可公开验证的安全电子拍卖方案

杨加喜[1]，李 磊[1,2]，王育民[1]

(1. 西安电子科技大学综合业务网国家重点实验室 西安 710071; 2. 郑州大学信息工程学院 郑州 450052)

【摘要】在大多数电子拍卖方案中，如果第三方勾结，那么投标者的标价不再保密。在任何情况下保持标价的秘密性是非常重要的，它们很可能是投标者重要的商业秘密。该文提出了一种可公开验证的安全电子拍卖，结合零知识证明协议，使拍卖方案可公开验证并达到最小泄漏。该方案泄漏的只是中标价，其余标价及其相互关系在任何勾结情况下都是保密的，而且，标价的正确性可以公开验证。该方案的效率远远高于最近Brandit提出的方案。

关 键 词 电子拍卖; 多方计算; 秘密分享; 零知识证明

中图分类号 TN918.1 文献标识码 A

Publicly Verifiable Secure Electronic Auction

YANG Jia-xi[1]，LI Lei[1,2]，WANG Yu-min[1]

(1. National Key Lab. of Integrated Service Networks, Xidian University Xi'an 710071;

2. School of Information Engineering, Zhengzhou University Zhengzhou 450052)

Abstract In the most of existing electronic auctions, the bidders' bids no longer remain confidential if the third parts collude. However, keeping the bids secret in any case is vital to the bidders because these evaluations may be their critical commercial secrets. This paper proposes a publicly verifiable secure electronic auction meeting such requirements. The only leakage is the selling price while the other bids and their relation keep confidential in any collusion. The scheme is more efficient than the recently proposed scheme due to Brandit.

Key words electronic auction; multiparty computation; secret sharing; zero-knowledge proof

电子拍卖是现实中拍卖的电子化，它是电子商务的一项基本业务。Internet网上有许多电子拍卖系统，如Yahao!、e-Bay.com等。然而这些拍卖系统由于缺少必要的安全机制等原因，降低了人们对这些系统的诚信度。密封式拍卖要求每个拍卖者秘密地提交他们的标价，能更有效地决定拍卖价格并具有秘密性，因而是一种研究较多的拍卖。文献[1-5]研究的电子拍卖方案利用的技术有：位承诺、Hash函数、多方的秘密计算等。网上较大的拍卖商e-Bay也引入了密封式电子拍卖。

一个安全的电子拍卖系统必须具有公平竞争的机制，中标者的标价具有有效性，必须能杜绝中标者的违约。为了防止投标者与拍卖行或卖方合谋等操纵，使投标者的隐私在拍卖过程中和拍卖后能够得到保密，必须进行匿名投标。一个密封式电子拍卖系统应满足下列要求：(1) 公平性，指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) 不可否认性，投标者投标后不能否认其投标；(3) 不可伪造性，投标者的投标不能被伪造；(4) 可证实性，可公开证明中标者标价的合法性；(5) 标价保密性，投标者的标价必须保密；(6) 不相关性，在揭标过程中投标和投标者不能对应起来；(7) 投标者匿名，投标参与者的身份(包括中标者的身份和未中标者的身份)必须保密。

本文提出一个安全的且可公开验证的电子拍卖协议，使得中标价的正确性可公开验证，这对防止舞弊是至关重要的。如拍卖行觉得计算出来的中标价不够高，可能宣布一个高于所有人投标的中标价使本次拍卖失败而没有人能够发现。因此，在拍卖中，任何勾结的情况下保持标价的秘密性和中标价的可公开验证性是本文要解决的问题，同时使拍卖的效率尽可能的高。

收稿日期：2006 – 12 – 28；修回日期：2007 – 05 – 16

基金项目：国家自然科学基金(60473027).

作者简介：杨加喜(1981 –)，男，博士生，主要从事密码学、电子商务安全方面的研究；王育民(1936 –)，男，教授，博士生导师，主要从事编码理论、密码学、信息安全主面的研究.

1　符号说明和预备知识

本文用到的一些记号和组成模块如下：〈g〉表示由g生成的循环群，G是一个高阶循环群，〈g〉=〈h〉$\subseteq G$，〈g〉中离散对数是困难的；H：$\{0,1\}^* \to \{0,1\}^l$是一个密码学杂凑函数，l是一个安全参数；a和b的级联表示为$a\|b$；zkp$\{x|R(x)\}$表示零知识证明示证者知道秘密x使得关系$R(x)$为真；Commit(x)表示对秘密x的承诺；Alice知道秘密x可以按如下方式向Bob承诺，Alice选取随机整数r并向Bob发送$C=g^x h^r$作为对x的承诺，Alice不可能找到$x_1 \neq x_2$使得Commit(x_1,r_1)=Commit(x_2,r_2)，除非它知道$\log_g h$。Bob即使有无限的计算能力也不可能从C提取任何有用的信息。这是一个陷门承诺，即如果Alice知道$\log_g h$则可以任意欺骗Bob[6]。本文将用到文献[7-9]的零知识证明：

$$\text{zkp}\{x|y=g^x\}$$

$$\text{zkp}\{x, r|y=g^x h^r \wedge y_1 = g_1^x\}$$

$$\text{zkp}\{x, r|y=g^x h^r \wedge x \in \{a_1,a_2,\cdots,a_t\}\}$$

考虑标价的编码方法。假定有n个投标者，他们所投的标价在$\{1,2,\cdots,v\}$当中。设投标者i投的标价为b_i $(1 \leqslant i \leqslant n, 1 \leqslant b_i \leqslant v)$。为了有效地计算出中标价，即最高价或最低价(只考虑最高价，最低价可以完全类似进行)，标价b_i $(1 \leqslant i \leqslant n, 1 \leqslant b_i \leqslant v)$编码成一个向量$\boldsymbol{\beta}_i = (0,\cdots 0,1,0,\cdots,0) = (x_{i1}, x_{i2}, \cdots, x_{iv})$，其中，第$b_i$个分量为1，其余分量为0，这些向量的和表示为：

$$\gamma = (\gamma_1,\gamma_2,\cdots,\gamma_v) = \sum_{i=1}^{n} \boldsymbol{\beta}_i = (\sum_{i=1}^{n} x_{i1}, \sum_{i=1}^{n} x_{i2}, \cdots, \sum_{i=1}^{n} x_{iv})$$

假定$n(t) = \#\{b_i | b_i \geqslant t\}$为投标者中其所投标价大于等于$t$的人数。假设这些投标者投的标价是不同的，那么$n(j)$关于$j$单调递减且有唯一的$j$满足$n(j)$=1。如果参与者能够合作测试是否有$n(j) = 1$而不泄漏进一步的信息，那么通过从$v$到1重复测试这一等式就可以安全地计算出投标者投的最大标价。

要求n个参与者能安全测试$\pm x_1 \pm x_2 \pm \cdots \pm x_n = a$而不泄漏进一步的信息，其中$x_i$ (i=1,2,$\cdots$,n)是参与者i的秘密输入，a是一个已知的整数，称这个问题为推广的匹配协议，它是匹配协议(n=2)的推广[10]。本文给出这个推广匹配协议的一个有效设计，并结合已知的零知识证明使协议具有可公开验证性。

(1) 对i=1,2,$\cdots$,n，参与者i公布$y_i = g^{x_i} h^{r_i}$作为对x_i的承诺。然后任何人都可以计算：

$$z_0 = y_1^{\pm 1} \cdots y_n^{\pm 1} g^{-a} = g^{\pm x_1 \pm \cdots \pm x_n - a} h^{\pm r_1 \pm \cdots \pm r_n}$$

(2) 参与者1随机选取整数s_1，公布：

$$z_1 = z_0^{s_1}, v_1 = h^{s_1}, \text{zkp}\{s_1 | z_1 = z_0^{s_1} \wedge v_1 = h^{s_1}\}$$

(3) 对i=2,3,$\cdots$,n，参与者i随机选择s_i，公布：

$$z_i = z_{i-1}^{s_i}, v_i = v_{i-1}^{s_i}, \text{zkp}\{s_i | z_i = z_{i-1}^{s_i} \wedge v_i = v_{i-1}^{s_i}\}$$

(4) 对i=1,2,$\cdots$,n，参与者i公布：

$$u_i = v_n^{\pm r_i}, \text{zkp}\{r_i | y_i = g^{x_i} h^{r_i} \wedge u_i = v_n^{\pm r_i}\}$$

(5) 如果$z_n = u_1 u_2 \cdots u_n$，返回1；否则返回0。如果涉及的零知识证明是安全的，那么每个欺骗者都将被检测到并被逐出协议。注意：

$$z_n = g^{(\pm x_1 \pm x_2 \pm \cdots \pm x_n - a)s_1 \cdots s_n} h^{(\pm r_1 \pm r_2 \pm \cdots \pm r_n)s_1 \cdots s_n}$$

$$u_1 u_2 \cdots u_n = h^{(\pm r_1 \pm r_2 \pm \cdots \pm r_n)s_1 s_2 \cdots s_n}$$

因此，返回值1表示$\pm x_1 \pm \cdots \pm x_n = a$；返回值0表示$\pm x_1 \pm \cdots \pm x_n \neq a$，输出显然是可以公开验证的。考虑在勾结攻击下，假设攻击者完全控制了n–1个参与者。如参与者i=2,3,$\cdots$,n，并试图提取参与者1的秘密输入。也就是，攻击者知道了$x_2, x_3, \cdots, x_n$和$s_2, s_3, \cdots, s_n$，希望提取x_1。攻击者能够计算$w = g^{(\pm x_1 \pm \cdots \pm x_n - a)s_1 s_2 \cdots s_n}$，其中$x_1$和$s_1$未知。设$b = \pm x_2 \pm x_3 \pm \cdots \pm x_n - a$，$c = s_2 s_3 \cdots s_n$。但是即使$x_1$所在的范围非常有限，攻击者从$w = g^{(b \pm x_1)cs_1}$中提取$x_1$也是不可能的。协议要求$O$(1)次模指数运算和$O$(1)轮通信。

上述协议记为：

$$EQ\{x_1, x_2, \cdots, x_n | y_1 = g^{x_1} h^{r_1} \wedge \cdots \wedge y_n = g^{x_n} h^{r_n} : (\pm x_1 \pm x_2 \pm \cdots \pm x_n, a)\}$$

2　电子拍卖协议

一个拍卖包括四个实体：注册中心(registration center)、拍卖商(auctioneer)、卖主(vendor)和投标者(bidder)。注册中心负责投标者参加投标注册；拍卖中心包括拍卖人和组织拍卖的人；卖主为想要卖商品的人；投标者为想得到商品的人。

假设投标者$i \in \{1,2,\cdots,n\}$有唯一认证过的签字公钥表示其身份。系统中拍卖商不参与计算中标价(相当于没有拍卖商)，只需监视拍卖过程和维护将涉及的公告牌，所有的数据都将发送到公告牌上。设允许的标价空间为$\{p_1, p_2, \cdots, p_v\}$，其中$p_1 < p_2 < \cdots < p_v$，这可以表示为$\{1,2,\cdots,v\}$。为了简化，对$i$=1,2,$\cdots$,$n$，假定不同投标者的$b_i$是不同的。

初始化：假设系统所有安全参数都已经由正确的程序产生，关于拍卖商品的信息、拍卖时间、投标规则和交易规则都已经公布在公告牌上。

注册：投标者公布他们的公钥和公钥证书到公告牌上，所有合法的公钥形成公钥列表L。

注册结束后，每一个合法的投标者都有一对公/私钥(Z_i, x_i)。投标者i按如下方式广播消息m：

$(m\|\text{phase}\|\text{No.}\|\text{sign}_{Z_i}(H(m\|\text{phase}\|\text{No.})))$。其中，$\text{sign}_{Z_i}$是以$Z_i$为验证公钥的数字签名；phase表示投标、开标和交易的时间片；No.在一定时间片内发送消息的序列号。该方式保证了数据的完整性，没有人能够篡改、伪造或重放一条消息而不被发现。在下面的描述中，为了简化将省去签字。

投标：投标者i选取他的秘密标价$b_i \in \{1,2,\cdots,v\}$并编码为：$\beta_i=(0,\cdots,0,1,0,\cdots,0)=(x_{i1},x_{i2},\cdots,x_{iv})$，(其中，第$b_i$个分量为1，其余分量为0)。对$j\in\{1,2,\cdots,v\}$，投标者$i$计算$y_{ij}=g^{x_{ij}}h^{r_{ij}}$，公布$(y_{i1},y_{i2},\cdots,y_{iv})$作为标书的公开形式。并用零知识方式证明标价编码是正确的：

$$\text{zkp}\{x_{ij}\,|\,y_{ij}=g^{x_{ij}}h^{r_{ij}}\wedge x_{ij}\in\{0,1\}\},\ j\in\{1,2,\cdots,v\}$$

$$\text{zkp}\{b_i,u_i\,|\,\prod_{j=1}^{v}y_{ij}^{\,2^j}=g^{2^{b_i}}h^{u_i}\wedge b_i\in\{1,2,\cdots,v\}\}$$

开标：

1) 计算中标价

设$z_{ik}=\prod_{j=k}^{v}y_{ij}=g^{\sum_{j=k}^{v}x_{ij}}h^{\sum_{j=k}^{v}r_{ij}}=g^{m_{ik}}h^{n_{ik}}$，其中$k\in\{1,2,\cdots,v\}$。

(1) 设置$k:=v$；

(2) 如果$\text{EQ}\{m_{1k},m_{2k},\cdots,m_{nk}\,|\,z_{1k}=g^{m_{1k}}h^{n_{1k}}\wedge\cdots\wedge z_{nk}=g^{m_{nk}}h^{n_{nk}}:(m_{1k}+m_{2k}+\cdots+m_{nk},1)\}=1$转(4)；否则$k:=k-1$；

(3) 重复(2)直到：

$$\text{EQ}\{m_{1k},\cdots,m_{nk}\,|\,z_{1k}=g^{m_{1k}}h^{n_{1k}}\wedge\cdots\wedge z_{nk}=g^{m_{nk}}h^{n_{nk}}:(m_{1k}+\cdots+m_{nk},1)\}=1$$

(4) 输出中标价k，中止程序。

2) 诚实性证明

投标者i公布$\text{zkp}\{m_{ik}\,|\,z_{ik}\,g^{-1}=h^{m_{ik}}\}$或$\text{zkp}\{m_{ik}\,|\,z_{ik}=h^{m_{ik}}\}$。

如果投标者i出示$\text{zkp}\{m_{ik}\,|\,z_{ik}\,g^{-1}=h^{m_{ik}}\}$，那么$\sum_{j=k}^{v}x_{ij}=1$，说明他投了最高标价；如果出示的是$\text{zkp}\{m_{ik}\,|\,z_{ik}=h^{m_{ik}}\}$，那么$\sum_{j=k}^{v}x_{ij}=0$，说明他投的标价低于中标价。由此确定出中标者身份。

3 协议分析

由于不同投标者的标价是不同的，所以$m_{1k}+m_{2k}+\cdots+m_{nk}$关于$k$严格下降，因此存在唯一的$k$使得$m_{1k}+m_{2k}+\cdots+m_{nk}=1$，$k$就是最高价位。上面的开标算法从$v$到1搜索中标价，在最坏的情况下需要$v$次调用基本的相等性测试。因此正确性是显然的。

由于方案中的承诺和零知识证明不会泄漏秘密标价的任何信息，而用到的相等性测试它只是判断是否有$m_{1k}+m_{2k}+\cdots+m_{nk}=1$，而不会泄漏进一步的信息，因此开标后计算出来的只是中标价，其余标价的保密性仍然保持，而且即使其余投标者勾结也不可能知道投标者i的秘密标价，中标者的标价不会泄漏。因此方案是抗勾结的。

由于每一条消息后面都有相应的数字签字(在简化的方案描述中省略了)，投标者不能否认他所投的标书或发送的数据。协议最后要求每一个投标者以零知识的方式证明他中标或者没有中标，不合作的投标者可能在最后一个阶段离开协议。但是，他们的身份容易被确定并将失去信用。另外，只要中标者提供了证明，拍卖仍然是有效的。而如果中标者不提供证明，其他$n-1$个投标者可以通过证明自己没有中标找出中标者。

最后，本文分析了方案的效率，并与具有同样安全属性的文献[11]方案比较。文献[11]也没有拍卖行，采用了可公开验证的(n,n)秘密分享实现可公开验证性，每一个投标者将其标价分成n个份额分发给n个投标者，阻止勾结起来获得秘密标价的信息。$|G|$表示G中元素的二进制长度。在本文的方案中，每一个投标者需要的通信轮数为$O(v)$，发送数据需要的带宽为$O(v|G|)$，模指数运算的次数为$O(v)$，而在文献[11]方案中，每一个投标者需要的通信轮数为$O(n)$，发送数据需要的带宽为$O(n^2v|G|)$，模指数运算的次数为$O(n^2v)$，显然本文方案的效率远远高于文献[11]方案，特别是计算和带宽的消耗上要少得多。

4 结 论

本文考虑了密封式电子拍卖中，在任何勾结的情况下保护投标者标价的秘密性，并使中标价的正确性可以公开验证，目前绝大多数拍卖方案都达不到这样的安全要求，然而这样的拍卖设计是必要的，特别是在重大的商业拍卖中，参与竞拍的商家希望在任何时候都不会泄漏他们的商业秘密。本文提出的拍卖方案：(1) 在任何勾结情况下保证标价的秘密性；(2) 可以公开验证中标价；(3) 不泄漏中标价以外标价之间的关系；(4) 中标者身份保持匿名。分析表明本文的方案是实用的，效率远远高于文献[11]方案。

(下转第46页)

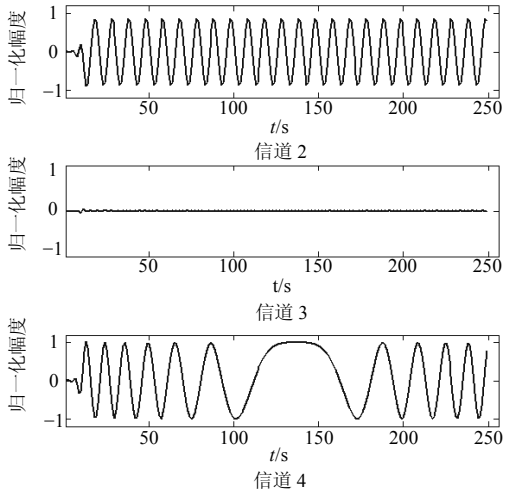

图6 输出信号波形

4 结束语

本文将WOLA滤波器组引入信道化接收机，分析了多相DFT滤波器组与WOLA滤波器组的内在联系，证明WOLA滤波器组是多相DFT滤波器组的一种推广形式，应用于信道化接收机时，具有参数设计灵活、计算复杂度低、硬件实现效率高等优点。WOLA滤波器组结构和多相DFT滤波器组结构一样高效，但没有后者的严格约束条件，是多相DFT滤波器组结构的一种推广形式，多相DFT滤波器组同样也可应用于短时傅里叶变换。

参 考 文 献

[1] HARRIS F, DICK C, RICE M. Digital receivers and transmitters using polyphase filter banks for wireless communications[J]. IEEE Transactions on Microwave Theory and Techniques, 2003, 51(4):1395-1412.
[2] CROCHIERE R E, RABINER L R. Multirate digital signal processing[M]. [S.l.]: Prentice-Hall Inc, 1983.
[3] BRENNAN R, SCHNEIDER T. An ultra low-power DSP system with a flexible filterbank[C]//The Thirty-Fifth Asilomar Conference on Signals, Systems and Computers. Pacific Grove, CA: IEEE, 2001: 809-813.
[4] BRENNAN R, SCHNEIDER T. A flexible filterbank structure for extensive signal manipulations in digital hearing aids[C]//Proc of International Symposium on Circuits and Systems. Monterey, CA: IEEE, 1998: 569-572.
[5] NIELS, P TANJA K, TRUONG Q. A general formulation of modulated filter banks[J]. IEEE Transactions on Signal Processing, 2004, 47(4): 986-1002.
[6] 刘开文. 基于短时综合相加法的语音盲信号分离的研究及其DSP实现[D]. 成都: 四川大学, 2004.
[7] 周良臣, 吕幼新. 基于DFT滤波器组的宽带信号谱分析方法[J]. 信号处理, 2004, 20(4): 217-220.
[8] 蒋宗明, 唐 斌, 吴 伟. 基于DFT滤波器组的多信号高效数字下变频[J]. 电子科技大学学报, 2005, 34(6): 743-746.

编 辑 税 红

(上接第26页)

参 考 文 献

[1] FRANKLIN M, REITHER M. The design and implemention of a secure auction service[J]. IEEE Trans on Software Engineering, 1996, 22(5): 302-312.
[2] MU Y, VARADHARAJAN V. An internet anonymous auction scheme[C]// Lecture Notes in Computer Science. Berlin: Springer-Verlag, 2001: 171-182.
[3] 黄秀姐, 林 群, 王燕鸣. 基于短群签名的安全电子拍卖方案[J]. 中山大学学报(自然科学版), 2006, 45(6): 21-25.
[4] SCHNOORR C C, CHANG Y F. Enhance anonymous auction protocols with freewheeling bids[C]//Proceedings of the 20th International Conference on Advanced Information Networking and Application. Austria:Vienna, 2006: 353-358.
[5] LIAW H T, JUANG W S, LIN C K. An electronic online bidding auction protocol with both security and efficiency[J]. Applied Mathematics and Compution, 2006, 174(2): 1487-1497.
[6] FUJISAKI E, OKAMOTO T. Statistical zero knowledge protocols to prove modula polynomial relations[C]// Proceedings of Cryptology-CRYPTO'97. Berlin: Springer-Verlag, 1997: 16-30.
[7] SCHNORR C. Efficient signature generation by smart cards[J]. Journal of Cryptology, 1991, 4(3): 161-174.
[8] CHAUM D, PEDEERSEN T R. Wallet databases with observers [C]// Advances in Cryptology-CRYPTO'92. Berlin: Springer-Verlag, 1993:89-105.
[9] WU Q, ZHANG J, WANG Y. Practical t-out-n oblivious transfer and its application[C]// ICICS'03. Berlin: Springer-Verlag, 2003.: 226-237.
[10] 伍前红, 张键红, 王育民. 一个高效的匹配协议[J]. 通信学报, 2004, 25(8): 139-145.
[11] BRANDIT F. Secure and private auctions without auctioneers [R]. Technical Report FKI-245-02. Institute fü Informatik, Technische University Muhen, 2002.

编 辑 张 俊