一个基于秘密分享和签密的高效多轮电子拍卖方案 [1]

张福泰 * ** 张方国 * 王育民 *

*(西安电子科技大学 ISN 国家重点实验室 西安 710071)
**(陕西师范大学计算机系 西安 710062)

摘 要 利用一个新的秘密分享方案和签密技术，提出了一个安全、高效的多轮电子拍卖方案. 在该方案中，除了中标人外其他投标人的投标价和标书自始至终是保密的；所有投标人都可以验证中标结果. 在消息的秘密传送中，使用了签密技术，同时实现了保密和认证，从而大大提高了效率. 同时该方案也可用于第二价位拍卖.

关键词 秘密分享，电子拍卖，签密，投标
中图号 TN918.1, TN919.3

1 引 言

拍卖是一种常见的商品交易方式. 电子拍卖是电子商务的重要组成部分，也是电子商务中极为活跃的一个方面. 常见的拍卖方式大致有 4 种类型：价格递增式拍卖或英式拍卖，价格递减式拍卖或荷兰式拍卖，密封式拍卖及第二价位拍卖. 在价格递增式拍卖中，拍卖行先给出所拍卖商品的最低限价 K，第 i 次投标时的标价为 $K+(i-1)\Delta$，直到只有一个投标人投标时为止. 中标者就是最后一次投标者，中标价就是他最后一次所投的价. 在价格递减式拍卖中，拍卖行先给出所拍卖商品的最高标价 K，在第 i 次投标时的标价为 $K-(i-1)\Delta$，第一个投标的人即为中标者，中标价为其投标价. 在密封式拍卖中，所有投标人把他们的标书密封 (如加密) 后送给拍卖行，拍卖行打开所有的标书以确定中标价和中标人，中标价为最高投标价. 在第二价位拍卖中，投标方式与密封式拍卖相同，投标价最高的投标人中标，而成交价为次最高投标价. 价格递增式拍卖花费的时间和通信代价都很高，而且会泄露有关投标人的许多信息 [1]. 价格递减式拍卖虽不会泄露除了中标人之外的其他投标人的任何信息，但时间代价也可能会很大. 密封式拍卖可能经一轮投标就可结束，但拍卖行会确切地知道所有投标人的出价，同时这种拍卖方式不利于商品的最优分配 [1]. 第二价位拍卖虽时间代价较小，但不能保护投标人的隐私. 文献 [2] 首次提出了采用匿名投标的拍卖方案，其方案可以防止一些投标人相互串通以操纵拍卖结果的行为. 文献 [3] 从密码学角度探讨了如何设计和实现安全的电子拍卖方案. 文献 [4] 给出了一个安全的网上第二价位拍卖方案. 文献 [5] 在假定了匿名信道的存在性的前提下，探讨了在拍卖中如何防止一些投标人相互串通以操纵拍卖结果及如何保护投标人隐私的问题. 文献 [6] 以公钥密码为基础提出了一个密封式电子拍卖方案，在其中假定了注册中心是分布式的，投标人的投标值不会直接泄露给任何人. 文献 [1,7, 8] 采用了基于 Shamir 秘密分享方案的多方安全计算协议，以使多个拍卖代理分享投标人的身份. 文献 [9] 采用可转换不可否认签字以保护投标人的秘密，然而，其方案中的通信量非常大.

我们以一个新的秘密分享方案和签密技术 [10] 为基础，采用类似于文献 [8] 中的方法，提出一个安全、高效的电子拍卖方案. 该方案不仅能保护投标人的隐私，而且效率高，易于实施，同时还能用于第二价位拍卖. 本文的安排如下：在第 2 节给出一个新的秘密分享方案；第 3 节介绍我们要用的签密方案；第 4 节提出我们的拍卖方案；第 5 节是简要给出对我们方案的安全性和效率的分析；最后是小结.

[1] 2000-06-16 收到，2001-03-06 定稿
国家自然科学基金重点资助项目，项目编号 19931010

2 基于 α-型秘密共享矩阵的秘密分享方案

2.1 α- 型秘密共享矩阵

设 $\alpha=(a_1,a_2,\cdots,a_t)^T$ 是有限域 GF(q) 上的一个 t 维非零列向量，G 是 GF(q) 上的 $t\times m$ 阶矩阵。称 G 是 GF(q) 上的 α- 型秘密共享矩阵，如果 G 的任意 t 个列向量是线性无关的，并且 G 的任意 $t-1$ 个列向量与 α 所构成的向量组是线性无关组。

2.2 基于 α- 型秘密共享矩阵的秘密分享系统

设 $\alpha=(a_1,a_2,\cdots,a_t)^T$ 是有限域 GF(q) 上的 t 维非零列向量，G 是 GF(q) 上的 $t\times m$ 阶 α-型秘密共享矩阵 ($t<m$)。设秘密空间为 GF(q)，秘密 $s\in$GF(q) 要由 m 个用户 $P_1,P_2,\cdots,P_m$ 分享，为此令 $U(s)=\{(s_1,s_2,\cdots,s_t)$：$s_i\in \mathrm{GF}(q)$，$i=1,\cdots,t$ 且 $a_1s_1+a_2s_2+\cdots+a_ts_t=s\}$，在 $U(s)$ 中随机选取一个 t 维向量 $(s_1,s_2,\cdots,s_t)$，令 $(v_1,v_2,\cdots,v_m)=(s_1,s_2,\cdots,s_t)G$，把 $v_1,v_2,\cdots,v_m$ 作为秘密份额依次秘密地发送给 m 个分享者。这样就构造了一个 (t,m) 秘密分享方案。若要用秘密份额 $v_{i_1},v_{i_2},\cdots,v_{i_t}$ 恢复秘密，只需用 G 的相应列向量 $G_{i_1},G_{i_2},\cdots,G_{i_t}$，由线性方程组 $(G_{i_1},G_{i_2},\cdots,G_{i_t})\ X=\alpha$ 解出 $X=(b_1,b_2,\cdots,b_t)^T$，然后可计算出秘密 $s=b_1v_{i_1}+b_2v_{i_2}+\cdots+b_tv_{i_t}$。

证明 由于 G 是 α- 型秘密共享矩阵，所以 G 的任意 t 列 $G_{i_1},G_{i_2},\cdots,G_{i_t}$ 是线性无关的。从而线性方程组 $(G_{i_1},G_{i_2},\cdots,G_{i_t})\ X=\alpha$ 有唯一解 $X=(b_1,b_2,\cdots,b_t)^T$，于是我们有 $b_1v_{i_1}+b_2v_{i_2}+\cdots+b_tv_{i_t}=(v_{i_1},v_{i_2},\cdots,v_{i_t})(b_1,b_2,\cdots,b_t)^T=(s_1,s_2,\cdots,s_t)(G_{i_1},G_{i_2},\cdots,G_{i_t})(b_1,b_2,\cdots,b_t)^T=(s_1,s_2,\cdots,s_t)(a_1,a_2,\cdots,a_t)^T=a_1s_1+a_2s_2+\cdots+a_ts_t=s$。

而对任意 $t-1$ 个秘密份额 $v_{i_1},v_{i_2},\cdots,v_{i_{t-1}}$ 来说，由于 $G_{i_1},G_{i_2},\cdots,G_{i_{t-1}},\alpha$ 是线性无关的，所以对任意的 $d\in$ GF(q)，线性方程组 $(x_1,x_2,\cdots,x_t)(G_{i_1},G_{i_2},\cdots,G_{i_{t-1}},\alpha)=(v_{i_1},v_{i_2},\cdots,v_{i_{t-1}},d)$ 都存在惟一的一组解。由于 d 的任意性，任何 $t-1$ 个秘密份额都无法得到有关秘密 s 的任何信息。 证毕

3 签密方案

在我们的方案中将采用签密技术，签密 [10] 把签字和加密有机地结合了起来，对既需要保密又需要认证的消息以签密方式传送能同时满足这两方面的要求，而且还能大大减少计算和通信代价 [10]，从而极大地提高通信效率。我们采用文献 [10] 中的签密方案，所不同的是，我们每次签密一组数据 (或者说一个向量)。方案的具体描述如下：

公开参数：p,q 表示足够大的素数 (p 至少 144bit，q 至少 512bit)，其中 $p|q-1$；g 表示 GF(q) 中的一个 p 阶元素；hash 表示输出至少为 128bit 的抗碰撞 hash 函数，KH 表示有密钥控制的单向 hash 函数；E，D 表示一个对称密码体制的加解密算法。

签密者 Alice 的密钥：私钥 $x_a\in\{1,2,\cdots,p-1\}$，公钥 $y_a(=g^{x_a}\mathrm{mod}q)$。

解签密者 Bob 的密钥：私钥 $x_b\in\{1,2,\cdots,p-1\}$，公钥 $y_b(=g^{x_b}\mathrm{mod}q)$。

Alice 对消息 m 的签密过程：随机选取 $x\in\{1,2,\cdots,p-1\}$，计算 $(K_1,K_2)=\mathrm{hash}(y_b^x\mathrm{mod}q)$，$c=E_{K_1}(m)$，$r=\mathrm{KH}_{K_2}(m)$，$s=x/(r+x_a)\mathrm{mod}p$. 密文为 (c,r,s)。

Bob 对密文 (c,r,s) 的解签密过程：计算 $(K_1,K_2)=\mathrm{hash}((y_ag^r)^{sx}b\mathrm{mod}q)$，$m=D_{K_1}(c)$，当且仅当 $\mathrm{KH}_{K_2}(m)=r$ 时接受 m。

Alice 对一组数据 (向量)$(m_1,m_2,\cdots,m_k)$ 的签密过程：随机选取 $x\in\{1,2,\cdots,p-1\}$，计算 $(K_1,K_2)=\mathrm{hash}(y_b^x\mathrm{mod}q)$，$c=(c_1,c_2,\cdots,c_k)=(E_{K_1}(m_1),E_{K_1}(m_2),\cdots,E_{K_1}(m_k))$，

$r=(r_1,r_2,\cdots,r_k)=(\mathrm{KH}_{K_2}(m_1),\mathrm{KH}_{K_2}(m_2),\cdots,\mathrm{KH}_{K_2}(m_k))$， $s=(s_1,s_2,\cdots,s_k)=(x/(r_1+x_a)\mathrm{mod}p,x/(r_2+x_a)\mathrm{mod}p,\cdots,x/(r_k+x_a)\mathrm{mod}p)$，密文为 (c,r,s)。

Bob 对密文 (c,r,s) 的解签密过程：计算 $(K_1,K_2)=\mathrm{hash}((y_ag^r)^{sx}\mathrm{mod}q)$，$m_i=D_{K_1}(c_i)$，$i=1,2,\cdots,k$，当且仅当对所有的 $i\in\{1,2,\cdots,k\}$，都有 $\mathrm{KH}_{K_2}(m_i)=r_i$ 时，接受 $(m_1,m_2,\cdots,m_k)$

广播式签密方案参见文献 [10]，可用类似于上面的方法把它修改成一次可签密多个数据的广播式签密方案。

4 拍卖方案

在我们的方案中有一个可信的注册中心 T，负责投标人及拍卖代理的注册，公布投标价位，并在最后确定中标人的身份；有 m 个拍卖代理，分别为 $P_1,P_2,\cdots,P_m$，他们负责接收投标人的标书，并确定出每一轮的最高投标价；有 n 个投标人，分别为 $B_1,B_2,\cdots,B_n$。他们各有自己的公开钥和私钥。每一轮拍卖有 k 个公开价位 $w_1,w_2,\cdots,w_k$。

假设诚实的拍卖代理至少为 t 个，且 $m-t$ 很小 (以防止少数几个拍卖代理串通而操纵拍卖)。

4.1 系统公开参数

p,q 表示足够大的素数 $(|q|\geq 512,p\geq 144)$，其中 $p|q-1$；g 表示 $\mathrm{GF}(q)$ 中的一个 p 阶元素；hash 表示输出至少为 128bit 的抗碰撞 hash 函数，KH 表示有密钥控制的单向 hash 函数；E，D 表示一个对称密码体制的加解密算法。

注册中心 T 的私钥为 $x_T\in\{1,2,\cdots,p-1\}$，相应的公钥为 $y_T=g^{x_T}(\mathrm{mod}q)$。$T$ 随机选取 $\mathrm{GF}(q)$ 上的 t 维非零维列向量 $\alpha=(a_1,a_2,\cdots,a_t)^T$，及 α-型秘密共享矩阵 G。公开自己的公钥、公钥证书、α、G。

4.2 注册

投标人注册：每一投标人 B_i 有私钥 $x_i\in\{1,2,\cdots,p-1\}$，公钥 $y_i=g^{x_i}$。B_i 把自己的公钥，公钥证书，及身份信息 ID_i 发送给 T，T 验证证书，若有效，则随机选取 $r_1,r_2,\cdots,r_k$，计算出与 B_i 的身份信息相关的身份识别号 $\mathrm{ID}_i^1,\mathrm{ID}_i^2,\cdots,\mathrm{ID}_i^k\in\mathrm{GF}(q)$，其中 $\mathrm{ID}_i^l=\mathrm{hash}(r_l,y_i^{x_T}(\mathrm{mod}q),\mathrm{ID}_i)$ (用 "," 表示级连)。这些身份号依次相应于 k 个公开的价位。然后 T 对这些身份识别号进行签密：随机选取 $x\in\{1,2,\cdots,p-1\}$，计算 $(K_1,K_2)=\mathrm{hash}(y_i^x\mathrm{mod}q)$，计算 $c=(c_1,c_2,\cdots,c_k)=(E_{K_1}(\mathrm{ID}_i^1),E_{K_1}(\mathrm{ID}_i^2),\cdots,E_{K_1}(\mathrm{ID}_i^k))$，$r=(r_1,r_2,\cdots,r_k)=(\mathrm{KH}_{K_2}(\mathrm{ID}_i^1),\mathrm{KH}_{K_2}(\mathrm{ID}_i^2),\cdots,\mathrm{KH}_{K_2}(\mathrm{ID}_i^k))$，$s=(s_1,s_2,\cdots,s_k)=(x/(r_1+x_i)\mathrm{mod}q,x/(r_2+x_i)\mathrm{mod}q,\cdots,x/(r_k+x_i)\mathrm{mod}q)$。最后再把 (c,r,s) 发给 B_i，同时 T 把 B_i 的公钥，公钥证书，身份信息以及 $\mathrm{ID}_i^1,\mathrm{ID}_i^2,\cdots,\mathrm{ID}_i^k$ 存入投标人档案库中。收到 (c,r,s) 后，B_i 对签密进行解密和验证，若合法，则接受 $\mathrm{ID}_i^1,\mathrm{ID}_i^2,\cdots,\mathrm{ID}_i^k$ 作为他在投标中的身份识别号，否则向注册中心返回收到的消息不合法的信息，并再次申请注册。

假定对任意 $l\in\{1,2,\cdots,k\}$ 及每一 $j\in\{1,2,\cdots,n\}$，两个以上的 ID_i^l 之和不等于任何一个 ID_j^l。

拍卖代理注册：设有 m 个拍卖代理，分别为 $P_1,P_2,\cdots,P_m$。每一拍卖代理 P_j 把自己的公钥 $z_j(=g^{u_j}\mathrm{mod}q,u_j\in\{1,2,\cdots,p-1\}$ 为相应的私钥) 公钥证书及身份信息发送给 T，T 验证后存入拍卖代理档案库中。T 公布 P_j 的公钥、公钥证书及 P_j 的编号 j。这样所有拍卖代理和所有投标人都知道 P_j 对应着 G 的列向量 G_j，$j=1,2,\cdots,m$。

所有投标人和所有拍卖代理都可验证 G 是 α-型秘密共享矩阵。

4.3 投标向量的计算

对公布的 k 个价位 $w_1, w_2, \cdots, w_k$，投标人 B_i 如下计算自己的投标向量：如愿意出价 w_l，则在 $U(\mathrm{ID}_i^l) = \{(s_1, s_2, \cdots, s_t)：\ s_i \in \mathrm{GF}(q)，\ i = 1, \cdots, t$ 且 $a_1 s_1 + a_2 s_2 + \cdots + a_t s_t = ID_i^l\}$ 中随机地选取一个行向量 $S_i^l = (s_{i1}^l, s_{i2}^l, \cdots, s_{it}^l)$，计算 $(v_{i1}^l, v_{i2}^l, \cdots, v_{im}^l) = S_i^l G$，如他不愿出价 w_l，则在 $U(0) = \{(s_1, s_2, \cdots, s_t)：\ s_i \in \mathrm{GF}(q)，\ i = 1, \cdots, t$ 且 $a_1 s_1 + a_2 s_2 + \cdots + a_t s_t = 0\}$ 中随机地选取一个非零行向量 $S_i^l = (s_{i1}^l, s_{i2}^l, \cdots, s_{it}^l)$，计算 $(v_{i1}^l, v_{i2}^l, \cdots, v_{im}^l) = S_i^l G$。他给代理 P_j 的投标向量为 $(v_{ij}^1, v_{ij}^2, \cdots, v_{ij}^k)$, $j = 1, 2, \cdots, m$。

4.4 投标

每一投标人 B_i 把给拍卖代理 P_j 的投标向量 $(v_{ij}^1, v_{ij}^2, \cdots, v_{ij}^k)$ 经签密后发送给 P_j。

收到各投标人的投标向量后，每一拍卖代理 P_j 把收到的投标向量解签密后计算 $V_j = (\sum_{i=1}^n v_{ij}^1, \sum_{i=1}^n v_{ij}^2, \cdots, \sum_{i=1}^n v_{ij}^k)^T$，$j = 1, 2, \cdots, m$。并以签密方式把 V_j 向其他代理，投标人及注册中心 T 广播。

4.5 确定最高投标价

任意 t 个代理 $P_{i_1}, P_{i_2}, \cdots, P_{i_t}$ 可计算 $\beta = (b_1, b_2, \cdots, b_t)^T$ 使得 $(G_{i_1}, G_{i_2}, \cdots, G_{i_t})\,\beta = \alpha$，及 $(c_1, c_2, \cdots, c_k)^T = b_1 V_{i_1} + b_2 V_{i_2} + \cdots + b_t V_{i_t}$，$c_i \neq 0$ 表示有人对标价 w_i 投标。找出使 $c_l \neq 0$ 的最大 l，w_l 就是最高投标价。每一投标人可验证 w_l 不低于自己的投标价。

4.6 中标人的确定

设 w_l 为最高投标价，代理人向所有投标人公布 c_l 的值，代理把 c_l 发送给 T，T 对其进行验证，然后在投标人档案库中查找是否有 $ID_i^l = c_l$，就可知道投最高价的是否只有一人。若只有一人，就可宣布中标人身份，并公布中标人发送给拍卖代理的经过签密的投标向量至少 t 个；否则宣布进行下一轮投标，并公布新一轮的 k 个投标价。一旦中标人身份被公布，所有投标人都可验证。

若进行第 2 价位拍卖，只需在宣布中标人身份的同时也宣布次高投标价。

4.7 正确性的证明

对任意 t 个代理 $P_{i_1}, P_{i_2}, \cdots, P_{i_t}$，由于 $G_{i_1}, G_{i_2}, \cdots, G_{i_t}$ 是线性无关的 t 维列向量，线性方程组 $(G_{i_1}, G_{i_2}, \cdots, G_{i_t})\,X = \alpha$ 有唯一解 $X = (b_1, b_2, \cdots, b_t)^T$，于是

$$
\begin{aligned}
(V_{i_1}, V_{i_2}, \cdots, V_{i_t}) \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_t \end{bmatrix} &= \begin{bmatrix} \sum_{j=1}^n v_{ji_1}^1 & \sum_{j=1}^n v_{ji_2}^1 & \cdots & \sum_{j=1}^n v_{ji_t}^1 \\ \sum_{j=1}^n v_{ji_1}^2 & \sum_{j=1}^n v_{ji_2}^2 & \cdots & \sum_{j=1}^n v_{ji_t}^2 \\ \vdots & \vdots & \vdots & \vdots \\ \sum_{j=1}^n v_{ji_1}^k & \sum_{j=1}^n v_{ji_2}^k & \cdots & \sum_{j=1}^n v_{ji_t}^k \end{bmatrix} \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_t \end{bmatrix} \\
&= \begin{bmatrix} b_1 \sum_{j=1}^n v_{ji_1}^1 & +b_2 \sum_{j=1}^n v_{ji_2}^1 + & \cdots & +b_t \sum_{j=1}^n v_{ji_t}^1 \\ b_1 \sum_{j=1}^n v_{ji_1}^2 & +b_2 \sum_{j=1}^n v_{ji_2}^2 + & \cdots & +b_t \sum_{j=1}^n v_{ji_t}^2 \\ \vdots & \vdots & \vdots & \vdots \\ b_1 \sum_{j=1}^n v_{ji_1}^k & +b_2 \sum_{j=1}^n v_{ji_2}^k + & \cdots & +b_t \sum_{j=1}^n v_{ji_t}^k \end{bmatrix} \\
&= \begin{bmatrix} \sum_{j=1}^n \sum_{s=1}^t b_i v_{ji_s}^1 \\ \sum_{j=1}^n \sum_{s=1}^t b_i v_{ji_s}^2 \\ \vdots \\ \sum_{j=1}^n \sum_{s=1}^t b_i v_{ji_s}^k \end{bmatrix} = \begin{bmatrix} \sum_{j=1}^n \mathrm{ID}_j^1 \\ \sum_{j=1}^n \mathrm{ID}_j^2 \\ \vdots \\ \sum_{j=1}^n \mathrm{ID}_j^k \end{bmatrix} = \begin{bmatrix} c_1 \\ c_2 \\ \vdots \\ c_k \end{bmatrix}
\end{aligned}
$$

5 安全性和效率分析

5.1 安全性与公正性

首先，由于投标过程中使用了签密技术，使得投标人的标书既具有保密性又具有认证性。我们所采用的签密方案的安全性 [10] 及秘密分享方案的安全性 [11] 保证了在投标过程中标书不会被泄露，也不会发生一个投标人的标书被攻击者伪造或替换的情况。其次，在投标过程中我们通过一个安全的秘密分享方案把投标人的标书在 m 个拍卖代理间分享，在相互勾结的拍卖代理不超过 $t-1$ 个的假设下，任何拍卖代理都不能得知任何一个投标人的投标价，这又保证了标书对拍卖代理的保密性. 所用的秘密分享方案的安全性，还保证了即使某一投标人与至多 $t-1$ 个拍卖代理勾结也无法得到有关其他任何投标人的投标价的有用信息. 直到拍卖结束，除了中标人的身份和投标价被公开外，其余投标人的标书均得到了保密。

我们方案的公正性体现在以下几个方面：(1) 在诚实的拍卖代理不少于 t 个的前提下，即使 $t-1$ 个拍卖代理相互勾结，由于他们无法得知任何投标人的投标价，因而也不能操纵拍卖过程；(2) 任何投标人即使和 $t-1$ 个拍卖代理相互勾结，也不能得到有关其他投标人投标价的任何有用信息；(3) 在中标人的身份及其中标价公布后，任何投标人都可验证其正确性，而且，由于同时还公布了中标人的 t 个经过签密的投标向量，因此中标人无法抵赖自己是真正的中标者。

5.2 效率

文献 [8] 中的方案与我们的方案类似，所不同的是，文献 [8] 中采用的是基于多项式 Lagrange 插值法的 Shamir 秘密分享方案。现对两个方案的效率比较如下：

5.2.1 *计算投标向量及确定最高投标价所需的计算量*　对文献 [8] 中的方案，对每一轮投标，每一投标人在投标时，先要随机选择 k 个 $t-1$ 次多项式，每一个相应于一个投标价，他给每一个拍卖代理的投标向量是一个 k 维向量，为使轮数较少，k 不能太小，一般地，k 与 t 为同一个量级，其中每一个分量需计算一个 $t-1$ 次多项式在一个给定点的值，所用的乘法次数为 $t-1$ 次，因此计算每一个投标向量需要 $k(t-1)$ 次乘法，计算复杂度为 $O(t^2)$；确定最高投标价时，任何 t 个拍卖代理合作共使用 k 次 Lagrange 插值法，其中每次所需的乘除法次数约为 $2t^2-2t$ 次，总的乘除法次数约为 $2k(t^2-t)$，计算复杂度为 $O(t^3)$。拍卖代理确定最高价所采用的 Lagrange 插值法不能预计算，也不能进行简化，且在每轮拍卖中都得重新计算。

对于我们的方案，在每一轮投标中，每一投标人在投标时，先要根据自己的身份信息选择 kt 个随机数 (k 个 t 维向量)，计算给每一个拍卖代理的投标向量平均需要 kt 次乘法，计算复杂度为 $O(t^2)$；确定最高投标价时，任何 t 个拍卖代理合作解一个线性方程组，再计算两个 t 维向量的内积，约需 $t^3/3+t/3$ 次乘法，计算复杂度为 $O(t^3)$，然而，这里的主要过程——解一个线性方程组是可以进行预计算的，而且可根据实际情况大量地减少计算量.

在实际实现时，拍卖代理的个数不必很大. 为了使拍卖的轮数比较少，每轮拍卖所设定的价位数 k 不能太小. 如果取 $m=k=10$，$t=7$，则对文献 [8] 中方案而言，在每一轮投标中，每一投标人计算所有投标向量需 60 次乘法，t 个拍卖代理合作确定最高价需要 840 次乘除法；对我们的方案而言，在每一轮投标中，每一投标人计算所有投标向量需 70 次乘法，t 个拍卖代理合作确定最高价约需 117 次乘法. 可见，(1) 在每一轮投标中，文献 [8] 中方案在这两方面的计算量是我们的方案的 4.8 倍还多。(2) 如果在我们的方案中，对 t 个拍卖代理合作解线性方程组进行预计算，并根据 G 的具体取值把求解过程加以简化，则运算量可进一步减少。(3) 在整个拍卖过程中，文献 [8] 中的运算量随着拍卖轮数的增加呈线性增长，而在我们的方案中，主要的计算——解线性方程组，在各轮中都是一样的，因此，随着拍卖轮数的增加，我们的方案在效率上的优势就更加明显地体现出来了. 以上面的 m，k，t 的取值为例，若拍卖的轮

数为 5，且在每一轮中都是同一组拍卖代理确定最高投标价，则对文献 [8] 中的方案，每一投标人计算投标向量及 t 个拍卖代理确定各轮的最高投标价所需的计算量为 $5\times(60+840)=4500$ 次乘除法，而我们的方案只需 $329/3+5\times(70+7)\approx 495$ 次乘法。文献 [8] 中方案的计算量是我们的 9 倍还多。(4) 当由同一组拍卖代理负责拍卖多件商品时，文献 [8] 中方案的计算量呈线性增长，而我们的方案中，主要的计算量，即 $O(t^3)$ 级的计算量 (解线性方程组) 在所有商品的拍卖中只需计算一次，呈线性增长的只是 $O(t)$ 级的计算量。以上面的 m， k， t 的取值为例，若拍卖的轮数为 5，且同时拍卖 3 件商品，则在文献 [8] 中的方案中，每一投标人计算投标向量及 t 个拍卖代理确定各轮的最高投标价所需的计算总量为 $3\times5\times(60+840)=13500$ 次乘除法，而我们的方案只需 $329/3+3\times5\times(70+7)\approx 1265$ 次乘法，文献 [8] 中方案的计算量是我们的 10 倍还多。

5.2.2 *加解密及认证过程的效率* 在实际实现时，必须对投标向量进行加密和签名，否则拍卖将无法顺利而公正的进行。通常对信息同时进行加密和签名，要采用公钥体制，先以发送者的私钥对信息签名，再以接收者的公钥加密，这样做的效率是很低的。而签密把加密和签名有机地结合到了一起，使得原本要用两个逻辑步骤完成的过程可在一个逻辑步骤内完成，因而大大提高了效率。根据文献 [10] 的分析，我们所采用的签密算法要比通常的先签名后加密方法减少大约 58% 的计算量和 70% 以上的通信代价。就我们所知，签密是目前同时实现保密和认证的最简洁和最有效的方法。因此我们的方案在实现保密和认证方面的效率要比其它方案高。文献 [8] 中的方案没有这方面的措施，因而在实现时容易发生投标人的标书被篡改、替换、及中标人抵赖等问题。

6 小 结

我们以一个新的秘密分享方案和签密技术为基础，提出了一个安全、高效的多轮电子拍卖方案。我们的方案能够对除了中标人外的其他所有投标人的投标价提供保密。由于在秘密信息的传送中使用了签密技术，同时实现了保密和认证，因而大大提高了方案的效率。而且中标结果具有可公开验证性，增加了拍卖的透明度和公证性。另外，我们的方案亦可用于第二价位拍卖。

参 考 文 献

[1] M. Harkavy, H. Kikuch, J. D. Tygar, Electronic auctions with private bids. Proc. of the 3rd USENIX Workshop on Electronic Commerce, Massachusetts, USA, 1998, 61–74.

[2] Y. Imamura, T. Matsumoto, H. Imai, Electronic anonymous bidding schemes, The 1994 Symposium on Cryptography and Information Security, SCIS94-11B, Tokyo, 1994. 152–156.

[3] M. K. Franklin, M. K. Reiter, The design and implementation of a secure auction sever, IEEE Trans. on Software Engineering, 1996, 22(5), 302–312.

[4] M. G. James, M. V. Sethaput, Internet secure vickery auction, Network and Computer Security. MIT Fall 1997 Available at : http://sonnet.eas.harvard.edu/auction/.

[5] T. Nakanishi, H. Watanabe, T. Fujiwara, T. Kasami, An anonymous bidding protocol using undeniable signature, The 1995 Symposium on Cryptography and Information Security, SCIS95-B1.4, Tokyo, 1995, 106–112.

[6] M. Kudo, Secure electronic sealed-bid auction protocol with public key cryptography, IEICE Transactions on Fundamentals of Electronics, Communications and Computer Science, 1998, E81-A(1), 20–27.

[7] H. Kikuchi, S. Nakanishi, Registration-free protocol for anonymous auction, Proceedings of Computer Security Symposium'98, London, 1998, 243–248.

[8] H. Kikuchi, M. Harkavy, J. D. Tygar, Multi-round anonymous auction protocols, Proc. of the First IEEE Workshop on Dependable and Real Time E-Commerce Systems, New York, 1998, 62–69.

[9] K. Sakurai, S. Miyazaki, A bulletin-board based digital auction scheme with bidding down strategy, International Workshop on Cryptographic Techniques and Commerce(CryptTEC'99), HongKong, 1999, 180–187.

[10] Yuliang Zheng, Signcrypytion and its applications in efficient public key solutions, Proc. of Information Security Workshop(ISW'97), Berlin, 1997, 201–218.

[11] 马文平, 认证码理论研究, [博士学位论文], 西安电子科技大学, 1999.

AN EFFICIENT ELECTRONIC AUCTION SCHEME BASED ON SECRET SHARING AND SIGNCRYPTION

Zhang Futai* **　　Zhang Fangguo*　　Wang Yumin*

*(*National Key Laboratory on ISN, Xidian University, Xi'an* 710071, China)

**(*Department of Computer Science, Shaanxi Normal Univ., Xi'an* 710062, China)

Abstract　A secure and efficient multi-round electronic auction scheme is presented using a new secret sharing scheme and the technique of signcryption. In this scheme, all bidder's bidding values are always kept secret except for the winner's. The technique of signcryption is used to ensure both the secrecy and authenticity of messages so that the efficiency is greatly improved. Moreover this scheme is also suitable for second-price auction.

Key words　Secret sharing scheme, Electronic auction, Signcryption, Bidding

张福泰:　男, 1965 年生, 副教授, 研究方向为密码学及电子商务.
张方国:　男, 1973 年生, 博士生, 研究方向为密码学及电子商务.
王育民:　男, 1936 年生, 教授, 博士生导师, 研究方向为通信安全及电子商务.