第34卷 第19期 计 算 机 工 程 2008年10月
Vol.34 No.19 Computer Engineering October 2008
·软件技术与数据库· 文章编号：1000—3428(2008)19—0032—03 文献标识码：A 中图分类号：TP309

基于环签名理论的电子拍卖方案

周菊香，赵一鸣
(复旦大学软件学院，上海 200433)

摘 要：基于环签名理论提出一个电子拍卖方案，适用于公司内部或者具有排外性的团体内部的拍卖，拍卖期间，成员可以在任何地点、任何时间提交自己的投标消息，等到拍卖结束后，再提交自己相应的投标值，匿名的同时又能证明投标消息的合法性，既证明了自己属于组内成员，又不会泄漏投标者的确切身份，保护了投标者的隐私。

关键词：环签名；电子拍卖；比特承诺；匿名性；hash函数

Electronic Auction Protocol Based on Ring Signature Theory

ZHOU Ju-xiang, ZHAO Yi-ming
(Software School, Fudan University, Shanghai 200433)

【Abstract】 This paper presents an electronic auction protocol based on ring signature theory. This protocol is designed for companies' exclusive auction. The bidders are allowed to submit their bid messages anywhere at any time during the bid period. After this period, they commit their bids. The protocol can protect their privacy, and verify the validity of the bidders. That is, every bidder can prove that he belongs to the group, while does not leak any information of his exact identity, which can protect the bidders' privacy better.

【Key words】 ring signature; electronic auction; bit commitment; anonymity; hash function

1 概述

电子拍卖系统[1]是现实拍卖系统的电子化，均由拍卖参与者、拍卖规则和仲裁机构组成。与现实中的拍卖相似，电子拍卖有一系列安全属性，主要可以归结为合法性和安全性这2个方面。在提高和改进电子拍卖方案的安全性方面，很多学者已经做出了显著的成绩。例如，匿名投标可以防止一些投标者串通[2]、抗匿名信道的研究[3]、以公钥密码为基础的分布式拍卖系统[4]以及基于Shamir秘密共享的多方安全计算协议[5]等。然而，当前已有的电子拍卖方案多是只关注匿名性，很少关注投标者是否有权参与拍卖。这与拍卖本身的目的和特点相关。然而，当拍卖有特殊情况，例如，只是为内部人员而组织的时候，目前已有的方案就无法满足这种排外性的要求。

本文给出了一个基于环签名的电子拍卖方案，该方案既满足拍卖的匿名性要求，又满足只有组内成员可以参加的要求，即外部人员由于不能共享这个组内的某些信息而无法产生合法的投标消息。

环签名其实就是简化了的群签名[6]，它要求只有该组成员可以完成签名，同时不泄漏签名者的确切身份。然而，与群签名不同的是，环签名不存在组织管理者，不存在回收过程，不需要组内成员之间的任何合作。组内的任何成员在已有自己的私钥和其他所有成员公钥的情况下，不需要其他成员的帮助即可签署消息，且不会受到其他成员的干预。

当验证者得到这样的一份签名后，除了能够验证该签名是否出自该组、是否合法以外，无法得到有关该成员身份的确切信息。并且，因为不存在组织管理者，所以也就不会像群签名那样，管理者可以查出签名者的确切身份，这就更好、更有效地保护了签名者的隐私，因此更适合于电子拍卖这样要求高度保密性的商务用途。

2 预备知识

2.1 一个已有的环签名方案(RSA版本)

Rivest和Shamir等人于2001年首次提出了环签名的概念，给出了基于RSA和Rabin的环签名方案[7]，并且证明RSA版本方案的安全性。随后在2005年他们又在此基础上给出了环签名的一些应用。

2.1.1 RSA陷门置换

每个成员 A_i 都有RSA公钥 $P_i=(n_i,e_i)$，定义了 Z_{n_i} 中的陷门置换 f_i：

$$f_i(x)=x^{e_i}(\mathrm{mod}\ n_i)$$

该式是Diffie-Hellman于1976年给出的公钥加密的模型。根据陷门置换理论，可以假设只有 A_i 能够逆向求解 f_i^{-1}，得到 x 的值。

2.1.2 对称加密

假设存在一个对称加密算法E，那么E_k就是长度为b bit的串的置换。在随机oracle模型下，假设oracle对于所有成员有关$E_k(x)$和$E_k^{-1}(y)$的新提问，都会给出全新的随机产生的答案。而对于已经提问过的，则会给出之前的答案。

2.1.3 结合函数(combining function)

定义$C_{k,v}(y_1, y_2, \cdots, y_r)=z$为结合函数。其中，$k$是输入；$v$是随机选取的初始值；$y_1, y_2, \cdots, y_r$是$\{0,1\}^b$上的任意值；输出$z$是$\{0,1\}^b$上的值。

基金项目：国家自然科学基金资助项目(60573054)
作者简介：周菊香(1983－)，女，硕士研究生，主研方向：密码与信息安全；赵一鸣，副教授
收稿日期：2007-11-24 **E-mail：**052053022@fudan.edu.cn

选定 k 和 v 的值后，结合函数有以下的特点：

(1)对于每个s, $0\le s\le r$，以及其他给定的输入y_i, $i\ne s$，方程$C_{k,v}$是从y_s到输出z的一一映射。

(2)对于每个s, $0\le s\le r$，给定一个b bit长度的值z，和除y_s以外的所有y_i值，可以求解满足$C_{k,v}(y_1, y_2,\cdots, y_r) = z$的$b$ bit长度的y_s值。

(3)如果一个攻击者不能逆向求解陷门方程$g_1, g_2, \cdots, g_r$，那么给定k, v和z，它就很难根据$C_{k,v}(g_1(x_1), g_2(x_2),\cdots, g_r(x_r))= z$求解$x_1,x_2,\cdots,x_r$的值。

在文献[7]中，作者给出的结合函数为以下形式：

$$C_{k,v}(y_1,y_2,\cdots,y_r) = E_k(y_r \oplus E_k(y_{r-1} \oplus E_k(y_{r-2} \oplus E_k(\cdots \oplus E_k(y_1 \oplus v)\cdots))))$$

其中，$y_1, y_2,\cdots, y_r$定义为$y_i=g_i(x_i)$。

只要输出 z 与 v 相等，该方程的计算过程就会连接成一个环形。这也是环签名名称的由来。

2.1.4 环签名的 RSA 版本

环签名的RSA版本[7]由环签名的生成和验证 2 个阶段 组成。

(1)环签名的生成：

一个成员P_s在拥有要被签名的消息m，自己的私钥S_s，以及组内成员的一系列公钥$P_1,P_2,\cdots,P_r$的情况下，该成员完成以下步骤：

1)计算密钥：P_s通过hash消息m，得到的值即作为对称密钥k：$k = h(m)$。

2)挑选一个随机值：P_s在$\{0, 1\}^b$上均匀地选取一个随机值v_s。

3)挑选r-1 个随机值：P_s为每个组内成员P_i($1\le i\le r$且$i\ne s$)在$\{0, 1\}^b$上均匀地选取随机值x_i，并且计算$y_i = g_i(x_i)$。

4)计算y_s：P_s计算方程$C_{k, vs}(y_1, y_2, \cdots, y_r) = v_s$。在假设前提下，赋予其他的成员任意值之后，该方程就只有唯一一个解y_s，而且可以计算出该值。

5)根据P_s的陷门置换计算出x_s：$x_s = g_s^{-1}(y_s)$。

6)提交环签名：消息m的签名定义为以下形式：$(P_1, P_2, \cdots, P_r; v_s; x_1, x_2, \cdots, x_r)$。

(2)环签名的检验：

验证者检验m的环签名$(P_1, P_2, \cdots, P_r; v_s; x_1, x_2, \cdots, x_r)$的过程如下：

1)根据陷门置换计算出$x_1, x_2, \cdots, x_r$对应的$y_1, y_2, \cdots, y_r$值：$y_i=g_i(x_i)$。

2)计算 k：验证者计算消息 m 的 hash 值，从而得到对称密钥 k 的值：$k = h(m)$。

3)检验环方程：检验第 1)步计算得到的$y_1, y_2, \cdots, y_r$的值是否满足等式$C_{k, vs}(y_1, y_2, \cdots, y_r)=v_s$。如果该等式成立，则验证者认为获得的签名是合法的，否则，拒绝接受该签名。

2.2 比特承诺

密码学中的比特承诺方案是密码学协议的重要组成部分，由 2 个阶段组成，经常应用在普通的电子拍卖中。现假设 Alice 要向 Bob 承诺一个比特 b，那么整个过程如下：

(1)提交阶段：Alice 向 Bob 提交与 b 相关的信息，此时，即使 Bob 作弊也无法求解 b。

(2)解提交阶段：Alice 向 Bob 证实自己提交的信息是 b，此时，即使 Alice 作弊也无法求解 b'($b'\ne b$)，使得 Bob 接受该值。

3 适用于团体内的电子拍卖方案

通常，电子拍卖都会选择与比特承诺相关的协议。现在，假设有一个团体打算举行拍卖，但是每个投标者都不愿意泄漏自己的身份，同时，又不愿意组外成员或者不符合条件的人员的加入，那么普通的电子拍卖协议就无法满足这里要求的排外性，因为在已有的方案中只是关注到投标者的公平性，没有考虑到投标者的合法性。

在此，可以使用环签名的一个变形。环签名的特点就是只有满足条件的组员才能产生合法的签名，且不受到任何成员的干预，也不存在管理者的影响，因为与群签名不同，环签名不存在组织管理者。

由于每个参与者的投标值是自己生成的，而不是像环签名中的消息 m 那样在组成员内部共享，因此环签名方案不能直接用于电子拍卖。另外，拍卖结束时要确定标王，所以每个投标者都要在保证不泄漏 ID 的情况下提交 ID 的相关信息，这也与环签名不同。因此，环签名要做一些变动才能适用于排外性的电子拍卖。

本文给出的电子拍卖方案如下：

(1)投标消息的生成

1)挑选投标值：投标者P_s挑选投标值m_s，hash之后的值作为对称密钥k_s：$k_s = h(m_s)$。

2)挑选一个随机值：P_s在$\{0, 1\}^b$上均匀地选取一个随机值v_s。

3)挑选r-1 个随机值：P_s为每个组内成员P_i($1\le i\le r$且$i\ne s$)在$\{0, 1\}^b$上均匀地选取随机值x_i，并且计算$y_i = g_i(x_i)$。

4)计算y_s：P_s计算方程：$C_{ks, vs}(y_1, y_2, \cdots, y_r) = v_s$。在假设前提下，赋予其他成员任意值之后，该方程就只有唯一解y_s，而且可以计算出该值。

5)根据P_s的陷门置换计算出x_s：$x_s = g_s^{-1}(y_s)$。

6)计算ID相关信息：P_s运算自己的ID_s的hash值$h(ID_s)$。

7)提交投标消息：P_s的投标消息定义为以下形式：$(P_1, P_2, \cdots, P_r; v_s; h(ID_s); x_1, x_2, \cdots, x_r)$。

(2)投标值对的提交

在投标阶段结束之后，任何人都不可以再提交自己的投标消息，此时，每个投标者提交自己的投标值对$(m_1, v_1), (m_2, v_2), \cdots, (m_j, v_j)$($0\le j\le r$)。其中，$v_1, v_2,\cdots, v_j$方便验证者后续验证工作，即验证者可以通过这些值快速将收到的投标值对与之前收到的投标消息一一对应。

(3)投标消息的检验

验证者检验每个投标消息$(P_1, P_2, \cdots , P_r; v_s; x_1, x_2, \cdots , x_r)$的过程如下：

1)比较所有投标值的大小，得到最大值m_i。

2)根据陷门置换计算出x_i对应的y_i值：$y_i = g_i(x_i)$。

3)验证k_s：验证者通过投标消息中的v_i找到与之对应的投标值对(m_i, v_i)，计算竞标值m_i的hash值，从而得到对称密钥k_i的值：$k_i = h(m_i)$。

4)检验环方程：检验计算得到的$y_1, y_2, \cdots, y_r$的值是否满足以下等式：$C_{ki, vi}(y_1, y_2, \cdots, y_r) = v_i$。如果该等式成立，则验证者认为获得的投标消息是合法的，并且P_i提交的投标值m_i是合法的。否则，验证者判定该投标者非法，拒绝接受该投标消息，剔除m_i后跳转到第 1)步，直到验证出第一个合法的投标者，即确定为标王。

(4)获胜的投标值的公布

公布获胜值后，只有标王才拥有自己的 *ID*，他可以凭借 *ID* 向验证者证明自己就是标王，从而在现实中完成竞标成功的后续工作，如缴纳资金、领取拍卖品等。而其他的参与者无法在多项式时间内计算出标王的 *ID*，从而无法冒名顶替。

4 方案的安全性及效率分析

本文基于环签名给出了一个适用于集体内的成员进行电子拍卖的方案。该方案的安全性不仅与环签名本身的安全性有关，还与它变动后涉及到的安全性有关。该方案较之环签名的主要变动在于：

(1)环签名要签署的消息 m 是给定的，而在电子拍卖方案中，投标者的投标值是自己生成的，并且每个投标者的投标值可能都不相同。这个不同点不涉及密码学中的任何安全性问题。

(2)在收到签名消息之后，环签名的验证者不需要接收任何消息即可判断签名的合法性，而在电子拍卖方案中，每个投标者都必须发送自己的投标值以证实之前提交的投标消息的合法性。

(3)在电子拍卖的最后一步，验证者公布获胜者的投标值，然后，标王发送自己的 *ID*，从而证明自己就是标王。这一步是环签名不需要的。

因此，本方案只需要证明涉及到的环签名方案的安全性以及变动中涉及到的密码学安全性即可。文献[7]给出了本文用到的环签名 RSA 版本的安全性证明，指出该环签名方案在随机 oracle 模型下是安全的：该方案满足匿名性要求，且不依靠任何复杂度理论的假设；任何组外成员(即攻击者)在向 oracle 询问多项式次问题(假设询问的问题集合为 S，则 $m\notin S$)之后，仍旧不可能以不可忽略的优势生成消息 m 的一个合法的环签名。

本文提出的方案与环签名的不同点在于只有(2)和(3)与安全性有关。其中，(2)的安全性只影响到电子拍卖安全属性中投标值不可伪造性的要求，(3)的安全性涉及到标王身份的不可伪造性的要求。

当拍卖过程结束后，所有的投标者发送投标值对。假设存在强抗碰撞 hash 函数，那么此时，即使投标者作弊，也不可能计算出 $m'(m'\neq m)$，满足 $h(m')=h(m)$。即每个投标者只能发送之前选择好的投标值以证实自己的组员身份和投标消息的合法性。所以此处仍然满足投标值不可伪造性的要求。与此相同，强抗碰撞 hash 函数的存在，也保证了电子拍卖对标王身份不可伪造性的要求。

由于电子拍卖的操作过程不是实时性的，因此对方案的效率没有过高要求。而本方案涉及到的合法计算都可以在多项式时间内完成，故该方案具有很强的可操作性。

5 结束语

本文基于环签名给出了在团体内部电子拍卖的方案，由于该方案不需要组织管理者，那么就不可能检验出投标者的具体身份，因此能够更好地保护投标者的隐私，只有在最后一步，标王会公布自己的 *ID*，然而这是合乎现实情况的，不违背隐私的要求。同时该方案又要求投标者能够证明自己属于该团体，从而有投标的权利，符合团体内部排外性的拍卖活动。文中给出的电子拍卖方案的安全性与文献[7]中的 RSA 版本的环签名方案相同，在随机 oracle 模型下是安全的。由于该方案所有的合法计算都可以在多项式时间时间内完成，因此具有很强的可操作性。但是，非法计算，如冒名顶替标王、篡改合理的投标值都无法在多项式时间内完成，故该方案具有很强的安全性。

参考文献

[1] Franklin M K, Reiter M K. The Design and Implementation of a Secure Auction Service[J]. IEEE Trans. on Software Engineering, 1996, 22(5): 302-312.

[2] lmamura Y, Matsumoto T, Imai H. Electronic Anonymous Bidding Scheme[C]//Proc. of the 1994 Symposium on Cryptography and Information Secufity. Tokyo, Japan: [s. n.], 1994: 152-156.

[3] Nakanishi T, Watanabc H, Fujiwara T, et al. An Anonymous Bidding Protocol Using Undeniable Signature[C]//Proc. of the 1995 Symposium on Cryptography and Information Security. Tokyo, Japan: [s. n.], 1995: 106-112.

[4] Kudo M. Secure Electronic Sealed-bid Auction Protocol with Public Key Cryptography[J]. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Science, 1998, 81(1): 20-27.

[5] Kikuchi H, Nakanishi S. Registration-free Protocol for Anonymous Auction[C]//Proc. of Computer Security Symposium. London, UK: [s. n.], 1998: 243-248.

[6] Chaum D, Eugène Van H. Group Signatures[C]//Proc. of the International Conference on the Theory & Application of Cryptographic Techniques. Berlin, Germany: Springer-Verlag, 1991: 257-265.

[7] Rivest R, Shamir A, Tauman Y. How to Leak a Secret[C]//Proc. of ASIACRYPT'01. New York, USA: Springer-Verlag, 2001: 552-565.

（上接第 31 页）

参考文献

[1] Buckley C, Salton G. Automatic Query Expansion Using SMART[C]//Proceedings of the 3rd Text Retrieval Conference. Gaithersburg, MD, USA: NIST Special Publication, 1995.

[2] Xu Jinxi, Croft B. Query Expansion Using Local and Global Document Analysis[C]//Proceedings of the 19th Annual International ACM SIGIR Conference on Research and Development in Information Retrieval. New York, USA: ACM Press, 1996.

[3] He Tingting, Qu Guozhong, Tu Xinhui, et al. Chinese Information Retrieval Based on Related Term Group[C]//Proceedings of the 5th NTCIR Workshop. Tokyo, Japan: [s. n.], 2005.

[4] Yang Lingpeng, Ji Donghong, Tang Li. Document Re-ranking Based on Global and Local Terms[C]//Proceedings of the 3rd SIGHAN Workshop on Chinese Language Processing. Barcelona, Spain: [s. n.], 2004.

[5] Molina H G, Tomasic A, Shoens K. Incremental Updates of Inverted Lists for Text Document Retrieval[C]//Proceedings of ACM International Conferernce on Management of Data. [S. l.]: ACM Press, 1994.