基于区块链的 VANET 无证书聚合签名方案

崔贵焕,柳　毅
(广东工业大学 计算机学院,广东 广州 510006)

摘　要:车载自组网(VANET)中频繁的通信和海量数据交互更易泄露车辆身份、位置、行驶路线等信息,交互验证的过程中证书开销会越来越大而且更容易遭受恶意攻击。为了解决以上问题,提出了基于区块链的 VANET 无证书聚合签名方案,消除证书开销,使用假名保护用户身份隐私。使用椭圆曲线加密算法实现无证书聚合签名,结合区块链的分布式存储实现信息共享、道路信息透明以及对恶意参与者的追踪。搭建以太坊私有链进行仿真,利用智能合约实现访问控制和交易,实验结果表明,在实现强匿名性、不可链接性、消息完整性、不可否认、可追踪、防篡改的安全性能的同时,通信开销相比同类方案中使用双线性配对方法降低了至少 85.8%。

关键词:车载自组网;区块链;无证书聚合签名;隐私保护;智能合约
中图分类号:TP309.2　　**文献标识码**:A　　**文章编号**:1673-629X(2023)10-0066-07
doi:10.3969/j.issn.1673-629X.2023.10.011

A Certificateless Aggregate Signature Scheme for VANET Based on Blockchain

CUI Gui-huan,LIU Yi
(School of Computer,Guangdong University of Technology,Guangzhou 510006,China)

Abstract:Frequent communication and massive data interaction in the vehicular ad hoc network (VANET) are more likely to disclose vehicle identity,location,driving route and other information. In the process of interactive verification,the certificate overhead will be larger,and it will be more vulnerable to malicious attacks. To solve these problems,a certificateless aggregate signature (CLAS) scheme for VANET based on blockchain is proposed,which eliminates certificate overhead and uses pseudonyms to protect users´ identity privacy. CLAS is realized by using the elliptic curve cryptography (ECC) algorithm,and information sharing,road information transparency and tracking of malicious participants are realized by combining the distributed storage of the blockchain. It builds the Ethereum private chain for simulation and uses the smart contract to achieve access control and transaction. The experimental results show the communication cost is reduced by at least 85.8% compared with the bilinear pairing method in the same scheme,while realizing the security performance of strong anonymity,unlinkability,message integrity,non-denial,traceable and tamper-proof.

Key words:vehicular ad hoc network/VANET;blockchain;certificateless aggregate signature;privacy protection;smart contract

0　引　言

近年来,物联网(IoT)[1]的快速发展,万物互联的概念经常被提及,车载自组网[2](VANET)利用物联网和现有科技进行车与 X(即车与车、基础设施、服务平台等)之间的网络通信,由于 VANET 通信是开放的,如果其中车辆共享信息不被保护,就可能会导致数据遭受被篡改、重放、拒绝服务等攻击,车主就可能面临非法追踪等安全问题。为了克服这些问题及最小化证书管理开销,无证书方案[3]被提出,后来为降低签名验证开销,聚合签名[4]概念被提出,并应用于移动支付、车联网[5-6]、数据安全领域[7]。结合二者优点,研究人员相继提出无证书聚合签名(CLAS)方案[8~22],将不同车辆产生的 n 个签名聚合成一个,运行聚合验证算法来验证,从而降低签名大小和验证开销。Gong 等[8]首次提出两种 CLAS 方案,并定义了安全模型。Horng 等[9]为车载传感器网络提出 CLAS 方案,后来被证明对恶意但被动的 KGC 攻击并不安全。Kumar 等[10]为 VANET 设计 CLS 方案和 CLAS 方案,Zhong 等[11]提出全聚合方案,但难以抵抗第二类敌手的签名伪造攻击。文献[12-13]都是基于双线性配对。Wang 等[14]

收稿日期:2023-01-10　　**修回日期**:2023-05-11
基金项目:广东省重点领域研发计划项目(2021B0101200002)
作者简介:崔贵焕(1992-),女,硕士研究生,CCF 会员(G6785G),通信作者,研究方向为信息安全、区块链;柳　毅(1976-),男,博士,教授,CCF 会员(13840M),研究方向为网络与信息安全。

提出 VANET 标准模型中的 CLAS 方案,在文献[15]基础上用于车联网。

为降低开销,Cui 等[16]提出不使用双线性配对的 CLAS 方案,给每辆车配备防篡改装置,但以这种方式实现防篡改太主观且安全性不能保障。Kamil 等[17]对文献[16]提出改进,但仍无法抵抗伪造攻击,后来他们提出新的聚合方案[18]。Zhao 等[19]证明了 Kamil 方案不足以抵御两类敌手的攻击并提出改进方案,但其方案的构建不正确。Han 等[20]使用聚合服务器进行聚合操作,但未提及聚合器的安全问题。随着区块链的广泛应用,在文献[21]中,Ali 等提出基于区块链用于 V2I 通信的无证书公钥签名方案。Ren 等[22]提出用两个双线性配对操作验证签名,但需昂贵计算成本。

该文提出基于区块链的 VANET 无证书聚合签名方案,将区块链技术和聚合签名应用于 VANET 中,减少车辆间的通信时间和实现高效的消息交换。与其他基于区块链的方案相比,该方案结合智能合约提升用户参与度。主要工作如下:

(1)提出基于区块链的无证书聚合签名方案,节省证书开销,提高传输效率,保护车辆的隐私。

(2)使用假名策略注册区块链发布任务,即使区块链上交易与现实生活重合,也能降低隐私暴露的可能。既保护隐私,又能对路况进行准确广播。

(3)添加智能合约实现访问控制和奖惩,便于用户获得便捷信息与相应奖励,确保其参与积极性。

在随机预言机模型下证明了该方案的安全性。利用链上——链下存储,实现六大安全性,与其它方案相比,该方案通信开销更低。

1　预备知识

1.1　ECDLP 困难性问题

椭圆曲线离散对数问题(ECDLP):两个大素数 p, q 和椭圆曲线 $E:y^3+ax+b(\mathrm{mod}p)$,其中 $a,b\in F_p$, $4a^3+27b^2\neq 0$,选取 q 阶群 G,生成元 P 为椭圆曲线上的一个点。已知 P 和 $aP\in G$,ECDLP 的目标是计算 $a\in Z_q^*$。

1.2　区块链

区块链[23]技术由中本聪提出,其本质是一个去中心化的分布式数据库,保存着包含所有交易且会不断增加的区块列表。它在参与节点之间维护一个数据块的链式结构,是个基于密码学的持续增长和不可变的数据记录[24]。目前研究人员正尝试将其应用金融供应链、位置隐私、匿名信誉系统等领域。

1.3　智能合约

智能合约[25]作为区块链网络上的去中心化程序运行,能够解决集中化应用程序中的数据消耗和延迟问题。在预定义条件下自动执行,而无需干预中心化的第三方,程序不可变且会永久保留在区块链网络。自动精准执行的特点提高了其信任度,适用于很多应用程序,被广泛应用于区块链。

2　基于区块链的无证书聚合签名方案

2.1　方案模型

如图 1 所示,该方案包含以下实体:交通管理中心(Traffic Management Center, TMC)、密钥生成中心(Key Generation Center, KGC)、区块链(Blockchain)、路边单元(Road Side Units, RSUs)和装有通信车载单元的车辆(Vehicle)。其中 TMC、KGC、RSU 间通信通过诸如传输层安全协议的安全有线网络进行,车辆间、车辆与 RSU 通过 DSRC 协议通信[26]。

(1)TMC:交通管理中心与 KGC 共同生成公共参数。参与生成假名,存储车辆真假名索引表、RSU 发送的数据。初始化后进入离线状态,直到接收虚假消息报告,追踪来源并处罚。

(2)KGC:与 TMC 共同生成系统参数,当车辆节点在 KGC 完成注册后,KGC 为其发放部分私钥。

(3)Vehicle:与其它实体通信,频繁广播交通信息。与 TMC 共同生成假名并根据需要更换假名。

(4)RSU:管理相应区域中的广播消息。RSU 验证并接收交通广播,将验证成功后的数据发送到 TMC,执行签名聚合操作。如发现虚假消息,上传消息到区块链防篡改同时上报给 TMC。

(5)Blockchain:负责对交易和聚合签名的验证和存储,利用智能合约实现访问控制和支付操作。

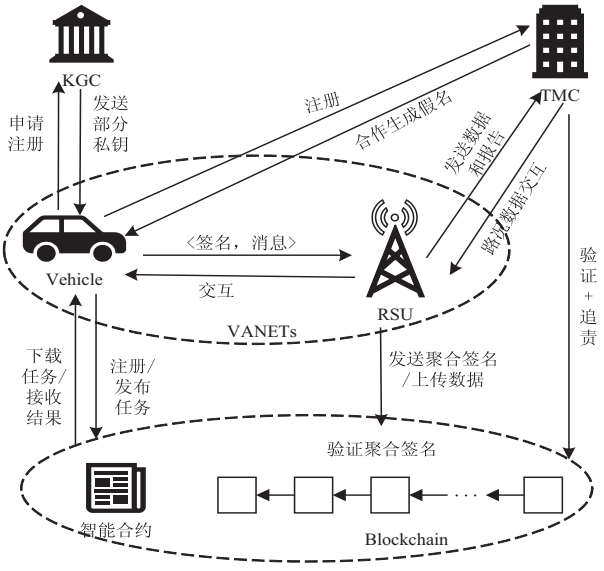

图 1　方案模型

2.2　方案构造

本节将详细描述所提方案,方案的部分符号说明如表 1 所示。

表 1 方案的部分符号说明

符号	描述	符号	描述
T_{pub}	TMC 的公钥	PSU_i	V_i 假名
K_{pub}	KGC 的公钥	PSK_{PSU_i}	V_i 部分私钥
p,q	两个大素数	VPK_i/ SK_i	V_i 公/私钥
G,p	椭圆曲线群及其生成元	x_i	V_i 的秘密值
H_0,H_1,H_2,H_3	安全哈希函数	σ_i	V_i 的签名
(D_j,Y_j)	RSU 身份	$\sigma=(U,S)$	聚合签名
RID_i	V_i 真名	T_i	假名生成时间

(1)系统初始化:该算法生成系统参数,由 TMC 与 KGC 执行。使用安全参数 s,TMC 和 KGC 选择两个大素数 p,q 和椭圆曲线 $E:y^3+ax+b(\mathrm{mod}p)$,其中 $a,b\in F_p$,$4a^3+27b^2\neq 0$,选取 q 阶群 G,生成元 P 为椭圆曲线上的一个点。KGC 随机选择主密钥 $a\in Z_q^*$,并计算 $K_{pub}=aP$。TMC 随机选择 $b\in Z_q^*$,并计算 $T_{pub}=bP$。选择 4 个安全哈希函数:$H_0:G\rightarrow Z_q^*$,$H_1:\{0,1\}^*\times G\rightarrow Z_q^*$,$H_2:\{0,1\}^*\times G\times G\times\{0,1\}^*\rightarrow Z_q^*$,$H_3:\{0,1\}^*\times\{0,1\}^*\times\{0,1\}^*\times G\times\{0,1\}^*\rightarrow Z_q^*$,生成公共参数:params = $\{p,q,G,P,K_{pub},T_{pub},H_0,H_1,H_2,H_3\}$。

(2)RSU 注册:RSU 向 TMC 注册,RSU_j 随机选择 $y_j\in Z_q^*$,计算公钥 $Y_j=y_jP$,TMC 为 RSU 生成身份标识 $D_j\in\{0,1\}^*$ 并将 (D_j,Y_j) 存入索引表。

(3)车辆假名生成:该算法由 V_i 和 TMC 执行。当车辆 V_i 加入 VANET 前,TMC 与 V_i 共同生成假名 PSU_i,并且车辆可以根据对所在区域隐私保护强度需求重新申请假名即变更假名。同时,TMC 建立 V_i 的假名和真实身份索引 (PSU_i,RID_i) 便于追踪。假名生成步骤:(a) V_i 随机选择参数 $\alpha_i\in Z_q^*$,$PID_{i,1}=\alpha_iP$,其中计算 $M_{i,1}=H_0(\alpha_iT_{pub})\oplus RID_i$,$RID_i$ 为 V_i 真实身份。之后 V_i 发送 $(RID_i,PID_{i,1},M_{i,1})$ 至 TMC。(b)TMC 验证 $RID_i=M_{i,1}\oplus H_0(bPID_{i,1})$ 是否相等,若相等,则计算 $PID_{i,2}=RID_i\oplus H_1(bPID_{i,1},T_i)$,其中 T_i 为生成假名时间,得到假名:$PSU_i=\{PID_{i,1},PID_{i,2},T_i\}$。$V_i$ 隔一段时间可以选择执行该算法更换新的假名。

(4)部分私钥生成:V_i 使用假名 PSU_i 向 KGC 发出请求部分私钥,KGC 随机选择 $r_i\in Z_q^*$,计算 $R_i=r_iP$,$h_{2i}=H_2(PSU_i,R_i,K_{pub},T_i)$,得部分私钥:$PSK_{PSU_i}=(r_i+ah_{2i})\mathrm{mod}p$,随后 KGC 通过安全通道发送 $\{PSK_{PSU_i},R_i,PSU_i\}$ 给 V_i。接收的时候,首先验证等式 $PSK_{PSU_i}P=R_i+h_{2i}K_{pub}$ 证明其合法性。

(5)车辆公私钥生成:车辆 V_i 随机选择 $x_i\in Z_q^*$ 作为秘密值,计算 $X_i=x_iP$,得到公私钥分别为:$SK_i=(x_i,PSK_{PSU_i})$、$VPK_i=(X_i,R_i)$。

(6)签名:为确保身份验证和消息完整性,消息 $m_i\in\{0,1\}^*$ 由对应车辆 V_i 签名后才能发出并上传至区块链,V_i 使用当前时间 TP_i,当前假名 PSU_i,公私钥 $VPK_i=(X_i,R_i)$、$SK_i=(x_i,PSK_{PSU_i})$ 进行签名,步骤:V_i 选择 $u_i\in Z_q^*$,计算:$U_i=u_iP$、$h_{1i}=H_1(PSU_i,X_i)$、$h_{3i}=H_3(PSU_i,m_i,x_i,U_i,TP_i)$、$S_i=[u_i+h_{3i}(PSK_{PSU_i}+h_{1i}x_i)]\mathrm{mod}p$,签名 $\sigma_i=(U_i,S_i)$,然后 V_i 广播签名消息 $\{PSU_i,VPK_i,m_i,TP_i,\sigma_i\}$。

(7)签名验证:RSU 接收到车辆广播的签名消息 $\{PSU_i,VPK_i,m_i,TP_i,\sigma_i\}$ 后执行该算法,对同时接收到的签名消息用公式 $S_iP=U_i+h_{3i}(R_i+h_{2i}K_{pub}+h_{1i}X_i)$ 验证。其中 $h_{1i}=H_1(PSU_i,X_i)$,$h_{2i}=H_2(PSU_i,R_i,K_{pub},T_i)$。如果验证通过则发送消息至 TMC 存储,并对同一时间接收到的消息进行聚合。如果有消息验证失败,则将消息发送至 TMC 进行存储的同时向 TMC 发送验证失败报告,TMC 通过区块链和身份索引表追踪。

(8)聚合签名:RSU 从不同车辆接收到签名消息 $\{PSU_i,VPK_i,m_i,TP_i,\sigma_i\}$,验证后,将接收到的有效签名 $\sigma_i=(U_i,S_i)$ 进行聚合。计算式(1)(2),其中 n 为签名个数。聚合签名为 $\sigma=(U,S)$。区块链存储聚合签名和消息 $\{D_j,(PSU_i,VPK_i,m_i,TP_i)_{i\in\{1,2,\cdots,n\}},\sigma\}$ 哈希值。

$$U=\sum_{i=1}^{n}U_i \tag{1}$$

$$S=\sum_{i=1}^{n}S_i \tag{2}$$

(9)聚合验证:区块链上的矿工收到聚合结果进行验证。输入聚合签名 σ、params、$VPK_i=(X_i,R_i)$。首先计算 h_{1i}、h_{2i}、h_{3i},矿工验证等式(3),其中 n 为签名个数,若等式成立,将其打包上传到区块链。

$$SP=U+\sum_{i=1}^{n}h_{3i}(R_i+h_{2i}K_{pub}+h_{1i}X_i) \tag{3}$$

(10)数据通信:车辆 V_i 使用假名加入 VANET,向 KGC 请求部分私钥,生成自己的公私钥。车辆在行驶过程中广播路况等信息,所发消息均经过签名,RSU 执行签名验证并将获得数据发送 TMC,同时聚合已验证成功的签名,将聚合签名以及向 TMC 所发消息的哈希值存储至区块链上;若部分验证失败,将验证成功的数据发送 TMC,验证成功的签名聚合后上链,同时向 TMC 报告验证失败消息以便追踪惩罚。车辆主要从 RSU 中获得可验证聚合签名的可信消息,也通过 V2V 交互获得信息。矿工验证聚合签名并发布到区块链。另外,车辆使用假名加入区块链,通过触发智能合约发送查询任务以及交易,不经过广播交互来查询相关服务信息,其他矿工(可以是车辆节点)解决任务

可获取奖励。如果接收任务结果验证为假,可向 TMC 举报并上链存证,TMC 追踪发布假消息的节点,然后向 RSU 发布命令撤销该节点并将其获得的该交易款退回。

其中步骤(1)~(9)为无证书签名及验证过程,步骤(10)描述了结合区块链实现数据的安全传输。

2.3　正确性证明

所提方案的正确性可以证明如下:

(1)部分私钥验证的正确性。

$$\begin{aligned}\mathrm{PSK}_{\mathrm{PSU}_i}P &= (r_i + ah_{2i})P = r_iP + ah_{2i}P = \\ &R_i + h_{2i}aP = R_i + h_{2i}K_{\mathrm{pub}}\end{aligned} \tag{4}$$

(2)签名验证的正确性。

$$\begin{aligned}S_iP &= [u_i + h_{3i}(\mathrm{PSK}_{\mathrm{PSU}_i} + h_{1i}x_i)]P = \\ &u_iP + h_{3i}(\mathrm{PSK}_{\mathrm{PSU}_i} + h_{1i}x_i)P = \\ &U_i + h_{3i}(r_iP + sh_{2i}P + h_{1i}x_iP) = \\ &U_i + h_{3i}(R_i + h_{2i}K_{\mathrm{pub}} + h_{1i}X_i)\end{aligned} \tag{5}$$

(3)聚合验证的正确性。

$$\begin{aligned}\mathrm{SP} &= \sum_{i=1}^{n}[u_i + h_{3i}(\mathrm{PSK}_{\mathrm{PSU}_i} + h_{1i}x_i)]P = \\ &\sum_{i=1}^{n}\{u_iP + h_{3i}(\mathrm{PSK}_{\mathrm{PSU}_i}P + h_{1i}x_iP)\} = \\ &\sum_{i=1}^{n}U_i + \sum_{i=1}^{n}h_{3i}(r_iP + ah_{2i}P + h_{1i}x_iP) = \\ &U + \sum_{i=1}^{n}h_{3i}(R_i + h_{2i}K_{\mathrm{pub}} + h_{1i}X_i)\end{aligned} \tag{6}$$

3　安全分析

3.1　安全模型

为了保护车辆隐私,该方案考虑了强匿名、不可链接性、消息完整性、不可否认、可追踪、防篡改,并抵御以下两种对手的攻击。对手 A_1:恶意用户的公钥替换攻击,即 A_1 可替换合法用户的公钥,但无法获取 KGC 系统主密钥。对手 A_2:恶意但被动的 KGC 攻击,即 A_2 可以访问 KGC 主密钥,但不能替换任何车辆的公钥。

3.2　安全性证明

引理 1:若对手 A_1 可以在随机预言机模型中以不可忽略的概率 ε_1 在多项式时间内伪造出有效签名,那么在多项式时间内,存在挑战者 C_1 在不可忽略的概率 ε' 解决 ECDLP,则认为该方案在对手 A_1 自适应选择消息和身份攻击下具有不可伪造性。

证明:假设挑战者算法 C_1 能有效解决 ECDLP 困难性问题,输入 (P,aP),目标是在交互中计算 a。

(1)初始化阶段:C_1 执行系统初始化算法,随机选择 s 作为主密钥,计算公共参数 params 并发送给 A_1,秘密保存 s。

(2)查询阶段:本阶段 A_1 提出一系列查询,这些查询由挑战者自适应回答。C_1 维护并初始化以下列表:$L_1=\{(\mathrm{PSU}_i,X_i)\}$,$L_2=\{(\mathrm{PSU}_i,R_i,K_{\mathrm{pub}},T_i)\}$,$L_3=\{(\mathrm{PSU}_i,m_i,x_i,U_i,\ \mathrm{TP}_i)\}$,$L_{\mathrm{PSK}}=\{(\mathrm{PSK}_{\mathrm{PSU}_i},R_i,\mathrm{PSU}_i)\}$,$L_{\mathrm{user}}=(\mathrm{PSU}_i,X_i,R_i,x_i,\mathrm{PSK}_{\mathrm{PSU}_i})$。

H_1 查询:当 A_1 询问 $H_1(\mathrm{PSU}_i,X_i)$ 时,如果 L_1 中存在元组 $(\mathrm{PSU}_i,X_i,h_{1i})$,$C_1$ 返回 h_{1i},如果不存在,则 C_1 随机选择 $h_{1i}\in Z_q^*$ 并设置 $h_{1i}=H_1(\mathrm{PSU}_i,X_i)$,然后将 h_{1i} 返回 A_1 并将元组 $(\mathrm{PSU}_i,X_i,h_{1i})$ 插入列表 L_1。H_2 查询:当 A_1 询问 $H_2(\mathrm{PSU}_i,R_i,K_{\mathrm{pub}},T_i)$ 时,如果 L_2 存在元组 $(\mathrm{PSU}_i,R_i,K_{pub},T_i,h_{2i})$,$C_1$ 返回 h_{2i},若没有,则 C_1 随机选择 $h_{2i}\in Z_q^*$ 并设置 $h_{2i}=H_2(\mathrm{PSU}_i,R_i,K_{\mathrm{pub}},T_i)$,然后将 h_{2i} 返回给 A_1 并将 $(\mathrm{PSU}_i,R_i,K_{\mathrm{pub}},T_i,h_{2i})$ 插入列表 L_2。H_3 查询:A_1 询问 $H_3(\mathrm{PSU}_i,m_i,x_i,U_i,\mathrm{TP}_i)$ 时,如果 L_3 中存在元组 $(\mathrm{PSU}_i,m_i,x_i,U_i,\mathrm{TP}_i,h_{3i})$,$C_1$ 返回 h_{3i},如果不存在,则 C_1 随机选择 $h_{3i}\in Z_q^*$ 并设置 $h_{3i}=H_3(\mathrm{PSU}_i,m_i,x_i,U_i,\ \mathrm{TP}_i)$,并将 h_{3i} 返回 A_1,将元组 $(\mathrm{PSU}_i,m_i,x_i,U_i,\mathrm{TP}_i,h_{3i})$ 插入 L_3。

(3)部分私钥 $\mathrm{PSK}_{\mathrm{PSU}_i}$ 查询:当 A_1 关于 PSU_i 部分私钥的查询,如若 L_{PSK} 中存在元组 $(\mathrm{PSK}_{\mathrm{PSU}_i},R_i,\mathrm{PSU}_i)$,则 C_1 返回 $\mathrm{PSK}_{\mathrm{PSU}_i}$。反之若 $\mathrm{PSU}_i=\mathrm{PSU}^*$,$C_1$ 终止,若 $\mathrm{PSU}_i\neq\mathrm{PSU}^*$,$C_1$ 随机选择 $c_i,d_i\in Z_q^*$,令 $c_i=\mathrm{PSK}_{\mathrm{PSU}_i}$,$d_i=H_2(\mathrm{PSU}_i,R_i,K_{\mathrm{pub}},T_i)$,计算 $R_i=\mathrm{PSK}_{\mathrm{PSU}_i}P-d_iK_{\mathrm{pub}}$ 后 C_1 添加 $(\mathrm{PSU}_i,R_i,K_{\mathrm{pub}},T_i,d_i)$ 到 L_2,添加 $(\mathrm{PSK}_{\mathrm{PSU}_i},R_i,\mathrm{PSU}_i)$ 至 L_{PSK}。

(4)创建用户查询:当 C_1 接收到 A_1 进行创建用户查询时,如果在列表 L_{user} 中存在着元组 $(\mathrm{PSU}_i,X_i,R_i,x_i,\mathrm{PSK}_{\mathrm{PSU}_i})$,则返回当前公钥 $\mathrm{VPK}_i=(X_i,R_i)$,否则 C_1 执行如下操作:如果 $\mathrm{PSU}_i=\mathrm{PSU}^*$,$C_1$ 选择 $c_i,x_i\in Z_q^*$ 计算 $R_i=c_iP,X_i=x_iP$ 后将 $(\mathrm{PSU}_i,X_i,R_i,x_i,\ \perp)$($\perp$ 表示空)存入 L_{user},返回公钥 $\mathrm{VPK}_i=(X_i,R_i)$,如果 $\mathrm{PSU}_i\neq\mathrm{PSU}^*$,$C_1$ 从 L_{PSK} 中查找元组 $(\mathrm{PSK}_{\mathrm{PSU}_i},R_i,\mathrm{PSU}_i)$,并选择 $x_i\in Z_q^*$ 令 $X_i=x_iP$ 输出 $\mathrm{VPK}_i=(X_i,R_i)$ 将 $(\mathrm{PSU}_i,X_i,R_i,x_i,\mathrm{PSK}_{\mathrm{PSU}_i})$ 存入 L_{user}。

(5)秘密值查询:A_1 进行该查询时,C_1 执行:当 $\mathrm{PSU}_i=\mathrm{PSU}^*$,$C_1$ 终止,当 $\mathrm{PSU}_i\neq\mathrm{PSU}^*$,$C_1$ 从 L_{user} 中查找 $(\mathrm{PSU}_i,X_i,R_i,x_i,\mathrm{PSU}_{\mathrm{PSU}_i})$ 并将 x_i 发给 A_1,若 L_{user} 中不存在,C_1 执行创建用户查询添加 x_i 到 L_{user},返回秘密值 x_i。

(6)公钥替换:A_1 想要替换 PSU_i 的公钥,选择新公钥后,C_1 从 L_{user} 中查找元组 $(\mathrm{PSU}_i,X_i,R_i,x_i,\mathrm{PSK}_{\mathrm{PSU}_i})$,然后更新列表为 $(\mathrm{PSU}_i,X_i',R_i',\perp,\perp)$。

(7)签名查询:当 C_1 收到询问 A_1 的签名 (PSU_i,m_i),若 $\mathrm{PSU}_i\neq\mathrm{PSU}^*$,$C_1$ 从 $L_1L_2L_{\mathrm{user}}$ 查找相应元组,选择 $u_i,h_{3i}\in Z_q^*$ 计算 $U_i=u_iP$,$S_i=[u_i+h_{3i}(\mathrm{PSK}_{\mathrm{PSU}_i}+h_{1i}x_i)]\bmod p$ 后生成有效签名 $\sigma_i=(U_i,S_i)$ 返回 A_1,将 $(\mathrm{PSU}_i,m_i,x_i,U_i,\mathrm{TP}_i,h_{3i})$ 添加到列表 L_3。若 $\mathrm{PSU}_i=$

PSU^*，C_1随机选择 $S_i \in Z_q^*$，计算 $U_i = S_iP - h_{3i}(R_i + h_{2i}K_{pub} + h_{1i}x_i)$，返回有效签名 $\sigma_i = (U_i, S_i)$ 给 A_1，并将 $(PSU_i, m_i, x_i, U_i, TP_i, h_{3i})$ 添加到 L_3。现在 A_1根据单个签名计算出 $\sigma = (U, S)$。

(8)伪造阶段：最后，A_1返回一组由 n 个车辆用户的通信假名 $PSU_i(i = 1 \sim n)$、对应的公钥 VPK_i、n 条消息 m_i、消息时间戳 TP_i 和一个伪造的聚合签名 $\sigma^* = (U^*, S^*)$。如果 $PSU_i \neq PSU^*$，算法 C_1 终止；如果 $PSU_i = PSU^*$，首先将 $\sigma^* = (U^*, S^*)$ 表示为 $\sigma^{*(1)} = (U^{*(1)}, S^{*(1)})$，由分叉引理 C_1在相同的以上询问操作下设置 H_3 产生不同的哈希值，A_1获得另外 2n 个伪造聚合签名 $\sigma^{*(j)} = (U^{*(j)}, S^{*(j)})(j = 2 \sim 2n + 1)$，这样就有了 $2n + 1$ 个聚合验证等式，因 $\sigma^{*(j)}$ 满足聚合验证方程，有 $S^{*(j)}P = \sum_{i=1}^{n} U_i^* + \sum_{i=1}^{n} h_{3i}^{*(j)}(R_i^* + h_{2i}^* K_{pub} + h_{1i}^* X_i)$，$u_i, r_i, a(i = 1 \sim n)$ 分别表示 $U_i R_i K_{pub}$ 的离散对数，其中 $U_i = u_iP$，$R_i = r_iP$，$K_{pub} = aP$，这些等式得到方程：$S^{*(j)} = \sum_{i=1}^{n} u_i^* + \sum_{i=1}^{n} h_{3i}^{*(j)}(r_i^* + ah_{2i}^* + h_{1i}^* x_i)$ $(j = 1 \sim 2n + 1)$，方程中 $u_i, r_i, x_i, a(i = 1 \sim n)$ 对于 C_1是未知的，现在 C_1根据以上线性无关方程求解这些未知值，并输出 a 作为 ECDLP 的解。

如要成功伪造签名，C_1输出 a 需满足以下条件：E_1：C_1在部分私钥和签名查询时未终止；E_2：A_1伪造的签名有效；E_3：在伪造身份中存在 $PSU_i = PSU^*$。

在询问阶段，如果 $PSU_i = PSU^*$ 的时候 C_1会终止，假设 $pr[PSU_i = PSU^*] = \theta$，则 C_1不终止的概率是 $1 - \theta$，则 $pr[E_1] \geqslant (1 - \theta)^{q_{psk} + q_{sig}}$，由对手 A_1以不可忽略的概率 ε_1 在多项式时间内伪造出有效的签名可知 $pr[E_1 \mid E_2] \geqslant \varepsilon$，另外，同时满足以上条件的 PSU_i，有 1 个 $PSU_i = PSU^*$，其余 $k - 1$ 个 $PSU_i \neq PSU^*$，$pr[E_1 \mid E_2 \wedge E_3] \geqslant \theta(1 - \theta)^{k-1}$，满足以上挑战者在不可忽略的概率 $\varepsilon' = \theta(1 - \theta)^{q_{psk} + q_{sig} + k - 1}\varepsilon_1$ 解决了椭圆离散对数难题。这与公理矛盾。其中 q_{psk} 为部分私钥查询次数，q_{sig} 为签名查询次数。

引理 2：如果对手 A_2可以在随机预言机模型中以不可忽略的概率 ε_2 在多项式时间内伪造出有效的签名，那么在多项式时间内，则存在挑战者 C_2在不可忽略的概率 ε'' 解决 ECDLP，则认为该方案在对手 A_2自适应攻击下具有不可伪造性。

证明：证明过程同引理 1，在此不再赘述。

3.3 安全需求分析

(1)强匿名性和不可链接性。

车辆用户 V_i 和 TMC 生成假名时，V_i 会随机选择 $\alpha_i \in Z_q^*$，通过两步来生成假名，V_i 掌握假名使用期限，尽管区块链具有透明性，利用假名注册区块链来发布任务，从而保护车辆用户的隐私，任何人无法通过两条或多条信息链接到同一用户并实现强匿名。

(2)消息完整性和不可否认。

从引理 1 和引理 2 的不可伪造性证明中也能看到在满足身份认证的同时充分保证了消息完整性。用户签名时会利用安全哈希函数，而且 RSU 会将验证失败的信息和聚合后的 hash 值上传区块链，TMC 通过哈希运算比较结果值进行监管，且一旦签名被冒用验证等式不会成立，多方验证保证不可否认。

(3)可追踪和防篡改。

由于恶意参与者不可避免，匿名保护车辆隐私，所以 TMC 拥有追查车辆身份的权利。如出现相应事件，RSU 将消息上链并报告假名给 TMC，TMC 通过区块链及索引表进行追踪。区块链上的发布如要修改，需重新发布，所有消息都可供追溯，聚合后的签名哈希值存入区块链，监管机构可有效追溯消息来认定车辆责任。

4 实验及性能分析

本节将从安全性、计算开销、通信开销等方面进行分析。使用 2 台 PC：Intel(R) Core(TM) i5-4460 CPU @ 3.20 GHz 和 AMD R5 4600H @3.00 GHz and 16 GB of RAM，通过 IntelliJ IDEA 调用 JPBC 库量化操作的时间消耗，在 64 位 Ubuntu18.04 下构建以太坊私链模拟车辆加入区块链后节点的交互通信以及交易过程，使用 truffle 框架实现界面交互，对智能合约主要函数的 gas 消耗和调用函数的响应时间进行测试。

4.1 安全性能分析

首先在安全性能上从 8 个方面与文献[14-17,21-22]进行了对比，如表 2 所示。文中方案不基于双线性配对运算，并且在强匿名性、不可链接性、可追踪性等方面表现优于其他方案。

4.2 开销分析

文中方案在计算开销和通信开销两方面与文献[14-15,21-22]进行对比，如表 3 和表 4 所示。其中 T_{bp} 为双线性配对运算时间，T_{bp-mul} 为双线性配对乘法运算时间，T_{bp-add} 为双线性配对加法运算时间，$T_{ECC-mul}$ 为椭圆曲线乘法运算时间，$T_{ECC-add}$ 为椭圆曲线加法运算时间，T_h 为单向哈希时间，分别为：6.086 ms，1.018 ms，0.007 ms，0.758 ms，0.047 ms，0.000 1 ms。

计算开销如表 3，文中方案中消息签名、RSU 验证开销、矿工聚合验证开销均较低。通信开销如表 4，其中双线性群 G_1、椭圆曲线群 G、Z_q^* 中元素、时间戳分别为 128 B、40 B、20 B、4 B。文献[21]中签名 $\sigma_i \in G_1$ 长度为 $|G_1| = 128$ bytes，该方案单个签名中包括 PID_i

$=(\mathrm{PID}_{i,1}\in G_1,\mathrm{PID}_{i,2}\in Z_q^*)$、$\sigma_i\in G_1$、$T_i$、$\mathrm{PK}_i(R_i\in G_1,U_i\in G_1)$ 共 536 bytes,传输聚合签名 σ_{agg},n 条消息,n 个假名,n 个公钥,需 $(3n+1)|G|+n|Z_q^*|$。文中方案传输签名消息共需 168 bytes,传输聚合签名消息 $\{D_j,(\mathrm{PSU}_i,\mathrm{VPK}_i,m_i,\mathrm{TP}_i)_{i\in\{1,2,\cdots,n\}},\sigma\}$ 所需通信开销为 $(n+2)|G|+(n+1)|Z_q^*|+2n|T|$。

表 2　安全性能对比

方案	强匿名性	不可链接性	是否使用双线性配对	可追踪性	防篡改	不可否认性	抵抗 A_1 攻击	抵抗 A_2 攻击
文献[14]	–	–	是	–	–	–	√	√
文献[15]	–	√	是	√	–	√	√	√
文献[16]	√	√	否	√	×	–	√	×
文献[17]	√	√	否	√	–	√	×	×
文献[21]	–	√	是	√	–	√	√	√
文献[22]	√	√	是	√	–	–	√	√
文中方案	√	√	否	√	√	√	√	√

注:"–"表示文章中未提及。

表 3　计算开销对比

方案	签名算法开销/数值	验证算法开销/数值	聚合验证算法开销/数值
文献[14]	$3T_{\mathrm{bp-mul}}+1T_{\mathrm{bp-add}}+2T_h$/3.061 ms	$3T_{\mathrm{bp}}+3T_{\mathrm{bp-mul}}+2T_{\mathrm{bp-add}}+3T_h$/21.326 ms	$3T_{\mathrm{bp}}+3nT_{\mathrm{bp-mul}}+(4n-2)T_{\mathrm{bp-add}}+3nT_h$ /(18.244 + 3.04n) ms
文献[15]	$3T_{\mathrm{bp-mul}}+1T_{\mathrm{bp-add}}+1T_h$/3.061 ms	$2T_{\mathrm{bp}}+2T_{\mathrm{bp-mul}}+3T_{\mathrm{bp-add}}+2T_h$/14.229 ms	$2T_{\mathrm{bp}}+3nT_{\mathrm{bp-mul}}+3nT_{\mathrm{bp-add}}+2nT_h$ /(12.172 + 3.075n) ms
文献[21]	$1T_{\mathrm{bp-mul}}+1T_h$/1.018 ms	$1T_{\mathrm{bp}}+1T_{\mathrm{bp-mul}}+1T_{\mathrm{bp-add}}+2T_h$/7.111 ms	$1T_{\mathrm{bp}}+nT_{\mathrm{bp-mul}}+nT_{\mathrm{bp-add}}+2nT_h$ /(6.086 + 1.025n) ms
文献[22]	$2T_{\mathrm{bp-mul}}+1T_h$/2.036 ms	$2T_{\mathrm{bp}}+1T_{\mathrm{bp-add}}$/12.179 ms	$2T_{\mathrm{bp}}+(3n-1)T_{\mathrm{bp-add}}$ /(11.154 + 3.054n) ms
文中方案	$1T_{\mathrm{ECC-mul}}+2T_h$/1.018 ms	$4T_{\mathrm{ECC-mul}}+3T_{\mathrm{ECC-add}}+3T_h$/3.173 ms	$(n+4)T_{\mathrm{ECC-mul}}+(n+2)T_{\mathrm{ECC-add}}+3nT_h$ /(3.126 + 0.805n) ms

表 4　通信开销对比

方案	签名长度/数值	聚合签名长度	单个签名传输开销/数值	聚合签名传输开销
文献[14]	$2|G_1|$/256 bytes	$(n+1)|G_1|$	$5|G_1|+|Z_q^*|$/660 bytes	$(4n+1)|G_1|+n|Z_q^*|$
文献[15]	$3|G_1|$/384 bytes	$3|G_1|+n|T|$	$7|G_1|+|T|$/900 bytes	$(4n+3)|G_1|+n|T|$
文献[21]	$|G_1|$/128 bytes	$n|G_1|$	$4|G_1|+|Z_q^*|+|T|$/536 bytes	$(3n+1)|G|+n|Z_q^*|$
文献[22]	$2|G_1|$/256 bytes	$2n|G_1|$	$3|G_1|+|Z_q^*|+|T|$/408 bytes	$(n+1)|G_1|$
文中方案	$|G|+|Z_q^*|$/60 bytes	$|G|+|Z_q^*|$	$3|G|+2|Z_q^*|+2|T|$/168 bytes	$(n+2)|G|+(n+1)|Z_q^*|+2n|T|$

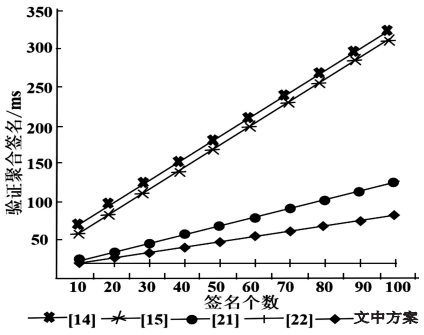

图 2　聚合验证计算开销对比

图 2 展示了聚合验证计算开销对比,文献[14-15,21]使用双线性配对运算,验证效率低开销较高。文献[22]虽然在计算开销上较低,但其利用 RSU 聚合和验证,加重 RSU 通信负担,文中方案由矿工聚合验证节省 RSU 开销,结合通信开销对比,文中方案基于无双线性配对运算,效率更高,优势更明显。

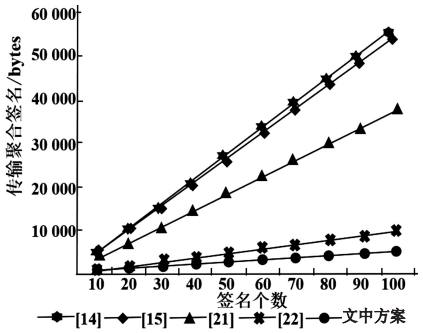

图 3　传输聚合签名通信开销对比

由图 3 传输聚合签名通信开销在消息个数变化时的对比看出,文中方案通信开销最低,相比开销最接近的文献[22]降低平均约 85.8%,当 $n = 10 \sim 100$ 变化时实验所得开销降低约 80.5%、85.4%、86.5%、87%、87.3%、85.8% 等。显然相比另外 3 个方案降低更多。

4.3 智能合约 gas 消耗

用户注册后才能进行任务发布/下载,未注册调用智能合约会触发 permission denied 事件提示注册。用户链上发布任务并标记为待解决,此时链上节点均可下载。合约收到 100 个该任务请求后将任务标为解决中,避免过多节点下载造成资源浪费。用户可能收到不同结果,选取满意结果后支付报酬并标记任务已解决。当聚合签名个数为 50 时,平均每 15 s 就能将 200 个聚合签名哈希值上链。实验表明,聚合签名从生成到最终上链平均时间约 0.075 s。表 5 是主要函数 gas 消耗和调用该函数响应时间测试。

表 5 智能合约主要函数 gas 消耗及响应时间

智能合约函数	描述	消耗的 gas/gwei	调用合约响应时间/ms
UserRegist	用户注册	64 245	2
task_release	发布任务/上传任务结果	67 546	4
task_receive	下载任务/接受任务结果	66 617	2
Reward	激励机制	22 635	3

过高的 gas 消耗会造成网络负担,从表 5 可以看出,用户注册、发布/上传任务结果、下载/接受任务结果所消耗的 gas 相差不大,以上智能合约 gas 消耗量小,各功能响应时间不超过 5 ms,响应迅速。

5 结束语

该文引入区块链并利用椭圆曲线构建无证书聚合签名方案,在降低了开销的同时,实现了强匿名性等六大安全性。降低了现有计算和通信负担,解决了巨大的证书管理开销问题。并通过实验证明了该方案的可行性,与其它方案相比,该方案的通信开销降低了 85.8% 以上,更适合应用于 VANET。另外,无限制的假名更换是不合理的,更换假名需要成本,未来的研究会围绕选择更合适的假名更换策略,进一步验证随机预言机模型和标准模型在应用中的差别,提升方案的实用性。

参考文献:

[1] GUAN Z,ZHANG Y,WU L,et al. APPA:an anonymous and privacy preserving data aggregation scheme for fog-enhanced IoT[J]. Journal of Network and Computer Applications,2019,125:82-92.

[2] MAHI M J N,CHAKI S,AHMED S,et al. A review on VANET research:perspective of recent emerging technologies [J]. IEEE Access,2022,10:65760-65783.

[3] AL-RIYAMI S S,PATERSON K G. Certificateless public key cryptography[C]//International conference on the theory and application of cryptology and information security. Berlin:Springer,2003:452-473.

[4] BONEH D,GENTRY C,LYNN B,et al. Aggregate and verifiably encrypted signatures from bilinear maps[C]//International conference on the theory and applications of cryptographic techniques. Berlin:Springer,2003:416-432.

[5] SU T,SHAO S,GUO S,et al. Blockchain-based internet of vehicles privacy protection system[J]. Wireless Communications and Mobile Computing,2020,2020:1-10.

[6] GUERNA A,BITAM S,CALAFATE C T. Roadside unit deployment in internet of vehicles systems:a survey[J]. Sensors,2022,22(9):3190.

[7] ZHANG L,KANG B,DAI F,et al. Hybrid and hierarchical aggregation-verification scheme for VANET[J]. IEEE Transactions on Vehicular Technology,2022,71(10):11189-11200.

[8] GONG Z,LONG Y,HONG X,et al. Two certificateless aggregate signatures from bilinear maps[C]//Eighth ACIS international conference on software engineering,artificial intelligence,networking,and parallel/distributed computing (SNPD 2007). Qingdao:IEEE,2007:188-193.

[9] HORNG S J,TZENG S F,HUANG P H,et al. An efficient certificateless aggregate signature with conditional privacy-preserving for vehicular sensor networks[J]. Information Sciences,2015,317:48-66.

[10] KUMAR P,KUMARI S,SHARMA V,et al. Secure CLS and CL-AS schemes designed for VANETs[J]. The Journal of Supercomputing,2019,75(6):3076-3098.

[11] ZHONG H,HAN S,CUI J,et al. Privacy-preserving authentication scheme with full aggregation in VANET[J]. Information Sciences,2019,476:211-221.

[12] MEI Q,XIONG H,CHEN J,et al. Efficient certificateless aggregate signature with conditional privacy preservation in IoV[J]. IEEE Systems Journal,2020,15(1):245-256.

[13] HU P,WANG Y,GONG B,et al. A secure and lightweight privacy-preserving data aggregation scheme for internet of vehicles[J]. Peer-to-Peer Networking and Applications,2020,13(3):1002-1013.

[14] WANG H,WANG L,ZHANG K,et al. A conditional privacy-preserving certificateless aggregate signature scheme in the standard model for VANETs[J]. IEEE Access,2022,10:15605-15618.

[15] DENG L,NING B,JIANG Y. A lightweight certificateless aggregation signature scheme with provably security in the

(下转第 127 页)