

一种数据排序方法、装置、设备及可读存储介质

技术领域

[01]本说明书涉及计算机技术领域，尤其涉及一种数据排序方法、装置、设备及可读存储介质。

背景技术

[02]随着人们对隐私数据关注度的提高，数据安全领域受到了广泛的关注。为了提高数据的隐私安全性，可以将数据以密文的形式存储。根据用户的实际需求，可以对密文进行各种类型的处理，如排序处理。

[03]但是，在对密文进行排序处理的过程中，仍然存在数据泄露的风险，降低了数据的隐私安全性。因此，如何保证数据的隐私安全性成为亟待解决的问题。

[04]基于此，本说明书提供一种数据排序方法。

发明内容

[05]本说明书提供一种数据排序方法、装置、设备及可读存储介质。

[06]本说明书采用下述技术方案：本说明书提供了一种数据排序方法，包括：确定待处理数组，并从所述待处理数组中选择一个基准密文；针对每个非基准密文，确定该非基准密文的第一噪音值，以所述第一噪音值取值范围的上限确定第一指定参数，并根据所述第一指定参数和所述第一噪音值，确定该非基准密文的待比较密文；根据所述第一指定参数更新所述基准密文，并将更新后的基准密文与该非基准密文的待比较密文进行大小比较，得到该非基准密文的第一比较结果；根据各非基准密文的第一比较结果，划分所述待处理数组，得到两个子数组；针对得到的每个子数组，将该子数组重新作为待处理数组，继续选择基准密文与非基准密文进行比较，继续确定各子数组，直至确定出的各子数组中包含单个密文为止；根据各数组之间的大小关系，确定各密文的排序结果。

[07]本说明书提供了一种数据排序装置，包括：基准密文选择模块，用于确定待处理数组，并从所述待处理数组中选择一个基准密文；待比较密文确定模块，用于针对每个非基准密文，确定该非基准密文的第一噪音值，以所述第一噪音值取值范围的上限确定第一指定参数，并根据所述第一指定参数和所述第一噪音值，确定该非基准密文的待比较

密文；第一比较模块，用于根据所述第一指定参数更新所述基准密文，并将更新后的基准密文与该非基准密文的待比较密文进行大小比较，得到该非基准密文的第一比较结果；划分模块，用于根据各非基准密文的第一比较结果，划分所述待处理数组，得到两个子数组；重新比较模块，用于针对得到的每个子数组，将该子数组重新作为待处理数组，继续选择基准密文与非基准密文进行比较，继续确定各子数组，直至确定出的各子数组中包含单个密文为止；排序模块，用于根据各数组之间的大小关系，确定各密文的排序结果。

[08]本说明书提供了一种计算机可读存储介质，所述存储介质存储有计算机程序，所述计算机程序被处理器执行时实现上述数据排序方法。

[09]本说明书提供了一种电子设备，包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序，所述处理器执行所述程序时实现上述数据排序方法。

[10]本说明书采用的上述至少一个技术方案能够达到以下有益效果：本说明书提供的数据排序方法中，根据非基准密文对应的第一噪音值和第一指定参数更新非基准密文，并将各非基准密文分别与更新后的基准密文进行比较，进而根据第一比较结果将待处理数组划分为多个子数组，将各子数组分别重新作为待处理数组，重复上述比较过程直至各数组只包含单一密文为止，以各数组之间的大小关系，确定各密文的排序结果，可见，在对密文排序的过程中，以噪音值和第一指定参数更新各非基准密文的方式，即使比较结果为非基准密文与基准密文相等，也不会泄露原始的非基准密文与基准密文之间的关系，提高了密文排序过程中数据的安全性和隐私保护性。

附图说明

[11]此处所说明的附图用来提供对本说明书的进一步理解，构成本说明书的一部分，本说明书的示意性实施例及其说明用于解释本说明书，并不构成对本说明书的不当限定。

[12]图1为本说明书中一种数据排序方法的流程示意图。

[13]图2为本说明书中一种数据排序方法的流程示意图。

[14]图3为本说明书提供的一种数据排序装置的示意图。

[15]图4为本说明书提供的对应于图1的电子设备示意图。

具体实施方式

[16]为使本说明书的目的、技术方案和优点更加清楚，下面将结合本说明书具体实施例及相应的附图对本说明书技术方案进行清楚、完整地描述。显然，所描述的实施例仅是本说明书一部分实施例，而不是全部的实施例。基于本说明书中的实施例，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，都属于本说明书保护的范围。

[17]另外，需要说明的是，本申请中所有获取信号、信息或数据的动作都是在遵照所在地国家相应的数据保护法规政策的前提下，并获得由相应装置所有者给予授权的情况下进行的。

[18]随着数字经济的蓬勃发展，数据的价值已得到社会的广泛认可。在大数据北京下，由于数据可被复制，且复制成本较低，如果以明文的形式对数据进行开发和流通，会导致数据规模化泄露的风险急剧增大，甚至侵害个人隐私以及国家安全。

[19]基于上述实际情况，为了克服数据容易复制这一问题，可以采用数据加密的方式，使得数据以密文形式流通，保证数据在流转、计算、融合等全链路安全可控。其中，密文可以是数据经加密后的形式，密文的多个持有方均无法从中获取原始数据的任何信息，一般情况下，可以利用密文进行加法、乘法、逻辑运算、比较等密态计算，由于密文计算的输入输出都是密文，且计算过程不会泄露（或仅有少量可容忍的泄露）输入输出信息。

[20]但在实际对密文进行处理的过程中，仍然存在数据泄露的风险。以密态计算为比较为例，其目的是为了将密文按照大小关系进行排列。目前的比较方案中可能会确定出“等于”的比较结果，也就是说，恶意的攻击方可以知道两个密文之间是否相等，这会导致密文的统计数据的泄露。例如，密态表中包含用户消费记录的月份信息，即使对月份信息进行了加密，如果在排序的过程中确定了若干月份之间的相等关系，就会泄露出用户在该月份存在多少条消费记录。

[21]基于此，本说明书提供一种数据排序方法，在对密文排序的过程中，以第一噪音值更新各非基准密文，即使比较结果为非基准密文与基准密文相等，也不会泄露非基准密文与基准密文之间的原始关系，提高了非基准密文的安全性和隐私保护性。

[22]以下结合附图，详细说明本说明书各实施例提供的技术方案。

[23]图1为本说明书提供的一种数据排序方法的流程示意图。

[24]S100: 确定待处理数组, 并从所述待处理数组中选择一个基准密文。

[25]本说明书实施例中提供一种数据排序方法, 该数据排序方法的执行过程可由用于执行密文处理的服务器等电子设备执行该数据排序方法, 该密文可以是预先存储在当前执行数据排序方法的电子设备(当前数据处理方), 也可以是执行数据排序方法的电子设备预先从若干其他数据持有方(其他存储密文的服务器)获取得到的, 本说明书对此不做限定。

[26]待处理数组中可以包含需要进行排序处理的各密文, 各密文在待处理数组中的初始排序可以是随机的, 也可以根据数据来源依次排列的, 本说明书不做限定。

[27]可选的, 为了进一步避免密文的信息泄露, 可以在具体的排序之前, 对待处理数组中的密文进行乱序操作, 即使恶意的参与方知晓了各密文之间的大小关系, 也无法获知各密文的具体信息及其统计信息。在本说明书实施例中, 乱序操作的目的是割裂打乱前各密文与打乱后各密文之间的对应关系, 所采用的方案可以是现有的任一可对密文进行打乱排序的乱序方案, 本说明书对此不做限定。另外, 乱序操作并非本说明书提供的数据排序方法中的必要操作, 可以根据具体的应用场景和安全等级确定是否需要执行乱序操作, 本说明书对此不做限定。

[28]在本说明书实施例中, 针对各密文进行排序的方案采用的基于快速排序(Quicksort)算法的改进方案, 因此, 可以首先从待处理数组包含的各密文中选择一个基准密文, 以该基准密文为基准值, 以待处理数组中包含的除基准密文外的其他密文作为非基准密文, 将各非基准密文都与基准密文进行大小比较, 以便基于各比较结果确定各非基准密文在待处理数组中的排序。

[29]S102: 针对每个非基准密文, 确定该非基准密文的第一噪音值, 以所述第一噪音值取值范围的上限确定第一指定参数, 并根据所述第一指定参数和所述第一噪音值, 确定该非基准密文的待比较密文。

[30]在实际应用中, 若比较方案中将比较结果以“大于”、“等于”和“小于”输出, 则会出现恶意的参与方窃取比较结果为“等于”的密文, 造成密文的信息泄露; 而另一方面, 待处理数组中可能会存在大量大小相等的密文, 如果在比较方案中将比较结果以“大于等于”和“小于”输出, 则会出现将大量大小相等的密文总是划分到同一个子数组的情况, 当子数组内绝大部分密文的大小都相等时, 在排序的过程中其算法复杂度可能出现增长的情况, 影响排序的效率。

[31]为此，在本说明书实施例中，通过确定第一噪音值，以非基准密文的第一噪音值改变比较过程中非基准密文的大小，将原本可能与基准密文大小相等的非基准密文，转换成与基准密文大小不相等的非基准密文。也就是说，就算原始的非基准密文是相等的，该相等的关系也不会体现在比较结果中，即使恶意参与方窃取到了非基准密文的比较结果，也无法获知非基准密文的具体信息和统计信息，增强了密文的安全性。

[32]具体的，各非基准密文的第一噪音值可以通过生成各非基准密文对应的随机数的方式得到，也可以根据各非基准密文在待处理数组中的原始排序序号确定，或者通过现有的任意方式确定，本说明书对此不限定。

[33]进一步的，由于可能存在下述情况：在非基准密文中添加了非基准密文的第一噪音值后，原本比基准密文小的非基准密文，却大于了基准密文，导致该非基准密文的比较结果发生了错误。为了避免上述情况的发生，在本说明书实施例中，以第一噪音值的取值范围的上限确定第一指定参数，并以第一指定参数为权重对该非基准密文进行加权，并将加权后的非基准密文与该非基准密文的第一噪音值相加，得到该非基准密文的待比较密文。由于第一指定参数大于非基准密文的第一噪音值，因此，第一噪音值在确定出的待比较密文中的占比就会变小，因此，第一噪音值的大小不会影响该非基准密文和基准密文之间的大小关系，便于后续以该基准密文的待比较密文，和基准密文进行大小比较，等到正确的比较结果。

[34]另外，需要说明的是，在确定出该非基准密文的待比较密文后，可以以待比较密文覆盖原来的非基准密文，还可以是将待比较密文暂时保存在缓存里，仅利用待比较密文进行排序，在排序结束后有选择的删除缓存中的待比较密文，本说明书对此不做限定。

[35]S104：根据所述第一指定参数更新所述基准密文，并将更新后的基准密文与该非基准密文的待比较密文进行大小比较，得到该非基准密文的第一比较结果。

[36]进一步的，由于在上述步骤 S102 中该非基准密文的待比较密文的确定过程中不仅采用了第一噪音值，还采用的第一指定参数作为权重对该非基准密文进行加权，为了使得基准密文能够通过对待比较密文比大小从而衡量出该非基准密文的大小，可以对基准密文采取与非基准密文相似的操作，即，以第一指定参数为权重，对基准密文进行加权，并以加权结果更新所述基准密文。

[37]例如，对于非基准密文的大小为 1，该非基准密文的第一噪音值为 2 时，若基准密文的大小为 2，则仅根据第一噪音值和该非基准密文确定待比较密文的大小为 3，此时，

原本该非基准密文是小于基准密文的，但是该基准密文的待比较密文却大于基准密文，第一噪音值导致了非基准密文的比较结果发生了错误。为此，可以以第一噪音值的取值范围的上限大小 3 为第一指定参数，此时，根据第一指定参数和第一噪音值，确定出的该非基准密文的待比较密文大小为 5，而根据第一指定参数更新后的基准密文则为 6，此时，该非基准密文的比较结果并没有发生改变。

[38]进一步的，在实际应用中，密文的比较过程需要网络交互的支持，即便是内网交互，一次交互的延迟也达到了 1ms 量级。网络交互延迟对串行操作的性能影响非常显著。例如，在上述网络延迟下，1 千个串行操作需要 1s，而 1 千个可以并发的操作，却可能只需要 2ms。如果在基于非基准密文的数据处理过程时无法实现并行化，则处理的性能下降得非常显著。

[39]由此，在将各非基准密文分别与基准密文进行比较的过程中可以基于并行的方式，同时得到各非基准密文分别与基准密文进行比较的比较结果，以便将网络交互延迟对数据排序性能的影响降到最低。

[40]另外，在本说明书实施例中，为了避免“相等”的比较结果泄露，按照非基准密文“大于等于”以及“小于”基准密文的方式，或者非基准密文“小于等于”以及“大于”基准密文的方式，得到比较结果，而具体是上述两种方式中的哪一种，可以根据具体的应用场景确定，本说明书对此不做限定。

[41]S106: 根据各非基准密文的第一比较结果，划分所述待处理数组，得到两个子数组。

[42]具体的，在本说明书实施例中，需要得到按照大小关系依次排序的数组，如按从大到小排序，或按从小到大排序。

[43]由于在本说明书实施例中，比较结果中不存在“相等”，所以比较结果仅存在两种类型，因此，在根据各非基准密文的第一比较结果将各基准密文划分到不同的字数组的过程中，一般情况下一个待处理数组的各密文会被划分到两个子数组中。其中，基准密文可被随机划分到这两个子数组中的任意一个子数组中。

[44]可选的，根据基准密文所在的子数组，可以直接确定基准密文在该子数组中的位置。例如，以按照从大到小的次序排序，对于将基准密文划分到“大于等于”的子数组中时，根据各非基准密文的第一比较结果可知，被划分到“大于等于”的子数组的非基准密文都是大于等于基准密文的，因此，可以直接确定基准密文在该“大于等于”的子数组中的位置为各密文的末尾，同理可得，如果基准密文被划分到“小于”的子数组中，则基准密文

在该“小于”的子数组中的位置为各密文的首位。

[45]当然，可选地，也可以不将基准密文划分到这两个子数组中的任意一个子数组中，而是将基准密文单独作为一个数组，排序在上述两个子数组中间。这样，基准密文所在的数组中仅包含基准密文本身一个密文，在下一次划分子数组时也不会再次被划分。并且，这种划分方式也不会泄露密文之间的相等关系，即使恶意的参与方获知了基准密文所在的数组的排序在上述两个子数组中间，也无法获知排序在基准密文所在的数组之前的子数组，或者排序在基准密文所在的数组之后的子数组的任何数值信息。例如，对于待处理数组 $\{x_1, x_2, x_3, x_4\}$ ，以 x_1 为基准密文，将待处理数组划分为 $\{x_2, x_4\}$ 和 $\{x_3\}$ 两个子数组，此时，可以 x_1 将作为独立的数组，排序在 $\{x_2, x_4\}$ 和 $\{x_3\}$ 中间，即确定出各密文之间的排序为 $\{x_2, x_4\}$ 、 $\{x_1\}$ 和 $\{x_3\}$ 。

[46]在本说明书一个可选的实施例中，可在将待处理数组划分为两个子数组之后，就将这两个子数组按照大小关系进行排序，例如，按从大到小排列时，将比较结果为“大于等于”的子数组排在比较结果为“小于”的子数组前面。当然，也可以在确定出各密文的大小关系之后在调整各密文的排序，本说明书对排序的时机不做具体限定。

[47]S108：针对得到的每个子数组，将该子数组重新作为待处理数组，继续选择基准密文与非基准密文进行比较，继续确定各子数组，直至确定出的各子数组中包含单个密文为止。

[48]由于待处理数组中包含的密文的数量可以是多个，因此，仅执行一次子数组的划分无法确定各密文之间的大小关系，因此上述步骤S100至S106需要重复多次才能够达到将原始的待处理数据中包含的各密文均按大小关系排列的目的。

[49]另外，划分子数组（或者可以理解为对各密文进行排序操作）的结束条件可以是子数组仅包含一个密文，当然，可选地，结束条件对应的子数组包含的密文的数量还可以是预先设置的数量阈值，该数量阈值可以根据具体的应用场景确定，本说明书对此不做限定。

[50]或者，可选地，可以以划分子数组的次数为结束条件，当划分子数组的次数高于预设次数阈值时，则停止进行排序。

[51]例如，待处理数组包含密文 $\{x_1, x_2, x_3, x_4\}$ ，以 x_1 为基准密文，分别确定非基准密文 x_2 与 x_1 的大小关系、非基准密文 x_3 与 x_1 的大小关系、非基准密文 x_4 与 x_1 的大小关系。如果 x_2 、 x_4 被划分到“大于等于” x_1 的子数组， x_3 被划分到“小于” x_1 的子数组，

则待处理数组可以排序为 $\{x_2, x_4, x_1\}$ 和 $\{x_3\}$ 。进一步的，对于子数组 $\{x_2, x_4, x_1\}$ ，由于该子数组中包含的密文不止一个，因此，需要针对该子数组再次进行划分，将该子数组重新作为待处理数组，选择 x_2 作为基准密文，确定 x_4 与 x_2 的大小关系， x_1 与 x_2 的大小关系，得到 x_4 被划分到“大于等于”的子数组，而 x_1 被划分到“小于”的子数组，由此，可以确定各密文的排序为 $\{x_4, x_2, x_1, x_3\}$ 。

[52]S110: 根据各数组之间的大小关系，确定各密文的排序结果。

[53]具体的，当执行完上述步骤 S108 后，可以将原本的待处理数组分割成多个只包含一个密文的数组，并且已经确定出各数组之间的大小关系，此时，根据各数组之间的大小关系，按照预设的大小排列方式将各数组进行排序，即可得到各密文的排序结果。

[54]在本说明书提供的排序方法中，根据非基准密文对应的第一噪音值和第一指定参数更新非基准密文，并将各非基准密文分别与更新后的基准密文进行比较，进而根据比较结果将待处理数组划分为多个子数组，将各子数组分别重新作为待处理数组，重复上述比较过程直至各数组只包含单一密文为止，以各数组之间的大小关系，确定各密文的排序结果，可见，在对密文排序的过程中，以噪音值和第一指定参数更新各非基准密文的方式，即使比较结果为非基准密文与基准密文相等，也不会泄露原始的非基准密文与基准密文之间的关系，提高了密文排序过程中数据的安全性和隐私保护性。

[55]在本说明书一个或多个实施例中，在如图 1 步骤 S102 针对每个非基准密文，确定该非基准密文的第一噪音值，可以分为两种情况：第一噪音值可以是密文，也可以是明文，以下针对这两种情况进行分别说明。

[56]对于第一种情况：当第一噪音值是密文时，可以采用以密态形式生成该非基准密文的密文随机数，作为该基准密文的第一噪音值。其中，所谓密态的形式生成的密文随机数，指的是随机数生成时就是以密文的形式生成的，即便是随机数的生成方，也不知道随机数的具体的信息。这样的好处是，非基准密文的第一噪音值的泄露不会引起非基准密文的比较结果的泄露，提高了密文排序的数据安全性。生成密文随机数的密态的形式可以是基于多方安全计算（Secure Multi-Party Computation, MPC）的密文生成、混淆电路（Garbled Circuit）等现有的密文随机数的生成方式，对生成密文随机数的具体密态形式可以根据预设的安全级别确定，或者根据其他具体的应用场景确定，只要是能够达到本说明书实施例中密文随机数的效果，即随机数生成时就是密文的形式，本说明书对具体的密态形式不做限定。

[57]对于第二种情况：当第一噪音值是明文时，一种可选的方式为直接生成随机数，将生成的随机数作为该非基准密文的第一噪音值。另一种可选的方式适用于多个数据处理方共同进行数据排序的场景，具体的，假设存在数据处理方 A、B、C 三方，这三方在 aby3 协议下，数据处理方 A 拥有密文分量 (a_1, a_2)、数据处理方 B 拥有密文分量 (a_1, a_3)、数据处理方 C 拥有密文分量 (a_2, a_3)。在生成随机数时，约定 a_1 和 a_3 为 0，此时，数据处理方 A 和 C 拥有的密文分量相同，这两方可以通过预共享的密钥分别生成随机数，然后交换生成的随机数确定该随机数是否匹配，若匹配，则可以采用该生成的随机数作为该非基准密文的第一噪音值。当然，明文形式的第一噪音值还可以采用现有的任意方案生成，本说明书对此不做限定。

[58]在本说明书一个或多个实施例中，在如图 1 步骤 S104 所示根据所述第一指定参数更新所述基准密文中，还可以在此基础上再添加第二噪音值的方式，保证以基准密文衡量非基准密文大小情况时的准确性，具体方案如下：首先，在该非基准密文的第一噪音值的取值范围内，确定所述基准密文的第二噪音值。

[59]具体的，在如图 1 步骤 S104 中仅根据第一指定参数更新基准密文，即以第一指定参数为权重对基准密文进行加权，然后以加权后的基准密文更新基准密文。也就是说，用加权后的基准密文与各非基准密文进行大小比较。但是由于确定待比较密文是还在加权后的非基准密文中添加了第一噪音值，因此，也可以在加权后的基准密文中添加噪音值。并且，为使得第二噪音值仅达到保护密文信息不被泄露的效果，所以，在第一噪音值的取值范围内确定第二噪音值，可以保证第二噪音值和第一噪音值的取值相差不会过大，避免改变非基准密文和基准密文之间的大小关系。另外，在对密文进行排序的过程中，第二噪音值的取值可以是固定的，也可以是在每次与非基准密文进行比较之前都确定的，本说明书对此不做限定。

[60]其次，以所述第一指定参数为权重，对所述基准密文进行加权。

[61]然后，根据加权后的基准密文以及所述基准密文的第二噪音值，更新所述基准密文。

[62]具体的，在加权后的基准密文的基础上加上基准密文的第二噪音值，得到更新后的基准密文，以确定出的更新后的基准密文更新基准密文。

[63]在本说明书一个可选的实施例中，在如图 1 步骤 S104 将更新后的基准密文与该非基准密文的待比较密文进行大小比较之前，还可以根据该非基准密文的待比较密文更新该非基准密文，以更新后的非基准密文与更新后的基准密文进行比较，得到第一比较结

果。

[64]进一步的，在得到第一比较结果之后，可以根据第一比较结果确定该非基准密文被划分到哪个子数组中，在此之后，由于当前非基准密文的值是加权并添加第一噪音值得到的，因此，要将当前非基准密文进行还原，具体的，根据所述第一指定参数的倒数确定第二指定参数，然后，针对每个已排序的密文，以所述第二指定参数为权重对该已排序的密文进行加权，取加权结果的整数部分更新该已排序的密文。

[65]其中，上述所说的已排序的密文，一般指的是已经得到第一比较结果后的密文，也即被分到子数组中的各非基准密文。

[66]上述还原以排序的密文的步骤可以是在每一次划分子数组时执行，也可以是在最终得到各密文的排序结果时执行，本说明书对上述还原已排序密文的步骤的执行时机不做限定。

[67]在本说明书一个可选的实施例中，在如图 1 步骤 S106 所示根据各非基准密文的第一比较结果，划分所述待处理数组，得到两个子数组之前，可以根据基准密文与非基准密文之间的大小关系，确定第二比较结果，进而，以第一比较结果和第二比较结果共同确定该非基准密文划分到哪个子数组中，具体方案如下，如图 2 所示：S200：针对每个非基准密文，判断该非基准密文是否与所述基准密文大小相等，若是，执行步骤 S202，否则执行步骤 S204。

[68]具体的，此时采用的非基准密文可以是未经过更新处理的非基准密文，基准密文也可以是未经过更新处理的基准密文。以密文的形式，确定该非基准密文与基准密文的大小关系。

[69]S202：生成随机数，并根据所述随机数和所述随机数取值范围内的数值阈值的大小关系，确定该非基准密文的第二比较结果。执行步骤 S206。

[70]如果该基准密文与基准密文相等，那么，为了不泄露该基准密文与基准密文之间的相等关系，可以随机生成该基准密文的第二比较结果。所谓的随机生成指定的，该基准密文的第二比较结果可以是大于等于（或小于等于）基准密文，也可以是小于（或大于）基准密文。为此，采用生成随机数的方式，将随机数与该随机数所在的取值范围内的数值阈值进行大小比较，并以随机数和数值阈值的大小关系作为该非基准密文的第二比较结果。通过执行此步骤，使得原本与基准密文大小相等的该基准密文可能被划分到任意一个子数组中，从而实现不泄露相等关系的密文的信息。

[71]S204: 根据该非基准密文和所述基准密文的大小关系, 确定该非基准密文的第二比较结果。

[72]对于该基准密文与基准密文不相等的情况, 可以直接根据该基准密文与基准密文之间的大小关系确定该非基准密文的第二比较结果。这是由于, 即使该基准密文与基准密文之间的大小关系发生了泄露, 也不会被恶意的参与方知晓该基准密文和基准密文的信息。

[73]S206: 判断该基准密文的第一比较结果与该基准密文的第二比较结果是否相同。若是, 执行步骤 S208, 否则执行步骤 S210。

[74]进一步的, 在确定了第二比较结果之后, 可以采用将第二比较结果与第一比较结果相结合的方式, 确定该非基准密文对应的子数组。

[75]S208: 根据该非基准密文的第一比较结果, 确定该非基准密文对应的子数组。

[76]具体的, 如果该非基准密文的第一比较结果和第二比较结果相同, 说明上述如图 1 步骤 S102 至 S104 的比较方案, 和上述步骤 S200 至 S204 的比较方案得到的比较结果是相同, 那么该比较结果是较为可信的, 所以可以直接以该非基准密文的第一比较结果(或者第二比较结果)作为划分该基准密文到哪个子数组的依据。

[77]S210: 重新随机生成该基准密文的第三比较结果, 并根据该基准密文的第三比较结果, 确定该非基准密文对应的子数组。

[78]具体的, 如果该非基准密文的第一比较结果和第二比较结果不同, 则说明上述如图 1 步骤 S102 至 S104 的比较方案, 和上述步骤 S200 至 S204 的比较方案得到的比较结果之间存在差异, 那么以哪个方案得到的比较结果作为划分该基准密文到子数组的依据都不合适, 此时, 可以重新生成一个第三比较结果, 以此作为划分该基准密文到哪个子数组的依据。具体的生成方式, 可以与上述步骤 S202 的方案类似, 此处不再赘述。

[79]图 3 为本说明书提供的一种数据排序装置示意图, 具体包括: 基准密文选择模块 300, 用于确定待处理数组, 并从所述待处理数组中选择一个基准密文; 待比较密文确定模块 302, 用于针对每个非基准密文, 确定该非基准密文的第一噪音值, 以所述第一噪音值取值范围的上限确定第一指定参数, 并根据所述第一指定参数和所述第一噪音值, 确定该非基准密文的待比较密文; 第一比较模块 304, 用于根据所述第一指定参数更新所述基准密文, 并将更新后的基准密文与该非基准密文的待比较密文进行大小比较, 得到该非基准密文的第一比较结果; 划分模块 306, 用于根据各非基准密文的第一比较结果,

划分所述待处理数组，得到两个子数组；重新比较模块 308，用于针对得到的每个子数组，将该子数组重新作为待处理数组，继续选择基准密文与非基准密文进行比较，继续确定各子数组，直至确定出的各子数组中包含单个密文为止；排序模块 310，用于根据各数组之间的大小关系，确定各密文的排序结果。

[80]可选地，所述待比较密文确定模块 302 具体用于，生成该非基准密文对应的随机数；确定指定密钥，并根据所述指定密钥对该非基准密文对应的随机数进行加密，得到密文随机数作为该非基准密文的第一噪音值。

[81]可选地，所述第一比较模块 304 具体用于，在该非基准密文的第一噪音值的取值范围内，确定所述基准密文的第二噪音值；以所述第一指定参数为权重，对所述基准密文进行加权；根据加权后的基准密文以及所述基准密文的第二噪音值，更新所述基准密文。

[82]可选地，所述装置还包括：第一更新模块 312，具体用于根据该非基准密文的待比较密文更新该非基准密文；所述第一比较模块具体用于，将更新后的基准密文与更新后的该非基准密文进行大小比较，得到该非基准密文的比较结果。

[83]可选地，所述装置还包括：第二更新模块 314，具体用于根据所述第一指定参数的倒数确定第二指定参数；针对每个已排序的密文，以所述第二指定参数为权重对该已排序的密文进行加权，取加权结果的整数部分更新该已排序的密文。

[84]可选地，所述装置还包括：第二比较模块 316，具体用于针对每个非基准密文，判断该非基准密文是否与所述基准密文大小相等；若是，生成随机数，并根据所述随机数和所述随机数取值范围内的数值阈值的大小关系，确定该非基准密文的第二比较结果；若否，根据该非基准密文和所述基准密文的大小关系，确定该非基准密文的第二比较结果。

[85]可选地，所述划分模块 306 具体用于判断该基准密文的第一比较结果与该基准密文的第二比较结果是否相同；若是，根据该非基准密文的第一比较结果，确定该非基准密文划分到的子数组；若否，重新随机生成该基准密文的第三比较结果，并根据该基准密文的第三比较结果，确定该非基准密文划分到的子数组。

[86]本说明书还提供了一种计算机可读存储介质，该存储介质存储有计算机程序，计算机程序可用于执行上述图 1 所示的数据排序方法。

[87]本说明书还提供了图 4 所示的电子设备的示意结构图。如图 4 所述，在硬件层面，该电子设备包括处理器、内部总线、网络接口、内存以及非易失性存储器，当然还可能

包括其他业务所需要的硬件。处理器从非易失性存储器中读取对应的计算机程序到内存中然后运行，以实现上述图 1 所示的数据排序方法。当然，除了软件实现方式之外，本说明书并不排除其他实现方式，比如逻辑器件抑或软硬件结合的方式等等，也就是说以下处理流程的执行主体并不限于各个逻辑单元，也可以是硬件或逻辑器件。

[88]在 20 世纪 90 年代,对于一个技术的改进可以很明显地区分是硬件上的改进(例如,对二极管、晶体管、开关等电路结构的改进)还是软件上的改进(对于方法流程的改进)。然而,随着技术的发展,当今的很多方法流程的改进已经可以视为硬件电路结构的直接改进。设计人员几乎都通过将改进的方法流程编程到硬件电路中来得到相应的硬件电路结构。因此,不能说一个方法流程的改进就不能用硬件实体模块来实现。例如,可编程逻辑器件(Programmable Logic Device, PLD)(例如现场可编程门阵列(Field Programmable Gate Array, FPGA))就是这样一种集成电路,其逻辑功能由用户对器件编程来确定。由设计人员自行编程来把一个数字系统“集成”在一片 PLD 上,而不需要请芯片制造厂商来设计和制作专用的集成电路芯片。而且,如今,取代手工地制作集成电路芯片,这种编程也多半改用“逻辑编译器(logic compiler)”软件来实现,它与程序开发撰写时所用的软件编译器相类似,而要编译之前的原始代码也得用特定的编程语言来撰写,此称之为硬件描述语言(Hardware Description Language, HDL),而 HDL 也并非仅有一种,而是有许多种,如 ABEL(Advanced Boolean Expression Language)、AHDL(Altera Hardware Description Language)、Confluence、CUPL(Cornell University Programming Language)、HDCal、JHDL(Java Hardware Description Language)、Lava、Lola、MyHDL、PALASM、RHDH(Ruby Hardware Description Language)等,目前最普遍使用的是 VHDL(Very-High-Speed Integrated Circuit Hardware Description Language)与 Verilog。本领域技术人员也应该清楚,只需要将方法流程用上述几种硬件描述语言稍作逻辑编程并编程到集成电路中,就可以很容易得到实现该逻辑方法流程的硬件电路。

[89]控制器可以按任何适当的方式实现,例如,控制器可以采取例如微处理器或处理器以及存储可由该(微)处理器执行的计算机可读程序代码(例如软件或固件)的计算机可读介质、逻辑门、开关、专用集成电路(Application Specific Integrated Circuit, ASIC)、可编程逻辑控制器和嵌入微控制器的形式,控制器的例子包括但不限于以下微控制器:ARC 625D、Atmel AT91SAM、Microchip PIC18F26K20 以及 Silicone Labs C8051F320,存储器控制器还可以被实现为存储器的控制逻辑的一部分。本领域技术人员也知道,除了以纯计算机可读程序代码方式实现控制器以外,完全可以通过将方法步骤进行逻辑编程来使得控制器以逻辑门、开关、专用集成电路、可编程逻辑控制器和嵌入微控制器等

的形式来实现相同功能。因此这种控制器可以被认为是一种硬件部件，而对其内包括的用于实现各种功能的装置也可以视为硬件部件内的结构。或者甚至，可以将用于实现各种功能的装置视为既可以是实现方法的软件模块又可以是硬件部件内的结构。

[90]上述实施例阐明的系统、装置、模块或单元，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。具体的，计算机例如可以为个人计算机、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何设备的组合。

[91]为了描述的方便，描述以上装置时以功能分为各种单元分别描述。当然，在实施本说明书时可以把各单元的功能在同一个或多个软件和/或硬件中实现。

[92]本领域内的技术人员应明白，本申请的实施例可提供为方法、系统、或计算机程序产品。因此，本申请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，本申请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。

[93]本申请是参照根据本申请实施例的方法、设备（系统）、和计算机程序产品的流程图和/或方框图来描述的。应理解可由计算机程序指令实现流程图和/或方框图中的每一流程和/或方框、以及流程图和/或方框图中的流程和/或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器，使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的装置。

[94]这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中，使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品，该指令装置实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能。

[95]这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上，使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和/或方框

图一个方框或多个方框中指定的功能的步骤。

[96] 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。

[97] 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。

[98] 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。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。

[99] 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。

[100] 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。

[101] 本说明书可以在由计算机执行的计算机可执行指令的一般上下文中描述，例如程序模块。一般地，程序模块包括执行特定任务或实现特定抽象数据类型的例程、程序、对象、组件、数据结构等等。也可以在分布式计算环境中实践本说明书，在这些分布式计算环境中，由通过通信网络而被连接的远程处理设备来执行任务。在分布式计算环境

中，程序模块可以位于包括存储设备在内的本地和远程计算机存储介质中。

[102] 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。

[103] 以上所述仅为本说明书的实施例而已，并不用于限制本说明书。对于本领域技术人员来说，本说明书可以有各种更改和变化。凡在本说明书的精神和原理之内所作的任何修改、等同替换、改进等，均应包含在本说明书的权利要求范围之内。

权利要求书

1、一种数据排序方法，所述方法包括：

确定待处理数组，并从所述待处理数组中选择一个基准密文；

针对每个非基准密文，确定该非基准密文的第一噪音值，以所述第一噪音值取值范围的上限确定第一指定参数，并根据所述第一指定参数和所述第一噪音值，确定该非基准密文的待比较密文；

根据所述第一指定参数更新所述基准密文，并将更新后的基准密文与该非基准密文的待比较密文进行大小比较，得到该非基准密文的第一比较结果；

根据各非基准密文的第一比较结果，划分所述待处理数组，得到两个子数组；

针对得到的每个子数组，将该子数组重新作为待处理数组，继续选择基准密文与非基准密文进行比较，继续确定各子数组，直至确定出的各子数组中包含单个密文为止；

根据各数组之间的大小关系，确定各密文的排序结果。

2、如权利要求1所述的方法，确定该非基准密文的第一噪音值，包括：

以密态形式生成该非基准密文的密文随机数，作为该非基准密文的第一噪音值。

3、如权利要求1所述的方法，根据所述第一指定参数更新所述基准密文，包括：

在该非基准密文的第一噪音值的取值范围内，确定所述基准密文的第二噪音值；

以所述第一指定参数为权重，对所述基准密文进行加权；

根据加权后的基准密文以及所述基准密文的第二噪音值，更新所述基准密文。

4、如权利要求1所述的方法，将更新后的基准密文与该非基准密文的待比较密文进行大小比较之前，所述方法还包括：

根据该非基准密文的待比较密文更新该非基准密文；

将更新后的基准密文与该非基准密文的待比较密文进行大小比较，得到该非基准密文的比较结果，包括：

将更新后的基准密文与更新后的该非基准密文进行大小比较，得到该非基准密文的比较结果。

5、如权利要求4所述的方法，所述方法还包括：

根据所述第一指定参数的倒数确定第二指定参数；

针对每个已排序的密文，以所述第二指定参数为权重对该已排序的密文进行加权，取加权结果的整数部分更新该已排序的密文。

6、如权利要求1所述的方法，根据各非基准密文的第一比较结果，划分所述待处理数组之前，所述方法还包括：

针对每个非基准密文，判断该非基准密文是否与所述基准密文大小相等；

若是，生成随机数，并根据所述随机数和所述随机数取值范围内的数值阈值的大小关系，确定该非基准密文的第二比较结果；

若否，根据该非基准密文和所述基准密文的大小关系，确定该非基准密文的第二比较结果。

7、如权利要求 6 所述的方法，根据各非基准密文的第一比较结果，划分所述待处理数组，包括：

判断该基准密文的第一比较结果与该基准密文的第二比较结果是否相同；

若是，根据该非基准密文的第一比较结果，确定该非基准密文对应的子数组；

若否，重新随机生成该基准密文的第三比较结果，并根据该基准密文的第三比较结果，确定该非基准密文对应的子数组。

8、一种数据排序装置，包括：

基准密文选择模块，用于确定待处理数组，并从所述待处理数组中选择一个基准密文；

待比较密文确定模块，用于针对每个非基准密文，确定该非基准密文的第一噪音值，以所述第一噪音值取值范围的上限确定第一指定参数，并根据所述第一指定参数和所述第一噪音值，确定该非基准密文的待比较密文；

第一比较模块，用于根据所述第一指定参数更新所述基准密文，并将更新后的基准密文与该非基准密文的待比较密文进行大小比较，得到该非基准密文的第一比较结果；

划分模块，用于根据各非基准密文的第一比较结果，划分所述待处理数组，得到两个子数组；

重新比较模块，用于针对得到的每个子数组，将该子数组重新作为待处理数组，继续选择基准密文与非基准密文进行比较，继续确定各子数组，直至确定出的各子数组中包含单个密文为止；

排序模块，用于根据各数组之间的大小关系，确定各密文的排序结果。

9、如权利要求 8 所述的装置，所述待比较密文确定模块用于，以密态形式生成该非基准密文的密文随机数，作为该非基准密文的第一噪音值。

10、如权利要求 8 所述的装置，所述第一比较模块用于，在该非基准密文的第一噪音值的取值范围内，确定所述基准密文的第二噪音值；以所述第一指定参数为权重，对所述基准密文进行加权；根据加权后的基准密文以及所述基准密文的第二噪音值，更新所述基准密文。

11、如权利要求 8 所述的装置，所述装置还包括：

第一更新模块，用于根据该非基准密文的待比较密文更新该非基准密文；

所述第一比较模块用于，将更新后的基准密文与更新后的该非基准密文进行大小比较，得到该非基准密文的比较结果。

12、如权利要求 11 所述的装置，所述装置还包括：

第二更新模块，用于根据所述第一指定参数的倒数确定第二指定参数；针对每个已排序的密文，以所述第二指定参数为权重对该已排序的密文进行加权，取加权结果的整数部分更新该已排序的密文。

13、如权利要求 8 所述的装置，所述装置还包括：

第二比较模块，用于针对每个非基准密文，判断该非基准密文是否与所述基准密文大小相等；若是，生成随机数，并根据所述随机数和所述随机数取值范围内的数值阈值的大小关系，确定该非基准密文的第二比较结果；若否，根据该非基准密文和所述基准密文的大小关系，确定该非基准密文的第二比较结果。

14、如权利要求 13 所述的装置，所述划分模块用于判断该基准密文的第一比较结果与该基准密文的第二比较结果是否相同；若是，根据该非基准密文的第一比较结果，确定该非基准密文划分到的子数组；若否，重新随机生成该基准密文的第三比较结果，并根据该基准密文的第三比较结果，确定该非基准密文划分到的子数组。

15、一种计算机可读存储介质，所述存储介质存储有计算机程序，所述计算机程序被处理器执行时实现上述权利要求 1~7 任一项所述的方法。

16、一种电子设备，包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序，所述处理器执行所述程序时实现上述权利要求 1~7 任一项所述的方法。