基于区块链的安全车联网数字取证系统

李萌[1]，司成祥[2]，祝烈煌[3]
（1. 合肥工业大学，安徽 合肥 230601；2. 国家计算机网络应急技术处理协调中心，北京 100029；
3. 北京理工大学，北京 100081）

摘　要：车联网大数据的出现对更好地理解车联网特点、掌握车联网用户需求和提升车联网服务质量具有极大的推动作用，然而恶意用户甚至不法分子利用车联网进行非法行为，造成车联网服务质量下降以及车联网事故难以定责。同时，在车联网数字取证过程中，还存在一些安全和隐私问题，如数据提供者的身份隐私和数据访问者的请求权限问题。因此，提出了一种基于区块链的安全车联网数字取证方案。首先数据请求者在一个证书中心注册后获得匿名证书，用于后续的数据上传。然后数据访问者注册后获得公私钥对和用户密钥，分别用于数据请求和数据解密，只有其属性满足特定要求才能解密得到正确证据。接下来可信度较高的若干个机构联合建立一个区块链，记录车联网取证过程中所有的数据上传交易和数据访问交易。最后，对方案的安全和隐私进行分析，并在以太坊平台上对其性能进行实验分析。

关键词：车联网；数字取证；区块链；安全；隐私
中图分类号：TP393.08
文献标识码：A
doi: 10.11959/j.issn.2096−3750.2020.00169

Secure vehicular digital forensics system based on blockchain

LI Meng[1], SI Chengxiang[2], ZHU Liehuang[3]
1. Hefei University of Technology, Hefei 230601, China
2. National Internet Emergency Center, Beijing 100029, China
3. Beijing Institute of Technology, Beijing 100081, China

Abstract: The emergence of vehicular big data has brought a great promotion to better understand characteristics of vehicular networks, grasp needs of users and improve service qualities. However, malicious users and criminals leverage vehicular networks to conduct illegal behaviors, resulting in a decline in the service quality and difficulties in determining the liability in vehicle accidents. At the same time, there are still some security and privacy issues in the vehicular digital forensics, such as the identity privacy of the data provider and the request control of the data requester. Therefore, a secure vehicular digital forensics scheme based on blockchain was proposed. Firstly, a data requester registered with a certificate authority and an anonymous certificate was obtained for the subsequent data uploading. Then, the data user obtained the public-private key pair and user key in registration, which were respectively used for the data requesting and data decryption. Only if certain attributes were held, the right plaintext could be decrypted. Next, a consortium blockchain was jointly established by several institutions with high credibility to record all data transactions. Finally, the security and privacy were experimentally analyzed, and the performance was tested based on the Ethereum platform.

Key words: vehicular networks, digital forensics, blockchain, security, privacy

收稿日期：2020−03−18；**修回日期：**2020−04−26
通信作者：祝烈煌，liehuangz@bit.edu.cn
基金项目：“十三五”装备预先研究项目（No.31511020401）；安徽省科技重大专项项目（No.201903a05020016）；国家自然科学基金资助项目（No.U1836102）
Foundation Items: The Pre-study Foundation of Weapons and Equipment (No.3151102401), The Anhui Science and Technology Key Special Program (No.201903a05020016), The National Natural Science Foundation of China (No.U1836102)

1 引言

近年来，随着车联网的发展，车辆内各种传感器和通信方式的更新换代使得车联网底层数据的实时获取和收集已不是难事[1]。同时，数据也推动了各类车联网服务的出现，如网约车服务[2]、路况监测[3]、停车位查找[4]和广告分发[5]等，这些服务巩固了车联网中数字世界与物理世界的纽带，也极大地提升了车联网用户的驾驶体验。

诸多车联网服务发展的同时，也催生了大规模且有价值的车联网数据。据报道[6]，预计在 2030 年仅司机数据就将成为万亿级工业的核心驱动力量，因为大数据清晰地展示了司机的驾驶行为，为广告商和保险公司带来了潜在价值，这些数据对研究人员更好地理解车联网特点、掌握车联网用户需求和提升车联网服务质量具有极大的推动作用。

尽管车联网的发展给人们的出行带来了许多便捷，但是也不乏恶意用户甚至不法分子利用车联网的优势进行恶意行为或非法行为[7-8]。如在发生肇事类的交通事故时，非诚实的肇事司机会因为没有监控而逃脱法律责任；在汽车发生故障时，保险公司因司机未能给出由于汽车本身原因引起故障的证据，而无法对其进行赔偿；在网约车服务过程中，有恶意司机发动错误位置攻击，以欺骗网约车服务提供商，从而骗取更多订单[2]；还有恶意司机会向路况监测服务中的路侧单元（RSU, road side unit）发送错误的驾驶信息，以干扰智能信号灯的正常规划[3]。近年来，有些不法分子利用汽车运输非法物品或者驱车逃离犯罪现场。国际刑事警察组织的官方定义指出，汽车犯罪指的是汽车盗窃与非法汽车交易以及汽车备用零件的非法交易。上述行为在全世界范围内对个人财产、商业活动、金融和公共安全都造成了负面影响[9]。

为了解决以上问题，车联网数字取证（VDF, vehicular digital forensics）[10-11]的作用变得越来越重要，逐渐成为学术界及工业界重点关注的研究课题之一。VDF 通过收集和分析车联网数据（如车速、转向、刹车、行车记录仪的视频等），帮助执法机构等相关部门及时确定相应的问题（如司机驾驶误操作、刹车片老化、车尾停车感应器失灵等）来源，对车联网中潜在的恶意行为和用户进行定位与追踪，降低了车联网的安全风险和用户损失。概括来说，将 VDF 分为 4 个步骤，即收集、检查、分析和汇报[12]，VDF 流程如图 1 所示。数据提供者上传数据的过程即数据收集过程，数据访问者对数据进行访问后需检查数据的真实性以及哪些数据与案件相关，并做深入分析，最终得出结论并进行汇报。

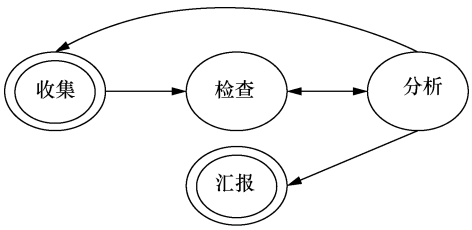

图 1 VDF 流程

此外，在 VDF 中，还存在一些安全和隐私问题。首先，基于集中式的取证模型面临恶意数据提供者或数据访问者篡改数据的风险，并且非法的数据访问者不能对取证数据进行访问。其次，数据提供者在上传数据（如录音或证词）时，不希望其真实身份被泄露，从而保护自身安全。最后，数据访问者在请求数据时，其访问权限必须被限制在一定的数据范围内，即数据访问者不能请求获得其访问权限以外的取证数据，实现数据隐私的进一步保护。

本文工作的挑战来自两个方面：1) 如何利用区块链保障车联网证据的安全管理；2) 如何保障数据提供者和数据访问者的隐私与访问控制。

为了解决上述两个问题，本文提出一种基于区块链的安全车联网数字取证（SVDF, secure vehicular digital forensics）方案。在 SVDF 方案中，数据提供者向一个证书中心（CA, certificate authority）注册后获得匿名证书，用于后续的数据上传；数据访问者注册后获得公私钥对和用户密钥，分别用于数据请求和数据解密，只有其属性满足特定要求才能解密得到正确的证据。可信度较高的若干个机构联合建立一个区块链，记录车联网取证过程中所有的数据上传交易和数据访问交易。同时，SVDF 方案将数据密文存储于分布式存储系统中，本文的贡献包括以下 3 个方面。

1) 为 VDF 设计了一种系统模型，分别由底层的用户、中层的 RSU 和上层的组织机构组成，并建立了相应的敌手模型，假设存在恶意数据篡改者和恶意数据访问者。

2) 在上述系统模型和安全模型的基础上，提出了 SVDF 方案。具体来说，借助匿名认证的方法[13]对数据提供者的真实身份进行条件隐私式验证，使

用基于属性加密算法[14]对数据访问者的数据请求进行访问控制，再通过搭建联盟区块链[12]提供数据记录的可验证性和防篡改性。

3) 对 SVDF 方案进行严格的安全与隐私证明，并通过以太坊测试网络对 SVDF 方案进行性能测试。

2 相关工作

区块链在车联网中已经有了初步应用和实践，本节主要分析区块链在 VDF 中的应用以及区块链在车联网其他场景中的应用。

2.1 区块链在 VDF 中的应用

Cebe 等[12]指出，智能网联汽车服务将为汽车厂商、汽车维修公司、司机和保险公司提供有价值的数据，这些数据对于 VDF 具有重要作用。文献[12]中将 VDF 系统的数据处理模型划分为收集、检查、分析和汇报 4 个环节，为车联网数据管理提出了一种基于许可链的架构，结合了车联网公钥基础设施和区块链，用以实现车联网用户的身份管理和隐私保护。其中，许可区块链中有 4 种角色，即队长（leader）、验证者（validator）、监测者（monitor unit）和用户（client）。验证者在每个时间段内选出一个队长，根据拜占庭共识机制创建新的区块。用户使用 IEEE 1609.2 标准中的匿名机制，在不同时间段内使用不同匿名来汇报数据。然而，此方案并没有考虑访问控制问题，即不同的数据访问者可以访问的数据是不同的。

2.2 区块链在车联网其他场景中的应用

边缘计算已经被应用于车联网中，Kang 等[15]指出，边缘节点在车联网中扮演着重要的角色，但是其半可信的安全假设会导致潜在的安全与隐私问题。文献[15]中利用联盟区块链和智能合约设计了一种面向车联网数据的安全点对点数据共享方案，边缘节点根据存储证明（proof-of-storage）共识机制更新区块链。

车联网中的广告分发服务帮助厂商和用户在车联网中及时地推广和获得最新的商品信息，Li 等[5]为了解决广告分发过程中因恶意司机合谋攻击骗取奖励而引发的公平性问题以及司机参与广告分发活动的隐私泄露问题，提出了一种基于区块链的公平与匿名广告分发方案。通过使用 Merkle 哈希树和智能合约技术，实现了验证司机是否收到广告的“广告接收证明”机制和检测司机多次索取广告转发费的机制，RSU 根据权益证明（proof-of-stake）共识机制维护区块链。

智能停车是一种常见的车联网服务，Wang 等[16]在利用私家停车位的智能停车服务[4]的基础上，提出了一种基于区块链的匿名智能停车方案。该方案使用分布式匿名证书机制对私家停车位所属人和司机的身份进行匿名认证，在一个停车位信息交换池中完成用户之间的停车位匹配后，借助门罗币的变种实现匿名支付，并在 RSU 节点之间实现区块链的更新和维护。

与现有方案相比，本文提出的 SVDF 系统提供了一种面向车联网的安全证据管理系统，并充分考虑了数据利益方的隐私问题。

3 问题描述

本节介绍了 SVDF 的系统模型，并给出了 SVDF 的安全模型，最后定义了本项工作的设计目标。

3.1 系统模型

SVDF 系统模型如图 2 所示，包括以下 6 个方面。

1) 数据提供者：感知与收集周边环境数据的设备，通过发送数据上传交易的形式，经过身份认证后，向车联网提供数据。数据提供者包含司机、行人和信号灯等，数据以密文形式存储于分布式存储系统中，而数据摘要存储于区块链网络中。

2) 数据访问者：通过发送数据访问交易的形式向车联网请求相应的数据，经过身份认证与访问权限验证后，从车联网中获得所需的数据，数据访问者包含执法人员和保险公司人员等。

3) RSU：负责接收数据提供者的数据，并验证数据请求者的身份和数据分组的完整性。

4) 区块链平台：由一群区块链节点搭建与维护，对车联网中的数据上传与数据访问进行记录。区块链节点包含执法部门、交通部门和保险公司等，区块链的作用是为了解决 VDF 系统中证据完整性和可验证性的保护问题。

5) 分布式存储系统：用于存储区块链网络中的加密数据分组。

6) CA：初始化整个车联网联盟区块链网络，注册各个实体，然后保持离线状态。

数据提供者提供证据，数据访问者访问证据，但是在实际应用中，一个实体可以同时充当数据提供者和数据访问者。RSU 是车联网中的辅助设施，

在区块链网络中作为验证的第一环节。区块链平台主要用于记录证据的上传与访问记录，由于其容量有限，所以需要借助分布式存储系统存储详细证据，所有注册信息都由 CA 保管。

VDF 系统对于数据提供者和数据访问者等实体而言，具有重要的意义，体现在能够为车联网中的证据提供一种安全、可验证和防篡改的运行环境。

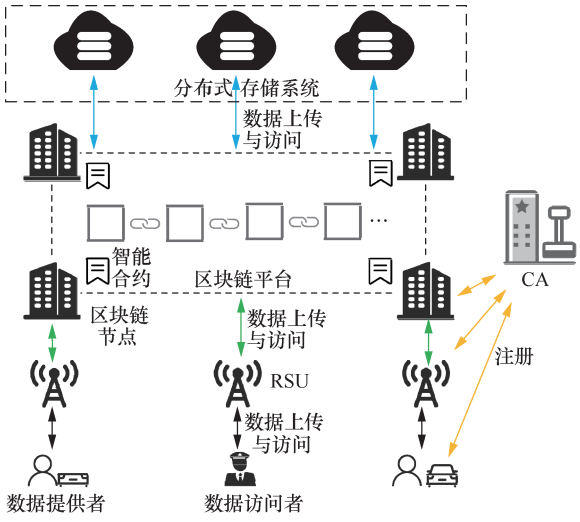

图 2 SVDF 系统模型

3.2 安全模型

在 SVDF 安全模型中，安全威胁来自两个方面，即内部敌手和外部敌手。

对于大部分实体而言，采用诚实而好奇（honest-but-curious）的安全假设，即大部分数据提供者与数据访问者会严格地执行既定协议，并如实地上传和访问证据，但是对其他实体的身份和数据感兴趣；剩余的数据访问者企图访问自身权限以外的区块链已有数据。一小部分 RSU 会因为设备故障或被敌手俘获而篡改数据提供者的数据，CA 是可信且难以被敌手俘获的。外部敌手可发送的攻击包括监听攻击、伪装攻击和重放攻击。

3.3 设计目标

本项工作的设计目标包括 4 个方面，即安全、隐私、访问控制和性能。

1) 安全：区块链网络中的数据上传交易和数据访问交易公开可验证并且防篡改，只有合法的实体才能对区块链的已有数据进行访问。

2) 隐私：数据提供者的真实身份需要向其他实体保密，且多次上传数据时的身份不能被链接。

3) 访问控制：数据提供者的明文数据只能被具有相应访问权限的实体访问。

4) 性能：本文所设计的车联网区块链系统对于数据提供者、数据访问者和区块链节点而言，所需的计算开销和通信代价较低。

4 预备知识

4.1 零知识证明

零知识证明（ZKPoK, zero-knowledge proof of knowledge）[17]是公钥密码学系统的有效构件之一，它可以使得一个证明者通过出示一些密码学证明的方式向一个验证者证明一句陈述的真实性，而不暴露自身的秘密信息。同时，证明还能展示证明者确实用指定函数和秘密信息进行了计算。零知识证明共有 3 个函数，即 Setup 函数（负责输出公共参数）、Prove 函数（负责生成陈述的证明）和 Verify 函数（负责验证证明的真实性）。假设现有证明者需要向验证者证明秘密信息 $(a_1,a_2,\cdots,a_n)$ 满足函数 F 的陈述，其形式为

$$\mathrm{ZKPoK}\{(a_1,a_2,\cdots,a_n)\,|\,F(a_1,a_2,\cdots,a_n)\} \tag{1}$$

零知识证明满足两个安全要求。1) 可靠性：如果证明者没有进行计算，那么它不能让验证者信服陈述；2) 零知识性：证明的验证过程不泄露证明者的秘密信息。

零知识证明经过改造后可以具备非交互式的特性[18]，即证明者与验证者之间只需进行一次信息的传递即可。

4.2 访问控制

基于属性加密的访问控制方法[14]确保了只有具有合法访问资格的数据访问者才能获得相应的数据，并且动态更新数据访问者的访问权限。具体来说，该方法由 7 个算法构成。

1) Setup(1^k)：初始化算法根据安全参数 1^k 输出主密钥 msk、公共参数 pp 和一组公共属性密钥 $\{\mathrm{pak}_a\}$。

2) USKeyGen(msk, ATT, $\{\mathrm{avk}_a\}_{a\in A}$)：根据主密钥 msk、一组属性 ATT 和一组属性版本密钥 $\{\mathrm{avk}_a\}_{a\in A}$，输出用户密钥 usk。

3) Encrypt(pp, $\{\mathrm{pak}_x\}$, m, $(\mathbb{A},\delta)$)：根据公共参数 pp、一组公共属性密钥 $\{\mathrm{pak}_a\}$、消息 m 和访问结构 $(\mathbb{A},\delta)$，输出密文 C。其中，$\mathbb{A}$ 是访问 m 必备的属性集合。

4) Decrypt(C, usk)：根据密文 C 和用户密钥

usk，输出消息 m。

5) UkeyGen(msk, $\mathrm{vk}_{\hat{a}}$)：根据主密钥 msk 和当前的版本密钥 $\hat{\mathrm{vk}}_{\hat{a}}$（需要撤销的属性是 $\hat{a}$），输出新的版本密钥 $\hat{\mathrm{vk}}_{\hat{a}}$ 和更新密钥 $\mathrm{uk}_{\hat{a}}$。

6) UkeyGen(usk, $\mathrm{uk}_{\hat{a}}$)：根据用户密钥 usk 和更新密钥 $\mathrm{uk}_{\hat{a}}$，输出新的用户密钥 $\hat{\mathrm{usk}}$。

7) UUpdate(C, $\mathrm{uk}_{\hat{a}}$)：根据密文 C 和更新密钥 $\mathrm{uk}_{\hat{a}}$，输出新密文 $\hat{C}$。

4.3 区块链

区块链是一个分布式环境中公开可验证且由一组实体共同维护的数字账本，它由包含了一定数量交易的区块串联组成。区块的产生时间由所有实体通过既定的共识机制而确定，实体通过竞争成为新区块的创建者而获得一定的奖励，该奖励也是实体参与维护区块链活动的动机。区块链根据实体准入机制的不同可以划分为 3 类，包括公共区块链、联盟区块链和私有区块链。

联盟区块链是一个半开放的公共账本，只针对若干个特定的实体或组织开放，即由若干个具有较高可信度的实体共同搭建和维护一个区块链，如著名的联盟区块链实例为 IBM 公司的 Hyperledger Fabric[19]。与公共区块链的区别在于，联盟区块链在某种程度上只属于联盟内部的实体所有，并且实体之间很容易达成共识。

5 方案

SVDF 的流程包括 5 个主要步骤，即系统初始化、实体注册、数据上传、数据请求和区块链维护。在系统初始化阶段，CA 生成系统参数；在实体注册阶段，数据提供者、数据访问者和区块链节点向 CA 注册，获得相应的密钥；在数据上传阶段，数据提供者向 RSU 上传数据；在数据请求阶段，数据访问者向区块链网络发送数据请求，并根据自身的属性和所获得的链接解密得到相应的数据；在区块链维护阶段，区块链节点根据网络中的交易和共识机制产生新的区块。

5.1 系统初始化

CA 根据安全参数 1^k 生成参数 $(q, G, G_{\mathrm{T}}, g, g_{\mathrm{T}}, e, H)$，$G$ 和 G_{T} 是 q 阶双线性群组，g 是 G 的生成元，g_{T} 是 G_{T} 的生成元，e 是双线性映射 $e: G\times G\to G_{\mathrm{T}}$，并且满足 $g_{\mathrm{T}}=e(g,g)$，H 是哈希函数 $H:\{0,1\}^{*}\to G$。CA 选择 3 个随机数 $x_1, x_2, x_3\leftarrow Z_q$，设置 $X_1=g^{x_1}$，$X_2=g^{x_2}$，$X_3=g^{x_3}$；设置主公钥 $\mathrm{mpk}=(q, G, G_{\mathrm{T}}, g, X_1, X_2, X_3)$ 和主私钥 $\mathrm{msk}=(x_1, x_2, x_3)$。CA 再选择 4 个随机数 $y_1, y_2, y_3, y_4\leftarrow Z_q$，计算 $g^{y_1}, g^{y_2^{-1}}, g^{y_2}, e(g,g)^{y_1}$；对于每一个属性 a，CA 选择一个随机数 $v_a\in Z_q$ 作为最初的属性版本密钥 $\mathrm{avk}_a=v_a$，设置公共属性密钥 $\mathrm{pak}_a=(\mathrm{pak}_{a,1}=H(a)^{v_a}, \mathrm{pak}_{a,2}=H(x)^{v_a y_3})$。最后，CA 将公共参数、mpk 和 $\{\mathrm{pak}_a\}$ 广播至区块链网络，将区块链交易池初始化为空。

5.2 实体注册

数据提供者选择两个随机数 $z_1, z_2\leftarrow Z_q$，计算 $M=g^{z_1}X_3^{z_2}$ 和一个零知识证明 $\pi=\mathrm{ZKPoK}\cdot\{(z_1,z_2)\,|\,M=g^{z_1}X_3^{z_2}\}$，并发送 M 和 π 给 CA 进行实名注册。如果 π 验证通过，则 CA 选择一个随机数 $r\leftarrow Z_q^{*}$，计算 $R=g^{r}$ 和签名 $s=(R_1=R, R_2=R^{x_2}, R_3=X_3^{rx_2}, R_4=R^{x_1}M^{rx_1x_2})$，返回 s 给数据提供者。数据提供者验证 s，然后设置私钥 $\mathrm{sk}=(s, z_1, z_2)$，生成一对 ECDSA 公私钥。

数据访问者向 CA 实名注册，CA 根据其身份为其分配一组属性 S，选择一个随机数 $t\leftarrow Z_q$，计算得到一个用户密钥 $\mathrm{usk}=(K=g^{y_1y_2^{-1}}\cdot g^{y_4ty_2^{-1}}, L=g^{t}, \forall a\in S: K_a=g^{ty_2^{2}}\cdot H(a)^{v_a ty_2})$，将 usk 返回给数据访问者，数据访问者生成一对 ECDSA 公私钥 $(\mathrm{pk}, \mathrm{sk})$。

区块链节点向 CA 实名注册，并生成一对 ECDSA 公私钥。CA 创建创世块，并广播给区块链网络，区块链节点记录创世块。

5.3 数据上传

数据提供者持有自身的数据 data，经执法人员的采集和对 $H(\mathrm{data})$ 的签名 σ 后，数据提供者和所在区域内的 RSU 执行以下步骤向区块链网络中发送数据上传交易 Tx^1。

1) 数据提供者选择两个随机数 $r_1, r_2\leftarrow Z_q^{*}$，计算盲签名 $\hat{\alpha}=(\hat{\alpha}_1, \hat{\alpha}_2, \hat{\alpha}_3, \hat{\alpha}_4)$。其中，$\hat{\alpha}_1=R_1^{r_1}$，$\hat{\alpha}_2=R_2^{r_1}$，$\hat{\alpha}_3=R_3^{r_1}$，$\hat{\alpha}_4=R_4^{r_1r_2}$。

2) 数据提供者在时间段 t 内，计算登录令牌 $\mathrm{Token}(t)=g_{\mathrm{T}}^{1/(z_1+t)}$。

3) 数据提供者提交 $(\hat{\alpha}, \mathrm{Token}(t))$ 给 RSU。

4) RSU 在本地数据库和区块链账本中查找 $\mathrm{Token}(t)$ 是否已存在，若存在，则拒绝数据提供者的数据；否则，继续执行下一步。

5) RSU 验证 $\hat{\alpha}$ 的合法性，如果式(2)的不等式和等式成立，则继续执行下一步；否则，终止。

$$\hat{\alpha}_1 \neq 1, e(g,\hat{\alpha}_2)=e(X_2,\hat{\alpha}_1), e(g,\hat{\alpha}_3)=e(X_3,\hat{\alpha}_2) \quad (2)$$

6) 数据提供者和RSU分别计算中间变量 v、v_1、v_2 和 v_3 为

$$\begin{aligned} &v=e(g,\hat{\alpha}_4), v_1=e(X_1,\hat{\alpha}_1),\\ &v_2=e(X_1,\hat{\alpha}_2), v_3=e(X_1,\hat{\alpha}_3) \end{aligned} \quad (3)$$

7) 数据提供者和 RSU 分别作为证明者和验证者进行零知识证明，如式(4)所示。

$$\begin{aligned} &\mathrm{ZKPoK}\{(z_1,z_2,z_2') \mid v^{z_2'}\\ &=v_1 v_2^{z_1} v_3^{z_2} \wedge \mathrm{Token}(t)=g_{\mathrm{T}}^{1/(z_1+t)}\}\\ &z_2'=z_2/2 \end{aligned} \quad (4)$$

8) 数据提供者生成一个数据密钥 key，用对称加密算法 SEnc 加密待上传数据 data。

$$c=\mathrm{SEnc}(\mathrm{key},\mathrm{data}) \quad (5)$$

9) 数据提供者定义访问结构 $(\mathbb{A},\delta)$，选择加密指数 $E\in Z_q$、随机向量 $\vec{V}=(E,E_2,\cdots,E_n)$。其中，$E_2,\cdots,E_n$ 用户共享 E。数据提供者计算 $\gamma_i=\vec{V}\cdot\mathbb{A}_i$，$1\leqslant i\leqslant l$。数据提供者选择随机数 $f_1,f_2,\cdots,f_l\in Z_q$，用 Encrypt 算法加密 key。

$$C=\left(C_1,C_2,C_i,D_{i,1},D_{i,2}\right), 1\leqslant i\leqslant l \quad (6)$$

$$\begin{aligned} &C_1=\mathrm{key}\cdot e(g,g)^{y_1 E}, C_2=g^{y_2 E},\\ &C_i=g^{y_1\gamma_i}\left(g^{y_2}\right)^{-f_i}\cdot H(\delta(i))^{-f_i V_{\delta(i)}} \end{aligned} \quad (7)$$

$$D_{i,1}=H(\delta(i))^{f_i V_{\delta(i)} y_3}, D_{i,2}=g^{f_i/y_2} \quad (8)$$

10) 数据提供者向 RSU 发送 C、数据类型 type、数据摘要 H(data)和 σ。

11) RSU 记录当前时间戳 t_s，对收到的数据和 t_s 做签名 σ_{RSU}，向区块链网络中发送 C 和数据上传交易自身的签名。

$$\mathrm{Tx}^1=\left(\hat{\alpha},\mathrm{Token}(t),\mathrm{type},H(\mathrm{data}),\sigma,t_s,\sigma_{\mathrm{RSU}}\right) \quad (9)$$

然后，将 C 存储于分布式存储系统中，Tx^1 被放入交易池中。

5.4 数据请求

数据访问者根据自身的数据类型 type 以及当前时间戳 t_s，使用其私钥生成一个签名 $\tilde{\sigma}$，向区块链网络发送数据请求交易如式(10)所示。

$$\mathrm{Tx}^2=(\mathrm{pk},\mathrm{type},t_s,\tilde{\sigma}) \quad (10)$$

持有相应数据的分布式存储系统节点向数据访问者返回密钥密文 C 和数据密文 c，数据访问者执行如下步骤进行解密。

1) 具有属性集合 $\mathbb{A}'$ 的数据访问者选择一组常数 $\{\mathrm{ct}_i\in Z_q\}_{i\in\{i:\delta(i)\in\mathbb{A}'\}}$，重构加密指数为

$$E=\sum_{i\in\{i:\delta(i)\in\mathbb{A}'\}}\mathrm{ct}_i\gamma_i \quad (11)$$

2) 数据访问者计算中间变量为

$$\frac{e(C_2,K)}{\prod_{i\in\{i:\delta(i)\in\mathbb{A}'\}}(e(C_i,L)e(D_{i,2},K_{\delta(i)}))^{\mathrm{ct}_i}}=e(g,g)^{y_1 E} \quad (12)$$

3) 数据访问者计算加密密钥 $\mathrm{key}=C_1/e(g,g)^{y_1 E}$，用解密算法解密 c 得到数据明文为

$$\mathrm{data}=\mathrm{SDec}(\mathrm{key},c) \quad (13)$$

5.5 区块链维护

所有的区块链节点根据权益证明（PoS, proof-of-stake）机制[20]选出一个当前领头节点，由其在交易池中选出 N 笔交易，创建新区块链并签名，将新区块链和签名广播至区块链网络中。其中，区块链节点的权益是指其产生的数据上传交易，因为它们不仅对区块链进行维护，也会充当数据提供者的身份。N 是一个可变值，根据应用程序的具体要求而定。

6 安全与隐私分析

本节将对 SVDF 的安全、隐私和访问控制特性进行分析。

6.1 安全

首先，数据提供者和数据访问者的交易数据全部在区块链网络中进行公开广播，对所有区块链实体公开可见，并且所有交易都有相应实体的签名。因此，数据上传交易和数据访问交易是公开可验证的，并且防篡改。

其次，区块链账本自身具有不可篡改性，保证了区块链网络中的数据上传交易和数据访问交易防篡改。只要数据被记录在车联网区块链上，那么就不会被轻易地更改。

最后，使用一种基于 LRSW（lysyanskaya, rivest, sahai and wolf）[21]和 DDHI（decisional Diffie-Hellman inversion）[22]假设的、仅限用户一次一登录的匿名认证方式[13]，保证只有合法实体才能对区块链的已存数据进行访问，而且每个合法实体在登录后不能发送任意多次消息。

6.2　隐私

在数据提供者登录系统时，使用一种匿名认证方式对其真实身份进行隐私保护式地认证，由于底层零知识证明的安全性，RSU 无法获得数据提供者所证明的秘密信息，即其真实身份（用 z_1, z_2 表示）。同时，在数据提供者登录系统时，对其签名进行盲化处理以及时间戳的差异化处理，使得每次登录的签名都不同而且无关联，从而保证了数据提供者多次上传的身份不能被链接。

6.3　访问控制

如果一个数据访问者不具备被访问数据原始持有者所要求的属性时，那么此访问者就不能获得该数据的明文，从而保证数据提供者的明文数据只能被具有相应访问权限的实体访问。这是因为该数据访问者无法根据自身的属性重构数据提供者的加密指数，从而无法解密得到数据密钥。如果数据访问者的某些属性被撤销，那么其在之后的请求中也不能获得相应数据的明文。

7　性能分析

本节将对 SVDF 的计算开销和通信代价进行实验和分析。

7.1　实验环境

在一台笔记本电脑（8 GB RAM，Intel Core i7-7500 CPU@2.70 GHz，Windows10 Home，Visual Studio2010）上搭建 SVDF 的仿真环境，使用 Ethereum 作为区块链平台，利用 MIRACL 库[23]作为密码库，将新区块的生成时间设定为 10 s。

7.2　计算开销

在数据请求阶段，每个数据请求者需要计算盲签名、登录令牌、数据摘要、零知识证明和数据密文，总用时约为 52 ms；验证者 RSU 需要验证盲签名和零知识证明，总用时约为 58 ms。在数据访问阶段，每个数据访问者需要计算签名、解密/加密指数和解密数据密文，总用时约为 0.1 s。数据提供者、RSU 和数据访问者的计算开销如图 3 所示。随着提供、验证和访问的数据越来越多，相应实体的计算开销也呈线性增长趋势。

7.3　通信代价

数据请求者每次向 RSU 发送数据时，都需要发送盲签名、登录令牌、数据类型、数据摘要、零知识证明和数据密文，其数据分组的长度为 1.46 KB。

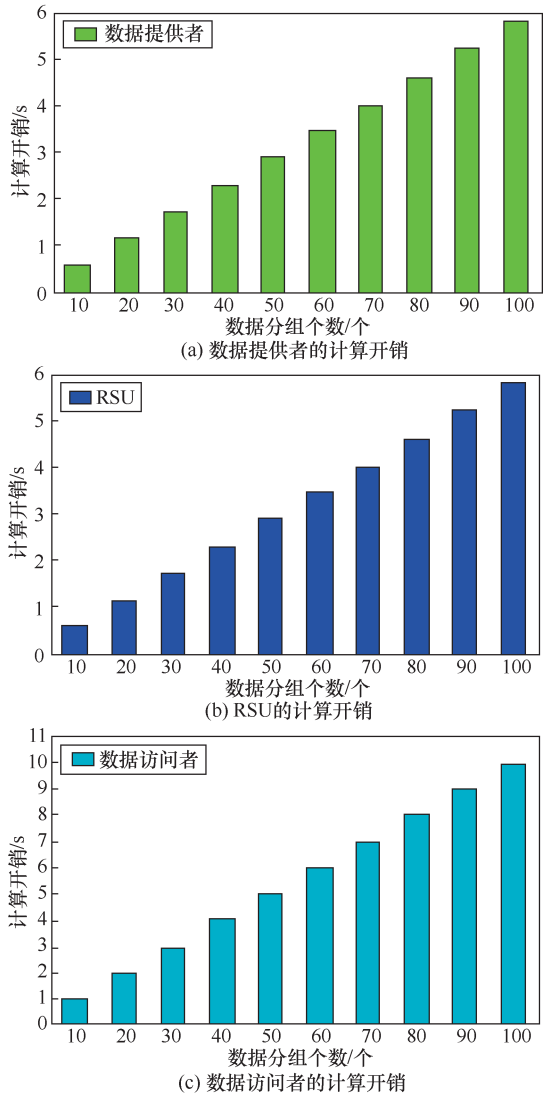

图 3　计算开销

RSU 在接收一个数据提供者的数据后，需要向区块链网络中发送数据密文和其数据上传交易，数据分组的长度为 1.15 KB。在接收一个数据访问者的请求后，需要发送 0.375 KB 的数据密文和签名给数据访问者。

数据访问者需要向 RSU 发送其公钥、数据类型、时间戳和签名，数据长度为 0.26 KB。

假设区块链网络中的数据提供者的数量为 N_1，数据访问者的数量为 N_2，通信代价分析如表 1 所示。

表 1　　**通信代价分析**

实体	通信代价/KB
数据提供者	1.46
RSU	$1.15N_1+0.375N_2$
数据访问者	0.26

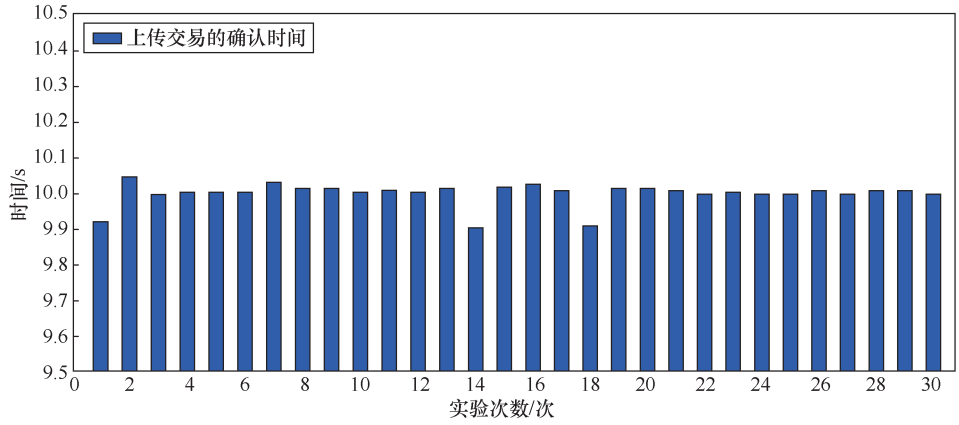

图 4 上传交易的确认时间

此外，对网络时延进行实验，即证据上传后到被写入区块链的确认时间。共进行 30 次实验，上传交易的确认时间如图 4 所示。由图 4 可知，上传交易的确认时间约为 10 s。

8 结束语

本文提出了一种基于区块链的 SVDF 方案，该方案可以实现车联网数据上传者的匿名身份认证和针对数据访问者的访问控制，并借助区块链记录所有数据上传和访问的记录，保证记录的公开可验证性和不可篡改性。同时，SVDF 还可以抵抗恶意数据上传者的篡改攻击和恶意数据访问者的非法请求。最后，对 SVDF 的安全属性与系统性能进行分析。

在未来的工作中，将结合现有实际案例继续挖掘基于区块链的 VDF 中潜在的安全与隐私问题，并设计相应的保护措施。此外，区块链只能提供证据上链之后的不可篡改性，而暂时无法充分保证证据上链之前的真实性[24]，所以接下来将在这方面做进一步的研究。

参考文献：

[1] CHENG N, LYU F, CHEN J Y, et al. Big data driven vehicular networks[J]. IEEE Network, 2018, 32(6): 160-167.

[2] LI M, ZHU L H, LIN X D. Efficient and privacy-preserving carpooling using blockchain-assisted vehicular fog computing[J]. IEEE Internet of Things Journal, 2019, 6(3): 4573-4584.

[3] LI M, ZHU L H, LIN X D. Privacy-preserving traffic monitoring with false report filtering via fog-assisted vehicular crowdsensing[J]. IEEE Transactions on Services Computing, 2019(99): 1-11.

[4] ZHU L H, LI M, ZHANG Z J, et al. ASAP: an anonymous smart-parking and payment scheme in vehicular networks[J]. IEEE Transactions on Dependable and Secure Computing, 2018(99): 1-12.

[5] LI M, WENG J, YANG A J, et al. Toward blockchain-based fair and anonymous ad dissemination in vehicular networks[J]. IEEE Transactions on Vehicular Technology, 2019, 68(11): 11248-11259.

[6] 余辰, 张丽娟, 金海. 大数据驱动的智能交通系统研究进展与趋势[J]. 物联网学报, 2018, 2(1): 56-63.
YU C, ZHANG L J, JIN H. Research progress and trend of big data-driven intelligent transportation system[J]. Chinese Journal on Internet of Things, 2018, 2(1): 56-63.

[7] NI J B, ZHANG A Q, LIN X D, et al. Security, privacy, and fairness in fog-based vehicular crowdsensing[J]. IEEE Communications Magazine, 2017, 55(6): 146-152.

[8] SHVETSOV A V, SHAROV V A, SHVETSOVA S V. Method of protection of pedestrian zones against the terrorist attacks made by means of cars including off-road vehicles and trucks[J]. European Journal for Security Research, 2017, 2: 119-129.

[9] 张彦, 张科, 曹佳钰. 边缘智能驱动的车联网[J]. 物联网学报, 2018, 2(4): 40-48.
ZHANG Y, ZHANG K, CAO J Y. Internet of vehicles empowered by edge intelligence[J]. Chinese Journal on Internet of Things, 2018, 2(4): 40-48.

[10] LACROIX J, EL-KHATIB K, AKALU R. Vehicular digital forensics: what does my vehicle know about me?[C]//6th ACM Symposium on Development and Analysis of Intelligent Vehicular Networks and Applications. ACM, 2016: 59-66.

[11] LE-KHAC N-A, JACOBS D, NIJHOFF J, et al. Smart vehicle forensics: challenges and case study[J]. Future Generation Computer Systems, 2018(99): 1-11.

[12] CEBE M, ERDIN E, AKKAYA K, et al. Block4Forensic: an integrated lightweight blockchain framework for forensics applications of connected vehicles[J]. IEEE Communications Magazine, 2018, 56(10): 50-57.

[13] LEE M Z, DUNN A M, WATERS B, et al. Anon-pass practical anonymous subscriptions[C]//34th IEEE Symposium on Security and Privacy (S&P). IEEE, 2013: 319-333.

[14] YANG K, JIA X H, REN K. Attribute-based fine-grained access control with efficient revocation in cloud storage systems[C]//8th ACM Symposium on Information, Computer and Communications Security (ACM ASIACCS). ACM, 2013: 523-528.

[15] KANG J W, YU R, HUANG X M, et al. Blockchain for secure and

efficient data sharing in vehicular edge computing and networks[J]. IEEE Internet of Things Journal, 2018, 6(3): 4660-4670.

[16] WANG L L, LIN X D, ZIMA E, et al. Towards airbnb-like privacy-enhanced private parking spot sharing based on blockchain[J]. IEEE Transactions on Vehicular Technology, 2020, 69(3): 2411-2423.

[17] FEIGE U, FIAT A, SHAMIR A. Zero-knowledge proofs of identity[J]. Journal of Cryptology, 1988, 1(2): 77-94.

[18] RACKOFF C, SIMON D R. Non-interactive zero-knowledge proof of knowledge and chosen ciphertext attack[C]//13th Annual International Cryptology Conference (CRYPTO). 1991: 433-444.

[19] ANDROULAKI E, BARGER A, BORTNIKOV V, et al. Hyperledger fabric: a distributed operating system for permissioned blockchains[C]// 13th European Conference on Computer Systems (EuroSys). 2018: 1-15.

[20] KIAYIAS A, RUSSELL A, DAVID B, et al. Ouroboros: a provably secure proof-of-stake blockchain protocol[C]//37th Annual International Cryptology Conference (CRYPTO). 2017: 357-388.

[21] CAMENISCH J, LYSYANSKAYA A. Signature schemes and anonymous credentials from bilinear maps[C]//24th Annual International Cryptology Conference (CRYPTO). 2004: 56-72.

[22] MITSUNARI S, SAKAI R, KASAHARA M. A new traitor tracing[J]. IEICE Transactions on Fundamentals, 2002, E85-A(2): 481-484.

[23] LI M, HU D, LAL C, et al. Blockchain-enabled secure energy trading with verifiable fairness in industrial Internet of things[J]. IEEE Transactions on Industrial Informatics (TII), 2020(99): 1-13.

[24] ZHANG F, CECCHETTI E, CROMAN K, et al. Town crier: an authenticated data feed for smart contracts[C]//23rd ACM Conference on Computer and Communications Security (CCS). ACM, 2016: 270-272.

[作者简介]

李萌（1988– ），男，安徽合肥人，博士，合肥工业大学副研究员，主要研究方向为应用密码学、安全与隐私、车联网、工业物联网、边缘计算、区块链等。

司成祥（1982– ），男，山东郯城人，博士，国家计算机网络应急技术处理协调中心工程师，主要研究方向为网络安全。

祝烈煌（1976– ），男，浙江衢州人，博士，北京理工大学教授，主要研究方向为物联网、云计算安全、区块链等。