第 38 卷 第 4 期
Vol.38 No.4

计 算 机 工 程
Computer Engineering

2012 年 2 月
February 2012

• 博士论文 •

文章编号：1000—3428(2012)04—0004—03 文献标识码：A 中图分类号：TP311

一种应用于双重数字签名的电子拍卖方案

王秀利，王 萌

(中央财经大学信息学院，北京 100081)

摘 要：针对电子拍卖中存在的身份匿名性等安全问题，基于秘密分享思想，提出一种安全高效的电子拍卖方案。应用双重数字签名，保证投标过程中参与者之间的信息传输安全。投标者采用临时身份投标，标价不直接发送给其他参与者。拍卖服务器根据单调递增函数所计算出的投标值判断中标者，若与注册中心计算结果相符，则投标结果有效。安全性分析结果表明，该方案满足电子拍卖的各项安全性要求，且计算简便、运算效率高。

关键词：电子拍卖；双重数字签名；秘密分享；可信第三方；单调递增函数；投标值

Electronic Auction Scheme Applied for Double Digital Signature

WANG Xiu-li, WANG Meng

(School of Information, Central University of Finance and Economics, Beijing 100081, China)

【Abstract】Aiming at the safety problems of identity anonymity in electronic auction, a safe and efficient scheme is designed based on secret sharing idea, which uses double digital signature to guarantee the safe information transfer among the parties. The bidder is covered by a temporary identity and the bid is send to others indirectly. The auction server can speculate the winner by arranging the figures calculated by a monotone increasing function. If the results from the auction server and the register manager are the same, the winner can be declared. Safety analysis result shows that the proposed scheme is not only secure but also simple and efficient.

【Key words】electronic auction; double digital signature; secret sharing; trusted third party; monotone increasing function; bid value

DOI: 10.3969/j.issn.1000-3428.2012.04.002

1 概述

电子拍卖是一项发展迅速的电子商务业务。电子拍卖方案一般由拍卖参与者(投标者、卖方和拍卖服务器)、拍卖规则和仲裁机构组成[1]。秘密分享思想是将一个秘密分解为多个子秘密，分别由多个参与者控制，只有把子秘密放在一起时才能揭示出秘密[2]。双重数字签名技术为解决电子拍卖的安全问题提供了一个有效的方法[3]。

本文将标价看作秘密，利用单调递增函数将标价转化为投标值，应用双重数字签名保证三方之间信息的安全传输。

2 基于双重数字签名的电子拍卖方案

2.1 方案设计

本文方案引入可信第三方(注册中心)，采取集中式最高价拍卖[1]。在拍卖过程中，只有注册中心知道投标者的真实身份(投标者的公钥)[4]。标价不直接发送给拍卖服务器和注册中心。拍卖结果由拍卖服务器和注册中心共同计算。满足电子拍卖方案所需的安全性要求[5]。

2.2 符号说明

对符号说明如下：

$B_i(i=1,2,\cdots,n)$：n 个投标者；

$b_i(i=1,2,\cdots,n)$：第 i 个投标者的标价；

$V_i(i=1,2,\cdots,n)$：第 i 个投标者的投标值；

$\xi_i(i=1,2,\cdots,n)$：第 i 个投标者产生投标值的随机参数；

PK_A：A 的公钥(Public Key)；

SK_A：A 的私钥(Secret Key)；

$EP_A(M)$：用 A 的公钥加密明文 M；

$DS_A(S)$：用 A 的私钥解密密文 S；

$ES_A(M)$：用 A 的私钥加密明文 M；

$DP_A(S)$：用 A 的公钥解密密文 S；

DDS_A：A 的双重数字签名；

VN_A：A 发出的中标通知(Victory Notice)。

2.3 具体步骤

2.3.1 初始化

初始化流程如下：

(1)拍卖服务器 AM(Auction Manager)向注册中心 RM(Register Manager)(其公钥对外公开)提交此次拍卖活动的相关信息 AI(Auction Information)和请求注册中心参与监督本次拍卖活动的信息 AS(Apply to be Supervised)，并用自己的私钥 SK_{AM} 对信息加密，形成 $ES_{AK}(AI, AS)$。同时，提交自己的公钥 PK_{AM}，以便 RM 检查身份和解密信息。以上全部信息用 RM 的公钥加密后形成 $EP_{RM}(PK_{AM}, ES_{AK}(AI, AS))$发送给 RM。

(2)RM 接收到信息后，解密信息，并检查 AM 的公钥 PK_{AM}，确认 AM 身份的合法性。再利用 PK_{AM} 解密剩余信息，检查拍卖信息 AI 和监督申请 AS 是否真实可信。

(3)检查通过后，RM 按照 RSA 加密体制为此次拍卖随机选择一对大素数 p 与 q，且大整数 $t=p\times q$，随后 RM 销毁 p 和 q。计算 t 的欧拉函数值 $T=\varphi(t)=(p-1)\times(q-1)$，则 T 为此次拍卖活动的关键参数。RM 将关键参数 T 用自己的私钥签名并用 AM 的公钥加密后发送给 AM，作为同意参与监督此次拍

基金项目：国家自然科学基金资助项目(60970143,70872120)；教育部科学技术研究基金资助重点项目(109016)；北京市自然科学基金资助项目(4112053, 9092014)；北京市教育委员会共建专项基金资助项目；中央财经大学“211 工程”三期重点学科建设基金资助项目；中央财经大学科研创新团队支持计划基金资助项目

作者简介：王秀利(1977－)，男，博士、CCF 会员，主研方向：网络与信息安全，电子商务；王 萌，本科生

收稿日期：2011-08-03 **E-mail：**xlwang.cufe@gmail.com

卖的证据。

(4)*RM* 在含有随机参数的单调递增函数库中随机选择一个函数 $F(x)$作为本次拍卖活动中投标值的计算公式。

(5)*AM* 接收 *RM* 发送的信息，保存关键参数 *T*，并公开发布拍卖信息 *AI*、公钥 PK_{AM} 关键参数 *T*。

初始化流程如图 1 所示。

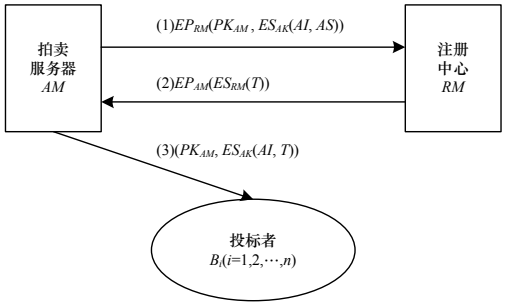

图 1　初始化流程

2.3.2　投标者注册

投标者注册流程如下：

(1)投标者 $Bi(i=1,2,\cdots,n)$向注册中心提交自己的公钥 PK_{Bi} 进行注册，并发送所要参加拍卖的关键参数 *T*。

(2)*RM* 在检查投标者身份和资格都合格后，根据关键参数 *T*，随机选择一个大的正整数 *ei*，使 *ei* 满足小于 *t*，且与 *T* 互素。然后计算 *ei* 的乘法逆元 d_i，即 $di\times ei=1 \bmod T$。则二元组(ei, T)、(di, T)构成投标者 *Bi* 在投标过程所使用的临时密钥对，选择(ei, T)为临时公钥，(di, T)为临时私钥，其中，*ei* 作为投标者 *Bi* 的拍卖身份。

(3)*RM* 将(ei, di)和投标值计算公式 $F(x)$加密后发送给 *Bi*。

(4)注册完毕以后，*RM* 将随机数表 $ei(i=1,2,\cdots,n)$发送给 *AM*，供 *AM* 在投标过程中检查投标者身份的合法性。

投标者注册流程如图 2 所示。

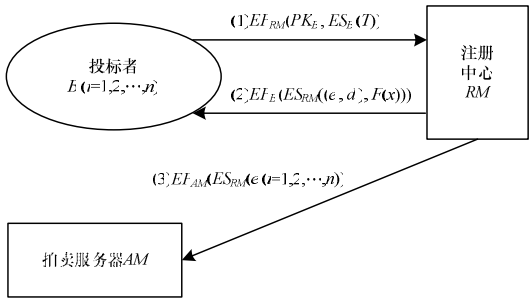

图 2　投标者注册流程

2.3.3　标价提交

标价提交流程如下：

(1)投标者 B_i 随机生成参数 ξ_i，将标价 *bi* 代入公式 $F(x)$计算投标值 *Vi*。

(2)计算投标值 *Vi* 和参数 ξ_i 数字摘要 $H(Vi)$、$H(\xi_i)$。

(3)将 $H(Vi)$和 $H(\xi_i)$连接起来形成投标报文 $H(V_i)|H(\xi_i)$。

(4)对投标报文 $H(Vi)|H(\xi_i)$再进行哈希运算，得到投标报文摘要 $H(H(Vi)|H(\xi_i))$。

(5)投标者 B_i 用自己的临时私钥(di, T)对投标报文摘要进行加密，形成密文：$DDS_{Bi}=(H(H(Vi)|H(\xi_i)))^{di} \bmod T$，则密文 DDS_{Bi} 为投标者 B_i 的双重数字签名。

(6)投标者 B_i 用临时公钥(ei, T)对投标值 *Vi*、$H(\xi_i)$以及双重数字签名 DDS_{Bi} 组成的信息加密，并将此密文和拍卖身份 *ei* 一同加密后发送给 *AM*。

(7)投标者 *Bi* 将 ξi、$H(Vi)$以及双重数字签名 DDS_{Bi} 组成的信息用真实私钥 SK_{Bi} 加密后发送给 *RM*。

提交标价的流程如图 3 所示。

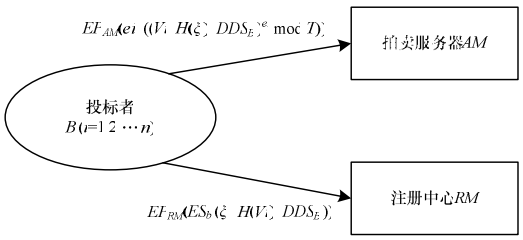

图 3　提交标价的流程

2.3.4　投标结束及开标

开标流程如下：

(1)*AM* 和 *RM* 按照既定截止期限，同时停止接收投标，*AM* 将接收到的投标者身份列表 $Ei(i=1,2,\cdots,k)$和接收到的投标值列表 $V_{Ei}(i=1,2,\cdots,k)$发送给 *RM*。*RM* 整理接收到投标信息的投标者拍卖身份列表，与 $Ei(i=1,2,\cdots,k)$进行对比，检查无误后发送确认信息 *SC*(Start Calculation)给 *AM*，通知 *AM* 开始计算拍卖结果，同时 *RM* 开始计算标价。

(2)由于投标值的计算公式为单调递增函数，因此 *AM* 可以推断投标值最高者为标价最高者，即中标者。*AM* 将计算出的中标者拍卖身份 *ev* 及其投标值 *Vv* 加密后发送给 *RM*。

(3)*RM* 根据标价计算中标者拍卖身份 *ev*'，将该投标者的标价和随机参数代入投标值计算公式得其投标值 *Vv*'，比较 *ev*、*ev*'和 *Vv*、*Vv*'，若相同说明 *AM* 和 *RM* 计算结果一致，则拍卖结果有效。

(4)*RM* 计算中标通知 VN_{RM} 的数字摘要 $H(VN_{RM})$和 $\xi_{Vv}|F(x)$的数字摘要 $H(\xi_{Vv}|F(x))$，并将这 2 个数字摘要连接后再次进行哈希运算，得到中标信息摘要 $H(H(VN_{RM})|H(\xi_{Vv}|F(x)))$，*RM* 用其私钥对中标信息摘要签名，即 $DDS_{RM}=ES_{RM}(H(H(VN_{RM})|H(\xi_{Vv}|F(x))))$，其中，$DDS_{RM}$ 为 *RM* 的双重数字签名。

(5)*RM* 将中标信息 VN_{RM}、$H(\xi_{Vv}|F(x))$、DDS_{RM} 加密后发送给中标者，将中标者的投标参数 ξ_{Vv}、投标值公式 $F(x)$、$H(VN_{RM})$、DDS_{RM} 加密后发送给 *AM*。

(6)*AM* 根据接收到的 ξ_{Vv}、$F(x)$计算出中标值，将中标通知 VN_{AM} 和中标标价 b_v 用中标者的临时公钥加密得密文 $S=(VN_{AM}|b_v)^{ev} \bmod T$，签名后发送给中标者。

(7)中标者在收到 *RM* 和 *AM* 2 封中标通知，并确认标价后，用私钥 SK_{BV} 签名 VN_{RM} 和 VN_{AM}，向 *RM* 发送 $ES_{BV}(ES_{AM}(VN_{AM}))$，向 *AM* 发送自己的公钥 PK_{BV} 以及 $ES_{BV}(ES_{RM}(VN_{RM}))$。此环节的流程如图 4 所示。

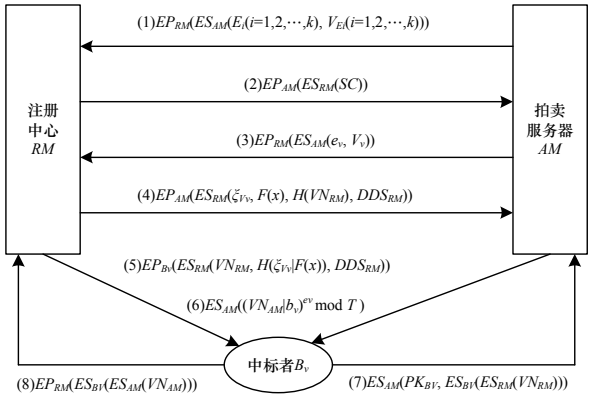

图 4　开标流程

2.3.5 拍卖结果

AM 公布中标者身份和中标价格。若无异议，则进入支付环节，若产生异议，可以向 *RM* 申请验证中标结果。

3 方案安全性及效率分析

3.1 安全性分析

3.1.1 投标者身份匿名性

在整个拍卖结果确定前，只有可信第三方知道投标者的真实身份，投标者在和拍卖服务器的交互过程中使用临时的拍卖身份。该临时身份由可信第三方根据 RSA 加密机制随机产生，因此，拍卖服务器、其他投标者均无法知道该投标者的真实身份，从而杜绝拍卖服务器与部分投标者串通或投标者之间勾结的作弊行为。

3.1.2 标价保密性

在投标过程中，采用双重数字签名技术和函数运算方法，保证标价的保密性。一方面标价不直接发送给拍卖服务器，而是将标价进行函数运算后得到的投标值发送给拍卖服务器；另一方面计算投标值的公式为单调递增且包含随机参数的函数，即使拍卖服务器通过不法方式得到计算投标值的函数，函数中的随机参数是投标者投标时随机产生的，故拍卖服务器也不能推算出标价。通过这两方面的技术应用，保证标价对拍卖服务器和其他投标者保密，从而确保拍卖活动公平有效。

3.1.3 不可伪造性

在应用双重数字签名技术进行投标时，投标者对其发送给 *AM* 和 *RM* 的信息均进行哈希运算，生成数字摘要。如果在信息传送过程中，有入侵者伪造或篡改投标信息，*AM* 或 *RM* 利用哈希函数生成伪造信息的数字摘要，将其和投标者产生的数字摘要对比，若不相符，则可判断信息无效，要求投标者重新发送投标信息。

3.1.4 不可否认性

在 *AM*、*RM* 和投标者的信息交互过程中，均采用非对称密钥加密体制对信息进行加密，发送方在发送信息前都用自己的私钥对信息加密，因此，如果接收方能够利用发送方的公钥成功解密信息，则证明该信息是发送方发送的。在确认中标结果时，中标者需要接收 *RM* 和 *AM* 两方发送的中标通知后才能够确认中标结果，并将确认声明发送给 *RM* 和 *AM*，*RM* 监督投标者不能否认其中标。*AM* 用中标者的临时公钥对中标通知进行加密，生成密文 $S=(VN|bv)^{ev} \bmod T$，若他人想虚构中标者身份，伪造确认信息，则需要知道中标者的临时私钥 *dv*。在已知 *T*、*ev* 的情况下求解 *dv*，等价于将大整数 *T* 分解为 2 个大素数，这在有限的计算时间内是不可能的，因此他人无法伪造中标者确认中标信息，故一旦中标声明产生，则中标者不能否认其确认中标。

3.1.5 时限性

投标开始前，只有在所有投标者完成注册后，*RM* 才将投标者的拍卖身份列表 $ei(i=1,2,\cdots,n)$发送给 *AM*，此时 *AM* 才能开始接受投标，确认投标者的身份是否合法。因此，拍卖服务器不能擅自提前开始投标。投标结束后，*AM* 须要和 *RM* 确认有效的投标名单后，才能开始计算投标结果。因此，拍卖服务器也不能擅自提前结束投标。

3.1.6 不可跟踪性

由于投标过程中，各投标者采用的是临时的拍卖身份，该身份是 *RM* 根据一定规则随机产生的，且和标价间不存在计算关系，因此任何投标者都无法根据标价推断投标者身份。

3.1.7 可公开验证性

由于中标结果是在 *RM* 和 *AM* 的共同计算下产生的，且 *RM* 为可信第三方，因此任何投标者都可以向 *RM* 申请验证中标结果。*RM* 只需要向申请者提供中标者的投标值 V_v 和随机参数 ξ_{Vv}，则该申请者可根据 $F(x)$计算出标价，并验证标价的正确性。

3.1.8 公平性

方案的每一步都是在可信第三方 *RM* 的监督下进行的，投标者均以平等的身份参与拍卖。

3.2 效率分析

本文方案的效率分析结果如表 1 所示。

表 1 本文方案效率分析

参与者分析项目	计算复杂度	通信复杂度
AM	$O(1)$	$O(n)$
RM	$O(n)$	$O(n)$
投标者	$O(1)$	$O(1)$

通常基于秘密共享思想设计的集中式电子拍卖方案是将标价分成 *n* 份，分几次提交给拍卖中心，如文献[6]提出的方案；基于秘密共享方法的分布式电子拍卖方案，则多是利用多维向量计算或者矩阵计算等较复杂的数学方法进行投标。如文献[7]设计的多方电子拍卖方案。

表 2 给出了本文方案与文献[6-7]方案在投标环节的计算复杂度对比。本文方案所需的计算仅涉及普通的乘法和加法，其通信轮数较少，具有较高的效率。

表 2 计算复杂度对比

方案	计算复杂度
本文方案	$O(n)$
文献[6]方案	$O(n^2)$
文献[7]方案	$O(n^2)$

4 结束语

本文基于秘密分享思想，应用双重数字签名技术设计了一个安全的密封式电子拍卖方案，并对该方案进行了安全性分析和效率分析。本文方案满足电子拍卖所需的投标者身份匿名性、标价保密性、不可否认性等各项安全性要求，具有安全高效的特点。

参考文献

[1] 孟 健. 电子拍卖协议研究[D]. 郑州: 解放军信息工程大学, 2006.

[2] 葛丽娜, 唐韶华. 基于圆性质的动态(*t*, *n*)门限秘密共享方案[J]. 计算机科学, 2009, 36(5): 99-103.

[3] 韩宝明, 杜 鹏, 刘 华. 电子商务安全与支付[M]. 北京: 人民邮电出版社, 2001.

[4] 王继林, 陈晓峰, 王育民. 一个安全的封闭式电子拍卖协议[J]. 电子学报, 2003, 31(10): 1578-1579.

[5] 曹 刚. 基于不可信第三方的电子拍卖方案[J]. 计算机工程, 2010, 36(20): 140-141.

[6] 张键红, 伍前红, 王育民. 基于秘密分享的一种新的电子拍卖[J]. 西安电子科技大学学报: 自然科学版, 2003, 30(5): 659-661.

[7] Kikuchi H, Harkavy M, Tyger D. Multi-round Anonymous Auction Protocols[C]//Proc. of the 1st IEEE Workshop on Dependable and Real-time E-commerce Systems. Berlin, Germany: [s. n.], 1998.

编辑 索书志