软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2019,30(6):1705−1720 [doi: 10.13328/j.cnki.jos.005746]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

可监管匿名认证方案*

王 震[1], 范 佳[1], 成 林[2], 安红章[1], 郑海彬[3], 牛俊翔[3]

[1](保密通信重点实验室,四川 成都 610041)

[2](中国信息安全评测中心,北京 100085)

[3](北京航空航天大学 电子信息工程学院,北京 100191)

通讯作者: 王震, E-mail: wz30cetc@126.com

摘 要: 随着互联网中隐私保护技术的发展,身份认证已成为保护计算机系统和数据安全的一道重要屏障.然而,信息技术的快速发展使传统身份认证手段暴露出一些弊端,例如,区块链技术的兴起对身份认证提出了更高的要求,在认证身份的同时需要保护用户的身份隐私等.采用匿名认证技术可解决用户身份隐私泄露的问题,但目前大多数方案未考虑可监管的问题,一旦用户出现不诚信行为,很难进行追责,因此,需要在匿名认证过程中建立监管机制.针对以上问题和需求,主要设计了一种可监管的匿名认证方案,通过匿名证书的方式确定用户的资源访问权限和使用权限,同时,用户在出示证书时可选择性地出示属性,确保用户的隐私信息不过度暴露;此外,方案中引入监管机制,可信中心(CA)对匿名认证过程进行监管,一旦出现欺诈行为,可对相关责任人进行追责.该方案主要采用安全的密码学算法构建,并通过了安全性的分析证明,能够高效实现可监管的匿名身份认证,适宜在区块链(联盟链)和其他具有匿名认证需求和可监管需求的系统中使用.

关键词: 身份认证;区块链;匿名性;可监管

中图法分类号: TP309

中文引用格式: 王震,范佳,成林,安红章,郑海彬,牛俊翔.可监管匿名认证方案.软件学报,2019,30(6):1705−1720. http://www.jos.org.cn/1000-9825/5746.htm

英文引用格式: Wang Z, Fan J, Cheng L, An HZ, Zheng HB, Niu JX. Supervised anonymous authentication scheme. Ruan Jian Xue Bao/Journal of Software, 2019,30(6):1705−1720 (in Chinese). http://www.jos.org.cn/1000-9825/5746.htm

Supervised Anonymous Authentication Scheme

WANG Zhen[1], FAN Jia[1], CHENG Lin[2], AN Hong-Zhang[1], ZHENG Hai-Bin[3], NIU Jun-Xiang[3]

[1](Science and Technology on Communication Security Laboratory, Chengdu 610041, China)

[2](China Information Technology Security Evaluation Center, Beijing 100085, China)

[3](School of Electrinic and Information Engineering, Beihang University, Beijing 100191, China)

Abstract: With the development of the privacy protection technology of the Internet, identity authentication has been a guardian of data andcomputer system. However, there exists some weaknesses in traditional identity authentication technology asit does notmeet requirements of the new information technology, i.e., the rise of the blockchain has raised higher requirements for identity authentication and it not only needs to identify different users but also has the necessary to protect the privacy of the users. Anonymous authentication technology is a method to protect users' privacy hiding, but most existing schemes do not supporta proper supervision mechanism. Once a user is dishonest, it is difficult to trackits real identity. Therefore, it is necessary to establish a regulatory mechanism in the process of

* 基金项目: 国家重点研发计划(2017YFB0802300)
Foundation item: National Key R&D Program of China (2017YFB0802300)
本文由区块链与数字货币技术专题特约编辑斯雪明教授和陈文光教授推荐.
收稿时间: 2018-06-26; 修改时间: 2018-10-12; 采用时间: 2018-12-18; jos 在线出版时间: 2019-03-27
CNKI 网络优先出版: 2019-03-27 16:40:36, http://kns.cnki.net/kcms/detail/11.2560.TP.20190327.1640.011.html

anonymous authentication. In this study, a supervised anonymous authentication scheme is proposed to solve above problems. On the one hand, access rights are provided for users by anonymous credentials, and users can selectively exposetheir attributes when they need to present their credentials. In this way, it can assure that users' information is under protection. On the other hand, a regulatory mechanism is introduced in anonymous authentication, which can track the real identity when cheating occurs.The supervised anonymous authentication scheme is constructed by secure cryptographic schemes and it is proved to be semantic secure. The proposed scheme is efficient and can be applied toconsortium blockchain and other supervised anonymous authentication systems.

Key words: identity authentication; blockchain; anonymity; supervision

1 引 言

互联网的发展使信息化服务逐渐渗透到人们生活的方方面面,传统活动逐渐被网上活动所替代.然而,互联网复杂、开放的特性也充满了未知的元素.随着隐私泄露、信息窃取等事件的发生,人与人之间的信任问题、隐私保护问题逐渐成为热点话题,而身份认证技术、隐私保护技术等安全技术也成为热点研究方向.

身份认证作为一种确认身份、授权的方式,被广泛应用于通信、金融、社交等方面.通过身份认证,可以确认用户是否拥有某种资源的访问权限或使用权限.

一种常用的身份认证方法是利用一个在线的身份提供者或证书发行者,用户每次进行身份验证时,发行人为用户身份的各种属性提供证明,但要求发行人时刻在线,增加了系统的负担.另外一种典型方法是用户通过离线的证书授权中心(certificate authority,简称 CA)预先得到关于各种属性的数字证书,然后直接向验证者出示数字证书,整个认证过程无需 CA 的参与.数字证书使用密码学技术,产生标识各方用户身份信息的一串数字,通过公开算法在互联网上提供验证用户身份的方式,数字证书由 CA 颁发,任何人可在网上验证数字证书的有效性.

目前,数字证书的标准为国际电信联盟(International Telecommunication Union,简称 ITU-T)制定的 X.509 标准(如图 1 所示).在 X.509 标准中,用户产生一对密钥,包括公钥和私钥,然后将公钥和多个属性发送给 CA, CA 为其颁发一个公钥的证书,并将公钥和证书维护在一个数据库中.证书中包括用户的属性信息和公钥信息等,CA 通过数据库可撤销或更新相应的证书.在验证时,验证者可确定一个访问策略,如要求用户出示属性 1 的证明,用户将证书发送给验证者,验证者利用 CA 的公钥进行验证.通过 X.509 数字证书标准,可实现数据完整性、身份确定性、不可否认性和防篡改性等功能.

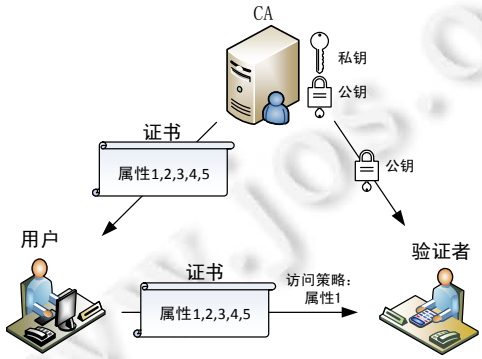


Fig.1 X.509 credentials

图 1 X.509 证书

然而,传统的 X.509 容易导致属性信息过度暴露的问题,在进行认证时,用户需要出示证书上的所有属性信息,从而导致信息泄露或遭到窃取.因此,需要采用匿名认证技术最大限度地减少曝光用户的属性信息.

Identity Mixer 是 IBM 于 2009 年提出的一种匿名证书的方案(如图 2 所示),主要解决传统方案中用户出示证书时过度暴露信息的问题,可以使用户选择性地出示证书中的属性信息,如验证者要求用户出示属性 1 的证明,用户可将证书转换为用户任何假名的有效标记,这些标识只包含原始凭证中的属性 1,并对其他属性进行隐藏,转换后的标记在 CA 的公钥下仍可验证,因此避免了用户属性信息的过度暴露.

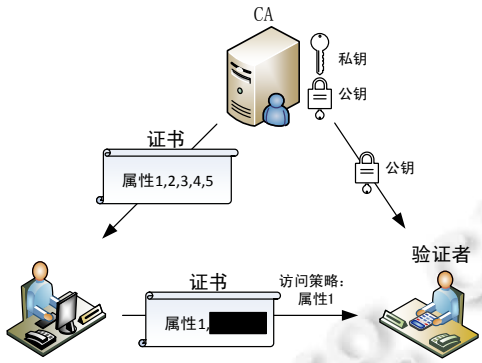


Fig.2 Identity mixer scheme

图 2 身份混淆器方案

该类方案虽然克服了传统 X.509 证书方案全属性暴露的问题,但存在一定的缺陷,即用户的身份无法监管,一旦出现欺诈行为,即使是 CA 也无法追踪到用户的真实身份.在医疗记录、家庭合约以及联盟链中的匿名交易、资产转移等领域,通常需要对用户身份进行监管,防止匿名滥用、失信行为的发生.

因此,本文主要针对认证过程中用户身份信息过度暴露和匿名证书无法监管的问题,采用密码学技术手段实现可监管的匿名认证方案.方案可应用于区块链中的匿名认证和匿名资产等方面,例如在联盟链中的匿名资产中,可以允许交易方在满足资产管理规定的条件下转移匿名资产.在交易过程中,交易方按照规定利用证书显示交易需要公开的内容,如资产来源银行代号、资产到账银行代号等,其他个人信息则可以进行隐藏,同时,资产的可监管性满足了审计业务的需求,审计人员可随时恢复出资产内容和交易方身份信息.

1.1 相关工作

在身份认证方面,X.509[1]第 1 个版本由国际电信联盟于 1988 年 7 月 3 日发布,设定了数字证书的标准,使数字证书作为身份认证的重要手段.之后,国际电信联盟又相继发表了 X.509 第 2、3 个版本,扩展了数字证书的应用,使其支持扩展的功能.2000 年,美国国家标准与技术研究院(National Institute of Standards and Technology,简称 NIST)给出了利用公钥技术实现数字签名和认证的指导意见[2],促进了公钥技术在认证方面的应用.之后,大量身份认证的方案[3−5]的出现是身份认证的技术逐渐成熟.

然而,大多数方案未考虑身份认证时的隐私保护问题,使用户在认证时容易暴露过多的身份信息或属性信息.因此,如何保证身份认证的匿名性逐渐成为一个热点问题.2004 年,Camenisch 和 Lysyanskaya 提出了基于双线性对的签名方案和匿名证书方案[6],用于身份的匿名认证,方案可应用于匿名电子投票、电子现金等方面.Man 等人基于 Boneh 等人提出的 BLS 短群签名方案[7],也提出了类似的匿名证书方案[8],方案可实现多次动态的认证,且签名证书长度为常数级的,使得方案具有较好的效率.除此之外,相似的匿名认证方案还有文献[9,10]等.在匿名证书的应用方面,IBM 提出的 Identity Mixer[11]可用于匿名认证和认证属性的传输,它允许用户进行身份验证而不收集其他任何个人数据.

Identity Mixer 的工作方式与传统公钥基础结构(PKI)中的客户端证书类似,但具有两个重要区别.

(1) 灵活的公共密钥:用户可以拥有多个独立的公钥(假名)用于同一个密钥,而不是每个验证者绑定到固定单个公钥,从而为每个验证者甚至每个会话使用不同的假名;

(2) 灵活的证书:用户的证书可以转换为用户任何假名的有效标记,这些标识只包含原始凭证中的一部分属性,转换后的标记在发行人的公钥下仍可验证.

传统的数字签名不能提供这种灵活性.Identity Mixer 方案基于 Camenisch-Lysyanskaya(CL)签名方案[12]构造,该签名方案含有高效的零知识证明和可验证加密算法,能在不打开签名的条件下证明签名者具有某些属性.

此外,文献[13]提出了云环境下的身份认证方案,通过无证书公钥密码体制,实现“口令+密钥”的双因子认证.然而方案需要保证认证节点服务器在线,增加了系统负担.文献[14]对匿名身份认证协议在云环境和多服务

器环境下的应用进行了分析,使用公钥技术保证匿名性,但文中仅对一些现存方案进行了分析比较,并未提出具有实用价值的方案.

以上方案均未考虑可监管的因素,限制了匿名认证在一些需要强制监管领域的应用,如医疗记录、家庭合约以及联盟链中的匿名交易、资产转移等方面.基于此,本方案通过结合 Identity Mixer 方案、群签名、零知识证明等密码学组件,设计出可监管的匿名认证方案,在实现匿名认证的同时进行强制监管,防止恶意欺诈、匿名滥用行为的发生.

群签名是一类特殊的数字签名,其概念[15]最早由 Chaum 和 Heyst 在 1991 年提出.群签名方案由签名者组成一个群体(简称群),群中的每个成员都能够以匿名的方式代表该群对消息进行签名,生成的签名用群公钥进行验证.一个好的群签名方案需满足以下基本的安全性要求:匿名性、可追踪性、不可伪造性、抗联合攻击性、不可链接性和防陷害性.但这些特征之间会有重合.直至 2003 年,Bellare 等人第 1 次给出群签名的严格定义和形式化的安全模型[16].该模型指出,群签名的最高安全特征为完全匿名性和完全可追踪性.

零知识证明概念[17]是由 Goldwasser 等人于 20 世纪 80 年代初提出的.零知识证明是指一方(证明者)能够在不向另一方(验证者)提供任何有用的信息的前提下,使得验证者能够相信某个论断是正确的.零知识证明分为交互式和非交互式,非交互零知识证明通过减少交互次数从而提高效率,一般采用 Fiat-Shamir 方案[18]将交互式零知识证明转化为非交互式零知识证明.

1.2 论文组织架构

本文第 1 节主要介绍身份认证的相关概念、目前工作存在的问题以及本文的主要工作.第 2 节介绍方案相关的预备知识,包括密码学基础概念和采用的方案.第 3 节对方案的构造进行详细的描述.第 4 节对方案的安全性进行证明.第 5 节对方案的效率和功能进行分析比较.第 6 节介绍方案的应用场景.最后,在第 7 节进行总结.

2 预备知识

2.1 双线性对

设 G_1,G_2,G_T 为 p 阶的循环群,Z_p 为 p 阶的整数群,g_1 为群 G_1 的生成元,g_2 为群 G_2 的生成元,若存在可计算的映射 $e:G_1\times G_2\to G_T$ 满足下列两个性质,则称 e 为双线性对.

(1) 双线性:对于任意 $\mu_1\in G_1,\mu_2\in G_2$,任意整数 $a,b\in Z_p$,都有 $e(\mu_1^a,\mu_2^b)=e(\mu_1,\mu_2)^{ab}$;

(2) 非退化性:$e(g_1,g_2)\neq 1$,即 $e(g_1,g_2)$ 为 G_T 的生成元.

一般地,$G_1\neq G_2$ 时称 e 为非对称双线性对;$G_1=G_2$ 时称 e 为对称双线性对.

2.2 群签名方案

群签名方案包含如下 5 种算法.

(1) 创建:一个产生群公钥、群管理员私钥和追踪密钥的概率多项式时间算法;

(2) 注册:一个用户和群管理员之间的交互式协议,使得用户成为一个新的群成员.执行该协议可以产生群成员的私钥和身份证书;

(3) 签名:一个概率算法,当输入一个消息和一个群成员的私钥后,输出对消息的群签名;

(4) 验证:一个概率算法,当输入消息、消息的群签名和群公钥后,输出关于签名有效性的判断;

(5) 追踪:一个在给定签名及群追踪密钥的条件下,输出签名者合法身份的算法.

安全性质包括完全匿名性和完全可追踪性等.完全匿名要求没有管理员的追踪密钥,攻击者在给予消息签名后不能恢复签名者的身份.完全可追踪性要求,互相勾结的群成员不能够创建一个群管理员无法追踪的有效签名.安全性质通过挑战者和敌手之间的一个游戏定义,完全匿名性和完全可追踪性可见文献[16]中的定义,本文不再给出具体描述.

2.3 零知识证明

零知识证明包括两个参与方:证明者 P 和验证者 V.对于承诺 $x\in L$,证据 w 和关系 R,$(x,w)\in R$,一个非交互式零知识证明 $NIZK\{x|(x,w)\in R\}$包含系统生成、证明和验证这 3 个算法.系统模型如下.

(1) 系统生成:输出公共参考字符串 CRS;

(2) 证明:证明者 P 完成对承诺 $x\in L$ 的证明;

(3) 验证:验证者 V 进行验证,若通过验证输出 1,否则输出 0.

当 P 与 V 完成一个协议后,这个协议是否是零知识证明协议,其必须满足下面 3 个条件.

(1) 完备性:如果 P 向 V 的声称是真的,则 V 以一个大的概率接受 P 的结论;

(2) 可靠性:如果 P 向 V 的声称是假的,则 V 以一个大的概率拒绝 P 的结论;

(3) 零知识性:如果 P 向 V 的声称是真的,在 V 不违背协议的前提下,无论 V 采用任何手段,除了接收到 P 给出的结论,V 无法获取有关 P 所声称内容的任何信息.

2.4 可监管匿名认证方案模型

可监管匿名认证方案包含 3 个参与方:可信中心(certificate authority,简称 CA)、用户和验证者.方案模型如图 3 所示.

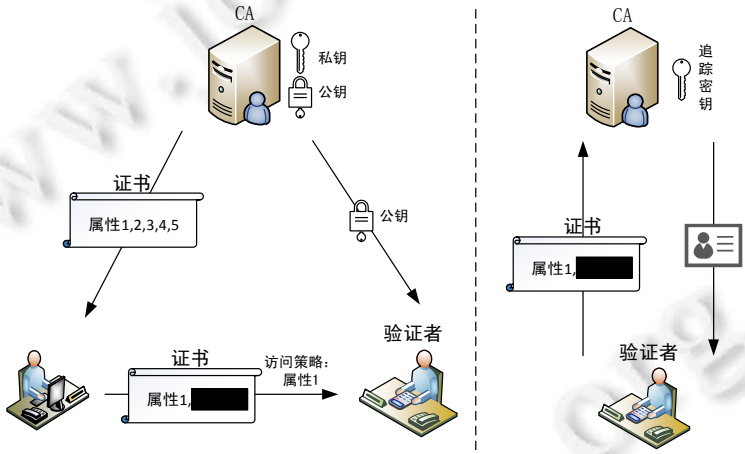


Fig.3 Model of supervised anonymous authentication scheme

图 3 可监管匿名认证方案模型

系统建立后,CA 产生发行密钥对、追踪密钥以及群公钥.然后用户进行注册,CA 为其分配一对私钥,同时,CA 根据用户提交的属性信息为用户颁发相关的证书.在用户出示证书时,验证者可指定用户证书上需要出示的属性(如属性 1),用户对证书进行签名,同时隐藏无需出示的属性值.验证者可对签名进行验证:若签名通过验证,则用户出示的证书有效;否则,用户出示的证书无效.若出现争端,验证者可将用户出示的证书发送给 CA 请求仲裁,CA 利用追踪密钥恢复出用户的真实身份.

一个完整的可监管匿名认证方案包含以下过程.

(1) 生成发行方密钥对$(ISK,IPK)\leftarrow Setup(1^{\lambda})$:输入安全参数 1^{λ},运行 $Setup$ 算法,输出 CA 的密钥对(ISK,IPK).发行方密钥对用户生成和验证用户的证书;

(2) 生成群密钥$(TK,GPK)\leftarrow GKey(1^{\lambda})$:输入安全参数 1^{λ},运行 $GKey$ 算法,输出追踪密钥 TK 和群公钥 GPK.追踪密钥由 CA 保存,用于从匿名证书中追踪用户的身份;群公钥用于出示和验证证书;

(3) 用户注册$(SK)\leftarrow UKey(ISK)$:输入 CA 的私钥 ISK,运行 $UKey$ 算法,输出用户私钥 SK.用户私钥用于出示证书,CA 将用户的私钥存入列表 $List$ 中,在身份追踪时,会将计算结果与用户的私钥比对,进而确定用户身份;

(4) 证书请求(*CertQst*)←*CQst*(*sk*,*IssuerNonce*):输入用户秘密值 *sk*,CA 发送给用户的随机数 *IssuerNonce*,运行 *CQst* 算法,输出用户的证书请求 *CertQst*;

(5) 证书请求验证(*b*)←*VerCQ*(*CertQst*,*IPK*):输入证书请求 *CertQst*、CA 公钥 *IPK*,运行 *VerCQ* 算法,输出字符 $b\in\{0,1\}$.若 $b=1$,则验证通过,CA 为用户生成证书;否则,CA 拒绝用户的请求;

(6) 生成证书(*Cert*)←*CertGen*(*ISK*,*IPK*,*CertQst*,*attr*):输入 CA 的密钥对(*ISK*,*IPK*)、证书请求 *CertQst*、用户属性值 *attr*,运行 *CertGen* 算法,输出用户的证书 *Cert*.CA 将证书发送给用户,用户进行验证:若通过验证,则证书有效,用户在本地存储证书;否则,证书无效;

(7) 出示证书(*Sig*)←*GSig*(*SK*,*sk*,*IPK*,*GPK*,*attr*,*Cert*,*m*):输入用户私钥 *SK*、用户秘密值 *sk*、CA 公钥 *IPK*、群公钥 *GPK*、属性值 *attr*、用户证书 *Cert*、消息 *m*,运行 *GSig* 算法,输出出示的证书(或签名)*Sig*;

(8) 出示证书验证(*b*)←*VerSig*(*Sig*,*IPK*,*GPK*,$attr_{ep}$,*m*):输入用户出示的证书 *Sig*、CA 公钥 *IPK*、群公钥 *GPK*、验证者指定用户需要出示的属性值 $attr_{ep}$、消息 *m*,运行 *VerSig* 算法,输出字符 $b\in\{0,1\}$.若 $b=1$,则验证通过,出示的证书有效;否则,出示的证书无效;

(9) 身份追踪(*SK*)←*Trac*(*Sig*,*TK*):输入用户出示的证书 *Sig*、CA 的追踪密钥 *TK*,运行 *Trac* 算法,输出匿名证书所对应的用户私钥 *SK*;然后 CA 将私钥和群内用户的私钥进行对比,从而追踪到用户的真实身份.

可监管的匿名证书方案的安全性质包括匿名性和可追踪性,安全性质通过语义安全性理论进行定义.

匿名安全要求没有 CA 机构的追踪密钥,攻击者在给予消息签名后不能恢复签名者的身份.根据安全性模型,即不存在任何多项式时间敌手$\mathcal{A}$,在下面匿名性模拟攻击游戏中以不可忽略的概率取得成功.

(1) 生成阶段:挑战者执行发行方密钥、群密钥算法,把生成的 CA 的公钥 *IPK* 和群公钥 *GPK* 发送给$\mathcal{A}$,保留 CA 的私钥 *ISK* 和追踪密钥 *TK*;

(2) 询问阶段 1:敌手$\mathcal{A}$可以对挑战者进行多项式有界次数的询问:

a) 注册询问:敌手$\mathcal{A}$请求询问用户 *i* 所对应的私钥 SK_i,挑战者执行注册算法并返回结果给$\mathcal{A}$;

b) 追踪询问:敌手$\mathcal{A}$选择一个出示的证书 *Sig* 请求询问,挑战者执行追踪算法并返回结果给$\mathcal{A}$;

(3) 挑战阶段:敌手$\mathcal{A}$选取两个用户 i_0,i_1、属性值 *attr* 和消息 m^*,然后发送给挑战者.挑战者首先运行注册算法产生相应私钥 SK_{i_0},SK_{i_1},然后随机选取 $b\in\{0,1\}$,执行证书算法生成证书 $Cert^*$,最后生成挑战证书 $Sig^*=GSig(SK_{i_b}^*,sk,IPK,GPK,attr,Cert^*,m^*)$ 并返回给敌手;

(4) 询问阶段 2:敌手$\mathcal{A}$同阶段 1 一样,可以对挑战者进行多项式有界次数的询问,但是不允许$\mathcal{A}$对用户 i_0,i_1 进行注册询问,且不允许对 Sig^* 进行追踪询问;

(5) 猜测阶段:询问阶段结束后,敌手$\mathcal{A}$输出一个比特 b',如果存在 $b'=b$,说明敌手$\mathcal{A}$成功进行了攻击.

敌手$\mathcal{A}$攻击成功的概率为 $Adv_{\mathcal{A}}^{anony}=|2\Pr[b'=b]-1|$.

可追踪性要求,互相勾结的群成员用户不能够创建一个群管理员无法追踪的有效签名.根据安全性模型,即不存在任何多项式时间敌手$\mathcal{A}$,在下面可追踪性模拟攻击游戏中以不可忽略的概率取得成功.

(1) 生成阶段:挑战者执行发行方密钥、群密钥算法,把生成的 CA 的公钥 *IPK* 和群公钥 *GPK* 发送给$\mathcal{A}$,保留 CA 的私钥 *ISK* 和追踪密钥 *TK*;

(2) 勾结阶段:敌手$\mathcal{A}$选择用户的私钥进行请求,然后添加腐败的群成员到列表$\mathcal{L}$.这里,$\mathcal{L}$表示腐败群成员的身份列表;同时,共谋行为意味着$\mathcal{A}$只能捕获他们的私钥,但不能命令他们做一些篡改操作;

(3) 询问阶段 1:敌手$\mathcal{A}$可以对挑战者进行多项式有界次数的询问.

a) 注册询问:敌手$\mathcal{A}$请求询问用户 *i* 所对应的私钥 SK_i,挑战者执行注册算法并返回结果给$\mathcal{A}$;

b) 签名询问:敌手$\mathcal{A}$选择用户私钥 *SK*、证书 *Cert* 和消息 *m* 请求询问,挑战者执行签名算法并返回结果 *Sig* 给$\mathcal{A}$;

c) 追踪询问:敌手$\mathcal{A}$选择一个出示的证书 *Sig* 请求询问,挑战者执行追踪算法并返回结果给$\mathcal{A}$;

(4) 挑战阶段:最终,敌手$\mathcal{A}$输出关于消息 m^* 的挑战签名 Sig^*.如果以下任意情况发生,则敌手$\mathcal{A}$攻击成功.

a) 出示的证书 Sig^*有效,但恢复出的私钥无效,即:

$$VerSig(Sig^*,IPK,GPK,attr_{ep},m^*)=1,Trac(Sig^*,TK)=\perp;$$

b) 出示的证书 Sig^*有效且未被询问过,但恢复出的私钥不属于勾结列表$\mathcal{L}$,即:

$$VerSig(Sig^*,IPK,GPK,attr_{ep},m^*)=1,Trac(Sig^*,TK)=SK_i\notin\mathcal{L}.$$

敌手$\mathcal{A}$攻击成功的概率为 $Adv_{\mathcal{A}}^{trace}=\Pr[\mathcal{A}\ wins]$.

3 可监管匿名认证方案

3.1 符号说明

本文方案主要涉及的符号变量和意义见表 1.

Table 1 Symbols and its notions in our scheme

表 1 本文的变量符号和意义

变量符号	意义	变量符号	意义
ISK	主私钥	*IPK*	主公钥
TK	身份追踪密钥	*SK*	用户私钥
IssuerNonce	CA 的随机数	*Nym*	用户假名
sk	用户的秘密值	*CertQst*	用户证书请求
attr	用户属性值	*Cert*	用户的证书
nonce	用户的随机数	*Sig*	用户出示的证书

3.2 可监管匿名认证方案

本文构造的可监管匿名认证方案结合了 Identity Mixer 方案[11]、BBS 群签名方案[7]和 Fiat-Shamir 方案[18]非交互式零知识证明技术,下面介绍具体的方案,方案流程如图 4 所示.

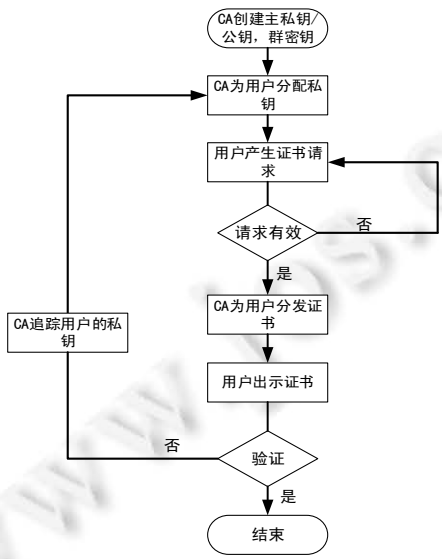


Fig.4 Algorithm flow of supervised anonymous authentication scheme

图 4 可监管匿名认证方案流程

可监管匿名认证方案包括以下过程.

(1) 生成发行方密钥对

设 G_1,G_2,G_T为 p 阶的循环群,Z_p为 p 阶的整数群,g_1为群 G_1的生成元,g_2为群 G_2的生成元,e 为可计算的双

线性对 $e:G_1\times G_2\to G_T$,H 为耐碰撞的哈希函数 $H:\{0,1\}^*\to\{0,1\}^*$.随机选择整数 $r\in Z_p$,设置 CA 私钥为 $ISK=r$,计算 $PK=g_2^r$,设置属性名列表为 $AttrName=[name_1,\ldots,name_k]$,其长度为 $len(AttrName)=k$,CA 通过属性名列表定义属性结构.随机选择整数 $r_1',r_2',\ldots,r_k'\in Z_p$,计算一组长度为 k 的随机数 $HAttr=[g_1^{r_1'},\ldots,g_1^{r_k'}]$.随机选择整数 $r_1,r_2,r_3\in Z_p$,计算 $HSK=g_1^{r_1}$,$Hrand=g_1^{r_2}$,$\overline{g}_1=g_1^{r_3}$,$\overline{g}_2=\overline{g}_1^{ISK}$.

然后计算关于 CA 私钥的零知识证明,记为 $NIZK\{ISK\mid PK=g_2^r\wedge\overline{g}_2=\overline{g}_1^r\}$,计算方法如下.

a) 随机选择整数 $\hat{r}\in Z_p$,计算 $\overline{t}_1=g_2^{\hat{r}}$,$\overline{t}_2=\overline{g}_1^{\hat{r}}$;

b) 计算挑战值 $c_r=H(\overline{t}_1,\overline{t}_2,g_2,\overline{g}_1,PK,\overline{g}_2)$;

c) 计算 s 值: $s_r=\hat{r}+c_r\cdot ISK$.

最终输出 CA 的密钥 $ISK=r$, $IPK=(g_1,g_2,PK,AttrName,HAttr,HSK,Hrand,\overline{g}_1,\overline{g}_2,c_r,s_r)$.

任何人可验证 CA 密钥是否正确,验证过程如下.

a) 计算 $\overline{t}_1'=g_2^{s_r}\cdot PK^{-c_r}$,$\overline{t}_2'=\overline{g}_1^{s_r}\cdot\overline{g}_2^{-c_r}$;

b) 计算挑战值 $c_r'=H(\overline{t}_1',\overline{t}_2',g_2,\overline{g}_1,PK,\overline{g}_2)$,判断 $c_r'=c_r$ 是否成立:若公示成立,则 CA 密钥正确;否则,CA 密钥不正确.

(2) 生成群密钥

随机选择整数 $\xi_1,\xi_2\in Z_p$,令 $h=g_1^{\xi_1\xi_2}$,$u=g_1^{\xi_2}$,$v=g_1^{\xi_1}$,则有 $u^{\xi_1}=v^{\xi_2}=h$.设置群追踪密钥为 $TK=(\xi_1,\xi_2)$,群公钥为 $GPK=(u,v,h)$.

(3) 用户注册

用户需利用身份信息向 CA 注册,得到相应的私钥.对于用户 i,CA 随机选择整数 $x\in Z_p$,计算 $K=g_1^{1/(ISK+x)}$,设置用户的私钥为 $SK=(K,x)$;同时,CA 将用户的私钥和对应的身份信息存储到表 $List$ 中.

(4) 证书请求

CA 随机选择一个整数 $IssuerNonce\in Z_p$ 并发送给用户.用户随机选择一个整数 $sk\in Z_p$ 作为自己的秘密值,然后随机选择整数 $creds\in Z_p$,计算假名(或承诺)$Nym=HSK^{sk}\cdot Hrand^{creds}$,然后计算关于秘密值 sk 和随机数 $creds$ 的零知识证明,记为 $NIZK\{sk,creds|Nym=HSK^{sk}\cdot Hrand^{creds}\}$,计算过程如下.

a) 随机选择整数 $r_s,r_d\in Z_p$,计算 $t=HSK^{r_s}\cdot Hrand^{r_d}$;

b) 计算挑战值 $c_{sk}=H(t,HSK,Nym,IssuerNonce)$;

c) 计算 s 值 $s_1=r_s+c_{sk}\cdot sk$,$s_2=rd_s+c_{sk}\cdot creds$.

最后输出证书请求 $CertQst=(Nym,IssuerNonce,c_{sk},s_1,s_2)$.

(5) 证书请求验证

CA 接收到用户的证书请求后,首先进行验证,验证过程如下.

a) 计算 $t''=HSK^{s_1}\cdot Hrand^{s_2}$,$t'=t''/Nym^{c_{sk}}$;

b) 计算挑战值 $c_{sk}'=H(t',HSK,Nym,IssuerNonce)$.判断 $c_{sk}'=c_{sk}$ 是否成立:若公示成立,则用户证书请求有效;否则,用户证书请求无效,CA 拒绝为用户颁发证书.

(6) 生成证书

设用户提交的属性值为 $attr=[attr_1,\ldots,attr_k]\in Z_p^k$,CA 首先选择随机整数 $e,s'\in Z_p$,然后计算 $B_1=g_1\cdot Nym\cdot Hrand^{s'}$,CA 利用公式(1)和公式(2)计算签名:

$$B=B_1\prod_{i=1}^{k}HAttr_i^{attr_i} \tag{1}$$

$$A=B^{\frac{1}{e+r}} \tag{2}$$

最后得到证书 $Cert=(A,B,e,s',attr)$.

(7) 出示证书

用户在交易时需要出示证书,验证者可指定需要出示的属性值,用户对需要隐藏的属性值(设共有 l 个)的下

标进行标记,记为 $HiddenIndices=[I_1,\ldots,I_l]$,其中,$I_i$ 为需要隐藏的属性值的下标.

用户首先随机选择整数 $r_n,\overline{r}_1,\overline{r}_2\in Z_p$,计算新的假名 $Nym_r=HSK^{sk}\cdot Hrand^{r_n}$,然后对证书中的签名随机化,计算 $A'=A^{\overline{r}_1},\overline{A}=A'^{-e}\cdot B^{\overline{r}_1},B'=Hrand^{-\overline{r}_2}\cdot B^{\overline{r}_1},s=creds+s',s_p=s-\overline{r}_2/\overline{r}_1$.然后,用户随机选择整数$\alpha,\beta\in Z_p$,产生两个辅助值$\delta_1=x\alpha,\delta_2=x\beta$,并计算关于用户私钥 x、秘密值 sk 和随机数 e,s,α,β的零知识证明,记为

$$NIZK\{x,sk,e,s,\alpha,\beta\mid Nym_r=HSK^{sk}\cdot Hrand^{r_n}\wedge A'=A^{\overline{r}_1}\wedge\overline{A}=A'^{-e}\cdot B^{\overline{r}_1}\wedge B'=Hrand^{-\overline{r}_2}\cdot B^{\overline{r}_1}\wedge s_p\}.$$

计算过程如下.

a) 随机选择整数 $r_{sk},r_e,r_{l_1},r_{l_2},r_{sp},r_{nr}\in Z_p$,设 $r_a=[r_{a_1},\ldots,r_{a_l}]\in Z_p^l$ 为 l 长度的一组随机整数,利用下列公式计算辅助值:

$$t_1=A'^{r_e}\cdot Hrand^{r_{l_1}} \tag{3}$$

$$t_2'=Hrand^{r_{sp}}\cdot B'^{r_{l_2}}\cdot HSK^{r_{sk}} \tag{4}$$

$$t_2=t_2'\cdot\prod\nolimits_{i\in HiddenIndices}HAttr_i^{r_{a_i}} \tag{5}$$

$$t_3=HSK^{r_{sk}}\cdot Hrand^{r_{nr}} \tag{6}$$

b) 随机选择整数 $r_\alpha,r_\beta,r_x,r_{\delta_1},r_{\delta_2}\in Z_p$,利用下列公式计算辅助值:

$$T_1=u^{\alpha} \tag{7}$$

$$T_2=v^{\beta} \tag{8}$$

$$T_3=K\cdot h^{\alpha+\beta} \tag{9}$$

$$R_1=u^{r_\alpha} \tag{10}$$

$$R_2=v^{r_\beta} \tag{11}$$

$$R_3=e(T_3,g_2)^{r_x}\cdot e(h,PK)^{-r_\alpha-r_\beta}\cdot e(h,g_2)^{-r_{\delta_1}-r_{\delta_2}} \tag{12}$$

$$R_4=T_1^{r_x}\cdot u^{-r_{\delta_1}} \tag{13}$$

$$R_5=T_2^{r_x}\cdot v^{-r_{\delta_2}} \tag{14}$$

c) 设签名的消息为 m,用户随机产生一个整数 $nonce\in Z_p$,然后利用下列公式计算挑战值:

$$c_h=H(t_1,t_2,t_3,A',\overline{A},B',Nym_r,T_1,T_2,T_3,R_1,R_2,R_3,R_4,R_5,m) \tag{15}$$

$$c=H(c_h,nonce) \tag{16}$$

d) 计算 s 值:

$$\begin{aligned}
&s_{sk}=r_{sk}+c\cdot sk,\\
&s_e=r_e-c\cdot e,\\
&s_{l_1}=r_{l_1}+c\cdot\overline{r}_2,\\
&s_{l_2}=r_{l_2}-c\cdot(1/\overline{r}_1),\\
&s_{sp}=r_{sp}+c\cdot s_p,\\
&s_{nr}=r_{nr}+c\cdot r_n,\\
&s_\alpha=r_\alpha+c\cdot\alpha,\\
&s_\beta=r_\beta+c\cdot\beta,\\
&s_x=r_x+c\cdot x,\\
&s_{\delta_1}=r_{\delta_1}+c\cdot\delta_1,\\
&s_{\delta_2}=r_{\delta_2}+c\cdot\delta_2;
\end{aligned}$$

对于 $0<i\leqslant l$,计算 $s_{a_i}=r_{a_i}+c\cdot attr_i$.

最终,用户出示的匿名证书(签名)为

$$Sig=(A',\overline{A},B',Nym_r,T_1,T_2,T_3,c,s_{sk},s_e,s_{l_1},s_{l_2},s_{sp},s_{nr},s_\alpha,s_\beta,s_{\delta_1},s_{\delta_2},s_{a_i},nonce) \tag{17}$$

(8) 出示证书验证

对于用户出示的证书,验证过程如下.

a) 验证 $e(PK,A')=e(g_2,\bar{A})$ 是否成立:若等式成立,则证书格式正确;否则,证书无效;

b) 利用下列公式计算辅助值:

$$t_1''=A'^{s_e}\cdot Hrand^{s_h} \tag{18}$$

$$t_1'=t_1''/(\bar{A}/B')^c \tag{19}$$

$$t_2'''=Hrand^{s_{sp}}\cdot B'^{s_{l_2}}\cdot HSK^{s_{s_k}} \tag{20}$$

$$t_2''=t_2'''\cdot\prod_{i\in HiddenIndices}HAttr_i^{s_{a_i}} \tag{21}$$

设需要出示的属性值下标集合记为 $Disclosure=[I_1,\ldots,I_{k-l}]$,计算:

$$t_2'=t_2''\cdot(g_1\prod_{i\in Disclosure}HAttr_i^{attr_i})^c \tag{22}$$

$$t_3''=HSK^{s_{sk}}\cdot Hrand^{s_{nr}} \tag{23}$$

$$t_3'=t_3''/Nym_r^c \tag{24}$$

$$R_1'=u^{s_\alpha}\cdot T_1^{-c} \tag{25}$$

$$R_2'=v^{s_\beta}\cdot T_2^{-c} \tag{26}$$

$$R_3'=e(T_3,g_2)^{s_x}\cdot e(h,PK)^{-s_\alpha-s_\beta}\cdot e(h,g_2)^{-s_{\delta_1}-s_{\delta_2}}\cdot(e(T_3,PK)/e(g_1,g_2))^c \tag{27}$$

$$R_4'=T_1^{s_x}\cdot u^{-s_{\delta_1}} \tag{28}$$

$$R_5'=T_2^{s_x}\cdot v^{-s_{\delta_2}} \tag{29}$$

c) 利用下列公式计算挑战值:

$$c_h'=H(t_1',t_2',t_3',A',\bar{A},B',Nym_r,T_1,T_2,T_3,R_1',R_2',R_3',R_4',R_5',m) \tag{30}$$

$$c'=H(c_h',nonce) \tag{31}$$

判断 $c'=c$ 是否成立:若等式成立,则用户出示的证书有效;否则,出示的证书无效.

(9) 身份追踪

若出现争端,验证者可将用户出示的证书 *Sig* 发送给 CA,请求仲裁.CA 利用追踪密钥 $TK=(\xi_1,\xi_2)$进行解密:

$$K'=T_3/(T_1^{\xi_1}\cdot T_2^{\xi_2}) \tag{32}$$

得到用户的私钥 *K'*,然后查找对比用户私钥的列表 *List*,最终追踪到用户的真实身份.

4 安全性分析

本文方案基于 Identity Mixer 方案[11]、BBS 群签名方案[7]和 Fiat-Shamir 方案[18]非交互式零知识证明协议构造,根据各模块的安全特性,下面给出匿名性和可追踪性安全性分析.

4.1 匿名性分析

本文方案的匿名性满足以下结论.

结论 1. 若 Identity Mixer 方案满足基本安全性质,BBS 群签名方案满足完全匿名性,且 Fiat-Shamir 零知识证明协议满足完备性、可靠性和计算零知识性,则本文可监管匿名认证方案满足匿名性.

证明:定义 $\mathcal{A}_{anony}$ 为攻击本文方案匿名性模拟攻击游戏的敌手,$\mathcal{A}_{idm}$ 为攻击 Identity Mixer 方案方案的敌手,$\mathcal{A}_{sg,f\text{-}anony}$ 为攻击群签名方案完全匿名性安全的敌手,$\mathcal{A}_{pof}$ 为攻击零知识证明协议的敌手.假设 $\mathcal{A}_{anony}$ 成功攻击了该方案的匿名性,定义一个多项式时间算法 $\mathcal{A}_\gamma\in(\mathcal{A}_{idm},\mathcal{A}_{sg,f\text{-}anony},\mathcal{A}_{pof})$包含攻击 Identity Mixer 方案、群签名方案和零知识证明协议等攻击者的能力.通过匿名模拟攻击游戏中 $\mathcal{A}_{anony}$ 的查询和 $\mathcal{A}_\gamma$ 的响应交互来构造 $\mathcal{A}_\gamma$,使其能够攻击 Identity Mixer 方案、群签名方案和零知识证明协议.即:若敌手 $\mathcal{A}_{anony}$ 成功攻击了该方案的匿名性,则 $\mathcal{A}_\gamma$ 就能以某一概率成功攻击 Identity Mixer 方案、群签名方案的完全匿名性和零知识证明协议.

根据匿名性定义的步骤,算法$\mathcal{A}_\gamma$和敌手$\mathcal{A}_{anony}$的交互运行如下.

(1) 生成阶段:算法$\mathcal{A}_\gamma$执行系统生成算法,通过分别运行$\mathcal{A}_{idm}$,$\mathcal{A}_{sg,f\text{-}anony}$,$\mathcal{A}_{pof}$在 Identity Mixer 方案、群签名方案和零知识证明模拟攻击游戏中产生的公共参数,生成匿名性模拟攻击游戏的公共参数 IPK 和 GPK,然后将公共参数发送给$\mathcal{A}_{anony}$,保留系统主密钥 ISK 和群追踪密钥 TK;

(2) 询问阶段 1:敌手$\mathcal{A}_{anony}$可以对算法$\mathcal{A}_\gamma$进行多项式有界次数的询问:

a) 注册询问:敌手$\mathcal{A}_{anony}$请求询问用户 i 所对应的私钥 SK_i,算法$\mathcal{A}_\gamma$通过运行$\mathcal{A}_{idm}$,$\mathcal{A}_{sg,f\text{-}anony}$,$\mathcal{A}_{pof}$在群签名方案模拟攻击游戏中的注册询问,将得到的注册询问结果返回给$\mathcal{A}_{anony}$;

b) 追踪询问:敌手$\mathcal{A}$选择一个出示的证书 Sig 请求询问,算法$\mathcal{A}_\gamma$通过运行$\mathcal{A}_{sg,f\text{-}anony}$在群签名方案模拟攻击游戏中的追踪询问,将得到的询问结果返回给$\mathcal{A}_{anony}$;

(3) 挑战阶段:敌手$\mathcal{A}_{anony}$选取两个用户 i_0,i_1、属性值 $attr$ 和消息 m^*.算法$\mathcal{A}_\gamma$首先运行群签名方案中的注册算法产生相应私钥 SK_{i_0},SK_{i_1},然后随机选取 $b\in\{0,1\}$,执行$\mathcal{A}_{idm}$,$\mathcal{A}_{sg,f\text{-}anony}$在 Identity Mixer 方案、群签名方案模拟游戏中的挑战阶段,得到生成证书 $Cert^*$,最后生成挑战证书 $Sig^*=GSig(SK_{i_b}^*,sk,IPK,GPK,attr,Cert^*,m^*)$ 并返回给敌手$\mathcal{A}_{anony}$;

(4) 询问阶段 2:敌手$\mathcal{A}_{anony}$与阶段 1 一样,可以对算法$\mathcal{A}_\gamma$进行多项式有界次数的询问,但是不允许$\mathcal{A}_{anony}$对用户 i_0,i_1 进行注册询问,且不允许对 Sig^*进行追踪询问;

(5) 猜测阶段:询问阶段结束后,敌手$\mathcal{A}_{anony}$输出一个比特 b',若存在 $b'=b$,说明敌手$\mathcal{A}_{anony}$成功进行了攻击.

敌手$\mathcal{A}_{anony}$成功概率为

$$\begin{aligned}
Adv_{\mathcal{A}_{anony}}(k)&=\Pr[Exp_{\mathcal{A}_{anony}}(k)=1]\\
&=\Pr[\mathcal{A}_{anony}(guess)=1\,|\,b=1]\cdot\Pr[b=1]+\Pr[\mathcal{A}_{anony}(guess)=0\,|\,b=0]\cdot\Pr[b=0]\\
&=\frac{1}{2}\Pr\left[\begin{matrix}\mathcal{A}_{idm}(guess=1)\\ \mathcal{A}_{sg,f\text{-}anony}(guess=1)\end{matrix}\middle|\,b=1\right]+\frac{1}{2}\Pr\left[\begin{matrix}\mathcal{A}_{idm}(guess=0)\\ \mathcal{A}_{sg,f\text{-}anony}(guess=0)\end{matrix}\middle|\,b=0\right]\\
&<\frac{1}{2}(\Pr[\mathcal{A}_{idm}(guess=1)\,|\,b=1]+\Pr[\mathcal{A}_{idm}(guess=0)\,|\,b=0])+\\
&\quad\frac{1}{2}(\Pr[\mathcal{A}_{sg,f\text{-}anony}(guess=1)\,|\,b=1]+\Pr[\mathcal{A}_{sg,f\text{-}anony}(guess=0)\,|\,b=0])\\
&=\Pr[Exp_{\mathcal{A}_{idm}}(k)=1]+\Pr[Exp_{\mathcal{A}_{sg,f\text{-}anony}}(k)=1]\\
&=Adv_{\mathcal{A}_{idm}}(k)+Adv_{\mathcal{A}_{sg,f\text{-}anony}}(k).
\end{aligned}$$

因此,如果攻击者$\mathcal{A}_{idm}$成功攻击 Identity Mixer 方案,攻击者$\mathcal{A}_{sg,f\text{-}anony}$成功攻击群签名方案的完全匿名性,攻击者$\mathcal{A}_{pof}$成功攻击零知识证明协议,则$\mathcal{A}_{anony}$在可监管匿名认证方案匿名性模拟攻击游戏中获胜.然而根据定理中对基本组件安全性的假设,我们得到敌手$\mathcal{A}_{anony}$攻击成功概率可以忽略不计,因此方案满足匿名性.

4.2 可追踪性分析

本文方案的可追踪性满足以下结论.

结论 2. 若 Identity Mixer 方案满足基本安全性质,BBS 群签名方案满足完全可追踪性,且 Fiat-Shamir 零知识证明协议满足完备性、可靠性和计算零知识性,则本文可监管匿名认证方案满足可追踪性.

证明:定义$\mathcal{A}_{trace}$为攻击本文方案可追踪性模拟攻击游戏的敌手,$\mathcal{A}_{idm}$为攻击 Identity Mixer 方案的敌手,$\mathcal{A}_{sg,f\text{-}trace}$为攻击群签名方案完全匿名性安全的敌手,$\mathcal{A}_{pof}$为攻击零知识证明协议的敌手.假设$\mathcal{A}_{trace}$成功攻击了该方案的可追踪性,定义一个多项式时间算法$\mathcal{A}_\eta\in(\mathcal{A}_{idm},\mathcal{A}_{sg,f\text{-}trace},\mathcal{A}_{pof})$包含攻击 Identity Mixer 方案、群签名方案和零知识证明协议等攻击者的能力.通过可追踪模拟攻击游戏中$\mathcal{A}_{trace}$的查询和$\mathcal{A}_\eta$的响应交互来构造$\mathcal{A}_\eta$,使其能够攻击 Identity Mixer 方案、群签名方案和零知识证明协议.即:如果敌手$\mathcal{A}_{trace}$成功攻击了该方案的可追踪性,则$\mathcal{A}_\eta$就能以某一概率成功攻击 Identity Mixer 方案、群签名方案的完全可追踪性和零知识证明协议.

根据可追踪性定义的步骤,算法$\mathcal{A}_\eta$和敌手$\mathcal{A}_{trace}$的交互运行如下.

(1) 生成阶段:算法$\mathcal{A}_\eta$执行系统生成算法,通过分别运行$\mathcal{A}_{idm}$,$\mathcal{A}_{sg,f\text{-}trace}$,$\mathcal{A}_{pof}$在 Identity Mixer 方案、群签名方案和零知识证明模拟攻击游戏中产生的公共参数,生成可追踪性模拟攻击游戏的公共参数 *IPK* 和 *GPK*,然后将公共参数发送给$\mathcal{A}_\eta$,保留系统主密钥 *ISK* 和群追踪密钥 *TK*;

(2) 勾结阶段:敌手$\mathcal{A}_{trace}$选择用户的私钥进行请求,算法$\mathcal{A}_\eta$通过运行$\mathcal{A}_{idm}$,$\mathcal{A}_{sg,f\text{-}trace}$群签名方案模拟攻击游戏中的勾结询问,将得到的询问结果返回给$\mathcal{A}_{trace}$,然后添加腐败的群成员到列表$\mathcal{L}$;

(3) 询问阶段 1:敌手$\mathcal{A}_{trace}$可以对算法$\mathcal{A}_\eta$进行多项式有界次数的询问.

a) 注册询问:敌手$\mathcal{A}_{trace}$请求询问用户 *i* 所对应的私钥 SK_i,算法$\mathcal{A}_\eta$通过运行$\mathcal{A}_{idm}$,$\mathcal{A}_{sg,f\text{-}trace}$,$\mathcal{A}_{pof}$在群签名方案模拟攻击游戏中的注册询问,将得到的注册询问结果返回给$\mathcal{A}_{trace}$;

b) 签名询问:敌手$\mathcal{A}_{trace}$选择用户私钥 *SK*、证书 *Cert* 和消息 *m* 请求询问,算法$\mathcal{A}_\eta$通过运行$\mathcal{A}_{idm}$,$\mathcal{A}_{sg,f\text{-}trace}$,$\mathcal{A}_{pof}$在 Identity Mixer 方案和群签名方案模拟攻击游戏中的签名询问,将得到的 *Sig* 返回给$\mathcal{A}_{trace}$;

c) 追踪询问:敌手$\mathcal{A}_{trace}$选择一个出示的证书 *Sig* 请求询问,算法$\mathcal{A}_\eta$通过运行$\mathcal{A}_{sg,f\text{-}trace}$在群签名方案模拟攻击游戏中的追踪询问,将得到的追踪询问结果返回给$\mathcal{A}_{trace}$;

(4) 挑战阶段:最终,敌手$\mathcal{A}_{trace}$输出关于消息 m^*的挑战证书 Sig^*.如果以下任意情况发生,则敌手$\mathcal{A}_{trace}$攻击成功.

a) 出示的证书 Sig^*有效,但恢复出的私钥无效,即 $Trac(Sig^*,TK)=\perp$;

b) 出示的证书 Sig^*有效且未被询问过,但恢复出的私钥不属于勾结列表$\mathcal{L}$,即 $Trac(Sig^*,TK)=SK_i\notin\mathcal{L}$.

根据算法$\mathcal{A}_\eta$和敌手$\mathcal{A}_{trace}$的交互,敌手$\mathcal{A}_{trace}$成功的概率为

$$\begin{aligned}Adv_{\mathcal{A}_{trace}}(k)&=\Pr[Exp_{\mathcal{A}_{trace}}(k)=1]\\&=\Pr[VerSig(Sig^*,IPK,GPK,attr_{ep},m^*)=1,Trac(TK,Sig^*)=\perp]+\\&\quad\Pr[VerSig(Sig^*,IPK,GPK,attr_{ep},m^*)=1,Trac(TK,Sig^*)=SK_i^*\notin\mathcal{L}]\\&=\Pr[Exp_{\mathcal{A}_{idm}}(k)=1]\cdot\Pr[Exp_{\mathcal{A}_{sg,f\text{-}trace}}(k)=1]\\&=Adv_{\mathcal{A}_{idm}}(k)\cdot Adv_{\mathcal{A}_{sg,f\text{-}trace}}(k).\end{aligned}$$

因此,如果攻击者$\mathcal{A}_{idm}$成功攻击 Identity Mixer 方案,攻击者$\mathcal{A}_{sg,f\text{-}trace}$成功攻击群签名方案的完全可追踪性,攻击者$\mathcal{A}_{pof}$成功攻击零知识证明协议,则$\mathcal{A}_{trace}$在可监管匿名认证方案可追踪性模拟攻击游戏中获胜.然而根据定理中对基本组件安全性的假设,我们得到敌手$\mathcal{A}_{trace}$攻击成功概率可以忽略不计,因此方案满足可追踪性.

5 方案对比分析

5.1 功能比较

本文方案相比 IdentiyMixer 方案增加了可监管的功能,CA 可以为群内用户分配密钥,并通过追踪密钥追踪用户的身份.本文方案在用户出示证书的部分增加了群签名技术,验证者在验证证书的同时也验证了用户匿名身份信息的正确性,如果出现争端,CA 可追踪到用户的身份,因此,本文方案具有强制监管的作用.此外,本文方案在增加强制监管功能的同时还保证了用户的匿名性,相比一般的身份监管方案,极大保护了用户的身份隐私.用户在交易时,只需出示相应的属性值,无需出示的属性值可以在证书中进行隐藏,满足了用户的隐私保护需求.但由于增加了可监管机制,本文方案并未实现 Identity Mixer 方案完全匿名性的功能,对第三方仍有一定的信任依赖.

5.2 效率分析

本文方案在 Identity Mixer 方案上增加了可监管的功能,下面对比原方案进行效率方面的比较.

选择椭圆曲线上的群 G_1,G_2,阶数 *p* 为 170bit 的大质数,群内元素的长度为 171bit(相当于 1024bit 的 RSA 方

案),大整数长度设为 170bit,G_T 内元素的长度设为 171bit.定义 E 为指数运算,H 为哈希运算,P 为双线性对运算,k 为全部属性个数,l 为隐藏属性个数.忽略乘法、加法运算,方案计算开销对比结果见表 2.

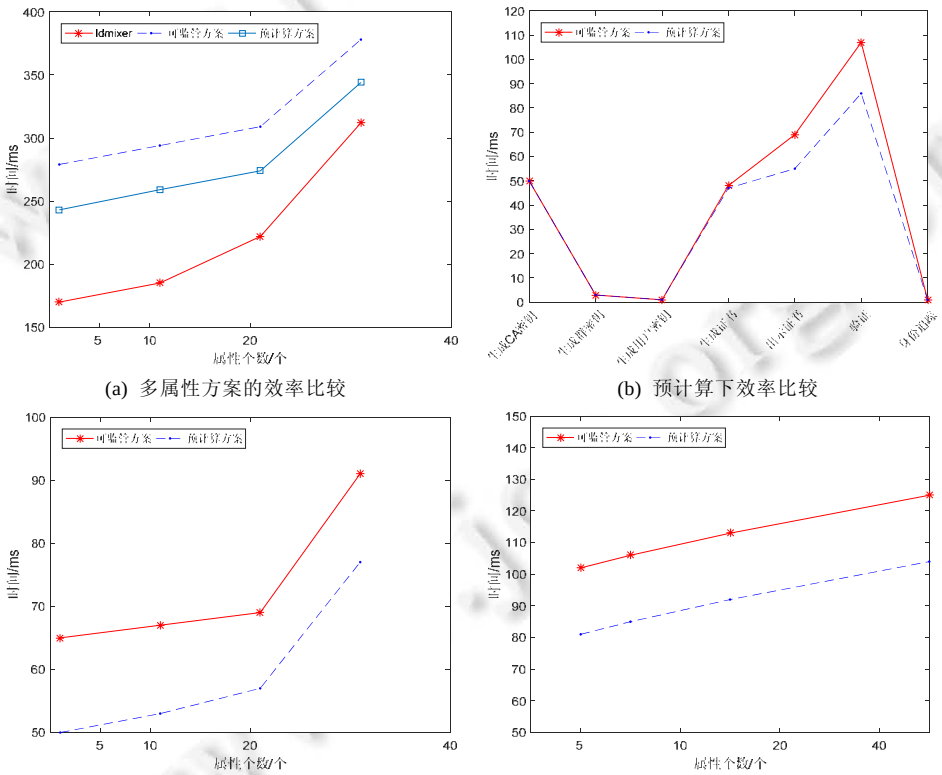
Table 2 Comparison between Identity Mixer scheme and ours in computation cost

表 2 本文方案和 Identity Mixer 方案的计算开销对比

	本文方案			Identity Mixer[12]
生成密钥	发行方 $(k+11)E+2H$	群密钥 $3E$	用户注册 E	$(k+11)E+2H$
证书请求	$4E+H$			$4E+H$
证书请求验证	$3E+H$			$3E+H$
生成证书	$(k+2)E$			$(k+2)E$
出示证书	$(l+26)E+2H+3P$			$(l+14)E+2H$
出示证书验证	$(k+22)E+2H+7P$			$(k+10)E+2H+2P$

由表 1 可知:本文方案由于增加可监管的功能,在出示证书和验证算法较 Identity Mixer 方案计算开销有所增加.在实际应用中,可通过预计算的方法(如提前计算 $e(h,PK)$, $HAttr_i^{attri}$ 等)进一步提高方案效率.经过预计算后,出示证书运行计算量可减少至 $26E+2H+3P$,验证证书计算量可减少至$(k-l+22)E+2H+4P$,整体方案可减少 5 次双线性对运算,k 次指数运算,但需增加$(k+5)\cdot 171$bit 存储量,其中,k 为全部属性的个数.

在 Win10 64 位,Inter(R) Core(TM) i7-7700@3.6GHz,16G 内存 PC 机上对方案进行仿真实现后,效率比对如图 5 所示.



(a) 多属性方案的效率比较

(b) 预计算下效率比较

(c) 出示证书效率比较

(d) 证书验证效率比较

Fig.5 Efficiency analysis of the schemes

图 5 方案效率分析

图 5(a)显示:当设定用户属性个数为 5,10,20,40 时,Identity Mixer 方案、本文方案以及预计算方案的效率随属性增加而降低.采用预计算方法可一定程度提高方案效率,但仍会比 Identity Mixer 方案效率略低.以上结果也验证了理论分析的正确性.图 5(b)显示,本文方案和预计算后的方案在出示证书和验证过程会有差别,即:预计算

只在出示证书和验证过程进行,与理论结论一致.图 5(c)和图 5(d)则进一步说明:只有出示证书部分和验证部分会随属性值增加而增加,方案其他过程效率与属性个数无关.通过方案对比分析,本文方案的效率相比 Identity Mixer 方案虽有一定程度的下降,但仍属于可接受的范围(整个方案耗时不足 0.5s),且存在提升的空间,具有较好的实用性.

方案的存储开销对比见表 3.由表 3 可知:由于可监管功能,方案在私钥长度和签名长度上相比 Identity Mixer 方案略有增加,但仍属于可接受的范围.

Table 3 Comparison between Identity Mixer scheme and ours in storage cost

表 3 本文方案和 Identity Mixer 方案的存储开销对比

	本文方案	Identity Mixer[11]
CA 私钥长度(bit)	510	170
用户私钥长度(bit)	513	170
公钥长度(bit)	$(k+5)\cdot 171+853$	$(k+5)\cdot 171+340$
证书长度(bit)	682	682
出示证书长度(bit)	$170l+3407$	$170l+2044$

综上所述,本文方案在增加可监管功能的同时,保证了良好的运行效率和存储性能,具有较好的功能性和实用性.

6 方案应用

随着网络的日益发达,金融、医疗、政务等领域的各种网络应用层出不穷,各种各样的系统和复杂的网络环境使得用户在进行身份认证时消耗成本和信任代价过高;同时,中心式的信任模型还存在泄露用户信息的风险,因此,急需采用新技术手段解决传统身份认证方法的不足.

针对以上问题,本文结合可监管匿名认证方案和区块链技术,设计了一种基于区块链的统一身份认证系统,旨在为用户和服务方提供统一身份认证、身份隐私保护和可监管的服务,系统模型如图 6 所示.

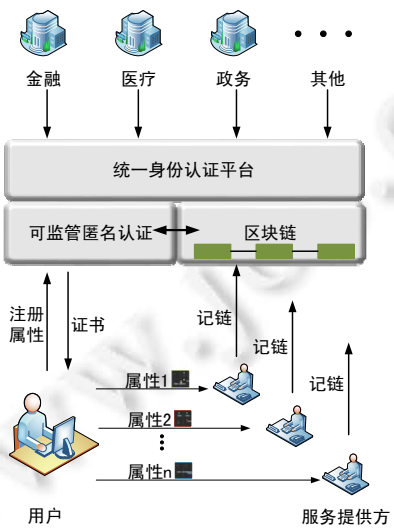


Fig.6 Model of unified identity authentication system

图 6 统一身份认证系统模型

系统由统一认证平台模块、服务提供方、用户等组成,而统一认证平台又分为可监管匿名认证模块和区块链模块.统一认证平台连接服务提供方,为用户提供认证服务.可监管匿名认证模块为用户颁发属性证书,提供属性证明,用户出示证书时只需出示部分属性,无需出示全部属性,可有效保护用户的身份隐私.区块链模块则

记录了用户出示的匿名证书和相关属性信息,可监管匿名认证模块可通过区块链查阅用户出示的属性信息,若出现争端,还可根据匿名证书恢复出用户的身份信息.

7 结 论

本文提出了一种可监管匿名认证方案,方案结合了匿名认证技术、群签名和零知识证明技术,在传统认证手段中引入了监管机制,使CA能够对匿名证书进行身份追踪.一方面,本方案解决了传统认证体制中用户身份、属性信息过度暴露的问题,采用匿名认证的技术手段保护用户的身份隐私,同时采用灵活的认证策略,使用户可以选择出示证书中的属性,避免过度暴露信息;另一方面,本文方案还解决了目前匿名认证手段无法监管的问题,旨在减少匿名滥用和失信行为的发生.结合可监管匿名认证技术和区块链技术,本文提出了统一身份认证系统模型,但未针对实际系统设计具体方案.此外,本文方案的效率还存在可提升的空间.因此,下一步工作是进一步提高方案的效率,拓展方案的应用范围,根据实际系统需求设计具体方案,使方案落实到具体应用上.

References:

[1] I'Anson C, Mitchell CJ. Security defects in CCITT recommendation X.509: The directory authentication framework. ACM SIGCOMM Computer Communication Review, 1990,20(2):30−34. [doi: 10.1145378570.378623]

[2] Lyons-Burke K. Federal agency use of public key technology for digital signatures and authentication. ADA393324. 2000.

[3] Weinshall D. Cognitive authentication schemes safe against spyware (short paper). In: Proc. of the IEEE Symp. on Security and Privacy. IEEE Computer Society, 2006. 295−300. [doi: 10.1109/SP.2006.10]

[4] Tsai CS, Lee CC, Hwang MS. Password authentication schemes: Current status and key issues. Int'l Journal of Network Security, 2006,3(2):101−115.

[5] Tian XJ, Zhu RW, Wong DS. Improved efficient remote user authentication schemes. Int'l Journal of Network Security, 2007,4(2):149−154. [doi: 10.6633/IJNS.200703.4(2).04]

[6] Camenisch J, Lysyanskaya A. Signature schemes and anonymous credentials from bilinear maps. In: Proc. of the Crypto 2004. 2004. 56−72. [doi: 10.1007/978-3-540-28628-8_4]

[7] Dan B, Boyen X, Shacham H. Short group signatures. In: Proc. of the Advances in Cryptology—CRYPTO 2004. Berlin, Heidelberg: Springer-Verlag, 2004. 41−55. [doi: 10.1007/978-3-540-28628-8_3]

[8] Man HA, Susilo W, Yi M, Sherman SMC. Constant-Size dynamic *k*-times anonymous authentication. IEEE Systems Journal, 2013, 7(2):249−261. [doi: 10.1109/JSYST.2012.2221931]

[9] Camenisch J, Dubovitskaya M, Robert RE. Concepts and languages for privacy-preserving attribute-based authentication. Journal of Information Security and Applications, 2014,19(1):25−44. [doi: 10.1016/j.jisa.2014.03.004]

[10] Camenisch J, Drijvers M, Lehmann A. Anonymous attestation using the strong diffie hellman assumption revisited. In: Proc. of the Int'l Conf. on Trust and Trustworthy Computing. Springer Int'l Publishing, 2016. 1−20. [doi: 10.1007/978-3-319-45572-3_1]

[11] Camenisch J. Specification of the Identity Mixer Cryptographic Library, Version 2.3.1. 2010. 1−49.

[12] Camenisch J, Lysyanskaya A. A signature scheme with efficient protocols. In: Proc. of the Int'l Conf. on Security in Communication Networks. Berlin, Heidelberg: Springer-Verlag, 2002. 268−289. [doi: 10.1007/3-540-36413-7_20]

[13] Wang ZH, Han Z, Liu JQ, Zhang DW, Chang L. ID authentication scheme based on PTPM and certificateless public key cryptography in cloud environment. Ruan Jian Xue Bao/Journal of Software, 2016,27(6):1523−1537 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/4992.htm [doi: 10.13328/j.cnki.jos.004992]

[14] Wang D, Li WT, Wang P. Crytanalysis of Three Anonymous Authentication Schemes for Multi-Server Environment. Ruan Jian Xue Bao/Journal of Software, 2018,29(7):1937−1952 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/5361.htm [doi: 10.13328/j.cnki.jos.005361]

[15] Chaum D, Van Heyst E. Group signatures. In: Proc. of the Advances in Cryptology—EUROCRYPT'91. LNCS 547, Springer-Verlag, 1991. 257−265. [doi: 10.1007/3-540-46416-6_22]

[16] Bellare M, Micciancio D, Warinschi B. Foundations of group signatures: Formal definitions, simplified requirements, and a construction based on general assumptions. In: Proc. of the Advances in Cryptology—EUROCRYPT 2003. Warsaw, 2003. 614–629. [doi: 10.1007/3-540-39200-9_38]

[17] Goldwasser S, Micali S, Rackoff C. The knowledge complexity of interactive proof systems. In: Proc. of the 17th ACM Symp. on Theory of Computing. 1985. 291–304. [doi: 10.1145/22145.22178]

[18] Fiat A, Shamir A. How to prove yourself: Practical solutions to identification and signature problems. In: Proc. of the Conf. on the Theory and Application of Cryptographic Techniques. Berlin, Heidelberg: Springer-Verlag, 1986. 186–194. [doi: 10.1007/3-540-47721-7_12]

附中文参考文献:

[13] 王中华,韩臻,刘吉强,张大伟,常亮.云环境下基于 PTPM 和无证书公钥的身份认证方案.软件学报,2016,27(6):1523−1537. http://www.jos.org.cn/1000-9825/4992.htm [doi: 10.13328/j.cnki.jos.004992]

[14] 汪定,李文婷,王平.对三个多服务器环境下匿名认证协议的分析.软件学报,2018,29(7):1937−1952. http://www.jos.org.cn/1000-9825/5361.htm [doi: 10.13328/j.cnki.jos.005361]

王震(1992－),男,河南洛阳人,工程师,主要研究领域为信息安全,区块链,密码学.

安红章(1981－),男,高级工程师,CCF 专业会员,主要研究领域为信息安全,区块链.

范佳(1982－),女,博士,高级工程师,主要研究领域为信息安全,密码学,区块链.

郑海彬(1989－),女,博士,主要研究领域为密码学应用,区块链的隐私保护.

成林(1983－),男,博士,助理研究员,主要研究领域为密码学,云计算,大数据.

牛俊翔(1996－),男,硕士,主要研究领域为区块链开发,智能合约.