

接收所述被动用户方发送的所述第一密文和所述主动用户索引;

基于所述第一密文进行同态加密得到第二密文,并将所述主动用户索引和所述第二密文发送至所述被动用户方,以使所述被动用户方对所述第二密文解密得到第二明文;

其中,所述被动用户方拥有的第一明文碎片与所述主动用户方拥有的第二明文碎片构成一组相关随机性关系,所述第一明文碎片包括所述第一明文和所述第二明文。

2.根据权利要求1所述的方法,其特征在于,所述基于所述第一密文进行同态加密得到第二密文包括:

将所述第一密文和第三密文相乘再与第四密文相加,得到所述第二密文;其中,所述第三密文为所述主动用户方基于所述主动用户公钥对第三明文加密得到的,所述第四密文为所述主动用户方基于所述主动用户公钥对第四明文加密得到的,所述第二明文碎片包括所述第三明文和所述第四明文。

3.根据权利要求1或2所述的方法,其特征在于,所述方法还包括:

删除所述主动用户标识及其对应的主动用户参数信息,所述主动用户参数信息包括所述主动用户公钥和所述主动用户索引。

4.根据权利要求1或2所述的方法,其特征在于,所述将所述主动用户标识对应的主动用户索引和主动用户公钥发送至所述被动用户方之前,还包括:

查询所述主动用户标识;

确定是否存在所述主动用户索引和所述主动用户公钥。

5.根据权利要求1或2所述的方法,其特征在于,所述所述接收被动用户方发送的主动用户标识之前,还包括:

接收并存储所述主动用户方发送的所述主动用户标识及其对应的主动用户参数信息,所述主动用户参数信息包括所述主动用户公钥和所述主动用户索引。

6.一种相关随机性的生成方法,其特征在于,应用于相关随机性的生成系统,所述相关随机性的生成系统包括代理服务方、主动用户方和被动用户方,所述方法由所述被动用户方执行;所述方法包括:

向所述代理服务方发送主动用户标识;

接收所述代理服务方发送的所述主动用户标识对应的主动用户索引和主动用户公钥;

基于所述主动用户公钥对第一明文加密得到第一密文,并将所述第一密文和所述主动用户索引发送至所述代理服务方,以使所述代理服务方基于所述第一密文进行同态加密得到第二密文;

接收所述代理服务方发送的所述主动用户索引和所述第二密文;

对所述第二密文解密得到第二明文;

其中,所述被动用户方拥有的第一明文碎片与所述主动用户方拥有的第二明文碎片构

成一组相关随机性关系,所述第一明文碎片包括所述第一明文和所述第二明文。

7.根据权利要求6所述的方法,其特征在于,所述对所述第二密文解密得到第二明文之前,还包括:

向所述主动用户方发送所述主动用户索引;

接收所述主动用户方发送的所述主动用户索引对应的主动用户私钥;

所述对所述第二密文解密得到第二明文包括:

基于所述主动用户私钥对所述第二密文解密得到所述第二明文。

8.一种相关随机性的生成装置,其特征在于,应用于相关随机性的生成系统,所述相关随机性的生成系统包括代理服务方、主动用户方和被动用户方,所述装置包括:

接收模块,用于接收被动用户方发送的主动用户标识;

发送模块,用于将所述主动用户标识对应的主动用户索引和主动用户公钥发送至所述被动用户方,以使所述被动用户方基于所述主动用户公钥对第一明文加密得到第一密文;

接收模块,还用于接收所述被动用户方发送的所述第一密文和所述主动用户索引;

加密模块,用于基于所述第一密文进行同态加密得到第二密文;

发送模块,还用于将所述主动用户索引和所述第二密文发送至所述被动用户方,以使所述被动用户方对所述第二密文解密得到第二明文;

其中,所述被动用户方拥有的第一明文碎片与主动用户方拥有的第二明文碎片构成一组相关随机性关系,所述第一明文碎片包括所述第一明文和所述第二明文。

9.一种相关随机性的生成装置,其特征在于,应用于相关随机性的生成系统,所述相关随机性的生成系统包括代理服务方、主动用户方和被动用户方,所述装置包括:

发送模块,用于向代理服务方发送主动用户标识;

接收模块,用于接收所述代理服务方发送的所述主动用户标识对应的主动用户索引和主动用户公钥;

加密模块,基于所述主动用户公钥对第一明文加密得到第一密文;

发送模块,还用于将所述第一密文和所述主动用户索引发送至所述代理服务方,以使所述代理服务方基于所述第一密文进行同态加密得到第二密文;

接收模块,还用于接收所述代理服务方发送的所述主动用户索引和所述第二密文;

解密模块,用于对所述第二密文解密得到第二明文;

其中,所述被动用户方拥有的第一明文碎片与主动用户方拥有的第二明文碎片构成一组相关随机性关系,所述第一明文碎片包括所述第一明文和所述第二明文。

10.一种相关随机性的生成系统,其特征在于,包括:代理服务方、主动用户方和被动用户方,其中,所述主动用户方拥有第二明文碎片;

所述被动用户方,用于向所述代理服务方发送主动用户标识;

所述代理服务方,用于接收所述被动用户方发送的所述主动用户标识,并将所述主动用户标识对应的主动用户索引和主动用户公钥发送至所述被动用户方;

所述被动用户方,还用于接收所述代理服务方发送的所述主动用户索引和所述主动用户公钥,基于所述主动用户公钥对第一明文加密得到第一密文,并将所述第一密文和所述主动用户索引发送至所述代理服务方;

所述代理服务方,还用于接收所述被动用户方发送的所述第一密文和所述主动用户索

引,基于所述第一密文进行同态加密得到第二密文,并将所述主动用户索引和所述第二密文发送至所述被动用户方;

所述被动用户方,还用于接收所述代理服务方发送的所述主动用户索引和所述第二密文,并对所述第二密文解密得到第二明文;

其中,所述被动用户方拥有的第一明文碎片与所述第二明文碎片构成一组相关随机性关系,所述第一明文碎片包括所述第一明文和所述第二明文。

相关随机性的生成方法及装置

技术领域

[0001] 本公开的实施例涉及联合计算技术领域,具体地,涉及相关随机性的生成方法及装置。

背景技术

[0002] 在隐私保护的计算领域,大量的使用到了密码学的计算,并且大多数方案都需要进行非对称密码计算操作和/或对称密码计算操作,以实现不同的功能。从这两种操作在消耗计算资源方面来看,非对称密码计算操作的消耗要远高于对称密码计算操作。因此一个优化方向是降低非对称密码操作的实际使用量。在具体实现中,通常把非对称密码操作提前到线下做预计算,实际线上计算时只需使用这些线下预计算的结果来作后续的计算。

[0003] 在多方联合计算中,通常需要联合计算一个相关的随机性,相关随机性必须使用非对称密码操作才能产生,故而通常是在线下生成这种相关随机性资源,以加速线上的计算。然而在上层应用中,线下计算获取相关随机性通常对于用户并不友好,例如在没有进行用户意义上真正的应用之前就有所操作(例如操作网络资源形成网络流量),造成线上资源的浪费。

发明内容

[0004] 本文中描述的实施例提供了一种相关随机性的生成方法、装置和计算机可读存储介质,不仅可以避免线上资源的浪费,解决用户不友好的问题,而且可以加速线上的计算,从而提升用户体验。此外,支持主动用户方和被动用户方不同时在线时,生成相关随机性。

[0005] 第一方面,本公开提供了一种相关随机性的生成方法,应用于相关随机性的生成系统,相关随机性的生成系统包括代理服务方、主动用户方和被动用户方,该方法由代理服务方执行。该方法包括:接收被动用户方发送的主动用户标识;将所述主动用户标识对应的主动用户索引和主动用户公钥发送至所述被动用户方,以使所述被动用户方基于所述主动用户公钥对第一明文加密得到第一密文;接收所述被动用户方发送的所述第一密文和所述主动用户索引;基于所述第一密文进行同态加密得到第二密文,并将所述主动用户索引和所述第二密文发送至所述被动用户方,以使所述被动用户方对所述第二密文解密得到第二明文。

[0006] 其中,所述被动用户方拥有的第一明文碎片与主动用户方拥有的第二明文碎片构成一组相关随机性关系,所述第一明文碎片包括所述第一明文和所述第二明文。

[0007] 在本公开的一些实施例中,所述基于所述第一密文进行同态加密得到第二密文包括:将所述第一密文和第三密文相乘再与第四密文相加,得到所述第二密文;其中,所述第三密文为所述主动用户方基于所述主动用户公钥对第三明文加密得到的,所述第四密文为所述主动用户方基于所述主动用户公钥对第四明文加密得到的,所述第二明文碎片包括所述第三明文和所述第四明文。

[0008] 在本公开的一些实施例中,该方法还包括:删除所述主动用户标识及其对应的主

动用户参数信息,所述主动用户参数信息包括所述主动用户公钥和所述主动用户索引。

[0009] 在本公开的一些实施例中,所述将所述主动用户标识对应的主动用户索引和主动用户公钥发送至所述被动用户方之前,还包括:查询所述主动用户标识;确定是否存在所述主动用户索引和所述主动用户公钥。

[0010] 在本公开的一些实施例中,所述接收所述被动用户方发送的主动用户标识之前,还包括:接收并存储所述主动用户方发送的所述主动用户标识及其对应的主动用户参数信息,所述主动用户参数信息包括所述主动用户公钥和所述主动用户索引。

[0011] 第二方面,本公开提供了一种相关随机性的生成方法,应用于相关随机性的生成系统,相关随机性的生成系统包括代理服务方、主动用户方和被动用户方,该方法由被动用户方执行。该方法包括:向代理服务方发送主动用户标识;接收所述代理服务方发送的所述主动用户标识对应的主动用户索引和主动用户公钥;基于所述主动用户公钥对第一明文加密得到第一密文,并将所述第一密文和所述主动用户索引发送至所述代理服务方,以使所述代理服务方基于所述第一密文进行同态加密得到第二密文;接收所述代理服务方发送的所述主动用户索引和所述第二密文;对所述第二密文解密得到第二明文。

[0012] 其中,所述被动用户方拥有的第一明文碎片与主动用户方拥有的第二明文碎片构成一组相关随机性关系,所述第一明文碎片包括所述第一明文和所述第二明文。

[0013] 在本公开的一些实施例中,所述对所述第二密文解密得到第二明文之前,还包括:向所述主动用户方发送所述主动用户索引;接收所述主动用户方发送的所述主动用户索引对应的主动用户私钥。

[0014] 所述对所述第二密文解密得到第二明文包括:基于所述主动用户私钥对所述第二密文解密得到所述第二明文。

[0015] 第三方面,本公开提供了一种相关随机性的生成装置,应用于相关随机性的生成系统,相关随机性的生成系统包括代理服务方、主动用户方和被动用户方。该装置包括:接收模块,用于接收被动用户方发送的主动用户标识;发送模块,用于将所述主动用户标识对应的主动用户索引和主动用户公钥发送至所述被动用户方,以使所述被动用户方基于所述主动用户公钥对第一明文加密得到第一密文;接收模块,还用于接收所述被动用户方发送的所述第一密文和所述主动用户索引;加密模块,用于基于所述第一密文进行同态加密得到第二密文;发送模块,还用于将所述主动用户索引和所述第二密文发送至所述被动用户方,以使所述被动用户方对所述第二密文解密得到第二明文。

[0016] 其中,所述被动用户方拥有的第一明文碎片与主动用户方拥有的第二明文碎片构成一组相关随机性关系,所述第一明文碎片包括所述第一明文和所述第二明文。

[0017] 第四方面,本公开提供了一种相关随机性的生成装置,应用于相关随机性的生成系统,相关随机性的生成系统包括代理服务方、主动用户方和被动用户方。该装置包括:发送模块,用于向代理服务方发送主动用户标识;接收模块,用于接收所述代理服务方发送的所述主动用户标识对应的主动用户索引和主动用户公钥;加密模块,基于所述主动用户公钥对第一明文加密得到第一密文;发送模块,还用于将所述第一密文和所述主动用户索引发送至所述代理服务方,以使所述代理服务方基于所述第一密文进行同态加密得到第二密文;接收模块,还用于接收所述代理服务方发送的所述主动用户索引和所述第二密文;解密模块,用于对所述第二密文解密得到第二明文。

[0018] 其中,所述被动用户方拥有的第一明文碎片与主动用户方拥有的第二明文碎片构成一组相关随机性关系,所述第一明文碎片包括所述第一明文和所述第二明文。

[0019] 第五方面,本公开提供了一种相关随机性的生成系统,包括:代理服务方、主动用户方和被动用户方,其中,所述主动用户方拥有第二明文碎片。

[0020] 所述被动用户方,用于向所述代理服务方发送主动用户标识;所述代理服务方,用于接收所述被动用户方发送的所述主动用户标识,并将所述主动用户标识对应的主动用户索引和主动用户公钥发送至所述被动用户方;所述被动用户方,还用于接收所述代理服务方发送的所述主动用户索引和所述主动用户公钥,基于所述主动用户公钥对第一明文加密得到第一密文,并将所述第一密文和所述主动用户索引发送至所述代理服务方;所述代理服务方,还用于接收所述被动用户方发送的所述第一密文和所述主动用户索引,基于所述第一密文进行同态加密得到第二密文,并将所述主动用户索引和所述第二密文发送至所述被动用户方;所述被动用户方,还用于接收所述代理服务方发送的所述主动用户索引和所述第二密文,并对所述第二密文解密得到第二明文。

[0021] 其中,所述被动用户方拥有的第一明文碎片与所述第二明文碎片构成一组相关随机性关系,所述第一明文碎片包括所述第一明文和所述第二明文。

[0022] 第六方面,本公开提供了一种电子设备,包括处理器,所述处理器用于执行存储于存储器的计算机程序,所述计算机程序被处理器执行时实现第一方面提供的任一方法的步骤。

[0023] 第七方面,本公开提供了一种电子设备,包括处理器,所述处理器用于执行存储于存储器的计算机程序,所述计算机程序被处理器执行时实现第二方面提供的任一方法的步骤。

[0024] 第八方面,本公开提供了一种计算机可读存储介质,其上存储有计算机程序,计算机程序在由处理器执行时实现第一方面提供的任一方法的步骤。

[0025] 第九方面,本公开提供了一种计算机可读存储介质,其上存储有计算机程序,计算机程序在由处理器执行时实现第二方面提供的任一方法的步骤。

[0026] 本公开提供的技术方案中,通过代理服务方接收被动用户方发送的主动用户标识,将主动用户标识对应的主动用户索引和主动用户公钥发送至被动用户方,以使被动用户方基于主动用户公钥对第一明文加密得到第一密文,接收被动用户方发送的第一密文和主动用户索引,基于第一密文进行同态加密得到第二密文,并将主动用户索引和第二密文发送至被动用户方,以使被动用户方对第二密文解密得到第二明文,自此被动用户方拥有第一明文和第二明文,即拥有第一明文碎片,由于主动用户方拥有第二明文碎片且第一明文碎片和第二明文碎片构成一组相关随机性关系,因此可以生成相关随机性。如此,通过引入代理服务方可以将相关随机性的计算放到前端,作为应用相同层级的功能,不仅可以避免线上资源的浪费,解决用户不友好的问题,而且可以加速线上的计算,从而提升用户体验。此外,通过引入代理服务方可以支持主动用户方和被动用户方不同时在线时,生成相关随机性。

附图说明

[0027] 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:

[0028] 图1是本公开实施例提供的一种相关随机性的生成系统的结构示意图;

[0029] 图2是本公开实施例提供的一种相关随机性的生成方法的流程示意图;

[0030] 图3是本公开实施例提供的另一种相关随机性的生成方法的流程示意图;

[0031] 图4是本公开实施例提供的又一种相关随机性的生成方法的流程示意图;

[0032] 图5是本公开实施例提供的一种相关随机性的生成装置的结构示意图;

[0033] 图6是本公开实施例提供的另一种相关随机性的生成装置的结构示意图;

[0034] 图7是本公开实施例提供的又一种相关随机性的生成装置的结构示意图;

[0035] 图8是本公开实施例提供的一种电子设备的结构示意图。

[0036] 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

[0037] 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。

[0038] 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。

[0039] 相关随机性通常包含两部分实体数据,称为碎片或者份额,由两方拥有其中之一。其中任一单独一方拥有的数据与随机数据没有任何区别,当将两方数据结合在一起时,他们具有一定的相关性,即分离时随机,结合时相关。

[0040] 不经意间线性计算(Oblivious linear functional evaluation,OLE)ux=w+v是一种常用的相关随机性关系,其中一方拥有其中的数值(u,v),单方面看数值(u,v)为随机数据。另一方拥有其中的数值(x,w),单方面看数值(x,w)也是随机数据。将(u,v)和(x,w)结合在一起时,具有相关随机性ux=w+v,两方运行某种协议产生这个相关随机性的过程称为OLE。

[0041] 本公开仅以OLE为例对相关随机性进行示例性说明,并不作为对相关随机性的限定,若采用其他相关随机性,其生成方法与OLE的生成方法类似。下面以几个具体的实施例来详细描述本公开的技术方案。

[0042] 图1是本公开实施例提供的一种相关随机性的生成系统的示意图,如图1所示,相关随机性的生成系统包括三方,分别为主动用户方C_1、被动用户方C_2和代理服务方P。其中,主动用户方C_1可以分别与被动用户方C_2和代理服务方P通信,被动用户方C_2和代理服务方P之间可通信。

[0043] 被动用户方C_2拥有的相关随机性碎片为第一明文碎片,主动用户方C_1拥有的相关

随机性碎片为第二明文碎片,第一明文碎片包括第一明文和第二明文,第二明文碎片包括第三明文和第四明文。

[0044] 示例性的,第一明文碎片为(x,w),第二明文碎片为(u,v),第一明文为x,第二明文为w,第三明文为u,第四明文为v,第一明文碎片(x,w)和第二明文碎片(u,v)构成的一组相关随机性关系为ux=w+v。

[0045] 主动用户方C_1、被动用户方C_2和代理服务方P分别用来执行本公开实施例提供的方法实施例的相关步骤。

[0046] 图2是本公开实施提供的一种相关随机性的生成方法的交互示意图,图2所示的实施例可应用于图1所示的系统中,如图2所示,相关随机性的生成方法步骤包括:

[0047] S101,被动用户方向代理服务方发送的主动用户标识。

[0048] 示例性的,被动用户方C_2需要与主动用户方C_1共同参与相关随机性的生成,主动用户方C_1对应的用户标识为主动用户标识ID_{C1},则被动用户方C_2将主动用户标识ID_{C1}发送至代理服务方P,以向代理服务方P查询是否代理了主动用户方C_1的碎片。

[0049] 代理服务方P拥有多个碎片代理记录,每个碎片代理记录中包括一个用户标识以及用户标识对应的公钥和索引,主动用户标识ID_{C1}可能是多个用户标识中的一个,也可能不存在于多个用户标识中。

[0050] S102,代理服务方将主动用户标识对应的主动用户索引和主动用户公钥发送至被动用户方。

[0051] 示例性的,代理服务方接收到主动用户标识ID_{C1}后,遍历所有碎片代理记录,查询所有碎片代理记录中是否存在主动用户标识ID_{C1},从而确定自身是否代理了主动用户方C_1的碎片。具体的,若所有碎片代理记录中存在主动用户标识ID_{C1},确定代理服务方P代理了主动用户方C_1的碎片,则返回主动用户标识ID_{C1}对应的主动用户索引index和主动用户公钥pk,并将主动用户索引index和主动用户公钥pk发送至被动用户方C_2。若所有碎片代理记录中不存在主动用户标识ID_{C1},确定代理服务方P未代理主动用户方C_1的碎片,则返回终止。

[0052] S103,被动用户方基于主动用户公钥对第一明文加密得到第一密文。

[0053] 示例性的,被动用户方C_2随机选择第一明文x,用接收到的主动用户公钥pk对第一明文x进行加密,得到第一密文Cx,即Cx=Enc(pk,x)。

[0054] S104,被动用户方将第一密文和主动用户索引发送至代理服务方。

[0055] 示例性的,被动用户方C_2将得到的第一密文Cx和主动用户索引index发送至代理服务方P,向代理服务方P请求密文的同态计算。

[0056] S105,代理服务方基于第一密文进行同态加密得到第二密文。

[0057] 示例性的,代理服务方P的主动用户方C_1的碎片代理记录中还包括第三密文Cu和第四密文Cv。代理服务方P接收到第一密文Cx和主动用户索引index后,将第一密文Cx和第三密文Cu相乘再与第四密文Cv相加,得到第二密文Cw,即$Cw = (Cx \otimes Cu) \oplus Cv$,其中,$\otimes$表示同态密文的乘法,$\oplus$表示同态密文的加法。

[0058] S106,代理服务方将第二密文和主动用户索引发送至被动用户方。

[0059] 示例性的,代理服务方P将第二密文Cw和主动用户索引index发送至被动用户方C_2。

[0060] S107,被动用户方对第二密文解密得到第二明文。

[0061] 示例性的,被动用户方C_2接收到第二密文Cw后,可以对第二密文Cw进行解密,得到第二明文w。如此,被动用户方C_2拥有第一明文x和第二明文w,即拥有第一明文碎片为(x,w)。

[0062] 此时,主动用户方C_1拥有第二明文碎片为(u,v),由于第一明文碎片(x,w)和第二明文碎片(u,v)构成相关随机性ux=w+v,自此主动用户方C_1和被动用户方C_2共同完成了相关随机性的生成。

[0063] 本公开实施例中,通过代理服务方接收被动用户方发送的主动用户标识,将主动用户标识对应的主动用户索引和主动用户公钥发送至被动用户方,以使被动用户方基于主动用户公钥对第一明文加密得到第一密文,接收被动用户方发送的第一密文和主动用户索引,基于第一密文进行同态加密得到第二密文,并将主动用户索引和第二密文发送至被动用户方,以使被动用户方对第二密文解密得到第二明文,自此被动用户方拥有第一明文和第二明文,即拥有第一明文碎片,由于主动用户方拥有第二明文碎片且第一明文碎片和第二明文碎片构成一组相关随机性关系,因此可以生成相关随机性。如此,通过引入代理服务方可以将相关随机性的计算放到前端,作为应用相同层级的功能,不仅可以避免线上资源的浪费,解决用户不友好的问题,而且可以加速线上的计算,从而提升用户体验。此外,通过引入代理服务方可以支持主动用户方和被动用户方不同时在线时,生成相关随机性。

[0064] 在一些实施例中,图3是本公开实施例提供的另一种相关随机性的生成方法的交互示意图,图3为图2所示实施例的基础上,执行S101之前还包括:

[0065] S201,主动用户方生成主动用户公钥、主动用户私钥和第二明文碎片。

[0066] 示例性的,主动用户方C_1随机生成第三明文u和第四明文v,还生成主动用户公钥pk和主动用户私钥sk,其中,第三明文u和第四明文v构成第二明文碎片为(u,v),主动用户公钥pk和主动用户私钥sk构成密钥对(pk,sk)。且密钥对(pk,sk)支持加法和乘法同态的同态加密方案。

[0067] S202,主动用户方基于主动用户公钥对第二明文碎片加密,得到第三密文和第四密文并生成主动用户索引。

[0068] 示例性的,主动用户方C_1用主动用户公钥pk对第三明文u加密得到第三密文Cu,即Cu=Enc(pk,u)。主动用户方C_1用主动用户公钥pk对第四明文v加密得到第四密文Cv,即Cv=Enc(pk,v)。随后生成相关随机性索引,即主动用户索引index。

[0069] S203,主动用户方将主动用户标识及其对应的主动用户参数信息发送至代理服务方。

[0070] 示例性的,主动用户参数信息包括主动用户索引index和主动用户公钥pk。主动用户方C_1可以将主动用户标识ID_{C1}、主动用户标识ID_{C1}对应的主动用户索引index和主动用户标识ID_{C1}对应的主动用户公钥pk发送至代理服务方P。

[0071] 在其他实施方式中,主动用户参数信息包括主动用户索引index、主动用户公钥pk、第三密文Cu和第四密文Cv。主动用户方C_1可以将主动用户标识ID_{C1}、主动用户标识ID_{C1}对应的主动用户索引index、主动用户标识ID_{C1}对应的主动用户公钥pk、主动用户标识ID_{C1}对应的第三密文Cu和主动用户标识ID_{C1}对应的第四密文Cv发送至代理服务方P。

[0072] 代理服务方P可以将接收到的主动用户标识ID_{C1}及其对应的主动用户参数信息进

行存储,方便后续的查询操作。

[0073] 在一些实施例中,图4是本公开实施例提供的又一种相关随机性的生成方法的交互示意图,图4为图2所示实施例的基础上,执行S107之前还包括:

[0074] S301,被动用户方向主动用户方发送主动用户索引。

[0075] 示例性的,被动用户方向C_2主动用户方C_1发送主动用户索引index。

[0076] S302,主动用户方向被动用户方发送主动用户索引对应的主动用户私钥。

[0077] 示例性的,主动用户方C_1接收到主动用户索引index后,将主动用户索引index对应的主动用户私钥sk发送给被动用户方向C_2。

[0078] 作为执行S107时的一种可能实现方式的具体描述,如图4所示:

[0079] S107',被动用户方基于主动用户私钥对第二密文解密得到第二明文。

[0080] 示例性的,被动用户方向C_2用接收到的主动用户私钥sk对第二密文Cw进行解密,得到第二明文w,即w=Dec(sk,Cw),再进行后续的应用。

[0081] 在一些实施例中,执行完S106之后可以删除代理服务方P存储的由主动用户索引index作为索引的碎片代理记录,每个碎片代理记录包括用户标识及其对应的用户参数信息,即删除主动用户标识ID_{C1}及其对应的主动用户参数信息。

[0082] 由于代理服务方P中每个碎片代理记录仅使用一次,使用后即无效,因此删除使用过的碎片代理记录可以释放代理服务方P的存储空间,便于继续存储碎片代理记录。

[0083] 在一些实施例中,执行完S107之后可以删除主动用户方C_1中存储的的由主动用户索引index作为索引的所有参数信息。其中,所有参数信息包括主动用户索引index、主动用户公钥pk、主动用户私钥sk和第二明文碎片(u,v)。

[0084] 由于主动用户方C_1中生成的每个索引以及对应的所有参数信息仅使用一次,使用后即无效,因此删除使用过的索引以及对应的所有参数信息可以释放主动用户方C_1的存储空间,便于继续存储新的索引对应的所有参数信息。

[0085] 本公开还提供了一种相关随机性的生成装置,应用于如图1所示系统,具体应用于代理服务方P。

[0086] 图5是本公开实施例提供的一种相关随机性的生成装置的结构示意图,如图5所示,相关随机性的生成装置包括:

[0087] 接收模块110,用于接收被动用户方发送的主动用户标识。发送模块120,用于将所述主动用户标识对应的主动用户索引和主动用户公钥发送至所述被动用户方,以使所述被动用户方基于所述主动用户公钥对第一明文加密得到第一密文。接收模块110,还用于接收所述被动用户方发送的所述第一密文和所述主动用户索引。加密模块130,用于基于所述第一密文进行同态加密得到第二密文。发送模块120,还用于将所述主动用户索引和所述第二密文发送至所述被动用户方,以使所述被动用户方对所述第二密文解密得到第二明文。

[0088] 其中,所述被动用户方拥有的第一明文碎片与主动用户方拥有的第二明文碎片构成一组相关随机性关系,所述第一明文碎片包括所述第一明文和所述第二明文。

[0089] 在一些实施例中,加密模块130,进一步用于将所述第一密文和第三密文相乘再与第四密文相加,得到所述第二密文。

[0090] 其中,所述第三密文为所述主动用户方基于所述主动用户公钥对第三明文加密得到的,所述第四密文为所述主动用户方基于所述主动用户公钥对第四明文加密得到的,所

述第二明文碎片包括所述第三明文和所述第四明文。

[0091] 在一些实施例中,相关随机性的生成装置还包括:

[0092] 删除模块,用于删除所述主动用户标识及其对应的主动用户参数信息,所述主动用户参数信息包括所述主动用户公钥和所述主动用户索引。

[0093] 在一些实施例中,相关随机性的生成装置还包括:

[0094] 查询模块,用于查询所述主动用户标识;确定是否存在所述主动用户索引和所述主动用户公钥。

[0095] 在一些实施例中,接收模块110,还用于接收所述主动用户方发送的所述主动用户标识及其对应的主动用户参数信息,所述主动用户参数信息包括所述主动用户公钥和所述主动用户索引。

[0096] 相关随机性的生成装置还包括:存储模块,用于存储所述主动用户方发送的所述主动用户标识及其对应的主动用户参数信息。

[0097] 本公开实施例的装置对应地可用于执行上述各方法实施例中代理服务方一侧的相关步骤,其实现原理和技术效果类似,此处不再赘述。

[0098] 本公开还提供了一种相关随机性的生成装置,应用于如图1所示的系统,具体应用于被动用户方C_2。

[0099] 图6是本公开实施例提供的另一种相关随机性的生成装置的结构示意图,如图6所示,相关随机性的生成装置包括:

[0100] 发送模块210,用于向代理服务方发送主动用户标识。接收模块220,用于接收所述代理服务方发送的所述主动用户标识对应的主动用户索引和主动用户公钥。加密模块230,基于所述主动用户公钥对第一明文加密得到第一密文。发送模块210,还用于将所述第一密文和所述主动用户索引发送至所述代理服务方,以使所述代理服务方基于所述第一密文进行同态加密得到第二密文。接收模块220,还用于接收所述代理服务方发送的所述主动用户索引和所述第二密文。解密模块240,用于对所述第二密文解密得到第二明文。

[0101] 其中,所述被动用户方拥有的第一明文碎片与主动用户方拥有的第二明文碎片构成一组相关随机性关系,所述第一明文碎片包括所述第一明文和所述第二明文。

[0102] 在一些实施例中,发送模块210,还用于向所述主动用户方发送所述主动用户索引。接收模块220,还用于接收所述主动用户方发送的所述主动用户索引对应的主动用户私钥。

[0103] 解密模块240,进一步用于基于所述主动用户私钥对所述第二密文解密得到所述第二明文。

[0104] 本公开实施例的装置对应地可用于执行上述各方法实施例中被动用户方一侧的相关步骤,其实现原理和技术效果类似,此处不再赘述。

[0105] 本公开还提供了一种相关随机性的生成装置,应用于如图1所示的系统,具体应用于主动用户方C_1。

[0106] 图7是本公开实施例提供的另一种相关随机性的生成装置的结构示意图,如图7所示,相关随机性的生成装置包括:

[0107] 生成模块310,用于生成主动用户公钥、主动用户私钥和第二明文碎片。加密模块320,用于基于主动用户公钥对第二明文碎片加密得到第三密文和第四密。生成模块310,还

用于生成主动用户索引。发送模块330,用于将主动用户标识及其对应的主动用户参数信息发送至代理服务方。

[0108] 在一些实施例中,相关随机性的生成装置还包括:接收模块,用于接收被动用户方发送的主动用户索引。

[0109] 发送模块330,还用于向被动用户方发送主动用户索引对应的主动用户私钥。

[0110] 本公开实施例的装置对应地可用于执行上述各方法实施例中主动用户方一侧的相关步骤,其实现原理和技术效果类似,此处不再赘述。

[0111] 本公开实施例提供的相关随机性的生成系统中,主动用户方拥有第二明文碎片。

[0112] 被动用户方,用于向所述代理服务方发送主动用户标识。代理服务方,用于接收所述被动用户方发送的所述主动用户标识,并将所述主动用户标识对应的主动用户索引和主动用户公钥发送至所述被动用户方。所述被动用户方,还用于接收所述代理服务方发送的所述主动用户索引和所述主动用户公钥,基于所述主动用户公钥对第一明文加密得到第一密文,并将所述第一密文和所述主动用户索引发送至所述代理服务方。所述代理服务方,还用于接收所述被动用户方发送的所述第一密文和所述主动用户索引,基于所述第一密文进行同态加密得到第二密文,并将所述主动用户索引和所述第二密文发送至所述被动用户方。所述被动用户方,还用于接收所述代理服务方发送的所述主动用户索引和所述第二密文,并对所述第二密文解密得到第二明文。

[0113] 其中,所述被动用户方拥有的第一明文碎片与所述第二明文碎片构成一组相关随机性关系,所述第一明文碎片包括所述第一明文和所述第二明文。

[0114] 本公开还提供一种电子设备,包括:处理器,所述处理器用于执行存储于存储器的计算机程序,所述计算机程序被处理器执行时实现上述方法实施例代理服务方一侧的步骤。

[0115] 本公开还提供一种电子设备,包括:处理器,所述处理器用于执行存储于存储器的计算机程序,所述计算机程序被处理器执行时实现上述方法实施例被动用户方一侧的步骤。

[0116] 本公开还提供一种电子设备,包括:处理器,所述处理器用于执行存储于存储器的计算机程序,所述计算机程序被处理器执行时实现上述方法实施例主动用户方一侧的步骤。

[0117] 图8本公开提供的一种电子设备的结构示意图,图8示出了适于用来实现本公开实施例实施方式的示例性电子设备的框图。图8示的电子设备仅仅是一个示例,不应对本公开实施例的功能和使用范围带来任何限制。

[0118] 如图8所示,电子设备12以通用计算设备的形式表现。电子设备12的组件可以包括但不限于:一个或者多个处理器16,系统存储器28,连接不同系统组件(包括系统存储器28和处理器16)的总线18。

[0119] 总线18表示几类总线结构中的一种或多种,包括存储器总线或者存储器控制器,外围总线,图形加速端口,处理器或者使用多种总线结构中的任意总线结构的局域总线。举例来说,这些体系结构包括但不限于工业标准体系结构(ISA)总线,微通道体系结构(MAC)总线,增强型ISA总线、视频电子标准协会(VESA)局域总线以及外围组件互连(PCI)总线。

[0120] 电子设备12典型地包括多种计算机系统可读介质。这些介质可以是任何能够被电

子设备12访问的介质,包括易失性和非易失性介质,可移动的和不可移动的介质。

[0121] 系统存储器28可以包括易失性存储器形式的计算机系统可读介质,例如随机存取存储器(RAM)30和/或高速缓存存储器32。电子设备12可以进一步包括其它可移动/不可移动的、易失性/非易失性计算机系统存储介质。仅作为举例,存储系统34可以用于读写不可移动的、非易失性磁介质(通常称为“硬盘驱动器”)。可以提供用于对可移动非易失性磁盘(例如“软盘”)读写的磁盘驱动器,以及对可移动非易失性光盘(例如CD-ROM、DVD-ROM或者其它光介质)读写的光盘驱动器。在这些情况下,每个驱动器可以通过一个或者多个数据介质接口与总线18相连。系统存储器28可以包括至少一个程序产品,该程序产品具有一组(例如至少一个)程序模块,这些程序模块被配置以执行本公开实施例各实施例的功能。

[0122] 具有一组(至少一个)程序模块42的程序/实用工具40,可以存储在例如系统存储器28中,这样的程序模块42包括但不限于操作系统、一个或者多个应用程序、其它程序模块以及程序数据,这些示例中的每一个或某种组合中可能包括网络环境的实现。程序模块42通常执行本公开实施例所描述的实施例中的功能和/或方法。

[0123] 处理器16通过运行存储在系统存储器28中的多个程序中的至少一个程序,从而执行各种功能应用以及数据处理,例如实现本公开实施例所提供的方法实施例。

[0124] 本公开还提供一种计算机可读存储介质,其上存储有计算机程序,该计算机程序被处理器执行时实现上述方法实施例的步骤。

[0125] 可以采用一个或多个计算机可读的介质的任意组合。计算机可读介质可以是计算机可读信号介质或者计算机可读存储介质。计算机可读存储介质例如可以是但不限于电、磁、光、电磁、红外线、或半导体的系统、装置或器件,或者任意以上的组合。计算机可读存储介质的更具体的例子(非穷举的列表)包括:具有一个或多个导线的电连接、便携式计算机磁盘、硬盘、随机存取存储器(RAM)、只读存储器(ROM)、可擦式可编程只读存储器(EPROM或闪存)、光纤、便携式紧凑磁盘只读存储器(CD-ROM)、光存储器件、磁存储器件、或者上述的任意合适的组合。在本文件中,计算机可读存储介质可以是任何包含或存储程序的有形介质,该程序可以被指令执行系统、装置或者器件使用或者与其结合使用。

[0126] 计算机可读的信号介质可以包括在基带中或者作为载波一部分传播的数据信号,其中承载了计算机可读的程序代码。这种传播的数据信号可以采用多种形式,包括但不限于电磁信号、光信号或上述的任意合适的组合。计算机可读的信号介质还可以是计算机可读存储介质以外的任何计算机可读介质,该计算机可读介质可以发送、传播或者传输用于由指令执行系统、装置或者器件使用或者与其结合使用的程序。

[0127] 计算机可读介质上包含的程序代码可以用任何适当的介质传输,包括但不限于无线、电线、光缆、RF等等,或者上述的任意合适的组合。

[0128] 可以以一种或多种程序设计语言或其组合来编写用于执行本公开操作的计算机程序代码,所述程序设计语言包括面向对象的程序设计语言—诸如Java、Smalltalk、C++,还包括常规的过程式程序设计语言—诸如“C”语言或类似的程序设计语言。程序代码可以完全地在用户计算机上执行、部分地在用户计算机上执行、作为一个独立的软件包执行、部分在用户计算机上部分在远程计算机上执行、或者完全在远程计算机或服务器上执行。在涉及远程计算机的情形中,远程计算机可以通过任意种类的网络——包括局域网(LAN)或广域网(WAN)域连接到用户计算机,或者,可以连接到外部计算机(例如利用因特网服务提

供商来通过因特网连接)。

[0129] 本公开还提供一种计算机程序产品,当所述计算机程序产品在计算机上运行时,使得所述计算机执行实现上述方法实施例的步骤。

[0130] 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。

[0131] 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。

[0132] 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,本公开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公开的范围。

[0133] 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。

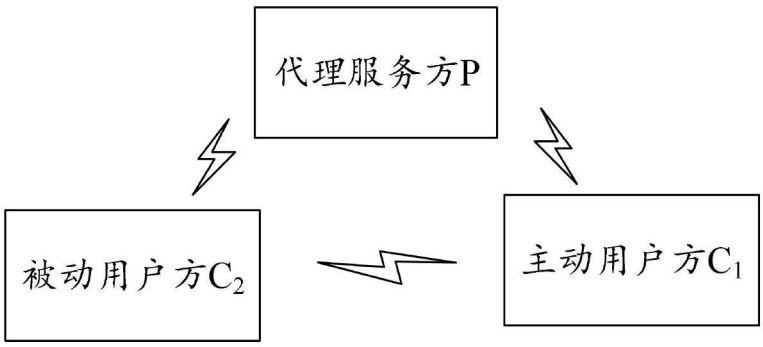

代理服务方P
被动用户方C_2
主动用户方C_1

图1

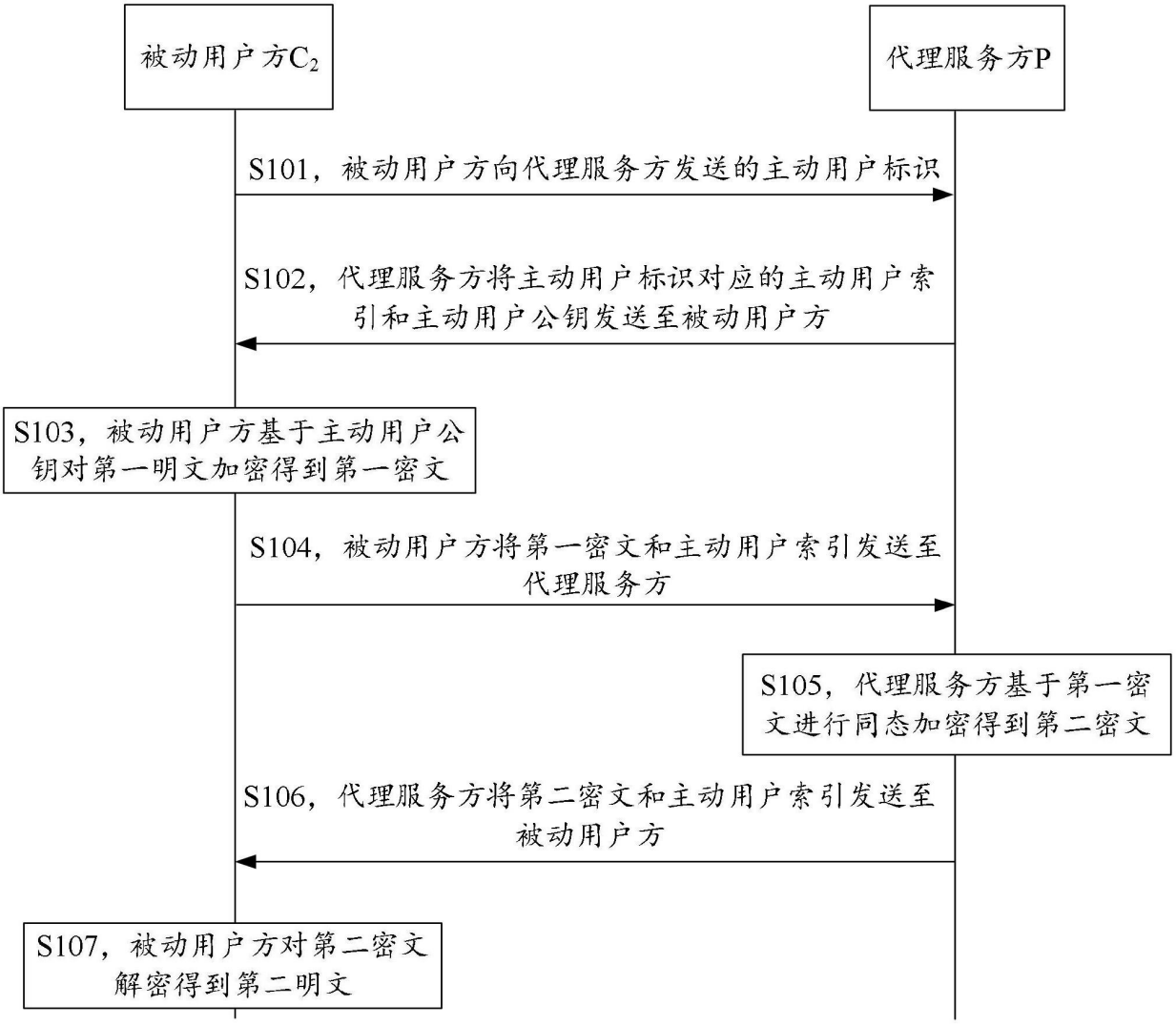

被动用户方C_2
代理服务方P
S101，被动用户方向代理服务方发送的主动用户标识
S102，代理服务方将主动用户标识对应的主动用户索引和主动用户公钥发送至被动用户方
S103，被动用户方基于主动用户公钥对第一明文加密得到第一密文
S104，被动用户方将第一密文和主动用户索引发送至代理服务方
S105，代理服务方基于第一密文进行同态加密得到第二密文
S106，代理服务方将第二密文和主动用户索引发送至被动用户方
S107，被动用户方对第二密文解密得到第二明文

图2

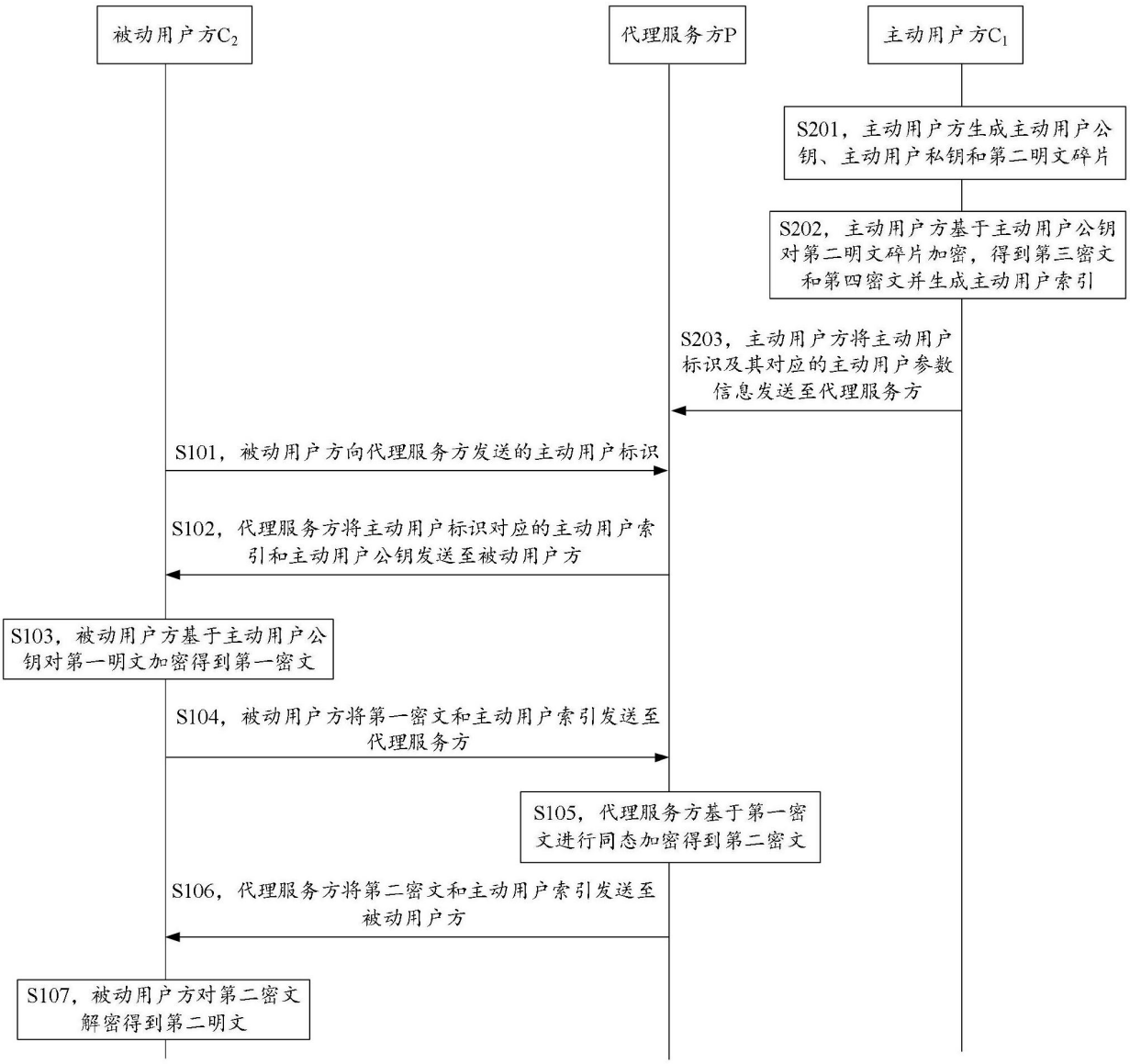

被动用户方C_2
代理服务方P
主动用户方C_1
S201，主动用户方生成主动用户公钥、主动用户私钥和第二明文碎片
S202，主动用户方基于主动用户公钥对第二明文碎片加密，得到第三密文和第四密文并生成主动用户索引
S203，主动用户方将主动用户标识及其对应的主动用户参数信息发送至代理服务方
S101，被动用户方向代理服务方发送的主动用户标识
S102，代理服务方将主动用户标识对应的主动用户索引和主动用户公钥发送至被动用户方
S103，被动用户方基于主动用户公钥对第一明文加密得到第一密文
S104，被动用户方将第一密文和主动用户索引发送至代理服务方
S105，代理服务方基于第一密文进行同态加密得到第二密文
S106，代理服务方将第二密文和主动用户索引发送至被动用户方
S107，被动用户方对第二密文解密得到第二明文

图3

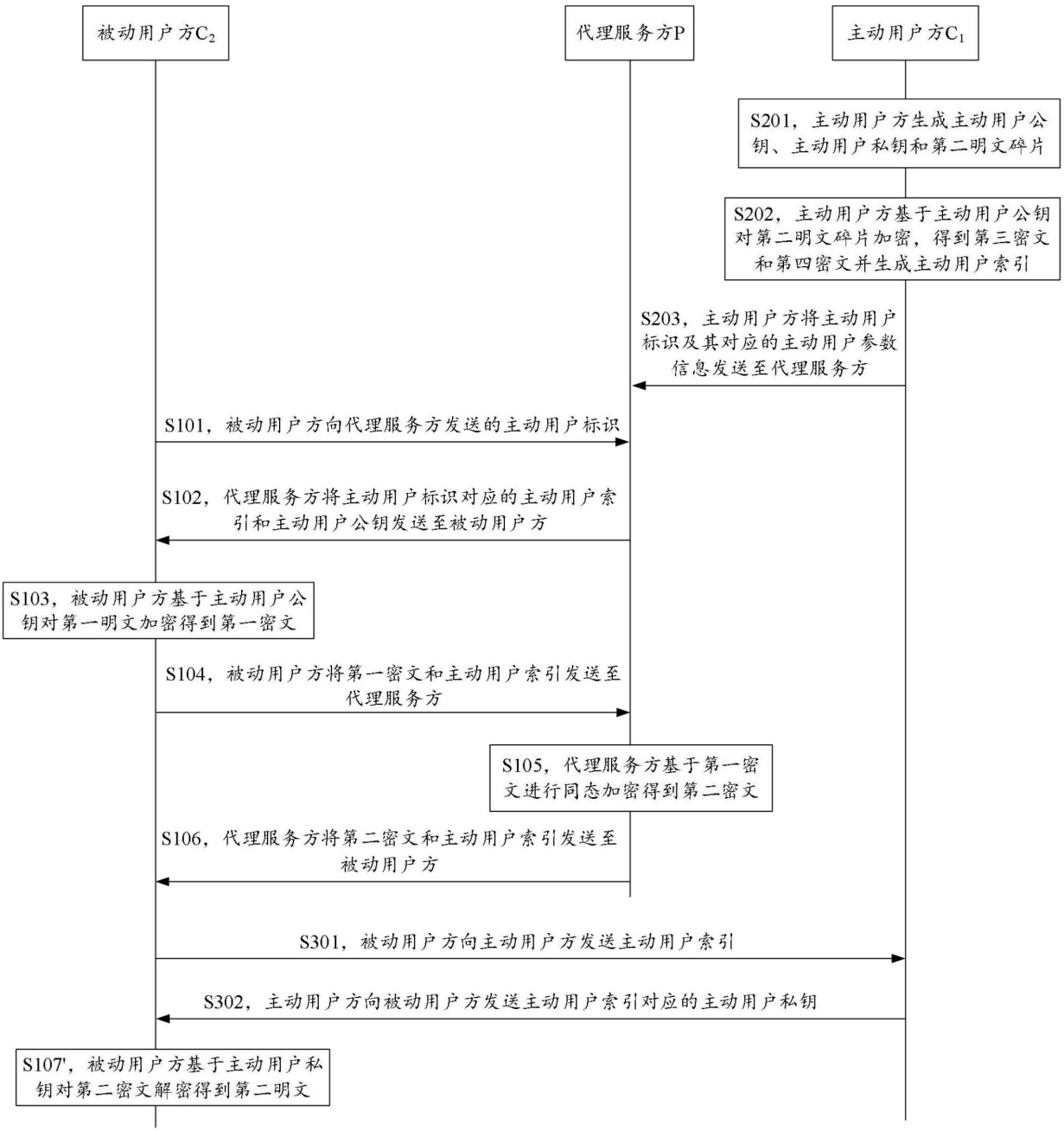

被动用户方C2
代理服务方P
主动用户方C1
S201，主动用户方生成主动用户公钥、主动用户私钥和第二明文碎片
S202，主动用户方基于主动用户公钥对第二明文碎片加密，得到第三密文和第四密文并生成主动用户索引
S203，主动用户方将主动用户标识及其对应的主动用户参数信息发送至代理服务方
S101，被动用户方向代理服务方发送的主动用户标识
S102，代理服务方将主动用户标识对应的主动用户索引和主动用户公钥发送至被动用户方
S103，被动用户方基于主动用户公钥对第一明文加密得到第一密文
S104，被动用户方将第一密文和主动用户索引发送至代理服务方
S105，代理服务方基于第一密文进行同态加密得到第二密文
S106，代理服务方将第二密文和主动用户索引发送至被动用户方
S301，被动用户方向主动用户方发送主动用户索引
S302，主动用户方向被动用户方发送主动用户索引对应的主动用户私钥
S107'，被动用户方基于主动用户私钥对第二密文解密得到第二明文

图4

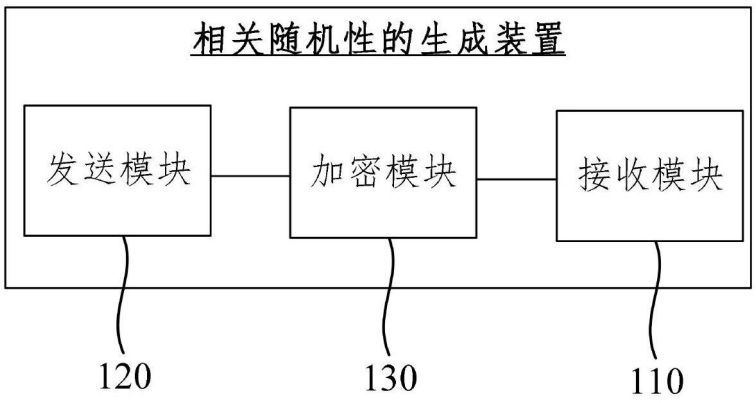

相关随机性的生成装置
发送模块
加密模块
接收模块
120
130
110

图5

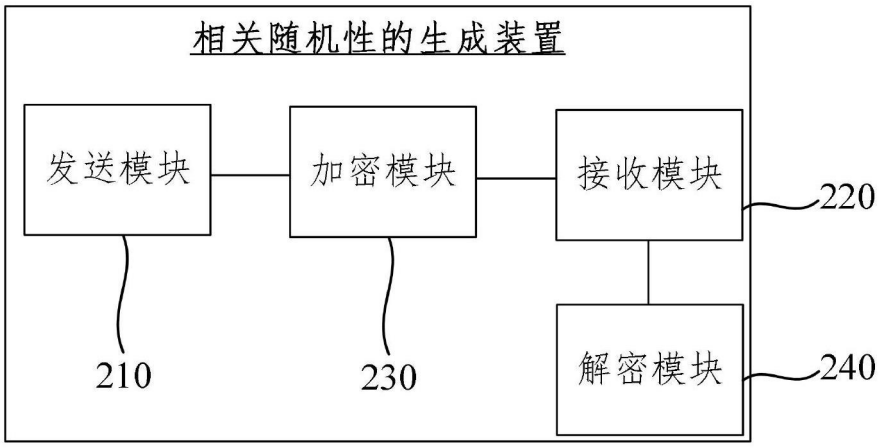

相关随机性的生成装置
发送模块
加密模块
接收模块
220
210
230
解密模块
240

图6

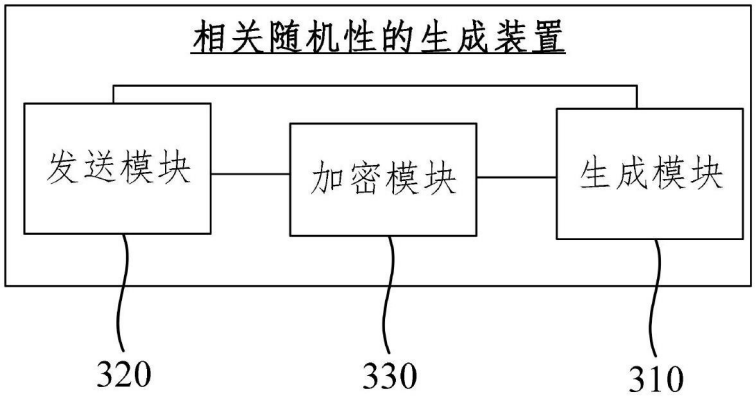

相关随机性的生成装置
发送模块
加密模块
生成模块
320
330
310

图7

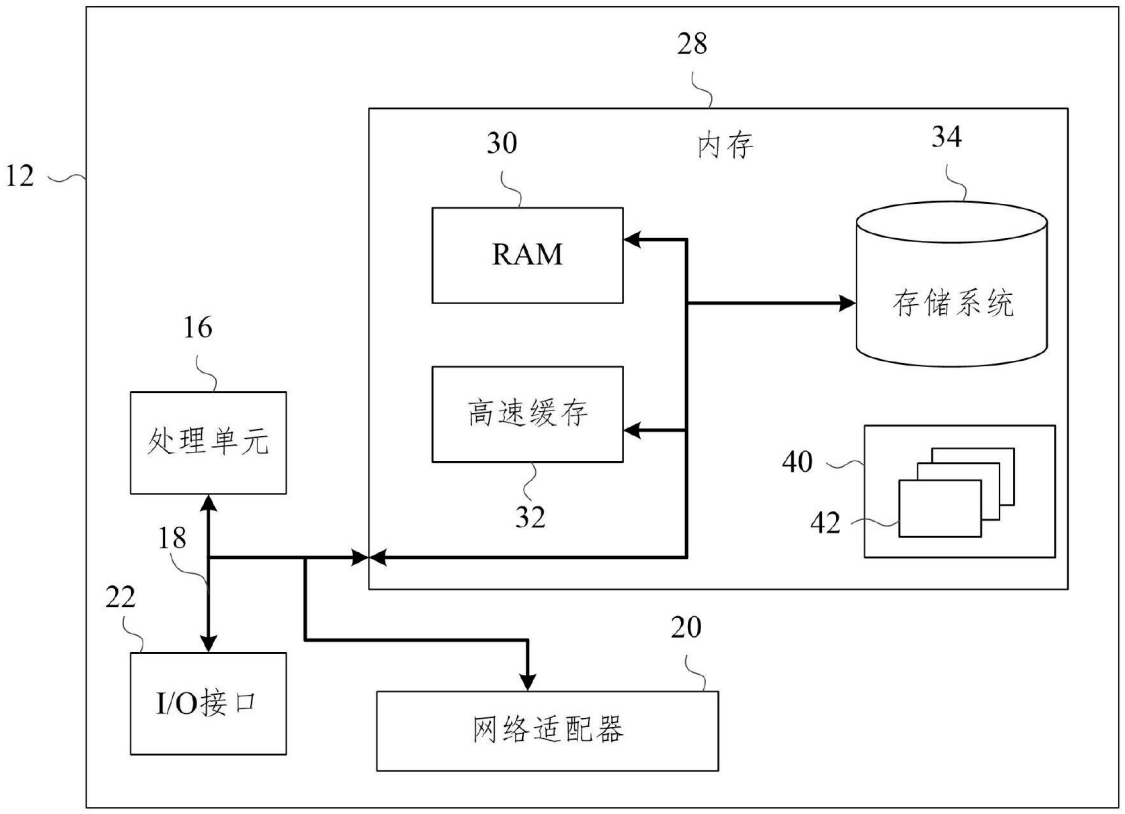


图8