doi:10.11959/j.issn.1000-436x.2015246

新型组织隐藏的认证密钥交换协议

温雅敏[1,2]，龚征[3,4]

（1. 广东财经大学 数学与统计学院，广东 广州 510320；2. 上海市信息安全综合管理技术研究重点实验室，上海 200240；
3. 华南师范大学 计算机学院，广东 广州 510631；4. 中国科学院 信息工程研究所 信息安全国家重点实验室，北京 100093）

摘 要：提出了一个实现组织集合交集认证策略的新型组织隐藏的密钥协商协议，2 个匿名用户从属的组织集合存在交集且元素个数至少为一个门限值时可以完成一次成功的秘密认证和密钥协商，同时保证集合交集之外的组织信息机密性。新协议在随机预言机模型下可证安全，并且在计算和通信性能上仍具备一定的优势。

关键词：组织隐藏；认证密钥交换；秘密握手；集合交集；可关联性

中图分类号：TP309.7 **文献标识码**：A

New affiliation-hiding authenticated key exchange protocol

WEN Ya-min[1,2], GONG Zheng[3,4]

(1.School of Mathematics and Statistics, Guangdong University of Finance and Economics, Guangzhou 510320, China;
2. Shanghai Key Laboratory of Integrated Administration Technologies for Information Security, Shanghai 200240, China;
3.School of Computer Science, South China Normal University, Guangzhou 510631, China;
4. State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China)

Abstract: A new affiliation-hiding authenticated key agreement protocol was proposed. The proposal enables two anonymous users to accomplish a successful secret authentication and key agreement when their groups set intersection is non-empty and the cardinality of the set intersection should not be less than a threshold value. Meanwhile, the affiliations of groups outside of the set intersection remain confidential. The proposal is provably secure under the random oracle model, and the performance of the scheme is still competitive.

Key words: affiliation-hiding; authenticated key agreement; secret handshakes; set intersection; link ability

1 引言

组织隐藏的认证密钥交换（AH-AKE, affiliation-hiding authenticated key exchange）[1,2]是一种特殊的认证密钥协商协议，除了实现安全会话密钥建立的功能，还能够达到秘密握手（SH, secret handshakes）方案[3]中组织隐藏的隐私保护认证功能。一般意义上基于公钥的认证和密钥交换协议在设计中没有考虑用户的隐私性保护，用户的身份和证书在实际认证中往往以明文的方式传输。而组织隐藏的认证密钥协商协议则需要保护用户的身份并隐藏其所从属的组织信息。AH-AKE 协议是在秘密握手方案的基础上构造的具有更强安全定义的密钥交换协议[2]，它的基本功能来源于秘密握手方案，仅允许相同组织内的成员实现相互地秘密认证。一个典型应用场景是 2 个 FBI 探员（例如，Alice 和 Bob）在公开网络希望识别彼此并秘密通信，由于 FBI 的身份信息是需要保密的，因此 Alice 或 Bob 在确保通信对方是 FBI

收稿日期：2014-07-24；**修回日期**：2015-06-30

基金项目：国家自然科学基金资助项目(61300204, 61572028)；广东省自然科学基金资助项目(2015A030313630, 2014A030313439, S2013020011913)；广东省高等学校优秀青年教师培养计划基金资助项目（Yq2013051）；广州市珠江科技新星专项基金资助项目（2014J2200006）；上海市信息安全综合管理技术研究重点实验室开放课题基金资助项目

Foundation Items: The National Natural Sciences Foundation of China (61300204, 61572028); The Natural Science Foundation of Guangdong Province(2015A030313630, 2014A030313439, S2013020011913); The Foundation for Distinguished Young Teachers in Higher Education of Guangdong Province (Yq2013051); The Project of Science and Technology New Star of Guangzhou Pearl River (2014J2200006); The Opening Project of Shanghai Key Laboratory of Integrated Administration Technologies for Information Security

的成员时才暴露自己的 FBI 身份。

上述实际组织隐藏的认证问题最早由 Balfanz 等[3]于 2003 年第一次提出并给出了简单的方案实现。随后，有许多基于不同密码学技术实现的两方秘密握手方案被陆续提出，主要划分为可关联(linkable)秘密握手方案和不可关联（unlinkable）秘密握手方案。可关联的秘密握手方案指同一个用户所执行的多次秘密握手实例可以通过伪名加以关联，如基于“CA-不经意公钥加密”[4]、基于 ElGamal 签名和数字签名算法(DSA)构建的方案[5]以及基于 RSA 的方案[6]等都是基于伪名实现的可关联秘密握手方案。上述方案还可以通过伪名证书的一次性使用实现秘密握手方案的不可关联性，使同一个用户所执行的多次秘密握手实例无法关联。然而伪名证书的一次性使用会增加系统的存储和计算开销，因此要实现不可关联方案更多地是采用可重用的群证书技术。结合 Balfanz 等[3]的方案和盲化技术，陆续有一些基于可重用证书不可关联方案被提出[7~10]。由于仅允许相同组织内成员秘密认证的基本功能在应用中存在一定的局限性，具有更丰富认证功能的不可关联秘密握手协议陆续被许多学者提出，例如 Ateniese 等[11]提出的动态和模糊的秘密握手方案，实现了更加灵活的认证策略，在 Ateniese 等方案的基础上，Sorniotti 和 Molva[12~14]也陆续提出了一些支持更灵活策略的双向认证方案。

大多数不可关联的秘密握手方案使群管理中心（GA, group authority）无法识别用户的握手行为，无法对其管理的组织成员实施追踪和撤销。虽然不可关联性为用户提供了很好的隐私性保护，但使群管理中心对群成员缺少有效的管理。在很多实际的应用场合，为了便于群组织的管理和协议的有效实现，允许用户的多次握手实例是可关联有时是必要的，例如在社交网络中某一个社团管理者需要区分其组织内不同成员的行为。可关联的秘密握手方案通过伪名证书为 GA 提供了有效的撤销和追踪方式，可以使组织的 GA 对其群成员进行有效的管理。许多面向群组织的实际应用中更多实现的是支持可关联的握手认证协议。因此，在可关联秘密握手这类实体认证协议基础上考虑更强攻击模型且保证会话密钥安全的 AH-AKE 协议首次被 Jarecki 等[1,2]提出。

AH-AKE 协议可应用于有多个组织存在的环境中，现有大多数 SH 协议和 AH-AKE 协议的认证策略考虑的是协议参与实体从属于某一个(single)组织。而随着网络应用需求的不断更新，用户往往同时从属于多个(multiple)不同的组织，新的认证策略也随之产生。当用户从属的多个组织用一个集合来表示，网络中 2 个匿名用户所从属的组织集合的交集不为空集或者交集元素个数至少为某个门限值可以作为 AH-AKE 新的认证策略，当且仅当协议双方所从属的组织满足上述认证策略时才能成功地协商出一个会话密钥，交集之外的用户组织信息仍保证是机密的。这类新型的隐私保护认证是在文献[2]中首次提出的组织发现(group discovery)问题，随后 Manulis 等在文献[15]中基于 RSA 给出了线性复杂度的有效实现。然而 RSA 系统中提供的群公钥在实际应用中不能有效地实现组织隐藏的安全要求，由此带来的计算开销相对较大，限制了协议的适用性和可靠性。因此，本文在文献[15]的基础上基于离散对数的困难性假设构造了一个新型的支持多组织交集的组织隐藏认证密钥交换协议，结合离散对数问题和索引隐藏消息编码技术提高协议的计算性能和良好的可移植性。

2　预备知识

2.1　复杂性假设

接下来介绍本文方案所涉及到的困难性问题和复杂性假设。

离散对数问题(DLP, discrete log problem)：假设 G 是素数阶为 p 的循环群，令 $g\in_R G$ 是 G 的生成元，给定 $g,h\in G$ 作为均匀分布的输入，输出满足 $h=g^x$ 的唯一整数 $x<p$。

DL 假设　如果不存在任一多项式时间算法能以不可忽略的概率解出离散对数问题，认为这是一个 DL 假设。

离散对数表示问题(DLRP, discrete logarithm representation problem)[16]：令 G 是素数阶为 p 的循环群，$g_1,\cdots,g_k\in G$ 是 G 的 $k\geqslant 2$ 个生成元。把 $(g_1,\cdots,g_k)$ 和 $h\in G$ 作为均匀分布的输入，输出唯一的一个 k 元组 $(a_1,\cdots,a_k)$，称之为 h 关于生成元 $(g_1,\cdots,g_k)$ 的表示，满足等式 $h=\prod_{i=1}^{k} g_i^{a_i}$。

DLR 假设　如果不存在多项式时间算法能以不可忽略的概率解出离散对数表示问题(DLRP)，认

为这是一个 DLR 假设。正如文献[16]中的描述，离散对数表示问题在计算复杂度上等价于离散对数问题。

2.2 索引隐藏消息编码

为了能对用户从属的多个组织信息实现有效的隐私保护，本文将借鉴文献[15]中使用的索引隐藏消息编码(IHME, index-hiding message encoding)技术，在此对该技术进行简要介绍。

定义 1 一个基于索引的消息编码方案是在一个索引空间 I 和一个消息空间 M 上定义的 2 个有效算法。

$iEncode(P)$:算法输入一个索引—消息对元组集合 $P=\{(i_1,m_1),\cdots,(i_n,m_n)\}\subseteq I\times M$，其中，每个索引 $i_1,\cdots,i_n$ 都是不同的，最后算法输出编码 S。

$iDecode(S,i)$：算法输入一个编码 S 和一个索引 $i\in I$，最后输出消息 $m\in M$。

如果 $iDecode(iEncode(P),i_j)=m_j$，那么这个基于索引的消息编码方案是正确的。

如果方案对消息进行编码时能隐藏索引，那么这个基于索引的消息编码方案是索引隐藏的(index-hiding)，下面给出其严格的形式化定义。

定义 2 $IHME=(iEncode,iDecode)$ 表示一个正确的基于索引的消息编码方案，令 $b\in\{0,1\}$ 是随机选择的比特，A=(A_1,A_2)表示 2 个攻击者，用攻击游戏 $Game_{A,IHME}(\kappa)$ 来形式化定义消息编码的索引隐藏。

1) 攻击者 A_1 首先选择 2 个大小为 n 的指标集合子集和对应的消息,即 $A_1(1^\kappa)\to(I_0,I_1,M')$ 其中,$I_0,I_1\subseteq I$ 且 $|I_0|=|I_1|=n$，$M'=(m'_1,\cdots,m'_{|I_0\cap I_1|})$ 且每个 $m'_j\in M$。

2) 把集合 I_b 除去 I_{1-b} 内指标的集合 $\frac{I_b}{I_{1-b}}$ 定义为 $\{i_1,\cdots,i_r\}$，并从消息空间中随机选择 r 个消息，其中，$r=n-|I_0\cap I_1|$。然后对这 r 对指标消息进行编码 $S\leftarrow iEncode\left(\{(i_j,m'_j)|i_j\in I_0\cap I_1\}\cup\left\{(i_j,m_j)|i_j\in\frac{I_b}{I_{1-b}}\right\}\right)$。

3) $b'\leftarrow A_2(S)$，攻击者 A_2 在给定编码 S 后尝试猜测比特 b。

4) 如果 $b'=b$，则游戏返回“1”，否则返回“0”。

定义攻击者 A 成功地概率优势 $Adv_{A,IHME}(\kappa)$ 为 $|\Pr[Game^0_{A,IHME}(\kappa)=1]-\Pr[Game^1_{A,IHME}(\kappa)=1]|$。如果这个概率优势是可忽略的，则 IHME 方案满足索引隐藏。

3 新型组织隐藏的认证密钥交换协议

为了能适应广泛的网络应用需求，针对用户从属于多个组织属性的前提下实现组织发现的双向认证问题，本文将在文献[15]的启发下基于有限域离散对数困难问题构造一个新型的可关联组织隐藏认证密钥交换协议，该构造也可以推广到椭圆曲线上实现。为了区别于之前的认证密钥交换协议，本文提出的新型方案定义为多组织环境下可关联组织隐藏的认证密钥交换(MLAH-AKE, multiple-groups linkable affiliation-hiding authenticated key exchange)。首先将给出 MLAH-AKE 基本的形式化模型和安全定义。

3.1 模型与安全定义

可关联的认证密钥协商协议的功能来源于秘密握手方案，借鉴组织隐藏认证密钥交换协议[2]及秘密握手[3]的模型和定义，MLAH-AKE 可类似推广定义为以下几个算法。

1) 系统建立(setup)。该算法选择一个安全参数 κ 输入后，输出公开的参数 params，系统参数可以被接下来创建的群组织所共用。

2) 组织创建(create group)。该算法的功能是创建一个新的组织 G，由其对应的群管理中心 GA 来完成。输入公开参数 params，群组织创建算法输出群的公私钥对 (gpk_G,gsk_G)。此外，GA 需建立用户撤销列表 url_G 并初始化为空集 Φ。

3) 成员加入(add member($U\leftrightarrow G_i$))。该算法是组织 G_i 的群管理中心 GA 和一个预期的群成员用户(如 U)共同交互完成的两方协议。用户 U 首先生成一个伪名 id_U 并和其他身份信息一起发送给 GA，由 GA 对用户真实身份进行检查和验证。如果用户符合加入组织 G_i 的条件并通过验证，GA 将利用群密钥为用户颁发群成员证书 $cred_{U,G_i}$，使用户成为该组织的合法成员。

4) 认证密钥交换/握手(handshake ($U_i\leftrightarrow U_j$))。该算法是有 2 个用户 U_i 和 U_j 执行的认证密钥协商（也可称为握手）协议，其中，每个用户都可能是多个组织的合法成员。假设用户 U_i 为协议的发起者，输入为 $(id_i,Glist_i,init)$，其中，id_i 是 U_i 的伪名，$Glist_i$ 包含用户 U_i 所从属的所有组织信息记录，每一条记录对应一个组织信息，包含有群公钥、群证

书和群撤销列表，以信息元组的形式表达为 $(gpk_{G_i}, cred_{U_i,G_i}, url_{G_i})$。对于用户 U_j，协议输入为 $(id_j, Glist_j, resp)$。一次握手会话的状态可以标记为 $\pi.state$，并且会不断更新。如果协议正在运行，则 $\pi.state \leftarrow running$。如果协议运行完成，则会话状态将根据协议双方是否满足认证策略更新为成功(accepted，输出为“1”)或者失败(rejected，输出为“0”)。

5) 撤销(revoke(G, id))。这个算法如果输入为 (G, id)，则由组织 G 的群管理中心执行并更新他的组织撤销列表 $url_G \leftarrow url_G \cup \{id\}$。

参照文献[15]中对组织隐藏认证密钥协商协议的安全要求和定义，本节在此基础上给出新型的 MLAH-AKE 协议需要满足 2 个基本安全要求的定义：可关联组织隐藏安全(LAH-Security, linkable affiliation-hiding security)和认证密钥交换安全(AKE-Security, authenticated key exchange security)。

1）可关联组织隐藏安全(LAH-Security)。这个安全要求的主要目标是保护 2 个协议参与方不属于交集的组织信息机密性，其形式化定义包含一个攻击者 A 和一个挑战者 F 之间的攻击游戏。$Game^{lah,b}(\kappa, m, n)$，攻击者的目标是对挑战者模拟的某个握手会话中的组织信息进行识别，这个安全定义类似于加密方案中使用不可区分的选择密文攻击可证安全方法，攻击者可以向挑战者询问 MLAH-AKE 方案算法的信息和执行结果，从而获得很好的训练。令攻击者 A 可以询问的预言机算法统一表示为 O={*CreateGroup*, *AddMember*, *Handshake*, *Revoke*}，攻击游戏 $Game^{lah,b}(\kappa, m, n)$ 可以定义为以下几个步骤。

step1　挑战者 F 模拟 MLAH-AKE 环境。创建 m 个用户 $U_1, \cdots, U_m$ 及其对应的伪名 $ID = \{id_1, \cdots, id_m\}$；建立 n 个群组织 $\tilde{G} = \{G_1, \cdots, G_n\}$，并且模拟每个具有伪名 id_i 的用户 U_i 加入组织 G_j，其中，$(i, j) \in [1, m] \times [1, n]$。

step2　攻击者 A^O 可以询问 O 中的算法获得足够的信息，然后输出 $(id^*, \tilde{G}_0^*, \tilde{G}_1^*, init)$，其中 $id^* \in ID$，$\tilde{G}_0^*, \tilde{G}_1^* \subseteq \tilde{G}$ 且 $|\tilde{G}_0^*| = |\tilde{G}_1^*|$，对 $\tilde{G}_0^*$ 和 $\tilde{G}_1^*$ 2 个集合的非交集部分定义为集合 $D^* = \left(\frac{\tilde{G}_0^*}{\tilde{G}_1^*}\right) \cup \left(\frac{\tilde{G}_1^*}{\tilde{G}_0^*}\right) = \frac{(\tilde{G}_0^* \cup \tilde{G}_1^*)}{(\tilde{G}_0^* \cap \tilde{G}_1^*)}$；

step3　挑战者 F 随机选择一个比特 $b \leftarrow_R \{0,1\}$，然后运行握手算法 Handshake($id^*, \tilde{G}_b^*, init$)，对应的会话定义为 π^*。

step4　攻击者 A^O 可以继续对 MLAH-AKE 方案中的算法进行询问，但有一定的限制。对与会话 π^* 相关的一些秘密信息不能被询问；如果与 id^* 握手的其他实体（会话 π'）的组织集合与 D^* 存在交集，那么与会话 π' 相关的一些秘密信息不能被询问；另外，当会话 π^* 执行结束前不能询问关于 $(id, G) \in ID \times D^*$ 的群证书等秘密信息。

step5　最后输出对随机比特位的猜测 b'，如果 $b = b'$，则攻击游戏成功输出为“1”，否则输出为“0”。

令攻击者成功的概率优势为 $Adv^{lah,b}(\kappa, m, n) = |\Pr[Game^{lah,0}(\kappa, m, n) = 1] - \Pr[Game^{lah,1}(\kappa, m, n) = 1]|$，如果该概率优势可以忽略的话，称方案 MLAH-AKE 是 LAH-security。

2) 认证密钥交换安全(AKE-security)。这个安全要求旨在保护协议双方协商出的密钥安全性，其形式化定义类似于普通认证密钥协商协议[17]给出的攻击模型，通过一个攻击者 A 和一个挑战者 F 之间的攻击游戏 $Game^{ake,b}(\kappa, m, n)$ 来定义，其中，包含会话新鲜性(session freshness)和完善的前向安全性(PFS, perfect forward secrecy)2 个性质。攻击者的目标是区分一个真实的会话密钥和随机产生的密钥，攻击者可以向挑战者询问 MLAH-AKE 方案对应的预言机 O 算法的信息和执行结果，从而获得很好的训练。攻击游戏 $Game^{ake,b}(\kappa, m, n)$ 可以定义为以下几个步骤。

step1　挑战者 F 模拟 MLAH-AKE 环境。创建 m 个用户 $U_1, \cdots, U_m$ 及其对应的伪名 $ID = \{id_1, \cdots, id_m\}$；建立 n 个群组织 $\tilde{G} = \{G_1, \cdots, G_n\}$，并且模拟每个具有伪名 id_i 的用户 U_i 加入组织 G_j，其中，$(i, j) \in [1, m] \times [1, n]$。

step2　攻击者 A^O 可以通过询问 O 中的握手算法与系统用户进行交互。

step3　在某个时刻，攻击者 A^O 向挑战者询问获得一个新鲜(fresh)会话 $\pi^*(id^*)$ 的密钥 K；根据新鲜会话的定义[2]，会话 π^* 握手成功并且与 π^* 相关的预言机算法没有被攻击者询问；此外与 π^* 握手的其他会话实体 $\pi'(id')$ 对应的秘密信息也没有被询问。

step4　挑战者 F 随机选择一个比特 $b \leftarrow_R \{0,1\}$，如果 $b = 1$，则会话密钥 $K = \pi^*.key$ 返回给攻击者；如果 $b = 0$，则随机生成一个密钥 $K \leftarrow_R \{0,1\}^\kappa$ 返回

给攻击者。

step5 攻击者 A^O 可以继续对 MLAH-AKE 方案中的算法进行询问，最后输出对随机比特位的猜测 b'，如果 $b=b'$，则攻击游戏成功输出为“1”，否则输出为“0”。

令攻击者成功的概率优势为 $Adv^{aka,b}(\kappa,m,n)=|2\Pr[Game^{aka,b}(\kappa,m,n)=b]-1|$，如果该概率优势可以忽略的话，称方案 MLAH-AKE 是 AKE-security。

3.2 MLAH-AKE 协议的新型构造

MLAH-AKE 协议的一个新型构造描述如下。

1) 系统建立（setup）。给定一个安全参数 κ，执行 $Setup(1^\kappa)\rightarrow params$。其中，$g\in Z_p^*$ 是群 Z_p^* 中 q 阶子群的生成元，$H_1:\{0,1\}^*\rightarrow Z_q$ 和 $H_2:\{0,1\}^*\rightarrow\{0,1\}^\kappa$ 是密码学散列函数。

2) 组织创建（creategroup）。MLAH-AKE 系统中任一组织 G_i 的 GA_i 随机选取 $gsk_i=x_i\leftarrow_R Z_q^*$ 作为该群组织的群私钥，然后输出群公钥 $gpk_i=y_i=g^{x_i}$。

3) 成员加入（addmember）。用户 U 允许加入到多个组织成为合法成员，以加入组织 G_i 为例，用户 U 把生成的伪名 id_U 以及其他身份信息发送给 GA_i，由 GA_i 验证用户的身份后为其签发群证书 $cred_{U,G_i}=(w_{Ui},t_{Ui})$，其中，$w_{Ui}=g^{\gamma_i}\bmod p$（$\gamma_i\leftarrow_R Z_q$），$t_{Ui}=\gamma_i+x_iH_1(id_U\|w_{Ui})$。这类似于由 GA_i 为用户 U 签发一个 Schnorr 签名[18]。

4) 认证密钥交换/握手（handshake）。假设用户 A 作为发起者与另一个用户 B 进行秘密通信，用户 A 和用户 B 各自都持有多个组织颁发的群证书，可以用集合的方式表示。令用户 A 的输入为 $(id_A,Glist_A,init)$，而用户 B 的对应输入为 $(id_B,Glist_B,resp)$。为了保护所从属的组织信息，他们希望通过握手协议实现双向认证和密钥协商，当且仅当用户 A 和用户 B 所从属的组织集合交集非空且集合元素个数至少为一个门限值时，握手协议才能执行成功，握手协议的具体实现包含以下 3 个步骤。

step1 $A\rightarrow B:\{id_A,S_A\}$

①用户 A 维护一个信息集合 P_A 用于对其从属的多个组织进行统一编码，P_A 初始化为空集，然后对 $Glist_A$ 中的每一条记录 $(gpk_{Ai},cred_{A,G_i},url_{Ai})=(y_{Ai},(w_{Ai},t_{Ai}),url_{Ai})$ 中的可编码信息并入集合 P_A 中，即 $P_A\leftarrow P_A\cup\{gpk_{Ai},w_{Ai}\}(i=1,\cdots,n)$，其中，$A$ 从属的真实组织记录为有效信息，其他为随机产生的信息。

②然后用户 A 对信息集合 P_A 实现索引隐藏的消息编码 $iEncode(P_A)\rightarrow S_A$，即定义一个多项式函数 $f_A=\sum_{k=0}^{n-1}a_kx^k$ 使对于集合 P_A 中的任一二元组 $\forall(gpk_{Ai},w_{Ai})\in P_A$ 都满足 $f_A(gpk_{Ai})=w_{Ai}$，最后输出编码 $S_A=(a_{n-1},\cdots,a_0)$。

③用户 A 最后把伪名 id_A 及编码 S_A 一并发送给用户 B。

step2 $B\rightarrow A:\{id_B,S_B,S_B'\}$

①用户 B 接收到 $\{id_A,S_A\}$ 后，则以类似的方式对自己所从属的多个组织实现统一编码，首先生成一个信息集合 P_B，然后输出编码 $iEncode(P_B)\rightarrow S_B$，即定义一个多项式函数 $f_B=\sum_{k=0}^{n-1}b_kx^k$ 使对于集合 P_B 中的任一二元组 $\forall(gpk_{Bj},w_{Bj})\in P_B(j=1,\cdots,n)$ 都满足 $f_B(gpk_{Bj})=w_{Bj}$，最后输出编码 $S_B=(b_{n-1},\cdots,b_0)$。

②对于组织列表 $Glist_B$ 中的每一条记录 $(gpk_{Bj},cred_{B,G_j},url_{Bj})=(y_{Bj},(w_{Bj},t_{Bj}),url_{Bj})$，首先检查 id_A 是否在记录中的组织撤销列表 url_{Bj} 中，对于用户 $id_A\notin url_{Bj}$ 的组织记录，依次对 S_A 进行解码生成 $w'_{Aj}\leftarrow iDecode(S_A,y_{Bj})$。

③运用解码生成的 w'_{Aj} 以及 t_{Bj} 计算 $r_{Bj}=(w'_{Aj}\cdot y_{Bj}^{H_1(id_A\|w'_{Aj})})^{t_{Bj}}$ 和 $c_{Bj}=H_2(y_{Bj}\|r_{Bj}\|\quad sid_B\|resp)$，其中，$sid_B$ 是这次会话的唯一标识符。

④对解码计算的信息进行编码，类似地初始化集合 $P'_B=\phi$，然后依次把 (y_{Bj},c_{Bj}) 循环并入集合 P'_B 中，即 $P'_B\leftarrow P'_B\cup\{(y_{Bj},c_{Bj})\}$。

⑤对 P'_B 进行索引隐藏编码，$iEncode(P'_B)\rightarrow S'_B$，即定义一个多项式函数 $f'_B=\sum_{k=0}^{n-1}b'_kx^k$ 使对于集合 P_B 中的任一二元组 $\forall(y_{Bj},c_{Bj})\in P'_B$ 都满足 $f'_B(y_{Bj})=c_{Bj}$，输出编码 $S'_B=(b'_{n-1},\cdots,b'_0)$。

⑥用户 B 把伪名 id_B 以及编码生成的 S_B,S'_B 一并返回给用户 A。

step3 $A\rightarrow B:\{S'_A\}$

①从用户 B 处接收到 $\{id_B,S_B,S'_B\}$ 之后，用户 A 对于组织列表 $Glist_A$ 中的每一条记录 $(gpk_{Ai},cred_{A,G_i},url_{Ai})=(y_{Ai},(w_{Ai},t_{Ai}),url_{Ai})$，首先检查 id_B 是否在记录中的组织撤销列表 url_{Ai} 中，对于用户 $id_B\notin url_{Ai}$ 的组织记录依次使用 $Glist_A$ 中的群公钥 $gpk_{Ai}=y_{Ai}$ 对 S_B 解码输出 $w'_{Bi}\leftarrow iDecode(S_B,y_{Ai})$，并

且计算 $r_{Ai}=(w'_{Bi}y_{Ai}^{H_1(id_B\|w'_{Bi})})^{t_{Ai}}$ 和 $c_{Ai}=H_2(y_{Ai}\|r_{Ai}\|sid_A\|init)$，其中，$sid_A$ 是这次会话的唯一标识符。

②然后用户 A 仍然使用 $Glist_A$ 中的群公钥 $gpk_{Ai}=y_{Ai}$ 对 S'_B 解码输出 $c'_{Bi}\leftarrow iDecode(S'_B,y_{Ai})$。

③用户 A 验证 $c'_{Bi}\overset{?}{=}H_2(y_{Ai}\|r_{Ai}\|sid_A\|resp)$ $(i=1,\cdots,n)$，如果上述 n 个等式都不成立，则说明用户 B 不符合用户 A 的认证策略，用户 A 返回一个随机编码值 $S'_A\leftarrow\{u_0,\cdots,u_{n-1}\}(u_i\leftarrow_R Z_q^*)$，协议输出为“0”。

④如果 n 个等式中至少有 d（认证策略确定的门限值）个等式成立，则说明用户 A 与用户 B 的组织集合存在交集并且满足门限认证策略，协议输出为“1”，协商出会话密钥 $K=H_2(g^{t_{Ak_1}t_{Bk_2}}\|\cdots\|g^{t_{Ak_d}t_{Bk_d}})$。其中，$k_i(i=1,\cdots,d)$ 对应于等式通过验证的组织下标。

⑤为了让用户 B 对用户 A 的组织信息进行确认，用户 A 将类似地初始化集合 $P'_A=\phi$，然后依次把 (y_{Ai},c_{Ai}) 循环并入集合 P'_A 中，即 $P'_A\leftarrow P'_A\cup\{(y_{Ai},c_{Ai})\}$。然后对 P'_A 进行索引隐藏编码，$iEncode(P'_A)\rightarrow S'_A$，即定义一个多项式函数 $f'_A=\sum_{k=0}^{n-1}a'_kx^k$ 使得对于集合 P'_A 中的任一二元组都 $\forall(y_{Ai},c_{Ai})\in P'_A$ 满足 $f'_A(y_{Ai})=c_{Ai}$，输出编码 $S'_A=(a'_{n-1},\cdots,a'_0)$ 并返回给用户 B。

⑥用户 B 最后类似地用 y_{Bj} 对 S'_A 进行解码输出 $c'_{Aj}\leftarrow iDecode(S'_A,y_{Bj})$，并依次验证 $c'_{Aj}\overset{?}{=}H_2(y_{Bj}\|r_{Bj}\|sid_B\|init)$ $(j=1,\cdots,n)$，验证至少有 d 个等式成立时才能成功协商出会话密钥，协议输出为“1”，否则认证不成功，协议输出为“0”。

5) 撤销 (revoke(G_i,id_A))。当用户 A 关于组织 G_i 的秘密信息被泄露或者用户 A 主动申请离开组织 G_i 时，则组织 G_i 的群管理中心把 id_A 移入撤销列表中并更新他的组织撤销列表 $url_{G_i}\leftarrow url_{G_i}\cup\{id_A\}$。

正确性（correctness）。根据上述 3 轮交互的认证密钥交换协议，可以看出如果用户 A 和用户 B 所从属的组织集合存在交集且至少有 d 个元素，则用户 A 和用户 B 在不泄露交集外组织信息的前提下能正确认证并协商出一个会话密钥。当用户 B 用自己的组织群公钥 $y_{Bj}(j=1,\cdots,n)$ 对 s_A 进行解码，而只有当 $y_{Bj}=y_{Aj}(j=i)$ 时才能正确解码，即用户 B 和用户 A 组织集合中第 j 个组织是相同的，从而获得 $w'_{Aj}=w_{Aj}$，可以用以下等式验证协议的正确性。

$$\begin{aligned}r_{Bj}&=(w'_{Aj}y_{Bj}^{H_1(id_A\|w'_{Aj})})^{t_{Bj}}=(w_{Aj}y_{Aj}^{H_1(id_A\|w_{Aj})})^{t_{Bj}}\\&=(g^{\gamma_{Aj}}g^{x_{Aj}H_1(id_A\|w_{Aj})})^{t_{Bj}}=(g^{\gamma_{Aj}+x_{Aj}H_1(id_A\|w_{Aj})})^{t_{Bj}}\\&=(g^{t_{Aj}})^{t_{Bj}}=(g^{t_{Bj}})^{t_{Aj}}\end{aligned}$$

类似地，用户 A 用自己的组织群公钥 $y_{Ai}(i=1,\cdots,n)$ 对 S_B 和 S'_B 解码，当 $y_{Ai}=y_{Bi}(i=j)$ 时才能正确解码出 $w'_{Bi}=w_{Bi}$ 以及 $c'_{Bi}=c_{Bj}=c_{Bi}$，利用 w'_{Bi} 可以正确计算出 $r_{Ai}=(g^{t_{Bi}})^{t_{Ai}}$，而用户 A 和用户 B 的会话标识符相等 $sid_A=sid_B$。用户 A 通过下列等式验证确认用户 B 的组织集合是否与用户 A 的组织集合存在 d 个元素交集

$$\begin{aligned}c'_{Bi}=c_{Bj}&=H_2(y_{Bj}\|r_{Bj}\|sid_B\|resp)\ (i=1,\cdots,n)\\&=H_2(y_{Ai}\|g^{t_{Aj}\cdot t_{Bj}}\|sid_A\|resp)\\&=H_2(y_{Ai}\|g^{t_{Bi}\cdot t_{Ai}}\|sid_A\|resp)\\&=H_2(y_{Ai}\|r_{Ai}\|sid_A\|resp)\end{aligned}$$

类似地，用户 B 也可以验证 $c'_{Aj}\overset{?}{=}H_2(y_{Bj}\|r_{Bj}\|sid_B\|init)$ 来确认用户 A 是否符合多组织交集的认证策略。因此，如果有 d 个等式成立，则用户 A 和用户 B 可以协商出一个会话密钥 $K=H_2(g^{t_{Ak_1}t_{Bk_2}}\|\cdots\|g^{t_{Ak_d}t_{Bk_d}})$，协议认证成功输出为“1”，否则，输出为“0”。

4　安全与性能分析

本节将对上述构造的 MLAH-AKE 方案的安全与性能进行简要分析，首先基于离散对数问题的困难性假设，证明新型的 MLAH-AKE 协议满足可关联组织隐藏安全（LAH-security）和认证密钥交换安全(AKE-security)。

4.1　安全分析

定理 1　基于 DLP 假设,MLAH-AKE 协议在随机预言机模型下证明是可关联组织隐藏安全（LAH-security）。

证明　根据 3.1 节中 LAH-security 的形式化定义，如果攻击者 A 参与的攻击游戏 $Game^{lah,b}(\kappa,m,n)$ 在多项式时间内以不可忽略的概率优势成功输出“1”，则挑战者 F 可以利用攻击者 A 的攻击能力在多项式时间内以不可忽略概率求解出 DL 问题。假设挑战者 F 面对一个 DL 问题实例 $(g,g_1=g^x)$，挑战者 F 将在攻击游戏中与攻击者 A 交互过程中巧妙地嵌入 DL 问题，挑战者 F 需要模拟预言机算法 O={*createg*roup, *addmember*, *handshake*, *re-*

voke}，其中，也包含随机预言机功能的散列函数询问。攻击者 A 将适应性地询问上述算法预言机，预言机根据不同的请求模拟对应的算法。为了充分发挥攻击者 A 的攻击能力，挑战者 F 在模拟上述预言机行为时返回的值和真正的算法产生的回答是不可区分的。

经过上述预言机的训练之后，攻击者 A 要成功完成攻击游戏 $Game^{lah,b}(\kappa,m,n)$，则需要能区分出挑战者 F 模拟的握手协议副本(transcript)是 handshake($id^*,\tilde{G}_0^*,init$)还是 handshake ($id^*,\tilde{G}_1^*,init$)。在此假设当 $b=1$ 时，handshake ($id^*,\tilde{G}_1^*,init$) 是按照协议步骤真实执行的，而当 $b=0$ 时，handshake ($id^*,\tilde{G}_0^*,init$)执行副本是由一个模拟器 SIM 随机生成。

挑战者 F 预先模拟 MLAH-AKE 环境，创建 m 个用户 $U_1,\cdots,U_m$ 及其对应的伪名 $ID=\{id_1,\cdots,id_m\}$；建立 n 个群组织 $\tilde{G}=\{G_1,\cdots,G_n\}$，并且模拟每个具有伪名 id_i 的用户 U_i 加入组织 G_j，其中，$(i,j)\in[1,m]\times[1,n]$。值得注意的是，在模拟成员加入（addmember）算法时，成员证书的生成来源于 Schnorr 签名，证明的思路将借鉴其中的分叉归约引理[19]。挑战者 F 模拟 addmember 算法，随机选择 $h_i,t_i\leftarrow_R Z_q^*$ 以及 $id_i\in\{0,1\}^\kappa$，然后计算 $w_i=g^{t_i}(g_1)^{-h_i}$ 和 $H_1(id_i,w_i)=h_i$，作为询问加入组织 $G\in\tilde{G}_1$ 的返回值。如果攻击者 A 想要攻破 $Game^{lah,b}(\kappa,m,n)$，则他必须能够以不可忽略的概率优势 ε 辨别出一个握手实例是由模拟器 SIM 产生的还是由挑战者 F 按照真实协议步骤模拟产生的。因为攻击者 A 至少有 $\frac{1}{2}$ 的概率可以猜对，攻击者 A 能猜对的概率为 $\frac{1}{2}+\varepsilon$。模拟器 SIM 随机产生的协议副本和一个真正的协议副本是不可区分的。根据握手副本 $\{(id_A,S_A),(id_B,S_B,S_B'),(S_A')\}$，再结合 IHME 方案的索引隐藏性[2],攻击者 A 必须能辨别出由 SIM 产生的随机编码译码的结果 $c_{Bi}'=iDecode(SIM(params),y_{Ai})$ 以及由挑战者 F 模拟的用户 B 实际解码计算的值 $c_{Bi}'\leftarrow iDecode(S_B',y_{Ai})$，并使 $c_{Bi}'=c_{Bj}=H_2(y_{Bj}\|g^{t_{Aj}t_{Bj}}\|sid_B\|resp)$。但是，这只能依赖于攻击者 A 在参与对应的认证密钥协商协议时能够构造出正确的关于组织证书信息的编码，并使挑战者 F 收到该编码后正确地解码并计算出 $r_{Bj}=(w_{Aj}'y_{Bj}^{H_1(id_A\|w_{Aj}')})^{t_{Bj}}=(g^{t_{Aj}})^{t_{Bj}}$。这意味着攻击者 A 在没有获得秘密的群证书 $cred_A$ 的前提下需伪造出有效的证书信息。因为群证书基于离散对数问题(DLP)由 Schnorr 签名构造的，根据分叉归约引理[19]，成功的伪造者 A 可以被挑战者 F 归约为一个提取器以不可忽略的概率获得 x 解决 DL 问题。综上所述，基于 DL 假设，可以推导出这与攻击者能成功攻破游戏 $Game^{lah,b}(\kappa,m,n)$ 的假设是相互矛盾的。定理 1 得证。

定理 2 基于DL假设,MLAH-AKE协议在随机预言机模型下证明是认证密钥交换安全(AKE-security)。

证明 AKE-security 由攻击者 A 和挑战者 F 之间的攻击游戏 $Game^{ake,b}(\kappa,m,n)$ 来形式化定义，其中，包含会话新鲜性(session freshness)和完善的前向安全性(PFS, perfect forward secrecy)2 个性质。攻击者的目标是区分一个真实的会话密钥和随机产生的密钥，攻击者可以向挑战者询问 MLAH-AKE 方案对应的预言机 O 算法的信息和执行结果，从而获得很好的训练。

如果攻击者 A 参与的攻击游戏 $Game^{ake,b}(\kappa,m,n)$ 在多项式时间内以不可忽略的概率优势成功输出“1”，则挑战者 F 可以利用攻击者 A 的攻击能力在多项式时间内以不可忽略概率求解出 DL 问题。参照文献[2]中的证明结论，采用简单的混合技术(hybrid argument)，可关联的组织隐藏安全性可以推导出完善前向安全性。直观上理解，这是因为在组织隐藏安全游戏 $Game^{lah,b}(\kappa,m,n)$ 中，需要比较由挑战者 F 模拟的真实的协议运行实例与由模拟器 SIM 产生的完全随机的执行实例。而对于认证密钥协商安全游戏 $Game^{ake,b}(\kappa,m,n)$，需要攻击者区分的是测试会话真实产生的密钥和随机产生的密钥。2 个攻击游戏的区别主要在于参数和协议的选取上。因此，可以按照类似于定理 1 的方式利用攻击者 A 作为提取器以不可忽略的概率优势解决 DL 问题。因此，基于 DL 困难性假设，攻击者 A 参与组织隐藏的认证密钥协商协议时想要辨别出这个认证实例的真实会话密钥也是不可行的。定理得证。

4.2 性能分析

这节将对本文提出的组织隐藏的认证密钥协商协议的性能进行简要分析。针对多组织环境下支持组织发现问题，现有的工作主要是文献[2]给出的基于 RSA 困难假设实现的组织隐藏密钥交换协议。

表 1　　**相关协议的性能比较**

协议	握手计算开销	握手通信开销/bit	困难性假设	组织发现	轮数
文献[3]	$4T_p$	4κ	双线性 Diffie-Hellman	单个组织	3 轮
文献[4]	$4T_e$	$4\kappa+6\lvert p\rvert$	计算 Diffie-Hellman	单个组织	4 轮
文献[2]	$2(\lvert\tilde{G}_A\rvert+\lvert\tilde{G}_B\rvert)T_e$	$2\lvert 2\kappa'+\kappa\rvert(\lvert\tilde{G}_A\rvert+\lvert\tilde{G}_B\rvert)$	RSA	组织交集非空	4 轮
本文	$(\lvert\tilde{G}_A\rvert+\lvert\tilde{G}_B\rvert)T_e$	$2\lvert q\rvert(\lvert\tilde{G}_A\rvert+\lvert\tilde{G}_B\rvert)$	DLP	d 个组织交集	3 轮

对于仅考虑用户从属于单个组织的组织隐藏密钥交换协议，即基础的两方秘密握手协议，选择效率较高的 2 个方案即文献[3,4]进行比较。因此，本节给出新型构造的 MLAH-AKE 协议与上述 3 个协议的性能比较。为了简明起见，针对组织隐藏认证密钥交换协议中存在主要开销的认证密钥交换（握手）算法分别给出计算和通信开销，其中，计算开销主要考虑模指数运算和双线性对运算，用 T_e 表示一个有限域的模指数运算的时间。用 T_p 表示椭圆曲线群上的一个双线性对运算的时间，具体性能数据如表 1 所示。

从表 1 可以看出本文提出 MLAH-AKE 握手协议的计算开销主要包含协议双方协商密钥及验证产生的模指数运算，准确地说，用户用户 A 启动执行一个握手会话 $Handshake(id_A,\tilde{G}_A,init)$ 需要估计 $\lvert\tilde{G}_A\rvert$ 个模 p 的指数运算，其中，$\lvert\tilde{G}_A\rvert$ 表示 A 所从属的组织集合个数。为了隐藏不同组织的群公钥参数的区别，基于 RSA 困难问题构造的文献[2]的方案需要增加额外的计算量来对参数进行填充。此外，即文献[2]方案的握手协议的每一个参与方在编码之前都需要增加一个模指数运算来盲化用户的群证书。而本文提出的基于 DL 问题构造的 MLAH-AKE 方案则直接对群证书的一部分进行编码，减少了在线的模指数运算，提高了一定的计算性能。在通信开销方面，MLAH-AKE 方案中的 $\lvert q\rvert$ 通常是 512 bit，而文献[2]的方案 $\lvert 2\kappa'+\kappa\rvert$ 则要大于 $\lvert q\rvert$。

另外，可以看出支持多组织交集的方案在计算和通信开销上要多于单个组织文献[3,4]的方案。这是由于在多组织环境下的认证密钥协商协议，计算开销的规模是与用户从属的组织个数呈线性关系，而索引隐藏的信息编码 s_A,s'_A 的大小也是与用户 A 从属组织的个数呈线性增长关系。而为了实现多组织交集策略的认证需求，增加的的开销是必要的。

因此，相对于能实现多组织发现问题的文献[2]方案,本文提出的新型组织隐藏的认证密钥协商协议在计算性能和通信开销上仍体现了一定的优势。

5　结束语

本文基于离散对数困难假设提出了一个新型组织隐藏的认证密钥协商协议 MLAH-AKE，允许群成员从属于多个不同组织的应用环境下使协议双方的组织集合存在交集且满足至少有 d 个组织相同时能够认证成功,同时保证交集之外组织信息的机密性。为了实现有效的追踪和撤销，方便群组织的管理，MLAH-AKE 方案保证用户多个实例的可关联性。基于 DL 困难性假设，MLAH-AKE 方案在随机预言机模型下是可证安全的，满足密钥协商协议的基本安全要求。

参考文献：

[1] JARECKI S, KIM J, TSUDIK G. Group secret handshakes or affiliation-hiding authenticated group key agreement[A]. Proceeding of CT-RSA 2007[C]. San Francisco, CA, USA, 2007.287-308.

[2] JARECKI S, KIM J, TSUDIK G. Beyond secret handshakes: affiliation-hiding authenticated key exchange[A]. Proceeding of CT-RSA 2008[C]. San Francisco, CA, USA, 2008.352-369.

[3] BALFANZ D, DURFEE G, SHANKAR N, *et al*. Secret handshakes from pairing-based key agreements[A]. Proceeding of IEEE Symposium on Security and Privacy[C]. Berkeley, California, USA,IEEE Computer Society,2003.180-196.

[4] CASTELLUCCIA C, JARECKI S, TSUDIK G. Secret handshakes from ca-oblivious encryption[A]. Proceedings of ASIACRYPT 2004[C]. Jeju Island, Korea, 2005. 293-307.

[5] ZHOU L, SUSILO W, MU Y. Three-round secret handshakes based on ElGamal and DSA[A]. Proceedings of ISPEC 2006[C]. Hangzhou,China, 2006. 332-342.

[6] VERGNAUD D. RSA-based secret handshakes[A]. Proceedings of International Workshop of Coding and Cryptography (WCC 2005)[C]. Bergen, Norway, 2005. 252-274.

[7] XU S H, YUNG M. K-anonymous secret handshakes with reusable credentials[A]. Proceedings of ACM Conference on Computer and Communications Security (CCS 2004)[C]. Washington DC, USA, 2004.158-167.

[8] JARECKI S, LIU X M. Unlinkable secret handshakes and key-private group key management schemes[A]. Proceedings of ACNS 2007[C]. Zhuhai, China, 2007. 270-287.

[9] WEN Y M, ZHANG F G, XU L L. Unlinkable secret handshakes from message recovery signature[J]. Chinese Journal of Electronics, 2010, 19,(4): 705-709.

[10] GU J, XUE Z. An improved efficient secret handshakes scheme with unlinkability[J]. IEEE Communication Letters, 2011, 15(2):259-261.

[11] ATENIESE G, BLANTON M, KIRSCH J. Secret handshakes with dynamic and fuzzy matching[A]. Proceedings of Network and Distributed System Security Symposium(NDSS 2007)[C]. San Diego, California, USA,2007.159-177.

[12] SORNIOTTI A, MOLVA R. Secret handshakes with revocation support[A]. Proceedings of ICISC 2009[C]. Seoul, Korea, 2009. 274-299.

[13] SORNIOTTI A, MOLVA R. A provably secure secret handshake with dynamic controlled matching [J]. Computers & Security, 2010,29(5): 619-627.

[14] SORNIOTTI A, MOLVA R. Federated secret handshakes with support for revocation[A]. Proceedings of ICICS 2010[C]. Barcelona,Spain, 2010. 218-234.

[15] MANULIS M, PINKAS B, POETTERING B. Privacy-preserving group discovery with linear complexity[A]. Proceedings of ACNS 2010[C]. Beijing, China ,2010.420-437.

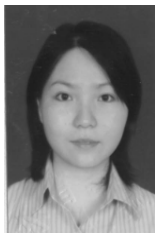
[16] BRANDS S. An Efficient off-line Electronic Cash System Based on the Representation Problem[R].Technical Report CS-R9323, CWI (Centre for Mathematics and Computer Science) Amsterdam, the Netherlands, 1993.

[17] BELLARE M, CANETTI R, KRAWCZYK H. A modular approach to the design and analysis of authentication and key exchange protocols (Extended Abstract)[A]. The ACM Symposium on Theory of Computing (STOC)[C]. San Francisco, CA, USA,1998. 419-428.

[18] SCHNORR C. Efficient identification and signatures for smart cards[A]. Proceeding of CRYPT0 1989[C]. Santa Barbara, CA, USA, 1989.239-252.

[19] POINTCHEVAL D, STERN J. Security proofs for signature schemes[A]. Proceedings of EUROCRYPT 1996[C]. Saragossa, Spain, 1996. 387-398.

作者简介：



温雅敏（1981-），女，江西赣州人，博士，广东财经大学副教授，主要研究方向为隐私保护密码学协议的设计与可证明安全。

龚征[通信作者]（1981-），男，江西南昌人，博士，华南师范大学副教授，主要研究方向为密码学与信息安全。E-mail: cis.gong@gmail.com。