

一种数据处理方法和装置

技术领域

[01] 本说明书实施例涉及数据处理技术领域，更具体地，涉及基于数据使用授权的数据处理方法和装置。

5 背景技术

[02] 在互联网大数据背景下，服务提供商（如信用评估机构、贷款机构、保险公司）在为对象（个人或企业、组织）提供服务时，经常会使用该对象的历史数据对对象进行评估（如信用、喜好等）。个人或企业在与对象开展业务（如商业合作），经常也需要对该对象进行评估（如信用、资产等）。评估需要用户的可信数据，而用户的数据分散在各个数据源（如银行、税务局、房产局等）中。为了保护对象的隐私和评估方法的隐私，现有的技术通常是在评估者（即数据使用方）和一个或多个数据源（即数据提供方）之间运行安全多方计算协议，以使得评估者得到评估结果。在安全多方计算中，主要基于密码学技术进行计算，计算过程中需要数据使用方和数据提供方等多方实时配合。

15 [03] 因此，需要一种更有效的用于保护各方数据安全的数据处理方案。

发明内容

[04] 本说明书实施例旨在提供一种更有效的数据处理方法和装置，以解决现有技术中的不足。

[05] 为实现上述目的，本说明书一个方面提供一种数据处理方法，所述方法在数据提供方执行，所述数据提供方拥有第一明文数据，所述方法包括：

20 [06] 获取所述第一明文数据的第一加密数据、用于解密所述第一加密数据的第一密钥、以及关于所述第一明文数据的授权信息；

[07] 向数据管理方发送验证请求，其中，所述数据管理方包括第一可信执行环境；

[08] 从所述数据管理方接收认证信息，并基于所述认证信息进行验证，其中，所述认证信息由所述第一可信执行环境生成；

25 [09] 在验证通过的情况下，将所述第一密钥和所述授权信息安全传输至所述第一可信

执行环境；以及

[10] 将所述第一加密数据提供给所述数据管理方。

[11] 本说明书另一方面提供一种数据处理方法，所述方法在数据提供方执行，所述数据提供方拥有第一明文数据，所述方法包括：

5 [12] 获取关于所述第一明文数据的授权信息；

[13] 向数据管理方发送验证请求，其中，所述数据管理方包括第一可信执行环境；

[14] 从所述数据管理方接收认证信息，并基于所述认证信息进行验证，其中，所述认证信息由所述第一可信执行环境生成；以及

10 [15] 在验证通过的情况中，将所述第一明文数据和所述授权信息安全传输至所述第一可信执行环境。

[16] 在一个实施例中，所述授权信息包括至少一个代码哈希值，所述至少一个代码哈希值分别为被允许使用所述第一明文数据的至少一个程序各自的代码哈希值。

[17] 在一个实施例中，所述授权信息包括与所述至少一个代码哈希值分别对应的至少一个访问权限信息，所述访问权限信息为关于相应程序的计算结果的信息。

15 [18] 在一个实施例中，所述访问权限信息为第二密钥，所述第二密钥用于加密相应的计算结果、由与该计算结果对应的计算结果使用方提供。

[19] 在一个实施例中，所述访问权限信息为空信息。

[20] 在一个实施例中，基于所述认证信息进行验证包括，基于所述认证信息验证：所述第一可信执行环境中是否安装有并正在执行用于数据使用授权的程序。

20 [21] 在一个实施例中，所述安全传输为加密传输。

[22] 本说明书另一方面提供一种数据处理方法，所述方法在数据管理方执行，所述数据管理方包括第一可信执行环境、并且存储有至少一份加密数据，其中，在所述第一可信执行环境中存储有至少一个第一密钥和与所述至少一个第一密钥分别对应的至少一份授权信息，其中，所述至少一个第一密钥用于分别解密所述至少一份加密数据以分别

25 获取至少一份明文数据，所述至少一份授权信息与所述至少一份明文数据分别对应，且所述授权信息为关于被允许使用相应的明文数据的至少一个程序的信息，所述方法包括：

[23] 接收数据使用方的数据请求，所述数据请求用于请求使用所述至少一份明文数据，

其中，所述数据使用方包括第二可信执行环境；

[24] 从所述数据使用方接收认证信息，所述认证信息由所述第二可信执行环境生成；

[25] 在所述第一可信执行环境中，对于每份所述授权信息，基于所述认证信息和该份授权信息进行验证；以及

5 [26] 对于每份所述授权信息，

[27] 在验证通过的情况中，由第一可信执行环境将与该份授权信息对应的第一密钥安全传输给所述第二可信执行环境，以及

[28] 将相应的加密数据提供给所述数据使用方。

[29] 本说明书另一方面提供一种数据处理方法，所述方法在数据管理方执行，所述数据管理方包括第一可信执行环境，其中，在所述第一可信执行环境中存储有至少一份明文数据、以及与所述至少一份明文数据分别对应的至少一份授权信息，其中，所述授权信息为关于被允许使用相应的明文数据的至少一个程序的信息，所述方法包括：

[30] 接收数据使用方的数据请求，所述数据请求用于请求使用所述至少一份明文数据，其中，所述数据使用方包括第二可信执行环境；

15 [31] 从所述数据使用方接收认证信息，其中，所述认证信息由所述第二可信执行环境生成；

[32] 在所述第一可信执行环境中，对于每份所述授权信息，基于所述认证信息和该份授权信息进行验证；以及

[33] 对于每份所述授权信息，在验证通过的情况中，由第一可信执行环境将与该份授权信息对应的明文数据安全传输给所述第二可信执行环境。

[34] 在一个实施例中，所述第一可信执行环境与所述第二可信执行环境位于一个平台、或不同的平台中。

[35] 在一个实施例中，从所述数据使用方接收认证信息包括，由所述第一可信执行环境接收从所述第二可信执行环境安全传输的认证信息。

25 [36] 在一个实施例中，所述认证信息中包括所述第二可信执行环境中安装并正在运行的第一程序的第一代码哈希值，其中，所述每份授权信息包括所述至少一个程序各自的代码哈希值，其中，对于每份所述授权信息，基于所述认证信息和该份授权信息进行验证包括，对于每份授权信息，验证所述第一代码哈希值是否为该份授权信息中包括的一

个代码哈希值。

[37] 在一个实施例中，每份所述授权信息中包括第一代码哈希值、和与所述第一代码哈希值对应的第二密钥，所述第二密钥用于对所述第一程序的计算结果进行加密、由与该计算结果对应的计算结果使用方提供，其中，所述方法还包括，对于每份所述授权信息，在验证通过的情况中，还由所述第一可信执行环境将所述第二密钥安全传输给所述第二可信执行环境。

[38] 在一个实施例中，所述数据管理方还包括数据存储模块，其中，所述至少一份加密数据被存储在所述数据存储模块中。

[39] 本说明书另一方面提供一种数据处理方法，所述方法在数据使用方执行，所述数据使用方包括第二可信执行环境，所述第二可信执行环境中运行有第一程序，所述方法包括：

[40] 向数据管理方发送数据请求，用于请求使用与数据管理方中存储的至少一份加密数据对应的至少一份明文数据，其中，所述数据管理方包括第一可信执行环境，在所述第一可信执行环境中存储有至少一个第一密钥和与所述至少一个第一密钥分别对应的至少一份授权信息，其中，所述至少一个第一密钥用于分别解密所述至少一份加密数据以分别获取所述至少一份明文数据，所述至少一份授权信息与所述至少一份明文数据分别对应，且所述授权信息为关于被允许使用相应的明文数据的至少一个程序的信息；

[41] 向所述数据管理方发送认证信息，以使得所述第一可信执行环境对于每份所述授权信息基于所述认证信息和该份授权信息进行验证，其中，所述认证信息由所述第二可信执行环境生成；

[42] 对于每份所述授权信息，在验证通过的情况中，由所述第二可信执行环境接收从所述第一可信执行环境安全传输的与该份授权信息对应的第一密钥；从所述数据管理方获取与该份授权信息对应的加密数据；在所述第二可信执行环境中使用该第一密钥对该加密数据进行解密，以获取相应的明文数据；以及

[43] 在所述第二可信执行环境中通过所述第一程序基于所述至少一份明文数据进行计算，以获取计算结果。

[44] 本说明书另一方面提供一种数据处理方法，所述方法在数据使用方执行，所述数据使用方包括第二可信执行环境，所述第二可信执行环境中运行有第一程序，所述方法包括：

[45] 向数据管理方发送数据请求，用于请求使用数据管理方中存储的至少一份明文数据，其中，所述数据管理方包括第一可信执行环境，在所述第一可信执行环境中存储有至少一份明文数据和与至少一份明文数据分别对应的至少一份授权信息，其中，所述授权信息为关于被允许使用相应的明文数据的至少一个程序的信息；

- 5 [46] 向所述数据管理方发送认证信息，以使得所述第一可信执行环境对于每份所述授权信息基于所述认证信息和该份授权信息进行验证，其中，所述认证信息由所述第二可信执行环境生成；

[47] 对于每份所述授权信息，在验证通过的情况中，由所述第二可信执行环境接收从所述第一可信执行环境安全传输的与该份授权信息对应的明文数据；以及

- 10 [48] 在所述第二可信执行环境中通过所述第一程序基于所述至少一份明文数据进行计算，以获取计算结果。

[49] 在一个实施例中，所述第一程序具有第一代哈希值，其中，每份授权信息中包括第一代哈希值、及与第一代哈希值对应的第二密钥，所述第二密钥用于对所述第一程序的计算结果进行加密、由该计算结果对应的计算结果使用方提供，所述方法还包括：

15

[50] 对于每份所述授权信息，在验证通过的情况中，由所述第二可信执行环境接收从所述第一可信执行环境安全传输的所述第二密钥；

[51] 在获取所述计算结果之后，在所述第二可信执行环境中确定与各份所述授权信息分别对应的各个第二密钥是否一致；以及

- 20 [52] 在各个所述第二密钥一致的情况中，在所述第二可信执行环境中使用所述第二密钥对所述计算结果进行加密，以获取加密计算结果。

[53] 在一个实施例中，所述方法还包括，在获取加密计算结果之后，将所述加密计算结果发送给所述计算结果使用方。

[54] 在一个实施例中，从所述数据管理方获取与该份授权信息对应的加密数据包括，

- 25 从所述数据管理方读取与该份授权信息对应的加密数据。

[55] 本说明书另一方面提供一种数据处理装置，所述装置在数据提供方实施，所述数据提供方拥有第一明文数据，所述装置包括：

[56] 获取单元，配置为，获取所述第一明文数据的第一加密数据、用于解密所述第一

加密数据的第一密钥、以及关于所述第一明文数据的授权信息；

[57] 发送单元，配置为，向数据管理方发送验证请求，其中，所述数据管理方包括第一可信执行环境；

5 [58] 验证单元，配置为，从所述数据管理方接收认证信息，并基于所述认证信息进行验证，其中，所述认证信息由所述第一可信执行环境生成；

[59] 安全传输单元，配置为，在验证通过的情况下，将所述第一密钥和所述授权信息安全传输至所述第一可信执行环境；以及

[60] 提供单元，配置为，将所述第一加密数据提供给所述数据管理方。

10 [61] 本说明书另一方面提供一种数据处理装置，所述装置在数据提供方实施，所述数据提供方拥有第一明文数据，所述装置包括：

[62] 获取单元，配置为，获取关于所述第一明文数据的授权信息；

[63] 发送单元，配置为，向数据管理方发送验证请求，其中，所述数据管理方包括第一可信执行环境；

15 [64] 验证单元，配置为，从所述数据管理方接收认证信息，并基于所述认证信息进行验证，其中，所述认证信息由所述第一可信执行环境生成；以及

[65] 安全传输单元，配置为，在验证通过的情况下，将所述第一明文数据和所述授权信息安全传输至所述第一可信执行环境。

[66] 在一个实施例中，所述验证单元还配置为，基于所述认证信息验证：所述第一可信执行环境中是否安装有并正在执行用于数据使用授权的程序。

20 [67] 本说明书另一方面提供一种数据处理装置，所述装置在数据管理方实施，所述数据管理方包括第一可信执行环境、并且存储有至少一份加密数据，其中，在所述第一可信执行环境中存储有至少一个第一密钥和与所述至少一个第一密钥分别对应的至少一份授权信息，其中，所述至少一个第一密钥用于分别解密所述至少一份加密数据以分别获取至少一份明文数据，所述至少一份授权信息与所述至少一份明文数据分别对应，且
25 所述授权信息为关于被允许使用相应的明文数据的至少一个程序的信息，所述装置包括：

[68] 第一接收单元，配置为，接收数据使用方的数据请求，所述数据请求用于请求使用所述至少一份明文数据，其中，所述数据使用方包括第二可信执行环境；

[69] 第二接收单元，配置为，从所述数据使用方接收认证信息，所述认证信息由所述

第二可信执行环境生成;

[70] 验证单元,配置为,在所述第一可信执行环境中,对于每份所述授权信息,基于所述认证信息和该份授权信息进行验证;以及

[71] 针对每份授权信息的第一安全传输单元,配置为,在验证通过的情况中,由第一可信执行环境将与该份授权信息对应的第一密钥安全传输给所述第二可信执行环境;以及

[72] 提供单元,配置为,将相应的加密数据提供给所述数据使用方。

[73] 本说明书另一方面提供一种数据处理装置,所述装置在数据管理方实施,所述数据管理方包括第一可信执行环境,其中,在所述第一可信执行环境中存储有至少一份明文数据、以及与所述至少一份明文数据分别对应的至少一份授权信息,其中,所述授权信息为关于被允许使用相应的明文数据的至少一个程序的信息,所述装置包括:

[74] 第一接收单元,配置为,接收数据使用方的数据请求,所述数据请求用于请求使用所述至少一份明文数据,其中,所述数据使用方包括第二可信执行环境;

[75] 第二接收单元,配置为,从所述数据使用方接收认证信息,其中,所述认证信息由所述第二可信执行环境生成;

[76] 验证单元,配置为,在所述第一可信执行环境中,对于每份所述授权信息,基于所述认证信息和该份授权信息进行验证;以及

[77] 针对每份所述授权信息的安全传输单元,配置为,在验证通过的情况中,由第一可信执行环境将与该份授权信息对应的明文数据安全传输给所述第二可信执行环境。

[78] 在一个实施例中,所述验证单元还配置为,由所述第一可信执行环境接收从所述第二可信执行环境安全传输的认证信息。

[79] 在一个实施例中,所述认证信息中包括所述第二可信执行环境中安装并正在运行的第一程序的第一代码哈希值,其中,所述每份授权信息包括所述至少一个程序各自的代码哈希值,其中,所述验证单元还配置为,对于每份授权信息,验证所述第一代码哈希值是否为该份授权信息中包括的一个代码哈希值。

[80] 在一个实施例中,每份所述授权信息中包括第一代码哈希值、和与所述第一代码哈希值对应的第二密钥,所述第二密钥用于对所述第一程序的计算结果进行加密、由与所述计算结果对应的计算结果使用方提供,其中,所述装置还包括第二安全传输单元,配

置为,对于每份所述授权信息,在验证通过的情况中,还由所述第一可信执行环境将所述第二密钥安全传输给所述第二可信执行环境。

[81] 本说明书另一方面提供一种数据处理装置,所述装置在数据使用方实施,所述数据使用方包括第二可信执行环境,所述第二可信执行环境中运行有第一程序,所述装置
5 包括:

[82] 第一发送单元,配置为,向数据管理方发送数据请求,用于请求使用与数据管理方中存储的至少一份加密数据对应的至少一份明文数据,其中,所述数据管理方包括第一可信执行环境,在所述第一可信执行环境中存储有至少一个第一密钥和与所述至少一个第一密钥分别对应的至少一份授权信息,其中,所述至少一个第一密钥用于分别解密
10 所述至少一份加密数据以分别获取所述至少一份明文数据,所述至少一份授权信息与所述至少一份明文数据分别对应,且所述授权信息为关于被允许使用相应的明文数据的至少一个程序的信息;

[83] 第二发送单元,配置为,向所述数据管理方发送认证信息,以使得所述第一可信执行环境对于每份所述授权信息基于所述认证信息和该份授权信息进行验证,其中,所述
15 认证信息由所述第二可信执行环境生成;

[84] 针对每份所述授权信息的第一接收单元,配置为,在验证通过的情况中,由所述第二可信执行环境接收从所述第一可信执行环境安全传输的与该份授权信息对应的第一密钥;获取单元,配置为,从所述数据管理方获取与该份授权信息对应的加密数据;解密单元,配置为,在所述第二可信执行环境中使用该第一密钥对该加密数据进行解密,
20 以获取相应的明文数据;以及

[85] 计算单元,配置为,在所述第二可信执行环境中通过所述第一程序基于所述至少一份明文数据进行计算,以获取计算结果。

[86] 本说明书另一方面提供一种数据处理装置,所述装置在数据使用方实施,所述数据使用方包括第二可信执行环境,所述第二可信执行环境中运行有第一程序,所述装置
25 包括:

[87] 第一发送单元,配置为,向数据管理方发送数据请求,用于请求使用数据管理方中存储的至少一份明文数据,其中,所述数据管理方包括第一可信执行环境,在所述第一可信执行环境中存储有所述至少一份明文数据和与所述至少一份明文数据分别对应的至少一份授权信息,其中,所述授权信息为关于被允许使用相应的明文数据的至少一

个程序的信息;

[88] 第二发送单元, 配置为, 向所述数据管理方发送认证信息, 以使得所述第一可信执行环境对于每份所述授权信息基于所述认证信息和该份授权信息进行验证, 其中, 所述认证信息由所述第二可信执行环境生成;

- 5 [89] 针对每份所述授权信息的第一接收单元, 配置为, 对于每份所述授权信息, 在验证通过的情况中, 由所述第二可信执行环境接收从所述第一可信执行环境安全传输的与该份授权信息对应的明文数据; 以及

[90] 计算单元, 配置为, 在所述第二可信执行环境中通过所述第一程序基于所述至少一份明文数据进行计算, 以获取计算结果。

- 10 [91] 在一个实施例中, 所述第一程序具有第一代哈希值, 其中, 每份授权信息中包括第一代哈希值、及与第一代哈希值对应的第二密钥, 所述第二密钥用于对所述第一程序的计算结果进行加密、由与该计算结果对应的计算结果使用方提供, 所述装置还包括,

- [92] 针对每份所述授权信息的第二接收单元, 配置为, 在验证通过的情况中, 由所述
15 第二可信执行环境接收从所述第一可信执行环境安全传输的与该份授权信息对应的第二密钥;

[93] 确定单元, 配置为, 在获取所述计算结果之后, 在所述第二可信执行环境中确定与各份所述授权信息分别对应的各个第二密钥是否一致, 以及

- [94] 加密单元, 配置为, 在各个所述第二密钥一致的情况中, 在所述第二可信执行环
20 境中使用所述第二密钥对所述计算结果进行加密, 以获取加密计算结果。

[95] 在一个实施例中, 所述装置还包括第三发送单元, 配置为, 在获取加密计算结果之后, 将所述加密计算结果发送给所述计算结果使用方。

[96] 在一个实施例中, 所述获取单元还配置为, 从所述数据管理方读取与该份授权信息对应的加密数据。

- 25 [97] 本说明书另一方面提供一种计算设备, 包括存储器和处理器, 其特征在于, 所述存储器中存储有可执行代码, 所述处理器执行所述可执行代码时, 实现上述任一项方法。

[98] 在根据本说明书实施例的数据处理方案中, 利用 TEE、RA 技术搭建了数据提供方可信的数据授权系统, 可以保证数据的隐私性, 多方数据的合规使用; 在设计上达成

了可以针对数据使用行为授权、可选择性地对数据融合的输出结果进行访问控制两个特性,以满足实际多方数据融合的通用入口、出口权限控制;数据授权系统作为中间层,为数据提供方和数据使用方解耦,数据提供方无需部署数据提供服务来实时配合融合业务传输数据,提升易用性。

5 附图说明

[99] 通过结合附图描述本说明书实施例,可以使得本说明书实施例更加清楚:

[100] 图 1 示出根据本说明书实施例的数据处理系统 100 的示意图;

[101] 图 2 示出根据本说明书实施例的一种数据处理方法流程图;

[102] 图 3 示意示出由数据提供方安全传输至第一 TEE 的信息;

10 [103] 图 4 示出根据本说明书实施例的一种数据处理方法流程图;

[104] 图 5 示出根据本说明书实施例的一种数据处理方法流程图;

[105] 图 6 示意示出在数据管理方中存储的数据;

[106] 图 7 示出根据本说明书实施例的一种数据处理方法流程图;

[107] 图 8 示出根据本说明书实施例的一种数据处理方法流程图;

15 [108] 图 9 示出根据本说明书实施例的一种数据处理方法流程图;

[109] 图 10 示出根据本说明书实施例的数据处理方法中数据提供方、数据管理方、数据使用方之间的交互图;

[110] 图 11 示出根据本说明书实施例的一种数据处理装置 1100;

[111] 图 12 示出根据本说明书实施例的一种数据处理装置 1200;

20 [112] 图 13 示出根据本说明书实施例的一种数据处理装置 1300;

[113] 图 14 示出根据本说明书实施例的一种数据处理装置 1400;

[114] 图 15 示出根据本说明书实施例的一种数据处理装置 1500;

[115] 图 16 示出根据本说明书实施例的一种数据处理装置 1600。

具体实施方式

[116] 下面将结合附图描述本说明书实施例。

[117] 图 1 示出根据本说明书实施例的数据处理系统 100 的示意图。如图 1 所示，系统 100 包括数据提供方 11、数据提供方 12、数据管理方 13、数据使用方 14 以及结果使用方 15。其中数据提供方 11/12 例如为银行、税务局、房产局等拥有原始数据的一方；数据管理方 13 相当于数据托管平台，包括第一可信执行环境(TEE)131 和存储模块 132，可由数据提供方将数据及其授权信息预先上传至数据管理方，以进行数据的使用授权，从而使得数据提供方不需在数据使用时实时在线；数据使用方 14 例如为信用评估机构、贷款机构、保险公司等服务提供商，其包括第二 TEE141；结果使用方 15 例如为数据使用方 14 的服务对象，如企业、个人等。数据提供方 11 可在验证第一 TEE 之后，将本地拥有的明文数据 X 的加密数据 X 上传至数据管理方 13 的存储模块 132，并将相应的用于解密的第一密钥和授权信息安全传输至数据管理方 13 的第一 TEE131，以由第一 TEE 进行对该明文数据 X 的使用授权管理。数据提供方 12 可以与数据提供方 11 类似地将其本地的明文数据 Y 的加密数据 Y 上传给存储模块 132，并将相应的第一密钥和授权信息安全传输至第一 TEE131。例如在数据使用方 14 向数据管理方 13 请求使用明文数据 X 时，第一 TEE 可根据与明文数据 X 对应的授权信息对第二 TEE141 进行验证，并在验证通过之后，将相应的第一密钥安全传输至第二 TEE，并将加密数据 X 提供给数据使用方，以授权数据使用方 14 使用该明文数据 X，例如在第二 TEE141 中基于该明文数据 X 进行模型计算。数据使用方 14 可通过与上述类似地方法从数据管理方 13 获取明文数据 Y。数据使用方 14 在例如基于明文数据 X 和明文数据 Y 获取计算结果之后，可基于第一 TEE 安全传输至第二 TEE 的计算结果密钥对该计算结果进行加密，并将加密的计算结果发送给提供所述计算结果密钥的结果使用方 15。

[118] 图 1 及上述描述只是对本说明书实施例的简单概述，并不限定本说明书实施例的范围，例如，在系统 100 中不限于包括两个数据提供方，可包括一个数据提供方，也可包括多个数据提供方，其都与上述类似地将其本地的数据托管给数据管理方 13。

[119] 图 2 示出根据本说明书实施例的一种数据处理方法流程图，所述方法在数据提供方执行，所述数据提供方拥有第一明文数据，所述方法包括：

[120] 在步骤 S202，获取所述第一明文数据的第一加密数据、用于解密所述第一加密数据的第一密钥、以及关于所述第一明文数据的授权信息；

[121] 在步骤 S204, 向数据管理方发送验证请求, 其中, 所述数据管理方包括第一可信执行环境;

[122] 在步骤 S206, 从所述数据管理方接收认证信息, 并基于所述认证信息进行验证, 其中, 所述认证信息由所述第一可信执行环境生成; 以及

- 5 [123] 在步骤 S208, 在验证通过的情况中, 将所述第一密钥和所述授权信息安全传输至所述第一可信执行环境; 以及

[124] 在步骤 S210, 将所述第一加密数据提供给所述数据管理方。

[125] 首先, 在步骤 S202, 获取所述第一明文数据的第一加密数据、用于解密所述第一加密数据的第一密钥、以及关于所述第一明文数据的授权信息。

- 10 [126] 所述第一加密数据可通过对第一明文数据进行对称加密或非对称加密获取。在对称加密的情况中, 所述第一密钥即为用于加密所述第一明文数据的密钥, 在非对称加密的情况中, 所述第一密钥为与用于加密所述第一明文数据的密钥不同的另一密钥。可以理解, 本文中的“第一”, “第二”等描述, 仅仅为了描述的简单而对相似概念进行区分, 并不具有其他限定作用。

- 15 [127] 在一个实施例中, 关于第一明文数据的授权信息包括可使用该第一明文数据的至少一个程序各自的代码哈希值。所述代码哈希值可以为程序的全部代码的哈希值, 也可以为程序在已知执行点的内存占有的哈希值。该至少一个程序即为数据提供者允许使用该第一明文数据的至少一个程序。例如, 在授权信息包括多个代码哈希值的情况中, 表示该第一明文数据可用于多个程序的计算。例如, 该第一明文数据为个人在预定时段内的交易数据, 该交易数据可用于个人信用评估的第一程序的计算、个人消费倾向的第二程序的计算、特定人群消费水平的第三程序的计算等, 则数据提供者(如银行)可在与该交易数据对应的授权信息中包括第一程序、第二程序和第三程序的代码哈希值, 以用于分别对第一程序、第二程序和第三程序的授权。
- 20

- [128] 在一个实施例中, 关于第一明文数据的授权信息还可以包括与各个代码哈希值分别对应的计算结果访问权限信息。在一个实施例中, 所述访问权限信息为第二密钥, 该第二密钥由计算结果使用方提供, 用于对通过与相应的代码哈希值对应的程序获取的计算结果进行加密。通常, 该对计算结果的加密为非对称加密, 即, 第二密钥是计算结果使用方的公钥, 而在对该加密的计算结果解密时, 需要用计算结果使用方的私钥进行解密。可以理解, 该对计算结果的加密也可以为对称加密。例如, 在上述授权信息中, 还
- 25

- 包括与第一程序的哈希值对应的第二密钥，该第二密钥例如为贷款机构服务对象（如企业或个人）的公钥，由该企业或个人预先传输给银行（数据提供者），在通过第一程序基于该第一明文数据获取相应的计算结果之后，数据使用者（如贷款机构）将使用该公钥对该计算结果进行加密，而所述企业或个人在获取该加密的计算结果之后，将使用其私钥进行解密，从而获取明文的计算结果。可以理解，在所述授权信息中并不是对于任一代码哈希值都包括相应的第二密钥。例如，在上述第三程序的情况中，其基于第一明文数据的计算结果是特定人群的消费水平，该结果并不涉及个人隐私，因此不需要对该计算结果进行加密，因此在授权信息中可不包括与第三程序的代码哈希值对应的第二密钥，即，所述访问权限信息为空信息。
- 5 [129] 可以理解，所述授权信息不限于包括所述代码哈希值和所述第二密钥，例如，所述授权信息可以包括可使用所述第一明文数据的程序的代码签名、基于预定加密算法的加密数据等等。
- [130] 在步骤 S204，向数据管理方发送验证请求，其中，所述数据管理方包括第一可信执行环境。
- 15 [131] 在一个实施例中，数据管理方包括授权模块，用于进行对数据使用方的数据使用授权。其中，授权模块为第一可信执行环境，其例如为通过 SGX、Trust Zone 等技术生成的可信执行环境（TEE，Trusted Execution Environment）。所述验证请求例如用于请求验证该第一 TEE 是否为可信执行环境、其中是否安装、并正在运行用于进行数据使用授权的程序等等。数据提供方可向第一 TEE 直接发送验证请求，或者可向数据管理方平台发送验证请求，并由所述平台将验证请求转发给第一 TEE。
- 20 [132] 在步骤 S206，从所述数据管理方接收认证信息，并基于所述认证信息进行验证，其中，所述认证信息由所述第一可信执行环境生成。
- [133] 第一 TEE 在接收所述验证请求之后，基于其内部机制生成认证信息，并将该认证信息发送给数据提供者以供其验证。所述认证信息例如包括所述第一 TEE 的签名信息、硬件信息和软件信息等。其中，所述签名信息例如通过第一 TEE 的硬件密钥生成；所述硬件信息例如包括，各种硬件的指标，比如 CPU 主频，内存容量等等；所述软件信息包括各个程序的代码哈希值、代码名称、版本、运行日志等。如本领域技术人员所知，TEE 可通过内存硬件执行对其中运行程序的“测量”，例如获取该程序的代码哈希值、该程序在特定执行点的内存占有的哈希值等等，并在所述认证信息中包括对所述程序的“测量”信息，由于该“测量”信息由该第一 TEE 自身实体（内存硬件）执行，而不
- 25
- 30

涉及任何软件、操作系统，因此是真实可信的。可以理解，所述认证信息不限于如上所述，例如，所述认证信息不必需包括签名信息、软件信息等，而可以只包括软件信息，以供数据提供方进行对第一 TEE 中运行程序的验证。

[134] 数据提供者在从第一 TEE 接收认证信息之后，可以基于所述认证信息验证所述第一 TEE 是否为可信执行环境，例如通过预先获取的第一 TEE 的硬件公钥验证所述签名信息是否为所述第一 TEE 的签名信息、验证所述第一 TEE 的硬件配置是否与预先获取的配置相符等等。第一 TEE 还可以将认证信息中包括的第一 TEE 对其中运行程序的“测量”信息与预先获取的用于进行数据使用授权的程序的代码哈希值相比较以进行验证，以确定第一 TEE 中是否安装并正在运行用于进行数据使用授权的程序。所述代码哈希值例如从由程序发布者提供的代码签名获取，或者从开源的所述程序计算获取。

[135] 在本说明书实施例中，基于认证信息的验证过程不限于如上所述，例如，所述认证信息中可能不包括第一 TEE 的硬件信息、签名信息等，相应地，数据提供方可通过为第一 TEE 提供技术支持的第三方服务器（如为围圈（Enclave）提供验证服务的 Intel 服务器）验证第一 TEE 的签名信息、硬件配置等。

[136] 可以理解，对于基于不同技术获取的 TEE，其提供的认证信息的具体内容、形式等会有一些差别，然而，其提供的认证都可使得数据使用者能够进行相应的验证，以确定该 TEE 是否为安全执行环境，和/或确定其中运行的程序是否是预期程序。另外，所述认证信息不限于由第一 TEE 发送给数据提供方，也可由数据管理方中其它模块从第一 TEE 获取所述认证信息并发送给数据提供方。

[137] 在步骤 S208，在验证通过的情况中，将所述第一密钥和所述授权信息安全传输至所述第一可信执行环境。

[138] 在通过上述验证确定第一 TEE 是可信执行环境，并且其可提供数据使用授权服务之后，数据提供者可将自己拥有的数据交给该数据管理方进行托管。具体是，首先，数据提供者将第一密钥和相应的授权信息安全传输至第一 TEE。所述安全传输例如为加密传输，通过在传输之前对待传输的数据进行加密，并在传输到接收方之后进行解密以使得接收方获取明文数据，保障了在传输过程中不会被恶意的第三方窃取明文数据，保障了数据传输的安全性。可以理解所述安全传输不限于加密传输，而可以采用本领域技术人员可获取的任意保障数据安全性的传输方式，如通过量子通信的安全传输方式等等。

[139] 图 3 示意示出由数据提供方安全传输至第一 TEE 的信息 A 的示意图。如图中所示，

由数据提供方安全传输至第一 TEE 的信息 A 与上述第一明文数据相对应, 包括第一密钥 A 和授权信息 A, 其中授权信息 A 如图中“第一密钥 A”下方的黑框所示包括: 对应的第一代哈希值和第二密钥 C、对应的第二代哈希值和第二密钥 D、以及第三代哈希值。其中, 第一密钥用于对第一加密数据进行解密以获取第一明文数据。第一代

5 码哈希值、第二代哈希值和第三代哈希值例如分别为上述第一程序、第二程序和第三程序的代码哈希值。第二密钥 C 例如为第一结果使用方 C 的公钥, 即, 第一程序基于第一明文数据的计算结果只授权给第一结果使用方 C 使用。类似地, 第二密钥 D 例如为第二结果使用方 D 的公钥, 即, 第二程序基于第一明文数据的计算结果只授权给第二结果使用方 D 使用。而在上述信息 A 中并没有与第三代哈希值对应的公钥, 也就是说, 第三程序基于第一明文数据的计算结果不涉及隐私数据, 不需要进行加密。可以

10 理解, 所述授权信息中不限于包括各个所述程序的代码哈希值, 而是根据授权的方式不同可包括不同的信息, 例如, 所述授权信息中可包括各个所述程序的代码签名、加密数据等等。另外, 所述第二密钥 C/D 不限于为相应结果使用方的公钥, 在对计算结果的加密方式为对称加密的情况下, 所述第二密钥 C/D 也可以用于对加密计算结果的解密。其中, 第二密钥中的“第二”用于与本文中的“第一密钥”相区分。

15

[140] 在步骤 S210, 将所述第一加密数据提供给所述数据管理方。

[141] 在一个实施例中, 由数据提供方将存储在本地的第一加密数据发送给数据管理方。在一个实施例中, 由数据管理方从数据提供方读取所述第一加密数据。例如, 在第一明文数据为例如银行提供的个人交易数据的情况下, 数据管理方例如可以基于个人身份标识 (例如身份证号码等)、数据标识等读取与该个人相关的第一加密数据。在一个实施

20 例中, 由数据提供方将存储第一加密数据的网盘地址发送给数据管理方以使其获取所述第一加密数据。

[142] 图 4 示出根据本说明书实施例的一种数据处理方法流程图, 所述方法在数据提供方执行, 所述数据提供方拥有第一明文数据, 所述方法包括:

25 [143] 在步骤 S402, 获取关于所述第一明文数据的授权信息;

[144] 在步骤 S404, 向数据管理方发送验证请求, 其中, 所述数据管理方包括第一可信执行环境;

[145] 在步骤 S406, 从所述数据管理方接收认证信息, 并基于所述认证信息进行验证, 其中, 所述认证信息由所述第一可信执行环境生成; 以及

[146] 在步骤 S408, 在验证通过的情况中, 将所述第一明文数据和所述授权信息安全传输至所述第一可信执行环境。

[147] 图 4 所示方法与图 2 所示方法不同在于, 数据提供方未对第一明文数据进行加密, 因此, 在步骤 S402, 仅获取关于所述第一明文数据的授权信息, 而没有获取第一明文数据的加密数据以及第一密钥。数据提供方在如上文所述对第一 TEE 进行验证之后, 在步骤 S408, 直接将第一明文数据和相关的授权信息一起安全传输至第一 TEE, 即, 不需要对第一明文数据进行加密以获取加密数据(也从而不需数据管理方的存储模块), 并且不需要分别提供加密数据、安全传输加密数据的解密密钥。由于第一 TEE 的安全机制, 第一明文数据以明文数据的形式存储与第一 TEE 中是安全的, 而通过安全传输的方式传输第一明文数据, 在传输过程中也不会泄露第一明文数据。因此, 通过该方式也可以安全地进行对第一明文数据的托管。

[148] 图 5 示出根据本说明书实施例的一种数据处理方法流程图, 所述方法在数据管理方执行, 所述数据管理方包括第一可信执行环境、并且存储有至少一份加密数据, 其中, 在所述第一可信执行环境中存储有至少一个第一密钥和与所述至少一个第一密钥分别对应的至少一份授权信息, 其中, 所述至少一个第一密钥用于分别解密所述至少一份加密数据以分别获取至少一份明文数据, 所述至少一份授权信息与所述至少一份明文数据分别对应, 且所述授权信息为关于被允许使用相应的明文数据的至少一个程序的信息, 所述方法包括:

[149] 在步骤 S502, 接收数据使用方的数据请求, 所述数据请求用于请求使用所述至少一份明文数据, 其中, 所述数据使用方包括第二可信执行环境;

[150] 在步骤 S504, 从所述数据使用方接收认证信息, 所述认证信息由所述第二可信执行环境生成;

[151] 在步骤 S506, 在所述第一可信执行环境中, 对于每份所述授权信息, 基于所述认证信息和该份授权信息进行验证; 以及

[152] 对于每份所述授权信息,

[153] 在步骤 S508, 在验证通过情况下, 由第一可信执行环境将与该份授权信息对应的第一密钥安全传输给第二可信执行环境; 以及

[154] 在步骤 S510, 将相应的加密数据提供给所述数据使用方。

[155] 图 6 示出数据管理方的存储模块和第一 TEE 中存储的数据的示意图。如图 6 所示,

存储模块中存储有加密数据 X 和加密数据 Y，其中，加密数据 X 例如由数据提供方 A 向数据管理方预先上传，其对应于明文数据 X，加密数据 Y 例如由数据提供方 B 向数据管理方预先上传，其对应于明文数据 Y。可以理解，所述加密数据 X/Y 不限于存储于存储模块中，例如，加密数据 X/Y 可存储于第一 TEE 中、或者可存储于云盘中等等。

5 [156] 第一 TEE 中存储有信息 A 和信息 B，其中信息 A 与加密数据 X 相关，其中包括第一密钥 A 和授权信息 A，信息 B 与加密数据 Y 相关，其中包括第一密钥 B 和授权信息 B。其中，第一密钥 A 用于对明文数据 X 进行加密和解密，授权信息 A 为关于明文数据 X 的授权信息，第二密钥 B 用于对明文数据 Y 进行加密和解密，授权信息 B 为关于明文数据 Y 的授权信息。其中，授权信息 A 的示例内容可参考图 3 所示。图 6 中虽然
10 只示意示出了两份加密数据和与其分别对应的两份信息，然而，第一 TEE 中不限于只存储两份信息，而是可以存储与多份加密数据分别对应的多份信息。另外，图 6 中的信息 A 和信息 B 分别对应于不同的数据提供方，本说明书实施例不限于此，信息 A 和信息 B 可对应于一个数据提供方，即，数据提供方 A 与数据提供方 B 可以为一个数据提供方，也就是说，明文数据 X 和明文数据 Y 可由一个数据提供方提供。在上述描述中，
15 加密数据 X 表示该加密数据是通过对明文数据 X 进行加密所获取的数据，加密数据 Y 可同样地解释，信息 A、第一密钥 A 和授权信息 A 表示其都与数据提供方 A 相关，信息 B、第一密钥 B 和授权信息 B 可同样地解释。

[157] 下面详细描述图 5 中的各个步骤。

[158] 首先，在步骤 S502，接收数据使用方的数据请求，所述数据请求用于请求使用所
20 述至少一份明文数据，其中，所述数据使用方包括第二可信执行环境。

[159] 数据使用方例如为信用评估机构，其在对用户进行信用评估时，可向数据管理方请求与该用户相关的例如两份数据，该两份数据例如分别由银行和税务部门向数据管理方预先提供。数据使用方例如可以基于用户身份标识（例如身份证号码等）、数据提供方标识、数据标识等获取与该用户相关的数据。所述数据使用方例如还可以为云计算平
25 台，其例如接收信用评估机构的委托通过模型对用户的信用评估进行计算。

[160] 数据使用方包括第二可信执行环境（即第二 TEE），在该第二 TEE 中运行有预定程序（例如第一程序），以用于基于上述明文数据 X 和明文数据 Y 进行例如 $F(X, Y)$ 的计算，从而通过第二 TEE 的安全机制，在计算过程中不会对外泄露明文数据 X 和明文数据 Y。在一个实施例中，第二 TEE 与第一 TEE 位于一个平台中，例如，在支付宝
30 平台中，可同时进行数据的托管、以及对用户进行信用评估，即所述支付宝平台既是数

据管理方，也是数据使用方。在该情况中，由于相关的数据使用授权、数据使用都是在第一 TEE 和第二 TEE 中进行，即通过硬件对数据隐私进行保护，从而即使数据管理方与数据使用方为同一方，也不影响数据的安全性。在第一 TEE 和第二 TEE 在一个平台的情况中，可由第二 TEE 向第一 TEE 发送数据使用请求。可以理解，在该情况中，也可以由第二 TEE 向数据管理方发送数据使用请求、或者由数据使用方向数据管理方或第一 TEE 发送数据使用请求。

[161] 在一个实施例，第一 TEE 与第二 TEE 位于不同的平台中，例如支付宝平台为数据管理方，其包括第一 TEE，而云计算平台为数据使用方，云计算平台中包括第二 TEE。在第一 TEE 和第二 TEE 在不同平台的情况中，可由数据使用方平台向数据管理方平台发送数据使用请求。类似地，也可以由数据使用方平台向第一 TEE 发送数据使用请求，或者也可由第二 TEE 向数据管理方平台或第一 TEE 发送数据使用请求。

[162] 数据使用方向数据管理方发送请求，以请求获取数据管理方中的至少一份加密数据对应的至少一份明文数据，即请求获取所述至少一份加密数据及相应的解密密钥（第一密钥）。

[163] 在步骤 S504，从所述数据使用方接收认证信息，所述认证信息由所述第二可信执行环境生成。

[164] 数据使用方可在发送数据请求之后将第二 TEE 生成的认证信息发送给数据管理方，也可以在数据管理方向数据使用方发送验证请求之后，将由第二 TEE 生成的认证信息发送给数据管理方。

[165] 第二 TEE 基于内部机制生成认证信息，以供数据管理方进行验证。所述认证信息例如包括所述第二 TEE 的签名信息、硬件信息和软件信息等。其中，所述签名信息例如通过第二 TEE 的硬件密钥生成；所述硬件信息例如包括，各种硬件的指标，比如 CPU 主频，内存容量等等；所述软件信息包括各个程序的代码哈希值、代码名称、版本运行日志等。如本领域技术人员可知，TEE 可通过内存硬件执行对其中运行程序的“测量”，例如获取该程序的代码哈希值、该程序在特定执行点的内存占有的哈希值等等，从而在所述认证信息中包括对所述程序的“测量”信息（例如，代码哈希值），由于该“测量”信息由该 TEE 自身实体（内存硬件）执行，而不涉及任何软件、操作系统，因此是真实可信的。可以理解，所述认证信息不限于如上所述，例如，所述认证信息不必需包括签名信息、软件信息等，而可以只包括软件信息，以供第一 TEE 进行对第二 TEE 中运行程序的验证。

[166] 在一个实施例中，第一 TEE 与第二 TEE 位于一个平台中，所述认证信息为平台内（Intra-Platform）认证信息，例如，在 SGX 技术中，生成文件“REPORT”作为所述平台内认证信息。在一个实施例中，第一 TEE 与第二 TEE 位于不同平台中，所述认证信息为平台间（Inter-Platform）认证信息。例如，在 SGX 技术中，TEE 生成文件“QUOTE”
5 作为所述平台间认证信息，以用于进行远程认证（RA，remote attestation）。平台内认证信息和平台间认证信息可具有不同的文件格式，加密方式等。例如，所述平台内认证信息（如 REPROT）可采用对称加密方式，所述平台间认证信息（如 QUOTE）可采用非对称加密方式等。在一个实施例中，所述认证信息中包括与第二 TEE 中的运行程序（如第一程序）相关的信息，为了不泄露运行程序中的模型数据（如参数、算法等），
10 由第二 TEE 向第一 TEE 安全传输该认证信息。在计算模型不需要进行保护的情况中，也可由第二 TEE 或数据使用方向数据管理方发送所述认证信息，并且数据管理方在接收所述认证信息之后将所述认证信息发送给第一 TEE。

[167] 在步骤 S506，在所述第一可信执行环境中，对于每份所述授权信息，基于所述认证信息和该份授权信息进行验证；

15 [168] 第一 TEE 在获取所述认证信息之后，在其内部通过基于该认证信息和数据使用方请求的至少一份数据各自对应的授权信息进行验证。例如，参考图 6，数据使用方请求使用明文数据 X 和明文数据 Y，第一 TEE 中与明文数据 X 对应的信息 A 中的授权信息例如包括可使用明文数据 X 的各个程序各自的代码哈希值，与明文数据 Y 对应的信息 B 中的授权信息例如包括可使用明文数据 Y 的各个程序各自的代码哈希值。第一 TEE 需
20 要基于认证信息、信息 A 和信息 B 进行验证。第一 TEE 可以基于所述认证信息验证所述第二 TEE 是否为可信执行环境，例如通过预先获取的第二 TEE 的硬件公钥验证所述签名信息是否为所述第二 TEE 的签名信息、验证所述第二 TEE 的硬件配置是否与预先获取的配置相符等等。第一 TEE 还可以基于所述认证信息中包括的第二 TEE 中运行程序的“测量”哈希值，验证该“测量”哈希值是否与所述信息 A 中包括的多个代码哈希
25 值中的一个匹配，以确定所述第二 TEE 中运行的程序是否可以授权使用所述明文数据 X 的程序。类似地，验证该“测量”哈希值是否与所述信息 B 中包括的多个代码哈希值中的一个匹配。其中，针对各份授权信息的验证可以先后进行、也可以并行进行，本申请对此并不限制。

[169] 如上文所述，所述授权信息中不限于包括各个程序的代码哈希值，例如还可以包
30 括各个程序的代码签名、代码加密数据等。例如，在授权信息中为代码签名的情况中，

第一 TEE 可基于代码签名和预先从例如数据提供方获取的相应代码的公钥，获取相应的代码哈希值，以用于上述验证。

[170] 在本说明书实施例中，基于认证信息的验证过程不限于如上所述，例如，所述认证信息中可能不包括第二 TEE 的硬件信息、签名信息等，相应地，数据管理方可通过为第二 TEE 提供技术支持的第三方服务器（如为围圈（Enclave）提供验证服务的 Intel 服务器）验证第二 TEE 的签名信息、硬件配置等。

[171] 可以理解，对于基于不同技术获取的 TEE，其提供的认证信息的具体内容、形式等会有一些差别，然而，其提供的认证信息都可使得数据使用者能够进行相应的验证，以确定该 TEE 是否为安全执行环境，和/或确定其中运行的程序是否是可授权的程序。

10 [172] 步骤 508-步骤 510 是针对数据使用方请求的至少一份明文数据对应的每份授权信息执行的步骤，对于每份授权信息，可依次地、或并行地执行步骤 508-步骤 510。在下面的描述中，描述了针对一份授权信息（例如如图 6 中所示的授权信息 A）执行步骤 508-510 作为示例。本领域技术人员可以理解，对于所述至少一份授权信息中的其它授权信息，可同样地执行步骤 508-510。

15 [173] 在步骤 S508，在验证通过的情况中，由第一可信执行环境将与该份授权信息对应的第一密钥安全传输给所述第二可信执行环境。

[174] 例如参考图 6 所示，在基于信息 A 和认证信息的验证通过之后，也就是说在第一 TEE 中验证第二 TEE 是可信执行环境，并且第二 TEE 中的运行程序的测量代码哈希值是明文数据 X 对应的授权代码哈希值之后，第一 TEE 可将第一密钥 A 安全传输给第二
20 TEE。

[175] 在步骤 S510，将相应的加密数据提供给所述数据使用方。

[176] 在一个实施例中，数据管理方在如上所述将第一密钥 A 安全传输给数据使用方之后，将其存储模块中存储的加密数据 X 发送给第二 TEE。在一个实施例中，由数据使用方从数据管理方的存储模块中读取加密数据 X。例如，在明文数据 X 为例如银行提供的个人交易数据的情况中，数据使用方例如可以基于个人身份标识（例如身份证号码等）、
25 数据提供方标识（如银行标识）、数据标识等读取与该个人相关的加密数据 X。

[177] 在一个实施例中，在所述加密数据 X 由数据管理方存入云盘中的情况中，数据管理方可将加密数据 X 的下载地址提供给数据使用方，以供其下载。

[178] 在一个实施例中，如图 3 所示，信息 A 中包括的授权信息 A 中还可能包括与部分

哈希代码值分别对应的结果使用方的第二密钥。例如，授权信息 A 中包括与第一代哈希值对应的第二密钥 C。在该情况中，在基于授权信息 A 的验证通过之后，第一 TEE 还将第二密钥 C 安全传输给第二 TEE，以用于对计算结果进行加密。

[179] 图 7 示出根据本说明书实施例的一种数据处理方法流程图，所述方法在数据管理方执行，所述数据管理方包括第一可信执行环境，其中，在所述第一可信执行环境中存储有至少一份明文数据、以及与所述至少一份明文数据分别对应的至少一份授权信息，其中，所述授权信息为关于被允许使用相应的明文数据的至少一个程序的信息，所述方法包括：

10 [180] 在步骤 S702，接收数据使用方的数据请求，所述数据请求用于请求使用所述至少一份明文数据，其中，所述数据使用方包括第二可信执行环境；

[181] 在步骤 S704，从所述数据使用方接收认证信息，其中，所述认证信息由所述第二可信执行环境生成；

[182] 在步骤 S706，在所述第一可信执行环境中，对于每份所述授权信息，基于所述认证信息和该份授权信息进行验证；以及

15 [183] 在步骤 S708，对于每份所述授权信息，在验证通过的情况下，由第一可信执行环境将所述至少一份明文数据安全传输给所述第二可信执行环境。

[184] 图 7 所示方法与图 4 所示方法相对应，通过图 4 所示的方法，使得在所述第一可信执行环境中存储有至少一份明文数据、以及与所述至少一份明文数据分别对应的至少一份授权信息。图 7 所示方法与图 5 所示方法不同在于，在验证通过之后，由第一 TEE 向第二 TEE 安全传输所述至少一份明文数据，而不需要由数据管理方将至少一份加密数据传输给第二 TEE，并由第一 TEE 向第二 TEE 安全传输与至少一份加密数据分别对应的第一密钥（解密密钥）。由于，所述至少一份明文数据在第一 TEE 中、在安全传输过程中、以及在第二 TEE 中都可以得到很好的保护，因此可保障该方法的安全性。

25 [185] 图 8 示出根据本说明书实施例的一种数据处理方法流程图，所述方法在数据使用方执行，所述数据使用方包括第二可信执行环境，所述第二可信执行环境中运行有第一程序，所述方法包括：

[186] 在步骤 S802，向数据管理方发送数据请求，用于请求使用与数据管理方中存储的至少一份加密数据对应的至少一份明文数据，其中，所述数据管理方包括第一可信执行环境，在所述第一可信执行环境中存储有至少一个第一密钥和与所述至少一个第一密钥

分别对应的至少一份授权信息，其中，所述至少一个第一密钥用于分别解密所述至少一份加密数据以分别获取所述至少一份明文数据，所述至少一份授权信息与所述至少一份明文数据分别对应，且所述授权信息为关于被允许使用相应的明文数据的至少一个程序的信息；

- 5 [187] 在步骤 S804，向所述数据管理方发送认证信息，以使得所述第一可信执行环境对于每份所述授权信息基于所述认证信息和该份授权信息进行验证，其中，所述认证信息由所述第二可信执行环境生成；

[188] 对于每份所述授权信息，

- 10 [189] 在步骤 S806，在验证通过的情况中，由所述第二可信执行环境接收从所述第一可信执行环境安全传输的与该份授权信息对应的第一密钥；

[190] 在步骤 S808，从所述数据管理方获取与该份授权信息对应的加密数据；

[191] 在步骤 S810，在所述第二可信执行环境中使用该第一密钥对该加密数据进行解密，以获取相应的明文数据；以及

- 15 [192] 在步骤 S812，在所述第二可信执行环境中通过所述第一程序基于所述至少一份明文数据进行计算，以获取计算结果。

[193] 图 8 所示方法是在数据使用方执行的与图 5 所示方法相对的方法，数据使用方中包括第二 TEE，第二 TEE 中例如运行有第一程序，第二程序在使用数据进行计算之前，首先从数据管理方请求相应的数据，然后在基于该相应的数据进行模型计算。因此步骤 S802-S810 的具体描述可参考上文中对步骤 S502-S508 的相应描述，在此不再赘述。

- 20 [194] 在步骤 S810，在所述第二可信执行环境中使用该第一密钥对该加密数据进行解密，以获取相应的明文数据。例如，第二 TEE 在如上文所述获取图 6 所示的第一密钥 A、并且从数据管理方的存储模块读取了加密数据 X 之后，在第二 TEE 中，可使用第一密钥 A 对加密数据 X 进行解密，从而获取明文数据 X。类似地，通过使用从数据管理方获取的第二密钥 B 对第二加密数据 Y 解密，从而可获取明文数据 Y。

- 25 [195] 在步骤 S812，在所述第二可信执行环境中通过所述第一程序基于所述至少一份明文数据进行计算，以获取计算结果。所述程序例如基于数据 X 和数据 Y 进行 $F(X, Y)$ 的计算，其中 $F(X, Y)$ 对应于特定计算模型，通过在第二 TEE 中运行所述第一程序，使用 $F(X, Y)$ 基于 X 和 Y 进行计算，从而获取计算结果。

[196] 在一个实施例中，如上文所述，对于每份授权信息，在验证通过之后，所述第一 TEE 还向第二 TEE 安全传输与代码哈希值对应的用于加密计算结果的密钥，如图 3 所示的第二密钥 C。所述第一程序例如具有第一代哈希值，其中，所述数据使用者请求的至少一份明文数据对应的每份授权信息中例如包括第一代哈希值、及与所述第一代
5 码哈希值对应的第二密钥（例如第二密钥 C），所述第二密钥用于对所述第一程序的计算结果进行加密、由与该计算结果对应的计算结果使用方提供。所述方法还包括，对于每份所述授权信息，在验证通过的情况中，由所述第二可信执行环境接收从所述第一可信执行环境安全传输的与该授权信息对应的第二密钥；在获取所述计算结果之后，在所述第二可信执行环境中确定与各份所述授权信息分别对应的各个第二密钥是否一致，例
10 如，确定从第一 TEE 接收的对应于加密数据 X 的第二密钥与对应于加密数据 Y 的第二密钥是否一致；以及，在各个所述第二密钥一致的情况中，在所述第二可信执行环境中使用所述第二密钥对所述计算结果进行加密，以获取加密计算结果，即，在所述第二密钥都是第二密钥 C 的情况中，使用第二密钥 C 对计算结果进行加密。可以理解，在上述情况中，第二密钥可以为非对称加密的加密密钥，即公钥，当将该加密的计算结果发
15 送给结果使用方 C 之后，结果使用方 C 将使用其私钥 C 对该加密的计算结果进行解密。然而，本实施例不限于此，例如，所述第二密钥可以为对称加密的密钥，即，结果使用方 C 在解密时也使用该第二密钥进行解密。

[197] 在获取加密的计算结果之后，可由第二 TEE 或数据使用方平台将该加密的计算结果发送给相应的结果使用方，或者可由相应的结果使用方从所述平台读取所述加密的
20 计算结果。

[198] 图 9 示出根据本说明书实施例的一种数据处理方法流程图，所述方法在数据使用方执行，所述数据使用方包括第二可信执行环境，所述方法包括：

[199] 在步骤 S902，向数据管理方发送数据请求，用于请求使用数据管理方中存储的至少一份明文数据，其中，所述数据管理方包括第一可信执行环境，在所述第一可信执行
25 环境中存储有所述至少一份明文数据和与所述至少一份明文数据分别对应的至少一份授权信息，其中，所述授权信息为关于被允许使用相应的明文数据的至少一个程序的信息；

[200] 在步骤 S904，向所述数据管理方发送认证信息，以使得所述第一可信执行环境对于每份所述授权信息基于所述认证信息和该份授权信息进行验证，其中，所述认证信息
30 由所述第二可信执行环境生成；

[201] 在步骤 S906, 对于每份所述授权信息, 在验证通过的情况中, 由所述第二可信执行环境接收从所述第一可信执行环境安全传输的与该份授权信息对应的明文数据; 以及

[202] 在步骤 S908, 在所述第二可信执行环境中通过所述第一程序基于所述至少一份明文数据进行计算, 以获取计算结果。

- 5 [203] 图 9 所示方法与图 7 所示方法相对, 其与图 8 所示方法不同在于, 在步骤 S906, 在验证通过的情况中, 接收从所述第一可信执行环境安全传输的所述至少一份明文数据, 即不是分开获取加密数据和相应的解密密钥, 从而不需要解密的步骤, 从而可以在步骤 S908, 直接通过所述第一程序基于所述至少一份明文数据进行计算, 获取计算结果。

- 10 [204] 图 10 示出根据本说明书实施例的数据处理方法中数据提供方、数据管理方、数据使用方之间的交互图。该三方交互中包括两个阶段, 第一阶段为数据提供方与数据管理方之间的交互, 包括: 在步骤 1001, 数据提供方获取第一明文数据的第一加密数据、用于解密第一加密数据的第一密钥、以及关于第一明文数据的授权信息; 在步骤 1002, 数据提供方向数据管理方发送验证请求; 在步骤 1003, 数据管理方在接收验证请求之后向数据提供方发送认证信息, 其中, 所述认证信息由所述第一可信执行环境生成; 在步骤 15 1004, 数据管理方基于认证信息进行验证; 以及在步骤 1005, 在验证通过之后, 数据管理方将所述第一密钥和授权信息安全传输至第一 TEE, 将第一加密数据提供给数据管理方。通过上述步骤, 数据提供方可将己方的数据托管给数据管理方, 以通过数据管理方进行对第三方使用第一明文数据的授权, 从而不需要在数据使用过程中实时在线。

- [205] 第二阶段为数据管理方与数据使用方之间的交互, 包括以下步骤: 在步骤 1006, 20 数据使用方向数据管理方发送数据请求, 以请求使用所述数据管理方中的至少一份明文数据; 在步骤 1007, 数据使用方向数据管理方发送认证信息, 所述认证信息由数据使用方中的第二 TEE 生成; 在步骤 1008, 在数据管理方的第一 TEE 中基于所述认证信息和第一 TEE 中已有的相关授权信息进行验证; 在步骤 1009, 对于每份授权信息, 在验证通过之后, 由第一可信执行环境将与该份授权信息对应的第一密钥安全传输给所述第二 25 可信执行环境, 并且, 数据管理方向数据使用方提供相应的加密数据; 在步骤 1010, 对于每份授权信息, 数据使用方在第二 TEE 中使用相应的密钥对相应的加密数据进行解密, 获取相应的明文数据; 在步骤 1011, 数据使用方在第二 TEE 中基于所述至少一份明文数据进行模型计算, 从而获取计算结果; 以及在步骤 1012, 数据使用方在第二 TEE 中使用授权信息中包括的第二密钥对计算结果加密。在获取加密的计算结果之后, 数据 30 使用方可将该加密结果发送给结果使用方, 或者也可以由结果使用方主动从数据使用方

读取所述加密结果。

[206] 图 11 示出根据本说明书实施例的一种数据处理装置 1100, 所述装置在数据提供方实施, 所述数据提供方拥有第一明文数据, 所述装置包括:

5 [207] 获取单元 111, 配置为, 获取所述第一明文数据的第一加密数据、用于解密所述第一加密数据的第一密钥、以及关于所述第一明文数据的授权信息;

[208] 发送单元 112, 配置为, 向数据管理方发送验证请求, 其中, 所述数据管理方包括第一可信执行环境;

[209] 验证单元 113, 配置为, 从所述数据管理方接收认证信息, 并基于所述认证信息进行验证, 其中, 所述认证信息由所述第一可信执行环境生成;

10 [210] 安全传输单元 114, 配置为, 在验证通过的情况中, 将所述第一密钥和所述授权信息安全传输至所述第一可信执行环境; 以及

[211] 提供单元 115, 配置为, 将所述第一加密数据提供给所述数据管理方。

[212] 在一个实施例中, 所述验证单元 113 还配置为, 基于所述认证信息验证: 所述第一可信执行环境中是否安装有并正在执行用于数据使用授权的程序。

15 [213] 图 12 示出根据本说明书实施例的一种数据处理装置 1200, 所述装置在数据提供方实施, 所述数据提供方拥有第一明文数据, 所述装置包括:

[214] 获取单元 121, 配置为, 获取关于所述第一明文数据的授权信息;

[215] 发送单元 122, 配置为, 向数据管理方发送验证请求, 其中, 所述数据管理方包括第一可信执行环境;

20 [216] 验证单元 123, 配置为, 从所述数据管理方接收认证信息, 并基于所述认证信息进行验证, 其中, 所述认证信息由所述第一可信执行环境生成; 以及

[217] 安全传输单元 124, 配置为, 在验证通过的情况中, 将所述第一明文数据和所述授权信息安全传输至所述第一可信执行环境。

25 [218] 图 13 示出根据本说明书实施例的一种数据处理装置 1300, 所述装置在数据管理方实施, 所述数据管理方包括第一可信执行环境、并且存储有至少一份加密数据, 其中, 在所述第一可信执行环境中存储有至少一个第一密钥和与所述至少一个第一密钥分别对应的至少一份授权信息, 其中, 所述至少一个第一密钥用于分别解密所述至少一份加密数据以分别获取至少一份明文数据, 所述至少一份授权信息与所述至少一份明文数据

分别对应，且所述授权信息为关于被允许使用相应的明文数据的至少一个程序的信息，所述装置包括：

[219] 第一接收单元 1301，配置为，接收数据使用方的数据请求，所述数据请求用于请求使用所述至少一份明文数据，其中，所述数据使用方包括第二可信执行环境；

- 5 [220] 第二接收单元 1302，配置为，从所述数据使用方接收认证信息，所述认证信息由所述第二可信执行环境生成；

[221] 验证单元 1303，配置为，在所述第一可信执行环境中，对于每份所述授权信息，基于所述认证信息和该份授权信息进行验证；以及

- 10 [222] 针对每份授权信息的第一安全传输单元 1304，配置为，在验证通过的情况中，由第一可信执行环境将与该份授权信息对应的第一密钥安全传输给所述第二可信执行环境；以及

[223] 提供单元 1350，配置为，将相应的加密数据提供给所述数据使用方。

[224] 在一个实施例中，所述验证单元 1303 还配置为，由所述第一可信执行环境接收从所述第二可信执行环境安全传输的认证信息。

- 15 [225] 在一个实施例中，所述认证信息中包括所述第二可信执行环境中安装并正在运行的第一程序的第一代码哈希值，其中，所述每份授权信息包括所述至少一个程序各自的代码哈希值，其中，所述验证单元 1303 还配置为，对于每份授权信息，验证所述第一代哈希值是否为该份授权信息中包括的一个代码哈希值。

- 20 [226] 在一个实施例中，每份所述授权信息中包括第一代哈希值、和与所述第一代哈希值对应的第二密钥，所述第二密钥用于对所述第一程序的计算结果进行加密、由与该计算结果对应的计算结果使用方提供，其中，所述装置还包括第二安全传输单元 1306，配置为，对于每份所述授权信息，在验证通过的情况中，还由所述第一可信执行环境将所述第二密钥安全传输给所述第二可信执行环境。

- 25 [227] 图 14 示出根据本说明书实施例的一种数据处理装置 1400，所述装置在数据管理方实施，所述数据管理方包括第一可信执行环境，其中，在所述第一可信执行环境中存储有至少一份明文数据、以及与所述至少一份明文数据分别对应的至少一份授权信息，其中，所述授权信息为关于被允许使用相应的明文数据的至少一个程序的信息，所述装置包括：

[228] 第一接收单元 1401, 配置为, 接收数据使用方的数据请求, 所述数据请求用于请求使用所述至少一份明文数据, 其中, 所述数据使用方包括第二可信执行环境;

[229] 第二接收单元 1402, 配置为, 从所述数据使用方接收认证信息, 其中, 所述认证信息由所述第二可信执行环境生成;

- 5 [230] 验证单元 1403, 配置为, 在所述第一可信执行环境中, 对于每份所述授权信息, 基于所述认证信息和该份授权信息进行验证; 以及

[231] 针对每份所述授权信息的安全传输单元 1404, 配置为, 在验证通过的情况中, 由第一可信执行环境将与该份授权信息对应的明文数据安全传输给所述第二可信执行环境。

- 10 [232] 图 15 示出根据本说明书实施例的一种数据处理装置 1500, 所述装置在数据使用方实施, 所述数据使用方包括第二可信执行环境, 所述第二可信执行环境中运行有第一程序, 所述装置包括:

[233] 第一发送单元 1501, 配置为, 向数据管理方发送数据请求, 用于请求使用与数据管理方中存储的至少一份加密数据对应的至少一份明文数据, 其中, 所述数据管理方包
15 括第一可信执行环境, 在所述第一可信执行环境中存储有至少一个第一密钥和与所述至少一个第一密钥分别对应的至少一份授权信息, 其中, 所述至少一个第一密钥用于分别解密所述至少一份加密数据以分别获取所述至少一份明文数据, 所述至少一份授权信息与所述至少一份明文数据分别对应, 且所述授权信息为关于被允许使用相应的明文数据的至少一个程序的信息;

- 20 [234] 第二发送单元 1502, 配置为, 向所述数据管理方发送认证信息, 以使得所述第一可信执行环境对于每份所述授权信息基于所述认证信息和该份授权信息进行验证, 其中, 所述认证信息由所述第二可信执行环境生成;

[235] 针对每份所述授权信息的

- 25 [236] 第一接收单元 1503, 配置为, 在验证通过的情况中, 由所述第二可信执行环境接收从所述第一可信执行环境安全传输的与该份授权信息对应的第一密钥; 获取单元 1504, 配置为, 从所述数据管理方获取与该份授权信息对应的加密数据; 解密单元 1505, 配置为, 在所述第二可信执行环境中使用该第一密钥对该加密数据进行解密, 以获取相应的明文数据; 以及

[237] 计算单元 1506, 配置为, 在所述第二可信执行环境中通过所述第一程序基于所述

至少一份明文数据进行计算，以获取计算结果。

[238] 在一个实施例中，所述第一程序具有第一代码哈希值，其中，每份授权信息中包括第一代码哈希值、及与第一代码哈希值对应的第二密钥，所述第二密钥用于对所述第一程序的计算结果进行加密、由与该计算结果对应的计算结果使用方提供，所述装置还包括，

[239] 针对每份所述授权信息的

[240] 第二接收单元 1507，配置为，在验证通过的情况中，由所述第二可信执行环境接收从所述第一可信执行环境安全传输的与该份授权信息对应的第二密钥；

[241] 确定单元 1508，配置为，在获取所述计算结果之后，在所述第二可信执行环境中确定与各份所述授权信息分别对应的各个第二密钥是否一致，以及

[242] 加密单元 1509，配置为，在各个所述第二密钥一致的情况中，在所述第二可信执行环境中使用所述第二密钥对所述计算结果进行加密，以获取加密计算结果。

[243] 在一个实施例中，所述装置还包括第三发送单元 1510，配置为，在获取加密计算结果之后，将所述加密计算结果发送给所述计算结果使用方。

[244] 在一个实施例中，所述获取单元 1504 还配置为，从所述数据管理方读取与该份授权信息对应的加密数据。

[245] 图 16 示出根据本说明书实施例的一种数据处理装置 1600，所述装置在数据使用方实施，所述数据使用方包括第二可信执行环境，所述第二可信执行环境中运行有第一程序，所述装置包括：

[246] 第一发送单元 161，配置为，向数据管理方发送数据请求，用于请求使用数据管理方中存储的至少一份明文数据，其中，所述数据管理方包括第一可信执行环境，在所述第一可信执行环境中存储有所述至少一份明文数据和与所述至少一份明文数据分别对应的至少一份授权信息，其中，所述授权信息为关于被允许使用相应的明文数据的至少一个程序的信息；

[247] 第二发送单元 162，配置为，向所述数据管理方发送认证信息，以使得所述第一可信执行环境对于每份所述授权信息基于所述认证信息和该份授权信息进行验证，其中，所述认证信息由所述第二可信执行环境生成；

[248] 针对每份所述授权信息的第一接收单元 163，配置为，对于每份所述授权信息，在

验证通过的情况下，由所述第二可信执行环境接收从所述第一可信执行环境安全传输的与该份授权信息对应的明文数据；以及

[249] 计算单元 164，配置为，在所述第二可信执行环境中通过所述第一程序基于所述至少一份明文数据进行计算，以获取计算结果。

5 [250] 本说明书另一方面提供一种计算设备，包括存储器和处理器，其特征在于，所述存储器中存储有可执行代码，所述处理器执行所述可执行代码时，实现上述任一项方法。

[251] 在根据本说明书实施例的数据处理方案中，利用 TEE、RA 技术搭建了数据提供方可信的数据授权系统，通过技术层面而非第三方信赖来保证中间数据授权平台不会窥探、篡改数据提供方的数据，同时运行速度快，支持任何代码可表示的融合计算，更有效率、更加通用；为数据授权系统、数据提供方以及数据使用方提出了一整套协议流程，通过该流程可以保证数据的隐私性，多方数据的合规使用；在设计上达成了可以针对数据使用行为授权、可选择性地对数据融合的输出结果进行访问控制两个特性，以满足实际多方数据融合的通用入口、出口权限控制；数据授权系统作为中间层，为数据提供方和数据使用方解耦，数据提供方一次上传即可，数据使用方多次使用不需要数据提供方重复上传，在重复使用数据时可以有效提升数据访问效率；数据授权系统在设计上允许数据提供方事先离线上传好即可，数据提供方无需部署数据提供服务来实时配合融合业务传输数据，提升易用性。

10

15

[252] 本说明书中的各个实施例均采用递进的方式描述，各个实施例之间相同相似的部分互相参见即可，每个实施例重点说明的都是与其他实施例的不同之处。尤其，对于系统实施例而言，由于其基本相似于方法实施例，所以描述的比较简单，相关之处参见方法实施例的部分说明即可。

20

[253] 上述对本说明书特定实施例进行了描述。其它实施例在所附权利要求书的范围内。在一些情况下，在权利要求书中记载的动作或步骤可以按照不同于实施例中的顺序来执行并且仍然可以实现期望的结果。另外，在附图中描绘的过程不一定要求示出的特定顺序或者连续顺序才能实现期望的结果。在某些实施方式中，多任务处理和并行处理也是可以的或者可能是有利的。

25

[254] 本领域普通技术人员应该还可以进一步意识到，结合本文中所公开的实施例描述的各示例的单元及算法步骤，能够以电子硬件、计算机软件或者二者的结合来实现，为了清楚地说明硬件和软件的可互换性，在上述说明中已经按照功能一般性地描述了各示

例的组成及步骤。这些功能究竟以硬件还是软件方式来执轨道，取决于技术方案的特定应用和设计约束条件。本领域普通技术人员可以对每个特定的应用来使用不同方法来实现所描述的功能，但是这种实现不应认为超出本申请的范围。

5 [255] 结合本文中所公开的实施例描述的方法或算法的步骤可以用硬件、处理器执轨道的软件模块，或者二者的结合来实施。软件模块可以置于随机存储器（RAM）、内存、只读存储器（ROM）、电可编程 ROM、电可擦除可编程 ROM、寄存器、硬盘、可移动磁盘、CD-ROM、或技术领域内所公知的任意其它形式的存储介质中。

10 [256] 以上所述的具体实施方式，对本申请的目的、技术方案和有益效果进行了进一步详细说明，所应理解的是，以上所述仅为本申请的具体实施方式而已，并不用于限定本申请的保护范围，凡在本申请的精神和原则之内，所做的任何修改、等同替换、改进等，均应包含在本申请的保护范围之内。

权利要求书

1.一种数据处理方法,所述方法在数据提供方执行,所述数据提供方拥有第一明文数据,所述方法包括:

获取所述第一明文数据的第一加密数据、用于解密所述第一加密数据的第一密钥、

5 以及关于所述第一明文数据的授权信息;

向数据管理方发送验证请求,其中,所述数据管理方包括第一可信执行环境;

从所述数据管理方接收认证信息,并基于所述认证信息进行验证,其中,所述认证信息由所述第一可信执行环境生成;

10 在验证通过的情况中,将所述第一密钥和所述授权信息安全传输至所述第一可信执行环境;以及

将所述第一加密数据提供给所述数据管理方。

2.一种数据处理方法,所述方法在数据提供方执行,所述数据提供方拥有第一明文数据,所述方法包括:

获取关于所述第一明文数据的授权信息;

15 向数据管理方发送验证请求,其中,所述数据管理方包括第一可信执行环境;

从所述数据管理方接收认证信息,并基于所述认证信息进行验证,其中,所述认证信息由所述第一可信执行环境生成;以及

在验证通过的情况中,将所述第一明文数据和所述授权信息安全传输至所述第一可信执行环境。

20 3.根据权利要求1或2所述的方法,其中,所述授权信息包括至少一个代码哈希值,所述至少一个代码哈希值分别为被允许使用所述第一明文数据的至少一个程序各自的代码哈希值。

4.根据权利要求3所述的方法,其中,所述授权信息包括与所述至少一个代码哈希值分别对应的至少一个访问权限信息,所述访问权限信息为关于相应程序的计算结果的信息。

5.根据权利要求4所述的方法,其中,所述访问权限信息为第二密钥,所述第二密钥用于加密相应的计算结果、由与该计算结果对应的计算结果提供方提供。

6.根据权利要求4所述的方法,其中,所述访问权限信息为空信息。

7.根据权利要求1或2所述的方法,其中,基于所述认证信息进行验证包括,基于
30 所述认证信息验证:所述第一可信执行环境中是否安装有并正在执行用于数据使用授权的程序。

8.根据权利要求 1 或 2 所述的方法, 其中, 所述安全传输为加密传输。

9.一种数据处理方法, 所述方法在数据管理方执行, 所述数据管理方包括第一可信执行环境、并且存储有至少一份加密数据, 其中, 在所述第一可信执行环境中存储有至少一个第一密钥和与所述至少一个第一密钥分别对应的至少一份授权信息, 所述至少一个第一密钥用于分别解密所述至少一份加密数据以分别获取至少一份明文数据, 所述至少一份授权信息与所述至少一份明文数据分别对应, 且所述授权信息为关于被允许使用相应的明文数据的至少一个程序的信息, 所述方法包括:

接收数据使用方的数据请求, 所述数据请求用于请求使用所述至少一份明文数据, 其中, 所述数据使用方包括第二可信执行环境;

10 从所述数据使用方接收认证信息, 所述认证信息由所述第二可信执行环境生成;

在所述第一可信执行环境中, 对于每份所述授权信息, 基于所述认证信息和该份授权信息进行验证; 以及

对于每份所述授权信息, 在验证通过的情况中, 由第一可信执行环境将与该份授权信息对应的第一密钥安全传输给所述第二可信执行环境, 以及将相应的加密数据提供给所述数据使用方。

10.一种数据处理方法, 所述方法在数据管理方执行, 所述数据管理方包括第一可信执行环境, 其中, 在所述第一可信执行环境中存储有至少一份明文数据、以及与所述至少一份明文数据分别对应的至少一份授权信息, 其中, 所述授权信息为关于被允许使用相应的明文数据的至少一个程序的信息, 所述方法包括:

20 接收数据使用方的数据请求, 所述数据请求用于请求使用所述至少一份明文数据, 其中, 所述数据使用方包括第二可信执行环境;

从所述数据使用方接收认证信息, 其中, 所述认证信息由所述第二可信执行环境生成;

25 在所述第一可信执行环境中, 对于每份所述授权信息, 基于所述认证信息和该份授权信息进行验证; 以及

对于每份所述授权信息, 在验证通过的情况中, 由第一可信执行环境将与该份授权信息对应的明文数据安全传输给所述第二可信执行环境。

11.根据权利要求 9 或 10 所述的方法, 其中所述第一可信执行环境与所述第二可信执行环境位于一个平台、或不同的平台中。

30 12.根据权利要求 9 或 10 所述的方法, 其中, 从所述数据使用方接收认证信息包括, 由所述第一可信执行环境接收从所述第二可信执行环境安全传输的认证信息。

13.根据权利要求9所述的方法,其中,所述认证信息中包括所述第二可信执行环境中安装并正在运行的第一程序的第一代码哈希值,其中,所述每份授权信息包括所述至少一个程序各自的代码哈希值,其中,对于每份所述授权信息,基于所述认证信息和该份授权信息进行验证包括,对于每份授权信息,验证所述第一代码哈希值是否为该份授权信息中包括的一个代码哈希值。

14.根据权利要求13所述的方法,其中,每份所述授权信息中包括第一代哈希值、与和所述第一代哈希值对应的第二密钥,所述第二密钥用于对所述第一程序的计算结果进行加密、由与该计算结果对应的计算结果提供方提供,其中,所述方法还包括,对于每份所述授权信息,在验证通过的情况中,还由所述第一可信执行环境将所述第二密钥安全传输给所述第二可信执行环境。

15.根据权利要求9所述的方法,其中,所述数据管理方还包括数据存储模块,其中,所述至少一份加密数据被存储在所述数据存储模块中。

16.一种数据处理方法,所述方法在数据使用方执行,所述数据使用方包括第二可信执行环境,所述第二可信执行环境中运行有第一程序,所述方法包括:

15 向数据管理方发送数据请求,用于请求使用与数据管理方中存储的至少一份加密数据对应的至少一份明文数据,其中,所述数据管理方包括第一可信执行环境,在所述第一可信执行环境中存储有至少一个第一密钥和与所述至少一个第一密钥分别对应的至少一份授权信息,其中,所述至少一个第一密钥用于分别解密所述至少一份加密数据以分别获取所述至少一份明文数据,所述至少一份授权信息与所述至少一份明文数据分别对应,且所述授权信息为关于被允许使用相应的明文数据的至少一个程序的信息;

20 向所述数据管理方发送认证信息,以使得所述第一可信执行环境对于每份所述授权信息基于所述认证信息和该份授权信息进行验证,其中,所述认证信息由所述第二可信执行环境生成;

25 对于每份所述授权信息,在验证通过的情况中,由所述第二可信执行环境接收从所述第一可信执行环境安全传输的与该份授权信息对应的第一密钥;从所述数据管理方获取与该份授权信息对应的加密数据;在所述第二可信执行环境中使用该第一密钥对该加密数据进行解密,以获取相应的明文数据;以及

在所述第二可信执行环境中通过所述第一程序基于所述至少一份明文数据进行计算,以获取计算结果。

30 17.一种数据处理方法,所述方法在数据使用方执行,所述数据使用方包括第二可信执行环境,所述第二可信执行环境中运行有第一程序,所述方法包括:

向数据管理方发送数据请求,用于请求使用数据管理方中存储的至少一份明文数据,其中,所述数据管理方包括第一可信执行环境,在所述第一可信执行环境中存储有所述至少一份明文数据和与所述至少一份明文数据分别对应的至少一份授权信息,其中,所述授权信息为关于被允许使用相应的明文数据的至少一个程序的信息;

- 5 向所述数据管理方发送认证信息,以使得所述第一可信执行环境对于每份所述授权信息基于所述认证信息和该份授权信息进行验证,其中,所述认证信息由所述第二可信执行环境生成;

对于每份所述授权信息,在验证通过的情况中,由所述第二可信执行环境接收从所述第一可信执行环境安全传输的与该份授权信息对应的明文数据;以及

- 10 在所述第二可信执行环境中通过所述第一程序基于所述至少一份明文数据进行计算,以获取计算结果。

18.根据权利要求 16 或 17 所述的方法,其中,所述第一程序具有第一代码哈希值,其中,每份授权信息中包括第一代码哈希值、及与第一代码哈希值对应的第二密钥,所述第二密钥用于对所述第一程序的计算结果进行加密、由该计算结果对应的计算结果

- 15 使用方提供,所述方法还包括,

对于每份所述授权信息,在验证通过的情况中,由所述第二可信执行环境接收从所述第一可信执行环境安全传输的与该份授权信息对应的第二密钥;

在获取所述计算结果之后,在所述第二可信执行环境中确定与各份所述授权信息分别对应的各个第二密钥是否一致;以及

- 20 在各个所述第二密钥一致的情况中,在所述第二可信执行环境中使用所述第二密钥对所述计算结果进行加密,以获取加密计算结果。

19.根据权利要求 18 所述的方法,还包括,在获取加密计算结果之后,将所述加密计算结果发送给所述计算结果使用方。

- 20.根据权利要求 16 所述的方法,其中,从所述数据管理方获取与该份授权信息对应的加密数据包括,从所述数据管理方读取与该份授权信息对应的加密数据。

21.一种数据处理装置,所述装置在数据提供方实施,所述数据提供方拥有第一明文数据,所述装置包括:

获取单元,配置为,获取所述第一明文数据的第一加密数据、用于解密所述第一加密数据的第一密钥、以及关于所述第一明文数据的授权信息;

- 30 发送单元,配置为,向数据管理方发送验证请求,其中,所述数据管理方包括第一可信执行环境;

验证单元,配置为,从所述数据管理方接收认证信息,并基于所述认证信息进行验证,其中,所述认证信息由所述第一可信执行环境生成;

安全传输单元,配置为,在验证通过的情况中,将所述第一密钥和所述授权信息安全传输至所述第一可信执行环境;以及

5 提供单元,配置为,将所述第一加密数据提供给所述数据管理方。

22.一种数据处理装置,所述装置在数据提供方实施,所述数据提供方拥有第一明文数据,所述装置包括:

获取单元,配置为,获取关于所述第一明文数据的授权信息;

10 发送单元,配置为,向数据管理方发送验证请求,其中,所述数据管理方包括第一可信执行环境;

验证单元,配置为,从所述数据管理方接收认证信息,并基于所述认证信息进行验证,其中,所述认证信息由所述第一可信执行环境生成;以及

安全传输单元,配置为,在验证通过的情况中,将所述第一明文数据和所述授权信息安全传输至所述第一可信执行环境。

15 23.根据权利要求 21 或 22 所述的装置,其中,所述授权信息包括至少一个代码哈希值,所述至少一个代码哈希值分别为被允许使用所述第一明文数据的至少一个程序各自的代码哈希值。

20 24.根据权利要求 23 所述的装置,其中,所述授权信息包括与所述至少一个代码哈希值分别对应的至少一个访问权限信息,所述访问权限信息为关于相应程序的计算结果的信息。

25.根据权利要求 24 所述的装置,其中,所述访问权限信息为第二密钥,所述第二密钥用于加密相应的计算结果、由与该计算结果对应的计算结果使用方提供。

26.根据权利要求 24 所述的装置,其中,所述访问权限信息为空信息。

25 27.根据权利要求 21 或 22 所述的装置,其中,所述验证单元还配置为,基于所述认证信息验证:所述第一可信执行环境中是否安装有并正在执行用于数据使用授权的程序。

28.根据权利要求 21 或 22 所述的装置,其中,所述安全传输为加密传输。

30 29.一种数据处理装置,所述装置在数据管理方实施,所述数据管理方包括第一可信执行环境、并且存储有至少一份加密数据,其中,在所述第一可信执行环境中存储有至少一个第一密钥和与所述至少一个第一密钥分别对应的至少一份授权信息,其中,所述至少一个第一密钥用于分别解密所述至少一份加密数据以分别获取至少一份明文数据,所述至少一份授权信息与所述至少一份明文数据分别对应,且所述授权信息为关于被允

许使用相应的明文数据的至少一个程序的信息,所述装置包括:

第一接收单元,配置为,接收数据使用方的数据请求,所述数据请求用于请求使用所述至少一份明文数据,其中,所述数据使用方包括第二可信执行环境;

5 第二接收单元,配置为,从所述数据使用方接收认证信息,所述认证信息由所述第二可信执行环境生成;

验证单元,配置为,在所述第一可信执行环境中,对于每份所述授权信息,基于所述认证信息和该份授权信息进行验证;以及

10 针对每份授权信息的,第一安全传输单元,配置为,在验证通过的情况中,由第一可信执行环境将与该份授权信息对应的第一密钥安全传输给所述第二可信执行环境;以及提供单元,配置为,将相应的加密数据提供给所述数据使用方。

30.一种数据处理装置,所述装置在数据管理方实施,所述数据管理方包括第一可信执行环境,其中,在所述第一可信执行环境中存储有至少一份明文数据、以及与所述至少一份明文数据分别对应的至少一份授权信息,其中,所述授权信息为关于被允许使用相应的明文数据的至少一个程序的信息,所述装置包括:

15 第一接收单元,配置为,接收数据使用方的数据请求,所述数据请求用于请求使用所述至少一份明文数据,其中,所述数据使用方包括第二可信执行环境;

第二接收单元,配置为,从所述数据使用方接收认证信息,其中,所述认证信息由所述第二可信执行环境生成;

20 验证单元,配置为,在所述第一可信执行环境中,对于每份所述授权信息,基于所述认证信息和该份授权信息进行验证;以及

针对每份所述授权信息的安全传输单元,配置为,在验证通过的情况中,由第一可信执行环境将与该份授权信息对应的明文数据安全传输给所述第二可信执行环境。

31.根据权利要求 29 或 30 所述的装置,其中所述第一可信执行环境与所述第二可信执行环境位于一个平台、或不同的平台中。

25 32.根据权利要求 29 或 30 所述的装置,其中,所述验证单元还配置为,由所述第一可信执行环境接收从所述第二可信执行环境安全传输的认证信息。

33.根据权利要求 29 所述的装置,其中,所述认证信息中包括所述第二可信执行环境中安装并正在运行的第一程序的第一代码哈希值,其中,所述每份授权信息包括所述至少一个程序各自的代码哈希值,其中,所述验证单元还配置为,对于每份授权信息,30 验证所述第一代码哈希值是否为该份授权信息中包括的一个代码哈希值。

34.根据权利要求 33 所述的装置,其中,每份所述授权信息中包括第一代码哈希值、

和与所述第一代码哈希值对应的第二密钥,所述第二密钥用于对所述第一程序的计算结果进行加密、由与该计算结果对应的计算结果使用方提供,其中,所述装置还包括第二安全传输单元,配置为,对于每份所述授权信息,在验证通过的情况中,还由所述第一可信执行环境将所述第二密钥安全传输给所述第二可信执行环境。

- 5 35.根据权利要求 29 所述的装置,其中,所述数据管理方还包括数据存储模块,其中,所述多个加密数据被存储在所述数据存储模块中。

36.一种数据处理装置,所述装置在数据使用方实施,所述数据使用方包括第二可信执行环境,所述第二可信执行环境中运行有第一程序,所述装置包括:

- 10 第一发送单元,配置为,向数据管理方发送数据请求,用于请求使用与数据管理方中存储的至少一份加密数据对应的至少一份明文数据,其中,所述数据管理方包括第一可信执行环境,在所述第一可信执行环境中存储有至少一个第一密钥和与所述至少一个第一密钥分别对应的至少一份授权信息,其中,所述至少一个第一密钥用于分别解密所述至少一份加密数据以分别获取所述至少一份明文数据,所述至少一份授权信息与所述至少一份明文数据分别对应,且所述授权信息为关于被允许使用相应的明文数据的至少一个程序的信息;
- 15

第二发送单元,配置为,向所述数据管理方发送认证信息,以使得所述第一可信执行环境对于每份所述授权信息基于所述认证信息和该份授权信息进行验证,其中,所述认证信息由所述第二可信执行环境生成;

- 20 针对每份所述授权信息的,第一接收单元,配置为,在验证通过的情况中,由所述第二可信执行环境接收从所述第一可信执行环境安全传输的与该份授权信息对应的第一密钥;获取单元,配置为,从所述数据管理方获取与该份授权信息对应的加密数据;解密单元,配置为,在所述第二可信执行环境中使用该第一密钥对该加密数据进行解密,以获取相应的明文数据;以及

- 25 计算单元,配置为,在所述第二可信执行环境中通过所述第一程序基于所述至少一份明文数据进行计算,以获取计算结果。

37.一种数据处理装置,所述装置在数据使用方实施,所述数据使用方包括第二可信执行环境,所述第二可信执行环境中运行有第一程序,所述装置包括:

- 30 第一发送单元,配置为,向数据管理方发送数据请求,用于请求使用数据管理方中存储的至少一份明文数据,其中,所述数据管理方包括第一可信执行环境,在所述第一可信执行环境中存储有所述至少一份明文数据和与所述至少一份明文数据分别对应的至少一份授权信息,其中,所述授权信息为关于被允许使用相应的明文数据的至少一个

程序的信息;

第二发送单元,配置为,向所述数据管理方发送认证信息,以使得所述第一可信执行环境对于每份所述授权信息基于所述认证信息和该份授权信息进行验证,其中,所述认证信息由所述第二可信执行环境生成;

- 5 针对每份所述授权信息的第一接收单元,配置为,对于每份所述授权信息,在验证通过的情况中,由所述第二可信执行环境接收从所述第一可信执行环境安全传输的与该份授权信息对应的明文数据;以及

计算单元,配置为,在所述第二可信执行环境中通过所述第一程序基于所述至少一份明文数据进行计算,以获取计算结果。

- 10 38.根据权利要求 36 或 37 所述的装置,其中,所述第一程序具有第一代码哈希值,其中,每份授权信息中包括第一代码哈希值、及与第一代码哈希值对应的第二密钥,所述第二密钥用于对所述第一程序的计算结果进行加密、由与该计算结果对应的计算结果使用方提供,所述装置还包括,

- 15 针对每份所述授权信息的第二接收单元,配置为,在验证通过的情况中,由所述第二可信执行环境接收从所述第一可信执行环境安全传输的与该份授权信息对应的第二密钥;

确定单元,配置为,在获取所述计算结果之后,在所述第二可信执行环境中确定与各份所述授权信息分别对应的各个第二密钥是否一致,以及

- 20 加密单元,配置为,在各个所述第二密钥一致的情况中,在所述第二可信执行环境中使用所述第二密钥对所述计算结果进行加密,以获取加密计算结果。

39.根据权利要求 38 所述的装置,还包括第三发送单元,配置为,在获取加密计算结果之后,将所述加密计算结果发送给所述计算结果使用方。

40.根据权利要求 36 所述的装置,其中,所述获取单元还配置为,从所述数据管理方读取与该份授权信息对应的加密数据。

- 25 41.一种计算设备,包括存储器和处理器,其特征在于,所述存储器中存储有可执行代码,所述处理器执行所述可执行代码时,实现权利要求 1-20 中任一项所述的方法。