

一个利用群签名的电子拍卖协议

苏云学¹, 祝跃飞¹, 闫丽萍²(1. 信息工程大学 信息工程学院, 河南 郑州 450002; 2. 信息工程大学 电子技术学院, 河南 郑州 450004)
(syx1991@163.net)

摘 要:利用群签名与可验证的秘密共享方案设计了一个新的密封投标的电子拍卖协议。在该协议中,多个拍卖者共同主持拍卖过程,所有的拍卖者通过可验证的秘密共享方案共享一个密钥,这使得投标者在投标时只需要一次加密,其计算量与拍卖者的数量无关;另外,中标者的身份是由群管理者根据中标者对投标消息的签名来确定的,所以一次注册后,投标者可同时参加多个拍卖活动,而不会泄露自己的身份。

关键词:电子拍卖;拍卖协议;投标;群签名**中图分类号:** TP393.08 **文献标识码:** A

Electronic auction protocol with group signature

SU Yun-xue¹, ZHU Yue-fei¹, YAN Li-ping²

(1. Net Engineering Department, Information Engineering University, Zhengzhou Henan 450002, China;

2. Electronic Technology Institute, Information Engineering University, Zhengzhou Henan 450004, China)

Abstract: Electronic auction is one of the methods of electronic commerce. A new sealed-bid electronic auction based on group signature and verifiable secret sharing scheme was proposed. In this protocol, multi-auctioneers participated in auction synchronously, and all auctioneers shared one key, therefore the bidder needed only one encryption in bidding, and the computation was independent of the number of auctioneers. In addition, the identity of the winner was identified by group manager according to signature of the winner's bidding message, therefore after registering once, bidder could participate in many auctions synchronously without disclosing his identity.

Key words: electronic auction; auction protocol; bid; group signature

0 引言

电子拍卖是网上价格协商的主要方式之一,它必须是安全的。电子拍卖的安全要求主要包括^[4]:(1)公平。应由出价最高的投标者中标,中标者必须支付规定的价格;(2)保密。除中标信息外,所有的其他投标信息应当保密;(3)匿名。除中标者的信息外,所有其他的投标者信息应当保密。

为了不泄露投标失败者的信息,文献[2]中使用了两个服务器 AM1 与 AM2,并使用代理不经意传输方法。AM2 是拍卖发布者,不参与拍卖过程,但由它确定中标者,AM1 是拍卖者。AM1 与 AM2 任何一方都不能泄露投标失败者的信息。但是,存在以下两个问题:(1)AM1 可能制造两份相同的消息,使得投标者的选择失败;(2)由于 AM2 知道投标者的密钥,可以伪造投标者的选择信息。文献[3]对文献[2]进行了改进,使用了可验证的代理不经意传输,但是仍不能避免第二种情况出现。Felix Brandt 设计了不需要拍卖者的拍卖协议,由投标者自行确定出中标者,物品出售者能对结果进行验证^[5,6]。但是投标者的通信量大,其计算量也随着投标者的增多而增加,而且其轮数多,协议复杂,特别是不利于第三方对拍卖过程进行监管,而某些时候是有这一要求的。文献[10]中的拍卖协议使用了群签名,由拍卖者把中标者的成员密钥传递给群管理者 GM,GM 根据该成员密钥确定中标者的

身份。但是,该协议中只有一个拍卖者,这就要求该拍卖者绝对可信;而且由于中标者的确定是由该投标者的成员密钥来确定的,而拍卖者是可获得该成员密钥的,所以,多次拍卖后,拍卖者就可以搜集大量中标者的成员密钥,之后,拍卖者就可以自行确定出中标者的身份,并可以确定出投标失败者的身份。事实上,GM 只需要投标信息的签名,就可以确定出该投标者的身份。

本文利用群签名^[8]以及秘密共享方案^[9]设计了一个新的拍卖协议。在该协议中,有多个拍卖者,所有的拍卖者共享一个私钥,并共同公布其公钥。投标者先到 GM 处申请成员证书,该成员证书可以长期使用。投标时,投标者对投标数据签名并加密,然后广播加密后的消息。所有的拍卖者共同对该消息进行解密。GM 根据中标者的签名确定出中标者的身份,而不需要中标者的成员密钥。

1 基本工具

\in_R 表示随机选取。 $H: \{0, 1\}^* \rightarrow \{0, 1\}^k$ 是好的哈希函数。 \parallel 表示连接。 p, q 是大素数, $q \mid p-1$, G 是 Z_p^* 的一个 q 阶子群,在 G 中求解离散对数是计算上不可行的。在 G 中选取生成元 g 。 $c[i]$ 表示串 c 的第 i 比特。 $a \in_R Z_q^*$ 。

定义 1 满足 $c = H(g \parallel h \parallel g^c)$ 的二元组 (c, s) 称为 h

收稿日期:2004-07-07;修订日期:2004-12-06

基金项目:国家 973 规划资助项目(G1999035804);国家自然科学基金资助项目(90204015);河南省自然科学基金资助项目(011105100)

作者简介:苏云学(1975-),男,四川仪陇人,博士研究生,主要研究方向:信息安全、协议设计与分析;祝跃飞(1962-),男,浙江杭州人,博士生导师,主要研究方向:为密码理论、信息安全;闫丽萍(1980-),女,山东沂源人,硕士研究生,主要研究方向:信息安全。

关于底 g 的离散对数知识证明, 记为 $SK\{\alpha \mid h = g^\alpha\}^{[8]}$ 。证明者如果知道整数 x , 满足 $h = g^x$, 则可如下计算:

证明者随机选取 $r \in_R Z_q^*$, 计算 $c = H(g \parallel h \parallel g^r)$, $s = r - cx$ 。

定义 2 设 $l \leq k$ 是安全参数。满足 $c = H(m \parallel y \parallel g \parallel a \parallel t_1 \parallel \dots \parallel t_l)$ 的 $(l+1)$ 元组 $(c, s_1, \dots, s_l) \in \{0, 1\}^k \times Z^l$ 称之为关于 g 与 a 的 y 的双重离散对数知识签名, 其中, 如果 $c[i] = 0$, 则 $t_i = g^{s_i}$, 否则 $t_i = y^{s_i}$ 。记为 $SKLOGLOG\{\alpha \mid y = g^\alpha\}^{(m)}^{[8]}$ 。证明者如果知道整数 x , 满足 $y = g^x$, 则可如下计算签名:

随机选取 $2^k \leq r_i \leq 2^{k+s} - 1$ ($1 \leq i \leq l$), 计算 $P_i = g^{r_i}$, $c = H(m \parallel g \parallel a \parallel y \parallel P_1 \parallel \dots \parallel P_l)$ 。计算 $s_i = r_i$, 若 $c[i] = 0$; 否则 $s_i = r_i - x$ ($1 \leq i \leq l$)。

定义 3 满足 $c = H(m \parallel y \parallel g \parallel a \parallel t_1 \parallel \dots \parallel t_l)$ 的 $(l+1)$ 元组 $(c, s_1, \dots, s_l) \in \{0, 1\}^k \times Z^l$ 称之为关于 g 与 a 的 y 的 e 次根的离散对数知识签名, 其中, 如果 $c[i] = 0$, 则 $t_i = g^{s_i}$, 否则 $t_i = y^{s_i}$ 。记为 $SKROOTLOG\{\alpha \mid y = g^\alpha\}^{(m)}^{[8]}$ 。证明者如果知道整数 x , 满足 $y = g^{x^e}$, 则如下计算:

选取 $r_i \in_R Z_q^*$ ($1 \leq i \leq l$), 计算 $P_i = g^{r_i}$, $c = H(m \parallel g \parallel a \parallel y \parallel P_1 \parallel \dots \parallel P_l)$ 。计算 $s_i = r_i$, 若 $c[i] = 0$; 否则 $s_i = r_i/x$ ($1 \leq i \leq l$)。

2 拍卖准备

本拍卖协议的参与方包括: 群管理者 GM、拍卖者 AU_i ($1 \leq i \leq M$), 投标者 B_i ($1 \leq i \leq N$), 在进行拍卖活动之前, 各方要进行一定的准备活动。

2.1 GM 生成群公钥

GM 选取一个 RSA 公钥 (n, e) , 一个大素数 $p, n \mid p-1$, 在 Z_p^* 中选取 n 阶循环群 G , 选取 G 的生成元 g, h , 且在 G 中求解离散对数是计算上不可行的; 选取元素 $a \in_R Z_n^*$ 模 n 的两个素因子都有大的乘法阶, 随机选取元素 u ; 选取一个常量 ε , 并设定密钥长度的上界 λ 。公开其群公钥为 $(n, e, G, a, u, g, \lambda, \varepsilon)$ 与 h 。最后, 选定并公开安全参数 l ($l \leq k$)。

2.2 拍卖者的共享密钥的生成

拍卖者 AU_i ($1 \leq i \leq M$) 共同生成一个共享密钥, 不需要第三方的参与, 该共享密钥可以多次使用。其生成过程如下:

(1) AU_i ($1 \leq i \leq M$) 在 Z_n 上随机生成两个多项式 f_i, h_i , 其中 $f_i(x) = a_0 + a_1x + \dots + a_{t-1}x^{t-1}$, $h_i(x) = b_0 + b_1x + \dots + b_{t-1}x^{t-1}$ 。 AU_i 广播 $B_{ik} = g^{a_{ik}h_{ik}} \bmod p$ ($k = 0, \dots, t-1$), $t < M$, 计算消息 $s_{ij} = f_i(j) \bmod n$, $s'_{ij} = h_i(j) \bmod n$, ($1 \leq j \leq M$), 秘密发送 (s_{ij}, s'_{ij}) 给 AU_j 。

(2) AU_j 对 (s_{ij}, s'_{ij}) 进行验证。 AU_j 检查 $g^{s'_{ij}h_{ij}} = \prod_{k=0}^{t-1} B_{ik}^{s_{ij}}$, 如果不成立, 则广播对 AU_i 的抗议。收到抗议后, AU_i 重新计算满足上式的 (s_{ij}, s'_{ij}) , 并广播。 AU_j 重新进行第二步。如果 AU_i 收到 $(t-1)$ 个抗议, 则被取消作为拍卖者的资格。

(3) 设 $H_0 := \{AU_j \mid AU_j \text{ 是有资格的拍卖者}\}$ 。所有的 $AU_j \in H_0$ 广播 $A_{jk} = g^{a_{jk}} \bmod p$ ($k = 0, \dots, t-1$)。 AU_j 验证 H_0 中的其他拍卖者的广播值是否正确, 即验证 $g^{s'_{ij}} = \prod_{k=0}^{t-1} A_{jk}^{s_{ij}}$ 是否成立。若均成立, 则计算公钥 $pk = \prod_{j \in H_0} g^{a_{jp}} = \prod_{j \in H_0} A_{jp}$ 。

AU_j 所拥有的秘密密钥份额为 $sk_j = \sum_{i \in H_0} s_{ij}$ 。

(4) 所有的拍卖者共同设计一个程序 program, 并选取一个对称密码算法, 其加、解密过程分别为 E_K, D_K , K 为密钥。 Program 根据所有拍卖者的输入, 对投标消息进行解密并验证投标者签名, 确定出中标者, 然后把该中标者的投标消息发送给 GM。由 GM 根据该消息确定出中标者的身份。

2.3 投标者注册

投标者 B_i ($1 \leq i \leq N$) 首先申请成为该投标组织的一员。 B_i 随机选取密钥 $x_i \in_R \{1, 2, \dots, 2^{k-1}\}$, 计算 $y_i = a^{x_i}$, $z_i = g^{x_i}$ 。并把 $y_i, z_i, SK\{x_i \mid y_i = a^{x_i}\}$ 秘密发送给 GM, GM 对此进行验证, 如果正确, 则计算 $cert_i = (y_i + u)^{1/e} \bmod n$, 并发送 $cert_i$ 给 B_i , $cert_i$ 就是 B_i 的成员证书。

3 投标

投标者 B_m ($1 \leq m \leq N$) 首先确定投标的数据 ($msg = amount \parallel date \parallel product$), 其中 $amount$ 为所投标的金额, $date$ 为投标时间, $product$ 为所被拍卖物品的描述。然后 B_m 如下计算投标消息:

(1) 随机选取 $\delta_1, \delta_2 \in_R Z_n^*$, 计算 $\tilde{g}_m = g^{\delta_1}$, $\tilde{z}_m = \tilde{g}_m^{y_m}$;

(2) 随机选取 $s_i, v_i \in_R Z_n^*$ ($1 \leq i \leq l$), 计算 $P_i = \tilde{g}_m^{s_i}$, $Q_i = \tilde{g}_m^{v_i}$, $c_1 = H(msg \parallel \tilde{g}_m \parallel \tilde{z}_m \parallel a \parallel P_1 \parallel \dots \parallel P_l)$, $c_2 = H(msg \parallel \tilde{g}_m \parallel \tilde{z}_m \parallel \tilde{g}_m^u \parallel a \parallel Q_1 \parallel \dots \parallel Q_l)$ 。

(3) 计算

$$r_i = \begin{cases} s_i, & c_1[i] = 0 \\ s_i - x_m, & c_1[i] = 1 \end{cases} \quad (1 \leq i \leq l)$$

与

$$t_i = \begin{cases} v_i, & c_2[i] = 0 \\ v_i / cert_m \bmod n, & c_2[i] = 1 \end{cases} \quad (1 \leq i \leq l)$$

$$V_1 = (c_1, r_i) = SKLOGLOG\{x_m \mid \tilde{z}_m = \tilde{g}^{x_m}\}^{(msg)}$$

确保 GM 能鉴别出 B_m 的身份,

$V_2 = (c_2, t_i) = SKROOTLOG\{cert_m \mid \tilde{z}_m \tilde{g}_m^u = \tilde{g}^{cert_m}\}^{(msg)}$ 证明了 B_m 是个合法的群成员。

(4) B_m 广播, ($A = g^{\delta_2}$, $B = E_{pk_{\delta_2}}(msg \parallel c_1 \parallel c_2 \parallel P_i \parallel Q_i \parallel r_i \parallel t_i)$)。 A, B 是投标者用拍卖者的共享密钥对投标数据加密后的消息, 保证至少有 t 个拍卖者合作解密后, GM 才能鉴别出中标者。

4 确定中标者

在投标过程结束后, 拍卖者收到所有投标者广播的投标消息。拍卖者、program 与 GM 共同确定出中标者及其出价。过程如下:

(1) 拍卖者 $AU_j \in H_0$ 在收到这些消息 (A, B) 后, 计算 A^{sk_j} , 并通过秘密信道发送给 program。

(2) Program 在收到至少 t 个 H_0 中的拍卖者的消息后, 对投标者的消息解密, 即计算 $A' = \prod_{k=0}^{t-1} A^{sk_k}$, $D_{A'}(B)$, 验证投标者的签名, 计算 $c'_1 = h(msg \parallel \tilde{g}_m \parallel \tilde{z}_m \parallel a \parallel P_1 \parallel \dots \parallel P_l)$ 与 $c'_2 = h(msg \parallel \tilde{g}_m \parallel \tilde{z}_m \parallel \tilde{g}_m^u \parallel a \parallel Q_1 \parallel \dots \parallel Q_l)$, 然后检验

$$P_i = \begin{cases} \tilde{g}_m^{s'_i}, & c'_1[i] = 0 \\ \tilde{z}_m^{s'_i}, & c'_1[i] = 1 \end{cases} \quad (1 \leq i \leq l)$$

$$Q_i = \begin{cases} \tilde{g}_m^{t'_i}, & c'_2[i] = 0 \\ (\tilde{z}_m \tilde{g}_m^u)^{t'_i}, & c'_2[i] = 1 \end{cases}$$

如果成立,则该投标消息是有效的,根据所有有效的投标消息的确定出中标的 *amount* 投标消息,最后把该中标消息明文发送给 GM。

(3) GM 收到中标消息后,验证该消息的签名。如果签名有效,则在投标者数据库中搜索其密钥 y_m 满足 $\bar{g}_m^{y_m} = \bar{z}_m$ 的投标者。该投标者即是中标者,并公布 $SK\{y_m \mid \bar{g}_m^{y_m} = \bar{z}_m\}$ 与中标消息。

所有的投标者均可对中标者及其出价的有效性进行验证。在大数分解问题与离散对数问题是困难的假设前提下,只有持有群成员密钥的投标者才能构造出自己投标消息的正确签名,该签名的正确性可通过群公钥进行验证,所以,通过确定中标者对中标消息的签名与中标消息中的 *amount* 是否正确,就可验证该中标者及其出价是否有效。

5 结语

本文所提出的电子拍卖协议使用了群签名,这使得该协议是可扩展的,即增加投标者并不会引起投标者计算量的增加。同时该协议采用了可验证的秘密共享方案,这使得即使有少数不诚实的拍卖者也会被检测出来,不会影响拍卖结果。另外,因为中标者的身份是由 GM 根据中标者对投标消息的签名来确定的,所以即使所有的拍卖者合谋也不能泄露投标者的身份。

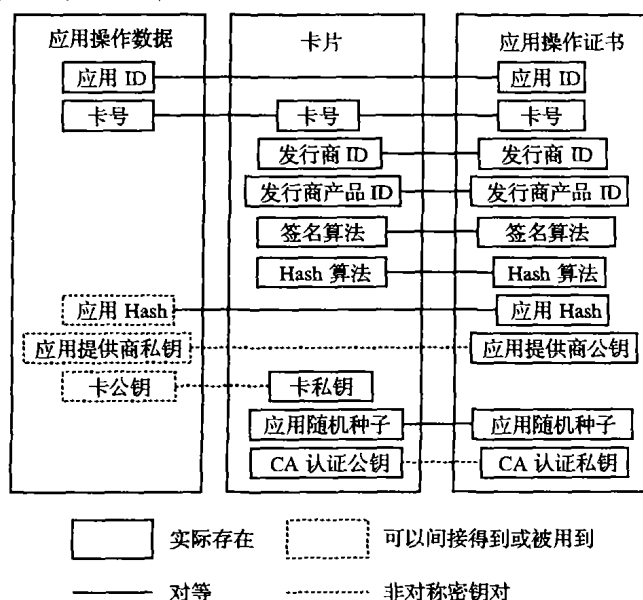
通过变化 program 中确定中标者及其应出价的规则,本文的电子拍卖协议可变化成最高价拍卖协议、次高价拍卖协议或者是 $(M+1)$ 价格拍卖协议。让中标者支付最高价时就成为最高价拍卖协议;而让中标者支付次高价,并公布次高价投标消息,此时就成为次高价拍卖协议,如果同时使 M 个投

标者中标,且均支付第 $(M+1)$ 高价时,就成为 $(M+1)$ 价格拍卖协议。

参考文献:

- [1] OMOTEA K. A study On Electronic Auction[D]. school of Information Science Japan Advanced Institute of Science and Technology, 2002.
- [2] NAOR M, PINKAS B, SUMNER R. Privacy Preserving Auctions and Mechanism Design[A]. proceeding of ACM conference on Electronic Commerce[C], 1999. 120 - 127.
- [3] JUELS A, SZYDLO M. A Two-Server, Sealed-Bid Auction Protocol [A]. Financial Cryptography '02[C], 2002.
- [4] BOYD C, MAO W. Security Issues for Electronic Auctions[R]. HP Labs Technical Report, 2000.
- [5] Felix Brandt. Fully Private Auctions in a Constant Number of Rounds. Financial Cryptography 2003 conference proceedings[C]. Gosier, Guadeloupe, 2003.
- [6] BRANDT F. A Verifiable, bidder-resolved Auction Protocol [A]. Proceedings of the 5th International Workshop on Deception, Fraud and Trust in Agent Societies[C], 2002. 18 - 25.
- [7] KIKUCHI H. $(M+1)$ st - Price Auction Protocol [A]. Proceeding of the 5th Annual Conference on Financial Cryptography. Volume 2339 of Lecture Notes in Computer Science[C]. Springer 2001. 351 - 363.
- [8] CAMENISCH J, STADER M. Efficient Group Signature Schemes for Large Groups [A]. Advances in Cryptology - Crypto'97[C]. Springer Verlag, 1997.
- [9] KIM J, KIM K, LEE C. An Efficient and Provably Secure Threshold Blind Signature [A]. ICISC'2001[C], 2001.
- [10] NGUYEN KQ, TRAORE J. An online public auction protocol protecting bidder privacy [A]. Proc. of ACISP 2000, LNCS 1841[C]. Springer-Verlag, 2000. 427 - 442.

(上接第 156 页)



1) 应用提供商密钥对。应用提供商公钥放在应用操作证书中,最终传给卡片,其私钥用于加密 KTU,从而达到加密应用操作数据中需要保密的数据的目的。在实际运用中,为了提高安全性,产生应用操作数据由应用提供商负责。

2) 卡密钥对,指用来实现应用操作的一对非对称密钥。此密钥对对于卡来说是特有的。在发卡时,由发行商向 CA 进行申请,并得到对应的公钥证书。在卡公钥使用时,可以从

卡的公钥证书中得到卡的公钥并可检验其真实性。

3) 应用随机种子,其目的是防止对同一应用进行重复下载、删除操作。应用 ID 与随机种子会记录在卡的应用历史目录中,卡会阻止重复的操作,提高安全性。

4) 签名算法与 Hash 算法用于标识应用操作证书所使用的算法,卡与应用操作证书必须匹配。

5) CA 认证密钥对。CA 提供一对认证密钥对,其私钥用于对应用操作证书的签名,而其公钥会公开于卡发行商,在发卡时写入卡中。

5 结语

本文运用 PKI 技术建立了多应用管理平台,并详细设计了应用操作数据(AOD)和应用操作证书(AOC)的内容与实现机制,最后分析了整个系统的安全性保证。通过此方案的实施,安全地实现了“一卡多用”系统中应用的动态下载、更新和删除。

参考文献:

- [1] 徐中华,刘玉珍,张焕国. 一种新的“一卡多用”智能卡模型[J]. 计算机工程, 2003, 29(5): 43 - 45.
- [2] Global Platform[EB/OL]. <http://www.globalplatform.org/>, 2004.
- [3] TOJI R, WADA Y, HIRATA S, et al. A Network-Based Platform for Multi-Application Smart Cards [A]. Fifth IEEE International Enterprise Distributed Object Computing Conference [C]. Seattle, Washington, September 04 - 07, 2001.
- [4] ELLIOTT J. MAOS tales [J]. IEEE Computing & Control Engineering Journal, 2002, 13(1): 43 - 46.
- [5] MAOSCO Ltd. MULTOS KMA File Interface Formats (external) [Z]. <http://www.multos.com>, 2004.