(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 111292461 A
(43)申请公布日 2020.06.16

(21)申请号 201811492711.X

(22)申请日 2018.12.07

(71)申请人 华为技术有限公司
地址 518129 广东省深圳市龙岗区坂田华为总部办公楼

(72)发明人 江山 曹建农 林钦亮

(74)专利代理机构 北京同立钧成知识产权代理有限公司 11205
代理人 张晓霞 刘芳

(51)Int.Cl.
G07C 13/00(2006.01)

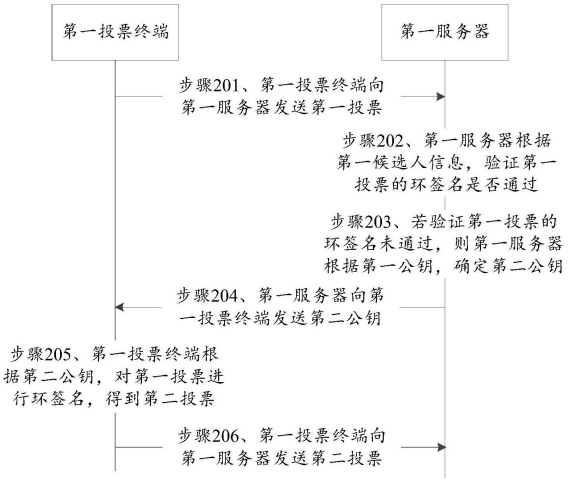
权利要求书3页 说明书18页 附图3页

(54)发明名称

电子投票方法、装置和存储介质

(57)摘要

本申请提供一种电子投票方法、装置和存储介质，该方法包括：接收第一投票终端发送的第一投票；所述第一投票为经过环签名后的投票，所述第一投票中包括第一候选人信息和与所述第一候选人信息对应的多个投票人的第一公钥；根据所述第一候选人信息，验证所述第一投票的环签名是否通过；若验证所述第一投票的环签名未通过，则根据所述第一公钥，确定第二公钥；向所述第一投票终端发送所述第二公钥，并接收所述第一投票终端发送的第二投票，所述第二投票为所述第一投票终端根据所述第二公钥对所述第一投票重新进行环签名后的投票。本申请提供的电子投票方法、装置和存储介质可以确保投票人的投票信息无法被推断出来，以保证投票的匿名性。



CN 111292461 A

1.一种电子投票方法,其特征在于,应用于第一服务器,所述方法包括:

接收第一投票终端发送的第一投票;所述第一投票为经过环签名后的投票,所述第一投票中包括第一候选人信息和与所述第一候选人信息对应的多个投票人的第一公钥;

根据所述第一候选人信息,验证所述第一投票的环签名是否通过;

若验证所述第一投票的环签名未通过,则根据所述第一公钥,确定第二公钥;

向所述第一投票终端发送所述第二公钥,并接收所述第一投票终端发送的第二投票,所述第二投票为所述第一投票终端根据所述第二公钥对所述第一投票重新进行环签名后的投票。

2.根据权利要求1所述的方法,其特征在于,所述根据所述第一候选人信息,验证所述第一投票的环签名是否通过,包括:

获取第一投票集合,所述第一投票集合中包括所述第一投票,以及除所述第一投票终端之外的其他多个第二投票终端发送的第二投票;所述第二投票中包括第二候选人信息和与所述第二候选人信息对应的多个投票人的第三公钥;

遍历所述第一投票集合中的所有候选人信息,在所述第一投票集合中删除与任一候选人信息对应的第一投票人的第四公钥,得到多个第二投票集合;所述第一投票人为所有投票人中的任意一个;所述第四公钥为所述第一公钥和所述第三公钥中的一个;

根据所述多个第二投票集合,验证所述第一投票的环签名是否通过。

3.根据权利要求2所述的方法,其特征在于,所述根据所述多个第二投票集合,验证所述第一投票的环签名是否通过,包括:

分别对所述多个第二投票集合中的每个第二投票集合构造无向图;

判断每个所述无向图的最大流是否均等于所述第一投票集合中投票的数量;

若每个所述无向图的最大流均等于所述第一投票集合中所述投票的数量,则确定所述第一投票的环签名通过;

若存在至少一个所述无向图的最大流不等于所述第一投票集合中所述投票的数量,则确定所述第一投票的环签名未通过。

4.根据权利要求1-3任一项所述的方法,其特征在于,所述根据所述第一公钥,确定第二公钥,包括:

从除所述第一公钥之外的其他公钥中,确定所述第二公钥。

5.根据权利要求3所述的方法,其特征在于,对所述第二投票集合构造无向图,包括:

分别确定所述第二投票集合中的所有第三候选人信息以及所有第二投票人的公钥;

根据所述第三候选人信息和所述第二投票人的公钥,构造所述无向图。

6.根据权利要求5所述的方法,其特征在于,所述根据所述第三候选人信息和所述第二投票人的公钥,构造所述无向图,包括:

将所述第二投票人的公钥确定为第一节点;

将所述第三候选人信息确定为第二节点;

分别构造所述第一节点和汇点之间的边,以及所述第二节点和源点之间的边;

分别构造各所述第二节点和与所述第二节点对应的所述第一节点之间的边,得到所述无向图。

7.根据权利要求1-6任一项所述的方法,其特征在于,所述接收所述第一投票终端发送

的第二投票之后，所述方法还包括：

向多个第二服务器发送所述第二投票。

8.一种电子投票方法，其特征在于，应用于投票终端，所述方法包括：

向第一服务器发送经过环签名后的第一投票，所述第一投票中包括第一候选人信息和与所述第一候选人信息对应的多个投票人的第一公钥；

接收所述第一服务器发送的第二公钥，所述第二公钥为所述第一服务器在根据所述第一候选人信息验证所述第一投票的环签名未通过时发送的；

根据所述第二公钥，对所述第一投票进行环签名，得到第二投票；

向所述第一服务器发送所述第二投票。

9.根据权利要求8所述的方法，其特征在于，所述向第一服务器发送经过环签名后的第一投票，包括：

获取除所述投票终端对应的投票人之外的其他n个投票人的公钥；其中，n为正整数；

根据所述n个公钥、所述投票终端对应的投票人的公钥和私钥，对第一投票进行环签名，得到环签名后的第一投票；

向所述第一服务器发送所述环签名后的第一投票。

10.根据权利要求9所述的方法，其特征在于，所述获取除所述投票终端对应的投票人之外的其他投票人的n个公钥，包括：

向多个第二服务器发送请求消息；

接收各所述第二服务器发送的响应消息，所述响应消息中包括所述n个公钥。

11.一种电子投票装置，其特征在于，包括：

接收单元，用于接收第一投票终端发送的第一投票；所述第一投票为经过环签名后的投票，所述第一投票中包括第一候选人信息和与所述第一候选人信息对应的多个投票人的第一公钥；

处理单元，用于根据所述第一候选人信息，验证所述第一投票的环签名是否通过；

所述处理单元，还用于在验证所述第一投票的环签名未通过时，根据所述第一公钥，确定第二公钥；

发送单元，用于向所述第一投票终端发送所述第二公钥；

所述接收单元，还用于接收所述第一投票终端发送的第二投票，所述第二投票为所述第一投票终端根据所述第二公钥对所述第一投票重新进行环签名后的投票。

12.根据权利要求11所述的装置，其特征在于，所述处理单元，具体用于：

获取第一投票集合，所述第一投票集合中包括所述第一投票，以及除所述第一投票终端之外的其他多个第二投票终端发送的第二投票；所述第二投票中包括第二候选人信息和与所述第二候选人信息对应的多个投票人的第三公钥；

遍历所述第一投票集合中的所有候选人信息，在所述第一投票集合中删除与任一候选人信息对应的第一投票人的第四公钥，得到多个第二投票集合；所述第一投票人为所有投票人中的任意一个；所述第四公钥为所述第一公钥和所述第三公钥中的一个；

根据所述多个第二投票集合，验证所述第一投票的环签名是否通过。

13.根据权利要求12所述的装置，其特征在于，所述处理单元，具体用于：

分别对所述多个第二投票集合中的每个第二投票集合构造无向图；

判断每个所述无向图的最大流是否均等于所述第一投票集合中投票的数量；

若每个所述无向图的最大流均等于所述第一投票集合中所述投票的数量，则确定所述第一投票的环签名通过；

若存在至少一个所述无向图的最大流不等于所述第一投票集合中所述投票的数量，则确定所述第一投票的环签名未通过。

14.根据权利要求11-13任一项所述的装置，其特征在于，所述处理单元，具体用于：

从除所述第一公钥之外的其他公钥中，确定所述第二公钥。

15.根据权利要求13所述的装置，其特征在于，所述处理单元，具体用于：

分别确定所述第二投票集合中的所有第三候选人信息以及所有第二投票人的公钥；

根据所述第三候选人信息和所述第二投票人的公钥，构造所述无向图。

16.根据权利要求15所述的装置，其特征在于，所述处理单元，具体用于：

将所述第二投票人的公钥确定为第一节点；

将所述第三候选人信息确定为第二节点；

分别构造所述第一节点和汇点之间的边，以及所述第二节点和源点之间的边；

分别构造各所述第二节点和与所述第二节点对应的所述第一节点之间的边，得到所述无向图。

17.根据权利要求11-16任一项所述的装置，其特征在于，

所述发送单元，还用于向多个第二服务器发送所述第二投票。

18.一种电子投票装置，其特征在于，包括：

发送单元，用于向第一服务器发送经过环签名后的第一投票，所述第一投票中包括第一候选人信息和与所述第一候选人信息对应的多个投票人的第一公钥；

接收单元，用于接收所述第一服务器发送的第二公钥，所述第二公钥为所述第一服务器在根据所述第一候选人信息验证所述第一投票的环签名未通过时发送的；

处理单元，用于根据所述第二公钥，对所述第一投票进行环签名，得到第二投票；

所述发送单元，用于向所述第一服务器发送所述第二投票。

19.根据权利要求18所述的装置，其特征在于，所述发送单元，具体用于：

获取除所述投票终端对应的投票人之外的其他n个投票人的公钥；其中，n为正整数；

根据所述n个公钥、所述投票终端对应的投票人的公钥和私钥，对第一投票进行环签名，得到环签名后的第一投票；

向所述第一服务器发送所述环签名后的第一投票。

20.根据权利要求19所述的装置，其特征在于，

所述发送单元，还用于向多个第二服务器发送请求消息；

所述接收单元，还用于接收各所述第二服务器发送的响应消息，所述响应消息中包括所述n个公钥。

电子投票方法、装置和存储介质

技术领域

[0001] 本申请实施例涉及区块链技术领域，尤其涉及一种电子投票方法、装置和存储介质。

背景技术

[0002] 随着互联网技术以及现代密码学技术的发展，电子投票作为一种新的投票方式，逐渐得到社会的关注，电子投票与传统投票相比，其优势在于计票的快捷准确、人力和开支的节省以及投票的易用性等方面。

[0003] 现有技术中，通常采用固定分组环签名的方式或随机分组环签名的方式进行投票，其中，对于固定分组环签名的投票方式，整个投票过程可以包括如下步骤：(1)投票装置向身份认证中心发送身份信息；(2)身份认证中心验证身份信息并向投票装置返回认证结果；(3)投票装置将认证结果发送给投票中心；(4)投票中心在确认认证结果为认证通过后，将n个投票人分成固定的k组，并向投票装置发送投票和投票人所在分组信息；(5)投票中心将登记信息发送给分布式账本，其中，登记信息中包括投票人身份信息认证结果、投票人公钥和由投票中心签名的信息；(6)分布式账本记录登记信息；(7)投票装置使用其所在分组的所有公钥和自己的私钥对投票信息进行环签名并发送投票；(8)监票中心核实收到的投票并发送给分布式账本；(9)分布式账本记录投票。

[0004] 对于随机分组环签名的投票方式，整个投票过程可以包括如下步骤：(1)投票装置向身份认证中心发送身份信息；(2)身份认证中心验证身份信息并向投票装置返回认证结果；(3)投票装置将认证结果发送给投票中心；(4)投票中心在确认认证结果为认证通过后，从已有投票人中随机选取k个，并将这k个投票人的公钥信息和投票发送给投票装置；(5)投票中心将登记信息发送给分布式账本，其中，登记信息中包括投票人身份信息认证结果、投票人公钥和由投票中心签名的信息；(6)分布式账本记录登记信息；(7)投票装置使用收到的k个公钥和自己的私钥对投票信息进行环签名并向监票中心发送投票；(8)监票中心核实收到的投票并发送给分布式账本；(9)分布式账本记录投票。

[0005] 然而，在上述两种投票方式中，当同一分组内的投票结果相同时，每个投票人的投票结果会被推断出来，例如：假设某一分组内包括A、B和C三个投票人，且候选人X得到了三张投票，则可以推断出A、B和C三个投票人均投了候选人X。因此，上述两种投票方式均无法保证投票过程的匿名性。

发明内容

[0006] 本申请实施例提供一种电子投票方法、装置和存储介质，可以确保投票人的投票信息无法被推断出来，以保证投票的匿名性。

[0007] 本申请第一方面提供一种电子投票方法，应用于第一服务器，所述方法包括：

[0008] 接收第一投票终端发送的第一投票；所述第一投票为经过环签名后的投票，所述第一投票中包括第一候选人信息和与所述第一候选人信息对应的多个投票人的第一公钥；

[0009] 根据所述第一候选人信息，验证所述第一投票的环签名是否通过；

[0010] 若验证所述第一投票的环签名未通过，则根据所述第一公钥，确定第二公钥；

[0011] 向所述第一投票终端发送所述第二公钥，并接收所述第一投票终端发送的第二投票，所述第二投票为所述第一投票终端根据所述第二公钥对所述第一投票重新进行环签名后的投票。

[0012] 在本方案中，第一候选人是指第一投票中所投的被投票人，而且，每一张投票中只能包括有一个候选人信息。另外，与第一候选人信息对应的多个投票人的第一公钥，是指第一投票终端对投票进行环签名时所使用的公钥。

[0013] 另外，若验证第一投票的环签名未通过，则说明可以根据第一投票推断出投票人的投票信息，也即第一投票不满足匿名性。

[0014] 在上述方案中，由于第一服务器在接收到第一投票终端发送的经过环签名后的第一投票后，将验证该第一投票的环签名是否通过，也即验证该第一投票是否能够保证投票的匿名性，若验证未通过，则第一服务器将确定第二公钥，第一投票终端将根据第一服务器确定出的第二公钥重新对第一投票进行环签名，使得投票人的投票信息无法被推断出来，由此可以保证投票的匿名性。

[0015] 在一种可能的实现方式中，所述根据所述第一候选人信息，验证所述第一投票的环签名是否通过，包括：

[0016] 获取第一投票集合，所述第一投票集合中包括所述第一投票，以及除所述第一投票终端之外的其他多个第二投票终端发送的第二投票；所述第二投票中包括第二候选人信息和与所述第二候选人信息对应的多个投票人的第三公钥；

[0017] 遍历所述第一投票集合中的所有候选人信息，在所述第一投票集合中删除与任一候选人信息对应的第一投票人的第四公钥，得到多个第二投票集合；所述第一投票人为所有投票人中的任意一个；所述第四公钥为所述第一公钥和所述第三公钥中的一个；

[0018] 根据所述多个第二投票集合，验证所述第一投票的环签名是否通过。

[0019] 在上述方案中，第一投票集合中，不仅包括有第一投票终端发送的第一投票，还包括除第一投票终端之外的其他多个第二投票终端各自发送的第二投票，和第一投票类似，每张第二投票中均包括有第二候选人信息和与第二候选人信息对应的多个投票人的第三公钥，其中，第二候选人信息为每张第二投票中所投的被投票人，而且，每一张第二投票中只能包括有一个候选人信息。其中，第二候选人信息可以和第一候选人信息相同，也可以和第一候选人信息不同，若第二候选人信息和第一候选人信息相同，则说明第一投票终端对应的投票人所投的候选人和第二投票终端对应的投票人所投的候选人相同。

[0020] 在一种可能的实现方式中，所述根据所述多个第二投票集合，验证所述第一投票的环签名是否通过，包括：

[0021] 分别对所述多个第二投票集合中的每个第二投票集合构造无向图；

[0022] 判断每个所述无向图的最大流是否均等于所述第一投票集合中投票的数量；

[0023] 若每个所述无向图的最大流均等于所述第一投票集合中所述投票的数量，则确定所述第一投票的环签名通过；

[0024] 若存在至少一个所述无向图的最大流不等于所述第一投票集合中所述投票的数量，则确定所述第一投票的环签名未通过。

[0025] 在上述方案中，若每个无向图的最大流均等于第一投票集合中投票的数量，则说明根据第一投票将无法推断出投票人的投票信息，即说明第一投票的匿名性可以得到保证，此时，将可以确定第一投票的环签名通过。

[0026] 若存在至少一个无向图的最大流不等于第一投票集合中投票的数量，则说明根据第一投票可以推断出投票人的投票信息，即说明第一投票的匿名性无法得到保证，此时，将可以确定第一投票的环签名未通过。

[0027] 在一种可能的实现方式中，所述根据所述第一公钥，确定第二公钥，包括：

[0028] 从除所述第一公钥之外的其他公钥中，确定所述第二公钥。

[0029] 在本方案中，第二服务器中存储有所有投票人的公钥，第一服务器可以从第二服务器中获取到所有投票人的公钥，这样，第一服务器将从所有投票人的公钥中，除第一公钥之外的其他公钥中确定第二公钥，在实际应用中，第一服务器将可以从其他公钥中随机选择一个公钥作为第二公钥，或者也可以遍历所有的其他公钥，选择一个可以保证第一投票匿名性的公钥作为第二公钥。

[0030] 在一种可能的实现方式中，对所述第二投票集合构造无向图，包括：

[0031] 分别确定所述第二投票集合中的所有第三候选人信息以及所有第二投票人的公钥；

[0032] 根据所述第三候选人信息和所述第二投票人的公钥，构造所述无向图。

[0033] 在一种可能的实现方式中，所述根据所述第三候选人信息和所述第二投票人的公钥，构造所述无向图，包括：

[0034] 将所述第二投票人的公钥确定为第一节点；

[0035] 将所述第三候选人信息确定为第二节点；

[0036] 分别构造所述第一节点和汇点之间的边，以及所述第二节点和源点之间的边；

[0037] 分别构造各所述第二节点和与所述第二节点对应的所述第一节点之间的边，得到所述无向图。

[0038] 在上述各方案中，可以增加无向图中的源点和汇点，并将第二投票人的公钥确定为第一节点，将第三候选人信息确定为第二节点，分别构造第一节点和汇点之间的边，以及第二节点和源点之间的边，再分别构造各第二节点和与第二节点对应的第一节点之间的边，从而可以得到无向图。

[0039] 在一种可能的实现方式中，所述接收所述第一投票终端发送的第二投票之后，所述方法还包括：

[0040] 向多个第二服务器发送所述第二投票。

[0041] 在本方案中，第一服务器会将接收到的第二投票发送给多个第二服务器，每个第二服务器均会记录接收到的第二投票，这样，既可以保证投票的透明性，而且可以避免投票的更改，从而保证投票的不可篡改性。

[0042] 在一种可能的实现方式中，所述接收第一投票终端发送的经过环签名后的第一投票，包括：

[0043] 接收所述第一投票终端发送的投票人的身份信息；

[0044] 对所述身份信息进行认证，得到认证结果；

[0045] 将所述认证结果发送给所述第一投票终端；

[0046] 接收所述第一投票终端根据所述认证结果发送的所述第一投票。

[0047] 在本方案中，在进行投票时，为了保证投票的合法性，首先需要对第一投票终端对应的投票人的身份信息进行认证。

[0048] 在一种可能的实现方式中，所述方法还包括：

[0049] 接收所述第一投票终端发送的所述投票人的公钥；

[0050] 将所述身份信息和所述公钥进行签名，得到签名信息；

[0051] 将所述认证结果、所述投票人的公钥和所述签名信息发送给多个第二服务器。

[0052] 其中，第二服务器为分布式账本。第一服务器将投票人的身份信息和接收到的公钥Pk进行签名，并将认证结果、投票人的公钥Pk和签名信息发送给分布式账本，分布式账本会将这些信息进行记录，从而可以保证信息的透明性以及不可篡改性。

[0053] 本申请第二方面提供一种电子投票方法，应用于投票终端，所述方法包括：

[0054] 向第一服务器发送经过环签名后的第一投票，所述第一投票中包括第一候选人信息和与所述第一候选人信息对应的多个投票人的第一公钥；

[0055] 接收所述第一服务器发送的第二公钥，所述第二公钥为所述第一服务器在根据所述第一候选人信息验证所述第一投票的环签名未通过时发送的；

[0056] 根据所述第二公钥，对所述第一投票进行环签名，得到第二投票；

[0057] 向所述第一服务器发送所述第二投票。

[0058] 在本方案中，由于第一服务器在接收到第一投票终端发送的经过环签名后的第一投票后，将验证该第一投票的环签名是否通过，也即验证该第一投票是否能够保证投票的匿名性，若验证未通过，则第一服务器将确定第二公钥，第一投票终端将根据第一服务器确定出的第二公钥重新对第一投票进行环签名，使得投票人的投票信息无法被推断出来，由此可以保证投票的匿名性。

[0059] 在一种可能的实现方式中，所述向第一服务器发送经过环签名后的第一投票，包括：

[0060] 获取除所述投票终端对应的投票人之外的其他n个投票人的公钥；其中，n为正整数；

[0061] 根据所述n个公钥、所述投票终端对应的投票人的公钥和私钥，对第一投票进行环签名，得到环签名后的第一投票；

[0062] 向所述第一服务器发送所述环签名后的第一投票。

[0063] 在一种可能的实现方式中，所述获取除所述投票终端对应的投票人之外的其他投票人的n个公钥，包括：

[0064] 向多个第二服务器发送请求消息；

[0065] 接收各所述第二服务器发送的响应消息，所述响应消息中包括所述n个公钥。

[0066] 在本方案中，由于第一服务器会将每个投票终端对应的投票人的公钥均发送给多个第二服务器进行保存，因此，每个第二服务器中均保存有所有的投票人的公钥，第一投票终端在进行环签名时，可以从第二服务器中获取除第一投票终端对应的投票人的公钥之外的其他n个投票人的公钥。

[0067] 在一种可能的实现方式中，所述向第一服务器发送经过环签名后的第一投票，包括：

[0068] 向所述第一服务器发送投票人的身份信息；

[0069] 接收所述第一服务器发送的对所述身份信息进行认证后的认证结果；

[0070] 根据所述认证结果，向所述第一服务器发送所述环签名后的第一投票。

[0071] 在本方案中，在进行投票时，为了保证投票的合法性，首先需要对第一投票终端对应的投票人的身份信息进行认证。

[0072] 在一种可能的实现方式中，所述方法还包括：

[0073] 向所述第一服务器发送所述投票终端对应的投票人的公钥，所述公钥用于指示所述第一服务器将所述身份信息和所述公钥进行签名。

[0074] 本申请第三方面提供一种电子投票装置，用于执行第一方面或第一方面的任意一种可能的实现方式中的方法。具体地，所述电子投票装置包括用于执行第一方面或第一方面的任意一种可能的实现方式中的方法的单元。

[0075] 本申请第四方面提供一种电子投票装置，用于执行第二方面或第二方面的任意一种可能的实现方式中的方法。具体地，所述电子投票装置包括用于执行第一方面或第一方面的任意一种可能的实现方式中的方法的单元。

[0076] 本申请第五方面提供一种服务器，包括存储器、处理器及存储在所述存储器上并可在所述处理器上运行的程序，所述处理器执行所述程序时实现第一方面所述的电子投票方法。

[0077] 本申请第六方面提供一种终端，包括存储器、处理器及存储在所述存储器上并可在所述处理器上运行的程序，所述处理器执行所述程序时实现第二方面所述的电子投票方法。

[0078] 本申请第七方面提供一种计算机可读存储介质，计算机可读存储介质中存储有指令，当其在计算机上运行时，使得计算机执行上述各方面的方法。

[0079] 本申请第八方面提供了一种包含指令的计算机程序产品，当其在计算机上运行时，使得计算机执行上述各方面的方法。

[0080] 本申请实施例提供的电子投票方法、装置和存储介质，第一服务器通过接收第一投票终端发送的经过环签名后的第一投票，该第一投票中包括第一候选人信息和与第一候选人信息对应的多个投票人的第一公钥，然后根据该第一候选人信息，验证第一投票的环签名是否通过，若验证第一投票的环签名未通过，则根据第一公钥，确定第二公钥，再向第一投票终端发送第二公钥，并接收第一投票终端发送的第二投票，该第二投票为第一投票终端根据第二公钥对第一投票重新进行环签名后的投票。由于第一服务器在接收到第一投票终端发送的经过环签名后的第一投票后，将验证该第一投票的环签名是否通过，也即验证该第一投票是否能够保证投票的匿名性，若验证未通过，则第一服务器将确定第二公钥，第一投票终端将根据第一服务器确定出的第二公钥重新对第一投票进行环签名，使得投票人的投票信息无法被推断出来，由此可以保证投票的匿名性。

附图说明

[0081] 图1为本申请实施例提供的一种系统架构示意图；

[0082] 图2为本申请实施例提供的电子投票方法的一种信令流程图；

[0083] 图3为本申请实施例提供的第二投票集合对应的无向图的示意图；

[0084] 图4为本申请实施例提供的一种电子投票装置的结构示意图；

[0085] 图5为本申请实施例提供的一种电子投票装置的结构示意图；

[0086] 图6为本申请另一实施例提供的服务器的结构示意图；

[0087] 图7为本申请另一实施例提供的投票终端的结构示意图。

具体实施方式

[0088] 以下，对本申请中的部分用语进行解释说明，以便于本领域技术人员理解。

[0089] 1)投票终端，为具有投票功能的设备，其可以是用户设备(user equipment，UE)、也可以是蜂窝电话、无绳电话、会话启动协议(session initiation protocol，SIP)电话、无线本地环路(wireless local loop，WLL)站、个人数字处理(personal digital assistant，PDA)设备、具有无线通信功能的手持设备、计算设备或连接到无线调制解调器的其它处理设备、车载设备、可穿戴设备等。

[0090] 作为示例而非限定，在本申请实施例中，该投票终端还可以是可穿戴设备。可穿戴设备也可以称为穿戴式智能设备，是应用穿戴式技术对日常穿戴进行智能化设计、开发出可以穿戴的设备的总称，如眼镜、手套、手表、服饰及鞋等。可穿戴设备即直接穿在身上，或是整合到用户的衣服或配件的一种便携式设备。可穿戴设备不仅仅是一种硬件设备，更是通过软件支持以及数据交互、云端交互来实现强大的功能。广义穿戴式智能设备包括功能全、尺寸大、可不依赖智能手机实现完整或者部分的功能，例如：智能手表或智能眼镜等，以及只专注于某一类应用功能，需要和其它设备如智能手机配合使用，如各类进行体征监测的智能手环、智能首饰等。

[0091] 2)私钥、公钥：是通过一种算法得到的密匙对，例如可以通过椭圆曲线计算得到。通常采用公钥和私钥对信息进行不对称加密，其中，用公钥加密的内容只能用对应的私钥解密，而用私钥加密的内容只能用对应的公钥进行解密。

[0092] 3)签名：将信息用发送方的私钥进行加密而生成的信息，是某个消息由发送方进行发送的凭证。

[0093] 4)环签名：签名者将自己的公钥和一个公钥集合进行混合，再用自己的私钥对消息进行的签名，是消息由公钥集合中某人发送的凭证，但是签名验证者无法分辨签名者的公钥。

[0094] 5)最大流：在一个图中，在边容量允许的情况下，从源点到汇点所能通过的最大流量。

[0095] 6)本申请中，“至少一个”可以是指一个或者多个，“多个”是指两个或两个以上。“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。“以上”或“以下”等所描述的范围包括边界点。

[0096] 7)本申请中的单元是指功能单元或逻辑单元。其可以为软件形式，通过处理器执行程序代码来实现其功能；也可以为硬件形式。

[0097] 本领域技术人员可以理解，本申请实施例提供的电子投票方法可以应用于电子投票系统中，其中，电子投票系统是将选票电子化以方便投票和计票的投票系统。相较于纸质的投票方式，电子投票系统具有以下特性：(1)计票更快速准确，电子投票可以直接使用计算机程序进行统计，相较于人工计票，更快速，并且错误率更低；(2)更环保，电子投票不需要使用纸质的选票；(3)更便捷，电子投票系统使用计算机程序来验证身份，领取选票，提交选票，整个过程更加便捷，这种便捷性也增加选民参与度。

[0098] 透明性、不可篡改性、合法性和匿名性是评价电子投票系统很重要的几个指标，其中，透明性，是指投票结束后所有选票都会被公开；不可篡改性是指选票一旦提交就不能被任何人(包括投票人自己)更改；合法性是指保证没有虚假票以及重复票的出现；匿名性是指每一张选票的投票人身份不可见也不能被推断出来。

[0099] 图1为本申请实施例提供的一种系统架构示意图。如图1所示，该系统包括多个投票终端101、身份认证中心服务器102、投票中心服务器103、监票中心服务器104和分布式账本服务器105。

[0100] 其中，投票终端101例如可以为UE，身份认证中心服务器102用于对投票终端101对应的投票人的身份进行验证，以保证投票的合法性，投票中心服务器103用于在投票人的身份验证通过后，向投票终端101发送投票，投票中心服务器103还用于将登记信息发送给分布式账本服务器105，其中，登记信息包括投票人身份信息的验证结果、投票人公钥和由投票中心服务器103进行签名后的信息。监票中心服务器104用于接收投票终端101发送的投票，并对接收到的投票进行核实，然后将核实后的投票发送给分布式账本服务器105。分布式账本服务器105中包含多台服务器，每台服务器中分别记录有登记信息以及经监票中心服务器104核实后的投票，这样选票信息一旦公布后，任何单方都无法修改选票，由此可以保证选票的不可篡改性。

[0101] 需要进行说明的是，图1中的身份认证中心服务器102、投票中心服务器103和监票中心服务器104可以为同一个服务器，即身份认证中心服务器102、投票中心服务器103和监票中心服务器104的功能可以集成在一个服务器中实现，当然，也可以为不同的服务器，即身份认证中心服务器102、投票中心服务器103和监票中心服务器104的功能可以分别部署在不同的服务器中实现。

[0102] 在图1所示的系统架构的基础上，目前通常采用固定分组环签名的方式或随机分组环签名的方式进行投票，其中，对于固定分组环签名的投票方式，整个投票过程可以包括如下步骤：(1)投票装置向身份认证中心发送身份信息；(2)身份认证中心验证身份信息并向投票装置返回认证结果；(3)投票装置将认证结果发送给投票中心；(4)投票中心在确认认证结果为认证通过后，将n个投票人分成固定的k组，并向投票装置发送投票和投票人所在分组信息；(5)投票中心将登记信息发送给分布式账本，其中，登记信息中包括投票人身份信息认证结果、投票人公钥和由投票中心签名的信息；(6)分布式账本记录登记信息；(7)投票装置使用其所在分组的所有公钥和自己的私钥对投票信息进行环签名并发送投票；(8)监票中心核实收到的投票并发送给分布式账本；(9)分布式账本记录投票。

[0103] 对于随机分组环签名的投票方式，整个投票过程可以包括如下步骤：(1)投票装置向身份认证中心发送身份信息；(2)身份认证中心验证身份信息并向投票装置返回认证结果；(3)投票装置将认证结果发送给投票中心；(4)投票中心在确认认证结果为认证通过后，

从已有投票人中随机选取k个，并将这k个投票人的公钥信息和投票发送给投票装置；(5)投票中心将登记信息发送给分布式账本，其中，登记信息中包括投票人身份信息认证结果、投票人公钥和由投票中心签名的信息；(6)分布式账本记录登记信息；(7)投票装置使用收到的k个公钥和自己的私钥对投票信息进行环签名并向监票中心发送投票；(8)监票中心核实收到的投票并发送给分布式账本；(9)分布式账本记录投票。

[0104] 然而，在上述两种投票方式中，当同一分组内的投票结果相同时，每个投票人的投票结果会被推断出来，因此，上述两种投票方式均无法保证电子投票过程的匿名性。

[0105] 本申请实施例考虑到这些情况，提出一种电子投票方法，第一服务器通过接收第一投票终端发送的经过环签名后的第一投票，该第一投票中包括第一候选人信息和与第一候选人信息对应的多个投票人的第一公钥，然后根据该第一候选人信息，验证第一投票的环签名是否通过，若验证第一投票的环签名未通过，则根据第一公钥，确定第二公钥，再向第一投票终端发送第二公钥，并接收第一投票终端发送的第二投票，该第二投票为第一投票终端根据第二公钥对第一投票重新进行环签名后的投票。由于第一服务器在接收到第一投票终端发送的经过环签名后的第一投票后，将验证该第一投票的环签名是否通过，也即验证该第一投票是否能够保证投票的匿名性，若验证未通过，则第一服务器将确定第二公钥，第一投票终端将根据第一服务器确定出的第二公钥重新对第一投票进行环签名，使得投票人的投票信息无法被推断出来，由此可以保证投票的匿名性。

[0106] 下面以具体的实施例对本发明的技术方案进行详细说明。下面这几个具体的实施例可以相互结合，对于相同或相似的概念或过程可能在某些实施例不再赘述。

[0107] 下面，先以身份认证中心服务器102、投票中心服务器103和监票中心服务器104为同一个服务器，即身份认证中心服务器102、投票中心服务器103和监票中心服务器104的功能均集成在第一服务器中，来说明本申请实施例提供的电子投票方法。

[0108] 图2为本申请实施例提供的电子投票方法的一种信令流程图。如图2所示，本实施例的方法可以包括：

[0109] 步骤201、第一投票终端向第一服务器发送第一投票。

[0110] 其中，该第一投票为经过环签名后的投票，该第一投票中包括第一候选人信息和与第一候选人信息对应的多个投票人的第一公钥。

[0111] 在本步骤中，第一投票终端可以为图1中所示的多个投票终端中的任意一个。在进行投票时，为了保证投票的合法性，首先需要对第一投票终端对应的投票人的身份信息进行认证。

[0112] 在一种可能的实现方式中，第一服务器将接收第一投票终端发送的投票人的身份信息，并对身份信息进行认证，得到认证结果，然后将认证结果发送给各第一投票终端，并接收第一投票终端根据认证结果发送的第一投票。另外，第一服务器还将接收第一投票终端发送的投票人的公钥，并对身份信息和公钥进行签名，得到签名信息，然后将认证结果、投票人的公钥和签名信息发送给多个第二服务器，第二服务器将记录认证结果、投票人的公钥和签名信息。

[0113] 具体的，第一投票终端在进行投票时，将会为投票人生成一对公私钥(Pk,Sk)，并将投票人的身份信息发送给第一服务器，第一服务器对身份信息进行认证，得到认证结果，其中若认证结果为认证通过，则说明投票人的身份是合法的，若认证结果为认证未通过，则

说明投票人的身份是非合法的，通过认证投票人的身份是否合法，从而可以保证投票的合法性。第一服务器在得到认证结果后，会将认证结果发送给第一投票终端，第一投票终端若确定出认证结果为认证通过，则向第一服务器发送投票人的公钥Pk，第一服务器将投票人的身份信息和接收到的公钥Pk进行签名，并将认证结果、投票人的公钥Pk和签名信息发送给第二服务器，即发送给分布式账本，以将这些信息进行记录。

[0114] 另外，第一投票终端若确定出认证结果为认证通过，则将会对投票进行环签名，并将经过环签名后的第一投票发送给第一服务器。具体的，第一投票终端将获取除第一投票终端对应的投票人之外的其他n个投票人的公钥，并根据n个公钥、投票终端对应的投票人的公钥和私钥，对投票进行环签名，得到经过环签名后的第一投票，然后向第一服务器发送第一投票，其中，n为正整数。

[0115] 在具体的实现过程中，由于第一服务器会将每个投票终端对应的投票人的公钥均发送给多个第二服务器进行保存，因此，每个第二服务器中均保存有所有的投票人的公钥，第一投票终端在进行环签名时，可以从第二服务器中获取除第一投票终端对应的投票人的公钥之外的其他n个投票人的公钥。可选的，第一服务器可以向多个第二服务器发送请求消息，该请求消息用于表示该第一服务器获取其他n个投票人的公钥，各第二服务器在接收到请求消息后，会向第一服务器发送响应消息，该响应消息中包括其他n个投票人的公钥。这样，第一投票终端将可以根据自身对应的投票人的公钥和私钥，以及其他n个投票人的公钥，对投票进行环签名，得到第一投票。

[0116] 其中，第一投票中包括有第一候选人信息和与第一候选人信息对应的多个投票人的第一公钥。第一候选人是指第一投票中所投的被投票人，而且，每一张投票中只能包括一个候选人信息。另外，与第一候选人信息对应的多个投票人的第一公钥，是指第一投票终端对投票进行环签名时所使用的公钥。

[0117] 举例来说，若第一投票终端对应的投票人的公私钥为(Pk1,Sk1)，第一投票终端从第二服务器中获取到的其他n个投票人的公钥分别为Pk2、Pk4、Pk5和Pk7，第一投票终端将根据Pk1、Sk1、Pk2、Pk4、Pk5和Pk7对投票进行环签名，从而得到经过环签名后的第一投票V，其中，V＝(G,C)，C为第一候选人信息，G＝(Pk1,Pk2,Pk4,Pk5和Pk7)。

[0118] 步骤202、第一服务器根据第一候选人信息，验证第一投票的环签名是否通过。

[0119] 在本步骤中，第一服务器在接收到第一投票终端发送的经过环签名后的第一投票后，将根据第一投票中的第一候选人信息，验证第一投票的环签名是否通过，即验证根据第一投票是否能够推断出投票人的投票信息，也即验证第一投票是否满足匿名性。

[0120] 在一种可能的实现方式中，可以通过如下方式验证第一投票的环签名是否通过：获取第一投票集合，该第一投票集合中包括第一投票，以及除第一投票终端之外的其他多个第二投票终端发送的第二投票，第二投票中包括第二候选人信息和与第二候选人信息对应的多个投票人的第三公钥；遍历第一投票集合中的所有候选人信息，在第一投票集合中删除与任一候选人信息对应的第一投票人的第四公钥，得到多个第二投票集合；第一投票人为所有投票人中的任意一个；第四公钥为第一公钥和第三公钥中的一个；根据多个第二投票集合，验证第一投票的环签名是否通过。

[0121] 具体的，在进行投票时，可能会存在多个投票终端向第一服务器发送投票，因此，第一服务器获取到的第一投票集合中，不仅包括有第一投票终端发送的第一投票，还包括

除第一投票终端之外的其他多个第二投票终端各自发送的第二投票，和第一投票类似，每张第二投票中均包括有第二候选人信息和与第二候选人信息对应的多个投票人的第三公钥，其中，第二候选人信息为每张第二投票中所投的被投票人，而且，每一张第二投票中只能包括有一个候选人信息。需要进行说明的是，第二候选人信息可以和第一候选人信息相同，也可以和第一候选人信息不同，若第二候选人信息和第一候选人信息相同，则说明第一投票终端对应的投票人所投的候选人和第二投票终端对应的投票人所投的候选人相同。

[0122] 另外，与第二候选人信息对应的多个投票人的第三公钥，是指每个第二投票终端对对应的第二投票进行环签名时所使用的公钥。

[0123] 例如：第一投票集合S中包括有(Pk1,Pk2,B1)，(Pk2,Pk3,B1)和(Pk1,Pk3,B2)这三张投票。其中，B1和B2表示候选人信息，Pk1和Pk2表示候选人B1对应的投票人的公钥，因此，(Pk1,Pk2,B1)表示公钥为Pk1和Pk2的投票人中的一个人投了候选人B1，Pk2和Pk3也表示候选人B1对应的投票人的公钥，(Pk2,Pk3,B1)表示公钥为Pk2和Pk3的投票人中的一个人投了候选人B1，Pk1和Pk3表示候选人B2对应的投票人的公钥，(Pk1,Pk3,B2)表示公钥为Pk1和Pk3的投票人中的一个人投了候选人B2。

[0124] 第一服务器在获取到第一投票集合后，将遍历第一投票集合中的所有候选人信息，在第一投票集合中依次删除与每个候选人信息对应的第一投票人的第四公钥，其中，第一投票人为所有投票人中的任意一个，也即对于每个候选人信息来说，也会在第一投票集合中遍历所有与该候选人信息对应的投票人，并在第一投票集合中删除与该候选人信息对应的投票人的第四公钥，其中，该第四公钥为第一投票中的第一公钥或者为第二投票中的第三公钥，这样，即可得到多个第二投票集合。

[0125] 举例来说，假设第一投票集合S＝{(Pk1,Pk2,B1)，(Pk2,Pk3,B1)，(Pk1,Pk3,B2)}，第一投票集合S中包括有B1和B2两个候选人，首先，对于候选人B1来说，与B1对应的投票人的公钥包括Pk1、Pk2和Pk3，分别在第一投票集合S中删除Pk1、Pk2和Pk3后，得到第二投票集合S1＝{(Pk2,B1)，(Pk2,Pk3,B1)，(Pk1,Pk3,B2)}、S2＝{(Pk1,B1)，(Pk3,B1)，(Pk1,Pk3,B2)}和S3＝{(Pk1,Pk2,B1)，(Pk2,B1)，(Pk1,Pk3,B2)}；对于候选人B2来说，与B2对应的投票人的公钥包括Pk1和Pk3，分别在第一投票集合S中删除Pk1和Pk3后，得到第二投票集合S4＝{(Pk1,Pk2,B1)，(Pk2,Pk3,B1)，(Pk3,B2)}以及S5＝{(Pk1,Pk2,B1)，(Pk2,Pk3,B1)，(Pk1,B2)}。

[0126] 第一服务器将根据得到的多个第二投票集合，验证第一投票的环签名是否通过。在一种可能的实现方式中，第一服务器将分别对多个第二投票集合中的每个第二投票集合构造无向图，并判断每个无向图的最大流是否均等于第一投票集合中投票的数量，若每个无向图的最大流均等于第一投票集合中投票的数量，则确定第一投票的环签名通过；若存在至少一个无向图的最大流不等于第一投票集合中投票的数量，则确定第一投票的环签名未通过。

[0127] 具体的，第一服务器在获得多个第二投票集合后，针对每个第二投票集合，将构造该第二投票集合对应的无向图。可选的，在对某个第二投票集合构造无线图时，将分别确定该第二投票集合中的所有第三候选人信息以及所有第二投票人的公钥，并根据确定出的第三候选人信息和第二投票人的公钥，构造无向图。

[0128] 示例性的，可以增加无向图中的源点和汇点，并将第二投票人的公钥确定为第一

节点，将第三候选人信息确定为第二节点，分别构造第一节点和汇点之间的边，以及第二节点和源点之间的边，再分别构造各第二节点和与第二节点对应的第一节点之间的边，从而可以得到无向图。

[0129] 举例来说，图3为第二投票集合对应的无向图的示意图，如图3所示，假设第二投票集合为S1＝{V1＝({A,B},1),V2＝({B,C},2)}，在该第二投票集合中，投票V1表示公钥为A的投票人和公钥为B的投票人中的某一个人投了候选人1；选票V2表示公钥为B的投票人和公钥为C的投票人中的某一个人投了候选人2，因此，该第二投票集合中的第三候选人信息包括候选人1和候选人2，将1和2确定为第二节点，该第二投票集合中的所有投票人的公钥包括A,B和C，将A,B和C确定为第一节点，其中，与候选人1对应的公钥为A和B，与候选人2对应的公钥为B和C。

[0130] 增加无向图中的源点S和汇点T，分别构造第一节点A,B和C与汇点T之间的边(A,T,1)、(B,T,1)和(C,T,1)，并构造第二节点1和2与源点S之间的边(1,S,1)和(2,S,1)，再构造第二节点1和与第二节点1对应的第一节点A和B之间的边(1,A,1)和(1,B,1)，构造，第二节点2和与第二节点2对应的第一节点B和C之间的边(2,B,1)和(2,C,1)，从而可以构造出第二投票集合对应的无向图。

[0131] 对于每个第二投票集合，在分别构造出对应的无向图之后，将判断每个无向图的最大流是否均等于第一投票集合中投票的数量，其中，无向图的最大流为在无向图中，在边容量允许的情况下，从源点到汇点所能通过的最大流量，如图3所示的无向图，其最大流为2。

[0132] 若每个无向图的最大流均等于第一投票集合中投票的数量，则说明根据第一投票将无法推断出投票人的投票信息，即说明第一投票的匿名性可以得到保证，此时，将可以确定第一投票的环签名通过。

[0133] 若存在至少一个无向图的最大流不等于第一投票集合中投票的数量，则说明根据第一投票可以推断出投票人的投票信息，即说明第一投票的匿名性无法得到保证，此时，将可以确定第一投票的环签名未通过。

[0134] 例如:假设第一投票集合S＝{(Pk1,Pk2,B1),(Pk2,Pk3,B1),(Pk1,Pk3,B2)}，第二投票集合S1＝{(Pk2,B1),(Pk2,Pk3,B1),(Pk1,Pk3,B2)}、S2＝{(Pk1,B1),(Pk3,B1),(Pk1,Pk3,B2)}、S3＝{(Pk1,Pk2,B1),(Pk2,B1),(Pk1,Pk3,B2)}、S4＝{(Pk1,Pk2,B1),(Pk2,Pk3,B1),(Pk3,B2)}以及S5＝{(Pk1,Pk2,B1),(Pk2,Pk3,B1),(Pk1,B2)}。对第二投票集合S1、S2、S3、S4和S5分别按照前述方式构造无向图，并判断每个无向图的最大流是否均等于第一投票集合中投票的数量3，若S1、S2、S3、S4和S5对应的无向图的最大流均等于3，则确定第一投票的环签名通过，若存在至少一个无向图的最大流不等于3，则确定第一投票的环签名未通过。

[0135] 步骤203、若验证第一投票的环签名未通过，则第一服务器根据第一公钥，确定第二公钥。

[0136] 在本步骤中，若第一服务器验证第一投票的环签名未通过，则第一服务器将根据第一投票中的第一公钥，确定第二公钥，也即混淆公钥。

[0137] 在一种可能的实现方式中，第一服务器根据第一公钥，确定第二公钥时，可以从除第一公钥之外的其他公钥中进行确定。

[0138] 具体的，第二服务器中存储有所有投票人的公钥，第一服务器可以从第二服务器中获取到所有投票人的公钥，这样，第一服务器将从所有投票人的公钥中，除第一公钥之外的其他公钥中确定第二公钥，在实际应用中，第一服务器将可以从其他公钥中随机选择一个公钥作为第二公钥，或者也可以遍历所有的其他公钥，选择一个可以保证第一投票匿名性的公钥作为第二公钥。

[0139] 示例性的，假设第一服务器获取到的所有投票人的公钥包括Pk1、Pk2、Pk3和Pk4，其中，第一投票中包括的第一公钥为Pk1和Pk2，则第一服务器将从Pk3和Pk4中确定第二公钥，如可以选择Pk3。

[0140] 需要进行说明的是，若第一服务器验证第一投票的环签名通过，则第一服务器将会向第一投票装置发送通知消息，以通知第一投票装置，第一投票的环签名通过，即第一投票的匿名性可以得到保证，此时，第一投票装置将第一投票发送给多个第二服务器，每个第二服务器会记录该第一投票。

[0141] 步骤204、第一服务器向第一投票终端发送第二公钥。

[0142] 步骤205、第一投票终端根据第二公钥，对第一投票进行环签名，得到第二投票。

[0143] 在本步骤中，第一服务器在确定出第二公钥后，会将确定出的第二公钥发送给第一投票终端。第一投票终端根据接收到的第二公钥，以及第一投票中包括的第一公钥，对第一投票重新进行环签名，从而得到第二投票。

[0144] 例如：若第一投票中包括的第一公钥为Pk1和Pk2，第一服务器确定出的第二公钥为Pk3，则第一服务器会将确定出的Pk3发送给第一投票终端，这样，第一投票终端将根据Pk1、Pk2和Pk3对第一投票重新进行环签名，从而得到第二投票。

[0145] 需要进行说明的是，采用第二公钥和第一公钥，对第一投票重新进行环签名后得到的第二投票，是无法推断出投票人的投票信息的，即该第二投票的匿名性是能够得到保证的。

[0146] 步骤206、第一投票终端向第一服务器发送第二投票。

[0147] 在本步骤中，第一投票终端根据第一公钥和第二公钥，对第一投票重新进行环签名后，会将得到的第二投票发送给第一服务器。

[0148] 可选的，第一服务器会将接收到的第二投票发送给多个第二服务器，每个第二服务器均会记录接收到的第二投票，这样，既可以保证投票的透明性，而且可以避免投票的更改，从而保证投票的不可篡改性。

[0149] 本申请实施例提供的电子投票方法，第一服务器通过接收第一投票终端发送的经过环签名后的第一投票，该第一投票中包括第一候选人信息和与第一候选人信息对应的多个投票人的第一公钥，然后根据该第一候选人信息，验证第一投票的环签名是否通过，若验证第一投票的环签名未通过，则根据第一公钥，确定第二公钥，再向第一投票终端发送第二公钥，并接收第一投票终端发送的第二投票，该第二投票为第一投票终端根据第二公钥对第一投票重新进行环签名后的投票。由于第一服务器在接收到第一投票终端发送的经过环签名后的第一投票后，将验证该第一投票的环签名是否通过，也即验证该第一投票是否能够保证投票的匿名性，若验证未通过，则第一服务器将确定第二公钥，第一投票终端将根据第一服务器确定出的第二公钥重新对第一投票进行环签名，使得投票人的投票信息无法被推断出来，由此可以保证投票的匿名性。

[0150] 下面，将说明图1中所示的身份认证中心服务器102、投票中心服务器103和监票中心服务器104为不同的服务器，即身份认证中心服务器102、投票中心服务器103和监票中心服务器104的功能均集成在不同的服务器中时，本申请实施例提供的电子投票方法。

[0151] 其中，第一投票终端在进行投票时，将会为投票人生成一对公私钥(Pk，Sk)，并将投票人的身份信息发送给身份认证中心服务器，身份认证中心服务器对身份信息进行认证，得到认证结果，其中，若认证结果为认证通过，则说明投票人的身份是合法的，若认证结果为认证未通过，则说明投票人的身份是非合法的，通过认证投票人的身份是否合法，从而可以保证投票的合法性。身份认证中心服务器在得到认证结果后，会将认证结果发送给第一投票终端，第一投票终端若确定出认证结果为认证通过，则向投票中心服务器发送投票人的公钥Pk，投票中心服务器将投票人的身份信息和接收到的公钥Pk进行签名，并将认证结果、投票人的公钥Pk和签名信息发送给第二服务器，即发送给分布式账本，以将这些信息进行记录。

[0152] 另外，第一投票终端若确定出认证结果为认证通过，则将会对投票进行环签名，并将经过环签名后的第一投票发送给监票中心服务器。其中，第一投票终端对投票进行环签名的方式，与前述方式中的环签名方式类似，可以参考前述方式中的相关描述，此处不再赘述。

[0153] 监票中心服务器将根据第一投票中包括的第一候选人信息，验证第一投票的环签名是否通过，并在验证第一投票的环签名未通过时，根据第一公钥，确定第二公钥，并将确定出的第二公钥发送给第一投票终端。

[0154] 其中，监票中心服务器验证第一投票的环签名是否通过，以及确定第二公钥的方式，与前述第一服务器验证第一投票的环签名是否通过，以及确定第二公钥的方式类似，可以参考前述方式中的相关描述，此处不再赘述。

[0155] 第一投票终端根据监票中心服务器发送的第二公钥，对第一投票重新进行环签名，得到第二投票后，将该第二投票发送给监票中心服务器，该监票中心服务器将第二投票发送给多个第二服务器，也即发送给分布式账本服务器，分布式账本服务器将记录接收到的第二投票。

[0156] 下面，将以具体的示例对本申请的方案进行进一步的说明。

[0157] 假设电子投票系统中包括三个投票人，他们的身份信息分别为ID1、ID2和ID3，公钥分别为Pk1、Pk2和Pk3，若第一服务器目前已经接收到投票终端发送的投票包括{(Pk1，Pk2，B1)，(Pk2，Pk3，B1)}，其中，第一张投票表示公钥为Pk1和Pk2的投票人ID1、ID2中的某一个人投了候选人B1，第二张投票表示公钥为Pk2和Pk3的投票人ID2、ID3中的某一个人投了候选人B1。

[0158] 对于投票人的身份信息验证的过程，可以参照前述实施例中的相关描述，此处不再赘述。

[0159] 假设第一投票终端对应的投票人的公钥为Pk3，且第一投票终端选择公钥Pk1和Pk3对投票进行环签名，得到第一投票V，其中，V＝(Pk1，Pk3，B2)，其中，B2为候选人，第一投票V表示公钥为Pk1和Pk3的投票人ID1、ID3中的某一个人投了候选人B2。第一投票终端将第一投票V发送给第一服务器。

[0160] 第一服务器接收到第一投票V后，将会更新当前所有的投票，以获取第一投票集合

S,其中,S＝{(Pk1,Pk2,B1),(Pk2,Pk3,B1),(Pk1,Pk3,B2)},遍历第一投票集合中的所有候选人信息,在第一投票集合中依次删除与每个候选人信息对应的第一投票人的第四公钥,从而得到多个第二投票集合,分别为S1＝{(Pk2,B1),(Pk2,Pk3,B1),(Pk1,Pk3,B2)}、S2＝{(Pk1,B1),(Pk3,B1),(Pk1,Pk3,B2)}、S3＝{(Pk1,Pk2,B1),(Pk2,B1),(Pk1,Pk3,B2)}、S4＝{(Pk1,Pk2,B1),(Pk2,Pk3,B1),(Pk3,B2)}和S5＝{(Pk1,Pk2,B1),(Pk2,Pk3,B1),(Pk1,B2)}。

[0161] 对于第二投票集合S2＝{(Pk1,B1),(Pk3,B1),(Pk1,Pk3,B2)},构造无向图后,确定出该无向图的最大流为2,小于第一投票集合S中投票的数量3,因此,可以确定出公钥为Pk2的投票人ID2一定投了候选人B1,这样,第一投票集合的匿名性不能得到保证,也即第一投票的环签名未通过。

[0162] 此时,第一服务器获取到所有投票人的公钥包括Pk1、Pk2和Pk3,且第一投票终端之前对投票进行环签名时所使用的公钥为Pk1和Pk3,因此,第一服务器将选择Pk2作为第二公钥,并验证发现添加第二公钥后的第一投票集合S＝{(Pk1,Pk2,B1),(Pk2,Pk3,B1),(Pk1,Pk2,Pk3,B2)}可以通过匿名性验证,因此,第一服务器将第二公钥Pk2发送给第一投票终端,第一投票终端将使用Pk1、Pk2和Pk3对第一投票重新进行环签名,得到第二投票V'＝(Pk1,Pk2,Pk3,B2),并将第二投票V'＝(Pk1,Pk2,Pk3,B2)发送给第一服务器,第一服务器再将第二投票V'＝(Pk1,Pk2,Pk3,B2)发送给多个第二服务器,即发送给分布式账本服务器,以对第二投票V'＝(Pk1,Pk2,Pk3,B2)进行记录。

[0163] 由于第一投票终端根据第二公钥和第一公钥,对第一投票重新进行环签名,由此可以保证投票的匿名性。另外,第一服务器将第二投票发送给多个第二服务器,每个第二服务器都会对第二投票进行记录,这样,可以保证投票的透明性和不可篡改性。

[0164] 本申请实施例提供的电子投票方法,第一服务器通过接收第一投票终端发送的经过环签名后的第一投票,该第一投票中包括第一候选人信息和与第一候选人信息对应的多个投票人的第一公钥,然后根据该第一候选人信息,验证第一投票的环签名是否通过,若验证第一投票的环签名未通过,则根据第一公钥,确定第二公钥,再向第一投票终端发送第二公钥,并接收第一投票终端发送的第二投票,该第二投票为第一投票终端根据第二公钥对第一投票重新进行环签名后的投票。由于第一服务器在接收到第一投票终端发送的经过环签名后的第一投票后,将验证该第一投票的环签名是否通过,也即验证该第一投票是否能够保证投票的匿名性,若验证未通过,则第一服务器将确定第二公钥,第一投票终端将根据第一服务器确定出的第二公钥重新对第一投票进行环签名,使得投票人的投票信息无法被推断出来,由此可以保证投票的匿名性。

[0165] 上文描述了本申请实施例提供的电子投票方法,下文将描述本申请实施例提供的服务器和投票终端。

[0166] 图4为本申请实施例提供的一种电子投票装置的结构示意图,该装置可以为服务器或位于服务器中的芯片或片上系统,可以用于执行上述方法实施例中第一服务器相关的动作,该装置包括:接收单元11、处理单元12和发送单元13。

[0167] 接收单元11用于接收第一投票终端发送的第一投票;所述第一投票为经过环签名后的投票,所述第一投票中包括第一候选人信息和与所述第一候选人信息对应的多个投票人的第一公钥;

[0168] 处理单元12用于根据所述第一候选人信息，验证所述第一投票的环签名是否通过；

[0169] 所述处理单元12还用于在验证所述第一投票的环签名未通过时，根据所述第一公钥，确定第二公钥；

[0170] 发送单元13用于向所述第一投票终端发送所述第二公钥；

[0171] 所述接收单元11还用于接收所述第一投票终端发送的第二投票，所述第二投票为所述第一投票终端根据所述第二公钥对所述第一投票重新进行环签名后的投票。

[0172] 本申请实施例提供的电子投票装置，接收单元11通过接收第一投票终端发送的经过环签名后的第一投票，该第一投票中包括第一候选人信息和与第一候选人信息对应的多个投票人的第一公钥，处理单元12根据该第一候选人信息，验证第一投票的环签名是否通过，若验证第一投票的环签名未通过，则根据第一公钥，确定第二公钥，发送单元13向第一投票终端发送第二公钥，接收单元11接收第一投票终端发送的第二投票，该第二投票为第一投票终端根据第二公钥对第一投票重新进行环签名后的投票。由于第一服务器在接收到第一投票终端发送的经过环签名后的第一投票后，将验证该第一投票的环签名是否通过，也即验证该第一投票是否能够保证投票的匿名性，若验证未通过，则第一服务器将确定第二公钥，第一投票终端将根据第一服务器确定出的第二公钥重新对第一投票进行环签名，使得投票人的投票信息无法被推断出来，由此可以保证投票的匿名性。

[0173] 可选的，所述处理单元12，具体用于：

[0174] 获取第一投票集合，所述第一投票集合中包括所述第一投票，以及除所述第一投票终端之外的其他多个第二投票终端发送的第二投票；所述第二投票中包括第二候选人信息和与所述第二候选人信息对应的多个投票人的第三公钥；

[0175] 遍历所述第一投票集合中的所有候选人信息，在所述第一投票集合中删除与任一候选人信息对应的第一投票人的第四公钥，得到多个第二投票集合；所述第一投票人为所有投票人中的任意一个；所述第四公钥为所述第一公钥和所述第三公钥中的一个；

[0176] 根据所述多个第二投票集合，验证所述第一投票的环签名是否通过。

[0177] 可选的，所述处理单元12，具体用于：

[0178] 分别对所述多个第二投票集合中的每个第二投票集合构造无向图；

[0179] 判断每个所述无向图的最大流是否均等于所述第一投票集合中投票的数量；

[0180] 若每个所述无向图的最大流均等于所述第一投票集合中所述投票的数量，则确定所述第一投票的环签名通过；

[0181] 若存在至少一个所述无向图的最大流不等于所述第一投票集合中所述投票的数量，则确定所述第一投票的环签名未通过。

[0182] 可选的，所述处理单元12，具体用于：

[0183] 从除所述第一公钥之外的其他公钥中，确定所述第二公钥。

[0184] 可选的，所述处理单元12，具体用于：

[0185] 分别确定所述第二投票集合中的所有第三候选人信息以及所有第二投票人的公钥；

[0186] 根据所述第三候选人信息和所述第二投票人的公钥，构造所述无向图。

[0187] 可选的，所述处理单元12，具体用于：

[0188] 将所述第二投票人的公钥确定为第一节点；

[0189] 将所述第三候选人信息确定为第二节点；

[0190] 分别构造所述第一节点和汇点之间的边，以及所述第二节点和源点之间的边；

[0191] 分别构造各所述第二节点和与所述第二节点对应的所述第一节点之间的边，得到所述无向图。

[0192] 可选的，所述发送单元13，还用于向多个第二服务器发送所述第二投票。

[0193] 本申请实施例提供的电子投票装置，可以执行上述对应的方法实施例，其实现原理和技术效果类似，在此不再赘述。

[0194] 需要说明的是，应理解以上装置的各个单元的划分仅仅是一种逻辑功能的划分，实际实现时可以全部或部分集成到一个物理实体上，也可以物理上分开。且这些单元可以全部以软件通过处理元件调用的形式实现；也可以全部以硬件的形式实现；还可以部分单元通过软件通过处理元件调用的形式实现，部分单元通过硬件的形式实现。例如，发送单元可以为单独设立的处理元件，也可以集成在该装置的某一个芯片中实现，此外，也可以以程序的形式存储于装置的存储器中，由该装置的某一个处理元件调用并执行该发送单元的功能。其它单元的实现与之类似。此外这些单元全部或部分可以集成在一起，也可以独立实现。这里所述的处理元件可以是一种集成电路，具有信号的处理能力。在实现过程中，上述方法的各步骤或以上各个单元可以通过处理器元件中的硬件的集成逻辑电路或者软件形式的指令完成。此外，以上发送单元是一种控制发送的单元，可以通过该装置的发送装置发送信息。

[0195] 以上这些单元可以是被配置成实施以上方法的一个或多个集成电路，例如：一个或多个特定集成电路(application specific integrated circuit，ASIC)，或，一个或多个微处理器(digital singnal processor，DSP)，或，一个或者多个现场可编程门阵列(field programmable gate array，FPGA)等。再如，当以上某个单元通过处理元件调度程序的形式实现时，该处理元件可以是通用处理器，例如中央处理器(central processing unit，CPU)或其它可以调用程序的处理器。再如，这些单元可以集成在一起，以片上系统(system-on-a-chip，SOC)的形式实现。

[0196] 图5为本申请实施例提供的一种电子投票装置的结构示意图，该装置可以为投票终端或投票终端中的芯片或片上系统，可以用于执行上述方法实施例中投票终端相关的动作，该装置包括：发送单元21、接收单元22和处理单元23。

[0197] 发送单元21用于向第一服务器发送经过环签名后的第一投票，所述第一投票中包括第一候选人信息和与所述第一候选人信息对应的多个投票人的第一公钥；

[0198] 接收单元22用于接收所述第一服务器发送的第二公钥，所述第二公钥为所述第一服务器在根据所述第一候选人信息验证所述第一投票的环签名未通过时发送的；

[0199] 处理单元23用于根据所述第二公钥，对所述第一投票进行环签名，得到第二投票；

[0200] 所述发送单元21用于向所述第一服务器发送所述第二投票。

[0201] 可选的，所述发送单元21，具体用于：

[0202] 获取除所述投票终端对应的投票人之外的其他n个投票人的公钥；其中，n为正整数；

[0203] 根据所述n个公钥、所述投票终端对应的投票人的公钥和私钥，对第一投票进行环

签名,得到环签名后的第一投票;

[0204] 向所述第一服务器发送所述环签名后的第一投票。

[0205] 可选的,所述发送单元21,还用于向多个第二服务器发送请求消息;

[0206] 所述接收单元22,还用于接收各所述第二服务器发送的响应消息,所述响应消息中包括所述n个公钥。

[0207] 本申请实施例提供的电子投票装置,可以执行上述对应的方法实施例,其实现原理和技术效果类似,在此不再赘述。

[0208] 需要说明的是,应理解以上装置的各个单元的划分仅仅是一种逻辑功能的划分,实际实现时可以全部或部分集成到一个物理实体上,也可以物理上分开。且这些单元可以全部以软件通过处理元件调用的形式实现;也可以全部以硬件的形式实现;还可以部分单元通过软件通过处理元件调用的形式实现,部分单元通过硬件的形式实现。例如,发送单元可以为单独设立的处理元件,也可以集成在该装置的某一个芯片中实现,此外,也可以以程序的形式存储于装置的存储器中,由该装置的某一个处理元件调用并执行该发送单元的功能。其它单元的实现与之类似。此外这些单元全部或部分可以集成在一起,也可以独立实现。这里所述的处理元件可以是一种集成电路,具有信号的处理能力。在实现过程中,上述方法的各步骤或以上各个单元可以通过处理器元件中的硬件的集成逻辑电路或者软件形式的指令完成。此外,以上发送单元是一种控制发送的单元,可以通过该装置的发送装置发送信息。

[0209] 以上这些单元可以是被配置成实施以上方法的一个或多个集成电路,例如:一个或多个特定集成电路(application specific integrated circuit,ASIC),或,一个或多个微处理器(digital singnal processor,DSP),或,一个或者多个现场可编程门阵列(field programmable gate array,FPGA)等。再如,当以上某个单元通过处理元件调度程序的形式实现时,该处理元件可以是通用处理器,例如中央处理器(central processing unit,CPU)或其它可以调用程序的处理器。再如,这些单元可以集成在一起,以片上系统(system-on-a-chip,SOC)的形式实现。

[0210] 图6为本申请另一实施例提供的服务器的结构示意图。如图6所示,本实施例提供的服务器可以包括:该服务器可以包括接收器30、处理器31、存储器32、发送器33和至少一个通信总线34。通信总线34用于实现元件之间的通信连接。存储器32可能包含高速RAM存储器,也可能还包括非易失性存储NVM,例如至少一个磁盘存储器,存储器中可以存储各种程序,用于完成各种处理功能以及实现本实施例的方法步骤。本实施例中的接收器30可以为相应的具有通信功能和接收信息功能的输入接口,本实施例中的发送器33可以为相应的具有通信功能和发送信息功能的输出接口。该处理器31,用于调用并执行该存储器32中存储的程序指令,当该处理器31执行该存储器32存储的程序指令时,该服务器用于执行本申请上述电子投票方法实施例中第一服务器侧的技术方案,其实现原理和技术效果类似,此处不再赘述。

[0211] 图7为本申请另一实施例提供的投票终端的结构示意图。如图7所示,本实施例提供的投票终端可以包括:该投票终端可以包括接收器40、处理器41、存储器42、发送器43和至少一个通信总线44。通信总线44用于实现元件之间的通信连接。存储器42可能包含高速RAM存储器,也可能还包括非易失性存储NVM,例如至少一个磁盘存储器,存储器中可以存储

各种程序，用于完成各种处理功能以及实现本实施例的方法步骤。本实施例中的接收器40可以为相应的具有通信功能和接收信息功能的输入接口，本实施例中的发送器43可以为相应的具有通信功能和发送信息功能的输出接口。该处理器41，用于调用并执行该存储器42中存储的程序指令，当该处理器41执行该存储器42存储的程序指令时，该投票终端用于执行本申请上述电子投票方法实施例中投票终端侧的技术方案，其实现原理和技术效果类似，此处不再赘述。

[0212] 本申请还提供一种存储介质，包括：可读存储介质和计算机程序，所述计算机程序用于实现前述任一实施例提供的电子投票方法。

[0213] 本申请还提供一种程序产品，该程序产品包括计算机程序(即执行指令)，该计算机程序存储在可读存储介质中。第一服务器的至少一个处理器可以从可读存储介质读取该计算机程序，至少一个处理器执行该计算机程序使得第一服务器实施前述各种实施方式提供的电子投票方法。

[0214] 本申请实施例还提供了一种电子投票装置，包括至少一个存储元件和至少一个处理元件、所述至少一个存储元件用于存储程序，该程序被执行时，使得所述电子投票装置执行上述任一实施例中的第一服务器的操作。

[0215] 本申请还提供一种程序产品，该程序产品包括计算机程序(即执行指令)，该计算机程序存储在可读存储介质中。投票终端的至少一个处理器可以从可读存储介质读取该计算机程序，至少一个处理器执行该计算机程序使得投票终端实施前述各种实施方式提供的电子投票方法。

[0216] 本申请实施例还提供了一种电子投票装置，包括至少一个存储元件和至少一个处理元件、所述至少一个存储元件用于存储程序，该程序被执行时，使得所述电子投票装置执行上述任一实施例中的投票终端的操作。

[0217] 实现上述各方法实施例的全部或部分步骤可以通过程序指令相关的硬件来完成。前述的程序可以存储于一可读取存储器中。该程序在执行时，执行包括上述各方法实施例的步骤；而前述的存储器(存储介质)包括：只读存储器(英文：read-only memory，缩写：ROM)、RAM、快闪存储器、硬盘、固态硬盘、磁带(英文：magnetic tape)、软盘(英文：floppy disk)、光盘(英文：optical disc)及其任意组合。

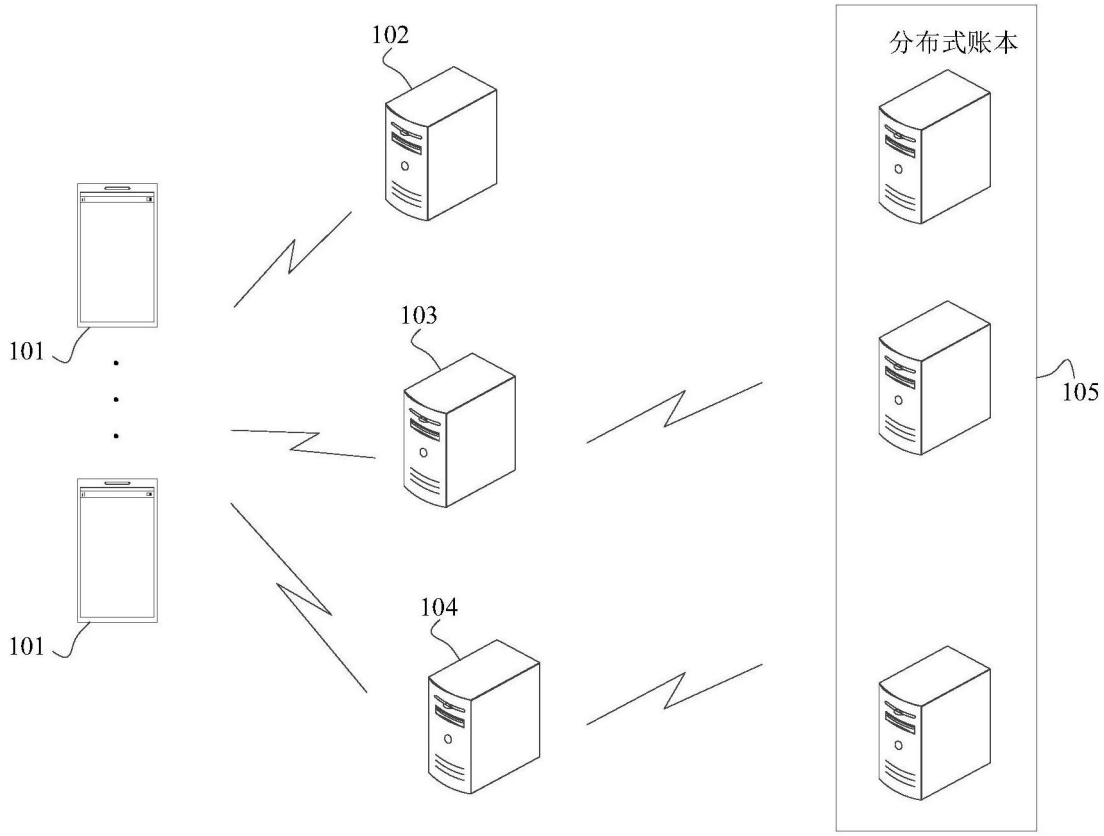


图1

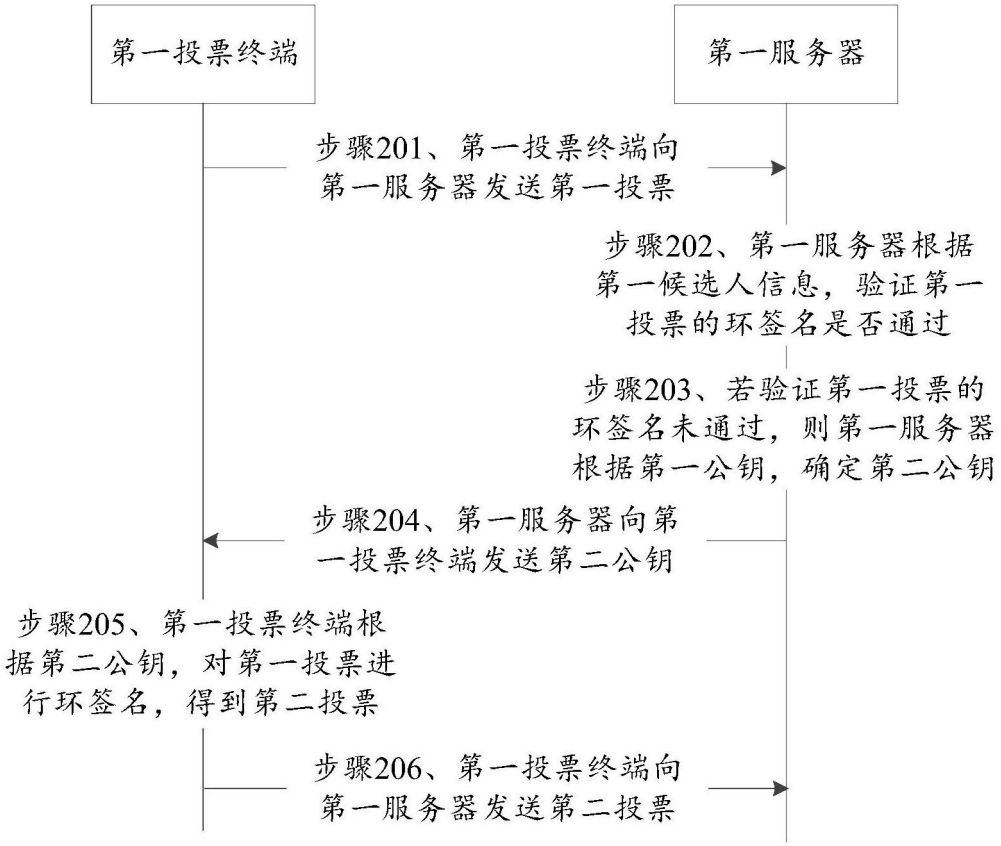

第一投票终端
第一服务器
步骤201、第一投票终端向第一服务器发送第一投票
步骤202、第一服务器根据第一候选人信息，验证第一投票的环签名是否通过
步骤203、若验证第一投票的环签名未通过，则第一服务器根据第一公钥，确定第二公钥
步骤204、第一服务器向第一投票终端发送第二公钥
步骤205、第一投票终端根据第二公钥，对第一投票进行环签名，得到第二投票
步骤206、第一投票终端向第一服务器发送第二投票

图2

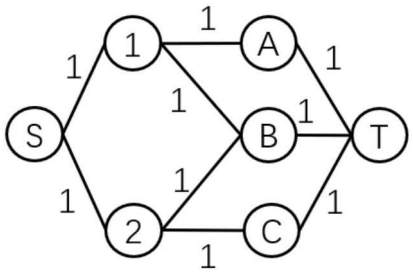

S
1
2
A
B
C
T
1

图3

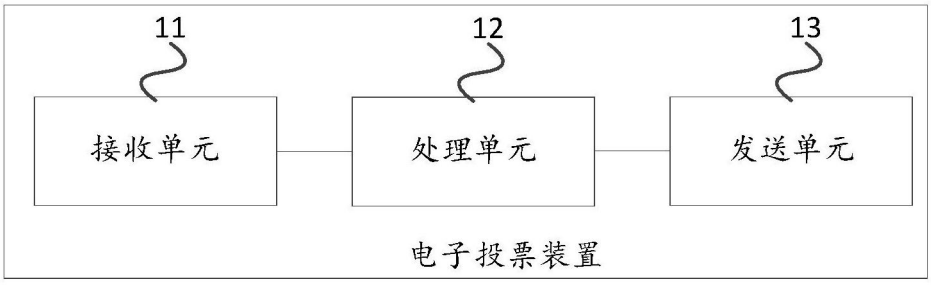

11
12
13
接收单元
处理单元
发送单元
电子投票装置

图4

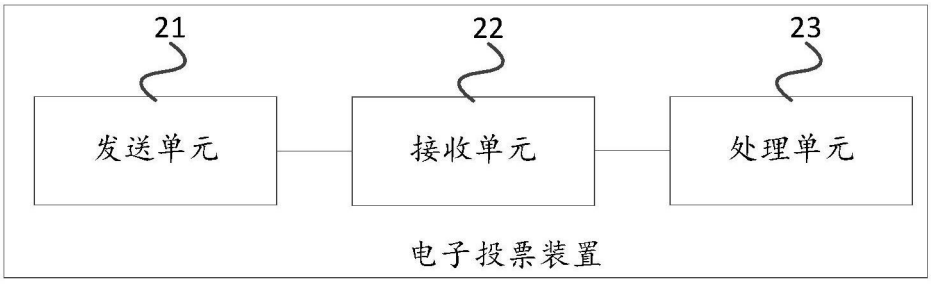

21
22
23
发送单元
接收单元
处理单元
电子投票装置

图5

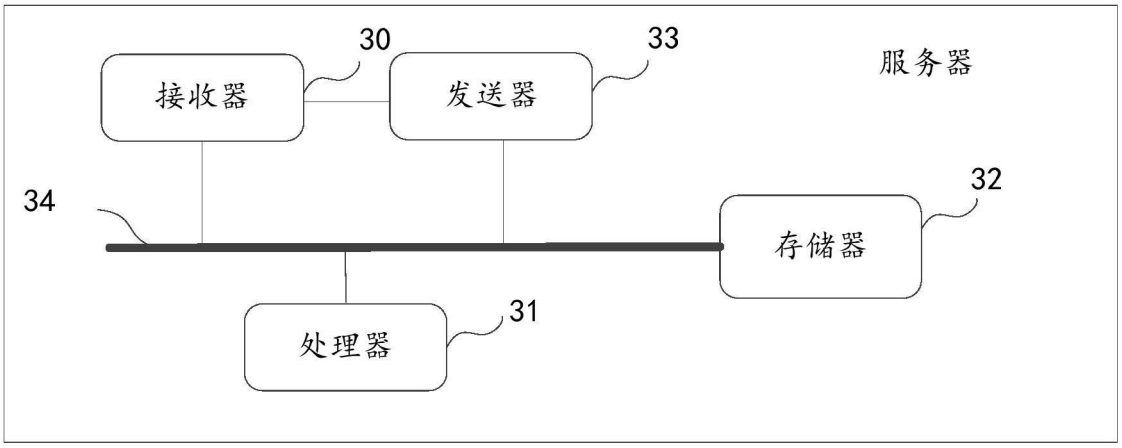

30
33
接收器
发送器
服务器
34
32
存储器
31
处理器

图6

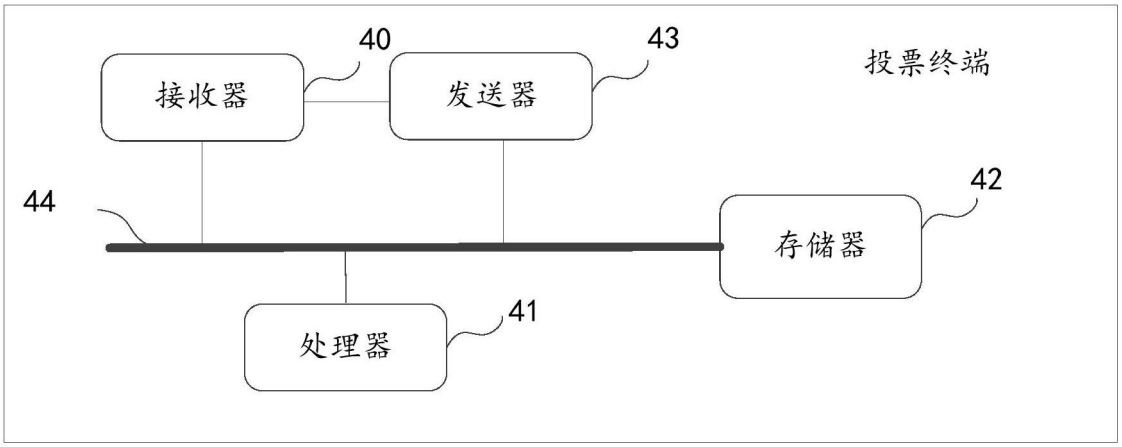

40
43
接收器
发送器
投票终端
44
42
存储器
41
处理器

图7