

面向车联网的匿名组密钥分发方案

何智旺, 王化群

(南京邮电大学计算机学院, 江苏 南京 210023)

摘要: 车载自组织网络 (VANET, vehicular ad hoc network) 作为智能交通系统的重要组成部分, 可在车辆行驶时提供驾驶信息等服务, 如防止碰撞、提高交通效率等。在可信第三方 (TTP, trusted third party) 和车辆进行交互时, 难免会受到窃听、篡改和伪造等安全威胁。现有的方案多是在 TTP 和车辆间进行密钥协商来创建会话密钥以保证会话的安全。但系统过度依赖 TTP 可能会受到单点故障的影响, 以及面临 TTP 向多个车辆发送相同信息时产生的信息冗余问题。同时, 创建组会话密钥所使用的密钥协商方式相较于分发方式会产生更多的交互数据和交互次数。提出面向车联网的匿名组密钥分发方案, 方案借助路侧单元 (RSU, road side unit) 来组织多个车辆创建组会话密钥, 使用基于身份的公钥密码和改进的多接收者加密方案实现 RSU 和车辆间的双向认证与组会话密钥的分发。在密钥分发的过程中, 只需要一次加密操作便可让所有组内成员获得一致的会话密钥。凭此可减少系统实体在认证和组通信时对 TTP 的过度依赖。通过形式化的安全性证明表明, 所提方案满足基本的安全要求。同时, 经过性能分析和对比, 所提方案的计算开销和通信开销比同类方案更有优势。

关键字: 车联网; 认证; 组会话密钥

中图分类号: TP309

文献标志码: A

DOI: 10.11959/j.issn.2096-109x.2023070

Anonymous group key distribution scheme for the internet of vehicles

HE Zhiwang, WANG Huaqun

School of Computer Science, Nanjing University of Posts and Telecommunications, Nanjing 210023, China

Abstract: Vehicular ad hoc networks (VANET) play a crucial role in intelligent transportation systems by providing driving information and services such as collision prevention and improved traffic efficiency. However, when a trusted third party (TTP) interacts with a vehicle in VANET, it can be vulnerable to security threats like eavesdropping, tampering, and forgery. Many existing schemes rely heavily on TTP for key negotiation to establish session keys and ensure session security. However, this over-reliance on TTP can introduce a single point of failure and redundancy issues when TTP sends the same information to multiple vehicles. Additionally, key negotiation methods

收稿日期: 2022-11-14; 修回日期: 2023-01-09

通信作者: 王化群, whq@njupt.edu.cn

基金项目: 国家自然科学基金 (62272238)

Foundation Item: The National Natural Science Foundation of China (62272238)

引用格式: 何智旺, 王化群. 面向车联网的匿名组密钥分发方案[J]. 网络与信息安全学报, 2023, 9(5): 127-137.

Citation Format: HE Z W, WANG H Q. Anonymous group key distribution scheme for the internet of vehicles[J]. Chinese Journal of Network and Information Security, 2023, 9(5): 127-137.

used for creating group session keys often result in increased interaction data and interaction times. An anonymous group key distribution scheme for the internet of vehicles was proposed to address these challenges. The Road Side Units (RSUs) were used to facilitate the creation of group session keys among multiple vehicles. Identity-based public key cryptography and an improved multi-receiver encryption scheme were utilized for communication between RSUs and vehicles, enabling two-way authentication and secure distribution of group session keys. During the key distribution process, a single encryption operation was sufficient to allow all group members to obtain a consistent session key. This reduced the reliance on TTP for authentication and group communication. Formal security proofs demonstrate that the proposed scheme satisfies basic security requirements. Furthermore, performance analysis and comparisons indicate that this scheme offers lower computational overhead and communication overhead compared to similar schemes.

Keywords: internet of vehicles, authentication, group session key

0 引言

近年来,无人驾驶的安全问题频发,如特斯拉辅助驾驶追尾事故。而智能交通系统引入VANET后,可为驾驶人员提供更安全的服务^[1],如紧急车辆警告、交通违规警告和路况警告等。VANET主要包括3种实体^[2]:TTP、RSU和车辆,通过将以上实体有机结合可显著提高交通效率、降低事故风险。无线通信短距离和车辆高移动性的特点,使得VANET易受到各种外部和内部攻击。故车辆隐私保护、身份认证和组会话密钥3个方面需要着重关注和研究。

针对车辆隐私保护,重点关注车辆身份的保护和消息的机密性。VANET中信息的交互基于露天无线电,因此,攻击者可通过轨迹追踪推断车辆的身份等敏感信息,并发动攻击(如虚假信息攻击),造成事故和伤害。故在信息传播的过程中,车辆的隐私保护十分必要。对于真实身份的保护,一般采用基于公钥基础设施的假名方案或基于数字签名的匿名消息认证协议。此外,车辆间也会进行行驶信息的交互,如车辆出现故障广播车辆信息(位置、方向等)。所以车辆间传递敏感信息时要保证信息的机密性,避免被恶意攻击者捕捉并利用。

设计VANET时,要考虑车辆的身份认证问题。在通信前,既要保护通信对方的真实身份,也要确保消息来源的真实可靠。在身份认证方面已有大量的研究工作,大致有3类^[3]:基于证书的密码系统、基于身份的密码系统和基于无证书的密码系统。在基于证书的密码系统中,需要借

助证书来管理车辆的公钥;在基于身份的密码系统中,公钥采用用户的个人身份信息(如邮箱等),无须证书来证明公钥的真实性;基于无证书的密码系统中,公私钥是半可信第三方和用户共同生成的。3种方案各有利弊。考虑到VANET受限于通信时间和距离,本文方案选择基于身份的密码系统来实现RSU和车辆间的相互认证。原因在于基于证书的密码系统需要大量的证书来认证车辆;基于无证书的密码系统需要多次交互才能生成车辆的公私钥,且存储复杂的公私钥对于资源受限的车辆而言,是不安全和低效的。此外,本文方案中通过聚合签名实现车辆身份的批量验证,提高认证的效率^[4]。

当TTP向多个车辆发送大量重复信息时,会引起系统的信息冗余问题,且TTP存在单点故障隐患。此时,系统可为合法车辆分发组密钥,仅需使用组密钥加密一次要传输的信息。在VANET中,设计一种高效的组密钥协商协议是组通信的一个难题^[1]。组密钥管理方案可分为两类:中心节点为其他成员分配一个通信密钥;每个组成员提供部分密钥,然后构成一个组密钥。虽然使用非对称加密技术也可满足此要求,但并不适用于资源受限的车联网。为降低计算成本和提高通信效率,协议需使用效率更高的对称加密。为进一步提高通信效率^[5],可使用组密钥分发的机制为一组车辆提供一个临时的组密钥来交互信息。

1 相关工作

身份验证是在授权实体访问网络前对其身份

进行验证的过程, 该机制确保只有有效的车辆方可加入 VANET 以保证通信的安全, 且恶意的车辆可被识别。对于身份的验证可通过签名来实现, 进而, 多实体的身份验证可利用聚合签名来批量处理。基于公钥密码体制的聚合签名的研究主要有 3 种。① Boneh 等^[6]在 2003 年设计了第一个以公钥基础设施 (PKI, public key infrastructure) 为基础的聚合签名方案, 将来自 n 个不同签名者的多个签名组合成一个短签名。此后, 出现了基于 PKI 的聚合代理签名方案^[7]、同步聚合签名方案^[8]和顺序聚合签名方案^[9]。② 基于身份的聚合签名 (ID-AS, identity-based aggregate signature) 方案相较于无证书签名方案, 其计算效率、成本和安全性更高。2004 年, Cheon 等^[10]提出了第一个基于身份的聚合签名方案, 解决了基于 PKI 的聚合签名方案中计算证书所带来的开销问题。之后, Shen 等^[11]在 CDH (computational Diffie-Hellman) 假设下提出一种安全高效的 ID-AS 方案; Iwasaki 等^[12]提出基于身份结构化聚合签名方案, 将结构化签名扩展到基于身份的签名中; Yang 等^[13]提出的 ID-AS 方案利用伪身份和云存储技术降低车载网的存储开销和提高认证效率。③ 为了解决 ID-AS 方案中的密钥托管问题, Castro 等^[14]提出无证书聚合签名 (CL-AS, certificateless aggregate signature) 方案, Xiong 等^[15]提出具有恒定配对计算开销的 CL-AS 方案, Hashimoto 等^[16]在 2019 年提出第一个具有固定大小的紧凑 CL-AS 方案。

组密钥管理技术的研究有如下几类: 非加密方案、公钥加密方案、对称加密和单向加密哈希函数方案、广播加密 (ConBE) 方案和多项式方案等。在加密方面的密钥管理研究中, 公钥加密方案大致分为 3 类^[17]: 基于证书的公钥加密方案、基于身份的公钥加密方案和无证书公钥加密方案。例如, Kumar 等^[18]阐述的基于 RSA 公钥密码的集中式组密钥分发协议, 虽然降低了密钥服务器的计算成本和存储复杂度, 但证书管理开销和资源受限设备对 RSA 的复杂计算不能高效处理。轻量级认证协议近年来广受关注, 此类型的认证协议有 3 个主要特点: 采用基于密码的双因素或三因素认证方法, 使用轻量级加密原语 (如

对称加密、加密哈希函数和按位异或操作), 云辅助。例如, Srinivas 等^[19]利用中国剩余定理和单向哈希函数设计的基于云的远程用户认证方案, 有效实现了远程用户与传感器节点间的相互认证和密钥管理。广播加密^[20]允许发送方不受组成员限制地选择任意成员子集作为接收方。例如, Zhong 等^[21]将广播加密用于 VANET 进行密钥分发, 所提出的基于身份的广播加密方案解决了相同信息在多个车辆间发送的冗余问题, 仅需一次加密便可为一组车辆生成定长的密文。基于多项式的密钥管理方案主要分为集中式和分布式两类。集中式密钥管理由一中心节点负责生成、分发和更新系统中各节点使用的会话密钥。例如, Gao 等在文献[22]中提出基于椭圆曲线的匿名多播方案, 通过多项式分发组密钥来获取更高的效率。为解决实体间信任缺乏的问题, 引入区块链技术, 使得密钥管理技术的研究趋向于去中心化, 即无须中心节点独立管理密钥, 而由所有成员共同管理密钥。例如, 文献[23]通过引入区块链分布式地解决了工业互联网中密钥的动态管理问题。本文方案借鉴 Wang 等^[24]提出的基于身份的多接收者加密方案, 提出一种组会话密钥分发方案, 在密文长度比较短的情况下, 满足了车联网的安全要求以及有效控制了发送方的加密成本。

2 预备知识、系统模型和安全模型

2.1 预备知识

假定 $(\mathcal{G}_1, \mathcal{G}_2)$ 是素数阶为 q 的双线性群对, q 是在安全参数 k 下的一个安全大素数, $\mathcal{G}_1$ 是一个加法循环群, $\mathcal{G}_2$ 是一个乘法循环群。假定 $\mathcal{G}_1, \mathcal{G}_2$ 上的离散对数问题是难解的。 $\mathcal{G}_1$ 到 $\mathcal{G}_2$ 的双线性映射为 $e: \mathcal{G}_1 \times \mathcal{G}_1 \rightarrow \mathcal{G}_2$ 。 $\mathcal{G}_1$ 上的生成元为 P 。双线性映射 e 满足如下性质。

- 1) 双线性: 对于 $\forall Q, R \in \mathcal{G}_1$ 和 $a, b \in \mathbb{Z}_q^*$, 有 $e(aQ, bR) = e(Q, R)^{ab}$ 。
- 2) 非退化性: $\exists Q, R \in \mathcal{G}_1$, 有 $e(Q, R) \neq 1_{\mathcal{G}_2}$ 。
- 3) 可计算性: 对于 $\forall Q, R \in \mathcal{G}_1$, 有一个高效的算法计算 $e(Q, R)$ 。

双线性映射 e 可由椭圆曲线上的修正 Weil^[25]对或 Tate^[26]对来构造, 在 $\mathcal{G}_1, \mathcal{G}_2$ 上的困难问题描

述如下。

(1) 计算 bilinear Diffie-Hellman (BDH)

敌手 $\mathcal{A}$ 在解决 $(\mathcal{G}_1, \mathcal{G}_2)$ 上计算 BDH 问题的优势为 $\text{Adv}_{\mathcal{A}}^{\text{CBDH}}$, 即

$$\text{Adv}_{\mathcal{A}}^{\text{CBDH}} = \Pr[\mathcal{A}(P, aP, bP, cP) = e(P, P)^{abc}]$$

若没有 t 时间的算法在 $(\mathcal{G}_1, \mathcal{G}_2)$ 上有至少 ϵ 的优势解决计算 BDH 问题, 则计算 BDH 是 (t, ϵ) 安全的。

(2) 决策 BDH

敌手 $\mathcal{A}$ 在解决 $(\mathcal{G}_1, \mathcal{G}_2)$ 上决策 BDH 问题的优势为 $\text{Adv}_{\mathcal{A}}^{\text{DBDH}}$, 即

$$\text{Adv}_{\mathcal{A}}^{\text{DBDH}} = |\Pr[\mathcal{A}(P, aP, bP, cP, e(P, P)^{abc}) = 0] - \Pr[\mathcal{A}(P, aP, bP, cP, T) = 0]|$$

若没有 t 时间的算法在 $(\mathcal{G}_1, \mathcal{G}_2)$ 上有至少 ϵ 的优势解决决策 BDH 问题, 则决策 BDH (t, ϵ) 是安全的。

2.2 系统模型

本文方案中存在 3 个实体, 分别是可信第三方、路侧单元和车辆 V_i , 系统模型如图 1 所示。

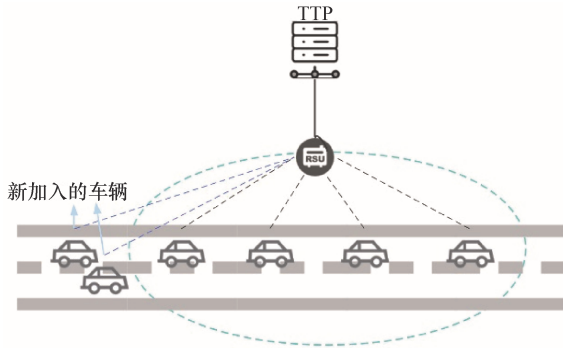


图 1 系统模型
Figure 1 System model

1) TTP 负责系统建立以及系统成员的注册和密钥的生成, 且对可疑车辆执行事后追查。

2) RSU 部署在道路周围, 由 TTP 为其生成身份的签名, 车辆通过签名验证 RSU 身份的合法性。诚信的 RSU 与车辆间利用专用短程通信协议进行通信, 由其动态聚合验证车辆的请求信息。同时, RSU 负责消息的转播。

3) 车辆在 TTP 处注册, 获得车辆临时身份和私钥等信息, 并使用这些信息向 RSU 发起认证

请求。车辆通过 RSU 分发的组会话密钥获取系统提供的服务, 以及定期告知群组内其他车辆有关车辆的交通状态信息, 如速度、方向等。

2.3 安全模型

基于身份的匿名多接收者加密 (ID-MRE, identity-based anonymous multi-receiver encryption) 方案存在 3 个不同的实体: TTP、RSU 和车辆。在阐述具体的安全模型前, 对于匿名 ID-MRE 方案的严格定义如下。

定义 1 (ID-MRE 的匿名性): 一个 ID-MRE 方案包含 4 个多项式时间算法: Setup、Extract、Encrypt 和 Decrypt。

1) Setup: TTP 生成主密钥 s 和相应的主公钥 P_{pub} 等其他参数, 将公共参数集表示为 params , params 是公开的, 而 s 是保密的。

2) Extract: TTP 在接收到车辆 V_i (其真实身份为 VID_i) 的私钥查询时, TTP 执行该算法生成对应的私钥 d_i 和假名 PID_i , 其中 $d_i = \text{Extract}(\text{params}, s, \text{VID}_i)$, TTP 将私钥发给车辆。

3) Encrypt: RSU 作为加密者选择多个车辆, 其身份表示为 $S = \{\text{ID}_1, \dots, \text{ID}_l\}$, 在输入参数集 params 和明文 M 后, 执行该加密算法生成密文 $C = \text{Encrypt}(\text{params}, S, M)$ 。

4) Decrypt: 车辆 V_i 作为解密者, 在接收到密文 C 之后, 使用参数集 params 和私钥 d_i 对其进行解密。最终, 得到明文 $M = \text{Decrypt}(\text{params}, C, d_i)$ 。

一个安全的 ID-MRE 方案必须要满足两个性质: 对自适应多身份选择密文攻击的匿名不可区分性 (ANON-sMID-CCA2) 和对自适应多身份选择密文攻击的不可区分性 (IND-sMID-CCA2)。假定 $\mathcal{A}$ 是一个多项式时间的敌手, $\mathcal{C}$ 是一个挑战者, Π 表示匿名 ID-MRE 方案。

定义 2 (ANON-sMID-CCA2): $\mathcal{A}$ 和 $\mathcal{C}$ 间执行以下游戏。

1) $\mathcal{C}$ 执行 $(\text{params}, \text{mpk}, \text{msk}) \leftarrow \text{KeyGen}(1^k)$, 并将 $(\text{params}, \text{mpk})$ 发给敌手 $\mathcal{A}$, 对主密钥 msk 进行秘密保存。 $\mathcal{A}$ 选择目标身份 $S = \{\text{ID}_0, \text{ID}_1\}$ 。

2) 第一轮查询: $\mathcal{A}$ 自适应地向 $\mathcal{C}$ 发出多次不同的查询, 每一次查询可以是如下的某一种。

① Extract 查询: 敌手请求任意身份 ID 的私

钥, $\mathcal{C}$ 通过执行 $\text{Extract}(\text{params}, \text{mpk}, \text{msk}, \text{ID})$ 获得私钥 sk_{ID} , 并将其转发给敌手。使用 S_1 表示所提取的身份集, 有交集 $S \cap S_1 = \emptyset$ 。

② Hash 查询: 敌手自适应地进行哈希函数的查询, $\mathcal{C}$ 将哈希值响应给敌手。

③ Decrypt 查询: 敌手自适应地进行解密查询, 对于敌手每一次的查询 (C^*, ID_i) , $\mathcal{C}$ 返回明文 M 。

敌手自适应地进行上述的 3 种查询, 每一次查询可以是基于上一次的查询结果。

3) 挑战: $\mathcal{C}$ 选择随机数 $\beta \in \{0, 1\}$ 以及身份集 $\{\text{ID}_2, \text{ID}_3, \dots, \text{ID}_t\}$, 使用 $\{\text{ID}_\beta, \text{ID}_2, \text{ID}_3, \dots, \text{ID}_t\}$ 和 params 信息生成信息 m^* 对应的密文 $C^* = \text{Encrypt}(\text{params}, \text{ID}_\beta, \text{ID}_2, \dots, \text{ID}_t, m^*)$, 将 C^* 返给 $\mathcal{A}$ 。

4) 第二轮查询: $\mathcal{A}$ 执行类似第一轮查询, 在 Extract 查询中, 使用 S_2 表示所提取的身份集, 交集的结果为 $S \cap (S_1 \cup S_2) = \emptyset$, 在 Decrypt 查询中, 约束结果为 $C \neq C^*$ 。

Guess: 最终, $\mathcal{A}$ 给出猜测的结果 $\beta' \in \{0, 1\}$, 若 $\beta' = \beta$, 则 $\mathcal{A}$ 赢得游戏。

满足上述描述的 $\mathcal{A}$ 被认为是 ANON-sMID-CCA2 敌手, 对于 $\mathcal{A}$ 的游戏猜测优势定义为

$$\text{Adv}_{\Pi}^{\text{ANON-sMID-CCA2}}(\mathcal{A}) = \left| \Pr[\beta' = \beta] - \frac{1}{2} \right|$$

在多项式运行时间 τ 内, 若敌手 $\mathcal{A}$ 的猜解优势 $\text{Adv}_{\Pi}^{\text{ANON-sMID-CCA2}}(\mathcal{A})$ 小于 ϵ , 则认为在任意

ANON-sMID-CCA2 敌手 $\mathcal{A}$ 的猜解下, 方案 Π 是 (τ, ϵ) -ANON-sMID-CCA2 安全的。

定义 3 (IND-sMID-CCA2): $\mathcal{A}$ 和 $\mathcal{C}$ 通过以下的游戏进行交互。

1) $\mathcal{C}$ 执行 $(\text{params}, \text{mpk}, \text{msk}) \leftarrow \text{KeyGen}(l^k)$, 并将 $(\text{params}, \text{mpk})$ 发给敌手 $\mathcal{A}$, 对主密钥 msk 进行秘密保存。 $\mathcal{A}$ 选择目标多重身份集 $S = \{\text{ID}_1, \dots, \text{ID}_t\}$, 其中 t 是一个正整数。

2) 第一轮查询: $\mathcal{A}$ 自适应地向 $\mathcal{C}$ 做出多次不同的查询, 每一次查询是 ANON-sMID-CCA2 中定义的 3 种查询 (Extract 查询、Hash 查询和 Decrypt 查询) 的任何一种, 查询同样可以是基于上一次的查询结果。

3) 挑战: 敌手 $\mathcal{A}$ 向 $\mathcal{C}$ 提供目标明文对

$\{M_0, M_1\}$, $\mathcal{C}$ 收到后, 选择随机数 $\beta \in \{0, 1\}$, 产生密文 $C^* = \text{Encrypt}(\text{params}, \text{ID}_1, \text{ID}_2, \dots, \text{ID}_t, M_\beta)$, 将 C^* 返回给 $\mathcal{A}$ 。

4) 第二轮查询: $\mathcal{A}$ 执行类似第一轮查询, 在 Extract 查询中, 使用 S_2 表示所提取的身份集, 交集的结果为 $S \cap (S_1 \cup S_2) = \emptyset$, 在 Decrypt 查询中, 约束结果为 $C \neq C^*$ 。

Guess: 最终, $\mathcal{A}$ 给出猜测的结果 $\beta' \in \{0, 1\}$, 若 $\beta' = \beta$, 则 $\mathcal{A}$ 赢得游戏。

满足上述描述的敌手 $\mathcal{A}$ 被认为是 IND-sMID-CCA2 敌手, 对 $\mathcal{A}$ 的游戏猜测优势定义为

$$\text{Adv}_{\Pi}^{\text{IND-sMID-CCA2}}(\mathcal{A}) = \left| \Pr[\beta' = \beta] - \frac{1}{2} \right|$$

在多项式运行时间 τ 内, 若敌手 $\mathcal{A}$ 的猜解优势 $\text{Adv}_{\Pi}^{\text{IND-sMID-CCA2}}(\mathcal{A})$ 小于 ϵ , 则认为在任意

IND-sMID-CCA2 敌手 $\mathcal{A}$ 的猜解下, 方案 Π 是 (τ, ϵ) -IND-sMID-CCA2 安全的。

3 本文方案

3.1 系统初始化

系统初始化过程如下, 具体的参数说明如表 1 所示。

表 1 参数说明
Table 1 Parameters description

参数	参数描述
$\mathcal{G}_1, \mathcal{G}_2$	$\mathcal{G}_1$ 是加法循环群, $\mathcal{G}_2$ 是乘法循环群
P	群 $\mathcal{G}_1$ 的生成元
$s \in \mathcal{Z}_q^*$	TTP 的私钥
$P_{\text{pub}} = sP$	TTP 的公钥
RID_{RSU}	RSU 的真实身份
u_{RSU}	RSU 的私钥
$\beta_i, t_i, r, \{\eta_1, \eta_2, \dots, \eta_n\}$	随机数
$\text{VID}_i, \text{PID}_i$	车辆 V_i 的真实身份和假名
d_i	车辆 V_i 的私钥
$T_{\text{cur}}, T'_{\text{cur}}, T_{\text{curr}}$	时间戳
$E_{\text{sk}}(m), D_{\text{sk}}(m)$	对信息 m 使用对称密钥进行加解密

1) TTP 选择随机数 $s \in \mathcal{Z}_q^*$ 作为私钥, 对应的公钥为 $P_{\text{pub}} = sP$ 。系统公开参数为

$$\begin{aligned} \text{params} &= \{\mathcal{G}_1, \mathcal{G}_2, q, e, P, P_{\text{pub}}, \\ H_1 : \{0,1\}^* &\rightarrow \mathcal{G}_1, h_1 : \mathcal{G}_1 \rightarrow \{0,1\}^\omega, \\ h_{2,3} : \{0,1\}^\omega &\rightarrow \{0,1\}^\omega, \\ h_4 : \{0,1\}^{2*} \times \{0,1\}^\omega \times \{0,1\}^\omega \times \mathcal{G}_1 &\rightarrow \{0,1\}^\omega \} \end{aligned}$$

2) RSU 通过安全信道向 TTP 提交自己的真实身份 $\text{RID}_{\text{RSU}} \in \{0,1\}^*$ 申请私钥。TTP 根据 RID_{RSU} 计算私钥 $u_{\text{RSU}} = sH_1(\text{RID}_{\text{RSU}})$ ，并对该身份进行签名 $\sigma_{\text{RSU}} = sH_1(h_1(P_{\text{pub}}) \parallel \text{RID}_{\text{RSU}})$ 以表示其是合法认证的 RSU。TTP 将 $\{u_{\text{RSU}}, \sigma_{\text{RSU}}\}$ 通过安全信道发给 RSU。

3) Extract: 车辆 V_i 选择随机数 β_i ，计算 $B_i = \beta_i P$ ，通过安全信道将自己的信息 $\{\text{VID}_i \in \{0,1\}^*, B_i\}$ 提交给 TTP 申请私钥。TTP 选择随机数 $\alpha_i \in Z_q^*$ ，计算 $A_i = \alpha_i P$ ，根据车辆身份信息 VID_i 为其计算假名 $\text{PID}_i = \text{VID}_i h_1(\alpha_i B_i)$ 以及私钥 $d_i = sQ_i$ ， $Q_i = H_1(\text{VID}_i)$ 。系统通过安全信道将 $\{d_i, A_i, \text{PID}_i, T_{\text{valid}}\}$ 发给车辆 V_i ，同时本地存放所有车辆的信息 $\{h_1(\alpha_i B_i), \text{PID}_i, Q_i, T_{\text{valid}}\}$ ，便于以后对违法车辆进行追踪。 T_{valid} 为私钥的有效期。

3.2 车辆与 RSU 相互认证并建立组会话密钥

(1) 车辆对 RSU 进行身份验证。

RSU 定时广播信息 $\{\text{RID}_{\text{RSU}}, \sigma_{\text{RSU}}, T_{\text{cur}}\}$ ， T_{cur} 为当前时间戳；车辆 V_i 行驶到 RSU 的通信范围内，验证信息的时间戳是否有效，即验证 $|T'_{\text{cur}} - T_{\text{cur}}| \leq \Delta T$ 是否成立，时间戳有效，则验证下面等式是否成立。

$$e(\sigma_{\text{RSU}}, P) = e(H_1(h_1(P_{\text{pub}}) \parallel \text{RID}_{\text{RSU}}), P_{\text{pub}})$$

等式成立，表示车辆 V_i 对 RSU 的身份验证通过；否则，验证失败，继续收集验证 RSU 的广播信息。

(2) 车辆对身份有效的 RSU 请求组会话密钥。

V_i 选择随机数 $t_i \in Z_q^*$ ，计算 $T_i = t_i P$ ， $C_i = H_1(\text{RID}_{\text{RSU}}, \text{PID}_i, h_1(T_i), \text{Session_Req}, T_{\text{cur}})$ ， $F_i = t_i C_i + d_i$ ，签名为 $\sigma_i = \{T_i, F_i\}$ 。将请求信息 $\text{Request} = \{\text{RID}_{\text{RSU}}, \text{PID}_i, \sigma_i, \text{Session_Req}, T_{\text{cur}}\}$ 通过公共通道发给 RSU，请求加入组并获得组会话密钥，其中 Session_Req 表示请求组会话密钥。

(3) RSU 验证车辆身份，若合法，则分配组密钥。

RSU 对请求信息做聚合签名验证前，先验证信

息的时效性，即验证 $|T'_{\text{cur}} - T_{\text{cur}}| \leq \Delta T$ 是否成立，时间无效，则拒绝请求；若时间有效，则通过 RSU 和 TTP 预先协商或分发的会话密钥向 TTP 提交 $(\text{PID}_1, \dots, \text{PID}_t)$ ，查询出 $(H_1(\text{VID}_1), \dots, H_1(\text{VID}_t))$ 。

RSU 选择一组随机数 $\eta = \{\eta_1, \eta_2, \dots, \eta_t\}$ ，其中 $\eta_i \in Z_q^*$ ，验证下列等式是否成立。

$$e\left(\sum_{i=1}^t \eta_i F_i, P\right) = \prod_{i=1}^t e(\eta_i C_i, T_i) e(\eta_i Q_i, P_{\text{pub}})$$

(4) 若上述等式成立，则 RSU 为验证成功的 t 个合法有效的车辆分发组会话密钥。

① 选择随机整数 $r \in Z_q^*$ 和 $\sigma \in \{0,1\}^\omega$ ，计算 $\text{seed} = h_2(\sigma)$ ， $U_1 = rP$ 。

② 对于 $i=1, \dots, t$ ，计算 $K_i = h_2(h_1(e(P_{\text{pub}}, Q_i)^r) \parallel (h_3(h_1(e(P_{\text{pub}}, Q_i)^r) \oplus \text{seed}))$ ，其中 $Q_i = H_1(\text{VID}_i)$ 。

③ 计算 $V = E_{\text{sk}}(m)$ ，sk 是根据使用的对称加密算法，以 seed 作为种子计算出的对称密钥。

④ 计算 $\rho = h_4(m, \text{seed}, K_1, \dots, K_t, U_1, V)$ 。

⑤ 形成密文 $C = (U_1, K_1, \dots, K_t, V, \rho)$ ，并将其向车辆广播。

3.3 车辆接收密文并计算出组密钥

对于身份为 PID_i 的接收者，输入系统参数、私钥 d_i 和密文 C ，其中 $i=1, \dots, t$ 。

1) 计算 $h_2(h_1(e(U_1, d_i)))$ ，与 C 中 K_j 的前 φ 位依次比较，若相等，则为对应的 K_i ，其中 $j=1, \dots, t$ 。

2) 根据下式计算 seed' ，以其为种子计算出对称密钥 sk； $\text{seed}' = h_3(h_1(e(U_1, d_i))) \oplus h_3(h_1(e(P_{\text{pub}}, Q_i)^r)) \oplus \text{seed}$ 。

3) 计算 $m' = D_{\text{sk}}(V)$ 。

4) 验证 $\rho = h_4(m', \text{seed}', K_1, \dots, K_t, U_1, V)$ 等式是否成立，若成立，则身份为 VID_i 的接收者接收组会话密钥 $\text{sk}' = \text{sk}$ ；否则，拒绝此密文。

4 安全性分析

4.1 形式化安全性证明

组会话密钥分发的实现基于匿名 ID-MRE 方案，其在 DBDH 假设下的 ANON-sMID-CCA2 安全性和 IND-sMID-CCA2 的安全性证明如下。

定理 1 匿名 ID-MRE 方案在 (T, ϵ) -

DBDHP 假设下是 $(\tau, q_{H_1}, q_{h_1}, q_{h_2}, q_{h_3}, q_{h_4}, q_e, q_d, \epsilon')$ -ANON-sMID-CCA2 安全的。其中， $\epsilon \geq \left(1 - \left(1 - \frac{1}{2^\varphi}\right)\left(1 - \frac{1}{2^\omega}\right)\right)\epsilon'$ ， $\tau = T + (q_{H_1} + q_e + q_d)\tau_1 + (t+1)\tau_2 + (q_{H_1} + q_{h_1} + q_{h_2} + q_{h_3} + q_{h_4} + q_e + q_d)O(1)$ 。 $q_{H_1}, q_{h_1}, q_{h_2}, q_{h_3}, q_{h_4}, q_e, q_d$ 分别代表哈希函数 H_1, h_1, h_2, h_3, h_4 , Extract 操作, Decryption 操作的查询次数。 τ_1, τ_2 分别表示在 $\mathbb{G}_1$ 上的标量乘法和双线性映射 e 的计算时间。

证明 假设 ANON-sMID-CCA2 敌手 $\mathcal{A}$ 在运行时间 τ 内有优势 $\text{Adv}_{\Pi}^{\text{ANON-sMID-CCA2}}(\mathcal{A}) \geq \epsilon'$ ，其中 Π 代表匿名 ID-MRE 方案。敌手 $\mathcal{A}$ 最多可做 q_e 次 Extract 查询， q_d 次 Decrypt 查询，对于哈希函数 H_1, h_1, h_2, h_3, h_4 最多可做 $q_{H_1}, q_{h_1}, q_{h_2}, q_{h_3}, q_{h_4}$ 次查询。假定表 $T_{H_1}, T_{h_1}, T_{h_2}, T_{h_3}, T_{h_4}$ 分别存储 H_1, h_1, h_2, h_3, h_4 的查询结果。挑战者 $\mathcal{C}$ 通过以下的游戏与敌手 $\mathcal{A}$ 进行交互。

Setup： $\mathcal{C}$ 输入数组 (P, P_1, P_2, P_3, T) ，将 $P_{\text{pub}} = P_1$ 设为系统公钥，对应的私钥是不公开的。其中，数组源自 $\mathcal{P}_{\text{BDH}}$ ($T = e(g, g)^{abc}$) 或 $\mathcal{R}_{\text{BDH}}$ (T 在群 $\mathbb{G}_2$ 中是不变且独立的)， $P_1 = aP, P_2 = bP, P_3 = cP$ ， a, b, c 是私密的。 $\mathcal{A}$ 选择两个可被挑战的身份 ID_0 和 ID_1 ，使用身份集 $S_a = \{\text{ID}_0, \text{ID}_1\}$ 表示。

(1) 第一轮查询

H_1 查询： $\mathcal{C}$ 输入 ID_i ，从表 T_{H_1} 中查询记录 $(*, \text{ID}_i, *)$ ，若查询到记录，则提取该记录 (c_i, ID_i, r_i) 。若 $c_i = 0$ ， $\mathcal{C}$ 将 $r_i P$ 返回给 $\mathcal{A}$ ；若 $c_i = 1$ ， $\mathcal{C}$ 将 $r_i P_3$ 返回给 $\mathcal{A}$ 。若未查询到记录，则若 $\text{ID}_i \notin S_a$ ， $\mathcal{C}$ 将 c_i 置为 0，选择 $r_i \in Z_q^*$ ，设置等式 $H_1(\text{ID}_i) = r_i P$ ，并将 $r_i P$ 作为响应回复给 $\mathcal{A}$ ；若 $\text{ID}_i \in S_a$ ， $\mathcal{C}$ 将 c_i 置为 1，选择 $r_i \in Z_q^*$ ，设置等式 $H_1(\text{ID}_i) = r_i P_3$ ，并将 $r_i P_3$ 作为响应回复给 $\mathcal{A}$ 。 $\mathcal{C}$ 在表 T_{H_1} 中添加记录 (c_i, ID_i, r_i) 。

h_1 查询： $\mathcal{C}$ 输入 $e_i \in G_1$ ，从表 T_{h_1} 中查询记录 $(e_i, *)$ ，若查询到记录，则提取记录 (e_i, t_i) ，并将 t_i 响应给 $\mathcal{A}$ ；否则， $\mathcal{C}$ 选择 $t_i \in \{0, 1\}^\omega$ ，设置等式 $h_1(e_i) = t_i$ ，将 t_i 响应给 $\mathcal{A}$ 。 $\mathcal{C}$ 将 (e_i, t_i) 存储

到表 T_{h_1} 中。

$h_{2,3}$ 查询： $\mathcal{C}$ 输入 $\sigma_j \in \{0, 1\}^\omega$ ，针对 h_2 或 h_3 查询从对应的表 T_{h_2} 或 T_{h_3} 中查询记录 $(\sigma_j, *)$ 。若查询到记录，则提取出记录 (σ_j, s_j) ，并将 s_j 响应给 $\mathcal{A}$ ；否则， $\mathcal{C}$ 选择 $s_j \in \{0, 1\}^\varphi$ 响应给 $\mathcal{A}$ ，设置等式 $h_2(\sigma_j) = s_j$ 或 $h_3(\sigma_j) = s_j$ ，同时，将 (σ_j, s_j) 写入表 T_{h_2} 或 T_{h_3} 中。

h_4 查询： $\mathcal{C}$ 以 $(m_i, \text{seed}_i, K_{1,i}, \dots, K_{t,i}, U_{1,i}, V_i)$ 为输入，从表 T_{h_4} 中查询记录 $(m_i, \text{seed}_i, K_{1,i}, \dots, K_{t,i}, U_{1,i}, V_i, *)$ 。若查询到记录，则提取出记录 $(m_i, \text{seed}_i, K_{1,i}, \dots, K_{t,i}, U_{1,i}, V_i, l_i)$ ，并将 l_i 响应给 $\mathcal{A}$ ；否则， $\mathcal{C}$ 选择 $l_i \in \{0, 1\}^\omega$ 响应给 $\mathcal{A}$ ，设置等式 $h_4(m_i, \text{seed}_i, K_{1,i}, \dots, K_{t,i}, U_{1,i}, V_i) = l_i$ ，将 $(m_i, \text{seed}_i, K_{1,i}, \dots, K_{t,i}, U_{1,i}, V_i, l_i)$ 写入表 T_{h_4} 中。

Extract： $\mathcal{C}$ 收到 $\text{ID}_i \notin S_a$ ，从 H_1 预言机查询得到 α_i ，并计算 $d_i = \alpha_i P_1$ 作为响应。由于 $d_i = \alpha_i P_1 = \alpha_i aP = aH(\text{ID}_i)$ 是用户 ID_i 的私钥，故当 $\text{ID}_i \in S_a$ 时， $\mathcal{C}$ 输掉游戏。在这一阶段， $\mathcal{A}$ 可以自适应地向挑战者 $\mathcal{C}$ 进行查询以提取用户的私钥。

Decrypt： $\mathcal{C}$ 获取到接收者密文对 (C, ID_j) ，其中 $C = (U_{1,i}, K_{1,i}, \dots, K_{t,i}, V_i, \rho_i)$ 。若 $\text{ID}_j \notin S_a$ ， $\mathcal{C}$ 可得到 d_i ，解密 C 得到明文 M 。若 $\text{ID}_j \in S_a$ ， $\mathcal{C}$ 查询表 T_{h_4} ，对于 $k = 1, \dots, t$ ， $\mathcal{C}$ 执行如下步骤。

① 令 x_k 和 z_k 分别表示 $K_{k,i}$ 的前 φ 位和后 φ 位长的比特，计算 $y_k = z_k \oplus \text{seed}_i$ 。

② $\mathcal{C}$ 从表 T_{h_2} 和 T_{h_3} 中分别判断记录 (σ_j, x_k) 和 (σ_j, y_k) 是否同时存在，若不同时存在，则 $\mathcal{C}$ 输出游戏失败，并结束；若存在，则继续进行如下操作。

③ 根据种子 seed_i 解密 V_i 得到明文 $m' = D_{\text{sk}'}(V_i)$ 。

④ $\mathcal{C}$ 查询记录 $(m', \text{seed}_i, K_{1,i}, \dots, K_{t,i}, U_{1,i}, V_i, l')$ 是否在表 T_{h_4} 中，若存在，将 m' 作为明文返回。否则，查询失败。根据加密的过程，失败的概率最大为 $1 - \left(1 - \frac{1}{2^\varphi}\right)\left(1 - \frac{1}{2^\omega}\right)$ 。

Challenge：敌手 $\mathcal{A}$ 将 $(\text{ID}_2, \text{ID}_3, \dots, \text{ID}_t, m^*)$ 和

S_d 发给挑战者。 C 选择 $\beta \in \{0,1\}$, 假定多接收者的身份集为 $S = \{ID_\beta, ID_2, ID_3, \dots, ID_t\}$ 。通过执行 Extract 操作, C 可得用户 $\{ID_\beta, ID_2, \dots, ID_t\}$ 的所有密钥, 令对应的密钥集为 $\{d_\beta, d_2, \dots, d_t\}$ 。 C 查询 H_1 得记录 $(c_\beta, ID_\beta, r_\beta)$, 其中 $c_\beta = 1$ 。 C 选择随机数 $\sigma \in \{0,1\}^\omega$, 并计算 $seed^* = h_2(\sigma), U_1 = P_2$, 以 $seed^*$ 为种子计算对称加密算法的密钥 sk^* 。对于 $i = 2, \dots, t$, C 选择 $x_i^*, y_i^* \in \{0,1\}^\rho$, 计算 $K_i^* = x_i^* \parallel (y_i^* \oplus seed^*)$, $K_\beta^* = x_\beta^* \parallel (y_\beta^* \oplus seed^*)$, $V^* = E_{sk^*}(m^*)$, $\rho^* = h_4(m^*, seed^*, K_2^*, \dots, K_t^*, K_\beta^*, U_1, V)$ 。最终, C 向敌手 A 发送密文 $C = (U_1, K_2^*, \dots, K_t^*, K_\beta^*, V^*, \rho^*)$ 。

(2) 第二轮查询

$H_1, h_1, h_2, h_3, h_4, \text{Extract}$ 和 Decrypt 的查询及响应和第一轮查询是类似的。最终, 敌手 A 输出 β' , 若 $\beta' = \beta$, 则 A 赢得游戏; 否则, A 输掉游戏。

若 $T = e(P, P)^{abc}$, 则 $T^{r_\beta} = e(bP, acP)^{r_\beta} = e(U_1, aH_1(ID_\beta)) = e(U_1, d_\beta)$ 。因此, C 是一个有效的密文。此外, T 是 G_2 上随机选取的元素, 因此, C 可以成功模拟 $\{H_1, h_1, h_2, h_3, h_4\}$ 随机预言机、密钥提取和解密预言机。可得

$$\Pr[A(P, aP, bP, cP, e(P, P)^{abc}) = 1] = \Pr[\beta' = \beta]$$

因此, A 在时间 T 内攻击方案的匿名性的概率为 ϵ' 。挑战者 C 在时间 $\tau = T + (q_{H_1} + q_e + q_d)\tau_1 + (t+1)\tau_2 + (q_{H_1} + q_{h_1} + q_{h_2} + q_{h_3} + q_{h_4} + q_e + q_d)O(1)$ 内破解决策 BDH 问题的概率为 $\epsilon \geq \left(1 - \left(1 - \frac{1}{2^\rho}\right)\left(1 - \frac{1}{2^\omega}\right)\right)\epsilon'$ 。

故基于决策 BDH 问题的难度假设, 匿名 ID-MRE 方案是 ANON-sMID-CCA2 安全的。

定理 2 匿名 ID-MRE 方案在 (T, ϵ) -DBDHP 假设下是 $(\tau, q_{H_1}, q_{h_1}, q_{h_2}, q_{h_3}, q_{h_4}, q_e, q_d, \epsilon')$ -IND-Smid-CCA2 安全的, 其中 $\epsilon \geq \left(1 - \left(1 - \frac{1}{2^\rho}\right)\left(1 - \frac{1}{2^\omega}\right)\right)\epsilon'$, $\tau = T + (q_{H_1} + q_e + q_d)\tau_1 + (t+1)\tau_2 + (q_{H_1} + q_{h_1} + q_{h_2} + q_{h_3} + q_{h_4} + q_e + q_d)O(1)$ 。 $q_{H_1}, q_{h_1}, q_{h_2}, q_{h_3}, q_{h_4}, q_e, q_d$ 分别表示哈希函数 H_1, h_1, h_2, h_3, h_4 ,

Extract, Decrypt 的查询次数。 τ_1, τ_2 分别表示在 G_1 上的标量乘法和双线性映射 e 的计算时间。

定理 2 的证明和定理 1 类似, 此处不再过多阐述。

4.2 非形式化安全性证明

除了从以上角度对方案的安全性进行分析外, 下面对方案性能做更加详细的分析。

(1) 正确性

若 TTP、RSU 和车辆均为诚实的, 则 RSU 可成功验证聚合签名, 根据车辆签名的生成, RSU 对单个签名的正确性验证如下。

$$e(F_i, P) = e(t_i C_i, P) e(s Q_i, P) = e(C_i, T_i) e(Q_i, P_{\text{pub}})$$

RSU 对聚合签名的正确性验证如下。

$$\begin{aligned} e\left(\sum_{i=1}^n \eta_i F_i, P\right) &= e\left(\sum_{i=1}^n \eta_i (t_i C_i + d_i), P\right) = \\ e\left(\sum_{i=1}^n \eta_i t_i C_i, P\right) e\left(\sum_{i=1}^n \eta_i s Q_i, P\right) &= \\ e(\eta_1 t_1 C_1, P) \cdots e(\eta_n t_n C_n, P) \cdot & \\ e(\eta_1 s Q_1, P) \cdots e(\eta_n s Q_n, P) &= \\ e(\eta_1 C_1, T_1) \cdots e(\eta_n C_n, T_n) \cdot e & \\ (\eta_1 Q_1, P_{\text{pub}}) \cdots e(\eta_n Q_n, P_{\text{pub}}) &= \\ \prod_{i=1}^n e(\eta_i C_i, T_i) e(\eta_i H_1(\text{VID}_i), P_{\text{pub}}) & \end{aligned}$$

对于车辆接收到的多接收者加密密文, 其中, 双线性对的正确性证明如下。

$$\begin{aligned} h_1(e(U_1, d_i)) &= h_1(e(rP, sH_1(\text{VID}_i))) = \\ h_1(e(sP, H_1(\text{VID}_i))^r) &= h_1(e(P_{\text{pub}}, Q_i)^r) \end{aligned}$$

(2) 双向认证

在车辆和 RSU 进行认证的过程中, 一方面车辆可通过 TTP 对 RSU 身份的签名进行认证; 另一方面, RSU 对想要加入群组的成员进行聚合签名验证, 以达到对车辆认证的目的。

(3) 匿名性

对于车辆的假名, 在向 TTP 进行注册时, 使用车辆的真实身份和 TTP 选择的随机数生成, 即 $\text{PID}_i = \text{VID}_i \oplus h_1(\alpha_i B_i) = \text{VID}_i \oplus h_1(\beta_i A_i)$ 。其中 $\alpha_i B_i$ 和 $\beta_i A_i$ 满足离散对数问题, 无法推导出其中的随机数 α_i 和 β_i 。在车辆生成签名和 RSU 验证

时,使用的是车辆的假名,而非其真实身份。故对于敌手而言,是无法获取到车辆的真实身份的。

(4) 重放攻击

RSU 收到车辆的请求信息 $\text{Request} = \{\text{RID}_{\text{RSU}}, \text{PID}_i, \sigma_i, \text{Session_Req}, T_{\text{curr}}\}$ 后,会先验证信息的时效性 $|T'_{\text{curr}} - T_{\text{curr}}| \leq \Delta T$ 。若时间差超过阈值 ΔT ,则拒绝该请求,且时间 T_{curr} 会用于签名 σ_i 的生成,修改 T_{curr} 的值并重放该请求信息是无法成功验证签名的。因此,攻击者利用截获的合法请求信息与 RSU 进行重复认证,会被及时发现并拒绝,即方案可有效抵抗重放攻击。

(5) 抗中间人攻击

攻击者在车辆和 RSU 间实施中间人攻击时,须使车辆相信其是一个合法的 RSU,同时使 RSU 相信其是一个合法的车辆。根据双向认证特性,攻击者无法伪装成二者中的任何一个。因此,方案在 RSU 和车辆间可有效抵抗中间人攻击。

5 性能分析

本节重点分析比较所提方案与文献[21]、文献[24]方案在组会话密钥产生、分发以及获取过程中所消耗的时间和通信成本。本文方案基于 Tate 双线性对 $e: \mathcal{G}_1 \times \mathcal{G}_1 \rightarrow \mathcal{G}_T$, 其中 $\mathcal{G}_1$ 是定义在超奇异椭圆曲线 $E: y^2 = x^3 + x \text{mod } g$ 上阶为 q 的加法群, g 为 512 bit 的素数, q 为 160 bit 的 Solinas 素数。方案的每一步运算操作使用 JPBC 库在配置为 2.21 GHz i7-8750H 16 GB 的主机上进行测试。表 2 列出了加解密时涉及的运算操作所需的时间。

假定接收组会话密钥的组成员有 n 个,针对各方案的计算开销和通信开销分析如下。

5.1 计算开销分析

在文献[21]方案中,TA 需要为组 $S = \{H(\text{rid}_i)\}_{i=1}^n$ 中的每一个成员计算 BK_{ID_i} , 即 n 次幂运算和 n 次哈希运算。在生成密文 CT_{IBBE} 时,需要计算 1 次配对运算, 3 次求幂运算, 1 次群 $\mathcal{G}_T$ 上的点乘运算。可得文献[21]方案的加密运行时间为 $(n+3) \cdot T_{\text{exp}} + n \cdot T_{\text{toZ}} + T_{bp} + T_{m-\mathcal{G}_T} \approx 15.51n + 57.68 \text{ ms}$ 。在组成员解密密文获取组会话密钥时,对于车辆而言,大量的计算开销会在计算 $h^{p_{j,s}(\beta)}$ 上,整体需要做 2 次配对运算、1 次群 $\mathcal{G}_T$ 上的点

乘运算、 n 次幂运算和 n 次群 $\mathcal{G}_1$ 上的点乘运算。可得文献[21]方案的解密运行时间为 $2 \cdot T_{bp} + T_{m-\mathcal{G}_T} + n \cdot T_{\text{exp}} + n \cdot T_{m-\mathcal{G}_1} \approx 46.89n + 20.15 \text{ ms}$ 。

表 2 运算操作所需的时间
Table 2 Time required for operation

符号	描述	时间/ms
T_{bp}	双线性配对运算所需的时间	8.97
T_{exp}	在群上做一次幂运算所需的时间	15.5
$T_{sm-\mathcal{G}_1}$	在群 $\mathcal{G}_1$ 上做一次数点乘法运算所需的时间	15.42
$T_{m-\mathcal{G}_1}$	在群 $\mathcal{G}_1$ 上做一次点乘运算所需的时间	31.39
$T_{m-\mathcal{G}_T}$	在群 $\mathcal{G}_T$ 上做一次点乘运算所需的时间	2.21
T_{hnp}	做一次哈希到点运算所需的时间	34.47
T_{sy}	做一次对称加密算法所需的时间	0.69
T_{gh}	做一次一般哈希运算所需的时间	0.02
T_{toZ}	将数据映射到 Z_q^* 所需要的时间	0.01

对于文献[24]方案,发送者产生密文 C 需要做 2 次数点乘法运算, $3n+1$ 次哈希运算, n 次哈希到点运算, n 次配对运算, n 次幂运算和 1 次对称加密运算, 即 $2 \cdot T_{sm-\mathcal{G}_1} + (3n+1) \cdot T_{gh} + n \cdot T_{hnp} + n \cdot T_{bp} + n \cdot T_{\text{exp}} + T_{sy} \approx 59n + 31.55 \text{ ms}$ 。对于解密运算,需要接收者从密文中匹配 R_i , 假设需要匹配 t 次才可匹配到对应的 R_j , 其中 $1 \leq i, j, t \leq n$ 。故接收者解密密文时,需要做 t 次配对运算, $2t+2$ 次哈希运算, t 次数点乘法运算, 1 次对称解密运算。即 $t \cdot T_{bp} + (2t+2) \cdot T_{gh} + t \cdot T_{sm-\mathcal{G}_1} + T_{sy} \approx 24.43t + 0.73 \text{ ms}$ 。

本文方案计算密文时,需要做 1 次数点乘法运算, n 次哈希到点运算, n 次配对运算, n 次幂运算, $3n+1$ 次哈希运算和 1 次对称加密运算。即 $T_{sm-\mathcal{G}_1} + n \cdot T_{bp} + n \cdot T_{hnp} + n \cdot T_{\text{exp}} + (3n+1) \cdot T_{gh} + T_{sy} \approx 59n + 16.13 \text{ ms}$ 。解密时,车辆需要匹配密文中的 K_i , 假设需要匹配 t 次方可找到对应的 K_i , 其中 $1 \leq i, j, t \leq n$ 。故车辆解出组会话密钥需要做 1 次配对运算, 4 次哈希运算和 1 次对称解密运算, 即 $T_{hnp} + 4 \cdot T_{gh} + T_{sy} \approx 35.24 \text{ ms}$ 。

表 3 列出了 3 个方案在加解密阶段所需要的运行时间,对 t 取平均比较次数 $n/2$ 。为了更直观地展示运行时间的对比,图 2 展示了随着组成员数量的改变,各方案加解密总运行时间的变化情

况。考虑到车辆计算能力远不如 RSU，解密时间越短越符合实际的需求，本文方案在运行时间上比另两个方案更有优势。

表 3 运行时间比较
Table 3 Run time comparison

方案	加密时间/ms	解密时间/ms	总时间/ms
文献[21]方案	$15.51n + 57.68$	$46.89n + 20.15$	$62.4n + 77.83$
文献[24]方案	$59n + 31.55$	$24.43n + 0.73$	$71.22n + 32.28$
本文方案	$59n + 16.13$	35.24	$59n + 51.37$

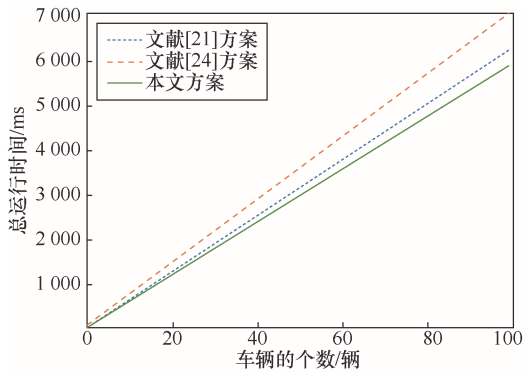


图 2 总运行时间对比
Figure 2 Total run time comparison

5.2 通信开销分析

对于每个方案，主要分析密文的结构来计算通信开销。群 G_1 的随机元素为 128 byte，针对不同的方案，依据需求选择长度为 20 byte、28 byte 和 48 byte 的哈希函数，对称加密密文长度为 16 byte，时间戳为 4 byte。各方案密文长度对比如表 4 所示。

表 4 密文长度对比
Table 4 Comparison of ciphertext lengths

方案	密文格式	长度/byte
文献[21]方案	(CT_{IBBE}, S, T_i) 和 BK_{ID_i}	$148n + 388$
文献[24]方案	$(R_1, \dots, R_n, U_1, U_2, V)$	$48n + 272$
本文方案	$(U_1, K_1, \dots, K_n, V, \rho)$	$28n + 164$

文献[21]方案中， CT_{IBBE} 密文的结构为 (CT_0, CT_1, CT_2) 。但车辆在获取组会话密钥时，还需要信息 S 和 BK_{ID_i} 。尤其是 BK_{ID_i} ，由于信息 β 对车辆是保密的，故对车辆而言获取该信息只能由 TA 计算并广播给车辆。车辆需从广播的信息

中提取出对应的 BK_{ID_i} ，若不能正确获取该信息，则无法解出组会话密钥。故 TA 广播信息的密文长度为 $128 \times 3 + 20n + 4 + 128n = 148n + 388$ byte。

文献[24]方案中，密文 $C = (R_1, \dots, R_n, U_1, U_2, V)$ ，其密文长度为 $48n + 128 \times 2 + 16 = 48n + 272$ byte。

本文方案中，密文 $C = (U_1, K_1, \dots, K_n, V, \rho)$ ，其密文长度为 $128 + 28n + 16 + 20 = 28n + 164$ byte。

6 结束语

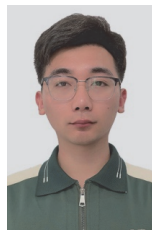
为了满足车联网中多个车辆共享安全数据的实际需求，本文提出一种基于身份的高效组密钥分发方案，在一定程度上可缓解 TTP 冗余问题带来的影响，也具备一定的分布式特性。同时，本文从形式化和非形式化两个方面详细阐述了所提方案的安全性和安全性能。通过计算开销和通信开销分析表明，本文方案比同类组密钥分发方案和所依照的多接收者加密方案有更高的效率。下一步工作会考虑更广泛的实际场景，如借助区块链实现跨域切换认证和更高级的组会话密钥的建立。

参考文献:

- [1] LI X C. Blockchain-based group key agreement protocol for vehicular ad hoc networks[J]. Computer Communications, 2022, 183: 107-120.
- [2] CHEN J N, HUANG Z J, ZHOU Y P, et al. Efficient certificate-based aggregate signature scheme for vehicular ad hoc networks[J]. IET Networks, 2020, 9(6): 290-297.
- [3] REN Y L, LI X Y, SUNSF, et al. Privacy-preserving batch verification signature scheme based on blockchain for vehicular ad-hoc networks[J]. Journal of Information Security and Applications, 2021, 58: 102698.
- [4] YANG X D, LIU R, WANG M D, et al. Identity-based aggregate signature scheme in vehicle ad-hoc network[C]//Proceedings of 2019 4th International Conference on Mechanical, Control and Computer Engineering (ICMCCE).2020: 1046-10463.
- [5] MOHANTY S, JENA D, PANIGRAHY S K. A secure RSU-aided aggregation and batch-verification scheme for vehicular networks[C]//International Conference on Soft Computing and Its Applications (ICSCA'2012). 2012: 174-178.
- [6] BONEH D, GENTRY C, LYNN B, et al. Aggregate and verifiably encrypted signatures from bilinear maps[M]//Lecture Notes in Computer Science. 2003: 416-432.
- [7] LI J, KIM K, ZHANG F G, et al. Aggregate proxy signature and verifiably encrypted proxy signature[C]//Proceedings of the 1st International Conference on Provable Security. 2007: 208-217.
- [8] AHN J H, GREEN M, HOHENBERGER S. Synchronized aggregate

- gate signatures: new definitions, constructions and applications[C]//Proceedings of the 17th ACM Conference on Computer and Communications Security. 2010: 473-484.
- [9] NEVEN G. Efficient sequential aggregate signed data[J]. IEEE Transactions on Information Theory, 2011, 57(3): 1803-1815.
- [10] CHEON J H. A new ID-based signature with batch verification[R]. Cryptology Eprint Archive Report, 2004.
- [11] SHEN L M, MA J F, LIUXM, et al. A secure and efficient ID-based aggregate signature scheme for wireless sensor networks[J]. IEEE Internet of Things Journal, 2017, 4(2): 546-554.
- [12] IWASAKI T, YANAI N, INAMURA M, et al. Tightly-secure identity-based structured aggregate signature scheme under the computational Diffie-Hellman assumption[C]//Proceedings of 2016 IEEE 30th International Conference on Advanced Information Networking and Applications (AINA). 2016: 669-676.
- [13] YANG X D, LIU R, WANG M D, et al. Identity-based aggregate signature scheme in vehicle ad-hoc network[C]//Proceedings of 2019 4th International Conference on Mechanical, Control and Computer Engineering (ICMCCE). 2020: 1046-10463.
- [14] CASTRO R, DAHAB R. Efficient certificate less signatures suitable for aggregation[J]. IACR Cryptol Eprint Arch, 2007, 2007: 454.
- [15] XIONG H, GUAN Z, CHEN Z, et al. An efficient certificateless aggregate signature with constant pairing computations[J]. Information Sciences, 2013, 219: 225-235.
- [16] HASHIMOTO K, OGATA W. Unrestricted and compact certificate less aggregate signature scheme[J]. Information Sciences, 2019, 487: 97-114.
- [17] GUO Y M, ZHANG Z F, GUO Y J. Anonymous authenticated key agreement and group proof protocol for wearable computing[J]. IEEE Transactions on Mobile Computing, 2022, 21(8): 2718-2731.
- [18] KUMAR V, KUMAR R, PANDEY S K. A computationally efficient centralized group key distribution protocol for secure multicast communications based upon RSA public key cryptosystem[J]. Journal of King Saud University-Computer and Information Sciences, 2020, 32(9): 1081-1094.
- [19] SRINIVAS J, DAS A K, KUMAR N, et al. Cloud centric authentication for wearable healthcare monitoring system[J]. IEEE Transactions on Dependable and Secure Computing, 2020, 17(5): 942-956.
- [20] FIAT A, NAOR M. Broadcast encryption[C]//Annual International Cryptology Conference. 1993: 480-491.
- [21] ZHONG H, ZHANGS, CUIJ, et al. Broadcast encryption scheme for V2I communication in VANETs[J]. IEEE Transactions on Vehicular Technology, 2022, 71(3): 2749-2760.
- [22] GAO R H, ZENG J W, DENG L Z. Efficient certificate less anonymous multi-receiver encryption scheme without bilinear pairings[J]. Mathematical Problems in Engineering, 2018, 2018: 1-13.
- [23] 张泽林, 王化群. 基于区块链的工业互联网动态密钥管理[J]. 计算机研究与发展, 2023, 60(2): 386-397.
- ZHANG Z L, WANG H Q. Dynamic key management of industrial Internet based on blockchain[J]. Journal of Computer Research and Development, 2023, 60(2): 386-397.
- [24] WANG H Q. Provably secure anonymous multi-receiver identity-based encryption with shorter ciphertext[C]//Proceedings of 2014 IEEE 12th International Conference on Dependable, Autonomic and Secure Computing. 2014: 85-90.
- [25] BONEH D, FRANKLIN M. Identity-based encryption from the Weil pairing[M]//Advances in Cryptology — CRYPTO 2001. 2001: 213-229.
- [26] MIYAJI A, NAKABAYASHI M, TAKANO S. Characterization of elliptic curve traces under FR-reduction[M]//Lecture Notes in Computer Science. 2001: 90-108.

[作者简介]



何智旺（1997—），男，安徽宿州人，南京邮电大学研究生，主要研究方向为密码学与信息安全。



王化群（1974—），男，江苏南京人，南京邮电大学教授，主要研究方向为应用密码学、区块链、云计算安全。