基于身份的多重代理签名的安全模型

霍 亮[1] 杨 柳[2] 李明祥[1]

(河北金融学院信息管理与工程系 保定 071051)[1] (河北大学经济管理实验中心 保定 071000)[2]

摘 要 多重代理签名是代理签名的重要的扩展形式。它允许一个原始签名人把他的签名权委托给一组代理签名人,只有所有的代理签名人合作才能产生有效的代理签名。将多重代理签名与基于身份的密码学结合起来,人们提出了一些基于身份的多重代理签名方案。不过,迄今为止还没有提出基于身份的多重代理签名的安全模型。文章给出了基于身份的多重代理签名的形式化定义和安全模型。

关键词 多重代理签名,基于身份的签名,基于身份的代理多重签名,安全模型

中图法分类号 TN918.1 **文献标识码** A

Formalized Security Model of Identity Based Multi-Proxy Signature

HUO Liang[1] YANG Liu[2] LI Ming-xiang[1]

(Department of Information Management and Engineering, Hebei Finance University, Baoding 071051, China)[1]

(Experimental Center of Economics and Management, Hebei University, Baoding 071000, China)[2]

Abstract Multi-proxy signature is an extension of the basic proxy signature primitive. In a multi-proxy signature scheme, an original signer can delegate his signing rights to a group of proxy signers. And only the cooperation of all the proxy signers can generate the proxy signature on behalf of the original signer. Combining multi-proxy signature with identity-based cryptography, some identity-based multi-proxy signature schemes have been proposed. But to date, no formalized security model has been provided for identity-based multi-proxy signature schemes. This paper gave the formal definition of identity-based multi-proxy signature schemes and formalize a notion of security for them.

Keywords Multi-proxy signature, Iidentity-based signature, Identity-based multi-proxy signature, Security model

1996年Mambo和Usuda等[1]提出了代理签名(Proxy signature,PS)的概念。在代理签名方案中有一个原始签名人和一个代理签名人,代理签名人能够代表原始签名人行使签名权。2000年Hwang和Shi[2]提出了多重代理签名(Multi-proxy signature,MPS)的概念。在多重代理签名方案中有一个原始签名人和一组代理签名人,只有所有的代理签名人合作才能产生有效的代理签名。可以看出,代理多重签名是(t,n)门限代理签名在$t=n$时的特殊情形。

2003年Boldyreva和Palacio等[3]提出了一个代理签名的安全模型,该模型不允许敌手获得代理私钥。2004年Malkin和Obana等[4]提出了一个多级代理签名的安全模型,该模型允许敌手获得自代理的私钥。2008年Schuldt和Matsuura等[5]提出了一个多级代理签名的安全模型,该模型允许敌手获得所有的代理私钥。显然,Schuldt等的模型比Boldyreva等的模型和Malkin等的模型能俘获更多的攻击。

1984年Shamir[6]提出了基于身份的密码体制的思想。2001年Boneh和Franklin[7]设计了一个实用的基于身份的加密方案。将多重代理签名与基于身份的密码学结合起来,人们提出了一些基于身份的多重代理签名(Identity based multi-proxy signature,IBMPS)方案[8,9]。不过,目前人们还没有提出基于身份的多重代理签名的安全模型。正是由于这一点,这些方案[8,9]都没有提供正式的安全性证明。本文形式化地定义了基于身份的多重代理签名,然后根据代理签名的安全模型[5]提出了一个基于身份的多重代理签名的安全模型。这为以后设计可证安全的基于身份的多重代理签名方案提供了必要的条件。

1 IBMPS的定义

一个IBMPS方案是一个基于身份的签名(Identity based signature,IBS)的扩展,设$IBS=\{\mathcal{G},\mathcal{E},\mathcal{S},\mathcal{V}\}$,IBMPS方案的原始签名人为$ID_A$,代理签名人为$\{ID_{B_1},ID_{B_2},\cdots,ID_{B_n}\}$,并且这组代理签名人的秘书为Clerk。则IBMPS$=\{\mathcal{G},\mathcal{E},\mathcal{S},\mathcal{V},(\mathcal{D},\mathcal{P}_1,\mathcal{P}_2,\cdots,\mathcal{P}_n),\mathcal{MPS},\mathcal{MPV}\}$。

$\mathcal{G}$是系统参数生成算法。它的输入是安全参数1^k,输出是系统参数*params*和主密钥*msk*,并且*params*是公开的。

$\mathcal{E}$是用户私钥生成算法。它的输入是(msk,ID),其中ID为用户的身份,输出是ID的私钥sk_{ID}。

$\mathcal{S}$是标准签名生成算法。它的输入是(sk_{ID},m),其中m是需要签名的消息,输出是ID在m上的签名σ。

$\mathcal{V}$是标准签名验证算法。它的输入是(ID,m,σ),如果σ是ID在m上的有效签名,则输出是Accept,否则,输出是Reject。

$(\mathcal{D},\mathcal{P}_1,\mathcal{P}_2,\cdots,\mathcal{P}_n)$是授权协议,它把原始签名人$ID_A$的签名权委托给代理签名人$\{ID_{B_1},ID_{B_2},\cdots,ID_{B_n}\}$。

霍 亮(1978—),男,博士,副教授,主要研究方向为信息安全,E-mail:comstarhuo@sohu.com。

①$\mathcal{D}$ 由原始签名人 ID_A 执行，它输入(ID_A，$\{ID_{B_1}, ID_{B_2}, \cdots, ID_{B_n}\}$，$w$，$sk_{ID_A}$)，其中 w 是授权证书，包括原始签名人的身份、所有代理签名人的身份、代理签名人的秘书 Clerk、代理签名的消息空间以及授权的期限等信息，$\mathcal{D}$ 与 $\mathcal{P}_i$ ($i=1,2,\cdots,n$)交互，但是它没有局部输出。

②$\mathcal{P}_i$ ($i=1,2,\cdots,n$)由代理签名人 ID_{B_i} 执行，它输入(ID_A，$\{ID_{B_1}, ID_{B_2}, \cdots, ID_{B_n}\}$，$sk_{ID_{B_i}}$)，$\mathcal{P}_i$ 与 $\mathcal{D}$ 交互，输出(ID_A，$\{ID_{B_1}, ID_{B_2}, \cdots, ID_{B_n}\}$，$w$，$psk_i$)，其中 psk_i 是部分代理私钥。

$\mathcal{MPS}$是多重代理签名生成算法。代理签名人 ID_{B_i} ($i=1,2,\cdots,n$)输入(ID_A，$\{ID_{B_1}, ID_{B_2}, \cdots, ID_{B_n}\}$，$w$，$psk_i$，$m$)，输出($ID_A$，$\{ID_{B_1}, ID_{B_2}, \cdots, ID_{B_n}\}$，$w$，$p\sigma_i$)，其中 $p\sigma_i$ 是部分代理签名，并将(ID_A，$\{ID_{B_1}, ID_{B_2}, \cdots, ID_{B_n}\}$，$w$，$p\sigma_i$)发送给代理签名人的秘书 Clerk。Clerk 根据(ID_A，$\{ID_{B_1}, ID_{B_2}, \cdots, ID_{B_n}\}$，$w$，$p\sigma_i$) ($i=1,2,\cdots,n$)输出($ID_A$，$\{ID_{B_1}, ID_{B_2}, \cdots, ID_{B_n}\}$，$w$，$p\sigma$)，其中 $p\sigma$ 是多重代理签名。

$\mathcal{MV}$是多重代理签名验证算法。它的输入是(m，(ID_A，$\{ID_{B_1}, ID_{B_2}, \cdots, ID_{B_n}\}$，$w$，$p\sigma$))，如果 $p\sigma$ 是$\{ID_{B_1}, ID_{B_2}, \cdots, ID_{B_n}\}$代表 ID_A 在 m 上的有效多重代理签名，则输出是 Accept，否则，输出是 Reject。

如果一个 IBMPS 方案满足下面两个要求，则这个 IBMPS 方案是正确的。

①基本的 IBS 方案是正确的。

②对于由 $\mathcal{E}(msk, ID_A)$生成的 sk_{ID_A}、由 $\mathcal{E}(msk, ID_{B_i})$ ($i=1,2,\cdots,n$)生成的 $sk_{ID_{B_i}}$、由 $\mathcal{D}(ID_A, \{ID_{B_1}, ID_{B_2}, \cdots, ID_{B_n}\}, w, sk_{ID_A})$和 $\mathcal{P}_i(ID_A, \{ID_{B_1}, ID_{B_2}, \cdots, ID_{B_n}\}, sk_{ID_{B_i}})$ ($i=1,2,\cdots,n$)生成的(ID_A，$\{ID_{B_1}, ID_{B_2}, \cdots, ID_{B_n}\}$，$w$，$psk_i$)以及任何符合证书 w 的消息 m，有

$\Pr[\mathcal{MPV}(m, \mathcal{MPS}(ID_A, \{ID_{B_1}, ID_{B_2}, \cdots, ID_{B_n}\}, w, psk_i, m)(i=1,2,\cdots,n)))=\text{Accept}]=1$

其中，概率是在 $\mathcal{E}$、$\mathcal{D}$、$\mathcal{P}_i$ ($i=1,2,\cdots,n$)和 $\mathcal{MPS}$随机抛币下得到的。

2 IBMPS 的安全模型

根据代理签名的安全概念[5]，我们可以定义 IBMPS 的安全概念。IBMPS 的安全概念是适应性选择消息和身份的攻击下的存在性不可伪造性(UF-CMIA)，可以通过一个在敌手 $\mathcal{A}$ 与挑战者 $\mathcal{C}$ 之间的游戏定义这个安全概念。

系统建立：$\mathcal{C}$ 选择安全参数 1^k，并运行 $\mathcal{G}(1^k)$生成系统参数 $params$ 和主密钥 msk，将 $params$ 发送给 $\mathcal{A}$。

询问：$\mathcal{A}$ 适应性地向 $\mathcal{C}$ 提出有限次数的询问，每一次询问是下面几种情形之一。

①用户私钥询问：$\mathcal{A}$ 选择(ID)，$\mathcal{C}$ 运行 $\mathcal{E}(msk, ID)$生成 sk_{ID}，并将 sk_{ID} 发送给 $\mathcal{A}$。

②标准签名询问：$\mathcal{A}$ 选择(ID，m)，$\mathcal{C}$ 运行 $\mathcal{E}(msk, ID)$生成 sk_{ID}，运行 $S(sk_{ID}, m)$生成 σ，并将 σ 发送给 $\mathcal{A}$。

③授权询问Ⅰ：$\mathcal{A}$ 选择(ID_A，$\{ID_{B_1}, ID_{B_2}, \cdots, ID_{B_n}\}$，$w$)，$\mathcal{C}$ 扮演代理签名人 ID_{B_i} ($i\in\{1,2,\cdots,n\}$)，A 扮演原始签名人 ID_A 和代理签名人 ID_j ($j=1,2,\cdots,i-1,i+1,\cdots,n$)。$\mathcal{C}$ 运行 $\mathcal{E}(msk, ID_{B_i})$生成 $sk_{ID_{B_i}}$，运行 $\mathcal{P}_i(ID_A, \{ID_{B_1}, ID_{B_2}, \cdots, ID_{B_n}\}, sk_{ID_{B_i}})$生成($ID_A$，$\{ID_{B_1}, ID_{B_2}, \cdots, ID_{B_n}\}$，$w$，$psk_i$)，并将($ID_A$，$\{ID_{B_1}, ID_{B_2}, \cdots, ID_{B_n}\}$，$w$，$psk_i$)发送给 $\mathcal{A}$，同时将(ID_{B_i}，w)加入到表 $pskList$ 中。

④授权询问Ⅱ：$\mathcal{A}$ 选择(ID_A，$\{ID_{B_1}, ID_{B_2}, \cdots, ID_{B_n}\}$，$w$)，$\mathcal{C}$ 扮演原始签名人 ID_A，$\mathcal{A}$ 扮演所有的代理签名人 ID_{B_i} ($i=1,2,\cdots,n$)。$\mathcal{C}$ 运行 $\mathcal{E}(msk, ID_A)$生成 sk_{ID_A}，然后运行 $\mathcal{D}(ID_A, \{ID_{B_1}, ID_{B_2}, \cdots, ID_{B_n}\}, w, sk_{ID_A})$，最后 $\mathcal{C}$ 将(ID_A，w)加入到表 $delList$ 中。

⑤授权询问Ⅲ：$\mathcal{A}$ 选择(ID_A，$\{ID_{B_1}, ID_{B_2}, \cdots, ID_{B_n}\}$，$w$)，其中 $ID_A=ID_{B_i}$ ($i\in\{1,2,\cdots,n\}$)，$\mathcal{C}$ 扮演原始签名人 ID_A 和代理签名人 ID_{B_i}，A 扮演代理签名人 ID_j ($j=1,2,\cdots,i-1,i+1,\cdots,n$)。$\mathcal{C}$ 运行 $\mathcal{E}(msk, ID_{B_i})$生成私钥 $sk_{ID_{B_i}}$，运行 $\mathcal{D}(ID_{B_i}, \{ID_{B_1}, ID_{B_2}, \cdots, ID_{B_n}\}, w, sk_{ID_{B_i}})$和 $\mathcal{P}_i(ID_{B_i}, \{ID_{B_1}, ID_{B_2}, \cdots, ID_{B_n}\}, sk_{ID_{B_i}})$生成($ID_{B_i}$，$\{ID_{B_1}, ID_{B_2}, \cdots, ID_{B_n}\}$，$w$，$psk_i$)，并将($ID_{B_i}$，$\{ID_{B_1}, ID_{B_2}, \cdots, ID_{B_n}\}$，$w$，$psk_i$)发送给敌手 $\mathcal{A}$，同时将(ID_{B_i}，w)加入到表 $pskList$ 中。

⑥多重代理签名询问Ⅰ：$\mathcal{A}$选择(ID_A，$\{ID_{B_1}, ID_{B_2}, \cdots, ID_{B_n}\}$，$w$，$m$)，$\mathcal{C}$扮演代理签名人 ID_{B_i} ($i\in\{1,2,\cdots,n\}$)，$\mathcal{A}$扮演原始签名人 ID_A、代理签名人 ID_j ($j=1,2,\cdots,i-1,i+1,\cdots,n$)和代理签名人的秘书 Clerk。$\mathcal{C}$ 运行 $\mathcal{E}(msk, ID_{B_i})$生成 $sk_{ID_{B_i}}$，运行 $\mathcal{P}_i(ID_A, \{ID_{B_1}, ID_{B_2}, \cdots, ID_{B_n}\}, sk_{ID_{B_i}})$生成($ID_A$，$\{ID_{B_1}, ID_{B_2}, \cdots, ID_{B_n}\}$，$w$，$psk_i$)，运行 $\mathcal{MPS}(ID_A, \{ID_{B_1}, ID_{B_2}, \cdots, ID_{B_n}\}, w, psk_i, m)$生成($ID_A$，$\{ID_{B_1}, ID_{B_2}, \cdots, ID_{B_n}\}$，$w$，$p\sigma_i$)，并将($ID_A$，$\{ID_{B_1}, ID_{B_2}, \cdots, ID_{B_n}\}$，$w$，$p\sigma_i$)发送给 $\mathcal{A}$，同时将(ID_{B_i}，w，m)加入到表 $mpsList$ 中。

⑦多重代理签名询问Ⅱ：$\mathcal{A}$选择(ID_A，$\{ID_{B_1}, ID_{B_2}, \cdots, ID_{B_n}\}$，$w$，$m$)，其中 $ID_A=ID_{B_i}$ ($i\in\{1,2,\cdots,n\}$)，$\mathcal{C}$扮演原始签名人 ID_A 和代理签名人 ID_{B_i}，$\mathcal{A}$扮演代理签名人 ID_j ($j=1,2,\cdots,i-1,i+1,\cdots,n$)和代理签名人的秘书 Clerk。$\mathcal{C}$ 运行 $\mathcal{E}(msk, ID_{B_i})$生成私钥 $sk_{ID_{B_i}}$，运行 $\mathcal{D}(ID_{B_i}, \{ID_{B_1}, ID_{B_2}, \cdots, ID_{B_n}\}, w, sk_{ID_{B_i}})$和 $\mathcal{P}_i(ID_{B_i}, \{ID_{B_1}, ID_{B_2}, \cdots, ID_{B_n}\}, sk_{ID_{B_i}})$生成($ID_{B_i}$，$\{ID_{B_1}, ID_{B_2}, \cdots, ID_{B_n}\}$，$w$，$psk_i$)，运行 $\mathcal{MPS}(ID_{B_i}, \{ID_{B_1}, ID_{B_2}, \cdots, ID_{B_n}\}, w, psk_i, m)$生成($ID_{B_i}$，$\{ID_{B_1}, ID_{B_2}, \cdots, ID_{B_n}\}$，$w$，$p\sigma_i$)，并将($ID_{B_i}$，$\{ID_{B_1}, ID_{B_2}, \cdots, ID_{B_n}\}$，$w$，$p\sigma_i$)发送给敌手 $\mathcal{A}$，同时将(ID_{B_i}，w，m)加入到表 $mpsList$ 中。

伪造：最后，$\mathcal{A}$输出一个伪造的签名，这个伪造的签名是下面 3 种情形之一。

①$\mathcal{A}$输出一个标准签名(m^*，ID^*，σ^*)，如果满足下面 3 个条件，则该签名是有效的。

- $V(m^*, ID^*, \sigma^*)=\text{Accept}$；
- (ID^*)没有提交用户私钥询问；
- (ID^*，m^*)没有提交标准签名询问。

②$\mathcal{A}$输出一个多重代理签名(ID_A^*，$\{ID_{B_1}^*, ID_{B_2}^*, \cdots, ID_{B_n}^*\}$，$w^*$，$p\sigma^*$)，如果满足下面 4 个条件，则该签名是有效的。

- $\mathcal{MPV}(m^*, (ID_A{}^*, \{ID_{B_1}{}^*, ID_{B_2}{}^*, \cdots, ID_{B_n}{}^*\}, w^*, p\sigma^*))=\text{Accept}$；
- ($ID_{B_i}^*$)($i\in\{1,2,\cdots,n\}$)没有提交用户私钥询问；
- ($ID_{B_i}^*$，w^*)$\notin pskList$；
- ($ID_{B_i}^*$，w^*，m^*)$\notin mpsList$。

③$\mathcal{A}$输出一个多重代理签名(ID_A^*，$\{ID_{B_1}^*, ID_{B_2}^*, \cdots,$

$ID_{B_n}^*\}, w^*, p\sigma^*)$，如果满足下面3个条件，则该签名是有效的。

• $\mathcal{MPV}(m^*, (ID_A^*, \{ID_{B_1}^*, ID_{B_2}^*, \cdots, ID_{B_n}^*\}, w^*, p\sigma^*)) = \text{Accept}$；

• (ID_A^*)没有提交用户私钥询问；

• $ID_A^* \neq ID_{B_i}^*$ $(i \in \{1,2,\cdots,n\})$，并且$(ID_A^*, w^*) \notin delList$。

如果$\mathcal{A}$伪造的签名是有效的，则游戏返回1，否则返回0。

我们将上述游戏的运行结果记为$Gm_{IBMPS,\mathcal{A}}^{UF\text{-}CMIA}(k)$，则敌手$\mathcal{A}$在上述游戏中的优势可定义为

$$Adv_{IBMPS,\mathcal{A}}^{UF\text{-}CMIA}(k) = \Pr[Gm_{IBMPS,\mathcal{A}}^{UF\text{-}CMIA}(k) = 1]$$

其中概率是在敌手和挑战者随机抛币下得到的。

对于一个IBMPS方案来说，如果敌手$\mathcal{A}$在上述游戏中的优势至少为ε、运行时间至多为t，并且敌手$\mathcal{A}$提交用户私钥询问的次数至多为q_e、授权询问的次数至多为q_d、签名询问的次数至多为q_s，则敌手$\mathcal{A}$被称为该IBMPS方案的$(\varepsilon, t, q_e, q_d, q_s)$-伪造者；如果这样的$(\varepsilon, t, q_e, q_d, q_s)$-伪造者不存在，则该IBMPS方案被称为$(\varepsilon, t, q_e, q_d, q_s)$-安全的。

可以看出，在上面的模型中，伪造情形②是敌手在不知道一个代理签名人的私钥而知道原始签名人的私钥和其余的代理签名人的私钥时对多重代理签名的伪造；伪造情形③是敌手在不知道原始签名人的私钥而知道所有代理签名人的私钥时对多重代理签名的伪造。因此我们提出的模型完全符合代理签名对强不可伪造性[10,11]的要求。另外，代理签名的安全定义[5]通过一种通用构造方法说明它是可达到的。我们的安全定义也可用类似的方法说明它是可达到的。

结束语 代理签名一提出就受到国内外学者的广泛关注，多重代理签名是代理签名的重要的扩展形式。将多重代理签名与基于身份的密码学结合起来，人们提出了一些基于身份的多重代理签名方案。可是，因为没有基于身份的多重代理签名的安全模型，所以这些方案都没有提供正式的安全性证明。本文形式化地定义了基于身份的多重代理签名，然后提出了一个基于身份的多重代理签名的安全模型。这为以后设计可证安全的基于身份的多重代理签名方案提供了重要的保证。

参考文献

[1] Mambo M, Usuda K, Okamoto E. Proxy signatures for delegating signing operation[C]// Proceedings of the 3rd ACM Conference on Computer and Communications Security (CCS'96). New York: ACM Press, 1996: 48-57

[2] Hwang S, Shi C. A simple multi-proxy signature scheme[C]// Proceedings of the 10th National Conference on Information Security. Hualien, Taiwan, 2000: 134-138

[3] Boldyreva A, Palacio A, Warinschi B. Secure proxy signature schemes for delegation of signing rights[R]. Cryptology ePrint Archive. Report 2003/096, 2003. http://eprint.iacr.org/

[4] Malklin T, Obana S, Yung M. The hierarchy of key evolving signatures and a characterization of proxy signatures[C]// Proceedings of Eurocrypt 2004, Lecture Notes in Computer Science 3027. Berlin: Springer-Verlag, 2004: 306-322

[5] Schuldt J C N, Matsuura K, Paterson K G. Proxy signatures secure against proxy key exposure[C]// Proceedings of Public Key Cryptography 2008 (PKC'08), Lecture Notes in Computer Science 4939. Berlin: Springer-Verlag, 2008: 141-161

[6] Shamir A. Identity-based cryptosystems and signature schemes [C]// Proceedings of Crypto 1984, Lecture Notes in Computer Science 196. Berlin: Springer-Verlag, 1984: 47-53

[7] Boneh D, Franklin M. Identity-based encryption from the Weil pairing[C]// Proceedings of Crypto 2001, Lecture Notes in Computer Science 2139. Berlin: Springer-Verlag, 2001: 213-229

[8] Chen X, Zhang F, Kim K. ID-based multi-proxy signature and blind multisignature from bilinear pairings[C]// Proceedings of KIISC (Korea Institute of Information Security and Cryptology) Conference 2003. Korea, 2003, 11-19

[9] Li X, Chen K. ID-based multi-proxy signature, proxy multi-signature and multi-proxy multi-signature schemes from bilinear pairings[J]. Applied Mathematics And Computation, 2005, 169 (1): 437-450

[10] Lee B, Kim H, Kim K. Strong proxy signature and its applications[C]// Proceedings of the 2001 Symposium on Cryptography and Information Security (SCIS'01). Oiso, Japan, 2001: 603-608

[11] Lee B, Kim H, Kim K. Secure mobile agent using strong non-designated proxy signature[C]// Proceedings of the 6th Australasian Conference on Information Security and Privacy (ACISP'01). Lecture Notes in Computer Science 2119. Berlin: Springer-Verlag, 2001: 474-486

(上接第40页)

[5] Lin H Y, Tzengw G. An efficient solution to the millionaires' problem based on homomorphic encryption [M]. Applied Cryptography and Network Security, LNCS 3531. Berlin: Springer-Verlag, 2005: 456-466

[6] Brankovic L, Estivill-Castro V. Privacy Issues in Knowledge Discovery and Data Mining [C]// Melbourne, Victoria, Australia: Proc. of Australian Institute of Computer Ethics Conference. 1999

[7] Atallah M J, Du W L. Secure multi-party computational geometry [C]// Dehne F K H A, Sack J R, T amassial R. Proceedings of Seventh International Workshop on Algorithms and Data Structures. London: Springer-Verlag, 2001: 165-179

[8] Li Shun-dong, Dai Yi-qi. Secure two-party computational geometry [J]. Journal of Computer Science and Technology, 2005, 20 (2): 258-263

[9] Luo Yong-long, Huang Liu-sheng, et al. A secure protocol for determining whether a point is inside a convex polygon[J]. Chinese Journal of Electronics, 2006, 15(4): 578-582

[10] 李顺东，戴一奇，王道顺. 几何相交的多方安全保密计算[J]. 清华大学学报：自然科学版，2007，47(10)：1692-1695

[11] 罗永龙，黄刘生. 空间几何对象相对位置判定中的私有信息保护[J]. 计算机研究与发展，2006，43(3)：410-416

[12] Tzeng W. Efficient 1-out-of-n oblivious transfer schemes with universally usable parameters [J]. IEEE Trans. on Computers, 2004, 53(2): 232-24

[13] Goldwasser S. Multi-party Computations: Past and Present [D]. Santa Barbara CA: [s. n.], 1997