(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 114363858 A
(43)申请公布日 2022.04.15

(21)申请号 202210274614.3

(22)申请日 2022.03.21

(71)申请人 苏州浪潮智能科技有限公司
地址 215100 江苏省苏州市吴中经济开发区郭巷街道官浦路1号9幢

(72)发明人 赵坤 李仁刚 赵雅倩 李茹杨 李雪雷

(74)专利代理机构 北京集佳知识产权代理有限公司 11227
代理人 柳虹

(51)Int.Cl.
H04W 4/40(2018.01)
H04W 12/041(2021.01)
H04W 60/00(2009.01)
H04L 9/32(2006.01)

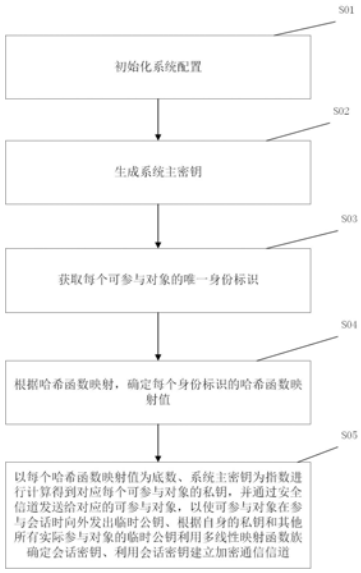
权利要求书2页 说明书7页 附图3页

(54)发明名称

蜂窝车联网协同通信的会话及注册方法、系统及相关组件

(57)摘要

本申请公开了一种蜂窝车联网协同通信的会话、注册方法、系统及相关组件，应用于密钥控制中心，该注册方法包括：初始化系统配置；生成系统主密钥；获取每个可参与对象的唯一身份标识；根据哈希函数映射，确定每个身份标识的哈希函数映射值；以每个哈希函数映射值为底数、系统主密钥为指数进行计算得到对应每个可参与对象的私钥，并通过安全信道发送给对应的可参与对象，以使可参与对象利用多线性映射函数族确定会话密钥、利用会话密钥建立加密通信信道。本申请基于多线性映射函数族的特性使得会话密钥快速计算确定，从而允许会话参与方快速更新，协同通信的自适应性高，能够满足蜂窝车联网对灵活性、及时性和可用性的高要求。



CN 114363858 A

1.一种蜂窝车联网协同通信的注册方法,其特征在于,应用于密钥控制中心,包括:

初始化系统配置;所述系统配置包括:根据每个可参与对象确定的循环群,基于每个所述循环群的生成元;映射为每个所述循环群的哈希函数映射、以所有所述可参与对象中的实际参与对象的所述生成元为原像输入的多线性映射函数族;

生成系统主密钥;

获取每个可参与对象的唯一身份标识;

根据所述哈希函数映射,确定每个所述身份标识的哈希函数映射值;

以每个所述哈希函数映射值为底数、所述系统主密钥为指数进行计算得到对应每个所述可参与对象的私钥,并通过安全信道发送给对应的所述可参与对象,以使所述可参与对象在参与会话时向外发出临时公钥、根据自身的所述私钥和其他所有实际参与对象的所述临时公钥利用所述多线性映射函数族确定会话密钥、利用所述会话密钥建立加密通信信道。

2.根据权利要求1所述注册方法,其特征在于,所述可参与对象包括:一个或多个智联汽车,和/或,一个或多个路侧单元,和/或,一个或多个云服务器。

3.根据权利要求1所述注册方法,其特征在于,所述多线性映射函数族具有以下特性:

$e_k(g,\cdots,g^a,\cdots,g)=e_k(g,\cdots,g,\cdots,g)^a$,其中$e_k$为所述多线性映射函数族,g为所述多线性映射函数族的任意原像输入,a为正整数;

非退化;

满足交换律。

4.一种蜂窝车联网协同通信的会话方法,其特征在于,应用于当前会话的任一实际参与对象,包括:

接收由权利要求1至3任一项所述蜂窝车联网协同通信的注册方法中密钥控制中心发送的私钥;

生成临时公钥并广播;

接收其他所述实际参与对象的临时公钥;

根据自身的所述私钥和其他所有所述实际参与对象的所述临时公钥,利用所述多线性映射函数族确定会话密钥;

利用所述会话密钥建立加密通信信道。

5.根据权利要求4所述会话方法,其特征在于,所述生成临时公钥并广播的过程,包括:

生成一个秘密保存于自身的临时数值;

以自身的哈希函数映射值为底数、所述临时数值为指数进行计算得到临时公钥并广播。

6.根据权利要求4所述会话方法,其特征在于,所述利用所述会话密钥建立加密通信信道后,还包括:

会话结束后,销毁所述临时公钥。

7.根据权利要求4所述会话方法,其特征在于,所述利用所述会话密钥建立加密通信信道后,还包括:

更新其他所述实际参与对象的临时公钥;

利用多线性映射函数族,根据更新的所述临时公钥更新所述会话密钥。

8.一种蜂窝车联网协同通信的注册系统,其特征在于,应用于密钥控制中心,包括:

初始化模块,用于初始化系统配置;所述系统配置包括:根据每个可参与对象确定的循环群,基于每个所述循环群的生成元;映射为每个所述循环群的哈希函数映射、以所有所述可参与对象中的实际参与对象的所述生成元为原像输入的多线性映射函数族;

密钥生成模块,用于生成系统主密钥;

接收模块,用于获取每个可参与对象的唯一身份标识;

第一计算模块,用于根据所述哈希函数映射,确定每个所述身份标识的哈希函数映射值;

第二计算模块,用于以每个所述哈希函数映射值为底数、所述系统主密钥为指数进行计算得到对应每个所述可参与对象的私钥,并通过安全信道发送给对应的所述可参与对象,以使所述可参与对象在参与会话时向外发出临时公钥、根据自身的所述私钥和其他所有实际参与对象的所述临时公钥利用所述多线性映射函数族确定会话密钥、利用所述会话密钥建立加密通信信道。

9.一种蜂窝车联网协同通信装置,其特征在于,包括:

存储器,用于存储计算机程序;

处理器,用于执行所述计算机程序时实现如权利要求1至3任一项所述蜂窝车联网协同通信的注册方法或4至7任一项所述蜂窝车联网协同通信的会话方法的步骤。

10.一种可读存储介质,其特征在于,所述可读存储介质上存储有计算机程序,所述计算机程序被处理器执行时实现如权利要求1至3任一项所述蜂窝车联网协同通信的注册方法或4至7任一项所述蜂窝车联网协同通信的会话方法的步骤。

蜂窝车联网协同通信的会话及注册方法、系统及相关组件

技术领域

[0001] 本发明涉及蜂窝车联网领域,特别涉及一种蜂窝车联网协同通信的会话及注册方法、系统及相关组件。

背景技术

[0002] 当前,蜂窝车联网(Cellular Based V2X,C-V2X)中各参与方协同合作,通过即时通信实现信息共享与应用服务,共同构建基于C-V2X的智慧交通与智慧城市。与此同时,各参与方迫切需要保护各自的隐私及数据安全,因此协同通信需要确保信道安全、内容安全和数据安全。

[0003] 对通信数据进行加密是实现多方协同安全通信的直接方法,而密钥协商是构建加密通信信道的有效技术。不同于传统具有周期性的会话密钥协商,C-V2X密钥协商需要满足车辆快速、随机移动的特点,协同安全通信要求会话密钥更新速度快,交互通信及计算频率高。进一步的,C-V2X中为提供多样化、高精度的智能服务要求提供数据的参与实体越多越好,而实际参与协同通信进行密钥协商的实体身份及个数不固定,固定参数输入的方法已不再适用,新场景要求密钥协商算法及其参数具有动态自适应互联组网的特点。因此,传统的会话密钥协商存在参与方实体数量受限、互联组网自适应性差、身份验证计算速度慢、密钥动态更新速度不及时等问题,无法适用于C-V2X这种对灵活性、即时性与可用性要求极高、身份认证与密钥协商机制交互通信次数频繁的应用场景。

[0004] 因此,如何提供一种解决上述技术问题的方案是目前本领域技术人员需要解决的问题。

发明内容

[0005] 有鉴于此,本发明的目的在于提供一种蜂窝车联网协同通信的会话及注册方法、系统及相关组件。其具体方案如下:

一种蜂窝车联网协同通信的注册方法,应用于密钥控制中心,包括:

初始化系统配置;所述系统配置包括:根据每个可参与对象确定的循环群,基于每个所述循环群的生成元;映射为每个所述循环群的哈希函数映射、以所有所述可参与对象中的实际参与对象的所述生成元为原像输入的多线性映射函数族;

生成系统主密钥;

获取每个可参与对象的唯一身份标识;

根据所述哈希函数映射,确定每个所述身份标识的哈希函数映射值;

以每个所述哈希函数映射值为底数、所述系统主密钥为指数进行计算得到对应每个所述可参与对象的私钥,并通过安全信道发送给对应的所述可参与对象,以使所述可参与对象在参与会话时向外发出临时公钥、根据自身的所述私钥和其他所有实际参与对象的所述临时公钥利用所述多线性映射函数族确定会话密钥、利用所述会话密钥建立加密通信信道。

[0006] 优选的，所述可参与对象包括：一个或多个智联汽车，和/或，一个或多个路侧单元，和/或，一个或多个云服务器。

[0007] 优选的，所述多线性映射函数族具有以下特性：

$e_k(g,\cdots,g^a,\cdots,g)=e_k(g,\cdots,g,\cdots,g)^a$，其中$e_k$为所述多线性映射函数族，g为所述多线性映射函数族的任意原像输入，a为正整数；

非退化；

满足交换律。

[0008] 相应的，本申请还公开了一种蜂窝车联网协同通信的会话方法，应用于当前会话的任一实际参与对象，包括：

接收由上文任一项所述蜂窝车联网协同通信的注册方法中密钥控制中心发送的私钥；

生成临时公钥并广播；

接收其他所述实际参与对象的临时公钥；

根据自身的所述私钥和其他所有所述实际参与对象的所述临时公钥，利用所述多线性映射函数族确定会话密钥；

利用所述会话密钥建立加密通信信道。

[0009] 优选的，所述生成临时公钥并广播的过程，包括：

生成一个秘密保存于自身的临时数值；

以自身的哈希函数映射值为底数、所述临时数值为指数进行计算得到临时公钥并广播。

[0010] 优选的，所述利用所述会话密钥建立加密通信信道后，还包括：

会话结束后，销毁所述临时公钥。

[0011] 优选的，所述利用所述会话密钥建立加密通信信道后，还包括：

更新其他所述实际参与对象的临时公钥；

利用多线性映射函数族，根据更新的所述临时公钥更新所述会话密钥。

[0012] 相应的，本申请还公开了一种蜂窝车联网协同通信的注册系统，应用于密钥控制中心，包括：

初始化模块，用于初始化系统配置；所述系统配置包括：根据每个可参与对象确定的循环群，基于每个所述循环群的生成元；映射为每个所述循环群的哈希函数映射、以所有所述可参与对象中的实际参与对象的所述生成元为原像输入的多线性映射函数族；

密钥生成模块，用于生成系统主密钥；

接收模块，用于获取每个可参与对象的唯一身份标识；

第一计算模块，用于根据所述哈希函数映射，确定每个所述身份标识的哈希函数映射值；

第二计算模块，用于以每个所述哈希函数映射值为底数、所述系统主密钥为指数进行计算得到对应每个所述可参与对象的私钥，并通过安全信道发送给对应的所述可参与对象，以使所述可参与对象在参与会话时向外发出临时公钥、根据自身的所述私钥和其他所有实际参与对象的所述临时公钥利用所述多线性映射函数族确定会话密钥、利用所述会话密钥建立加密通信信道。

[0013] 相应的，本申请还公开了一种蜂窝车联网协同通信装置，包括：

存储器，用于存储计算机程序；

处理器，用于执行所述计算机程序时实现如上文任一项所述蜂窝车联网协同通信的注册方法或上文任一项所述蜂窝车联网协同通信的会话方法的步骤。

[0014] 相应的，本申请还公开了一种可读存储介质，所述可读存储介质上存储有计算机程序，所述计算机程序被处理器执行时实现如上文任一项所述蜂窝车联网协同通信的注册方法或上文任一项所述蜂窝车联网协同通信的会话方法的步骤。

[0015] 本申请公开了一种蜂窝车联网协同通信的注册方法，应用于密钥控制中心，包括：初始化系统配置；生成系统主密钥；获取每个可参与对象的唯一身份标识；根据哈希函数映射，确定每个身份标识的哈希函数映射值；以每个哈希函数映射值为底数、系统主密钥为指数进行计算得到对应每个可参与对象的私钥，并通过安全信道发送给对应的可参与对象，以使可参与对象利用多线性映射函数族确定会话密钥、利用会话密钥建立加密通信信道。本申请基于哈希函数映射和多线性映射函数族分发私钥，进一步利用私钥确定会话密钥，多线性映射函数族的特性使得会话密钥快速计算确定，从而允许会话参与方快速更新，协同通信的自适应性高，能够满足蜂窝车联网对灵活性、及时性和可用性的高要求。

附图说明

[0016] 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，还可以根据提供的附图获得其他的附图。

[0017] 图1为本发明实施例中一种蜂窝车联网协同通信的注册方法的步骤流程图；

图2为本发明实施例中一种蜂窝车联网协同通信的会话方法的结构分布图；

图3为本发明实施例中一种蜂窝车联网协同通信的注册系统的结构分布图。

具体实施方式

[0018] 下面将结合本发明实施例中的附图，对本发明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发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都属于本发明保护的范围。

[0019] 传统的会话密钥协商存在参与方实体数量受限、互联组网自适应性差、身份验证计算速度慢、密钥动态更新速度不及时等问题，无法适用于C-V2X这种对灵活性、即时性与可用性要求极高、身份认证与密钥协商机制交互通信次数频繁的应用场景。

[0020] 本申请基于哈希函数映射和多线性映射函数族分发私钥，进一步利用私钥确定会话密钥，多线性映射函数族的特性使得会话密钥快速计算确定，从而允许会话参与方快速更新，协同通信的自适应性高，能够满足蜂窝车联网对灵活性、及时性和可用性的高要求。

[0021] 本发明实施例公开了一种蜂窝车联网协同通信的注册方法，应用于密钥控制中心，参见图1所示，包括：

S01：初始化系统配置；

其中，系统配置包括：根据每个可参与对象确定的循环群，基于每个循环群的生成元；映射为每个循环群的哈希函数映射、以所有可参与对象中的实际参与对象的生成元为原像输入的多线性映射函数族。具体的，第i个循环群G_i的生成元为g_i，也即$G_i=\langle g_i\rangle$，其中i为正整数，令$G_1=G$，$g_1=g$；进一步的，哈希函数映射可表示为H:{0,1}*àG，将任意字符串映射为循环群G的元素且满足哈希函数基本性质要求；多线性映射函数族可表示为e_k:G*G*…*GàG，其中k为不小于2的正整数，表示实际会话协商时参与对象的个数，多线性映射函数族e_k将k个循环群G中的元素作为原像输入，且在本实施例中，多线性映射函数族需要满足下面特性：

$e_k(g,\cdots,g^a,\cdots,g)=e_k(g,\cdots,g,\cdots,g)^a$，其中$e_k$为所述多线性映射函数族，g为所述多线性映射函数族的任意原像输入，a为正整数；

非退化，即g为G的生成元时，$e_k(g,\cdots,g,\cdots,g)$是G_k的生成元；

满足交换律，即k个原像输入可以任意交换位置。

[0022] 具体的，本实施例中多线性映射函数族的构造方法，包括但不限于离散对数、椭圆曲线等形式。

[0023] S02：生成系统主密钥；

具体的，密钥控制中心的密钥为系统主密钥，一般由云计算或服务器设置生成，可将该系统主密钥记为MSK=s，相应的，此时系统公钥为$PK=g^s$，该系统公钥公开，可通过公告板查询，也可利用公共信道广播，而系统主密钥由密钥控制中心秘密保存。

[0024] S03：获取每个可参与对象的唯一身份标识；

具体的，该唯一身份标识由每个可参与对象进行初始化生成，可记为ID_i，i为正整数，该唯一身份标识可作为对应的可参与对象的公钥公开，密钥控制中心收到该唯一身份标识相当于在蜂窝车联网协同通信的通信系统中进行注册。

[0025] S04：根据哈希函数映射，确定每个身份标识的哈希函数映射值；

具体的，每个身份标识ID_i对应的哈希函数映射值记为$g_{ID_i}=H(ID_i)$，i=1,2,…；

S05：以每个哈希函数映射值为底数、系统主密钥为指数进行计算得到对应每个可参与对象的私钥，并通过安全信道发送给对应的可参与对象，以使可参与对象在参与会话时向外发出临时公钥、根据自身的私钥和其他所有实际参与对象的临时公钥利用多线性映射函数族确定会话密钥、利用会话密钥建立加密通信信道。

[0026] 可以理解的是，在蜂窝车联网协同通信的通信系统中，可参与对象包括：一个或多个智联汽车，和/或，一个或多个路侧单元，和/或，一个或多个云服务器。其中，智联汽车、路侧单元、云服务器的个数均可根据实际会话需求进行设置，参与会话的可参与对象为实际参与对象，每次参与会话时必然存在两个或以上的可参与对象，例如一个智联汽车和一个路侧单元，或者三个智联汽车、两个路侧单元和一个云服务器。

[0027] 具体的，每个可参与对象的私钥可表示为$SK_{ID_i}=g_{ID_i}^{\ s}$，利用非公开的安全信道发送给对应的可参与对象，如果可参与对象参与会话，则可利用该私钥及其他数值生成会话密钥。

[0028] 具体的，任一实际参与对象可将自身的私钥和其他所有实际参与对象的临时公钥作为原像输入，利用多线性映射函数族自行确定会话密钥，假设某场会话中，共k个实际参与对象，第i个实际参与对象的会话密钥可表示为：

$K\_i=e_k(g_{ID\_1}^{r\_1},\cdots, g_{ID\_(i-1)}^{r\_(i-1)},SK_{ID\_i}, g_{ID\_(i+1)}^{r\_(i+1)},\cdots, g_{ID\_k}^{r\_k})^{r\_i}$,

$g_{ID_1}^{r_1}$为第一个实际参与对象向外发出的临时公钥,可表示为以其哈希函数映射值为底数、r_1为指数的形式,r_1可以为一个临时生成的数值,从而计算出临时公钥,也可以直接生成一个数值可以如上表示的临时公钥,r_1并非首要必须的数值。其他实际参与对象的临时公钥以此类推。

[0029] 根据上文中关于多线性映射函数族的特性,可以得到以下推论:

$K\_i=e_k(g_{ID\_1}^{r\_1},\cdots, g_{ID\_(i-1)}^{r\_(i-1)}, SK_{ID\_i}, g_{ID\_(i+1)}^{r\_(i+1)},\cdots, g_{ID\_k}^{r\_k})^{r\_i}$

$= e_k(g_{ID\_1},\cdots, g_{ID\_(i-1)}, g_{ID\_i}, g_{ID\_(i+1)},\cdots, g_{ID\_k})^{r\_1*\cdots*r\_k*s}$

因此K_1=K_2=…=K_k,即所有实际参与对象生成的会话密钥一致,从而能够构建基于对称密码算法的安全加密通信信道。

[0030] 本申请实施例公开了一种蜂窝车联网协同通信的注册方法,应用于密钥控制中心,包括:初始化系统配置;生成系统主密钥;获取每个可参与对象的唯一身份标识;根据哈希函数映射,确定每个身份标识的哈希函数映射值;以每个哈希函数映射值为底数、系统主密钥为指数进行计算得到对应每个可参与对象的私钥,并通过安全信道发送给对应的可参与对象,以使可参与对象利用多线性映射函数族确定会话密钥、利用会话密钥建立加密通信信道。本实施例基于哈希函数映射和多线性映射函数族分发私钥,进一步利用私钥确定会话密钥,多线性映射函数族的特性使得会话密钥快速计算确定,从而允许会话参与方快速更新,协同通信的自适应性高,能够满足蜂窝车联网对灵活性、及时性和可用性的高要求。

[0031] 相应的,本申请还公开了一种蜂窝车联网协同通信的会话方法,应用于当前会话的任一实际参与对象,参见图2所示,该方法包括:

S11:接收由上文任一项蜂窝车联网协同通信的注册方法中密钥控制中心发送的私钥;

S12:生成临时公钥并广播;

进一步的,步骤S12生成临时公钥并广播的过程,可以包括:

生成一个秘密保存于自身的临时数值;

以自身的哈希函数映射值为底数、临时数值为指数进行计算得到临时公钥并广播。

[0032] 对第i个实际参与对象来说,其临时数值为r_i,其临时公钥为$g_{ID_i}^{r_i}$,除了这种生成临时数值再计算临时公钥的方法,也可跳过生成临时数值的步骤直接生成一个临时公钥,只要保证该临时公钥满足可表示为指数幂的形式即可,该形式保证了所有实际参与对象的会话密钥一致。

[0033] S13:接收其他实际参与对象的临时公钥;

S14:根据自身的私钥和其他所有实际参与对象的临时公钥,利用多线性映射函数族确定会话密钥;

具体的,假设某场会话中,共k个实际参与对象,第i个实际参与对象的会话密钥可表示为:

$K\_i=e_k(g_{ID\_1}^{r\_1},\cdots, g_{ID\_(i-1)}^{r\_(i-1)},SK_{ID\_i}, g_{ID\_(i+1)}^{r\_(i+1)},\cdots, g_{ID\_k}^{r\_k})^{r\_i}$。

[0034] 由于多线性映射函数族的特性,可得出:

$K\_i=e_k(g_{ID\_1}^{r\_1},\cdots, g_{ID\_(i-1)}^{r\_(i-1)}, SK_{ID\_i}, g_{ID\_(i+1)}^{r\_(i+1)},\cdots, g_{ID\_k}^{r\_k})^{r\_i}$

$= e_k(g_{ID\_1},\cdots, g_{ID\_(i-1)}, g_{ID\_i}, g_{ID\_(i+1)},\cdots, g_{ID\_k})^{r\_1*\cdots*r\_k*s}$

因此K_1=K_2=…=K_k,即所有实际参与对象生成的会话密钥一致,从而能够构建基于对称密码算法的安全加密通信信道。

[0035] S15:利用会话密钥建立加密通信信道。

[0036] 进一步的,利用会话密钥建立加密通信信道后,还包括:

会话结束后,销毁临时公钥。

[0037] 进一步的,利用会话密钥建立加密通信信道后,还包括:

更新其他实际参与对象的临时公钥;

利用多线性映射函数族,根据更新的临时公钥更新会话密钥。

[0038] 可以理解的是,由于多线性映射函数族的特性,如果当前会话中其他实际参与对象发生了变化,不需要重新完整计算会话密钥,可在原来会话密钥的基础上,根据变化的实际参与对象的临时公钥对会话密钥进行更新,以当前会话中增加了n个实际参与对象为例,当前实际参与对象的新的会话密钥为:K'_k=e_{k+n}(K_k,…,$g_{ID\_(n-1)}$,g_{ID_n}),且K'_1=K'2=…=K'_k=…=K'_k+n,

其中K'_k为更新后的会话密钥,K_k为未更新时的原会话密钥。

[0039] 更新时不需要重新交互、认证及重复计算,大幅降低了资源和耗时。

[0040] 本实施例上文实施例中私钥控制中心根据哈希函数映射和多线性映射函数族分发的私钥,进一步利用私钥确定会话密钥,多线性映射函数族的特性使得会话密钥快速计算确定,从而允许会话参与方快速更新,协同通信的自适应性高,能够满足蜂窝车联网对灵活性、及时性和可用性的高要求。

[0041] 相应的,本申请还公开了一种蜂窝车联网协同通信的注册系统,应用于密钥控制中心,参见图3所示,包括:

初始化模块1,用于初始化系统配置;所述系统配置包括:根据每个可参与对象确定的循环群,基于每个所述循环群的生成元;映射为每个所述循环群的哈希函数映射、以所有所述可参与对象中的实际参与对象的所述生成元为原像输入的多线性映射函数族;

密钥生成模块2,用于生成系统主密钥;

接收模块3,用于获取每个可参与对象的唯一身份标识;

第一计算模块4,用于根据所述哈希函数映射,确定每个所述身份标识的哈希函数映射值;

第二计算模块5,用于以每个所述哈希函数映射值为底数、所述系统主密钥为指数进行计算得到对应每个所述可参与对象的私钥,并通过安全信道发送给对应的所述可参与对象,以使所述可参与对象在参与会话时向外发出临时公钥、根据自身的所述私钥和其他所有实际参与对象的所述临时公钥利用所述多线性映射函数族确定会话密钥、利用所述会话密钥建立加密通信信道。

[0042] 在一些具体的实施例中,所述可参与对象包括:一个或多个智联汽车,和/或,一个或多个路侧单元,和/或,一个或多个云服务器。

[0043] 在一些具体的实施例中,所述多线性映射函数族具有以下特性:

$e_k(g,\cdots,g^a,\cdots,g)=e_k(g,\cdots,g,\cdots,g)^a$,其中$e_k$为所述多线性映射函数族,g为所述多线性映射函数族的任意原像输入,a为正整数;

非退化;

满足交换律。

[0044] 本实施例基于哈希函数映射和多线性映射函数族分发私钥，进一步利用私钥确定会话密钥，多线性映射函数族的特性使得会话密钥快速计算确定，从而允许会话参与方快速更新，协同通信的自适应性高，能够满足蜂窝车联网对灵活性、及时性和可用性的高要求。

[0045] 相应的，本申请还公开了一种蜂窝车联网协同通信装置，包括：

存储器，用于存储计算机程序；

处理器，用于执行所述计算机程序时实现如上文任一项所述蜂窝车联网协同通信的注册方法或上文任一项所述蜂窝车联网协同通信的会话方法的步骤。

[0046] 相应的，本申请还公开了一种可读存储介质，所述可读存储介质上存储有计算机程序，所述计算机程序被处理器执行时实现如上文任一项所述蜂窝车联网协同通信的注册方法或上文任一项所述蜂窝车联网协同通信的会话方法的步骤。

[0047] 其中具体有关所述蜂窝车联网协同通信的注册方法或所述蜂窝车联网协同通信的会话方法的细节内容，可以参照上文实施例中的相关描述，此处不再赘述。

[0048] 其中本实施例中蜂窝车联网协同通信装置及可读存储介质，具有与上文实施例中所述蜂窝车联网协同通信的注册方法或所述蜂窝车联网协同通信的会话方法相同的技术效果，此处不再赘述。

[0049] 最后，还需要说明的是，在本文中，诸如第一和第二等之类的关系术语仅仅用来将一个实体或者操作与另一个实体或操作区分开来，而不一定要求或者暗示这些实体或操作之间存在任何这种实际的关系或者顺序。而且，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、物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、物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、物品或者设备中还存在另外的相同要素。

[0050] 以上对本发明所提供的一种蜂窝车联网协同通信的会话及注册方法、系统及相关组件进行了详细介绍，本文中应用了具体个例对本发明的原理及实施方式进行了阐述，以上实施例的说明只是用于帮助理解本发明的方法及其核心思想；同时，对于本领域的一般技术人员，依据本发明的思想，在具体实施方式及应用范围上均会有改变之处，综上所述，本说明书内容不应理解为对本发明的限制。

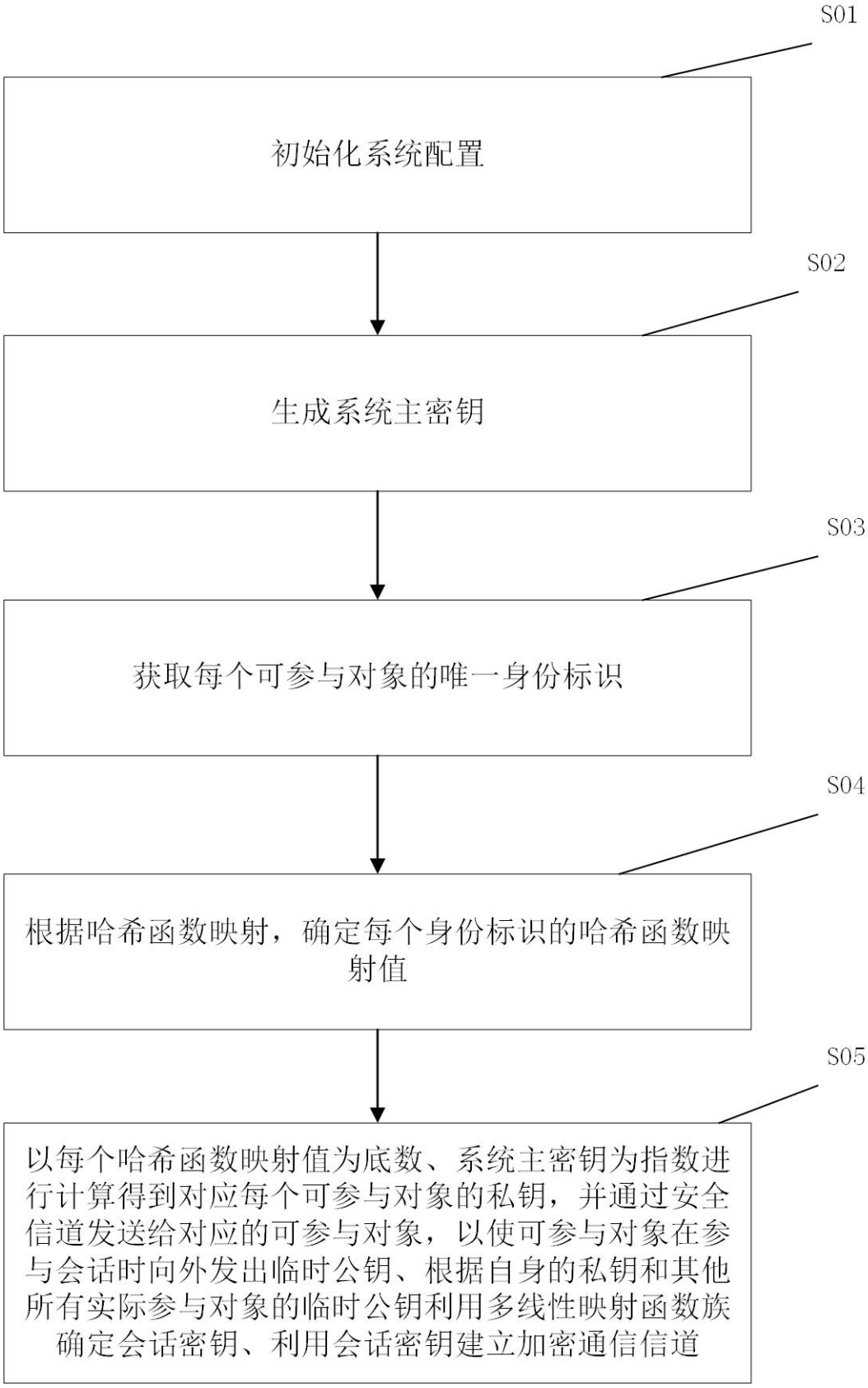

S01
初始化系统配置
S02
生成系统主密钥
S03
获取每个可参与对象的唯一身份标识
S04
根据哈希函数映射，确定每个身份标识的哈希函数映射值
S05
以每个哈希函数映射值为底数、系统主密钥为指数进行计算得到对应每个可参与对象的私钥，并通过安全信道发送给对应的可参与对象，以使可参与对象在参与会话时向外发出临时公钥、根据自身的私钥和其他所有实际参与对象的临时公钥利用多线性映射函数族确定会话密钥、利用会话密钥建立加密通信信道

图1

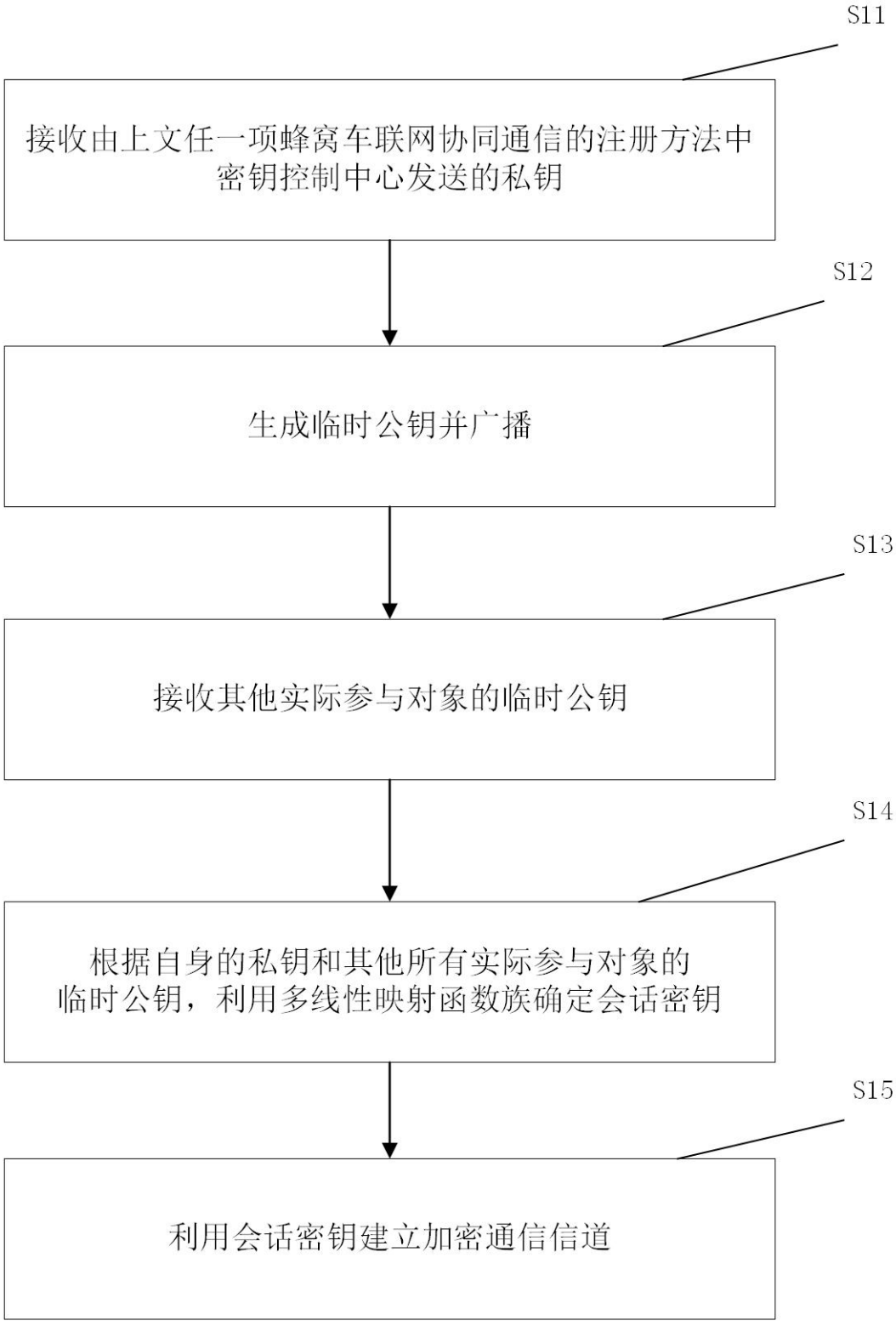

S11
接收由上文任一项蜂窝车联网协同通信的注册方法中密钥控制中心发送的私钥
S12
生成临时公钥并广播
S13
接收其他实际参与对象的临时公钥
S14
根据自身的私钥和其他所有实际参与对象的临时公钥，利用多线性映射函数族确定会话密钥
S15
利用会话密钥建立加密通信信道

图2

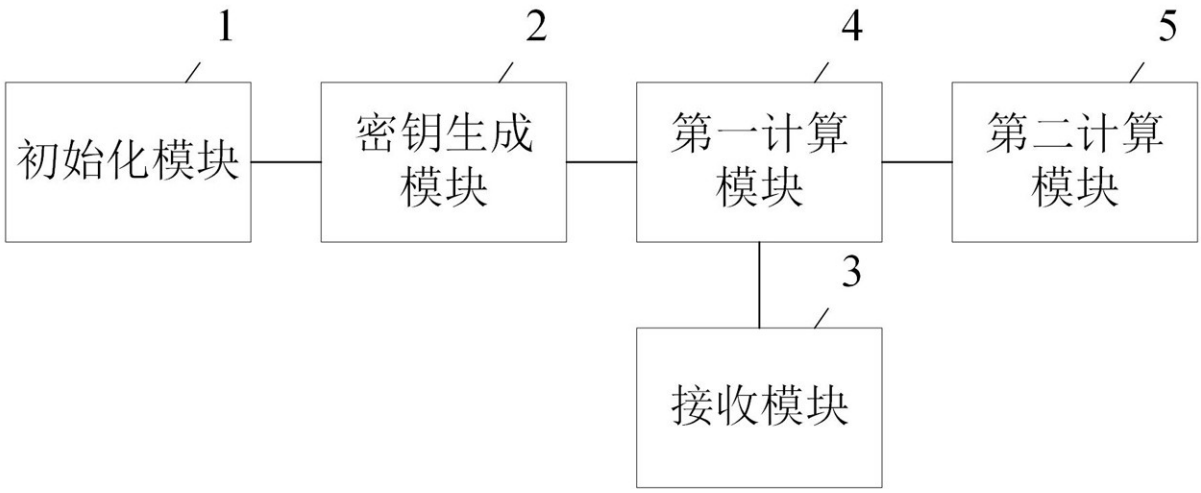


图3