(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 107612870 B
(45)授权公告日 2021.01.05

(21)申请号 201610543643.X
(22)申请日 2016.07.11
(65)同一申请的已公布的文献号
申请公布号 CN 107612870 A
(43)申请公布日 2018.01.19
(73)专利权人 香港理工大学深圳研究院
地址 518000 广东省深圳市南山区高新技术产业园南区粤兴一道18号香港理工大学产学研大楼205室
(72)发明人 宋宇波 肖斌
(74)专利代理机构 深圳中一专利商标事务所 44237
代理人 张全文
(51)Int.Cl.
H04L 29/06(2006.01)
H04L 9/30(2006.01)
审查员 刘叶

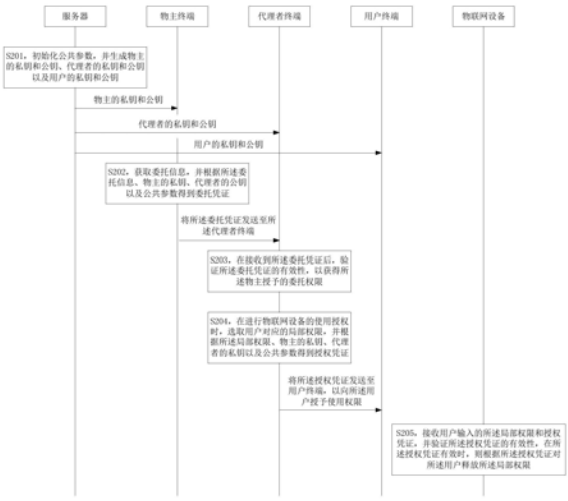
权利要求书2页 说明书10页 附图7页

(54)发明名称

物联网设备的委托授权方法、服务器、终端及物联网设备

(57)摘要

本发明适用于网络安全技术领域，提供了一种物联网设备的委托授权方法、服务器、终端及物联网设备，所述方法包括：服务器初始化公共参数，定义物主、代理者以及用户的私钥和公钥；物主终端根据所述委托信息、物主的私钥、代理者的公钥以及公共参数得到委托凭证，并将其发送至代理者终端；所述代理者终端验证所述委托凭证的有效性；以及根据所述局部权限、物主的私钥、代理者的私钥以及公共参数得到授权凭证，并将其发送至用户终端；所述物联网设备接收并验证用户输入的授权凭证，在所述授权凭证有效时，则根据所述授权凭证对所述用户释放所述局部权限。本发明实现了对物联网设备在被分享使用时的权限管理，以及保护了物主的隐私信息。



CN 107612870 B

1.一种物联网设备的委托授权方法,其特征在于,所述方法包括:

服务器初始化公共参数,并生成物主的私钥和公钥、代理者的私钥和公钥以及用户的私钥和公钥;

物主终端获取委托信息,并根据所述委托信息、物主的私钥、代理者的公钥以及公共参数得到委托凭证,将所述委托凭证发送至代理者终端,以向所述代理者授予委托权限;

所述代理者终端在接收到所述委托凭证后,验证所述委托凭证的有效性,以获得所述物主授予的委托权限;

在进行物联网设备的使用授权时,所述代理者终端选取用户对应的局部权限,并根据所述局部权限、物主的私钥、代理者的私钥以及公共参数得到授权凭证,将所述授权凭证发送至用户终端,以向所述用户授予使用权限;

所述物联网设备接收用户输入的所述局部权限和授权凭证,并验证所述授权凭证的有效性,在所述授权凭证有效时,则根据所述授权凭证对所述用户释放所述局部权限。

2.如权利要求1所述的物联网设备的委托授权方法,其特征在于,所述服务器初始化公共参数,并生成物主的私钥和公钥、代理者的私钥和公钥以及用户的私钥和公钥包括:

服务器选取两个q阶的第一循环群G_1和第二循环群G_2,其中,q为大素数,且在第一循环群G_1和第二循环群G_2上的离散对数问题是难解的,定义第一循环群G_1的生成元P和Q,定义双线性映射$e:G_1\times G_1\rightarrow G_2$,定义Hash函数$H:\{0,1\}^*\times G_1\rightarrow Z_q$;

定义物主的私钥X_{Owner}、代理者的私钥X_{Proxy}、用户的私钥X_{User},则物主的公钥$Y_{Owner}=X_{Owner}P$、代理者的公钥$Y_{Proxy}=X_{Proxy}P$、用户的公钥$Y_{User}=X_{User}P$。

3.如权利要求2所述的物联网设备的委托授权方法,其特征在于,所述物主终端获取委托信息,并根据所述委托信息、物主的私钥、代理者的公钥以及公共参数得到委托凭证,将所述委托凭证发送至所述代理者终端,以向所述代理者授予委托权限包括:

物主终端定义委托信息集合w,其中,$w=(M_i)_{i=1}^n$,M_i表示与物主身份、代理者身份、委托权限或者有效期相关的信息;

根据所述委托信息集合w和Hash函数构建消息摘要集合w_H,以及根据所述消息摘要集合w_H构建第一多项式m(X),其中,$w_H=\{H(M_i)_{i=1}^n\}$, $m(X)=\prod_{i=1}^n(X-H(M_i))$;

选取n阶随机多项式r(X),根据所述第一多项式m(X)、第一循环群G_1的生成元P和Q、物主的私钥X_{Owner}计算中间参数C,其中,$C=m(X_{Owner})P+r(X_{Owner})Q$;

利用物主的私钥X_{Owner}对所述中间参数C、代理者身份ID_{Proxy}以及代理者的公钥Y_{Proxy}进行签名,生成委托证书$Cert_{Owner}$,其中,$Cert_{Owner}=S(C||ID_{Proxy}||Y_{Proxy},X_{Owner})$;

将所述物主的公钥Y_{Owner}、随机多项式值$r(X_{Owner})$、委托信息集合w、中间参数C以及委托证书$Cert_{Owner}$作为委托凭证发送至所述代理者终端,以向所述代理者授予委托权限。

4.如权利要求3所述的物联网设备的委托授权方法,其特征在于,所述代理者终端在接收到所述委托凭证后,验证所述委托凭证的有效性,以获得所述物主授予的委托权限包括:

代理者终端在接收到所述委托凭证后,根据委托信息集合w和Hash函数构建消息摘要集合w_H,以及根据所述消息摘要集合w_H构建第一多项式m(X),其中,$w_H=\{H(M_i)_{i=1}^n\}$, $m(X)=\prod_{i=1}^n(X-H(M_i))$;

根据所述第一多项式m(X)、物主的公钥Y_{Owner}以及第一循环群G_1的生成元P和Q验证等式

$C=m(Y_{Owner})P+r(Y_{Owner})Q$是否成立，若成立，则委托证书$Cert_{Owner}$是有效的，获得所述物主授予的委托权限。

5.如权利要求4所述的物联网设备的委托授权方法，其特征在于，所述在进行物联网设备的使用授权时，所述代理者终端选取用户对应的局部权限，并根据所述局部权限、物主的私钥、代理者的私钥以及公共参数得到授权凭证，将所述授权凭证发送至用户终端，以向所述用户授予使用权限包括：

在进行授权时，所述代理者终端选择用户对应的局部权限M_1，根据Hash函数计算所述局部权限M_1的消息摘要值h_M以及根据n阶随机多项式$r(X)$计算消息摘要值h_M的随机多项式值r_M，其中，$h_M=H(M_1)$，$r_M=r(h_M)$；

选取随机数g，根据所述随机数g构建第二多项式$\Phi(X)$和第三多项式$\hat{\phi}(X)$，其中，第二多项式$\phi(X)=\frac{m(X)-m(g)}{X-g}$，第三多项式$\hat{\phi}(X)=\frac{r(X)-r(g)}{X-g}$，(X-g)可被m(X)-m(g)整除；

根据所述第二多项式$\Phi(X)$、第三多项式$\hat{\phi}(X)$和第一循环群G_1的生成元P和Q、物主的私钥X_{Owner}，计算局部权限授权凭证W_M，其中，$W_M=\phi(X_{Owner})P+\hat{\phi}(X_{Owner})Q$；

利用代理者的私钥X_{Proxy}对所述局部权限授权凭证W_M、随机多项式值r_M以及物主的公钥Y_{Owner}进行签名，生成授权证书$Cert_{Proxy}$，其中，$Cert_{Proxy}=S(W_M||r_M||Y_{Owner},X_{Proxy})$；

将中间参数C、局部权限授权凭证W_M、随机多项式值r_M以及委托证书$Cert_{Owner}$、授权证书$Cert_{Proxy}$作为授权凭证发送至所述用户终端，以向所述用户授予使用权限。

6.如权利要求5所述的物联网设备的委托授权方法，其特征在于，所述物联网设备接收用户输入的所述局部权限和授权凭证，并验证所述授权凭证的有效性，在所述授权凭证有效时，则根据所述授权凭证对所述用户释放所述局部权限包括：

所述物联网设备接收用户输入的局部权限M_1和授权凭证，使用物主的公钥Y_{Owner}对委托证书$Cert_{Owner}$的有效性进行验证，以及使用代理者的公钥Y_{Proxy}对授权证书$Cert_{Proxy}$的有效性进行验证；

若所述委托证书$Cert_{Owner}$和所述授权证书$Cert_{Proxy}$均有效，则验证等式$e(C,P)=e(W_M,Y_{Owner}-h_MP)\cdot e(r_MQ,P)$是否成立，若成立则根据所述授权凭证对所述用户释放使用权限。

物联网设备的委托授权方法、服务器、终端及物联网设备

技术领域

[0001] 本发明属于网络安全技术领域，尤其涉及一种物联网设备的委托授权方法、服务器、终端及物联网设备。

背景技术

[0002] 随着移动通信技术的发展，人们可以随时随地地通过智能设备访问网络，并与连接在网络上的其他智能设备进行通信。用户或设备可以通过网络搜索所需的设备并与之交换数据，以提供用户所需的服务。

[0003] 对于城市设施和公共服务，用户既可以是使用者，也可以成为提供者。用户可以对外共享自己的个人设施和资源，比如汽车、停车位、房屋、场所等，从而帮助政府更有效合理地管理和利用城市设施及个人资源，改善交通、医疗、教育、旅游等各领域的管理效率和服务质量，促进城市的和谐发展。在如此开放分享的城市物联网环境中，物联网设备有可能被多次分享使用，因此共享设备的使用权可以从物主传递到不同的用户(比如朋友和朋友的朋友)，然而，现有技术无法实现对共享设备使用权限的安全传递，无法对物主的身份等隐私信息进行有效保护。

发明内容

[0004] 鉴于此，本发明实施例提供一种物联网设备的委托授权方法、服务器、终端及物联网设备，以实现对物联网设备在被分享使用时的权限管理，以及保护物主的隐私信息。

[0005] 第一方面，提供了一种物联网设备的委托授权方法，所述方法包括：

[0006] 服务器初始化公共参数，并生成物主的私钥和公钥、代理者的私钥和公钥以及用户的私钥和公钥；

[0007] 物主终端获取委托信息，并根据所述委托信息、物主的私钥、代理者的公钥以及公共参数得到委托凭证，将所述委托凭证发送至所述代理者终端，以向所述代理者授予委托权限；

[0008] 所述代理者终端在接收到所述委托凭证后，验证所述委托凭证的有效性，以获得所述物主授予的委托权限；

[0009] 在进行物联网设备的使用授权时，所述代理者终端选取用户对应的局部权限，并根据所述局部权限、物主的私钥、代理者的私钥以及公共参数得到授权凭证，将所述授权凭证发送至用户终端，以向所述用户授予使用权限；

[0010] 所述物联网设备接收用户输入的所述局部权限和授权凭证，并验证所述授权凭证的有效性，在所述授权凭证有效时，则根据所述授权凭证对所述用户释放所述局部权限。

[0011] 第二方面，提供了一种服务器，所述服务器包括：

[0012] 初始化模块，用于选取两个q阶的第一循环群G_1和第二循环群G_2，其中，q为大素数，且在第一循环群G_1和第二循环群G_2上的离散对数问题是难解的，定义第一循环群G_1的生成元P和Q，定义双线性映射$e:G_1\times G_1\rightarrow G_2$，定义Hash函数$H:\{0,1\}^{/}\times G_1\rightarrow Z_q$；

[0013] 定义模块，用于定义物主的私钥X_{Owner}、代理者的私钥X_{Proxy}、用户的私钥X_{User}，则物主的公钥$Y_{Owner}=X_{Owner}P$、代理者的公钥$Y_{Proxy}=X_{Proxy}P$、用户的公钥$Y_{User}=X_{User}P$。

[0014] 第三方面，提供了一种终端，所述终端包括：

[0015] 定义模块，用于定义委托信息集合w，其中，$w=(M_i)_{i=1}^n$，M_i表示与物主身份、代理者身份、委托权限或者有效期相关的信息；

[0016] 构建模块，用于根据所述委托信息集合w和Hash函数构建消息摘要集合w_H，以及根据所述消息摘要集合w_H构建第一多项式m(X)，其中，$w_H=\{H(M_i)_{i=1}^n\}$，$m(X)=\prod_{i=1}^n(X-H(M_i))$；

[0017] 计算模块，用于选取n阶随机多项式r(X)，根据所述第一多项式m(X)、第一循环群G_1的生成元P和Q计算中间参数C，其中，$C=m(X_{Owner})P+r(X_{Owner})Q$；

[0018] 委托证书生成模块，用于利用物主的私钥X_{Owner}对所述中间参数C、代理者身份ID_{Proxy}以及代理者的公钥Y_{Proxy}进行签名，生成委托证书$Cert_{Owner}$，其中，$Cert_{Owner}=S(C||ID_{Proxy}||Y_{Proxy},X_{Owner})$；

[0019] 委托凭证发送模块，用于将所述物主的公钥Y_{Owner}、随机多项式值$r(X_{Owner})$、委托信息集合w、中间参数C以及委托证书$Cert_{Owner}$作为委托凭证发送至所述代理者终端，以向所述代理者授予委托权限。

[0020] 第四方面，提供了一种终端，所述终端包括：

[0021] 第一构建模块，用于在接收到所述委托凭证后，根据委托信息集合w和Hash函数构建消息摘要集合w_H，以及根据所述消息摘要集合w_H构建第一多项式m(X)，其中，$w_H=\{H(M_i)_{i=1}^n\}$，$m(X)=\prod_{i=1}^n(X-H(M_i))$；

[0022] 验证模块，用于根据所述第一多项式m(X)、物主的公钥Y_{Owner}以及第一循环群G_1的生成元P和Q验证等式$C=m(Y_{Owner})P+r(Y_{Owner})Q$是否成立，若成立，则委托证书$Cert_{Owner}$是有效的，获得所述物主授予的委托权限；

[0023] 第一计算模块，用于在进行授权时，选择用户对应的局部权限M_1，根据Hash函数计算所述局部权限M_1的消息摘要值h_M以及根据n阶随机多项式r(X)计算消息摘要值h_M的随机多项式值r_M，其中，$h_M=H(M_1)$，$r_M=r(h_M)$；

[0024] 第二构建模块，用于选取随机数g，根据所述随机数g构建第二多项式Φ(X)和第三多项式$\hat{\phi}(X)$，其中，第二多项式$\phi(X)=\frac{m(X)-m(g)}{X-g}$，第三多项式$\hat{\phi}(X)=\frac{r(X)-r(g)}{X-g}$，(X-g)可被m(X)-m(g)整除；

[0025] 第二计算模块，用于根据所述第二多项式Φ(X)、第三多项式$\hat{\phi}(X)$和第一循环群G_1的生成元P和Q，计算局部权限授权凭证W_M，其中，$W_M=\phi(X_{Owner})P+\hat{\phi}(X_{Owner})Q$；

[0026] 授权证书生成模块，用于利用代理者的私钥X_{Proxy}对所述局部权限授权凭证W_M、随机多项式值r_M以及物主的公钥Y_{Owner}进行签名，生成授权证书$Cert_{Proxy}$，其中，$Cert_{Proxy}=S(W_M||r_M||Y_{Owner},X_{Proxy})$

[0027] 授权凭证发送模块，用于将中间参数C、局部权限授权凭证W_M、随机多项式值r_M以及委托证书$Cert_{Owner}$、授权证书$Cert_{Proxy}$作为授权凭证发送至所述用户终端，以向所述用户授

予使用权限。

[0028] 第五方面，提供了一种物联网设备，所述物联网设备包括：

[0029] 第一验证模块，用于接收用户输入的局部权限M_1和授权凭证，所述授权凭证包括中间参数C、局部权限授权凭证W_M、随机多项式值r_M以及委托证书$Cert_{Owner}$、授权证书$Cert_{Proxy}$，使用物主的公钥Y_{Owner}对委托证书$Cert_{Owner}$的有效性进行验证，以及使用代理者的公钥Y_{Proxy}对授权证书$Cert_{Proxy}$的有效性进行验证；

[0030] 第二验证模块，用于若所述委托证书$Cert_{Owner}$和所述授权证书$Cert_{Proxy}$均有效，则验证等式$e(C,P)=e(W_M,Y_{Owner}-h_MP)\cdot e(r_MQ,P)$是否成立，若成立则根据所述授权凭证对所述用户释放使用权限；

[0031] 其中，所述e表示双线性映射，且$e:G_1\times G_1\rightarrow G_2$，所述$G_1$表示第一循环群，所述$G_2$表示第二循环群，所述P和Q表示第一循环群$G_1$的生成元，所述$h_M$表示根据Hash函数计算的所述局部权限$M_1$的消息摘要值$h_M$。

[0032] 通过本发明实施例，实现了对物联网设备在被分享使用时的权限管理，物主可以委托代理者进行授权，代理者可以代表物主向其他用户授予对物联网设备的使用权限，且在用户与物联网设备交互的过程中无需涉及与物主的身份信息、委托权限及有效期等相关的信息，从而起到了匿名授权的作用，有效地保护了物主的隐私信息。

附图说明

[0033] 为了更清楚地说明本发明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发明的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他附图。

[0034] 图1是本发明实施例提供的物联网设备的委托授权系统的组成框图；

[0035] 图2是本发明实施例提供的物联网设备的委托授权方法的实现流程图；

[0036] 图3是本发明实施例提供的物联网设备的委托授权方法中步骤S201的实现流程图；

[0037] 图4是本发明实施例提供的物联网设备的委托授权方法中步骤S202的实现流程图；

[0038] 图5是本发明实施例提供的物联网设备的委托授权方法中步骤S204的实现流程图；

[0039] 图6是本发明实施例提供的服务器的组成结构图；

[0040] 图7是本发明实施例提供的终端的组成结构图；

[0041] 图8是本发明另一实施例提供的终端的组成结构图；

[0042] 图9是本发明实施例提供的物联网设备的组成结构图。

具体实施方式

[0043] 为了使本发明的目的、技术方案及优点更加清楚明白，以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。

[0044] 图1示出了本发明实施例提供的物联网设备的委托授权系统的组成框图。

[0045] 在本发明实施例中，所述物联网设备的委托授权系统包括服务器1、物主终端2、代理者终端3、用户终端4以及至少一个物联网设备5。

[0046] 所述服务器1作为证书机构，用于初始化公共参数，以及生成物主的私钥和公钥、代理者的私钥和公钥以及用户的私钥和公钥。通过离线的方式，将所述物主的私钥和公钥发送给所述物主终端2、将所述代理者的私钥和公钥发送给所述代理者终端3以及将用户的私钥和公钥发送给所述用户终端4。

[0047] 所述物主终端2与物主对应，为物主方使用的终端，包括但不限于智能手机、平板电脑等智能设备。在本发明实施例中，所述物主终端2用于获取委托信息，并根据所述委托信息、物主的私钥、代理者的公钥以及公共参数得到委托凭证，将所述委托凭证发送至所述代理者终端，以向所述代理者授予委托权限。其中，所述委托凭证为物主委托代理者向其他用户授予使用所述物联网设备5的权限凭证，即将对物联网设备使用权限的授权能力传递给代理者。

[0048] 所述代理者终端3与代理者对应，为代理者方使用的终端，包括但不限于智能手机、平板电脑等智能设备。在本发明实施例中，所述代理者终端3用于在接收到所述委托凭证后，验证所述委托凭证的有效性，以获得所述物主授予的委托权限；在进行物联网设备的使用授权时，则选取用户对应的局部权限，并根据所述局部权限、物主的私钥、代理者的私钥以及公共参数得到授权凭证，将所述授权凭证发送至用户终端，以向所述用户授予使用权限。其中，所述授权凭证为代理者代表物主授权其他用户使用所述物联网设备5的权限凭证，即将对物联网设备的使用权限传递给用户。

[0049] 所述用户终端4与用户对应，为用户方使用的终端，包括但不限于智能手机、平板电脑等智能设备。在本发明实施例中，所述用户终端4用于接收代理者终端3发送的授权凭证，以及向用户展示所述授权凭证。

[0050] 当用户需要使用物联网设备5时，则通过输入所述局部权限和授权凭证来获取许可。此时，所述物联网设备5通过接收用户输入的所述授权凭证，并验证所述授权凭证的有效性，在所述授权凭证有效时，则根据所述授权凭证对所述用户释放使用权限；否则，若授权凭证无效时，则授权失败。

[0051] 示例性地，所述物主终端2、代理者终端3以及用户终端4与服务器1之间可以通过互联网连接通信，所述用户终端4和所述物联网设备5之间可以通过蓝牙技术连接通信。当然，上述连接方式仅为本发明的一个优选示例，在实际应用中，也可以使用其他方式实现连接通信。

[0052] 图2示出了本发明实施例提供的物联网设备的委托授权方法的实现流程。

[0053] 在本发明实施例中，所述方法应用于上述图1实施例中所述的物联网设备的委托授权系统。

[0054] 参阅图2，所述方法包括：

[0055] 在步骤S201中，服务器初始化公共参数，并生成物主的私钥和公钥、代理者的私钥和公钥以及用户的私钥和公钥。

[0056] 在这里，所述公共参数为系统运行所必须的初始参数，记为Params。在本发明实施例中，所述Params＝{G_1,G_2,q,P,e,H}，其中，所述G_1和G_2表示q阶循环群，所述P表示循环群G_1

的生成元，所述e表示双线性映射，所述H表示安全的Hash函数。

[0057] 作为本发明的一个优选示例，图3示出了本发明实施例提供的物联网设备的委托授权方法中步骤S201的具体实现流程。参阅图3，所述步骤S201包括：

[0058] 在步骤S301中，服务器选取两个q阶的第一循环群G_1和第二循环群G_2，其中，q为大素数，且在第一循环群G_1和第二循环群G_2上的离散对数问题是难解的，定义第一循环群G_1的生成元P和Q，定义双线性映射$e:G_1\times G_1\rightarrow G_2$，定义Hash函数$H:\{0,1\}^*\times G_1\rightarrow Z_q$。

[0059] 在步骤S302中，定义物主的私钥X_{Owner}、代理者的私钥X_{Proxy}、用户的私钥X_{User}，则物主的公钥$Y_{Owner}=X_{Owner}P$、代理者的公钥$Y_{Proxy}=X_{Proxy}P$、用户的公钥$Y_{User}=X_{User}P$。

[0060] 在本发明实施例中，服务器1在完成对物主的私钥和公钥、代理者的私钥和公钥以及用户的公钥和私钥的初始化之后，通过离线的方式，分别将所述物主的私钥和公钥发送给所述物主终端2、将所述代理者的私钥和公钥发送给所述代理者终端3以及将用户的私钥和公钥发送给所述用户终端4。所述群Z_q表示Hash函数$\{0,1\}^*\times G_1$的结果。

[0061] 在步骤S202中，物主终端获取委托信息，并根据所述委托信息、物主的私钥、代理者的公钥以及公共参数得到委托凭证，将所述委托凭证发送至所述代理者终端，以向所述代理者授予委托权限。

[0062] 在这里，所述委托信息为与物主的身份信息、代理者的身份信息、委托权限及有效期相关的信息。委托权限表示物主分配给代理者的可授权范围。

[0063] 作为本发明的一个优选示例，图4示出了本发明实施例提供的物联网设备的匿名授权部分委托方法中步骤S202的具体实现流程。参阅图4，所述步骤S202包括：

[0064] 在步骤S401中，物主终端定义委托信息集合w，其中，$w=(M_i)_{i=1}^n$，M_i表示与物主身份、代理者身份、委托权限或者有效期相关的信息。

[0065] 在步骤S402中，根据所述委托信息集合w和Hash函数构建消息摘要集合w_H，以及根据所述消息摘要集合w_H构建第一多项式m(X)，其中，$w_H=\{H(M_i)_{i=1}^n\}$，$m(X)=\prod_{i=1}^n(X-H(M_i))$。

[0066] 在步骤S403中，选取n阶随机多项式r(X)，根据所述第一多项式m(X)、第一循环群G_1的生成元P和Q、物主的私钥X_{Owner}计算中间参数C，其中，$C=m(X_{Owner})P+r(X_{Owner})Q$。

[0067] 在步骤S404中，利用物主的私钥X_{Owner}对所述中间参数C、代理者身份ID_{Proxy}以及代理者的公钥Y_{Proxy}进行签名，生成委托证书$Cert_{Owner}$，其中，$Cert_{Owner}=S(C||ID_{Proxy}||Y_{Proxy},X_{Owner})$。

[0068] 在步骤S405中，将所述物主的公钥Y_{Owner}、随机多项式值$r(X_{Owner})$、委托信息集合w、中间参数C以及委托证书$Cert_{Owner}$作为委托凭证发送至所述代理者终端，以向所述代理者授予委托权限。

[0069] 在步骤S203中，所述代理者终端在接收到所述委托凭证后，验证所述委托凭证的有效性，以获得所述物主授予的委托权限。

[0070] 在本发明实施例中，代理者终端3在接收到所述委托凭证后，根据委托信息集合w和Hash函数构建消息摘要集合w_H，其中，$w_H=\{H(M_i)_{i=1}^n\}$；然后，根据所述消息摘要集合w_H构建第一多项式m(X)，其中$m(X)=\prod_{i=1}^n(X-H(M_i))$。所述代理者终端3根据所述第一多项式m(X)、物主的公钥Y_{Owner}以及第一循环群G_1的生成元P和Q验证等式$C=m(Y_{Owner})P+r(Y_{Owner})Q$是

否成立;若成立,则委托证书$Cert_{Owner}$是有效的,获得所述物主授予的委托权限。代理者可以代表物主授予用户所述物理网设备的使用权限。

[0071] 在步骤S204中,在进行物联网设备的使用授权时,所述代理者终端选取用户对应的局部权限,并根据所述局部权限、物主的私钥、代理者的私钥以及公共参数得到授权凭证,将所述授权凭证发送至用户终端,以向所述用户授予使用权限。

[0072] 在本发明实施例中,在获取到委托权限后,代理者可以针对不同信任度的用户授予不同的使用权限,从而实现了对用户的局部授权。

[0073] 作为本发明的一个优选示例,图5示出了本发明实施例提供的物联网设备的委托授权方法中步骤S204的具体实现流程。参阅图5,所述步骤S204包括:

[0074] 在步骤S501中,在进行授权时,所述代理者终端选择用户对应的局部权限M_1,根据Hash函数计算所述局部权限M_1的消息摘要值h_M以及根据n阶随机多项式r(X)计算消息摘要值h_M的随机多项式值r_M,其中,$h_M=H(M_1)$,$r_M=r(h_M)$。

[0075] 在步骤S502中,选取随机数g,根据所述随机数g构建第二多项式Φ(X)和第三多项式$\hat{\phi}(X)$,其中,第二多项式$\phi(X)=\frac{m(X)-m(g)}{X-g}$,第三多项式$\hat{\phi}(X)=\frac{r(X)-r(g)}{X-g}$,(X-g)可被m(X)-m(g)整除。

[0076] 在步骤S503中,根据所述第二多项式Φ(X)、第三多项式$\hat{\phi}(X)$和第一循环群G_1的生成元P和Q、物主的私钥X_{Owner},计算局部权限授权凭证W_M,其中,$W_M=\phi(X_{Owner})P+\hat{\phi}(X_{Owner})Q$。

[0077] 在这里,通过计算得到的局部权限授权凭证W_M反映了用户和代理者的社交关系以及根据两者之间的亲密度授予的相应权限。

[0078] 在步骤S504中,利用代理者的私钥X_{Proxy}对所述局部权限授权凭证W_M、随机多项式值r_M以及物主的公钥Y_{Owner}进行签名,生成授权证书$Cert_{Proxy}$,其中,$Cert_{Proxy}=S(W_M||r_M||Y_{Owner},X_{Proxy})$。

[0079] 在步骤S505中,将中间参数C、局部权限授权凭证W_M、随机多项式值r_M以及委托证书$Cert_{Owner}$、授权证书$Cert_{Proxy}$作为授权凭证发送至所述用户终端,以向所述用户授予使用权限。

[0080] 在这里,本发明实施例以中间参数C、局部权限授权凭证W_M、随机多项式值r_M以及委托证书$Cert_{Owner}$、授权证书$Cert_{Proxy}$作为授权凭证,代理者终端3发送给用户的授权凭证无需包括物主的身份信息、委托权限以及有效期等信息,从而起到了保护物主隐私的作用。

[0081] 在步骤S205中,物联网设备接收用户输入的所述局部权限和授权凭证,并验证所述授权凭证的有效性,在所述授权凭证有效时,则根据所述授权凭证对所述用户释放所述局部权限。

[0082] 在这里,当用户需要访问物联网设备时,则将用户终端4接收的授权凭证以及局部权限M_1递交给物联网设备5,以发出使用请求。

[0083] 所述物联网设备5接收用户输入的所述局部权限M_1和授权凭证,使用物主的公钥Y_{Owner}对委托证书$Cert_{Owner}$的有效性进行验证,以及使用代理者的公钥为Y_{Proxy}对授权证书$Cert_{Proxy}$的有效性进行验证。

[0084] 若所述委托证书$Cert_{Owner}$和所述授权证书$Cert_{Proxy}$均有效时，则验证等式$e(C,P)=e(W_M,Y_{Owner}-h_MP)\cdot e(r_MQ,P)$是否成立，若成立则接收用户的使用请求，根据所述授权凭证对所述用户释放使用权限；否则，用户的使用请求失败。

[0085] 在本发明实施例中，用于签名的算法可以为椭圆曲线公钥加密算法，所使用的Hash函数可以为SHA256算法。应当理解，这些加密算法仅为本发明实施例的一个优选示例，也可以使用其他加密算法。

[0086] 通过本发明实施例，实现了对物联网设备在被分享使用时的权限管理，物主可以委托代理者进行授权，代理者可以代表物主向其他用户授予对物联网设备的使用权限，且在用户与物联网设备交互的过程中无需涉及与物主的身份信息、委托权限及有效期等相关的信息，从而起到了匿名授权的作用，有效地保护了物主的隐私信息，为开放的智慧城市物联网环境中的设备共享服务提供了有效的保障。

[0087] 图6示出了本发明实施例提供的服务器的组成结构，为了便于说明，仅示出了与本发明实施例相关的部分。

[0088] 在本发明实施例中，所述服务器用于实现上述图1、图2或图3所示的物联网设备的委托授权方法中的服务器1的功能，作为证书机构，生成系统运行所必须的公共参数、公钥和私钥。参阅图6，所述服务器包括：

[0089] 初始化模块11，用于选取两个q阶的第一循环群G_1和第二循环群G_2，其中，q为大素数，且在第一循环群G_1和第二循环群G_2上的离散对数问题是难解的，定义第一循环群G_1的生成元P和Q，定义双线性映射$e:G_1\times G_1\rightarrow G_2$，定义Hash函数$H:\{0,1\}^*\times G_1\rightarrow Z_q$；

[0090] 定义模块12，用于定义物主的私钥X_{Owner}、代理者的私钥X_{Proxy}、用户的私钥X_{User}，则物主的公钥$Y_{Owner}=X_{Owner}P$、代理者的公钥$Y_{Proxy}=X_{Proxy}P$、用户的公钥$Y_{User}=X_{User}P$。

[0091] 在本发明实施例中，服务器1在完成对物主的私钥和公钥、代理者的私钥和公钥以及用户的公钥和私钥的初始化之后，通过离线的方式，分别将所述物主的私钥和公钥发送给所述物主终端2、将所述代理者的私钥和公钥发送给所述代理者终端3以及将用户的私钥和公钥发送给所述用户终端4。

[0092] 图7示出了本发明实施例提供的终端的组成结构，为了便于说明，仅示出了与本发明实施例相关的部分。

[0093] 在本发明实施例中，所述终端用于实现上述图1、图2或图4所示的物联网设备的委托授权方法中的物主终端2的功能，作为物主方使用的设备，实现将对物联网设备使用权限的授权能力传递给代理者。可选地，所述终端包括但不限于智能手机、平板电脑等智能设备。

[0094] 参阅图7，所述终端包括：

[0095] 定义模块21，用于定义委托信息集合w，其中，$w=(M_i)_{i=1}^n$，M_i表示与物主身份、代理者身份、委托权限或者有效期相关的信息；

[0096] 构建模块22，用于根据所述委托信息集合w和Hash函数构建消息摘要集合w_H，以及根据所述消息摘要集合w_H构建第一多项式m(X)，其中，

$$w_H=\{H(M_i)_{i=1}^n\},\quad m(X)=\prod_{i=1}^n(X-H(M_i));$$

[0097] 计算模块23，用于选取n阶随机多项式r(X)，根据所述第一多项式m(X)、第一循环群G_1的生成元P和Q、物主的私钥X_{Owner}计算中间参数C，其中，$C=m(X_{Owner})P+r(X_{Owner})Q$；

[0098] 委托证书生成模块24，用于利用物主的私钥X_{Owner}对所述中间参数C、代理者身份ID_{Proxy}以及代理者的公钥Y_{Proxy}进行签名，生成委托证书$Cert_{Owner}$，其中，$Cert_{Owner}=S(C||ID_{Proxy}||Y_{Proxy},X_{Owner})$；

[0099] 委托凭证发送模块25，用于将所述物主的公钥Y_{Owner}、随机多项式值$r(X_{Owner})$、委托信息集合w、中间参数C以及委托证书$Cert_{Owner}$作为委托凭证发送至代理者终端，以向所述代理者授予委托权限。

[0100] 图8示出了本发明另一实施例提供的终端的组成结构，为了便于说明，仅示出了与本发明实施例相关的部分。

[0101] 在本发明实施例中，所述终端用于实现上述图1、图2或图5所示的物联网设备的委托授权方法中的代理者终端3的功能，作为代理者方使用的设备，实现代表物主的身份将对物联网设备的使用权限传递给用户。可选地，所述终端包括但不限于智能手机、平板电脑等智能设备。

[0102] 参阅图8，所述终端包括：

[0103] 第一构建模块31，用于在接收到所述委托凭证后，根据委托信息集合w和Hash函数构建消息摘要集合w_H，以及根据所述消息摘要集合w_H构建第一多项式m(X)，其中，$w_H=\{H(M_i)_{i=1}^n\}$，$m(X)=\prod_{i=1}^n(X-H(M_i))$；

[0104] 验证模块32，用于根据所述第一多项式m(X)、物主的公钥Y_{Owner}以及第一循环群G_1的生成元P和Q验证等式$C=m(Y_{Owner})P+r(Y_{Owner})Q$是否成立，若成立，则委托证书$Cert_{Owner}$是有效的，获得所述物主授予的委托权限；

[0105] 第一计算模块33，用于在进行授权时，选择用户对应的局部权限M_1，根据Hash函数计算所述局部权限M_1的消息摘要值h_M以及根据n阶随机多项式r(X)计算消息摘要值h_M的随机多项式值r_M，其中，$h_M=H(M_1)$，$r_M=r(h_M)$；

[0106] 第二构建模块34，用于选取随机数g，根据所述随机数g构建第二多项式φ(X)和第三多项式$\hat{\phi}(X)$，其中，第二多项式$\phi(X)=\frac{m(X)-m(g)}{X-g}$，第三多项式$\hat{\phi}(X)=\frac{r(X)-r(g)}{X-g}$，(X-g)可被m(X)-m(g)整除；

[0107] 第二计算模块35，用于根据所述第二多项式φ(X)、第三多项式$\hat{\phi}(X)$和第一循环群G_1的生成元P和Q、物主的私钥X_{Owner}，计算局部权限授权凭证W_M，其中，$W_M=\phi(X_{Owner})P+\hat{\phi}(X_{Owner})Q$；

[0108] 授权证书生成模块36，用于利用代理者的私钥X_{Proxy}对所述局部权限授权凭证W_M、随机多项式值r_M以及物主的公钥Y_{Owner}进行签名，生成授权证书$Cert_{Proxy}$，其中，$Cert_{Proxy}=S(W_M||r_M||Y_{Owner},X_{Proxy})$

[0109] 授权凭证发送模块37，用于将中间参数C、局部权限授权凭证W_M、随机多项式值r_M以及委托证书$Cert_{Owner}$、授权证书$Cert_{Proxy}$作为授权凭证发送至用户终端，以向所述用户授予使用权限。

[0110] 在这里，本发明实施例以中间参数C、局部权限授权凭证W_M、随机多项式值r_M以及委托证书$Cert_{Owner}$、授权证书$Cert_{Proxy}$作为授权凭证，终端发送给用户的授权凭证无需包括物主的身份信息、委托权限以及有效期等信息，从而起到了保护物主隐私的作用。

[0111] 图9示出了本发明另一实施例提供的物联网设备的组成结构，为了便于说明，仅示出了与本发明实施例相关的部分。

[0112] 在本发明实施例中，所述物联网设备用于实现上述图1或图2所示的物联网设备的委托授权方法中的物联网设备5的功能，包括但不限于接入互联网的智能设备。参阅图9，所述物联网设备包括：

[0113] 第一验证模块51，用于接收用户输入的局部权限M_1和授权凭证，所述授权凭证包括中间参数C、局部权限授权凭证W_M、随机多项式值r_M以及委托证书$Cert_{Owner}$、授权证书$Cert_{Proxy}$，使用物主的公钥Y_{Owner}对委托证书$Cert_{Owner}$的有效性进行验证，以及使用代理者的公钥Y_{Proxy}对授权证书$Cert_{Proxy}$的有效性进行验证；

[0114] 第二验证模块52，用于若所述委托证书$Cert_{Owner}$和所述授权证书$Cert_{Proxy}$均有效，则验证等式$e(C,P)=e(W_M,Y_{Owner}-h_MP)\cdot e(r_MQ,P)$是否成立，若成立则根据所述授权凭证对所述用户释放使用权限；

[0115] 其中，所述e表示双线性映射，且$e:G_1\times G_1\rightarrow G_2$，所述$G_1$表示第一循环群和所述$G_2$表示第二循环群，所述P和Q表示第一循环群$G_1$的生成元，所述$h_M$表示根据Hash函数计算的所述局部权限$M_1$的消息摘要值$h_M$。

[0116] 需要说明的是，本发明实施例中的装置可以用于实现上述方法实施例中的全部技术方案，其各个功能模块的功能可以根据上述方法实施例中的方法具体实现，其具体实现过程可参照上述实例中的相关描述，此处不再赘述。

[0117] 通过本发明实施例，实现了对物联网设备在被分享使用时的权限管理，物主可以授权代理者向其他用户分享物联网设备的使用权限；且在用户与物联网设备交互的过程中无需涉及与物主的身份信息、委托权限及有效期等相关的信息，从而起到了匿名授权的作用，有效地保护了物主的隐私信息，为开放的智慧城市物联网环境中的设备共享服务提供了有效的保障。

[0118] 本领域普通技术人员可以意识到，结合本文中所公开的实施例描述的各示例的单元及算法步骤，能够以电子硬件、或者计算机软件和电子硬件的结合来实现。这些功能究竟以硬件还是软件方式来执行，取决于技术方案的特定应用和设计约束条件。专业技术人员可以对每个特定的应用来使用不同方法来实现所描述的功能，但是这种实现不应认为超出本发明的范围。

[0119] 所属领域的技术人员可以清楚地了解到，为描述的方便和简洁，上述描述的装置和单元的具体工作过程，可以参考前述方法实施例中的对应过程，在此不再赘述。

[0120] 在本申请所提供的几个实施例中，应该理解到，所揭露的物联网设备的委托授权方法、服务器、终端及物联网设备，可以通过其它的方式实现。例如，以上所描述的装置实施例仅仅是示意性的，例如，所述模块、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，例如多个单元或组件可以结合或者可以集成到另一个系统，或一些特征可以忽略，或不执行。另一点，所显示或讨论的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，装置或单元的间接耦合或通信连接，可以是电性，机械或其它的形式。

[0121] 所述作为分离部件说明的单元可以是或者也可以不是物理上分开的，作为单元显示的部件可以是或者也可以不是物理单元，即可以位于一个地方，或者也可以分布到多个

网络单元上。可以根据实际的需要选择其中的部分或者全部单元来实现本实施例方案的目的。

[0122] 另外，在本发明各个实施例中的各功能单元、模块可以集成在一个处理单元中，也可以是各个单元、模块单独物理存在，也可以两个或两个以上单元、模块集成在一个单元中。

[0123] 所述功能如果以软件功能单元的形式实现并作为独立的产品销售或使用时，可以存储在一个计算机可读取存储介质中。基于这样的理解，本发明的技术方案本质上或者说对现有技术做出贡献的部分或者该技术方案的部分可以以软件产品的形式体现出来，该计算机软件产品存储在一个存储介质中，包括若干指令用以使得一台计算机设备(可以是个人计算机，服务器，或者网络设备等)执行本发明各个实施例所述方法的全部或部分步骤。而前述的存储介质包括:U盘、移动硬盘、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。

[0124] 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所述以权利要求的保护范围为准。

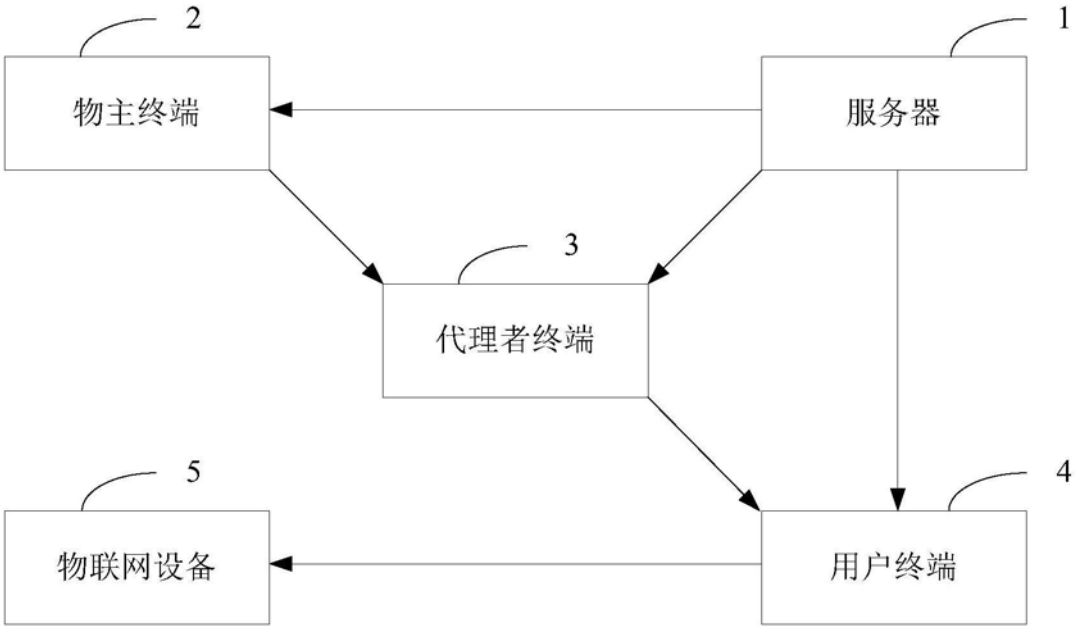


图1

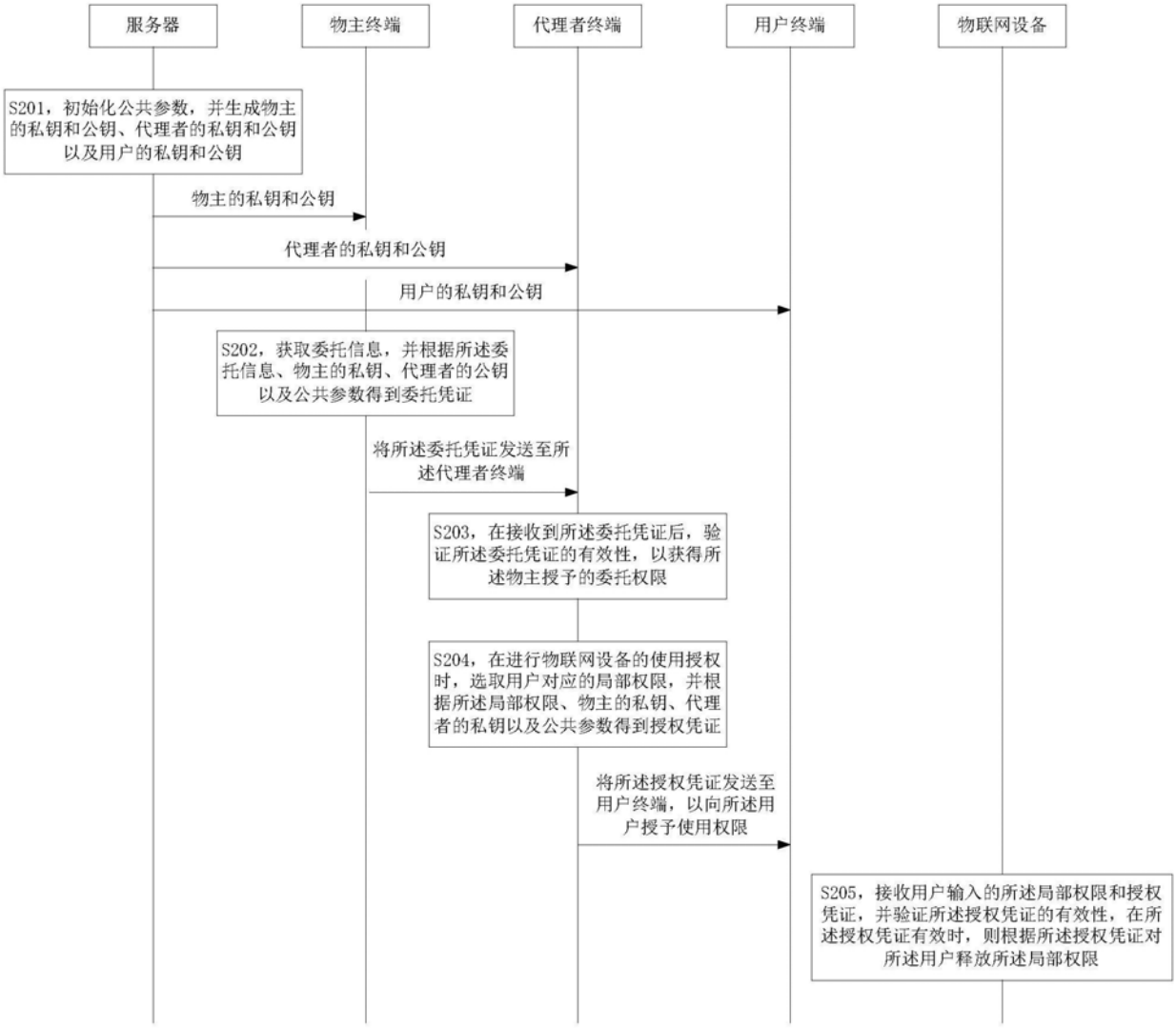

服务器
物主终端
代理者终端
用户终端
物联网设备
S201，初始化公共参数，并生成物主的私钥和公钥、代理者的私钥和公钥以及用户的私钥和公钥
物主的私钥和公钥
代理者的私钥和公钥
用户的私钥和公钥
S202，获取委托信息，并根据所述委托信息、物主的私钥、代理者的公钥以及公共参数得到委托凭证
将所述委托凭证发送至所述代理者终端
S203，在接收到所述委托凭证后，验证所述委托凭证的有效性，以获得所述物主授予的委托权限
S204，在进行物联网设备的使用授权时，选取用户对应的局部权限，并根据所述局部权限、物主的私钥、代理者的私钥以及公共参数得到授权凭证
将所述授权凭证发送至用户终端，以向所述用户授予使用权限
S205，接收用户输入的所述局部权限和授权凭证，并验证所述授权凭证的有效性，在所述授权凭证有效时，则根据所述授权凭证对所述用户释放所述局部权限

图2

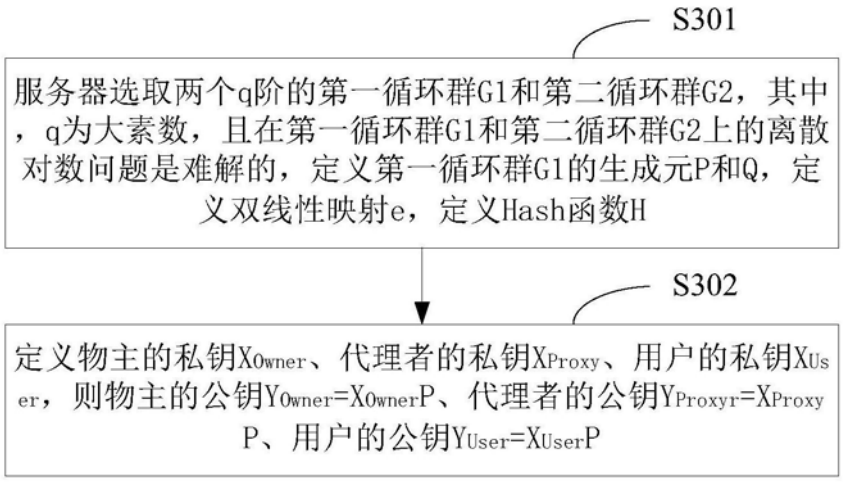

S301
服务器选取两个q阶的第一循环群G1和第二循环群G2，其中，q为大素数，且在第一循环群G1和第二循环群G2上的离散对数问题是难解的，定义第一循环群G1的生成元P和Q，定义双线性映射e，定义Hash函数H
S302
定义物主的私钥X_{Owner}、代理者的私钥X_{Proxy}、用户的私钥X_{User}，则物主的公钥$Y_{Owner}=X_{Owner}P$、代理者的公钥$Y_{Proxyr}=X_{Proxy}P$、用户的公钥$Y_{User}=X_{User}P$

图3

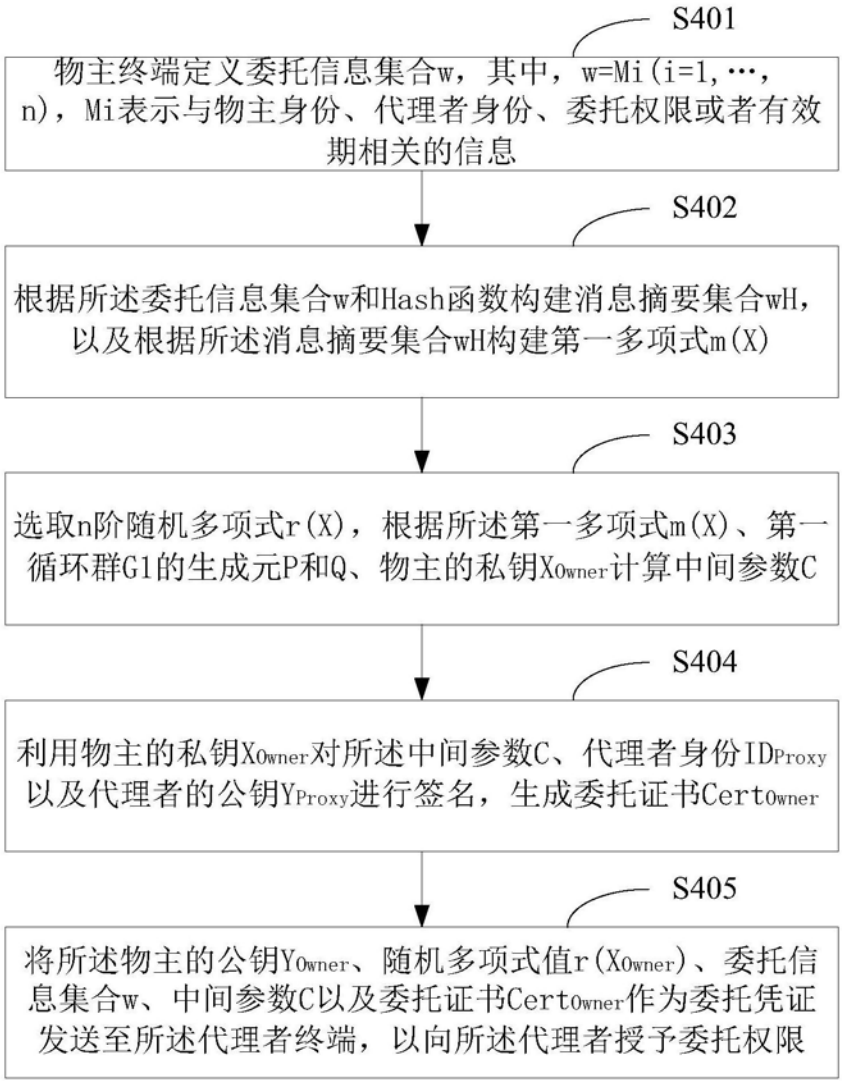

S401
物主终端定义委托信息集合w，其中，w=Mi(i=1,…，n)，Mi表示与物主身份、代理者身份、委托权限或者有效期相关的信息
S402
根据所述委托信息集合w和Hash函数构建消息摘要集合wH，以及根据所述消息摘要集合wH构建第一多项式m(X)
S403
选取n阶随机多项式r(X)，根据所述第一多项式m(X)、第一循环群G1的生成元P和Q、物主的私钥XOwner计算中间参数C
S404
利用物主的私钥XOwner对所述中间参数C、代理者身份IDProxy以及代理者的公钥YProxy进行签名，生成委托证书CertOwner
S405
将所述物主的公钥YOwner、随机多项式值r(XOwner)、委托信息集合w、中间参数C以及委托证书CertOwner作为委托凭证发送至所述代理者终端，以向所述代理者授予委托权限

图4

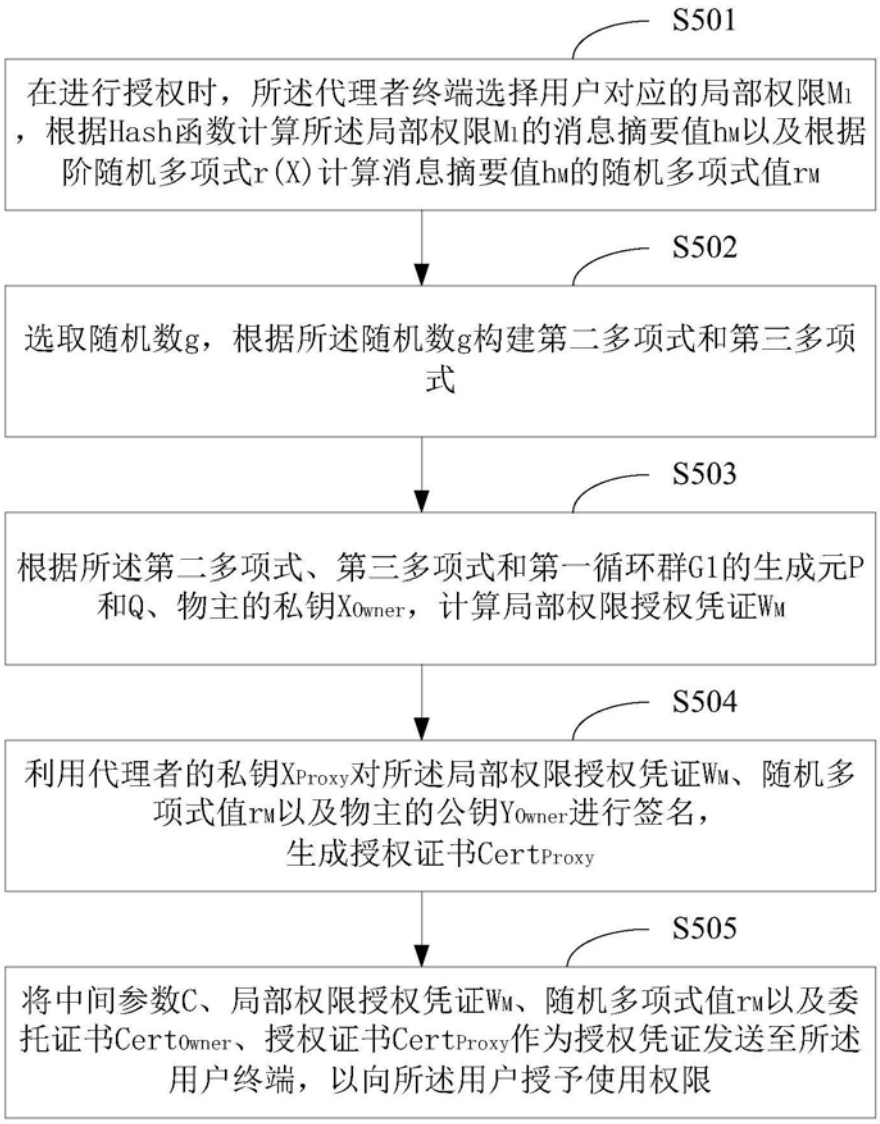

S501
在进行授权时，所述代理者终端选择用户对应的局部权限M_1，根据Hash函数计算所述局部权限M_1的消息摘要值h_M以及根据阶随机多项式r(X)计算消息摘要值h_M的随机多项式值r_M
S502
选取随机数g，根据所述随机数g构建第二多项式和第三多项式
S503
根据所述第二多项式、第三多项式和第一循环群G1的生成元P和Q、物主的私钥X_{Owner}，计算局部权限授权凭证W_M
S504
利用代理者的私钥X_{Proxy}对所述局部权限授权凭证W_M、随机多项式值r_M以及物主的公钥Y_{Owner}进行签名，生成授权证书$Cert_{Proxy}$
S505
将中间参数C、局部权限授权凭证W_M、随机多项式值r_M以及委托证书$Cert_{Owner}$、授权证书$Cert_{Proxy}$作为授权凭证发送至所述用户终端，以向所述用户授予使用权限

图5

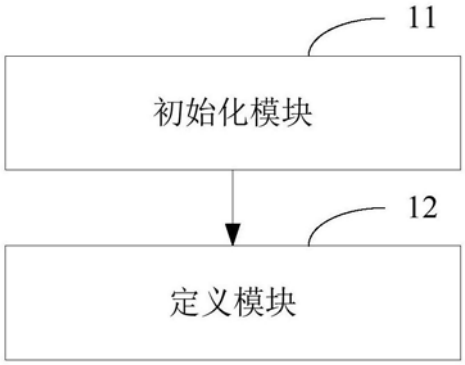

11
初始化模块
12
定义模块

图6

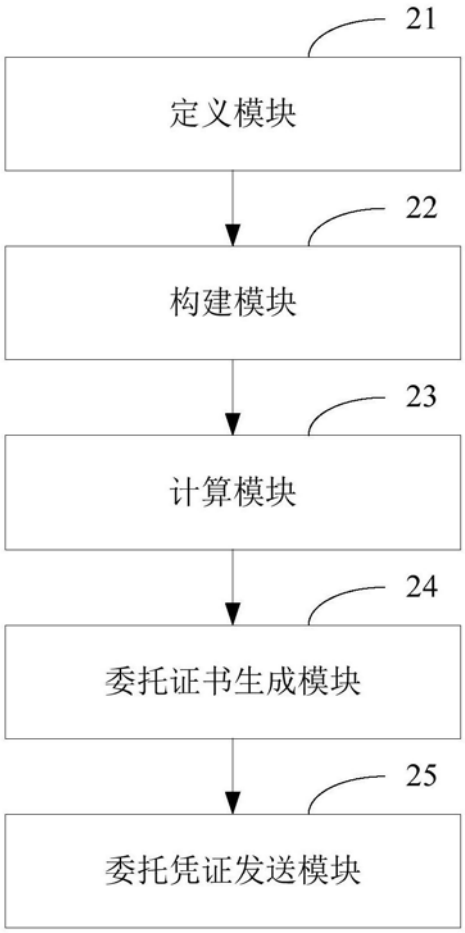


图7

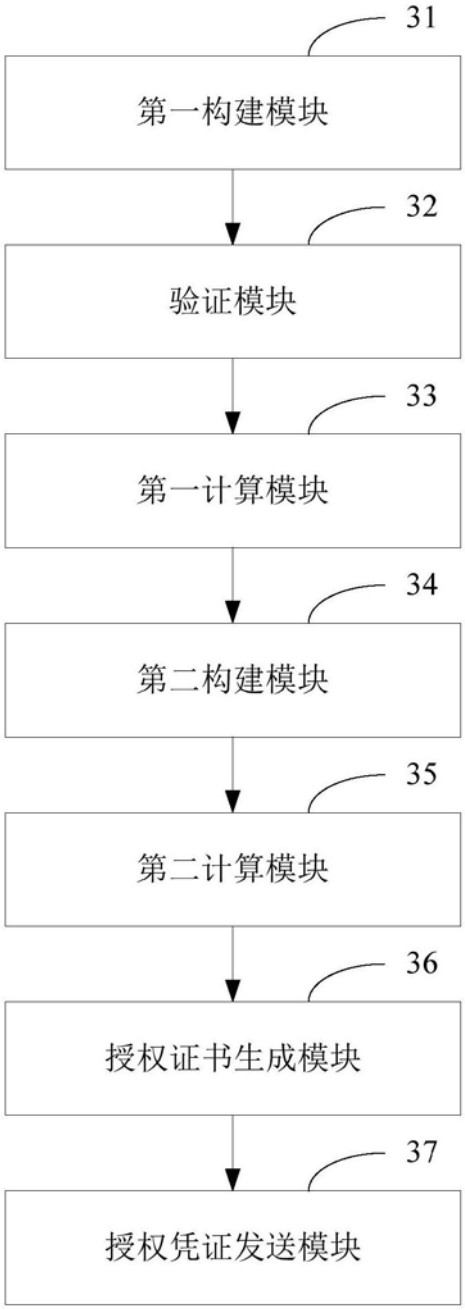

31
第一构建模块
32
验证模块
33
第一计算模块
34
第二构建模块
35
第二计算模块
36
授权证书生成模块
37
授权凭证发送模块

图8

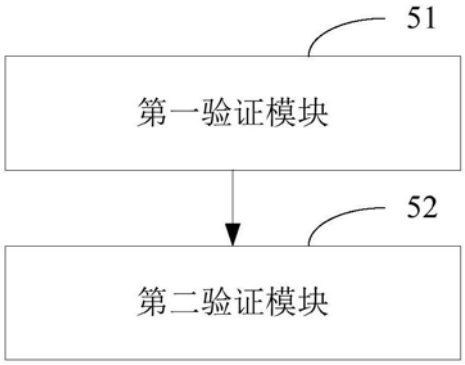


图9