

股权激励系统中的数据处理的方法和装置

技术领域

本申请实施例涉及软件技术领域，并且更具体地，涉及一种股权激励系统
5 中的数据处理的装置和方法。

背景技术

员工持股计划（Employee Stock Ownership Plan，ESOP）（又可以称为
10 员工持股制度）是员工所有权的一种实现形式，是企业所有者与员工分享企业所有权和未来收益权的一种制度安排。由于长期激励系统中存储的都是公司授予员工长期激励的信息，属于非常机密的级别，不允许任何不相关的人员可以查询到，包括开发和运维人员。

传统方案中，通过一种对称加密的方式对数据进行加密。但是，在发生
15 数据泄露时，通常密钥和密文可能会一起泄露，或者密钥在传输过程中也可能被截获。

因此，如何对敏感信息进行数据处理，以保证数据的安全性亟待解决。

发明内容

本申请实施例提供了一种股权激励系统中的数据处理的方法和装置，能
20 够提高了数据的安全性。

第一方面，提供了一种股权激励系统中的数据处理的方法，该方法包括：
获取映射关系，所述映射关系包括至少一种数据类型和至少一种加密方式的
对应关系；根据所述映射关系，确定第一数据的第一数据类型对应的第一加
密方式；根据所述第一加密方式，对所述第一数据进行加密得到第一密文；
25 根据所述第一密文和所述第一加密方式，生成第一数据包；向所述股权激励系统中的第二设备发送所述第一数据包。

第一设备获取包括至少一种数据类型和至少一种加密方式的对应关系的
映射关系，并根据该映射关系确定第一数据的数据类型对应的第一加密方
式，再根据该第一加密方式生成第一数据包，最后将该第一数据包发送给第
30 二设备。这样第一设备根据不同的数据类型使用不同给的加密方式，使得第二设备根据加密标识进行解密得到第一数据。也就是说，本申请实施例通过对不同的数据类型进行了不同的加密方式，从而在不影响正常使用的前提下，提高了数据的安全性。

在一种可能的实现方式中，所述第一加密方式为随机填充加密方式、非随机加密方式或长文本加密方式。

在一种可能的实现方式中，在所述第一加密方式为长文本加密方式的情况下，所述根据所述第一加密方式，对所述第一数据进行加密得到第一密文
5 包括：通过第一密钥对所述第一数据进行加密得到所述第一密文，所述第一密钥为所述第一数据对应的密钥；对所述第一密钥进行加密得到第二密文；其中，所述根据所述第一密文和所述第一加密方式，生成第一数据包包括：根据所述第一密文、所述第一加密方式和所述第二密文，生成所述第一数据包。

10 在一种可能的实现方式中，在所述第一加密方式为随机填充加密方式的情况下，所述根据所述第一加密方式，对所述第一数据进行加密得到第一密文包括：通过第一密钥对所述第一数据进行加密得到所述第一密文，所述第一密钥为随机密钥；其中，所述根据所述第一密文和所述第一加密方式，生成第一数据包包括：根据所述第一密文和所述第一加密方式，生成所述第一
15 数据包。

在一种可能的实现方式中，在所述第一加密方式为非随机填充加密方式的情况下，所述根据所述第一加密方式，对所述第一数据进行加密得到第一密文包括：通过第一密钥对所述第一数据进行加密得到所述第一密文，所述
20 第一密钥为固定密钥；其中，所述根据所述第一密文和所述第一加密方式，生成第一数据包包括：根据所述第一密文和所述第一加密方式，生成所述第一数据包。

在一种可能的实现方式中，所述对所述第一密钥进行加密得到第二密文包括：通过第二密钥对所述第一密钥进行加密得到所述第二密文，其中，所述
25 第二密钥为所述第一设备和所述第二设备约定的密钥。

在一种可能的实现方式中，所述对所述第一密钥进行加密得到第二密文包括：通过第二密钥对所述第一密钥进行加密得到所述第二密文，所述第二
30 密钥为所述第二设备中私钥对应的公钥。

在一种可能的实现方式中，在所述第一设备向所述第二设备发送所述第一数据包之前，还包括：所述第一设备拼接所述第一密文和所述第二密文得
30 到所述第一数据包。

在一种可能的实现方式中，所述根据所述第一密文和所述第一加密方

式，生成第一数据包包括：

将所述第一加密方式对应的加密标识作为前缀生成所述第一数据包

第二方面，提供了一种股权激励系统中的数据处理的方法，应用于所述股权激励系统中的第二设备，其特征在于，包括：接收来自所述股权激励系统中的第一设备发送的第一数据包，所述第一数据包包括第一密文和前缀；
5 根据所述前缀对应的加密方式，对所述第一密文进行解密得到第一数据，所述加密方式为随机填充加密方式、非随机加密方式或长文本加密方式；对所述第一数据，进行数据处理。

第二设备接收来自第一设备的第一数据包，并根据该第一数据包的前缀
10 确定加密方式，进而采用对应的解密方式进行解密。也就是说，本申请实施例通过对不同的数据类型进行了不同的加密方式，从而在不影响正常使用的前提下，提高了数据的安全性。

第三方面，提供了一种终端设备，包括处理器和存储器。该存储器用于存储计算机程序，该处理器用于调用并运行该存储器中存储的计算机程序，
15 执行上述第一方面或第二方面中任一方面中的方法。

第四方面，提供了一种计算机可读存储介质，用于存储计算机程序，该计算机程序使得计算机执行上述第一方面至第二方面中的任一方面中的方法。

第五方面，提供了一种计算机程序产品，包括计算机程序指令，所述计算机程序指令使得计算机执行上述第一方面至第二方面中的任一方面中的方法。
20

第六方面，提供了一种计算机程序，当其在计算机上运行时，使得计算机执行上述第一方面至第二方面中的任一方面中的方法。

第七方面，提供了一种通信系统，该通信系统包括用于执行上述第一方面中的任一方面的装置和用于执行上述第二方面中的任一方面的装置。
25

通过上述技术方案，第一设备通过对第一密钥对第一数据进行加密得到第一密文，以及对该第一密钥进行加密得到第二密文，并将包括该第一密文和该第二密文的第一数据包发送给第二设备，使得第二设备解密第二密文得到第一密钥后才能根据第一密钥对第一密文进行解密得到该第一数据。这样
30 保证了第一数据不会在开发、运维人员对数据库访问时查询到，从而提高了数据的安全性。

附图说明

- 图 1 是本申请实施例应用的一种加密流程的示意性图。
- 图 2 是本申请实施例提供的业务层与加解密服务通信的加密示意图。
- 图 3 是本申请实施例提供的一种基于数据包加密的示意图。
- 5 图 4 是本申请实施例提供的一种数据处理的方法的示意性流程图。
- 图 5 是本申请实施例提供的一种具体数据处理的方法的示意性流程图。
- 图 6 是根据本申请实施例提供的一种数据处理的装置的示意性框图。
- 图 7 是根据本申请实施例提供的一种数据处理的装置的示意性结构图。
- 图 8 是根据本申请实施例提供的另一种数据处理的装置的示意性框图。
- 10 图 9 是根据本申请实施例提供的另一种数据处理的装置的示意性结构图。

具体实施方式

- 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描述，显然，所描述的实施例是本申请一部分实施例，而不是全部的实施例。针对本申请中的实施例，本领域普通技术人员在没有做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。
- 15

- 图 1 示出了加密流程的示意图。数据加密发生在数据插入数据库（data base，DB）之前，加密后将密文存储在数据库中；解密数据发生在读取 DB 之后，将数据从 DB 取出后进行解密。
- 20

应理解，在下文示出的实施例中，第一、第二以及各种数字编号仅为描述方便进行的区分，并不用来限制本申请实施例的范围。

- 图 2 示出了业务层与加解密服务通信的加密示意图。业务层与加解密服务将对称密钥通过非对称加密的结果分发对称密钥，实现信息完整性验证。数据包包含被加密的内容和被加密的用于加密该内容的密钥。使用接收方的公钥来加密加密密钥，但这并不是必须的，也可以使用发送方和接收方预共享的对称密钥来加密。当接收方收到数据包时，先用私钥或预共享密钥解密，得到加密密钥，再用该密钥解密密文，获得原文。本实施例通过将加密数据的数据密钥封入数据包中存储、传递和使用，不再使用主密钥直接加解密数据。每条数据都存在进行数据加密的密钥，称之为 data_key，data_key 统一经过密钥管理的密钥进行加密，随着数据保存在 DB、缓存或者文件中。
- 25
- 30

例如，图 3 示出了一种基于数据包加密的示意图。

具体地，加密流程可以是 ESOP 端将明文字段发送给 KMS 端，KMS 端生成密钥，并根据该密钥对明文字段进行加密得到密文字段，以及对该密钥进行加密得到加密密钥，最后将加密密钥和密文字段一起发送给 ESOP 服务端；或者，加密流程还可以是 ESOP 端将用于加密明文字段的密钥发送给 KMS 端，KMS 端根据该密钥对明文字段进行加密得到密文字段，以及对该密钥进行加密得到加密密钥，最后将加密密钥和密文字段一起发送给 ESOP 服务端。

具体地，解密流程可以是 ESOP 服务端将加密密钥和密文字段一起发送给 KMS 端，KMS 端对加密密钥进行解密得到解密后的密钥，并根据解密后的密钥对密文字段进行解密得到明文字段，最后将明文字段发送给 ESOP。

图 4 示出了本申请实施例股权激励系统中的数据处理的方法的示意性流程图。

可以理解的是，本申请实施例的执行主体可以是第一设备，该第一设备可以是股权激励系统中的第一设备可以是业务方（ESOP_service），即 ESOP 业务方的服务器设备。

401，获取映射关系，该映射关系包括至少一种数据类型和至少一种加密方式的对应关系。

本实施例中的数据类型和至少一种加密方式之间的映射关系如表 1 所示。本实施例中的加密方式包括但不限于随机填充加密、非随机填充加密、长文本加密和不加密。具体地，按照安全性能由强到弱的排序为：随机填充加密>非随机填充加密>长文本机密>不加密。其中，随机填充加密具有无法支持密文查询和大于 4k 的长文本加密耗时较长的缺点。因此，非随机填充加密和长文本加密比较常用。

表 1

加密方式	前缀	说明	适用数据类型
随机填充加密	FUTUS001	每次明文 A 对应随机的密文 B	不涉及查询的字段
非随机填充加密	FUTUS002	每次明文 A 对应固定的密文 B	索引/查询相关的字段
长文本加密	FUTUS\$TyThg4Kn MMKH5G1n\$	通过加密密钥的方式进行本地 AES 加密操作	长度大于预设阈值的文本或文件
不加密	无	明文	非敏感数据

如表 1 所示，本实施例中的数据类型中，不涉及查询的字段包括：备注信息，通讯地址等等管理人员不会进行检索的信息；查询相关字段包括：用

户姓名、证件号、电话号码等管理人员需要通过这些信息查询到数据；长度大于预设阈值的文本或文件包括：数据报表等各类 excel 文件，电子合同 pdf 文件；非敏感数据包括：各类配置项等。

在本申请一实施例中，前缀用于标识密文是用哪种方式加密的，就是数据加密完后，需要给他贴个标签，标明是用哪种方式加密的，这样解密时就知道用哪种方式解密。比如明文 ABC，如果用填充加密方式进行加密，那么就需要发送给加密机两个信息一个是加密类型：填充加密，还有一个是明文：ABC。然后加密机加密后就会返回密文 XXYYZZ，这时候就需要进行存储到数据库里，填充加密对应的标识密文为 FUTU\$001，就会存为 FUTU\$001XXYYZZ。如果改为使用非填充加密，那么加密机返回的密文就是 SSDDFF。这时候存数据库就会存为 FUTU\$002SSDDFF。然后解密的时候，需要根据这个前缀告诉加密机用哪些方式解密。如果只传给对方密文 XXYYZZ，并通知对方解密方式为填充解密，那么就能解密成功。如果只传给对方密文 XXYYZZ，并通知对方解密方式是非填充解密，那么就会解密失败。

可选地，本申请实施例中的加密方式可以是前述表 1 中的四种加密方式中的任一种。

可选地，本申请实施例中的数据类型可以是表 1 中四种加密方式分别对应的数据类型。

可以理解的是，步骤 401 可以是第一设备自己生成的，也可以是用户设定的，还可以其他设备发送的指令指定的，本申请对此不进行限定。

还可以理解的是，对于表 1 中的不加密方式，相互双方可以直接明文交互，不需要进行加密。为方便描述，下述实施例中，以表 1 中除不加密数据之外的其他类型进行描述，但本申请并不限于此。

402，根据该映射关系，确定第一数据的第一数据类型对应的第一加密方式。

具体地，该第一设备在获取到第一数据的情况下，可以根据该映射关系，确定该第一数据的数据类型对应的第一加密方式。

在本申请一实施例中，在获取到第一数据之后，首先确定第一数据对应的数据类型，再基于数据类型从映射关系中确定其对应的加密方式。具体的，本实施例中确定数据类型的过程可以包括如下步骤：

确定所述第一数据对应的文本长度，并基于所述文本长度与预设阈值之间的对比结果，确定所述第一数据是否为一类数据，所述一类数据包括长度大于预设阈值的文本或文件；

5 基于第一目标字符类型，将所述第一目标字符类型与所述第一数据中的字符进行匹配，根据匹配结果判断所述第一数据中是否包含目标字段，若是，则所述第一数据为二类数据，所述第一目标字符类型包括姓名或者号码，所述二类数据包括索引或查询相关的字段。

403，根据该第一加密方式，对该第一数据进行加密得到第一密文。

10 在一种可能的实现方式中，若第一加密方式为长文本加密方式的情况下，步骤 403 具体可以是第一设备通过第一密钥对第一数据进行加密得到第一密文，该第一密钥为第一数据对应的密钥。此外，该第一设备还对该第一密钥进行加密得到第二密文。

15 具体地，针对不同用户的敏感信息，第一设备采用不同的密钥。或者针对不同的公司采用不同的密钥。也就是说，不同公司间采用不同的密钥，不同用户采用不同的密钥，使用这种方式来达到隔离的效果，保证公司只能拿到加解密自己的数据，用户也不能解密他人的数据。

可以理解的是，该第一数据可以是用户的敏感数据。例如，该敏感信息为员工的持股激励信息（即员工的期权与股票信息）。

20 可选地，第一设备对第一密钥进行加密具体可以是该第一设备通过第二密钥对该第一密钥进行加密得到该第二密文。

可选地，该第二密钥为该第一设备和第二设备预先约定的密钥。

具体地，第一设备在和第二设备进行数据处理之前，预先约定相同的密钥。这样第一设备可以通过和第二设备约定的密钥对第一密钥进行加密。也就是说，第一设备通过约定密钥加密之后，第二设备通过约定密钥才能解密。

25 可以理解的，本申请中的第二设备可以是服务端（KMS_service）。

可选地，该第一设备通过第二密钥对该第一密钥进行加密得到第二密钥，该第二密钥为该第二设备中私钥对应的公钥。

30 具体地，第一设备和第二设备之间可以设置一对公钥和私钥。其中，公钥和私钥是通过一种算法得到的一个密钥对（即一个私钥和一个公钥）。向外界公开的称为“公钥”，自己保留的称为“私钥”。通过这种算法得到的密钥对能保证在世界范围内是唯一的。也就是说，第一设备通过公钥对第一

秘钥加密后，只有通过私钥才能解密。

在另一种可能的实现方式中，若该第一加密方式为随机填充加密方式的情况下，步骤 403 具体可以是第一设备通过第一秘钥对第一数据进行加密得到第一密文，该第一秘钥为随机秘钥。

- 5 在又一种可能的实现方式中，若该第一加密方式为非随机填充加密方式的情况下，步骤 403 具体可以是第一设备通过第一秘钥对第一数据进行加密得到第一密文，该第一密文为固定秘钥。

404，根据该第一密文和第一加密方式，生成第一数据包。

- 10 可选地，步骤 404 具体可以是该第一设备将第一加密方式对应的加密标识作为前缀生成该第一数据包。

例如，如前述，若第一加密方式为填充加密，填充加密对应的加密标识为 FUTU\$001，则对于第一密文 XXYYZZ 和填充加密方式生成的第一数据包为 FUTU\$001XXYYZZ；若第一加密方式为非填充方式，非填充加密对应的加密标识为 FUTU\$002，则对于第一密文 SSDDFF 和非填充加密方式生成的第一数据包为 FUTU\$002SSDDFF。

可以理解的是，该加密标识还可以是其他方式，本申请对此不进行限定。

需要说明的是，若该第一加密方式为长文本加密方式，长文本加密方式对应的加密方式为 FUTU\$TyThg4KnMMKH5G1n\$，则需要根据第一密文、第二密文和该加密标识共同生成第一数据包。

- 20 在一种可能的实现方式中，密文和加密标识可以通过拼接的方式生成数据包。

具体地，加密标识和第一密文可以是以加密标识在前，第一密文在后的方式进行拼接的。或者对于加密标识、第一密文和第二密文生成第一数据包的方式可以是加密标识在前，第二密文在后，第一密文在最后的的方式进行拼接。例如，如图 3 所示，data_key 在前，密文字段在后。

可以理解的是，第一数据包还可以是通过其他拼接方式生成，例如，嵌套，组合等。

- 30 示例性的，在将密文和加密标识嵌套的过程中，为了保证密文和加密标识的安全性，本实施例中可以基于第一数据和密文的数据属性计算对应的嵌入位置，之后基于该嵌入位置，将加密标识嵌入到密文中对应的位置处，例如，计算到对应的嵌入位置为 n，则以密文的第一个字符开始，将加密标识

增加到 n 位置处，并将密文中的 n 位置及其之后的字符往后推。具体的，本实施例中可以通过如下公式确定嵌入位置：

$$n = \text{size_cip} \bmod (\log 2 \text{size_cip})$$

其中， size_cip 表示密文的数据量， $\bmod$ 表示取余运算， n 表示加密标识在密文中对应的嵌入位置。通过上述计算方式确定嵌入位置，以基于该嵌入位置将加密标识插入到密文中。进一步的，在对加密之后的数据进行解密时，可以基于同样的方式计算得到嵌入位置，之后提取加密密文，对加密密文进行解密之后再基于密钥对密文进行解密。通过上述方式提高了加密方式的安全性，进而提高了第一数据的安全性。

405，该第一设备向第二设备发送第一数据包。相应的，第二设备接收来自该第一设备的第一数据包，该第一数据包包括第一密文和前缀。

406，该第二设备根据该前缀对应的加密方式，对所述第一密文进行解密得到第一数据。

可选地，若该加密方式为长文本加密方式，则该第二设备通过第三密钥对该第二密文进行解密得到该第一密钥，该第二设备根据该第一密钥对该第一密钥进行解密得到第一数据。

可选地，该第三密钥为该第二密钥对应的密钥。

在一种可能的实现方式中，该第三密钥为该第一设备和该第二设备预先约定的密钥。

在另一种可能的实现方式中，该第三密钥为上述公钥对应的私钥。

407，该第二设备对该第一数据进行数据处理。

具体地，第二设备对第一数据进行数据处理可以是按照第一数据指示进行相应操作，也可以是将第一数据转发给其他设备，本申请对此不进行限定。

可选地，步骤 407 之后，该第二设备可以将对第一数据处理后得到的第二数据加密后发送给该第一设备。

本申请实施例中，第一设备获取包括至少一种数据类型和至少一种加密方式的对应关系的映射关系，并根据该映射关系确定第一数据的数据类型对应的第一加密方式，再根据该第一加密方式生成第一数据包，最后将该第一数据包发送给第二设备。这样第一设备根据不同的数据类型使用不同给的加密方式，使得第二设备根据加密标识进行解密得到第一数据。也就是说，本申请实施例通过对不同的数据类型进行了不同的加密方式，从而在不影响正

常使用的前提下，提高了数据的安全性。

图 5 示出了本申请实施例的一种具体的数据处理的方法的示意性流程图。

可以理解的是，下述以第一设备为 ESOP_service，第二设备为 KMS_servic
5 为例进行说明，但本申请并不限于此。

在加密方式为长文本加密方式的情况下，ESOP_service 与 KMS_servic 预先约定通过 RSA 算法配对的公钥 PUB 和私钥 PRI。KMS_servic 将私钥发送给 ESOP_service，而将私钥自己保留且不对外暴露。

501，ESOP_service 生成 256bit 长度的随机字符串，该随机字符串用于
10 作为高级加密标准（Advanced Encryption Standard，AES）加密的密钥 K1；
502，ESOP_service 构建需要加密的数据，具体结构为 json 字符串 PLAIN；
503，ESOP_service 通过密钥 K1 对 PLAIN 进行加密得到密文 CIPHER；
504，ESOP_service 通过密钥 PUB 对密钥 K1 进行加密得到密文 K2；
可以理解的是，本申请对步骤 503 和步骤 504 的先后顺序不进行限定。
15 505，ESOP_service 将 CIPHER 和 K2 进行拼接，并发送给 KMS_servic；
506，KMS_servic 获取拼接后的 CIPHER 和 K2；
507，KMS_servic 通过 PUB 对应的 PRI 对密文 K2 进行解密得到 K1；
508，KMS_servic 通过 K1 对 CIPHER 进行解密得到 PLAIN；
509，KMS_servic 对 PLAIN 进行数据处理得到 PLAIN2；
20 510，KMS_servic 通过 K1 对 PLAIN2 进行加密得到 CIPHER2，并将 CIPHER2 反馈给 ESOP_service；

可以理解的是，KMS_servic 也可以继续对 K1 进行加密。例如，采用与 ESOP_service 约定的密钥对 K1 进行加密。

511，ESOP_service 使用 K1 对 CIPHER2 进行解密得到 PLAIN2。

25 可以理解的是，若 KMS_servic 对 K1 进行加密，则 ESOP_service 可以先解密 K1，再根据 K1 对 PLAIN2 进行加密。

以上结合附图详细描述了本申请的具体实施方式，但是，本申请并不限于上述实施方式中的具体细节，在本申请的技术构思范围内，可以对本申请的技术方案进行多种简单变型，这些简单变型均属于本申请的保护范围。例如，在上述具体实施方式中所描述的各个具体技术特征，在不矛盾的情况下，
30 可以通过任何合适的方式进行组合，为了避免不必要的重复，本申请对各种

可能的组合方式不再另行说明。又例如，本申请的各种不同的实施方式之间也可以进行任意组合，只要其不违背本申请的思想，其同样应当视为本申请所公开的内容。

还应理解，在本申请的各种方法实施例中，上述各过程的序号的大小并不意味着执行顺序的先后，各过程的执行顺序应以其功能和内在逻辑确定，而不对本申请实施例的实施过程构成任何限定。应理解这些序号在适当情况下可以互换，以便描述的本申请的实施例能够以除了图示或描述的那些以外的顺序实施。

上文结合图 1 至图 5，详细描述了本申请的方法实施例，下文结合图 6 至图 9，详细描述本申请的装置实施例。

图 6 是本申请实施例的数据处理的装置 600 的示意性框图。如图 6 所示，所述数据处理的装置 600 可包括处理单元 610 和收发单元 620。

该处理单元 610，用于获取映射关系，所述映射关系包括至少一种数据类型和至少一种加密方式的对应关系；

该处理单元 610，还用于根据所述映射关系，确定第一数据的第一数据类型对应的第一加密方式；

该处理单元 610，还用于根据所述第一加密方式，对所述第一数据进行加密得到第一密文；

该处理单元 610，还用于根据所述第一密文和所述第一加密方式，生成第一数据包；

该收发单元 620，用于向所述股权激励系统中的第二设备发送所述第一数据包。

可选地，所述第一加密方式为随机填充加密方式、非随机加密方式或长文本加密方式。

可选地，在所述第一加密方式为长文本加密方式的情况下，该处理单元 620 具体用于：

通过第一密钥对所述第一数据进行加密得到所述第一密文，所述第一密钥为所述第一数据对应的密钥；

对所述第一密钥进行加密得到第二密文；

根据所述第一密文、所述第一加密方式和所述第二密文，生成所述第一数据包。

可选地，在所述第一加密方式为随机填充加密方式的情况下，该处理单元 620 具体用于：

通过第一密钥对所述第一数据进行加密得到所述第一密文，所述第一密钥为随机密钥；

5 根据所述第一密文和所述第一加密方式，生成所述第一数据包。

可选地，在所述第一加密方式为非随机填充加密方式的情况下，该处理单元 620 具体用于：

通过第一密钥对所述第一数据进行加密得到所述第一密文，所述第一密钥为固定密钥；

10 根据所述第一密文和所述第一加密方式，生成所述第一数据包。

可选地，该处理单元 620 具体用于：通过第二密钥对所述第一密钥进行加密得到所述第二密文，其中，所述第二密钥为所述第一设备和所述第二设备约定的密钥。

15 可选地，该处理单元 620 具体用于：通过第二密钥对所述第一密钥进行加密得到所述第二密文，所述第二密钥为所述第二设备中私钥对应的公钥。

可选地，该处理单元 620，还用于拼接所述第一密文和所述第二密文得到所述第一数据包。

可选地，该处理单元 620，还用于将所述第一加密方式对应的加密标识作为前缀生成所述第一数据包。

20 应理解，装置实施例与方法实施例可以相互对应，类似的描述可以参照方法实施例。为避免重复，此处不再赘述。具体地，在该实施例中数据处理的装置 600 可以对应于执行本申请实施例的方法 400 的相应主体，并且数据处理的装置 600 中的各个模块的前述和其它操作和/或功能分别为了实现图 4 中的各个方法，或图 4 中的方法中的相应流程，为了简洁，在此不再赘述。

25 上文中结合附图从功能模块的角度描述了本申请实施例的装置和系统。应理解，该功能模块可以通过硬件形式实现，也可以通过软件形式的指令实现，还可以通过硬件和软件模块组合实现。具体地，本申请实施例中的方法实施例的各步骤可以通过处理器中的硬件的集成逻辑电路和/或软件形式的指令完成，结合本申请实施例公开的方法的步骤可以直接体现为硬件译码处理器执行完成，或者用译码处理器中的硬件及软件模块组合执行完成。可选地，软件模块可以位于随机存储器，闪存、只读存储器、可编程只读存储器、

30

电可擦写可编程存储器、寄存器等本领域的成熟的存储介质中。该存储介质位于存储器，处理器读取存储器中的信息，结合其硬件完成上述方法实施例中的步骤。

如图 7 是本申请实施例提供的数据处理的装置 700 的示意性框图。

5 如图 7 所示，该数据处理的装置 700 可包括：

存储器 710 和处理器 720，该存储器 710 用于存储计算机程序，并将该程序代码传输给该处理器 720。换言之，该处理器 720 可以从存储器 710 中调用并运行计算机程序，以实现本申请实施例中的通信方法。

例如，该处理器 720 可用于根据该计算机程序中的指令执行上述方法
10 400 中的步骤，或方法 500 中的步骤。

在本申请的一些实施例中，该处理器 720 可以包括但不限于：

通用处理器、数字信号处理器（Digital Signal Processor，DSP）、专用
集成电路（Application Specific Integrated Circuit，ASIC）、现场可编程门阵
列（Field Programmable Gate Array，FPGA）或者其他可编程逻辑器件、分
15 立门或者晶体管逻辑器件、分立硬件组件等等。

在本申请的一些实施例中，该存储器 710 包括但不限于：

易失性存储器和/或非易失性存储器。其中，非易失性存储器可以是只读
存储器（Read-Only Memory，ROM）、可编程只读存储器（Programmable ROM，
PROM）、可擦除可编程只读存储器（Erasable PROM，EPROM）、电可擦
20 除可编程只读存储器（Electrically EPROM，EEPROM）或闪存。易失性存
储器可以是随机存取存储器（Random Access Memory，RAM），其用作外
部高速缓存。通过示例性但不是限制性说明，许多形式的 RAM 可用，例如
静态随机存取存储器（Static RAM，SRAM）、动态随机存取存储器（Dynamic
RAM，DRAM）、同步动态随机存取存储器（Synchronous DRAM，SDRAM）、
25 双倍数据速率同步动态随机存取存储器（Double Data Rate SDRAM，DDR
SDRAM）、增强型同步动态随机存取存储器（Enhanced SDRAM，ESDRAM）、
同步连接动态随机存取存储器（synch link DRAM，SLDRAM）和直接内存
总线随机存取存储器（Direct Rambus RAM，DR RAM）。

在本申请的一些实施例中，该计算机程序可以被分割成一个或多个模
30 块，该一个或者多个模块被存储在该存储器 710 中，并由该处理器 720 执行，
以完成本申请提供的编码方法。该一个或多个模块可以是能够完成特定功能

的一系列计算机程序指令段，该指令段用于描述该计算机程序在该数据处理的装置 900 中的执行过程。

可选的，如图 7 所示，该数据处理的装置 700 还可包括：

收发器 730，该收发器 730 可连接至该处理器 720 或存储器 710。

5 其中，处理器 720 可以控制该收发器 730 与其他设备进行通信，具体地，可以向其他设备发送信息或数据，或接收其他设备发送的信息或数据。收发器 730 可以包括发射机和接收机。收发器 730 还可以进一步包括天线，天线的数量可以为一个或多个。

应当理解，该数据处理的装置 700 中的各个组件通过总线系统相连，其中，总线系统除包括数据总线之外，还包括电源总线、控制总线和状态信号总线。

图 8 是本申请实施例的数据处理的装置 800 的示意性框图。如图 8 所示，所述数据处理的装置 800 可包括处理单元 810 和收发单元 820。

该收发单元 820，用于接收来自所述股权激励系统中的第一设备发送的第一数据包，所述第一数据包包括第一密文和前缀；

该处理单元 810，用于根据所述前缀对应的加密方式，对所述第一密文进行解密得到第一数据，所述加密方式为随机填充加密方式、非随机加密方式或长文本加密方式；

该处理单元 810，还用于对所述第一数据，进行数据处理。

20 可选的，该处理单元 810 还通过第三密钥对第二密文进行解密得到所述第一密钥，其中，所述第三密钥为所述第二设备与所述第一设备约定的密钥。

可选的，该处理单元 810 还用于通过第三密钥对第二密文进行解密得到所述第一密钥，其中，所述第三密钥为与所述第一设备中公钥对应的私钥。

可选的，所述第一数据包为对所述第一密文和第二密文拼接得到的。

25 应理解，装置实施例与方法实施例可以相互对应，类似的描述可以参照方法实施例。为避免重复，此处不再赘述。具体地，在该实施例中数据处理的装置 800 可以对应于执行本申请实施例的方法 400 的相应主体，并且数据处理的装置 800 中的各个模块的前述和其它操作和/或功能分别为了实现图 4 中的各个方法，或图 4 中的方法中的相应流程，为了简洁，在此不再赘述。

30 上文中结合附图从功能模块的角度描述了本申请实施例的装置和系统。应理解，该功能模块可以通过硬件形式实现，也可以通过软件形式的指令实

现，还可以通过硬件和软件模块组合实现。具体地，本申请实施例中的方法实施例的各步骤可以通过处理器中的硬件的集成逻辑电路和/或软件形式的指令完成，结合本申请实施例公开的方法的步骤可以直接体现为硬件译码处理器执行完成，或者用译码处理器中的硬件及软件模块组合执行完成。可选地，软件模块可以位于随机存储器，闪存、只读存储器、可编程只读存储器、电可擦写可编程存储器、寄存器等本领域的成熟的存储介质中。该存储介质位于存储器，处理器读取存储器中的信息，结合其硬件完成上述方法实施例中的步骤。

如图 9 是本申请实施例提供的数据处理的装置 900 的示意性框图。

如图 9 所示，该数据处理的装置 900 可包括：

存储器 910 和处理器 920，该存储器 910 用于存储计算机程序，并将该程序代码传输给该处理器 920。换言之，该处理器 920 可以从存储器 910 中调用并运行计算机程序，以实现本申请实施例中的通信方法。

例如，该处理器 920 可用于根据该计算机程序中的指令执行上述方法 400 中的步骤，或方法 500 中的步骤。

在本申请的一些实施例中，该处理器 920 可以包括但不限于：

通用处理器、数字信号处理器（Digital Signal Processor，DSP）、专用集成电路（Application Specific Integrated Circuit，ASIC）、现场可编程门阵列（Field Programmable Gate Array，FPGA）或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件等等。

在本申请的一些实施例中，该存储器 910 包括但不限于：

易失性存储器和/或非易失性存储器。其中，非易失性存储器可以是只读存储器（Read-Only Memory，ROM）、可编程只读存储器（Programmable ROM，PROM）、可擦除可编程只读存储器（Erasable PROM，EPROM）、电可擦除可编程只读存储器（Electrically EPROM，EEPROM）或闪存。易失性存储器可以是随机存取存储器（Random Access Memory，RAM），其用作外部高速缓存。通过示例性但不是限制性说明，许多形式的 RAM 可用，例如静态随机存取存储器（Static RAM，SRAM）、动态随机存取存储器（Dynamic RAM，DRAM）、同步动态随机存取存储器（Synchronous DRAM，SDRAM）、双倍数据速率同步动态随机存取存储器（Double Data Rate SDRAM，DDR SDRAM）、增强型同步动态随机存取存储器（Enhanced SDRAM，ESDRAM）、

同步连接动态随机存取存储器 (synch link DRAM, SLDRAM) 和直接内存总线随机存取存储器 (Direct Rambus RAM, DR RAM)。

在本申请的一些实施例中, 该计算机程序可以被分割成一个或多个模块, 该一个或者多个模块被存储在该存储器 910 中, 并由该处理器 920 执行, 以完成本申请提供的编码方法。该一个或多个模块可以是能够完成特定功能的一系列计算机程序指令段, 该指令段用于描述该计算机程序在该数据处理的装置 900 中的执行过程。

可选的, 如图 9 所示, 该数据处理的装置 900 还可包括:

收发器 930, 该收发器 930 可连接至该处理器 920 或存储器 910。

其中, 处理器 920 可以控制该收发器 930 与其他设备进行通信, 具体地, 可以向其他设备发送信息或数据, 或接收其他设备发送的信息或数据。收发器 930 可以包括发射机和接收机。收发器 930 还可以进一步包括天线, 天线的数量可以为一个或多个。

应当理解, 该数据处理的装置 900 中的各个组件通过总线系统相连, 其中, 总线系统除包括数据总线之外, 还包括电源总线、控制总线和状态信号总线。

根据本申请的一个方面, 提供了一种数据处理的装置, 包括处理器和存储器, 该存储器用于存储计算机程序, 该处理器用于调用并运行所述存储器中存储的计算机程序, 使得所述编码器执行上述方法实施例的方法。

根据本申请的一个方面, 提供了一种计算机存储介质, 其上存储有计算机程序, 该计算机程序被计算机执行时使得该计算机能够执行上述方法实施例的方法。或者说, 本申请实施例还提供一种包含指令的计算机程序产品, 该指令被计算机执行时使得计算机执行上述方法实施例的方法。

根据本申请的另一个方面, 提供了一种计算机程序产品或计算机程序, 该计算机程序产品或计算机程序包括计算机指令, 该计算机指令存储在计算机可读存储介质中。计算机设备的处理器从计算机可读存储介质读取该计算机指令, 处理器执行该计算机指令, 使得该计算机设备执行上述方法实施例的方法。

换言之, 当使用软件实现时, 可以全部或部分地以计算机程序产品的形式实现。该计算机程序产品包括一个或多个计算机指令。在计算机上加载和执行该计算机程序指令时, 全部或部分地产生按照本申请实施例该的流程或

功能。该计算机可以是通用计算机、专用计算机、计算机网络、或者其他可编程装置。该计算机指令可以存储在计算机可读存储介质中，或者从一个计算机可读存储介质向另一个计算机可读存储介质传输，例如，该计算机指令可以从一个网站站点、计算机、服务器或数据中心通过有线（例如同轴电缆、5 光纤、数字用户线（digital subscriber line，DSL））或无线（例如红外、无线、微波等）方式向另一个网站站点、计算机、服务器或数据中心进行传输。该计算机可读存储介质可以是计算机能够存取的任何可用介质或者是包含一个或多个可用介质集成的服务器、数据中心等数据存储设备。该可用介质可以是磁性介质（例如，软盘、硬盘、磁带）、光介质（例如数字视频光盘10（digital video disc，DVD））、或者半导体介质（例如固态硬盘（solid state disk，SSD））等。

应理解，在本申请实施例中，“与 A 对应的 B”表示 B 与 A 相关联。在一种实现方式中，可以根据 A 确定 B。但还应理解，根据 A 确定 B 并不意味着仅仅根据 A 确定 B，还可以根据 A 和/或其它信息确定 B。

15 在本申请的描述中，除非另有说明，“至少一个”是指一个或多个，“多个”是指两个或两个以上。另外，“和/或”，描述关联对象的关联关系，表示可以存在三种关系，例如，A 和/或 B，可以表示：单独存在 A，同时存在 A 和 B，单独存在 B 的情况，其中 A、B 可以是单数或者复数。字符“/”一般表示前后关联对象是一种“或”的关系。“以下至少一项(个)”或其类似表达，是指的这些项中的任意组合，包括单项(个)或复数项(个)的任意20 组合。例如，a、b、或 c 中的至少一项(个)，可以表示：a、b、c、a-b、a-c、b-c、或 a-b-c，其中 a、b、c 可以是单个，也可以是多个。

还应理解，本申请实施例中出现的第一、第二等描述，仅作示意与区分描述对象之用，没有次序之分，也不表示本申请实施例中设备个数的特别25 限定，不能构成对本申请实施例的任何限制。

还应理解，说明书中与实施例有关的特定特征、结构或特性包括在本申请的至少一个实施例中。此外，这些特定的特征、结构或特性可以任意适合的方式结合在一个或多个实施例中。

此外，术语“包括”和“具有”以及他们的任何变形，意图在于覆盖不排他的30 包含，例如，包含了一系列步骤或单元的过程、方法、系统、产品或服务器不必限于清楚地列出的那些步骤或单元，而是可包括没有清楚地列出的或

对于这些过程、方法、产品或设备固有的其它步骤或单元。

本领域普通技术人员可以意识到，结合本文中所公开的实施例描述的各示例的模块及算法步骤，能够以电子硬件、或者计算机软件和电子硬件的结合来实现。这些功能究竟以硬件还是软件方式来执行，取决于技术方案的特
5 定应用和设计约束条件。专业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。

在本申请所提供的几个实施例中，应该理解到，所揭露的设备、装置和方法，可以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，该模块的划分，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，例如多个模块或组件可以结合或者可以集成到另一个系
10 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，装置或模块的间接耦合或通信连接，可以是电性，机械或其它的形式。

作为分离部件说明的模块可以是或者也可以不是物理上分开的，作为模块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单元上。可以根据实际的需要选择其中的部分或者全部模块来实现本实施例方案的目的。例如，在本申请各个实施例中的各功能模块可以集成在一个处理模块中，也可以是各个模块单独物理存在，也可以两个或两个以上模块集成在一个模块中。
15

以上仅为本申请的具体实施方式，但本申请的保护范围并不局限于此，任何熟悉本技术领域的技术人员在本申请揭露的技术范围内，可轻易想到变化或替换，都应涵盖在本申请的保护范围之内。因此，本申请的保护范围应以该权利要求的保护范围为准。
20

权利要求

1、一种股权激励系统中的数据处理的方法，应用于股权激励系统中的第一设备，其特征在于，包括：

5 获取映射关系，所述映射关系包括至少一种数据类型和至少一种加密方式的对应关系；

根据所述映射关系，确定第一数据的第一数据类型对应的第一加密方式；

根据所述第一加密方式，对所述第一数据进行加密得到第一密文；

根据所述第一密文和所述第一加密方式，生成第一数据包；

10 向所述股权激励系统中的第二设备发送所述第一数据包。

2、根据权利要求 1 所述的方法，其特征在于，所述第一加密方式为随机填充加密方式、非随机加密方式或长文本加密方式。

3、根据权利要求 2 所述的方法，其特征在于，在所述第一加密方式为长文本加密方式的情况下，所述根据所述第一加密方式，对所述第一数据进行加密得到第一密文包括：

15 通过第一密钥对所述第一数据进行加密得到所述第一密文，所述第一密钥为所述第一数据对应的密钥；

对所述第一密钥进行加密得到第二密文；

20 其中，所述根据所述第一密文和所述第一加密方式，生成第一数据包包括：

根据所述第一密文、所述第一加密方式和所述第二密文，生成所述第一数据包。

4、根据权利要求 2 所述的方法，其特征在于，在所述第一加密方式为随机填充加密方式的情况下，所述根据所述第一加密方式，对所述第一数据进行加密得到第一密文包括：

25 通过第一密钥对所述第一数据进行加密得到所述第一密文，所述第一密钥为随机密钥；

其中，所述根据所述第一密文和所述第一加密方式，生成第一数据包包括：

30 根据所述第一密文和所述第一加密方式，生成所述第一数据包。

5、根据权利要求 4 所述的方法，其特征在于，在所述第一加密方式为

非随机填充加密方式的情况下，所述根据所述第一加密方式，对所述第一数据进行加密得到第一密文包括：

通过第一密钥对所述第一数据进行加密得到所述第一密文，所述第一密钥为固定密钥；

5 其中，所述根据所述第一密文和所述第一加密方式，生成第一数据包包括：

根据所述第一密文和所述第一加密方式，生成所述第一数据包。

6、根据权利要求 3 所述的方法，其特征在于，所述对所述第一密钥进行加密得到第二密文包括：

10 通过第二密钥对所述第一密钥进行加密得到所述第二密文，其中，所述第二密钥为所述第一设备和所述第二设备约定的密钥。

7、根据权利要求 3 所述的方法，其特征在于，所述对所述第一密钥进行加密得到第二密文包括：

15 通过第二密钥对所述第一密钥进行加密得到所述第二密文，所述第二密钥为所述第二设备中私钥对应的公钥。

8、根据权利要求 3 所述的方法，其特征在于，在所述第一设备向所述第二设备发送所述第一数据包之前，还包括：

所述第一设备拼接所述第一密文和所述第二密文得到所述第一数据包。

9、根据权利要求 1 至 8 中任一项所述的方法，其特征在于，所述根据
20 所述第一密文和所述第一加密方式，生成第一数据包包括：

将所述第一加密方式对应的加密标识作为前缀生成所述第一数据包。

10、一种股权激励系统中的数据处理的方法，应用于所述股权激励系统中的第二设备，其特征在于，包括：

25 接收来自所述股权激励系统中的第一设备发送的第一数据包，所述第一数据包包括第一密文和前缀；

根据所述前缀对应的加密方式，对所述第一密文进行解密得到第一数据，所述加密方式为随机填充加密方式、非随机加密方式或长文本加密方式；

对所述第一数据，进行数据处理。

11、一种数据处理的装置，包括用于执行如权利要求 1 至 10 中的任一
30 项所述方法的模块。

12、一种数据处理的装置，其特征在于，包括处理器和存储器，所述存

存储器中存储有指令，所述处理器执行所述指令时，使得所述装置执行权利要求 1 至 10 任一项所述的方法。

- 13、一种计算机可读存储介质，其特征在于，所述存储介质中存储有计算机程序或指令，当所述计算机程序或指令被执行时，实现如权利要求 1 至 5 10 中任一项所述的方法。

14、一种计算机程序产品，其特征在于，包括计算机程序代码，当所述计算机程序代码被通信设备运行时，使得所述通信设备执行权利要求 1-10 中任一项所述的方法。