群智网络中基于区块链的有序聚合签名认证方案

杨坤伟,杨 波,周彦伟
(陕西师范大学计算机科学学院,陕西西安 710062)

摘 要: 传统的中心化认证机制存在单点故障和证书签发不透明等问题,难以适用具有高度自治性和动态多变性的群智网络,因此本文提出了一个基于区块链的轻量级认证机制和一个有序聚合签名方案,二者结合实现了点对点的去中心认证. 在认证机制中,区块链作为一个去中心化的底层存储数据库,用来记录密钥、证书、签名和所有其他相关信息,通过对用户节点的公钥证书进行有序签名可以证明其身份的真实性,同时形成一条具有公信力的证书链. 针对现有有序聚合签名方案公钥长度较长、验证效率低下的问题,基于BLS签名提出了一个新的有序聚合签名方案,并在有序聚合认证密钥模型下证明了方案的不可伪造性,分析了该方案所具有的公开验证性等安全属性. 与现有方案相比较,本文方案的公钥和签名长度更短,且签名长度与用户数无关,更适用于带宽较低的群智网络环境.

关键词: 群智网络; 有序聚合签名; 区块链; 公开验证; 身份认证
中图分类号: TP309 **文献标识码:** A **文章编号:** 0372-2112(2022)02-0358-08
电子学报URL:http://www.ejournal.org.cn **DOI:**10.12263/DZXB.20200905

A Sequential Aggregate Signature Authentication Scheme Based on Blockchain for Crowdsensing System

YANG Kun-wei, YANG Bo, ZHOU Yan-wei
(*School of Computer Science, Shaanxi Normal University, Xi'an, Shaanxi* 710062, *China*)

Abstract: Due to the single point failure and opacity of certificate issuance in traditional centralized authentication mechanism, it is difficult to apply to crowdsensing system with high autonomy and dynamic variability. In order to solve this problem, a lightweight authentication mechanism based on blockchain and a new sequential aggregate signature scheme is proposed in this paper. The combination of the two can implements a peer-to-peer de-centralization authentication. In our authentication mechanism, the blockchain acts as a de-centralized underlying storage database for recording keys, certificates, signatures and all other related information. Users can prove the authenticity of their identity with the sequential aggregate signature in the public key certificates of other nodes and establish creditable certificate chains. To solve the problem of long public key length and low verification efficiency in the existing sequential aggregate signature scheme, a new scheme for sequential aggregate signature is proposed based on BLS short signature scheme and its unforgeability is proven under the sequential aggregate certified-key model. This paper also discusses such security properties of the schemes as public verifiability. Compared with other existing sequential aggregate signature schemes in the computationally complexity, the new scheme is more acceptable to the low bandwidth environment of crowdsensing system in that the length of public key and signature is independent of the number of users.

Key words: crowdsensing system; sequential aggregate signatures; blockchain technology; public verifiability; authentication mechanism

1 引言

随着共享经济的不断发展,群体智能已经在各行各业中得到深度应用,目前已经引起了学术界和产业界的广泛关注.《中国人工智能2.0发展战略研究》[1]定义了群体智能的概念:通过吸引、汇聚和管理大规模参与者,以竞争和合作等多种自主协同方式来共同应对

收稿日期:2020-08-18;修回日期:2021-03-02;责任编辑:孙瑶
基金项目:国家重点研发计划(No.2017YFB0802000);国家自然科学基金(No.U2001205,No.61772326,No.61802241,No.61802242);"十三五"国家密码发展基金(No.MMJJ20180217);中央高校基本科研业务费(No.GK202003079,No.GK202007033,No.2020TS087)

挑战性任务,特别是开放环境下的复杂系统决策任务,涌现出来的超越个体智力的智能形态. 群智网络任务管理从角色构成上可以分为管理平台、任务发布者和任务执行者三元模型,从逻辑上可以自上而下分为应用层、网络层和终端层,如图1所示. 应用层提供众包任务的用户管理、任务发布和任务回收等功能. 网络层主要提供众包任务的网络通信,包括(移动)互联网、物联网、无线传感网和无线自组织网等形态. 终端层作为感知数据的来源,通过各类智能设备或传感器收集与众包任务相关的数据并上传.

图1　群智网络逻辑分层

在群体智能各类应用中,身份认证是不可缺少的重要环节,成为保护用户数据安全的重要屏障. 公钥基础设施(Public Key Infrastructure,PKI)作为网络安全建设的基础与核心,提供密钥和数字证书[2]管理服务. 然而,集中式的PKI机制在群智网络环境中面临CA(Certification Authority)不可信、被攻击、单点故障以及证书签发不透明等问题,使得传统的集中式PKI机制已经难以适应规模日益庞大和复杂的网络环境.

针对上述问题,研究人员开始将目光投向基于区块链的身份认证技术[3~12],考虑利用区块链中数据不可篡改和分布式存储等特点优化传统的PKI体制,实现去中心化的身份认证. 文献[6]提出了基于区块链技术的分布式证书管理模型Certcoin,利用区块链记录用户证书,通过将用户身份与证书公钥相关联并定义挑战-应答机制,实现了PKI体制的去中心化. 模型中,去中心化的证书签发与记录机制避免了CA的单点故障问题和证书签发过程不透明的问题,对于女巫攻击有更强的抵抗性. 文献[8]针对传统PKI系统的中心化和不透明性提出了一个替代方案(Smart Contract-based PKI,SCPKI),该方案是基于分布式网络模型和区块链上的智能合约设计的,其具有运行公钥基础设施和身份管理的功能,机制中公钥和标识属性存储在区块链上,由智能合约管理,以便在发布恶意证书时很容易被检测出来. 文献[9]针对现有交互频繁的信息服务信任域之间不能实现安全、高效的跨域认证的问题,提出了一种基于区块链的跨异构域认证方案,在基于身份的密码体制(Identity-Based Cryptography,IBC)内设置区块链域代理服务器参与密钥生成,并与PKI域区块链证书服务器等构成联盟链模型,利用区块链去中心化、数据不易篡改等优点保证模型内第三方服务器的可信性.

然而,上述基于区块链的分布式身份认证方案均没有考虑现实签名认证应用中多用户或多机构对消息签名的情况,忽略了认证过程中大量签名信息会增加网络传输带宽和区块链存储空间等问题.

解决这些问题的一个有效办法是,在基于区块链的身份认证过程中引入有序聚合签名技术,将任意多个签名压缩为一个签名,将任意多个签名的验证简化为一次验证. 使用有序聚合签名来代替多个单一签名会节省大量存储空间,大幅减少验证时间,可以为多用户提供不可否认性,对许多应用都有良好的支撑作用,具有广阔的应用前景. 在Eurocrypt 2004上,Lysyanskaya等人[10]基于RSA提出了第一个有序聚合签名方案,每一个签名者在一个有序的聚合签名中加入一个自己所选择的消息签名,形成一个新的有序聚合签名,有序聚合签名的结构有层次性,像洋葱一样,即第一个签名是在聚合的最里面,后续签名向外依次延伸,这种结构很好地反映了签名的顺序特性,并且签名长度与普通签名长度相同. Lu等人[11]在Eurocrypt 2006上基于Waters的签名方案提出了一个标准模型下的有序聚合签名方案,该方案不要求签名者知道签名消息的顺序,并且聚合签名长度更短、验证效率更快,方案的安全性基于有序聚合认证密钥模型,在该模型中,敌手需掌握所选择的公钥序列对应的私钥. 2011年,Schrder[13]通过对Lysyanskaya签名方案的改进,提出了一个新的有序聚合签名方案,具有密钥长度短的优势,其中公钥为两个群元素. 2015年,Lee等人[14]在标准模型下基于静态假设提出了一个有序聚合签名方案,该方案中公钥元素为常数,签名和验证算法只需要进行常数次对运算. 同年,赵慧艳等人[15]为了应对聚合签名中的密钥泄露问题,将并行密钥隔离机制扩展到聚合签名系统中,给出了并行密钥隔离聚合签名的概念,同时提出了第一个并行密钥隔离聚合签名方案,并在随机预言模型下证明了方案的安全性,但是方案不具备有序性.

由于现有有序聚合签名方案的签名长度和公钥长度较长,签名验证效率较低,不适用于基于区块链的轻量级身份认证,因此本文基于BLS签名[16]提出了一个新的有序聚合签名方案,方案在效率方面有所提升,更

适用于具有高度自治性、多样性及涌现性特点的群智网络. 同时,利用区块链的不可篡改和去中心化的特点以及信任网络(web of trust, wot)[17]的分布式认证思想,提出一个基于区块链的轻量级身份认证模型,实现端对端的去中心认证. 将有序聚合签名嵌入到基于区块链的身份认证机制中,能有效满足多人签名认证和证书追加签名等需求,在实际应用中具有独特优势.

2 基础知识

2.1 双线性映射

设 G_1 和 G_2 是阶为大素数 p 的乘法群,映射 $e: G_1 \times G_1 \to G_2$ 是一个双线性映射,e 满足以下性质.

(1)双线性:如果对于任意的 $P, Q \in G_1$ 和任意的 $a, b \in Z$,都有 $e(aP, bQ)=e(P, Q)^{ab}$,就说 $e: G_1 \times G_1 \to G_2$ 是双线性的.

(2)非退化性:这个映射不会将 $G_1 \times G_1$ 中的所有对映射为 G_2 的单位元,因为 G_1, G_2 同为素数阶群,这意味着如果 P 是 G_1 的单位元,那么 $e(P, P)$ 是 G_2 的单位元.

(3)可计算性:对于任意的 $P, Q \in G_1$,都有有效的算法来计算 $e(P, Q)$.

2.2 BLS签名方案

BLS签名方案的安全性基于乘法群上的CDH问题的困难性假设[16]. 方案包含密钥生成算法、签名算法和验证算法,采用了一个全域哈希函数 $h: \{0,1\}^* \to G^*$,具体算法如下所述.

(1)密钥生成算法:选择一个随机数 $x \in Z_p$,计算 $y=g^x \in G$,私钥为 $\mathrm{SK}=x$,公钥为 $\mathrm{PK}=y$.

(2)签名算法:对于消息 $M \in \{0,1\}^*$,计算 $h=H(M)$,输出签名 $\sigma=h^x \in G$.

(3)验证算法:输入消息 M 和签名 σ,如果 (g, h, y, σ) 为一个有效的CDH四元组,就返回1,否则输出0.

2.3 有序聚合签名

一个有序聚合签名方案包括密钥生成算法、有序聚合签名算法、聚合验证算法. 与普通聚合签名不同,有序聚合签名算法输入不仅包括签名所需的私钥和对应的待签名消息,而且还包含一个截至当前时点,基于 $\ell-1$ 个签名者对 $\ell-1$ 个对应消息的聚合签名 σ,算法将新的签名添加进 σ 中,产生一个新的基于 ℓ 个签名者对 ℓ 个对应消息的聚合签名 σ^*. 聚合验证算法,输入一个聚合签名和对应的公钥序列和消息序列,验证聚合签名是否有效,算法具体过程如图2所示.

2.4 安全模型

本文基于文献[11]提出的有序聚合认证密钥模型(the sequential Aggregate certified-key model),挑战者B给定敌手A一个随机选择的挑战公钥,敌手A有选择除了挑战公钥对应私钥外的所有密钥和访问有序聚合签名谕言机的能力. 与传统的聚合签名模型不同,该模型中增加了密钥认证询问环节,要求敌手证明在询问签名谕言机和伪造过程中使用的非挑战公钥是正确生成的. 敌手A需要提交相关非挑战密钥对给挑战者B,B即可构造除挑战密钥外的有序聚合签名. 敌手的目标是存在性伪造一个包含挑战密钥的有序聚合签名,敌手的优势 $\mathrm{Adv}_{\mathrm{A}}$ 被定义为在下面游戏中获胜的概率.

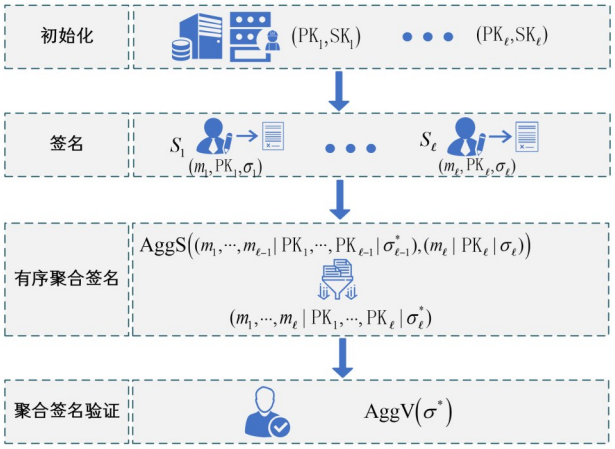


图2 有序聚合签名

初始化:挑战者B新建一个公钥认证列表 $C \leftarrow \phi$,随机生成一对密钥 $(\mathrm{PK}, \mathrm{SK})$,将挑战公钥PK给定敌手A.

认证询问:敌手A提交密钥对 $(\mathrm{PK}', \mathrm{SK}')$ 以证明公钥PK′的有效性,如果PK′是对应SK′的有效公钥,挑战者B将PK′添加至列表 C 中.

聚合签名询问:敌手A适应性地基于挑战公钥PK和其选择的消息 M 进行有序聚合签名询问,同时提供一个基于一系列消息 $\boldsymbol{M}=(M_1, M_2, \cdots, M_{i-1})$ 和对应公钥 $\mathbf{PK}=(\mathrm{PK}_1, \mathrm{PK}_2, \cdots, \mathrm{PK}_{i-1})$ 的有序聚合签名 σ. 首先,算法检查签名 σ 的有效性,其中对应的每一个公钥 $\mathrm{PK}_i \in C$,挑战公钥PK不在公钥序列 **PK** 中,如果以上都成立,则输出一个由谕言机产生的新的签名 $\sigma'=(\mathrm{SK}, M, S, \boldsymbol{M}, \mathbf{PK})$.

伪造:敌手A输出 i 个不同的公钥 **PK**,这里的 i 至多为 n,并且这里的公钥长度可以与询问阶段的公钥长度不相等,但是其中必须要包含挑战公钥PK,A同时输出与公钥序列对应的消息序列 $\boldsymbol{M}$ 和一个基于这 i 个用户的有序的聚合签名 σ,不失一般性,将 PK_1 视为最里层的公钥.

敌手A获胜,当且仅当该有序聚合签名 σ 是一个对应于消息序列 $\boldsymbol{M}$ 和公钥序列 **PK** 的有效的有序聚合签名,并且 σ 是非平凡的,即在伪造过程中用到的挑战公钥PK必须出现在 **PK** 序列中,对应的签名消息 M 必须

在签名询问过程中没有被询问过,基于挑战公钥的签名可以在有序聚合签名的任何位置.

如果不存在t时间的敌手发起q_C次认证询问和q_S次签名询问后以超过ε的优势赢得以上游戏,则称有序聚合签名方案是$(t,q_C,q_S,n,\varepsilon)$安全的,其中$n$表示聚合签名的长度上界.

3　基于区块链的认证管理机制

3.1　基于区块链认证管理的事务结构

基于区块链的认证机制是对系统内注册用户的身份合法性进行鉴别,验证用户身份信息和公钥信息是否一致、有效的一个过程. 基本思想是在区块链网络中,允许用户实体自主管理身份信息、创建自身公钥信息和签名他人的公钥信息,通过有序聚合签名合约可以将任意多个用户签名按顺序压缩为一个聚合签名,并存储于区块链中. 当需要对某一用户的公钥和其身份进行验证的时候,仅需对单一的聚合签名进行验证即可达到对所有用户签名的验证的效果. 在本文的认证机制中,以区块链中事务的形式来进行身份认证管理,下面对认证机制中的模块进行静态描述.

用户:表示群智网络中所有参与认证的人、自组织或者智能体,是区块链中相关数据的拥有者,可以发起针对各类事务的请求,如签名事务、撤销事务等.

钱包:作为基于区块链认证的管理端,由公钥进行标识,为用户提供密钥生成服务、证书生成和管理服务、单证书的签名服务以及认证相关事务创建,利用钱包可以将事务发布至区块链或从区块链上检索相关事务.

地址:是用户公钥的哈希值,拥有相应私钥的用户拥有该地址,使用地址来标识机制中的所有用户. 地址在区块链网络中是公开共享的,可用于注册证书和请求认证.

数据区块:是区块链网络中的底层数据结构,由区块头和区块体组成,区块头封装了前一个区块的地址、当前区块的目标哈希值、当前区块的共识随机数、Merkle根、时间戳等信息. 区块体存储着区块创建过程中的所有认证事务数据,区块之间按时间顺序形成固定的链式结构. 由于区块头中包含了区块体的Merkle根和前一个区块的哈希值,因此通过哈希运算即可验证该区块直至创世区块的所有区块是否被篡改.

事务数据:是基于区块链的身份认证集中存储实际操作的相关数据,通过智能合约事务来管理证书、公钥、认证签名的发布、聚合签名的生成以及证书或者签名的撤销.

P2P网络:网络中每个节点处于对等的地位,既是资源和服务的使用者又是提供者,没有主、从之分,整个网络中不存在中心节点,每个节点都可对任意对等节点做出响应,提供计算资源、存储资源等.

智能合约:存储在区块链上的脚本程序,能够在网络节点上自动运行. 作为区块链2.0的核心特性,智能合约可以在去中心的环境下自动按照程序设定规则完成一系列安全、可信、公开的操作.

3.2　基于区块链的身份认证框架和工作流程

本文考虑群智网络中终端节点物理位置、节点身份、环境属性等因素的影响,提出一个高效的适用于群智网络的认证机制. 机制将区块链作为一个去中心化的认证数据库,利用其分布式及链式结构存储事务数据,节点通过发布身份和公钥的绑定信息实现证书的生成,将密钥校验机制、身份认证机制和密钥撤销机制都写入智能合约,由合约自主判定完成,具体过程如图3所示.

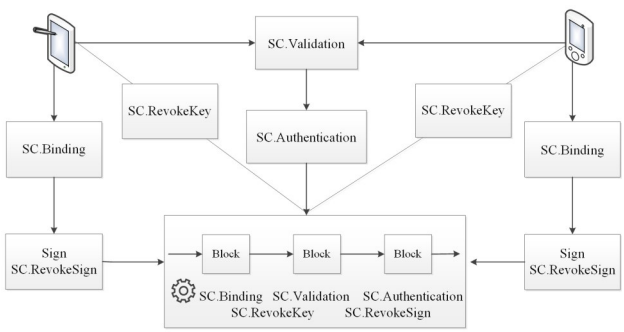


图3　基于区块链的身份认证机制

本文以区块链中的事务为载体对身份认证进行管理. 认证机制管理中包括证书信息管理和签名信息管理,分别以证书类事务和签名类事务的形式发布至区块链中. 证书信息由节点自身通过绑定身份属性信息和公钥信息产生,证书被发布到区块链后,可以进行更新、签名、撤销等操作,其历史操作记录都会被区块链永久保存,以便于审计和追溯. 交易事务中仅包含事务标识符、公钥信息、身份属性信息和签名信息,并没有包含占用存储资源很多的其他信息. 同时,提出使用有序聚合签名方案来提高认证管理机制中签名验证效率,节省传输带宽和存储空间. 表1描述了认证机制中的相关符号.

Step1(密钥生成)　终端节点通过自身的区块链钱包生成密钥对(PK,SK),对外公布公钥PK,私钥SK秘密保存. 节点可以通过公钥的身份属性,遍历整个区块链去检索公钥.

Step2(身份绑定)　首先,由SC.Validation验证合约校验公钥格式的正确性. 验证内容有格式标准、密钥长度、密钥期限、是否撤销等. 当公钥格式验证通过之后便可以调用身份绑定合约(SC.Binding)将节点的相

表1 符号描述

符号	描述
ID	表示事务标识符
Attributes	节点身份属性信息
PK	节点公钥
SK	节点私钥
T_x	事务信息
Timestamp	时间戳
σ	签名信息
Cert	公钥证书

关身份属性信息Attributes与公钥PK绑定,建立节点PK和Attributes的绑定关系证书Cert,并将Cert发布至区块链中保存,具体过程见算法1.

算法1 身份绑定

输入:

- ID_B: 当前证书事务标识符.
- PK_B: 证书节点自身公钥.
- SK_B: 证书节点自身私钥.
- Attributes: 证书节点身份属性信息.

具体过程:

1. 调用验证合约SC.Validation校验公钥PK_B格式的正确性.
2. 建立节点PK_B和Attributes的绑定关系,生成证书Cert.

$$Cert=(PK_B, Attributes, Timestamp)$$

3. 对证书进行签名,得到$\sigma=Sign_{SK_B}(Cert)$.
4. 通过证书事务发布至区块链

$$T_x=(ID_B, Cert, \sigma).$$

输出:证书事务T_x.

Step3(证书签名) 允许满足证书签名条件的可信节点对其信任的节点证书进行签名操作,并将签名结果上传至区块链中,从而向其他节点证明自己对该证书中公钥有效性的认可. 同时,节点可以通过调用密钥撤销合约SC.RevokeSign对自身的签名进行撤销.

Step4(聚合签名) 考虑在实际应用中存在多用户对证书的认证签名的情况,使用有序聚合签名技术将多个认证签名压缩为一个签名,实现签名压缩,减小签名的存储空间. 聚合签名的长度与用户数无关,更适用于带宽较低的网络环境,具体过程见算法2.

Step5(身份认证) 节点通过调用身份认证合约SC.Authentication验证聚合签名,从而判断验证节点公钥证书的有效性,具体过程见算法3.

认证机制允许节点在区块链中发布签名撤销证书来撤销自己的签名,同时节点可以通过调用密钥撤销合约SC.RevokeKey对自身的公钥进行撤销. 秘钥撤销分为节点主动撤销和过期撤销两种模式:主动撤销是通过调用密钥撤销合约,节点向区块链中发送密钥撤销证书,实现密钥撤销;过期撤销则根据密钥的时间戳

算法2 聚合签名

输入:

- ID_S: 当前签名事务标识符.
- PK_i: 签名节点自身公钥.
- $Cert_i$: 签名节点所签证书.
- σ_i: 节点对证书的签名.

具体过程:

1. 通过区块链获取到相关签名元组$(PK_i, Cert_i, \sigma_i)$.
2. 通过有序聚合签名算法AggS(·)计算得到聚合签名σ^*.

$$\sigma^*=AggS(PK_1, PK_2, \cdots, PK_\ell, Cert_1, Cert_2, \cdots, Cert_\ell, \sigma_1, \sigma_2, \cdots, \sigma_\ell)$$

3. 通过签名事务发布至区块链

$$T_x=(ID_S, \sigma^*, Timestamp).$$

输出:签名事务T_x.

算法3 身份认证

输入:

- σ^*: 聚合签名.
- PK_i: 任意签名节点公钥.

具体过程:

1. 通过区块链获取到相关证书的聚合签名σ^*.
2. 通过调用身份认证合约SC.Authentication的聚合验证算法AggV判定证书签名的有效性.

输出: AggV验证通过输出1,否则输出0.

设定密钥的有效期,到期后自动撤销. 区块链作为一个去中心化的底层存储数据库,用于记录公钥、证书、签名等相关信息. 利用区块链,用户拥有对自己身份的自主控制.

4 有序聚合签名方案

4.1 方案介绍

为了能够提高基于区块链的认证管理机制中的签名验证效率,节省传输带宽和存储空间,本文基于BLS签名方案提出了一个新的有序聚合签名方案. 方案中签名由两个群元素组成,分别记为S_1和S_2,其中S_2是对签名方案中随机数的承诺,当一个签名者想要在一个有序聚合签名(S_1, S_2)中添加他对某个消息的签名时,他需要将自己计算的部分签名与S_1相乘,同时更新计算的随机数. 方案中选择阶为素数$q(q>2^k)$并且k为安全参数的循环群G,g为群G的一个生成元,用t来表示时间戳,方案采用了一个抗碰撞的哈希函数$H_1:\{0,1\}^*\times\{0,1\}^*\rightarrow G$.

密钥生成算法:算法随机选择$x\in Z_q^*$,计算$U=g^x$,用户的公钥$PK=U$,私钥$SK=x$.

聚合签名算法:用户输入私钥SK和一个待签名的消息$M^*\in\{0,1\}^*$,同时输入一个现有的基于消息序列$\boldsymbol{M}=(M_1, M_2, \cdots, M_i)$和对应公钥序列$\boldsymbol{PK}=(PK_1, PK_2, \cdots, PK_i)$的有序聚合签名$\sigma'=(S_1', S_2')$,算法首

先利用下面的聚合验证算法验证签名σ'的有效性. 如果签名验证无效,则算法终止并退出. 如果签名验证有效,假设$|\mathbf{PK}|=|\boldsymbol{M}|=\ell$,对于每一个$i(1\leqslant i\leqslant \ell)$,$M_{[i]}$与$\mathrm{PK}_{[i]}$相对应,其中$\mathrm{PK}_{[i]}=U_i=g^{x_i}\in G$,算法首先计算$h_{\ell+1}=H_1(M^*,t)$,然后计算$w_1=S_1'\cdot h_{\ell+1}^{x}\cdot(S_2')^{x}$和$w_2=S_2'$,其中有序聚合签名元组$S_1'=\prod_{i=1}^{\ell}h_i^{x_i}\cdot\left(\prod_{i=1}^{\ell}U_i\right)^{r}$,$S_2'=g^{r}$.

计算结果(w_1,w_2)是消息$\boldsymbol{M}/\!/M^*$基于公钥$\mathbf{PK}/\!/\mathrm{PK}$的一个有效签名,其中$w_2=S_2'=g^{r}$,但是签名需要重新增加随机性,选择一个随机的$r'\in Z_q^*$计算$S_1=w_1\cdot\left(\prod_{i=1}^{\ell+1}U_i\right)^{r'}=\prod_{i=1}^{\ell+1}h_i^{x_i}\cdot\left(\prod_{i=1}^{\ell+1}U_i\right)^{r'+r}$和$S_2=w_2\cdot g^{r'}=g^{r'+r}$,这里的$x_{\ell+1}$即当前用户私钥.

显然,$\sigma=(S_1,S_2)$是一个基于消息序列$\boldsymbol{M}/\!/M^*$,对应公钥$\mathbf{PK}/\!/\mathrm{PK}$和随机数$r+r'$的一个有效的有序聚合签名,算法输出$\sigma=(S_1,S_2)$.

聚合签名验证算法:输入一个公钥序列**PK**、消息序列$\boldsymbol{M}$以及一个对应的有序聚合签名$\sigma=(S_1,S_2)$. 如果任意一个公钥在**PK**中出现了两次,或者任意一个**PK**中的公钥没有被验证,又或者$|\mathbf{PK}|\neq|\boldsymbol{M}|$,则输出无效并且终止. 否则,设$|\mathbf{PK}|=\ell$,当$\ell=0$,则输出有效,其中$S_1=S_2=1$. 当$1\leqslant i\leqslant\ell$,验证等式$e(S_1,g)\cdot e\left(S_2,\prod_{i=1}^{\ell+1}U_i\right)^{-1}=\prod_{i=1}^{\ell+1}e(h_i,U_i)$是否成立,如果等式成立则输出有效,否则输出无效.

4.2　安全性证明

定理1　本文有序聚合签名方案是$(t,q_C,q_S,n,\varepsilon)$不可伪造的,当且仅当BLS签名方案是$(t',q',\varepsilon')$不可伪造的,其中$t'=t+O(q_C+nq_S+n),q'=q_S,\varepsilon'=\varepsilon$.

证明　本文的安全性证明基于文献[11]提出的有序聚合认证密钥模型,与传统的聚合签名模型不同,该模型中增加了密钥认证询问环节,要求敌手证明在签名询问和伪造过程中使用的非挑战公钥是正确生成的. 敌手A需要提交相关非挑战密钥对给挑战者B,B即可构造除挑战密钥外的有序聚合签名. 敌手A的目标是存在性地伪造一个包含挑战密钥的有序聚合签名.　证毕

假设存在一个敌手A成功伪造聚合签名的优势为ε,构造一个挑战者B,通过调用敌手A的能力来伪造BLS签名. 给定挑战BLS签名的公钥$\mathrm{PK}^*=U^*=g^{x^*}$,挑战者B与敌手A的交互过程如图4所示.

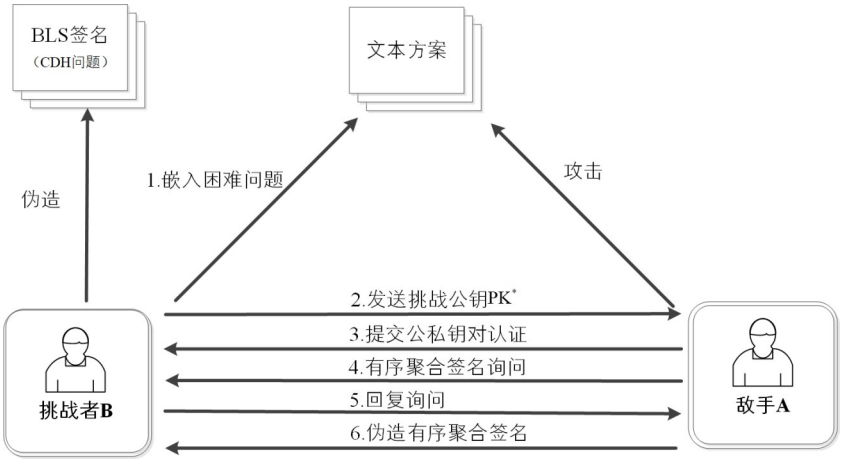


图4　方案的安全性证明思路

初始化:挑战者B新建一个公钥认证列表$C\leftarrow\phi$,并将挑战公钥PK^*发送给敌手A.

认证询问:敌手A提交一系列公钥进行认证,为了证明这些公钥的有效性,A同时提交这些公钥对应的私钥,挑战者B检查公私钥对的有效性,如果有效,则将密钥对记录在列表C中.

聚合签名询问:敌手A基于挑战公钥PK^*和其选择的消息M进行有序聚合签名询问,同时提供一个基于消息序列$\boldsymbol{M}$和对应的公钥序列**PK**的有序聚合签名σ'. 首先,挑战者B检查签名σ'的有效性,确保其中对应的每一个公钥$\mathrm{PK}_i\in C$,并且PK^*不在公钥序列**PK**中,$|\mathbf{PK}|<n$. 如果上述任何情况不成立,则B返回失败;否则,B询问自己的签名谕言机得到消息M基于公钥PK^*的一个签名σ,随后,B利用本文的有序聚合签名算法把基于**PK**和$\boldsymbol{M}$的有序聚合签名σ'添加至σ中. 这是因为B掌握密钥认证列表C,即知道每一个非挑战公钥**PK**[i]对应的私钥. 所以,输出结果是一个基于$\boldsymbol{M}/\!/M$和对应公钥$\mathbf{PK}/\!/\mathrm{PK}^*$的有序聚合签名.

伪造:A输出一个基于新的消息序列$\boldsymbol{M}$和对应公钥序列**PK**的伪造有序聚合签名$\sigma^*=(S_1^*,S_2^*)$,该伪造必

须是非平凡的，即挑战公钥 PK^* 必须出现在 **PK** 中，并且对应的消息 $M^* \in \boldsymbol{M}$ 没有出现在 A 的聚合签名询问过程中. 该伪造的聚合签名必须能够通过聚合签名验证算法，并且除了挑战公钥外，其余公钥必须存在于密钥认证列表 C 中.

由于方案的聚合签名验证算法没有顺序的限制，不失一般性，将挑战公钥 PK^* 和对应消息 M^* 的索引序号设定为 1. 设定 $|\mathbf{PK}|=|\boldsymbol{M}|=\ell$，对于 $1 \leqslant i \leqslant \ell$，$\mathbf{PK}[i]=U_i \in G, \boldsymbol{M}[i] \in \{0,1\}^*$，则 $\mathrm{PK}^*=\mathrm{PK}[1]=U_1, M^*=M[1]$.

挑战者 B 根据以上信息计算一个基于单个消息 M^* 和对应挑战公钥 PK^* 的签名 (S_1, S_2). 具体计算方式为

$$S_1 \leftarrow S_1^* \cdot \prod_{i=2}^{\ell}\left(h_i^{x_i} \cdot \left(S_2^*\right)^{x_i}\right)^{-1}, S_2 \leftarrow S_2^*.$$

随后，挑战者 B 验证如下：

$$\begin{aligned}
&e\left(S_1, g\right) \cdot e\left(S_2, (U_1)\pi\right)^{-1} \\
&= e\left(S_1^*, g\right) \cdot e\left(S_2^*, (U_1)\right)^{-1} \cdot \prod_{i=2}^{\ell} e\left(h_i^{x_i}, g\right)^{-1} \cdot \prod_{i=2}^{\ell} e\left(\left(S_2^*\right)^{x_i}, g\right)^{-1} \\
&= e\left(S_1^*, g\right) \cdot \prod_{i=2}^{\ell} e\left(h_i^{x_i}, g\right)^{-1} \cdot \prod_{i=1}^{\ell} e\left(\left(S_2^*\right)^{x_i}, g\right)^{-1} \\
&= e\left(S_1^*, g\right) \cdot \prod_{i=1}^{\ell} e\left(S_2^*, U_i\right)^{-1} \cdot \prod_{i=2}^{\ell} e\left(h_i, U_i\right)^{-1} \\
&= \prod_{i=1}^{\ell} e\left(h_i, U_i\right) \cdot \prod_{i=2}^{\ell} e(h_i, U_i)^{-1} \\
&= e\left(h_1, U_1\right)
\end{aligned}$$

通过上述计算可以看出 (S_1, S_2) 是一个基于单个消息 M^* 和对应挑战公钥 PK^* 的有效签名，其中 S_1 即 BLS 签名元组，S_2 是对签名中随机数的承诺. 因为敌手 A 没有对 M^* 发起聚合签名询问，挑战者 B 也就没有发起对 M^* 的签名询问，所以签名 $\sigma=(S_1, S_2)$ 是一个非平凡的基于 BLS 的伪造签名. 挑战者 B 返回结果并终止游戏.

通过以上游戏过程可以看出，当敌手 A 伪造成功时，挑战者 B 也同样成功，即 $\varepsilon'=\varepsilon$. 挑战者 B 发起的签名询问次数与敌手 A 发起的有序聚合签名次数一致，即 $q'=q_S$. 挑战者 B 的运行时间是敌手 A 的运行时间加上处理 A 的查询和计算开销时间，每一次的密钥认证查询可以在 $O(1)$ 时间内处理完成，每一次聚合签名查询可以在 $O(n)$ 时间内完成，最终的结果可以通过 A 在 $O(n)$ 时间内的伪造得到，即 $t'=t+O(q_C+nq_S+n)$.

4.3 性能及效率分析

4.3.1 去中心化

本文方案中，群智网络中的终端节点通过区块链客户端产生密钥对（PK，SK），通过身份绑定合约建立节点 PK 和 ID 的证书 Cert，并将 Cert 发布至区块链中保存，证书 Cert 的有效性通过节点的有序聚合签名进行担保，整个过程中不存在可信第三方的参与. 区块链作为一个去中心化的底层存储数据库保证认证过程公开、透明、可审计.

4.3.2 公开验证性

本文方案中，当签名者与接收者关于签名的真实性存在争议，需公开验证发送者身份时，接收者可以将公开的消息签名元组 $(\mathrm{PK}, M, \sigma=(S_1, S_2))$ 发送给任意的可信第三方，第三方只需验证等式 $e(S_1, g) \cdot e\left(S_2, \prod_{i=1}^{\ell+1} U_i\right)^{-1}=\prod_{i=1}^{\ell+1} e(h_i, U_i)$ 是否成立，无需任何私有信息即可完成签名的有效性验证. 因此，本文方案具有公开验证性.

4.3.3 不可否认性

由定理 1 证明可知，本文有序聚合签名方案对敌手具有不可伪造性，同时，由公开验证性可知，任何可信第三方均可公开验证签名者的身份. 所以，本文有序聚合签名方案具有不可否认性.

4.3.4 效率分析

将本文方案与现有相关方案[10,11,13~15]的计算效率进行比较. 表 2 中相关符号的具体含义如下：n 代表参与者数量上界；E_B 表示双线性映射运算；E_M 表示群上的乘法运算；E_E 表示指数运算；L_G 表示群中元素的长度；L_B 表示双线性对的长度.

表 2 效率比较结果

方案	公钥长度	签名长度	验证效率	困难性问题
[10]	L_G	L_G	$2nE_E$	RSA
[11]	$L_B+(n+1)L_G$	$2L_G$	$2E_B+/nk(2E_M)$	CDH
[13]	$2L_G$	$4L_G$	nE_B+nE_E	LRSW
[14]-1	$11L_G$	$8L_G$	$8E_B+4nE_E$	Static
[14]-2	$13L_G$	$6L_G$	$6E_B+3nE_E$	Static
[15]	$(n+2)L_G$	$(n+1)L_G$	$4E_B+(n+2)E_M$	CDH
本文	L_G	$2L_G$	$(n+2)E_B$	CDH

5 结束语

本文提出了一种面向群智网络的基于区块链的身份认证机制，并构造了一个新的有序聚合签名方案，分析了方案的安全属性. 本文将区块链技术与有序聚合签名技术相结合，借助区块链所具有的不可篡改、可审计等特点，实现了对公钥证书的自动化管理，认证过程更加灵活. 证书签发和公钥发布以公开、透明的形式存放在区块链中，用户可以对其进行查询，解决了证书签发的不透明问题.

本文提出的身份认证机制只给出了基本的认证流程框架，关于用户身份或者属性信息的隐私性保护没有涉及. 在接下来的工作中，考虑通过零知识证明等技术实现匿名认证，达到对终端用户的安全管理和隐私保护.

参考文献

[1] 中国人工智能2.0发展战略研究项目组. 中国人工智能2.0发展战略研究[M]. 杭州: 浙江大学出版社, 2019.

[2] I' ANSON C, MITCHELL C. Security defects in CCITT recommendation X. 509[J]. ACM SIGCOMM Computer Communication Review, 1990, 20(2): 30-34.

[3] LU Y, TANG Q, WANG G L. ZebraLancer: Private and anonymous crowdsourcing system atop open blockchain [C]//2018 IEEE 38th International Conference on Distributed Computing Systems(ICDCS). New York: IEEE, 2018: 853-865.

[4] HAMMI M T, HAMMI B, BELLOT P, et al. Bubbles of Trust: A decentralized blockchain-based authentication system for IoT[J]. Computers & Security, 2018, 78: 126-142.

[5] HAMMI M T, BELLOT P, SERHROUCHNI A. BCTrust: A decentralized authentication blockchain-based mechanism[C]//2018 IEEE Wireless Communications and Networking Conference(WCNC). New York: IEEE, 2018: 1-6.

[6] FROMKNECHT C, VELICANU D, YAKOUBOV S. Certcoin: A namecoin based decentralized authentication system[C]//Massachusetts Institute of Technology. Cambridge: MIT, 2014: 46-56.

[7] HAMMUDOGLU J S, SPARREBOOM J, RAUHAMAA J I, et al. Portable Trust: Biometric-based authentication and blockchain storage for self-sovereign identity systems [EB/OL]. (2017)[2020]. https://arxiv.org/abs/1706.03744.

[8] AL-BASSAM M. SCPKI: A smart contract-based PKI and identity system[C]//Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts. New York: ACM, 2017: 35-40.

[9] 马晓婷, 马文平, 刘小雪. 基于区块链技术的跨域认证方案[J]. 电子学报, 2018, 46(11): 2571-2579.
MA X T, MA W P, LIU X X. A cross domain authentication scheme based on blockchain technology[J]. Acta Electronica Sinica, 2018, 46(11): 2571-2579. (in Chinese)

[10] LYSYANSKAYA A, MICALI S, REYZIN L, et al. Sequential aggregate signatures from trapdoor permutations [C]//Advances in Cryptology-EUROCRYPT 2004. Berlin: Springer, 2004: 74-90.

[11] LU S, OSTROVSKY R, SAHAI A, et al. Sequential aggregate signatures and multisignatures without random oracles[C]//Advances in Cryptology-EUROCRYPT 2006. Berlin: Springer, 2006: 465-485.

[12] CAMENISCH J, LYSYANSKAYA A. Signature schemes and anonymous credentials from bilinear maps[C]//Advances in Cryptology-CRYPTO 2004. Berlin: Springer, 2004: 56-72.

[13] SCHRÉDER D. How to aggregate the CL signature scheme[C]//European Symposium on Research in Computer Security. Berlin: Springer, 2011: 298-314.

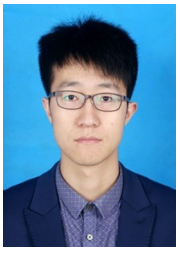
[14] LEE K, LEE D H, YUNG M. Sequential aggregate signatures with short public keys without random oracles[J]. Theoretical Computer Science, 2015, 579: 100-125.

[15] 赵慧艳, 于佳, 李朦, 等. 并行密钥隔离聚合签名[J]. 电子学报, 2015, 43(5): 1035-1040.
ZHAO H Y, YU J, LI M, et al. Parallel key-insulated aggregate signature[J]. Acta Electronica Sinica, 2015, 43 (5): 1035-1040. (in Chinese)

[16] BONEH D, BOYEN X, SHACHAM H. Short group signatures[C]//Advances in Cryptology-CRYPTO 2004. Berlin: Springer, 2004: 41-55.

[17] CARONNI G. Walking the web of trust[C]//Proceedings IEEE 9th International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises(WET ICE 2000). New, York: IEEE, 2000: 153-158.

作者简介



杨坤伟　男, 1990年出生于陕西省咸阳市. 陕西师范大学计算机科学学院博士生. 研究方向为密码学、信息安全.
E-mail: yangkunwei@snnu.edu.cn

杨　波　男, 1963年出生于陕西省富平县. 教授, 博士生导师, 陕西省"百人计划"特聘教授. 研究方向为密码学、信息安全.
E-mail: byang@snnu.edu.cn

周彦伟　男, 1986年出生于甘肃省通渭县. 陕西师范大学计算机科学学院博士生. 研究方向为密码学、匿名通信技术.
E-mail: zhouyanwei1986@163.com