(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 111447072 B
(45)授权公告日 2022.04.15

(21)申请号 202010231558.6

(22)申请日 2020.03.27

(65)同一申请的已公布的文献号
申请公布号 CN 111447072 A

(43)申请公布日 2020.07.24

(73)专利权人 苏州链原信息科技有限公司
地址 215000 江苏省苏州市苏州工业园区若水路388号E1005室

(72)发明人 郭宇 孙志鹏 卢艺文 叶存 胡宇光

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

审查员 邱德洁

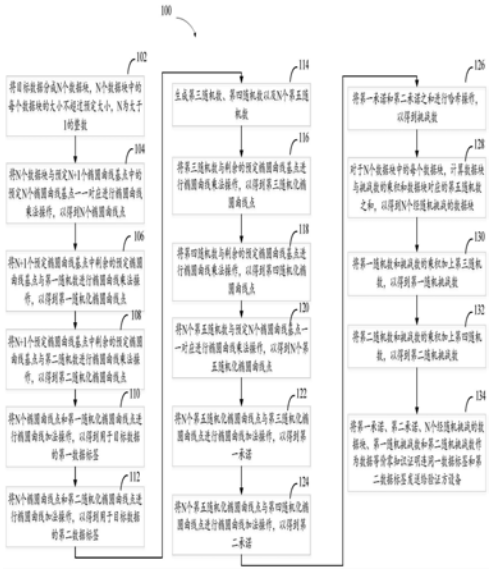
权利要求书2页 说明书9页 附图3页

(54)发明名称

用于生成数据等价零知识证明的方法、设备及存储介质

(57)摘要

根据本公开的示例实施例，提供了用于生成数据等价零知识证明的方法、电子设备及计算机存储介质。在该方法中，在数据方设备处，将目标数据分成N个数据块，基于N个数据块和预定N+1个椭圆曲线基点、第一随机数和第二随机数，生成用于目标数据的第一数据标签和第二数据标签，基于第三随机数、第四随机数以及N个第五随机数和预定N+1个椭圆曲线基点，得到第一承诺、第二承诺、N个经随机挑战的数据块、第一随机挑战数和第二随机挑战数，作为数据标签等价零知识证明连同第一数据标签和第二数据标签发送给验证方设备。由此，本发明能够零知识地验证两个数据标签所对应数据是否等价，而不泄露数据明文。



CN 111447072 B

1.一种用于生成数据等价零知识证明的方法,包括:

在数据方设备处,将目标数据分成N个数据块,所述N个数据块中的每个数据块的大小不超过预定大小,N为大于1的整数;

将所述N个数据块与预定N+1个椭圆曲线基点中的预定N个椭圆曲线基点一一对应进行椭圆曲线乘法操作,以得到N个椭圆曲线点;

将所述预定N+1个椭圆曲线基点中剩余的预定椭圆曲线基点与第一随机数进行椭圆曲线乘法操作,以得到第一随机化椭圆曲线点;

将所述预定N+1个椭圆曲线基点中剩余的预定椭圆曲线基点与第二随机数进行椭圆曲线乘法操作,以得到第二随机化椭圆曲线点;

将所述N个椭圆曲线点和所述第一随机化椭圆曲线点进行椭圆曲线加法操作,以得到用于所述目标数据的第一数据标签;

将所述N个椭圆曲线点和所述第二随机化椭圆曲线点进行椭圆曲线加法操作,以得到用于所述目标数据的第二数据标签;

生成第三随机数、第四随机数以及N个第五随机数;

将所述第三随机数与所述剩余的预定椭圆曲线基点进行椭圆曲线乘法操作,以得到第三随机化椭圆曲线点;

将所述第四随机数与所述剩余的预定椭圆曲线基点进行椭圆曲线乘法操作,以得到第四随机化椭圆曲线点;

将所述N个第五随机数与所述预定N个椭圆曲线基点一一对应进行椭圆曲线乘法操作,以得到N个第五随机化椭圆曲线点;

将所述N个第五随机化椭圆曲线点与所述第三随机化椭圆曲线点进行椭圆曲线加法操作,以得到第一承诺;

将所述N个第五随机化椭圆曲线点与所述第四随机化椭圆曲线点进行椭圆曲线加法操作,以得到第二承诺;

将所述第一承诺和所述第二承诺之和进行哈希操作,以得到挑战数;

对于所述N个数据块中的每个数据块,计算所述数据块与所述挑战数的乘积和所述数据块对应的第五随机数之和,以得到N个经随机挑战的数据块;

将所述第一随机数和所述挑战数的乘积加上所述第三随机数,以得到第一随机挑战数;

将所述第二随机数和所述挑战数的乘积加上所述第四随机数,以得到第二随机挑战数;以及

将所述第一承诺、所述第二承诺、所述N个经随机挑战的数据块、所述第一随机挑战数和所述第二随机挑战数作为数据等价零知识证明连同所述第一数据标签和所述第二数据标签发送给验证方设备。

2.根据权利要求1所述的方法,其中所述预定大小包括椭圆曲线的域宽度。

3.根据权利要求1所述的方法,其中所述预定N个椭圆曲线基点包括所述预定N+1个椭圆曲线基点中的前或后预定N个椭圆曲线基点。

4.一种用于验证数据等价的方法,包括:

在验证方设备处,从数据方设备接收第一数据标签、第二数据标签、第一承诺、第二承

诺、N个经随机挑战的数据块、第一随机挑战数和第二随机挑战数；

将所述第一承诺和所述第二承诺之和进行哈希操作，以得到挑战数；

将所述N个经随机挑战的数据块与预定N+1个椭圆曲线基点中的预定N个椭圆曲线基点一一对应进行椭圆曲线乘法操作，以得到N个椭圆曲线点；

将所述第一随机挑战数与所述预定N+1个椭圆曲线基点中剩余的预定椭圆曲线基点进行椭圆曲线乘法操作，以得到第一随机挑战椭圆曲线点；

将所述第二随机挑战数与所述预定N+1个椭圆曲线基点中剩余的预定椭圆曲线基点进行椭圆曲线乘法操作，以得到第二随机挑战椭圆曲线点；

将所述N个椭圆曲线点与所述第一随机挑战椭圆曲线点进行椭圆曲线加法，以得到第一待验证椭圆曲线点；

将所述N个椭圆曲线点与所述第二随机挑战椭圆曲线点进行椭圆曲线加法，以得到第二待验证椭圆曲线点；

将所述挑战数与所述第一数据标签进行椭圆曲线乘法的乘积和所述第一承诺相加，以得到经挑战的第一数据标签；

将所述挑战数与所述第二数据标签进行椭圆曲线乘法的乘积和所述第二承诺相加，以得到经挑战的第二数据标签；

响应于确定所述经挑战的第一数据标签等于所述第一待验证椭圆曲线点且所述经挑战的第二数据标签等于所述第二待验证椭圆曲线点，确定所述第一数据标签所对应的数据和所述第二数据标签所对应的数据等价。

5.根据权利要求4所述的方法，其中所述预定N个椭圆曲线基点包括所述预定N+1个椭圆曲线基点中的前或后预定N个椭圆曲线基点。

6.根据权利要求4所述的方法，所述第一数据标签、所述第二数据标签、所述第一承诺、所述第二承诺、所述N个经随机挑战的数据块、所述第一随机挑战数和所述第二随机挑战数根据权利要求1所述方法而生成。

7.一种电子设备，包括：

至少一个处理单元；以及

至少一个存储器，所述至少一个存储器被耦合到所述至少一个处理单元并且存储用于由所述至少一个处理单元执行的指令，所述指令当由所述至少一个处理单元执行时，使得所述设备执行根据权利要求1至6任一项所述的方法的步骤。

8.一种计算机可读存储介质，其上存储有计算机程序，所述计算机程序被机器执行时实现根据权利要求1至6中任一项所述的方法。

用于生成数据等价零知识证明的方法、设备及存储介质

技术领域

[0001] 本公开的实施例总体涉及信息处理领域，具体涉及用于生成数据等价零知识证明的方法、用于验证数据等价的方法、电子设备及计算机存储介质。

背景技术

[0002] 通过区块链对数据进行管理是区块链的常见场景。传统方案大多对数据进行哈希运算得到数据的摘要值，然后将摘要值作为数据的标签，提交到区块链保存。由于哈希运算是确定性运算，相同的数据会得到相同的哈希值，这样在链上有泄露机密信息的风险。

发明内容

[0003] 本公开的实施例提供了用于生成数据等价零知识证明的方法、用于验证数据等价的方法、电子设备及计算机存储介质，由此能够通过零知识证明验证数据标签所对应的数据具有等价性，而不泄露数据明文，提高了数据验证的安全性。

[0004] 在本公开的第一方面，提供了一种用于生成数据等价零知识证明的方法。该方法包括：在数据方设备处，将目标数据分成N个数据块，所述N个数据块中的每个数据块的大小不超过预定大小，N为大于1的整数；将所述N个数据块与预定N+1个椭圆曲线基点中的预定N个椭圆曲线基点一一对应进行椭圆曲线乘法操作，以得到N个椭圆曲线点；将所述预定N+1个椭圆曲线基点中剩余的预定椭圆曲线基点与第一随机数进行椭圆曲线乘法操作，以得到第一随机化椭圆曲线点；将所述预定N+1个椭圆曲线基点中剩余的预定椭圆曲线基点与第二随机数进行椭圆曲线乘法操作，以得到第二随机化椭圆曲线点；将所述N个椭圆曲线点和所述第一随机化椭圆曲线点进行椭圆曲线加法操作，以得到用于所述目标数据的第一数据标签；将所述N个椭圆曲线点和所述第二随机化椭圆曲线点进行椭圆曲线加法操作，以得到用于所述目标数据的第二数据标签；生成第三随机数、第四随机数以及N个第五随机数；将所述第三随机数与所述剩余的预定椭圆曲线基点进行椭圆曲线乘法操作，以得到第三随机化椭圆曲线点；将所述第四随机数与所述剩余的预定椭圆曲线基点进行椭圆曲线乘法操作，以得到第四随机化椭圆曲线点；将所述N个第五随机数与所述预定N个椭圆曲线基点一一对应进行椭圆曲线乘法操作，以得到N个第五随机化椭圆曲线点；将所述N个第五随机化椭圆曲线点与所述第三随机化椭圆曲线点进行椭圆曲线加法操作，以得到第一承诺；将所述N个第五随机化椭圆曲线点与所述第四随机化椭圆曲线点进行椭圆曲线加法操作，以得到第二承诺；将所述第一承诺和所述第二承诺之和进行哈希操作，以得到挑战数；对于所述N个数据块中的每个数据块，计算所述数据块与所述挑战数的乘积和所述数据块对应的第五随机数之和，以得到N个经随机挑战的数据块；将所述第一随机数和所述挑战数的乘积加上所述第三随机数，以得到第一随机挑战数；将所述第二随机数和所述挑战数的乘积加上所述第四随机数，以得到第二随机挑战数；以及将所述第一承诺、所述第二承诺、所述N个经随机挑战的数据块、所述第一随机挑战数和所述第二随机挑战数作为数据等价零知识证明连同所述第一数据标签和所述第二数据标签发送给验证方设备。

[0005] 在本公开的第二方面，提供了一种电子设备。该电子设备包括：至少一个处理单元；以及至少一个存储器，所述至少一个存储器被耦合到所述至少一个处理单元并且存储用于由所述至少一个处理单元执行的指令，所述指令当由所述至少一个处理单元执行时，使得所述设备执行根据本公开的第一方面所述的方法的步骤。

[0006] 在本公开的第三方面，提供了一种计算机可读存储介质，其上存储有计算机程序，所述计算机程序被机器执行时实现根据本公开的第一方面所述的方法。

[0007] 在本公开的第四方面，提供了一种用于验证数据等价的方法。该方法包括：在验证方设备处，从数据方设备接收第一数据标签、第二数据标签、第一承诺、第二承诺、N个经随机挑战的数据块、第一随机挑战数和第二随机挑战数；将所述第一承诺和所述第二承诺之和进行哈希操作，以得到挑战数；将所述N个经随机挑战的数据块与预定N+1个椭圆曲线基点中的预定N个椭圆曲线基点一一对应进行椭圆曲线乘法操作，以得到N个椭圆曲线点；将所述第一随机挑战数与所述预定N+1个椭圆曲线基点中剩余的预定椭圆曲线基点进行椭圆曲线乘法操作，以得到第一随机挑战椭圆曲线点；将所述第二随机挑战数与所述预定N+1个椭圆曲线基点中剩余的预定椭圆曲线基点进行椭圆曲线乘法操作，以得到第二随机挑战椭圆曲线点；将所述N个椭圆曲线点与所述第一随机挑战椭圆曲线点进行椭圆曲线加法，以得到第一待验证椭圆曲线点；将所述N个椭圆曲线点与所述第二随机挑战椭圆曲线点进行椭圆曲线加法，以得到第二待验证椭圆曲线点；将所述挑战数与所述第一数据标签进行椭圆曲线乘法的乘积和所述第一承诺相加，以得到经挑战的第一数据标签；将所述挑战数与所述第二数据标签进行椭圆曲线乘法的乘积和所述第二承诺相加，以得到经挑战的第二数据标签；如果确定所述经挑战的第一数据标签等于所述第一待验证椭圆曲线点且所述经挑战的第二数据标签等于所述第二待验证椭圆曲线点，则确定所述第一数据标签所对应的数据和所述第二数据标签所对应的数据等价。

[0008] 在本公开的第五方面，提供了一种电子设备。该电子设备包括：至少一个处理单元；以及至少一个存储器，所述至少一个存储器被耦合到所述至少一个处理单元并且存储用于由所述至少一个处理单元执行的指令，所述指令当由所述至少一个处理单元执行时，使得所述设备执行根据本公开的第四方面所述的方法的步骤。

[0009] 在本公开的第六方面，提供了一种计算机可读存储介质，其上存储有计算机程序，所述计算机程序被机器执行时实现根据本公开的第四方面所述的方法。

[0010] 提供发明内容部分是为了以简化的形式来介绍对概念的选择，它们在下文的具体实施方式中将被进一步描述。发明内容部分无意标识本公开的关键特征或必要特征，也无意限制本公开的范围。

附图说明

[0011] 通过结合附图对本公开示例性实施例进行更详细的描述，本公开的上述以及其它目的、特征和优势将变得更加明显，其中，在本公开示例性实施例中，相同的参考标号通常代表相同部件。

[0012] 图1示出了根据本公开的实施例的用于生成数据等价零知识证明的方法100的示意流程图；

[0013] 图2示出了根据本公开的实施例的用于验证数据等价的方法200的示意流程图；以

及

[0014] 图3示意性示出了适于用来实现本公开实施例的电子设备300的框图。

[0015] 在各个附图中，相同或对应的标号表示相同或对应的部分。

具体实施方式

[0016] 下面将参照附图更详细地描述本公开的优选实施例。虽然附图中显示了本公开的优选实施例，然而应该理解，可以以各种形式实现本公开而不应被这里阐述的实施例所限制。相反，提供这些实施例是为了使本公开更加透彻和完整，并且能够将本公开的范围完整地传达给本领域的技术人员。

[0017] 在本文中使用的术语“包括”及其变形表示开放性包括，即“包括但不限于”。除非特别申明，术语“或”表示“和/或”。术语“基于”表示“至少部分地基于”。术语“一个示例实施例”和“一个实施例”表示“至少一个示例实施例”。术语“另一实施例”表示“至少一个另外的实施例”。术语“第一”、“第二”等等可以指代不同的或相同的对象。下文还可能包括其他明确的和隐含的定义。应当理解，本文中的“数据标签”也可以称为“数据摘要”、“数据指纹”等。

[0018] 如上所述，由于哈希运算是确定性运算，相同的数据会得到相同的哈希值，这样在链上有泄露机密信息的风险。

[0019] 为了至少部分地解决上述问题以及其他潜在问题中的一个或者多个，本公开的示例实施例提出了一种用于生成数据等价零知识证明的方案。在该方案中，在数据方设备处，将目标数据分成N个数据块，N个数据块中的每个数据块的大小不超过预定大小，N为大于1的整数，将N个数据块与预定N+1个椭圆曲线基点中的预定N个椭圆曲线基点一一对应进行椭圆曲线乘法操作，以得到N个椭圆曲线点，将预定N+1个椭圆曲线基点中剩余的预定椭圆曲线基点与第一随机数进行椭圆曲线乘法操作，以得到第一随机化椭圆曲线点，将预定N+1个椭圆曲线基点中剩余的预定椭圆曲线基点与第二随机数进行椭圆曲线乘法操作，以得到第二随机化椭圆曲线点，将N个椭圆曲线点和第一随机化椭圆曲线点进行椭圆曲线加法操作，以得到用于目标数据的第一数据标签，将N个椭圆曲线点和第二随机化椭圆曲线点进行椭圆曲线加法操作，以得到用于目标数据的第二数据标签，生成第三随机数、第四随机数以及N个第五随机数，将第三随机数与剩余的预定椭圆曲线基点进行椭圆曲线乘法操作，以得到第三随机化椭圆曲线点，将第四随机数与剩余的预定椭圆曲线基点进行椭圆曲线乘法操作，以得到第四随机化椭圆曲线点，将N个第五随机数与预定N个椭圆曲线基点一一对应进行椭圆曲线乘法操作，以得到N个第五随机化椭圆曲线点，将N个第五随机化椭圆曲线点与第三随机化椭圆曲线点进行椭圆曲线加法操作，以得到第一承诺，将N个第五随机化椭圆曲线点与第四随机化椭圆曲线点进行椭圆曲线加法操作，以得到第二承诺，将第一承诺和第二承诺之和进行哈希操作，以得到挑战数，对于N个数据块中的每个数据块，计算数据块与挑战数的乘积和数据块对应的第五随机数之和，以得到N个经随机挑战的数据块，将第一随机数和挑战数的乘积加上第三随机数，以得到第一随机挑战数，将第二随机数和挑战数的乘积加上第四随机数，以得到第二随机挑战数，以及将第一承诺、第二承诺、N个经随机挑战的数据块、第一随机挑战数和第二随机挑战数作为数据等价零知识证明连同第一数据标签和第二数据标签发送给验证方设备。

[0020] 在上述方案中，通过加入随机数来生成数据标签来保护数据安全性，使得一份数据可产生不同数据标签，通过不同数据标签，任何第三方无法获知数据标签背后的数据的关联性，而通过提供零知识证明，可以让验证方验证不同数据标签对应的数据的等价性。此外，基于椭圆曲线的数据标签技术，通过椭圆曲线离散对数难题来保证数据标签本身的安全性；数据标签不超过预定大小，例如椭圆曲线的域宽度，因此其尺寸非常短小，适合各种区块链场景；由于采用了椭圆曲线基点对数据原文进行加密并对数据标签进行随机化，数据标签不会泄露数据原文的任何信息，实现信息隐藏的效果；数据标签保证唯一性，一旦数据标签上链，则与原始数据绑定，有效阻止恶意用户篡改原始数据。

[0021] 图1显示出了根据本公开的实施例的用于生成数据等价零知识证明的方法100的示意流程图。例如，方法100可以由数据方设备或如图3所示的电子设备300来执行。应当理解的是，方法100还可以包括未示出的附加框和/或可以省略所示出的框，本公开的范围在此方面不受限制。

[0022] 在框102处，在数据方设备处，将目标数据分成N个数据块，N个数据块中的每个数据块的大小不超过预定大小，N为大于1的整数。预定大小可以包括椭圆曲线的域宽度。例如，椭圆曲线的域宽度为256比特，则数据块的大小可以不超过256比特，例如不超过31字节。每个数据块的大小可以相同或不同。数据方设备例如但不限于终端设备、服务器等。本文中的目标数据包括但不限于例如位置数据、金融数据、健康数据、生物特征数据等等。

[0023] 在框104处，将N个数据块与预定N+1个椭圆曲线基点中的预定N个椭圆曲线基点一一对应进行椭圆曲线乘法操作，以得到N个椭圆曲线点。例如，将数据块数值化的结果与对应的预定椭圆曲线基点进行椭圆曲线乘法操作，也就是倍乘，得到该数据块所对应的椭圆曲线点。倍乘可以通过椭圆曲线加法操作来实现，例如椭圆曲线基点为G，2*G可以通过G+G来实现，3*G可以通过G+G+G来实现。预定N+1个椭圆曲线基点例如可以是预先确定并公开的或者数据方和验证方预先协调一致的。在一些实施例中，预定N个椭圆曲线基点包括预定N+1个椭圆曲线基点中的前或后预定N个椭圆曲线基点。例如，数据块表示为M1，M2到MN，后N个预定椭圆曲线基点表示为G1到GN，M1与G1对应，M2与G2对应，以及MN与GN对应，则N个椭圆曲线点表示为M1*G0，M2*G1到MN*GN，本文中“*”表示椭圆曲线乘法操作。

[0024] 在一些实施例中，N+1个预定椭圆曲线基点例如可以通过以下步骤生成：将N+1个不同值分别与预定字符串拼接得到的N+1个结果哈希到椭圆曲线上的点，以得到N+1个椭圆曲线基点。N+1个不同值可以包括N+1个连续整数，例如0到N，1到N+1等。预定字符串例如可以是任何公开的随机或不随机的字符串。

[0025] 备选地或者附加地，在一些实施例中，将N+1个不同值分别与预定字符串拼接得到的N+1个结果哈希到椭圆曲线上的点可以包括将N+1个不同值分别与预定字符串拼接，以得到N+1个结果，将N+1个结果进行哈希，以得到N+1个哈希结果，以及将N+1个哈希结果映射到椭圆曲线上的点，以得到N+1个椭圆曲线基点。将值与预定字符串拼接例如可以将值拼接在预定字符串之前或之后，得到拼接的字符串。哈希操作可以采用任何合适的哈希操作，例如SHA256等。将哈希结果映射到椭圆曲线上的点可以采用例如尝试递增法(Try and Increment method)、沙鲁沃斯汀算法(Shallue-Woestijne Algorithm)等方法或其他合适的群哈希方法。

[0026] 在框106处，将N+1个预定椭圆曲线基点中剩余的预定椭圆曲线基点与第一随机数

进行椭圆曲线乘法操作，以得到第一随机化椭圆曲线点。例如，剩余的椭圆曲线基点表示为G0，第一随机数表示为R1，则第一随机化椭圆曲线点表示为R1*G0。

[0027] 在框108处，将N+1个预定椭圆曲线基点中剩余的预定椭圆曲线基点与第二随机数进行椭圆曲线乘法操作，以得到第二随机化椭圆曲线点。例如，剩余的椭圆曲线基点表示为G0，第一随机数表示为R2，则第二随机化椭圆曲线点表示为R2*G0。

[0028] 在框110处，将N个椭圆曲线点和第一随机化椭圆曲线点进行椭圆曲线加法操作，以得到用于目标数据的第一数据标签。例如，第一数据标签L1＝R1*G0+M1*G1+M2*G2+M3*G3+M4*G4+…+MN*GN，本文中“+”表示椭圆曲线加法操作。两个椭圆曲线点进行加法操作可以通过计算这两个椭圆曲线点连线与椭圆曲线之间的交点关于X轴对称的点来得到。多个椭圆曲线点的加法操作可以拆分成两两椭圆曲线点的加法操作，最终得到一个椭圆曲线点，也就是用于目标数据的数据标签。

[0029] 在框112处，将N个椭圆曲线点和第二随机化椭圆曲线点进行椭圆曲线加法操作，以得到用于目标数据的第二数据标签。例如，第二数据标签L2＝R2*G0+M1*G1+M2*G2+M3*G3+M4*G4+…+MN*GN。

[0030] 在框114，处，生成第三随机数、第四随机数以及N个第五随机数。第三随机数例如表示为R3，第四随机数例如表示为R4，N个第五随机数例如表示为R51，R52，...，R5N。

[0031] 在框116处，将第三随机数与剩余的预定椭圆曲线基点进行椭圆曲线乘法操作，以得到第三随机化椭圆曲线点。例如剩余的预定椭圆曲线基点表示为G0，第三随机数例如表示为R3，则第三随机化椭圆曲线点表示为R3*G0。

[0032] 在框118处，将第四随机数与剩余的预定椭圆曲线基点进行椭圆曲线乘法操作，以得到第四随机化椭圆曲线点。例如剩余的预定椭圆曲线基点表示为G0，第四随机数例如表示为R4，则第四随机化椭圆曲线点表示为R4*G0。

[0033] 在框120处，将N个第五随机数与预定N个椭圆曲线基点一一对应进行椭圆曲线乘法操作，以得到N个第五随机化椭圆曲线点。例如，N个预定椭圆曲线基点表示为G1到GN，R51与G1对应，R52与G2对应，...，以及G5N与GN对应，N个第五随机化椭圆曲线点表示为R51*G1，R52*G2，...，R5N*GN。

[0034] 在框122处，将N个第五随机化椭圆曲线点与第三随机化椭圆曲线点进行椭圆曲线加法操作，以得到第一承诺。第一承诺C1例如表示为R3*G0+R51*G1+R52*G2+...+R5N*GN。

[0035] 在框124处，将N个第五随机化椭圆曲线点与第四随机化椭圆曲线点进行椭圆曲线加法操作，以得到第二承诺。第二承诺C2例如表示为R4*G0+R51*G1+R52*G2+...+R5N*GN。

[0036] 在框126处，将第一承诺和第二承诺之和进行哈希操作，以得到挑战数。挑战数E例如表示为hash(C1+C2)。这里的和为椭圆曲线加法之和，也就是第一承诺和第二承诺进行椭圆曲线加法操作得到的椭圆曲线点。对椭圆曲线点进行哈希操作可以包括将椭圆曲线点的X坐标或Y坐标进行哈希操作，得到哈希值作为挑战数。

[0037] 在框128处，对于N个数据块中的每个数据块，计算数据块与挑战数的乘积和数据块对应的第五随机数之和，以得到N个经随机挑战的数据块。例如，数据块M1与R51对应，数据块M2与R52对应，数据块MN与R5N，以此类推。N个经随机挑战的数据块例如表示为R51+E*M1，R52+E*M2，...，R5N+E*MN。

[0038] 在框130处，将第一随机数和挑战数的乘积加上第三随机数，以得到第一随机挑战

数。第一随机挑战数例如表示为R3+E*R1。

[0039] 在框132处，将第二随机数和挑战数的乘积加上第四随机数，以得到第二随机挑战数。第二随机挑战数例如表示为R4+E*R2。

[0040] 在框134处，将第一承诺、第二承诺、N个经随机挑战的数据块、第一随机挑战数和第二随机挑战数作为数据等价零知识证明连同一数据标签和第二数据标签发送给验证方设备。

[0041] 由此，通过加入随机数来生成数据标签来保护数据安全性，使得一份数据可产生不同数据标签，通过不同数据标签，任何第三方无法获知数据标签背后的数据的关联性，而通过提供零知识证明，可以让验证方验证不同数据标签对应的数据的等价性。此外，基于椭圆曲线的数据标签技术，通过椭圆曲线离散对数难题来保证数据标签本身的安全性；数据标签不超过预定大小，例如椭圆曲线的域宽度，因此其尺寸非常短小，适合各种区块链场景；由于采用了椭圆曲线基点对数据原文进行加密并对数据标签进行随机化，数据标签不会泄露数据原文的任何信息，实现信息隐藏的效果；数据标签保证唯一性，一旦数据标签上链，则与原始数据绑定，有效阻止恶意用户篡改原始数据。

[0042] 图2显示出了根据本公开的实施例的用于验证数据等价的方法200的示意流程图。例如，方法200可以由验证方设备或如图3所示的电子设备300来执行。应当理解的是，方法200还可以包括未示出的附加框和/或可以省略所示出的框，本公开的范围在此方面不受限制。

[0043] 在框202处，在验证方设备处，从数据方设备接收第一数据标签、第二数据标签、第一承诺、第二承诺、N个经随机挑战的数据块、第一随机挑战数和第二随机挑战数。验证方设备例如但不限于是终端设备、服务器等。

[0044] 在一些实施例中，第一数据标签、第二数据标签、第一承诺、第二承诺、N个经随机挑战的数据块、第一随机挑战数和第二随机挑战数可根据上述方法100而生成。

[0045] 在框204处，将第一承诺和第二承诺之和进行哈希操作，以得到挑战数。例如，第一承诺表示为C1，第二承诺表示为C2，则挑战数E＝hash(C1+C2)，详情可参见上文，这里不再赘述。

[0046] 在框206处，将N个经随机挑战的数据块与预定N+1个椭圆曲线基点中的预定N个椭圆曲线基点一一对应进行椭圆曲线乘法操作，以得到N个椭圆曲线点。在一些实施例中，预定N个椭圆曲线基点包括预定N+1个椭圆曲线基点中的前或后预定N个椭圆曲线基点。例如，N个经随机挑战的数据块表示为R51+E*M1，R52+E*M2，...，R5N+E*MN，分别与预定N个椭圆曲线基点G1，G2，....，GN一一对应，则N个椭圆曲线点表示为(R51+E*M1)*G1，(R52+E*M2)*G2，...，(R5N+E*MN)*GN。

[0047] 在框208处，将第一随机挑战数与预定N+1个椭圆曲线基点中剩余的预定椭圆曲线基点进行椭圆曲线乘法操作，以得到第一随机挑战椭圆曲线点。例如剩余的预定椭圆曲线基点表示为G0，第一随机挑战数表示为R3+E*R1，则第一随机挑战椭圆曲线点表示为(R3+E*R1)*G0。

[0048] 在框210处，将第二随机挑战数与预定N+1个椭圆曲线基点中剩余的预定椭圆曲线基点进行椭圆曲线乘法操作，以得到第二随机挑战椭圆曲线点。例如剩余的预定椭圆曲线基点表示为G0，第二随机挑战数表示为R4+E*R2，则第一随机挑战椭圆曲线点表示为(R4+E*

R2)*G0。

[0049] 在框212处，将N个椭圆曲线点与第一随机挑战椭圆曲线点进行椭圆曲线加法，以得到第一待验证椭圆曲线点。第一待验证椭圆曲线点例如表示为(R3+E*R1)*G0+(R51+E*M1)*G1+(R52+E*M2)*G2+...+(R5N+E*MN)*GN。

[0050] 在框214处，将N个椭圆曲线点与第二随机挑战椭圆曲线点进行椭圆曲线加法，以得到第二待验证椭圆曲线点。第二待验证椭圆曲线点例如表示为(R4+E*R2)*G0+(R51+E*M1)*G1+(R52+E*M2)*G2+...+(R5N+E*MN)*GN。

[0051] 在框216处，将挑战数与第一数据标签进行椭圆曲线乘法的乘积和第一承诺相加，以得到经挑战的第一数据标签。第一数据标签例如表示为L1，经挑战的第一数据标签例如表示为C1+E*L1＝R3*G0+R51*G1+R52*G2+...+R5N*GN+E*(R1*G0+M1*G1+M2*G2+M3*G3+M4*G4+…+MN*GN)＝(R3+E*R1)*G0+(R51+E*M1)*G1+(R52+E*M2)*G2+…+(R5N+E*MN)*GN。

[0052] 在框218处，将挑战数与第二数据标签进行椭圆曲线乘法的乘积和第二承诺相加，以得到经挑战的第二数据标签。第二数据标签例如表示为L2，经挑战的第二数据标签例如表示为C2+E*L2＝R4*G0+R51*G1+R52*G2+...+R5N*GN+E*(R2*G0+M1*G1+M2*G2+M3*G3+M4*G4+…+MN*GN)＝(R4+E*R2)*G0+(R51+E*M1)*G1+(R52+E*M2)*G2+…+(R5N+E*MN)*GN。

[0053] 在框220处，确定是否经挑战的第一数据标签等于第一待验证椭圆曲线点且经挑战的第二数据标签等于第二待验证椭圆曲线点。从上面的表达式可以看出，如果第一数据标签对应的数据和第二数据标签对应的数据等价，那么经挑战的第一数据标签等于第一待验证椭圆曲线点以及经挑战的第二数据标签等于第二待验证椭圆曲线点。

[0054] 如果在框220处确定经挑战的第一数据标签等于第一待验证椭圆曲线点且经挑战的第二数据标签等于第二待验证椭圆曲线点，则在框222处确定第一数据标签所对应的数据和第二数据标签所对应的数据等价。

[0055] 由此，能够基于数据方设备提供的零知识证明，验证两个数据标签对应的数据的等价性，而无需数据方设备泄露数据明文信息，提高了数据验证的安全性，保证数据隐私，并且数据等价性判断的计算量很小。

[0056] 图3示意性示出了适于用来实现本公开实施例的电子设备300的框图。上文所述的数据方设备和验证方设备可由电子设备300实现。如图所示，设备300包括中央处理单元(CPU)301，其可以根据存储在只读存储器(ROM)302中的计算机程序指令或者从存储单元308加载到随机访问存储器(RAM)303中的计算机程序指令，来执行各种适当的动作和处理。在RAM303中，还可存储设备300操作所需的各种程序和数据。CPU 301、ROM 302以及RAM303通过总线304彼此相连。输入/输出(I/O)接口305也连接至总线304。

[0057] 设备300中的多个部件连接至I/O接口305，包括：输入单元306，例如键盘、鼠标等；输出单元307，例如各种类型的显示器、扬声器等；存储单元308，例如磁盘、光盘等；以及通信单元309，例如网卡、调制解调器、无线通信收发机等。通信单元309允许设备300通过诸如因特网的计算机网络和/或各种电信网络与其他设备交换信息/数据。

[0058] 处理单元301执行上文所描述的各个方法和处理，例如执行方法100-200。例如，在一些实施例中，方法100-200可被实现为计算机软件程序，其被存储于机器可读介质，例如存储单元308。在一些实施例中，计算机程序的部分或者全部可以经由ROM302和/或通信单元309而被载入和/或安装到设备300上。当计算机程序加载到RAM 303并由CPU 301执行时，

可以执行上文描述的方法100-200的一个或多个操作。备选地，在其他实施例中，CPU 301可以通过其他任何适当的方式(例如，借助于固件)而被配置为执行方法100-200的一个或多个动作。

[0059] 本公开可以是方法、装置、系统和/或计算机程序产品。计算机程序产品可以包括计算机可读存储介质，其上载有用于执行本公开的各个方面的计算机可读程序指令。

[0060] 计算机可读存储介质可以是可以保持和存储由指令执行设备使用的指令的有形设备。计算机可读存储介质例如可以是——但不限于——电存储设备、磁存储设备、光存储设备、电磁存储设备、半导体存储设备或者上述的任意合适的组合。计算机可读存储介质的更具体的例子(非穷举的列表)包括：便携式计算机盘、硬盘、随机存取存储器(RAM)、只读存储器(ROM)、可擦式可编程只读存储器(EPROM或闪存)、静态随机存取存储器(SRAM)、便携式压缩盘只读存储器(CD-ROM)、数字多功能盘(DVD)、记忆棒、软盘、机械编码设备、例如其上存储有指令的打孔卡或凹槽内凸起结构、以及上述的任意合适的组合。这里所使用的计算机可读存储介质不被解释为瞬时信号本身，诸如无线电波或者其他自由传播的电磁波、通过波导或其他传输媒介传播的电磁波(例如，通过光纤电缆的光脉冲)、或者通过电线传输的电信号。

[0061] 这里所描述的计算机可读程序指令可以从计算机可读存储介质下载到各个计算/处理设备，或者通过网络、例如因特网、局域网、广域网和/或无线网下载到外部计算机或外部存储设备。网络可以包括铜传输电缆、光纤传输、无线传输、路由器、防火墙、交换机、网关计算机和/或边缘服务器。每个计算/处理设备中的网络适配卡或者网络接口从网络接收计算机可读程序指令，并转发该计算机可读程序指令，以供存储在各个计算/处理设备中的计算机可读存储介质中。

[0062] 用于执行本公开操作的计算机程序指令可以是汇编指令、指令集架构(ISA)指令、机器指令、机器相关指令、微代码、固件指令、状态设置数据、或者以一种或多种编程语言的任意组合编写的源代码或目标代码，编程语言包括面向对象的编程语言—诸如Smalltalk、C++等，以及常规的过程式编程语言—诸如“C”语言或类似的编程语言。计算机可读程序指令可以完全地在用户计算机上执行、部分地在用户计算机上执行、作为一个独立的软件包执行、部分在用户计算机上部分在远程计算机上执行、或者完全在远程计算机或服务器上执行。在涉及远程计算机的情形中，远程计算机可以通过任意种类的网络—包括局域网(LAN)或广域网(WAN)—连接到用户计算机，或者，可以连接到外部计算机(例如利用因特网服务提供商来通过因特网连接)。在一些实施例中，通过利用计算机可读程序指令的状态信息来个性化定制电子电路，例如可编程逻辑电路、现场可编程门阵列(FPGA)或可编程逻辑阵列(PLA)，该电子电路可以执行计算机可读程序指令，从而实现本公开的各个方面。

[0063] 这里参照根据本公开实施例的方法、装置(系统)和计算机程序产品的流程图和/或框图描述了本公开的各个方面。应当理解，流程图和/或框图的每个方框以及流程图和/或框图中各方框的组合，都可以由计算机可读程序指令实现。

[0064] 这些计算机可读程序指令可以提供给通用计算机、专用计算机或其它可编程数据处理装置的处理单元，从而生产出一种机器，使得这些指令在通过计算机或其它可编程数据处理装置的处理单元执行时，产生了实现流程图和/或框图中的一个或多个方框中规定的功能/动作的装置。也可以把这些计算机可读程序指令存储在计算机可读存储介质中，这

些指令使得计算机、可编程数据处理装置和/或其他设备以特定方式工作，从而，存储有指令的计算机可读介质则包括一个制造品，其包括实现流程图和/或框图中的一个或多个方框中规定的功能/动作的各个方面的指令。

[0065] 也可以把计算机可读程序指令加载到计算机、其它可编程数据处理装置、或其它设备上，使得在计算机、其它可编程数据处理装置或其它设备上执行一系列操作步骤，以产生计算机实现的过程，从而使得在计算机、其它可编程数据处理装置、或其它设备上执行的指令实现流程图和/或框图中的一个或多个方框中规定的功能/动作。

[0066] 附图中的流程图和框图显示了根据本公开的多个实施例的系统、方法和计算机程序产品的可能实现的体系架构、功能和操作。在这点上，流程图或框图中的每个方框可以代表一个模块、程序段或指令的一部分，模块、程序段或指令的一部分包含一个或多个用于实现规定的逻辑功能的可执行指令。在有些作为替换的实现中，方框中所标注的功能也可以以不同于附图中所标注的顺序发生。例如，两个连续的方框实际上可以基本并行地执行，它们有时也可以按相反的顺序执行，这依所涉及的功能而定。也要注意的是，框图和/或流程图中的每个方框、以及框图和/或流程图中的方框的组合，可以用执行规定的功能或动作的专用的基于硬件的系统来实现，或者可以用专用硬件与计算机指令的组合来实现。

[0067] 以上已经描述了本公开的各实施例，上述说明是示例性的，并非穷尽性的，并且也不限于所披露的各实施例。在不偏离所说明的各实施例的范围和精神的情况下，对于本技术领域的普通技术人员来说许多修改和变更都是显而易见的。本文中所用术语的选择，旨在最好地解释各实施例的原理、实际应用或对市场中的技术的技术改进，或者使本技术领域的其它普通技术人员能理解本文披露的各实施例。

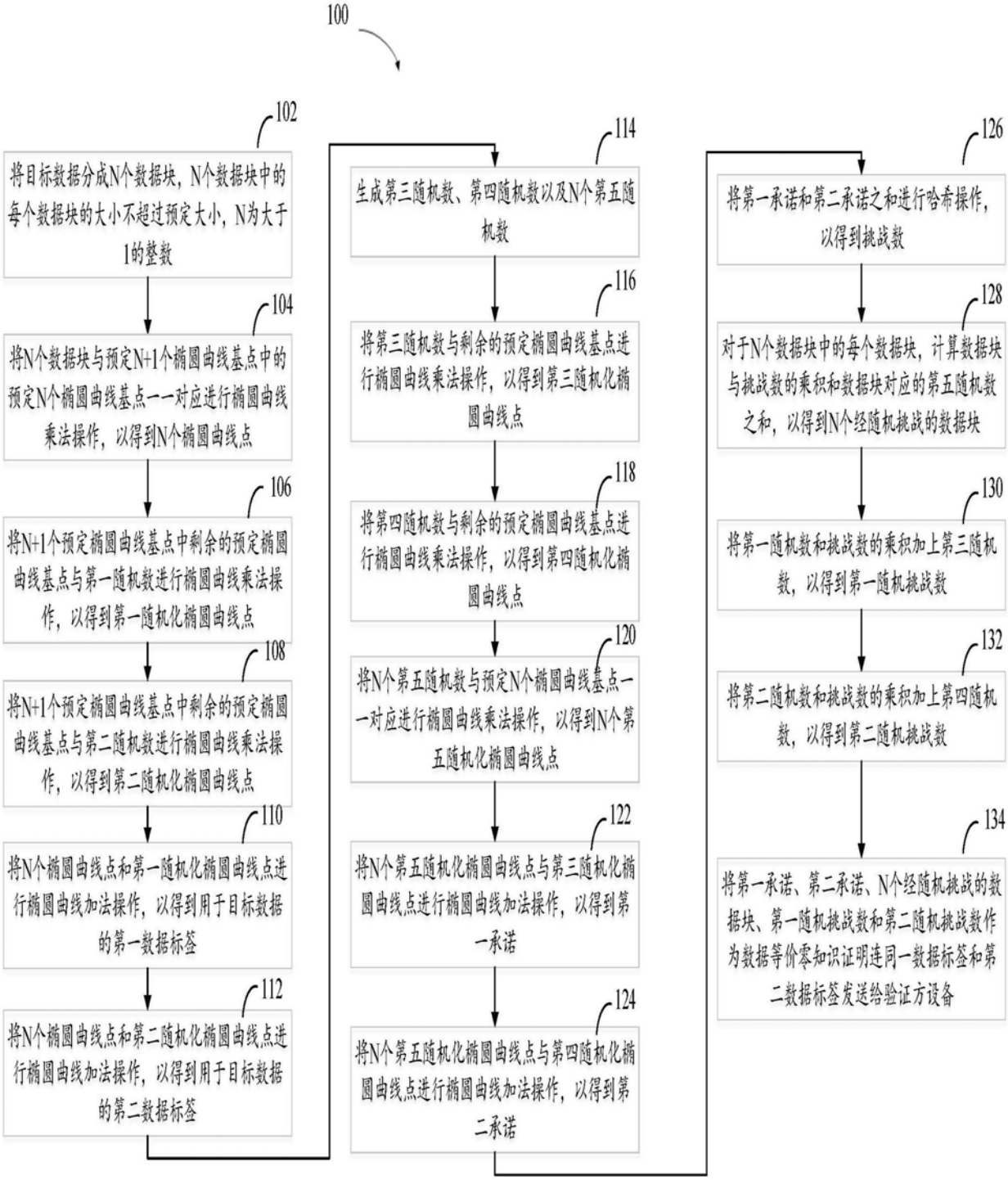

100
102
将目标数据分成N个数据块，N个数据块中的每个数据块的大小不超过预定大小，N为大于1的整数
104
将N个数据块与预定N+1个椭圆曲线基点中的预定N个椭圆曲线基点一一对应进行椭圆曲线乘法操作，以得到N个椭圆曲线点
106
将N+1个预定椭圆曲线基点中剩余的预定椭圆曲线基点与第一随机数进行椭圆曲线乘法操作，以得到第一随机化椭圆曲线点
108
将N+1个预定椭圆曲线基点中剩余的预定椭圆曲线基点与第二随机数进行椭圆曲线乘法操作，以得到第二随机化椭圆曲线点
110
将N个椭圆曲线点和第一随机化椭圆曲线点进行椭圆曲线加法操作，以得到用于目标数据的第一数据标签
112
将N个椭圆曲线点和第二随机化椭圆曲线点进行椭圆曲线加法操作，以得到用于目标数据的第二数据标签
114
生成第三随机数、第四随机数以及N个第五随机数
116
将第三随机数与剩余的预定椭圆曲线基点进行椭圆曲线乘法操作，以得到第三随机化椭圆曲线点
118
将第四随机数与剩余的预定椭圆曲线基点进行椭圆曲线乘法操作，以得到第四随机化椭圆曲线点
120
将N个第五随机数与预定N个椭圆曲线基点一一对应进行椭圆曲线乘法操作，以得到N个第五随机化椭圆曲线点
122
将N个第五随机化椭圆曲线点与第三随机化椭圆曲线点进行椭圆曲线加法操作，以得到第一承诺
124
将N个第五随机化椭圆曲线点与第四随机化椭圆曲线点进行椭圆曲线加法操作，以得到第二承诺
126
将第一承诺和第二承诺之和进行哈希操作，以得到挑战数
128
对于N个数据块中的每个数据块，计算数据块与挑战数的乘积和数据块对应的第五随机数之和，以得到N个经随机挑战的数据块
130
将第一随机数和挑战数的乘积加上第三随机数，以得到第一随机挑战数
132
将第二随机数和挑战数的乘积加上第四随机数，以得到第二随机挑战数
134
将第一承诺、第二承诺、N个经随机挑战的数据块、第一随机挑战数和第二随机挑战数作为数据等价零知识证明连同一数据标签和第二数据标签发送给验证方设备

图1

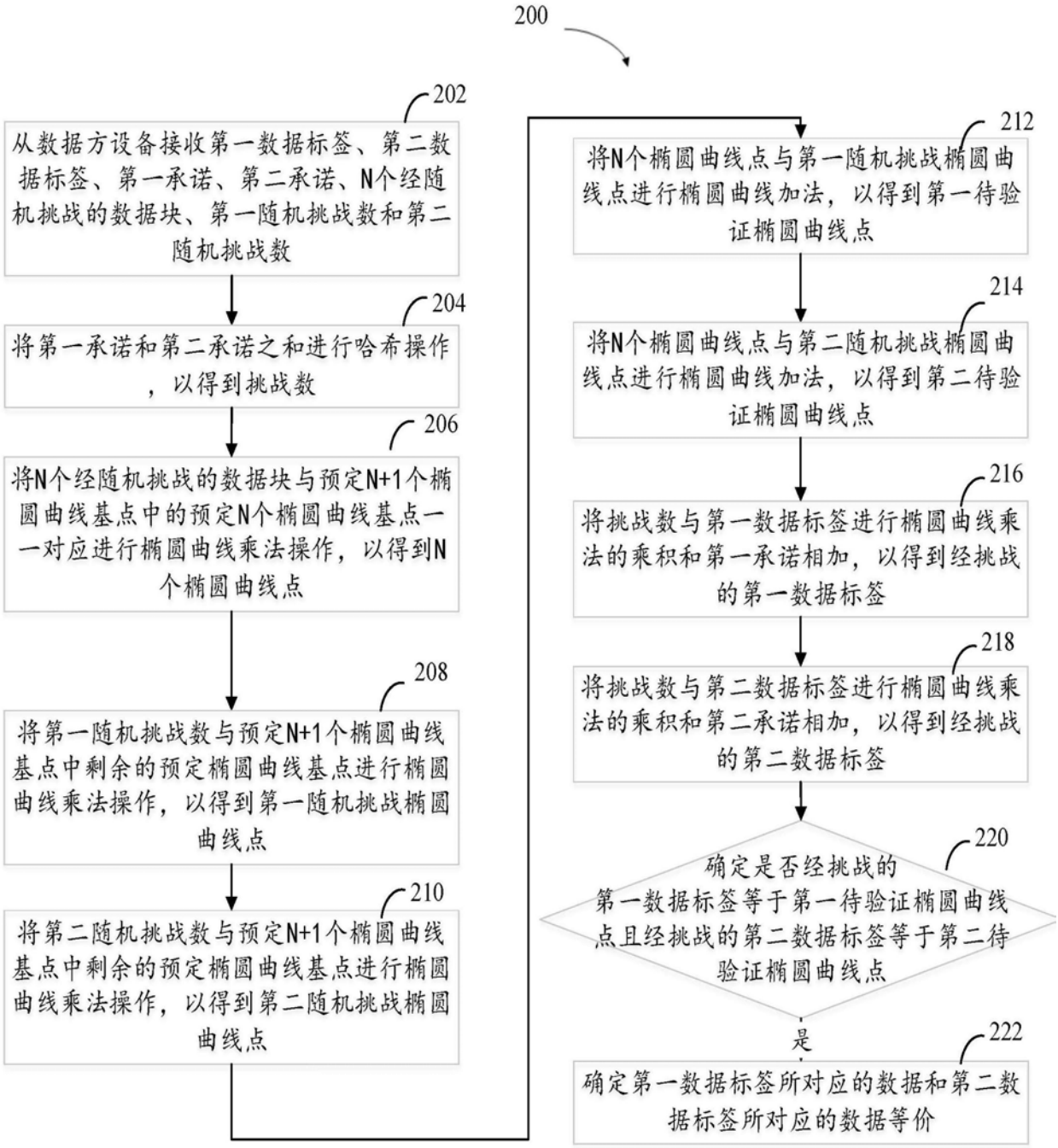

200
202
从数据方设备接收第一数据标签、第二数据标签、第一承诺、第二承诺、N个经随机挑战的数据块、第一随机挑战数和第二随机挑战数
204
将第一承诺和第二承诺之和进行哈希操作，以得到挑战数
206
将N个经随机挑战的数据块与预定N+1个椭圆曲线基点中的预定N个椭圆曲线基点一一对应进行椭圆曲线乘法操作，以得到N个椭圆曲线点
208
将第一随机挑战数与预定N+1个椭圆曲线基点中剩余的预定椭圆曲线基点进行椭圆曲线乘法操作，以得到第一随机挑战椭圆曲线点
210
将第二随机挑战数与预定N+1个椭圆曲线基点中剩余的预定椭圆曲线基点进行椭圆曲线乘法操作，以得到第二随机挑战椭圆曲线点
212
将N个椭圆曲线点与第一随机挑战椭圆曲线点进行椭圆曲线加法，以得到第一待验证椭圆曲线点
214
将N个椭圆曲线点与第二随机挑战椭圆曲线点进行椭圆曲线加法，以得到第二待验证椭圆曲线点
216
将挑战数与第一数据标签进行椭圆曲线乘法的乘积和第一承诺相加，以得到经挑战的第一数据标签
218
将挑战数与第二数据标签进行椭圆曲线乘法的乘积和第二承诺相加，以得到经挑战的第二数据标签
220
确定是否经挑战的第一数据标签等于第一待验证椭圆曲线点且经挑战的第二数据标签等于第二待验证椭圆曲线点
是
222
确定第一数据标签所对应的数据和第二数据标签所对应的数据等价

图2

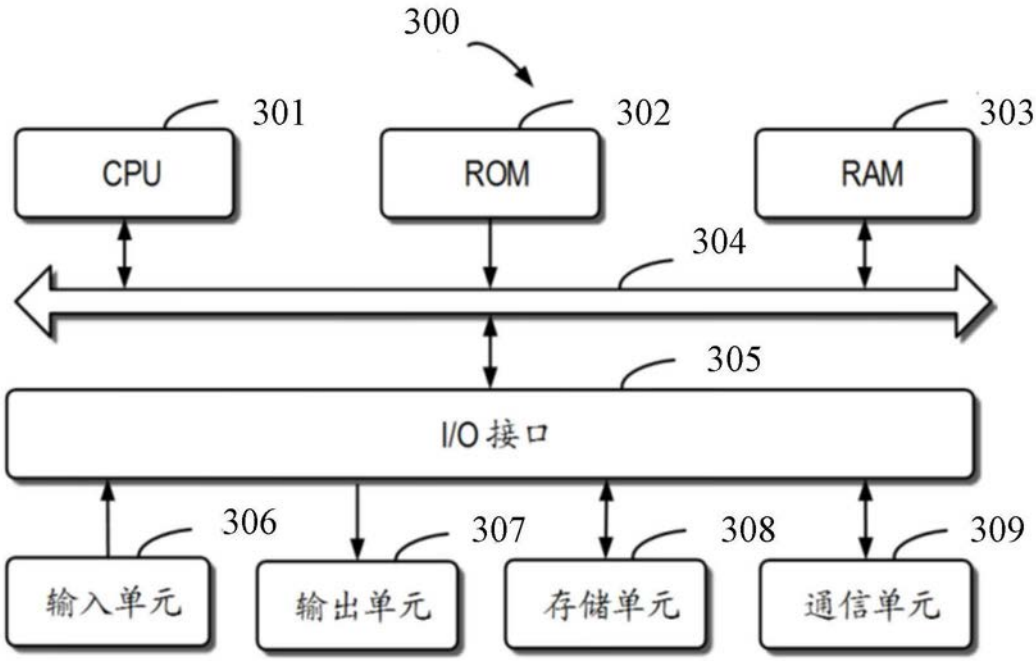

300
301
CPU
302
ROM
303
RAM
304
305
I/O 接口
306
输入单元
307
输出单元
308
存储单元
309
通信单元

图3