(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 110266478 B
(45)授权公告日 2021.05.18

(21)申请号 201910472125.7

(22)申请日 2019.05.31

(65)同一申请的已公布的文献号
申请公布号 CN 110266478 A

(43)申请公布日 2019.09.20

(73)专利权人 联想(北京)有限公司
地址 100085 北京市海淀区上地西路6号2幢2层201-H2-6

(72)发明人 马逸龙 过晓冰 王云浩

(74)专利代理机构 北京派特恩知识产权代理有限公司 11270
代理人 姚璐 张颖玲

(51)Int.Cl.
H04L 9/08(2006.01)
H04L 9/06(2006.01)

(56)对比文件
CN 104539423 A,2015.04.22
CN 107248909 A,2017.10.13
CN 109672539 A,2019.04.23

审查员 董智青

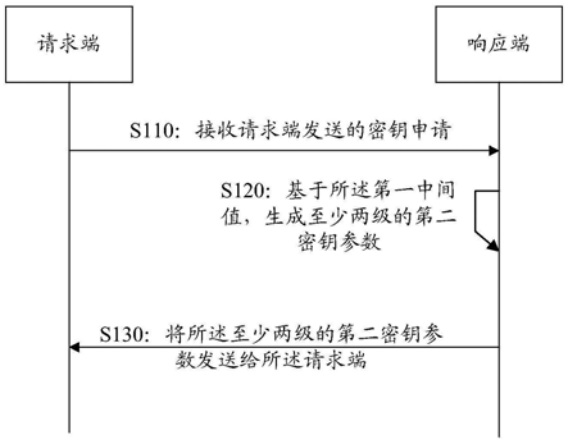
权利要求书2页 说明书15页 附图4页

(54)发明名称

一种信息处理方法、电子设备

(57)摘要

本发明实施例提供一种信息处理方法、电子设备。所述信息处理方法包括:接收请求端发送的密钥申请,所述密钥申请携带有第一中间值;所述第一中间值为所述请求端基于所述第一密钥参数生成;基于所述第一中间值,生成至少两级的第二密钥参数;将所述至少两级的第二密钥参数发送给所述请求端;所述至少两级的第二密钥参数和所述第一密钥参数,共同用于供所述请求端生成私钥。



CN 110266478 B

1.一种信息处理方法,包括:

接收请求端发送的密钥申请,所述密钥申请携带有第一中间值;所述第一中间值为所述请求端基于第一密钥参数生成;

基于所述第一中间值,生成至少两级的第二密钥参数;所述至少两级的第二密钥参数包括:第一级响应端的第二密钥参数、中间级响应端的第二密钥参数和最后一级响应端的第二密钥参数;

将所述至少两级的第二密钥参数发送给所述请求端;所述至少两级的第二密钥参数和所述第一密钥参数,共同用于供所述请求端生成私钥。

2.根据权利要求1所述的方法,所述基于所述第一中间值,生成至少两级的第二密钥参数,包括:

若当前响应端为第一级响应端,接收所述第一中间值;基于所述第一中间值,生成所述第一级响应端的第二密钥参数;将所述第一级响应端的第二密钥参数发送给第二级响应端;

若当前响应端为中间级响应端,接收前一级响应端的第二密钥参数;基于所述前一级响应端的第二密钥参数,生成所述中间级响应端的第二密钥参数;将所述中间级响应端的第二密钥参数发送给后一级响应端;

若当前响应端为最后一级响应端,接收前一级响应端的第二密钥参数;基于所述前一级响应端的第二密钥参数,生成所述最后一级响应端的第二密钥参数。

3.根据权利要求1所述的方法,所述第二密钥参数包括:公钥参数;

所述方法还包括:

将至少两级的所述公钥参数通过区块链的共识验证之后,记录在区块链中。

4.根据权利要求1所述的方法,所述第二密钥参数包括:私钥参数;

所述基于所述第一中间值,生成至少两级的第二密钥参数,包括:

获取请求端发送的标识信息;

生成随机数以及第三密钥参数;

基于所述第一中间值、所述标识信息及所述随机数,生成哈希值;

利用第一函数以所述哈希值、所述随机数及所述第三密钥参数为已知量,计算获得私钥参数。

5.根据权利要求4所述的方法,所述利用第一函数以所述哈希值、所述随机数及所述第三密钥参数为已知量,计算获得私钥参数,包括:

将所述哈希值进行二进制转换,获得32位的第一数值;

获得所述第一数值的高16位二进制以及低16位二进制;

将所述高16位二进制进行十进制转换,获得第一子数值;

将所述低16位二进制进行十进制转换,获得第二子数值;

基于所述第一子数值与所述随机数的乘积,及所述第二子数值与所述第三密钥参数的乘积,计算获得私钥参数。

6.一种信息处理方法,包括:

基于第一密钥参数,获得第一中间值;

向响应端发送携带有所述第一中间值的密钥申请;

接收所述响应端基于所述第一中间值返回的至少两级的第二密钥参数;所述至少两级的第二密钥参数包括:第一级响应端的第二密钥参数、中间级响应端的第二密钥参数和最后一级响应端的第二密钥参数;

基于所述至少两级的第二密钥参数和所述第一密钥参数,生成私钥。

7.根据权利要求6所述的方法,所述接收所述响应端基于所述第一中间值返回的至少两级的第二密钥参数,包括:

接收所述响应端返回的第一级响应端的第二密钥参数、中间级响应端的第二密钥参数及最后一级响应端的第二密钥参数;

其中,所述第一级响应端的第二密钥参数基于所述第一中间值生成;所述第一级响应端的第二密钥参数用于发送给第二级响应端;

所述中间级响应端的第二密钥参数基于前一级响应端的第二密钥参数生成;所述中间级响应端的第二密钥参数用于发送给后一级响应端;

所述最后一级响应端的第二密钥参数基于前一级响应端的第二密钥参数生成;所述最后一级响应端的第二密钥参数用于发送给请求端。

8.根据权利要求6所述的方法,所述第二密钥参数包括:私钥参数和公钥参数;

所述基于至少两级的第二密钥参数和所述第一密钥参数,生成私钥,包括:

基于最后一级响应端的私钥参数和所述第一密钥参数,确定临时私钥参数;

验证所述临时私钥参数与所述至少两级的公钥参数的对应关系;

若验证通过,确定所述临时私钥参数为私钥。

9.一种电子设备,包括:

第一接收模块,用于接收请求端发送的密钥申请,所述密钥申请携带有第一中间值;所述第一中间值为所述请求端基于第一密钥参数生成;

第一生成模块,用于基于所述第一中间值,生成至少两级的第二密钥参数;所述至少两级的第二密钥参数包括:第一级响应端的第二密钥参数、中间级响应端的第二密钥参数和最后一级响应端的第二密钥参数;

第一发送模块,用于将所述至少两级的第二密钥参数发送给所述请求端;所述至少两级的第二密钥参数和所述第一密钥参数,共同用于供所述请求端生成私钥。

10.一种电子设备,包括:

计算模块,用于基于第一密钥参数,获得第一中间值;

第二发送模块,用于向响应端发送携带有所述第一中间值的密钥申请;

第二接收模块,用于接收所述响应端基于所述第一中间值返回的至少两级的第二密钥参数;所述至少两级的第二密钥参数包括:第一级响应端的第二密钥参数、中间级响应端的第二密钥参数和最后一级响应端的第二密钥参数;

第二生成模块,用于基于所述至少两级的第二密钥参数和所述第一密钥参数,生成私钥。

一种信息处理方法、电子设备

技术领域

[0001] 本发明涉及通信领域的技术领域，尤其涉及一种信息处理方法、电子设备。

背景技术

[0002] 目前公钥密码体制有以下三种方案：基于证书的公钥密码体制PKI、基于标识的公钥密码体制IBC以及无证书公钥密码体制CLPKC。其中，采用PKI需要使用证书权威机构CA颁发证书来建立用户实体与公钥之间的联系，然而证书的管理(例如颁发、更新、撤销)不仅操作复杂，还需要消耗很多计算资源和存储资源。其中IBC虽然消除了对证书的依赖；但是用户的公钥由用户标识唯一确定，用户的私钥由信任权威机构生成。因而采用IBC会引入了私钥托管问题，且用户签名不具有唯一性和不可否认性。其中CLPKC虽然不使用证书，但是该CLPKC是仅采用一个密钥生成中心的架构，因而使用该方案存在因该密钥生成中心作恶或被攻破而带来的系统安全性问题。

发明内容

[0003] 本发明实施例提供了一种信息处理方法、电子设备。

[0004] 本发明的技术方案是这样实现的：

[0005] 一种信息处理方法，包括：

[0006] 接收请求端发送的密钥申请，所述密钥申请携带有第一中间值；所述第一中间值为所述请求端基于所述第一密钥参数生成；

[0007] 基于所述第一中间值，生成至少两级的第二密钥参数；

[0008] 将所述至少两级的第二密钥参数发送给所述请求端；所述至少两级的第二密钥参数和所述第一密钥参数，共同用于供所述请求端生成私钥。

[0009] 上述方案中，所述基于所述第一中间值，生成至少两级的第二密钥参数，包括：

[0010] 若当前响应端为第一级响应端，接收所述第一中间值；基于所述第一中间值，生成所述第一级响应端的第二密钥参数；将所述第一级响应端的第二密钥参数发送给第二级响应端；

[0011] 若当前响应端为中间级响应端，接收前一级响应端的第二密钥参数；基于所述前一级响应端的第二密钥参数，生成所述中间级响应端的第二密钥参数；将所述中间级响应端的第二密钥参数发送给后一级响应端；

[0012] 若当前响应端为最后一级响应端，接收前一级响应端的第二密钥参数；基于所述前一级响应端的第二密钥参数，生成所述最后一级响应端的第二密钥参数。

[0013] 上述方案中，所述将所述至少两级的第二密钥参数发送给所述请求端，包括：

[0014] 将所述第一级响应端的第二密钥参数、所述中间级响应端的第二密钥参数及所述最后一级响应端的第二密钥参数发送给所述请求端。

[0015] 上述方案中，所述第二密钥参数包括：公钥参数；

[0016] 所述方法还包括：

[0017] 将所述至少两级的所述公钥参数通过区块链的共识验证之后，记录在区块链中。

[0018] 上述方案中，所述第二密钥参数包括：私钥参数；

[0019] 所述基于所述第一中间值，生成至少两级的第二密钥参数，包括：

[0020] 获取请求端发送的标识信息；

[0021] 生成随机数以及第三密钥参数；

[0022] 基于所述第一中间值、所述标识信息及所述随机数，生成哈希值；

[0023] 利用第一函数以所述哈希值、所述随机数及所述第三密钥参数为已知量，计算获得私钥参数。

[0024] 上述方案中，所述利用第一函数以所述哈希值、所述随机数及所述第三密钥参数为已知量，计算获得私钥参数，包括：

[0025] 将所述哈希值进行二进制转换，获得32位的第一数值；

[0026] 获得所述第一数值的高16位二进制以及低16位二进制；

[0027] 将所述高16位二进制进行十进制转换，获得第一子数值；

[0028] 将所述低16位二进制进行十进制转换，获得第二子数值；

[0029] 基于所述第一子数值与所述随机数的乘积，及所述第二子数值与所述第三密钥参数的乘积，计算获得私钥参数。

[0030] 上述方案中，所述方法还包括：

[0031] 若当前响应端为第一级响应端，将所述第一级响应端的第三密钥参数中公钥参数发送给中间级响应端和/或最后一级响应端；

[0032] 若当前响应端为中间级响应端，将所述中间级响应端的第三密钥参数中公钥参数发送给第一级响应端和/或最后一级响应端；

[0033] 若当前响应端为最后一级响应端，将所述最后一级响应端的第三密钥参数中公钥参数发送给第一级响应端和/或中间级响应端。

[0034] 本发明实施例还提供了一种信息处理方法，包括：

[0035] 基于第一密钥参数，获得第一中间值；

[0036] 向响应端发送携带有所述第一中间值的密钥申请；

[0037] 接收所述响应端基于所述第一中间值返回的至少两级的第二密钥参数；

[0038] 基于所述至少两级的第二密钥参数和所述第一密钥参数，生成私钥。

[0039] 上述方案中，所述基于第一密钥参数，获得第一中间值，包括：

[0040] 利用单向函数以所述第一密钥参数为已知量，计算得到第一中间值。

[0041] 上述方案中，所述接收所述响应端基于所述第一中间值返回的至少两级的第二密钥参数，包括：

[0042] 接收所述响应端返回的第一级响应端的第二密钥参数、中间级响应端的第二密钥参数及最后一级响应端的第二密钥参数；

[0043] 其中，所述第一级响应端的第二密钥参数基于所述第一中间值生成；所述第一级响应端的第二密钥参数用于发送给第二级响应端；

[0044] 所述中间级响应端的第二密钥参数基于前一级响应端的第二密钥参数生成；所述中间级响应端的第二密钥参数用于发送给后一级响应端；

[0045] 所述最后一级响应端的第二密钥参数基于前一级响应端的第二密钥参数生成；所

述最后一级响应端的第二密钥参数用于发送给请求端。

[0046] 上述方案中，所述第二密钥参数包括：私钥参数和公钥参数；

[0047] 所述基于所述至少两级的第二密钥参数和所述第一密钥参数，生成私钥，包括：

[0048] 基于最后一级响应端的私钥参数和所述第一密钥参数，确定临时私钥参数；

[0049] 验证所述临时私钥参数与所述至少两级的公钥参数的对应关系；

[0050] 若验证通过，确定所述临时私钥参数为私钥。

[0051] 上述方案中，所述第二密钥参数包括：公钥参数；

[0052] 所述方法还包括：

[0053] 获取至少两级的第三密钥参数以及所述至少两级的所述公钥参数；

[0054] 基于所述至少两级的公钥参数、标识信息及所述至少两级的第三密钥参数，生成公钥。

[0055] 上述方案中，所述获取至少两级的所述公钥参数，包括：

[0056] 获取记录在区块链中的至少两级的所述公钥参数；所述记录在区块链中的公钥参数为通过区块链共识验证后的公钥参数。

[0057] 上述方案中，所述获取至少两级的第三密钥参数，包括：

[0058] 基于第一级响应端、中间级响应端以及最后一级响应端中的至少一个响应端获取各响应端的第三密钥参数中公钥参数。

[0059] 本发明实施例还提供了一种电子设备，包括：

[0060] 第一接收模块，用于接收请求端发送的密钥申请，所述密钥申请携带有第一中间值；所述第一中间值为所述请求端基于所述第一密钥参数生成；

[0061] 第一生成模块，用于基于所述第一中间值，生成至少两级的第二密钥参数；

[0062] 第一发送模块，用于将所述至少两级的第二密钥参数发送给所述请求端；所述至少两级的第二密钥参数和所述第一密钥参数，共同用于供所述请求端生成私钥。

[0063] 本发明实施例还提供了一种电子设备，包括：

[0064] 计算模块，用于基于第一密钥参数，获得第一中间值；

[0065] 第二发送模块，用于向响应端发送携带有所述第一中间值的密钥申请；

[0066] 第二接收模块，用于接收所述响应端基于所述第一中间值返回的至少两级的第二密钥参数；

[0067] 第二生成模块，用于基于所述至少两级的第二密钥参数和所述第一密钥参数，生成私钥。

[0068] 本发明实施例所述提供的信息处理方法，响应端接收请求端发送的密钥申请，所述密钥申请携带有第一中间值；所述第一中间值为所述请求端基于所述第一密钥参数生成；基于所述第一中间值，生成至少两级的第二密钥参数，而并非直接生成私钥，而私钥的生成由请求端基于所述至少两级的第二密钥参数以及第一密钥参数生成；如此，响应端无需托管请求端的私钥，在网络中也没有传输私钥，减少了私钥在托管和传输过程中的泄露现象，减少了因为泄露导致的安全问题。

[0069] 且，本发明实施例中，由于可以基于第一中间值，生成至少两级的第二密钥参数，也就是说私钥的生成并非基于一个响应端的第二密钥参数生成，而是基于至少两个级别的响应端的第二密钥参数生成；如此，即便至少两个级别的响应端中部分响应端被攻破或者

作恶(例如部分第二密钥参数泄露),私钥也不容易被破解,从而进一步提高了私钥的安全性。

附图说明

[0070] 图1为本发明实施例提供的一种信息处理方法的流程示意图;

[0071] 图2为本发明一实施例中的区块链结构示意图;

[0072] 图3为本发明实施例提供的另一种信息处理方法的流程示意图;

[0073] 图4为本发明实施例提供的一种信息处理装置示意图;

[0074] 图5为本发明实施例提供的另一种信息处理装置示意图;

[0075] 图6为本发明实施例提供的又一种信息处理方法的流程示意图;

[0076] 图7为本发明一实施例中验签算法签名的示意图;

[0077] 图8为本发明实施例提供的一种电子设备的硬件结构示意图。

具体实施方式

[0078] 下结合附图及实施例,对本发明进行进一步详细说明。应当理解,此处所描述的具体实施例仅仅用以解释本发明,并不用于限定本发明。

[0079] 除非另有定义,本文所使用的所有的技术和科学术语与属于本发明的技术领域的技术人员通常理解的含义相同。本文中在本发明的说明书中所使用的术语只是为了描述具体的实施例的目的,不是旨在于限制本发明。本文所使用的术语“和/或”包括一个或多个相关的所列项目的任意的和所有的组合。

[0080] 如图1所示,本发明实施例提供了一种信息处理方法,包括:

[0081] 步骤S110:接收请求端发送的密钥申请,所述密钥申请携带有第一中间值;所述第一中间值为所述请求端基于所述第一密钥参数生成;

[0082] 步骤S120:基于所述第一中间值,生成至少两级的第二密钥参数;

[0083] 步骤S130:将所述至少两级的第二密钥参数发送给所述请求端;所述至少两级的第二密钥参数和所述第一密钥参数,共同用于供所述请求端生成私钥。

[0084] 这里,所述第一密钥参数可以是请求端随机生成的秘密值;所述第二密钥参数包括但不限于各响应端的私钥参数和/或私钥参数。

[0085] 本发明实施例所提供的信息处理方法,应用于响应端;所述响应端包括至少两级的响应端;所述响应端为各种类型的电子设备;所述电子设备包括终端、服务器或者通信网元等。

[0086] 在一些实施例中,所述响应端包括N个密钥生成中心(KGC);所述N为大于或等于2的自然数。

[0087] 响应端会从请求端接收密钥申请,在本发明实施例中,密钥申请携带的是第一中间值;所述第一中间值可以是请求端基于第一密钥参数生成的。所述响应端接收到第一中间值后,基于所述第一中间值生成第二密钥参数,而非直接生成私钥。所述第二密钥参数用于请求端根据所述第一密钥参数以及第二密钥参数生成私钥。如此,响应端不用管理请求端的私钥,也不用将私钥通过网络传输给请求端,减少了托管和传输私钥导致的私钥泄露现象,减少了因为泄露导致的安全问题。

[0088] 且，由于所述响应端为包括至少两级的响应端，生成至少两级的第二密钥参数；也就是说私钥的生成并非基于一个响应端的第二密钥参数生成，而是基于至少于两个级别的响应端的第二密钥参数生成；如此，即便至少两个级别的响应端中的部分响应端被攻破或者作恶(例如部分第二密钥参数泄露)，私钥也不容易被破解，从而进一步提高了私钥的安全性。

[0089] 在一些实施例中，所述步骤S120，包括：

[0090] 若当前响应端为第一级响应端，接收所述第一中间值；基于所述第一中间值，生成所述第一级响应端的第二密钥参数；将所述第一级响应端的第二密钥参数发送给第二级响应端；

[0091] 若当前响应端为中间级响应端，接收前一级响应端的第二密钥参数；基于所述前一级响应端的第二密钥参数，生成所述中间级响应端的第二密钥参数；将所述中间级响应端的第二密钥参数发送给后一级响应端；

[0092] 若当前响应端为最后一级响应端，接收前一级响应端的第二密钥参数；基于所述前一级响应端的第二密钥参数，生成所述最后一级响应端的第二密钥参数。

[0093] 例如，若所述响应端包括N个密钥生成中心；所述N个密钥生成中心分别为第1个密钥生成中心、第2个密钥生成中心、……第N-1个密钥生成中心、第N个密钥生成中心；所述N为大于或等于2的自然数；则所述第1个密钥生成中心为第一级响应端，所述2个密钥生成中心、……、所述第N-1个密钥生成中心为中间级响应端；所述第N个密钥生成中心为最后一级响应端。

[0094] 在一些实施例中，所述将所述至少两级的第二密钥参数发送给所述请求端，包括：

[0095] 将所述第一级响应端的第二密钥参数、所述中间级响应端的第二密钥参数及所述最后一级响应端的第二密钥参数发送给所述请求端。

[0096] 在一实施例中，所述响应端包括N个密钥生成中心；所述N个密钥生成中心分别为第1个密钥生成中心、第2个密钥生成中心、……第N-1个密钥生成中心、第N个密钥生成中心；所述第1个密钥生成中心接收请求端发送的密钥申请，所述密钥申请中携带第一中间值X_A；并基于所述X_A，生成所述第1个密钥生成中心的第二密钥参数$(PA_1、z_1)$；所述第2个密钥生成中心接收所述第1个密钥生成中心发送的$(PA_1、z_1)$；基于所述$(PA_1、z_1)$，生成第2个密钥生成中心的第二密钥参数$(PA_2、z_2)$；并将所述$(PA_2、z_2)$发送给第3个密钥生成中心；依次类推；所述第N-1密钥生成中心接收第N-2个密钥生成中心发送的$(PA_{N-2}、z_{n-2})$；基于所述$(PA_{N-2}、z_{n-2})$生成第N-1个密钥生成中心的第二密钥参数$(PA_{N-1}、z_{n-1})$；并将所述$(PA_{N-1}、z_{n-1})$发送个第N个密钥生成中心；所述第N个密钥生成中心接收所述第N-1个密钥生成发送的$(PA_{N-1}、z_{n-1})$；基于所述$(PA_{N-1}、z_{n-1})$生成所述第N个密钥生成中心的第二密钥参数$(PA_n、z_n)$；其中，所述$PA_1、PA_2、……PA_{N-1}、PA_N$为所述第二密钥参数中的公钥参数；所述$z_1、z_2、……z_{n-1}、z_n$为所述第二密钥参数的私钥参数；所述第1个密钥生成中心、第2个密钥生成中心、……第N-1个密钥生成中心、第N个密钥生成中心分别将$PA_1、PA_2、……PA_{N-1}、PA_N$发送给所述请求端；所述第N个密钥生成中心将所述$z_n$发送给所述请求端。

[0097] 在另一实施例中，所述响应端包括N个密钥生成中心；所述N个密钥生成中心分别为第1个密钥生成中心、第2个密钥生成中心、……第N-1个密钥生成中心、第N个密钥生成中心；所述第1个密钥生成中心接收请求端发送的密钥申请，所述密钥申请中携带第一中间值

X_A;并基于所述X_A,生成所述第1个密钥生成中心的第二密钥参数(PA_1、z_1);所述第2个密钥生成中心接收所述第1个密钥生成中心发送的(PA_1、z_1);基于所述(PA_1、z_1),生成第2个密钥生成中心的第二密钥参数(PA_2、z_2);并将所述(PA_1、PA_2、z_2)发送给第3个密钥生成中心;依次类推;所述第N-1密钥生成中心接收第N-2个密钥生成中心发送的(PA_1、PA_2、……PA_{N-2}、z_{N-2});基于所述(PA_{N-2}、z_{n-2})生成第N-1个密钥生成中心的第二密钥参数(PA_{N-1}、z_{n-1});并将所述(PA_1、PA_2、……PA_{N-2}、PA_{N-1}、z_{n-1})发送个第N个密钥生成中心;所述第N个密钥生成中心接收所述第N-1个密钥生成发送的(PA_1、PA_2、……PA_{n-2}、PA_{N-1}、z_{n-1});基于所述(PA_{N-1}、z_{n-1})生成所述第N个密钥生成中心的第二密钥参数(PA_N、z_n);其中,所述PA_1、PA_2、……PA_{N-1}、PA_N为所述第二密钥参数中的公钥参数;所述z_1、z_2、……z_{n-1}、z_n为所述第二密钥参数的私钥参数;所述第N个密钥生成中心将(PA_1、PA_2、……PA_{N-1}、PA_N、z_n)发送给所述请求端。

[0098] 在一些实施例中,所述响应端还接收用户的标识信息,所述标识信息用于与所述第二密钥参数中的公钥参数,共同用于生成哈希值;基于所述哈希值,生成所述第二密钥参数的私钥参数。

[0099] 本发明实施例,构建了一个多响应端的密钥生成体制,可以基于多个响应端生成多个第二密钥参数,且其中多个响应端中后一个响应端的第二密钥参数是基于前一个响应端的密钥生成参数而生成的,而私钥是基于所有响应端的第二密钥参数才能生成;如此,当其中部分响应端作恶或者部分响应端的第二密钥生成参数被泄露,所述私钥也不容易被破解。如此,采用本发明实施例的多响应端的密钥生成体制,能够具备容忍一定数量的响应端被攻破的情况发生,能够大大提高私钥的安全性。

[0100] 在一些应用中,所述多响应端的密钥生成体制可应用在区块链中,可以解决联盟链中CA证书体制过于臃肿的问题。

[0101] 例如,在一些实施例中,所述第二密钥参数包括:公钥参数;所述方法还包括:将所述至少两级的所述公钥参数通过区块链的共识验证之后,记录在区块链中。

[0102] 在本发明实施例中,可以通过共识验证,使得所述公钥参数获得区块链中的每个节点的信任。而将所述密钥参数记录在区块链中,可以使得任意一个节点都可以从区块链中获取用户对应的各个KGC(即响应端)的公钥参数;如此,可以使得多方运营商不需要各自保存各用户对应的各个KGC的公钥参数,能够节约存储资源;同时,由于是使用了本发明实施例中的多响应端的密钥生成体制替代了联盟链中CA证书体制,从而可以解决联盟链中CA证书体制过于臃肿的问题。

[0103] 在一些实施例中,所述方法还包括:若当前响应端为第一级响应端,将所述第一级响应端的第三密钥参数中公钥参数发送给中间级响应端和/或最后一级响应端;

[0104] 若当前响应端为中间级响应端,将所述中间级响应端的第三密钥参数中公钥参数发送给第一级响应端和/或最后一级响应端;

[0105] 若当前响应端为最后一级响应端,将所述最后一级响应端的第三密钥参数中公钥参数发送给第一级响应端和/或中间级响应端。

[0106] 在本发明实施例中,区块链中的各节点都可以获取其它节点对应的响应端(例如KGC)的公钥参数,可使得各个KGC的公钥参数可以共享;如此,有利于某个节点获取部分或者全部KGC进行加密、解密和/或签名认证等操作。

[0107] 在实际应用中,应用上述多响应端的密钥生成体制代替现有的CA体制。如图2所

示，联盟链中以节点作为基本单元，一个联盟链中可包含若干个组织，每个组织可包含若干个节点；其中，一个组织可包括一个KGC。所述多响应端的密钥生成体制包括KGC_1、KGC_2和KGC_3；所述KGC_1、所述KGC_2和所述KGC_3分别与多个节点Peer连接。应用在区块链中的多响应端的密钥生成体制的信息处理方法包括以下步骤：

[0108] 步骤S1：区块链系统初始化阶段；

[0109] 具体地，各组织启动各自的KGC；所述KGC之间使用可信手段分享主公钥。各节点peer基于注册的标识信息ID以及各自的第三密钥参数中的主私钥，生成第二密钥参数。其中，所述第二密钥参数包括公钥参数和私钥参数；所述第三密钥参数包括主公钥和主私钥。

[0110] 在一可选实施例中，将各KGC所属组织下节点的部分公钥参数写入创世块。

[0111] 步骤S2：背书环节；

[0112] 具体地，发起节点将交易消息进行封装；并使用所述私钥参数进行签名，获得所述签名结果；将所述身份标识、所述交易消息、所述公钥参数、所述签名结果发送给背书节点。所述背书节点执行验签算法，若验签通过则进行交易的模拟执行，将执行结果返回给所述发起节点；若确定所述发起节点收到足够的所述背书节点通过的交易消息后，将所述交易消息的封装发给排序节点。

[0113] 在一可选实施例中，所述发起节点不发送公钥参数；所述背书节点通过区块链的创始块信息获取所述公钥参数。

[0114] 步骤S3：排序环节；

[0115] 具体的，所述排序节点对时间窗内的所有有效交易进行排序、出块；使用反熵算法将块信息广播给区块链中的所有节点。

[0116] 步骤S4：确认环节。

[0117] 具体地，所有节点验证、记录、并确认块信息内的交易，将所述交易写入区块链，并更新账本状态。

[0118] 在一些实施例中，所述第二密钥参数包括：私钥参数；

[0119] 所述步骤S120，包括：

[0120] 获取请求端发送的标识信息；

[0121] 生成随机数以及第三密钥参数；

[0122] 基于所述第一中间值、所述标识信息及所述随机数，生成哈希值；

[0123] 利用第一函数以所述哈希值、所述随机数及所述第三密钥参数为已知量，计算获得私钥参数。

[0124] 其中，所述基于所述第一中间值、所述标识信息及所述随机数，生成哈希值的一种实现方式是：可以基于所述第一中间参数以及所述随机数，生成第二密钥参数的公钥参数；基于所述标识信息以及所述第二密钥参数的公钥参数生成哈希值。

[0125] 这里，所述哈希值可以为所述标识信息与所述第二密钥参数的公钥参数的串接。例如，所述ID为1212，所述第二密钥参数的公钥参数为21345；则所述哈希值为121221345。

[0126] 在本发明实施例中，是利用用户的标识信息与第二密钥参数的公钥参数，共同生成第二密钥的私钥参数，即将用户的标识信息与所述公钥参数绑定在一起，可以大大降低替换公钥攻击、假冒身份攻击和伪造签名攻击的情况出现。

[0127] 在一实施例中，所述利用第一函数以所述哈希值、所述随机数及所述第三密钥参

数为已知量，计算获得私钥参数，包括：

[0128] 将所述哈希值进行二进制转换，获得32位的第一数值；

[0129] 获得所述第一数值的高16位二进制以及低16位二进制；

[0130] 将所述高16位二进制进行十进制转换，获得第一子数值；

[0131] 将所述低16位二进制进行十进制转换，获得第二子数值；

[0132] 基于所述第一子数值与所述随机数的乘积，及所述第二子数值与所述第三密钥参数的乘积，计算获得私钥参数。

[0133] 例如，所述哈希值为2^{20}进行二进制转换，获得32位的第一数值为：00000000000100000000000000000000；获得所述第一数值的高16位二进制为：0000000000010000，以及所述第一数值的低16位二进制为：0000000000000000；将所述高16位二进制进行十进制转换，获得第一子数值为：16；将所述低16位二进制进行十进制转换，获得第二子数值为：0；这里，由于所述第二子数值为0，则所述第二子数值与所述第三密钥参数的乘积为0；所述基于所述第一子数值与所述随机数的乘积，及所述第二子数值与所述第三密钥参数的乘积，计算获得私钥参数为基于所述第一子数值与所述随机数的乘积计算获得私钥参数。

[0134] 在本实施例中，可以将哈希值进行高16位二进制以及低16位二进制的拆分，基于高16位二进制进行十进制转换获得的第一子数值以及低16位二进制进行十进制转换第二进行计算；如此，提供了一种获取私钥参数的算法，同时该算法比较简单易实现，可以简化私钥参数的计算。且，由于本发明实施例是利用基于第一子数值与所述随机数的乘积、以及所述第二子数值与第三密钥参数的乘积，计算获得所述私钥参数；而该种计算方式与椭圆曲线的计算式相关，若所述第一中间值的获取是基于椭圆曲线的生成元为已知量而利用单线函数获取的，则该种计算方式与椭圆曲线算法相匹配，能够进一步优化算法，提升计算效率。

[0135] 如图3所示，本发明实施例提供了一种信息处理方法，包括：

[0136] 步骤S210：基于第一密钥参数，获得第一中间值；

[0137] 步骤S220：向响应端发送携带有所述第一中间值的密钥申请；

[0138] 步骤S230：接收所述响应端基于所述第一中间值返回的至少两级的第二密钥参数；

[0139] 步骤S240：基于所述至少两级的第二密钥参数和所述第一密钥参数，生成私钥。

[0140] 本发明实施例所提供的信息处理方法，应用于请求端；所述请求端为各种类型的电子设备；所述电子设备包括终端、服务器或者通信网元等。

[0141] 其中，所述第一密钥参数为所述请求端生成随机参数，所述随机参数为秘密值。

[0142] 在本发明实施例中，请求端可以随机生成第一密钥参数，基于所述第一密钥参数获得第一中间值；使响应端会从基于所述第一中间值生成第二密钥参数，而非直接生成私钥；所述私钥仍是由所述请求端基于所述第一密钥参数生成以及第二密钥参数生成。如此，请求端对所述私钥有绝对的生成管理权限，且响应端不用管理请求端的私钥，也不用将私钥通过网络传输给请求端，减少了托管和传输私钥导致的私钥泄露现象，减少了因为泄露导致的安全问题。

[0143] 且，在本发明实施例中，由于是获取响应端返回的至少两级的第二密钥参数，基于所述至少两级的第二密钥参数和所述第一密钥参数是，生成私钥；如此，即便所述至少两级

的第二密钥参数的部分第二密钥参数被泄露，私钥也不容易被破解，从而进一步提高了私钥的安全性。

[0144] 在一些实施例中，所述步骤S210，包括：

[0145] 利用单向函数以所述第一密钥参数为已知量，计算得到第一中间值。

[0146] 为了防止第一中间值在网络中进行了传输，被非法端获取到了之后，基于第一中间值以及获取所述第一中间值的函数自行推导出第一密钥参数，再通过拦截第二密钥参数推导出请求端的私钥的现象，在本实施例中，所述第一函数为单向函数。

[0147] 单向函数又称之为单射函数，单向函数具有如下特点：

[0148] 对于每一个输入，函数值都容易计算(多项式时间)，但是给出一个随机输入的函数值，算出原始输入却比较困难(无法在多项式时间内使用确定性图灵机计算)。如此，即便非法端拿到了第二密钥参数和所述单向函数，推导出所述第一密钥参数的难度也是非常大的，如此，大大增加了第一密钥参数被破解的难度，降低了私钥被泄露的风险，提升了私钥的安全性。

[0149] 在一些实施例中，所述步骤S230，包括：

[0150] 接收所述响应端返回的第一级响应端的第二密钥参数、中间级响应端的第二密钥参数及最后一级响应端的第二密钥参数；

[0151] 其中，所述第一级响应端的第二密钥参数基于所述第一中间值生成；所述第一级响应端的第二密钥参数用于发送给第二级响应端；

[0152] 所述中间级响应端的第二密钥参数基于前一级响应端的第二密钥参数生成；所述中间级响应端的第二密钥参数用于发送给后一级响应端；

[0153] 所述最后一级响应端的第二密钥参数基于前一级响应端的第二密钥参数生成；所述最后一级响应端的第二密钥参数用于发送给请求端。

[0154] 其中，所述接收所述响应端返回的第一级响应端的第二密钥参数、中间级响应端的第二密钥参数及最后以及响应端的第二密钥参数的一种实现方式是：从所述最后一级响应端，接收所述第一级响应端的第二密钥参数、所述中间级响应端的第二密钥参数以及所述最后一级响应端的第二密钥参数。

[0155] 所述接收所述响应端返回的第一级响应端的第二密钥参数、中间级响应端的第二密钥参数及最后以及响应端的第二密钥参数的另一种实现方式是：从所述第一级响应端接收所述第一级响应端的第二密钥参数，从所述中间级响应端接收所述中间级响应端的第二密钥参数，从所述最后一级响应端接收所述最后一级响应端的第二密钥参数。

[0156] 在本发明实施例中，各响应端的第二密钥参数都是基于前一个响应端的第二密钥参数生成；如此，当即便其中部分响应端的第二密钥参数被泄露，也不容易获得私钥，从而可以大大提高破解私钥的难度，提高私钥的安全性。

[0157] 在一些实施例中，所述第二密钥参数包括：私钥参数和公钥参数；

[0158] 所述基于所述至少两级的第二密钥参数和所述第一密钥参数，生成私钥，包括：

[0159] 基于最后一级响应端的私钥参数和所述第一密钥参数，确定临时私钥参数；

[0160] 验证所述临时私钥参数与所述至少两级的公钥参数的对应关系；

[0161] 若验证通过，确定所述临时私钥参数为私钥。

[0162] 在请求端获得公钥参数和私钥参数之后，需要对公钥和私钥进行验证，减少请求

端和/或响应端在密钥生成过程中的错误导致的生成的密钥对无法使用的现象。如此，在本实施例中，会验证所述私钥和公钥的验证关系，从而获得正确的私钥。

[0163] 在另一些实施例中，所述方法还包括：获取至少两级的第三密钥参数以及所述至少两级的所述公钥参数；

[0164] 基于所述至少两级的公钥参数、标识信息及所述至少两级的第三密钥参数，生成公钥。

[0165] 这里，所述第三密钥参数包括：公钥参数和私钥参数；所述第三密钥参数的公钥参数为响应端的主公钥；所述第三密钥参数的私钥参数为所述响应端的主私钥；所述主公钥对其它响应端或请求端公开；例如，在区块链系统中，所述主公钥被记录在区块链中；所述主私钥不对其它响应端以及请求端公开。

[0166] 在本发明实施例中，请求端并非直接从响应端获取公钥，而是基于第二密钥参数的公钥参数以及标识信息获取；如此，可以实现自动隐藏对用户公钥的认证，只有标识信息为特定的标识信息的用户才具有与所述私钥对应的公钥。

[0167] 在一些实施例中，所述方法还包括：基于所述公钥对消息进行加密；获得加密后的密文。

[0168] 在另一些实施例中，所述方法还包括：基于所述私钥对密文进行解密；所述密文为利用所述私钥对应的公钥进行加密的消息。

[0169] 在一些实施例中，所述获取至少两级的所述公钥参数，包括：

[0170] 获取记录在区块链中的至少两级的所述公钥参数；所述记录在区块链中的公钥参数为通过区块链共识验证后的公钥参数。

[0171] 例如，当所述多响应端的密钥生成体制应用于区块链中，若响应端将其第二密钥参数中的公钥参数记录在区块链中，所述请求端可以从区块链中获取多响应端生成的第二密钥参数中的公钥参数；如此，能够使得系统节省存储空间，能够简化获取公钥参数的操作。

[0172] 在一些实施例中，所述获取至少两级的第三密钥参数，包括：

[0173] 基于第一级响应端、中间级响应端以及最后一级响应端中的至少一个响应端获取各响应端的第三密钥参数中公钥参数。

[0174] 在本发明实施例中，所述各响应端的第三密钥参数的公钥参数是可以公开的；所述响应端为区块链系统中的各节点时，可通过将各节点信息之间的共享实现各第三密钥参数的公钥参数的共享，从而使得所述请求端可以仅基于一个或几个响应端获取公钥参数以及私钥参数，从而进一步简化了获得公钥和私钥的操作。

[0175] 如图4所示，本发明实施例还提供了一种电子设备，包括：

[0176] 第一接收模块31，用于接收请求端发送的密钥申请，所述密钥申请携带有第一中间值；所述第一中间值为所述请求端基于所述第一密钥参数生成；

[0177] 第一生成模块32，用于基于所述第一中间值，生成至少两级的第二密钥参数；

[0178] 第一发送模块33，用于将所述至少两级的第二密钥参数发送给所述请求端；所述至少两级的第二密钥参数和所述第一密钥参数，共同用于供所述请求端生成私钥。

[0179] 本发明实施例所述的电子设备即对应于前述的响应端。

[0180] 在一些实施例中，所述第一生成模块32，用于若当前响应端为第一级响应端，接收

所述第一中间值;基于所述第一中间值,生成所述第一级响应端的第二密钥参数;将所述第一级响应端的第二密钥参数发送给第二级响应端;

[0181] 若当前响应端为中间级响应端,接收前一级响应端的第二密钥参数;基于所述前一级响应端的第二密钥参数,生成所述中间级响应端的第二密钥参数;将所述中间级响应端的第二密钥参数发送给后一级响应端;

[0182] 若当前响应端为最后一级响应端,接收前一级响应端的第二密钥参数;基于所述前一级响应端的第二密钥参数,生成所述最后一级响应端的第二密钥参数。

[0183] 在一些实施例中,所述第一发送模块33,用于将所述第一级响应端的第二密钥参数、所述中间级响应端的第二密钥参数及所述最后一级响应端的第二密钥参数发送给所述请求端。

[0184] 在一些实施例中,所述第二密钥参数包括:公钥参数;

[0185] 所述电子设备还包括:第一处理模块34,用于将所述至少两级的所述公钥参数通过区块链的共识验证之后,记录在区块链中。

[0186] 在一些实施例中,所述第一发送模块33,还用于若当前响应端为第一级响应端,将所述第一级响应端的第三密钥参数中公钥参数发送给中间级响应端和/或最后一级响应端;若当前响应端为中间级响应端,将所述中间级响应端的第三密钥参数中公钥参数发送给第一级响应端和/或最后一级响应端;若当前响应端为最后一级响应端,将所述最后一级响应端的第三密钥参数中公钥参数发送给第一级响应端和/或中间级响应端。

[0187] 在一些实施例中,所述第二密钥参数包括:私钥参数;

[0188] 所述第一生成模块32,还用于获取请求端发送的标识信息;生成随机数以及第三密钥参数;基于所述第一中间值、所述标识信息及所述随机数,生成哈希值;利用第一函数以所述哈希值、所述随机数及所述第三密钥参数为已知量,计算获得私钥参数。

[0189] 在一些实施例中,所述第一生成模块32,还用于将所述哈希值进行二进制转换,获得32位的第一数值;获得所述第一数值的高16位二进制以及低16位二进制;将所述高16位二进制进行十进制转换,获得第一子数值;将所述低16位二进制进行十进制转换,获得第二子数值;基于所述第一子数值与所述随机数的乘积,及所述第二子数值与所述第三密钥参数的乘积,计算获得私钥参数。

[0190] 如图5所示,本发明实施例还提供一种电子设备,包括:

[0191] 计算模块41,用于基于第一密钥参数,获得第一中间值;

[0192] 第二发送模块42,用于向响应端发送携带有所述第一中间值的密钥申请;

[0193] 第二接收模块43,用于接收所述响应端基于所述第一中间值返回的至少两级的第二密钥参数;

[0194] 第二生成模块44,用于基于所述至少两级的第二密钥参数和所述第一密钥参数,生成私钥。

[0195] 本发明实施例所述的电子设备即对应于前述的请求端。

[0196] 在一些实施例中,所述计算模块41,用于利用单向函数以所述第一密钥参数为已知量,计算得到第一中间值。

[0197] 在一些实施例中,所述第二接收模块,用于接收所述响应端返回的第一级响应端的第二密钥参数、中间级响应端的第二密钥参数及最后一级响应端的第二密钥参数;

[0198] 其中，所述第一级响应端的第二密钥参数基于所述第一中间值生成；所述第一级响应端的第二密钥参数用于发送给第二级响应端；

[0199] 所述中间级响应端的第二密钥参数基于前一级响应端的第二密钥参数生成；所述中间级响应端的第二密钥参数用于发送给后一级响应端；

[0200] 所述最后一级响应端的第二密钥参数基于前一级响应端的第二密钥参数生成；所述最后一级响应端的第二密钥参数用于发送给请求端。

[0201] 在一些实施例中，所述第二密钥参数包括：私钥参数和公钥参数；

[0202] 所述第二生成模块44，用于基于最后一级响应端的私钥参数和所述第一密钥参数，确定临时私钥参数；

[0203] 验证所述临时私钥参数与所述至少两级的公钥参数的对应关系；

[0204] 若验证通过，确定所述临时私钥参数为私钥。

[0205] 在一些实施例中，所述第二密钥参数包括：公钥参数；

[0206] 所述第二接收模块43，用于获取至少两级的第三密钥参数以及所述至少两级的所述公钥参数；

[0207] 所述第二生成模块44，用于基于所述至少两级的公钥参数、标识信息及所述至少两级的第三密钥参数，生成公钥。

[0208] 在一些实施例中，所述第二接收模块43，还用于获取记录在区块链中的至少两级的所述公钥参数；所述记录在区块链中的公钥参数为通过区块链共识验证后的公钥参数。

[0209] 在一些实施例中，所述第二接收模块43，还用于基于第一级响应端、中间级响应端以及最后一级响应端中的至少一个响应端获取各响应端的第三密钥参数中公钥参数。

[0210] 以下结合上述任意实施例提供一个具体示例：

[0211] 在本方案中涉及三个算法：系统初始化算法、私钥生成算法、公钥生成算法。如图6所示，本示例提供的方法可包括如下步骤：

[0212] S21.系统初始化：

[0213] (1)设有N个KGC；所述N个KGC使用统一的椭圆曲线参数{E,G,n}；其中，所述E：$y^2=x^3+ax+b$为有限域F_q上的椭圆曲线；n为素数；G是E上的一个n阶基点；$h_0()$，$h_1()$...$h_m()$是一组$\{0,1\}^*\rightarrow[1,n-1]$的哈希(hash)函数；其中，所述m为大于或等于1的正整数。

[0214] (2)所述N个KGC生成各自的主公钥P_i和主私钥s_i；所述s_i不公开，所述P_i公开；其中，所述i为大于或等于1的正整数；所述N个KGC包括：KGC_1、KGC_2、……、KGC_N；所述N为大于或等于2的正整数。

[0215] 这里，所述主公钥为上述实施例中的第三密钥参数的公钥参数；所述主私钥为上述实施例中的第三密钥参数的私钥参数。

[0216] 步骤S22.私钥生成：

[0217] (1)标识信息为ID的用户实体A随机生成秘密值x_A(基于公开参数n)，计算椭圆曲线上点$X_A=x_A*G$，将所述ID、X_A发送给KGC_1。

[0218] 这里，所述x_A为上述实施例中的第一密钥参数；所述X_A为上述实施例中的第一中间值。

[0219] (2)KGC_1收到(ID,X_A)后，检验其合法性；若确定所述(ID,X_A)合法，随机生成y_1；计算椭圆曲线上点$PA_1=X_A+y_1*G$；计算摘要$e_1=h(ID||PA_1)$，将e_1拆分并计算$z_1=e_1[0:15]*y_1+$

$e_1[16:31]*s_1$;将所述PA_1、所述ID及所述z_1发送给KGC_2。

[0220] 这里,所述“||”表示数据的串接;所述$e_1=h(ID||PA_1)$表示所述ID后面串接PA_1。

[0221] 这里,所述y_1为上述实施例的随机数。

[0222] 这里,所述$e_1[0:15]$表示所述e_1转换为32位的二进制后,提取该32位二进制的高16位二进制,基于所述高16位二进制获取的十进制数;所述$e_1[16:31]$表示所述e_1转换为32位的二进制后,提取该32位二进制的低16位二进制,基于所述低16位二进制获取的十进制数。

[0223] 这里,所述PA_1为上述实施例中的第二密钥参数的公钥参数;所述z_1为上述实施例中的第二密钥参数的私钥参数。可以理解的是,所述PA_1可以认为是部分公钥;所述z_1可以认为是部分私钥。

[0224] (3)所述KGC_2接收所述PA_1、所述ID及所述z_1;并随机生成y_2;计算$PA_2=PA_1+y_2*G$;计算摘要$e_2=h(ID||PA_2)$,将e_2拆分并计算$z_2=z_1+e_2[0:15]*y_2+e_2[16:31]*s_2$,并将$\{PA_1,PA_2\}$、所述ID及所述$z_2$发送给后面的$KGC_3$。

[0225] 这里,所述y_2为上述实施例的随机数。

[0226] 这里,所述$e_2[0:15]$表示所述e_2转换为32位的二进制后,提取该32位二进制的高16位二进制,基于所述高16位二进制获取的十进制数;所述$e_2[16:31]$表示所述e_2转换为32位的二进制后,提取该32位二进制的低16位二进制,基于所述低16位二进制获取的十进制数。

[0227] 这里,所述PA_2为上述实施例中的第二密钥参数的公钥参数;所述z_2为上述实施例中的第二密钥参数的私钥参数。可以理解的是,所述PA_2可以认为是部分公钥;所述z_2可以认为是部分私钥。

[0228] (4)依次类推,直到最后一个KGC_N收到KGC_{N-1}发来的$\{PA_1,PA_2,\cdots,PA_{N-1}\}$、所述ID及所述$z_{n-1}$;并随机生成$y_n$;计算$PA_N=PA_{N-1}+y_n*G$;计算摘要$e_n=h(ID||PA_N)$;将$e_n$拆分并计算$z_n=z_{n-1}+e_n[0:15]*y_n+e_n[16:31]*s_n$;并将$\{PA_1,PA_2,\cdots,PA_N\}$及所述$z_n$发送给用户实体A。

[0229] 这里,所述y_n为上述实施例的随机数。

[0230] 这里,所述$e_n[0:15]$表示所述e_n转换为32位的二进制后,提取该32位二进制的高16位二进制,基于所述高16位二进制获取的十进制数;所述$e_n[16:31]$表示所述e_n转换为32位的二进制后,提取该32位二进制的低16位二进制,基于所述低16位二进制获取的十进制数。

[0231] 这里,所述PA_N为上述实施例中的第二密钥参数的公钥参数;所述z_n为上述实施例中的第二密钥参数的私钥参数。可以理解的是,所述PA_N可以认为是部分公钥;所述z_n可以认为是部分私钥。

[0232] (5)用户接收到$\{PA_1,PA_2,\cdots,PA_N\}$及所述$z_n$后,计算$e_i=h(ID||PA_i)$,然后验证$(e_1[0:15]*x_A+z_n)*G=\sum_{i=1}^{N}e_i[0:15]*PA_i+e_i[16:32]*P_i$;如果该公式验证通过,获取用户的私钥$d_A=e_1[0:15]*x_A+z_n$。

[0233] S23.公钥生成:

[0234] 获取所述N个KGC的公钥参数$\{PA_1,PA_2,\cdots,PA_N\}$以及所述N个KGC的主公钥$\{P_1,P_2,\cdots,P_N\}$;计算摘要$e_i=h(ID||PA_i)$;计算公钥:$Q_A=\sum_{i=1}^{N}e_i[0:15]*PA_i+e_i[16:32]*P_i$。

[0235] 在实际应用中,可将上述方案可应用于密钥签名中。例如,用户实体A使用私钥$d_A=e_1[0:15]*x_A+z_n$对消息msg进行签名,可基于上述的椭圆曲线参数,获得签名值sig;所述

用户实体A将所述sig、所述ID、所述msg以及$\{PA_1,PA_2,\cdots,PA_N\}$发送给用户实体B;用户实体B接收到所述sig、所述ID、所述msg以及$\{PA_1,PA_2,\cdots,PA_N\}$,计算摘要$e_i=h(ID||PA_i)$;然后计算$Q_A=\sum_{i=1}^{N}e_i[0:15]*PA_i+e_i[16:32]*P_i$;并使用标准验签算法验证签名verify(sig,msg,Q_A);所述标准验签算法如图7所示。

[0236] 在另一些实施例中,上述方案也可应用于加密、解密算法中。例如,用户实体B获取用户实体A的部分公钥$\{PA_1,PA_2,\cdots,PA_N\}$;基于所述部分公钥计算实际公钥$Q_A$;用户实体B用户实体A的实际公钥加密消息sig;并加密的密文发送给用户实体A;用户实体A可基于所述自身的私钥$d_A=e_1[0:15]*x_A+z_n$对所述密文进行解密。

[0237] 这里需要指出的是:以下电子设备和存储介质的描述,与上述信息处理方法项描述是类似的,同方法的有益效果描述,不做赘述。对于本发明电子设备实施例中未披露的技术细节,请参照本发明信息处理方法实施例的描述而理解。

[0238] 如图8所述,本发明实施例公开了一种电子设备,所述电子设备包括:所述电子设备包括:处理器51、通信接口52和存储器53;其中,

[0239] 所述处理器51通常控制终端设备或网络设备的总体操作。

[0240] 通信接口52可以使终端设备或网络设备通过网络与其他终端或服务器通信。

[0241] 存储器53配置为存储由处理器51可执行的指令和应用,还可以缓存待处理器51以及终端中各模块待处理或已经处理的数据(例如,图像数据、音频数据、语音通信数据和视频通信数据),可以通过闪存(FLASH)或随机访问存储器(Random Access Memory,RAM)实现。

[0242] 可以理解的是,本文描述的处理器51可能是一种集成电路芯片,具有信号的处理能力。在实现过程中,上述方法的各步骤可以通过处理器51中的硬件的集成逻辑电路或者软件形式的指令完成。该存储介质位于存储器53,处理器51读取存储器53中的信息,结合其硬件完成上述方法的步骤。

[0243] 本发明又一实施例提供了一种计算机存储介质,该计算机可读存储介质存储有可执行程序,所述可执行程序被处理器执行时,可实现应用于所述电子设备的信息处理方法的步骤。例如,如图1、图3、图6所示的方法中的一个或多个。

[0244] 在本申请所提供的几个实施例中,应该理解到,所揭露的设备和方法,可以通过其它的方式实现。以上所描述的设备实施例仅仅是示意性的,例如,所述单元的划分,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,如:多个单元或组件可以结合,或可以集成到另一个系统,或一些特征可以忽略,或不执行。另外,所显示或讨论的各组成部分相互之间的耦合、或直接耦合、或通信连接可以是通过一些接口,设备或单元的间接耦合或通信连接,可以是电性的、机械的或其它形式的。

[0245] 上述作为分离部件说明的单元可以是、或也可以不是物理上分开的,作为单元显示的部件可以是、或也可以不是物理单元,即可以位于一个地方,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全部单元来实现本实施例方案的目的。

[0246] 另外,在本发明各实施例中的各功能单元可以全部集成在一个处理模块中,也可以是各单元分别单独作为一个单元,也可以两个或两个以上单元集成在一个单元中;上述集成的单元既可以采用硬件的形式实现,也可以采用硬件加软件功能单元的形式实现。本

领域普通技术人员可以理解:实现上述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计算机可读取存储介质中,该程序在执行时,执行包括上述方法实施例的步骤;而前述的存储介质包括:移动存储设备、只读存储器(ROM,Read-Only Memory)、随机存取存储器(RAM,Random Access Memory)、磁碟或者光盘等各种可以存储程序代码的介质。

[0247] 本申请所提供的几个方法实施例中所揭露的方法,在不冲突的情况下可以任意组合,得到新的方法实施例。

[0248] 本申请所提供的几个产品实施例中所揭露的特征,在不冲突的情况下可以任意组合,得到新的产品实施例。

[0249] 本申请所提供的几个方法或设备实施例中所揭露的特征,在不冲突的情况下可以任意组合,得到新的方法实施例或设备实施例。

[0250] 以上所述,仅为本发明的具体实施方式,但本发明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发明揭露的技术范围内,可轻易想到变化或替换,都应涵盖在本发明的保护范围之内。因此,本发明的保护范围应以所述权利要求的保护范围为准。

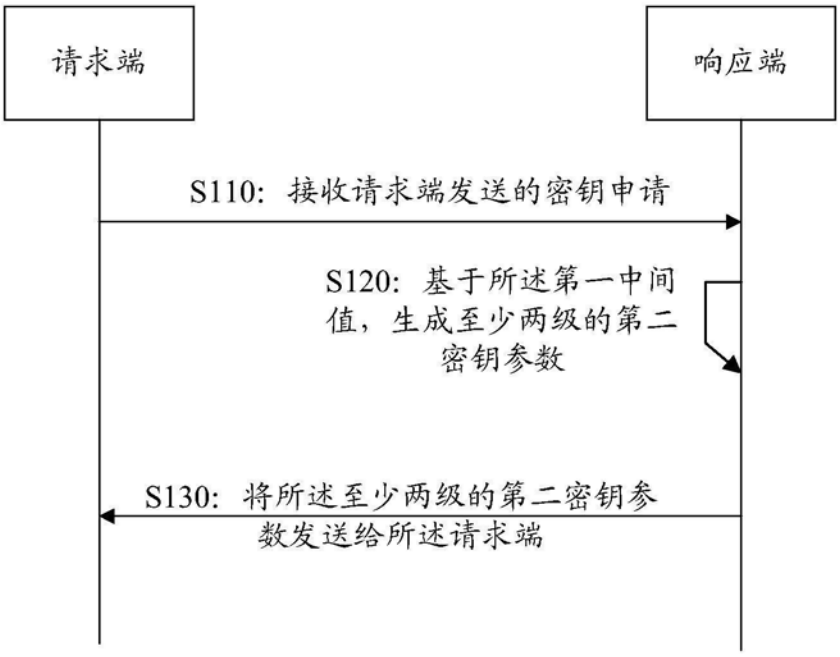

请求端
响应端
S110：接收请求端发送的密钥申请
S120：基于所述第一中间值，生成至少两级的第二密钥参数
S130：将所述至少两级的第二密钥参数发送给所述请求端

图1

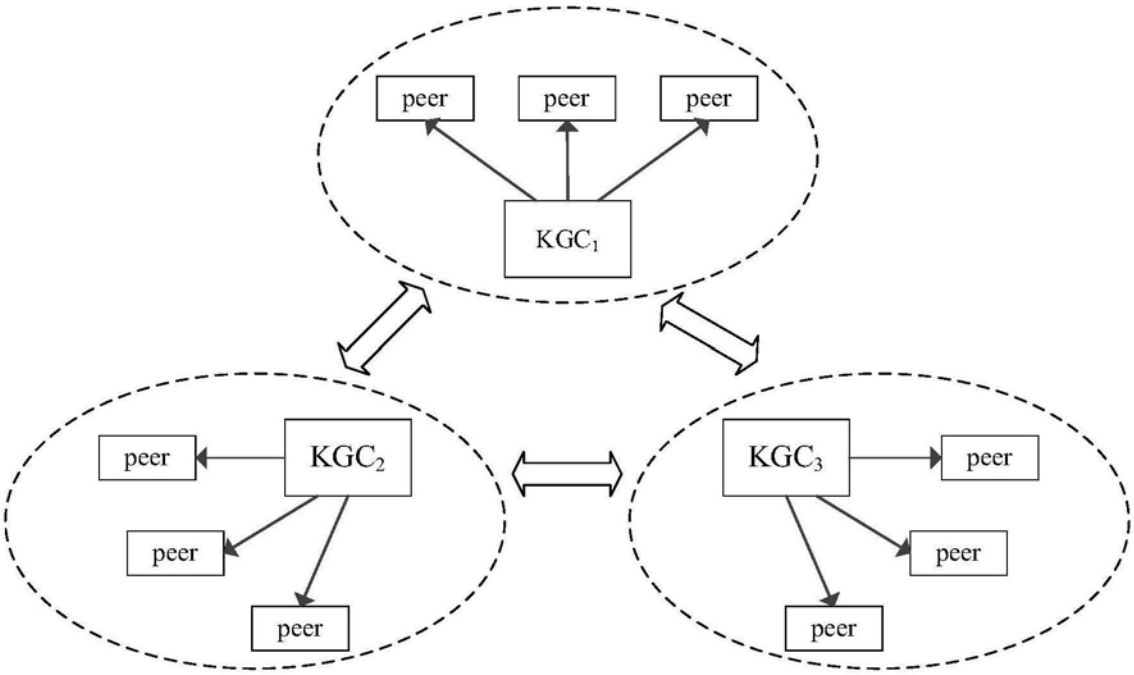

peer
peer
peer
KGC1
KGC2
peer
peer
peer
KGC3
peer
peer
peer

图2

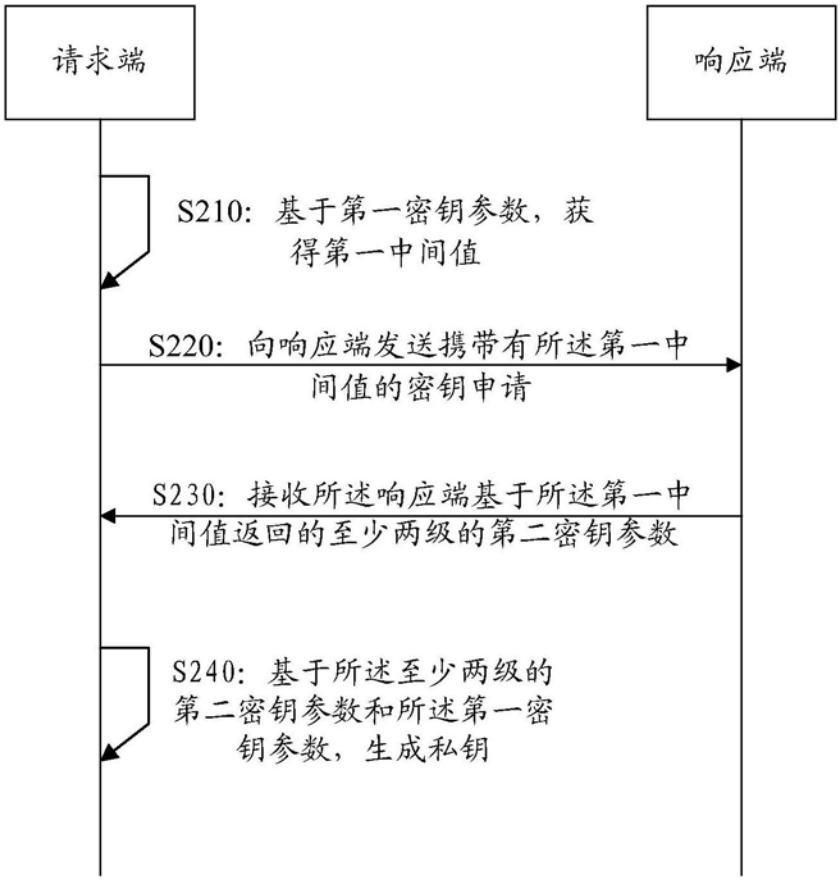

请求端
响应端
S210：基于第一密钥参数，获得第一中间值
S220：向响应端发送携带有所述第一中间值的密钥申请
S230：接收所述响应端基于所述第一中间值返回的至少两级的第二密钥参数
S240：基于所述至少两级的第二密钥参数和所述第一密钥参数，生成私钥

图3

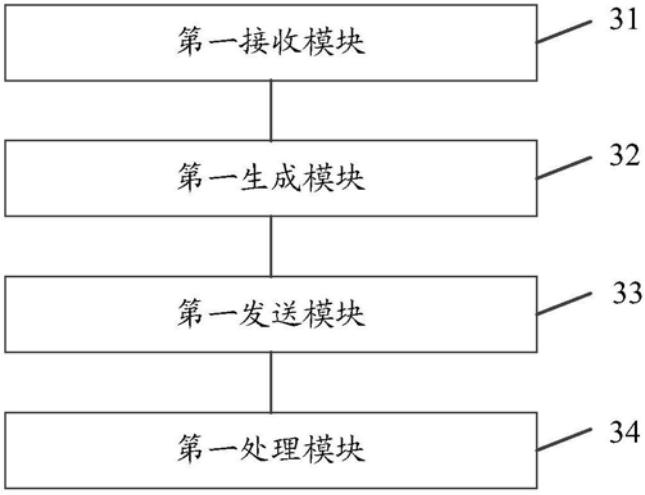

第一接收模块
31
第一生成模块
32
第一发送模块
33
第一处理模块
34

图4

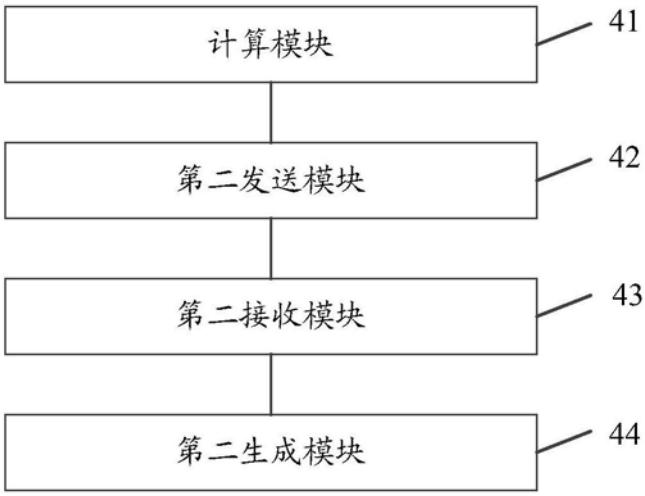

计算模块
41
第二发送模块
42
第二接收模块
43
第二生成模块
44

图5

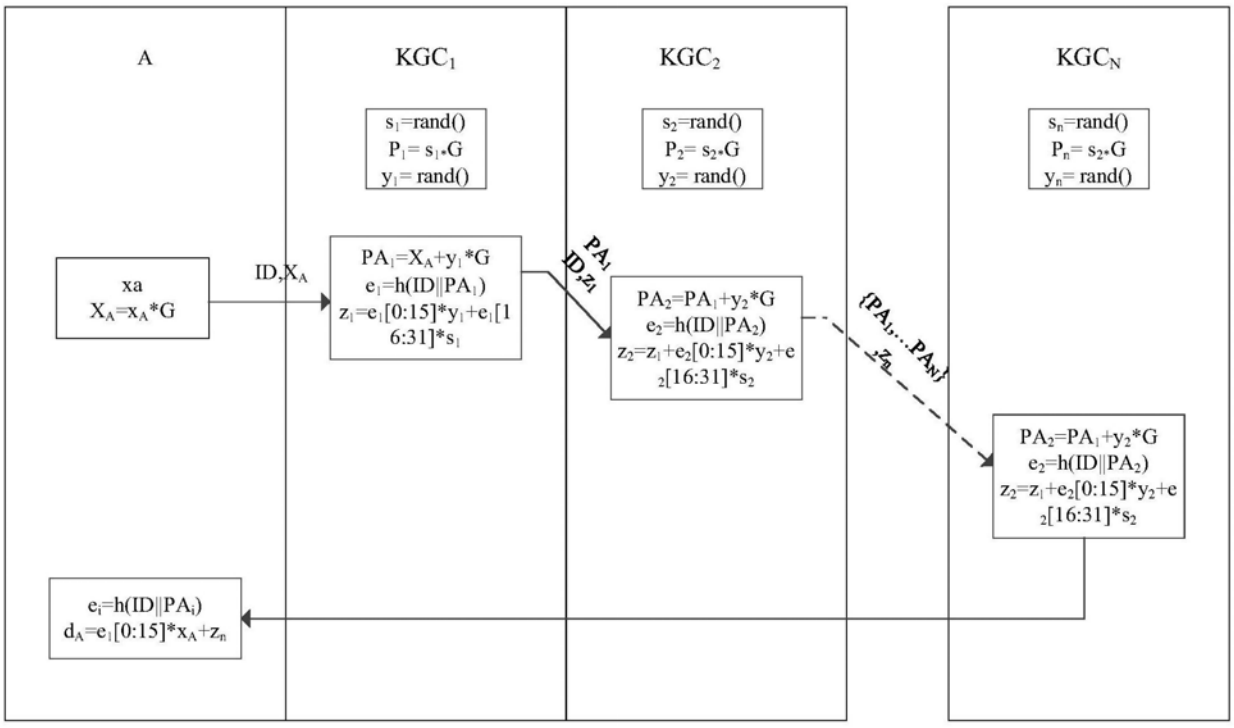

A
KGC1
KGC2
KGCN
s1=rand()
P1= s1*G
y1= rand()
s2=rand()
P2= s2*G
y2= rand()
sn=rand()
Pn= s2*G
yn= rand()
xa
XA=xA*G
ID,XA
PA1=XA+y1*G
e1=h(ID||PA1)
z1=e1[0:15]*y1+e1[16:31]*s1
PA1
ID,z1
PA2=PA1+y2*G
e2=h(ID||PA2)
z2=z1+e2[0:15]*y2+e2[16:31]*s2
{PA1,...PAn}
zn
PA2=PA1+y2*G
e2=h(ID||PA2)
z2=z1+e2[0:15]*y2+e2[16:31]*s2
ei=h(ID||PAi)
dA=e1[0:15]*xA+zn

图6

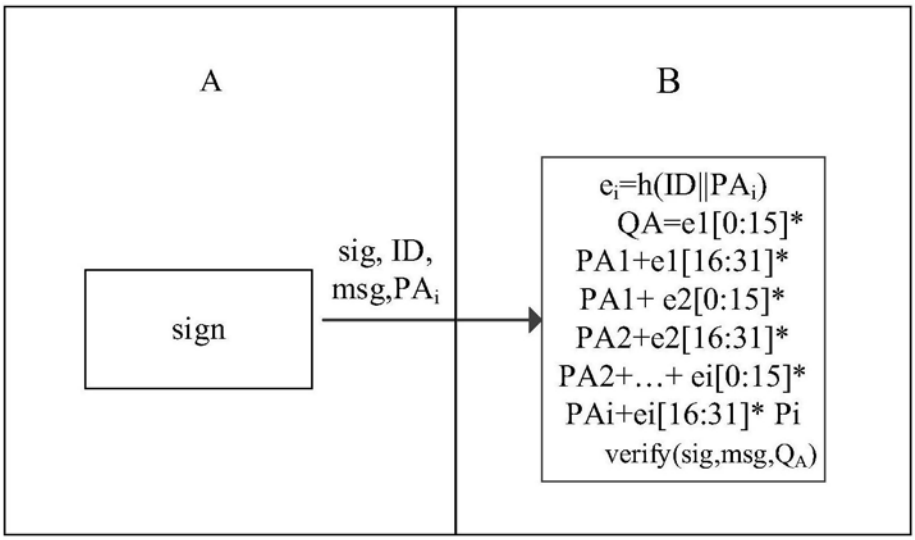

A
B
sign
sig, ID,
msg,PA$_i$
e_i=h(ID||PA$_i$)
QA=e1[0:15]*
PA1+e1[16:31]*
PA1+ e2[0:15]*
PA2+e2[16:31]*
PA2+…+ ei[0:15]*
PAi+ei[16:31]* Pi
verify(sig,msg,Q$_A$)

图7

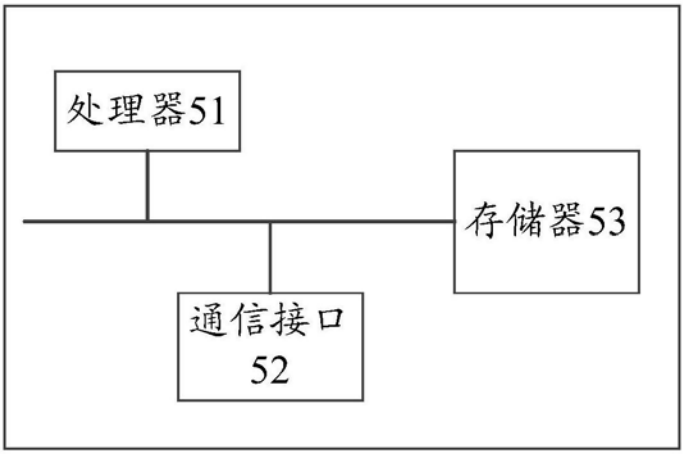

处理器51
存储器53
通信接口
52

图8