DOI:10.11830/ISSN.1000-5013.202202009

层次匿名群签名的概念与构建

程小刚[1],郭韧[2],周长利[1],陈永红[1],卢正添[1]

(1. 华侨大学 计算机科学与技术学院,福建 厦门 361021;
2. 华侨大学 工商管理学院,福建 泉州 362021)

摘要: 针对现有群签名的匿名范围不可变且应用上有一定局限性的问题,提出一种层次匿名群签名的概念.将成员所在的单位组织成层次架构,在生成群签名时根据具体的应用自主选择匿名层次,从而灵活适应不同匿名级别的需求.基于多变量多项式、RSA 假设和知识签名等方法,构建一个高效的层次匿名群签名方案,将层次组织架构与作为密匙的多项式的解空间对应起来.

关键词: 群签名;层次匿名;知识签名;模多项式;RSA 假设

中图分类号: TN 918.4 **文献标志码:** A **文章编号:** 1000-5013(2022)06-0819-06

Concept and Construction of Group Signature With Hierarchy Anonymity

CHENG Xiaogang[1], GUO Ren[2], ZHOU Changli[1],
CHEN Yonghong[1], LU Zhengtian[1]

(1. College of Computer Science and Technology, Huaqiao University, Xiamen 361021, China;
2. College of Business Administration, Huaqiao University, Quanzhou 362021, China)

Abstract: Aiming at the problem that the anonymous range of the existing group signature is immutable and there are some limitations in application, a concept of group signature with hierarchical anonymous is proposed. The unit of members is organized into a hierarchical structure, when generating the group signature, the anonymous level is selected independently according to the specific application, so as to flexibly meet the needs of different anonymous levels. Based on multivariable polynomial, RSA assumption and knowledge signature methods, an efficient hierarchical anonymous group signature scheme is constructed, which corresponds the hierarchical organization structure to the solution space of the polynomial as the key.

Keywords: group signature; hierarchical anonymity; knowledge signature; modular polynomial; RSA assumption

群签名是一种具有中心地位的密码系统[1-2],具有匿名和可追踪的良好特性,在电子投票[3-4]、电子货币[5-6]、电子拍卖[7-8]、可信计算[9-10]、车载互联网[11-13]和隐私保护[14]等领域应用广泛[15-16].群签名的概念是 1991 年由 Chaum 和 Heyst 提出的[1].1997 年,Camenisch 等[17]提出的 CS97 群签名方案,在群签名构建上具有十分重要的意义,其实现群公钥及签名的长度、签名和验证的计算复杂度都独立于群的大小,但其安全性基于随机预言模型(ROM).在标准模型下构建的群签名一般是利用两种签名方案,给群

收稿日期: 2022-02-17

通信作者: 程小刚(1973-),男,讲师,博士,主要从事应用密码学、量子信息技术的研究.E-mail:cxg@hqu.edu.cn.

基金项目: 国家自然科学基金青年科学基金资助项目(61802134);福建省社会科学规划资助项目(FJ2021B163,FJ2020B044);福建省泉州市社会科学规划项目(2021D04);华侨大学中青年教师科技创新资助计划项目(ZQN-811)

成员的证书为群管理员(GM)的签名,群成员利用此证书再生成群签名.GS08中提出的在标准模型下安全的、基于双线性群的高效非交互零知识证明方案,是第1种可对一大类关系进行零知识证明的方案.因此,GS08被广泛用于各种标准模型下安全群签名方案的构建[15].

把单位组织成层次结构的密码系统有一些相关工作,如基于身份的层次加密(HIBE)[18-20].由于基于身份的加密(IBE)系统中所有用户的私钥都由某个中心生成,负担较重,HIBE系统可由上层单位把下层单位的密匙生成工作委托给下层组织,如身份公钥 Alice.hqu.edu.cn 对应的私钥原来由中心生成,而在HIBE系统中此工作可由中心委托华侨大学来生成(即 hqu.edu.cn 负责生成所有 *.hqu.edu.cn 的私钥),而华侨大学的私钥又可由教育部门来生成(即 edu.cn 负责生成所有 *.edu.cn 的私钥),从而极大地降低了中心的负担.文献[21]中提出层次撤销群签名的概念,即在撤销时利用组织的层次结构进行灵活的撤销.层次群签名[22-23]可应用于匿名信用卡,在打开签名时,有多个被组织成层次结构的GM,签名者是树的叶子节点,GM可以打开签名,但每个GM只能打开本层.

传统群签名的匿名性只在本群内是匿名的,其匿名范围是不可变的.实现自主匿名群签名的简单做法是组织树中的每个单位生成自己的群签名方案,群成员向每个单位申请加入并获得相应的私钥,这样的缺点是没有实现单位的层次关系的限制.因此,本文提出一种匿名性可变的层次匿名群签名的概念,将成员所在的单位组织成层次架构,这样在生成群签名时可根据具体的应用自主选择匿名层次,这与层次撤销群签名在某种程度上是一种对偶关系;构建的方案能强制实现单位间的层次关系,即不属于本单位的成员不能加入与生成群签名.

1 初步知识

定义1 层次匿名群签名由下列5个概率多项式算法构成.

1) 设置(Setup).GM将部门内所在单位组织成层次结构,叶子节点是人,即群成员,并生成层次结构中各单位的群公钥(GPK)和负责成员加入的群私钥(GSK).

2) 加入(Join).成员申请加入群,GM在核实其身份信息之后,可利用GSK生成其成员私钥(MSK),用于生成群签名.

3) 签名(Sign).生成群签名时,成员可选择其匿名层次,即在从根到其叶子节点路径上任选一个单位,对应其群公钥,利用其MSK生成相应的群签名.

4) 验证(Verify).验证时,验证方能验证群签名的合法性(根据签名中包含的单位信息),但不清楚是此群中哪个成员生成的签名.

5) 打开(Open).当出现争议时,GM可打开签名找出真正的签名者.

由上述定义可见,与普通的群签名相比,层次匿名群签名在签名时,位于叶子节点的成员可选择匿名级别,即可选择从根到其自身路径上的任一个单位作为匿名范围,上层单位代表匿名性较高(即把自己隐藏在更大的组中),而下层单位匿名性较低(即其所在单位成员较少).这样一个层次匿名群签名密码系统就可适应多种不同的需求.

知识签名是对消息 m 的签名,对拥有某个知识(如离散对数、大整数因子分解等)的非交互式零知识证明,通常表示为

$$\mathrm{SPK}\{x:x\text{ 是某个难题的解}\}(m).$$

上式中:m 是签名的消息;x 是签名方拥有的秘密知识(即签名私钥).

而数学难题是签名方案对应的公钥,如著名的基于离散对数和ROM模型的Schnorr签名方案,公钥为$\{g,h,p\}$,私钥为 x,满足关系 $h=g^x \bmod p$,其签名就是

$$\mathrm{SPK}\{x:h=g^x \bmod p\}(m).$$

构造为

$$(R,s)=\{g^r \bmod p, r+H(m\|R\|h)\times x\}.$$

上式中:r 为随机数;H 为ROM的哈希函数;$R=g^r \bmod p$.

验证方程为

$$g^s=R\times h^{H(m\|R\|h)}.$$

定义 2　可追踪性安全定义模型. 博弈游戏定义敌手为 A，挑战者为 C，即

1) C 作为群管理员 GM，生成层次群签名各单位的 GPK 和 GSK，并把 GPK 发给敌手 A；

2) 利用 GPK，A 可以向 GM 申请加入群成为群成员，并得到成员私钥 MSK；A 也可以申请得到对某个消息 m 的群签名 S_m；A 还可以要求得到某个群成员的私钥 MSK；

3) A 输出一个消息和签名对(m,S_m)，如果签名合法，且 A 未要求查询得到过 m 的群签名，且签名不能被 GM 追踪为 A 已经查询过或攻破过的群成员，则称 A 赢得胜利.

可追踪性安全指没有多项式时间的敌手 A 能以高概率赢得上述博弈游戏.

2　层次匿名群签名的构建

2.1　构建方法

1) 设置(Setup). 最上层群公钥为 1 个随机多项式(变量个数对应层次结构高度)，即

$$ax^i+by^j+cz^k+dw^l+ev^s+fu^t+g=0 \bmod N.$$

上式中：$a,b,c,d,e,f,g\in\mathbf{Z}_N^*$ 为多项式系数，是随机常数；i,j,k,l,s,t 为每项次数，是随机常数；x,y,z,w,v,u 为变量；N 为一安全的 RSA 模数，即 N 为 2 个大素数 p 和 q 之积，(p,q)为打开签名的私钥.

而下面每层的单位又有 1 个公钥多项式，变量个数逐渐减少，每个最小的组公钥是 1 个有 2 个变量的随机多项式，即

$$a_{n-1}x^{i_{n-1}}+b_{n-1}y^{j_{n-1}}+c_{n-1}=0 \bmod N.$$

假定树的高度为 n，类似地，倒数第 2 层组织的公钥是 1 个有 3 个变量的随机多项式，即

$$a_{n-2}x^{i_{n-2}}+b_{n-2}y^{j_{n-2}}+c_{n-2}z^{k_{n-2}}+d_{n-2}=0 \bmod N.$$

另外，要求生成这些随机多项式时，从根到叶子节点上的路径上所有公钥多项式中同一个变量的指数是互素的(主要是为了增强匿名性，使上、下层单位之间的群签名不可链接).

2) 加入(Join). 当某个成员要加入时，从最底层开始，随机选择 1 个 x_r，那么，GM 利用持有的私钥(即 N 的因子分解 p 和 q)，可解出对应的 y_r 满足

$$a_{n-1}x_r^{i_{n-1}}+b_{n-1}y_r^{j_{n-1}}+c_{n-1}=0 \bmod N.$$

把(x_r,y_r)代入上一层方程，GM 又可以解出 z_r，满足

$$a_{n-2}x_r^{i_{n-2}}+b_{n-2}y_r^{j_{n-2}}+c_{n-1}z_r^{k_{n-2}}+d_{n-2}=0 \bmod N.$$

mod 依次往上，直到最高层得到用户的全部私钥$(x_r,y_r,z_r,w_r,v_r,u_r)$，满足

$$ax_r^i+by_r^j+cz_r^k+dw_r^l+ev_r^s+fu_r^t+g=0 \bmod N.$$

3) 签名(Sign). 最高层公钥多项式对应的线性化方程为

$$aX+bY+cZ+dW+eV+fU+g=0 \bmod N.$$

上式中：$X=x^i;Y=y^j;Z=z^k;W=w^l;V=v^s;U=u^t \bmod N$.

签名时，签名者公布其 X_m,Y_m,Z_m,W_m,V_m,U_m，这些公开信息要满足上述的线性化方程，即

$$aX_m+bY_m+cZ_m+dW_m+eV_m+fU_m+e=0 \bmod N.$$

然后，零知识证明其拥有相应的私钥，即知识签名表示为

$$\mathrm{SPK}\{x,y,z,w,v,u:X_m=x^i,Y_m=y^j,Z_m=z^k,W_m=w^l,V_m=v^s,U_m=u^t \bmod N\}(m).$$

类似地，签名的叶子节点用户可选择从根到其路径上的任一节点单位的公钥多项式，来生成相应的签名，即层次匿名群签名.

证明 $\mathrm{SPK}\{x:X_m=x^i\}(m)$可高效实现如下：对消息 m 的知识签名为(t,T)，其中，$t=x^{H(m)}r \bmod N$，r 为随机数，$T=r^i \bmod N$；验证签名就是验证方程 $t^i=X^{H(m)}T \bmod N$ 是否成立.

4) 验证(Verify). 由上述可知，签名就是针对某个公钥多项式的知识签名 SPK，所以，验证就是验证 SPK 是否成立. 由于 SPK 的零知识特性，验证方只能知道公开的信息$\{X_m,Y_m,Z_m,W_m,V_m,U_m\}$，但不知道具体是哪个成员签署的.

5) 打开(Open). 若后期有争议发生，GM 利用成员加入时保存的相关信息，根据$\{X_m,Y_m,Z_m,W_m,V_m,U_m\}$可以很容易追踪出是哪个成员所做的群签名. 因此，GM 可利用 GSK$=(p,q)$计算出 X_m 对应的

成员私钥 x_m,从而在自己的数据库中查找此私钥是分配给哪个用户的.

2.2 一个简单的例子

以简单的二层组织架构为例(更多的层次只需增加变量的个数即可),最上层有3个变量的随机公钥多项式为

$$f_1(x,y,z)=x^5+245y^{11}+137z^7+92=0 \bmod 323(17\times 19).$$

设第2层有2个单位,那么,各自可选1个2个变量的随机多项式作为公钥,如

$$f_{21}(x,y)=x^7+135y^7+31=0 \bmod 323,$$

$$f_{22}(x,y)=x^{11}+231y^5+27=0 \bmod 323.$$

对于组织1,GM可根据以下步骤生成成员私钥:随机取 $x=3$,由 f_{21} 解出 $y=202$,再把($x=3$,$y=202$)代入 f_1,解出 $z=39$,容易验证

$$f_1(3,202,39)=3^5+245\times 202^{11}+137\times 39^7+92=0 \bmod 323,$$

$$f_{21}(3,202)=3^7+135\times 202^7+31=0 \bmod 323,$$

即此成员的私钥为MSK=(3,202,39).GM可将此MSK发给成员,并在自己的数据库中保存此MSK和对应成员的身份信息,用于以后打开签名.利用此MSK,成员可以生成群签名.签名时,若此成员想实现最大匿名性,那么,可以利用MSK=(3,202,39)和最高层的公钥多项式

$$f_1(x,y,z)=x^5+245y^{11}+137z^7+92=0 \bmod 323,$$

按以下方式进行签名.先计算

$$X_m=3^5 \bmod 323=243,\quad Y_m=202^{11} \bmod 323=179,\quad Z_m=39^7 \bmod 323=248,$$

并把(X_m,Y_m,Z_m)作为签名的一部分;然后,针对要签名的消息 m,再生成知识签名,即

$$\mathrm{SPK}\{(x,y,z):X_m=x^5,Y_m=y^{11},Z_m=z^7\}(m).$$

最终的群签名为

$$(X_m,Y_m,Z_m,\mathrm{SPK}).$$

验证签名时,验证方要先验证(X_m,Y_m,Z_m)是否满足线性化的公钥多项式方程,即 $X_m+245Y_m+137Z_m+92=0 \bmod 323$ 是否成立,这里显然

$$243+245\times 179+137\times 248+92=78\ 166=242\times 323=0 \bmod 323$$

成立.如果不成立,则拒绝签名;如果成立,再继续验证上述知识签名是否合法.

若此成员想生成一个以其所在的组织1为匿名范围的群签名,那么,可以利用MSK中的(3,202),先计算

$$X_m=3^7=249 \bmod 323,\quad Y_m=202^7=297 \bmod 323.$$

然后,生成知识签名

$$\mathrm{SPK}\{(x,y):X_m=x^7,Y_m=y^7\}(m).$$

验证时,验证方要先验证(X_m,Y_m)是否满足线性化的 f_{21},即 $X_m+135Y_m+31=0 \bmod 323$ 是否成立,这里显然

$$249+135\times 297+31=40\ 375=125\times 323=0 \bmod 323$$

成立.若成立,再验证知识签名是否合法.

打开签名时,对于上述的第1种签名,GM只要利用GSK=(p,q)进行求解,即 $X_m^{1/5}$,$Y_m^{1/11}$,$Z_m^{1/7}$,从而得到该成员的私钥(3,202,39),查找自己的数据库,实现追踪.类似地,对于上述的第2种签名,GM可计算 $X_m^{1/7}$,$Y_m^{1/7}$,从而得到(3,202),也可以通过查找数据库追踪出具体的签名成员方.

3 安全性分析与证明

定理1 基于RSA假设,上述层次匿名群签名时是可追踪的.

证明:挑战者C作为GM生成GPK(即一随机多项式和RSA模数 N,变量个数等于组织层次架构高度),GSK满足 $N=pq$,并将GPK发给敌手A进行如下游戏.

1) A可以申请加入群,此时,C只要利用自己的群私钥GSK生成成员私钥(即对应于公钥多项式

的解）发送给 A 即可.

2）A 要求获得对某个消息相对某个群组的群签名，此时，C 可以利用自己的群私钥 GSK 生成相应群组中某个成员私钥；然后，利用此私钥生成相应的层次群签名（即上述知识签名）即可.

3）A 要求获得某个群成员的私钥，此时，C 利用保存在数据库中该成员的相关信息查找或生成其私钥；然后，发送给 A 即可.

4）最后，如果 A 能够生成 1 个合法的群签名，而 GM 不能追踪到该签名的签名方（即 A 没有查询过此消息此单位的群签名，且 A 没有从 C 获得过本次签名中所用的成员私钥），则称 A 赢得此次游戏. 如果 A 能以不可忽略的概率赢得游戏，那么，证明利用 A 可以攻破 RSA 假设，即 A 能够造出成员私钥 (x', y')，满足群公钥多项式

$$ax'^{i}+by'^{j}+c=0 \bmod N.$$

首先，找到 (X', Y')，满足

$$aX'+bY'+c=0 \bmod N$$

是简单的，随机选择 1 个 X'，可解此线性方程得到相应的 Y'. 下面证明要同时获取 x', y' 满足

$$x'^{i}=X', \qquad y'^{j}=Y' \bmod N$$

是困难的，即

1）敌手 A 可先选择随机的 x'，再计算 $X'=x'^{i}$，那么，根据 RSA 是随机置换的假设，X' 是随机的，相应的 Y' 也是随机的，所以，要对随机的 Y' 取其 j 次根，即 $Y'^{1/j}$ 根据 RSA 假设是困难的；

2）敌手 A 也可以选择已有的 X（即从上述游戏中获取的 X），那么，Y 也就确定了，此时，GM 就可追踪到了.

匿名性：由上述构建可见，群签名就是 $\{X_m, Y_m, Z_m, \cdots\}$ 和 SPK，这些显然都不包含任何成员信息，即验证方只能验证签名是否合法，但不知道是哪个成员做的签名，即签名是匿名的. 在上述的签名方案中，由于在签名时要公布 X_m, Y_m, Z_m 等信息，所以，不是完全匿名的，即同一成员相对同一单位所做的群签名是可链接的，不是完全匿名的. 但由于要求在根到叶子节点的路径上，所有公钥多项式中的同一个变量的指数是互素的，则根据 RSA 是随机置换的假设，公开信息也是随机的，从而在不同匿名级别的签名中，同一个成员是不可链接的.

因此，一个重要的公开问题就是如何构建完全匿名（即同一成员针对同一单位所做的群签名也是不可链接的）的层次匿名群签名方案.

4　讨论

提出一种新的层次匿名群签名的概念，将组织的不同部门单位作为层次机构，叶子节点作为群成员个人，群成员在生成群签名时，可以选择自己的匿名层次，即在签名时可以选择把自己隐藏在小组或大组之中，方便成员在不同的应用中使用不同的签名方式. 基于多变量多项式、RSA 假设和知识签名技术，构建一个具体的方案，但方案的缺陷在于没有实现完全匿名，只是有限匿名，即同一个成员对同一个单位所做的群签名虽然是匿名的，但是是可链接的.

因此，下一步重要的研究课题就是如何构建实用、高效的完全匿名的层次匿名群签名方案. 另一工作方向是降低中心管理员负担，即考虑结合 HIBE 和文中的层次匿名方案，构建既能实现层次匿名，又能实现层次管理的方案，即上层管理员可以把成员加入等工作委托给下层单位管理员，从而缓解中心管理员的负担，并考虑如何做到在中心管理员和下层管理员之间合理的工作分配问题，综合考虑管理员的成员密钥生成工作、成员撤销工作及签名打开等工作的合理分配与协调.

参考文献：

[1] CHAUM D, HEYST E. Group signatures[C]// Proceedings of the 10th Annual International Conference on Theory and Application of Cryptographic Techniques Advances in Cryptology. Brighton: Springer, 1991: 257-265. DOI: 10.1007/3-540-46416-6_22.

[2] 冯翰文，刘建伟，伍前红. 后量子安全的群签名和环签名[J]. 密码学报，2021，8(2)：193-201. DOI：10.13868/j.cnki.

jcr.000430.

[3] 陈晓峰,王育民.基于匿名通讯信道的安全电子投票方案[J].电子学报,2003,31(3):390-393.DOI:10.3321/j.issn:0372-2112.2003.03.019.

[4] MALINA L,SMRZ J,HAJNY J,*et al*.Secure electronic voting based on group signatures[C]//38th International Conference on Telecommunications and Signal Processing.Prague:IEEE Press,2015:6-10.DOI:10.1109/TSP.2015.7296214.

[5] 李梦东,杨义先,马春光,等.由群签名实现的可撤销匿名性的电子现金方案[J].北京邮电大学学报,2005,28(2):30-33.DOI:10.3969/j.issn.1007-5321.2005.02.008.

[6] MAITLANDG,BOYD C.Fair electronic cash based on a group[C]//International Conference on Information and Communications Security.Xi′an:Springer,2001:461-465.DOI:10.1007/3-540-45600-7_51.

[7] 姬东耀,王育民.一个基于群签名的安全电子拍卖协议[J].电子学报,2002,30(1):18-21.DOI:10.3321/j.issn:0372-2112.2002.01.005.

[8] LEE C,HO P,HWANG M.A secure e-auction scheme based on group signatures[J].Information Systems Frontiers,2009,11(3):335-343.DOI:10.1007/s10796-008-9094-3.

[9] 莫家庆,胡忠望,林瑜华.基于特定区间承诺值证明机制改进的DAA认证方案[J].计算机科学,2012,39(8):111-114.DOI:10.3969/j.issn.1002-137X.2012.08.024.

[10] BRICKELLE F,CAMENISCH J,CHEN Liqun.Direct anonymous attestation[C]//Proceedings of the 11th ACM Conference on Computer and Communications Security.Washington DC:ACM,2004:132-145.DOI:10.1145/1030083.1030103.

[11] 张建明,赵玉娟,江浩斌,等.车辆自组网的位置隐私保护技术研究[J].通信学报,2012,33(8):180-189.

[12] 吴亚联,朱紫琦,黄盟标,等.基于区块链的VANETs群签名方案[J].吉林大学学报(工学版),2022,52(5):1161-1167.DOI:10.13229/j.cnki.jdxbgxb20210119.

[13] 赵臻,陈杰,张跃宇,等.VANET中高效撤销的批量验证群签名方案[J].密码学报,2016,3(3):292-306.DOI:10.13868/j.cnki.jcr.000129.

[14] 刁一晴,叶阿勇,张娇美,等.基于群签名和同态加密的联盟链双重隐私保护方法[J].计算机研究与发展,2022,59(1):172-181.DOI:10.7544/issn1000-1239.20200576.

[15] 程小刚,王箭,杜吉祥.群签名综述[J].计算机应用研究,2013,30(10):2881-2886.DOI:10.3969/j.issn.1001-3695.2013.10.001.

[16] 程小刚,郭韧,陈永红.群签名成员撤销综述[J].小型微型计算机系统,2016,37(11):2520-2526.

[17] CAMENISCH J,STADLER M.Efficient group signature schemes for large groups[C]//Advances in Cryptology:CRYPTO′97.Berlin:Springer,1997:410-424.DOI:10.1007/BFb0052252.

[18] WATERS B.Dual system encryption:Realizing fully secure IBE and HIBE under simple assumptions[C]//Proceedings of the 29th Annual International Cryptology Conference on Advances in Cryptology.Santa Barbara:Springer,2009:619-636.DOI:10.1007/978-3-642-03356-8_36.

[19] KALYANI D,SRIDEVI R.New hierarchical identity based encryption with maximum hierarchy[J].International Journal of Network Security,2019,21(1):40-46.

[20] BONEH D,BOYEN X,GOH E J.Hierarchical identity based encryption with constant size ciphertext[C]//24th Annual International Conference on the Theory and Applications of Cryptographic Techniques.Aarhus:Springer,2005:440-456.DOI:10.1007/11426639_26.

[21] 程小刚,郭韧,周长利.层次撤销群签名:概念与构建[J].密码学报,2021,8(1):142-153.DOI:10.13868/j.cnki.jcr.000427.

[22] TROLIN M,WIKSTRÖM D.Hierarchical group signatures[C]//Proceedings of the 32nd International Conference on Automata,Languages and Programming.Lisbon:Springer,2005:446-458.DOI:10.1007/11523468_37.

[23] HOU Lin,LIN Dongdai,LIU Renzhang.Hierarchical group signature with verifier-local revocation revisited[J].Science China Information Sciences,2022,65(8):189103.DOI:10.1007/s11432-019-2709-7.

(**责任编辑**:黄晓楠 **英文审校**:吴逢铁)