(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 106549952 B
(45)授权公告日 2019.06.21

(21)申请号 201610940634.4

(22)申请日 2016.10.25

(65)同一申请的已公布的文献号
申请公布号 CN 106549952 A

(43)申请公布日 2017.03.29

(73)专利权人 中国科学院信息工程研究所
地址 100093 北京市海淀区闵庄路甲89号
专利权人 中国科学院数据与通信保护研究教育中心

(72)发明人 朱文涛 闫伸 潘适然 王平建

(74)专利代理机构 北京科迪生专利代理有限责任公司 11251
代理人 成金玉 卢纪

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 9/32(2006.01)
H04L 9/30(2006.01)

(56)对比文件
CN 102325131 A,2012.01.18,
CN 101083530 A,2007.12.05,
CN 101997688 A,2011.03.30,
CN 103647762 A,2014.03.19,
US 2014095873 A1,2014.04.03,
Jing Xu, Wen-Tao Zhu, Deng-Guo Feng.An efficient mutual authentication and key agreement protocol preserving user anonymity in mobile networks.《Computer Communications》.2011,第34卷(第3期),
Pan S., Yan S., Zhu WT.Security Analysis on Privacy-Preserving Cloud Aided Biometric Identification Schemes.《Information Security and Privacy. ACISP 2016. Lecture Notes in Computer Science》.2016,第9723卷

审查员 王一凡

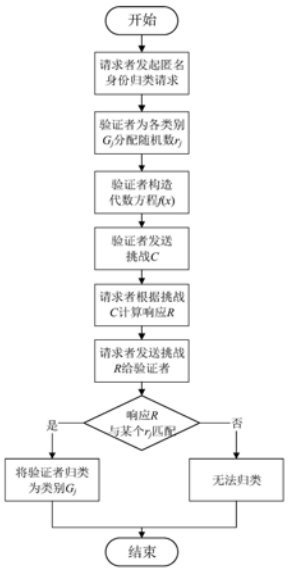
权利要求书2页 说明书4页 附图2页

(54)发明名称

一种基于代数方程的匿名身份归类识别方法

(57)摘要

本发明涉及一种基于代数方程的匿名身份归类识别方法,使得验证者无需获知用户的具体身份,就可完成对用户的身份归类;本发明基于代数方程完成对用户身份的归类,无需使用复杂的密码学方案,减小了识别过程的通信延时与计算开销,且软硬件实现的成本低;同时,本发明可灵活实现对用户类别的变更;作为一种通用框架,本发明适用于现实中的多种应用场景。



CN 106549952 B

1.一种基于代数方程的匿名身份归类识别方法,其特征在于:所述方法包括身份归类初始化过程和识别过程两部分;

一、初始化过程

各用户U_i与验证者V分别共享一个随机数k_i作为秘密信息,且U_i不应泄露k_i,i=1,2,...,n;所述各用户分别属于互不重叠的类别$G_1,G_2,...,G_m$其中的一个,且n≥m;

二、识别过程

当请求者P向验证者V发起身份归类请求时,所述请求者P可以为用户或非用户,验证者V启动识别过程如下:

(1)验证者V为类别$G_1,G_2,...,G_m$分别分配不同的新鲜随机数$r_1,r_2,...,r_m$,并选取此次识别过程的即时参数s,s为序列号或时间戳或新鲜随机数,由验证者V在每次识别过程开始时重新选取;

(2)验证者V根据每个用户U_i的秘密信息k_i与其所在类别G_j对应的r_j构造代数方程f(x),$r_j\in\{r_1,\cdots,r_m\}$,使得当输入为根据即时参数s与秘密信息k_i得到的哈希值$h(s,k_i)$时,代数方程f(x)的输出为r_j;h(•)表示单向哈希函数,$h(s,k_i)$表示以s和k_i为输入时的哈希函数值;

(3)验证者V将即时参数s与步骤(2)中得到的代数方程f(x)的各系数以适当的形式作为挑战C发送给请求者P;

(4)请求者P以即时参数s以及其持有的秘密信息k为函数输入计算哈希值h(s,k),并把它带入方程f(x)得到f(h(s,k))来作为对挑战C的响应R,然后将R发送给验证者V;当请求者P为某一用户时,k为请求者P与V在初始化过程中共享的k_i;

(5)验证者V验证其在步骤(1)中选取的随机数$r_1,\cdots,r_m$中是否存在某一个与响应R相等,若存在$r_j\in\{r_1,\cdots,r_m\}$满足R=r_j,则将请求者P归类至r_j对应的类别G_j,即将请求者归类至第j个组,输出j;否则输出0,表示无法归类,也即识别失败。

2.根据权利要求1所述的一种基于代数方程的匿名身份归类识别方法,其特征在于:所述识别过程的步骤(2)中,构造代数方程f(x)利用代数方法,所述代数方法包括拉格朗日插值法、牛顿插值法。

3.根据权利要求1所述的一种基于代数方程的匿名身份归类识别方法,其特征在于:所述识别过程的步骤(2)中,当只存在一个类别G_1时,验证者V使用代数方法构造代数方程f(x)时,应引入虚拟的类别和归属于这些类别的虚拟用户,并基于所有的真实用户和虚拟用户构造挑战;或者验证者V不采用代数方法而直接构造代数方程$f(x)=\prod_{i=1}^{n}(x-h(s,k_i))+r_1$。

4.根据权利要求1所述的一种基于代数方程的匿名身份归类识别方法,其特征在于:所述识别过程的步骤(3)中,所述以适当的形式是,当代数方程f(x)某个系数为整数时,验证者V直接发送该系数;当某个系数为分数时,验证者V以分子和分母这两个整数相结合的形式进行发送;当数学过程在整数域$\mathbb{Z}_p=\{1,\ 2,\ \ldots,\ p\text{-}1\}$中,即在模p的意义下进行,且p为素数时,验证者将分数系数转换为分母模p的乘法逆元与分子之积来发送。

5.根据权利要求1所述的一种基于代数方程的匿名身份归类识别方法,其特征在于:识别过程中,当用户数与类别数相等,即n=m时,每个类别中仅存在一个用户,验证者对用户

完成归类就可获知其确切身份，在上述情况下，匿名归类过程将为身份认证过程。

6.根据权利要求1所述的一种基于代数方程的匿名身份归类识别方法，其特征在于：识别过程中，当仅存在一个类别，即类别数m＝1时，验证者通过归类过程仅能分辨出请求者是用户或非用户，而无法获知任何更多的信息。

7.根据权利要求1所述的一种基于代数方程的匿名身份归类识别方法，其特征在于：所述方法可扩展至不同类别之间存在重叠的情况，此时，验证者只需将重叠部分单独视为一个新的类别即可。

一种基于代数方程的匿名身份归类识别方法

技术领域

[0001] 本发明涉及信息安全领域，尤其涉及一种基于代数方程的隐私保护的粗粒度身份识别方法，也即身份归类方法。

背景技术

[0002] 身份识别技术已被广泛地应用于各种系统中以确认用户身份的真实性。在典型的身份识别场景中，身份的识别方(称为验证者)需对用户的具体身份进行识别。然而，在很多实际应用场景(如门禁系统)中，验证者无需知道用户的具体身份，只需判断出用户所属的类别或群组即可。

发明内容

[0003] 本发明技术解决问题：克服现有技术的不足，提供一种基于代数方程的匿名身份归类识别方法，同时保证用户身份信息的匿名性和识别方案的简洁性。

[0004] 本发明主要涉及验证者与用户两类实体，它们构成本发明所涉及的身份归类系统。其中，验证者为诚实但可能好奇的，即验证者严格遵守规定的协议流程工作，但同时有可能试图去获知用户的具体身份。向验证者发起匿名的身份归类请求的实体可能为用户或非用户，统一将发起该请求的实体称为请求者。本发明旨在实现验证者对匿名请求者的正确归类，并同时保证用户的具体身份不被验证者与可能存在的外部窃听者获知；所述“正确归类”是指将用户归类到所属类别，并识别出非用户。

[0005] 本发明采用的技术方案如下：

[0006] 所使用的符号统一约定如下。$h(\cdot)$为抗碰撞的单向哈希函数(其特点是输入长度任意但输出长度固定，在实际计算中不能从输出值反推出输入，且在有限时间内找到哈希值相等的两个不同输入值不可行)。身份归类系统中验证者为V。身份归类系统中有n个用户$U_1,U_2,\ldots,U_n$，他们来自于m个互不重叠的类别$G_1,G_2,\ldots,G_m$，且$n\geq m$。

[0007] 如图1所示，本发明一种基于代数方程的匿名身份归类识别方法，包括初始化和识别过程两部分。

[0008] 实现步骤如下：

[0009] 一、初始化过程

[0010] 各用户U_i与验证者V分别共享一个随机数k_i作为秘密信息，且U_i不应泄露k_i。

[0011] 二、识别过程

[0012] 如图2所示，当请求者P向身份归类系统发起匿名的身份归类请求时，验证者V启动识别过程。

[0013] (1)验证者V为身份归类系统中的类别$G_1,G_2,\ldots,G_m$分别分配不同的新鲜随机数$r_1,r_2,\ldots,r_m$，并选取此次识别过程的即时参数s。s可为序列号、时间戳、新鲜随机数等，由验证者V在每次识别过程开始时重新选取。

[0014] (2)验证者V根据每个用户U_i的秘密信息k_i与该用户所在类别对应的随机数r_j构造

代数方程f(x)，使得当输入为h(s,k_i)时，f(x)的输出为r_j；这里$r_j \in \{r_1,\cdots,r_m\}$，h(•)表示单向哈希函数，h(s,$k_i$)表示以s和$k_i$为输入时的哈希函数值。

[0015] (3)验证者V将即时参数s与步骤(2)中得到的f(x)的各系数以适当的形式作为挑战C发送给请求者P。

[0016] (4)请求者P以即时参数s以及其持有的秘密信息k为函数输入计算h(s,k)，并将f(h(s,k))作为对挑战C的响应R发送给验证者V。

[0017] (5)验证者V验证其在步骤(1)中选取的随机数$r_1,\cdots,r_m$中是否存在某一个与响应R相等，若存在$r_j \in \{r_1,\cdots,r_m\}$满足$R=r_j$，则将请求者P归类至$r_j$对应的类别$G_j$，即将请求者归类至第j个组，输出j；否则输出0，表示无法归类，也即识别失败。

[0018] 另外，针对上述各步骤还有进一步的限定如下：

[0019] 为降低计算开销，所有数学过程(如随机数的选取、代数方程的构造过程等)可在整数域$\mathbb{Z}_p=\{1,\ 2,\ \ldots,\ p-1\}$中(即在模p的意义下)进行，其中p建议选取结构合理且充分大的素数。

[0020] 所述识别过程步骤(2)中，验证者V根据h(s,k_i)和r_j，利用代数方法(如拉格朗日插值法、牛顿插值法等)构造方程f(x)。特别地，当系统中只存在一个类别G_1时，验证者V使用代数方法构造代数方程时，应引入虚拟的类别和归属于这些类别的虚拟用户，并基于所有的真实用户和虚拟用户构造f(x)；或者验证者V不采用代数方法而直接构造代数方程$f(x)=\prod_{i=1}^{n}(x-h(s,k_i))+r_1$。

[0021] 所述识别过程步骤(3)中，验证者将代数方程的各系数以适当的形式发送给请求者。其“以适当的形式”是为了保证代数方程的运算结果的准确性。例如，当代数方程f(x)某个系数为整数时，验证者直接发送该系数；当某个系数为分数时，验证者以分子和分母这两个整数相结合的形式进行发送。特别地，当所有数学过程在模p意义下进行且p为素数时，验证者可以将分数系数转换为分母模p的乘法逆元与分子之积来发送。

[0022] 所述识别过程步骤(4)中，当请求者为身份归类系统中某一用户时，k为请求者与验证者V共享的k_i。

[0023] 进一步的，当身份归类系统中用户数与类别数相等，即n＝m时，每个类别中仅存在一个用户，验证者对用户完成归类就可获知其确切身份。在上述情况下，本发明中的匿名归类过程将完全退化为身份认证过程。

[0024] 进一步的，当身份归类系统中仅存在一个类别，即m＝1时，验证者通过归类过程仅能分辨出请求者是用户或非用户，而无法获知任何更多的信息。

[0025] 进一步的，本发明可扩展至不同类别之间存在重叠的身份归类系统中，此时，验证者只需将重叠部分单独视为一个新的类别即可。例如，当某个身份归类识系统包含两个类别G_1和G_2，且$G_1 \cap G_2$不为空集时，验证者只需将$G_1 \cap G_2$单独提升为一个新的类别即可。

[0026] 与现有技术相比，本发明的有益效果为：

[0027] (1)本发明提出了一种粗粒度的身份识别方法，使得验证者无需获知用户的确切身份就可正确判断用户所属的类别，简单易行。

[0028] (2)本发明基于简单的挑战与响应，简化了识别过程，降低了用户与验证者之间的通信延时。

[0029] (3)本发明提出的方法基于代数方程实现，识别过程只涉及基本的数学运算，如$\mathbb{Z}_p$域中的加减乘除，便于软硬件实现。特别地，当p为结构合理的素数时，识别过程仅涉及模p意义下的加法与乘法运算，并能加速对模p的计算，可进一步降低用户侧的实现难度。

[0030] (4)本发明提出的方法支持用户所属类别的变更，当身份归类系统中某一用户对应的类别发生变化时，验证者仅需在构建代数方程时使用新类别对应的随机数进行计算；特别地，当系统需排除某一用户时，验证者仅需在识别过程中，不使用该用户的秘密信息构建代数方程即可，保证用户身份信息的匿名性。

[0031] (5)本发明适用于现实中的多种应用场景。

附图说明

[0032] 图1为本发明方法实现流程图；

[0033] 图2为本发明基于代数方程的匿名身份归类识别方法示意图。

[0034] 图3为本发明中基于拉格朗日插值法构造代数方程的身份归类方法示意图。

具体实施方式

[0035] 为了使本发明的目的、技术方案和优点更加清晰明白，以下将结合具体实施例，并参照附图对本发明做详细的说明。

[0036] 本实施例以具有5个用户U_1，…，U_5以及2个互不重叠的类别G_1和G_2的身份归类系统为例对匿名身份归类识别的过程进行具体说明，其中，U_1、U_2、U_3属于G_1，U_4、U_5属于G_2，验证者使用拉格朗日插值法构造代数方程f(x)。具体实现步骤为：

[0037] 一、系统初始化过程

[0038] 用户U_1，…，U_5分别与验证者共享秘密信息k_1，…，$k_5\in\mathbb{Z}_p$，其中p为足够大的素数。

[0039] 二、识别过程

[0040] 如图3所示，当用户U_2作为请求者P向系统提交身份归类请求时，验证者V启动识别过程。

[0041] (1)验证者V分别给G_1和G_2分配不同的新鲜随机数r_1，$r_2\in\mathbb{Z}_p$，并选取新鲜随机数s作为即时参数。

[0042] (2)验证者V构造代数方程f(x)，使得$f(h(s,k_1))=f(h(s,k_2))=f(h(s,k_3))=r_1$，$f(h(s,k_4))=f(h(s,k_5))=r_2$。根据拉格朗日插值法，$f(x)=r_1(l(1)+l(2)+l(3))+r_2(l(4)+l(5))$，其中$l(i)=\prod_{t=1,t\neq i}^{5}\frac{x-h(s,k_t)}{h(s,k_i)-h(s,k_t)}$。随后，验证者V将f(x) mod p以$a_0+a_1x+a_2x^2+a_3x^3+a_4x^4$的形式表示，其中mod表示取模运算。

[0043] (3)验证者V以适当的形式发送s和系数a_0，a_1，a_2，a_3，a_4作为给请求者P的挑战C。

[0044] (4)请求者P将$h(s,k_2)$代入$a_0+a_1x+a_2x^2+a_3x^3+a_4x^4$，并将计算结果对p取模后作为对挑战C的响应R发送给验证者V。

[0045] (5)验证者V收到来自请求者P的响应R后，将R与r_1、r_2比较。在本例中$R=r_1$，则请求者V将请求者P归类为第1个类别G_1，并输出1作为识别结果。

[0046] 综上所述，本发明提出的一种基于代数方程进行匿名身份归类识别的方法，使得验证者无需获知用户的具体身份，就可完成对用户的身份归类。本发明基于代数方程完成对用户身份的归类，无需使用复杂的密码学方案，减小了识别过程的通信延时与计算开销，且软硬件实现的成本低。同时，本发明可灵活实现对用户类别的变更。

[0047] 以上所述实施例仅为更好的说明本发明的目的、技术方案和有益效果。所应理解的是，以上所述仅为本发明的具体实施例而已，并不用于限制本发明，凡在本发明的精神和原则之内所做的任何修改、等同替换、改进等，均应包含在本发明的保护范围之内。

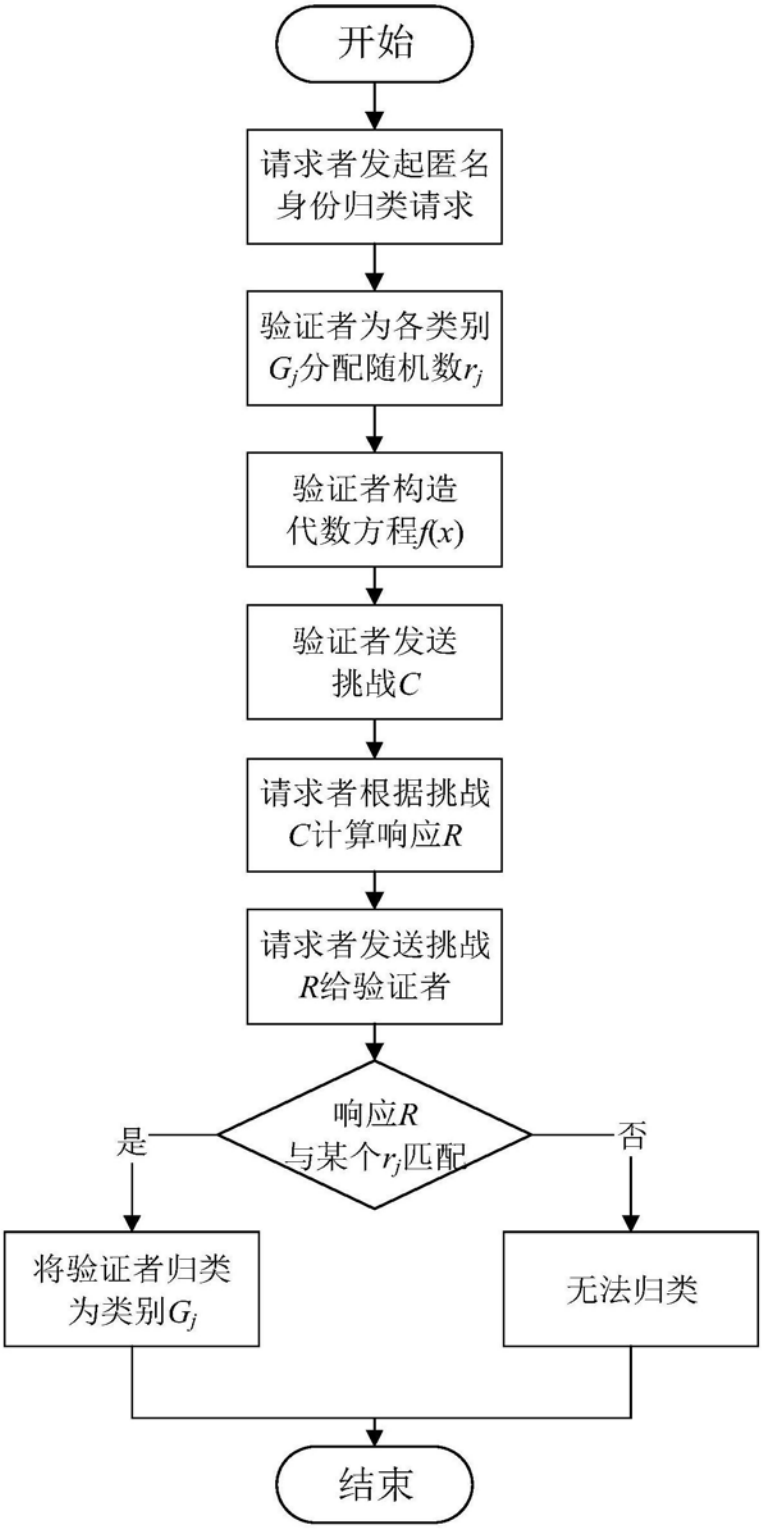

开始
请求者发起匿名身份归类请求
验证者为各类别G_j分配随机数r_j
验证者构造代数方程$f(x)$
验证者发送挑战C
请求者根据挑战C计算响应R
请求者发送挑战R给验证者
响应R与某个r_j匹配
是
否
将验证者归类为类别G_j
无法归类
结束

图1

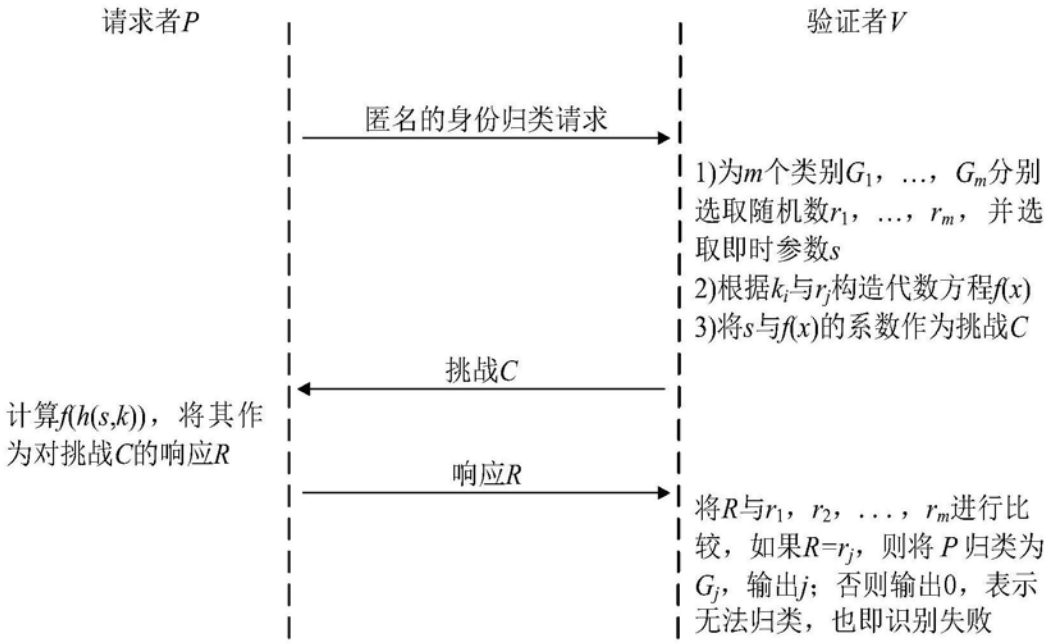

请求者P
验证者V
匿名的身份归类请求
1)为m个类别G_1，…，G_m分别选取随机数r_1，…，r_m，并选取即时参数s
2)根据k_i与r_j构造代数方程f(x)
3)将s与f(x)的系数作为挑战C
挑战C
计算f(h(s,k))，将其作为对挑战C的响应R
响应R
将R与r_1，r_2，...，r_m进行比较，如果$R=r_j$，则将P归类为G_j，输出j；否则输出0，表示无法归类，也即识别失败

图2

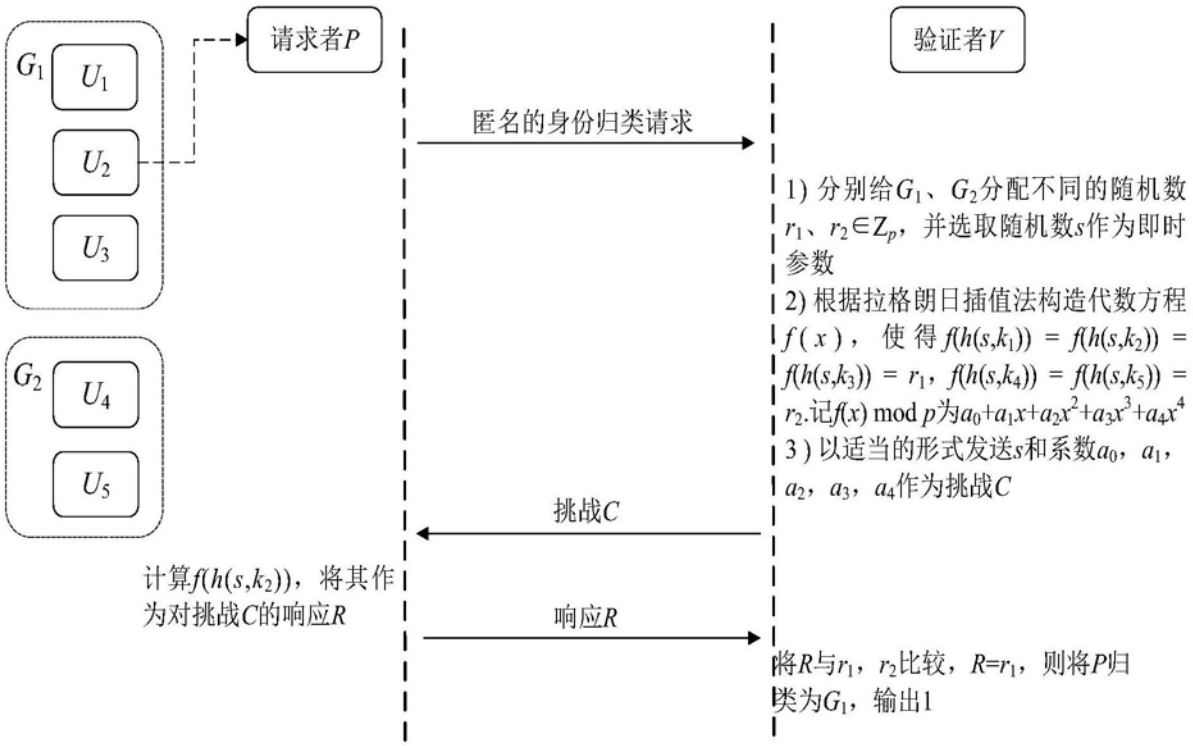

G_1
U_1
U_2
U_3
G_2
U_4
U_5
请求者P
验证者V
匿名的身份归类请求
1) 分别给G_1、G_2分配不同的随机数r_1、$r_2 \in Z_p$，并选取随机数s作为即时参数
2) 根据拉格朗日插值法构造代数方程f(x)，使得$f(h(s,k_1)) = f(h(s,k_2)) = f(h(s,k_3)) = r_1$，$f(h(s,k_4)) = f(h(s,k_5)) = r_2$.记f(x) mod p为$a_0+a_1x+a_2x^2+a_3x^3+a_4x^4$
3) 以适当的形式发送s和系数a_0，a_1，a_2，a_3，a_4作为挑战C
挑战C
计算$f(h(s,k_2))$，将其作为对挑战C的响应R
响应R
将R与r_1，r_2比较，$R=r_1$，则将P归类为G_1，输出1

图3