基于短群签名的安全电子拍卖方案*

黄秀姐[1]，林 群[2]，王燕鸣[1,3]
（1. 中山大学 数学与计算科学学院，广东 广州 510275；
2. 韩山师范学院 数学与信息技术学院，广东 潮州 521041；
3. 中山大学 岭南学院，广东 广州 510275）

摘 要：提出了基于双线性对的密码体制在电子拍卖系统中应用的首个方案，利用短群签名技术设计了一个公开的电子拍卖。与其他利用群签名技术设计的电子拍卖方案相比，该方案不仅满足电子拍卖的安全性要求，而且其通信量和存储空间大大节省了。还可以将新方案修改成一个密封式的安全电子拍卖方案，并使之满足相对隐私性。

关键词：电子拍卖；群签名；双线性对
中图分类号：TP309.2 文献标识码：A 文章编号：0529-6579（2006）06-0021-05

电子化已成为现代信息社会生活的一个重要手段，各种电子商务活动计划正逐渐进入各企事业单位的日常工作议程。电子拍卖作为电子商务活动的重要形式之一，各种拍卖行、拍卖代理系统如 eBay, Amazon.com, Yahoo等已在现实生活中发挥着重要作用。电子拍卖方案按照标价公开与否，可分为公开标价拍卖和密封式拍卖。公开标价拍卖系统中，每个投标者可以匿名投标，而且可以多次投标。公开标价的拍卖有价格递增拍卖（英式拍卖）和价格递减拍卖（荷式拍卖）两种形式。密封式标价拍卖系统中，投标者一次性秘密地把标信息提交给拍卖行；在开标阶段，最高价位（或最低价位）的投标者被确认为中标者。

群签名技术是设计安全电子拍卖方案的一个重要的工具[1-3]。这些方案用到的群签名都是基于RSA问题的。其中，文[3]利用的是一个可转化的群签名，但是该群签名方案的理论安全性没有被证明；文[2]利用的是文[4]中的签名方案，虽然该签名方案在安全性方面得到了证明，但由于其计算量和通信量非常大，使得拍卖方案的效率很低；文[1]利用文[5]中的群签名方案，由于签名长度较长以及密钥管理的问题，此拍卖方案在效率上也不是很高。近年来，基于身份的密码体制的研究取得了显著的成果，如文[6-8]，这为密码学的发展开辟了新的空间。基于身份的密码体制的一个有力工具就是双线性对，在 Boneh等人提出的短签名[8]和短群签名[6]等方案都应用到了。本文首次设计出了基于双线性对的密码体制在电子拍卖系统中的应用方案，它是利用[6]中的短群签名技术设计而成的公开电子拍卖方案。该方案不仅满足电子拍卖方案的安全性要求，而且与其他利用群签名技术设计的电子拍卖方案相比，其通信和存储资源大大节省了。同时，本文将新方案修改成一个密封式的安全电子拍卖方案，并使之满足相对隐私性。

1 困难性假设和拍卖模型概述

1.1 双线性群（Bilinear Groups）

定义 1 设 G_1 和 G_2 是两个素数阶（阶数为 p）的乘法循环群，g_1 与 g_2 分别是 G_1 与 G_2 的生成元；Ψ 是从 G_2 到 G_1 的一个同态映射，且 $\Psi(g_2)=g_1$；e 是一个映射：$G_1\times G_2\to G_T$，且 e 满足以下性质：

（1）双线性：对 G_1 和 G_2 中的任意元素 u 和 v 有 $e(u^a, v^b)=e(u, v)^{ab}$，其中，$a, b\in Z_p$；

（2）非退化性：$e(g_1, g_2)\neq 1$。

则称 e 是一个双线性映射；称 (G_1, G_2) 是一对双线性群，如果 G_1 和 G_2 中的群运算，映射 Ψ 以及双线性映射都是能够有效运算的。

如果 $G_1=G_2$，就称 G_1 是一个双线性群。

1.2 困难性假设

（1）Strong Diffie-Hellman（SDH）假设[9]

定义 2 假设 G_1 和 G_2 是两个素数阶（阶数为 p）的乘法循环群，g_1 与 g_2 分别是 G_1 与 G_2 的生成

* 收稿日期：2006-01-06
基金项目：国家自然科学基金资助项目（10271119 10571181）
作者简介：黄秀姐（1982年生），女，博士生；通讯联系人：王燕鸣；E-mail: hxjmcs2006@hotmail.com

元。给定 $(q+2)$元数组 $(g, g^{x}, g^{x^2}, \cdots, g^{x^q})$，要求输出满足 $A^{x+x}=g$的二元组 $(A, x)(x\in Z_p^*)$的问题称为 q-SDH问题。

q-SDH假设是指：不存在一个概率多项式时间算法能够以不可忽略的概率解决 G_1和 G_2的 q-SDH问题。

(2) 线性决策假设[6]

定义 3 已知群 G_1, g是其生成元，u, v, h也是 G_1的任意生成元，给定数组 $(u^a, v^b, h^c)\in {}_RG_1$后，判断等式 $a+b=c$是否成立的问题称为线性决策问题。

线性决策假设是指：不存在概率多项式时间算法，能够以不可忽略的概率解决线性决策问题。

1.3 知识签名

$G=\langle g\rangle$是一个循环群，其阶数 $\#G$未知，但其比特数 l_G(即 $2^{l_G-1}\leqslant \#G\leqslant 2^{l_G}$)是公开的。假设有一个抗碰撞的 hash函数 $H: \{0,1\}^* \to \{0,1\}^k$以及安全参数 $\varepsilon>1$。

定义 4 $y\in G$关于底 g的离散对数 x的一个知识签名是一个满足 $c=H(y\| g\| g^s y^c\| m)$的二元数组 $(c, s)\in \{0,1\}^k\times \pm\{0,1\}^{\varepsilon(l_G+k)+1}$，记为 $SPK\{(\alpha): y=g^{\alpha}\}(m)$。

1.4 电子拍卖模型

一般情况下，电子拍卖方案可以分为以下几个步骤：

1) 拍卖系统设置阶段：注册中心和拍卖行选择系统参数并公布这些参数及有关拍卖品的信息(如拍卖编号、拍卖时间等)；

2) 注册阶段：每个竞拍者到注册中心进行身份注册；

3) 投标阶段：投标者向拍卖行投标；

4) 中标者确定阶段：判断中标者的身份及出价，完成交易。

1.5 电子拍卖方案的安全性要求

1) 拍卖的公平性(fairness)：所有投标者地位一样，没有一方比其他方有更有利的条件；

2) 不可伪造性(bid unforgeability)：投标者的投标不能被伪造；

3) 投标者的匿名性(bidder anonymity)：投标者的身份必须保密；

4) 标价保密性(bid privacy)：投标者的标价必须保密；

5) 不可否认性(winner non-repudiation)：投标者中标后不能否认其投标；

6) 不可联系性(bids unlinkability)：同一个投标者的两次合法投标是不可联系的；

7) 可公开证明性(public verifiability)：可公开证明中标者的投标是否合法；

8) 可追踪性(traceability)：中标者能够被追踪到。

公开标价的电子拍卖方案满足 1), 2), 3), 5), 6), 7), 8)等性质；密封式的电子拍卖一般要满足 1), 2), 3), 4), 5), 7), 8)等性质。

2 一个新的公开电子拍卖方案

符号说明：RM表示注册中心，AM表示拍卖行，u_i表示第 i个投标者($i\in\{1, \cdots, l\}$)。

本节根据文[1, 6]提出一个新的公开标价的电子拍卖方案，与先前的利用基于 RSA问题的群签名设计的电子拍卖方案相比，它的一个显著特点就是通信量和存储空间大大节省了。

2.1 系统初始设置

(G_1, G_2)是一对双线性群，$H: \{0,1\}^* \to Z_p$是一个安全的 hash函数，RM随机选择 $h, h_1\in {}_RG_1\setminus\{1_{G_1}\}$, $\zeta_1, \zeta_2\in {}_RZ_p^*$, $u, v\in {}_RG_1$且满足 $u^{\zeta_1}=v^{\zeta_2}=h$, $w=g_2^{\gamma}\in G_2$，其中 $(\zeta_1, \zeta_2, \gamma)$对任何人保密，$(g, g_2, h, h_1, u, v, w)$作为公钥公开。

2.2 注册认证(用户与注册中心之间的协议)

1) u_i向 RM提交身份 ID_i和自己的公钥 C_i: $C_i=h_1^{a_i}\in G_1$，其中 $a_i\in {}_RZ_p^*$是保密的。

2) RM对信息 ID_i进行审查。若合格，则与 u_i发生以下协议：

① u_i随机选择 $k\in {}_RZ_p^*$，计算 $T=e(h, g_2)^k$，并把 T发送给 RM；

② RM返回给 u_i一个值 $c\in {}_RZ_p^*$作为回应；

③ u_i计算 $s_i=k+ca_i$，并发送 s_i给 RM；

④ RM验证等式 $e(h, g_2)^{s_i}=T\cdot e(C_i, g_2)^c$是否成立。

若等式成立，则 RM执行第 3)步。

说明：以上协议可看成是群 G_1中，C_i关于底 h_1的离散对数的一个知识签名，只需把 c替代为一个安全的 hash函数作用下的值，也就是 u_i向 RM提交 $(ID_i, C_i, proof=\{SPK(\alpha): C_i=h_1^{\alpha}\}(m))$。

3) RM向 u_i颁发证书 $Cert_i=(A_i, x_i)$，它满足 $A_i^{x+x_i}\cdot C_i=g$，并把 (A_i, x_i)与 u_i的一一对应关系做成一个列表 List_RM秘密存储起来。

4) u_i对接收到的证书 (A_i, x_i)进行验证：判断等式 $e(A_i, wg_2^{x_i})\cdot e(h, g_2^{a_i})=e(g, g_2)$是否成立。

若等式成立，则 u_i认为该证书有效，自己的签名私钥是 (A_i, x_i)和 a_i。

2.3 投标(u_i向 AM提交标信息 bid_i)

投标者 u_i向 AM提交标信息 $bid_i=(M, SIG_i)$，

其中 M_i包括了投标者的注册信息和出价，M_i= auction ID_i ‖ price p_i；SIG_i是投标者对消息 M_i的签名：

$$SIG_i = SPK\{(\alpha, \beta, x, y, \varepsilon, \eta):$$
$$T_1 = u^{\alpha} \wedge T_2 = v^{\beta} \wedge T_1^{x} \cdot u^{\varepsilon} = 1 \wedge T_2^{x} \cdot v^{\eta} = 1$$
$$\wedge e(T_3, g_2)^{x} \cdot e(h, w)^{-\alpha-\beta} \cdot e(h, g_2)^{-\varepsilon-\eta} \cdot e(h, g_2)^{y}$$
$$= e(g_1, g_2) / e(T_3, w)\}(M_i)$$

u_i产生签名 SIG_i的过程如下：

1）随机选择 α, $\beta \in_R Z_p^*$，计算

$$T_1 = u^{\alpha}, \quad T_2 = v^{\beta}, \quad T_3 = A_i h^{\alpha+\beta},$$
$$\delta_1 = x_i \cdot \alpha, \quad \delta_2 = x_i \cdot \beta;$$

2）随机选择 r_{α}, r_{β}, r_{x_i}, r_{a_i}, r_{δ_1}, $r_{\delta_2} \in_R Z_p^*$，令

$$R_1 = u^{r_{\alpha}}, \quad R_2 = v^{r_{\beta}},$$
$$R_4 = T_1^{r_{x_i}} \cdot u^{-r_{\delta_1}}, \quad R_5 = T_2^{r_{x_i}} \cdot v^{-r_{\delta_2}},$$
$$R_3 = e(T_3, g_2)^{r_{x_i}} \cdot e(h, w)^{-r_{\alpha}-r_{\beta}} \cdot$$
$$e(h, g_2)^{-r_{\delta_1}-r_{\delta_2}} \cdot e(h, g_2)^{-r_{\alpha_i}}$$

3）计算

$$c = H(M_i, T_1, T_2, T_3, R_1, R_2, R_3, R_4, R_5) \in Z_p$$

4）计算 $s_{\alpha} = r_{\alpha} + c \cdot \alpha$, $s_{\beta} = r_{\beta} + c \cdot \beta$,

$$s_{x_i} = r_{x_i} + c \cdot x, \quad s_{a_i} = r_{a_i} + c \cdot a_i$$
$$s_{\delta_1} = r_{\delta_1} + c \cdot \delta_1, \quad s_{\delta_2} = r_{\delta_2} + c \cdot \delta_2;$$

则签名为

$$SIG_i = \sigma = (T_1, T_2, T_3, c, s_{\alpha}, s_{\beta}, s_{x_i}, s_{a_i}, s_{\delta_1}, s_{\delta_2})$$

2.4　确定中标者（AM与 RM共同判断出中标者）

1）投标结束后，AM对收到的所有的标 bid_i = (M_i, SIG_i)进行验证如下：

由 $\sigma = (T_1, T_2, T_3, c, s_{\alpha}, s_{\beta}, s_{x_i}, s_{a_i}, s_{\delta_1}, s_{\delta_2})$先计算出 R_1, R_2, R_3, R_4, R_5：

$$R_1 = u^{s_{\alpha}} / T_1^{c}, \qquad R_2 = v^{s_{\beta}} / T_2^{c}$$
$$R_4 = T_1^{s_{x_i}} \cdot u^{-s_{\delta_1}}, \quad R_5 = T_2^{s_{x_i}} \cdot v^{-s_{\delta_2}}$$
$$R_3 = e(T_3, g_2)^{s_{x_i}} \cdot e(h, w)^{-s_{\alpha}-s_{\beta}} \cdot e(h, g_2)^{-s_{\delta_1}-s_{\delta_2}} \cdot$$
$$e(h, g_2)^{s_{a_i}} \cdot (e(T_3, w) / e(g_1, g_2))^{c};$$

并检验等式 $c = H(M_i, T_1, T_2, T_3, R_1, R_2, R_3, R_4, R_5)$是否成立。若成立，则该投标者的标是合法的。

最后，AM再对所有合法的投标进行比较，找出最高价位的投标 bid_i并将其公布在公告栏上。

2）RM根据公告栏上的 bid_i按照上面的验证方法验证其合法性。若合法，则可由签名 $SIG_i = \sigma$ = $(T_1, T_2, T_3, c, s_{\alpha}, s_{\beta}, s_{x_i}, s_{a_i}, s_{\delta_1}, s_{\delta_2})$计算出投标者的身份信息 A_i：

$$T_3 / (T_1^{x_1} \cdot T_2^{x_2}) = A_i$$

再利用存储列表 List— RM找到与 (A_i, x_i)对应的 u_i。最后，RM宣布 u_i为中标者，把 u_i的信息通知给商家。

3　新方案的安全性和效率讨论

3.1　安全性分析

1）公平性：投标者直接的地位是一样的，没有优势上的差别。

2）匿名性：投标者的身份只有 RM才可以打开。因为投标者的签名是

$$SIG_i = (T_1, T_2, T_3, c, s_{\alpha}, s_{\beta}, s_{x_i}, s_{a_i}, s_{\delta_1}, s_{\delta_2})$$

(T_1, T_2, T_3)是身份信息 A_i的一个线性加密[6]，根据文[6]知道若决策线性假设（LA)成立，则线性加密方案对选择明文攻击来说是语义安全的。

3）不可伪造性：因为投标者签名时，除了用到证书 $Cert_i = (A_i, x_i)$外，还用秘密私钥 $a_i (C_i = h^{a_i})$，而 a_i是任何人（包括 RM和 AM)都不知道的。

4）不可否认性：因为从中标者的签名 SIG_i = $\sigma = (T_1, T_2, T_3, c, s_{\alpha}, s_{\beta}, s_{x_i}, s_{a_i}, s_{\delta_1}, s_{\delta_2})$中，RM可以识别出中标者的身份：

$$T_3 / (T_1^{x_1} \cdot T_2^{x_2}) = A_i$$

5）可追踪性：RM可以从签名中识别出中标者的身份，从而对中标者进行追踪。

6）可验证性：任何人都可以验证中标者所投的标的合法性。

7）不可联系性：除了 RM可以打开投标者的秘密身份之外，任何人不知道每个签名所对应的投标者身份。给定两个标，其签名分别为：

$$SIG_i = \sigma = (T_1, T_2, T_3, c, s_{\alpha}, s_{\beta}, s_{x_i}, s_{a_i}, s_{\delta_1}, s_{\delta_2}),$$
$$SIG_i' = \sigma' = (T_1', T_2', T_3', c', s_{\alpha}', s_{\beta}', s_{x_i}', s_{a_i}', s_{\delta_1}', s_{\delta_2}')$$

要判断这两个签名是否是同一个人签的，就是要判断 $\log_{\eta} T_3 / T_3'$与 $\log_{\eta} T_1 / T_1' + \log_{\eta} T_2 / T_2'$的和是否相等。由决策线性假设（LA)可知这是不可能做到的。

3.2　效率分析

与以前拍卖方案相比，本方案中所用的是短群签名方案，因此所得到的拍卖方案在通信量和存储空间上有了很大的改进。在相同的安全性要求下，我们假设双线性群的选择与文[7]中的一样：E是有限域 F_q上的椭圆曲线 $y^2 = x^3 + 1$, $q = 2 \pmod 3$，E中的元素是 171 bits；G_1和 G_2都是 E的一个 p阶子群且 $q = 6p - 1$，G_T是 $F_{q^2}^*$上的一个 p阶子群；素数 p为 170 bits，$|n| = 1200$，又假设 LXS方案[1]中的系统参数为 $\varepsilon = 9/8$, $l = 600$, $\lambda_1 = 2880$, $\lambda_2 = 2400$, $\gamma_1 = 3420$, $\gamma_2 = 2880$, $k = 160$, $|n| = 1200$.

考虑通信量的比较，考虑群公钥时，需要描述双线性群。根据上一段的假设，将新方案与[1]中 LXS方案做比较，得到比较结果可见表 1。由此表看到方案的通信量和存储空间大大节省了。

表 1 比较结果 (单位: Bytes)

Tab. 1 Comparison results

拍卖方案	签名长度	群公钥	签名私钥	注册密钥	追踪密钥
LXS方案	3280	1050	1088	900	300
新方案	212	171	62	22	40

再考虑计算量。在新方案中，成员注册、投标、验证标书和确定中标者时所需的主要计算量，具体可见表 2. 其中, e表示双线性对运算, ex表示指数运算。

表 2 主要计算量

Tab. 2 Comparison of computation

拍卖方案	成员注册	投标	验证标书	确定中标者
新方案	$2e$, $6ex$	$1e$, $13ex$	$1e$, $14ex$	$2ex$

4 密封式的电子拍卖方案

本节介绍分析一个由新的公开电子拍卖方案修改而成的密封式电子拍卖方案。修改后的方案仍分为 4个阶段，其中，系统初始设置和注册认证 2个阶段与第 2节的方案一致，而对投标和确定中标者 2个阶段做了一些修改，具体如下：

4.1 投标阶段 (u_i向 AM提交标信息 bid_i)

投标者 u_i向 AM发送 $bid_i=(M_i, SIG_i)$，其中 $M_i=Enc(pk_{AM}, m_i)$, $m_i=$ auction ID$_i$ || price p_i, $Enc(pk, m)$ 表示用用户 的公钥 pk加密消息 m 后得到的密文；

$$SIG_i=SPK\{(\alpha,\beta,x,y,\varepsilon,\eta):$$
$$T_1=u^{\alpha}\wedge T_2=v^{\beta}\wedge T_1^{x}\cdot u^{\varepsilon}=1\wedge T_2^{x}\cdot v^{\eta}=1$$
$$\wedge e(T_3,g_2)^{x}\cdot e(h,w)^{-\alpha-\beta}\cdot e(h,g_2)^{-\varepsilon-\eta}\cdot e(h,g_2)^{y}$$
$$=e(g_1,g_2)/e(T_3,w)\}(M_i)$$

AM对收到的标进行验证，若通过验证，则将 $bid_i=(M_i, SIG_i)$公布在公告栏上。

4.2 确定中标者阶段

AM对收到的所有的标 $bid_i=(M_i, SIG_i)$做如下工作：

1) AM对所有的 M_i分别进行解密：

$$Dec(sk_{AM}, M_i)=m_i$$

$Dec(sk, m)$就是 利用其私钥 sk对 m进行解密；

2) AM对获得的所有的 m_i进行比较，找出最高标价 price p_i，并将其对应的标信息 M_i告诉 RM；

3) RM根据收到的 M_i在 AM的公告栏中找出 $bid_i=(M_i, SIG_i)$，根据 $SIG_i=\sigma$计算如下：

$$T_3/(\hat{T}_1\cdot\hat{T}_2)=A_i$$

则可利用存储列表 List— RM找到与 (A_i, x_i)对应的 u_i，即知道了中标者的身份。

类似于 3.1节，可分析得到新的密封式电子拍卖方案满足公平性、不可伪造性、匿名性、不可否认性和可追踪性。标价的保密性是因为投标者的出价利用 AM的公钥进行加密，保证了除他自己和 AM之外的任何人都不能知道他的出价是多少。可公开证明性可以更强，即任何人都可以验证任何一个投标是否合法。所以，新的密封式电子拍卖方案满足了安全电子拍卖方案的性质。同时此密封式拍卖方案还满足相对隐私性[10]：拍卖结束后，尽管所有投标都是公布在 AM的公告栏上的，但是 AM只能知道每个投标相应的出价，却不知道其对应的投标者是谁；而 RM只能知道每个投标的投标者身份，却不知道其出价是多少。因此，只要 RM与 AM不相互勾结就能保证密封式拍卖方案的安全要求。

5 结 语

本文利用 BBS短群签名方案设计了一个公开的安全电子拍卖方案[6]，首次提出了基于双线性对的密码体制在电子拍卖系统中的实际应用。该方案满足电子拍卖方案的安全性要求，而且与其他利用群签名技术设计的电子拍卖方案相比，在通信量和存储空间上大大节省了。同时本文将新方案修改成一个密封式的安全电子拍卖方案，并使之满足相对隐私性。

参考文献：

[1] LIU Xin, XU Qiu-liang, SHANG Jiu-qing. A Public Auction Scheme Based on Group Signature[C]. Proceedings of the 3rd International Conference on Information Security, Shanghai, China, November 14—16, 2004, Vol. 85. New York: ACM, 2004: 136—142.

[2] NGUYEN K, TRAORT J. An online public auction protocol protecting bidder privacy[C]. ACISP 2000, LNCS 1841. Berlin: Springer—Verlag, 2000: 427—442.

[3] SAKURAI K, MIYAZAKI S. An anonymous electronic bidding protocol based on a new convertible group signature scheme[C]. ACISP 2000, LNCS 1841. Berlin: Springer—Verlag, 2000: 385—399.

[4] CAMENISH J, STADLER M. Efficient group signature scheme for large groups[C]. CRYPTO 1997, LNCS 1294. Berlin: Springer—Verlag, 1997: 410—424.

[5] ATENIESE G, CAMENISH J, JOYE M, et al. A practical and provably secure coalition—resistent group signature scheme[C]. CRYPTO 2000, LNCS 1880. Berlin: Springer—Verlag, 2000: 255—270.

[6] BONEH D, BOYEN X, SHACHAM H. Short Group Signature[C]. CRYPTO 2004, LNCS 3152. Berlin: Springer-Verlag, 2004: 41-55.
[7] BONEH D, FRANKLIN M. Identity-based encryption from the weil pairing[C]. CRYPTO 2001, LNCS 2139. Berlin: Springer-Verlag, 2001: 213-229.
[8] BONEH D, LYNN B, SHACHAM H. Short signatures from the weil pairing[C]. AISACRYPT 2001, LNCS 2248. Berlin: Springer-Verlag, 2001: 514-532.
[9] BONEH D, BOYEN X. Short signatures without random oracles[C]. EUROCRYPT 2004, LNCS 3027. Berlin: Springer-Verlag, 1994: 56-73.
[10] PENG K, BOYD C, DAWSON E, et al. Efficient implementation of relative bid privacy in sealed-bid auction[C]. WISA 2003, LNCS 2908. Berlin: Springer-Verlag, 2004: 244-256.

Secure Electronic Auction Schemes Based on the Short Group Signature

HUANG Xiu-jie[1], LIN Qun[2], WANG Yan-ming[1,3]
(1. School of Mathematics and Computational Science, Sun Yat-sen University, Guangzhou 510275, China;
2. Institute of Mathematics and Information Technology, Hanshan Normal University, Chaozhou 521041, China;
3. Lingnan College, Sun Yat-sen University, Guangzhou 510275, China)

Abstract: A public electronic auction scheme based on short group signature is designed, which is the first scheme of the applications of the pairing-based cryptography on electronic auctions. Comparing with former auction schemes based on group signatures, the new one satisfies all main properties of common secure public auction schemes, and its communication and storage are much lower. At last, a sealed-bid auction scheme is proposed, which is transformed from the public one and satisfies the property of relative bid privacy.
Key words: electronic auction; group signature; pairing

(上接第 10页)

Qualitative Analysis on a Type of Competitive Dynamic System on Time-scales

LI Yan-hui[1], HUANG Wen-qiang[2], ZHU Si-ming[1]
(1. School of Mathematics and Computational Science, Sun yat-sen University, Guangzhou 510275, China;
2. China Airlines Company Limited, Guangzhou 510406, China)

Abstract: Qualitative analysis of nonlinear dynamic system on time-scales is studied. Two properties are firstly discussed, and the concept "contain curve" is brought. Based on the graininess function $\mu(t)$, function $x(t)$ of dynamic system on time-scales can be divided into two cases: $x(t)$ jumps from one contain curve to another in discrete points; While $x(t)$ is along contain curve in continuous time t. Then the planar Volterra competitive system on time-scales is qualitatively analyzed. Applying the conclusion to the competition between two populations, the death of one population in finite time can be explained.
Key words: dynamic system on time-scales; qualitative analysis; Volterra competitive system