(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 113922962 A
(43)申请公布日 2022.01.11

(21)申请号 202111061784.5

(22)申请日 2021.09.10

(71)申请人 杭州溪塔科技有限公司
地址 310012 浙江省杭州市西湖区文三路478号华星时代广场A座20层2001、2010室

(72)发明人 王晓亮 张亚宁

(74)专利代理机构 北京德崇智捷知识产权代理有限公司 11467
代理人 邢飞飞 王欣

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

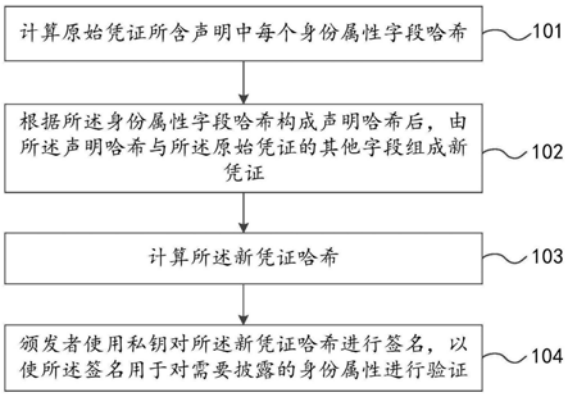
权利要求书2页 说明书9页 附图4页

(54)发明名称

一种数字身份属性的选择性披露方法和装置

(57)摘要

本说明书实施例公开了一种数字身份属性的选择性披露方法和装置,其中方法,应用于第一组件,包括:计算原始凭证所含声明中的每个身份属性字段哈希;根据所述身份属性字段哈希构成声明哈希后,由所述声明哈希与所述原始凭证的其他字段组成新凭证;计算所述新凭证哈希;所述颁发者使用私钥对所述新凭证哈希进行签名,以使所述签名用于对需要披露的身份属性进行验证。本发明的方案应用于数字身份验证场景下,验证者只能获得持有者披露的身份属性信息,持有者无需担心其他身份属性信息被泄露。



CN 113922962 A

1.一种数字身份属性的选择性披露方法,其特征在于,应用于第一组件,包括:

计算原始凭证所含声明中的每个身份属性字段哈希;

根据所述身份属性字段哈希构成声明哈希后,由所述声明哈希与所述原始凭证的其他字段组成新凭证;

计算所述新凭证哈希;

颁发者使用私钥对所述新凭证哈希进行签名,以使所述签名用于对需要披露的身份属性进行验证。

2.根据权利要求1所述的方法,其特征在于,根据所述身份属性字段哈希构成声明哈希为以指定形式拼接构成。

3.根据权利要求1所述的方法,其特征在于,所述第一组件在进行哈希计算时使用唯一选定的哈希算法。

4.一种数字身份属性的选择性披露装置,其特征在于,包括:

哈希计算模块,用于计算指定数据哈希值;

凭证管理模块,用于根据所述身份属性字段哈希构成声明哈希后,由所述声明哈希与所述凭证的其他字段组成新凭证;

签名生成模块,用于使用私钥对所述新凭证哈希进行签名,以使所述签名用于对需要披露的身份属性进行验证。

5.一种数字身份属性的选择性披露方法,其特征在于,凭证持有者向验证者提交需披露的身份属性字段以及无需披露的身份属性字段哈希以及原始凭证后,应用于第二组件,包括:

所述验证者获得需披露的所述身份属性字段;

计算需披露的所述身份属性字段哈希;

根据需披露的所述身份属性字段哈希和无需披露的所述身份属性字段哈希构成声明哈希后,由所述声明哈希与所述原始凭证的其他字段组成新凭证;

计算所述新凭证哈希;

使用凭证发行方公钥对所述原始凭证的签名进行验证;

若所述新凭证哈希与所述原始凭证哈希相等,以确认需披露的所述身份属性的真实性。

6.根据权利要求5所述的方法,其特征在于,根据需披露的所述身份属性字段哈希和无需披露的所述身份属性字段哈希构成声明哈希为以指定形式拼接构成。

7.根据权利要求5所述的方法,其特征在于,所述第二组件在进行哈希计算时使用唯一选定的哈希算法。

8.一种数字身份属性的选择性披露装置,其特征在于,包括:

哈希计算模块,用于计算指定数据哈希值;

凭证管理模块,用于根据需披露的所述身份属性字段哈希和无需披露的所述身份属性字段哈希构成声明哈希后,由所述声明哈希与所述原始凭证的其他字段组成新凭证;

签名解密模块,用于使用凭证发行方公钥对所述原始凭证哈希签名进行解密,得到原始凭证哈希;

哈希比较模块,用于比较所述新凭证哈希与所述原始凭证哈希是否相等,以确认身份

属性真实性。

9.一种数字身份属性的选择性披露系统，其特征在于，包括第一组件和第二组件，其中，

所述第一组件计算原始凭证所含声明中的每个身份属性字段哈希，根据所述身份属性字段哈希构成声明哈希后，由所述声明哈希与所述凭证的其他字段组成新凭证并计算第二凭证哈希，使用私钥对所述新凭证哈希进行签名，以使所述签名用于对需要披露的身份属性进行验证；

所述第二组件所述验证者获得需披露的所述身份属性字段，计算需披露的所述身份属性字段哈希，根据需披露的所述身份属性字段哈希和无需披露的所述身份属性字段哈希构成声明哈希后，由所述声明哈希与原始凭证的其他字段构成新凭证并计算所述新凭证哈希，使用凭证发行方公钥对所述原始凭证哈希签名进行解密，得到原始凭证哈希，若所述新凭证哈希与所述原始凭证哈希相等，则确认身份属性真实性；

所述第一组件生成所述持有者签名后，由所述第二组件根据所述持有者签名验证持有者提交的需披露的所述身份属性。

10.一种电子设备，其特征在于，包括：

处理器；以及

被安排成存储计算机可执行指令的存储器，所述可执行指令在被执行时使所述处理器执行权利要求1至3任一项所述的方法。

11.一种电子设备，其特征在于，包括：

处理器；以及

被安排成存储计算机可执行指令的存储器，所述可执行指令在被执行时使所述处理器执行权利要求5至7任一项所述的方法。

12.一种计算机可读存储介质，其特征在于，所述计算机可读存储介质存储一个或多个程序，所述一个或多个程序当被包括多个应用程序的电子设备执行时，使得所述电子设备执行权利要求1至3任一项所述的方法。

13.一种计算机可读存储介质，其特征在于，所述计算机可读存储介质存储一个或多个程序，所述一个或多个程序当被包括多个应用程序的电子设备执行时，使得所述电子设备执行权利要求5至7任一项所述的方法。

一种数字身份属性的选择性披露方法和装置

技术领域

[0001] 本说明书涉及计算机软件技术领域，尤其涉及一种数字身份属性的选择性披露方法、装置和电子设备。

背景技术

[0002] 随着互联网技术的发展，身份认证技术得到了广泛的应用，但同时也给持有者带来了隐私问题，特别是当持有者只需要披露自己的某些身份属性时，当前普遍做法是持有者出示自己的数字证书，数字证书中包含持有者全部身份属性以及一个颁发者的签名，这样会披露其他的身份属性，为持有者带来隐私风险。因此设计出一种能够由持有者选择披露指定身份属性的方案是有意义的。

发明内容

[0003] 本说明书实施例的目的是针对上述问题，提供一种数字身份属性的选择性披露方法和装置。

[0004] 为解决上述技术问题，本说明书实施例是这样实现的：

[0005] 第一方面，提出了一种数字身份属性的选择性披露方法，应用于第一组件，包括：

[0006] 计算原始凭证所含声明中的每个身份属性字段哈希；

[0007] 根据所述身份属性字段哈希构成声明哈希后，由所述声明哈希与所述原始凭证的其他字段组成新凭证；

[0008] 计算所述新凭证哈希；

[0009] 所述颁发者使用私钥对所述新凭证哈希进行签名，以使所述签名用于对需要披露的身份属性进行验证。

[0010] 第二方面，提出了一种数字身份属性的选择性披露装置，包括：

[0011] 哈希计算模块，用于计算指定数据哈希值；

[0012] 凭证管理模块，用于根据所述身份属性字段哈希构成声明哈希后，由所述声明哈希与所述原始凭证的其他字段组成新凭证；

[0013] 签名生成模块，用于使用私钥对所述新凭证哈希进行签名，以使所述签名用于对需要披露的身份属性进行验证。

[0014] 第三方面，提出了一种数字身份属性的选择性披露方法，凭证持有者向验证者提交需披露的身份属性字段以及无需披露的身份属性字段哈希以及原始凭证后，应用于第二组件，包括：

[0015] 所述验证者获得需披露的所述身份属性字段；

[0016] 计算需披露的所述身份属性字段哈希；

[0017] 根据需披露的所述身份属性字段哈希和无需披露的所述身份属性字段哈希构成声明哈希后，由所述声明哈希与所述原始凭证的其他字段组成新凭证；

[0018] 计算所述新凭证哈希；

[0019] 使用凭证发行方公钥对所述原始凭证的签名进行验证；

[0020] 若所述新凭证哈希与所述原始凭证哈希相等，以确认需披露的所述身份属性的真实性。

[0021] 第四方面，提出了一种数字身份属性的选择性披露装置，包括：

[0022] 哈希计算模块，用于计算指定数据哈希值；

[0023] 凭证管理模块，用于根据需披露的所述身份属性字段哈希和无需披露的所述身份属性字段哈希构成声明哈希后，由所述声明哈希与所述原始凭证的其他字段组成新凭证；

[0024] 签名解密模块，用于使用凭证发行方公钥对所述原始凭证哈希签名进行解密，得到原始凭证哈希；

[0025] 哈希比较模块，用于比较所述新凭证哈希与所述原始凭证哈希是否相等，以确认身份属性真实性。

[0026] 第五方面，提出了一种数字身份属性的选择性披露系统，包括第一组件和第二组件，其中，

[0027] 所述第一组件计算原始凭证所含声明中的每个身份属性字段哈希，根据所述身份属性字段哈希构成声明哈希后，由所述声明哈希与所述凭证的其他字段组成新凭证并计算第二凭证哈希，使用私钥对所述新凭证哈希进行签名，以使所述签名用于对需要披露的身份属性进行验证；

[0028] 所述第二组件所述验证者获得需披露的所述身份属性字段，计算需披露的所述身份属性字段哈希，根据需披露的所述身份属性字段哈希和无需披露的所述身份属性字段哈希构成声明哈希后，由所述声明哈希与原始凭证的其他字段构成新凭证并计算所述新凭证哈希，使用凭证发行方公钥对所述原始凭证哈希签名进行解密，得到原始凭证哈希，若所述新凭证哈希与所述原始凭证哈希相等，则确认身份属性真实性；

[0029] 所述第一组件生成所述持有者签名后，由所述第二组件根据所述持有者签名验证持有者提交的需披露的所述身份属性。

[0030] 第六方面，提出了一种电子设备，包括：处理器；以及

[0031] 被安排成存储计算机可执行指令的存储器，所述可执行指令在被执行时使所述处理器执行第一方面所述的方法。

[0032] 第七方面，提出了一种计算机可读存储介质，所述计算机可读存储介质存储一个或多个程序，所述一个或多个程序当被包括多个应用程序的电子设备执行时，使得所述电子设备执行第一方面所述的方法。

[0033] 第八方面，提出了一种电子设备，包括：处理器；以及

[0034] 被安排成存储计算机可执行指令的存储器，所述可执行指令在被执行时使所述处理器执行第三方面所述的方法。

[0035] 第九方面，提出了一种计算机可读存储介质，所述计算机可读存储介质存储一个或多个程序，所述一个或多个程序当被包括多个应用程序的电子设备执行时，使得所述电子设备执行第三方面所述的方法。

[0036] 本说明书可以达到至少以下技术效果：

[0037] 本发明的方案应用于数字身份验证场景下，验证者只能获得持有者披露的身份属性信息，持有者无需担心其他身份属性信息被泄露。

附图说明

[0038] 为了更清楚地说明本说明书实施例或现有技术中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本说明书中记载的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动性的前提下，还可以根据这些附图获得其他的附图。

[0039] 图1为本说明书实施例提供的数字身份属性的选择性披露方法步骤示意图之一。

[0040] 图2为本说明书实施例提供的数字身份属性的选择性披露方法步骤示意图之二。

[0041] 图3为本说明书的一个实施例提供的数字身份属性的选择性披露装置结构示意图之一。

[0042] 图4为本说明书的一个实施例提供的数字身份属性的选择性披露装置结构示意图之二。

[0043] 图5为本说明书的一个实施例提供的电子设备的结构示意图。

具体实施方式

[0044] 为了使本技术领域的人员更好地理解本说明书中的技术方案，下面将结合本说明书实施例中的附图，对本说明书实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅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作出创造性劳动前提下所获得的所有其他实施例，都应当属于本说明书保护的范围。

[0045] 关键术语

[0046] 分布式数字身份DID：是由字符串组成的标识符，用来代表一个数字身份，它是一种去中心化可验证的标识符，实体可自主完成DID的注册、解析、更新或者撤销操作，不需要中央注册机构就可以实现全球唯一性。通常，一个实体可以拥有多个身份，由实体自己进行管理、维护，不同的身份之间没有关联信息，可有效避免身份信息被第三方归集。DID的核心模型是分布式数字身份标识符和可验证凭证流转，核心技术是分布式账本和密码学技术，这二者的结合用以创建不可抵赖、且不可篡改的身份记录。

[0047] DID有关角色：(1)颁发者Issuer，就是证书的颁发机构，比如身份证就是公安机关作为颁发者，毕业证书就是大学作为颁发者；(2)持有者Holder，就是证书的持有人，就是我们这些普通人；(3)验证者Verifier，就是在我们使用证书时查看我们证书的人或者机构。比如：我们入住酒店，前台要验证我们的身份证，那么酒店前台就是验证者。再比如：我们入职新公司时需要提供大学毕业证书，新公司HR就是验证者。DID注册系统Verifiable Data Registry就是我们存储了DID标识和DID文档的地方，通过DID标识可以查询到对应的DID文档。

[0048] 可验证凭证(Verifiable Credentials，简称VC)：是一个DID传递给另一个DID的某些属性做背书而发出的描述性声明，并附加了自己的数字签名，用以证明这些属性的真实性，可以认为是一种数字证书。一个VC也是一个JSON字符串，包括如下信息：(1)VC元数据，主要就是发行人、发行日期、声明的类型等信息；(2)声明Claim，一个或者多个关于主体的说明。比如身份证作为公安机关颁发给我的VC，在声明中会包含：姓名、性别、出生日期、民族、住址等信息；(3)证明Proofs，通常就是颁发者的数字签名，保证了本VC能够被验证，

防止VC内容被篡改以及验证VC的颁发者。

[0049] 可验证表达(Verifiable Presentation,简称VP):Verifiable presentation简称VP,可验证表达是VC持有者向验证者表名自己身份的数据。一般情况下,我们直接出示VC全文即可,但是在某些情况下,出于隐私保护的需要,我们并不需要出示完整的VC内容,只希望选择性披露某些属性,或者不披露任何属性,只需要证明某个断言即可。一个VP也是一个JSON字符串,包括如下信息:(1)VP元数据,主要包含了版本、JSON对象的类型等信息;(2)VC列表,要对外展示的VC的内容,但如果是选择性披露或者隐私保护的情形,可能就不包含任何VC;(3)证明Proofs,主要就是持有者对本VP的签名信息。

[0050] 下面通过具体的实例对本说明书所涉及的一种数字身份属性的选择性披露方案进行详述。

[0051] 实施例一

[0052] 本实施例以实际生活中身份证件属性披露为例子进行说明。在实际生活中,如果没有数字身份技术,那么当身份证件持有者在需要出示并核验身份证件的时候,势必会将身份证件上的所有属性信息都提供验证者,这是一种无选择性披露身份属性的方式。但是,有了数字身份DID技术后,可以将先身份证件信息生成数字身份,在数字身份情况下才可能实现身份属性的选择性披露。

[0053] 以住酒店为例,需要登记证件持有者的姓名和身份证号用于身份验证。但是持有者民族和住址等信息与酒店登记并无直接关系,如果全部出示提交验证,那么可能酒店前台人员就可能出于各方面的原因,偷偷把住址信息记下了或者泄露到网上,给证照本人的生活带来各种麻烦,这就需要对持有者的身份属性进行选择性披露,以便降低个人信息泄露的风险。

[0054] 根据以上情景描述,可以看出,是由双向共同作用来实现上述实施例。一方面是如何将证件持有者的身份属性生成DID数字身份属性,并为相应的可验证凭证VC签名。另一方面是当数字身份持有者有选择地将部分身份属性提交验证时,验证者能够仅根据提交的部分身份属性来验证其真实性,即验证可验证表达VP真实性。因此,本实施例将第一方面抽象为生成数字身份属性的可验证凭证VC一侧,也就是说是生成持有者的全部数字身份属性,本说明书中定义为第一组件;将第二方面抽象为生成数字身份属性的可验证表达VP一侧,也就是说是持有者仅提供必要的身份属性来进行验证,本说明书中定义为第二组件。

[0055] 综上,本实施例提出一种数字身份属性的选择性披露系统,包括第一组件和第二组件,其中,

[0056] 所述第一组件计算原始凭证所含声明中的每个身份属性字段哈希,根据所述身份属性字段哈希构成声明哈希后,由所述声明哈希与所述凭证的其他字段组成新凭证并计算第二凭证哈希,使用私钥对所述新凭证哈希进行签名,以使所述签名用于对需要披露的身份属性进行验证;

[0057] 所述第二组件所述验证者获得需披露的所述身份属性字段,计算需披露的所述身份属性字段哈希,根据需披露的所述身份属性字段哈希和无需披露的所述身份属性字段哈希构成声明哈希后,由所述声明哈希与原始凭证的其他字段构成新凭证并计算所述新凭证哈希,使用凭证发行方公钥对所述原始凭证哈希签名进行解密,得到原始凭证哈希,若所述新凭证哈希与所述原始凭证哈希相等,则确认身份属性真实性;

[0058] 所述第一组件生成所述持有者签名后，由所述第二组件根据所述持有者签名验证持有者提交的需披露的所述身份属性。

[0059] 实施例二

[0060] 参照图1所示，为本说明书实施例提供的数字身份属性的选择性披露方法步骤示意图，该方法的执行主体是生成数字身份属性的可验证凭证VC一侧，也就是说是生成持有者的全部数字身份属性，本说明书中定义为第一组件；所述第一组件具体可以是应用服务程序(含软件客户端)也可以是终端等电子设备。本说明书示例如下。

[0061]
```
{
 // VC 声明的具体内容
  “credentialSubject”: {
 //持有者的 DID
  “id”:“did:cid:110101190001010001”,
 // 声明内容:姓名、性别、生日、民族、住址等
  “name”:”小明”,
  “gender”:”男”,
  “birthdate”:”1900-01-01”,
  “nation”:”汉”,
  “address”:”A 省 B 市 C 区 D 街道 xxx 号”,
}
```

[0062] 所述方法可以包括以下步骤：

[0063] 步骤101：计算原始凭证所含声明中的每个身份属性字段哈希。

[0064] 具体地，上述身份证号id、姓名name、性别gender、出生日期birthday、民族nation、家庭住址address都是原始VC的声明Claim部分的身份属性。对上述身份属性进行哈希计算，对于能够实现本发明方案的哈希算法均可用来实现本发明的实施例。但是，由于本实施例中还涉及其他步骤的哈希计算，因此在进行哈希计算时应全程使用唯一选定的哈希算法，以确保计算一致性。

[0065] 步骤102：根据所述身份属性字段哈希构成声明哈希后，由所述声明哈希与所述原始凭证的其他字段组成新凭证。

[0066] 可选地，根据所述身份属性字段哈希构成声明哈希为以指定形式拼接构成。具体地，可以按照上述身份属性的声明顺序，将计算好的身份属性哈希字符串顺次拼接构成新的凭证，而新凭证属于计算新凭证签名的中间“产物”。

[0067] 步骤103：计算所述新凭证哈希。具体地，本实施例中在进行哈希计算时应使用唯一选定的哈希算法，以确保计算一致性，此处不再赘述。

[0068] 步骤104：颁发者使用私钥对所述新凭证哈希进行签名，以使所述签名用于对需要披露的身份属性进行验证。

[0069] “proof”:{

[0070] “creator”:“did:公安部门ID#keys-1”,

[0072] “type”:“Secp256k1”,

[0073] “signatureValue”:

[0074] “3044022051757c2de7032a0c887c3fcef02ca3812fede7ca748254771b9513d8e2bb”

[0075] }

[0076] 上述示例中的签名signatureValue,即为依据新凭证形成的VC签名。这里需要说明的是,签名形成的过程使用的是实现约定好的私钥。

[0077] 参照图2所示,为本说明书实施例提供的数字身份属性的选择性披露方法步骤示意图,该方法的执行主体是生成数字身份属性的可验证表达一侧,也就是说是持有者仅提供必要的身份属性来进行验证,本说明书中定义为第二组件;所述第二组件具体可以是应用服务程序(含软件客户端)也可以是终端等电子设备。所述方法可以包括以下步骤:

[0078] 凭证持有者向验证者提交需披露的身份属性字段以及无需披露的身份属性字段哈希以及原始凭证。这里需要说明的是,需披露的身份属性字段是以原值的形式提交的,而不需要披露的身份属性字段是以哈希值的形式提交的;同时,持有者向验证者提交的原始凭证,也就是第一组件最终为持有者生成的带有签名的凭证。在完成上述提交后,包括:

[0079] 步骤201:所述验证者获得需披露的所述身份属性字段。

[0080] 步骤202:计算需披露的所述身份属性字段哈希。

[0081] 步骤203:根据需披露的所述身份属性字段哈希和无需披露的所述身份属性字段哈希构成声明哈希后,由所述声明哈希与所述原始凭证的其他字段组成新凭证。

[0082] 可选地,根据需披露的所述身份属性字段哈希和无需披露的所述身份属性字段哈希构成声明哈希为以指定形式拼接构成。具体地,可以按照上述身份属性的声明顺序,将计算好的身份属性哈希字符串顺次拼接构成新的凭证,而新凭证属于计算新凭证签名的中间“产物”。

[0083] 步骤204:计算所述新凭证哈希。

[0084] 步骤205:使用凭证发行方公钥对所述原始凭证的签名进行验证。这里需要说明的是,签名验证的过程使用的是实现约定好的与形成签名相对应的私钥。

[0085] 步骤206:若所述新凭证哈希与所述原始凭证哈希相等,以确认需披露的所述身份属性的真实性。

[0086] 可选地,所述第二组件在进行哈希计算时全程使用唯一选定的哈希算法。

[0087] 实施例三

[0088] 图3为本说明书的一个实施例提供的一种数字身份属性的选择性披露装置300的结构示意图。请参考图3,在一种实施方式中数字身份属性的选择性披露装置包括:

[0089] 哈希计算模块301,用于计算指定数据哈希值;

[0090] 凭证管理模块302,用于根据所述身份属性字段哈希构成声明哈希后,由所述声明哈希与所述原始凭证的其他字段组成新凭证;

[0091] 签名生成模块303,用于使用私钥对所述新凭证哈希进行签名,以使所述签名用于对需要披露的身份属性进行验证。

[0092] 图4为本说明书的一个实施例提供的数字身份属性的选择性披露装置400的结构示意图。请参考图4,在一种实施方式中数字身份属性的选择性披露装置包括:

[0093] 哈希计算模块401,用于计算指定数据哈希值;

[0094] 凭证管理模块402,用于根据需披露的所述身份属性字段哈希和无需披露的所述身份属性字段哈希构成声明哈希后,由所述声明哈希与所述原始凭证的其他字段组成新凭证;

[0095] 签名解密模块403,用于使用凭证发行方公钥对所述原始凭证哈希签名进行解密,得到原始凭证哈希;

[0096] 哈希比较模块404,用于比较所述新凭证哈希与所述原始凭证哈希是否相等,以确认身份属性真实性。

[0097] 应理解,本说明书实施例的数字身份属性的选择性披露装置还可执行图1至图2中数字身份属性的选择性披露装置(或设备)执行的方法,并实现数字身份属性的选择性披露装置(或设备)在图1至图2所示实施例的功能,在此不再赘述。

[0098] 实施例四

[0099] 图5是本说明书的一个实施例电子设备的结构示意图。请参考图5,在硬件层面,该电子设备包括处理器,可选地还包括内部总线、网络接口、存储器。其中,存储器可能包含内存,例如高速随机存取存储器(Random-Access Memory,RAM),也可能还包括非易失性存储器(non-volatile memory),例如至少1个磁盘存储器等。当然,该电子设备还可能包括其他业务所需要的硬件。

[0100] 处理器、网络接口和存储器可以通过内部总线相互连接,该内部总线可以是ISA(Industry Standard Architecture,工业标准体系结构)总线、PCI(Peripheral Component Interconnect,外设部件互连标准)总线或EISA(Extended Industry Standard Architecture,扩展工业标准结构)总线等。所述总线可以分为地址总线、数据总线、控制总线等。为便于表示,图5中仅用一个双向箭头表示,但并不表示仅有一根总线或一种类型的总线。

[0101] 存储器,用于存放程序。具体地,程序可以包括程序代码,所述程序代码包括计算机操作指令。存储器可以包括内存和非易失性存储器,并向处理器提供指令和数据。

[0102] 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,在逻辑层面上形成共享资源访问控制装置。处理器,执行存储器所存放的程序,并具体用于执行以下操作:

[0103] 应用于第一组件,包括:

[0104] 计算原始凭证所含声明中的每个身份属性字段哈希;

[0105] 根据所述身份属性字段哈希构成声明哈希后,由所述声明哈希与所述凭证的其他字段组成新凭证;

[0106] 计算所述新凭证哈希;

[0107] 所述颁发者使用私钥对所述新凭证哈希进行签名,以使所述签名用于对需要披露的身份属性进行验证。

[0108] 或者,

[0109] 凭证持有者向验证者提交需披露的身份属性字段以及无需披露的身份属性字段哈希以及原始凭证后,应用于第二组件,包括:

[0110] 所述验证者获得需披露的所述身份属性字段;

[0111] 计算需披露的所述身份属性字段哈希；

[0112] 根据需披露的所述身份属性字段哈希和无需披露的所述身份属性字段哈希构成声明哈希后，由所述声明哈希与所述原始凭证的其他字段组成新凭证；

[0113] 计算所述新凭证哈希；

[0114] 使用凭证发行方公钥对所述原始凭证的签名进行验证；

[0115] 若所述新凭证哈希与所述原始凭证哈希相等，以确认需披露的所述身份属性的真实性。

[0116] 上述如本说明书图1至图2所示实施例揭示的一种数字身份属性的选择性披露方法可以应用于处理器中，或者由处理器实现。处理器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中的硬件的集成逻辑电路或者软件形式的指令完成。上述的处理器可以是通用处理器，包括中央处理器(Central Processing Unit,CPU)、网络处理器(Network Processor,NP)等；还可以是数字信号处理器(Digital Signal Processor,DSP)、专用集成电路(Application Specific Integrated Circuit,ASIC)、现场可编程门阵列(Field－Programmable Gate Array,FPGA)或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件。可以实现或者执行本说明书实施例中公开的各方法、步骤及逻辑框图。通用处理器可以是微处理器或者该处理器也可以是任何常规的处理器等。结合本说明书实施例所公开的方法的步骤可以直接体现为硬件译码处理器执行完成，或者用译码处理器中的硬件及软件模块组合执行完成。软件模块可以位于随机存储器，闪存、只读存储器，可编程只读存储器或者电可擦写可编程存储器、寄存器等本领域成熟的存储介质中。该存储介质位于存储器，处理器读取存储器中的信息，结合其硬件完成上述方法的步骤。

[0117] 当然，除了软件实现方式之外，本说明书实施例的电子设备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定于各个逻辑单元，也可以是硬件或逻辑器件。

[0118] 实施例五

[0119] 本说明书实施例还提出了一种计算机可读存储介质，该计算机可读存储介质存储一个或多个程序，该一个或多个程序包括指令，该指令当被包括多个应用程序的便携式电子设备执行时，能够使该便携式电子设备执行图1至图4所示实施例的方法，并具体用于执行以下方法：

[0120] 应用于第一组件，包括：

[0121] 计算原始凭证所含声明中的每个身份属性字段哈希；

[0122] 根据所述身份属性字段哈希构成声明哈希后，由所述声明哈希与所述凭证的其他字段组成新凭证；

[0123] 计算所述新凭证哈希；

[0124] 所述颁发者使用私钥对所述新凭证哈希进行签名，以使所述签名用于对需要披露的身份属性进行验证。

[0125] 或者，

[0126] 凭证持有者向验证者提交需披露的身份属性字段以及无需披露的身份属性字段哈希以及原始凭证后，应用于第二组件，包括：

[0127] 所述验证者获得需披露的所述身份属性字段；

[0128] 计算需披露的所述身份属性字段哈希；

[0129] 根据需披露的所述身份属性字段哈希和无需披露的所述身份属性字段哈希构成声明哈希后，由所述声明哈希与所述原始凭证的其他字段组成新凭证；

[0130] 计算所述新凭证哈希；

[0131] 使用凭证发行方公钥对所述原始凭证的签名进行验证；

[0132] 若所述新凭证哈希与所述原始凭证哈希相等，以确认需披露的所述身份属性的真实性。

[0133] 总之，以上所述仅为本说明书的较佳实施例而已，并非用于限定本说明书的保护范围。凡在本说明书的精神和原则之内，所作的任何修改、等同替换、改进等，均应包含在本说明书的保护范围之内。

[0134] 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。

[0135] 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。

[0136] 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。

[0137] 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。

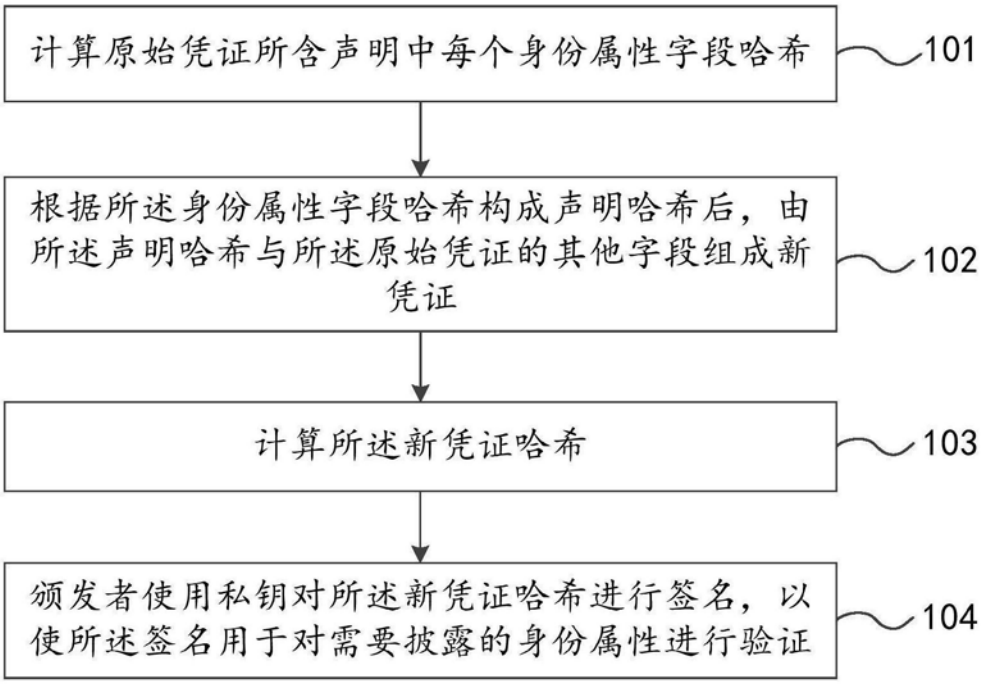

计算原始凭证所含声明中每个身份属性字段哈希
101
根据所述身份属性字段哈希构成声明哈希后，由所述声明哈希与所述原始凭证的其他字段组成新凭证
102
计算所述新凭证哈希
103
颁发者使用私钥对所述新凭证哈希进行签名，以使所述签名用于对需要披露的身份属性进行验证
104

图1

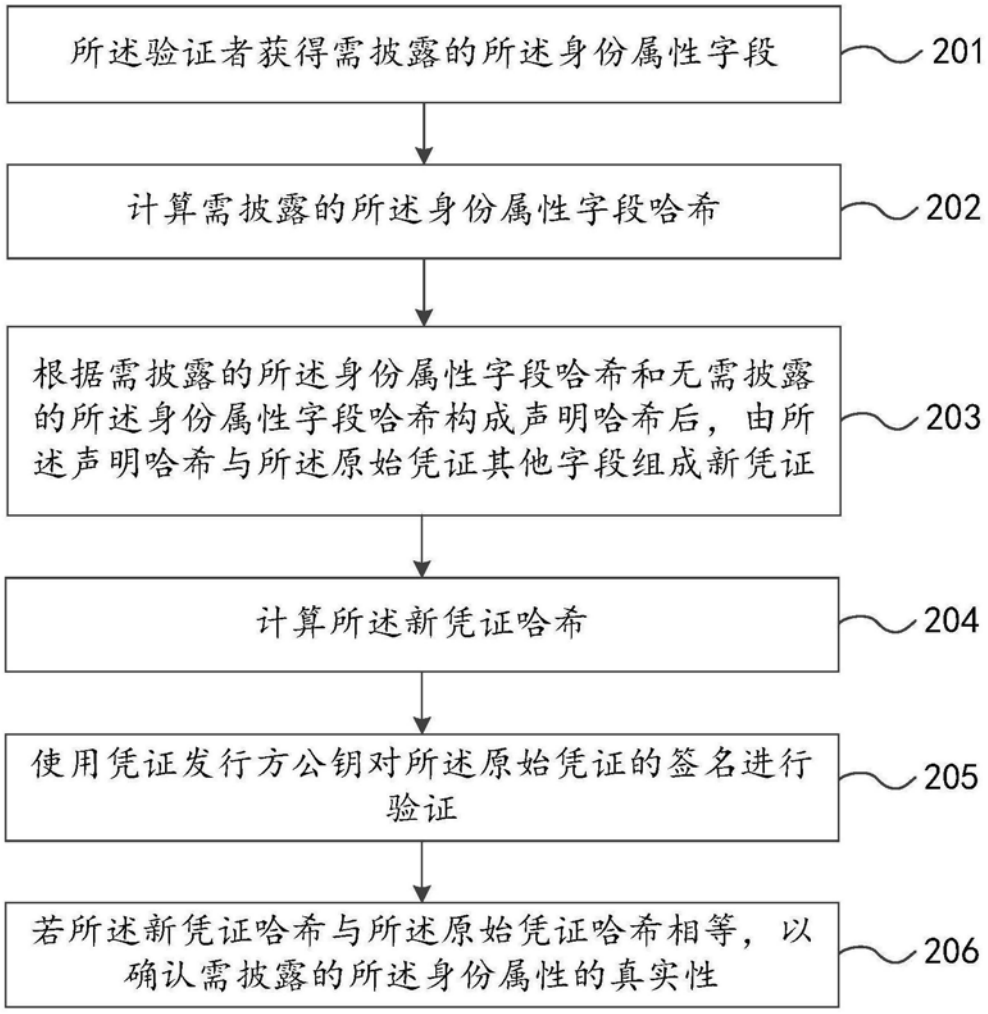

所述验证者获得需披露的所述身份属性字段
201
计算需披露的所述身份属性字段哈希
202
根据需披露的所述身份属性字段哈希和无需披露的所述身份属性字段哈希构成声明哈希后，由所述声明哈希与所述原始凭证其他字段组成新凭证
203
计算所述新凭证哈希
204
使用凭证发行方公钥对所述原始凭证的签名进行验证
205
若所述新凭证哈希与所述原始凭证哈希相等，以确认需披露的所述身份属性的真实性
206

图2

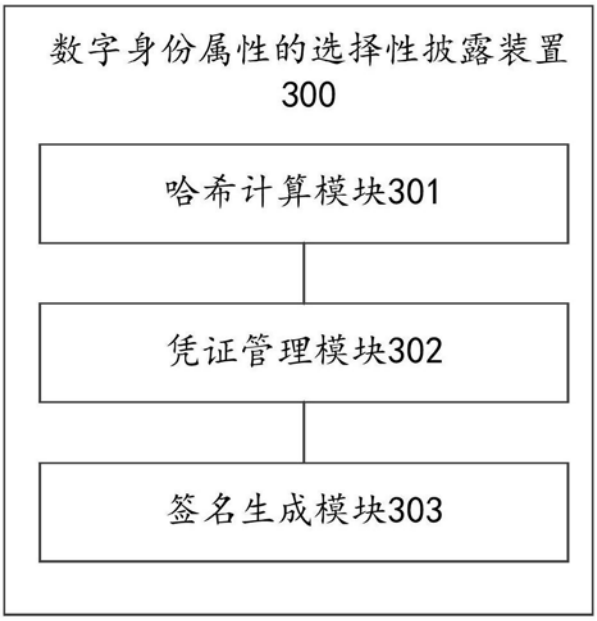

数字身份属性的选择性披露装置
300
哈希计算模块301
凭证管理模块302
签名生成模块303

图3

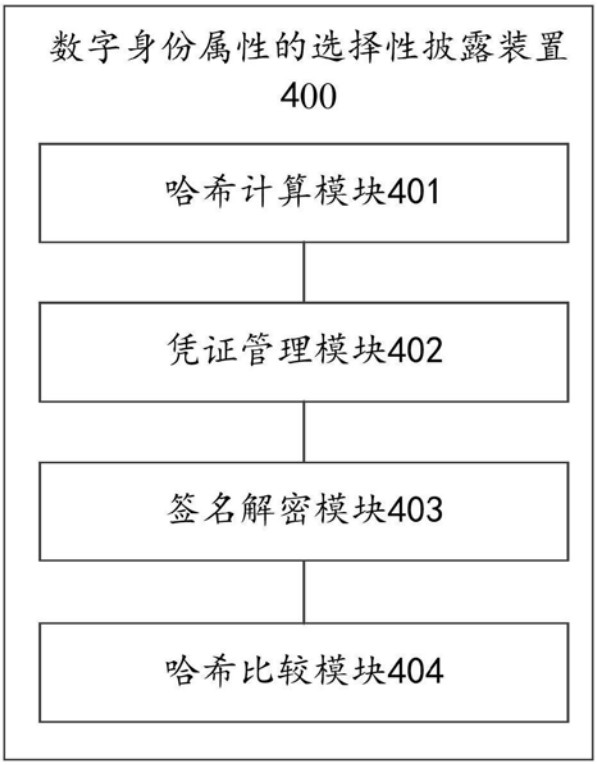

数字身份属性的选择性披露装置
400
哈希计算模块401
凭证管理模块402
签名解密模块403
哈希比较模块404

图4

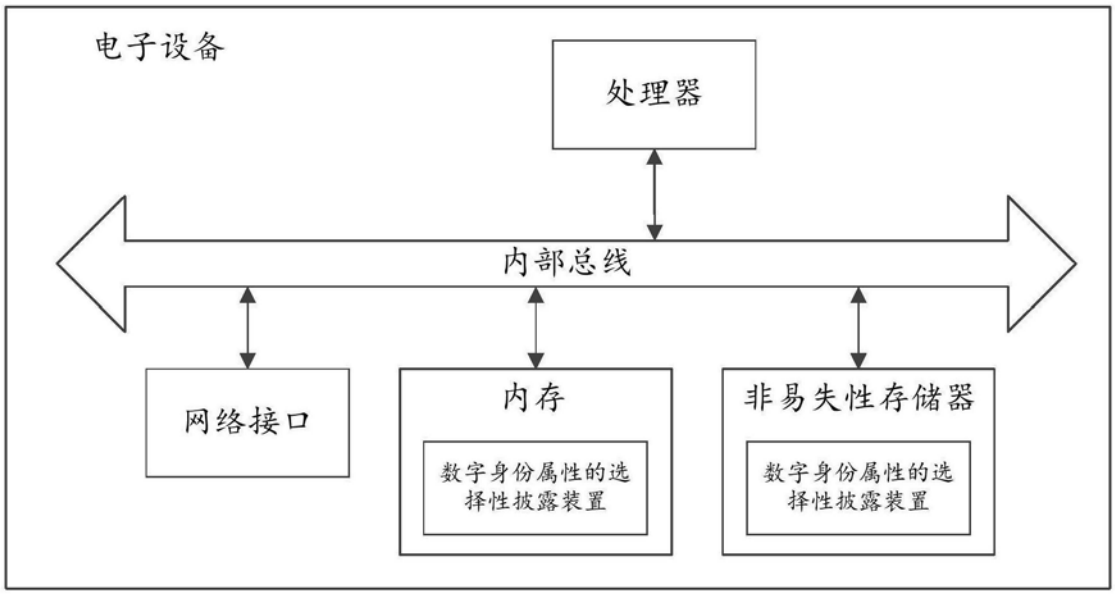

电子设备
处理器
内部总线
网络接口
内存
数字身份属性的选择性披露装置
非易失性存储器
数字身份属性的选择性披露装置

图5