一种新的 Vickrey 安全拍卖协议

陈晓峰, 毛 剑, 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: 利用比特承诺协议、多方安全计算协议及 ElGamal 加密方案, 本文给出了一种新的 Vickrey 安全拍卖协议. 该协议具有匿名性, 秘密性, 高效性, 同时它支持商品最优分配原理. 即使某一投标者与拍卖行相互勾结时, 也不会影响协议的安全性与有效性.

关键词: 秘密标价; 第二价位; 比特承诺
中图分类号: TB11 文献标识码: A 文章编号: 0372-2112 (2002) 04-0471-02

A New Secure Vickrey Auction Protocol

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

Abstract: A new secure Vickrey auction protocol is presented in this paper by using the bit commitment protocol, multi-party secure computation protocol and the ElGamal encryption scheme. With the advantages of anonymity, privacy, efficiency, the protocol also supports the optimal distribution of goods, Even when some bidder works together with the auctioneer, the protocol is still secure and valid.

Key words: sealed bids; the second-price; bit commitment

1 引言

随着 Internet 的迅速发展, 电子商务活动(电子银行, 电子拍卖)已成为生活中的基本活动, 人们可以在网上方便的购物或拍卖物品, 各种拍卖行、拍卖代理系统(如 Nomad)也相继成立[1]. 常见的三种拍卖方式有: 价格递增拍卖(英式拍卖), 价格递减拍卖(荷式拍卖), 密封式标价拍卖[2]. 英式拍卖及荷式拍卖的优点是尽可能的使商品以真实的最高价出售. 然而, 英式拍卖有许多缺点: 拍卖时间与最终的出售价成正比; 通信时间随最终出售价的增加而呈超线性的增加. 荷式拍卖也存在通信时间过长, 效率过低的缺点. 密封式标价拍卖虽然可在单轮通信中完成, 但拍卖行一般会知道各投标者的出价, 而且不支持商品最优分配[8]. 经济学家 Vickrey 结合了英式拍卖与密封式标价拍卖的优点, 设计出一种新的拍卖方式——第二价位拍卖[3]. 象密封式标价拍卖一样, 投标者将标价送给拍卖行, 第一价位中标, 但中标者只付出第二价位的价格. 第二价位原理支持商品分配最优化, Vickrey 因此获得 1996 年 Nobel 经济学奖. 这种拍卖方式通讯时间固定, 并且使投标者尽可能的以真实的最高价投标, 但是它仍不保持标价的秘密性. 许多学者对 Vickrey 拍卖的性能进行了研究, 事实上, 如何在不泄露投标者的标价的前提下求出第二价位以及尽可能的减少拍卖的通讯时间及费用是一个困难问题.

本文利用比特承诺协议、多方安全计算协议及 ElGamal 加密方案给出了一种新的 Vickrey 安全拍卖协议, 该协议的优点如下: (1) 遵循第二价位原理, 从而使商品分配达到最优. (2) 通讯时间及费用少, 拍卖效率高. (3) 匿名性: 采用 Bit 承诺协议, 投标人的身份不公开. 即使拍卖行求出了第二价位, 也无法知道第二价位投标者的身份. (4) 保密性: 任何投标者都不知道其它投标者的标价.

2 拍卖性质

(1)拍卖主体: 若干投标者, 拍卖行, 注册中心. 图 1 给出协议所使用的拍卖模型: n 个投标者, 一个注册中心, 两个拍卖行 $auc1$, $auc2$(并且 $auc1$ 与 $auc2$ 不会相互勾结来欺骗投标者)[6].

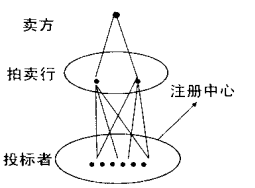

图 1 拍卖模型

(2)拍卖过程: 拍卖开始之前每个投标者首先向注册中心提交拍卖申请, 注册中心验证申请的合法性后分配给该申请者一个秘密的身份号. 拍卖行宣布拍卖开始后, 每个投标者提交他们的标价(公开竞价或者秘密投标)给拍卖行. 经过一段时间后, 拍卖行宣布投标结束. 最后, 拍卖行宣布最高价位者获胜并且该投标者公开承诺(或标价).

(3)理想的拍卖应具有以下的性质: 标价的匿名性, 投标者身份的秘密性, 公平性(最高价位者中标), 不可否认性(中标后不能反悔), 高效实用性.

3 准备工作

3.1 Bit 承诺协议[7]

A 想向 B 承诺未来发生的一个事件预测 Bit, 但在事件出现前不对 B 泄露; 另一方面要使 B 确信 A 对他所做出的承诺不会改变.

承诺生成:

(1)A 生成两个随机数 R_1 和 R_2.

(2)A 将 R_1 和 R_2 及承诺消息 Bit b 组成 (R_1, R_2, b).

(3)A 计算 (R_1, R_2, b) 的单向函数值 $H(R_1, R_2, b)$, 并随机选择一个数 R_1, 将 $(H(R_1, R_2, b), R_1)$ 送给 B.

收稿日期: 2000-10-20; 修回日期: 2001-04-08
基金项目: 国家自然科学基金(No. 19931010)

© 1994-2010 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

承诺兑现:

(4) A 将原消息(R_1, R_2, b)送给 B.

(5) B 计算(R_1, R_2, b)的单向杂凑值, 并与(3)中收到的值相比较. 同时还将(4)中的 R_1 与(3)中收到的 R_1 比较, 如果一致, 证明 A 的承诺合法.

3.2 多方安全计算协议[7]

A 知道整数 i 且 B 知道整数j, 协议结束后, A 和 B 都知道$i \geq j$ 或$i < j$, 但都没有得到关于 i 和j 的进一步信息.

(1) B 选择一个大随机数x, 私下计算 $k = E_A(x)$.

(2) B 将$k - j$ 告诉A.

(3)A 私下计算$y_u = D_A(k - j + u)$, $1 \leq u \leq 100$. 然后随机选择一个大素数 P(P 的大小大致比x 小, P 和x 的大小提前约定好).

A 私下计算$z_u = (y_u \bmod P)$, $1 \leq u \leq 100$, 对所有 u 和$v \neq u$, 验证$|z_u - z_v| \geq 2$, $0 < z_u < P - 1$, 如果不成立, A 选择另一个素数直到成功为止.

(4) A 按顺序告诉B 下面一串数字

$$z_1, z_2, \cdots, z_i, z_{i+1} + 1, z_{i+2} + 1, \cdots, z_{i+100} + 1, P$$

(5) B 验证: 该数字串的第j 个数是否同余x 模p, 如果是他断言: $i \geq j$; 否则 $i < j$.

(6) B 告诉A 结果.

3.3 拍卖参数

(1) 令 P 是一个 1024 比特的素数, g 是有限域$GF(P)$的一个生成元, P, g 公开, $auc\,2$ 随机选择一个秘密参数 l 并且公开$g^l \bmod P$. 每个投标者 W_i 选择他的秘密钥s_i, 公开 $g^{s_i} \bmod P$. $auc\,2$ 随机选择一个秘密序列$\{a_t, 0 \leq t \leq n\}$, $1 \leq a_t \leq 10^4$.

(2) 每个投标者从注册中心得到一个 1024 比特的素数 $P^{(i)}$, 然后他随机选择一个大约 1024 比特的数 d_i, $(d_i, P^{(i)}) = 1$, d_i, $P^{(i)}$保密, e_i 是$d_i \bmod P^{(i)}$的逆并且公开.

(3) 假定投标者的数目不超过 100. 由于$\sum_{t=0}^{n} a_t p_i^t \leq 10^4 \dfrac{1 - p_i^n}{1 - p_i}$ $\leq 10^{300} \leq P^{(i)}$, 有 $\sum_{t=0}^{n} a_t p_i^t \bmod P^{(i)} = \sum_{t=0}^{n} a_t p_i^t$, 其中 p_i 是 W_i 的标价. 如果 n 大于 100, 可以用以下两种办法处理:

(a)使用多轮拍卖的方法将投标者分为许多小组(每一小组的人数不超过 100), 每一小组的胜者进入下一轮.

(b) 使用 3.2 节的协议淘汰一些投标者: 拍卖行给出一个价格, 当投标者的标价小于此价格时, 该投标者被淘汰出局. 这样在实际拍卖过程中可能提高拍卖效率.

4 安全 Vickrey 拍卖协议

这一节给出安全的 Vickrey 拍卖协议:

(1) 每个投标者 W_i 选择标价 p_i, 并且使用 3.1 节的协议发送$(H(R_i, R'_i, p_i), R_i)$给 $auc\,1$.

(2) W_i 计算$\{e_i p_i^t \bmod P^{(i)}; 0 \leq t \leq n\}$并发送给 $auc\,2$.

(3) $auc\,2$ 计算$\sum_{t=0}^{n} a_t e_i p_i^t \bmod P^{(i)}$的值并发送给 W_i.

(4) W_i 利用私钥 d_i 计算出$\sum_{t=0}^{n} a_t p_i^t \bmod P^{(i)}$(即$\sum_{t=0}^{n} a_t p_i^t$), 然后发送: $(g^{s_i} \bmod P, g^{ks_i} p_i \bmod P, \sum_{t=0}^{n} a_t p_i^t)$给 $auc\,1$.

(5) 假定$\sum_{t=0}^{n} a_t p_i^t$ 的次最大值是$\sum_{t=0}^{n} a_t p_{n-1}^t$, $auc\,1$ 发送$(g^{s_{n-1}} \bmod P, g^{ls_{n-1}} p_{n-1} \bmod P)$给 $auc\,2$, $auc\,2$ 计算第二价位 p_{n-1}并告诉 $auc\,1$.

(6) $auc\,1$ 宣布最高价位者以价格 p_{n-1}中标, 同时中标者兑现承诺.

5 协议分析

对 $auc\,1$ 来说, 由$(g^{s_i} \bmod P, g^{ks_i} p_i \bmod P)$求 p_i 必须解离散对数问题; 而且由于他不能由方程组$\sum_{t=0}^{n} a_t p_i^t = V_i$, $i = 1, 2, \cdots, n$, 恢复出$\{a_t, 0 \leq t \leq n\}$, 所以用逼近法也无法求出各标价 p_i; 对 $auc\,2$ 来说, 他只能计算出第二价位而不能知道该价位的投标者, 并且无法计算其它价位. 所以只要 $auc\,1$ 与 $auc\,2$ 不相互勾结, 我们的方案就可以保证标价的秘密性及投标者身份的匿名性; 对投标者来说, 由于使用了 Bit 承诺协议, 一旦他中标就必须兑现承诺, 所以他也无法欺骗拍卖行.

6 结论

安全性是电子商务活动的前提, 网上的欺诈行为使得网上交易进展缓慢. 本文给出了一种较为理想的 Vickrey 安全拍卖协议. 本文的主要贡献是在不泄露投标者的标价的前提下求出第二价位并且保持投标者身份的匿名性. 当然, 如何进一步提高拍卖效率, 减少通信时间与费用, 防止投标者与拍卖行之间的勾结欺诈需要做进一步的工作[4, 5, 8].

参考文献:

[1] T Sandholm, Q B Huai. Nomad: mobile agent system for an internet-based auction house [J]. IEEE Internet Computer, 2000, 4(2): 80-86.

[2] M Gaynor, J Megquier, V Sethaput. Secure Vickrey Auction Protocol [DB/OL]. http://sonnet.eas.harvard.edu/auction/paper.html, 2000.

[3] W Vickrey. Counterspeculation, auctions, and competitive sealed tenders [J]. Journal of Finance, 1961, 16(1): 8-37.

[4] P Milgrom. Auction theory [A], In Advances in Economic Theory 1985: Fifth World Congress [C]. NewYork: Cambridge University Press, 1985.

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

[6] H Kikuch, M Harkavy, J D Tygar. Multi-round anonymous auction protocols [A]. Proc. of the First IEEE Workshop on Dependable and Real-time E-Commence systems [C]. 1998: 62-69.

[7] B Schneier, Applied Cryptography [M]. England: John Wiley & Sons, Inc, 1996.

[8] M Harkavy, H Kikuch, J D Tygar. Electronic auction with private bids [A]. Proc. of the 3rd USENIX Workshop on Electronic Commence [C]. Boston, 1998.

作者简介:

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电子商务, 椭圆曲线密码.

毛 剑 男, 1978 年生, 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电子商务, 网络安全.

© 1994-2010 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net