一种匿名的高效 M+1 电子拍卖*)

杨加喜[1] 谭新莲[2] 王育民[1]

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

摘 要 为了实现投标者的身份匿名，给出了一个基于 RSA 函数的 M+1 电子拍卖方案，任何投标者不能否认所投的标书，未中标价不会被泄露。该方案执行开标算法至多需要 p 轮交互，至多 $2p\log_2 t$ 次模乘法运算，其中 p 是标价的个数，t 是 RSA 公钥。计算量与投标者的数量无关，方案安全、高效，远高于现有拍卖方案的效率。

关键词 电子拍卖，秘密分享，RSA 函数

An Anonymous Efficient (M+1)-st Electronic Auction

YANG Jia-Xi[1] TAN Xin-Lian[2] WANG Yu-Min[1]

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

(School of Information Engineering, Zhengzhou University, Zhengzhou 450052)[2]

Abstract Security and privacy are the crucial condition in the seal-auction design. A new scheme for (M+1)-st electronic sealed-bid auctions based on the RSA function is presented, which preserves losing bids and bidders's anonymous identities. No bidder can repudiate his or her bid. In our scheme, opening bids requires at most p rounds of interactions and $2p\log_2 t$ modular multiplications where p is the range of bids and t is the RSA public-key. The computational cost is independent of the number of bidders. The scheme is secure and much more efficient than the previous schemes.

Keywords Electronic auction, Secret sharing, RSA function

1 引言

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。目前 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可信性。现有的拍卖提供较弱的安全性和保密性。密封式拍卖要求每个拍卖者秘密地提交他们的标价。由于密封拍卖能更有较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[1～4]对其进行了讨论，研究电子拍卖的方案较多如：秘密共享、位承诺、Hash 函数、多方的秘密计算等。最近网上的最大拍卖商 e-Bay 也引入密封式电子拍卖。

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和黑社会操纵，使投标者的隐私在拍卖过程中和拍卖后能够得到保密，就必须进行匿名投标。一个密封式电子拍卖系统应满足下列要求[5]：(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(包括中标者的的身份和未中标者的身份)必须保密。

文中考虑密封的 M+1 价拍卖，即要拍卖 M 个单位的同一种物品，M 个出高价者中标，每个中标者购买一个单位，但统一按照未中标者中出的最高价位(M+1 价位)付款。如果令 M=1，则为 Vickrey 拍卖(出最高价位者中标，中标者按次高价付款)。经济学家 Vickrey 证明了第二价位原理支持商品分配最优化，且降低了出价人串通的可能，Vickrey 因此获得 1996 年 Nobel 经济学奖。Wurman 等[6]证明了 M+1 价拍卖同 Vickrey 拍卖一样满足激励竞争机制，即投标者的最优策略为其愿意出的真实价。由于中标价是第 M+1 价位，即所有未中标者的最高价，每一个投标者按其愿意出的最高价投标增大了其中标的机会而不必担心其是否出价太高。

本文旨在提出一个安全、简单高效的 M+1 价电子拍卖协议，即能有效保护投标者的隐私，满足效率高，易于实施的要求。

2 拍卖协议

一个拍卖包括 4 个实体：注册中心(Registration Center)，拍卖行(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；卖主是想要卖商品的人；投标者为想得到商品的人。

设 A_1，A_2 是两个可信赖的拍卖行，$B_i(i=1,2,\cdots,n)$ 为 n 个投标者。N 是一个 RSA 模数，其分解未知，且 $n\leqslant\log_2 N$。$h(\cdot)$为一个可公开获取的密码学哈希函数。$V=\{v_1,v_2,\cdots,v_p\}$为所有标价，用 $P=\{1,2,\cdots,p\}$表示，其中 $v_i<v_{i+1}$，t 是一奇素数，l 是一个安全参数。BB 为电子公告牌。

初始化：每个投标者 B_i 首先用公开身份向注册中心提交投标申请，注册中心验证申请的合法性后，安全地分配给投标者两个临时秘密身份 ID_{i1}，ID_{i2} 和一个注册顺序号，注册顺序号设为 i，并分别对$(ID_{i1}\parallel i)$ 和$(ID_{i2}\parallel i)$ 签字。投标者 B_i 通过安全信道分别向 A_1 和 A_2 发送注册顺序号 i 和注册中心的签字。A_1 和 A_2 分别生成并通过安全信道发送一次性

*)基金项目：国家自然科学基金资助项目(60473027)。**杨加喜** 博士研究生，研究方向：密码学，电子商务安全；**王育民** 教授，博士生导师，研究方向：编码理论，密码学，信息安全等。

随机数 k_{i1} 和 k_{i2} 给投标者 B_i，其中 $k_{i1}, k_{i2} \in \{0,1\}^l$，$l$ 是安全参数。A_1 和 A_2 将收到的数据和一次性随机数 k_{i1} 和 k_{i2} 存入本地数据库。

投标：假设每个投标者的投标价不同，投标者 B_i 选取他的秘密标价 $b_i \in \{1,2,\cdots,p\}$ 并冗余编码为

$\beta_{i1} = Encode(b_i, A_1) = (x_{i1}, \cdots, x_{ip})$ 和

$\beta_{i2} = Encode(b_i, A_2) = (y_{i1}, \cdots, y_{ip})$

其中 $x_{ij}, y_{ij} \in_R \{0,1\}$ 使得当时 $j = b_i$，$x_{ij} \oplus y_{ij} = 1$；当 $j \neq b_i$ 时，$x_{ij} \oplus y_{ij} = 0$。

投标者 B_i 选择一次性随机比特串 $r_{i1}, r_{i2} \in \{0,1\}^l$，发送 $c_{i1} = h(\beta_{i1} \| r_{i1} \oplus k_{i1} \| i \| ID_{i1})$ 和 $c_{i2} = h(\beta_{i2} \| r_{i2} \oplus k_{i2} \| i \| ID_{i2})$ 到公告牌 BB 作为对投标的承诺。再通过安全信道向拍卖行 A_1 和 A_2 分别发送 $(\beta_{i1} \| r_{i1} \| i \| ID_{i1})$ 和 $(\beta_{i2} \| r_{i2} \| i \| ID_{i2})$。$A_1$ 和 A_2 首先验证注册中心的签字，然后从本地数据库中取出 k_{i1} 和 k_{i2} 并验证 $c_{i1} = h(\beta_{i1} \| r_{i1} \oplus k_{i1} \| i \| ID_{i1})$ 和 $c_{i2} = h(\beta_{i2} \| r_{i2} \oplus k_{i2} \| i \| ID_{i2})$ 是否成立，接受通过所有验证的投标为合法标书，对使用过的 k_{i1} 和 k_{i2} 进行标记。

开标：① 确定中标价（M+1 价）。当投标期结束后，执行下面的算法，利用 A_1 和 A_2 的交互将求出中标价（M+1 价）。

(1) $s_i := 0$，$k_i := p+1$；

(2) $k_i := k-1$；

A_1 计算并发送 $X_k = (x_{1k} \| \cdots \| x_{nk})^t \bmod N$ 到公告牌 BB，A_2 计算并发送 $Y_k = (y_{1k} \| \cdots \| y_{nk})^t \bmod N$ 到公告牌 BB；

(3) 如果 $X_k \neq Y_k (\Leftrightarrow (x_{1k} \| \cdots \| x_{nk}) \neq (y_{1k} \| \cdots \| y_{nk}))$，则 $s_i := s+1$；

(4) 如果 s=M+1，则输出中标价为 k 并终止程序；否则转(2)。

②确定中标人。利用 A_1 和 A_2 的交互将确定出中标人。

对于投标者 B_i，A_1 计算并发送 $M_i = (x_{i(k+1)} \| \cdots \| x_{ip})^t \bmod N$ 到公告牌 BB，A_2 计算并发送 $N_i = (y_{i(k+1)} \| \cdots \| y_{ip})^t \bmod N$ 到公告牌 BB。

如果 $M_i \neq N_i (\Leftrightarrow (x_{i(k+1)} \| \cdots \| x_{ip}) \neq (y_{i(k+1)} \| \cdots \| y_{i(k+1)}))$，说明投标者 B_i 的投的标价 b_i 大于 k，则投标者 B_i 中标，否则投标者 B_i 没有中标。

3 协议分析

投标者身份的匿名性：由于拍卖行 A_1 和 A_2 只知道临时身份，对于其他投标者和外部攻击者，这种临时身份也不知道，因此投标者的身份是匿名的。

不可否认性：任何投标者不能否认所投的标书，因为标书中包含了他或她的秘密临时身份，通过与注册中心合作，可以找到恶意的参与者。

标价的秘密性：由于 $(\beta_{i1} \| r_{i1} \| i \| ID_{i1})$ 和 $(\beta_{i2} \| r_{i2} \| i \| ID_{i2})$ 与 b_i 是相互独立的，任意单个的拍卖行不可能知道投标者所投标价，投标者与任意一个拍卖行勾结也不可能知道其他投标者所投标价，除非两个拍卖行勾结。由于 RSA 模数 N 分解未知，从 $X_k = (x_{1k} \| \cdots \| x_{nk})^t \bmod N$ 不可能知道 $(x_{1k} \| \cdots \| x_{nk})$，同样从 $Y_k = (y_{1k} \| \cdots \| y_{nk})^t \bmod N$ 中也不可能知道 $(y_{1k} \| \cdots \| y_{nk})$。因此，即使开标后，上述结论仍然成立，协议满足标价的秘密性。

不可伪造性：一份完整的标书包括发送到公告牌的承诺和发送给两个拍卖行的数据，其中包含了投标者临时秘密身份和一次性随机数的信息。由于除注册中心以外的任何人不可能事先知道投标者的临时秘密身份，除拍卖行以外没有人事先知道一次性随机数，因此任何人不可能伪造一份合法的标书。

抗重放攻击：由于拍卖行对使用过的一次性随机数 k_{i1} 和 k_{i2} 进行了标记，攻击者在计算上不可能重放以前拍卖活动中合法的标书而不被发现。

高效性：执行开标算法至多需要 p 轮交互，至多 $2p \log_2 t$ 次模乘法运算，与参与者的数量无关，故拍卖方案是高效的、实用的。

结论 文中提出了一种新的基于 RSA 函数的 M+1 电子拍卖方案，可以保护投标者的匿名身份，任何投标者不能否认所投的标书，未中标价不被泄露，伪造一份合法的标书或重放以前拍卖活动中合法的标书而不被发现，在计算上都是不可能的。该方案执行开标算法在最坏的情况下只需 p 轮交互，$2p \log_2 t$ 次模乘法运算，与投标者的数量无关，协议安全、高效。

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 Kikuchi H, Harkavy M, Tyger D. Multi-round Anonymous Auction Protocols [C]. In: Proceedings of the First IEEE Workshop on Dependable and Real-time E-commerce System. Berlin: Springer Verlag, 1998. 62～69

3 Kudo M. Secure Electronic Sealed-bid Auction Protocol with Public Key Cryptography [J]. IEICE Trans on Fundamental, 1998, E81-A(1): 20～27

4 Mu Y, Varadharajan V. An Internet Anonymous Auction Scheme [C]. Lecture Notes in Computer Science, Berlin: Springer Verlag, 2001. 171～182

5 杨加喜，王育民. 一种安全高效的 M+1 电子拍卖[J]. 网络安全技术与应用，2006,11:87～89

6 Wurman P R, Walsh W E, Wellman M P. Flexible double auction for electronic commerce: Theory and Implementation, Decision Support System, 24. 17～27 [DB/OL]. http://www.csc.ncsu.edu/faculty/wurman/papers/Wurman-Dss-98.pdf,2002-05-15

(上接第 103 页)

提供了有力的保证。

总结 本文对采用基于 ASP.NET 构建的 B/S 结构的项目管理系统的安全模式设计进行了讨论，这种基于 Web 的应用系统的安全体系设计相对于传统的 C/S 模式，既要考虑数据访问的安全，又要考虑网络的安全。Web 开发平台 ASP.NET 的安全访问机制使得 Web 的安全性和可靠性得到了基本的保障，采用 B/S 的三层架构，将显示层、中间层、数据层在逻辑上相互独立，减少了耦合度，保证了系统的安全。采用了身份验证、权限控制、数据加密、存储过程访问数据库等多种安全策略保证了数据的安全，限制了网络的入侵，最终保障了网络系统的安全

参 考 文 献

1 李兰友，杨晓光编著. ASP.NET 实用程序设计[M]. 清华大学出版社，2005

2 邹显春，张为群. 一种主动网络管理系统结构的分析与研究[J]. 计算机科学，2006(10)

3 李敏波. ASP.NET 1.1 高级编程[M]. 清华大学出版社，2005

4 (美)Basiura R，等著. 王晓娜，黄开枝译. ASP.NET 安全性高级编程[M]. 清华大学出版社，2003

5 王珺，王崇骏，谢俊元，陈世福. 基于 Agent 的网络入侵检测技术的研究[J]. 计算机科学，2006(12)