

一个基于群签名的密封式电子拍卖方案

赵建峰,唐西林

(华南理工大学 理学院,广东 广州 510640)

摘 要: 利用基于双线性对的 W 群签名,提出了一个新的密封式电子拍卖方案.与以往基于群签名技术提出的同类方案相比该方案不但满足电子拍卖的安全性要求,而且在用户加入群时不需要交互式零知识证明,并且具有签名短、步骤简略、签名验证简单等特点.

关键词: 电子拍卖;群签名;双线性映射;Hash 函数

中图分类号: TP309

文献标识码: A

文章编号: 1000-7180(2010)05-0174-03

Sealed-bid Electronic Auction Scheme Based on Group Signature

ZHAO Jian-feng, TANG Xi-lin

(School of Science, South China University of Technology, Guangzhou 510640, China)

Abstract: With the help of group signature based on bilinear pairing, a new sealed-bid electronic auction scheme is presented. Comparing with the former auction schemes based on group signatures, the new one not only satisfies all main properties of common secure public auction schemes, but also have some other characteristics: don't need identification and signature when the user take part in the group, the short of length, compendary steps, easily to verify, ect.

Key words: electronic auctioning; group signature; bilinear pairing; Hash function

1 引言

随着互联网技术的迅猛发展,作为电子商务的重要组成部分电子拍卖愈来愈受到人们的关注.电子拍卖作为传统拍卖形式的在线实现,卖方可以借助网络平台来展示自身的商品,可以避免传统拍卖中实物的移动节约了拍卖成本,买家也可以足不出户的完成竞拍.

一个拍买系统一般由注册中心、拍卖行、投标者、卖方四部分组成,其拍卖步骤分为:

- ① 系统初始化;
- ② 注册阶段;
- ③ 投标阶段;
- ④ 确定中标者.

电子拍卖方案在安全性上必须满足:

- ① 公平性;
- ② 匿名性;
- ③ 不可否认性;
- ④ 不可伪造性;
- ⑤ 公开可验证性;
- ⑥ 不可联系性.

在现有的电子拍卖方案中群签名是一个重要的

工具,以往很多的电子拍卖^[1-2]都是基于群签名技术提出来的.在文献[2]中是利用基于双线性对的群签名方案提出的电子拍卖协议,虽然较以往的方案有所改进,但是其签名过程过于繁琐和签名长度过长不便于操作^[3],文中以文献[4]提出的 W 群签方案为基础结合承诺协议将其转化为一个高效的密封式电子投标协议.该方案与以往的基于群签名技术提出的电子拍卖协议相比没有用到交互式零知识证明,能有效防止用户和拍卖行的联合作弊,而且签名简略,通信量和计算量大大减少^[5].

2 预备知识

2.1 承诺协议

承诺协议^[6]是密码学中的重要组成部分,多用于执行协议的双方不能完全信赖的情况:A 想要向 B 承诺消息 b 但是又不想让 B 在时间 T 内知道消息的任何内容,经过时间 T 后, A 可以向 B 发送原消息

b, B 可以验证所承诺消息的正确性.

(1) A 选取两个随机数 R_1, R_2 ;

(2) 对于要承诺的消息 b, A 用单向 Hash 函数 H 作用, 得到 $H(R_1, R_2, b)$;

(3) A 将 $(H(R_1, R_2, b), R_1)$ 发送给 B ;

(4) 经过时间 T 后 A 将 (R_1, R_2, b) 发送给 B , B 可以验证 A 所承诺消息的正确性.

2.2 双线性群

设 G_1, G_2 都是为 n 阶乘法群, 其中 $n = pq, p, q$ 是两个大素数且 $p \neq q$. g 是 G_1 的生成元. 存在一个双线性映射 $e: G_1 \times G_1 \rightarrow G_2$ 且满足:

(1) 双线性性: 等式 $e(u^a, v^b) = e(u, v)^{ab}$ 对于任意的 $u, v \in G_1, a, b \in Z$ 都成立;

(2) 非退化性: $e(g, g) \neq 1$;

(3) 可计算性: 对于任意的 $u, v \in G_1, e$ 可以有有效的计算 $e(u, v)$; 则称 G_1 为一个双线性群.

2.3 安全性假设

(1) Strong Diffie _ Hellman(SDH)假设

假设 G_1 是一个双线性群, 给定 $(l+1)$ 维数组 $(g, g^w, g^{w^2}, g^{w^3}, \dots, g^{w^l})$, 其中 $w \in Z_p^*$. 不存在一个概率多项式时间算法能够不可忽略的概率计算出一个数组 $(c, g^{1/w+c}) \in Z_p^* \times G_p$.

(2) Hidden Strong Diffie _ Hellman(HSDH) 假设

设一个三元数组 $(g, h, g^w) \in G_1^3$, 给定 $(l-1)$ 组 $(g^{1/(w+c_i)}, g^{c_i}, h^{c_i}) \in G_1$, 不存在一个不可忽略的概率多项式时间算法输出一个不同于这 $(l-1)$ 组的 $(g^{1/(w+c)}, g^c, h^c) \in G_1$.

(3) Subgroup Decision(SD) 假设

对于一个数组 (p, q, G_1, G_2, e) , 如果 G_q 是 G_1 的一个阶数为 q 的子群. 从 G_q 中或 G_1 中选择一个 w , 不存一个概率多项式时间算法能以不可忽略的超过 $1/2$ 的概率去决定 w 是否属于 G_q .

2.4 电子公告牌

用户与拍卖行以及拍卖行和注册中心之间的通信信道是一个具有存储能力的公共的广播信道, 为“电子公告牌(BBS)”, 它具有以下性质: (1) 任何人都可以读取它的信息; (2) 一个合法用户可以而且只能在属于他的指定位置写信息; (3) 任何人不能擦除他人的信息.

3 新的电子拍卖方案

RM(注册中心): 审核用户资料并向用户发放

签名证书, 并协助拍卖行撤销中标者的匿名性, 公布中标者.

AM(拍卖行): 负责发布拍卖物品的信息, 检验标书的有效性, 公布中标者的标书.

U_i (投标者): 参与拍卖活动的买方.

3.1 系统初始化

注册中心 RM 首先选择具有相同长度的两个大素数 $p, q, n = pq$. 选取 G_1 的一个子群 G_q , 其生成元为 h . 再选取一个单向函数 H . 将 $PK = (g, u, v, w, h, H)$ 作为公钥在 BBS 上公布出来, 其中 $u, v \in G_1, w = g^x$, RM 将 (x, q) 作为私钥保存起来. 拍卖行将所要进行拍卖的物品的相关资料发布到 BBS 上.

3.2 用户注册阶段

(1) 用户 U_i 向注册中心 RM 出示合法的身份后, 注册中心随机选择一个 $s_i \in Z$, 且满足 $x + s_i \in Z_n^*$, 将 (s_i, U_i) 保存起来计算:

$$\begin{aligned} SK_i &= (K_1, K_2, K_3, K_4, K_5) \\ &= (g^{1/(x+s_i)}, u^{1/(x+s_i)}, v^{1/(x+s_i)}, g^{s_i}, u^{s_i}) \end{aligned}$$

作为 U_i 的签名密钥发送给 U_i ;

(2) U_i 用户在接收到 SK_i 后验证:

$$\begin{aligned} e(K_1, wK_4) &= e(g, g); \\ e(K_2, wK_4) &= e(u, g); \\ e(K_3, wK_4) &= e(v, g); \\ e(K_4, u) &= e(K_5, g). \end{aligned}$$

如果以上等式成立则 U_i 用户接受其为签名证书, 否则让注册中心重新颁发签名证书.

3.3 投标阶段

(1) 对于要签名的标书 m_i , 用户 U_i 随机选取一个 $s \in Z_n^*$ 并用自己的身份证书 SK_i 计算:

$$\begin{aligned} \alpha &= (\alpha_1, \alpha_2, \alpha_3) = (K_1^m, K_2 K_3^s, K_4, K_5) \\ &= ((g^{m_i} u v^s)^{1/(x+s_i)}, g^{s_i}, u^{s_i}) \end{aligned}$$

(2) 随机选取 $t_1, t_2, t_3 \in Z_n$ 对 α 进行盲化, 计算 $\sigma_1 = \alpha_1 \cdot h^{t_1}, \sigma_2 = \alpha_2 \cdot h^{t_2}, \sigma_3 = \alpha_3 \cdot h^{t_3}, \pi_1 = h^{t_1 t_2} \cdot (\alpha_1)^{t_2} \cdot (\alpha_2 w)^{t_1}, \pi_2 = u^{t_2} g^{-t_3}$, 在随机选取 $r_1, r_2 \in Z_n^*$, 计算 $H_i = H(r_1, r_2, m_i)$ 然后而得到最终的签名: $(\sigma_1, \sigma_2, \sigma_3, \pi_1, \pi_2, s, m_i)$ 及标书的 Hash 承诺 (H_i, r_1) .

(3) 待所有的用户把自己对标书的 Hash 承诺都发送到 BBS 后, AM 宣布开始投标;

(4) 用户将自己的标书签名 $(\sigma_1, \sigma_2, \sigma_3, \pi_1, \pi_2, s, m_i)$ 和 (H_i, r_1, r_2) 发送给拍卖行 AM, AM 宣布投标结束.

3.4 确定中标者

拍卖行 AM 首先根据用户的标书签名找出出价最高者,并验证其哈希承诺是否正确,签名是否正确,验证:

$$e(\sigma_1, w\sigma_2) = e(\pi_1, h)e(g^m; uv^s, g),$$

$$e(\sigma_2, u) = e(h, \pi_2)e(\sigma_3, g).$$

如果成立则说明签名合法标书有效,否则标书无效. AM 将追踪到的最高价位的标书签名及 Hash 承诺公布在 BBS 上.

RM 根据 AM 公布在公告栏上的中标信息找出使得等式 $(\sigma_2)^q = (g^{s_i})^q$ 成立的 s_i , 从而找出相应的 U_i , 并在 BBS 上宣布 U_i 为中标者.

4 协议分析

(1) 安全性分析

① 公平性: 开始投标时, 所有的竞标者都已对自己的标书进行了承诺, 所以当宣布投标结束后 Hash 承诺保证了标书无法被改动, 防止了拍卖行和用户的相互勾结, 用户在投标前无法从拍卖行那里得到其它标书的信息, 因此具有公平性.

② 匿名性: 假设 RM 是可信的, 包括 AM 在内如果没有注册中心 RM 的帮助, 任何人都不能得到竞拍者的任何信息.

③ 不可否认性: 由于注册中心可以根据中标者的签名撤销其匿名性, 因此中标者无法否认.

④ 不可伪造性: 要想伪造合法的签名标书, 必须知道 RM 的私钥, 根据 Diffie-Hellman 假设, 这显然是不能实现的.

⑤ 公开可验证性: 根据 AM 公布的中标者标书的签名和 Hash 承诺, 任何人都可以验证其合法性.

⑥ 不可联系性: 因为投标者的标书都经过了盲化, 所以找不出投标者和标书之间的联系.

(2) 效率性分析

在本方案中用户在加入群时没有用到交互式零

知识证明, 签名的长度短, 验证简单, 因此在计算量和通信量方面都有较大的改善, 而且还可以一次注册多次使用.

5 结束语

文中利用基于双线性对的群签名技术和 Hash 承诺, 提出了一个新的高效的密封式电子拍卖协议. 与以往基于群签名技术提出的电子拍卖协议相比该协议的通信量和计算量小, 可以防止拍卖行和用户的勾结, 也同时进行多件商品的拍买, 而且具有一次注册多次使用等性质. 同时文中方案也可以很容易改造成第二价位秘密投标协议.

参考文献:

- [1] 姬东耀, 王育民. 一个基于群签名的安全电子拍卖协议[J]. 电子学报, 2002, 30(1): 18-21.
- [2] 黄秀姐, 林群, 王燕鸣. 基于短群签名的安全电子买卖方案[J]. 中山大学学报, 2006, 45(6): 21-25.
- [3] Xavier B, Water B. Compact groupsignatures without random oracles[C]// IN Advances in Cryptology - EUROCRYPT 2006. Berlin: Springerlag, LNCS 4004: 427-444.
- [4] Wang ShaoHui. Modification and improvement on group signature scheme without random oracles[C]// Proc, ISECS'08. USA: Washington, 2008: 462-466.
- [5] 叶春涛, 张昊, 吴铤, 等. 一种安全的公认的电子拍卖方案[J]. 微电子学与计算机, 2008, 25(5): 225-228.
- [6] 宋春来, 殷新春, 孟纯煜. 基于部分盲签名和散列链的安全电子投票方案[J]. 微电子学与计算机, 2006, 23(9): 206-208.

作者简介:

赵建峰 男, (1984-), 硕士研究生. 研究方向是密码学与信息安全.

唐西林 男, (1962-), 博士, 教授. 研究方向为计算智能与信息处理、密码学.