一个安全的密封式电子拍卖方案

王继林, 陈晓峰, 王育民
(西安电子科技大学 ISN 国家重点实验室, 陕西西安 710071)

摘 要: 如何保护投标者隐私和防止中标者反悔是设计安全电子拍卖方案的关键技术. 本文利用单向函数 $z=x^y \bmod n$ 给出了一个实现密封式电子拍卖的方案. 该方案除满足投标者匿名、投标价保密、不可否认性和强可验证性等安全要求外, 还具有技术简单、通信量小和几乎不需要可信赖第三方参与等优点.

关键词: 密封式电子拍卖; 单向函数; 匿名性; 隐私保护
中图分类号: TB11 文献标识码: A 文章编号: 0372-2112 (2003) 10-1578-02

A Secure Sealed-bid Electronic Auction Scheme

WANG Ji-lin, CHEN Xiao-feng, WANG Yu-min
(National Key Lab. of ISN, Xidian University, Xi. an, Shaanxi 710071, China)

Abstract: The protection of bidder privacy and the prevention of bidder default are the keys in the designing of Secure Electronic Auction Scheme. This paper gives a secure sealed-bid auction scheme using only a one-way function. Our scheme can satisfy all the secure requirements of sealed-bid auction stated and has the advantages similar to the scheme of [1].

Key words: sealed auction scheme; one-way function; bidder anonymity; privacy protection

1 引言

目前, 很多电子拍卖系统缺乏必要的安全机制, 投标者的隐私不能得到有效保护, 也无法阻止投标者或拍卖行(拍卖服务器)的欺诈及中标者的违约等行为. 为了防止上述情况的发生, 很多学者进行了深入研究. 本文利用单向函数 $z=x^y \bmod n$, 给出了一个密封式安全电子拍卖方案. 该方案的特点是: (1) 安全性好, 方案能够满足第 2 部分叙述的密封式电子拍卖的所有安全性要求; 方案中的参数选取是 RSA 参数, 是公认的安全参数; (2) 技术简单, 仅使用了 $z=x^y \bmod n$; (3) 对可信赖的第三方的依赖小, 仅需注册获取匿名服务. 我们的方案和文[1]中的方案比, 采用的技术是相似的, 也要求投标者在开标阶段必须与拍卖服务器保持通信; 但我们的方案不需要签字技术和公钥证书的支持, 能够实现匿名性.

2 电子拍卖的安全性需求和研究现状

一般按投标价是否公开把电子拍卖系统分为开放式和密封式拍卖系统. 在开放式拍卖系统中, 投标价是公开的, 允许投标者竞标, 最后出价最高者获胜. 在密封式拍卖系统中, 每个投标者秘密提交一个投标价, 在规定时间后才能打开投标.

安全的电子拍卖系统必须提供公平竞争的机制, 中标者的胜出必须无异议, 必须能杜绝串通和中标者违约等行为. 概括起来, 电子拍卖系统有下列安全需求: (1) 公平性, 指投标者地位一样, 系统设计无偏向性, 有办法解决争议和违约; (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, 可公开证明最终的中标者的合法性; (5) 投标价保密, 投标者的投标价保密; (6) 时限性, 确保在投标结束后, 才能打开投标; (7) 不可跟踪性, 其他参与者无法断定哪些投标对应同一个投标者; (8) 投标者匿名, 投标者的个人材料在开标前和开标后保密. 很显然, 对于开放式拍卖系统, 希望能够实现(1)~(4)、(7)、(8), 而对于密封式拍卖系统, 希望能够实现(1)~(6)、(8).

根据前述安全需求, 有关能够实现参与者身份保密和防止参与者抵赖的技术和手段以及预防作弊和违约的办法都可用来设计安全电子拍卖方案. 这些技术主要有数字签字中的盲签字和公平盲签字技术、群签字和群盲签字技术、零知识证明理论、不可否认协议、最优公平交换协议、秘密分享和可验证秘密分享协议、Bit 承诺和 Hash 函数等. 值得注意的是, 一种安全电子拍卖方案的设计往往要综合应用上述工具, 仅靠一种技术去实现是有很大难度的(我们仅见到文献[1]).

从信赖关系上看, 已有的方案可分为两大类. 一类利用秘密分享机制在相互无关的多个拍卖服务器或参与者中把投标分布, 当不诚实的服务器或参与者个数在门限之内时, 即可实现上述要求[3], 但要实现可证实性, 这种方案需要高效的可验证秘密共享协议的支持, 遗憾的是到目前尚无理想的这种协议. 另一类是基于存在一个可信赖或半可信赖的第三方的[4, 5]. 我们认为后者更具有优势, 因为其在通信量和计算量方面都明显优于前者, 而前者着重要加强的第三方的可信性随着电子化进程的推进是可以由一个实体担当的. 我们的方案也是基于后者的.

3 密封式安全电子拍卖方案

方案的模型假设同文[1], 方案中 h 表示从低到高共有 h 个允许的投标价; $z_{r,j}$ 表示在拍卖服务器从最高价 p_h 到低检查到 p_r 时, 第 j 个投标者 B_j 提交的承诺.

(1) 系统准备 拍卖服务器 A 发布要拍卖的物品, 并按照从小到大的顺序发布可接受的拍卖价 p_i(i= 1, 2, , , h) 且令 s= h;

(2) 注册 每个投标者 B_j(j= 1, 2, , , m) 到注册中心(可

收稿日期: 2002-04-04; 修回日期: 2003-02-18
基金项目: 国家自然科学基金资助课题(No. 60073052)

信赖的第三方)注册. 注册中心检查投标者的身份和资格, 为每一个合法的 B_j 选取一对大随机数(x_j, y_j)给 B_j, 其中 y_j 作为 B_j 的匿名身份; 另外注册中心按照 RSA 体制的参数要求为本次拍卖选取一个大整数 $n= pq$. p, q 是强素数, 然后销毁 p 和 q, 把 n 公布给投标参与者. 注册完毕后, 注册中心把由 y_j 构成的随机数表提交给拍卖服务器供拍卖服务器在投标过程中检查投标者的合法性;

(3) 投标　若 B_j 的投标价为 p_k, 则 B_j 提交$(y_j, z_{h,j})$给拍卖服务器 A, 这里

$$z_{r,j}= x_j^{X_r} \bmod n,\ X_r= \begin{cases} (y_j+ p_k)\ y_j^{r-k} & r \geq k \\ 1 & r< k \end{cases}.$$

A 查阅随机数表判定 y_j 的合法性从而决定是否接受投标并发布合法投标者$(y_j, z_{h,j})$;

(4) 开标　在开标阶段, 拍卖服务器 A 执行下列步骤:

A 要求所有投标者 B_j 提交$(y_j, z_{s-1,j})$并发布 $z_{s-1,f}$, 对 j = 1, 2, , , m 验证下列公式:

$$z_{s,j}= z_{s-1,j}^{y_j} \bmod n \qquad (1)$$

如果对所有的 j 式(1)都成立, 则 A 得出没有投标者对 p_s 投标的结论. A 令 s= s- 1. 重新执行步骤 4. 如果式(1)对某些 j 不成立, 则 A 对该j 验证下列公式:

$$z_{s,j}= z_{s-1,j}^{y_j+ p_s} \bmod n \qquad (2)$$

如式(2)满足, 则 A 宣布匿名为 y_j 的投标者中标. 如某个 j 的 $z_{s-1,j}$对式(1)、(2)都不满足, 则该 j 对应的投标有欺诈行为;

(5) 对于有多个满足式(2)的情况, 如需要, 可进入下一轮拍卖.

4　安全性分析

本方案满足第二部分提出的有关对密封拍卖的所有安全性要求.

(1)投标价保密　由于函数 $z= x^y \bmod n$ 的单向性和 x_j 的随机性, 在 B_j 仅提供$z_{s-1,j}$而不提供$z_{s-2,j}$的情况下, 任何别的参与者(不含注册中心)是无法确定 B_j 的$z_{s-2,j}$的, 因为这需要分解 n 或求解离散对数问题. 根据 s 的取值, 仅在所有上一轮的 $z_{s,j}$和$z_{s-1,j}$都满足式(1), 即对相应的 p_s 无投标者的情况下, 投标者才提交 $z_{s-2,j}$进行下一轮更低投标价的验证, 直至出价最高的中标者即满足式(2)者出现. 这样做的本质是使 B_j 的$z_{h,j}, z_{h-1,j}, ,$ 构成一个承诺链, 即 $z_{s-1,j}$是对$z_{s,j}$的承诺, 每个 B_j 的承诺链的长度不一样, 由其投标价决定, 最后仅有中标者因其承诺链的长度最短打开了承诺, 低于中标价的投标者因其 $z_{s,j}$和$z_{s-1,j}$满足式(1)而又不再继续提供后面的承诺 $z_{s-2,j}$, 别人无法确定出其投标价, 因而未中标者的投标信息是不会被暴露的;

(2) 正确性和强可验证性　s 的取值是从 h 开始, 在所有投标者 B_j 的$z_{s,j}$和$z_{s-1,j}$都满足式(1)的情况下令 s= s- 1, 直至有满足式(2)的出价最高的中标者出现. 由于所有 B_j 的$z_{s,j}$和$z_{s-1,j}$是发布的, 任何人都可以根据式(1)和(2)证明中标者中标、未中标者被淘汰的正确性;

(3) 不可否认性和不可伪造性　在已知的情况下要构造 $z_{k-1,j}$, 使得 $z_{k-1,j}$满足式(1)而 $z_{k-1,j}$满足式(2), 或在 $z_{k-1,j}$满足式(2)而 $z_{k-1,j}$满足式(1), 都等价于在已知 z 和 y 的情况下求式 $z= x^y \bmod n$ 的根, 这等价于分解 n 的困难性, 因而投标者无法否认其投标. 伪造者由于不知道 x_j 能被发现出来, 即便是拍卖服务器也无法作弊;

(4)投标者匿名性　我们引入了注册中心作为可信赖的第三方, 注册中心给每一个投标者一对随机数作为投标者的匿名身份, 从而实现了投标者的匿名性;

(5)时限性和公平性　我们的方案在没有投标者配合的情况下是无法打开投标的, 因而方案很好的满足了时限性要求. 方案的公平性是隐含在其它几个性质之中的.

5　结论

我们利用单向函数 $z= x^y \bmod n$ 给出了一个安全的密封电子拍卖方案, 该方案除具有投标者匿名、投标价保密、不可否认性和强可验证性等安全特性外, 还具有技术简单和几乎不需要可信赖第三方参与等优点. 我们的设计该方案的思想是基于文献[1, 2]的, 和文[1]中方案相比, 本方案不需要数字签字和证书支持, 技术更加简单. 我们方案的计算量比文[1]的方案略大一些, 通信量大致相当. 值得注意的是文[1]所采用的 Hash 函数从原理上讲也是单向函数. 我们将研究这两个方案的共性, 以归纳出一类通用的密封电子拍卖方案模型.

参考文献:

[1] Koutarou Suzuki, et al. Efficient sealed2bid auction using Hash chain [A]. Proc. of Third Inter. Con. On ICISC [C]. Seoul, Korea, 2000. LNCS 2015, Springer2Verlag, 2001. 183- 191.

[2] Josh Benaloh, et al. One2way accumulators: A decentralized alternative to digital signatures [A]. Advances in Cryptology EUROCRYPT. 93 [C]. Lofthus, Norway, 1993. LNCS 765, Springer2Verlag, 1994. 274- 285.

[3] Matthew K Franklin, Michael K. Reiter. The design and implementation of a secure auction service [J]. IEEE Transaction on software Engineering, 1996, 22(5): 302- 312.

[4] Yi Mu and vijay Varadharajan. An internet anonymous auction scheme [A]. Proc. of Third Inter. Con. On ICISC [C]. Seoul, Korea, 2000. LNCS 2015, Springer2Verlag, 2001. 171- 182.

[5] Kouichi Sakurai, et al. An Anonymous electronic bidding protocol based on a new convertible group signature scheme [A]. ACISP2000 [C]. Brisbane, Australia. LNCS1841, Springer2Verlag, 2000. 385- 399.

作者简介:

王继林　男, 1965 年生于河南柘城, 西安电子科技大学 ISN 国家重点实验室博士研究生, 副教授, 研究方向为签字技术与电子商务.

陈晓峰　男, 1976 年生于陕西宝鸡, 西安电子科技大学 ISN 国家重点实验室博士研究生, 感兴趣的研究方向为椭圆曲线密码与电子商务.