软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2019,30(6):1692−1704 [doi: 10.13328/j.cnki.jos.005745]

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

基于 SM9 算法可证明安全的区块链隐私保护方案*

杨亚涛[1,3], 蔡居良[1], 张筱薇[1], 袁 征[2,3]

[1](北京电子科技学院 电子与通信工程系,北京 100070)

[2](北京电子科技学院 密码科学与技术系,北京 100070)

[3](西安电子科技大学 通信工程学院,陕西 西安 710071)

通讯作者: 杨亚涛, E-mail: yy2008@163.com

摘 要: 为了解决区块链交易过程中的隐私泄漏问题,对 SM9 标识密码算法进行改进,提出了基于身份认证的多 KGC 群签名方案.以联盟链为基础,设计了基于 SM9 算法可证明安全的区块链隐私保护方案,并对以上方案进行安全性与效率分析.通过分析证明,方案具有签名不可伪造、保证节点匿名及前向安全等特性.通过效率分析:该方案较 Al-Riyami 等人提出的无证书签名方案减少 2 次双线性对运算,验签效率提高约 40%;较 Tseng 等人与 Chen 等人提出的方案分别减少 4 次与 2 次指数运算,计算效率整体得到提高.该方案通过多 KGC 群签名保护交易双方的用户身份,实现在节点间进行身份验证的同时,保护了节点的隐私.

关键词: 联盟区块链;无证书公钥密码体制;双线性对;群签名;可证明安全

中图法分类号: TP309

中文引用格式: 杨亚涛,蔡居良,张筱薇,袁征.基于 SM9 算法可证明安全的区块链隐私保护方案.软件学报,2019,30(6):1692−1704. http://www.jos.org.cn/1000-9825/5745.htm

英文引用格式: Yang YT, Cai JL, Zhang XW, Yuan Z. Privacy preserving scheme in block chain with provably secure based on SM9 algorithm. Ruan Jian Xue Bao/Journal of Software, 2019,30(6):1692−1704 (in Chinese). http://www.jos.org.cn/1000-9825/5745.htm

Privacy Preserving Scheme in Block Chain with Provably Secure Based on SM9 Algorithm

YANG Ya-Tao[1,3], CAI Ju-Liang[1], ZHANG Xiao-Wei[1], YUAN Zheng[2,3]

[1](Departmentof Electronics and Communications Engineering, Beijing Electronics Science & Technology Institute, Beijing 100070, China)

[2](Department of Cryptography Science and Technology, Beijing Electronics Science & Technology Institute, Beijing 100070, China)

[3](School of Communication Engineering, Xidian University, Xi'an 710071, China)

Abstract: In order to solve the problem of privacy leakage in the transaction process of block chain, by improving the SM9 identification cryptography algorithm, a multi KGC group signature scheme based on SM9 algorithm was proposed for the first time. Based on the alliance chain, a privacy preserving scheme in block chain with provably secure was designed based on SM9 algorithm. By analyzing the security and efficiency about this scheme, it is proved that the proposed scheme has many advantages, such as signature unforgery, the node anonymity, forward security, and so on. By analyzing the efficiency, the proposed scheme decreases twice bilinear pairing operations compared with the certificateless signature scheme proposed by Al-Riyami S Ss', and the efficiency of signature verifying is increased by about 40%. Moreover, the proposed scheme cuts down four times and twice exponent operations compared with

* 基金项目: "十三五"国家密码发展基金(MMJJ20170110)
Foundation item: State Cryptography Development Fund of the 13th Five-year Plan (MMJJ20170110)
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: 2018-06-25; 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.20190327.1640.010.html

schemes of Tseng Y Ms' and Chen Ys', the overall calculation efficiency is improved. The user identity of two parties can be protected by the cryptographic operation, and the privacy preserving of the nodes is achieved.

Key words: alliance block chain; certificateless public key cryptography; bilinear pairing; group signature; provable security

区块链技术因其"去中心化"与"去信任化"等特点,可在可信第三方不参与的情况下与陌生节点之间进行安全的信息传递,有效提高了信息交互效率,降低交互成本,在比特币、供应链等领域具有较为广阔的前景[1].哈希算法以及数字签名算法在区块链中应用广泛,用以验证区块以及交易的正确性.区块链在实际场景中应用时,不仅需要核验节点的公钥地址,还应验证各个节点的真实身份.传统的 PKI 体制因为可信中心的权重过大,不符合区块链"去中心化"与"去信任化"的特点.因此,无证书的加密与签名方案[2]可以在区块链技术中得到应用.2012 年,Yu 等人[3]提出一种在标准模型下可证明安全的无证书签名方案,但该方案需要使用 5 次以上的双线性对运算,计算效率较低.同年,Gong 等人[4]提出基于椭圆曲线的无证书密码体制,但其并不能有效抵抗第一类超级攻击者的攻击.2017 年,Tseng 等人[5]提出一种抗连续泄漏攻击的安全无证书签名方案.

隐私泄露是区块链技术中不容忽视的问题[6].与传统中心化结构不同,区块链机制不依赖特定中心节点处理与存储数据,因此可以避免恶意中心或因其他原因导致的中心信息泄露[7].但为了验证交易信息,区块链中的所有交易记录必须公开,因此将显著增加信息泄露风险.Kosba 等人[8]认为,交易地址暴露于区块链环境中容易被跟踪查找.因为区块链技术与当前 IT 架构存在区别,以往的隐私保护方案并不适用.所以,区块链的隐私保护需要更具针对性的机制[9].2013 年,Miers 等人[10]基于比特币提出了拥有匿名性的区块链数字货币方案——零币.该方案通过运用零知识证明等密码学技术,以隐藏用户地址、切断交易双方联系的方式保证了交易的非关联性,从而达到匿名与不可追踪的效果.但该方案基于公有链进行设计,区块生成速度与比特币近似,无法进行高效率的交易流通,并且节点需要额外维护货币作废列表以保证交易的惟一性,在一定程度上影响了交易验证的效率.2016 年,Shen 等人[11]提出了基于环签名的区块链秘密交易方案.该方案随机选取无关地址后连同交易发起方进行环签名,达到混淆交易用户身份的目的.但该方案与零币方案均存在因切断交易关联性而导致溯源性较差的问题,难以在实际场景中得到应用,并且单次交易信息量过大,而该方案的匿名性取决于参与环签名的地址数量,为缩小交易信息量而减少地址个数,也将面临去匿名化的风险.

群签名的概念由 Chaum 和 Heyst[12]在 1991 年提出后,它以独特的性质引起人们的关注并被广泛研究.群签名允许群体中任何一名成员代表整个群体对消息进行匿名签名.与普通数字签名一样,群签名可以公开验证,并且发生纠纷时,群管理员可以打开群签名以揭露签名者的真实身份.基于身份的群签名方案具有在身份标识验证的基础上,采用群签名的方式保护用户的隐私,兼具二者特点,在区块链环境中具有应用价值.目前,许多基于身份的群签名方案被提出.2008 年,Zhang 等人[13]提出一种针对恶意 PKG 的无证书群签名方案.2010 年,陈虎等人[14]提出一种高效的无证书签名与群签名方案,具有前向安全性等特点,但其并不能使用户的不同交易隐蔽关联性,无法直接应用于区块链中.2012 年,Zhan 等人[15]提出基于身份的门限群签名方案.同年,Cheng 等人[16]提出了实用的基于身份的群签名方案.2015 年,Lin 等人[17]提出一种基于群签名和基于身份签名的安全隐私保护协议.2017 年,Bande 等人[18]提出具有验证者本地撤销的安全隐私保护群签名方案,其安全性基于强 RSA 假设.但该方案并非基于身份,所以难以抵抗公钥替换攻击.以上方案虽然可以实现无证书签名以及利用群签名保护签名者隐私,但均没有针对区块链特殊架构进行设计,无法应用于区块链高开放度的环境中,对节点身份进行隐藏与保护.

本文的贡献在于,提出一种基于 SM9 算法可证明安全的区块链隐私保护方案,对现有 SM9 算法进行适当优化,提出了一种基于 SM9 算法的群签名方案,以区块链中的联盟链为应用环境,实现对交易过程的隐私保护.方案效率较现有方案相比,所需指数运算与双线性对运算均有减少,运算效率得到提升,可以为联盟链的应用提供有效安全和隐私保护支撑.

1 预备知识

1.1 区块链与联盟链

区块链是一种按照时间顺序将数据区块以链条的方式组合成特定的数据结构[19],并以密码学方式保证的不可篡改和不可伪造的去中心化共享总账,能够安全存储简单的、有先后关系的、能在系统内验证的数据[20].区块链可以看做存储数字记录的数据库,数据库由网络节点共享,节点可以提交新的记录,区块链网络通过共识机制保证节点之间数据的一致性,记录一旦被输入,就永远不会被更改或删除.

总体上区块链可以分为 3 种类型:公有链、联盟链和私有链,本文设计的隐私保护方案主要在联盟链中实现.在联盟链中,区块链的区块和交易的有效性由预先设定的一个验证者群体决定,这个验证群体形成一个联盟.例如,要使得联盟链中的一个区块有效,需要联盟中 50%以上的成员认可通过,新区块才有效.区块链上的信息可以是公开的,也可以只对联盟成员可见.

1.2 SM9标识密码算法

SM9 密码算法涉及有限域、椭圆曲线、椭圆曲线上双线性对的运算等基本知识和技术[21],其中,SM9 数字签名算法包括数字签名生成算法和验证算法.签名者持有一个标识和一个相应的私钥,该私钥由密钥生成中心(key generation center,简称 KGC)通过主私钥和签名者的标识结合产生.签名者用自身私钥对数据产生数字签名,验证者用签名者的标识生成其公钥,验证签名的有效性,即验证发送数据的真实性、完整性和数据发送者的身份.

1.3 群签名

群签名是由包含下面过程的数字签名方案[22]组成.

(1) 创建:一个用以产生群公钥和私钥的多项式时间概率算法;
(2) 加入:一个用户和群管理员之间使用户成为群管理员的交互式协议.执行该协议可以产生群员的私钥和成员证书,并使群管理员得到群成员的私有密钥;
(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,输出对消息的签名;
(4) 验证:一个在输入消息原文、对消息的群签名以及群公钥后验证签名是否有效的算法;
(5) 打开:一个在给定一个签名及群私钥的条件下,确认签名人的合法身份的算法.

2 区块链隐私保护方案设计

本文提出一种适用于区块链技术的隐私保护方案,通过对广播交易信息中用户身份信息进行多 KGC 群签名运算,实现隐藏用户身份以及同一用户不同交易之间的关联性.具体描述如下.

2.1 节点构成

本方案基于联盟链进行设计,节点由主要节点与次要节点构成,具体结构如图 1 所示.

其中,主要节点负责维护区块链参数与历史数据,进行区块链中所使用的 SM9 多 KGC 签名算法以及群签名算法的参数初始化,参与区块生成以及管理次要节点的加入与相关密钥的分发.设现有 k 个 KGC,则所有 KGC 首先商定随机数 $ks\in[1,N-1]$,并各自持有另一个随机数 $ke_j\in[1,N-1]$,其中,j 表示第 j 个 KGC.每个 KGC 计算 G_2 中的元素 $P_{pub\text{-}s}=[ks]P_2$ 与 $P_{pub\text{-}j}=[ke_j]P_2$,之后,依次计算 $P_{pub\text{-}e}=\sum_{i=1}^{j}P_{pub\text{-}j}$,直到 $j=k$ 为止,使得 $P_{pub\text{-}e}=\left[\sum_{i=1}^{k}ke_j\right]P_2$,则签名主密钥对为$(ke,P_{pub\text{-}s},P_{pub\text{-}e})$.每个 KGC 秘密保存 ks 与自己持有的 ke,公开 $P_{pub\text{-}s}$ 与 $P_{pub\text{-}e}$.次要节点 A 的标识为 ID_A,为了产生次要节点 A 的签名私钥 ds_A,KGC 首先在有限域上计算 $t_1=H_1(ID_A||hid,N)+ks$,若 t 不为 0,则计算 $t_j=ke_j\cdot t_1^{-1} \bmod N$;然后将结果发送给次要节点 A;最后,A 在本地计算 $ds_A=\left[\sum_{j=1}^{k}t_j\right]P_1$,得到自己的私钥.

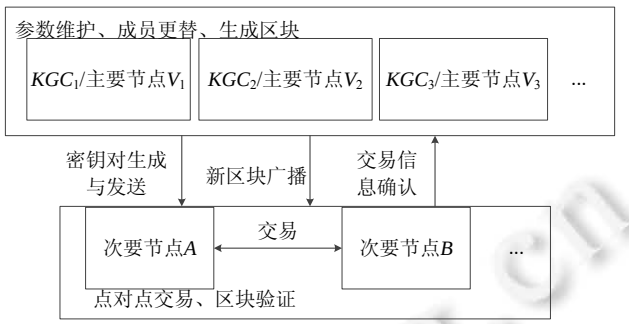

Fig.1 Composition of nodes in the scheme

图 1 方案节点构成

次要节点持有各自的签名密钥对与群签名密钥对,次要节点为群签名中的用户,次要节点之间可进行交易,完成区块链中点对点交易信息传递的流程.交易商定结束,需对信息进行群签名后进行广播,新区块将交易信息写入并由各个节点确认后即为生效.

2.2 交易流程

次要节点之间需要使用签名来验证对方身份,并使用群签名生成需要广播的交易信息.

签名具体步骤如下.

1. 签名生成

设消息为比特串 M,则次要节点 A 若需要对其进行数字签名,则首先计算群 G_T 中元素 $g=e(P_1,P_{pub\text{-}e})$,并选取随机数 $r\in[1,N-1]$,计算 $w=g^r$ 以及整数 $h=H_2(M\|w,N)$,之后,计算整数 $l=(r-h) \bmod N$,若 l 为 0,则重新选取随机数;l 不为 0 时,则最后计算 $S=[l]ds_A$,可得到关于消息 M 的签名(h,S).

2. 签名验证

设验证者为次要节点 B,其接收到的消息 M'的签名为(h',S'),如需要验证签名,则需要首先验证 $h'\in[1,N-1]$ 以及 $S'\in G_1$,若均成立,则计算群 G_T 中的元素 $g=e(P_1,P_{pub\text{-}e})$,再计算群 G_T 中的元素 $t=g^{h'}$ 与整数 $h_1=H_1(ID_A\|hid,N)$,之后计算群 G_2 中的元素 $P=[h_1]P_2+P_{pub\text{-}s}$ 与群 G_T 中的元素 $u=e(S',P)$,再计算群 G_T 中的元素 $w'=u\cdot t$,最后计算 $h_2=H_2(M'\|w',N)$并与 h'进行比较,若一致,则验证通过.

相比 SM9 标准的签名验签算法,考虑到联盟区块链中多个主要节点与 KGC 的功能要求,我们提出采用多 KGC 模式对标准 SM9 签名算法的参数生成步骤进行改进,将 KGC 的功能分配于主要节点,主要节点共同参与参数维护与密钥生成,符合联盟链部分去中心化的架构要求,以及将无证书体制与联盟区块链运作模式结合的需要.因签名算法基于 SM9 算法进行改进,故加密算法改进方式于此类似,不再赘述.

群签名主要功能如下.

1. 创建

设群管理员(group manager,简称 GM)的身份为 ID_{GM},则其需要向全部 KGC 申请建立群,KGC 在核实 GM 身份后,将 ID_{GM} 记录,以便之后 KGC 对新加入的成员生成并发放群私钥.申请群成功后,该群的公钥即为 GM 身份 ID_{GM}.群管理员的私钥则由签名算法生成并交由管理员 GM 保存.

2. 加入

当次要节点 A 想加入群时,主要分两种情况.

(1) KGC 不在群中,则由 GM 核实次要节点 A 的身份 ID_A,核对通过后,将 ID_A 通过改进的 SM9 算法进行签名后,通过安全信道发送至 KGC.KGC 对 GM 的签名进行验证,完成后提取出 ID_A,商定 $ks\in[1,N-1]$以及每个 KGC 各自持有 $ke_j\in[1,N-1]$,首先计算 $d_1=[H_1(ID_{GM}\|hid,N)+ks]^{-1} \bmod N$,再根据 ID_A 计算 $d_2=[H_1(ID_A\|hid,N)+ks]^{-1} \bmod N$,得出 $ds'_A=[d_2]P_1$,之后,每个 KGC 计算 $ds_{A_j}=[ke_j]ds'_A$,次要节点 A 将每个 KGC 的 ds_{A_j} 相加,即可得到签名私钥

$ds_A=[d_2]\left[\sum_{j=1}^{k}ke_j\right]P_1$.之后,$A$ 将结果重新发送给所有 KGC.KGC 重新计算一次,得 $ds'_{AG}=[d_2]\left[\sum_{j=1}^{k}ke_j\right]\cdot ke_j\cdot[d_1]\cdot P_1$,发送给次要节点 A,次要节点 A 最后运算 $ds_{AG}=\sum_{j=1}^{k}ds'_{AG}=[d_2]\left[\sum_{j=1}^{k}ke_j\right]\left[\sum_{j=1}^{k}ke_j\right][d_1]P_1$,可得到次要节点 A 的群私钥 ds_{AG}.至此,次要节点 A 加入成功,其群密钥对为(ds_A,ds_{AG},ID_A,ID_{GM}),其中:ds_A,ds_{AG} 为私钥,由 A 保存;ID_{GM} 为 GM 身份,亦为群签名的唯一标识.同时,KGC 需要保存用户的身份 ID_A.

(2) 若 KGC 在群中,则次要节点 A 可直接将自己的身份 ID_A 通过安全信道送于 KGC 核实,通过后,群密钥对生成方法与第 1 种情况相同.

3. 群签名

若群中次要节点 A 要对消息 M 进行群签名,则其需要首先计算 $g=e(P_1,P_{pub\text{-}e})$,并秘密选取随机数 $r_1\in[1,N-1]$ 与 $r_2\in[1,N-1]$,计算 $w=g^{r_1}$,之后计算 $h=H_2(M\|w,N)$,计算 $S_1=(r_2^{-1})\cdot(r_1-h)\cdot ds_A$ 与 $S_2=(r_2^{-1})(r_1-h)\cdot ds_{AG}$,最后计算 $h_1=H_1(ID_A\|hid,N)$,$P_{3'}=[h_1]P_2+P_{pub\text{-}s}$,$P_3=[r_2]P_{3'}$,得出次要节点 A 对消息 M 的群签名(h,P_3,S_1,S_2).

4. 验证

对于接收到的消息 M'与其群签名 (h',P'_3,S'_1,S'_2) ,群中次要节点 B 若想验证其是否属于群 ID_{GM},则需要首先计算 $h_1=H_1(ID_{GM}\|hid,N)$,接着计算 $P=[h_1]P_2+P_{pub\text{-}s}$,之后计算 $u_1=e(S_2,P)$与 $u_2=e(S_1,P_{pub\text{-}e})$,若 $u_1\neq u_2$,则验证不通过;否则继续计算 $u=e(S_1,P_3)$,$g=e(P_1,P_{pub\text{-}e})$与 $t=g^{h'}$,最终计算 $w'=u\cdot t$,得到 $h=H_2(M'\|w',N)$.对比 h'与 h,一致则验证通过,至此可证明该消息由群 ID_{GM} 中某个成员所签名.

5. 打开

在区块链交易中,节点间进行信息交互时需要核对对方身份,所以将签名算法与群签名算法一同使用,当需要核实信息签名来源时,KGC 可根据所持有的用户信息 ID_A 找到该用户所属密钥,并查看是否已被撤销或更新,以确定交易产生的时间以及是否合法.

6. 系统维护与成员撤销

当 GM 需要撤销群成员节点时,在将要撤销的成员信息中记录“已作废”标记;而当系统参数需要更新时,KGC 可重新生成系统参数,并且更新用户信息,分发给群成员新的密钥对.同时保留曾经使用的系统参数.

次要节点之间的交易流程如图 2 所示.

Fig.2 Transaction process between the nodes

图 2 节点间交易流程

交易进行时,发起方节点 A 需将与本次交易相关的上次交易信息的所属编号 $Num(TX_0)$,与上次交易中,节点 A 所属的哈希值 $Hash_A(TX_0)$,使用与上次交易相同的群签名要素 $P_3(A)$进行群签名(h,$P_3(A)$,S_1,S_2)后,结合本此交易的待交易信息 $UTXO_0(B)$(如货币数量等)进行签名,使用接收方节点 B 的身份为公钥进行加密,并将信息传递给节点 B.交易请求信息①中包含的内容为

$$\left.\begin{array}{l} Enc(Num(TX_0)\|Hash_A(TX_0)\|GSig(Num(TX_0)\|Hash_A(TX_0))\|UTXO_0(B)\|\\ Sig(Num(TX_0)\|Hash_A(TX_0)\|GSig(Num(TX_0)\|Hash_A(TX_0))\|UTXO_0(B))) \end{array}\right\} \tag{1}$$

其中,$Sig(M)$表示基于 SM9 算法的多 KGC 签名方案,$GSig(M)$表示使用本文设计的群签名方案.

节点 B 接受后,使用私钥进行解密,使用节点 A 的公钥验证签名,以及使用群身份进行群签名验证,全部通过并且核对本次交易的输入 $P_3(A)$与上次交易的输出 $P_3(A)'$是否一致,相同后确认交易信息,无误后组合 $Num(TX_0)$, $Hash_A(TX_0)$以及 $UTXO_0(B)$,并计算其哈希值,作为所属自己的本次交易输出哈希值,并将此数据进行群签名 $(h,P_3(B),S_1,S_2)$,最终将结果签名,使用节点 A 公钥进行加密,返回节点 A,交易确认信息②中包含的内容为

$$\left.\begin{array}{l} Enc(Hash(Num(TX_0)\|Hash_A(TX_0)\|UTXO_0(B))\|GSig(Hash(Num(TX_0)\|Hash_A(TX_0)\|UTXO_0(B)))\|\\ Sig(Hash(Num(TX_0)\|Hash(TX_0)\|UTXO_0(B))\|GSig(Hash(Num(TX_0)\|Hash_A(TX_0)\|UTXO_0(B))))) \end{array}\right\} \tag{2}$$

节点 A 解密验签通过后,将交易信息进行广播,并入新生区块中,广播的交易信息(TX)结构如图 3 所示.

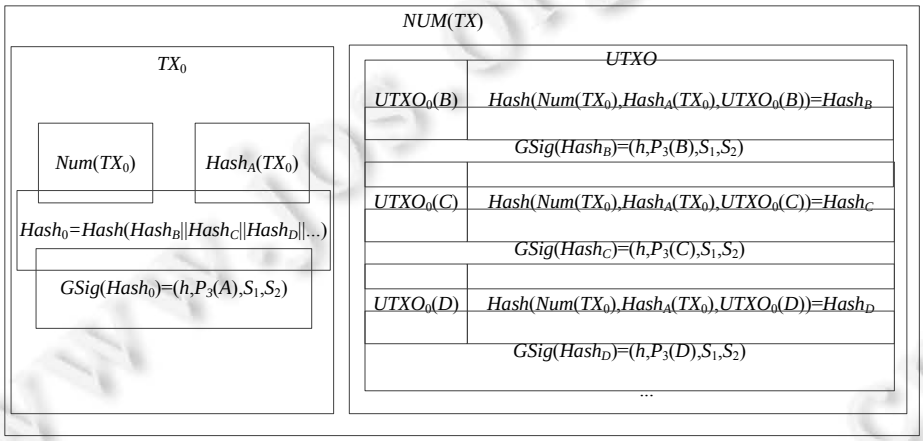

Fig.3 Transaction information TX to be verified

图 3 需要验证的交易信息 TX

广播的交易信息主要包括与本次交易关联的上次交易信息 TX_0 以及本次交易的输出 $UTXO.TX_0$ 用于追溯上次交易的相关信息,并据此核对本次交易输入是否合理;$UTXO$ 主要包括各个输出所属的交易信息 $UTXO_0$ 以及输出哈希值与群签名,除了用于各个节点的确认之外,也作为下次交易输入的核对信息.

2.3 区块生成及验证

本方案基于联盟链,主要节点负责区块生成.各主要节点首先需商定区块生成的共识算法,确保不会生成分叉区块.次要节点不能生成区块.区块结构如图 4 所示.

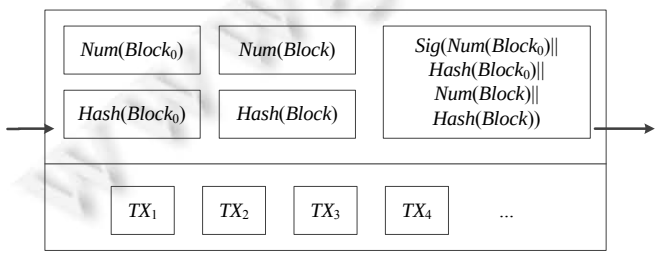

Fig.4 Block structure and information contained

图 4 区块结构与所含信息

其中,新生区块需要记录上一个区块的编号 $Num(Block_0)$以及其哈希值 $Hash(Block_0)$来保证区块之间的关

联性.同时,生成区块时,需要确定本区块的编号 $Num(Block)$并计算本区块中全部数据的哈希值 $Hash(Block)$,将此 4 个数据组合,进行签名,最后发布.

各节点在接受新区块时,需对其进行身份验证,确认其为主要节点生成,并且与最近一次生成的区块相关联后,再进行交易信息验证流程.各次要节点接收到交易信息后,需要首先验证其群签名是否有效,验证通过后,寻找与此交易输入关联的上一次的交易输出 $UTXO_0$,核对本次交易输入端的 P_3 与上次交易输出端的 P_3' 是否相同:若一致,则本次交易验证通过.当本次交易经过全部次要节点中半数以上验证通过后,才可并入新区块中.至此,节点 A 与 B 的交易确认有效.

2.4 具体流程

本方案在保护节点用户身份隐私的同时,因交易采用 UTXO 的形式,具有可溯源特性.在实际场景,如供货链、物品买卖、房屋租赁等交易中,不同节点用户交易过程中可能会产生纠纷,通过应用本方案,可进行溯源追责.本方案的具体交易流程如图 5 所示.

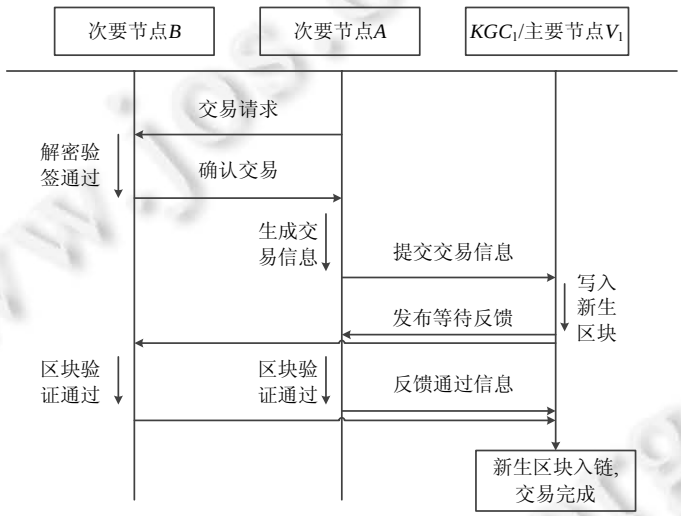

Fig.5 Specific transaction process

图 5 具体交易流程

交易流程说明如下.

1) 当次要节点 A 准备向 B 发起交易时,需首先将与本次交易关联的上次的交易输出以及本次的交易内容进行签名与群签名,加密处理后,形成如公式(1)所示内容,发送至次要节点 B;

2) 节点 B 收到后进行解密与验签,审核交易信息无误后,附上自己关于此次交易自身的群签名,做签名加密处理后,形成如公式(2)所示内容,返回节点 A;

3) 节点 A 审核无误后,将所有相关信息组合成如图 3 所示的等待入链的交易信息,包括上次交易的编号 $Num(TX_0)$及哈希值 $Hash_A(TX_0)$、本次交易输入输出的群签名 $GSig(Hash_0)$与 $GSig(Hash_B)$等内容,发送至主要节点 V_1.此时,交易发起方节点 A 与接收方节点 B 等候新区块发布与审核;

4) 主要节点 V_1 将收到的所有交易信息以图 4 所示的结构写入新生区块,发布区块并等待次要节点反馈,所有进行交易后等待的次要节点收到发布的新区块后,对其中信息进行群签名验签,并将验签结果返回主要节点 V_1;

5) 当 V_1 收到当前参与交易节点半数以上的验签通过信息后,将新生区块并入链中.至此,所有在此区块中的交易生效,交易流程结束.

上述交易流程中采用 UTXO 的交易方式,所有节点均可通过查看已入链区块的交易信息进行交易溯源.如

在货物买卖场景中,若交易接收方收到的货物出现了质量问题,则可以通过对该次交易逐链溯源的方式,找到该货物的首发地址,即为主要节点的供货商或该货物的生产厂家进行追责.

3 方案安全性与效率分析

3.1 方案正确性证明

对于签名算法,在签名验证阶段,需要验证 h_2 与 h'是否相等,因为 $h_2=H_2(M'||w',N)$,$h'=H_2(M||w,N)$,验证二者是否相等等价于验证 w 与 w'是否相等.因为 $u=e(S',P)$,而:

$$u=e(S',P)=e([l]ds_A,[h_1]P_2+P_{pub\text{-}s})=e([r-h]ds_A,[h_1]P_2+P_{pub\text{-}s})=e(P_1,P_2)^{(r-h)\left[\sum_{j=1}^{k}t_j\right]\cdot(h_1+ks)}=e(P_1,P_2)^{(r-h)\left[\sum_{j=1}^{k}ke_j\right]\cdot(h_1+ks)};$$

又因:

$$t=g^{h'}=e(P_1,P_{pub\text{-}e})^h=e\left(P_1,\left[\sum_{i=1}^{k}ke_j\right]P_2\right)^h=e(P_1,P_2)^{h\cdot\left[\sum_{i=1}^{k}ke_j\right]},$$

则:

$$w'=u\cdot t=e(P_1,P_2)^{(r-h)\left[\sum_{j=1}^{k}ke_j\right]}\cdot e(P_1,P_2)^{h\cdot\left[\sum_{i=1}^{k}ke_j\right]}=e(P_1,P_2)^{r\cdot\left[\sum_{j=1}^{k}ke_j\right]}=e(P_1,P_{pub\text{-}e})^r=w.$$

所以验证通过,签名算法正确性得到证明.

对于群签名算法,在群签名验证阶段,需要比对 u_1 与 u_2 是否一致,所以其正确性证明如下:

$u_1=e(S_2,P)=e(S_2,([h_1]P_2+P_{pub\text{-}s}))=e(S_2,([h_1]P_2+[ks]P_2))$,而:

$$\begin{aligned}S_2&=(r_2^{-1})(r_1-h)\cdot ds_{AG}\\&=(r_2^{-1})(r_1-h)\cdot[d_2]\left[\sum_{j=1}^{k}ke_j\right]\left[\sum_{j=1}^{k}ke_j\right][d_1]P_1\\&=(r_2^{-1})(r_1-h)\cdot[d_2]\left[\sum_{j=1}^{k}ke_j\right]\left[\sum_{j=1}^{k}ke_j\right][H_1(ID_{GM}\|\ hid,N)+ks]^{-1}P_1.\end{aligned}$$

由双线性对性质可得:

$$\begin{aligned}u_1&=e(S_2,P)\\&=e(S_2,([h_1]P_2+[ks]P)_2)\\&=e(P_1,P_2)^{(r_2^{-1})(r_1-h)\cdot[d_2]\left[\sum_{j=1}^{k}ke_j\right]\left[\sum_{j=1}^{k}ke_j\right][H_1(ID_{GM}\|hid,N)+ks]^{-1}\cdot[H_1(ID_{GM}\|hid,N)+ks]}\\&=e(P_1,P_2)^{(r_2^{-1})(r_1-h)\cdot[d_2]\left[\sum_{j=1}^{k}ke_j\right]\left[\sum_{j=1}^{k}ke_j\right]},\\u_2&=e(S_1,P_{pub\text{-}e})\\&=e\left((r_2^{-1})(r_1-h)\cdot ds_A,\left[\sum_{i=1}^{k}ke_j\right]P_2\right)\\&=e\left((r_2^{-1})(r_1-h)\cdot[d_2]\left[\sum_{j=1}^{k}ke_j\right]P_1,\left[\sum_{i=1}^{k}ke_j\right]P_2\right)\\&=e(P_1,P_2)^{(r_2^{-1})(r_1-h)\cdot[d_2]\left[\sum_{j=1}^{k}ke_j\right]\cdot\left[\sum_{i=1}^{k}ke_j\right]}.\end{aligned}$$

二者结果一致,所以可继续执行下面的验证过程.而:

$$u=e(S_1,P_3)=e(P_1,P_2)^{(r_2^{-1})(r_1-h)\cdot[d_2]\left[\sum_{j=1}^{k}ke_j\right]\cdot r_2\cdot[H_1(ID_A\|hid,N)+ks]}=e(P_1,P_2)^{(r_1-h)\cdot\left[\sum_{j=1}^{k}ke_j\right]},$$

$$w'=u\cdot t=e(P_1,P_2)^{(r_1-h)\cdot\left[\sum_{j=1}^{k}ke_j\right]}\cdot e(P_1,P_2)^{H_2(M\|w,N)\cdot\left[\sum_{j=1}^{k}ke_j\right]}=e(P_1,P_2)^{r_1\cdot\left[\sum_{j=1}^{k}ke_j\right]}=w.$$

二者同样一致,所以验证通过,方案正确性得到证明. □

3.2 方案安全性证明

3.2.1 不可伪造性

根据无证书签名的安全模型[3]可知,方案需要做到成员密钥对于签名不可伪造.

- 第 1 类敌手——公钥替换攻击

对于签名算法,因为基于身份的无证书签名算法使用节点的 ID 为公钥进行签名,所以可抵抗公钥替换攻击.对于群签名算法,敌手 E_1 知道群节点 A 的公钥 ID_A,若利用此身份进行通信,则必须伪造该身份的密钥对.

假设敌手伪造了节点 A 的密钥对 $(ds'_A,ds'_{AG},ID'_A,ID_{GM})$,则利用此密钥对进行群签名 $S'_1=(r_2^{-1})(r_1-h)\cdot ds'_A$ 与 $S'_2=(r_2^{-1})(r_1-h)\cdot ds'_{AG}$.节点 B 在收到签名后,验证 $u_1=e(S'_2,P)$ 与 $u_2=e(S'_1,P_{pub\text{-}e})$ 是否一致.因为敌手无法得到系统主密钥 ks 与 ke,所以 u_1=u_2 的概率极小,验证通过概率极小.因此敌手无法伪造节点 A 的密钥对,本方案可以抵抗公钥替换攻击.

- 第 2 类敌手——恶意的 KGC 攻击

对于签名算法,设敌手 E_2 为本方案中的恶意 KGC,其知道系统主密钥 ks 与其自己持有的 ke_j.在本群签名方案中,因为由多个 KGC 共同维护方案所需的系统参数,ks 由全部 KGC 共同商定,而 ke_j 仅自己知道,由用户签名私钥 $ds_A=[d_2]\left[\sum_{j=1}^{k}ke_j\right]P_1$ 可知,每个 KGC 在不能得到用户私钥 $ds_A=\left[\sum_{j=1}^{k}t_j\right]P_1$ 的情况下,只能求出与自己持有的 ke_j 相关的 ds_A=$[d_2][ke_j]P_1$,存在椭圆曲线上求解离散对数难题,使得敌手根据 S=$[l]ds_A$ 与 ke_j 求得 $\left[\sum_{j=1}^{k}ke_j\right]P_1$ 是困难的.因此,只要存在任何一个可信 KGC,则本方案便可抵抗恶意 KGC 攻击.

对于群签名算法,敌手 E_2 为本方案中的恶意 KGC,其知道系统主密钥 ks 与其自己持有的 ke_j.在本群签名方案中,因为由多个 KGC 共同维护方案所需的系统参数,ks 由全部 KGC 共同商定,而 ke_j 仅自己知道,由用户签名私钥 $ds_A=[d_2]\left[\sum_{j=1}^{k}ke_j\right]P_1$ 与群私钥 $ds_{AG}=[d_2]\left[\sum_{j=1}^{k}ke_j\right]\left[\sum_{j=1}^{k}ke_j\right][d_1]P_1$ 可知,每个 KGC 只能求出与自己持有的 ke_j 相关的 ds_A=$[d_2][ke_j]P_1$ 与 $ds'_{AG}=[d_2]\left[\sum_{j=1}^{k}ke_j\right]\cdot ke_j\cdot[d_1]\cdot P_1$,存在椭圆曲线上求解离散对数难题,使得敌手根据 $\left[\sum_{j=1}^{k}ke_j\right]P_1$ 与 ke_j 求得 $\left[\sum_{j=1}^{k}ke_j\right]$ 是困难的.因此,只要存在任意可信 KGC,则本方案便可抵抗恶意的 KGC 攻击.

在区块生成与验证阶段中,主要节点负责生成区块,所生成区块中包含其自身签名,各节点需要验证后方可并入链中.除了主要节点,其余节点均不能生成区块,除了由主要节点生成的合法区块,任何新区块均为无效区块,保证了新生区块的不可伪造性.各个节点验证 TX 时,需要验证输入与输出的群签名,通过后才能并入区块,保证了交易信息的不可伪造性.

3.2.2 前向与后向安全性

当群签名方案的系统参数需要更新时,KGC 需重新商定 ks 以及根据各自持有的 ke_j 确定主私钥,向所有节点发放新的密钥对.以前的系统参数仍要保留,群成员节点可以根据当时生效的参数来验证更新前的签名.对于系统参数而言,由于 ks 与 ke_j 均为随机选取,所以二者在更新前后不存在联系,敌手无法根据当前阶段的密钥伪造更新前的密钥.若敌手持有更新前的密钥,也无法加入群,同时也无法伪造当前阶段正确的群签名.

3.3 方案匿名性分析

给定合法的群签名(h,P_3,S_1,S_2),从算法流程可知:签名验证过程中,仅使用群身份 ID_{GM} 作为公钥进行验证,来判断是否为群内成员节点,但不能验证具体成员节点身份.

由于 $S_1=(r_2^{-1})\cdot(r_1-h)\cdot ds_A, ds_A=[H_1(ID_A\|hid,N)+ks]^{-1}\left[\sum_{j=1}^{k}ke_j\right]P_1$,该算法为包含杂凑函数的单向算法,同时存在椭圆曲线上求解离散对数难题,使得确定签名者身份 ID_A 在计算上是不可行的.因为 $P_3=[r_2]P_{3'}$,存在椭圆曲线上求解离散对数难题,使得判断同一用户的两次不同签名是否关联,在计算上同样不可行,保证了方案的匿名性.本方案在交易流程中,节点间进行交易需要进行签名认证,双方需确认对方身份,在确认 TX 中,各节点仅能验证群签名(h,P_3,S_1,S_2)是否正确,无法获知具体签名者身份,在两次关联的 TX 中,仅上次输出与本次输入的 P_3 相同,判断此用户的其他交易生成的 P_3 与本次交易是否关联在计算上不可行.因此保证了方案的匿名性.

3.4 方案效率与安全性分析

本方案基于 SM9 算法改进设计,除了初始参数与密钥生成之外,签名验签步骤基本一致,所以计算代价与 SM9 数字签名算法基本相同.而本方案还可有效抵抗恶意 KGC 攻击,弥补了 SM9 数字签名算法的不足.

为了说明本方案的运算效率与安全性,本文列举几种典型方案进行对比.现定义符号 T_E 表示指数运算,T_M 表示群中元素点乘运算,T_B 表示双线性对运算.由于 ds_A 为区块链中群成员节点持有,可将 $g=e(ds_A,P_2)$视为预运算,不作为运算步骤考虑.可得到性能对比分析表,见表 1.

Table 1 Comparison of efficiency and security

表 1 方案效率与安全性对比

方案	签名效率	验签效率	第 1 类攻击	第 2 类攻击
文献[2]方案	$4T_M+7T_E$	$T_M+T_E+5T_B$	√	×
文献[23]方案	T_M+4T_E	$T_M+T_E+3T_B$	√	√
文献[24]方案	$3T_M+2T_E$	$2T_M+3T_B$	√	√
文献[25]方案	$3T_M+T_B$	$3T_M+T_B$	√	√
SM9 签名算法	T_M+T_E	$T_B+2T_E+T_M$	√	×
本方案	$2T_M+T_E$	T_M+3T_B	√	√

在上述运算过程中,双线性对运算消耗资源较多,因此主要比较该运算在方案中的使用次数[26].从表 1 中可以看出:本文的方案在验签步骤上较文献[2]减少 2 次双线性对运算,验签效率提高约 40%;与文献[23,24]相比,虽然双线性对运算的使用次数相同,但本方案指数运算分别减少 4 次与 2 次,计算效率整体得到提高.本方案与 SM9 算法与文献[25]相比整体效率相当.对于方案安全性,文献[2]与 SM9 签名算法均无法抵抗第二类攻击,本方案通过多 KGC 的方式,安全性更高,满足了区块链节点认证以及交易信息确认中保护身份隐私的需要.

除此之外,本文列举两种主流的区块链系统隐私保护方案进行对比.考虑到实际应用中可能发生的追责情况,方案应在保护隐私的同时,满足一定的溯源性,且为了满足高频率的交易请求,区块生成时间应在保证安全的基础上拥有较快的生成速率.对比分析表见表 2.

Table 2 Comparison of different privacy preserving schemes

表 2 隐私保护方案对比

方案	匿名性	交易关联性	溯源性	交易信息量
文献[10]方案	强	弱	弱	25KB
文献[11]方案	强	较弱	较弱	15KB
本方案	强	弱	较强	2KB~5KB

通过表 2 对比可以看出:在交易关联性方面,文献[11]方案由于交易发起方通过环签名的方式隐藏身份,但通过统计分析等方法,仍存在暴露关联交易的风险;本方案在具有强匿名性的同时,由于 $P_3=[r_2]P_{3'}$,同一节点用户的不同交易均存在密码学计算困难问题,无法证明关联,保证了弱关联性.在溯源性方面,由于文献[10]方案采

用货币“生成-销毁”以及零知识证明认证的方式来代替用户间的交易过程,导致溯源性弱;而本方案沿用区块链中的 UTXO 方式进行区块生成,使得交易仍可溯源,在实际场景应用中,主要节点需要公开身份,而本方案初始交易均需由主要节点发起,故可在需要情况下进行溯源追踪.在交易信息量方面,文献[10,11]方案每笔交易需要产生的数据量较大,本方案在保证性能的前提下,交易信息量分别为两种隐私保护方案的 1/5 与 1/3,减轻了区块容量的压力,方案更适用于实际应用,具有较高的安全性与通信效率.

4 方案仿真

本文主要测试方案中所使用的群签名算法的运行时间以及主要节点生成新区块后验证成功与并入链中所需的时间.方案仿真使用 Java 语言进行测试,使用 Windows 系统,CPU2.4GHz,内存为 4GB.新生区块由一个主要节点产生,并由 10 个次要节点进行验证.由图 6~图 8 可知,群签名生成与验证所需时间为 21.632ms 与 46.141ms,所需时间较短;对于生成交易信息过程,在节点确认信息无误的情况下,生成发送至主要节点的交易信息所需时间为 133.642ms,所需时间较短;而对于区块验证过程,在不考虑区块内容传输时间的情况下,过半数节点验证通过,新生区块合理并入链中所需时间为 63.572ms;主要节点产生新区块的间隔定为 2s,由此可知,在拥有 10 个次要节点时,一次交易从产生到有效所需的时间为 2.063s,交易时间相对较短,可以满足区块链交易实际需要.

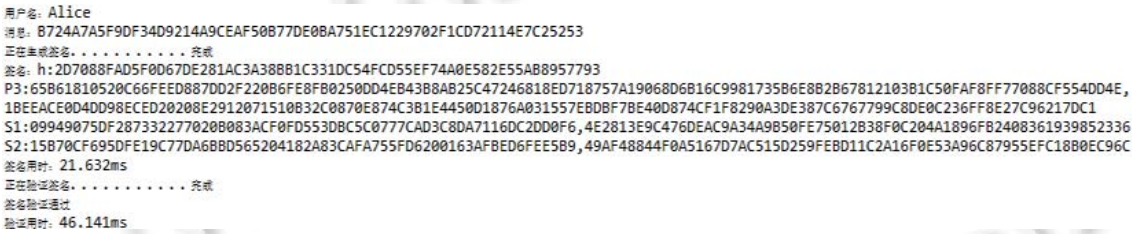

Fig.6 Time for signing and verifying

图 6 签名与验签所用时间

Fig.7 Time to generate transaction information

图 7 交易信息生成所用时间

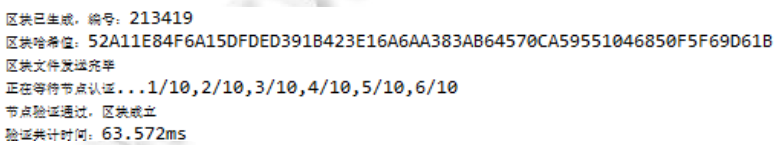

Fig.8 Time for block generation

图 8 区块并入成功所需时间

5 结 论

本文通过将 SM9 算法、群签名与区块链技术相结合,提出并设计了一种可应用于区块链环境中的隐私保

护方案,通过多 KGC 群签名机制隐藏了交易双方的节点身份.通过安全性证明与效率分析,本方案具有签名不可伪造性、可保证节点匿名性及前向安全性,计算效率较目前提出的方案有较大提升.综合而言,本方案在运算时间与安全性方面整体具有较大优势,可实现在节点间进行身份验证的同时,保护节点隐私的目的,符合联盟区块链部分去中心化和保护节点隐私的要求.本方案可应用于大量需要验证用户身份的场合,如房屋租赁、实物交易等等.如何根据具体应用场景简化交易流程,提高单位时间内的交易数量,可以作为下一阶段的研究工作.

References:

[1] Shao QF, Jin CQ, Zhang Z, Qian WN, Zhou AY. Blockchain: Architecture and research progress. Chinese Journal of Computers, 2018,41(5):969−988 (in Chinese with English abstract).

[2] Al-Riyami SS, Paterson KG. Certificateless public key cryptography. Proc. of the ASIACRYPT, 2003,2894(2):452−473.

[3] Yu Y, Mu Y, Wang G, Xia Q, Yang B. Improved certificateless signature scheme provably secure in the standard model. IET Information Security, 2012,6(2):102−110.

[4] Gong P, Li P. Further improvement of a certificateless signature scheme without pairing. Int'l Journal of Communication Systems, 2014,27(10):2083−2091.

[5] Tseng YM, Huang SS, Wu JD. Secure certificateless signature resisting to continual leakage attacks. In: Proc. of the Int'l Conf. on Applied System Innovation. 2017. 1263−1266.

[6] Swan M. Blockchain thinking: The brain as a decentralized autonomous corporation. IEEE Technology & Society Magazine, 2015, 34(4):41−52.

[7] Chiesa A, Green M, Liu JC, Miao PH, Miers I, Mishra P. Decentralized anonymous micropayments. In: Proc. of the Advances in Cryptology (EUROCRYPT 2017). 2017.

[8] Kosba A, Miller A, Shi E, Wen ZK, Papamanthou C. Hawk: The blockchain model of cryptography and privacy-preserving smart contracts. In: Proc. of the Security and Privacy. IEEE, 2016. 839−858.

[9] Qian WN, Shao QF, Zhu YC, Jin CQ, Zhou AY. Research problems and methods in blockchain and trusted data management. Ruan Jian Xue Bao/Journal of Software, 2018,29(1):150−159 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/5434.htm [doi: 10.13328/j.cnki.jos.005434]

[10] Miers I, Garman C, Green M, Rubin AD. Zerocoin: Anonymous distributed E-cash from Bitcoin. In: Proc. of the IEEE Symp. on Security & Privacy. 2013. 397−411.

[11] Shen N, Adam M. Ring confidential transactions. Ledger, 2016,1(1):1−18.

[12] Chaum D, Heyst EV. Group signatures. In: Proc. of the Advances in Cryptology (EUROCRYPT'91). Berlin, Heidelberg: Springer-Verlag, 1991. 257−265.

[13] Zhang G, Wang S. A certificateless signature and group signature schemes against malicious PKG. In:Proc. of the Int'l Conf. on Advanced Information Networking and Applications. IEEE Computer Society, 2008. 334−341.

[14] Chen H, Zhu CJ, Song RS. Efficient certificateless signature and group signature schemes. Journal of Computer Research and Development, 2010,47(2):231−237 (in Chinese with English abstract).

[15] Zhang Z, Ye Y. A new ID-based threshold group signature scheme. In: Proc. of the Int'l Conf. on Wireless Communications, Networking and Mobile Computing. IEEE, 2012. 1−4.

[16] Cheng X, Zhou S, Yu J, Li X, Ma H. A practical ID-based group signature scheme. Journal of Computers, 2012,7(11):842−849.

[17] Lin XD, Lu RX. GSIS: Group signature and ID-based signature-based secure and privacy-preserving protocol. In: Proc. of the Vehicular Ad Hoc Network Security and Privacy. John Wiley & Sons, Inc., 2015. 216−220.

[18] Bande AS, Shikalpure SG. Secure and privacy preserving group signature scheme with verifier local revocation. In: Proc. of the 2017 Int'l Conf. on Computational Intelligence in Data Science (ICCIDS 2017). Chennai, 2017. 1−5.

[19] Zhu LH, Gao F, Shen M, Li Y, Zheng B, Mao H, Wu Z. Survey on privacy preserving techniques for blockchain technology. Journal of Computer Research and Development, 2017,54(10):2170−2186 (in Chinese with English abstract).

[20] Kiayias A, Russell A, David B, Oliynykov R. Ouroboros: A provably secure proof-of-stake blockchain protocol. In: Proc. of the Int'l Cryptology Conf. (CRYPTO 2017). LNCS 10401, Springer-Verlag, 2017. 357−388.

[21] State Cryptography Administration. SM9 identity-based cryptographic algorithms. GM/T0044-2016 (in Chinese with English abstract).

[22] Zhang FT, Zhang FG, Wang YM. Group signature and its applications. Journal of China Institute of Communications, 2001,22(1): 77−85 (in Chinese with English abstract).

[23] Li YQ, Li JG, Zhang YC. Certificateless signature scheme without random oracles. Journal on Communications, 2015,36(4): 185−194 (in Chinese with English abstract).

[24] Tseng YM, Huang SS, Wu JD. Secure certificateless signature resisting to continual leakage attacks. In: Proc. of the Int'l Conf. on Applied System Innovation (ICASI 2017). 2017. 1263−1266.

[25] Chen Y, Zhao Y, Xiong H, Yue F. A certificateless strong designated verifier signature scheme with non-delegatability. Int'l Journal of Network Security, 2017,19(4):573−582.

[26] Fan AW, Yang ZF, Xie LM. Security analysis and improvement of strongly secure certificate less signature scheme. Journal on Communications, 2014,35(5):118−123 (in Chinese with English abstract).

附中文参考文献:

[1] 邵奇峰,金澈清,张召,钱卫宁,周傲英.区块链技术:架构及进展.计算机学报,2018,41(5):969−988

[9] 钱卫宁,邵奇峰,朱燕超,金澈清,周傲英.区块链与可信数据管理:问题与方法.软件学报,2018(1):150−159. http://www.jos.org.cn/1000-9825/5434.htm [doi: 10.13328/j.cnki.jos.005434]

[14] 陈虎,朱昌杰,宋如顺.高效的无证书签名和群签名方案.计算机研究与发展,2010,47(2):231−237.

[19] 祝烈煌,高峰,沈蒙,李艳东,郑宝昆,毛洪亮,吴震.区块链隐私保护研究综述.计算机研究与发展,2017,54(10):2170−2186.

[21] 国家密码管理局.SM9 标识密码算法.GM/T0044-2016.

[22] 张福泰,张方国,王育民.群签名及其应用.通信学报,2001,22(1):77−85.

[23] 李艳琼,李继国,张亦辰.标准模型下安全的无证书签名方案.通信学报,2015,36(4):185−194.

[26] 樊爱宛,杨照峰,谢丽明.强安全无证书签名方案的安全性分析和改进.通信学报,2014,35(5):118−123.

杨亚涛(1978－),男,河南汝州人,博士,副教授,主要研究领域为无线安全,密码学.

张筱薇(1995－),女,硕士生,主要研究领域为信息安全,密码学.

蔡居良(1993－),男,硕士生,主要研究领域为信息安全,密码学.

袁征(1968－),女,博士,教授,博士生导师,主要研究领域为密码设计,密码分析.