多属性交集的秘密握手方案设计

温雅敏[1] 张方国[2),3)] 龚 征[4)]

[1)](广东财经大学统计与数学学院 广州 510320)

[2)](中山大学数据科学与计算机学院 广州 510006)

[3)](广东省信息安全技术重点实验室 广州 510006)

[4)](华南师范大学计算机学院 广州 510631)

摘 要 秘密握手方案是保证组织信息隐藏的双向匿名认证协议,仅允许同一个组织的合法群成员实现匿名地双向认证且协商出秘密的会话密钥,组织外部的用户或敌手无法识别或成功执行一次秘密握手协议. Ateniese 等人 2007 年首次建立了秘密握手的模糊匹配模型,从单个属性推广到允许用户持有多个属性的认证策略.然而,大多数已提出的多属性匹配的秘密握手方案所需的计算或通信性能和属性个数呈平方数量级关系,并不适用于属性个数递增和资源受限的应用环境.因此,如何设计并线性优化多个属性认证策略的秘密握手方案且使之运用于资源受限的移动社交网络等环境中仍值得进一步研究.为了更有效地实现多属性交集的双向认证策略,本文借鉴授权秘密集合交集协议的思路,基于 RSA 签名构造多个属性证书,可实现通过聚合的方法线性优化秘密握手协议中参与方的计算和通信开销.把授权秘密集合交集协议和秘密握手协议融合到一个三轮交互协议中,不需要单独执行秘密集合交集协议,使得方案的性能得到了进一步优化.基于 RSA 问题的困难性假设,给出了新型秘密握手方案在随机预言机模型下的安全分析.通过与相关方案的比较,文中给出各方案所需的计算时间开销及性能变化趋势图.最后,理论和实验数据分析显示本文设计的方案在性能优化和多属性匹配的认证功能上达到了平衡.

关键词 组织隐藏;秘密握手;模糊匹配;多属性交集;授权秘密集合交集

中图法分类号 TP309 **DOI 号** 10.11897/SP.J.1016.2020.01433

The Design of Multi-Attribute Intersection Secret Handshake Scheme

WEN Ya-Min[1)] ZHANG Fang-Guo[2),3)] GONG Zheng[4)]

[1)](*School of Statistics and Mathematics, Guangdong University of Finance and Economics, Guangzhou* 510320)

[2)](*School of Data and Computer Science, Sun Yat-sen University, Guangzhou* 510006)

[3)](*Guangdong Key Laboratory of Information Security, Guangzhou* 510006)

[4)](*School of Computer Science, South China Normal University, Guangzhou* 510631)

Abstract Based on anonymous credentials, unidirectional anonymous authentication protocols enable the verifier only to identify the prover to be a legitimate member certified by an organization. For applications with higher levels of privacy, it is also desirable to protect the affiliations of users. A secret handshake scheme is an anonymous bi-directional authentication protocol which achieves affiliation-hiding and user privacy protection. It allows legitimate members of the same organization to achieve private mutual authentication and negotiate a session key, while ensuring that the affiliation is not disclosed to external users and attackers. Ateniese et al. first established the fuzzy matching model for secret handshakes in 2007. The fuzzy matching model provides an

收稿日期:2019-03-20;在线发布日期:2019-09-10.本课题得到国家自然科学基金(61672550,61572028,61300204)、国家社会科学基金(14BXW031)、国家重点研发计划(2017YFB0802503)、国家密码管理局"十三五"国家密码发展基金密码理论课题(MMJJ20180206)、广东省基础与应用基础研究基金项目(2019A1515011797,2016A030310027,2018A030313954,2014A030313609)、广州市科技计划项目(201802010044)、国家留学基金委项目(201808440097)和广东财经大学大数据审计团队项目资助.**温雅敏**(通信作者),博士,副教授,主要研究方向为密码学与信息安全.E-mail:wenyamin@gdufe.edu.cn.**张方国**,博士,教授,主要研究领域为密码学与信息安全.**龚 征**,博士,教授,主要研究领域为信息系统安全.E-mail:cis.gong@gmail.com.

extension of secret handshakes which allows users to hold multiple attributes and achieves approximate matching. However, most of the proposed secret handshake schemes with multi-attribute matching is not very efficient as their computational or communication performance is quadratic with the number of attributes. And thus such schemes are not suitable for the resource-constrained applications with increasing number of attributes. Therefore, how to design and linearly optimize the secret handshake scheme with multi-attribute authentication policies and apply it to resource-constrained mobile social networks is still worth to further research and generalize. Inspired by Ateniese et al.'s fuzzy-matching model, we presented an authentication policy with supporting multi-attribute intersection, which enables the multiple attributes of users to be represented as the set. Specifically, on the condition that their attributes set intersection is not empty set or its cardinality is not less than a threshold value, two anonymous participants can execute a successful secret mutual authentication. The Authorized Private Set Intersection (APSI) protocol is the authorized version of PSI protocol, which demands the elements of the client to be authorized by a trusted third party and only allows the client to obtain the intersection from the server. For multiple authorizations, most of APSI protocols need more computational and communication overhead which are quadratic complexity with the number of attributes. In order to implement the authentication strategy of multi-attribute matching more effectively, we applied the idea of the APSI protocol to construct a new bi-directional secret handshake protocol supporting multi-attribute intersection matching. In particular, the new proposal enables multiple attributes certificates to be aggregated by using the RSA signature which leads to achieve linear optimization. The main advantage of our new scheme is to integrate an APSI protocol into the three-round secret handshake protocol, and thus improving the performance without the help of the extra private set intersection. Based on the difficulty assumption of the RSA problem, the security analysis of our new proposal was presented under the random oracle model. By comparing with related multi-attribute matching schemes, we demonstrated the computational overhead of the related schemes in the different phases of secret handshakes. Meanwhile, we also gave the trend diagram of the performance with the increasing number of attributes. Therefore, the theoretical and empirical tests illustrate that our new proposal in this paper achieves a balance in performance optimization and multi-attribute matching authentications.

Keywords affiliation-hiding; secret handshakes; fuzzy matching; multi-attribute intersection; authorized private set intersection

1 引 言

对于许多网络应用,例如电子商务,电子政务和社交网络,匿名认证在保护用户隐私方面起着非常重要的作用.用户希望服务提供方在认证过程中只能验证其身份的合法性,恶意的窃听者或服务提供方不能获取其他隐私信息.匿名证书(Anonymous Credentials)作为一项重要的匿名认证技术得到了广泛的关注.验证者通过匿名证书只能识别出用户是属于某个认证中心(Certificate Authority,CA)管理的合法用户,但不知道该用户到底是谁,从而保护了用户的隐私信息.虽然匿名证书在一定程度上能很好地解决隐私保护的身份认证问题,但匿名证书在单向认证过程中至少要向验证方暴露用户从属的组织信息(即公开显示证书由哪一个 CA 签发).然而,在隐私级别更高的应用中,为用户签发证书的 CA 信息也需要得到保护.尤其在两个秘密组织(如联邦调查局)成员间的双向认证和信息共享应用中,组织隐藏的安全需求显得更加重要.

秘密握手方案(Secret Handshake Scheme,SHS)正是为了解决组织隐藏的隐私保护认证问题而提出的新技术,基于双线性配对,秘密握手的概念由 Balfanz 等人[1]首次提出,当且仅当两个用户来自于

同一个组织时才能实现匿名地双向认证，并协商出秘密的会话密钥. 随后研究者们基于其他密码学工具构造了一系列方案，如计算 Diffie-Hellman 问题[2-3]、RSA 问题[4]等. 基于组织发现问题[5]，国内学者构造了组织隐藏认证密钥交换协议[6]. 但是，上述这些方案实例传送的信息中包含用户的伪名，这使得用户行为是可关联的(linkable)，即外部敌手可以识别出协议的多次执行是由同一个用户参与的. 用户使用一次性伪名(one-time pseudonym)及其证书可实现不可关联性. 但组织管理中心需要为同一个用户存储和计算多个伪名证书，这将大大增加管理中心的负担. 因此，允许用户证书的可重用同时实现不可关联性是后续研究的主要工作. 在随机预言机安全模型下，Xu 和 Yung 首次提出“k-anonymous”的不可关联方案[7]、Jarecki 和 Liu 提出运用广播加密和群密钥管理技术构造不可关联方案[8]以及通过盲化用户证书方式实现的证书可重用方案[9-11].

在 2007 年 NDSS 会议上，Ateniese 等人[12]首次建立了秘密握手的动态和模糊匹配模型，并给出了在标准模型下可证安全的实现. 基于动态匹配模型，研究者们陆续提出了一些变型的扩展方案[13-14]、动态控制匹配[15]方案等. 此外，用户主动离开组织或秘密信息被泄露的情形需要在系统中增加可撤销或追踪的功能，因此能实现撤销或追踪的秘密握手协议[16-20]也陆续被提出. 借鉴代理签名的思想，秘密握手方案扩展到实现可授权的秘密双向认证协议[21-22]. 近几年对于秘密握手方案的研究侧重于功能及实际应用扩展，例如新型设计的“k-times”认证秘密握手[23]，以及适用于移动医疗病症匹配的秘密握手协议[24]. 2018 年 ISPEC 会议上 Tian 等人[25]提出了可否认的秘密握手模型.

通过对上述参考文献的研究，现有大部分协议的设计主要采用的是以组织信息为属性的单个(Single)属性匹配的认证策略. 而在互联网上交友或在商务交易过程中存在新的认证应用需求，用户之间不局限于只认证或匹配是否来自于同一个组织，还需要进一步认证对方是否有其他深层属性与之契合. 假设某个用户是健身俱乐部的会员，为了提供更好的服务，会员属性信息可以具体细化成若干个属性，如客户职业、运动爱好、运动时间以及是否持有 VIP 卡等. 会员之间可以通过社交网络进行秘密交互来寻找更多爱好、时间等信息相匹配的会员相约一起运动或交流. 因此，为了能适应更灵活的认证需求，秘密握手的功能有必要考虑在单属性匹配的基础上推广到多个属性匹配的协议实现.

支持多属性匹配的秘密握手方案相对较少，目前主要分为两类，第一类是由 Ateniese 等人提出的基于门限体制设计的模糊匹配方案[12](Secret Handshake with Fuzzy Matching，SH-FM)，Wen 等人在多组织环境中给出不可关联模糊匹配秘密握手协议[26]以及应用扩展方案[27](Private Mutual Authentication with Fuzzy Matching，PMA-FM). 上述方案在执行握手协议之前需调用秘密集合交集(Private Set Intersection，PSI)[28]协议确定参与方是否符合多个属性的认证策略. 然而 PSI 协议作为一个两方计算协议的黑盒，在握手协议执行之前将输出双方多个属性是否符合认证策略的结果，这将使得外部敌手识别出双方是否处于匹配的状态，违反了握手协议应该达到的窃听者无法区分的安全要求. 为了解决这个问题，对于认证不匹配的情形，SH-FM 方案[12]要求用户使用随机数继续完成后续握手协议. 此外，SH-FM 方案[12]和 PMA-FM[27]方案单独执行完 PSI 协议后再执行握手协议，将增加协议双方的计算和存储开销. 第二类是基于属性加密实现表达式认证策略的握手方案，包括 Hou 等人提出的支持动态表达式匹配策略的秘密握手[29](Secret Handshakes with Dynamic Expressive Matching Policy，SH-DEM)和 Liu 等人提出的基于属性的握手[30](Attribute-Based Handshake，ABH)两个方案. 上述两个方案[29-30]核心技术是基于密文策略的属性加密算法实现一般访问结构，需公开传输指定的访问策略矩阵，存在较高的通信开销.

在基于 PSI 实现模糊匹配方案[12,26-27]的启发下，本文的主要研究思路是提高通信和计算效率的同时实现多属性匹配策略. 如何在秘密握手协议执行前不单独执行作为黑盒的 PSI 协议而在三轮交互握手中能支持多属性交集的策略是待解决的关键问题. PSI 协议[28]是一种特殊的两方安全计算协议，在不泄露两个参与方各自秘密信息集合的前提下通过交互协作计算出交集，在军事、医疗和社交网络等信息共享领域都有重要的应用，近年来得到了广泛关注. 根据底层采用技术的不同，PSI 协议主要分为三类[31]，分别是基于公钥加密机制[28,32]、基于混淆电路(Garbled Circuit)[33]以及基于不经意传输(Oblivious Transfer)构造的 PSI 协议[34]. 近三年国内外学者陆续针对提高计算、通信效率及恶意敌手模型安全的要求，在欧密、美密等著名国际信息安全会议上提出了一系列更高效安全的 PSI 协议，例如

基于双执行的抗恶意攻击的 PSI 协议[35]，基于同态加密构造的集合大小不对称的高效的 PSI 协议[36-37]，Pinkas 等人基于混淆电路和不经意可编程的伪随机函数等技术实现的计算和通信开销高效的 PSI 协议[38-39]，2019 年 CRYPTO 会议录用的基于不经意传输扩展等技术构造的 PSI 协议[40]在平衡计算和通信开销上达到最优，基于文献[12,27]的思路，最新的轻量级门限 PSI 协议仍可作为独立模块辅助实现多属性模糊匹配的秘密握手协议，可提高整体的实现性能. 虽然近年陆续提出了一些 PSI 协议性能优化构造的方案，但上述大多数 PSI 协议构造仍侧重于单向的交集计算和集合元素的隐私，没有提供对元素的授权验证功能，不能直接用来构造秘密握手方案. 标记的(labeled)的 PSI 协议[37]增加了识别元素的标记功能，但方案实现考虑的是交互双方集合元素不对称(unbalanced)的应用场景，是否能运用该技术实现元素授权标记以及构造双向对称的秘密握手协议有待进一步研究.

授权秘密集合交集(Authorized PSI，APSI)协议[32]是基于公钥密码机制构造的 PSI 协议的可授权变型，客户端的集合元素需要获得可信第三方的签名授权，符合秘密握手协议中用户属性需获得组织管理中心授权的应用. 另外，文献[31]对基于公钥密码机制构造的 PSI 协议性能分析中提到文献[32]中基于 RSA 聚集器的构造性能达到最优. 因此，本文基于 APSI 协议的构造探索实现更优化的多属性交集的秘密握手方案.

APSI 协议[32]由 De Cristofaro 等人最早提出，基于 RSA 签名、IBE 和 Schnorr 签名可实现基本的 APSI 协议，但基于 RSA 和 Schnorr 签名的基本构造在多元素集合的情形下需要平方级的通信和计算开销，基于 IBE 的 APSI 构造需要配对计算的支持，而基于 Schnorr 签名的 APSI 构造无法达到不可关联性. 因此文献[32]仅基于 RSA 签名给出了线性优化的 APSI 构造，且不会使用开销较大的配对计算，较好地平衡了性能和前向安全要求.

基于模糊匹配模型[12]和 APSI 协议[32]元素可授权性质，本文采用多属性交集匹配的认证策略，即通信双方的授权属性集合验证存在交集(或交集元素个数不少于某一个门限值)就可以成功地执行秘密握手，并且仍能保证用户的组织信息隐藏及交集之外属性的匿名性. 我们在两方交互握手执行前不需要执行一个单独的 PSI 协议以预先确定交集，在三轮握手协议中融合 APSI 协议，在授权认证的前提下计算交集的技术，基于 RSA 聚合签名实现线性优化 APSI 协议[32]的方法设计了新型有效的多属性交集的秘密握手(Multi-Attribute Intersection Secret Handshake，MAI-SH)方案.

本文第 2 节介绍 RSA 困难性假设、APSI 协议及秘密握手方案的定义和安全要求；第 3 节给出 MAI-SH 方案的具体构造；第 4 节给出 MAI-SH 方案的安全和性能分析；第 5 节是对全文的总结和展望.

2 预备知识

2.1 RSA 困难性假设

RSA 问题(RSA Problem)[41]. 输入 N,e,c，其中 $N=pq$ 是两个素数 p 和 q 的乘积，e 是满足 $\gcd(e,(p-1)(q-1))=1$ 的整数，$c=M^e(\mathrm{mod}N)\in\mathbb{Z}_N^*$，RSA 问题是输入 N,e,c 后求解出满足 $c=M^e(\mathrm{mod}N)$ 的整数 $M\in\mathbb{Z}_N^*$.

RSA 困难性假设. 在多项式时间内能求解出 RSA 困难问题的算法存在的概率是可忽略的 ε. 即对任意多项式时间算法 $\mathcal{A}$，任意多项式函数 $poly(\cdot)$ 和充分大的 L 都有

$$\Pr[\mathcal{A}(N,e,c)=M)\,|\,c=M^e\mathrm{mod}N]\leq\varepsilon\leq\frac{1}{poly(L)}.$$

2.2 授权秘密集合交集协议定义

PSI 协议[28]由系统建立(*Setup*)和交互计算(*Interaction*)两个算法组成，包含客户端(Client)和服务器端(Server)两个实体，且输入各自持有的元素集合 $C=\{c_1,\cdots,c_v\}$ 和 $S=\{s_1,\cdots,s_w\}$. 客户端通过调用 *Interaction* 算法计算获得交集 $C\cap S$. APSI 协议[32]要求客户端元素需获得可信第三方授权才能参与交互协议并获得正确的交集结果，包含 Client、Server 和可信的授权中心(CA)三个实体，由以下 3 个算法组成：

(1) 系统建立(*Setup*). 给定足够安全的参数 κ，*Setup* 算法生成系统共享的公开参数 *params*.

(2) 授权(*Authorize*). 该算法由 CA 和 Client 交互完成，Client 集合中的每个元素 c_i 获得 CA 用其私钥 *sk* 签发的授权 σ_i(签名).

(3) 交互计算(*Interaction*). APSI 协议的核心算法，由 Client 和 Server 交互完成交集计算. Client 输入信息及授权集合 $C=\{(c_1,\sigma_1),\cdots,(c_v,\sigma_v)\}$，Server 输入信息集合 $S=\{s_1,\cdots,s_w\}$，其中 v 和 w 分别代表 Client 和 Server 集合的元素个数. 最后，

Interaction 算法输出的结果是 Client 获得交集 $\{s_j \in S \mid \exists (c_i, \sigma_i) \in C, c_i = s_j \wedge Vrfy_{pk}(\sigma_i, c_i) = 1\}$，其中 pk 是 CA 对应于 sk 的公钥，而 $Vrfy$ 是 CA 签发授权中的验证算法.

APSI 协议的安全要求包括正确性、客户端隐私和服务器端隐私. 正确性要求如果 Client 持有正确授权的集合元素，*Interaction* 算法将以压倒性概率使得 Client 获得正确的交集. 客户端隐私要求 Client 集合的元素不能泄露给恶意的 Server 以及敌手. 服务器端隐私要求 Client 只能识别与 Server 集合存在交集的元素，交集之外的元素仍保证是机密的.

2.3　秘密握手方案定义与安全要求

一个秘密握手方案允许系统内包含多个独立的组织机构 $(G_1, G_2, \cdots)$，每个组织机构内部允许加入若干个合法的成员 $(U_1, U_2, \cdots)$. 秘密握手方案的核心握手协议由两个用户交互完成，两个参与方需获得同一个组织管理中心签发的证书才能成功地实现匿名双向认证，同时建立一个秘密的会话密钥. 结合基本的秘密握手[1]的定义，在此给出支持多属性交集的秘密握手方案的算法定义和需要达到的安全要求：

(1) 系统建立 ($Setup(1^\kappa)$). 给定一个安全参数 κ，执行系统初始化算法，输出的是秘密握手系统各组织和用户共享的公开参数 *params*.

(2) 创建组织 ($CreateGroup(G_i)$). 基于公开参数 *params*，系统内每一个组织的管理中心 (Group Authority，GA) 将独立生成各自的群密钥对，包括群公钥 gpk_i 和群私钥 gsk_i，从而创建一个独立的组织 G_i.

(3) 加入成员 ($AddMember(U, G_i)$). 假设一个用户 U 申请加入某一个组织 G_i，则该组织的 GA 首先查验 U 的申请材料以确认是否使其成为合法群成员，在此允许一个用户申请持有 n 个属性 (标记为 $Att_U = \{u_1, \cdots, u_n\}$) 并获得 GA 签发的属性证书 $S_U = \{\sigma_{U1}, \cdots, \sigma_{Un}\}$. 每一个属性证书 σ_{Ui} 本质上是 GA 用群私钥 gsk_i 对属性 u_i 计算的一个签名.

(4) 秘密握手 ($Handshake(A, B)$). 两个匿名用户 A 和 B 通过执行该协议识别彼此是否来自于同一个组织并且达到多属性集合交集的匹配，从而建立起一个秘密通信信道. A 与 B 输入各自的秘密属性证书信息，按照算法步骤执行协议，如果协议的交互双方 A 与 B 符合多属性交集的认证策略，则他们各自参与协议的输出结果都是“1”，并能计算出一个有效的会话密钥用于后续的通讯. 如果认证不能通过，则协议输出结果为“0”.

一个安全的 *Handshake* 协议需满足以下几个基本的安全要求：正确性、防伪造性、防侦测性和不可关联性. 由于正确性的定义相对简单故不过多讨论，在此通过攻击游戏及概率优势重点给出防伪造性、防侦测性和不可关联性的形式化安全定义. 首先需根据安全性质模拟一个敌手 $\mathcal{A}$ 和一个挑战者 $\mathcal{B}$ 之间的攻击游戏，为了实现效率优化，本文构造的安全方案考虑的敌手是半诚实 (semi-honest adversaries) 模型，即敌手忠实地遵守协议步骤，且不曲解与其输入相关的任何信息. 假设敌手 $\mathcal{A}$ 可以通过访问预言机 $O = \{O_{CG}, O_{AM}, O_{HS}, O_H, O_{H_i}\}$ 获得训练，其中预言机 O_{CG}, O_{AM}, O_{HS} 分别表示 $\mathcal{B}$ 模拟创建组织、加入成员和握手协议算法的输出返回给 $\mathcal{A}$，O_H 和 O_{H_i} 是 $\mathcal{B}$ 对询问哈希函数模拟的随机预言机.

(a) 正确性 (Correctness). 如果协议的交互双方 A 与 B 属于同一个组织且具备的属性交集元素个数不少于门限值 d，则秘密握手协议成功的概率趋近 1 成立.

(b) 防伪造性 (Impersonator Resistance，IR). 任何敌手 $\mathcal{A}$ 都不能伪造成一个符合认证策略的群成员成功执行秘密握手协议，即概率优势

$$\left|\Pr[Game_{\mathcal{A}}^{\mathrm{IR},b=0}(\kappa)=1]-\Pr[Game_{\mathcal{A}}^{\mathrm{IR},b=1}(\kappa)=1]\right|$$

标记为 $Adv_{\mathcal{A}}^{\mathrm{IR}}(\kappa) \leq \frac{1}{poly(L)}$ 是可忽略的，其中 $poly(L)$ 是对充分大 L 的任意多项式函数. IR 的攻击游戏定义为 $Game_{\mathcal{A}}^{\mathrm{IR},b}(\kappa)$，具体包含以下 4 个阶段：

① 系统建立阶段. 模拟算法 $Setup(1^\kappa)$ 生成公开参数 *params*.

② 询问阶段. $\mathcal{A}$ 对预言机提出询问 $\mathcal{A}^O(params)$，模拟预言机的算法返回对应的输出，其中询问到的用户或组织的秘密信息集合标记为 *Cor*.

③ 挑战阶段. $\mathcal{A}$ 首先确定伪造目标组织 G^* 的成员与另一个成员 (U^*, Att^*) 成功握手，其中 U^* 持有的多个属性集为 Att^*，且满足 $(G^*, U^*) \notin Cor$. 然后 $\mathcal{A}$ 发起攻击执行握手协议 $Handshake(\mathcal{A}, U^*)$，$U^*$ 的执行副本由 $\mathcal{B}$ 模拟生成. $\mathcal{A}$ 试图伪造成一个具有属性集 $Att_{\mathcal{A}}$ 的合法用户，并使 U^* 确信 $\mathcal{A} \in G^*$ 且符合多属性的交集策略 $|Att_{\mathcal{A}} \cap Att^*| \geq d$. 在此定义 $Att^* = \{u_0^*, u_1^*\}$，$\mathcal{B}$ 随机选取 $b \leftarrow_R \{0,1\}$，然后模拟持有属性 u_b^* 的合法用户 U^* 参与到握手协议 $Handshake(\mathcal{A}, U^*)$ 中.

④ 输出阶段. 最后，$\mathcal{A}$ 输出 b^*. 如果 $b^* = b$，则

$Game_{\mathcal{A}}^{\mathrm{IR},b}(\kappa)$输出为“1”，并意味着敌手$\mathcal{A}$在游戏$Game_{\mathcal{A}}^{\mathrm{IR},b}(\kappa)$中获胜. 否则，$\mathcal{A}$失败且$Game_{\mathcal{A}}^{\mathrm{IR},b}(\kappa)$输出为“0”终止该游戏.

(c) 防侦测性(Detector Resistance，DR). 监听者或敌手尝试通过监听协议通信信息或主动参与协议识别诚实用户的组织或属性等秘密信息是不可行的. 即敌手$\mathcal{A}$在攻击游戏中的概率优势$|\Pr[Game_{\mathcal{A}}^{\mathrm{DR},b=0}(\kappa)=1]-\Pr[Game_{\mathcal{A}}^{\mathrm{DR},b=1}(\kappa)=1]|$标记为$Adv_{\mathcal{A}}^{\mathrm{DR}}(\kappa)\leq\frac{1}{poly(L)}$是可忽略的，其中$poly(L)$是对充分大$L$的任意多项式函数. DR的攻击游戏定义为$Game_{\mathcal{A}}^{\mathrm{DR},b}(\kappa)$，包含以下4个阶段：

① 系统建立阶段. 模拟算法$Setup(1^{\kappa})$生成公开参数$params$.

② 询问阶段. $\mathcal{A}$对预言机提出询问$\mathcal{A}^{O}(params)$，模拟预言机的算法返回对应的输出，其中询问到的用户或组织的秘密信息集合标记为Cor.

③ 挑战阶段. $\mathcal{A}$首先确定攻击侦测的组织和用户为(G^*,U^*,Att^*)，其中U^*持有的多个属性集为Att^*，且满足$(G^*,U^*)\notin Cor$. 然后，$\mathcal{B}$执行抛掷硬币算法随机生成$b\leftarrow_R\{0,1\}$. 如果$b=1$，$\mathcal{B}$模拟真实用户U^*产生的副本与$\mathcal{A}$执行握手协议$Handshake(\mathcal{A},U^*)$. 如果$b=0$，$\mathcal{A}$与产生随机副本的随机模拟机$\mathcal{R}$执行握手协议$Handshake(\mathcal{A},\mathcal{R})$.

④ 输出阶段. $\mathcal{A}^{O}(params)\xrightarrow{\text{guess}}b^*$，敌手通过输出$b^*$作为对$b$的猜测. 如果$b^*=b$，则$\mathcal{A}$赢得防侦测游戏，并最后输出“1”. 否则$\mathcal{A}$攻击失败输出“0”并终止该游戏.

(d) 不可关联性(Unlinkability). 由同一个用户参与执行的多个$Handshake$协议实例不能被敌手识别和关联. 形式化定义不可关联性的攻击游戏$Game_{\mathcal{A}}^{\mathrm{Unlink},b}(\kappa)$，即$\mathcal{A}$在攻击游戏中的概率优势$|\Pr[Game_{\mathcal{A}}^{\mathrm{Unlink},b=0}(\kappa)=1]-\Pr[Game_{\mathcal{A}}^{\mathrm{Unlink},b=1}(\kappa)=1]|$标记为$Adv_{\mathcal{A}}^{\mathrm{Unlink}}(\kappa)\leq\frac{1}{poly(L)}$是可忽略的，其中$poly(L)$是对充分大$L$的任意多项式函数. $Game_{\mathcal{A}}^{\mathrm{Unlink},b}(\kappa)$类似地包含以下4个阶段：

① 系统建立阶段. 模拟算法$Setup(1^{\kappa})$生成公开参数$params$.

② 询问阶段. $\mathcal{A}$对预言机提出询问$\mathcal{A}^{O}(params)$，模拟预言机的算法返回对应的输出，其中询问到的用户或组织的秘密信息集合标记为Cor.

③ 挑战阶段. $\mathcal{A}$首先确定攻击的目标组织和用户为(G^*,U^*,Att^*)，其中U^*持有的多个属性集为Att^*，且满足$(G^*,U^*)\notin Cor$. 然后，$\mathcal{B}$执行抛掷硬币算法随机生成$b\leftarrow_R\{0,1\}$. 如果$b=0$，$\mathcal{B}$模拟真实用户U^*与$\mathcal{A}$运行两次$Handshake(\mathcal{A},U^*)$握手协议；如果$b=1$，$\mathcal{B}$模拟两个不同的合法用户$U^*$和$V^*$分别与$\mathcal{A}$执行$Handshake(\mathcal{A},U^*)$和$Handshake(\mathcal{A},V^*)$.

④ 输出阶段. $\mathcal{A}^{O}(params)\xrightarrow{\text{guess}}b^*$，敌手$\mathcal{A}$通过输出$b^*$作为对$b$的猜测. 如果$b^*=b$，则$\mathcal{A}$在游戏$Game_{\mathcal{A}}^{\mathrm{Unlink},b}(\kappa)$中获胜，并最后输出“1”. 否则$\mathcal{A}$攻击失败输出“0”并终止该游戏.

3 多属性交集的秘密握手方案设计

基于RSA签名实现的线性优化APSI协议[32]，本节给出一个新型的支持多属性交集的秘密握手MAI-SH方案设计. 算法描述中的群公钥/群私钥中的群区别于有限域的群，代表的是组织管理中心，方案构造包含以下4个算法：

(1) 系统建立($Setup(1^{\kappa})$). 系统输入足够安全的参数κ和κ'，其中κ'是满足安全参数κ的前提下使得RSA困难假设基于$2\kappa'$长度合数下成立的最小整数，定义哈希函数$H:\{0,1\}^*\rightarrow\{0,1\}^{\kappa}$.

(2) 创建组织($CreateGroup(G_i)$). MAI-SH系统中每个组织G_i由其各自的GA_i负责管理组织成员的验证和加入等功能，每个GA_i为组织G_i生成群公钥和群私钥对. 首先产生一个$2\kappa'$比特大小的RSA模数$N_i=p_iq_i$，其中$p_i=2p_i'+1$，$q_i=2q_i'+1$，而且p_i,q_i,p_i',q_i'都是素数. 然后随机选取一个群元素$g_i\in_R\mathbb{Z}_{N_i}^*$，使得$g_i$是$\mathbb{Z}_{N_i}^*$最大子群$QR_{N_i}$的生成元($QR_{N_i}$是$\mathrm{mod}N_i$的二次剩余群). 按照RSA算法的标准方式生成对应的指数(e_i,d_i)(即满足$d_i=e_i^{-1}\mathrm{mod}\varphi(N_i)$)，这样该组织$G_i$的群公钥为$gpk_i=(N_i,g_i,e_i)$，群私钥为$gsk_i=(p_i,q_i,d_i)$. 最后选取该组织的哈希函数$H_i:\{0,1\}^*\rightarrow\mathbb{Z}_{N_i}$.

(3) 加入成员($AddMember(U,G_U)$). 申请人U请求成为组织G_U的合法成员，G_U的管理中心GA_U审核U提交的身份及其他属性信息，验证通过后为该用户签发组织证书，GA_U按照数据库记录的命名标准对属性进行统一管理和下标的标注. 假设用户可申请由GA_U针对不同属性签发的多个属性证书，用户持有一个属性集合($Att_U=\{u_1,\cdots,u_v\}$)及其对应的属性证书列表($S_U=\{\sigma_{U1},\cdots,\sigma_{Uv}\}$)，其中$\sigma_{Ui}=h_{Ui}^{d}(\mathrm{mod}N_U)$，$h_{Ui}=H_i(u_i)$，$v$是用户$U$的属性个数.

(4)秘密握手($Handshake(A,B)$). 假定参与协议的两个实体分别标记为用户 A(发起者)与用户 B(响应者),A 和 B 通过三轮秘密握手协议确认彼此是否符合多属性交集的认证策略,参与协议过程中分别输入他们各自的秘密信息,包括组织(分别标记为 G_A 和 G_B)和属性证书集合(S_A 和 S_B). A 和 B 诚实地执行以下两方协议,并且按照组织约定的多属性交集认证策略建立会话密钥. 首先给出协议描述中涉及到的参数和符号的相关定义,如表 1 所示.

表 1　方案参数定义对应表

参数/符号	定义
$A\rightarrow B:\{\}$	A 向 B 发送消息{}内的消息
$B\rightarrow A:\{\}$	B 向 A 发送消息{}内的消息
Att_A,Att_B	A 和 B 的多个属性的集合
S_A,S_B	A 和 B 的多个属性证书的集合
a_i,h_{Ai}	A 的第 i 个属性及其哈希值
b_j,h_{Bj}	B 的第 j 个属性及其哈希值
σ_{Ai},σ_{Bj}	A 的第 i 个属性证书和 B 的第 j 个属性证书
$\leftarrow_R$	从右侧集合中均匀随机产生一个变量
θ_A,θ_B	A 和 B 的多个属性哈希值的聚合
θ_A^*,θ_B^*	A 和 B 的多个属性证书的聚合
θ_{Ai}	A 除去第 i 个属性剩余属性哈希值的聚合
θ_{Bj}	B 除去第 j 个属性剩余属性哈希值的聚合
θ_{Ai}^*	A 除去第 i 个剩余属性证书的聚合
θ_{Bj}^*	B 除去第 j 个剩余属性证书的聚合

$Handshake$ 协议包括以下 3 轮详细交互步骤:

I. $A\rightarrow B:\{X_A,Y_A,Z_A\}$

a. 用户 A 属于组织 G_A,对应的群公钥和群私钥分别为 $gpk_A=(N_A,g_A,e_A)$,$gsk_A=d_A$. 假设 A 在 G_A 中具备 v 个属性 $Att_A=\{a_1,\cdots,a_v\}$,并获得签发的属性证书集 $S_A=\{\sigma_{A1},\cdots,\sigma_{Av}\}$,其中 $\sigma_{Ai}=h_{Ai}^{d_A}(\mathrm{mod}N_A)$,$h_{Ai}=H_A(a_i)$,$i\in[1,\cdots,v]$.

b. A 首先选取一个随机数 $r_A\leftarrow_R\mathbb{Z}_{N_A}^*$,然后计算出多个属性哈希值的聚合 $\theta_A=\prod_{i=1}^{v}h_{Ai}$,多个属性证书的聚合 $\theta_A^*=\prod_{i=1}^{v}\sigma_{Ai}$. 随机选取 $\lambda_A\leftarrow_R[0,\cdots,2^{2\kappa'+\kappa}/N_A]$,$A$ 基于随机数 r_A 和 λ_A 对聚合的多属性证书分别生成盲化值 X'_A 及其隐藏组织公钥模数的扩展值 X_A,其中 $X'_A=(-1)^{\mu_A}\theta_A^*\cdot g_A^{r_A}(\mathrm{mod}N_A)$,$\mu_A\leftarrow_R\{0,1\}$,$X_A=X'_A+\lambda_A\cdot N_A$.

c. 针对具备的每个属性 $a_i(i\in[1,\cdots,v])$,A 除去 a_i 计算出剩余 $v-1$ 个属性哈希及其证书的聚合值 $\theta_{Ai}=\prod_{l=1,l\neq i}^{v}h_{Al}$,$\theta_{Ai}^*=\theta_A^*/\sigma_{Ai}$. 然后选取随机数 $r_{Ai}\leftarrow_R\mathbb{Z}_{N_A}^*$ 和 $\lambda_{Ai}\leftarrow_R[0,\cdots,2^{2\kappa'+\kappa}/N_A]$,计算出剩余多属性证书聚合后的盲化扩展值 $Y_{Ai}=(-1)^{\mu_{Ai}}\theta_{Ai}^*\cdot g_A^{r_{Ai}}(\mathrm{mod}N_A)+\lambda_{Ai}\cdot N_A$,其中 $\mu_{Ai}\leftarrow_R\{0,1\}$,随后构成集合 $Y_A=\{Y_{A1},\cdots,Y_{Av}\}$.

d. A 用群公钥 gpk_A 及随机数 μ_A,r_A,λ_A 计算 $Z_A=(-1)^{\mu_A}\cdot g_A^{e_A\cdot r_A}(\mathrm{mod}N_A)+\lambda_A\cdot N_A$ 用于双向认证后的会话密钥协商,最后 A 把 X_A,Y_A 以及 Z_A 一并发送给 B.

II. $B\rightarrow A:\{X_B,Y_B,Z_B,Y'_A,T_B\}$

a. 用户 B 属于组织 G_B,群公钥和群私钥分别为 $gpk_B=(N_B,g_B,e_B)$,$gsk_A=d_B$. 假设 B 在组织 G_B 中具备 ω 个属性 $Att_B=\{b_1,\cdots,b_\omega\}$,获得签发的属性证书集 $S_B=\{\sigma_{B1},\cdots,\sigma_{B\omega}\}$,其中 $\sigma_{Bj}=h_{Bj}^{d_B}(\mathrm{mod}N_B)$,$h_{Bj}=H_B(b_j)$,$j\in[1,\cdots,\omega]$.

b. B 首先选取一个随机数 $r_B\leftarrow_R\mathbb{Z}_{N_B}^*$,然后计算出多个属性哈希值的聚合 $\theta_B=\prod_{j=1}^{\omega}h_{Bj}$,多个属性证书的聚合 $\theta_B^*=\prod_{j=1}^{\omega}\sigma_{Bj}$. 随机选取 $\lambda_B\leftarrow_R[0,\cdots,2^{2\kappa'+\kappa}/N_B]$,$B$ 基于随机数 r_B 和 λ_B 对聚合的多属性证书分别生成盲化值 X'_B 及其隐藏组织公钥模数的扩展值 X_B,其中 $X'_B=(-1)^{\mu_B}\theta_B^*\cdot g_B^{r_B}(\mathrm{mod}N_B)$,$\mu_B\leftarrow_R\{0,1\}$,$X_B=X'_B+\lambda_B\cdot N_B$.

c. 针对每个属性 $b_j(j\in[1,\cdots,\omega])$,$B$ 除去 b_j 计算出剩余 $\omega-1$ 个属性哈希及其证书的聚合值,$\theta_{Bj}=\prod_{l=1,l\neq j}^{\omega}h_{Bl}$,$\theta_{Bj}^*=\theta_B^*/\sigma_{Bj}$. 然后随机选取 $r_{Bj}\leftarrow_R\mathbb{Z}_{N_B}^*$ 和 $\lambda_{Bj}\leftarrow_R[0,\cdots,2^{2\kappa'+\kappa}/N_B]$,计算出剩余多属性证书聚合后的盲化扩展值 $Y_{Bj}=(-1)^{\mu_{Bj}}\theta_{Bj}^*\cdot g_B^{r_{Bj}}(\mathrm{mod}N_B)+\lambda_{Bj}\cdot N_B$,其中 $\mu_{Bj}\leftarrow_R\{0,1\}$. 随后构成集合 $Y_B=\{Y_{B1},\cdots,Y_{B\omega}\}$.

d. B 用群公钥 gpk_B 及随机数 μ_B,r_B,λ_B 计算 $Z_B=(-1)^{\mu_B}\cdot g_B^{e_B\cdot r_B}(\mathrm{mod}N_B)+\lambda_B\cdot N_B$ 用于双向认证后的会话密钥协商.

e. B 根据接收到的 X_A 和 Y_A 生成多属性交集计算所需的匹配集合,首先针对集合 Y_A 中的每一个元素 Y_{Ai} 计算 $Y'_{Ai}=(Y_{Ai})^{2e_Br_B}(\mathrm{mod}N_B)+\lambda_B\cdot N_B$,生成一个新的集合 $Y'_A=\{Y'_{A1},\cdots,Y'_{Av}\}$.

f. B 针对每个属性 $b_j(j\in[1,\cdots,\omega])$,计算 $K_{Bj}=(X_A^{e_B}/h_{Bj})^{2r_B}\ \mathrm{mod}N_B$,然后计算哈希值 $t_{Bj}=H(K_{Bj})$ 作为第 j 个属性的匹配令牌,并组成集合 $T_B=\{t_{B1},\cdots,t_{B\omega}\}$.

g. 最后,用户 B 把 X_B,Y_B,Z_B 以及计算生成的 Y'_A,T_B 一并返回给用户 A.

III. $A\rightarrow B$:$\{Y'_B, T_A\}$

a. A 根据接收到的 Z_B,Y'_A 和 T_B 验证 B 的属性集合中是否有 d 个属性与自己的属性集合匹配,A 首先针对每个属性 $a_i(i\in[1,\cdots,v])$ 所对应的随机数以及集合 Y'_A 中的每一个元素 Y'_{Ai} 分别计算出 $t'_{Ai}=H(Y'_{Ai}\cdot Z_B^{2r_A}\cdot Z_B^{-2r_{Ai}})$,生成集合 $T'_A=\{t'_{A1},\cdots,t'_{Av}\}$.

b. 然后 A 将对 $T'_A=\{t'_{A1},\cdots,t'_{Av}\}$ 和 $T_B=\{t_{B1},\cdots,t_{B\omega}\}$ 进行交集计算 $Set_A=T'_A\cap T_B$. 认证策略要求 Set_A 不为空集并且元素个数不少于门限值 d,A 将通过验证 Set_A 的元素个数 $I_A=|Set_A|$ 来确认 B 是否符合认证策略,如果认证成功,协议输出为"1",协商出会话密钥 Key_A 等于 $H(Z_B^{2r_A}\|\theta_{Ak_1}^{2r_B}\cdot g_A^{2e_Ar_Ar_B}\|\cdots\|\theta_{Ak_{I_A}}^{2r_B}\cdot g_A^{2e_Ar_Ar_B})$,其中 $k_l(l=1,\cdots,I_A)$ 对应于 A 在交集中元素的属性下标.

c. 为了让 B 对 A 的属性信息进行认证确认,A 首先针对集合 Y_B 中的每一个元素 Y_{Bj} 计算 $Y'_{Bj}=(Y_{Bj})^{2e_Ar_A}(\mathrm{mod}N_A)+\lambda_A\cdot N_A$,生成新的集合 $Y'_B=\{Y'_{B1},\cdots,Y'_{B\omega}\}$ 用于 B 的匹配计算.

d. A 针对每个属性 $a_i(i\in[1,\cdots,v])$,计算 $K_{Ai}=(X_B^{e_A}/h_{Ai})^{2r_A}\mathrm{mod}N_A$,然后计算哈希值 $t_{Ai}=H(K_{Ai})$ 作为第 i 个属性的匹配令牌,并生成 $T_A=\{t_{A1},\cdots,t_{Av}\}$,最后将 Y'_B 和 T_A 发送给 B.

e. 用户 B 根据接收到的 Z_A,Y'_B 和 T_A 验证 A 的属性集合中是否有 d 个属性与自己的属性集合匹配,B 首先针对每个属性 $b_j(j\in[1,\cdots,\omega])$ 以及集合 Y'_B 中的每一个元素 Y'_{Bj} 分别计算出 $t'_{Bj}=H(Y'_{Bj}\cdot Z_A^{2r_B}\cdot Z_A^{-2r_{Bj}})$,生成集合 $T'_B=\{t'_{B1},\cdots,t'_{B\omega}\}$.

f. 然后 B 对 $T'_B=\{t'_{B1},\cdots,t'_{B\omega}\}$ 和 $T_A=\{t_{A1},\cdots,t_{Av}\}$ 计算交集 $Set_B=T'_B\cap T_A$. B 验证 $I_B=|Set_B|$ 不少于 d 确认用户 A 是否符合认证策略,如果认证成功,协议输出为"1",协商出会话密钥 $Key_B=H(Z_A^{2r_B}\|\theta_{Bk_1}^{2r_A}\cdot g_B^{2e_Br_Br_A}\|\cdots\|\theta_{Bk_{I_B}}^{2r_A}\cdot g_B^{2e_Br_Br_A})$,其中 $k_l(l=1,\cdots,I_B)$ 对应于 B 在交集中元素的属性下标,否则认证不成功,协议输出为"0".

简明起见,本节进一步给出 *Handshake* 协议核心算法的流程示意图,如图 1 所示.

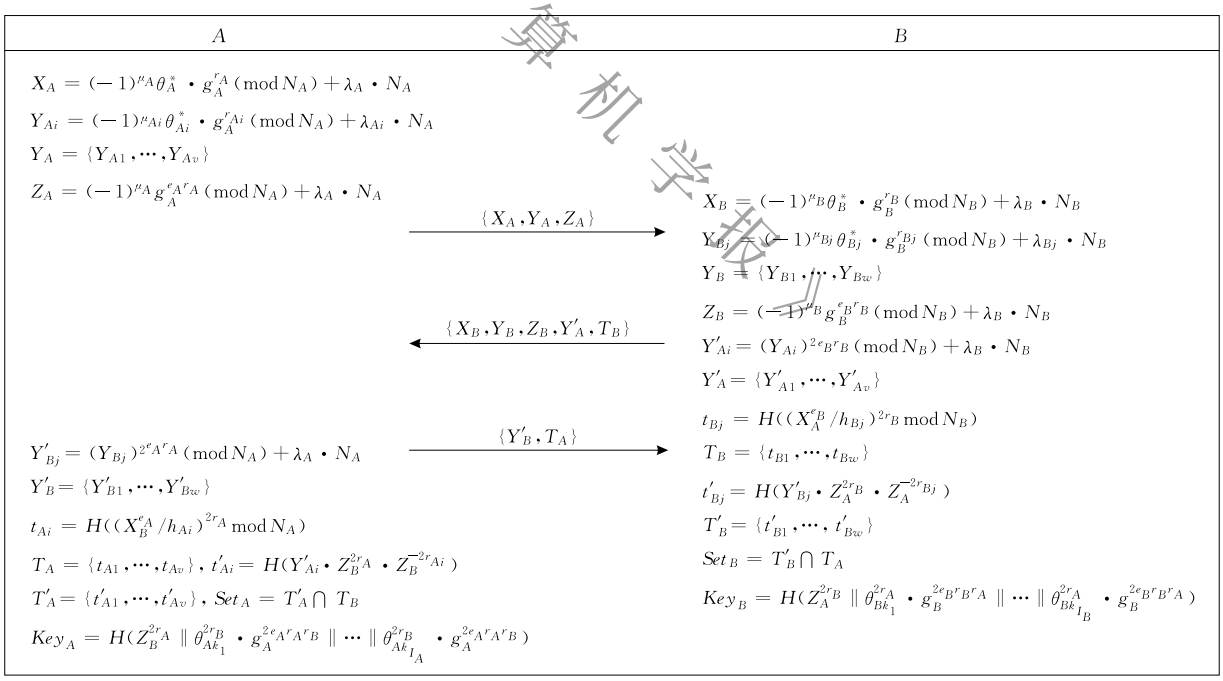

图 1 秘密握手协议流程示意图

正确性分析(Correctness). 如果 A 和 B 从属的组织相同并且具备的属性集合交集的元素个数不少于 d,则 A 和 B 可以各自计算出正确的会话密钥用于后续的信息传输,同时不能达到匹配即交集以外的属性信息仍然是保密的且不会被双方所识别. 注意到,当 A 在交互协议第二轮接收到信息后,将进行属性交集的匹配计算,在这个交集计算过程中同时会对 B 是否和 A 来自于同一个组织进行验证. 因为只有当 $gpk_A=(N_A,g_A,e_A)=gpk_B=(N_B,g_B,e_B)$,$H_A=H_B$ 时才能正确计算出交集元素,即 B 和 A 同属于一个组织并且有 d 个属性相同. 例如当属性 $a_i=b_j$ 时,则 $t'_{Ai}=t_{Bj}$,可以由以下等式验证协议的正确性.

$$t'_{Ai}=H(Y'_{Ai}\cdot Z_B^{2r_A}\cdot Z_B^{-2r_{Ai}})$$

$$=H((Y_{Ai})^{2e_Br_B}\cdot Z_B^{2r_A}\cdot Z_B^{-2r_{Ai}})$$
$$=H((\theta_{Ai}^{*}\cdot g_A^{r_{Ai}})^{2e_Br_B}\cdot Z_B^{2r_A}\cdot Z_B^{-2r_{Ai}})$$
$$=H((\theta_{Ai})^{2r_B}\cdot g_A^{2r_{Ai}e_Br_B}\cdot g_B^{2e_Br_Br_A}\cdot g_B^{-2r_{Ai}e_Br_B})$$
$$=H((\theta_{Ai})^{2r_B}\cdot g_B^{2e_Br_Br_A}),$$
$$t_{Bj}=H(K_{Bj})=H((X_A^{e_B}/h_{Bj})^{2r_B})$$
$$=H\left(\left(\prod_{i=1}^{v}H_A^2(a_i)\cdot g_A^{2r_Ae_B}/H_B^2(b_j)\right)^{r_B}\right)$$
$$=H(\theta_{Ai}^{2r_B}\cdot g_A^{2e_Br_Ar_B}).$$

类似地，B 计算出 $t'_{Bj}(j\in[1,\cdots,\omega])$，并和接收到的集合 $T_A=\{t_{A1},\cdots,t_{Av}\}$ 计算交集，当 $gpk_A=gpk_B$，且属性匹配($b_j=a_i$)时，则 $t'_{Bj}=t_{Ai}$. 因此通过匹配 $t'_{Bj}=t_{Ai}$，B 可以计算出密钥 Key_B，只要 A 和 B 来自于同一个组织且符合至少 d 个属性匹配时就能保证 $Key_A=Key_B$，进而保证协议双方能认证成功.

4　安全与性能分析

4.1　安全分析

秘密握手方案的安全要求包括正确性、防伪造性、防侦测性和不可关联性，在上一节已经证明协议的正确性，本节在此分别简要证明在随机预言机模型及半诚实敌手模型下 MAI-SH 方案满足防伪造性、防侦测性和不可关联性的安全性质.

定理 1.　在随机预言机模型下，MAI-SH 基于 RSA 困难性假设证明可以达到防伪造性.

证明. MAI-SH 协议的防伪造性通过一个敌手 $\mathcal{A}$ 和一个挑战者 $\mathcal{B}$ 之间实施的攻击游戏 $Game_{\mathcal{A}}^{\mathrm{IR},b}(\kappa)$ 定义，$\mathcal{A}$ 的目标是伪造一个合法的群成员和 $\mathcal{B}$ 模拟的群成员执行一次成功的秘密握手协议，使得 $Game_{\mathcal{A}}^{\mathrm{IR},b}(\kappa)$ 以不可忽略的概率优势输出“1”. 正如 2.3 节对攻击游戏的定义，在随机预言机模型下证明 MAI-SH 达到 IR 的安全性包含以下 4 个阶段：

① 系统建立阶段. $\mathcal{B}$ 执行 $Setup(1^{\kappa})$ 生成 MAI-SH 系统共享的参数和哈希函数.

② 询问阶段. 敌手 $\mathcal{A}$ 选择消息向挑战者 $\mathcal{B}$ 询问多次 MAI-SH 系统中各个算法的输出结果 $\mathcal{A}^{O}(params)$，挑战者 $\mathcal{B}$ 模拟 MAI-SH 环境执行对应算法的步骤，创建 m 个组织 $\widetilde{G}=\{G_1,\cdots,G_m\}$，$\widetilde{m}$ 个用户 $U_1,\cdots,U_{\widetilde{m}}$ 及其对应的属性集 $Att_{U_j}=\{u_{j1},\cdots,u_{jv}\}$；并且模拟每个具有属性集 Att_{U_j} 的用户 U_j 加入组织 G_i，其中 $(i,j)\in[1,m]\times[1,\widetilde{m}]$，$\mathcal{B}$ 根据敌手的询问返回对应的输出结果并存储在集合 Cor 中. 例如当模拟 $CreateGroup(G_i)$ 的预言机 O_{CG} 算法时，$\mathcal{B}$ 按照算法为每个对 O_{CG} 的询问($l\in[1,q_{CG}(\kappa)\backslash l^{*}]$)正常输出对应组织的参数值 $(N_l,p_l,q_l,g_l,e_l,d_l,H_l)$. 当敌手对加入成员算法预言机 O_{AM} 进行询问时，挑战者 $\mathcal{B}$ 使用各个组织的密钥按照 $AddMember(U,G_U)$ 步骤为群成员签发属性证书 $(S_U=\{\sigma_{U1},\cdots,\sigma_{Uv}\})$. 对于属性的哈希函数计算的询问 O_{H_l}，$\mathcal{B}$ 模拟生成对应的哈希值返回，对于第 $l\in[1,q_H(\kappa)\backslash l^{*}]$ 次询问，$\mathcal{B}$ 随机选取 $\sigma_{u_l}\leftarrow_R\mathbb{Z}_N^{*}$，然后返回 $h_{U_l}=H_l(u_l)=\sigma_{u_l}^{e_l}$. 同时把询问返回的值存入 $HList$ 哈希列表. 对于生成会话密钥的哈希函数询问 O_H，$\mathcal{B}$ 随机生成 κ 位比特串返回. 针对挑战阶段敌手关于 H 的询问，定义 $HQuery$ 是 $\mathcal{A}$ 询问 $H(K^{*})$ 以计算匹配令牌的事件，其中 K^{*} 需与 $(X_{\mathcal{A}}^{e}/H^{*}(u_b^{*}))^{2r^{*}}\bmod N$ 匹配以成功完成协议. 此外，$\mathcal{B}$ 可模拟合法的群成员身份完成 $Handshake(\mathcal{A},\mathcal{B})$ 协议，并生成对 O_{HS} 询问的输出副本. 上述预言机的输出符合均匀分布，$\mathcal{B}$ 模拟预言机的反馈结果和实际系统算法生成的返回值对于敌手而言是不可识别的.

③ 挑战阶段. 敌手 $\mathcal{A}$ 的目标是伪造成组织 G^{*} 的成员，并与另一个成员 (U^{*},Att^{*}) 完成一次成功的握手协议. 挑战者 $\mathcal{B}$ 的目标是解决一个 RSA 问题(即给定 $N,e,c=M^{e}$，求出 M)，在攻击游戏中 $\mathcal{B}$ 需要利用 $\mathcal{A}$ 的攻击能力来解决他面临的 RSA 问题. l^{*} 标记的是 $\mathcal{B}$ 针对目标组织 G^{*} 的算法模拟，在询问阶段要求 $(G^{*},U^{*},Att^{*})\notin Cor$. 对于 G^{*} 的组织创建，$\mathcal{B}$ 输出 (N,e,g) 作为 G^{*} 的公钥，并选取对应 N 的哈希函数 H^{*}. 对于加入成员算法的模拟，$\mathcal{B}$ 生成随机数集合作为 U^{*} 的属性证书 $S_{U^{*}}=\{\sigma_{U_1^{*}},\cdots,\sigma_{U_v^{*}}\}$，对于任意属性值 u_i^{*} 的哈希值，$\mathcal{B}$ 模拟输出 $H^{*}(u_i^{*})=(\sigma_{U_i^{*}})^{e}$，对应的哈希值存储在 $HList$ 列表中. Att^{*} 集合内关于属性哈希值的询问 $O_{H^{*}}(u_i^{*})$，则返回 $H^{*}(u_i^{*})=c^{\cdot}(\gamma_i)^{e}(\gamma_i\in_R\mathbb{Z}_N^{*})$，其中 $u_i^{*}(i=1,\cdots,v)\in Att^{*}$. 如果已知 $(H^{*}(u_i^{*}))^{d}$，$\mathcal{B}$ 可以从中提取出 $c^{d}=(H^{*}(u_i^{*}))^{d}/\gamma_i=M$.

敌手 $\mathcal{A}$ 在询问阶段向 $\mathcal{B}$ 多次询问 O 预言机获得了足够信息和训练后，将正式向 $\mathcal{B}$ 发起挑战攻击 MAI-SH 系统的防伪造性. 敌手 $\mathcal{A}$ 伪装成一个群成员(具备属性 $Att_{\mathcal{A}}$)与挑战者 $\mathcal{B}$ 模拟的用户 U^{*} 执行 $Handshake(\mathcal{A},U^{*})$ 协议($|Att_{\mathcal{A}}\cap Att^{*}|\geq d$). 在此定义 $Att^{*}=\{u_0^{*},u_1^{*}\}(d=1)$ 中，$\mathcal{B}$ 随机生成 $b\leftarrow_R\{0,1\}$，然后嵌入 RSA 问题构造关于 u_b^{*} 符合算法步骤的数据流. $\mathcal{A}$ 首先需伪造与属性证书相关的消息副

本 $X_{\mathcal{A}}$,$Y_{\mathcal{A}}=\{y_0^*,y_1^*\}$,$Z_{\mathcal{A}}$ 并传送给 $\mathcal{B}$. 然后 $\mathcal{B}$ 按照算法步骤模拟生成 X^*,Y^*,Z^*,$Y'_{\mathcal{A}}$ 以及 T^*,其中 $Z^*=g^{(1+e\alpha)}=g^{e(d+\alpha)}(\alpha\leftarrow_R\mathbb{Z}_{N/4})$,$Y'_{\mathcal{A}}=(y_b^*)^{(1+e\alpha)}$. $\mathcal{A}$ 在接收到 Z^* 和 $Y'_{\mathcal{A}}$ 后结合自己产生的随机数 $Z_{\mathcal{A}}$ 生成 K^*,并向预言机发出哈希询问. 敌手 $\mathcal{A}$ 要成功执行握手协议需要 $HQuery$ 事件发生,其中 $r^*=d+\alpha$,即 $\mathcal{A}$ 所询问的 K^* 等于 $((X_{\mathcal{A}})^e/H^*(u_b^*))^{2(d+\alpha)}$. 由于已知 $X_{\mathcal{A}}$,$H^*(u_b^*)$,e 和 α,$\mathcal{B}$ 可以计算出 $(H^*(u_b^*))^d$,进而可以帮助 $\mathcal{B}$ 计算出 $c^d=(H^*(u_b^*))^d/\gamma_b=M$.

④输出阶段. $\mathcal{A}$ 输出 b^* 作为对 b 的猜测,如果正确输出 $b^*=b$,$Handshake(\mathcal{A},\mathcal{B})$ 能成功输出"1",则 $\mathcal{A}$ 能以不可忽略的概率优势在 $Game_{\mathcal{A}}^{\mathrm{IR},b}(\kappa)$ 游戏中获胜. 否则,$\mathcal{A}$ 在 $Game_{\mathcal{A}}^{\mathrm{IR},b}(\kappa)$ 游戏中输出"0"说明攻击失败.

参照文献[5,32]的安全分析,如果 $\mathcal{A}$ 要以不可忽略的概率优势赢得游戏,所需的前提是发生 $HQuery$ 询问事件. 根据协议描述和安全模型中的敌手和挑战者的模拟算法,$HQuery$ 询问事件发生的概率是可忽略的 $Nq_H/2^{\kappa}$,挑战者嵌入 RSA 问题模拟目标组织和成员失败的概率是可忽略的,即挑战者 $\mathcal{B}$ 在挑战阶段嵌入 RSA 问题模拟与敌手交互的副本和真实副本是不可区分的. 对于用户所持属性集合个数 $n>2$ 和交集个数 $d>1$ 的情形,敌手在 m 个组织中探测多属性交集攻击的难度更大,敌手的优势更弱. 因此,本文参照文献[32]仅考虑用户属性集合个数为 2,交集个数为 1 的安全模型分析敌手在攻击优势更强的情况下成功的概率也是可忽略的. 假设求解出 RSA 困难问题的概率为 ε,$\mathcal{B}$ 能至少以 $\varepsilon/4m$ 的概率值[5]从与 $\mathcal{A}$ 的交互协议副本中抽取出相关信息,并利用 $\mathcal{A}$ 的攻击能力求解出 RSA 问题,即攻破 RSA 困难问题求解出 M. 而由于多项式时间内 RSA 问题仍然是困难的假设前提,可反证敌手 $\mathcal{A}$ 伪造成一个合法群成员执行一次成功的秘密握手协议并成功赢得 $Game_{\mathcal{A}}^{\mathrm{IR},b}(\kappa)$ 游戏的概率优势是可忽略的. 因此,MAI-SH 协议基于 RSA 困难性假设可以达到防伪造性. 证毕.

定理 2. 在随机预言机模型下,MAI-SH 协议基于 RSA 困难性假设证明达到防侦测性和不可关联性.

证明. 对于防侦测性的安全证明,定义敌手 $\mathcal{A}$ 和一个挑战者 $\mathcal{B}$ 之间实施一个攻击游戏 $Game_{\mathcal{A}}^{\mathrm{DR},b}(\kappa)$,包含系统初始化、询问、挑战和输出 4 个阶段,其中初始化与询问计算和定理 1 的描述类似,敌手 $\mathcal{A}$ 可以自适应地选择消息执行对预言机 $O=\{O_{CG},O_{AM},O_{HS},O_H,O_{H_i}\}$ 的多次询问,$\mathcal{B}$ 按照 MAI-SH 系统的算法步骤生成系统参数并返回对应算法的正确应答,简明起见在此不再赘述,主要给出随机预言机模型下的归约思路. $\mathcal{A}$ 经过对预言机的多次询问获得足够的训练后,向 $\mathcal{B}$ 发起攻击挑战,目标是通过与 $\mathcal{B}$ 的交互游戏中能以不可忽略的概率优势区分 $\mathcal{B}$ 的消息副本是真实用户产生的还是随机产生的. $\mathcal{B}$ 在挑战阶段把待解决的 RSA 问题实例嵌入在消息副本中,通过与 $\mathcal{A}$ 的交互并利用其攻击能力提取出 RSA 问题的答案.

在关键的攻击挑战阶段,假定一个随机数产生算法 $\mathcal{R}$ 作为模拟器参与 $Handshake$ 协议仿真输出一个参与方的返回值. 然后挑战者 $\mathcal{B}$ 执行抛硬币算法随机选取 $b\leftarrow_R\{0,1\}$,如果 $b=0$,由模拟器 $\mathcal{R}$ 与 $\mathcal{A}$ 执行握手协议 $Handshake(\mathcal{A},\mathcal{R})$,产生的协议副本是随机产生的数据序列;如果 $b=1$,$\mathcal{B}$ 将按照定理 1 中模拟的方法嵌入 RSA 问题构造某一个具有对应属性值 u_b^* 的合法用户 U^* 参与协议 $Handshake(\mathcal{A},U^*)$ 产生数据输出(如 $\{X^*,Y^*,Z^*,Y'_{\mathcal{A}},T^*\}$),模拟的目标组织和成员秘密信息不能被 $\mathcal{A}$ 询问 $(G^*,U^*)\notin Cor$.

攻击游戏 $Game_{\mathcal{A}}^{\mathrm{DR},b}(\kappa)$ 的最后输出阶段则要求敌手 $\mathcal{A}$ 输出对 b 的猜测 b^*. 如果 $b^*=b$,则认为 $\mathcal{A}$ 在 $Game_{\mathcal{A}}^{\mathrm{DR},b}(\kappa)$ 游戏中获得成功,否则攻击失败.

$\mathcal{A}$ 成功猜对的概率至少是 $\frac{1}{2}$,$\mathcal{A}$ 成功的概率可以表示为 $\frac{1}{2}+Adv_{\mathcal{A}}^{\mathrm{DR}}(\kappa)$,其中 $Adv_{\mathcal{A}}^{\mathrm{DR}}(\kappa)$ 代表敌手成功的概率优势. 如果 $Adv_{\mathcal{A}}^{\mathrm{DR}}(\kappa)$ 是不可忽略的,我们认为 $\mathcal{A}$ 成功攻破了系统的防侦测性. 敌手 $\mathcal{A}$ 若以不可忽略的概率优势猜出 b,前提是 $\mathcal{A}$ 能在交互过程中对传送的信息和 $\mathcal{B}$ 产生的信息进行匹配,进而辨别出所返回的是由 $\mathcal{R}$ 模拟生成的一系列随机数还是由 $\mathcal{B}$ 按真实协议步骤实际计算的返回值. 具体地,$\mathcal{A}$ 在参与秘密握手协议时能够伪造出正确的基于属性证书(签名)的盲化证明脚本,并使得 $\mathcal{B}$ 收到 $\mathcal{A}$ 发送的脚本 $X_{\mathcal{A}}$ 和 $Y_{\mathcal{A}}$ 后能正确地解析出多属性交集元素. 此外,$\mathcal{A}$ 在双向握手算法中根据 $\mathcal{B}$ 返回的脚本恢复出对应的交集元素,进而完成双向的认证功能.

参照文献[5,32]分析以及定理 1 的证明思路，挑战者$\mathcal{B}$在防侦测游戏中可运用$\mathcal{A}$的攻击能力来解决嵌入的 RSA 问题. 因此，基于多项式时间内 RSA 问题是困难的假设，敌手$\mathcal{A}$能攻破 MAI-SH 系统的防侦测性的概率优势是可忽略的.

对于不可关联性质的证明，基本思路和防侦测性类似，允许敌手多次询问$\mathcal{B}$模拟的预言机，不同的是在$\mathcal{A}$实施攻击挑战阶段，定义的攻击游戏$Game_{\mathcal{A}}^{\mathrm{Unlink},b}(\kappa)$要求$\mathcal{B}$与$\mathcal{A}$运行两个 $Handshake$ 协议实例. $\mathcal{B}$执行抛硬币算法输出 $b\leftarrow_R\{0,1\}$，如果 $b=0$，$\mathcal{B}$模拟同一个群成员 U^* 与$\mathcal{A}$执行两次握手协议 $Handshake(\mathcal{A},U^*)$；如果 $b=1$，$\mathcal{B}$则模拟不同的群成员 U^*和 V^*分别与$\mathcal{A}$执行 $Handshake(\mathcal{A},U^*)$和$Handshake(\mathcal{A},V^*)$. 在攻击游戏$Game_{\mathcal{A}}^{\mathrm{Unlink},b}(\kappa)$的最后阶段让$\mathcal{A}$输出对 b 的猜测 b^*. 如果猜对了，则$\mathcal{A}$赢得游戏，并使得 $Game_{\mathcal{A}}^{\mathrm{Unlink},b}(\kappa)$输出“1”，否则输出“0”. 由于 $Handshake$ 协议交互过程中产生的数据符合均匀分布，同一个成员参与每次认证协议都选用不同的随机数，从而两次认证实例是否来自于同一个成员是不可区分的. 因此，敌手能成功的概率优势

$$\left|\Pr[Game_{\mathcal{A}}^{\mathrm{Unlink},b=0}(\kappa)=1]-\Pr[Game_{\mathcal{A}}^{\mathrm{Unlink},b=1}(\kappa)=1]\right|$$

是可忽略的，即$Adv_{\mathcal{A}}^{\mathrm{Unlink}}(\kappa)\leq\frac{1}{poly(L)}$，其中 $poly(L)$是对足够大 L 的多项式函数. 如果敌手以不可忽略的概率优势对同一群成员执行的两次认证协议进行关联，则挑战者$\mathcal{A}$可以采用与定理 1 类似的归约方法，把 RSA 问题实例嵌入到交互协议的副本中并从中利用$\mathcal{A}$的攻击能力解析出 RSA 问题的解答. 因此，MAI-SH 方案基于 RSA 困难性假设证明可以达到不可关联性.　　证毕.

4.2　性能分析

正如引言部分所述，支持多属性策略的秘密握手方案主要包括 Ateniese 等人提出的模糊匹配秘密握手方案(SH-FM[12])，Wen 等人在多组织环境下提出的模糊匹配的秘密双向认证(PMA-FM[27])，Hou 等人提出的支持动态表达式匹配策略的秘密握手方案(SH-DEM[29])和 Liu 等人提出的基于属性的秘密握手方案(ABH[30])这四篇代表文献，因此本节在各个算法阶段与上述 4 个方案进行分析比较给出对 MAI-SH 方案的性能分析. 对计算开销的评估，主要检测协议所需要的时间耗费较高的双线性对和模幂计算，其他选取参数、加法乘法及哈希等计算量不做考量，用“—”表示. 具体的计算开销比较如表 2 所示，其中 T_p和 T_e分别代表单个双线性对和模幂运算的时间. 经试验测试，T_p和 T_e所需时间分别估计是 5.427 ms 和 2.42 ms. 为了不暴露协议参与方持有的属性集合大小以及各个方案的统一性，在此对 MAI-SH 方案的双方所持属性个数统一为 $v=w=n$，而 d 代表的是模糊匹配门限认证策略中最少需达到的属性个数.

表 2　相关方案的计算性能比较

方案	系统建立	创建组织	加入成员	秘密握手
SH-FM[12]	$(2n+3)T_e$	—	$n(n+6)T_e$	$(2d+1)T_p+(n(n+4))T_e+(d+2)T_e$
PMA-FM[27]	—	T_e	$n(n+6)T_e$	$(2d+2)T_p+(n(n+8))T_e+(d+2)T_e$
SH-DEM[29]	—	T_p+2T_e	$(2n+3)T_e$	$(4n+3)T_p+(12n+4)T_e$
ABH[30]	T_p+T_e	—	$(4n+3)T_e$	$(3n+2)T_p+(6n+1)T_e$
MAI-SH	—	T_e	T_e	$(6n+5)T_e$

由于 SH-FM 方案[12]的构造来源于基于模糊身份加密的方法，每一个声称的组织本质上是通过标识名称的方法来区分的，因此在表 2 的系统建立阶段 SH-FM 方案[12]需要$(2n+3)$模幂计算的开销，而创建组织阶段不需要生成独立的群密钥对，只需要保存系统初始化时产生的秘密的$(n+2)$个模幂值作为签发属性证书的私钥，其中的 n 代表用户持有的属性个数也是标识组织名称中的比特长度. ABH 方案[30]的系统构造类似于 SH-FM 方案[12]，系统中的组织并不是独立管理的，而是共享同一个组织管理中心生成的群密钥对. PMA-FM[27]，SH-DEM[29]和 MAI-SH 方案构造则考虑了多个独立组织的系统环境，在创建组织算法中需要建立独立的密钥对，表 2 数据显示 PMA-FM[27]和 MAI-SH 方案在创建独立组织算法中所需计算量最优.

对于加入成员算法，SH-FM[12]和 PMA-FM[27]方案基于模糊身份加密技术实现在计算开销上需要$O(n^2)$的模幂运算，SH-DEM[29]和 ABH[30]方案需要$O(n)$的模幂运算，而 MAI-SH 方案只需要一个模幂运算. 在交互式的秘密握手协议中，由于协议双方计算的对称性，我们给出的是其中一个参与方所需的计算量. 从表 2 的分析结果显示，SH-FM[12]和

PMA-FM[27]方案仍然需要 $O(n^2)$的模幂运算以及 $O(d)$的双线性对运算，SH-DEM[29]和 ABH[30]方案需要 $O(n)$的模幂运算和双线性对运算. 相对于上述 4 个方案，MAI-SH 方案只需要 $O(n)$的模幂运算.

在实现多个属性匹配过程中，虽然 SH-DEM[29]和 ABH[30]方案采用基于密文策略的属性加密方法实现了一般的访问策略，但协议双方指定的认证结构矩阵在交互过程中需要公开传输，部分访问策略信息不能得到保护. 另外，SH-DEM[29]和 ABH[30]方案在具体的实现过程中存储和通信的开销都会相应地增加，其中所需存储和传输的认证策略矩阵内元素包含 $O(n^2)$的通信量，其他方案的通信量和属性个数呈 $O(n)$的线性关系. 考虑到在移动社交网络等资源受限环境下实现多属性匹配的功能，需寻求平衡通信计算性能和访问策略功能的方案.

MAI-SH 方案构造借鉴 APSI 的思想实现多属性交集的认证策略，对于协议参与方 A 和 B 分别持有 v 和 w 个属性的情形，最初的方法需要计算和传送 $v\cdot w$ 的消息认证码(如$\{t_{11},\cdots,t_{vw}\}$)，通过 RSA 签名构造多个属性证书可实现聚合的特性(如 $\theta_A=\prod_{i=1}^{v}\sigma_{Ai}$，$\theta_{Ai}^{*}=\theta_A^{*}/\sigma_{Ai}$)对握手协议的通信和计算开销实现线性优化，协议参与方握手需要返回的消息及认证码(如 $Y'_A=\{Y'_{A1},\cdots,Y'_{Av}\}$，$T_B=\{t_{B1},\cdots,t_{Bw}\}$)所需的计算和存储开销可以从 $O(v\cdot w)$降低到 $O(v+w)=O(n)$计算量. 此外，为了实现模糊匹配的认证策略，SH-FM[12]和 PMA-FM[27]方案在执行握手协议之前需执行一个独立的秘密集合交集协议以确认对方是否符合认证策略，而 MAI-SH 构造把 APSI 协议融合到三轮握手协议中，不需要额外执行 PSI 协议. 因此，MAI-SH 整体方案的实现得到了进一步优化.

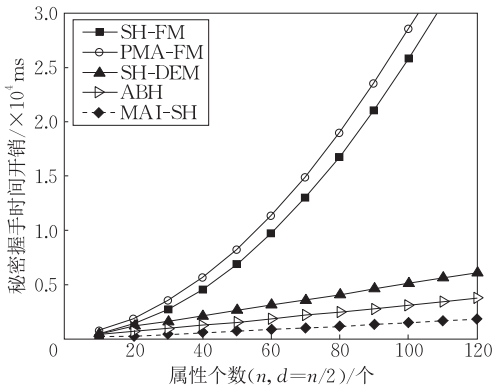

图 2 相关方案握手协议性能递增趋势图

考虑到协议双方持有多个属性的情形，在表 2 数据的基础上给出上述 5 个握手协议随着属性个数增加所需的计算量性能递增趋势图，如图 2 所示. 当属性个数 $n=50$ 时，假设 $d=n/2$，用户执行 SH-FM[12]和 PMA-FM[27]方案分别需要约 6876 ms 和 7365 ms，SH-DEM[29]及 ABH[30]方案分别需要约 2563 ms 和 1553 ms，而本文提出的 MAI-SH 方案所需的时间开销约是 738 ms. 因此，结合表 2、图 2 及上述理论分析，MAI-SH 协议在实现多属性交集匹配的认证策略的同时仍保证了较好的计算和通信性能，使之更能适用于资源受限的移动社交网络应用中.

5 结束语

本文基于模糊匹配模型设计了新型的多属性交集秘密握手 MAI-SH 方案，允许用户持有多个独立的属性特征及可验证的属性证书，使得两个参与方的属性集合交集不为空集或交集元素个数不小于一个门限值时能够秘密认证成功，同时保证交集之外组织信息的机密性. 基于 RSA 聚合签名实现 APSI 线性优化的技术，MAI-SH 方案支持具有多属性的两个用户间实现秘密双向认证，同时保证通信计算性能与属性个数呈线性递增关系，通信和计算开销达到了较好的线性优化性能. 因此，新型 MAI-SH 方案的设计可适用于资源受限的移动社交网络、医疗资源共享和推荐系统等应用中. 在未来的工作中可进一步探索基于 IBE 和 Schnorr 签名构造的 APSI 实现安全高效的多属性交集秘密握手方案的线性优化方法及其扩展应用.

致 谢 衷心感谢评审专家和编辑们对本文提出的宝贵意见和建议!

参 考 文 献

[1] Balfanz D, Durfee G, Shankar N, et al. Secret handshakes from pairing-based key agreements//Proceeding of the IEEE Symposium on Security and Privacy. Berkeley, USA, 2003: 180-196

[2] Castelluccia C, Jarecki S, Tsudik G. Secret handshakes from CA-oblivious encryption//Proceedings of the 10th International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT 2004). Jeju Island, Korea, 2005: 293-307

[3] Zhou L, Susilo W, Mu Y. Three-round secret handshakes based on ElGamal and DSA//Proceedings of the Information Security Practice and Experience Conference 2006. Hangzhou, China, 2006: 332-342

[4] Vergnaud D. RSA-based secret handshakes//Proceedings of the International Workshop of Coding and Cryptography (WCC 2005). Bergen, Norway, 2005: 252-274

[5] Jarecki S, Kim J, Tsudik G. Beyond secret handshakes: Affiliation-hiding authenticated key exchange//Proceeding of the Cryptographers' Track at the RSA Conference (CT-RSA 2008). San Francisco, USA, 2008: 352-369

[6] Wen Ya-Min, Gong Zheng. New affiliation-hiding authenticated key exchange protocol. Journal on Communications, 2015, 36(9): 82-90(in Chinese)
(温雅敏，龚征. 新型组织隐藏的认证密钥交换协议. 通信学报，2015，36(9)：82-90)

[7] Xu S, Yung M. *K*-anonymous secret handshakes with reusable credentials//Proceedings of the ACM Conference on Computer and Communications Security (CCS 2004). Washington, USA, 2004: 158-167

[8] Jarecki S, Liu X. Unlinkable secret handshakes and key-private group key management schemes//Proceedings of the Applied Cryptography and Network Security (ACNS 2007). Zhuhai, China, 2007: 270-287

[9] Wen Y, Zhang F, Xu L. Unlinkable secret handshakes from message recovery signature. Chinese Journal of Electronics, 2010, 19(4): 705-709

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

[11] Wen Ya-Min, Gong Zheng. A new unlinkable secret handshake scheme. Computer Engineering, 2013, 39(3): 152-156(in Chinese)
(温雅敏，龚征. 一个新型不可关联秘密握手方案. 计算机工程，2013，39(3)：152-156)

[12] Ateniese G, Blanton M, Kirsch J. Secret handshakes with dynamic and fuzzy matching//Proceedings of the Network and Distributed System Security Symposium (NDSS 2007). San Diego, USA, 2007: 159-177

[13] Wen Y, Gong Z. A dynamic matching secret handshake scheme without random oracles//Proceedings of the Network and System Security (NSS 2014). Xi'an, China, 2014: 409-420

[14] Kulshrestha P, Pal A K. A new secret handshakes scheme with dynamic matching based on ZSS. International Journal of Network Security and Its Applications, 2015, 7(1): 67-78

[15] Sorniotti A, Molva R. A provably secure secret handshake with dynamic controlled matching. Computers & Security, 2010, 29(5): 619-627

[16] Kawai Y, Yoneyama K, Ohta K. Secret handshake: Strong anonymity definition and construction//Proceedings of the Information Security Practice and Experience (ISPEC 2009). Xi'an, China, 2009: 219-229

[17] Jarecki S, Liu X. Private mutual authentication and conditional oblivious transfer//Proceedings of the International Cryptology Conference (CRYPTO 2009). Santa Barbara, USA, 2009: 90-107

[18] Sorniotti A, Molva R. Secret handshakes with revocation support//Proceedings of the 12th International Conference on Information Security and Cryptology (ICISC 2009). Seoul, Korea, 2009: 274-299

[19] Sorniotti A, Molva R. Federated secret handshakes with support for revocation//Proceedings of the International Conference on Information Systems (ICICS 2010). Barcelona, Spain, 2010: 218-234

[20] Wen Y, Zhang F. A new revocable secret handshake scheme with backward unlinkability//Proceedings of the European Public Key Infrastructure Workshop (EuroPKI 2010). Athens, Greece, 2011: 17-30

[21] Wen Y, Zhang F. Delegatable secret handshake scheme. Journal of Systems and Software, 2011, 84(12): 2284-2292

[22] Wen Ya-Min, Gong Zheng. New delegatable private mutual authentication protocol. Computer Science, 2013, 40(6): 94-99(in Chinese)
(温雅敏，龚征. 新型可授权的秘密双向认证协议. 计算机科学，2013，40(6)：94-99)

[23] Tian Y, Zhang S, Yang G, et al. Privacy-preserving *k*-time authenticated secret handshakes//Proceedings of the Australasian Conference on Information Security and Privacy (ACISP 2017). Auckland, New Zealand, 2017: 281-300

[24] He D, Kumar N, Wang H, et al. A provably-secure cross-domain handshake scheme with symptoms-matching for mobile healthcare social network. IEEE Transactions on Dependable and Secure Computing, 2018, 15(4): 633-645

[25] Tian Y, Li Y, Zhang Y, et al. DSH: Deniable secret handshake framework//Proceedings of the 14th International Conference on Information Security Practice and Experience (ISPEC 2018). Tokyo, Japan, 2018: 341-353

[26] Wen Y, Gong Z. An unlinkable secret handshake with fuzzy matching for social networks//Proceedings of the International Conference on P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC 2013). Compiegne, France, 2013: 347-353

[27] Wen Y, Gong Z. Private mutual authentications with fuzzy matching. International Journal of High Performance Systems Architecture, 2014, 5(1): 3-12

[28] Freedman M, Nissim K, Pinkas B. Efficient private matching and set intersection//Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT 2004). Interlaken, Switzerland, 2004: 1-19

[29] Hou L, Lai J, Liu L. Secret handshakes with dynamic express matching policy//Proceedings of the Australasian Conference on Information Security and Privacy (ACISP 2016). Melbourne, Australia, 2016: 461-476

[30] Liu Y, Wang H, Li T, et al. Attribute-based handshake protocol for mobile healthcare social networks. Future Generation Computer Systems, 2018, 86(9): 873-880

[31] Shen Li-Yan, Chen Xiao-Jun, Shi Jin-Qiao, Hu Lan-Lan. Survey on private preserving set intersection technology. Journal of Computer Research and Development, 2017, 54(10): 2153-2169(in Chinese)
(申立艳, 陈小军, 时金桥, 胡兰兰. 隐私保护集合交集计算技术研究综述. 计算机研究与发展, 2017, 54(10): 2153-2169)

[32] De Cristofaro E, Tsudik G. Practical private set intersection protocols with linear complexity//Proceedings of the Financial Cryptography and Data Security. Tenerife, Canary Islands, 2010: 143-159

[33] Huang Y, Evans D, Katz J. Private set intersection: Are garbled circuits better than custom protocols//Proceedings of the Network and Distributed System Security Symposium (NDSS). San Diego, USA, 2012: 1-15

[34] Pinkas B, Schneider T, Zohner M. Scalable private set intersection based on OT extension. ACM Transactions on Privacy and Security, 2018, 21(2): 7

[35] Rindal P, Rosulek M. Malicious-secure private set intersection via dual execution//Proceedings of the ACM SIGSAC Conference on Computer and Communications Security (CCS 2017). Dallas, USA, 2017: 1229-1242

[36] Chen H, Laine K, Rindal P. Fast private set intersection from homomorphic encryption//Proceedings of the ACM SIGSAC Conference on Computer and Communications Security (CCS 2017). Dallas, USA, 2017: 1243-1255

[37] Chen H, Huang Z, Laine K, et al. Labeled PSI from fully homomorphic encryption with malicious security//Proceedings of the ACM SIGSAC Conference on Computer and Communications Security (CCS 2018). Toronto, Canada, 2018: 1223-1237

[38] Pinkas B, Schneider T, Weinert C, et al. Efficient circuit-based PSI via cuckoo hashing//Proceedings of the Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT 2018). Tel Aviv, Israel, 2018: 125-157

[39] Pinkas B, Schneider T, Tkachenko O, et al. Efficient circuit-based PSI with linear communication//Proceedings of the Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT 2019). Darmstadt, Germany, 2019: 122-153

[40] Pinkas B, Rosulek M, Trieu N, et al. SpOT-Light: Lightweight private set intersection from sparse OT extension//Proceedings of the International Cryptology Conference (CRYPTO 2019). Santa Barbara, USA, 2019: 401-431

[41] Rivest R L, Shamir A, Adleman L. A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, 1978, 21(2): 120-126

WEN Ya-Min, Ph. D., associate professor. Her research interests include cryptography and information security.

ZHANG Fang-Guo, Ph. D., professor. His main research interests include cryptography and information security.

GONG Zheng, Ph. D., professor. His research interest is information system security.

Background

With a rapid development of online applications such as e-business, e-government and social networks, privacy is more and more attracted by people. Anonymous authentication plays a pivotal role among the whole privacy concerns. In some sensitive applications, the leakage of affiliation is not acceptable for full privacy concerns. The prover will reveal his affiliation if and only if the verifier holds the same one, and vice versa. Balfanz et al. first proposed the solution named Secret Handshake for realizing private mutual authentication, which not only protects the identity information of participants, but also provides a privacy-preserving property on their affiliations. In the original definition of secret handshakes, authentication will succeed if and only if the participants belong to the same single organization. Normally, a trusted third-party called Group Authority (GA) distributes group credentials to its members. Such members in the same group can execute secret handshakes to anonymously authenticate with each other.

After Balfanz et al.'s initial work, many secret handshake schemes have been proposed from different cryptographic primitives, such as CA-oblivious encryption, ElGamal, RSA and message recovery signature. Our research groups have proposed some secret handshakes based on message recovery signature. However, it is still not deeply studied how to achieve anonymous authentication and key agreement between users who hold multiple attributes in common. There are few existing works to effectively support such authentication policy. For solving this problem more efficiently, a new multiple-attribute intersection secret handshake scheme is proposed in this paper. Our proposal enables two anonymous users to accomplish a successful secret authentication and key agreement when their attributes set intersection is not an empty set. Meanwhile, the attributes outside of the set intersection remain confidential. Furthermore, by combining the authorized private set intersection to three-round secret handshakes, the new proposal achieves a linearly optimized construction while there is no need to deploy extra private set intersection protocol. Based on the difficulty assumptions of the RSA problem, we presented the secure analysis of our proposal under the random oracle model. Compared with the related schemes, the performance of our new scheme is linear-complexity.

This paper constructed a new secret handshake scheme by using the authorized private set intersection, which is the first research part about authorized private set intersection and its applications from the Project "Research on Private Set Intersection Protocols for Privacy-Preserving Information Sharing". The project focuses on some important techniques for realizing privacy-preserving information sharing, which is supported by the National Nature Science Foundation of China (Grant No. 61300204). This paper is also supported by the National Nature Science Foundation of China (Grant Nos. 61672550, 61572028), the National Social Science Foundation of China (Grant No. 14BXW031), the National Key R&D Program of China (Grant No. 2017YFB0802503), the National Cryptography Development Fund (Grant No. MMJJ20180206), the Guangdong Basic and Applied Basic Research Foundation (Grant Nos. 2019A1515011797, 2016A030310027, 2018A030313954, 2014A030313609), the Science and Technology Project of Guangzhou (Grant No. 201802010044), the China Scholarship Council (Grant No. 201808440097) and the Research Team of Big Data Audit from Guangdong University of Finance and Economics.