基于签密和区块链的车联网电子证据共享方案

杨小东[1]，席婉婷[1]，王嘉琪[1]，陈艾佳[1]，王彩芬[2]
（1. 西北师范大学计算机科学与工程学院，甘肃 兰州 730070；
2. 深圳技术大学大数据与互联网学院，广东 深圳 518118）

摘 要：针对车联网电子证据共享中的隐私和安全问题，提出了一种基于签密和区块链的车联网电子证据共享方案。所提方案将证据密文和证据报告分别存储于云服务器和区块链，以实现电子证据的安全存储与共享。利用基于身份的签密技术保证了数据的机密性，运用代理重加密技术实现了保险公司对车联网电子证据的共享。引入聚合签名技术，降低了多个车辆用户签名验证的计算开销；采用信誉激励机制提高了电子证据的可靠性。安全性分析表明，所提方案满足数据的机密性、完整性、可验证性和不可伪造性。与现有方案相比，所提方案在计算开销方面具有一定优越性。

关键词：车联网；电子证据；基于身份的签密；代理重加密；区块链；聚合签名
中图分类号：TP309.7
文献标识码：A
DOI: 10.11959/j.issn.1000−436x.2021237

Electronic evidence sharing scheme of Internet of vehicles based on signcryption and blockchain

YANG Xiaodong[1], XI Wanting[1], WANG Jiaqi[1], CHEN Aijia[1], WANG Caifen[2]
1. College of Computer Science & Engineering, Northwest Normal University, Lanzhou 730070, China
2. College of Big Data and Internet, Shenzhen Technology University, Shenzhen 518118, China

Abstract: To solve the problems of privacy and security in the electronic evidence sharing of Internet of vehicles, a sharing scheme of electronic evidence in the Internet of vehicles based on signcryption and blockchain was proposed. The evidence ciphertext and the evidence report were stored in the cloud server and the block chain respectively to realize the secure storage and sharing of the electronic evidence. The identity-based signcryption technology was used to ensure the confidentiality of data, and the proxy re-encryption technology was used to realize the sharing of electronic evidence of Internet of vehicles by insurance companies. The aggregation signature technique was introduced to reduce the computation cost of multi vehicle user signature verification. The reliability of electronic evidence was improved by using credibility incentive mechanism. Security analysis shows that the proposed scheme achieves data confidentiality, integrity, verifiability and unforgeability. Compared with the existing schemes, the proposed scheme has certain advantages in terms of computational overhead.

Keywords: Internet of vehicles, electronic evidence, identity-based signcryption, proxy re-encryption, blockchain, signature aggregation

收稿日期：2021−09−04；**修回日期**：2021−12−03
基金项目：国家自然科学基金资助项目（No.61662069, No.61562077, No.61702552）；中国博士后科学基金资助项目（No.2017M610817）；兰州市科技计划基金资助项目（No.2013-4-22）；西北师范大学青年教师科研能力提升计划基金资助项目（No.NWNU-LKQN-14-7）
Foundation Items: The National Natural Science Foundation of China (No.61662069, No.61562077, No.61702552), China Postdoctoral Science Foundion Funded Project (No.2017M610817), The Science and Technology Project of Lanzhou City (No.2013-4-22), The Research Ability Improvement Project of Young Teachers of Northwest Normal University (No.NWNU-LKQN-14-7)

1　引言

车联网[1]是车、路、人协同的开放融合网络，是借助现代通信技术实现信息共享的移动通信系统。车联网中车辆行驶数据、交通状态数据和交通事故数据的共享，不仅能够实现路况监测以避免交通混乱，也能够为交通执法部门和保险公司等提供重要信息。例如，交通执法部门可以通过车辆行驶数据调查事故原因；保险公司可以将交通事故数据作为理赔证据等。然而，车联网数据在促进智慧交通发展的同时，也面临着严峻的数据安全挑战。由于车联网数据具有巨大的经济价值，恶意用户利用车联网进行非法行为的情况频频发生[2]，数据被窃取或伪造可能会造成车联网交通事故难以定责等问题。

电子证据[3]作为一种新型的证据，是利用电子设备进行传递、存储和共享的一切形式的证据。传统证据的提取依赖于人工，人工取证费时费力且效率极低；而电子证据具有收集迅速、易于保存、占用空间少和便于审查核实的特点，它的共享则能够更高效地解决车联网交通事故的追责及赔偿等问题。然而，电子证据因其本身较脆弱且依赖存储介质，易被丢失、修改和伪造[4]。如发生肇事类交通事故时，无有效证据或责任人故意伪造证据会导致定责困难或追责出现偏颇。保险公司的赔偿可能随之出现偏差造成重大利益损失，且追责有失公允也会导致司法部门公信力下降。因此，电子证据共享过程中的隐私泄露与数据安全问题亟待解决。

基于身份的签密[5]和代理重加密技术[6]可以通过对数据加密来解决数据隐私与安全问题。基于身份的签密具有更短的密文和更小的计算开销，对数据既签名又加密保证了数据的机密性和不可否认性。代理重加密技术使用重加密密钥进行密文转换，将授权者的密文转换成被授权者可以解密的密文，实现了第三方用户对授权方数据的共享。然而，基于身份的签密和代理重加密技术依赖于半可信第三方，通常存在数据存储中心化的问题。云服务器通常在执行用户命令的同时，仍对用户的信息保持好奇，因此其是半可信的。集中化存储的云服务器很容易遭到不法分子的攻击，造成隐私数据的篡改、丢失或泄露[7]。

区块链技术[8]是一种具有去中心化、数据难以篡改、可追溯、不可伪造等特性的信任机制，为电子证据在车联网中的共享提供了新的去中心化的解决方案。区块链技术可以在防止证据被篡改的同时，实现电子证据的分布式安全存储。然而，区块链技术现阶段存在性能瓶颈[9]，无法大规模存储车联网电子证据数据。随着区块链交易数据的增长，节点记录数据的时间也不断延长，数据确认的时延也会越来越高，因此单纯使用区块链存储和共享车联网电子证据存在效率低下的问题。

针对上述问题，本文提出了基于签密和区块链技术的车联网电子证据共享方案。该方案采用链上存储证据报告、链下存储证据密文的方式，将云的海量存储能力和区块链的难以篡改性结合进行优势互补；利用基于身份的签密和代理重加密技术对电子证据进行加密，实现了证据的机密性、身份可验证性和不可否认性。同时，通过管理车辆用户的信誉值，提高了数据的可靠性；采用聚合签名技术降低了签名验证的计算开销。

2　相关工作

电子取证逐渐替代传统人工取证，一定程度上解决了证据收集依赖人工、取证效率低下、证据容易失真等问题。但是目前还面临着安全和隐私挑战，如证据提供车辆的隐私保护问题和电子证据易受攻击被篡改和伪造的问题。因此，车联网电子证据共享成为公共法治及智慧交通领域重点关注的研究课题之一。

为了解决数据隐私泄露和共享安全问题，Malone 等[10]在数字签名体制[11]的基础上利用双线性对计算构造了第一个基于身份的签密方案，保证了数据的机密性、消息的完整性和不可否认性；但其明文的签名在密文中可见，Libert 等[12]随后指出该方案是不安全的。Karati 等[13]介绍了一种新的基于身份的双线性对签名加密方案，实现了身份的可追溯性；但由于其计算量大不适合在交通场景中短时间内对大量车辆签名进行验证。Boneh 等[14]提出的聚合签名解决了多个签名的验证问题，签名验证者仅需验证聚合后的一个签名即可，提高了系统中签名的验证速率。Blaze 等[15]提出代理重加密机制实现了密文转换，解决了实际应用中的细粒度解密权限分配问题；但该方案的授权人与代理人可以串通获取授权人的私钥，即存在合谋攻击安全风险。Hundera 等[16]和 Luo 等[17]将云计算技术引入代理重签密方案，降低了大量数据的存储成本，满足了云

端数据的机密性和完整性的安全需求；但其方案仍消耗较高昂的计算成本，且存在数据存储中心化和数据易被篡改的问题。

区块链技术的出现为数据易被篡改和伪造的问题提供了一种新的解决方案[18-19]，区块链能够确保数据的去中心化存储、难以篡改和不可伪造。Zhang 等[20]提出了一个基于区块链的云取证方案，该方案在提供证据同时可实现身份的隐私保护；但方案的效率和安全均受限于中心信任节点。Malamas 等[21]提出了一种基于移动物联网的取证框架，利用区块链获取证据保证了证据完整性和可靠性；但密钥管理技术烦琐，无法适用于车联网场景。Huang 等[22]提出了一种基于区块链的云计算电子取证模型，该模型可以防止取证各方的串谋篡改；但不能满足并发请求，算法效率需要进一步优化。Oham 等[23]利用区块链技术存取证据，提出了一种自动车辆归责框架，该框架能够解决车辆与司法部门间在交通事故中的信任问题，但无法避免数据确认时延高的问题。Li 等[24]对电子证据加密实现了数据的安全存储及细粒度访问控制，通过区块链技术保证了数据记录的防篡改性；但该方案存在大量双线性对运算，计算开销较大并不高效。

为此，本文基于签密和区块链技术提出了一个新的车联网电子证据共享方案。利用云服务器存储电子证据密文，区块链存储包含证据哈希值及签名等的证据报告，这样既能防止云服务器伪造或篡改证据，又能减轻区块链的存储负担。使用基于身份的签密和代理重加密算法加密电子证据保证数据机密性，为所有进行通信的实体生成匿名身份以保护其身份隐私。因此，本文方案既解决了车联网电子证据的安全共享问题，又实现了证人即车辆用户的隐私保护需求，使电子证据共享更加高效、安全。

3 车联网电子证据共享模型

本节首先重点介绍了模型的逻辑框架与实体功能，然后给出车联网电子证据共享模型的设计目标。

3.1 模型的逻辑框架与实体功能

本文提出将区块链与云服务器相结合，实现数据的链上（区块链）+链下（云服务器）混合存储；同时，利用签密和代理重加密技术，实现了车辆用户的隐私保护和电子证据的安全共享。如图 1 所示，基于区块链的车联网电子证据共享模型包括可信机构（TA, trusted authority）、认证机构（CA, certification authority）、车辆（V_i, vehicle）、路边单元（RSU, road-side unit）、区块链（BC, blockchain）、云服务器（CS, cloud server）和保险公司（IC, insurance company）7 个实体，其中 TA 对应图 1 中的车辆管理所，CA 对应图 1 中的交通警察局。

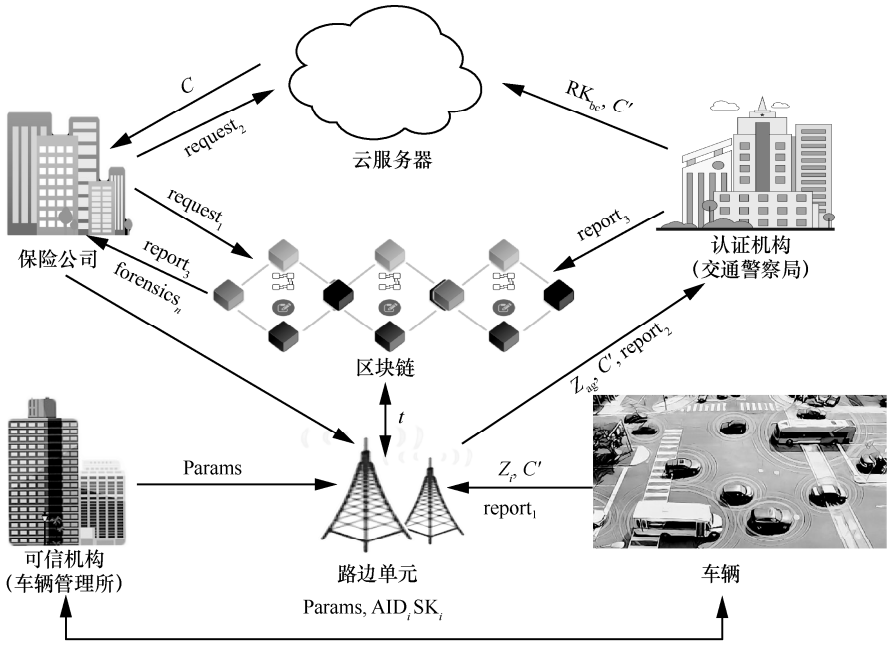

图 1 车联网电子证据共享模型框架

各个实体的具体介绍如下。

1) 可信机构：负责进行全局设置，车辆和路边单元需到车辆管理所登记注册。

2) 认证机构：负责生成代理密钥，管理并更新车辆的信誉值。

3) 车辆：参与取证任务，负责收集证据并对其进行签密。

4) 路边单元：负责验证每个车辆的签名，并将有效的一组车辆签名进行聚合。

5) 区块链：负责将证据报告存储在记录池中，保险公司需先入链查找证据报告，再根据报告请求云服务器返回证据密文。

6) 云服务器：负责进行代理重加密并存储证据密文，具有足够的存储和计算资源。云服务器验证证据密文的有效性，无效则拒绝存储。

7) 保险公司：将取证任务委托给路边单元，通过云服务器获取证据密文并解密得到有效证据，对提供有效证据的车辆给予报酬奖励。

3.2 模型的设计目标

该模型旨在达到如下设计目标。

1) 数据共享。采用云存储和加密技术实现了多对多的共享，车辆用户将电子证据加密存储在云服务器中，保险公司通过解密获取电子证据。车辆用户借助云服务器将电子证据共享给需要有效证据的保险公司。

2) 隐私保护。利用基于身份的签密技术，为车辆生成匿名身份进行交互使其真实身份不被泄露，同时也通过加密数据在共享过程中保护电子证据的数据隐私。

3) 安全高效。采用了区块链和云计算相结合的混合存储以保证证据数据的安全。区块链中的数据记录的防篡改性以及云服务器强大的存储、计算能力可以确保电子证据的安全存储。聚合签名和代理重加密技术的应用能够很好地提高方案效率，实现数据高效共享。

4 方案的详细构造及设计

方案主要包括系统初始化、实体注册、证据收集、证据上传、证据访问和激励机制 6 个步骤。

4.1 系统初始化

TA 选择一个安全参数 1^{λ} 并执行如下操作。

1) TA 选择一个大素数 p，2 个阶为 p 的循环群 G_0 和 G_T，其中 G 是群 G_0 的生成元。循环群满足双线性映射 $e: G_0 \times G_0 \to G_T$。

2) TA 选择 4 个安全的哈希函数：$H_1: \{0,1\}^* \to G_0$，$H_2: G_0 \times G_T \to Z_p^*$，$H_3: G_0 \times G_0 \times G_0 \times G_T \times G_T \to Z_p^*$ 和 $H_4: G_0 \times G_0 \times G_T \to Z_p^*$。

3) TA 选择随机数 $\alpha \in Z_p^*$ 作为主密钥，并设置 $P_{\text{pub}} = \alpha G$ 作为系统公钥。

4) TA 秘密保存主密钥 $\text{msk} = \alpha$，公开全局参数 $\text{Params} = \{G_0, G_T, e, G, P_{\text{pub}}, H_1, H_2, H_3, H_4\}$，并将区块链记录池初始化为空。

4.2 实体注册

车辆都需要在 TA 处进行登记注册。车辆通过安全信道将自己的真实身份发送给 TA，对于真实身份为 RID_i 的车辆用户，TA 为其生成匿名身份 AID_i 来保护身份隐私，具体注册步骤如下。

1) TA 选择哈希函数 $H_1: \{0,1\}^* \to G_0$，计算 $\text{AID}_i = H_1(\text{RID}_i)$，$\text{AID}_i$ 为车辆用户的匿名身份，TA 秘密保存注册信息表 $\text{registry} = \{\text{RID}_i, \text{AID}_i\}$。

2) TA 根据车辆匿名身份 AID_i，计算 $\text{SK}_i = \text{mskAID}_i = \alpha \text{AID}_i$ 作为车辆用户的私钥。

3) TA 将车辆匿名身份和用户私钥 $\{\text{AID}_i, \text{SK}_i\}$ 通过一个安全信道发送给用户。

4) 如果进行取证任务的车辆用户出现任何违规或非法行为，TA 可以根据 AID_i 查询注册信息表 registry 来曝光该车辆的真实身份以进行追查。

5) 区块链节点向 TA 实名注册，TA 创建创世块并广播给整个区块链网络，区块链节点记录创世块。

4.3 证据收集

路边单元 RSU 接受 IC 委托的取证任务后，邀请事故路段车辆进行如下证据收集操作。

1) IC 将取证任务 $\text{forensics}_n = \{n, \text{AID}_c, u_n\}$ 委托给 RSU，其中包括取证任务编号 n、保险公司匿名身份 AID_c 和取证车辆信誉值要求 u_n。

2) RSU 邀请事故发生路段周围车辆 $(V_1, V_2, \cdots, V_j)$ 收集事故相关证据数据附上签名并上传。经过事故路段但无证据的车辆 V_f 驶离该路段也可将任务附上签名广播给周围的车辆，以提高取证任务完成的效率。

3) RSU 将车辆收集的事故相关证据发送至 CA，由 CA 的交通执法人员根据 forensics_n 筛选出有效的证据，并对相关证据数据进行代理重加密；

若无有效证据则由 RSU 继续广播证据收集任务。

4.4 证据上传

车辆、路边单元和认证机构执行以下流程向区块链网络和云服务器安全地上传证据数据。

1) 车辆签密

取证车辆对行车记录仪拍到的现场照片、视频以及事故车辆行驶状态数据等证据进行签密，以保证其他实体交互过程中是不知道证据明文的。无证据车辆将取证任务附上签名广播给周围车辆。

① 取证车辆 V_i 选取随机数 $\varepsilon \in Z_p^*$，获取当前设备的时间戳 $t \in \{0,1\}^*$ 作为登录令牌，计算 $X = \varepsilon \mathrm{AID}_i$，$Y = H_2(X, M \| t)$ 和 $Z_i = (\varepsilon + Y)\mathrm{SK}_i$ 得到签名 $\sigma_i = (Z_i, G)$，其中证据 $M \in G_T$。

② 车辆 V_i 计算 $S = e(\varepsilon \mathrm{SK}_i, \mathrm{AID}_b)$，$y = MS$，$U = H_3(X, Z_i, y, \mathrm{AID}_i, \mathrm{AID}_b)$ 和 $R = \varepsilon U$，其中 AID_b 是 CA 的匿名身份。V_i 对证据数据 M 加密生成一级密文 $C' = (X, Z_i, y, R)$。车辆 V_i 生成证据报告 1，即 $\mathrm{report}_1 = \{n, Z_i, H_2(M), t\}$，并上传 Z_i、一级密文 C' 及 report_1 至路边单元 RSU。

③ 离开事故路段 RSU 范围的无证据车辆 V_f 将取证任务发送给目前路段的 $\mathrm{RSU}_{\mathrm{now}}$，由 $\mathrm{RSU}_{\mathrm{now}}$ 将 $\mathrm{forensics}_n$ 作为消息广播给周围车辆。$\mathrm{RSU}_{\mathrm{now}}$ 选取随机数 $\psi \in Z_p^*$，计算 $\mathrm{SK}_R = \mathrm{msk} H_1(\mathrm{RID}_R) = \alpha \mathrm{AID}_R$，$X_R = \psi \mathrm{AID}_R$，$Y_R = H_2(X_R, \mathrm{forensics}_n)$ 和 $Z_R = (\psi + Y_R)\mathrm{SK}_R$，得到签名 $\sigma_R = (Z_R, G)$，将 $\{\mathrm{forensics}_n, Z_R\}$ 广播给周围车辆，收到消息的车辆通过计算 $e(Z_R, G) = e(X_R + Y_R \mathrm{AID}_R, P_{\mathrm{pub}})$ 对签名是否有效进行验证。

2) 聚合签名生成

路边单元验证车辆签名是否合法，并为持有合法签名的一组车辆进行如下操作生成聚合签名。

① RSU 在区块链账本和本地数据库中查找 t 是否已经存在。如果存在，则拒绝该车辆提供的证据，避免重复存证；否则，RSU 继续进行聚合签名。

② RSU 首先对每个车辆的签名 $\sigma_i = (Z_i, G)$ $(1 \leqslant i \leqslant j)$ 通过计算等式 $e(Z_i, G) = e(X + Y\mathrm{AID}_i, P_{\mathrm{pub}})$ 进行验证。若等式成立，则该签名合法，RSU 将持有合法签名的一组车辆的匿名身份生成列表 $V_{\mathrm{legal}} = \{\mathrm{AID}_1, \mathrm{AID}_2, \cdots, \mathrm{AID}_j\}$，RSU 为该组车辆生成聚合签名 $\sigma_{\mathrm{ag}} = (Z_{\mathrm{ag}}, G)$，其中 $Z_{\mathrm{ag}} = \sum_{i=1}^{j} Z_i$。若验证失败，则签名无效，该车辆存在上传虚假证据的可能，RSU 可将车辆匿名身份举报给 TA，TA 可以公开该车辆真实身份，CA 也相应地降低该车辆的信誉值。

③ 车辆身份验证通过后，RSU 生成证据报告 2，即 $\mathrm{report}_2 = \{n, Z_{\mathrm{ag}}, V_{\mathrm{legal}}, \mathrm{AID}_c, H_2(M), t\}$，并将 Z_{ag}、一级密文 C' 及 report_2 上传至 CA。

3) 代理重加密及密文存储

CA 对聚合签名进行验证，若签名合法，则执行以下操作进行代理重加密，并将经过签密和代理重加密的证据密文进行如下存储。

① 交通执法人员根据 $\mathrm{forensics}_n$、证据报告和信誉值 value_i 筛选出有效的证据，其中 CA 管理的车辆信誉值初始均为相同数值，仅提交过证据的车辆的匿名身份会被 CA 保存，并对该车辆的信誉值进行更新。

② CA 通过计算 $e(Z_{\mathrm{ag}}, G) = e(\sum_{i=1}^{j} X + Y\mathrm{AID}_i, P_{\mathrm{pub}})$ 对聚合签名 σ_{ag} 进行批量验证。如果验证通过，则签名合法，CA 生成重加密密钥进行代理重加密；否则，聚合/签名无效，该 RSU 节点存在被非法攻陷的可能，CA 可向 TA 举报该 RSU 节点。

③ CA 计算 $W = H_4(e(\mathrm{SK}_b, \mathrm{AID}_c), \mathrm{AID}_b, \mathrm{AID}_c)$ 和 $\mathrm{RK}_{bc} = W - \mathrm{SK}_b$ 生成重加密密钥 RK_{bc}。

④ CA 记录当前时间戳 T_s，生成并向区块链网络中发送证据报告 3，即 $\mathrm{report}_3 = \{n, \sigma_{\mathrm{ag}}, \mathrm{AID}_i, \mathrm{AID}_b, \mathrm{AID}_c, H_2(M), t, T_s, \mathrm{value}_i\}$。CA 将 report_3 存放入区块链记录池中，并通过安全信道将重加密密钥 RK_{bc} 及一级密文 C' 发送给云服务器 CS。

⑤ CS 通过重加密密钥对 C' 进行代理重加密，CS 计算 $U = H_3(X, Z_i, y, \mathrm{AID}_i, \mathrm{AID}_b)$，验证等式 $e(R, \mathrm{AID}_i) = e(U, X)$ 是否成立，若验证通过则计算 $y' = ye(X\mathrm{RK}_{bc})$，生成二级密文 $C = (X, Z_i, y')$ 并存储。其中，CS 通过等式 $e(R, \mathrm{AID}_i) = e(U, X)$ 来检验证据密文的有效性，若密文无效则拒绝重加密和存储密文。

4.5 证据访问

保险公司 IC 发送访问请求，在接收到云服务器 CS 的证据密文后，执行解密操作获取证据明文，具体步骤如下。

1) IC 根据取证编号、伪名以及当前时间戳 T_s 向区块链网络请求访问证据报告，数据请求为

$\text{request}_1=\{n,\text{AID}_c,T_s,P_{\text{pub}}\}$，持有相应数据记录的区块链节点向 IC 返回证据报告 report_3。

2) IC 根据证据报告向云服务器发送 request_2 请求证据密文，云服务器向保险公司返回证据密文 C。

3) IC 对证据密文 C 进行解密，IC 通过计算 $W=H_4(e(\text{AID}_b,\text{SK}_c),\text{AID}_b,\text{AID}_c)$，$S'=e(X,W)$ 和 $M=y'(S')^{-1}$ 解密得到有效证据 M。

4) IC 通过计算 $Y=H_2(X,M)$ 可以验证证据完整性；通过等式 $e(Z_i,G)=e(X+Y\text{AID}_i,P_{\text{pub}})$ 可以对证据源进行身份验证。

4.6 激励机制

保险公司 IC 根据证据报告中车辆信誉值 value_i 的高低对证据进行评估。IC 通过奖励机制来刺激、鼓励更多车辆收集并提供有效证据。一旦该有效证据被 IC 成功接受，则对对应的车辆用户进行报酬奖励。

CA 初始时根据信誉感知激励机制为不同的车辆 V_i 设置不同的信誉值。当 IC 发布取证任务并且车辆 V_i 竞争参与这些任务时，感知平台会根据 V_i 的信誉值 value_i 进行选择，优先交由信誉值高的 V_i 参与取证任务。对 V_i 的信誉值 value_i 进行更新后，V_i 可再次进入下一轮的任务竞争中。通过该激励机制，可以刺激车辆用户提高任务完成率和参与率。

当有取证任务要处理时，CA 为每个不同的取证任务设置一个信誉阈值，用 u_n 表示。IC 为鼓励更多 V_i 参与完成取证任务，会在每个任务处理完成后为对应 V_i 提供奖励报酬。报酬函数用 $P_n=\dfrac{1}{a(l(r)+1)}u_nB(r)$ 来表示，其中 a 为正常数，B 为初始成本预算。通过这种方式，保险公司初始时会提供很高的报酬来鼓励车辆用户参与取证任务，随着车辆用户参与的比例 $l(r)$ 越来越高，报酬会慢慢趋于平稳。

5 安全性分析

本节将从正确性、机密性、不可伪造性这 3 个方面对本文所提方案进行安全性分析。

5.1 正确性

1) 签名的正确性验证

路边单元 RSU 需要对车辆 V_i 的签名进行正确性验证，以确保提供证据的该车辆身份是合法的。RSU 计算式(1)进行验证，当等式成立时车辆 V_i 的身份才合法，其对电子证据的签名才有效。具体证明如下。

$$\begin{aligned}&e(Z_i,G)=e((\varepsilon+Y)\text{SK}_i,G)=\\&e(\varepsilon\text{mskAID}_i+Y\text{SK}_i,G)=\\&e(X+Y\text{AID}_i,G\text{msk})=e(X+Y\text{AID}_i,P_{\text{pub}})\end{aligned}\quad(1)$$

验证得出等式成立，即该车辆签名有效。路边单元 RSU 将所有合法车辆的签名聚合起来形成新签名发送给 CA，CA 同样需要验证聚合签名是否有效。当验证等式 $e(Z_{\text{ag}},G)=e(\sum_{i=1}^{j}X+Y\text{AID}_i,P_{\text{pub}})$ 成立时，该聚合签名有效。

2) 证据密文解密正确性验证

云服务器 CS 通过重加密密钥 RK_{bc} 对一级密文进行代理重加密后的密文为 $C=(X,Z_i,y')$。保险公司 IC 向云服务器请求获取证据密文后，根据 CA 的匿名身份 AID_b 和 IC 的私钥 SK_c 计算 $W=H_4(e(\text{AID}_b,\text{SK}_c),\text{AID}_b,\text{AID}_c)$ 和 $S'=e(X,W)$。IC 通过式(2)可以计算得到证据明文，具体证明如下。

$$\begin{aligned}&y'(S')^{-1}=ye(X,\text{RK}_{bc})e(X,W)^{-1}=\\&Me(\varepsilon\text{SK}_c,\text{AID}_i)e(X,(W-\text{SK}_c))e(X,W)^{-1}=\\&\frac{Me(X,\text{SK}_c)e(X,(W-\text{SK}_c))}{e(X,W)}=\frac{Me(X,W)}{e(X,W)}=M\end{aligned}\quad(2)$$

IC 可以通过解密计算 $y'(S')^{-1}=M$ 得到证据明文，即本文方案的证据密文解密正确。

5.2 机密性

本文将基于身份的签密与代理重加密结合起来，保证了车联网环境下电子证据共享过程中的机密性。机密性是指除了提供证据的车辆及使用证据的保险公司外，其他实体都不知道证据的具体内容。在本文中，车辆用户 V_i 对电子证据 M 进行签密，将加密后的一级证据密文 C' 发送给 CA；CA 生成代理重加密密钥 RK_{bc} 发送给云服务器 CS，CS 对一级密文代理重加密后进行密文存储。当保险公司 IC 希望访问一起事故的电子证据时，根据取证编号 n、公司伪名 AID_c 等生成访问请求 request_1。IC 将访问请求发送给区块链网络以获取证据报告 report_3，再根据证据报告向云请求证据密文 C，最终解密得到电子证据明文。由于 V_i 收集的证据经过了 CS 的代理重加密，因此只有被授权的合法保险公司 RID_c 才能正确解密证据密文，其他实体无法获取任何有关电子证据的具体内容。具体证明过程见附录 1。

5.3 不可伪造性

在传统车联网数据共享方案中，由于云服务器是半可信的且存在响应时延的问题，因此车辆将证据全部发送至云服务器进行处理会存在较大安全风险。本文利用云服务器和区块链混合存储以及基于身份的签名技术，保证了电子证据的不可伪造性。车辆 V_i 上传的证据报告和保险公司 IC 的访问记录对所有区块链实体公开可见，并且所有链上的数据都具有公开可验证、防篡改性。只要数据被记录在车联网区块链上，就不会被轻易地伪造和篡改。车辆 V_i 进行数据交互时使用的都是匿名身份 AID_i，非法攻击者即使成功冒充身份，也会因为不知道系统主密钥 α 而不能生成用户私钥 SK_i。因此，非法攻击者无法伪造合法的车辆用户签名 $\sigma_i=(Z_i,G)$，而伪造的无效签名则不能通过等式 $e(Z_i,G)=e(X+Y\mathrm{AID}_i,P_{\mathrm{pub}})$ 的完整性验证。具体证明过程见附录 2。

6 性能分析

本节分析了方案的激励性，并从计算开销方面对所提方案与现有方案进行分析和比较。

6.1 激励机制

本文方案引入信誉值是为了使取证任务快速被车辆用户处理完成，即在更短的时间内获得更高的任务完成比率。在图 2 中可以看出在一段时间内本文信誉激励机制能很快地处理完取证任务，并在处理任务速度方面具有较好的稳定性。通过设置取证任务的信誉值，区别划分车辆用户，选择信誉值高的车辆用户来处理取证任务。这样通过影响取证任务的信誉阈值 u_n 和保险公司支付的报酬 P_n，从而使车辆用户参与比例 $l(r)$ 不断增大，并最终趋于平稳。

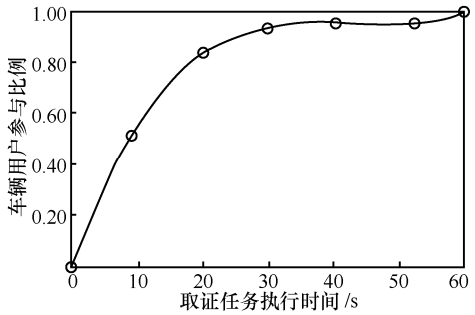

图 2 取证任务完成趋势（$l(r)$ 稳定前）

在保证取证任务顺利处理完成的基础上，减少保险公司支付给车辆用户的报酬 P_n，从而保险公司可以降低对车辆用户奖励的预算，减少成本的投入。当参与车辆足够多时不需要再对车辆用户进行激励。图 3 表明 $l(r)$ 稳定后的一段时间内，在保证取证任务顺利完成的基础上，可以减少保险公司支付给车辆用户的报酬 P_n，从而使其投入成本减少。综上所述，本文中选择了信誉高的车辆用户处理取证任务，使车辆用户参与比例 $l(r)$ 不断增大，保险公司需要支付给车辆用户的报酬 P_n 逐渐减少；即该信誉激励机制在有效提高任务处理效率的同时，降低了保险公司的成本开销。

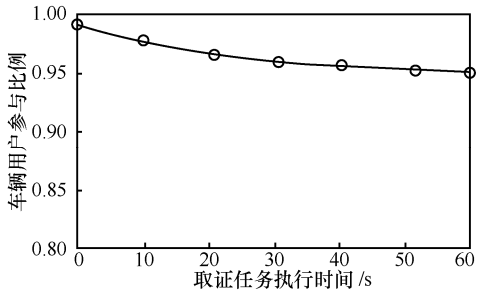

图 3 取证任务完成趋势（$l(r)$ 稳定后）

6.2 计算开销

本节采用对比分析的方式，将本文方案与 Yu 等[6]方案、Hundera 等[16]方案和 Luo 等[17]方案的计算开销进行了比较。由于这些方案是在双线性对上构建的，因此通过评估标量乘法运算、指数运算和双线性对运算消耗的时间来比较不同方案的计算开销。各个方案的加解密算法计算开销如表 1 所示，其中，M 表示一个标量乘运算，E 表示一个指数运算，P 表示一个双线性运算。

表 1 方案计算开销比较

方案	代理密钥生成	加密	解密
Yu 等方案	$2M+2P+1E$	$3M+1P+1E$	$1M+4P+1E$
Hundera 等方案	$2M+2P$	$2M$	$2M+4P$
Luo 等方案	$2M+1P$	$2M+1P+3E$	$2M+1P+3E$
本文方案	$1P$	$4M+1P$	$1M+4P$

本文仿真实验在 Intel Core i5-7400 CPU@ 3 GHz 平台上使用 Pairing-Based Crypto（PBC）函数库实现，所使用硬件环境为 4 GB 处理器内存和 64 位 Windows 10 操作系统。通过仿真实验对比了本文方案及相关 3 种方案的计算开销，对比结果如图 4 所示。本文方案生成代理密钥、加密和解密消耗的总时间为 151.96 ms，是 4 个方案中计算开销最少的，因此本文车联网电子证据共享方案是高效的。

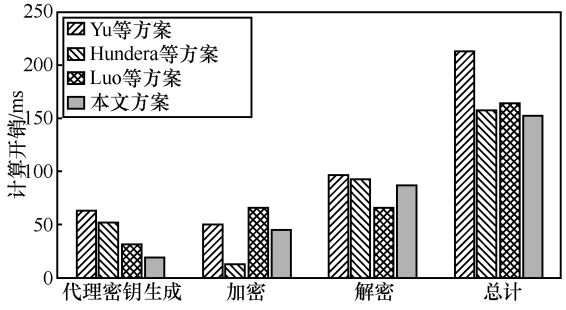

图 4　各方案计算开销比较结果

6.3　签名验证

在使用更高效方案对电子证据加解密的同时，本文使用的聚合签名技术也降低了计算开销。聚合签名技术是将不同消息上不同用户分别签署的多个签名聚合成一个短签名。聚合签名进行验证后，验证者可以判断所接收签名的有效性，很大程度上提高了消息验证的效率。本文方案中单个签名验证和聚合签名验证的计算开销比较如表 2 所示，其中 j 为单个签名的个数。

表 2　单个签名验证和聚合签名验证的计算开销比较

验证方式	验证计算开销
单个签名验证	$jM+2jP$
聚合签名验证	$jM+2P$

通过实验对比本文方案中单个签名验证和聚合签名验证的计算开销，结果如图 5 所示。当存在多个签名时，聚合签名的验证时间远小于单个签名累加的验证时间。因此，本文方案中采用的聚合签名技术极大地降低了签名验证的开销，使电子证据共享方案更加高效。

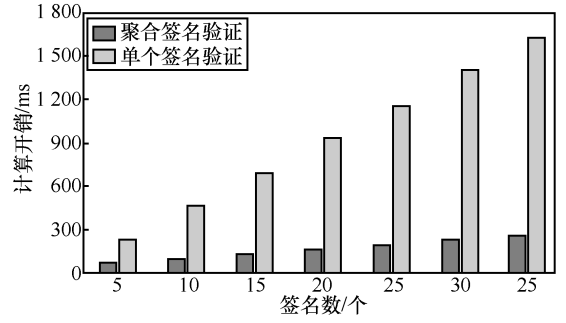

图 5　签名验证开销比较

7　结束语

本文针对车联网电子证据共享中的隐私安全和效率问题，提出了一种基于区块链的车联网电子证据共享方案。该方案不仅实现了证据数据的隐私保护及安全共享，也保证了证据上传者与各实体的匿名交互。借助区块链记录所有证据报告，确保了电子证据不会被篡改和伪造。采用聚合签名和代理重加密技术，使方案具有更优的计算高效性和可靠性。引入信誉激励机制，在有效提高任务处理效率的同时，减少了保险公司支付奖励报酬的成本。最后，通过仿真从计算开销等方面验证了方案的高效性。目前本文匿名交互不足以完全保护用户隐私，只能保证真名被隐藏，无法阻止敌手进行会话链接来判断两次不同的匿名会话来自相同的车辆。在未来的工作中，将继续结合车联网应用场景设计出更安全、高效的隐私保护方案。

附录 1　机密性证明

定理 1　如果 DBDH 问题是困难的，则本文签密方案在适应性选择密文攻击下满足机密性，即不存在一个攻击者能在多项式时间内以不可忽略的优势攻破本文方案。

证明　如果存在一个概率多项式时间敌手 $\mathcal{A}$ 可以以不可忽略的优势 τ 选择性地攻破本文方案，那么能够构造一个概率多项式时间算法使挑战者 $\mathcal{B}$ 以不可忽略的优势攻破 DBDH 假设。即给定挑战者 $\mathcal{B}$ 一个随机的 DBDH 问题实例 $(G,aG,bG,cG,X\in G_T)$，$\mathcal{B}$ 判断等式 $Z=e(G,G)^{abc}$ 是否成立。

系统建立。挑战者 $\mathcal{B}$ 运行系统初始化算法，将挑战参数 $\text{Params}=\{G_0,G_T,e,G,P_{\text{pub}},H_1,H_2,H_3,H_4\}$ 发送给攻击者 $\mathcal{A}$。

阶段 1　$\mathcal{A}$ 可以对挑战者 $\mathcal{B}$ 做有限次数的适应性询问。$\mathcal{A}$ 首先对身份 AID_i 做 H_1 询问后，才能将其询问结果用于其他询问。$\mathcal{A}$ 不可以利用签密询问的结果来进行解密询问。

H_1 询问。当 $\mathcal{A}$ 输入数据 $(\text{RID}_i,\text{AID}_i,h_1)$，$\mathcal{B}$ 以此格式设置列表 L_1。当 $\mathcal{A}$ 查询 $H_1(\text{RID}_i,\text{AID}_i)$ 时，若 $(\text{RID}_i,\text{AID}_i,h_1)$ 在列表 L_1 中存在，则返回 h_1 给 $\mathcal{A}$；否则，$\mathcal{B}$ 随机选取 $h_1\in Z_p^*$，添加记录 $(\text{RID}_i,\text{AID}_i,h_1)$ 至列表 L_1 中并返回 h_1 给 $\mathcal{A}$。

H_2 询问。当 $\mathcal{A}$ 输入数据 $(\text{AID}_i,\varepsilon,M,t,\text{SK}_i,h_2,Z_i)$，$\mathcal{B}$ 以此格式设置列表 L_2。当 $\mathcal{A}$ 查询 $H_2(\text{AID}_i,\varepsilon,M,t,\text{SK}_i)$ 时，若 L_2 中有相对应的记录 $(\text{AID}_i,\varepsilon,M,t,\text{SK}_i,h_2)$，则返回 h_2 给 $\mathcal{A}$；否则，$\mathcal{B}$ 随机选择 $\sigma\in\{0,1\}$，其中 $\sigma=(Z_i,G)$。当 $\sigma=0$ 时，$\mathcal{B}$ 随机选取 $h_2\in Z_p^*$，添加记录 $(\text{AID}_i,\varepsilon,M,t,\text{SK}_i,h_2,Z_i)$ 至列表 L_2 中并返回 h_2 给 $\mathcal{A}$；当 $\sigma=1$ 时，令 $h_2=\perp$ 并返回 $\perp$ 给 $\mathcal{A}$。

H_3 询问。当 $\mathcal{A}$ 输入数据 $(\mathrm{AID}_b,\varepsilon,M,\mathrm{SK}_i,Z_i,h_3,C')$，$\mathcal{B}$ 以此格式设置列表 L_3。当 $\mathcal{A}$ 查询 $H_3(\mathrm{AID}_b,\varepsilon,M,\mathrm{SK}_i,Z_i)$ 时，若 L_3 中有相对应的记录 $(\mathrm{AID}_b,\varepsilon,M,\mathrm{SK}_i,Z_i,h_3)$，则返回 h_3 给 $\mathcal{A}$；否则，$\mathcal{B}$ 随机选择 $C'\in\{0,1\}$。当 $C'=0$ 时，$\mathcal{B}$ 随机选取 $h_3\in Z_p^*$，添加 $(\mathrm{AID}_b,\varepsilon,M,\mathrm{SK}_i,Z_i,h_3,C')$ 至列表 L_3 中并返回 h_3 给 $\mathcal{A}$；当 $C'=1$ 时，令 $h_3=\perp$ 并返回 $\perp$ 给 $\mathcal{A}$。

H_4 询问。当 $\mathcal{A}$ 输入数据 $(\mathrm{AID}_c,\varepsilon,M,\mathrm{SK}_b,Z_i,\mathrm{RK}_{bc},h_4,C)$，$\mathcal{B}$ 以此格式设置列表 L_4。当 $\mathcal{A}$ 查询 $H_4(\mathrm{AID}_c,\varepsilon,M,\mathrm{SK}_b,Z_i,\mathrm{RK}_{bc})$ 时，若 L_4 中有相对应的记录 $(\mathrm{AID}_c,\varepsilon,M,\mathrm{SK}_b,Z_i,\mathrm{RK}_{bc},h_4)$，则返回 h_4 给 $\mathcal{A}$；否则，$\mathcal{B}$ 随机选择 $C\in\{0,1\}$。当 $C=0$ 时，$\mathcal{B}$ 随机选取 $h_4\in Z_p^*$，添加 $(\mathrm{AID}_c,\varepsilon,M,\mathrm{SK}_b,Z_i,\mathrm{RK}_{bc},h_4,C)$ 至列表 L_4 中并返回 h_4 给 $\mathcal{A}$；当 $C=1$ 时，令 $h_4=\perp$ 并返回 $\perp$ 给 $\mathcal{A}$。

私钥询问。当 $\mathcal{B}$ 收到关于车辆 RID_i 的私钥询问时，$\mathcal{B}$ 在列表 L_1 中寻找相对应的记录 $(\mathrm{RID}_i,\mathrm{AID}_i)$。如果车辆身份 RID_i 属于路边单元邀请的一组车辆 V^*，$\mathcal{B}$ 计算私钥 $\mathrm{SK}_i=\alpha\mathrm{AID}_i$ 并将其返回 $\mathcal{A}$；否则，挑战者 $\mathcal{B}$ 失败并终止挑战。

签密询问。当 $\mathcal{B}$ 收到 $(\mathrm{RID}_1,\mathrm{RID}_2,M)$ 的签密询问时，如果 $\mathrm{RID}_1\neq\mathrm{RID}_i$ 且 $\mathrm{RID}_2\neq\mathrm{RID}_b$，则调用签密步骤回答 $\mathcal{A}$；若 $\mathrm{RID}_1=\mathrm{RID}_i$ 且 $\mathrm{RID}_2=\mathrm{RID}_b$，$\mathcal{B}$ 根据下列方法给出一级密文。

步骤 1　$\mathcal{B}$ 选取随机数 $\varepsilon\in Z_p^*$，计算 $X=\varepsilon\mathrm{AID}_i$，$Y=H_2(X,M\|t)$ 和 $Z_i=(\varepsilon+Y)\mathrm{SK}_i$；

步骤 2　计算 $S=e(\varepsilon\mathrm{SK}_i,\mathrm{AID}_b)$ 和 $y=MS$；

步骤 3　将 $U=H_3(X,Z_i,y,\mathrm{AID}_i,\mathrm{AID}_b)$ 存储在列表 L_3 中，若发生碰撞，重做步骤 1～步骤 3；

步骤 4　计算 $R=\varepsilon U$ 并输出一级密文 $C'=(X,Z_i,y,R)$；

重加密密钥询问。当 $\mathcal{B}$ 收到 $(\mathrm{RID}_2,\mathrm{RID}_3)$ 的重加密密钥询问时，$\mathcal{B}$ 在列表 L_4 中寻找相对应的记录。如果 $\mathrm{RID}_2\neq\mathrm{RID}_b$ 且 $\mathrm{RID}_3\neq\mathrm{RID}_c$，而且表中存在记录 $(\mathrm{AID}_3,\mathrm{SK}_2,\mathrm{RK}_{bc})$，则返回 RK_{bc}。如果 $\mathrm{RID}_2=\mathrm{RID}_b$ 且 $\mathrm{RID}_3=\mathrm{RID}_c$，则 $\mathcal{B}$ 设置 $\mathrm{AID}_b=H_1(\mathrm{RID}_b)$ 和 $\mathrm{AID}_c=H_1(\mathrm{RID}_c)$，计算 $W=H_4(e(\mathrm{SK}_b,\mathrm{AID}_c),\mathrm{AID}_b,\mathrm{AID}_c)$ 和 $\mathrm{RK}_{bc}=W-\mathrm{SK}_b$，最后挑战者 $\mathcal{B}$ 将重加密密钥 RK_{bc} 返回给 $\mathcal{A}$；否则，挑战者 $\mathcal{B}$ 失败并终止挑战。

重加密询问。当 $\mathcal{B}$ 收到 $(\mathrm{RID}_2,\mathrm{RID}_3,C')$ 的重加密询问时，如果 $\mathrm{RID}_2\neq\mathrm{RID}_b$ 且 $\mathrm{RID}_3\neq\mathrm{RID}_c$，则调用重加密步骤回答 $\mathcal{A}$；若 $\mathrm{RID}_2=\mathrm{RID}_b$ 且 $\mathrm{RID}_3=\mathrm{RID}_c$，$\mathcal{B}$ 执行如下步骤得到二级密文。

步骤 1　计算 $\mathrm{AID}_i=H_1(\mathrm{RID}_i)$；

步骤 2　在列表 L_3 中查询 $U=H_3(X,Z_i,y,\mathrm{AID}_i,\mathrm{AID}_b)$ 并计算 $y'=ye(X\mathrm{RK}_{bc})$；

步骤 3　返回二级密文 $C=(X,Z_i,y')$ 给 $\mathcal{A}$。

解密询问。挑战者 $\mathcal{B}$ 接收到 $\mathcal{A}$ 关于密文的解密询问时，如果满足 $\mathrm{RID}_2\neq\mathrm{RID}_b$ 且 $\mathrm{RID}_3\neq\mathrm{RID}_c$，那么 $\mathcal{B}$ 执行解密操作并将其结果返回给 $\mathcal{A}$；否则，$\mathcal{B}$ 输出 $\perp$，即输入的密文无效，无法执行解密操作。如果 $\mathrm{RID}_2=\mathrm{RID}_b$ 且 $\mathrm{RID}_3=\mathrm{RID}_c$，则挑战者 $\mathcal{B}$ 执行如下步骤获取证据明文。

步骤 1　计算 $\mathrm{SK}_c=\alpha\mathrm{AID}_c$；

步骤 2　计算 $W=H_4(e(\mathrm{AID}_b,\mathrm{SK}_c),\mathrm{AID}_b,\mathrm{AID}_c)$ 和 $S'=e(X,W)$；

步骤 3　计算证据明文 $M=y'(S')^{-1}$ 并将结果返回给攻击者 $\mathcal{A}$。

挑战。$\mathcal{A}$ 选取长度相等的消息 M_0 和 M_1，将其发送给 $\mathcal{B}$。$\mathcal{B}$ 选择 $\mu\in\{0,1\}$ 并按照以下步骤计算密文 C^*。

步骤 1　随机选择 $\theta\in Z_p^*$，计算 $X=\theta\mathrm{AID}_i$，$Y=H_2(X,M)$ 和 $Z_i=(\theta+Y)\mathrm{SK}_i$；

步骤 2　计算 $S=e(\theta\mathrm{SK}_i,\mathrm{AID}_b)$，$y=MS$，$U=H_3(X,Z_i,y,\mathrm{AID}_i,\mathrm{AID}_b)$ 和 $R=\theta U$；

步骤 3　输出一级密文 $C''=(X,Z_i,y,R)$；

步骤 4　计算 $W=H_4(e(\mathrm{SK}_b,\mathrm{AID}_c),\mathrm{AID}_b,\mathrm{AID}_c)$ 并生成重加密密钥 $\mathrm{RK}_{bc}=W-\mathrm{SK}_b$；

步骤 5　计算 $U=H_3(X,Z_i,y,\mathrm{AID}_i,\mathrm{AID}_b)$ 和 $y'=ye(X\mathrm{RK}_{bc})$；

步骤 6　生成二级密文 $C^*=(X,Z_i,y')$。

阶段 2　$\mathcal{A}$ 继续进行同阶段 1 中的各种适应性询问，但是 $\mathcal{A}$ 不可以对目标身份做私钥询问。

响应。如果 $\mu'=\mu$，则 $\mathcal{B}$ 输出 1；若 $\mu'\neq\mu$，则 $\mathcal{B}$ 输出 0。

如果 $Z=e(G,G)^{abc}$，则 C^* 是有效密文，因此 $\mathcal{A}$ 有优势 τ 区分 μ，有 $\Pr[\mu'=\mu|\ Z=e(G,G)^{abc}]=\frac{1}{2}+\tau$。如果 $Z\neq e(G,G)^{abc}$，那么 $\mu=1$ 或 $\mu=0$ 时，密文每个部分具有一样的概率分布，也就是说，在区分 μ 上的优势是可以忽略的，所以 $\Pr[\mu'=\mu|Z\neq e(G,G)^{abc}]=1/2$。

假设在多项式时间 t 内，$\mathcal{A}$ 最多进行 q_s 次签密询问、q_{rk} 次代理密钥询问、q_r 次重加密询问、q_d 次解密询问和 $q_{H_i}(i=1,2,3,4)$ 次哈希询问。$\mathcal{B}$ 在多项式时间 $t'<t+O(q_{\mathrm{rk}}+q_s+q_rq_{H_2}+q_dq_{H_2})t_p$ 内成功解决 DBDH 的概率为 $\tau'>(\tau-q_s(q_s+q_{H_2})2^{1-k})/2q_{H_1}$，即挑战者 $\mathcal{B}$ 能够以一个不可忽略的优势解决 DBDH 问题。但这一问题已被证明是困难的，所以攻击者 $\mathcal{A}$ 能以不可忽略的优势 τ 攻击本文方案这一假设不成立，本文方案满足机密性要求。证毕。

附录 2　不可伪造性证明

定理 2　如果 CDH 困难问题成立，本文所提方案可以抵抗适应性选择消息攻击下的存在性伪造攻击，即不存在一个攻击者以不可忽略的优势攻破本文方案。

证明　如果存在一个多项式时间的敌手 $\mathcal{A}$ 在适应性选择消息攻击下以不可忽略的优势攻破了本文方案，那么能够构造一个多项式时间算法使挑战者 $\mathcal{B}$ 以不可忽略的优势攻破 CDH 问题，即给定 $\mathcal{B}$ 已知 (aG,bG)，最终可以计算出 abG。

系统建立。挑战者 $\mathcal{B}$ 进行系统初始化，设置系统公钥为 $P_{\text{pub}}=\alpha G$，生成系统参数 Params 并将其发送给 $\mathcal{A}$。$\mathcal{B}$ 维护和更新列表 L_1,L_2,L_3,L_4，其分别对应对 H_1,H_2,H_3,H_4 的询问结果。

阶段 1　$\mathcal{A}$ 必须首先对身份 RID_i 做 H_1 询问之后，才能将其用做其他询问。$\mathcal{A}$ 不可以利用签名询问的结果来进行解签名询问。H_1,H_2,H_3 和 H_4 询问与定理 1 中同理。

私钥询问。当 $\mathcal{A}$ 对身份为 RID_i 的车辆进行私钥询问时，$\mathcal{B}$ 在列表 L_1 中寻找相对应的记录 $(\text{RID}_i,\text{AID}_i)$。如果身份为 RID_i 的车辆属于路边单元邀请的车辆组 V^*，$\mathcal{B}$ 计算私钥 $\text{SK}_i=\alpha\text{AID}_i$ 并将其返回 $\mathcal{A}$；否则，挑战者 $\mathcal{B}$ 失败并终止挑战。

签名询问。$\mathcal{A}$ 对 (RID_i,M) 的签名进行询问，挑战者 $\mathcal{B}$ 选取随机数 $\varepsilon\in Z_p^*$，根据 RID_i 的私钥 SK_i 来执行 H_2 询问；计算得到 $X=\varepsilon\text{AID}_i$，$Y=H_2(X,M\,\|\,t)$ 和 $Z_i=(\varepsilon+Y)\text{SK}_i$ 对应列表 L_2 中 $(\text{AID}_i,\varepsilon,M,t,\text{SK}_i,h_2,Z_i)$，则 $\mathcal{B}$ 将签名 $\sigma=(Z_i,G)$ 返回 $\mathcal{A}$。

解签名询问。挑战者 $\mathcal{B}$ 接收到 $\mathcal{A}$ 关于签名的解签名询问时，如果满足 $\text{RID}_2\neq\text{RID}_b$ 且 $\text{RID}_3\neq\text{RID}_c$，那么 $\mathcal{B}$ 执行解密操作并将其结果返回给 $\mathcal{A}$；否则，$\mathcal{B}$ 输出 $\perp$，即输入的密文无效，无法执行解密操作。

伪造。最后 $\mathcal{A}$ 输出一个有效的签名 (RID_i,M,σ)，$\mathcal{B}$ 计算得到 $Y=H_2(X,M)$，其中 $X=\varepsilon\text{AID}_i$ 是 RID_i 的原始签名公钥。$\mathcal{A}$ 验证等式 $e(Z_i,G)=e(X+Y\text{AID}_i,P_{\text{pub}})$ 是否成立，若不成立则 $\mathcal{B}$ 失败并终止挑战；否则，得到等式 $e(Z_i^*,G)=e(X+Y^*\text{AID}_i,P_{\text{pub}})$，其中 $\sigma^*=(Z_i^*,G)$。若签名 $\sigma=\sigma^*$，那么 $\mathcal{B}$ 能够解决 CDH 困难问题，$\mathcal{B}$ 可以输出 $abG=(Y-Y^*)^{-1}(Z_i-Z_i^*)$。

假设在多项式时间 t 内，$\mathcal{A}$ 最多进行 q_s 次签名询问、q_{sk} 次密钥询问、q_u 次解签名询问和 $q_{H_i}(i=1,2,3,4)$ 次哈希询问。与定理 1 的概率分析过程相同，挑战者 $\mathcal{B}$ 成功在多项式时间 $t'<120\,686q_{H_1}q_{H_2}(t+O(q_{\text{sk}}+q_s+q_uq_{H_2})t_P)2^k/\tau(2^k-1)$ 内解决 CDH 的概率为 $\tau'>10(q_s+1)(q_s+q_{H_2})q_{H_1}/(2^k-1)$，即如果 $\mathcal{A}$ 能成功伪造合法的签名，则挑战者 $\mathcal{B}$ 能够解决 CDH 困难问题。但 CDH 问题已被证明是困难的，所以攻击者 $\mathcal{A}$ 无法以可忽略的概率伪造有效的签名欺骗挑战者，证明了本文方案的签名算法是安全的。证毕。

参考文献：

[1] ZHOU H B, XU W C, CHEN J C, et al. Evolutionary V2X technologies toward the Internet of vehicles: challenges and opportunities[J]. Proceedings of the IEEE, 2020, 108(2): 308-323.

[2] SUN Y C, WU L, WU S Z, et al. Attacks and countermeasures in the Internet of vehicles[J]. Annals of Telecommunications, 2017, 72(5): 283-295.

[3] CASEY E. The chequered past and risky future of digital forensics[J]. Australian Journal of Forensic Sciences, 2019, 51(6): 649-664.

[4] VAN B E, LIU V T. Digital evidence: challenging the presumption of reliability[J]. Journal of Digital Forensic Practice, 2006, 1(1): 19-26.

[5] BOYEN X. Multipurpose identity-based signcryption[C]//Advances in Cryptology - CRYPTO 2003. Berlin: Springer, 2003: 383-399.

[6] YU H F, WANG Z C, LI J M, et al. Identity-based proxy signcryption protocol with universal composability[J]. Security and Communication Networks, 2018: 1-11.

[7] KUMAR R, GOYAL R. On cloud security requirements, threats, vulnerabilities and countermeasures: a survey[J]. Computer Science Review, 2019, 33: 1-48.

[8] HERBADJI A, GOUMIDI H, HARBI Y, et al. Blockchain for Internet of vehicles security[C]//Blockchain for Cybersecurity and Privacy. First edition. Boca Raton: CRC Press, 2020: 159-197.

[9] 蔡振华, 林嘉韵, 刘芳. 区块链存储：技术与挑战[J]. 网络与信息安全学报, 2020, 6(5): 11-20.
CAI Z H, LIN J Y, LIU F. Blockchain storage: technologies and challenges [J]. Chinese Journal of Network and Information Security, 2020, 6(5): 11-20.

[10] MALONE L J. Identity-based signcryption[J]. IACR Cryptology ePrint Archive, 2002: 98.

[11] BELLARE M, NAMPREMPRE C, NEVEN G. Security proofs for identity-based identification and Signature schemes[J]. Journal of Cryptology, 2009, 22(1): 1-61.

[12] LIBERT B, QUISQUATER J J. A new identity based signcryption scheme from pairings[C]//Proceedings of 2003 IEEE Information Theory Workshop (Cat. No.03EX674). Piscataway: IEEE Press, 2003: 155-158.

[13] KARATI A, ISLAM S H, BISWAS G P, et al. Provably secure identity-based signcryption scheme for crowdsourced industrial Internet of things environments[J]. IEEE Internet of Things Journal, 2018, 5(4): 2904-2914.

[14] BONEH D, GENTRY C, LYNN B, et al. Aggregate and verifiably encrypted signatures from bilinear maps[C]//Lecture Notes in Computer Science. Berlin: Springer, 2003: 416-432.

[15] BLAZE M, BLEUMER G, STRAUSS M. Divertible protocols and atomic proxy cryptography[C]//Lecture Notes in Computer Science. Berlin: Springer, 1998: 127-144.

[16] HUNDERA N W, MEI Q, XIONG H, et al. A secure and efficient identity-based proxy signcryption in cloud data sharing[J]. KSII Transactions on Internet and Information Systems, 2020, 14(1):

455-472.

[17] LUO W, MA W P. Secure and efficient proxy re-encryption scheme based on key-homomorphic constrained PRFs in cloud computing[J]. Cluster Computing, 2019, 22(2): 541-551.

[18] 曾诗钦, 霍如, 黄韬, 等. 区块链技术研究综述：原理、进展与应用[J]. 通信学报, 2020, 41(1): 134-151.
ZENG S Q, HUO R, HUANG T, et al. Survey of blockchain: principle, progress and application[J]. Journal on Communications, 2020, 41(1): 134-151.

[19] ZHANG P Y, ZHOU M C. Security and trust in blockchains: architecture, key technologies, and open issues[J]. IEEE Transactions on Computational Social Systems, 2020, 7(3): 790-801.

[20] ZHANG Y, WU S Y, JIN B, et al. A blockchain-based process provenance for cloud forensics[C]//Proceedings of 2017 3rd IEEE International Conference on Computer and Communications (ICCC). Piscataway: IEEE Press, 2017: 2470-2473.

[21] MALAMAS V, DASAKLIS T, KOTZANIKOLAOU P, et al. A forensics-by-design management framework for medical devices based on blockchain[C]//Proceedings of 2019 IEEE World Congress on Services (SERVICES). Piscataway: IEEE Press, 2019: 35-40.

[22] 黄晓芳, 徐蕾, 杨茜. 一种区块链的云计算电子取证模型[J]. 北京邮电大学学报, 2017, 40(6): 120-124.
HUANG X F, XU L, YANG X. Blockchain model of cloud Forensics (MT)[J]. Journal of Beijing University of Posts and Telecommunications, 2017, 40(6): 120-124.

[23] OHAM C, KANHERE S S, JURDAK R, et al. A blockchain based liability attribution framework for autonomous vehicles[EB]. 2018.

[24] 李萌, 司成祥, 祝烈煌. 基于区块链的安全车联网数字取证系统[J]. 物联网学报, 2020, 4(2): 49-57.
LI M, SI C X, ZHU L H. Secure vehicular digital forensics system based on blockchain[J]. Chinese Journal on Internet of Things, 2020, 4(2): 49-57.

[作者简介]

杨小东（1981− ），男，甘肃天水人，博士，西北师范大学教授，主要研究方向为代理重签名和云计算安全。

席婉婷（1997− ），女，陕西铜川人，西北师范大学硕士生，主要研究方向为车联网安全与隐私保护。

王嘉琪（1997− ），女，甘肃兰州人，西北师范大学硕士生，主要研究方向为可搜索加密与隐私保护。

陈艾佳（1995− ），女，甘肃兰州人，西北师范大学硕士生，主要研究方向为网络与信息安全。

王彩芬（1963− ），女，河北安国人，博士，深圳技术大学教授，主要研究方向为密码学与信息安全。

通 信 学 报

2021 年（第 42 卷）总目次

专题：面向未来移动网络的大规模组网关键技术

专题：卫星通信技术

专题：确定性网络

专题：计算机通信与网络系统安全技术

学 术 论 文

综　　述

学 术 通 信

Journal on Communications

Contents List Vol.42 (2021)

Topics: Strategic Technologies to Massive Connecting for the Future Mobile Networks

Topics: Satellite Communications Technology

Topics: Deterministic Network

Topics: New Technology of Computer Communication and Network System Security

Papers

Comprehensive Reviews

Correspondences

致　　谢

《通信学报》自 1980 年创刊以来，承蒙各位专家学者的支持和厚爱，为我刊审阅了大量来稿。在新年到来之际，我们谨向 2021 年关心和支持我刊，在百忙中为我刊审稿的专家学者致以崇高的敬意和深深的感谢。希望各位专家能继续支持我们的工作，感谢你们付出的辛勤劳动！恭祝各位专家新年愉快！

2021 审稿专家名单

（如有遗漏敬请包涵，排名不分先后）

艾　渤　安　鹏　白恩健　白智全　包建荣　包晓安　鲍　煦　边　山　蔡文郁　曹春杰　曹桂兴　曹海林
曹利峰　曹腾飞　曹卫平　曾　琦　柴争义　常晓林　陈本辉　陈　朝　陈　晨　陈德运　陈东明　陈芳炯
陈　刚　陈海光　陈海华　陈后金　陈嘉兴　陈　晶　陈　恺　陈鲁生　陈美娟　陈　翔　陈燕俐　陈玉玲
陈　哲　陈智雄　程　剑　程杰仁　程庆丰　崔琪楣　代　彬　邓晓衡　丁恩杰　丁进良　丁举鹏　丁　群
丁世飞　丁宇新　董　俊　董丽华　董晓梅　董学文　董　颖　董振江　杜　蛟　杜军平　杜瑞颖　杜瑞忠
杜之波　方　箭　方　娟　方　巍　冯景瑜　冯　径　冯友宏　付安民　付绍静　付　伟　付永钢　付　钰
傅友华　高建彬　高　隽　高振国　高志鹏　龚　俭　龚　征　谷大武　顾仁涛　官　科　管　武　桂　冠
郭　滨　郭方方　郭　磊　郭　庆　郭迎春　韩益亮　何海涛　贺鹏飞　洪　飞　洪劲松　洪　伟　胡东辉
胡青松　胡学先　胡轶宁　胡永健　胡　勇　胡致远　华　光　华惊宇　黄传河　黄冬艳　黄海生　黄华军
黄开枝　黄梦醒　黄　韬　黄添强　黄欣沂　霍树民　吉根林　纪其进　贾春福　贾　敏　简　鑫　姜　明
姜　禹　蒋　鹏　蒋卫恒　金澈清　金晨辉　靳小龙　巨　刚　康海燕　柯品惠　寇　广　赖英旭　兰巨龙
李爱平　李晨亮　李春国　李德识　李　枫　李古月　李光辉　李　海　李　鹤　李　晖　李建华　李建江
李　剑　李军怀　李领治　李　宁　李　强　李仁发　李融林　李少谦　李陶深　李婉婷　李伟生　李旭杰
李　璇　李学华　李　俨　李勇军　李玉峰　李　云　李正权　李致远　廖　勇　林金朝　林　敏　刘安丰
刘　飞　刘功亮　刘光军　刘宏展　刘建华　刘连山　刘林峰　刘　留　刘　淼　刘乃安　刘奇旭　刘绍辉
刘婷婷　刘万涛　刘西蒙　刘玉玲　刘玉岭　刘　渊　刘媛妮　龙　军　卢建民　罗　彪　罗智勇　吕文俊
马昌社　马东堂　马建峰　马　礼　马　啸　牛少彰　牛奕龙　潘海为　潘　俊　庞辽军　裴　超　裴庆祺
彭　伟　彭　鑫　普园媛　亓　晋　齐丽娜　钱　峰　钱丽萍　钱亚冠　钱志鸿　乔　蕊　秦宝东　秦　川

卿朝进　邱恭安　邱卫东　曲海鹏　任艳丽　阮　彤　沙学军　尚凤军　佘　堃　申利民　沈海澜　沈　航

沈　华　沈连丰　沈玉龙　沈振萍　谌　刚　盛泳潘　宋广佳　宋铁成　苏　新　孙　聪　孙国林　谈　玲

谭晓衡　汤红波　唐　飞　唐振民　陶小峰　滕志军　田海博　田　辉　田有亮　田增山　万鸣华　汪春霆

汪　定　汪　俊　汪一鸣　王　安　王　琛　王尔申　王风宇　王　刚　王高丽　王公仆　王海涛　王海舟

王　恒　王洪玉　王　健　王　鹃　王汝言　王瑞锦　王尚广　王仕果　王天枢　王　威　王　巍　王兴元

王　毅　王永建　王　勇　王占山　王昭顺　魏　杰　魏忠诚　文伟平　吴　铤　吴　帆　吴　凡　吴　昊

吴家皋　吴礼发　吴　蒙　吴　强　吴　巍　吴晓平　吴宣利　吴　怡　吴哲夫　吴振强　武小年　席　亮

夏金祥　夏　琦　肖　斌　肖利民　肖绍球　肖　泳　谢绒娜　谢显中　谢　永　邢成文　熊　钢　熊金波

熊　余　徐启建　徐少毅　徐位凯　徐雅斌　徐煜华　许文俊　许晓荣　玄世昌　薛广涛　延志伟　闫成新

颜学雄　阳春华　杨东升　杨高波　杨恒伏　杨宏宇　杨家轩　杨　健　杨　洁　杨　军　杨　亮　杨万扣

杨　维　杨亚涛　杨　哲　杨　震　叶阿勇　叶　苗　于银辉　余礼苏　余翔宇　袁　琪　袁　征　詹　杰

张成文　张大龙　张大伟　张　迪　张海波　张海君　张　恒　张焕国　张建敏　张　军　张　科　张　磊

张立军　张连明　张　琳　张　平　张士兵　张　涛　张　薇　张　伟　张伟哲　张文彬　张艳硕　张友春

张玉军　张玉清　张长江　张治中　赵海涛　赵　亮　赵瑞杰　赵小敏　赵永利　赵　跃　郑福春　郑国强

郑　凯　郑学强　郑作亚　仲　红　周建江　周南润　周四望　周亚建　周一青　周　宇　周志刚　朱凤华

朱　辉　朱建明　朱立东　朱　琦　朱巧明　朱政宇　邹北骥　邹德清

2020 年《通信学报》优秀论文

（排名不分先后）

曾诗钦, 霍如, 黄韬, 等. 区块链技术研究综述: 原理、进展与应用[J]. 通信学报, 2020, 41(1):134-151.
ZENG S Q, HUO R, HUANG T, et al. Survey of blockchain: principle, progress and application[J]. Journal on Communications, 2020, 41(1):134-151.

袁亮, 俞啸, 丁恩杰, 等. 矿山物联网人-机-环状态感知关键技术研究[J]. 通信学报, 2020, 41(2):1-12.
YUAN L, YU X, DING E J, et al. Research on key technologies of human-machine-environment states perception in mine Internet of things[J]. Journal on Communications, 2020, 41(2):1-12.

徐勇军, 李国权, 陈前斌, 等. 基于非正交多址接入异构携能网络稳健能效资源分配算法[J]. 通信学报, 2020, 41(2): 84-96.
XU Y J, LI G Q, CHEN Q B, et al. Robust energy efficiency for SWIPT-enabled heterogeneous NOMA network[J]. Journal on Communications, 2020, 41(2): 84-96.

肖斌, 景如霞, 毕秀丽, 等. 基于分组 SIFT 的图像复制粘贴篡改快速检测算法[J]. 通信学报, 2020, 41(3): 62-70.
XIAO B, JING R X, BI X L, et al. Fast copy-move forgery detection algorithm based on group SIFT[J]. Journal on Communications, 2020, 41(3): 62-70.

王雪, 金涛, 钱志鸿, 等. D2D 中继辅助通信的能效优化算法研究[J]. 通信学报, 2020, 41(3): 71-79.
WANG X, JIN T, QIAN Z H, et al. Research on maximizing energy efficiency for relay-aided D2D communication[J]. Journal on Communications, 2020, 41(3): 71-79.

赵临东, 庄文芹, 陈建新, 等. 异构蜂窝网络中分层任务卸载：建模与优化[J]. 通信学报, 2020, 41(4): 34-44.
ZHAO L D, ZHUANG W Q, CHEN J X, et al. Hierarchical task offloading in heterogeneous cellular network: modeling and optimization[J]. Journal on Communications, 2020, 41(4): 34-44.

牛凯, 戴金晟, 朴珵楠. 面向 6G 的极化码与极化处理[J]. 通信学报, 2020, 41(5): 9-17.
NIU K, DAI J C, PIAO J N. Polar codes and polar processing for 6G wireless systems[J]. Journal on Communications, 2020, 41(5): 9-17.

谢莎, 李浩然, 李玲香, 等. 太赫兹通信技术综述[J]. 通信学报, 2020, 41(5): 168-186.
XIE S, LI H R, LI L X, et al. Survey of terahertz communication technology[J]. Journal on Communications, 2020, 41(5): 168-186.

张平, 李世林, 刘宜明,等. 区块链赋能的边缘异构计算系统中资源调度研究[J]. 通信学报, 2020, 41(10): 1-14.
ZHANG P, LI S L, LIU Y M, et al. Resource management in blockchain-enabled heterogeneous edge computing system[J]. Journal on Communications, 2020, 41(10): 1-14.

赵海涛, 张唐伟, 陈跃, 等. 基于 DQN 的车载边缘网络任务分发卸载算法[J]. 通信学报, 2020, 41(10): 172-178.
ZHAO H T, ZHANG T W, CHEN Y, et al. Task distribution offloading algorithm of vehicle edge network based on DQN[J]. Journal on Communications, 2020, 41(10): 172-178.

通信学报

Journal on Communications

发行代号：国内2-676 / 国外M395　2021年12月25日出版　定价：98.00元

ISSN 1000-436X

12