文章编号:1005－0523(2006)02－0092－04

电子招投标系统的安全性研究

温雅敏[1],涂淑琴[2],祖建樱[3]

(广东商学院,广东 广州 510320;2.华南农业大学 信息学院,510640;3.南昌大学 软件学院,江西 南昌 330029)

摘要:对电子招投标系统的安全性问题进行了分析,通过引入新型身份认证机制、并在 Shamir 门限可验证秘密共享方案的基础上进行改进,较好地解决了其中的问题.

关 键 词:电子招投标;密钥更新;身份认证;秘密共享

中图分类号:TP391 **文献标识码**:A

1 前言

21 世纪以来,电子政务成为中国信息化领域最受关注的发展重点.电子招投标系统作为其中的重要组成部分是实现中国政府信息化的重要环节;该系统的实现可以节省政府采购成本,扩大投标方的数量,是提高政府采购效率、体现政府采购"公开、公正、公平"原则的必然选择.然而,除了现实环境中存在的电子支付、评标体系、法律保障等问题的限制,我们认为当前的电子招投标系统的主要问题是它不能保证招投标的公正性和安全性,只是起一个信息发布平台的作用,没有实现真正意义上的电子招投标系统.因此,本文通过引进密钥更新机制确保系统对身份的认证,并运用改进后的秘密共享方案实现对标底的保密,从而较好地解决了在电子招投标系统中存在的安全性问题.

2 E-bidding 安全隐患

针对电子招投标系统而言,安全隐患有其特殊性,主要表现在以下几点:

1) 投标者身份的伪冒:由于网上操作和交易的特殊性,没有现实生活中面对面的操作,因此,如果有非法者盗得投标公司的密钥,他就可以伪冒投标者的身份进行非法操作,这对投标公司乃至招标实体都将造成巨大的损失.

2) 投标书的泄密:首先,标书在传送过程中被非法者盗得;其次,由于投标代理或招标者的违规操作,造成在开标之前投标者的投标信息被公开,这也将损害投标者的权益,破坏投标的公平性.

为解决上述问题,本文借鉴一次性口令原理[4],设计了一种新型身份认证机制;并在 Shamir 门限可验证秘密共享方案的基础上进行改进以实现对标底的保密设计.

3 新型身份认证

身份认证中安全的最大威胁就是密钥泄密,对密码的分析造成的危害远远没有密码泄漏的危险大.因此,在本系统当中,借鉴一次性口令原理对密钥进行更新,设计了一种新的身份认证机制.

3.1 基于一次性口令原理的密钥更新

一次性口令是每次使用后口令内容都发生变化的口令,系统不是给用户分配一个静态口令,而是分配一个静态数学函数,系统给函数提供变量

收稿日期:2005－06－25

作者简介:温雅敏(1981－),女,江西宁都人,助教,硕士研究生,研究方向为电子商务与信息安全.

值，用户计算和返回函数值．这个系统也称作问答．其工作原理如图 1 所示．

用户(U) $\xrightarrow{(ID_U, f^n(x_0))}$系统($S$)

第一次登录：$\xrightarrow{(ID_U, f^{n-1}(x_0))}$验证 $f^n(x_0)=f(f^{n-1}(x_0))$是否成立

第二次登录：$\xrightarrow{(ID_U, f^{n-2}(x_0))}$验证 $f^{n-1}(x_0)=f(f^{n-2}(x_0))$是否成立

依此类推

……

图 1　一次性口令原理

1) 核心思想：客户端系统使用单向函数，以用户、密钥(种子)作为输入，生成一系列一次性私钥．其作用是使得攻击者即使得到了某一次登录的私钥，仍然不能伪造其他任一阶段的签名．

2) 密钥更新过程：用户从注册一个公钥 PK 和保持私人相应的密钥(我们定义为 SK_0)开始．在公钥 PK 被期望有效的时间内，公钥保持不变，用户每次登录时根据一次性口令原理生成不同密钥进行签名，验证服务器利用上一次用户成功登录时的数据来验证当前的数据．详细来说，在 i 周期开始时候，用户将产生的种子(Seed)利用一个公共的单向函数 f 计算 $n-i$(计数值 Counter)次获得 SK_i，服务器通过计算 $f(f^{n-i})$是否等于 SK_{i-1}来验证其合法性，之后删除 SK_{i-1}并保存 SK_i．此时攻击者不能从 SK_i 中获取老的密码，因为后者是前一个密码的单向函数．

3.2　新型身份认证流程

为实现拥有密钥更新机制的身份认证，要经过四个过程：注册、密钥生成、签名、身份验证、密钥更新，如图 2 所示．下面分别从各个过程进行讲述．这里假定投标者为 A，招投标中心也就是注册中心为 B．

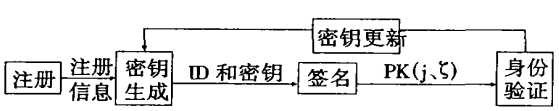

图 2　新型身份认证流程

注册：商家向注册中心递交个人注册信息 lg：$A \xrightarrow{lg} B$

密钥生产算法 KG：B 收到 A 的注册信息 lg 后，验证其合法性，若合法，则选用一个安全参数 $k\in N$、方案运行的所有参数、以及时间序列 T，返回 A 的标识号 ID_A、一个基本公钥 PK 和相应的基本密钥 SK_0，并向 A 颁发证书，A 成为该证书的合法持有者．

签名算法 Sgn：用当前密钥 SK_j 和消息 M 来返回一个第 j 次登录的签名 M'．我们写为

$$(j,\xi)\xleftarrow{R} Sgn_{skj}(M)$$

签名总是由当前登录次数 j 和标志 ξ 构成．

身份验证 vf：用公钥 PK，消息 M 和候选签名 (j,ζ)来返回一位 b，1 表示接受，0 表示拒绝．我们写为

$$b\leftarrow Vf_{PK}(M,(j,\xi))$$

密钥更新算法 Upd：服务器从数据库读取种子 Seed、当前计数值 Counter．根据单向函数更新当前密钥：$\text{PresentSK}\leftarrow f^{counter}(\text{combination}(\text{ID},\text{Seed}))$．

3.3　安全性分析

在本系统当中，借鉴一次性口令原理进行密钥更新，可以防止密钥丢失或泄漏之后，被非法者多次违规使用，能够及早的发现密钥的泄漏情况．即使密钥被泄漏，只要及时发现，合法的投标者可以重新去注册中心修改密钥，这样，非法者就无法再次使用以前的密钥．另外，当投标者经身份认证被确认为合法用户时，系统将自动对用户的私钥进行更新．这样，在需要进行投标的时候，合法用户就能使用最新的密钥对自己的投标信息即标书进行签名，以确保开标的时候，标书没有被篡改过，并能保证投标者无法抵赖自己的投标行为．

4　基于秘密共享的标底保密

利用秘密共享技术可以控制任何需要多个人共同控制的秘密信息、命令，是信息安全和数据保密中的重要手段．相对于单钥和公钥加密体制而言，秘密共享技术在保密强度和适用性方面都更适合于本系统来实施对标底的保密．

现有的门限可验证秘密共享方案[5,6]运用到电子招投标系统中仍存在以下问题：(1)服务器都处在招投标中心使得招投标中心的权利过大；(2)尽管利用了秘密共享，但由于过于信任招投标中心而无法避免招投标中心多台机器管理员的勾结．

因此，笔者在 Shamir 门限可验证秘密共享方案的基础上进行改进，将秘密的分发者(这里就是投标者)作为秘密分享的一分子，并且在秘密重构的过程中，分发者必须是重构组中的一员，否则，秘密将无法重构．这样，投标者成为了秘密重构的必备

参与者,从而阻止了招标中心一手包办.

4.1 新的门限可验证秘密共享

1) 系统的参与者及主要参数

系统的参与者:秘密的分发者 $D(dealer)$, n 个分享者 $P_1, P_2, \cdots P_n$, t 是门限值.

系统参数 p, q 为大素数, $q=(p-1)/2$, g 为素数域的乘法群 $GF(p)$[5] 中的 q 阶生成元,使得在 $GF(p)$ 中计算以 g 为底的离散对数是不可行的.

2) 秘密份额的产生算法(Share)

分发者 D 共享者($D, P_2, P_3 \cdots P_n$)

选取 $GF(p)$ 上的一个 $t-1$ 次多项式 S_j 就是 D 发送给第 J 个分

$h(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{i-1} x^{i-1}$ $\xrightarrow{S_j(j=2,3\cdots n)}$ 享者 P_j 的秘密份额保密

$a_0 = h(0) = S$ 其中 S 为秘密

计算 $S_j = h(x_j) \bmod p, j=1,2,\cdots n$,

保留 $S_1, h(x)$

3) 验证算法(verify)

验证者 V 根据 D 公布的公开信息验证以下等式是否成立, t 为门限值:

$$y = \prod_{j=1}^{t} v_j^{a_j} (\bmod p),\ u_j = \prod_{k=1}^{t} v_k^{c_{kj}} (\bmod p),\ j=1,2,\cdots n$$

若这些等式都成立,则可断定 D 在分发秘密份额的过程中没有欺骗行为.否则说明 D 有欺骗行为.

每一 P_j 可通过 $g^{s_j} = u_j = \prod_{k=1}^{t} v_k^{c_{kj}} (\bmod p$ 来验证自己所得到的秘密份额是否有效.若两个等式中至少有一个不成立,则说明 D 给自己的秘密份额是无效的,这时,他向 D 发送一个抱怨信息,同时公布 s_j (即 S_j),并要求 D 重新给自己发送有效的秘密份额,直到通过验证为止.

4) 恢复算法(recover)

D 自身所保留的一份影子,外加任意 t 个或 t 个以上的分享者可协作恢复出秘密 S.这里,分发者 D 所保留的影子在信息恢复过程中是必需的.

不妨设 $D, P_2, P_3, \cdots P_t$ 要合作恢复秘密, $(x_2, x_2), \cdots, (x_t, s_t)$ 可根据 LaGrange(拉格朗日)多项式插值法,结合 D 所保留的第一份影子 S_1,合作恢复出 $h(x)$.并计算出秘密 $s = h(0)$.

5) 验证算法及恢复算法的正确性

验证算法的正确性:由秘密份额的产生算法可知,如果 D 正确地分发秘密份额,则应有 $\sum_{j=1}^{t} a_j b_j = s$, 其中 $a=(a_1, a_2, \cdots, a_t)^T$ 是公开的, $b_1, b_2, \cdots, b_t$ 是 D 在方程 $\sum_{j=1}^{t} a_j x_j = s(\bmod q)$ 的解空间中随机选取的秘密值.因此必有① $y = g^s = \prod_{j=1}^{t} v_j^{a_j} (\bmod p)$ 同时由于 $(s_1, s_2, \cdots, s_t) = (b_1, b_2, \cdots, b_t)$ C 其中 $C = (c_{ij})$ 是在 GF(q)上的公开的秘密分享矩阵,这意味着 $s_j = \sum_{k=1}^{t} b_k c_{kj} (\bmod p)$, 因此有② $g^{s_j} = \prod_{k=1}^{t} (g^{b_k})^{c_{kj}} = \prod_{k=1}^{t} v_k^{c_{kj}} (\bmod p)$

反之,若①成立,则意味着 $y = g^s = \prod_{j=1}^{t} v_j^{a_j} (\bmod p) = g^{\sum_{j=1}^{t} a_j b_j} (\bmod p)$.从而有 $S = \sum_{j=1}^{t} a_j b_j (\bmod q)$.3,这说明:$(b_1, b_2, \cdots b_t)$ 的选择是正确的;若②成立,则意味着 $g^{sk} = uk = \prod_{j=1}^{t} v_j^{c_{jk}} (\bmod q) = g^{\sum_{j=1}^{t} b_j g_k} (mod p)$

从而有 $s_k = \sum_{j=1}^{t} b_j c_{jk} (\bmod q)$,这说明 s_k 的选择是正确的;因此①及对所有的 j,②都成立就可保证秘密份额的分发过程是正确的.

4.2 标底保密评选流程

为保护未中标者标书的知识产权,本系统针对评标标准仅为标底金额的情况,基于秘密共享机制设计了一个能保证标底保密性的安全、合理的评选流程.

本流程从标值出发,标书的评选按照标底的价格评出赢家和最后的竞价.在这里,将标值定义为 $(B_{i1}, B_{i2}, \cdots B_{id})$,这里 B_{i1} 代表了标值的最高位,这样就将每一个标值从最高位到最低位进行比较,最多比较 d 轮,每一轮评选后保留当前出价最高位的所有投标者集合 Y_i,这样 Y_i 就将是可能的赢家所在的集合,第一轮中 $Y_1 = \{B_1, B_2 \cdots\}$.如图 3 所示.

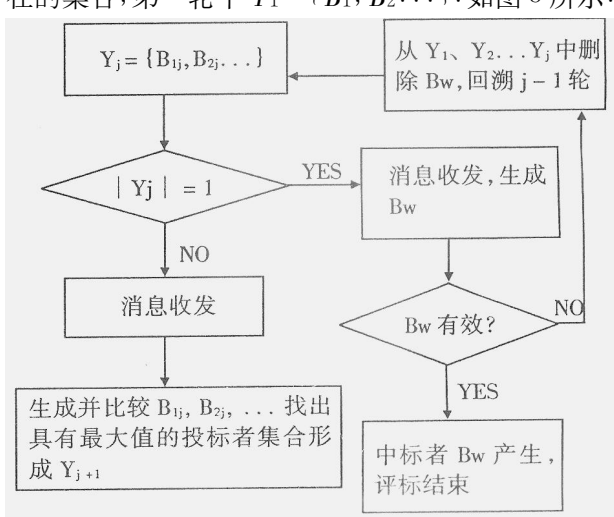

图 3 标底保密流程

对其中第 j 轮的描述如下：当招投标中心收到消息后，首先分析其有效性，对于有问题的消息，发现并定位出错的服务器，任何正确的服务器都能够恢复出 B_{ij}，B_i 在[0，…，$c-1$]范围取值，具有最大 Bij 值的投标者集合成为新的 Y_{j+1}. 如果 $|Y_{j+1}|>1$，说明还需要进行一轮比较，直到 $|Y_{j+1}|=1$ 为止，表示已经找到了所需的投标者，将中标者设为 B_w.

在这个方案当中，对于中标者的评选都是通过程序执行，在标书的评选过程中，按照标值由高位 $Bi1$ 往低位 Bid 的方向进行恢复和比较，可以不要恢复出完整标价即可选出出价最高的投标者，这时只要恢复赢家的完整标书即可，并宣布中标者和竞价. 对于那些未中标者的报价都实行了保密，在一定程度上对未中标者隐私进行了保护.

4.3　安全性分析

攻击者在此阶段的攻击有三种

1) 设法由公开信息推导出秘密. 这类情况的发生有两种可能的方式；一是由 $y=g^s$ 直接推导 s，这在计算离散对数不可行的假设下是办不到的. 二是由 $v_1, v_2, \ldots, v_t, u_1, u_2, \ldots, u_n$ 来推导出 s，由于计算离散对数的困难性，攻击者无法得到 $b_1, b_2, \ldots, b_t$，也无法得到任何 s_k，从而无法得到 S.

2) 设法得到满足的 $\sum_{j=1}^{t} a_j b_j = s$ 的 $(b_1, b_2, \ldots, b_t)$，然后按照秘密份额的产生方法计算出给各分享者的秘密份额. 由于计算离散对数是不可行的，攻击者无法从公开信息 $v_1, v_2, \ldots, v_t$ 得到分发者产生秘密份额所使用的 $(b_1, b_2, \ldots, b_t)$. 因此攻击者攻击成功相当于随机猜测满足 $\sum_{j=1}^{t} a_j b_j = s$ 的 $(b_1, b_2, \ldots, b_t)$ 获得成功，其概率仅为 $1/q^{t-1}$.

3) 在获得不超过 $t-1$ 个秘密份额的情况下，推导出 s. 攻击者即使与 $t-1$ 个分享者串通，由他们所持有的 $t-1$ 个秘密份额及公开信息也无法得到其他任何一个分享者的秘密份额. 由于在计算离散时数不可行的假设下，公开信息不能提供有关秘密 s 和分享者所持有的秘密份额的任何有用信息，而由 $t-1$ 个秘密份额恢复出秘密 s 相当于在 $GF(q)$ 中随机猜测 s 获得成功，其概率仅为 $1/q$.

5　结束语

本文运用了多种安全技术，包括基于一次性口令的密钥更新，秘密共享，标底保密等，在一定程度上提高了整个投标工作的安全性. 但我们在研究中深深感到，电子招投标系统还存在许多值得进一步研究的问题，尤其值得重视的问题是：(1)如何设定有效的评标标准以杜绝腐败；(2)如何跟踪中标者对合约的执行情况，即投标者信用等级的评定；(3)如何组建网上评标专家库和选择委员.

参考文献：

[1] Qi ming，Wen ya-min. The Design And Application of Credit CA Certificate[J]. Proceedings of the third international conference on E-commerce engineering. 2003. 623－626.

[2] Lingmei Mao，Ming Qi. Technology of Cipher Coder-the Soul of E-commerce[J]. International Business in the Era of Economy Globalization. 2001.

[3] Haller N，Metz C，Nesser P，etc. A One－Time Password System[J]. RFC 2289. 1995－02.

[4] G.J.Simmons. "How to (Really) Share a Secret，" Advances in Cryptology? [M]. CRYPTO '88 Proceedings，Springer－Verlag，1990.

[5] 毛玲梅. 电子招投标系统公正性与安全性研究与实现[C]. 华南理工大学硕士学位论文. 2003，31－48.

Research on Security of E-bidding

WEN Ya-min[1]，TU Shu-qin[2]，ZU Jian-ying[3]

(Guangdong University of Business Studies，Guangzhou 510320；2. Information College，South China Agriculture Univ.，510640；3. Software College，Nanchang Univ.，Nanchang 330029，China)

Abstract：In this paper，we analyze some problems about the security of e-bidding system，and which would be solved preferably through introducing the new identity authentication，especially improving the secret sharing scheme based on Shamir's thought.

Key words：e-bidding；key updating；identity authentication；secret sharing