基于无证书聚合签名的导航信息更新方案

丁晓晖[1],曹素珍[1],窦凤鸽[1],马佳佳[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:车联网中实时的路况导航信息更新在安全驾驶、缓解交通拥堵等方面有着极其重要的作用,但如何保护用户隐私不被泄露是实时路况导航信息更新时所面临的一大挑战。为有效地解决该问题,提出了一种适用于车联网的具有实时导航信息更新功能的无证书聚合签名方案。方案中当导航公司需要访问数据时,雾节点将车辆广播的签名消息聚合后上传给可信中心,经可信中心批量验证后再将其反馈给导航公司。可信中心为车辆用户生成临时假名,实现用户身份的匿名性,满足了条件隐私保护的要求。利用聚合签名技术,降低了计算与通信开销。引入审查机制,进一步保证签名的安全性与可靠性。最后,基于椭圆曲线中的离散对数困难问题,证明了方案在适应性选择消息攻击下,满足存在性不可伪造。数值分析结果表明方案在计算开销方面具有一定的优越性。

关键词:导航信息更新;无证书密码体制;聚合签名;无双线性对;审查机制;条件隐私保护
中图分类号:TP311 **文献标识码**:A **文章编号**:1673-629X(2022)06-0112-08
doi:10.3969/j.issn.1673-629X.2022.06.019

Navigation Information Updating Scheme Based on Certificateless Aggregate Signature in Vehicle Networking

DING Xiao-hui[1],CAO Su-zhen[1],DOU Feng-ge[1],MA Jia-jia[1],WANG Cai-fen[2]
(1. School of Computer Science and Engineering,Northwest Normal University,Lanzhou 730070,China;
2. School of Big Data and Internet,Shenzhen Technology University,Shenzhen 518118,China)

Abstract:Real-time road navigation information update in vehicle networking plays an extremely important role in safe driving and alleviating traffic congestion. However,how to protect users' privacy from disclosure is a major challenge in real-time road navigation information update. In order to solve this problem effectively,a certificateless aggregate signature scheme with real-time navigation information update function is proposed,which is suitable for vehicle networking. In the scheme,when the navigation company needs to access the data,the fog node aggregates the signature message of the vehicle broadcast and uploads it to the trusted center,and then feeds it back to the navigation company after batch verification by the trusted center. The trusted center generates temporary pseudonyms for vehicle users,realizes the anonymity of user identity,and meets the requirements of conditional privacy protection. The aggregate signature technology is used to reduce the computing and communication overhead. A review mechanism is introduced to further ensure the security and reliability of the signature. Finally,based on the discrete logarithm difficulty problem in the elliptic curve,it is proved that the scheme satisfies the existence and cannot be forged under the adaptive selection message attack. The results of numerical analysis show that the scheme has some advantages in terms of computational cost.

Key words: navigation information update; certificateless cryptosystem; aggregate signature; no bilinear pair; review mechanism; conditional privacy protection

0 引 言

随着传感器技术与人工智能技术的快速发展,传统汽车已经与信息技术相结合,衍生出了一种更加安全智能的驾驶环境-车联网[1](Internet of vehicles,VANETs)。VANETs 是智慧城市的重要组成部分,为实时路况导航信息更新提供数据支持,有效的导航信息可以帮助驾驶员更加及时准确地做出选择,从而降低交通事故的发生率,在缓解交通拥堵、安全驾驶等方面都有着极为重要的作用[2]。

为了能够完成实时的路况导航信息更新,及时有

收稿日期:2021-07-14 **修回日期**:2021-11-18
基金项目:国家自然科学基金资助项目(61662069,61662071)
作者简介:丁晓晖(1997-),男,硕士研究生,研究方向为网络与信息安全;曹素珍,硕士,副教授,研究方向为密码学与网络信息安全。

效地获取相应路段的交通状态,近年来提出了一些方案[3],在这些方案中,车辆用户同意将自己收集到的路况信息上传给导航公司,但是这也增加了用户隐私泄露的风险。文献[4]提出的一种高效的基于区块链的车载社交网络隐私保护方案中,采取为车辆用户生成假名的方式实现隐私保护,降低了车辆用户身份隐私泄露的风险。车辆用户在注册过程中由可信中心(trusted authority,TA)为其生成假名,车辆用户使用假名进行通信可以很好地保护自己的隐私,但当其出现违法行为时,TA 可以通过其假名恢复出其真实身份,实现条件隐私保护。

此外,如果无法保证车联网环境中信息的真实性,将会引发严重的通信安全问题。VANETs 常采用消息签名技术来实现消息的合法性与可认证性。与此同时,通常采用聚合签名技术来降低 VANETs 中的通信开销,2003 年 Boneh 等人[5]首先在欧洲密码会上提出了聚合签名的概念。聚合签名技术可以将多个用户的签名消息压缩成一个签名消息进行处理,从而提高消息的认证效率,非常适合 VANETs 通信环境。文献[6]提出了一种基于 PKI 的聚合签名方案,该方案具有良好的安全性,可抵抗多种安全攻击。但管理和维护证书会造成极大的开销,不太适用于 VANETs。文献[7]基于椭圆曲线密码体制和通用的单向散列函数,提出了一种 VANETs 中有效的基于身份的条件隐私保护认证方案,虽解决了证书管理问题,但却存在密钥托管问题。恶意的密钥生成中心可以轻易地冒充用户进行签名,从而给系统带来严重的安全威胁。利用无证书密码体制构造签名方案[8]可以解决密钥托管问题。Al-Riyami 和 Paterson[9]在 2003 年的亚洲密码会上首次提出了无证书密码体制,在使用无证书密码体制构造签名方案时,密钥生成中心仅生成用户的部分私钥,用户随机选取一个秘密值与部分私钥一起形成自己的完整私钥,保证签名安全。文献[10-11]提出了 VANETs 中基于无证书的聚合签名方案,虽然这些方案适合车联网环境且满足安全需求,但文献[10-11]提出的方案涉及双线性对运算,在增加计算难度的同时也给 VANETs 通信环境带来了极大的通信负担。为解决该问题,文献[12-15]针对 VANETs 通信环境提出了一种无双线性对的无证书聚合签名方案,基于椭圆曲线离散对数困难问题构造了更为轻量的聚合签名方案,大大提高了计算效率。遗憾的是,Zhao 等人[12]指出文献[14]提出的方案被不可抵抗无证书密码体制中 A_{I} A_{II} 类敌手攻击,文献[15]提出的方案不可抵抗 A_{II} 类敌手攻击。此外,尽管 Zhao 等人[12]以及 Xu 等人[13]提出的方案是安全有效的,但是他们的方案都只被用于传统的车联网环境,因此,提出一个安全高效的具备导航更新功能的无证书聚合签名方案是很有必要的。

基于上述情况,该文提出了车联网中基于无证书聚合签名的导航信息更新方案。主要工作有以下几个方面:

(1)无证书密码体制既能有效解决 PKI 密码体制中的证书管理问题又可解决基于身份的密码体制中的密钥托管问题。因此本基于无证书密码体制,该文提出了一种适用于 VANETs 环境的安全高效的实时路况导航信息更新方案,在保证安全性的同时又可以有效降低 VANETs 环境的通信负担。

(2)通过为车辆用户生成临时假名,实现了对车辆用户信息的条件隐私保护。用户在通信过程中不用担心泄露自己的隐私,在用户有违法行为时,TA 可通过假名恢复出用户的真实身份,对其进行追踪。

(3)基于椭圆曲线离散对数困难问题构造了高效安全的聚合签名方案,方案在构造过程中不涉及双线性对运算,具有轻量化的优势,更适合 VANETs 中快响应低延时的计算需求,能够极大缩短用户端签名时间,降低计算开销,提高应用效率。

(4)为进一步提高车辆签名的可靠性,方案中引入了审查机制,可信中心为参与任务的每一个车辆颁发信誉值,当某一个车辆公开自己的签名消息时,范围内其他符合信誉值要求的车辆会对该签名消息进行审查,若同意该签名消息,车辆会对其进行签名。若不同意该签名消息,将向可信中心举报该车辆用户。

(5)该方案实现了数据的机密性、完整性、可靠性、身份的可认证性以及不可否认性,并给出了严格的安全性证明。通过实验数值分析表明,该方案具有明显的效率优势。

1　预备知识

1.1　符号说明

主要符号说明见表 1。

表 1　主要符号说明

符号	含义
s	系统主密钥
P_K	系统主公钥
h	哈希函数
$f()$	时间戳计算函数
ID_i	车辆真实身份
VID_i	车辆假身份
ID_R	雾节点身份信息
(A_i,SV_i)	车辆用户的部分私钥
SK_i	车辆用户的秘密值
PK_i	车辆用户的用户公钥
F_i	车辆用户的临时假名

1.2 椭圆曲线

设方程 $y^2 = x^3 + ax + b \bmod p$ 上所有的点和一个无穷远点 O 构成的集合称为椭圆曲线 $E_p(a,b)$，其中，a,b,x,y 都在 $E_p(a,b)$ 上，p 为大素数。在给定的运算下，集合中的所有点可以组成 Abel 群，记为 G，运算法则如下：

(1)假设 p 是 $E_p(a,b)$ 上的点，无穷远点是 O，那么 $p + O = p$；

(2)假设 p 是 $E_p(a,b)$ 上的点，它的加法逆元是 $Q = -p$，那么 $Q + p = O$；

(3)倍点运算：$np = \underbrace{p + p + \cdots + p}_{n}$，其中 $n \in Z_q^*$。

1.3 困难问题

椭圆曲线离散对数问题(elliptic curve discrete logarithm problem，ECDLP)：假定 G 为一个加法循环群，P 作为群 G 的生成元，G 的阶为 q，$Q \in G_P$。已知 P 和 Q，求满足 $ap = Q$ 的整数 a 是困难的。

2 方案的系统模型

在基于无证书聚合签名的导航信息更新方案中，导航公司将需要收集的道路路况信息任务发送给 TA，TA 接收到任务之后会将信息通过雾节点发送给范围内的车辆用户，在范围内的车辆用户接收到任务后，会根据任务进行相应信息的收集，收集完成后会将相应的消息签名之后广播，附近的一组满足信誉值要求的车辆会对签名消息进行审查，若认为签名合法且消息真实有效，便对该签名消息进行签名并上传给雾节点，否则将向 TA 举报该车辆用户。雾节点收集到各个车辆用户广播的签名消息后，会对消息签名的合法性进行认证，验证合法后会将签名消息进行聚合，然后打包发送给可信中心 TA。TA 接收到消息后，会对签名消息进行批量认证，若消息合法，便将消息回馈给导航公司，否则丢弃该消息，并追究相应的违法用户。系统模型如图 1 所示，它共由五个实体组成：

(1)导航公司：导航公司需要大量的实时信息来动态更新导航信息，然而导航公司本身是不具备这个能力的，因此它将相应的任务发放给可信中心 TA，之后再根据 TA 反馈回来的信息完成相应的导航信息更新工作。

(2)可信中心 TA：可信中心 TA 被认为是完全可信的，一般由政府机构担任。在该方案中，TA 主要负责车辆以及雾节点的注册，同时为了保护车辆的隐私，在注册过程中会为车辆生成伪身份，但当车辆出现违法行为时，TA 也可从其伪身份中获取他的真实身份，并且追究其相应的责任。此外，可信中心还负责为车辆用户生成信誉值，并负责信誉值的更新。最后，可信中心会对雾节点发送过来的聚合签名消息进行批量认证，认证通过后将其发送给导航公司。

(3)密钥生成中心(key generation center，KGC)：KGC 被认为是半可信的，主要负责系统参数建立以及密钥生成。当其收到可信中心发送的车辆伪身份信息后，会执行密钥生成算法，为车辆用户生成部分私钥。

(4)雾节点：雾节点一般分布在道路两侧，用来广播 TA 发布的任务信息以及收集车辆用户所广播的签名消息，雾节点在 TA 进行注册。在收集到范围内车辆的签名消息后，它会首先验证消息的合法性，若合法雾节点会对其进行聚合，并将聚合后的消息发送给可信中心 TA。

(5)车辆用户：车辆用户在接收到雾节点广播的任务后，若有符合任务要求的信息，车辆用户会将其签名之后进行广播。此外，车辆用户还需完成对附近其他车辆用户的签名消息进行审查的工作。

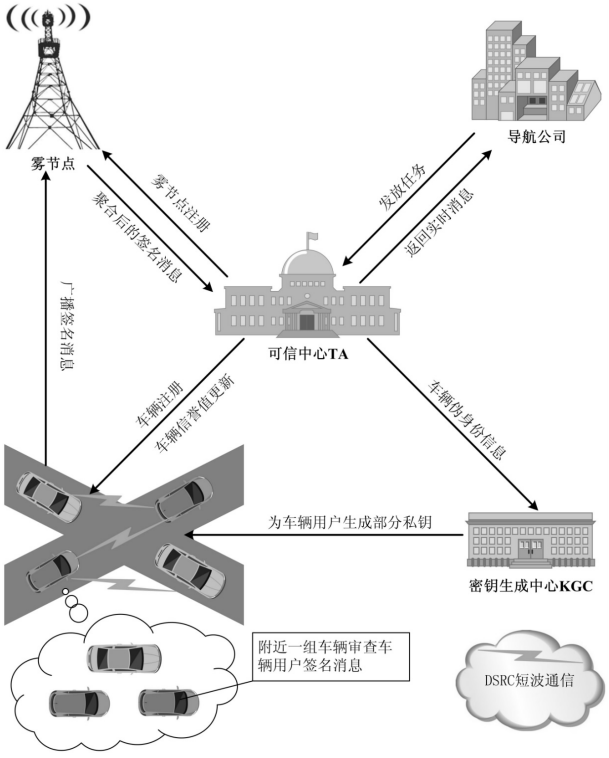

图 1 系统模型

3 方案描述

(1)系统建立算法。

密钥生成中心 KGC 建立一个椭圆曲线 $E_p(a,b)$：$y^2 = x^3 + ax + b \bmod p$，这其中 p 是一个大素数，$a,b \in E_p$。选取一个位于椭圆曲线上的点 P 作为群 G 的生成元，G 的阶为 q。设 $s \in Z_q^*$ 为系统的主密钥，则主公钥为 $P_K = s \cdot P$。选取五个安全的哈希函数 h_1,h_2,h_3,h_4,h_5：$\{0,1\}^* \rightarrow Z_q^*$ 作为系统的哈希函数。选取当前时间 t_i，使用函数 $f(t_i)$ 计算值作为当前的时间

戳。最后 KGC 公开系统参数: $\text{paras}=\{E_p(a,b),G,p,q,P,P_K,h_1,h_2,h_3,h_4,h_5,f()\}$ 。

(2)雾节点注册阶段。

雾节点执行该算法完成注册,雾节点选取自己的秘密值 $R_i\in Z_q^*$,计算其公钥 $P_{KR}=R_i\cdot P$,并将其公钥进行广播,然后将自身的公钥以及身份信息 ID_R 通过安全信道发送给 TA。

(3)车辆注册阶段。

车辆需要在可信中心处进行注册,为实现条件隐私保护,TA 会为车辆生成一个假身份,车辆使用假身份进行通信时,不会泄露自身的真实身份信息,但当车辆出现违法行为时,TA 可以通过其假身份恢复出其真实身份,并追究车辆相应的责任。设车辆的真实身份为 ID_i ,选取当前时间为 t_i ,使用函数 $f(t_i)$ 计算当前时间戳。TA 为其生成假身份 $\text{VID}_i=h_1(\text{ID}_i,f(t_i))$ 。TA 保存 $(\text{ID}_i,f(t_i),\text{VID}_i)$,然后将 VID_i 发送给 KGC 用来生成部分私钥。此外可信中心还将为车辆生成信誉值,并负责信誉值的更新。

(4)部分私钥生成算法。

密钥生成中心执行该算法为车辆用户生成部分私钥。密钥生成中心 KGC 输入系统参数 paras ,系统主密钥 s ,以及车辆的假身份 VID_i 。然后随机选取 $a_i\in Z_q^*$,计算 $A_i=a_i\cdot P$, $h_{a_i}=h_2(A_i\parallel P_K\parallel f(t_i))$, $\text{SV}_i=a_i+h_{a_i}\cdot s\bmod q$ 。并将 (A_i,SV_i) 发送给 VID_i 作为其部分私钥。

(5)用户秘密值生成算法。

车辆用户随机选取 $b,r_i^1,r_i^2\in Z_q^*$,选取当前时间为 t_i ,使用函数 $f(t_i)$ 计算得当前时间戳。计算 $\text{SK}_i^1=h_3(r_i^1\parallel f(t_i)\parallel P_K)$, $\text{SK}_i^2=h_3(r_i^2\parallel f(t_i)\parallel P_K)$,则用户秘密值为 $\text{SK}_i=b(\text{SK}_i^1+\text{SK}_i^2)$,公钥为 $\text{PK}_i=\text{SK}_i\cdot P$ 。用户将自己的秘密值保存,并将公钥公开。

(6)假名生成算法。

为保证方案具有时效性,TA 执行本算法为车辆生成临时假名。当在相应的时间范围内,使用该假名进行签名的消息才被认为是有效的。当车辆离开相应路段或者超出相应的时间范围,临时假名将被撤销。TA 选取当前时间为 t_i ,使用函数 $f(t_i)$ 计算得当前时间戳。计算 $\text{ID}_i^*=\text{VID}_i\oplus h_3(\text{PK}_R\parallel\text{PK}_i\parallel f(t_i))$,则车辆的临时假名为 $F_i=(\text{ID}_i^*,f(t_i))$ 。

(7)任务发放。

导航公司将任务 $\text{task}_i=(j,\text{area},\text{type},\text{tr})$ 发送给 TA,这其中 j 为本次任务的编号, area 为需要收集信息的大致路段, type 为收集信息的类型要求, tr 为对车辆用户要求的信誉阈值。TA 根据要求将相应任务下发给相应路段的雾节点,雾节点接受到任务后会把任务进行广播,满足任务要求且信誉值符合规定的车辆会将收集到的消息签名之后进行广播,相应路段其他车辆在验证签名消息合法后将其重新签名发送给雾节点,雾节点会将所有的签名消息进行认证后进行聚合,并发送给 TA。

(8)数据的收集及上传。

为了提高收集数据的可靠性与准确性,当一个车辆 V_A 广播自己的签名消息后,附近的一组满足信誉值要求的车辆 $(V_1\cdots V_n)$ 会首先验证 V_A 的签名是否合法,若合法,车辆用户会验证消息 m 是否真实有效。如果车辆用户不同意该消息,可及时向可信中心 TA 进行举报,TA 经过调查后若确认车辆 V_A 违规,会扣除车辆 V_A 以及同意消息 m 车辆用户的信誉值,同时增加不同意消息 m 车辆用户的信誉值。若车辆用户信誉值过低,可信中心则会撤销该车辆用户的身份。若车辆用户 $(V_1\cdots V_n)$ 同意消息 m ,则对该消息进行签名,并将签名后的消息全部上传给雾节点,雾节点进行认证后将签名消息进行聚合,然后将聚合签名消息发送给可信中心进行认证。以下是数据收集与上传的具体过程:

①签名算法。

车辆用户 V_A 执行签名算法对自己收集到的消息 m_i 进行签名。V_A 随机选取 $c_i\in Z_q^*$,计算 $C_i=c_i\cdot P$ 。计算 $h_s=h_5(m_i,F_i,\text{PK}_i,A_i,C_i)$, $h_j=h_5(m_i,A_i,F_i,C_i,\text{PK}_i)$, $Q_i=c_i+h_j\,\text{SK}_i+h_s\,\text{SV}_i\bmod q$,则签名 $\sigma_i=(C_i,Q_i)$ 。并广播签名与消息 m_i 。

②附近车辆用户审查阶段。

当附近车辆用户 $(V_1\cdots V_n)$ 接收到车辆用户广播的签名 $\sigma_i=(C_i,Q_i)$ 与消息 m_i 之后,若同意消息 m_i 真实且有效,则验证等式:

$$Q_iP=C_i+h_s\cdot A_i+h_s\cdot h_{a_i}\cdot P_K+h_j\cdot\text{PK}_i$$

是否成立。若成立,则认为 V_A 的签名合法,其他车辆 $(V_1\cdots V_n)$ 对消息 m_i 进行签名,并广播发送给附近的雾节点。若附近车辆用户认为车辆用户 V_A 存在违法行为,可将其向可信中心举报。可信中心在验证之后会对相应车辆用户的信誉值进行增加或扣除。

③雾节点聚合签名阶段。

雾节点在接收到 n 个车辆用户的签名消息后,会首先验证每个车辆用户的签名消息是否合法,对于合法的签名消息雾节点会将其进行聚合,对于违法的签名消息,雾节点会将其摒弃,并上报 TA 对其进行违法追踪,扣除其信誉值。首先雾节点对每一个单一的消息进行计算:

$$h_s=h_5(m_i,F_i,\text{PK}_i,A_i,C_i)$$

$$h_j=h_5(m_i,A_i,F_i,C_i,\text{PK}_i)$$

$$h_{a_i}=h_2(A_i\parallel P_K\parallel f(t_i))$$

验证等式：

$$Q_iP = C_i + h_s \cdot A_i + h_s \cdot h_{a_i} \cdot P_K + h_j \cdot \mathrm{PK}_i$$

是否成立。若成立，则接受该签名消息，否则将其丢弃。对于验证成功的 n 个车辆用户 $\{v_1, v_2, \cdots, v_n\}$ 的 n 个签名消息：

$$\{(m_1, \sigma_1 = (C_1, Q_1)) \cdots (m_n, \sigma_n = (C_n, Q_n))\};$$

进行聚合。计算 $Q = \sum_{i=1}^{n} Q_i$，输出聚合签名 $\sigma = (C_1, \cdots, C_n, Q)$，并将聚合后的签名消息发送给可信中心进行验证。

④可信中心批量认证阶段。

可信中心接收到聚合签名后，通过以下等式进行批量验证：

$$QP = \sum_{i=1}^{n} C_i + \sum_{i=1}^{n} h_s \cdot A_i + \left(\sum_{i=1}^{n} h_s \cdot h_{a_i}\right) \cdot P_K + \sum_{i-1}^{n} h_j \cdot PK_i$$

若成立，则接受该消息，并将其反馈给导航公司。否则丢弃该消息，并追查违法用户。

(9)导航信息更新。

导航公司接受到可信中心发送过来的消息后，会根据消息及时地更新相应路段的导航信息，大大地缓解交通压力的同时降低事故发生率。

4 安全性分析

4.1 正确性分析

对单个签名进行正确性验证。

验证等式：

$$Q_iP = C_i + h_s \cdot A_i + h_s \cdot h_{a_i} \cdot P_K + h_j \cdot \mathrm{PK}_i$$

是否成立，验证过程如下：

$$\begin{aligned} Q_iP &= (c_i + h_j\,\mathrm{SK}_i + h_s\,\mathrm{SV}_i)P = \\ &c_iP + h_j\,\mathrm{SK}_iP + h_s\,\mathrm{SV}_iP = \\ &C_i + h_j\,\mathrm{PK}_i + h_s(a_i + h_{a_i}s)P = \\ &C_i + h_j\,\mathrm{PK}_i + h_sa_iP + h_sh_{a_i}sP = \\ &C_i + h_j\,\mathrm{PK}_i + h_sA_i + h_sh_{a_i}P_K \end{aligned}$$

得证。

同理，可以通过对下列等式进行验证，得出聚合签名的正确性：

$$QP = \sum_{i=1}^{n} C_i + \sum_{i=1}^{n} h_s \cdot A_i + \left(\sum_{i=1}^{n} h_s \cdot h_{a_i}\right) \cdot P_K + \sum_{i-1}^{n} h_j \cdot \mathrm{PK}_i$$

4.2 安全性证明

该文的聚合签名方案是基于无证书的密码体制，依据文献[16]提出的安全模型，该方案的安全性考虑两种不同的敌手，第一类普通敌手 A_I 以及第二类超级敌手 A_{II}。

定理 1：在随机预言模型中，如果在多项式时间内存在一个普通敌手 A_I 能够以不可忽略的概率 ε 赢得游戏，那么一定存在一个挑战者能够以以下的优势解决 ECDLP 困难问题：

$$\varepsilon^* \geqslant \left(1 - \frac{q_{h2}}{q}\right)^{q_{cu}} \left(1 - \frac{1}{q_{cu}}\right)^{q_k} \left(1 - \frac{q_{h3}}{q}\right)\left(1 - \frac{q_{h4}}{q}\right)\left(1 - \frac{q_{h5}}{q}\right)\frac{1}{q_{cu}}\varepsilon$$

其中，q_{h2}、q_{h3}、q_{h4}、q_{h5} 表示对应的哈希预言机查询次数，q_{cu} 表示创建用户预言机查询次数，q_k 表示用户的部分私钥查询次数。

证明：假设一个普通敌手 A_I 在方案中能够以不可忽略的优势 ε 赢得游戏，即成功伪造目标用户 VID_i 的有效签名，则认为与其交互的挑战者 CE 能够成功解决 ECDLP 困难问题。CE 与 A_I 按照如下步骤进行游戏交互。

(1)初始化阶段。

挑战者 CE 执行算法构建系统，并令 $Q = P_K$，挑战者公开系统参数，并建立维护以下四个列表：

L_1 列表 $(\mathrm{VID}, A, P_K, T_{h_2})$

L_2 列表 $(\mathrm{VID}, \mathrm{PK}_i, T_{h_3})$

L_3 列表 $(\mathrm{VID}, m, F_i, \mathrm{SK}_i, A)$

L_4 列表 $(\mathrm{VID}, m, F_i, \mathrm{SK}_i, A, T_{h_4}, T_{h_5}, C, Q)$

(2)预言机查询阶段。

在本阶段，第一类普通敌手与挑战者之间进行预言机交互。

h_2 预言机查询：

普通敌手 A_I 以 VID 进行询问，若 VID 在 L_1 列表中已经存在，则返回 T_{h_2} 给敌手 A_I。若不存在，则挑战者执行部分私钥预言机查询，随机选取 $a \in Z_q^*$，计算 $A = a \cdot P$，$T_{h_2} = h_2(A_i \| P_K \| f(t_i))$，并将 T_{h_2} 返回给敌手 A_I。

h_3 预言机查询：

普通敌手 A_I 以 VID 进行询问，若在 L_2 列表中已经存在相应元组，则返回 T_{h_3} 给敌手 A_I。若不存在，则挑战者执行用户秘密值预言机查询，随机选取 $b, r_1, r_2 \in Z_q^*$，计算 $\mathrm{SK}_1 = h_3(r_1 \| f(t_i) \| P_K)$，以及 $\mathrm{SK}_2 = h_3(r_2 \| f(t_i) \| P_K)$，$\mathrm{SK} = b(\mathrm{SK}_1 + \mathrm{SK}_2)$，$T_{h_3} = \mathrm{SK} \cdot P$，并将 T_{h_3} 返回给敌手 A_I。

h_4 预言机查询：

普通敌手 A_I 以 (VID, m) 进行询问，若在 L_3 列表中已经存在相应元组，则返回 T_{h_4} 给敌手 A_I。若不存在，则挑战者执行用户秘密值预言机查询，以及部分私钥预言机查询。随机选取 $c \in Z_q^*$，$C = c \cdot P$。计算 $T_{h_4} = h_4(m, F, \mathrm{PK}, A, C)$ 并将 T_{h_4} 返回给敌手 A_I。

h_5 预言机查询：

普通敌手 A_I 以 (VID,m) 进行询问,若在 L_4 列表中已经存在相应元组,则返回 T_{h_5} 给敌手 A_I。若不存在,则挑战者执行用户秘密值预言机查询,以及部分私钥预言机查询。计算 $T_{h_5}=h_5(m_i,F_i,\mathrm{PK}_i,A_i,C_i)$ 并将 T_{h_5} 返回给敌手 A_I。

用户创建预言机查询:

敌手 A_I 以 VID 向挑战者进行询问,挑战者查询 L_3 列表,若元组不存在列表中,则执行如下操作:

①当 $\mathrm{VID}=\mathrm{VID}_m$ 时。

挑战者随机选择随机选取:

$a,T_{h_2}\in Z_q^*$

$b,r_1,r_2\in Z_q^*$

计算:

$A=a\cdot P$

$\mathrm{SK}_1=h_3(r_1\|f(t_i)\|P_K)$

$\mathrm{SK}_2=h_3(r_2\|f(t_i)\|P_K)$

$\mathrm{SK}=b(\mathrm{SK}_1+\mathrm{SK}_2),\mathrm{PK}=\mathrm{SK}\cdot P,\mathrm{SV}=\perp$

②当 $\mathrm{VID}\neq\mathrm{VID}_m$ 时。

挑战者随机选择随机选取:

$\mathrm{SV},\mathrm{SK},a,T_{h_2}\in Z_q^*$

计算:

$A=a\cdot P$

$A=\mathrm{SK}\cdot P-T_{h_2}\cdot Q$

然后将其添加到相应的列表中。若有相应的元组,则挑战者查询 L_1 列表,若存在相应的 (VID,A,T_{h_2}),验证是否满足 $h_2(A,Q)\rightarrow T_{h_2}$,若不满足,则挑战者结束本次游戏,否则返回用户信息。

用户秘密值预言机查询:

普通敌手 A_I 以 VID 进行询问,挑战者查询 L_3 列表,若在 L_3 列表中已经存在相应元组,则返回 (PK,SK) 给敌手 A_I。

若不存在,挑战者随机选取:

$b,r_1,r_2\in Z_q^*$

计算:

$\mathrm{SK}_1=h_3(r_1\|f(t_i)\|P_K)$

$\mathrm{SK}_2=h_3(r_2\|f(t_i)\|P_K)$

$\mathrm{SK}=b(\mathrm{SK}_1+\mathrm{SK}_2)$

$\mathrm{PK}=\mathrm{SK}\cdot P$

并将 (PK,SK) 返回给敌手 A_I。

部分私钥预言机查询:

设在有效的多项式时间内,挑战者 A_I 最多进行 q_k 次部分私钥询问。敌手以 VID 进行询问,当 $\mathrm{VID}=\mathrm{VID}_m$ 时,挑战者输出 $\perp$,并终止游戏。当 $\mathrm{VID}\neq\mathrm{VID}_m$ 时,挑战者查询 L_3 列表,若在 L_3 列表中已经存在相应元组,挑战者返回 (A,SV) 给 A_I,若不存在相应的元组,挑战者随机选取 $a,\mathrm{SV}\in Z_q^*$,计算 $A=a\cdot P$。并返回 (A,SV) 给 A_I。

公钥预言机查询:

敌手以 VID 进行询问,挑战者查询 L_3 列表,若在 L_3 列表中已经存在相应元组,挑战者返回 (A,PK) 给 A_I,若不存在相应的元组,挑战者执行用户秘密值预言机查询以及部分私钥预言机查询。然后将 (A,PK) 返回给 A_I。

签名预言机查询:

当挑战者以 ($m_i,A_i,F_i,\mathrm{VID}_i$) 进行询问时,挑战者随机选择:

$Q_i,h_s,h_j\in Z_q^*$

$T_{h_{2i}}=h_2(A_i\|P_K\|f(t_i))$

并将 $\{A_i,T_{h_{2i}}\}$ 加入到 L_1 列表中。

令:

$C_i=Q_iP-h_s\cdot A_i-h_s\cdot T_{h_{2i}}\cdot P_K-T_{h_{3i}}\cdot\mathrm{PK}_i$

将 (m_i,C_i,Q_i,A_i) 插入到 L_3L_4 中。

(3)输出阶段。

最后,敌手 A_I 输出 (VID,A,m) 的一个伪造签名,此时,若 $\mathrm{VID}\neq\mathrm{VID}_m$,则挑战者宣布失败,否则,挑战者从签名预言机中找到如下签名消息:

$(m_i,\sigma_i=(A_i,Q_i),F_i,C_i,\mathrm{PK}_i)$

若挑战者赢得游戏,则有:

$$Q_iP=C_i+h_s\cdot A_i+h_s\cdot T_{h_{2i}}\cdot P_K+T_{h_{3i}}\cdot\mathrm{PK}_i \quad (1)$$

敌手 A_I 能够在多项式时间内以不同的 Q_i,h_s,重新构造一个新的有效的签名:

$(m_i,\sigma_i^*=(A_i,Q^*),F_i,C_i^*,\mathrm{PK}_i)$

即以下等式成立:

$$Q_i^*P=C_i^*+h_s^*\cdot A_i+h_s^*\cdot T_{h_{2i}}\cdot P_K+T_{h_{3i}}\cdot\mathrm{PK}_i \quad (2)$$

根据式(1)以及式(2),挑战者 C 可以计算出:

$$(Q_i-Q_i^*)\cdot P=(h_i-h_i^*)T_{h_{2i}}s\cdot P \quad (3)$$

由式(3)挑战者可以解出 $s=\dfrac{(Q_i-Q_i^*)}{(h_i-h_i^*)T_{h_{2i}}}\bmod q$。即挑战者解决了 ECDLP 问题。

最后,计算挑战者 CE 解决 ECDLP 困难问题的优势,若挑战者能够成功解决 ECDLP 问题,应同时满足以下两种情况:

E_1:挑战者 CE 从来没有终止过游戏。

E_2:Q_i^* 对于消息 (VID_m,m) 来说,是一个合法签名。

所以,挑战者取胜的概率为:

$$\varepsilon^*=\mathrm{pr}[E_1\wedge E_2]=\mathrm{pr}[E_1]\mathrm{pr}[E_1\mid E_2] \quad (4)$$

这其中,$\mathrm{pr}[E_1\mid E_2]=\varepsilon$。

又经过游戏过程分析计算得:

$$\mathrm{pr}[E_1]=(1-\frac{q_{h2}}{q})^{q_{re}}(1-\frac{1}{q_{cu}})^{q_{k}}(1-\frac{q_{h3}}{q})(1-$$

$$\frac{q_{h4}}{q})(1-\frac{q_{h5}}{q})\frac{1}{q_{cu}} \tag{5}$$

所以,由式(4)、式(5)可以得出:

$$\varepsilon^{*} \geqslant (1-\frac{q_{h2}}{q})^{q_{cu}}(1-\frac{1}{q_{cu}})^{q_{k}}(1-\frac{q_{h3}}{q})(1-\frac{q_{h4}}{q})(1-\frac{q_{h5}}{q})\frac{1}{q_{cu}}\varepsilon$$

显然,若挑战者 CE 能够以优势 ε^{*} 成功伪造出一个签名,那么挑战者便可以解决 ECDLP 问题,然而在随机预言模型下,ECDLP 问题是困难问题,也就是说敌手的优势是不存在的。即该方案可以抵抗敌手 A_I 的伪造攻击。证明完毕。

定理 2:在随机预言模型中,如果在多项式时间内存在一个超级敌手 A_{II} 能够以不可忽略的概率 ε 赢得游戏,那么一定存在一个挑战者能够以以下的优势解决 ECDLP 困难问题:

$$\varepsilon^{*} \geqslant (1-\frac{q_{h2}}{q})^{q_{cu}}(1-\frac{1}{q_{cu}})^{q_{k}}(1-\frac{1}{q_{cu}})^{q_{m}}(1-\frac{q_{h3}}{q})(1-\frac{q_{h4}}{q})(1-\frac{q_{h5}}{q})\frac{1}{q_{cu}}\varepsilon$$

其中,q_{h2}、q_{h3}、q_{h4}、q_{h5} 表示对应的哈希预言机查询次数,q_{cu} 表示创建用户预言机查询次数,q_b 表示用户的部分私钥查询次数,q_m 表示用户秘密值查询次数。

经证明,该方案能够抵抗超级敌手 A_{II} 的伪造攻击,方案安全,证明过程与定理 1 类似,篇幅限制,在此不再赘述。

5 性能分析

5.1 方案性能对比

符号说明如表 2 所示。

表 2 符号说明

符号	含义
T_{bp}	双线性对运算
T_{bm}	双线性对中点乘运算
T_{ba}	双线性对中加法运算
T_{em}	椭圆曲线中点乘运算
T_{ea}	椭圆曲线中加法运算
T_h	哈希运算

表 3 各方案主要性能对比

方案	文献[17]	文献[15]	文献[11]	文中方案
机密性	√	√	√	√
匿名性	√	√	√	√
不可链接性	√	√	√	√
无双线性对	×	√	×	√
可抵抗 A_I 类敌手攻击	×	√	√	√
可抵抗 A_{II} 类敌手	√	×	√	√

如表 3 所示,将方案所满足的主要性能同竞争方案做分析比对,结果表明,文献[17]提出的方案不满足无双线性对且不能抵抗 A_I 类敌手攻击。文献[15]采用椭圆曲线构造了更轻量的密码方案,但其却不能抵抗恶意的 KGC 攻击。文献[11]提出的无证书聚合签名方案虽满足安全性要求,但其却有着极大的计算开销,在 VANETs 环境中会造成极大的通信负担。文中方案在满足所有的安全性要求的同时采用椭圆曲线构造了更为轻量的无证书聚合签名方案,更适用于 VANETs 通信环境。

5.2 方案计算开销对比

如表 4 所示,文献[11]提出的无证书聚合签名方案在签名算法部分的总计算开销为 $5T_{bm}+3T_{ba}+4T_h$,在验证算法部分的总计算开销为 $4T_{bp}+2T_{bm}+T_{ba}+4T_h$,在聚合签名算法部分的总开销为 $4T_{bp}+7nT_{bm}+nT_{ba}+4nT_h$。同理可得文献[17]以及文献[15]所提出方案的总计算开销。

表 4 方案计算开销

方案	签名算法	验证算法	聚合签名算法
文献[17]	$2T_{bm}+T_{ba}+T_h$	$3T_{bp}+T_{bm}+T_{ba}+2T_h$	$3T_{bp}+nT_{bm}+nT_{ba}+2nT_h$
文献[15]	$T_{em}+T_{ea}+T_h$	$3T_{em}+2T_{ea}+2T_h$	$(n+2)T_{em}+(n+2)T_{ea}+2nT_h$
文献[11]	$5T_{bm}+3T_{ba}+4T_h$	$4T_{bp}+2T_{bm}+T_{ba}+4T_h$	$4T_{bp}+7nT_{bm}+nT_{ba}+4nT_h$
文中方案	$T_{em}+2T_h$	$5T_{em}+3T_{ea}+3T_h$	$(3n+2)T_{em}+3nT_{ea}+3nT_h$

在文中方案中,签名算法的总计算开销为 $T_{em}+2T_h$,验证算法的总计算开销为 $5T_{em}+3T_{ea}+3T_h$,聚合签名算法的总开销为 $(3n+2)T_{em}+3nT_{ea}+3nT_h$。可以看出,由于采用椭圆曲线构造了无证书聚合签名方案,避免了复杂的双线性对运算,使得文中方案在计算开销方面较文献[11,17]提出的无证书聚合签名方案有较大优势。

为了更清楚地对比方案的计算效率,在配备 Intel Core i5-7500 处理器,3.0 GHz 主频,以及 8 GB 的内存环境下进行了一个模拟实验。结果如图 2、图 3 所示,将该文提出的方案同文献[11,15,17]等的方案进行计算效率对比。

结果表明,该文提出的方案在签名算法以及验证算法方面的计算效率较文献[11,17]提出的方案有明显优势,与文献[15]基本相当。但文献[15]提出的方案不能抵抗 A_{II} 类敌手攻击,因此安全性不如文中方

案。此外文中方案采用了聚合签名技术,进一步降低了计算开销,使其可以满足通信计算开销极大的 VANETs 环境。

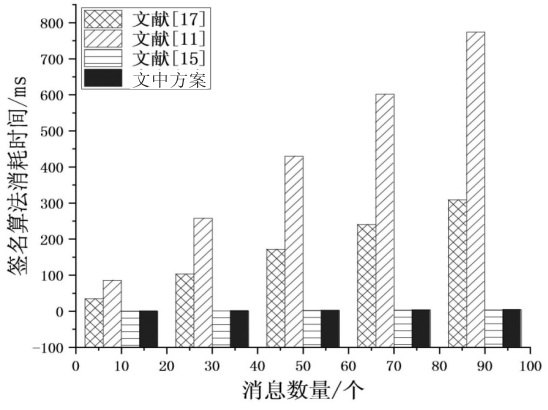

图 2　签名算法消耗时间

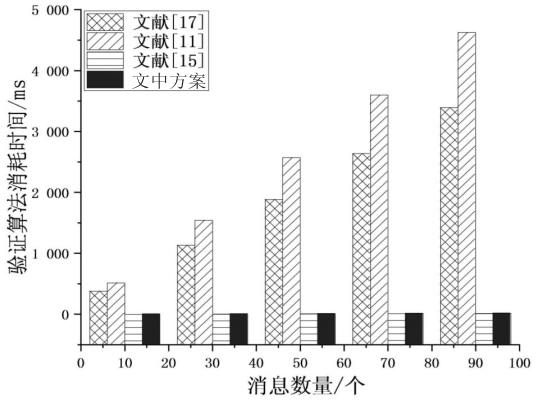

图 3　验证算法消耗时间

6　结束语

针对 VANETs 中路况导航信息更新中的安全隐私问题,提出了一种基于无证书密码体制具有条件隐私保护以及审查机制的无证书聚合签名方案,并通过严格的安全性证明表述了方案的安全性。通过生成临时假名,实现车辆用户的条件隐私保护。方案的构造过程中未使用双线性对运算,并使用聚合签名技术使得方案的计算开销大大降低。通过与其他方案的性能分析对比表明,该方案在安全性及计算效率上有明显优势,适用于 VANETs 应用环境。

参考文献:

[1] ALESSANDRINI A, CAMPAGNA A, SITE P D, et al. Automated vehicles and the rethinking of mobility and cities[J]. Transportation Research Procedia, 2015, 5: 145-160.

[2] 赖成喆,张　敏,郑　东. 一种安全高效的无人驾驶车辆地图更新方案[J]. 计算机研究与发展, 2019, 56(10): 2277-2286.

[3] DEMIR I, HUGHES F, RAJ A, et al. Generative street addresses from satellite imagery[J]. ISPRS International Journal of Geo-Information, 2018, 7(3): 84-106.

[4] PU Y, XIANG T, HU C, et al. An efficient blockchain-based privacy preserving scheme for vehicular social networks[J]. Information Sciences, 2020, 540: 308-324.

[5] 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.

[6] HA J. An efficient and robust anonymous authentication scheme in global mobility networks[J]. International Journal of Security and Its Applications, 2015, 9(10): 297-312.

[7] ALI I, LAWRENCE T, LI F. An efficient identity-based signature scheme without bilinear pairing for vehicle-to-vehicle communication in VANETs[J]. Journal of Systems Architecture, 2020, 103: 101692.

[8] 宋　成,张明月,彭维平,等. 基于非线性对的车联网无证书批量匿名认证方案研究[J]. 通信学报, 2017, 38(11): 35-43.

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

[10] XU Zhiyan, HE Debiao, KUMAR N, et al. Efficient certificate less aggregate signature scheme for performing secure routing in VANETs[J]. Security and Communication Networks, 2020(2): 1-12.

[11] 赵　楠,章国安,谷晓会. VANET 中隐私保护的无证书聚合签名方案[J]. 计算机工程, 2020, 46(1): 114-120.

[12] ZHAO Y, HOU Y, WANG L, et al. An efficient certificateless aggregate signature scheme for the Internet of Vehicles[J]. Transactions on Emerging Telecommunications Technologies, 2020, 31(5): e3708.

[13] XU G, ZHOU W, SANGAIAH A K, et al. A security-enhanced certificateless aggregate signature authentication protocol for INVANETS[J]. IEEE Network, 2020, 34(2): 22-29.

[14] KAMIL I A, OGUNDOYIN S O. An improved certificateless aggregate signature scheme without bilinear pairings for vehicular ad hoc networks[J]. Journal of Information Security and Applications, 2019, 44: 184-200.

[15] CUI J, ZHANG J, ZHONG H, et al. An efficient certificateless aggregate signature without pairings for vehicular ad hoc networks[J]. Information Sciences, 2018, 451: 1-15.

[16] JIA X, HE D, LIU Q, et al. An efficient provably-secure certificateless signature scheme for Internet-of-Things deployment[J]. Ad Hoc Networks, 2018, 71: 78-87.

[17] 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.