(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 115242514 A
(43)申请公布日 2022.10.25

(21)申请号 202210876365.5

(22)申请日 2022.07.25

(71)申请人 深圳市洞见智慧科技有限公司
地址 518000 广东省深圳市福田区福田街道岗厦社区彩田路3069号星河世纪A栋3603B8

(72)发明人 黄一珉 王湾湾 何浩 姚明

(74)专利代理机构 广州三环专利商标代理有限公司 44202
专利代理师 陈舟苗

(51)Int.Cl.
H04L 9/40(2022.01)
H04L 9/14(2006.01)
H04L 9/32(2006.01)
H04L 9/30(2006.01)
H04L 9/08(2006.01)

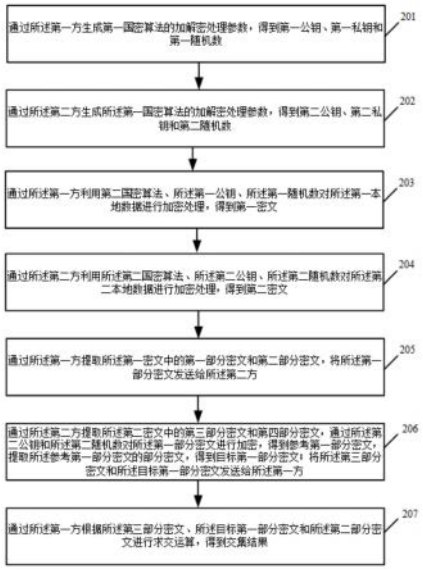
权利要求书3页 说明书12页 附图4页

(54)发明名称

基于国密的隐私集合求交方法、系统及相关设备

(57)摘要

本申请实施例公开了一种基于国密的隐私集合求交方法、系统及相关设备，所述方法包括：生成第一国密算法的第一公钥、第一私钥、第一随机数、第二公钥、第二私钥和第二随机数；利用第二国密算法、第一公钥、第一随机数对第一本地数据进行加密，得到第一密文；利用第二国密算法、第二公钥、第二随机数对第二本地数据进行加密，得到第二密文；提取第一密文中的第一部分密文和第二部分密文；提取第二密文中的第三部分密文和第四部分密文，通过第二公钥和第二随机数对第一部分密文进行加密并提取部分密文，得到目标第一部分密文；根据第三部分密文、目标第一部分密文和第二部分密文求交，得到交集结果。采用本申请实施例可扩充国密算法应用场景。



CN 115242514 A

1.一种基于国密的隐私集合求交方法,其特征在于,应用于两方计算系统,所述两方计算系统包括第一方和第二方,所述第一方对应第一本地数据,所述第二方对应第二本地数据;所述方法包括:

通过所述第一方生成第一国密算法的加解密处理参数,得到第一公钥、第一私钥和第一随机数;

通过所述第二方生成所述第一国密算法的加解密处理参数,得到第二公钥、第二私钥和第二随机数;

通过所述第一方利用第二国密算法、所述第一公钥、所述第一随机数对所述第一本地数据进行加密处理,得到第一密文;

通过所述第二方利用所述第二国密算法、所述第二公钥、所述第二随机数对所述第二本地数据进行加密处理,得到第二密文;

通过所述第一方提取所述第一密文中的第一部分密文和第二部分密文,将所述第一部分密文发送给所述第二方;

通过所述第二方提取所述第二密文中的第三部分密文和第四部分密文,通过所述第二公钥和所述第二随机数对所述第一部分密文进行加密,得到参考第一部分密文,提取所述参考第一部分密文的部分密文,得到目标第一部分密文;将所述第三部分密文和所述目标第一部分密文发送给所述第一方;

通过所述第一方根据所述第三部分密文、所述目标第一部分密文和所述第二部分密文进行求交运算,得到交集结果。

2.根据权利要求1所述的方法,其特征在于,所述通过所述第一方利用第二国密算法、所述第一公钥、所述第一随机数对所述第一本地数据进行加密处理,得到第一密文,包括:

通过所述第一方利用所述第二国密算法对所述第一本地数据进行哈希运算,得到第一哈希运算结果;

利用所述第一公钥和所述第一随机数对所述第一哈希运算结果进行加密处理,得到所述第一密文。

3.根据权利要求1所述的方法,其特征在于,所述通过所述第二方利用所述第二国密算法、所述第二公钥、所述第二随机数对所述第二本地数据进行加密处理,得到第二密文,包括:

通过所述第二方利用所述第二国密算法对所述第二本地数据进行哈希运算,得到第二哈希运算结果;

利用所述第二公钥和所述第二随机数对所述第二哈希运算结果进行加密处理,得到所述第二密文。

4.根据权利要求1-3任一项所述的方法,其特征在于,在所述第一加密算法为sm2算法时,所述通过所述第一方提取所述第一密文中的第一部分密文和第二部分密文,包括:

通过所述第一方利用第一椭圆曲线参数对所述第一密文进行密文提取,得到第一C1密文、第一C2密文和第一C3密文;

将所述第一C2密文确定为所述第一部分密文;

将所述第一C1密文和所述第一C3密文进行拼接,得到所述第二部分密文。

5.根据权利要求4所述的方法,其特征在于,所述通过所述第二方提取所述第二密文中

的第三部分密文和第四部分密文，包括：

通过所述第二方利用第二椭圆曲线参数对所述第二密文进行密文提取，得到第二C1密文、第二C2密文和第二C3密文；

将所述第二C2密文确定为所述第三部分密文；

将所述第二C1密文和所述第二C3密文进行拼接，得到所述第二部分密文。

6.根据权利要求1-3任一项所述的方法，其特征在于，所述通过所述第一方根据所述第三部分密文、所述目标第一部分密文和所述第二部分密文进行求交运算，得到交集结果，包括：

通过所述第一方将所述第二部分密文和所述目标第一部分密文进行拼接，得到拼接密文；

利用所述第一私钥解密所述拼接密文，得到解密结果；

将所述解密结果与所述第三部分密文进行求交运算，得到交集结果。

7.一种两方计算系统，其特征在于，应用于两方计算系统，所述两方计算系统包括第一方和第二方，所述第一方对应第一本地数据，所述第二方对应第二本地数据；其中，

所述第一方，用于生成第一国密算法的加解密处理参数，得到第一公钥、第一私钥和第一随机数；

所述第二方，用于生成所述第一国密算法的加解密处理参数，得到第二公钥、第二私钥和第二随机数；

所述第一方，用于利用第二国密算法、所述第一公钥、所述第一随机数对所述第一本地数据进行加密处理，得到第一密文；

所述第二方，用于利用所述第二国密算法、所述第二公钥、所述第二随机数对所述第二本地数据进行加密处理，得到第二密文；

通过所述第一方，用于提取所述第一密文中的第一部分密文和第二部分密文，将所述第一部分密文发送给所述第二方；

通过所述第二方，用于提取所述第二密文中的第三部分密文和第四部分密文，通过所述第二公钥和所述第二随机数对所述第一部分密文进行加密，得到参考第一部分密文，提取所述参考第一部分密文的部分密文，得到目标第一部分密文；将所述第三部分密文和所述目标第一部分密文发送给所述第一方；

所述第一方，用于根据所述第三部分密文、所述目标第一部分密文和所述第二部分密文进行求交运算，得到交集结果，将所述交集结果发送给所述第二方。

8.根据权利要求7所述的系统，其特征在于，在所述通过所述第一方利用第二国密算法、所述第一公钥、所述第一随机数对所述第一本地数据进行加密处理，得到第一密文方面，所述第一方具体用于：

利用所述第二国密算法对所述第一本地数据进行哈希运算，得到第一哈希运算结果；

利用所述第一公钥和所述第一随机数对所述第一哈希运算结果进行加密处理，得到所述第一密文。

9.一种电子设备，其特征在于，包括处理器、存储器，所述存储器用于存储一个或多个程序，并且被配置由所述处理器执行，所述程序包括用于执行如权利要求1-6任一项所述的方法中的步骤的指令。

10.一种计算机可读存储介质,其特征在于,存储用于电子数据交换的计算机程序,其中,所述计算机程序使得计算机执行如权利要求1-6任一项所述的方法。

基于国密的隐私集合求交方法、系统及相关设备

技术领域

[0001] 本申请涉及隐私计算技术领域以及计算机技术领域，具体涉及一种基于国密的隐私集合求交方法、系统及相关设备。

背景技术

[0002] 随着人工智能的发展，数据的价值越来越受到重视。隐私集合求交(private set intersection,PSI)是指参与方在不泄露额外信息的前提下，得到各自持有数据的交集，是隐私计算领域一个重要技术，在隐私保护的实名认证、联合风控、数据探查等领域具有良好的应用前景。

[0003] 目前的隐私集合求交技术鲜有采用国密的方案，这使得PSI技术在一些安全性和自主可控性要求较高的场景无法适用，如涉及大型银行，国家机关等的合作场景。

发明内容

[0004] 本申请实施例提供了一种基于国密的隐私集合求交方法、系统及相关设备，可以扩充国密算法的应用场景。

[0005] 第一方面，本申请实施例提供一种基于国密的隐私集合求交方法，应用于两方计算系统，所述两方计算系统包括第一方和第二方，所述第一方对应第一本地数据，所述第二方对应第二本地数据；所述方法包括：

通过所述第一方生成第一国密算法的加解密处理参数，得到第一公钥、第一私钥和第一随机数；

通过所述第二方生成所述第一国密算法的加解密处理参数，得到第二公钥、第二私钥和第二随机数；

通过所述第一方利用第二国密算法、所述第一公钥、所述第一随机数对所述第一本地数据进行加密处理，得到第一密文；

通过所述第二方利用所述第二国密算法、所述第二公钥、所述第二随机数对所述第二本地数据进行加密处理，得到第二密文；

通过所述第一方提取所述第一密文中的第一部分密文和第二部分密文，将所述第一部分密文发送给所述第二方；

通过所述第二方提取所述第二密文中的第三部分密文和第四部分密文，通过所述第二公钥和所述第二随机数对所述第一部分密文进行加密，得到参考第一部分密文，提取所述参考第一部分密文的部分密文，得到目标第一部分密文；将所述第三部分密文和所述目标第一部分密文发送给所述第一方；

通过所述第一方根据所述第三部分密文、所述目标第一部分密文和所述第二部分密文进行求交运算，得到交集结果。

[0006] 第二方面，本申请实施例提供了一种两方计算系统，应用于两方计算系统，所述两方计算系统包括第一方和第二方，所述第一方对应第一本地数据，所述第二方对应第二本

地数据;其中,

所述第一方,用于生成第一国密算法的加解密处理参数,得到第一公钥、第一私钥和第一随机数;

所述第二方,用于生成所述第一国密算法的加解密处理参数,得到第二公钥、第二私钥和第二随机数;

所述第一方,用于利用第二国密算法、所述第一公钥、所述第一随机数对所述第一本地数据进行加密处理,得到第一密文;

所述第二方,用于利用所述第二国密算法、所述第二公钥、所述第二随机数对所述第二本地数据进行加密处理,得到第二密文;

通过所述第一方,用于提取所述第一密文中的第一部分密文和第二部分密文,将所述第一部分密文发送给所述第二方;

通过所述第二方,用于提取所述第二密文中的第三部分密文和第四部分密文,通过所述第二公钥和所述第二随机数对所述第一部分密文进行加密,得到参考第一部分密文,提取所述参考第一部分密文的部分密文,得到目标第一部分密文;将所述第三部分密文和所述目标第一部分密文发送给所述第一方;

所述第一方,用于根据所述第三部分密文、所述目标第一部分密文和所述第二部分密文进行求交运算,得到交集结果,将所述交集结果发送给所述第二方。

[0007] 第三方面,本申请实施例提供一种电子设备,包括处理器、存储器、通信接口以及一个或多个程序,其中,上述一个或多个程序被存储在上述存储器中,并且被配置由上述处理器执行,上述程序包括用于执行本申请实施例第一方面中的步骤的指令。

[0008] 第四方面,本申请实施例提供了一种计算机可读存储介质,其中,上述计算机可读存储介质存储用于电子数据交换的计算机程序,其中,上述计算机程序使得计算机执行如本申请实施例第一方面中所描述的部分或全部步骤。

[0009] 第五方面,本申请实施例提供了一种计算机程序产品,其中,上述计算机程序产品包括存储了计算机程序的非瞬时性计算机可读存储介质,上述计算机程序可操作来使计算机执行如本申请实施例第一方面中所描述的部分或全部步骤。该计算机程序产品可以为一个软件安装包。

[0010] 实施本申请实施例,具备如下有益效果:

可以看出,本申请实施例中所描述的基于国密的隐私集合求交方法、系统及相关设备,应用于两方计算系统,该两方计算系统包括第一方和第二方,第一方对应第一本地数据,第二方对应第二本地数据;通过第一方生成第一国密算法的加解密处理参数,得到第一公钥、第一私钥和第一随机数;通过第二方生成第一国密算法的加解密处理参数,得到第二公钥、第二私钥和第二随机数;通过第一方利用第二国密算法、第一公钥、第一随机数对第一本地数据进行加密处理,得到第一密文;通过第二方利用第二国密算法、第二公钥、第二随机数对第二本地数据进行加密处理,得到第二密文;通过第一方提取第一密文中的第一部分密文和第二部分密文,将第一部分密文发送给第二方;通过第二方提取第二密文中的第三部分密文和第四部分密文,通过第二公钥和第二随机数对第一部分密文进行加密,得到参考第一部分密文,提取参考第一部分密文的部分密文,得到目标第一部分密文;将第三部分密文和目标第一部分密文发送给第一方;通过第一方根据第三部分密文、目标第一部

分密文和第二部分密文进行求交运算，得到交集结果，采用了国密算法，可以更自主可控，另外也扩充国密算法的应用场景。

附图说明

[0011] 为了更清楚地说明本申请实施例或现有技术中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本申请的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

[0012] 图1是本申请实施例提供的一种用于实现基于国密的隐私集合求交方法的两方计算系统的结构示意图；

图2是本申请实施例提供的一种基于国密的隐私集合求交方法的流程示意图；

图3是本申请实施例提供的另一种基于国密的隐私集合求交方法的流程示意图；

图4是本申请实施例提供的一种电子设备的结构示意图。

具体实施方式

[0013] 为了使本技术领域的人员更好地理解本申请方案，下面将结合本申请实施例中的附图，对本申请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申请一部分实施例，而不是全部的实施例。基于本申请中的实施例，本领域普通技术人员在没有作出创造性劳动前提下所获得的所有其他实施例，都属于本申请保护的范围。

[0014] 本申请的说明书和权利要求书及上述附图中的术语“第一”、“第二”等是用于区别不同对象，而不是用于描述特定顺序。此外，术语“包括”和“具有”以及它们任何变形，意图在于覆盖不排他的包含。例如包含了一系列步骤或单元的过程、方法、系统、产品或设备没有限定于已列出的步骤或单元，而是可选地还包括没有列出的步骤或单元，或可选地还包括对于这些过程、方法、产品或设备固有的其他步骤或单元。

[0015] 在本文中提及“实施例”意味着，结合实施例描述的特定特征、结构或特性可以包含在本申请的至少一个实施例中。在说明书中的各个位置出现该短语并不一定均是指相同的实施例，也不是与其它实施例互斥的独立的或备选的实施例。本领域技术人员显式地和隐式地理解的是，本文所描述的实施例可以与其它实施例相结合。

[0016] 本申请实施例所描述计算节点可以为电子设备，电子设备可以包括智能手机(如Android手机、iOS手机、Windows Phone手机等)、平板电脑、掌上电脑、行车记录仪、服务器、笔记本电脑、移动互联网设备(MID,Mobile Internet Devices)或穿戴式设备(如智能手表、蓝牙耳机)等，上述仅是举例，而非穷举，包含但不限于上述电子设备，该电子设备也可以为云服务器，或者，该电子设备也可以为计算机集群。本申请实施例中，结果方、发送方均可以为上述电子设备。

[0017] 本申请实施例中，国密算法即为国家商用密码算法。是由国家密码管理局认定和公布的密码算法标准及其应用规范，其中部分密码算法已经成为国际标准。如SM系列密码，SM代表商密，即商业密码，是指用于商业的、不涉及国家秘密的密码技术。

[0018] 下面对本申请实施例进行详细介绍。

[0019] 相关技术中的PSI技术大多可分为4类：基于公钥的方案，基于不经意传输

(Oblivious Transfer, OT)的方案,基于同态加密(homomorphic encryption,HE)的方案和基于混淆电路(garbled circuit,GC)的方案。对应的,目前的国密算法中的公钥加密算法(sm2)可应用于基于公钥的PSI方案。相关技术中的隐私集合求交技术尚未采用国密的方案,这使得PSI技术在一些安全性和自主可控性要求较高的场景无法适用,如涉及大型银行,国家机关等的合作场景。

[0020] 请参阅图1,图1是本申请实施例提供的一种用于实现基于国密的隐私集合求交方法的两方计算系统的架构示意图,如图所示,本两方计算系统可以包括第一方和第二方;所述第一方对应第一本地数据,所述第二方对应第二本地数据;基于该两方计算系统可以实现如下功能:

通过所述第一方生成第一国密算法的加解密处理参数,得到第一公钥、第一私钥和第一随机数;

通过所述第二方生成所述第一国密算法的加解密处理参数,得到第二公钥、第二私钥和第二随机数;

通过所述第一方利用第二国密算法、所述第一公钥、所述第一随机数对所述第一本地数据进行加密处理,得到第一密文;

通过所述第二方利用所述第二国密算法、所述第二公钥、所述第二随机数对所述第二本地数据进行加密处理,得到第二密文;

通过所述第一方提取所述第一密文中的第一部分密文和第二部分密文,将所述第一部分密文发送给所述第二方;

通过所述第二方提取所述第二密文中的第三部分密文和第四部分密文,通过所述第二公钥和所述第二随机数对所述第一部分密文进行加密,得到参考第一部分密文,提取所述参考第一部分密文的部分密文,得到目标第一部分密文;将所述第三部分密文和所述目标第一部分密文发送给所述第一方;

通过所述第一方根据所述第三部分密文、所述目标第一部分密文和所述第二部分密文进行求交运算,得到交集结果,将所述交集结果发送给所述第二方。

[0021] 可选的,所述通过所述第一方利用第二国密算法、所述第一公钥、所述第一随机数对所述第一本地数据进行加密处理,得到第一密文,包括:

通过所述第一方利用所述第二国密算法对所述第一本地数据进行哈希运算,得到第一哈希运算结果;

利用所述第一公钥和所述第一随机数对所述第一哈希运算结果进行加密处理,得到所述第一密文。

[0022] 可选的,所述通过所述第二方利用所述第二国密算法、所述第二公钥、所述第二随机数对所述第二本地数据进行加密处理,得到第二密文,包括:

通过所述第二方利用所述第二国密算法对所述第二本地数据进行哈希运算,得到第二哈希运算结果;

利用所述第二公钥和所述第二随机数对所述第二哈希运算结果进行加密处理,得到所述第二密文。

[0023] 可选的,在所述第一加密算法为sm2算法时,所述通过所述第一方提取所述第一密文中的第一部分密文和第二部分密文,包括:

通过所述第一方利用第一椭圆曲线参数对所述第一密文进行密文提取，得到第一C1密文、第一C2密文和第一C3密文；

将所述第一C2密文确定为所述第一部分密文；

将所述第一C1密文和所述第一C3密文进行拼接，得到所述第二部分密文。

[0024] 可选的，所述通过所述第二方提取所述第二密文中的第三部分密文和第四部分密文，包括：

通过所述第二方利用第二椭圆曲线参数对所述第二密文进行密文提取，得到第二C1密文、第二C2密文和第二C3密文；

将所述第二C2密文确定为所述第三部分密文；

将所述第二C1密文和所述第二C3密文进行拼接，得到所述第二部分密文。

[0025] 可选的，所述通过所述第一方根据所述第三部分密文、所述目标第一部分密文和所述第二部分密文进行求交运算，得到交集结果，包括：

通过所述第一方将所述第二部分密文和所述目标第一部分密文进行拼接，得到拼接密文；

利用所述第一私钥解密所述拼接密文，得到解密结果；

将所述解密结果与所述第三部分密文进行求交运算，得到交集结果。

[0026] 请参阅图2，图2是本申请实施例提供的一种基于国密的隐私集合求交方法的流程示意图，应用于图1所示的两方计算系统，所述两方计算系统包括第一方和第二方，所述第一方对应第一本地数据，所述第二方对应第二本地数据；如图所示，本基于国密的隐私集合求交方法包括：

201、通过所述第一方生成第一国密算法的加解密处理参数，得到第一公钥、第一私钥和第一随机数。

[0027] 其中，第一国密算法可以包括任一国密算法，例如，SM系列国密算法，具体可以为以下至少一种：sm2国密算法、sm9国密算法等等，在此不做限定。

[0028] 具体实现中，可以第一方生成第一国密算法的加解密处理参数，从而，可以得到第一公钥、第一私钥和加密需要的第一随机数。

[0029] 其中，第一本地数据、第二本地数据均可以为一个数据集合，该数据集合可以包括多条数据组，每一数据组可以包括多个数据，每一数据可以对应一个标签信息，每一数据可以理解为一个信息字段，其用于表述标签信息的内容，标签信息可以包括以下至少一种：身份卡号(ID-CARD)、电话号码(Phone Number)、银行卡号(Bank Card)、社保账号、社交账号、学号、工号等等，在此不做限定。

[0030] 本申请实施例中，本地数据中的每一行数据可以对应一个ID，该ID是每一行数据的唯一标识符，每一行都不相同，如：身份证号，手机号或自增序号。

[0031] 举例说明下，具体实现中，银行C想利用运营商B的数据进行联合建模，评估用户的风险等级。则开始建模之前，双方需提供相同用户的画像标签，但双方不想暴露各自本地的非交集用户。他们可采用隐私集合求交技术获得双方的交集用户。

[0032] 202、通过所述第二方生成所述第一国密算法的加解密处理参数，得到第二公钥、第二私钥和第二随机数。

[0033] 其中，具体实现中，可以第二方生成第一国密算法的加解密处理参数，从而，可以

得到第二公钥、第二私钥和加密需要的第二随机数。

[0034] 203、通过所述第一方利用第二国密算法、所述第一公钥、所述第一随机数对所述第一本地数据进行加密处理，得到第一密文。

[0035] 其中，可以通过第一方利用第二国密算法对第一本地数据进行哈希运算，再基于第一公钥、第一随机数对哈希运算结果进行加密处理，得到第一密文，例如，可以将hash后的结果进行sm2加密，得到密文M。

[0036] 可选的，上述步骤203，通过所述第一方利用第二国密算法、所述第一公钥、所述第一随机数对所述第一本地数据进行加密处理，得到第一密文，可以包括如下步骤：

31、通过所述第一方利用所述第二国密算法对所述第一本地数据进行哈希运算，得到第一哈希运算结果；

32、利用所述第一公钥和所述第一随机数对所述第一哈希运算结果进行加密处理，得到所述第一密文。

[0037] 具体实现中，通过第一方利用第二国密算法对第一本地数据进行哈希运算，得到第一哈希运算结果，再可以利用第一公钥和第一随机数对第一哈希运算结果进行加密处理，得到第一密文，如此，可以实现一次加密处理，有助于提升数据安全性。

[0038] 204、通过所述第二方利用所述第二国密算法、所述第二公钥、所述第二随机数对所述第二本地数据进行加密处理，得到第二密文。

[0039] 具体实现中，其中，可以通过第二方利用第二国密算法对第二本地数据进行哈希运算，再基于第二公钥、第二随机数对哈希运算结果进行加密处理，得到第二密文。

[0040] 可选的，上述步骤204，通过所述第二方利用所述第二国密算法、所述第二公钥、所述第二随机数对所述第二本地数据进行加密处理，得到第二密文，可以包括如下步骤：

41、通过所述第二方利用所述第二国密算法对所述第二本地数据进行哈希运算，得到第二哈希运算结果；

42、利用所述第二公钥和所述第二随机数对所述第二哈希运算结果进行加密处理，得到所述第二密文。

[0041] 具体实现中，通过第二方利用第二国密算法对第二本地数据进行哈希运算，得到第二哈希运算结果，利用第二公钥和第二随机数对第二哈希运算结果进行加密处理，得到第二密文，如此，可以实现一次加密处理，有助于提升数据安全性。

[0042] 205、通过所述第一方提取所述第一密文中的第一部分密文和第二部分密文，将所述第一部分密文发送给所述第二方。

[0043] 具体实现中，通过第一方提取第一密文中的第一部分密文和第二部分密文，将第一部分密文发送给第二方。例如，可以通过sm2算法提取第一密文中的C1、C2、C3密文，可以将C2作为第一部分密文，C1和C3进行拼接作为第二部分密文。

[0044] 可选的，在所述第一加密算法为sm2算法时，上述步骤205，通过所述第一方提取所述第一密文中的第一部分密文和第二部分密文，可以包括如下步骤：

51、通过所述第一方利用第一椭圆曲线参数对所述第一密文进行密文提取，得到第一C1密文、第一C2密文和第一C3密文；

52、将所述第一C2密文确定为所述第一部分密文；

53、将所述第一C1密文和所述第一C3密文进行拼接，得到所述第二部分密文。

[0045] 本申请实施例中，第一椭圆曲线参数可以为sm2算法的椭圆曲线参数。

[0046] 具体的，可以通过第一方利用第一椭圆曲线参数对第一密文进行密文提取，得到第一C1密文、第一C2密文和第一C3密文，再将第一C2密文确定为第一部分密文，将第一C1密文和第一C3密文进行拼接，得到第二部分密文。

[0047] 举例说明下，可以利用sm2算法的椭圆曲线参数(椭圆曲线基点的阶n)，得到密文中椭圆曲线上点的长度(记为len=n的比特长度，通常为64)，并依此定位第一C1密文、第一C2密文和第一C3密文，第一C2密文的起始位置由公式2*len+64计算得到，即C2 = M[2*len+64:]，M中前半部分的密文则为第一C1密文和第一C3密文的拼接，记为C1||C3= M[:2*len+64]。

[0048] 本申请实施例中，可以基于sm2算法的椭圆曲线上点的运算，因为sm2算法的加密结果不仅包含椭圆曲线上的点(C1)，还包括了点和原文拼接的一个hash值(C3)，以及原文的加密结果(C2)，即SM2密文是由C1，C3，C2拼接而成，记为(C1||C3||C2)，因此，需要将对应组成部分提取出来进行加解密操作。

[0049] 206、通过所述第二方提取所述第二密文中的第三部分密文和第四部分密文，通过所述第二公钥和所述第二随机数对所述第一部分密文进行加密，得到参考第一部分密文，提取所述参考第一部分密文的部分密文，得到目标第一部分密文；将所述第三部分密文和所述目标第一部分密文发送给所述第一方。

[0050] 具体实现中，也可以采用上述步骤205类似方法，提取第二密文中的第三部分密文和第四部分密文，第三部分密文与第一部分密文对应，第四部分密文与第二部分密文对应，再通过第二公钥和第二随机数对第一部分密文进行加密，得到参考第一部分密文，即二次密文，再可以提取参考第一部分密文的部分密文，得到目标第一部分密文，将第三部分密文和目标第一部分密文发送给第一方。例如，可以利用第三椭圆曲线参数对参考第一部分密文进行密文提取，得到C1密文、C2密文和C3密文，再将C2密文作为目标第一部分密文。

[0051] 本申请实施例中，第三椭圆曲线参数可以为sm2算法的椭圆曲线参数。第一椭圆曲线参数、第二椭圆曲线参数、第三椭圆曲线参数可以相同或者不同。

[0052] 可选的，上述步骤206、通过所述第二方提取所述第二密文中的第三部分密文和第四部分密文，可以包括如下步骤：

61、通过所述第二方利用第二椭圆曲线参数对所述第二密文进行密文提取，得到第二C1密文、第二C2密文和第二C3密文；

62、将所述第二C2密文确定为所述第三部分密文；

63、将所述第二C1密文和所述第二C3密文进行拼接，得到所述第二部分密文。

[0053] 本申请实施例中，第二椭圆曲线参数可以为sm2算法的椭圆曲线参数。第一椭圆曲线参数、第二椭圆曲线参数可以相同或者不同。

[0054] 具体的，可以通过第二方利用第二椭圆曲线参数对第二密文进行密文提取，得到第二C1密文、第二C2密文和第二C3密文，再将第二C2密文确定为第三部分密文，将第二C1密文和第二C3密文进行拼接，得到第四部分密文。

[0055] 举例说明下，可以利用sm2算法椭圆曲线参数(椭圆曲线基点的阶n)，得到密文中椭圆曲线上点的长度(记为len=n的比特长度，通常为64)，并依此定位第二C1密文、第二C2密文和第二C3密文，第二C2密文的起始位置由公式2*len+64计算得到，即C2 = M[2*len+

64:],M中前半部分的密文则为第二C1密文和第二C3密文的拼接,记为C1||C3= M[:2*len+64]。

[0056] 207、通过所述第一方根据所述第三部分密文、所述目标第一部分密文和所述第二部分密文进行求交运算,得到交集结果。

[0057] 具体实现中,第二部分密文与目标第一部分密文可以进行拼接,得到拼接密文,再利用第一私钥对其进行解密,得到解密结果,再将其与第三部分密文进行求交运算,便可以得到交集结果。当然,还可以将交集结果发送给第二方。

[0058] 本申请实施例中,能够扩充了国密算法的应用场景,还可以保证了隐私集合求交过程的安全、可靠、可控,以及降低了隐私集合求交过程的通信量。

[0059] 具体的,一方面国密算法是由国家密码局认定的国产商用密码算法,国家自主可控。密码安全是一个国家综合国力和竞争力的重要标志,密码技术作为国家自主可控的核心技术,在维护国家安全、促进经济发展方面发挥着越来越重要的作用,另一方面国密算法在加密强度或运算性能上都优于同类国际通用算法,因为采用的椭圆曲线加密国密算法,相较普通的公钥加密算法,相同安全等级要求下,密钥长度更短,所以密文更小,可以显著降低通讯量。

[0060] 可选的,上述步骤207,通过所述第一方根据所述第三部分密文、所述目标第一部分密文和所述第二部分密文进行求交运算,得到交集结果,可以包括如下步骤:

71、通过所述第一方将所述第二部分密文和所述目标第一部分密文进行拼接,得到拼接密文;

72、利用所述第一私钥解密所述拼接密文,得到解密结果;

73、将所述解密结果与所述第三部分密文进行求交运算,得到交集结果。

[0061] 具体实现中,可以通过第一方将第二部分密文和目标第一部分密文进行拼接,得到拼接密文,再利用第一私钥解密拼接密文,得到解密结果,最后,可以将解密结果与第三部分密文进行求交运算,得到交集结果。

[0062] 本申请实施例中,可以利用sm3和sm2算法,通过改造现有的基于Diffie-Hellmann密钥协商的PSI方案,提出了一种基于国密的PSI方案,扩充了国密算法的应用场景,保证了隐私集合求交过程的安全、可靠、可控。此外因为采用的是椭圆曲线加密方案,降低了PSI过程的通信量。

[0063] 本申请实施例中,在第一国密算法为sm2国密算法、第二国密算法为sm3国密算法时,则提出了一种基于国密(sm2和sm3)的隐私集合求交方案,进而,扩充了国密算法的应用场景,保证了隐私集合求交过程的安全、可靠、可控。

[0064] 具体实现过程,在第一方为C方,第二方为B方的情况下,如图3所示,B方、C两方基于国密的隐私集合求交过程可以包括如下步骤:

S1、B、C双方各自生成sm2算法中公私钥及sm2加密时需要的随机数k,并缓存;

S2、B、C双方用sm3算法对用于隐私集合求交的数据ID进行hash,例如,可以利用sm3算法对本地数据ID进行hash。

[0065] S3、B、C双方将各自hash后的结果进行sm2加密,得到密文M,即:各自利用公钥和随机数,加密hash后的ID,即可以得到密文M。

[0066] S4、B、C双方各自根据椭圆曲线参数提取sm2密文中C1,C3,C2,具体的:利用sm2椭

圆曲线参数，得到密文中椭圆曲线上点的长度(记为len)，并依此定位hash值加密的密文，密文起始位置由公式2*len+64计算得到，即C2 = M[2*len+64:]，M中前半部分的密文则为C1和C3的拼接，记为C1||C3= M[:2*len+64]。

[0067] S5、C方将本方C2发送给B方。

[0068] S6、B方接收C方信息C2，并利用本方缓存的公钥和随机数加密该C2，具体的，利用本方缓存的公钥和随机数对C2进行sm2加密，得到C方C2二次加密的密文。

[0069] S7、利用步骤S4中相同的方法提取二次加密密文的C2，即根据椭圆曲线参数提取新密文中的C2；将其与B方C2一同发给C方，即B方将本地的C2和C方加密后再提取的C2一同发给C方。

[0070] S8、C方接收B方信息，将C、C3和二次加密的本方数据ID的C2拼接，利用缓存的私钥解密拼接后的密文，得到的结果即为本方数据ID利用B方公钥加密的结果。

[0071] S9、将步骤S8中解密后的结果与C方接收的B方C2本地求交集。

[0072] S10、C方发送交集结果给B方，B方则可以接收交集结果。

[0073] 可以看出，本申请实施例中所描述的基于国密的隐私集合求交方法，应用于两方计算系统，该两方计算系统包括第一方和第二方，第一方对应第一本地数据，第二方对应第二本地数据；通过第一方生成第一国密算法的加解密处理参数，得到第一公钥、第一私钥和第一随机数；通过第二方生成第一国密算法的加解密处理参数，得到第二公钥、第二私钥和第二随机数；通过第一方利用第二国密算法、第一公钥、第一随机数对第一本地数据进行加密处理，得到第一密文；通过第二方利用第二国密算法、第二公钥、第二随机数对第二本地数据进行加密处理，得到第二密文；通过第一方提取第一密文中的第一部分密文和第二部分密文，将第一部分密文发送给第二方；通过第二方提取第二密文中的第三部分密文和第四部分密文，通过第二公钥和第二随机数对第一部分密文进行加密，得到参考第一部分密文，提取参考第一部分密文的部分密文，得到目标第一部分密文；将第三部分密文和目标第一部分密文发送给第一方；通过第一方根据第三部分密文、目标第一部分密文和第二部分密文进行求交运算，得到交集结果，采用了国密算法，可以更自主可控，另外也扩充国密算法的应用场景。

[0074] 与上述实施例一致地，请参阅图4，图4是本申请实施例提供的一种电子设备的结构示意图，如图所示，该电子设备包括处理器、存储器、通信接口以及一个或多个程序，上述一个或多个程序被存储在上述存储器中，并且被配置由上述处理器执行，应用于两方计算系统，所述两方计算系统包括第一方和第二方，所述第一方对应第一本地数据，所述第二方对应第二本地数据；本申请实施例中，上述程序包括用于执行以下步骤的指令：

通过所述第一方生成第一国密算法的加解密处理参数，得到第一公钥、第一私钥和第一随机数；

通过所述第二方生成所述第一国密算法的加解密处理参数，得到第二公钥、第二私钥和第二随机数；

通过所述第一方利用第二国密算法、所述第一公钥、所述第一随机数对所述第一本地数据进行加密处理，得到第一密文；

通过所述第二方利用所述第二国密算法、所述第二公钥、所述第二随机数对所述第二本地数据进行加密处理，得到第二密文；

通过所述第一方提取所述第一密文中的第一部分密文和第二部分密文，将所述第一部分密文发送给所述第二方；

通过所述第二方提取所述第二密文中的第三部分密文和第四部分密文，通过所述第二公钥和所述第二随机数对所述第一部分密文进行加密，得到参考第一部分密文，提取所述参考第一部分密文的部分密文，得到目标第一部分密文；将所述第三部分密文和所述目标第一部分密文发送给所述第一方；

通过所述第一方根据所述第三部分密文、所述目标第一部分密文和所述第二部分密文进行求交运算，得到交集结果。

[0075] 可选的，在所述通过所述第一方利用第二国密算法、所述第一公钥、所述第一随机数对所述第一本地数据进行加密处理，得到第一密文方面，上述程序包括用于执行以下步骤的指令：

通过所述第一方利用所述第二国密算法对所述第一本地数据进行哈希运算，得到第一哈希运算结果；

利用所述第一公钥和所述第一随机数对所述第一哈希运算结果进行加密处理，得到所述第一密文。

[0076] 可选的，在所述通过所述第二方利用所述第二国密算法、所述第二公钥、所述第二随机数对所述第二本地数据进行加密处理，得到第二密文方面，上述程序包括用于执行以下步骤的指令：

通过所述第二方利用所述第二国密算法对所述第二本地数据进行哈希运算，得到第二哈希运算结果；

利用所述第二公钥和所述第二随机数对所述第二哈希运算结果进行加密处理，得到所述第二密文。

[0077] 可选的，在所述第一加密算法为sm2算法时，在所述通过所述第一方提取所述第一密文中的第一部分密文和第二部分密文方面，上述程序包括用于执行以下步骤的指令：

通过所述第一方利用第一椭圆曲线参数对所述第一密文进行密文提取，得到第一C1密文、第一C2密文和第一C3密文；

将所述第一C2密文确定为所述第一部分密文；

将所述第一C1密文和所述第一C3密文进行拼接，得到所述第二部分密文。

[0078] 可选的，在所述通过所述第二方提取所述第二密文中的第三部分密文和第四部分密文方面，上述程序包括用于执行以下步骤的指令：

通过所述第二方利用第二椭圆曲线参数对所述第二密文进行密文提取，得到第二C1密文、第二C2密文和第二C3密文；

将所述第二C2密文确定为所述第三部分密文；

将所述第二C1密文和所述第二C3密文进行拼接，得到所述第二部分密文。

[0079] 可选的，在所述通过所述第一方根据所述第三部分密文、所述目标第一部分密文和所述第二部分密文进行求交运算，得到交集结果方面，上述程序包括用于执行以下步骤的指令：

通过所述第一方将所述第二部分密文和所述目标第一部分密文进行拼接，得到拼接密文；

利用所述第一私钥解密所述拼接密文,得到解密结果;

将所述解密结果与所述第三部分密文进行求交运算,得到交集结果。

[0080] 本申请实施例还提供一种计算机存储介质,其中,该计算机存储介质存储用于电子数据交换的计算机程序,该计算机程序使得计算机执行如上述方法实施例中记载的任一方法的部分或全部步骤,上述计算机包括电子设备。

[0081] 本申请实施例还提供一种计算机程序产品,上述计算机程序产品包括存储了计算机程序的非瞬时性计算机可读存储介质,上述计算机程序可操作来使计算机执行如上述方法实施例中记载的任一方法的部分或全部步骤。该计算机程序产品可以为一个软件安装包,上述计算机包括电子设备。

[0082] 需要说明的是,对于前述的各方法实施例,为了简单描述,故将其都表述为一系列的动作组合,但是本领域技术人员应该知悉,本申请并不受所描述的动作顺序的限制,因为依据本申请,某些步骤可以采用其他顺序或者同时进行。其次,本领域技术人员也应该知悉,说明书中所描述的实施例均属于优选实施例,所涉及的动作和模块并不一定是本申请所必须的。

[0083] 在上述实施例中,对各个实施例的描述都各有侧重,某个实施例中没有详述的部分,可以参见其他实施例的相关描述。

[0084] 在本申请所提供的几个实施例中,应该理解到,所揭露的装置,可通过其它的方式实现。例如,以上所描述的装置实施例仅仅是示意性的,例如上述单元的划分,仅仅为一种逻辑功能划分,实际实现时可以有另外的划分方式,例如多个单元或组件可以结合或者可以集成到另一个系统,或一些特征可以忽略,或不执行。另一点,所显示或讨论的相互之间的耦合或直接耦合或通信连接可以是通过一些接口,装置或单元的间接耦合或通信连接,可以是电性或其它的形式。

[0085] 上述作为分离部件说明的单元可以是或者也可以不是物理上分开的,作为单元显示的部件可以是或者也可以不是物理单元,即可以位于一个地方,或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部单元来实现本实施例方案的目的。

[0086] 另外,在本申请各个实施例中的各功能单元可以集成在一个处理单元中,也可以是各个单元单独物理存在,也可以两个或两个以上单元集成在一个单元中。上述集成的单元既可以采用硬件的形式实现,也可以采用软件功能单元的形式实现。

[0087] 上述集成的单元如果以软件功能单元的形式实现并作为独立的产品销售或使用时,可以存储在一个计算机可读取存储器中。基于这样的理解,本申请的技术方案本质上或者说对现有技术做出贡献的部分或者该技术方案的全部或部分可以以软件产品的形式体现出来,该计算机软件产品存储在一个存储器中,包括若干指令用以使得一台计算机设备(可为个人计算机、服务器或者网络设备等)执行本申请各个实施例上述方法的全部或部分步骤。而前述的存储器包括:U盘、只读存储器(ROM,Read-Only Memory)、随机存取存储器(RAM,Random Access Memory)、移动硬盘、磁碟或者光盘等各种可以存储程序代码的介质。

[0088] 本领域普通技术人员可以理解上述实施例的各种方法中的全部或部分步骤是可以通过程序来指令相关的硬件来完成,该程序可以存储于一计算机可读存储器中,存储器可以包括:闪存盘、只读存储器(英文:Read-Only Memory ,简称:ROM)、随机存取器(英文:

Random Access Memory,简称:RAM)、磁盘或光盘等。

[0089] 以上对本申请实施例进行了详细介绍,本文中应用了具体个例对本申请的原理及实施方式进行了阐述,以上实施例的说明只是用于帮助理解本申请的方法及其核心思想;同时,对于本领域的一般技术人员,依据本申请的思想,在具体实施方式及应用范围上均会有改变之处,综上所述,本说明书内容不应理解为对本申请的限制。

图1

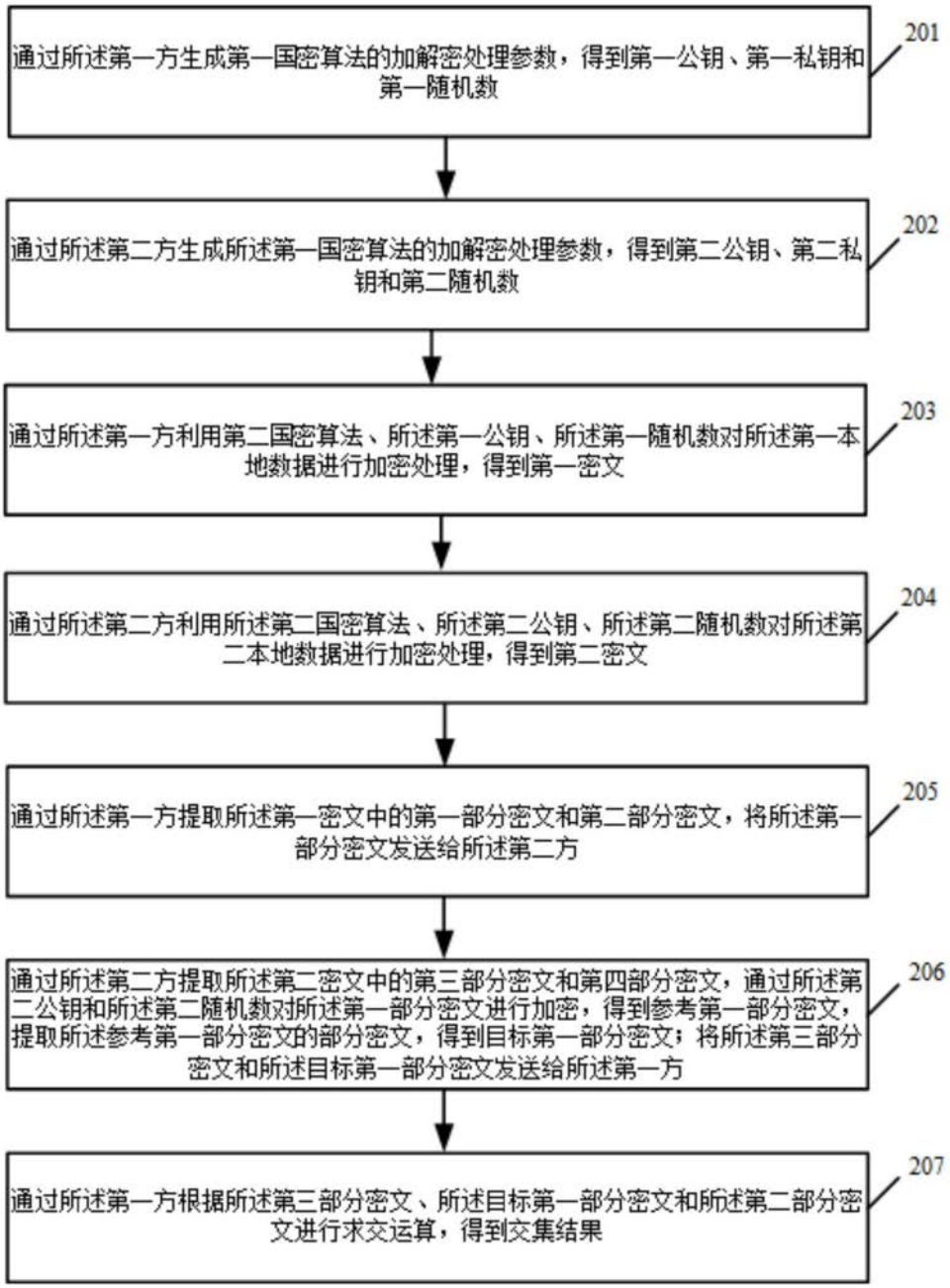

通过所述第一方生成第一国密算法的加解密处理参数，得到第一公钥、第一私钥和第一随机数
201
通过所述第二方生成所述第一国密算法的加解密处理参数，得到第二公钥、第二私钥和第二随机数
202
通过所述第一方利用第二国密算法、所述第一公钥、所述第一随机数对所述第一本地数据进行加密处理，得到第一密文
203
通过所述第二方利用所述第二国密算法、所述第二公钥、所述第二随机数对所述第二本地数据进行加密处理，得到第二密文
204
通过所述第一方提取所述第一密文中的第一部分密文和第二部分密文，将所述第一部分密文发送给所述第二方
205
通过所述第二方提取所述第二密文中的第三部分密文和第四部分密文，通过所述第二公钥和所述第二随机数对所述第一部分密文进行加密，得到参考第一部分密文，提取所述参考第一部分密文的部分密文，得到目标第一部分密文；将所述第三部分密文和所述目标第一部分密文发送给所述第一方
206
通过所述第一方根据所述第三部分密文、所述目标第一部分密文和所述第二部分密文进行求交运算，得到交集结果
207

图2

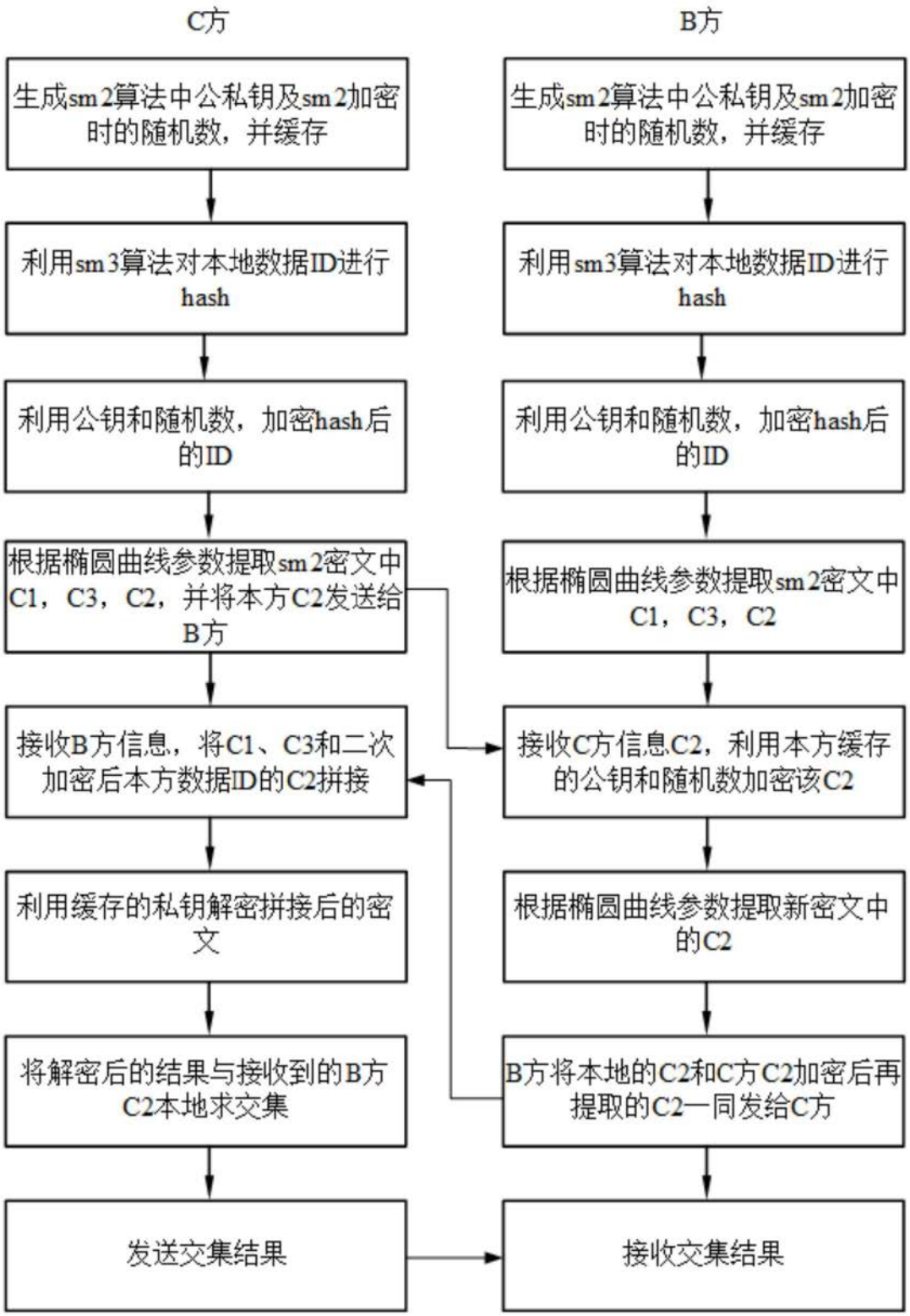

C方
B方
生成sm2算法中公私钥及sm2加密时的随机数，并缓存
生成sm2算法中公私钥及sm2加密时的随机数，并缓存
利用sm3算法对本地数据ID进行hash
利用sm3算法对本地数据ID进行hash
利用公钥和随机数，加密hash后的ID
利用公钥和随机数，加密hash后的ID
根据椭圆曲线参数提取sm2密文中C1，C3，C2，并将本方C2发送给B方
根据椭圆曲线参数提取sm2密文中C1，C3，C2
接收B方信息，将C1、C3和二次加密后本方数据ID的C2拼接
接收C方信息C2，利用本方缓存的公钥和随机数加密该C2
利用缓存的私钥解密拼接后的密文
根据椭圆曲线参数提取新密文中的C2
将解密后的结果与接收到的B方C2本地求交集
B方将本地的C2和C方C2加密后再提取的C2一同发给C方
发送交集结果
接收交集结果

图3

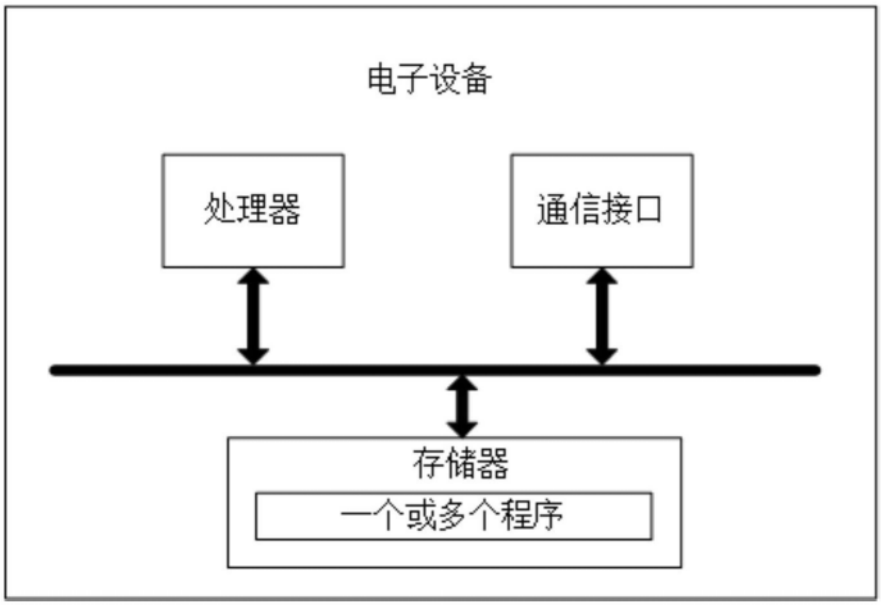


图4