一个 M+1 电子拍卖方案的密码学分析

张春生[1],姚绍文[2],王世普[2]
ZHANG Chun-sheng[1],YAO Shao-wen[2],WANG Shi-pu[2]

1.安庆师范学院 计算机与信息学院,安徽 安庆 246011
2.云南大学 软件学院,昆明 650091
1.College of Computer and Information,Anqing Teachers College,Anqing,Anhui 246011,China
2.College of Software,Yunnan University,Kunming 650091,China
E-mail:zhangchs@ynu.edu.cn

ZHANG Chun-sheng,YAO Shao-wen,WANG Shi-pu.Cryptanalysis of (M+1)-st auction scheme.Computer Engineering and Applications,2009,45(11):111-113.

Abstract: This paper analyzes Wu et al's (M+1)-st auction scheme and shows that in their scheme,the presupposition of different bids of different bidders isn't tenable.On the other hand,when several bidders simultaneously bid the maximum price or second,the scheme can't implement (M+1)-st auction (namely tie problem).So their scheme isn't applied value.This paper furnishes effective technique to solve the problem.

Key words: (M+1)-st auction;secure multi-party computation;tie;zero-knowledge proof;privacy protection

摘 要:分析了伍前红等人最近提出的 M+1 电子拍卖方案,指出该方案假设不同投标者的标价不同的前提条件是不能成立的;另一方面,当有多个投标者同时投了最高价或次高价时,协议将不能实现 M+1 价位电子拍卖(称为结点问题),因此方案不具有实用价值。给出了解决这一问题的有效算法。

关键词:M+1 密封拍卖;安全多方计算;结点;零知识证明;隐私保护
DOI:10.3778/j.issn.1002-8331.2009.11.034 **文章编号**:1002-8331(2009)11-0111-03 **文献标识码**:A **中图分类号**:TP309

1 引言

近年来,随着电子商务活动的开展,电子拍卖得到了广泛地研究[1-6],但大多不具有实用价值。目前,影响电子拍卖协议应用的关键因素主要有以下几个方面:(1)保持投标者标价的秘密性。现有的绝大多数电子拍卖方案或多或少要求第三方(拍卖行)相互不勾结[1-3],然而,这在现实生活中,他们在幕后勾结是可能的,而且,即使他们勾结了,投标者也一无所知,因此,在任何情况下保持投标者标价的秘密性是非常重要的。(2)中标价的可公开验证性,即在投标过程中,投标者希望中标价的正确性可以公开验证,这对防止舞弊是至关重要的。(3)结点问题,即有几个投标者同时投了最高价或次高价,这是密封式电子拍卖方案中至今没有解决的问题。(4)拍卖的效率尽可能高。

伍前红等人提出的 M+1 电子拍卖方案中[4],拍卖泄漏的只是中标价,其余标价及其相互关系在任何勾结情况下都是保密的,而且,标价的正确性可以公开验证,在效率上比 Brandit[5]提出的方案效率高得多,但是,该方案是在假设不同投标者的标价是不同的条件下设计的,这一条件在实际应用时是不能成立的,详见第 3 章分析;另一方面,当有多个投标者同时投了最高价或次高价时,该方案按照注册的先后顺序,先注册者先中标,这种方法也是不能实现的,因为执行协议后,不能确定出中标价和中标者,因此该方案不具有实用价值。本文给出了解决这一问题的有效算法,在允许不同投标者的标价可以相同的情况下给出拍卖协议。

2 伍前红等人的方案

2.1 符号

本文用到的一些记号和组成模块:$<g>$表示由 g 生成的循环群。G 是一个高阶循环群。$<g>=<h>\subseteq G$。$<g>$中离散对数是困难的。$H:\{0,1\}^*\rightarrow\{0,1\}^l$ 是一个密码学杂凑函数,l是一个安全参数。a 和 b 的级联表示为 $a\|b$。$ZKP\{x|R(x)\}$表示零知识证明,证明示证者知道秘密 x 使得关系 $R(x)$为真。$Commit(x)$表示对秘密 x 的承诺。Alice 知道秘密 x 可以按如下方式向 Bob承诺。Alice 选取随机整数 r 并向 Bob 发送 $C=g^xh^r$ 作为对 x 的承诺。Alice 不可能找到 $x_1\neq x_2$ 使得 $Commit(x_1,r_1)=Commit(x_2,r_2)$,除

基金项目:安徽省自然科学基金(the Natural Science Foundation of Anhui Province of China under Grant No.2006KJ081B);云南省网络信息技术专项基金项目(No.2004IT11)。

作者简介:张春生(1968-),男,讲师,主要研究方向:网络与信息安全;姚绍文(1966-),男,教授,博士生导师,主要研究方向:语义 Web 技术、网络协议工程、网络分布式计算、着色 Petri 网(CPN)建模、知识工程技术等;王世普(1958-),男,教授,硕士生导师,主要研究方向为网络分布式应用、网络信息处理。

收稿日期:2008-02-25 **修回日期**:2008-05-05

非她知道 $log_g h$。Bob 即使有无限的计算力也不可能从 C 提取任何有用的信息。这是一个陷门承诺,即如果 Alice 知道 $log_g h$ 则可以任意欺骗 Bob,详细可参阅文献[7]。本文将用到下列零知识证明:$ZKP\{x|y=g_x\}$[8],$ZKP\{x,r|y=g^x h^r \wedge y_1=g_1^x\}$[9],$ZKP\{x,r|y=g^x h^r \wedge x\in\{a_1,a_2,\cdots a_t\}\}$[10]。

2.2 协议设计

这里先介绍设计的基本思想。事实上推广了 A.Yao[11]的百万富翁协议,其中,两个百万富翁希望比较他们的财富但都不希望泄漏进一步的信息。也就是说,在本文的设计中,有 n 个参与者 $1,2,\cdots n$,各有一个秘密数 b_i 在$\{1,2,\cdots v\}$中,没有任何第三方的帮助,可能存在严重的勾结,他们将安全计算出第 $t(t=M+1)$个最大(最小)的 b_i 而不泄漏进一步的信息,并且要求结果能够公开验证。

首先考虑标价的编码方法。设投标者 i 的标价为 $b_i(1\leqslant i\leqslant n,1\leqslant b_i\leqslant v)$。为了有效地计算出中标价,即第 t 个最高价或最低价(只考虑最高价,最低价可以完全类似进行)标价 $b_i(1\leqslant i\leqslant n,1\leqslant b_i\leqslant v)$编码成一个向量:

$$\boldsymbol{\beta}_i=(\underbrace{0,0,\cdots,1}_{b_i},\underbrace{0,\cdots,0}_{v-b_i})=(x_{i,1},\cdots,x_{i,v})$$

这些向量的和表示为:

$$\boldsymbol{\gamma}=\sum_{i=1}^{n}\boldsymbol{\beta}_i=(\gamma_1,\cdots,\gamma_v)=(\sum_{i=1}^{n}x_{i,1},\cdots,\sum_{i=1}^{n}x_{i,v})$$

注意到 $n(t)=\sum_{j=t}^{v}\gamma_j=\#\{b_i|b_i\geqslant t\}$为参与者中其秘密数大于等于 t 的人数。假设这些秘密整数是不同的,那么 $n(j)$关于 j 单调递减且有惟一的 j 满足 $n(j)=t$。如果参与者能够合作测试是否有 $n(j)=t$ 而不泄漏进一步的信息,那么通过从 v 到 1 重复测试这一等式就可以安全地计算出第 t 个最大的秘密整数。

2.2.1 推广的匹配协议

在上面的讨论中,要求 n 个参与者能安全测试$\pm x_1\pm\cdots\pm x_n=a$而不泄漏进一步的信息,其中 $x_i(i=1,2,\cdots,n)$是参与者 i 的秘密输入,a 是一个已知的整数。称这个问题为推广的匹配协议,它是匹配协议($n=2$[12])的推广,其中两个富翁比较他们的财富是否相等而不泄漏进一步的信息。下面给出这个推广的匹 配协议的一个有效设计,并结合已知的零知识证明使协议具有可公开验证性。

(1)对 $i=1,2,\cdots n$,参与者 i 公布 $y_i=g^{x_i}h^{r_i}$作为对 x_i 的承诺。然后任何人都可以计算:

$$z_0=y_1^{\pm1}\cdots y_n^{\pm1}g^{-a}=g^{\pm x_1\pm\cdots\pm x_n-a}h^{\pm r_1\pm\cdots\pm r_n}$$

(2)参与者 1 随机选取整数 s_1,公布:

$$z_1=z_0^{s_1},v_1=h^{s_1},ZKP\{s_1|z_1=z_0^{s_1}\wedge v_1=h^{s_1}\}$$

(3)对 $i=2,\cdots,n$,参与者 i 随机选择 s_i,公布:

$$z_i=z_{i-1}^{s_i},v_i=v_{i-1}^{s_i},ZKP\{s_i|z_i=z_{i-1}^{s_i}\wedge v_i=v_{i-1}^{s_i}\}$$

(4)对 $i=1,2,\cdots,n$,参与者 i 公布:

$$u_i=v_n^{\pm r_i},ZKP\{r_i|y_i=g^{x_i}h^{r_i}\wedge u_i=v_n^{\pm r_i}\}$$

(5)如果 $z_n=u_1u_2\cdots u_n$,返回 1;否则返回 0。如果涉及到的零知识证明是安全的,那么每个欺骗者都将被检测到并被逐出协议。注意到:

$$z_n=g^{(\pm x_1\pm\cdots\pm x_n-a)s_1\cdots s_n}h^{(\pm r_1\pm\cdots\pm r_n)s_1\cdots s_n}$$

$$u_1u_2\cdots u_n=h^{(\pm r_1\pm\cdots\pm r_n)s_1\cdots s_n}$$

因此,返回值 1 表示$\pm x_1\pm\cdots\pm x_n=a$,返回值 0 表示$\pm x_1\pm\cdots\pm x_n\neq a$,输出显然是可以公开验证的。现在考虑勾结攻击。假设攻击者完全控制了 $n-1$ 个参与者,比如说,参与者 $i=2,\cdots,n$,并试图提取参与者 1 的秘密输入。也就是,攻击者知道了 $x_2,\cdots,x_n$ 和 $s_2,\cdots,s_n$,希望提取 x_1。攻击者能够计算 $w=g^{(\pm x_1\pm\cdots\pm x_n-a)s_1\cdots s_n}$,其中 x_1 和 s_1 未知。设 $b=\pm x_2\pm\cdots\pm x_n-a,c=s_2\cdots s_n$,但是即使 x_1 所在的范围非常有限,攻击者从 $w=g^{(b\pm x_1)cs_1}$提取 x_1 也是不可能的。协议要求 O(1)次模指数运算和 O(1)轮通信。记上述协议为:

$$EQ\{x_1,\cdots,x_n|y_1=g^{x_1}h^{r_1}\wedge\cdots\wedge y_n=g^{x_n}h^{r_n}:(\pm x_1\pm x_2\pm\cdots\pm x_n,a)\}$$

2.2.2 第 M+1 价位密封拍卖

假设投标者 $i\in\{1,2,\cdots,n\}$有惟一认证过的签字公钥表示其身份。系统中拍卖行不参与计算中标价(相当于没有拍卖行),只需监视拍卖过程和维护将涉及到的公告牌,所有的数据都将发送到公告牌上。设允许的标价空间为$\{p_1,\cdots,p_v\}$,其中 $p_1<\cdots<p_v$。这可以表示为$\{1,2,\cdots,v\}$。为了简化,对 $i=1,2,\cdots,n$,假定不同投标者的 b_i 是不同的。可以按如下方式实现:设投标者 i 的标书 b_i 最高的$\lfloor\log v\rfloor+1$位表示他投的标价,而后面的低位比特表示他的注册顺序号,也就是说,如果投标者 i 第一个注册,那么他的注册顺序号就是 1,依此类推。

初始化:假设系统所有安全参数都已经由正确的程序产生,关于拍卖商品的信息、卖时间、投标规则、标规则和交易规则都已经公布在公告牌上。

注册:投标者公布他们的公钥和公钥证书到公告牌上,所有合法的公钥形成公钥列表 L。

注册结束后,每一个合法的投标者都有一对公/私钥(Z_i,x_i)。不失一般性,假设投标者 i 拥有 Z_i。要求投标者 i 按如下方式广播消息 $m:(m\parallel phase\parallel No.\parallel sign_{Z_i}(H(m\parallel phase\parallel No.)))$,其中 $sign_{Z_i}$ 是以 Z_i 为验证公钥的数字签名,$phase$ 表示投标、开标和交易的时间片,$No.$在一定时间片内发送消息的序列号。这种方式保证了数据的完整性,没有人能够篡改、伪造或重放一条消息而不被发现。在下面的描述中,为了简化将省去签字。

投标:投标者 i 选取他的秘密标价 $b_i\in\{1,2,\cdots,v\}$并编码为:

$$\boldsymbol{\beta}_i=(\underbrace{0,0,\cdots,1}_{b_i},\underbrace{0,\cdots,0}_{v-b_i})=(x_{i,1},\cdots,x_{i,v})$$

对 $j\in\{1,2,\cdots,v\}$,投标者 i 计算 $y_{i,j}=g^{x_{i,j}}h^{r_{i,j}}$,公布$(y_{i,1},\cdots,y_{i,v})$作为标书的公开形式,并用零知识方式证明标价编码是正确的。

$$ZKP\{x_{i,j}|y_{i,j}=g^{x_{i,j}}h^{r_{i,j}}\wedge x_{i,j}\in\{0,1\}\}$$

$$j\in\{1,2,\cdots,v\}$$

$$ZKP\{b_i,u_i|\prod_{j=1}^{v}y_{i,j}^{2^j}=g^{2^{b_i}}h^{u_i}\wedge b_i\in\{1,2\cdots,v\}\}$$

开标:

(1)计算中标价

$$z_{i,J}=\prod_{j=v}^{J}y_{i,j}=g^{\sum_{j=v}^{J}x_{i,j}}h^{\sum_{j=v}^{J}r_{i,j}}=g^{s_{i,J}}h^{\delta_{i,J}},j\in\{1,2,\cdots,v\}$$

①设置 $J:=v$;

②如果:$EQ\{s_{1,J},\cdots s_{n,J}|z_{1,J}\}=g^{s_{1,J}}h^{\delta_{1,J}}\wedge\cdots\wedge z_{n,J}=g^{s_{n,J}}h^{\delta_{n,J}}:(s_{1,J}+\cdots+s_{n,J},M+1)=1$,转步骤④;否则 $J:=J-1$;

③重复步骤②直到 $EQ\{s_{1,J},\cdots s_{n,J}|z_{1,J}\}=g^{s_{1,J}}h^{\delta_{1,J}}\wedge\cdots\wedge z_{n,J}=$

$g^{s_{n,J}}h^{\delta_{n,J}}:(s_{1,J}+\cdots+s_{n,J},M+1)=1$;

④输出中标价 J,中止程序。

(2)诚实性证明

投标者 i 公布 $ZKP\{\delta_{i,J-1}|z_{i,J-1}g^{-1}=h^{\delta_{i,J-1}}\}$或 $ZKP\{\delta_{i,J-1}|z_{i,J-1}=h^{\delta_{i,J-1}}\}$。如果投标者 i 出示 $ZKP\{\delta_{i,J-1}|z_{i,J-1}g^{-1}=h^{\delta_{i,J-1}}\}$那么他投了最高标价。如果出示的是 $ZKP\{\delta_{i,J-1}|z_{i,J-1}=h^{\delta_{i,J-1}}\}$那么他投的标价低于中标价。中标者身份确定出来。

3　密码学分析

通过分析 2.2 节的协议设计,注意到协议能够顺利执行的前提条件是不同投标者的标价是不同的,但是,这个前提条件通过以下几点分析是不能成立的:

(1)上述协议执行时,每一个投标者需要的通信轮数和模指数运算的次数均为 $O(v)$,每一个投标者需要发送的数据为 $O(v|G|)$[4],$|G|$表示 G 中元素的二进制表示长度。由于不同投标者的标价不同,要求参与投标的人数必须小于标价的编码范围,即 $n<v$;又因为协议执行的效率与 v 有关($O(v)$),典型实现(如 $v=128$,$n=100$),上述方案需要几分钟。因此,上述协议在实际应用时,v 不能太大,否则效率将成为协议执行的瓶颈,v 值又进一步限制了参与投标的人数不能太多,这对较大型的电子拍卖来说,限制投标者人数在较少的范围内将是不实用的。

(2)上述协议泄漏的只是中标价,其余标价及其相互关系在任何勾结情况下都是保密的[4]。由于每一个投标者的标价都是保密的,如何能够检测和控制使得投标者的标价互不相同是个难题,显然,要求不同投标者的标价是不同的前提条件是无法实现的。

(3)第 2.2.2 节的开标算法从最高价 v 到最低价 1 搜索中标价,由于假设不同投标者的标价是不同的,所以 $s_{1,J}+\cdots+s_{n,J}$ 关于 J 严格下降,因此存在惟一的 J 使得 $s_{1,J}+\cdots+s_{n,J}=M+1$。但是,根据第②点的分析,协议在执行时必然存在标价相同的情况,如果有多个投标者同时投了最高价或次高价,将不存在 J 使得 $s_{1,J}+\cdots+s_{n,J}=M+1$。例如:现在假设拍卖 3 个相同的商品,即 $M=3$,所有投标者所投的最高价是 $j_1(1<j_1\leqslant v)$,下面几种情况都将不能实现 $M+1$ 价位拍卖:

①如果有 4 个投标者同时投了 j_1 的价位,此时,执行上述协议将不能实现 $M+1$ 价位拍卖,因为 $M+1$ 价位表示未中标者出的最高价位。

②如果有 5 个即以上投标者同时投了 j_1 的价位,此时,执行上述协议也不能实现 $M+1$ 价位拍卖,因为不存在 J 使得 $s_{1,J}+\cdots+s_{n,J}=M+1$。

③如果有 a 个($1\leqslant a\leqslant 3$)投标者同时投了 j_1 的价位,在 j_1 的下一价位 j_2 有 b 个投标者同时投了 j_2,只要满足 $a+b\geqslant 5$,那么,执行上述协议都将不能实现 $M+1$ 价位拍卖,因为不存在 J 使得 $s_{1,J}+\cdots+s_{n,J}=M+1$。

4　改进方案

通过第 3 章的分析,可知伍前红等人提出的 $M+1$ 电子拍卖方案是不实用的,为此,提出改进方案如下:

本文的方案允许不同投标者投相同的标价。改进的方案只需改变原方案的开标算法,如下所示。

开标:

(1)计算中标价

$$z_{i,J}=\prod_{j=v}^{J}y_{i,j}=g^{\sum_{j=v}^{J}x_{i,j}}h^{\sum_{j=v}^{J}r_{i,j}}=g^{s_{i,J}}h^{\delta_{i,J}},j\in\{1,2,\cdots,v\}$$

设置 $a:=M+1$;

①设置 $J:=v$;

②如果 $EQ\{s_{1,J},\cdots s_{n,J}|z_{1,J}\}=g^{s_{1,J}}h^{\delta_{1,J}}\wedge\cdots\wedge z_{n,J}=g^{s_{n,J}}h^{\delta_{n,J}}:(s_{1,J}+\cdots+s_{n,J},a)=1$;

③输出 J、a,中止程序;

④否则 $J:=J-1$;

⑤如果 $J\geqslant 1$ 转步骤②;

⑥否则 $a:=a+1$ 转步骤①。

(2)诚实性证明

投标者 i 公布 $ZKP\{\delta_{i,J-1}|z_{i,J-1}g^{-1}=h^{\delta_{i,J-1}}\}$或 $ZKP\{\delta_{i,J-1}|z_{i,J-1}=h^{\delta_{i,J-1}}\}$。如果投标者 i 出示 $ZKP\{\delta_{i,J-1}|z_{i,J-1}g^{-1}=h^{\delta_{i,J-1}}\}$,那么他投了最高标价。如果出示的是 $ZKP\{\delta_{i,J-1}|z_{i,J-1}=h^{\delta_{i,J-1}}\}$,那么他投的标价低于中标价。中标者身份确定出来。

(3)算法分析

改进的开标算法考虑了有多个投标者同时投了最高价或次高价的情况,该算法在有多个投标者同时投了最高价或次高价时,每一个投标者需要的通信轮数和模指数运算的次数均为 $O((a-M)v)$。现以计算中标价算法的步骤③的输出情况来进行分析:

①如果输出的 $a=M+1$,算法中的步骤⑥没有执行,表明没有多人在最高价或次高价投了相同的标价,输出的 J 为中标价,方案的执行效果同伍前红等人的方案;

②如果输出的 $a>M+1$,算法中的步骤⑥执行,表明有多个投标者同时投了最高价或次高价,输出的 J 不能作为中标价,因为此时中标者的人数大于 M,要先用 J 来确定投了最高价的投标者,然后再采用下列两种方法之一来确定最后的中标者:方法一,按照注册的先后顺序,先注册者先中标[4];方法二,让投了最高价的这些投标者再进行第二轮投标,同时为了减少在最高价或次高价投相同标价的概率,将第二轮投标的标价区间的最低价设为上一轮中标价,而标价数量仍然为 v 个。

对上述的两种方法,方法一不能满足电子拍卖的公平性要求,即应由出价最高的投标者中标,因此,应该优先考虑采用方法二。

5　结论

随着电子商务活动的开展,电子拍卖得到了广泛研究。本文分析了伍前红等人最近提出的 $M+1$ 电子拍卖方案,指出该方案不具有实用价值并给出了一个实用的 $M+1$ 电子拍卖方案。

参考文献:

[1] Abe M,Suzuki K.$M+1$-st price auction using homomorphic encryption[C]//Proceedings of the 5th International Conference on Public Key Cryptography(PKC-02).Berlin:Springer-Verlag,2002:115-124.

[2] Chida K,Kobayashi K,Morita H.Efficient sealed-bid auctions for massive numbers of bidders with lump comparison[C]//Proceedings of the International Information Security Conference (ISC) 2001. Berlin:Springer-Verlag,2001:408-419.

(下转 119 页)