(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 110035070 B
(45)授权公告日 2021.07.23

(21)申请号 201910202006.X

(22)申请日 2019.03.18

(65)同一申请的已公布的文献号
申请公布号 CN 110035070 A

(43)申请公布日 2019.07.19

(73)专利权人 创新先进技术有限公司
地址 开曼群岛大开曼岛乔治镇医院路27号开曼企业中心

(72)发明人 孙勇 赵原

(74)专利代理机构 北京博思佳知识产权代理有限公司 11415
代理人 林祥

(51)Int.Cl.
H04L 29/06(2006.01)

(56)对比文件
CN 107508796 A,2017.12.22
CN 107610453 A,2018.01.19
CN 103546515 A,2014.01.29
CN 104484902 A,2015.04.01
CN 107924339 A,2018.04.17
CN 106339763 A,2017.01.18
CN 107172210 A,2017.09.15

审查员 谭雪

权利要求书4页 说明书10页 附图2页

(54)发明名称

用于拼车的数据处理方法和装置

(57)摘要

本说明书的一个或多个实施例提供了一种用于拼车的数据处理方法和装置，应用于包括拼车服务终端、拼车用户客户端、和安全计算模块的业务数据处理系统；所述方法包括：目标拼车用户客户端向所述拼车服务终端发送目标拼车请求，其中，所述目标拼车请求包括所述目标拼车用户的身份标识和被所述目标拼车用户对应的目标传输密钥加密的目标拼车地址；所述拼车服务终端向所述安全计算模块发送所述目标拼车请求；所述安全计算模块基于所述目标传输密钥对所述目标拼车地址解密；所述安全计算模块根据预设的拼车用户匹配逻辑，基于解密后的目标拼车地址与所述安全计算模块已获取的其他拼车用户的拼车地址进行匹配，以获得拼车分配结果。

CN 110035070 B

1.一种用于拼车的数据处理方法,应用于包括拼车服务终端、拼车用户客户端、和安全计算模块的数据处理系统;所述拼车服务终端与所述安全计算模块通信连接,且所述拼车服务终端与所述拼车用户客户端通信连接;所述安全计算模块与所述拼车用户客户端协商有与所述拼车用户对应的传输密钥;所述方法包括:

目标拼车用户客户端向所述拼车服务终端发送目标拼车请求;其中,所述目标拼车请求包括所述目标拼车用户的身份标识和目标拼车地址,且所述目标拼车地址被所述目标拼车用户对应的目标传输密钥加密;以使所述拼车服务终端在接收到所述目标拼车请求时,向所述安全计算模块发送所述目标拼车请求,并由所述安全计算模块基于所述身份标识获得与所述目标拼车用户对应的目标传输密钥,基于所述目标传输密钥对所述目标拼车地址解密,根据预设的拼车用户匹配逻辑,基于解密后的目标拼车地址与所述安全计算模块已获取的其他拼车用户的拼车地址进行匹配,以获得拼车分配结果,返回给所述拼车服务终端;

从所述拼车服务终端接收所述拼车分配结果。

2.根据权利要求1所述的方法,所述安全计算模块与所述拼车用户客户端协商以获得与所述拼车用户对应的传输密钥的过程,包括:

拼车用户客户端向所述拼车服务终端发送被加密的第一密钥,其中,所述第一密钥被基于所述安全计算模块的公钥加密;

所述拼车服务终端将所述被加密的第一密钥发送至所述安全计算模块;

所述安全计算模块基于自身的私钥对所述被加密的第一密钥解密,以获得所述第一密钥;

所述安全计算模块根据预设的传输密钥计算规则,基于所述第一密钥计算获得所述传输密钥。

3.根据权利要求2所述的方法,所述传输密钥等于所述第一密钥。

4.根据权利要求2所述的方法,所述第一密钥为所述拼车用户客户端选择的随机公钥,所述传输密钥为所述随机公钥与所述安全计算模块自身的私钥的乘积,所述乘积等于所述随机公钥对应的随机私钥与所述安全计算模块自身的公钥的乘积。

5.根据权利要求1至4中任一权利要求所述的方法,所述拼车分配结果包括可与所述目标拼车用户参与拼车的其他拼车用户的身份标识。

6.根据权利要求5所述的方法,所述拼车分配结果还包括可与所述目标拼车用户参与拼车的其他拼车用户的目标拼车地址,其中,所述其他拼车用户的目标拼车地址被所述安全计算模块基于所述目标传输密钥加密;

所述方法还包括:所述拼车用户客户端基于所述目标传输密钥对所述目标拼车地址解密。

7.一种用于拼车的数据处理方法,应用于包括拼车服务终端、拼车用户客户端、和安全计算模块的数据处理系统;所述拼车服务终端与所述安全计算模块通信连接,且所述拼车服务终端与所述拼车用户客户端通信连接;所述安全计算模块与所述拼车用户客户端协商有与所述拼车用户对应的传输密钥;所述方法包括:

所述拼车服务终端接收目标拼车用户客户端发送的目标拼车请求,其中,所述目标拼车请求包括所述目标拼车用户的身份标识和目标拼车地址,且所述目标拼车地址被所述目

标拼车用户客户端对应的目标传输密钥加密；

将所述目标拼车请求发送至所述安全计算模块；以使所述安全计算模块基于所述身份标识获得与所述目标拼车用户对应的目标传输密钥，基于所述目标传输密钥对所述目标拼车地址解密，并根据预设的拼车用户匹配逻辑，基于解密后的目标拼车地址与所述安全计算模块已获取的其他拼车用户的拼车地址进行匹配，以获得拼车分配结果，返回给所述拼车服务终端；

接收所述安全计算模块发送的拼车分配结果；

向所述目标拼车用户客户端发送所述拼车分配结果。

8.根据权利要求7所述的方法，所述安全计算模块与所述拼车用户客户端协商以获得与所述拼车用户对应的传输密钥的过程，包括：

拼车用户客户端向所述拼车服务终端发送被加密的第一密钥，其中，所述第一密钥被基于所述安全计算模块的公钥加密；

所述拼车服务终端将所述被加密的第一密钥发送至所述安全计算模块；

所述安全计算模块基于自身的私钥对所述被加密的第一密钥解密，以获得所述第一密钥；

所述安全计算模块根据预设的传输密钥计算规则，基于所述第一密钥获得所述传输密钥。

9.根据权利要求8所述的方法，所述传输密钥等于所述第一密钥。

10.根据权利要求8所述的方法，所述第一密钥为所述拼车用户客户端选择的随机公钥，所述传输密钥为所述随机公钥与所述安全计算模块自身的私钥的乘积，所述乘积等于所述随机公钥对应的随机私钥与所述安全计算模块自身的公钥的乘积。

11.根据权利要求7至10中任一权利要求所述的方法，所述拼车分配结果包括可与所述目标拼车用户参与拼车的其他拼车用户的身份标识。

12.根据权利要求11所述的方法，所述拼车分配结果还包括可与所述目标拼车用户参与拼车的其他拼车用户的目标拼车地址，其中，所述其他拼车用户的目标拼车地址被所述安全计算模块基于所述目标传输密钥加密。

13.一种用于拼车的数据处理方法，应用于包括拼车服务终端、拼车用户客户端、和安全计算模块的数据处理系统；所述拼车服务终端与所述安全计算模块通信连接，且所述拼车服务终端与所述拼车用户客户端通信连接；所述安全计算模块与所述拼车用户客户端协商有与所述拼车用户对应的传输密钥；所述方法包括：

所述安全计算模块获取所述拼车用户客户端向所述拼车服务终端发送的目标拼车请求，其中，所述目标拼车请求包括所述目标拼车用户的身份标识和目标拼车地址，且所述目标拼车地址被所述目标拼车用户对应的目标传输密钥加密；

基于所述目标拼车用户的身份标识获得与所述目标拼车用户对应的目标传输密钥；

基于所述目标传输密钥对所述目标拼车地址解密；

根据预设的拼车用户匹配逻辑，基于解密后的目标拼车地址与所述安全计算模块已获取的其他拼车用户的拼车地址进行匹配，以获得拼车分配结果；

向所述拼车服务终端发送所述拼车分配结果；以使所述拼车服务终端向所述目标拼车用户客户端发送所述拼车分配结果。

14.根据权利要求13所述的方法，所述安全计算模块与所述拼车用户客户端协商以获得与所述拼车用户对应的传输密钥的过程，包括：

拼车用户客户端向所述拼车服务终端发送被加密的第一密钥，其中，所述第一密钥被基于所述安全计算模块的公钥加密；

所述拼车服务终端将所述被加密的第一密钥发送至所述安全计算模块；

所述安全计算模块基于自身的私钥对所述被加密的第一密钥解密，以获得所述第一密钥；

所述安全计算模块根据预设的传输密钥计算规则，基于所述第一密钥获得所述传输密钥。

15.根据权利要求14所述的方法，所述传输密钥等于所述第一密钥。

16.根据权利要求14所述的方法，所述第一密钥为所述拼车用户客户端选择的随机公钥，所述传输密钥为所述随机公钥与所述安全计算模块自身的私钥的乘积，所述乘积等于所述随机公钥对应的随机私钥与所述安全计算模块自身的公钥的乘积。

17.根据权利要求13至16中任一权利要求所述的方法，所述拼车分配结果包括可与所述目标拼车用户参与拼车的其他拼车用户的身份标识。

18.根据权利要求17所述的方法，所述拼车分配结果还包括可与所述目标拼车用户参与拼车的其他拼车用户的目标拼车地址，其中，所述其他拼车用户的目标拼车地址被所述安全计算模块基于所述目标传输密钥加密；

所述方法还包括：所述拼车用户客户端基于所述目标传输密钥对所述目标拼车地址解密。

19.一种用于拼车的数据处理装置，应用于包括拼车服务终端、拼车用户客户端、和安全计算模块的数据处理系统；所述拼车服务终端与所述安全计算模块通信连接，且所述拼车服务终端与所述拼车用户客户端通信连接；所述安全计算模块与所述拼车用户客户端协商有与所述拼车用户对应的传输密钥；所述装置用于拼车用户客户端，包括：

发送单元，用于向所述拼车服务终端发送目标拼车请求；其中，所述目标拼车请求包括所述目标拼车用户的身份标识和目标拼车地址，且所述目标拼车地址被所述目标拼车用户对应的目标传输密钥加密；以使所述拼车服务终端在接收到所述目标拼车请求时，向所述安全计算模块发送所述目标拼车请求，并由所述安全计算模块基于所述身份标识获得与所述目标拼车用户对应的目标传输密钥，基于所述目标传输密钥对所述目标拼车地址解密，根据预设的拼车用户匹配逻辑，基于解密后的目标拼车地址与所述安全计算模块已获取的其他拼车用户的拼车地址进行匹配，以获得拼车分配结果，返回给所述拼车服务终端；

接收单元，用于从所述拼车服务终端接收所述拼车分配结果。

20.一种用于拼车的数据处理装置，应用于包括拼车服务终端、拼车用户客户端、和安全计算模块的数据处理系统；所述拼车服务终端与所述安全计算模块通信连接，且所述拼车服务终端与所述拼车用户客户端通信连接；所述安全计算模块与所述拼车用户客户端协商有与所述拼车用户对应的传输密钥；所述装置用于所述拼车服务终端，包括：

接收单元，用于接收目标拼车用户客户端发送的目标拼车请求，其中，所述目标拼车请求包括所述目标拼车用户的身份标识和目标拼车地址，且所述目标拼车地址被所述目标拼车用户客户端对应的目标传输密钥加密；

发送单元，用于将所述目标拼车请求发送至所述安全计算模块；以使所述安全计算模块基于所述身份标识获得与所述目标拼车用户对应的目标传输密钥，基于所述目标传输密钥对所述目标拼车地址解密，并根据预设的拼车用户匹配逻辑，基于解密后的目标拼车地址与所述安全计算模块已获取的其他拼车用户的拼车地址进行匹配，以获得拼车分配结果，返回给所述拼车服务终端；

所述接收单元，进一步用于接收所述安全计算模块发送的拼车分配结果；

所述发送单元，进一步用于向所述目标拼车用户客户端发送所述拼车分配结果。

21.一种用于拼车的数据处理装置，应用于包括拼车服务终端、拼车用户客户端、和安全计算模块的数据处理系统；所述拼车服务终端与所述安全计算模块通信连接，且所述拼车服务终端与所述拼车用户客户端通信连接；所述安全计算模块与所述拼车用户客户端协商有与所述拼车用户对应的传输密钥；所述装置用于所述安全计算模块，包括：

获取单元，获取所述拼车用户客户端向所述拼车服务终端发送的目标拼车请求，其中，所述目标拼车请求包括所述目标拼车用户的身份标识和目标拼车地址，且所述目标拼车地址被所述目标拼车用户对应的目标传输密钥加密；

所述获取单元，进一步用于基于所述目标拼车用户的身份标识获得与所述目标拼车用户对应的目标传输密钥；

解密单元，基于所述目标传输密钥对所述目标拼车地址解密；

计算匹配单元，用于根据预设的拼车用户匹配逻辑，基于解密后的目标拼车地址与所述安全计算模块已获取的其他拼车用户的拼车地址进行匹配，以获得拼车分配结果；

发送单元，用于向所述拼车服务终端发送所述拼车分配结果；以使所述拼车服务终端向所述目标拼车用户客户端发送所述拼车分配结果。

22.一种计算机设备，包括：存储器和处理器；所述存储器上存储有可由处理器运行的计算机程序；所述处理器运行所述计算机程序时，执行如权利要求1到6任意一项所述的方法。

23.一种计算机设备，包括：存储器和处理器；所述存储器上存储有可由处理器运行的计算机程序；所述处理器运行所述计算机程序时，执行如权利要求7到12任意一项所述的方法。

24.一种计算机设备，包括：存储器和处理器；所述存储器上存储有可由处理器运行的计算机程序；所述处理器运行所述计算机程序时，执行如权利要求13到18任意一项所述的方法。

用于拼车的数据处理方法和装置

技术领域

[0001] 本说明书涉及网络通信和数据处理技术领域，尤其涉及一种用于拼车的数据处理方法和装置。

背景技术

[0002] 在实际的业务应用中，拼车服务终端由于处理多种业务服务类型可被多个客户端或其他业务处理设备访问，拼车服务终端上处理的数据信息，尤其是与用户相关的数据信息，容易被其他客户端或业务处理设备获取，以造成数据泄露的安全风险。

发明内容

[0003] 有鉴于此，本说明书一个或多个实施例提供一种用于拼车的数据处理方法及装置、计算机设备。

[0004] 为实现上述目的，本说明书一个或多个实施例提供技术方案如下：

[0005] 根据本说明书一个或多个实施例的第一方面，提出了一种用于拼车的数据处理方法，应用于包括拼车服务终端、拼车用户客户端、和安全计算模块的数据处理系统；所述拼车服务终端与所述安全计算模块通信连接，且所述拼车服务终端与所述拼车用户客户端通信连接；所述安全计算模块与所述拼车用户客户端协商有与所述拼车用户对应的传输密钥；所述方法包括：

[0006] 目标拼车用户客户端向所述拼车服务终端发送目标拼车请求，其中，所述目标拼车请求包括所述目标拼车用户的身份标识和目标拼车地址，且所述目标拼车地址被所述目标拼车用户对应的目标传输密钥加密；

[0007] 从所述拼车服务终端接收拼车分配结果。

[0008] 根据本说明书一个或多个实施例的第二方面，提出了一种用于拼车的数据处理方法，应用于包括拼车服务终端、拼车用户客户端、和安全计算模块的数据处理系统；所述拼车服务终端与所述安全计算模块通信连接，且所述拼车服务终端与所述拼车用户客户端通信连接；所述安全计算模块与所述拼车用户客户端协商有与所述拼车用户对应的传输密钥；所述方法包括：

[0009] 所述拼车服务终端接收目标拼车用户客户端发送的目标拼车请求，其中，所述目标拼车请求包括所述目标拼车用户的身份标识和目标拼车地址，且所述目标拼车地址被所述目标拼车用户客户端对应的目标传输密钥加密；

[0010] 将所述拼车请求数据发送至所述安全计算模块；

[0011] 接收所述安全计算模块发送的拼车分配结果；

[0012] 向所述目标拼车用户客户端发送所述拼车分配结果。

[0013] 根据本说明书一个或多个实施例的第三方面，提出了一种用于拼车的数据处理方法，应用于包括拼车服务终端、拼车用户客户端、和安全计算模块的数据处理系统；所述拼车服务终端与所述安全计算模块通信连接，且所述拼车服务终端与所述拼车用户客户端通

信连接;所述安全计算模块与所述拼车用户客户端协商有与所述拼车用户对应的传输密钥;所述方法包括:

[0014] 所述安全计算模块获取所述拼车服务终端发送的目标拼车请求,其中,所述目标拼车请求包括所述目标拼车用户的身份标识和目标拼车地址,且所述目标拼车地址被所述目标拼车用户对应的目标传输密钥加密;

[0015] 基于所述目标拼车用户的身份标识获得与所述目标拼车用户对应的目标传输密钥;

[0016] 基于所述目标传输密钥对所述目标拼车地址解密;

[0017] 根据预设的拼车用户匹配逻辑,基于解密后的目标拼车地址与所述安全计算模块已获取的其他拼车用户的拼车地址进行匹配,以获得拼车分配结果;

[0018] 向所述拼车服务终端发送所述拼车分配结果。

[0019] 根据本说明书一个或多个实施例的第四方面,提出了一种用于拼车的数据处理装置,应用于包括拼车服务终端、拼车用户客户端、和安全计算模块的数据处理系统;所述拼车服务终端与所述安全计算模块通信连接,且所述拼车服务终端与所述拼车用户客户端通信连接;所述安全计算模块与所述拼车用户客户端协商有与所述拼车用户对应的传输密钥;所述装置用于拼车用户客户端,包括:

[0020] 发送单元,用于向所述拼车服务终端发送目标拼车请求,其中,所述目标拼车请求包括所述目标拼车用户的身份标识和目标拼车地址,且所述目标拼车地址被所述目标拼车用户对应的目标传输密钥加密;

[0021] 接收单元,用于从所述拼车服务终端接收拼车分配结果。

[0022] 根据本说明书一个或多个实施例的第五方面,提出了一种用于拼车的数据处理装置,应用于包括拼车服务终端、拼车用户客户端、和安全计算模块的数据处理系统;所述拼车服务终端与所述安全计算模块通信连接,且所述拼车服务终端与所述拼车用户客户端通信连接;所述安全计算模块与所述拼车用户客户端协商有与所述拼车用户对应的传输密钥;所述装置用于所述拼车服务终端,包括:

[0023] 接收单元,用于接收目标拼车用户客户端发送的目标拼车请求,其中,所述目标拼车请求包括所述目标拼车用户的身份标识和目标拼车地址,且所述目标拼车地址被所述目标拼车用户客户端对应的目标传输密钥加密;

[0024] 发送单元,用于将所述拼车请求数据发送至所述安全计算模块;

[0025] 所述接收单元,进一步用于接收所述安全计算模块发送的拼车分配结果;

[0026] 所述发送单元,进一步用于向所述目标拼车用户客户端发送所述拼车分配结果。

[0027] 根据本说明书一个或多个实施例的第六方面,提出了一种用于拼车的数据处理装置,应用于包括拼车服务终端、拼车用户客户端、和安全计算模块的数据处理系统;所述拼车服务终端与所述安全计算模块通信连接,且所述拼车服务终端与所述拼车用户客户端通信连接;所述安全计算模块与所述拼车用户客户端协商有与所述拼车用户对应的传输密钥;所述装置用于所述安全计算模块,包括:

[0028] 获取单元,获取所述拼车服务终端发送的目标拼车请求,其中,所述目标拼车请求包括所述目标拼车用户的身份标识和目标拼车地址,且所述目标拼车地址被所述目标拼车用户对应的目标传输密钥加密;

[0029] 所述获取单元，进一步用于基于所述目标拼车用户的身份标识获得与所述目标拼车用户对应的目标传输密钥；

[0030] 解密单元，基于所述目标传输密钥对所述目标拼车地址解密；

[0031] 计算匹配单元，用于根据预设的拼车用户匹配逻辑，基于解密后的目标拼车地址与所述安全计算模块已获取的其他拼车用户的拼车地址进行匹配，以获得拼车分配结果；

[0032] 发送单元，用于向所述拼车服务终端发送所述拼车分配结果。

[0033] 根据本说明书一个或多个实施例的第七方面，提出了一种计算机设备，包括：存储器和处理器；所述存储器上存储有可由处理器运行的计算机程序；所述处理器运行所述计算机程序时，执行上述目标拼车用户客户端执行的数据处理方法步骤。

[0034] 根据本说明书一个或多个实施例的第一方面，提出了一种计算机设备，包括：存储器和处理器；所述存储器上存储有可由处理器运行的计算机程序；所述处理器运行所述计算机程序时，执行上述拼车服务终端执行的数据处理方法步骤。

[0035] 根据本说明书一个或多个实施例的第一方面，提出了一种计算机设备，包括：存储器和处理器；所述存储器上存储有可由处理器运行的计算机程序；所述处理器运行所述计算机程序时，执行上述安全计算模块执行的数据处理方法步骤。

[0036] 应用本说明书所提供的用于拼车的数据处理方法、装置、计算机设备，通过设置一安全计算模块与拼车服务终端连接，利用上述安全计算模块对拼车服务终端从用户客户端获取的加密的拼车请求进行解密和拼车用户匹配处理，并将匹配处理的结果通过拼车服务终端发送回用户客户端。涉及拼车用户数据隐私安全的拼车请求(可包括用户的拼车地址，用户的拼车地址可涉及用户隐私)虽然经过拼车服务终端，但是拼车服务终端传递的涉及拼车用户数据隐私安全的信息可为加密信息，避免了在拼车服务终端可能发生的数据泄露等安全风险。

附图说明

[0037] 图1为本说明书一示例性实施例提供的用于拼车的业务数据处理系统进行数据处理的流程图；

[0038] 图2为本说明书一示例性实施例提供的应用于拼车服务终端的数据处理装置的示意图；

[0039] 图3为本说明书一示例性实施例提供的应用于拼车用户客户端的数据处理装置的示意图；

[0040] 图4为本说明书一示例性实施例提供的应用于安全计算模块的数据处理装置的示意图；

[0041] 图5为运行本说明书所提供的一种或多种业务数据处理装置实施例的一种硬件结构图。

具体实施方式

[0042] 这里将详细地对示例性实施例进行说明，其示例表示在附图中。下面的描述涉及附图时，除非另有表示，不同附图中的相同数字表示相同或相似的要素。以下示例性实施例中所描述的实施方式并不代表与本说明书一个或多个实施例相一致的所有实施方式。相

反，它们仅是与如所附权利要求书中所详述的、本说明书一个或多个实施例的一些方面相一致的装置和方法的例子。

[0043] 需要说明的是：在其他实施例中并不一定按照本说明书示出和描述的顺序来执行相应方法的步骤。在一些其他实施例中，其方法所包括的步骤可以比本说明书所描述的更多或更少。此外，本说明书中所描述的单个步骤，在其他实施例中可能被分解为多个步骤进行描述；而本说明书中所描述的多个步骤，在其他实施例中也可能被合并为单个步骤进行描述。

[0044] 本说明书所提供的各实施例所描述的数据处理方法，可应用于包括拼车服务终端、拼车用户客户端和安全计算模块的数据处理系统。上述拼车服务终端可包括共享乘车服务提供商为接收用户的拼车请求、进行拼车匹配等业务而设置的计算机设备、或计算机集群等终端。拼车用户客户端为拼车用户为提起拼车请求、接收拼车分配结果等业务而持有的计算机设备终端。上述安全计算模块可以通过软件实现，也可以通过硬件或者软硬件结合的方式实现；以软件实现为例，作为逻辑意义上的模块，可通过集成在上述拼车服务终端中，通过拼车服务终端的CPU(Central Process Unit，中央处理器)将对应的计算机程序指令读取到内存中运行形成的；从硬件层面而言，该安全计算模块既可以为独立于拼车服务终端之外的、包含CPU、内存以及存储器的硬件设备；也可以为与拼车服务终端部分共享硬件设施的软硬结合模块。例如，该安全计算模块的处理器为上述拼车服务终端的处理器中划分设定的部分区域，该安全计算模块为基于上述处理器的部分区域而建立的软硬件结合计算处理模块，如基于Intel芯片的enclave可信安全计算环境，等。

[0045] 图1为本说明书一示例性实施例提供的用于拼车的业务数据处理系统的数据处理流程示意图。如图1所示，上述拼车服务终端与上述安全计算模块通信连接，且上述拼车服务终端与上述拼车用户客户端通信连接。值得注意的是，本说明书各实施例所述的“通信连接”包括但不限于终端设备之间、或终端设备与模块之间直接通信连接，还可包括终端设备之间、或终端设备与模块之间通过其他终端设备的间接通信连接等。

[0046] 在本实施例中，上述安全计算模块与拼车用户客户端协商有与所述拼车用户对应的传输密钥，上述传输密钥可用于对安全计算模块与拼车用户客户端间待通信传输的业务数据进行加密或解密。由于上述传输密钥仅被安全计算模块和拼车用户客户端协商获知，上述拼车服务终端由于无法获知传输密钥，而无法对其传输或存储的、被上述传输密钥加密的业务数据进行解密，从而无法获知被加密的业务数据的原文。

[0047] 如图1所示，本说明书提供的一个或多个实施例所提供的数据处理方法包括：

[0048] 步骤102，目标拼车用户客户端向所述拼车服务终端发送目标拼车请求，其中，所述目标拼车请求包括所述目标拼车用户的身份标识和目标拼车地址，且所述目标拼车地址被所述目标拼车用户对应的目标传输密钥加密。

[0049] 上述目标拼车用户的身份标识可以为被上述数据处理系统可知的、用于识别该目标拼车用户的唯一性标识ID。上述目标拼车地址可包括目标拼车用户欲与其他用户(可为司机用户或乘车用户)拼车的行程、或拼车的目的地、或拼车的起始地等位置信息。上述目标拼车地址由于包括目标拼车用户的位置或出行信息，而具有个人私密性；尤其是当上述目标拼车地址包括目标拼车用户的家庭住址、或公司地址等信息时，一些拼车用户不愿意向其他拼车用户泄露上述目标拼车地址信息。

[0050] 步骤104,所述拼车服务终端向所述安全计算模块发送所述目标拼车请求。

[0051] 所述拼车服务终端在获取所述目标拼车请求后,将上述目标拼车请求透出传输至安全计算模块。如上所述,由于拼车服务终端不具有上述目标传输密钥,因此上述拼车服务终端不能获知上述涉及目标用户隐私的目标拼车地址的原文信息,从而防止了上述目标拼车地址信息在该拼车服务终端的泄露。在本实施例中,上述拼车服务终端可与上述安全计算模块直接连接,而将上述包括所述目标拼车用户的身份标识和目标拼车地址的目标拼车请求发送至上述安全计算模块。

[0052] 步骤106,所述安全计算模块基于所述目标拼车用户的身份标识获得与所述目标拼车用户对应的目标传输密钥。

[0053] 由于所述安全计算模块已与所述拼车用户客户端协商有与所述拼车用户对应的传输密钥,基于所述目标拼车用户的身份标识,所述安全计算模块可获得与所述目标拼车用户对应的目标传输密钥。

[0054] 关于上述安全计算模块与上述拼车用户客户端协商所述传输密钥的过程,可以包括:

[0055] 拼车用户客户端向所述拼车服务终端发送被加密的第一密钥,其中,所述第一密钥被基于所述安全计算模块的公钥加密;

[0056] 所述拼车服务终端将所述被加密的第一密钥发送至所述安全计算模块;

[0057] 所述安全计算模块基于自身的私钥对所述被加密的第一密钥解密,以获得所述第一密钥;

[0058] 所述安全计算模块根据预设的传输密钥计算规则,基于所述第一密钥计算获得所述传输密钥。

[0059] 上述安全计算模块可以将经过协商获得的传输密钥存储于上述拼车服务终端不能访问的区域以进行密钥管理,从而达到传输密钥与拼车服务终端的物理隔离;进一步地,为安全保险起见,安全计算模块可以定期或每隔设定的目标用户的目标拼车请求发送次数,与目标拼车用户客户端重新协商传输密钥。或者,上述目标拼车用户客户端可以在每次发送目标拼车请求的同时发送上述被加密的第一密钥,以使上述安全计算模块可以先基于自身的私钥解密上述被加密的第一密钥,以获取针对本次目标拼车请求数据的传输密钥,进而再解密上述第一业务数据;这样一次一密,更加提高了对上述目标拼车数据中包含的隐私数据,如目标拼车地址数据的安全保护。

[0060] 本领域的技术人员应知,预设的传输密钥计算规则不同,基于上述第一密钥获得与拼车用户对应的传输密钥的方式也不同。

[0061] 在一示出的实施方式中,上述传输密钥等于所述第一密钥。在另一示出的实施方式中,数据处理系统可约定安全计算模块与拼车用户客户端可采用相同椭圆曲线加密算法及基点选择中的DH交换密钥作为加密业务数据(如目标拼车地址数据)的传输密钥;在使用DH交换密钥作为传输密钥时,安全计算模块的公钥与拼车用户客户端的私钥的乘积,和安全计算模块的私钥与拼车用户客户端的公钥的乘积相同,均可作为上述传输密钥;因此,只要获知拼车用户客户端的公钥,安全计算模块即可基于自身私钥与拼车用户客户端的公钥的乘积来进行对业务数据的解密及对业务数据处理结果的加密等操作。

[0062] 进一步地,拼车用户客户端可以定期更换公钥-私钥对,以提高业务数据传输的安

全系数。类似地，拼车用户客户端基于更换公钥(以下称为随机公钥)，与安全计算模块协商传输密钥的过程可包括：

[0063] 所述拼车用户客户端将被加密的随机公钥发送至所述拼车服务终端，其中，所述随机公钥被基于所述安全计算模块的公钥加密；

[0064] 所述拼车服务终端将上述被加密的随机公钥再发送至所述安全计算模块；

[0065] 所述安全计算模块基于自身的私钥对所述被加密的随机公钥解密，以获得所述随机公钥；

[0066] 所述安全计算模块计算所述随机公钥与自身的私钥的乘积，获得所述传输密钥。

[0067] 类似地，上述拼车用户客户端的随机公钥可以定期更换，或者，做到一次一密，以进一步地提高业务数据传输时的安全性；具体过程在此不再赘述。

[0068] 除了上述几个实施例所述的安全计算模块与拼车用户客户端协商传输密钥的具体过程，本领域技术人员基于现有加密技术而想到的其他具体协商过程，均应属于本说明书所描述的协商传输密钥的保护范围内。

[0069] 步骤108，所述安全计算基于所述目标传输密钥对所述目标拼车地址解密。

[0070] 步骤110，所述安全计算模块根据预设的拼车用户匹配逻辑，基于解密后的目标拼车地址与所述安全计算模块已获取的其他拼车用户的拼车地址进行匹配，以获得拼车分配结果。

[0071] 上述安全计算模块可根据本实施例所述的步骤102至108所述的方法获取多个待拼车用户的目标拼车地址，然后根据系统预设的拼车用户匹配逻辑，为上述目标拼车用户匹配符合上述拼车用户匹配逻辑的其他拼车用户。本说明书并不限定上述拼车用户匹配逻辑的具体内容，安全计算模块可基于各个待拼车用户的起始位置相似度、或终点位置相似度、或行程相似度等指标为用户匹配符合系统阈值设置的其他拼车用户。

[0072] 本领域的技术人员容易知道，上述拼车分配结果可以包括拼车成功或拼车失败等通知类消息，还可包括可与所述目标拼车用户参与拼车的其他拼车用户的身份标识，或上述其他拼车用户的其他信息。在又一示出的实施方式中，经其他拼车用户的授权，上述拼车分配结果还可以包括可与所述目标拼车用户参与拼车的其他拼车用户的目标拼车地址，其中，为了使上述其他拼车用户的目标拼车地址信息对上述拼车服务终端保持隐秘，所述其他拼车用户的目标拼车地址被所述安全计算模块基于所述目标传输密钥加密。

[0073] 步骤112，所述安全计算模块向所述拼车服务终端发送所述拼车分配结果。

[0074] 步骤114，所述拼车服务终端向所述拼车用户客户端发送所述拼车分配结果。

[0075] 当上述拼车分配结果包括被所述目标传输密钥加密的其他参与拼车的用户的地址信息时，本实施例所述的方法还包括步骤116，所述拼车用户客户端基于所述目标传输密钥对所述目标拼车地址解密。

[0076] 在本实施例中，通过设置安全计算模块，以在安全计算模块内部进行拼车请求数据的解密和基于拼车请求数据的拼车用户匹配计算处理，并将拼车分配结果发送回用户客户端。上述过程中，涉及拼车用户隐私的数据信息(至少包括拼车用户的地址信息)对拼车拼车服务终端均是不可见的，由此保证了上述拼车用户隐私的数据信息(至少包括拼车用户的地址信息)不会在拼车拼车服务终端被泄露。

[0077] 如前所述，上述安全计算模块可以由拼车服务终端独立运行的软件实现，以在软

件层面达到数据隔离;为了进一步提高安全计算模块数据处理的数据安全性,上述安全计算模块也可以与拼车服务终端共享部分硬件或不共享硬件独立硬件的形式结合来实现。

[0078] 不共享硬件的独立硬件的形式可以理解为将上述安全计算模块完全运行在独立的终端设备上,上述安全计算模块与上述拼车服务终端可通过各终端的通信模块连接。部分共享硬件的形式随着计算机处理器技术的发展成为了可能:例如拼车服务终端可将合法的业务数据计算处理程序封装在CPU的一个可信计算环境中,保护其不受恶意软件或程序的攻击,特权或者非特权的软件或程序都无法访问该可信计算环境,也就是说,一旦业务处理程序和业务数据位于上述可信计算环境中,即便操作系统或者和VMM(Hypervisor)也无法影响上述可信计算环境里面的代码和数据。

[0079] 通过上述的可信计算环境划分技术,上述安全计算模块的处理器为上述拼车服务终端的处理器中划分设定的部分区域,也从物理上达到了业务数据及业务数据的处理对拼车服务终端的物理隔离。而且,相较于完全独立的硬件终端模式,上述基于可信计算环境技术设置安全计算模块的实施方式,便于开发,降低了运营成本;属于本说明书所提供的较优的实施方式。

[0080] 与上述流程实现对应,本说明书的实施例还提供了多种数据处理装置。上述装置可以通过软件实现,也可以通过硬件或者软硬件结合的方式实现。以软件实现为例,作为逻辑意义上的装置,是通过所在设备的CPU(Central Process Unit,中央处理器)将对应的计算机程序指令读取到内存中运行形成的。从硬件层面而言,除了图5所示的CPU、内存以及存储器之外,该数据处理装置所在的设备通常还包括用于进行无线信号收发的芯片等其他硬件,和/或用于实现网络通信功能的板卡等其他硬件。

[0081] 图2所示为本说明书所提供的一种用于拼车的数据处理装置20,应用于包括拼车服务终端、拼车用户客户端、和安全计算模块的数据处理系统;所述拼车服务终端与所述安全计算模块通信连接,且所述拼车服务终端与所述拼车用户客户端通信连接;所述安全计算模块与所述拼车用户客户端协商有与所述拼车用户对应的传输密钥;所述装置20用于拼车用户客户端,包括:

[0082] 发送单元202,用于向所述拼车服务终端发送目标拼车请求,其中,所述目标拼车请求包括所述目标拼车用户的身份标识和目标拼车地址,且所述目标拼车地址被所述目标拼车用户对应的目标传输密钥加密;

[0083] 接收单元204,用于从所述拼车服务终端接收拼车分配结果。

[0084] 在又一示出的实施方式中,所述拼车分配结果包括可与所述目标拼车用户参与拼车的其他拼车用户的身份标识。

[0085] 在又一示出的实施方式中,所述拼车分配结果还包括可与所述目标拼车用户参与拼车的其他拼车用户的目标拼车地址,其中,所述其他拼车用户的目标拼车地址被所述安全计算模块基于所述目标传输密钥加密;

[0086] 所述装置还包括:解密单元206,用于基于所述目标传输密钥对所述目标拼车地址解密。

[0087] 图3示意了本说明书又一实施例提供的于拼车的数据处理装置30,应用于包括拼车服务终端、拼车用户客户端、和安全计算模块的数据处理系统;所述拼车服务终端与所述安全计算模块通信连接,且所述拼车服务终端与所述拼车用户客户端通信连接;所述安全

计算模块与所述拼车用户客户端协商有与所述拼车用户对应的传输密钥;所述装置30用于所述拼车服务终端,包括:

[0088] 接收单元302,用于接收目标拼车用户客户端发送的目标拼车请求,其中,所述目标拼车请求包括所述目标拼车用户的身份标识和目标拼车地址,且所述目标拼车地址被所述目标拼车用户客户端对应的目标传输密钥加密;

[0089] 发送单元304,用于将所述拼车请求数据发送至所述安全计算模块;

[0090] 所述接收单元302,进一步用于接收所述安全计算模块发送的拼车分配结果;

[0091] 所述发送单元304,进一步用于向所述目标拼车用户客户端发送所述拼车分配结果。

[0092] 在又一示出的实施方式中,所述拼车分配结果包括可与所述目标拼车用户参与拼车的其他拼车用户的身份标识。

[0093] 在又一示出的实施方式中,所述拼车分配结果还包括可与所述目标拼车用户参与拼车的其他拼车用户的目标拼车地址,其中,所述其他拼车用户的目标拼车地址被所述安全计算模块基于所述目标传输密钥加密;

[0094] 图4示意了本说明书又一实施例提供的用于拼车的数据处理装置40,应用于包括拼车服务终端、拼车用户客户端、和安全计算模块的数据处理系统;所述拼车服务终端与所述安全计算模块通信连接,且所述拼车服务终端与所述拼车用户客户端通信连接;所述安全计算模块与所述拼车用户客户端协商有与所述拼车用户对应的传输密钥;所述装置40用于所述安全计算模块,包括:

[0095] 获取单元402,获取所述拼车服务终端发送的目标拼车请求,其中,所述目标拼车请求包括所述目标拼车用户的身份标识和目标拼车地址,且所述目标拼车地址被所述目标拼车用户对应的目标传输密钥加密;

[0096] 所述获取单元402,进一步用于基于所述目标拼车用户的身份标识获得与所述目标拼车用户对应的目标传输密钥;

[0097] 解密单元404,基于所述目标传输密钥对所述目标拼车地址解密;

[0098] 计算匹配单元406,用于根据预设的拼车用户匹配逻辑,基于解密后的目标拼车地址与所述安全计算模块已获取的其他拼车用户的拼车地址进行匹配,以获得拼车分配结果;

[0099] 发送单元406,用于向所述拼车服务终端发送所述拼车分配结果。

[0100] 在又一示出的实施方式中,所述拼车分配结果包括可与所述目标拼车用户参与拼车的其他拼车用户的身份标识。

[0101] 在又一示出的实施方式中,所述拼车分配结果还包括可与所述目标拼车用户参与拼车的其他拼车用户的目标拼车地址,其中,所述其他拼车用户的目标拼车地址被所述安全计算模块基于所述目标传输密钥加密。

[0102] 上述各个装置中各个单元的功能和作用的实现过程具体详见上述方法中对应步骤的实现过程,相关之处参见方法实施例的部分说明即可,在此不再赘述。

[0103] 以上所描述的装置实施例仅仅是示意性的,其中所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模块,即可以位于一个地方,或者也可以分布到多个网络模块上。可以根据实际的需要选择其

中的部分或者全部单元或模块来实现本说明书方案的目的。本领域普通技术人员在不付出创造性劳动的情况下,即可以理解并实施。

[0104] 上述实施例阐明的装置、单元、模块,具体可以由计算机芯片或实体实现,或者由具有某种功能的产品来实现。一种典型的实现设备为计算机,计算机的具体形式可以是个人计算机、膝上型计算机、蜂窝电话、相机电话、智能电话、个人数字助理、媒体播放器、导航设备、电子邮件收发设备、游戏控制台、平板计算机、可穿戴设备或者这些设备中的任意几种设备的组合。

[0105] 与上述方法实施例相对应,本说明书的实施例还提供了一种计算机设备,该计算机设备包括存储器和处理器。其中,存储器上存储有能够由处理器运行的计算机程序;处理器在运行存储的计算机程序时,执行本说明书实施例中拼车服务终端执行的业务数据处理方法的各个步骤。对拼车服务终端执行的业务数据处理方法的各个步骤的详细描述请参见之前的内容,不再重复。

[0106] 与上述方法实施例相对应,本说明书的实施例还提供了一种计算机设备,该计算机设备包括存储器和处理器。其中,存储器上存储有能够由处理器运行的计算机程序;处理器在运行存储的计算机程序时,执行本说明书实施例中拼车用户客户端执行的业务数据处理方法的各个步骤。对拼车用户客户端执行的业务数据处理方法的各个步骤的详细描述请参见之前的内容,不再重复。

[0107] 与上述方法实施例相对应,本说明书的实施例还提供了一种计算机设备,该计算机设备包括存储器和处理器。其中,存储器上存储有能够由处理器运行的计算机程序;处理器在运行存储的计算机程序时,执行本说明书实施例中安全计算模块执行的业务数据处理方法的各个步骤。对安全计算模块执行的业务数据处理方法的各个步骤的详细描述请参见之前的内容,不再重复。

[0108] 以上所述仅为本说明书的较佳实施例而已,并不用以限制本说明书,凡在本说明书的精神和原则之内,所做的任何修改、等同替换、改进等,均应包含在本说明书保护的范围之内。

[0109] 在一个典型的配置中,计算设备包括一个或多个处理器(CPU)、输入/输出接口、网络接口和内存。

[0110] 内存可能包括计算机可读介质中的非永久性存储器,随机存取存储器(RAM)和/或非易失性内存等形式,如只读存储器(ROM)或闪存(flash RAM)。内存是计算机可读介质的示例。

[0111] 计算机可读介质包括永久性和非永久性、可移动和非可移动媒体可以由任何方法或技术来实现信息存储。信息可以是计算机可读指令、数据结构、程序的模块或其他数据。

[0112] 计算机的存储介质的例子包括,但不限于相变内存(PRAM)、静态随机存取存储器(SRAM)、动态随机存取存储器(DRAM)、其他类型的随机存取存储器(RAM)、只读存储器(ROM)、电可擦除可编程只读存储器(EEPROM)、快闪记忆体或其他内存技术、只读光盘只读存储器(CD-ROM)、数字多功能光盘(DVD)或其他光学存储、磁盒式磁带,磁带磁磁盘存储或其他磁性存储设备或任何其他非传输介质,可用于存储可以被计算设备访问的信息。按照本文中的界定,计算机可读介质不包括暂存电脑可读媒体(transitory media),如调制的数据信号和载波。

[0113] 还需要说明的是，术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要素的过程、方法、商品或者设备不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种过程、方法、商品或者设备所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括所述要素的过程、方法、商品或者设备中还存在另外的相同要素。

[0114] 本领域技术人员应明白，本说明书的实施例可提供为方法、系统或计算机程序产品。因此，本说明书的实施例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，本说明书的实施例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。


拼车用户
客户端
102
114
116
拼车服务终端
104
112
安全计算
模块
106
108
110

图1

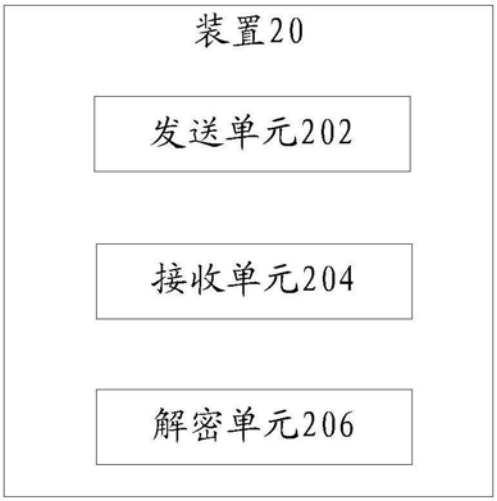
装置20
发送单元202
接收单元204
解密单元206

图2


装置30
接收单元302
发送单元304

图3

图4

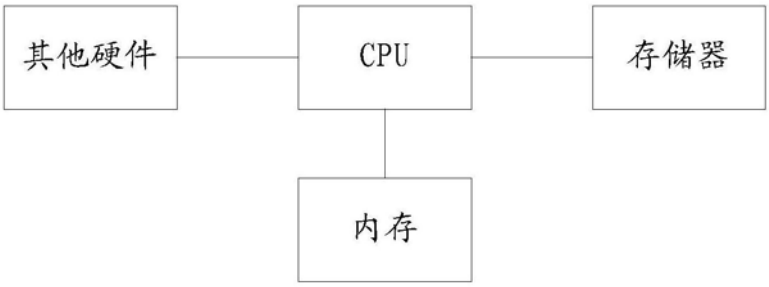

图5