

文章编号:1000-582X(2004)11-0066-05

# 实时空中的多重向量代数在集对分析中的应用\*

段绍光

(重庆大学数理学院,重庆 400030)

**摘要:**联系数是赵克勤先生在其专著《集对分析及其初步应用》中所提出的一个重要的数学工具,属于系统论和方法论的范畴,旨在统一由于模糊、随机、中介和信息不完全所导致的不确定性度量。试图将 Venzo de Sabbata 教授所采用的与 Dirac 代数同构的实时空中的多重向量代数应用于集对分析中的联系数,从而相应地推广了联系数的范畴。

**关键词:**实空间;多重向量;代数;集对分析;联系数;旋量;流形

**中图分类号:** O412.1; O413.1; O411; NO3; N3

**文献标识码:** A

## 1 集对分析

世界是不确定性与确定性的矛盾统一体。各种系统、各种事物,在某种条件下,某种层次上,体现出不确定性;而在另一种条件下,另一种层次上,体现出确定性,因此,如何运用对立统一的观点,从整体和全局上研究不确定性和确定性,是有待深入探讨的重要问题。

集对分析(Set Pair Analysis,简记为 SPA)是我国学者赵克勤<sup>[1]</sup>先生经过近20年思考于1989年在其专著《集对分析及其初步应用》中所提出的一种联系数  $a + bi + cj$  统一处理模糊、随机、中介和信息不完全所致不确定性的系统理论和方法。其特点是对客观存在的种种不确定性给予客观承认,并把不确定性与确定性作为一个既确定又不确定的同异反系统(同一、差异、对立系统)进行辩证分析和数学处理,集对分析的理论和方法至今已在科学技术和社会经济的许多领域得到广泛的应用。

现在回到集对分析的观点。从层次的角度看,所谓“不确定量”是指在宏观上可以取确定的值,而在微观上不确定取值的一种量。这种不确定量也是一种常见量,对于这种不确定量,要同时从确定性和不确定性两个方面去描述之。于是形成联系数概念,一种把一定范围内的确定性与不确定性联系起来的数,从而在一定意义上使集对分析从一个全新的角度来建立理论和提供方法。具有独到的见解和新颖的思路。

设给定两个集合  $A$  和  $B$ ,并设这两个集合组成集对  $H = (A, B)$ ,在某个具体的问题背景(设为  $W$ )下,对集对  $H$  的特性展开分析,共得到  $N$  个特性,其中:有  $S$  个为集对  $H$  中的两个集合  $A$  和  $B$  所共有;在  $P$  个特性上集合  $A$  和  $B$  相对立,在其余的  $F = N - S - P$  个特性上既不相互对立,又不为这两个集合所共有,则称比值:  $S/N$  为这两个集合在问题  $W$  下的同一度,简称同一度;  $F/N$  为这两个集合在问题  $W$  下的差异度,简称差异度;  $P/N$  为这两个集合在问题  $W$  下的对立度,简称对立度,并用式子

$$\mu(W) = \frac{S}{N} + \frac{F}{N}i + \frac{P}{N}j = a + bi + cj$$

加以统一表示,式中的  $\mu$  就称为  $A, B$  两个集合的联系度。因此,两个集合的联系度  $\mu$  是研究对象——集对  $H$  在指定问题背景  $W$  意义下某个分析过程  $T$  的函数,即:

$$\mu = f(H, W, T)$$

从而  $\mu$  是有关两个集合或一个系统在指定的问题和某个分析过程中所得到的同一度、差异度、对立度的代数和,又常称其为联系度表达式,但在运算分析时,  $\mu$  又可视为一个数,并称为联系数。

### 1.1 联系度 $\mu$ 的结构

#### 1.1.1 联系度 $\mu$ 的层次性

系统具有层次性,由于联系度是个系统,自然就有相应的层次性,笼统而言,联系度  $\mu$  具有宏观、微观两

\* 收稿日期:2004-06-20

作者简介:段绍光(1963-),男,湖南保靖人,重庆大学讲师,主要从事非线性光学、电磁场、天体物理学和宇宙演化的研究。

个层次。

就联系度  $\mu$  的定义式而言,  $N, S, F, P, j$  可看作处在宏观层次上, 是确定不确定系统在宏观层次上的参量;  $i$  则应看作处在微观层次上的一个参量,  $i$  并不是联系度确立过程中确定的, 而是在  $\mu$  中的  $a, b, c$  确立之后, “赋予  $b$ ”的 ( $a + b + c = 1$ ), 目的在于进一步体现  $b$  是对不确定性联系程度的一种刻画, 并使“ $bi$ ”这一项能同时体现不确定联系可以在一定条件下确定这一面和在一条件下不能确定这一面, 后者事实上反映了不确定性的本质。“ $bi$ ”这一项实际上是联系度  $\mu$  中宏观层次上的参量与微观层次上的参量的一个结合点, 把这个点加以剖析, 可以进一步看出联系度  $\mu$  的层次性。

联系度中的  $b$  是可以不断被“分解”的。  $b$  被分解的过程, 也是  $i$  不断取值的过程。  $b$  一般被分解成同、异、反 3 个部分, 与之对应的  $i$  也就同时取 3 个值。“ $i$ ”同时取几个值这件事在集对分析理论中有极为重要的意义。它深刻地揭示了不确定性的本质。

### 1.1.2 联系度 $\mu$ 的可展性

联系度  $\mu$  在同一层次上是可以展开的, 其一般展

$$\mu = \sum_{p=1}^n a_p + \sum_{p=1}^n b_p i + \sum_{p=1}^n c_p j$$

或 
$$\mu = \sum_{p=1}^n a_p + \sum_{p=1}^n b_p i_p + \sum_{p=1}^n c_p j_p$$

### 1.1.3 联系度 $\mu$ 的 T 形结构

当把  $\mu$  在同一层次的展开与  $\mu$  的层次分析结合起来时, 就得到形状像个“T”字的层次展开图。故称为 T 形结构。

T 形结构表明了联系度  $\mu$  可以同时在这个水平上作无穷展开, 在铅垂面上作无穷层次的深入, 这一横向到边, 纵向到底的结构特征有着重要的理论与实践意义。从分形的角度看, 联系度  $\mu$  的 T 形结构具有明显的分形特征——自相似性。

注意, 不要以为  $\mu$  中仅仅只有从  $b$  中不断分出“ $a$ ”和“ $c$ ”这样一种机制。事实上, 在较为深入和细致的研究中, 还需考虑从  $a$  中分出“ $b$ ”和“ $c$ ”; 以及从  $c$  中分出“ $a$ ”和“ $b$ ”, 这些情况表明, 集对分析中的联系度看上去简单, 其实隐含着某种复杂性。至于把静态的联系度推广为动态的联系度, 即把  $\mu$  推广成  $\mu(t)$ , 则情况更加复杂, 涉及系统复杂性。

### 1.2 联系度 $\mu$ 的功能

- 1) 对模糊不确定性的描述;
- 2) 对模糊不确定性夹带由不知道引起的不确定性的描述;

- 3) 对不知道引起的不确定性的描述;
- 4) 对随机不确定性的描述;
- 5) 对随机不确定性夹带模糊不确定性又夹带由不知道引起的不确定性的描述。

### 1.3 常见对立概念的 5 种类型

#### 1.3.1 倒数型对立

特征方程为:  $K \times 1/K = 1$ , 其中  $K$  是大于 1 的正整数,  $1/K$  为  $K$  的倒数。

#### 1.3.2 有无型对立

特征方程为:  $K \times 0 = 0$ , 其中  $K$  仍为大于 1 的正整数, 另一个与  $K$  对立的就用 0 来表征。

#### 1.3.3 正负型对立

特征方程为:  $1 \times (-1) = -1$

#### 1.3.4 虚实型对立

特征方程为:  $1 \times \sqrt{-1} = \sqrt{-1}$

#### 1.3.5 互补型对立

特征方程为:  $A + B = 1$ , 方程中的  $A$  与  $B$  一般取值在  $[0, 1]$ 。  $B = 1 - A = \bar{A}$ ,  $A$  的补。

### 1.4 不确定性的分类

- 1) 倒数型对立, 对应于模糊不确定;
- 2) 有无型对立, 对应于随机不确定;
- 3) 正负型对立, 对应于中介不确定;
- 4) 虚实型对立, 对应于由不知道引起的不确定;
- 5) 互补型对立, 对应于由信息不完全导致的不确定。

### 1.5 集对分析与现代物理

现代量子物理对微观物质运动状态的描述与集对分析的同异反态势描述如出一辙, 量子可以在同一时刻既在这个地方又不在这个地方与联系度中的  $i$  可以同时取不同的值, 光的波粒两象性与联系度的既确定又不确定性, 以及物理上的 Heisenberg 测不准原理与  $i$  可以同时取不同值之联系等, 都说明集对分析的思想方法与现代物理有着深刻和广泛的联系, 集对分析中的联系度与不确定量的概念有重要的物理意义。

## 2 多重向量代数

笔者<sup>[2]</sup>曾介绍意大利国际著名物理学家 Venzo de Sabbata 教授在关于广义相对论在实时空中的引力量子化的开创工作。他认为考虑早期宇宙时就必须用量子论来研究基本粒子物理学和用广义相对论来研究宇宙学, 但广义相对论是在实时空中得到发展的, 而量子论则需要复流形, 如何才能将广义相对论与量子论协调起来? V. D. Sabbata 卓识地认为: 解决的办法是靠那种不含任何复数的时空几何微分学来重新表述

Dirac理论<sup>[3-6]</sup>。

### 2.1 多重向量概念

考虑这样一种几何代数,它采用多重向量概念将虚数单位*j*视为旋转生成元,将张量和旋量置于同一基点上,两者均在实时空中描述。

Hestenes 时空代数<sup>[7]</sup>自动协调了时空的几何结构,首先引入外积  $a \wedge b$ ,它与通常向量分析中的叉积  $a \times b$ 有所不同,它不是一个标量或一个向量,它是一个有向面积或二重向量,指向包含  $a$  和  $b$  的那个平面。

可以将这个概念推广到具有更高维数或级的对象的乘积,即若具有 2 级的二重向量  $a \wedge b$  沿着另一具有 1 级的向量  $c$  扫过,就会得到一个具有 3 级的三重向量  $(a \wedge b) \wedge c$ ,它是一个有向体积,这样就引出多重向量概念。

现定义几何积:它是内积与外积之和,即

$$ab = a \cdot b + a \wedge b \tag{1}$$

将一个标量(内积  $a \cdot b$ )加到一个二重向量(外积  $a \wedge b$ )的结果,是一个同时具有标量部分和二重向量部分的对象,正如实数与虚数相加会得到一个同时具有实部和虚部的对象,后者称为复数,同样前者称为“多重向量”。仿效将复数(用  $j$  表示虚数单位)中分离分量  $x$  和  $iy$  的写法可将几何积简写为  $ab = a \cdot b + a \wedge b$ ,例如,考虑二维空间,取两个正交标准向量  $\sigma_1$  和  $\sigma_2$  有

$$\sigma_1 \cdot \sigma_1 = \sigma_2 \cdot \sigma_2 = 1, \sigma_1 \cdot \sigma_2 = 0 \tag{2}$$

$$\sigma_1 \wedge \sigma_1 = \sigma_2 \wedge \sigma_2 = 0 \tag{3}$$

外积  $\sigma_1 \wedge \sigma_2$  为一有向面积,于是就有 4 个独立基向量为:标量 1,向量  $\sigma_1, \sigma_2$  和二重向量

$$\sigma_1 \wedge \sigma_2 \tag{4}$$

利用这 4 个基元可组成一个多重向量:

$$A = a_0 1 + a_1 \sigma_1 + a_2 \sigma_2 + a_3 \sigma_1 \wedge \sigma_2 \tag{5}$$

为了定义两个多重向量  $A$  与  $B$  的乘积(其中  $B = b_0 1 + b_1 \sigma_1 + b_2 \sigma_2 + b_3 \sigma_1 \wedge \sigma_2$ ),先看 4 个几何基元是如何相乘的,即

$$\sigma_1^2 = \sigma_1 \sigma_1 = \sigma_1 \cdot \sigma_1 + \sigma_1 \wedge \sigma_1 = 1 = \sigma_2^2 \tag{6}$$

和

$$\begin{aligned} \sigma_1 \sigma_2 &= \sigma_1 \cdot \sigma_2 + \sigma_1 \wedge \sigma_2 = \\ \sigma_1 \wedge \sigma_2 &= -\sigma_2 \wedge \sigma_1 = -\sigma_2 \sigma_1 \end{aligned} \tag{7}$$

由于几何积是可结合的,由此

$$(\sigma_1 \sigma_2) \sigma_1 = -\sigma_2 \sigma_1 \sigma_1 = -\sigma_2, (\sigma_1 \sigma_2) \sigma_2 = \sigma_1 \tag{8}$$

也有

$$\sigma_1 (\sigma_1 \sigma_2) = \sigma_2 \text{ 和 } \sigma_2 (\sigma_1 \sigma_2) = -\sigma_1 \tag{9}$$

其次

$$(\sigma_1 \wedge \sigma_2)^2 = \sigma_1 \sigma_2 \sigma_1 \sigma_2 = -\sigma_1 \sigma_1 \sigma_2 \sigma_2 = -1 \tag{10}$$

上述推导的结果之一是二重向量  $\sigma_1 \wedge \sigma_2$  具有将自己所在平面内的向量  $\sigma_1$  和  $\sigma_2$  旋转  $90^\circ$  的几何功效;这个性质表明二重向量  $\sigma_1 \wedge \sigma_2$  扮演单位虚数  $i$  的角色。

所以二重向量  $\sigma_1 \wedge \sigma_2$  为有向面积的单位,也是该平面内的旋转生成元,故可简捷地用  $i$  来表示二重向量  $\sigma_1 \wedge \sigma_2 = \sigma_1 \sigma_2$ 。

推广到三维空间,将第 3 个正交标准向量  $\sigma_3$  加到基元中就可构成

$$\text{标量 } 1, \text{ 向量 } \sigma_1, \sigma_2, \sigma_3, \text{ 二重向量 } \sigma_1 \sigma_2, \sigma_2 \sigma_3, \sigma_3 \sigma_1, \text{ 三重向量 } \sigma_1 \sigma_2 \sigma_3 \text{ (有向体元)} \tag{11}$$

由这 8 个对象就可定义多重向量。

考虑下面这些关系式:

$$(\sigma_1 \sigma_2) \sigma_3 = \sigma_1 \sigma_2 \sigma_3 \tag{12}$$

$$(\sigma_1 \sigma_2 \sigma_3) \sigma_k = \sigma_k (\sigma_1 \sigma_2 \sigma_3), k = 1, 2, 3 \tag{13}$$

和

$$(\sigma_1 \sigma_2 \sigma_3)^2 = \sigma_1 \sigma_2 \sigma_3 \sigma_1 \sigma_2 \sigma_3 = -\sigma_1 \sigma_2 \sigma_1 \sigma_2 \sigma_3^2 = -1 \tag{14}$$

于是三重向量  $\sigma_1 \sigma_2 \sigma_3$  就可以写为

$$\sigma_1 \sigma_2 \sigma_3 = \sigma_1 \wedge \sigma_2 \wedge \sigma_3 = i \tag{15}$$

$\sigma_1 \sigma_2 \sigma_3$  三重向量是 3 维空间中最高级对象(客体),并且是 3 维空间中的单位赝标量,  $i$  为一几何客体,与虚数单位有所不同,为一标量(复数)。

必须注意一个非常重要的事实:将这个 3 重向量分别乘以  $\sigma_3, \sigma_1$  和  $\sigma_2$  就得到:

$$\begin{cases} (\sigma_1 \sigma_2 \sigma_3) \sigma_3 = \sigma_1 \sigma_2 = i \sigma_3 \\ (\sigma_1 \sigma_2 \sigma_3) \sigma_1 = \sigma_2 \sigma_3 = i \sigma_1 \\ (\sigma_1 \sigma_2 \sigma_3) \sigma_2 = \sigma_3 \sigma_1 = i \sigma_2 \end{cases} \tag{16}$$

即为 Pauli 代数,其中  $\sigma_1 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \sigma_2 =$

$$i \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \sigma_3 = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \text{ 为 Pauli 矩阵。}$$

重要的事实是旋转生成元可以诠释为自旋。在 4 维时空中,由 4 个正交标准向量可以构造 16 个几何元,即

1 个标量 1, 4 个向量  $\gamma_\mu (\mu = 0, 1, 2, 3)$ , 6 个二重向量  $(\sigma_k, i\sigma_k) (k = 1, 2, 3)$

4 个赝向量  $i\gamma_\mu (\mu = 0, 1, 2, 3)$ , 1 个赝标量  $i$  (17)

其中  $\sigma_k$  为 Pauli 矩阵。

$$\sigma_k = \gamma_k \gamma_0 \tag{18}$$

而 4 维时空的单位赝标量为

$$i = \gamma_0 \gamma_1 \sigma_2 \sigma_3 = \sigma_1 \sigma_2 \sigma_3 \quad (19)$$

代数(17)为时空代数或实 Dirac 代数。基底(17)的偶数基元与由式(16)定义的 Pauli 代数完全一致。由于关系式(19),  $\sigma_k$  依次满足 3 维 Euclid 空间中的一组基元的要求

$$\sigma_k \cdot \sigma_j = \frac{1}{2}(\sigma_k \sigma_j + \sigma_j \sigma_k) = \delta_{kj} \quad (20)$$

Pauli 代数(16)是 Dirac 代数(17)对选择单位类时向量  $\gamma_0$  的偶维子代数, 并且是旋量的一个 8 维线性空间, 亦即是 8 维实时空中的一类旋量流形。

### 2.2 多重向量的应用

由于在 Dirac 理论中有一个完全反对称自旋密度, 因此有理由引入挠率三重向量

$$Q = Q^{\alpha\beta\gamma} \gamma_\alpha \wedge \gamma_\beta \wedge \gamma_\gamma \quad (21)$$

作为时空代数的一个元素, 其中  $\{\gamma_\alpha\}$  为基向量, 关于它们有几何积

$$\gamma_\alpha \gamma_\beta = g_{\alpha\beta} + \gamma_\alpha \wedge \gamma_\beta = \gamma_\alpha \cdot \gamma_\beta + \gamma_\alpha \wedge \gamma_\beta \quad (22)$$

其次, 给出曲率二重向量

$$\Omega^{\alpha\beta} = \frac{1}{2} R^{\alpha\beta\mu\nu} \gamma_\mu \wedge \gamma_\nu \quad (23)$$

就可以构成曲率三重向量

$$R^\alpha = \Omega^{\alpha\beta} \wedge \gamma_\beta = \frac{1}{2} R^{\alpha\beta\mu\nu} \gamma_\mu \wedge \gamma_\nu \wedge \gamma_\beta \quad (24)$$

在 Sabbata 的理论<sup>[4]</sup>中挠率和曲率视为共轭变量, 他认为每一粒子不仅有质量, 而且也有自旋, 正如质量与时空的曲率有关, 自旋与时空的另一几何性质——挠率(亦称时空第二曲率)有关, 笔者认为挠率与曲率是有差异的, 可用集对分析中的联系数表示: 广义相对论引力 = 时空的弯曲(曲率) + [时空的扭曲(挠率)] $i$

三重向量  $Q$  与  $R^\alpha$  的几何积的反对称部分为

$$[Q, R^\alpha] = \frac{1}{2} QR^\alpha - R^\alpha Q \quad (25)$$

两个三重向量之间的这种乘积类型给出了一个二重向量, 例如

$$[\gamma_0 \wedge \gamma_1 \wedge \gamma_2, \gamma_0 \wedge \gamma_1 \wedge \gamma_3] = \gamma_2 \wedge \gamma_3 \quad (26)$$

用几何代数的语言, 复数的虚数单位被一个二重向量所替代。于是就得到典型的对应关系式[参看方程(21)、(23)、(24)]

$$[Q, R^\alpha] = \frac{1}{2}(QR^\alpha - R^\alpha Q) =$$

$$\frac{1}{2}[Q^{\mu\alpha\beta} \gamma_\mu \wedge \gamma_\nu \wedge \gamma_\beta, R^{\alpha\tau\eta\delta} \gamma_\tau \wedge \gamma_\nu \wedge \gamma_\beta] =$$

$$\frac{1}{2}(Q^{\mu\alpha\beta} R^{\alpha\tau\eta\delta} - R^{\alpha\tau\eta\delta} Q^{\mu\alpha\beta}) \gamma_\mu \wedge \gamma_\tau =$$

$$\gamma_1 \wedge \gamma_2 L_{pl}^{-3} \quad (27)$$

其中  $L_{pl}$  为 Planck 长度。

现在笔者试图进一步将上面介绍的 Venzo de Sabbata 教授所采用的与 Dirac 代数同构的实时空中的多重向量应用于集对分析中的联系数:

4 维时空中的 16 个几何元的线性组合可表示为

$$\begin{aligned} \mu &= a_0 \cdot 1 + \sum_{\mu=0}^3 a_\mu \gamma_\mu + \sum_{k=1}^3 a'_k \sigma_k + \\ &\sum_{k=1}^3 a''_k i \sigma_k + \sum_{\mu=0}^3 a'''_\mu i \gamma_\mu + a_{15} i = \\ &a_0 \cdot 1 + \sum_{\mu=0}^3 a_\mu \gamma_\mu + \sum_{k=1}^3 a'_k \gamma_k \gamma_0 + \\ &\sum_{k=1}^3 a''_k i \gamma_k \gamma_0 + \sum_{\mu=0}^3 a'''_\mu i \gamma_\mu + a_{15} i = \\ &a_0 \cdot 1 + a_{15} i + \sum_{\mu=0}^3 a_\mu \gamma_\mu + \sum_{k=1}^3 a'_k \gamma_k \gamma_0 + \\ &\sum_{k=1}^3 a''_k i \gamma_k \gamma_0 + \sum_{\mu=0}^3 a'''_\mu i \gamma_\mu \end{aligned}$$

它由不同的几何元: 标量 1 (零阶张量)、向量  $\gamma_\mu$ 、二重向量  $\gamma_k \wedge \gamma_0$  (旋转生成元, 自旋) 和  $i \gamma_k \wedge \gamma_0$ , 三重向量  $i \gamma_\mu$  和赝标量(体积)  $i$  所构成。承载不同的信息和能量, 蕴含极其丰富的内涵。从而相应地推广了联系数的范畴。其中  $\sigma_k$  为 Pauli 矩阵。  $\gamma_0$  为单位类时向量。  $\gamma_1$ 、 $\gamma_2$  和  $\gamma_3$  分别为单位空间坐标向量。

### 参考文献:

- [1] 赵克勤. 集对分析及其初步应用[M]. 杭州: 浙江科学技术出版社, 2000.
- [2] 段绍光. 广义相对论在实时空中的引力量子化的新进展[J]. 重庆大学学报(自然科学版), 2002, 25(1): 109-112.
- [3] DATTA B K, SABBATA V D, RONCHETTI L. Quantization of gravity in real space - time [J]. Nuovo Cimento 1998, 113B(6): 711-732.
- [4] SABBATA V D, RONCHETTI L. A Hamiltonian Formulation of Gravitational Theory that Allows One to Consider Curvature and Torsion as Conjugate Variables [J]. Foundation of Physics. 1999, 29(7): 1 099-1 117.
- [5] SABBATA VD, Quantum Gravity [J]. Nuovo Cimento A, 1996, 107(3): 80-93.
- [6] BORZESZKOWSKI H H V, TREDER H J. Spin in Gravity [A]. in Quantum Gravity [C]. World Scientific, Singapore: [s. n.], 1996. 32-42.
- [7] HESTENES D. Clifford Algebra to Geometric Calculus [M]. Reidel, Dordrecht, the Netherlands: [s. n.], 1982.

## Application of Multivector Algebra in Real Space-time to Set Pair Analysis

DUAN Shao-guang

(College of Mathematics and Science, Chongqing University, Chongqing 400030, China)

**Abstract:** The contact number is an important mathematical tool of systems theory and methods in the monograph *Set Pair Analysis and Its Preliminary Applications* written by Zhao Keqin for unitizedly processing the uncertainties due to the fuzzy, stochastic, intermediate and information uncomplete about something. The article applies the multivector algebra which is isomorphism with the real Dirac algebra in the real space-time adopted by Venzo de Sabbata to the contact number of set pair analysis, and consequently, the contact number is generalized correspondingly.

**Key words:** real space-time; multivector; algebra; set pair analysis; contact number; spinor; manifold

(编辑 张 革)

---

(上接第 65 页)

## Distributed Generation of Shared RSA Keys in Mobile Ad Hoc Networks

SHEN Ying<sup>1</sup>, YANG Tian-yi<sup>1</sup>, LIU Yi-liang<sup>2</sup>

(1. College of Automation, Chongqing University, Chongqing 400030, China;

2. Information Security Research Institute, Chongqing Institute of Technology, Chongqing 400050, China)

**Abstract:** Mobile Ad hoc NETWORKS(MANET) is a totally new concept in which mobile nodes are able to communicate together over wireless links in an independent manner, without needing any fixed physical infrastructure and centralized organizational/administrative infrastructure. However, the nature of ad hoc networks makes them very vulnerable to security threats. Generation and distribution of shared keys for CA(Certification Authority) is challenging in security solution based on distributed PKI/CA. Those solutions that have been proposed in the literature and some issues are discussed. This paper propose the solution of distributed generation of shared CA keys based on threshold RSA cryptosystems, with which the security and robustness of system is enhanced.

**Key words:** Mobile Ad Hoc Networks; keys generation; self-organization; RSA; security

(编辑 张 革)