一个基于群签名的安全电子拍卖协议

姬东耀[1,2],王育民[2]
(1. 中国科学院研究生院信息安全国家重点实验室,北京 100039;2. 西安电子科技大学 ISN 国家重点实验室,陕西西安 710071)

摘 要: 基于群签名技术和 Shamir's 门限方案,设计了一个适于分布式松耦合广播/预约系统使用的安全电子拍卖协议. 协议不仅保证了投标者对所投价位的不可否认性和匿名性,而且保证了拍卖代理对接收标书的不可否认性. 与先前工作相比,本文的方案提供了较高的安全特性,而且更适合于分布式大规模的网上拍卖.

关键词: 分布式系统; 安全; 电子拍卖; 广播/预约结构; 群签名
中图分类号: TP393 **文献标识码**: A **文章编号**: 0372-2112 (2002) 01-0018-04

A Distributed Secure Electronic Auction Protocol Based on Group Signatures

JI Dong-yao[1,2], WANG Yu-min[2]
(1. *National Key Laboratory of Information Security Graduate School, Academia Sinica, Beijing* 100039, *China*;
2. *National Key Laboratory on ISN, Xidian University, XI'an, Shaanxi* 710071, *China*)

Abstract: A new distributed secure electronic auction protocol based on group signatures and Shamir's threshold secret sharing scheme is proposed. This protocol is designed for a loosely coupled broadcast/subscribe architecture. The protocol not only guarantees the non-repudiation and anonymity of the bidder, but also ensures the non-repudiation of the bid received. Compared with previous work, our protocol can provide more security, and is suitable for large scale distributed auction.

Key words: distributed systems; security; electronic auction; broadcast/subscribe architecture; group signatures

1 引言

拍卖是常用的确定价格的交易活动,Internet 为分布式拍卖提供了极好的环境,它为许多人参与到拍卖中创造了机会. 分布式电子拍卖系统一般由卖方委托一些代理拍卖商进行拍卖,投标者可以向任一代理拍卖商提交标书,系统有一注册机构负责代理拍卖商的授权和投标者的登记,以防有争议时调停. 本文研究密封式安全电子拍卖,其中秘密标被广播竞争一拍卖物的所有权,投标期截止后秘密标被打开并按照一些公开的原则选择中标者. 分布式安全电子拍卖需要满足:(1) 至少有一个正常拍卖代理服务器决定拍卖开始,投标才能开始. (2) 一个正常拍卖代理服务器停止接收标值,至少要有一个正常拍卖代理服务器决定投标期结束. (3) 投标者的身份和标的内容在投标期结束前不能泄露. (4) 投标期限后接收到的标无效. (5) 投标者能证明他们的标在投标期限内被接收. (6) 中标者按照一些公开的确定的规则决定,并保证中标者支付相应的钱而且可以得到拍卖物. 松耦合分布式系统是由多个计算机经过通信网络连接而成,通信网络可以是局域网,也可以是远程网,计算机之间采用报文交换方式通信,与紧耦合系统相比,没有很强的进程组成员的概念,不需要原子多路发送,时常采用广播/预约结构[2],系统成员通过一条虚拟信息总线发布/预约消息进行通信. 它的极大的灵活性,自适应性和效率非常适合于广域网. 在广播/预约系统中,消息有一个主题域与内容域,广播者在一些主题下广播消息,用户预约自己关心的主题并接收在那些主题下广播的消息. 主题可以层次化地组织,消息内容和格式能按照应用的需要进行定义,同时广播/预约系统也可提供广播者和预约者的匿名性. 对于有一个拍卖主题的拍卖方案,用变址数标识一个特定的拍卖并表明消息是否发给拍卖代理服务器或投标者,拍卖代理服务器和投标者都广播和预约由协议定义的一些主题下的适当消息. 对于一特定的拍卖,拍卖代理服务器及其数目都是确定的. 因为网络不是完全可靠的,消息可能被延迟,丢失或乱序,但协议不容忍任意的网络失败,如一个攻击者截获所有消息仅让他自己的消息通过. 我们假定的消息将在一定时间内广播到一充分大的网络中,一些路由失败或攻击,不管它是永久的还是瞬时的,只能影响网络中的一个比较小的部分. 同时假定一些代理拍卖服务器也可能是不诚实的,但可以利用 Byzantine 模型[3]把它和拍卖服务器协议分开,取消它广播的消息和预约的消息;拍卖代理服务器和投标者对消息加密和签名要使用公钥密码系统,所以投标前需要有一证书管理机构(CA)为他们提供公钥证书,而且这必须和拍卖活动分开进行.

收稿日期:2000-05-10;修回日期:2001-07-19
基金项目:国家自然科学基金(No. 19931010);高等学校博士点基金(No. 2000070101)

2 原有方案的分析

Yao 的百万富翁协议[4]可以使两个百万富翁比较谁更有钱而不公开他们各自的财富,这样的协议可以用于拍卖协议.这种拍卖协议的优点是只有中标者的出价是公开的,非中标人的价格,除了他自己以外,拍卖代理和其他投标者都不知道.然而,其缺点是投标人在每次拍卖代理询问他的时候,他可以随时改变其投标值而不会被发现.其次,这种拍卖协议的效率较低,只适用于小型拍卖,而且协议还不能保证中标者一定能付他承诺的钱.Franklin 和 Reiter 基于可验证签名共享技术,给出一个利用电子现金秘密投标进行电子拍卖的方案[1],方案成功防止了分布式拍卖中单个代理拍卖服务器改变标值或私自决定中标者.同时保证了中标者的公正性和从中标者以电子现金形式收集支付.然而,每个投标消息和拍卖代理服务器同步消息发送需要原子多路发送原语,在一个大的系统中这可能成为一个瓶颈.而且没有中标者的电子现金需要退还回去,而用户却没有拍卖代理服务器的不可否认证据;投标者的身份对拍卖代理商是公开的,不能保证投标者的消费隐私权.Ki Kuchi,Harkavy 和 Tygar 提出了一种基于 Shamir 秘密共享方案的一种密封式拍卖协议[5].该协议克服了 Franklin 和 Reiter 协议的缺点,保证了即使是拍卖代理也不知道任何投标者的投标值.但该协议却不能保证中标者一定能付钱.针对这些问题,本文提出一个新的拍卖协议,克服了上述缺陷,取得了比较高的安全特性.

3 新的电子拍卖协议

本文所提协议基于分布式松耦合广播/预约系统,可以用某种承诺标值投标.

群签名技术:协议采用了群签名密码技术,群签名允许群体中的任一成员代表群体签名,该签名可用一公开的群公钥验证,同时它还实现了签名者的匿名性.发生争议时可由群管理机构识别出签名者.目前公认的比较有效的群签名方案是 CS97 群签名方案[6],它首次提出了群公钥和签字长度都不依赖于群成员的个数的群签字方案,为群签字走向实用排除了最大的障碍.该方案基于 RSA 公钥体制,Schnorr 签名体制及双重离散对数的知识签名 $SKLOGLOG$ 和离散对数的 e 次根的知识签名 $SKROOTLOG$.具体描述如下:

创建:注册机构选一 RSA 公钥 (n, e),一个 n 阶循环群 $G = < g >$,元素 $a \in Z_n^*$ 模 n 的两个素数因子有大的乘法阶,私钥长度的上界 λ 和一个常数 ε.这些常数的选取应使在 G 中计算以 g 和 a 为底的离散对数及以 g 为底的离散对数的 e 次根的计算是不可行的.群公钥为 $Y = (n, e, G, g, a, \lambda, \varepsilon)$.

加入:当 Alice 要参加投标时,她选一私钥 $x \in \{0, 1, \cdots, 2^{\lambda} - 1\}$,计算 $y = a^x \pmod n$ 及她的成员钥 $z = g^y$.她把 y, z 及对 y 的承诺(如她对 y 的签名)发送给注册机构并向其证明她知道 y 关于底的离散对数(可以用离散对数的知识签名).当注册机构确信她知道这一离散对数时,就发给她一个成员证书:$v = (y + 1)^{1/e} \pmod n$.

签字:为对消息 m 签字,计算以下数值:

$\tilde{g} = g^r$,对随机选取的 $r \in_R Z_n^*$;$\tilde{z} = \tilde{g}^y$;

$V_1 = SKLOGLOG[\alpha: \tilde{z} = \tilde{g}^{a^{\alpha}}](m)$;$V_2 = SKROOTLOG[\beta: \tilde{z}\tilde{g} = \tilde{g}^{\beta}](m)$

得到对 m 的签名为 $(\tilde{g}, \tilde{z}, V_1, V_2)$.

验证:可以通过检验知识签名 V_1 和 V_2 的正确性来验证签字,因为签名实际上就是证明 Alice 属于这个群体.V_1 用来证明:对于 Alice 知道的一个 α,$\tilde{z}\tilde{g}$ 一定具有形式 $\tilde{z}\tilde{g} = \tilde{g}^{a^{\alpha}+1}$;$V_2$ 用来证明:Alice 知道 $a^{\alpha} + 1$ 的 e 次根.

打开:给定对消息 m 的一个签字 $(\tilde{g}, \tilde{z}, V_1, V_2)$,注册机构可通过检测对哪一个投标者 P

$$\tilde{g}^{y_P} = \tilde{z}$$

来确定签名人的身份(其中 y_P 是 P 的成员钥 z_P 关于底 g 的离散对数).

协议描述:假定有 n 个拍卖代理服务器,用 $S_1, S_2, \cdots, S_n$ 表示.拍卖开始前,注册机构为这 n 个拍卖代理服务器秘密产生一共享密钥 δ,并把这一密钥 δ 用自己的私钥签名,然后分别用 $S_1, S_2, \cdots, S_n$ 的公钥加密发送给各拍卖代理服务器.对于一确定的拍卖,n 是固定的.服务器 S_i 用 s_i 标识;投标者用 B_j 表示,用 j 标识;若要保持投标者的匿名性,投标前投标者 B_j 产生一私有的大的随机数 r_j,计算 $h(r_j) = b_j$ 作为投标者 j 的投标身份,并把 b_j 登记在注册机构它的记录中.而 j 的真实身份不出现在标书中,只有注册机构知道投标者的真实身份.其中 h 为一消息杂凑函数(如 MD5)[7].拍卖用 aid 来标识,所有与这一拍卖有关的消息都公布在这一主题下.对于消息 a,$[a]^i$ 表示对消息 a 用服务器 S_i 的公钥进行加密;$[a]_i$ 表示对消息 a 用服务器 S_i 的私钥进行签名,消息 a 可以从 $[a]^i$ 中恢复,任一协议参加方都可以对签名进行验证.协议中所有从代理拍卖服务器中发出的消息必须签名,以便这些消息得到其他服务器的认可,并由此推断服务器的当前状态.协议中使用了一个 $(t + 1, n)$ 门限方案,其中 t 是容许出错的服务器的最大数 $(n \geq 3t + 1)$.$SH_i(s)$ 表示 shmir 门限方案[8]中秘密 s 的第 i 份.

S(1) **开始投标**　当代理拍卖服务器 S_i 按预定时间决定拍卖开始时,它广播一个开始消息:$aid \parallel s_i \parallel [aid, s_i, START]_i$.当 S_i 从至少 $t + 1$ 个不同服务器收到开始消息时,它认为投标开始并开始接收投标者发来的投标消息.

B(1) **广播标值**　如果一个投标者 B_j 决定投一个标值 y_j 时,y_j 是某种承诺标值数据.B_j 按照 shmir 门限方案把 $y_j \parallel b_j$ 分成 n 份:$x_{ij} = SH_i(y_j)$,$i = 1, \cdots, n$.然后产生投标消息:$M_j = aid \parallel b_j \parallel [x_{1j}]^1 \parallel \cdots, \parallel [x_{nj}]^n$.并把它向所有代理拍卖服务器广播.

S(2) **标值接收**　代理拍卖服务器 S_i 在投标期限内收到投标者 B_j 产生投标消息 M_j 时,它广播一个收据消息:$aid \parallel b_j \parallel s_i \parallel [\text{hash}(aid, T_i, M_j)]_i$ 其中 T_i 为一系统时戳,hash 可能是一些标准的单向杂凑函数(如 MD5).

B(2) **提交标值**　当一个投标者 B_j 从服务器 S_i 收到一个收据时,它通过检查 hash 值上的签名来验证收据的有效性,如果投标者 B_j 从至少 $2t + 1$ 个不同服务器收到有效收据时,

就进入提交阶段. 这时, B_j 广播一用他的群签名私钥 x 签名的确认消息 $aid \| b_j \| [\mathrm{hash}(aid, M_j)]_x$, 以示其收到足以恢复标书的有效收据, 并为所投标值负责. 按照我们正常服务器的假定, 最终所有正常服务器将会收到并认可所有正确格式的标; 所有正常投标者也会收到各拍卖代理服务器的正确收据.

S(3) **结束投标** 当 S_i 按预定时间准备结束投标时, 它广播一个签名的结束消息: $aid \| s_i \| [aid, s_i, close]_i$ 如果 S_i 从至少 $t+1$ 个不同服务器收到结束消息时, 它决定投标期结束并停止接收投标者标值.

若 S_i 共收到 L_i 个标, 令 R_i 表示其标值由 S_i 收到的投标者的标号的集合, R_i 中有 L_i 个元素, 对于每一 $k \in R_i$, S_i 解密 B_k 所投标值中用它的公钥加密的那一份, 得到 x_{ik}, 然后广播一个它收到的标集的指纹消息:

$$aid \| s_i \| [\{\mathrm{hash}(aid, (b_k, x_{ik}, M_k))\}_{K \in R_i}]_i$$

这个指纹包含一列三元组的 hash 值的签名, 每个三元组包含投标者标识, S_i 的分享秘密及完整的投标消息.

S(4) **开标** 在一限定的时间内, 所有正常服务器都停止接收标并公布它们的指纹, 因为至多有 t 个服务器出错, 所以至少有 $n-t$ 个指纹被公布. 在一限定时间内, 每一个正常服务器 S_i 将从所有其他正常服务器收到指纹, 它们重新公布各自收到的指纹, 并把其中不一致的指纹当作是从一出错的服务器发来的, 从而把它剔除. 这样所有正常服务器最后收到同样的指纹消息的集合. 最后, S_i 公布它收到的标的集合消息, 这一标的集合消息先用 S_i 的私钥签名然后用 n 个拍卖代理服务器的共享密钥 δ 加密. 标的集合消息中包含 hash 到指纹的哪些标的集合. 这个标集消息是: $aid, s_i, [\{(b_k, x_{ik}, M_k)\}_{k \in Ri}]i$, 只有 n 个拍卖代理服务器能得到这些消息.

S(5) **标的重构** 在一限定的时间内, 每个正常服务器 S_i 将收到从别的正常服务器发来的所有标集消息, 当 S_i 收到从 S_j 发来的标集消息时, 它首先计算这一消息的 hash 值看它是否与从 S_j 发来的指纹匹配, 如果不匹配, 则意味着 S_j 是一出错的服务器, 从而这一消息将被 S_i 和其他正常服务器剔除. 它们重新公布各自收到的标集消息, 并把其中不一致的标集当作是从一出错服务器发来并把它剔除. 重新公布的标集消息都是用各拍卖代理服务器的共享密钥 δ 加密的, 窃听者不能获得最后确定的标集消息, 这样所有正常服务器最后收到同样的标集消息的集合.

S_i 重构 B_j 所投标如下: 令 T_{ik} 表示这样的服务器 S_j 的标号的集合: S_i 从 S_j 收到了包含 M_k 的标集消息.

对于每一 $k \in T_{ik}$, S_i 能提取 B_k 所投标 y_k 中 S_j 能解密的那一份, 即 x_{jk}, 计算 $[x_{jk}]^j$ 并与 M_k 的第 j 份比较, 如果一样, 则说明 x_{jk} 是有效的, 可以用来重构标值 $y_k \| b_j$.

如果 T_{ik} 至少包含 $t+1$ 个元素, 那么 S_i 能利用门限方案构造一个值 $y'_k \| b'_j$, 它应该等于 $y_k \| b_j$.

如果存在一些 j 使得 $[SH_j(y'_k)]^j \neq [x_{jk}]^j$, 其中 $[x_{jk}]^j$ 是从 M_k 中提取的, 那么 S_i 剔除 B_k 所投标.

按上述方法 S_i 能重构标集并按照一些公开的规则决定中标者. 所有正常的拍卖代理服务器都将构造出同样的标集, 因为正常的代理拍卖服务器占 2/3 以上, 所以大多数服务器同意最后的选择.

S(6) **宣布中标者** 每个正常的拍卖代理服务器 S_i 公布签名消息: $A_{id} \| b_j \| [aid \| b_j]_i$ 当投标者 B_j 得到至少 $2t+1$ 个这样的消息, 同时卖方与注册机构也收到至少 $2t+1$ 个这样的消息, 拍卖成功, 中标者可以向卖方出示他私有的随机数 r_j, 卖方验证 $h(r_j) = b_j$, 双方即可成交. 如有争议, 注册机构可以利用各方拥有的证据调停.

4 新协议的安全性分析

新协议满足了分布式安全拍卖的基本需求. 新协议中投标者和拍卖代理服务器通过广播/预约机制通信, 所以适合于大规模的网上拍卖, 而且通过消息的广播与预约剔除掉不一致的消息, 进而剔除掉传递这些不一致消息的服务器, 使系统能容忍一些拍卖代理服务器的出错. 所有正常拍卖代理服务器按照规定的时间广播投标开始和结束消息, 并严格遵守协议规程, 投标者则不断呈递自己的标书, 所以剔除掉一些出错服务器后, 存在至少 $t+1$ 个服务器最后收到同样的标集消息的集合, 从而保证投标者标书的恢复以及中标者的确定.

新协议采用了 $(t+1, n)$ 门限方案, 因为至多有 t 个拍卖代理服务器出错, 所以即使它们都相互勾结, 也不会恢复出标值或宣布中标者, 所以拍卖中 1/3 服务器的出错, 不会影响投标结果.

新协议中投标者广播的消息用拍卖代理服务器的公钥加密, 而拍卖代理服务器广播的消息或是一些消息摘要或是用各拍卖代理服务器的共享密钥加密的消息, 使得拍卖过程中传输的消息具有良好的保密性. 而且各拍卖代理服务器广播的消息都有它们的签名, 使得每个服务器都要为它自己的行为负责.

新协议可采用承诺标值投标. 群签名用来保证投标者对所投价位的不可否认性. 如果拍卖对象是电子产品, 如软件或 postscript 文件, 每个投标者放一临时公钥在它的标里, 文件可以用中标者临时公钥加密传输, 我们可以使用 $(t+1, n)$ 门限方案把文件分拆, 分别分给 n 个拍卖代理服务器, 每个代理服务器公布用中标者提供的公钥加密的分享. 中标者可以用他从 $t+1$ 个正常服务器得到 $t+1$ 份分享重构原文件, 并且临时公钥不需要证书, 因为这关系用户自己的利益.

新协议提供了收据服务, 这在许多金融活动中时常是必需的, 投标者可以用它来证明他的标书在投标截止期前被代理拍卖服务器收到.

采用群签名技术对代理服务器承诺, 既保证了投标者的匿名性, 也保证了投标者对标值的不可否认性. 拍卖主要要求公正性, 实时性要求不是很高, 群签名的效率是可以忍受的.

如果按照一些公开的确定性的规则最后没有确定出赢者, 可从步骤 1 开始下一轮投标.

5 结论

基于 Shamir's $(t+1, n)$ 门限方案, 群签名技术设计了一个适于分布式松耦合广播/预约系统使用的安全电子拍卖协

议.协议除保证了安全分布式拍卖的基本需求外,还保证了投标者和拍卖代理服务器的不可否认性及投标者的匿名性,在分布式松耦合广播/预约系统中实现了安全性和容错性,与先前工作相比,我们的协议提供了更高的安全特性,而且适合于分布式大规模拍卖.

参考文献:

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

[2] B Oki ,M Pfluegl ,A Siegel ,D Skeen. The information bus-an architecture for extensible distributed systems [J]. ACM Operating Systems Review ,1993 ,27(5) :58 - 68.

[3] L Lamport ,R Shostak ,M Pease. The byzantine generals problem [J]. ACM Transactions on Programming Languages and Systems. 1982 ,4 (3) :382 - 401.

[4] Yao A C. Protocols for secure computations [A]. Proceeding of the 27th IEEE Symposium on Foundations of Computer Science [C] ,1986 :162 - 167.

[5] H Kikuch ,M Harkavy ,J D Tygar. Multi-round anonymous auction protocols [A]. Proceedings of the First IEEE Workshop on Dependable and Real-Time E-Commerce Systems [C] ,1998 :62 - 69.

[6] Jan Camenisch ,Markus Stadler. Efficient group signature schemes for large groups [A]. Advances in Cryptology-Crypto97 [C] ,Lecture notes in computer science 1294 ,Springer-Verlag 1997 :410 - 424.

[7] R Revest. The MD5 message-digest algorithm [S]. Internet RFC 1321 , 1992.

[8] A Shamir. How to share a secret [J]. Communication of ACM ,November ,1979 ,22(1) :612 - 613.

作者简介:

姬东耀　男.1965 年 3 月出生于陕西省靖边县.西安电子科技大学计算机学院讲师,博士生,研究方向为网络安全与电子商务.

王育民　男.1936 年出生.西安电子科技大学通信工程学院教授,博士生导师,长期从事信息论、编码与密码学的教学和科研工作.e-mail :ymwang @xidian. edu. cn.