车载自组网中可证明安全的无证书认证方案

曾 萍[①] 郭瑞芳*[①②] 马英杰[①] 高 原[①] 赵 耿[①]

[①](北京电子科技学院 北京 100070)

[②](西安电子科技大学 西安 710000)

摘 要：认证协议的设计是目前车载自组网(VANET)安全领域的研究热点。现有的认证方案中普遍存在密钥托管带来的安全问题，以及使用计算量大的双线性对导致认证效率很低。针对以上问题，该文提出可证明安全的无证书批认证方案，方案中车辆的密钥由车辆自身和一个密钥生成中心共同生成，解决密钥需要托管给第三方维护的问题；方案的签名构造不使用计算量大的对运算，减少了计算开销；引入批认证来减少路边设施的认证负担，提高认证效率。基于求解椭圆曲线上的离散对数问题的困难性假设，在随机预言机模型中证明了该方案可以抵抗自适应选择消息和身份攻击，从而抵抗更改攻击和假冒攻击，并具有匿名性、可追踪性等特点。与现有方案相比，该方案实现了更高效的认证。

关键词：认证；无证书；批认证；可证明安全的；匿名性

中图分类号：TN918; TN393.08 **文献标识码**：A **文章编号**：1009-5896(2020)12-2873-09

DOI: 10.11999/JEIT190883

Provable Security Certificateless Authentication Scheme for Vehicular Ad hoc Network

ZENG Ping[①] GUO Ruifang[①②] MA Yingjie[①] GAO Yuan[①] ZHAO Geng[①]

[①](*Beijing Electronic Science&Technology Institute*, *Beijing* 100070, *China*)

[②](*Xidian University*, *Xi'an* 710000, *China*)

Abstract: The design of authentication protocol is a hot topic in the field of the security of Vehicular Ad hoc NETwork (VANET). There are security problems caused by key escrow in the existing authentication schemes. In order to solve this problem and achieve secure and efficient verification, an efficient pairing-free certificateless authentication scheme with batch verification is proposed, in which the key of the vehicle is generated by the vehicle itself and a key generation center, which solves the problem that the key needs to be managed to the third party for maintenance. The bilinear pairing operation, one of the most complex operations in modern cryptography, is not used in the generation of vehicle's signatures to reduce the computation cost of message verification. Unforgebility of the schemes against adaptively chosen-message and identity attack is proved under the difficulty of computing the discrete logarithm problem in the random oracle model to guarantee resistancy against modification and impersonation attacks, and has the characteristics of anonymity and traceability. Compared to the existing schemes, the proposed scheme is more efficient.

Key words: Authentication; Certificateless; Batch verification; Provable security; Anonymity

1 引言

在车载自组网(Vehicular Ad hoc NETwork, VANET)中，车载单元需定期广播基于位置的交通信息，从而为驾驶者提供安全的驾乘环境[1]。然而，由于车辆节点的高速移动性，VANET网络在受到攻击后不能立即检测出来，驾驶者面临很大的安全风险[2–4]。因此，在车辆进入网络之前对车辆身份的合法性和入网后广播消息的真实性进行认证来防止非法攻击显得尤为重要。基于身份的认证技术由于既能减少在基于PKI的认证方案和基于匿名证书的认证过程中产生的证书开销[5,6]，又能结合签名技术实现安全性的优点，从而得到了广泛的应用[7–9]。

2012年，Shim[10]提出了一种VANETs中的认证方案，方案实现了有条件的隐私保护。但该方案需要使用私钥生成器(PKG)来生成用户的私钥，如

收稿日期：2019-11-04；改回日期：2020-10-19；网络出版：2020-10-23

*通信作者： 郭瑞芳 fang_wankai@163.com

基金项目：国家自然科学基金(61772047)

Foundation Item: The National Natural Science Fouundation of China (61772047)

果PKG被攻击，则会造成密钥泄露。文献[11]设计了一种适用于VANET的分布式条件隐私保护认证协议，并证明了该协议在随机预言模型中是安全的。

为了满足车载网中的低时延通信要求，文献[12]提出了基于身份的聚合签名认证方案，该方案支持分层聚合和批验证，大大减少了车辆和其他实体的传输与存储开销，从而提高了认证效率。文献[13]提出基于多可信授权和一次性身份的聚合签名技术的认证协议，降低了认证时间。并且，在该方案中如果车辆被攻击，只对同一路边单元覆盖范围内的车辆有影响。文献[14]和文献[15]分别通过在批认证过程中引入安全系数和在签名密钥的生成过程中引入椭圆曲线上点的x坐标来抵抗批认证过程中可能存在的安全风险。上述认证方案大都基于椭圆曲线上的计算量很大的双线性对，针对该问题，文献[16]提出了一个不使用双线性对的认证方案，减少了计算开销。

传统基于身份的认证方案中主要由一个可信第三方生成车辆的密钥，从而普遍存在需要密钥托管的问题，而在无证书的密码体制中，密钥生成中心(Key Generation Center, KGC)只生成与用户身份相关的部分私钥，用户选取一部分秘密信息，与部分私钥结合一起生成私钥，同时解决密钥托管和证书管理问题。因此，无证书认证方案越来越受到关注[17,18]。Karati等人[19]提出了一种适用于工业物联网环境的轻量级无证书签名方案，但Zhang等人[20]指出该方案是不安全的，并且方案的安全证明是不正确的。文献[21]中提出一种强不可伪造的安全无证书签名方案，并证明了该方案在抗哈希碰撞问题和计算Diffle-Hellman困难问题假设下是安全不可伪造的。2020年，谢永等人[22]提出了一种可证安全的车联网无证书聚合签名改进方案，但该方案没有考虑聚合签名认证过程中一个错误消息导致整个聚合签名认证不通过，从而丢弃整个聚合消息集的情况，这些消息集中通常包含很多有效的、重要的与交通相关消息。

在上述研究的基础上，本文提出了一个可证明安全的VANET中无证书批认证方案。方案不使用计算量大的双线性对，减少了计算开销；车辆的真实身份被秘密保存，使用假名通信，并由路边设施生成假身份进一步实现通信的匿名性；在认证阶段，方案引入了批认证来确保认证的及时性。在随机预言机模型中证明方案的安全性，并对方案的性能进行分析。

2 无证书批认证协议设计

2.1 系统模型

方案的系统模型如图1所示，下面对这4个实体做简要介绍。

(1) TA (Trusted Authority)：假设TA完全可信且永远不被破坏。它存储着所有车辆及RSU的身份信息，以及一个身份撤销列表。

(2) KGC (Key Generation Center)：主要用于生成与车辆身份有关的部分私钥。假设TA和KGC永远不会串谋。

(3) RSU (RoadSide Unit)：路边单元是指安装在车道旁边或车道上方的通信及计算机设备，通过无线信道与车载单元连接，完成实时高速通信。

(4) OBU (On-Board Unit)：负责广播与交通相关的信息、位置标识和驾驶状态等，获得VANET提供的服务。

2.2 协议设计

本文设计的认证协议主要包括Setup, Partial KeyExtract, UserKeyGen, PseudoIdentityGen, Sign和Verify 6个算法。具体描述如下。

2.2.1 系统建立算法(Setup)

(1) 系统初始化：

(a) TA选择阶为q的循环群G, P为G的一个生成元。选取有限域F_q上的椭圆曲线$E_q(a,b):y^2\equiv x^3+ax+b(\bmod q)$，其中$x,y\in[0,q-1],4a^3+27b^2(\bmod q)\neq 0$

(b) TA选择一个随机数$s\in Z_q^*$作为系统主密钥，计算公钥$P_T=sP$；KGC选择一个随机数$s_1\in Z_q^*$作为它的私钥，计算公钥$P_K=s_1P$。

TA和KGC随机选取5个哈希函数$h:G\to Z_q^*$, $h_1:\{0,1\}^*\to Z_q^*$, $h_2:\{0,1\}^*\times G\times G\to Z_q^*$, $h_3,h_4:\{0,1\}^*\times G$，$h_3,h_4:\{0,1\}^*\times G\times\{0,1\}^*\times\{0,1\}^*\to Z_q^*$。

TA和KGC公布系统参数{P, G, q, h_1, h_2, h_3, h_4, P_T, P_K}，并秘密保存s,s_1。

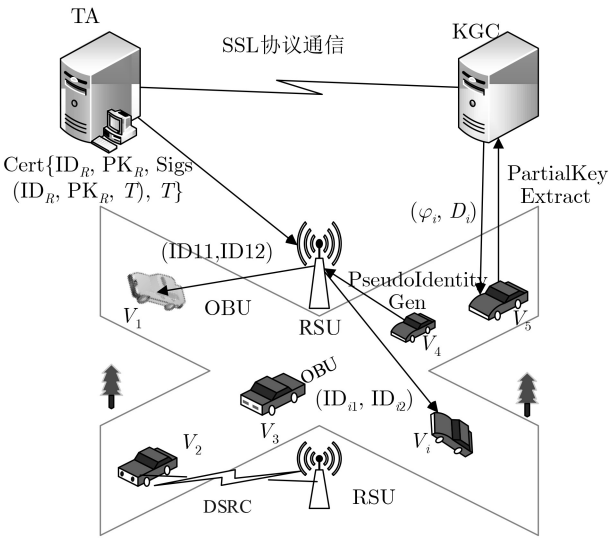

图 1 VANET系统通信模型

(2) RSU初始化：对于每一个RSU, TA随机选择$k_r \in Z_q^*$作为RSU的私钥，计算$\mathrm{PK}_r = k_r P$作为RSU的公钥。然后，随机选取$h \in Z_q^*$，计算$\mathrm{Sig}_r = k_r + \mathrm{sh}(\mathrm{ID}_r||\mathrm{PK}_r||T)$作为RSU的签名。

(3) 车辆初始化：当车辆V_i第1次注册时，TA为每辆车分发1个真实身份RID和1个用于激活防篡改设施的密码PWD，为了保护车辆的身份隐私，TA计算$Q_i = h_i(\mathrm{RID}_i)$，以$\mathrm{AID}_i = (Q_i, \mathrm{RID}_i \oplus h(\beta P_T))$作为车辆$V_i$的匿名身份进行后续通信，当且仅当TA可以根据$Q_i$知道车辆的真实身份。并将$\{\mathrm{PWD}, \mathrm{AID}_i, \mathrm{Sig}_s(\mathrm{AID}_i||\beta P)\}$预先装载到车辆的防篡改设备中。

2.2.2 部分私钥提取算法(PartialKeyExtract)

该算法由KGC运行。当车辆V_i请求生成部分公钥时，KGC首先检查该车辆是否在撤销列表(由TA通过安全信道传递给KGC)中，如果在，则阻止该车辆的进一步通信；否则，KGC随机选取$d_i \in Z_q^*$，计算$D_i = d_i P$, $\varphi_i = d_i + s_1 h_2(Q_i||D_i||P_K) \bmod q$，并将$(\varphi_i, D_i)$通过安全信道传给$V_i$。$V_i$可以通过$\varphi_i P = D_i + P_K h_2(Q_i||D_i||P_K)$来验证KGC生成的部分私钥的合法性。

2.2.3 用户密钥生成算法(UserKeyGen)

该算法由车辆运行。车辆V_i随机选取$x_i \in Z_q^*$作为秘密值，计算$X_i = x_i P$，则V_i的公钥为$\mathrm{PK}_i = (X_i, D_i)$，私钥为$\mathrm{SK}_i = (x_i, \varphi_i)$。

2.2.4 假身份生成算法(PseudoIdentityGen)

当V_i第1次进入RSU覆盖的区域时，V_i检查RSU的证书是否到期，并用TA的公钥检查签名的可靠性。如果T未到期，且签名的确是TA的，则V_i将$\{\mathrm{AID}_i, \mathrm{Sig}_s(\mathrm{AID}_i||\beta P)\}$发给RSU，并请求生成假身份。

RSU收到请求后，首先检查该车辆V_i是否在撤销列表(撤销列表由TA通过安全信道传递给RSU)中，如果在，则拒绝该请求，并广播通知网络中其他实体该车辆已被撤销；否则，RSU用TA的公钥检查签名的可靠性，如果签名可靠，RSU使用AID_i，随机选取$r_i \in Z_q^*$，生成假身份$\mathrm{ID}_i = (\mathrm{ID}_{i1}, \mathrm{ID}_{i2}, T_i)$，其中，$\mathrm{ID}_{i2} = \mathrm{RID}_i \oplus h(\beta P_T) \oplus h(R_t r_i P_T)$，其中$T_i$为假名身份的有效周期，在$T_i$过期前，车辆需进行假名身份的更新，以防止攻击者连续跟踪同一假名而链接到车辆真实身份。

2.2.5 签名生成算法(Sign)

给定消息$M_i = (m_i, T_i)$，V_i选择随机数$w_i = Z_q^*$，计算$W_i = w_i P$, $h_{3i} = h_3(\mathrm{ID}_i||D_i||X_i||T_i)$, $h_{4i} = h_4(\mathrm{ID}_i||M_i||W_i||X_i||T_i)$，生成签名$\sigma_i = h_{4i}(h_{3i}x_i + w_i) + \varphi \bmod q$。

因此，车辆V_i在消息M_i上的签名为(σ_i, W_i)，其中T_i是一个消息时戳用来防止重放攻击。

2.2.6 签名验证算法(Verify)

该算法由RSU运行，来确保车辆广播消息的可靠性。当有大量消息同时聚集在同一RSU处时，引入批认证来提高认证效率，减少认证时延。

(1) 单一验证：RSU收到车辆的消息后，依次执行以下步骤；

(a) RSU根据$T_R - T_i \le \Delta T$判断消息的新鲜性，其中，T_R为RSU接收到消息的时刻，T_i为车辆发送消息的时刻，ΔT为系统可容忍的最大时延。如果上式成立执行下一步；否则，RSU拒绝该消息。

(b) RSU通过检查下式是否成立来验证签名可靠性。

$$\sigma_i P = h_{4i}(h_{3i}X_i + W_i) + D_i + P_K h_{1i} \tag{1}$$

正确性证明如下：

$$\begin{aligned}\sigma_i P &= h_{4i}(h_{3i}x_i + w_i)P + \varphi_i P \\ &= h_{4i}(h_{3i}X_i + W_i) + (d_i + h_{1i}s_1)P \\ &= h_{4i}(h_{3i}X_i + W_i) + D_i + h_{1i}P_K。\end{aligned}$$ 证毕

若式(1)成立，RSU接收该消息，否则，拒绝该消息。

(2) 批认证：当RSU在同一时刻收到车辆广播的n条不同的消息$(m_i||t_i)_{1\sim n}$时，RSU依次执行以下步骤：

(a) 根据时戳$(t_i)_{1\sim n}$判断消息的时效性。如果消息新鲜，执行下一步；否则，RSU拒绝该消息。

(b) 为防止敌手攻击批量求和，RSU随机选取小向量[14]$\boldsymbol{a} = (a_1, a_2, \cdots, a_n), a_i \in [1, 2^t]$，验证式(2)是否成立

$$\begin{aligned}\left(\sum_{i=1}^{n} a_i\sigma_i\right)P = &\sum_{i=1}^{n} a_i(D_i + P_K h_{1i}) \\ &+ \sum_{i=1}^{n} a_i h_{4i}(h_{3i}X_i + W_i)\end{aligned} \tag{2}$$

正确性证明如下：

$$\begin{aligned}&\left(\sum_{i=1}^{n} a_i\sigma_i\right)P \\ &= \left(\sum_{i=1}^{n} a_i(h_{4i}(h_{3i}x_i + w_i) + \varphi_i)\right)P \\ &= \left(\sum_{i=1}^{n} a_i(h_{4i}(h_{3i}x_i + w_i) + d_i + s_1 h_{1i})\right)P \\ &= \sum_{i=1}^{n} a_i(D_i + P_K h_{1i}) + \sum_{i=1}^{n} a_i h_{4i}(h_{3i}x_i + W_i)。\end{aligned}$$

证毕

若式(2)成立，RSU接收该消息，否则，拒绝该消息。

如果式(2)成立，表明这批消息是有效的，并且消息发送者的身份是合法的。否则，说明这次认证的消息中至少存在1个虚假消息。此时，如果将该批消息都丢弃，不仅导致认证效率低下，还会丢弃一些重要的合法消息。因此，本文采用二分查找算法结合批认证来快速找出不合法的消息，并将这些不合法消息拥有者的假名存入列表InvalidList。具体算法实现如表1所示。

根据上述算法，RSU最终输出m个广播虚假消息的车辆假名列表 InvalidList=$\{\mathrm{ID}_1, \mathrm{ID}_2, \cdots, \mathrm{ID}_m\}$，其中，$1 \le m \le n$。RSU从该批消息对应的初始假名集合中减去InvalidList列表中的假名，就能得到广播合法消息的车辆假名列表ValidList。RSU接受这些ValidList中存在的合法车辆广播的消息，并将InvalidList列表通过安全通道传给TA，TA根据这些假名身份检索出车辆的真实身份，并将其放入身份撤销列表。

当车辆V_j想要对周围车辆的广播消息进行有效性认证时，(1)首先，车辆V_j用RSU的公钥检查$\mathrm{Sig}_{\mathrm{sr}}$(InvalidList)是否由RSU发送的，如果是，进行步骤(2)，否则，采用批认证算法进行检测；(2)车辆V_j从周围车辆的所有的假名列表集合里减去RSU广播的InvalidList中存在的假名，得到合法车辆的假名列表ValidList；接着采用批认证算法验证这些合法车辆发送的消息是否满足式(2)，如果不满足，该车辆运行无效消息查找算法找出不合法车辆的假名身份，并将该结果反馈给TA, TA检查RSU的可靠性，并将不合法车辆的真实身份放入身份撤销列表；否则，该车辆接受RSU的认证结果，拒绝与假名身份存在于InvalidList中的车辆建立通信。

表 1 批认证过程中无效消息查找算法(二分查找算法)

输入：List=$\{\mathrm{ID}_i, M_i, W_i, \sigma_i, T_i\}$

输出：InvalidList=$\{\mathrm{ID}_1, \mathrm{ID}_2, \cdots, \mathrm{ID}_m\}$

```
(1) Function
(2) batch And Search(List, InvalidList, Index, low, high)
(3)   /*Function batchAuth(List, low, high)表示对消息数组下
      标Index属于[low, high]的消息进行式(2)所述批认证，成功
      则返回true，失败则返回false*/
(4)   if (batchAuth(List, Index Low, high)) then
(5) return true
(6) else if (low==high)
(7)     Invalid List.append(List[low])
(8)     return Invalid List
(9)     else
(10)        mid=(low+high)/2
(11)        batch And Search(List, InvalidList, Index, low, mid)
(12)        batch And Search(List, InvalidList, Index, mid+1,
            high)
(13)    end if
(14)    return InvalidList
(15)  end if
(16)  end Function
(17)  for i:=1 to n do
(18)    batch And Search(List, InvalidList, i, 1, n)19: end for
```

3 安全性证明与分析

3.1 安全性证明

定义1：离散对数问题(Discrete Logarithm Problem, DLP)：假设G是由P生成的阶数为q的循环加法群，q为一个大素数，给定$P, aP \in G(a \in Z_q^*$是未知的随机数)，计算出a的概率在多项式时间内是可以忽略的。

定理1(不可伪造性)：如果不存在任何多项式界的敌手能以一个不可忽略的概率优势赢得以下两个游戏，则称该无证书消息认证方案在自适应选择消息和身份下是存在性不可伪造的，定理1的证明由引理1和引理2推出。游戏如下：

Game1(针对类型I敌手A1的游戏)：

系统初始化阶段：挑战者B运行Setup算法生成系统参数params和主密钥s，将params发送给敌手A，并将s秘密保存。

敌手A适应性地执行下面的一系列预言机询问：

(1) Hash Query: A可在任意时刻向方案中用到的所有Hash值发起Hash预言机询问，挑战者B返回相应的哈希值。

(2) Extract-Partial-Key (ID_i)：当A需要得到用户ID_i的部分私钥时，向挑战者B发送请求，B运行方案中定义的部分密钥提取算法，生成用户ID_i的部分私钥，返回给A。

(3) Request Public Key (ID_i)：当B收到A对ID_i的公钥询问时，B运行UserKeyGen算法生成ID_i的公钥PK_i，并将其返回给A。

(4) Request Secret Value (ID_i)：当A询问ID_i的秘密值时，B运行UserKeyGen算法并将生成的秘密值x_i返回给A。如果ID_i的公钥PK_i已被替换，B返回$\perp$。

(5) Replace Public Key ($\mathrm{ID}_i, \mathrm{PK}_i'$)：由于无证书公钥密码系统中没有提供公钥的认证，攻击者A可以以选取的公钥PK_i'替换ID_i'的原有公钥PK_i而不被发觉。

(6) Request Signing (ID_i, M_i): A可以向B询问

身份ID_i关于任意消息M的签名，挑战者B运行Sign算法生成相应的签名并返还给A。

最后，A生成$(M^*, \mathrm{ID}^*, \sigma^*)$，其中，$\sigma^*$为用户$\mathrm{ID}_i$在消息$M_i^*$上的签名。如果满足下面的条件则A在游戏中获胜。

(a) Verify $(\mathrm{params}, \mathrm{ID}^*, \sigma^*)$=1；

(b) ID^* 从来都没有提交给Extract-Partial-Key询问且(M^*, σ^*)从来都没有提交给RequestSigning询问。

Game2(针对类型II敌手A2的游戏)：

系统初始化阶段：挑战者B运行Setup算法生成系统参数params和主密钥s，将params和s发送给敌手A。

A2可以适应性的执行多项式数量级界的与Game1中完全类似预言机询问，不同的是A2拥有系统主密钥且在询问阶段不再进行Replace Public Key询问和Extract-Partial-Key询问，这里不再赘述。

上述攻击者A1不具备获得系统主密钥的能力，且任何时候都不能够得到挑战目标的完整私钥；攻击者A2拥有系统的主密钥，可以提取用户的部分私钥，但是不能实施伪造用户公钥的攻击。

引理1：如果在随机预言机模型(RO)中存在一个类型I敌手A1，他能够在至多进行T_{PPK}次部分私钥提取查询、T_{PK}次公钥查询、$T_i(i=1\sim4)$次Hash查询以及T_{S}次签名查询后伪造一个合法的签名，则椭圆曲线上DLP问题将是可以解决的。

证明：给定$(P, Q=aP)$为群G上DLP问题的一个实例，其中$a\in Z_q^*, P\in G$。然后挑战者B与敌手A1进行交互，在交互过程中，视所有哈希函数为随机预言机，B的目标是求出a。以下步骤分别为B利用A1求出a的过程。

(1) 系统初始化阶段：B运行Setup算法，生成系统参数params并令$P_K=aP$，然后将params发送给A1, B随机选取ID_I作为这次游戏的挑战身份，A执行以下询问。

(2) 询问阶段：在此阶段A1适应性地进行多项式数量级界的以下预言机询问。为避免冲突，B在此过程中维护以下6个列表$L_i(i=1\sim4)$, L_{PSK}, L_{PK}，列表起初全部为空。

h_1询问：B维护一个h_1列表$L_1=\{(Q_k, \mathrm{ID}_k)\}$。当A对$\mathrm{ID}_i$进行$h_1$询问时，B首先查看列表$L_1$，如果$\mathrm{ID}_i$已被执行$\mathrm{h}_1$询问，直接返回$Q_i$；否则，B随机选择$Q_i\in Z_q^*$，然后将$(Q_i, \mathrm{ID}_i)$添加到列表$L_1$，返回$Q_i$给A1。

h_2询问：B维护一个h_2列表$L_2=\{(Q_k, D_k, P_k, h_{2k})\}$，每当B收到一个$h_2$询问时，B首先查看$h_2$列表，如果有相关查询记录则直接返回相应$h_{2i}$；否则，B选择随机数$h_{2i}\in Z_q^*$，令$h_{2i}=h_2(Q_i, D_i, P_K)$，返回$h_{2i}$给A，并将$(Q_i, D_i, P_K, h_{2i})$添加到列表$L_2$中。

h_3询问：B维护一个h_3列表$L_3=\{(\mathrm{ID}_k, D_k, X_k, T_k, h_{3k})\}$。当A1进行$h_3$询问时，B先查看$L_3$列表，如果有相关查询记录则B直接返回$h_{3i}$；否则，B选择一个随机数$h_{3i}\in Z_q^*$，令$h_{3i}=(\mathrm{ID}_i, D_i, X_i, T_i)$，并将$h_{3i}$返回给A1，然后将$(\mathrm{ID}_i, D_i, X_i, T_i, h_{3i})$ 添加到L_3中。

h_4询问：B维护一个h_4列表$L_4=\{(\mathrm{ID}_k, M_k, W_k, X_k, T_k, h_{4k})\}$。当A1进行$h_4$询问时，B先查看$L_4$列表中是否已经存在记录$(\mathrm{ID}_i, M_i, W_i, X_i, T_i)$，如果存在，则B直接返回$h_{4i}$；否则，B选择一个随机数$h_{4i}\in Z_q^*$，令$h_{4i}=(\mathrm{ID}_i, M_i, W_i, X_i, T_i)$，并将$h_{4i}$返回给A1，然后将$(\mathrm{ID}_i, M_i, W_i, X_i, T_i, H_{4i})$添加到$L_4$中。

Extract-Partial-Private-Key(ID_i)询问：当A1发出部分私钥提取询问时，B首先检索L_{PSK}列表，如果在L_{PSK}列表中已经存在元组$(\mathrm{ID}_i, \varphi_i, D_i)$，则返回$\varphi_i$给A1；否则，如果$\mathrm{ID}_i\neq\mathrm{ID}_I$, B随机选取$a_i\in Z_q^*$，令$\varphi_i=a_i$，将$(\mathrm{ID}_i, \varphi_i, D_i)$插入到列表$L_{\mathrm{PSK}}$中，并返回$\varphi_i$给A1。如果$\mathrm{ID}_i=\mathrm{ID}_I$, B放弃并终止询问。

RequestPublicKey(ID_i): B维护一个包含元组$(\mathrm{ID}_k, x_k, X_k)$的$L_{\mathrm{PK}}$列表。当B收到一个关于$\mathrm{ID}_i$的公钥询问时，如果$(\mathrm{ID}_i, x_i, X_i)$已经存在于$L_{\mathrm{PK}}$列表，B直接返回$X_i$；否则，B执行如下操作：

(a) 如果$\mathrm{ID}_i\neq\mathrm{ID}_I$, B随机选取$a_i, b_i, x_i\in Z_q^*$，令 $X_i=x_iP$ ， $D_i=a_iP-b_iP_K$ ， $h_2(Q_1||D_i||P_K)=b_i$，返回X_i给A1，并将(Q_i, D_i, P_K, b_i)和$(\mathrm{ID}_i, x_i, X_i)$分别添加到$L_2$列表和$L_{\mathrm{PK}}$列表中。

(b) 如果$\mathrm{ID}_i=\mathrm{ID}_I$, B随机选取$a_i, b_i, x_i\in Z_q^*$，令$X_i=x_iP$, $D_i=a_iP$, $h_2(Q_1||D_i||P_K)=b_i$，返回X_i给A1，并将(Q_i, D_i, P_k)和$(\mathrm{ID}_i, x_i, X_i)$分别添加到$L_2$列表和$L_{\mathrm{PK}}$列表中。

RequestSecretValue(ID_i)：当A1对ID_i进行秘密值询问时，如果$\mathrm{ID}_i=\mathrm{ID}_I$, B放弃并终止；否则，B查找列表$L_{\mathrm{PK}}$，如果存在记录$(\mathrm{ID}_i, x_i, X_i)$，B返回$x_i$；如果不存在，B执行公钥查询生成元组$(x_i, X_i)$，返回$x_i$给A1并将$(x_i, X_i)$添加到$L_{\mathrm{PK}}$列表中。

ReplacePublicKey$(\mathrm{ID}_i, \mathrm{PK}_i')$：当A1对$\mathrm{ID}_i$进行公钥替换询问时，B首先从$L_{\mathrm{PK}}$中找到相应的记录$(\mathrm{ID}_i, x_i, X_i)$(如果不存在，对$\mathrm{ID}_i$进行公钥查询)，将$X_i$替换成A自由选取的$X_i'$，并令$x_i=\perp$。

Request Signing(ID_i, M_i)：当A1对(ID_i, M_i)进行签名询问时，B首先进行h_1, h_2, h_3, h_4请求，分

别从列表L_1, L_2, L_3, L_4, L_{PSK}, L_{PK}中恢复Q_i和元组$(Q_i, D_i, P_K, h_2 i)$, $(\mathrm{ID}_i, D_i, X_i, h_3 i)$, $(\mathrm{ID}_i, M_i, W_i, X_i, T_i, h_4 i)$, $(\mathrm{ID}_i, \varphi_i, D_i)$, $(\mathrm{ID}_i, x_i, X_i)$。然后，B随机选取$\sigma_i \in Z_q^*$，令$W_i = g_i^{-1}(\sigma_i P - D_i - P_K h_{2i}) - h_{3i} X_i$。

因为$\sigma_i P = g_i(W_i + h_{3i} X_i) + D_i + P_K h_{2i}$成立，故上述签名$\sigma_i$是一个有效的签名。

伪造：最后，A1输出伪造的签名$(\mathrm{ID}^*, M^*, \sigma^*, W^*)$。这里$\mathrm{ID}^*$未曾既提交给Extract-Partial-Private-Key预言机，又同时提交给RequestSecret-Value预言机；(ID^*, M^*) 也没有被用以进行签名询问过。如果$\mathrm{ID} \neq \mathrm{ID}^*$，则B失败。否则，B查找$L_{\mathrm{PSK}}$和$L_{\mathrm{PK}}$列表，利用分叉引理，在多项式时间内可以得到两组有效签名$(\mathrm{ID}_I, M_i, \sigma_i, W_i)$和$(\mathrm{ID}_I, M_i, \sigma_{i^*}, W_i)$，其中$\sigma_i = h_{4i}(h_{3i} x_i + w_i) + \varphi_i \bmod q$ 和 $\sigma_i{}^* = h_{4i}{}^*(h_{3i} x_i + w_i) + \varphi_i \bmod q$，且$g_i \neq g_i{}^*$。根据$X_i = x_i P$, $P_K = s_1 P = aP$, $D_i = a_i P$, B可以成功地通过以下计算从这两个合法签名中计算出a。因为$W_i = h_{4i}{}^{-1}(\sigma_i P - D_i - P_K h_{2i}) - h_{3i} X_i$, $W_i = (h_{4i}{}^{-1})^*(\sigma_i{}^* P - D_i - P_K h_{2i}) - h_{3i} X_i$。

令$h_{4i}{}^{-1} = b$，可以得到，$a = h_{2i}^{-1}(b^* \sigma_i^* - b\sigma_i)/(b^* - b) - h_{2i}^{-1} a_i$，即B解出了DLP的一个实例$a$。证毕

引理2：如果在随机预言机模型(RO)中存在一个类型II敌手A2，他能够在至多进行T_{PPK}次部分私钥提取查询、T_{PK}次公钥查询、$T_i(i=2\sim4)$次Hash查询以及T_{S}次签名查询后伪造一个合法的签名，则椭圆曲线上DLP问题将是可以解决的。

证明：给定$(P, Q = \alpha P)$为群G上DLP问题的一个实例，B的目标是求出α。

系统初始化阶段：B运行Setup算法，生成系统参数params，令$P_K = s_1 P$, B随机选取ID_I作为这次游戏的挑战身份，然后B将params和s_1发送给A2, A2执行以下询问。

询问阶段：B在此过程维护4个列表L_2, L_3, L_4, L_{PK}，列表起初全部为空。除公钥提取询问和签名询问外，其他同定理1，这里不再赘述。

RequestPublicKey(ID_i)：B维护一个包含元组$(\mathrm{ID}_k, x_k, X_k)$的$L_{\mathrm{PK}}$列表。当B收到一个关于$\mathrm{ID}_i$的公钥询问时，如果$(\mathrm{ID}_i, x_i, X_i)$已经存在于$L_{\mathrm{PK}}$列表，B直接返回$X_i$；否则，B执行如下操作：

(1) 如果$\mathrm{ID}_i \neq \mathrm{ID}_I$, B随机选取$d_i, x_i \in Z_q^*$，令$X_i = x_i P$, $D_i = d_i P$, $h_2(Q_i || D_i || P_K) = h_{2i}$，返回$X_i$给A2，并将$(Q_i, D_i, P_k, h_{2i})$ 和$(\mathrm{ID}_i, x_i, X_i)$分别添加到$L_2$列表和$L_{\mathrm{PK}}$列表中。

(2) 如果$\mathrm{ID}_i = \mathrm{ID}_I$, B随机选取$d_i \in Z_q^*$，令$D_i = d_i P$, $h_2(Q_i || D_i || P_K) = h_{2i}$, $X_i = Q = \alpha P$，返回X_i给A2，并将(Q_i, D_i, P_K, h_{2i})和$(\mathrm{ID}_i, \perp, X_i)$分别添加到$L_2$列表和$L_{\mathrm{PK}}$列表中。

RequestSigning(ID_i, M_i)：当B收到签名询问时，首先从列表 L_2, L_3, L_4, L_{PK}中恢复元组(Q_i, D_i, P_K, h_{2i})，$(\mathrm{ID}_i, D_i, X_i, T_i, h_{3i})$，$(\mathrm{ID}_i, M_i, W_i, X_i, T_i, h_{4i})$，$(\mathrm{ID}_i, x_i, X_i)$。

如果$\mathrm{ID}_i \neq \mathrm{ID}_I$，说明B知道$\mathrm{ID}_i$的完整私钥和秘密值，可以按正常方式完成签名。否则，B随机选取$\sigma_i \in Z_q^*$，令$X_i = \alpha P$，$W_i = \beta P = \sigma_i P - h_{3i} X_i - h_{4i}^{-1} \varphi_i P$，返回签名$(W_i, \sigma_i)$给A2。可以通过式(1)验证该签名是有效的。

伪造签名阶段与引理1类似，这里不再赘述，最后，B可以成功解出$\alpha = h_{3i}^{-1}(\sigma_i^* - \sigma_i)/(h_{4i}^* - h_{4i}) - h_{3i}^{-1}\beta$。则B解出了DLP的一个实例$\alpha$。然而这与定义1中求解椭圆曲线上的DLP的困难性假设矛盾，所以，上述两类攻击者成功伪造一个有效的签名的概率也是可以忽略的。由定理1知，本文所提出的方案在自适应选择消息和身份攻击下是存在性不可伪造的。 证毕

3.2 安全性分析

(1) 车辆的匿名通信：一方面，网络中车辆的真实身份仅有TA知道，并且车辆进入网络后都使用假身份(由TA生成)进行通信；另一方面，在每个RSU范围内，RSU都会为其生成假名，攻击者要想通过假名检索出车辆的真实身份，可以通过计算$\mathrm{RID} = \mathrm{ID}_{i2} \oplus h_0'(\beta P_T) \oplus h_1(R_t r_i P_T)$ 或$\mathrm{RID} = \mathrm{ID}_{i2} \oplus h_0'(\beta P_T) \oplus h_1(s\mathrm{ID}_{i1})$实现。但同时，攻击者需要从$\mathrm{ID}_{i1} = R_t r_i P$中解出$r_i$和从$P_T = sP$中解出$s$，由DLP的困难性假设知，这个概率是可以忽略的。因此，方案实现了车辆的身份隐私保护。

(2)可追溯性和可撤销性：已知假身份$\mathrm{ID}_i = (\mathrm{ID}_{i1}, \mathrm{ID}_{i2})$，只有TA可以通过(RID, s)检索出车辆的真实身份：$\mathrm{ID}_{i2} \oplus h_{1'}(\beta P_T) \oplus h_{2'}(s\mathrm{ID}_{i1}) = \mathrm{RID} \oplus h_{2'}(R_t r_i P_T) \oplus h_{1'}(\beta P_T) \oplus h_{1'}(\beta P_T) \oplus h_{2'}(s\mathrm{ID}_{i1}) = \mathrm{RID}$。

本文中，TA维护并实时更新一个车辆的身份撤销列表，当车辆发送虚假消息时，TA可以通过上式计算出车辆的真实身份，并将其存入该身份撤销列表中。TA通过一个安全通道将存放非法车辆的身份撤销列表传给RSU，即使一个被撤销身份的车辆可以向RSU发出假名身份生成请求，RSU可以通过检索该身份撤销列表并拒绝该请求。

可见，方案在实现身份隐私保护的同时，又能实现可追溯性，即当车辆发送错误消息误导网络中其他实体时，TA可以根据该车辆发送的消息中携带的身份标识追溯出车辆的真实身份，并将该身份放入

身份撤销列表中，阻断该车辆在网络中的进一步通信。因此，方案实现了有条件的隐私保护，即只保护合法车辆的隐私，而对不法车辆的隐私进行披露。

(3) 抵抗假冒攻击：方案中每条消息$(\mathrm{ID}_i, M_i, \sigma_i, W_i, T_i)$都包含一个车辆的签名$\sigma_i$，如果攻击者想要假冒一个合法车辆的身份去发送消息，它需要在该消息里附上签名。由定理1知，攻击者不可能通过伪造出一个合法车辆的身份或假冒其他车辆的身份生成一个有效的签名，每个车辆生成的签名都应该验证是否满足式(1)和式(2)，如果不能通过验证，则生成的签名无效，发送的消息也就无效。因此，该方案可以抵抗假冒攻击。

(4) 抵抗重放攻击：σ_i是车辆V_i在消息M_i上的签名，根据定理1可知，方案中实体生成的签名具有不可伪造性，而车辆发送的每条消息$(\mathrm{ID}_i, M_i, \sigma_i, W_i, T_i)$中都会附有该车辆对消息的签名$\sigma_i$，任何关于消息$(\mathrm{ID}_i, M_i, \sigma_i, W_i, T_i)$的更改都可以看作是更改了签名$\sigma_i$，与定理1中证明的方案满足签名的不可伪造性矛盾；并且，任何消息的签名可以通过验证式(1)和式(2)是否成立来检测。如果签名没有通过认证，说明签名不合法，即使是同一条消息M_i，不同的签名也会导致发送的消息$(\mathrm{ID}_i, M_i, \sigma_i, W_i, T_i)$不同。因此，该方案可以抵抗更改攻击。

(5) 抵抗重放攻击：为了保证消息的时效性，RSU在收到车辆发送的消息后，首先检查消息的新鲜性。令T_R表示RSU接收到消息的时间，T_i表示车辆V_i发送消息的时间戳，ΔT 为系统可容忍的网络延迟。如果满足$T_R - T_i \le \Delta T$，那么RSU接收此消息，否则说明该消息过期，拒绝此消息。

4　性能仿真与分析

本节从计算开销和通信开销两个方面对提出的方案与以往的方案[12,15,17]进行分析和比较。

4.1　计算开销

本文仿真环境为WIN10 64 bit，硬件环境为Intel CORE i5 2.3 GHz。本文所提出的认证方案是基于miracl仿真库开发的，在miracl库当中循环群G上的元素占据32 Byte的空间，而经过双线性变换后的群(G_1)的元素占用64 Byte的空间。所涉及的密码运算及运行时间如下：

T_{par}=4.2110 ms(双线性对运算)，$T_{\mathrm{mul}\text{-}G}$=0.4420 ms($G$上的标量点乘)，$T_{\mathrm{exp}}$=0.0050 ms(模乘)，$\mathrm{T}_{\mathrm{mul}\text{-}G1}$=1.7090 ms($G_1$上标量点乘)，$T_{\mathrm{mtp}}$=4.4060 ms (MapToPoint哈希)，$T_{\mathrm{pa}\text{-}G1}$=0.0071 ms ($G_1$上点加)，$T_{\mathrm{pa}\text{-}G}$=0.0018 ms($G$上点加)，$T_{\mathrm{h}}$=0.0001 ms(单向哈希)。不同方案的计算开销如表2所示。

虽然Zhang等人[12]的方案签名生成所需时间比本文少，但整个签名生成加认证的总开销却比本文的高很多。图2为4个方案的总开销仿真图。当n=3000时，本文的认证效率相比于Bayat等人[15]、Horng等人[17]和Zhang等人[12]的方案分别提升了82.64%, 88.66%和78.94%。图3为引入批认证后方案的认证开销仿真图，可以看出，本文的方案认证所需时间明显小于其他3个方案。

4.2　通信开销

为了进行比较，我们假设哈希输出的位长和时间戳T_i分别为20 Byte和4 Byte，整数域Z_q^*中的元素为20 Byte。如前一节所述，G_1和G中每个元素的大小分别为64×2=128 Byte和20×2=40 Byte。不同方案通信开销的比较如表3所示。可以看出，与其他3个方案相比，本文所提出的方案提供了较低的通信开销。虽然Zhang等人[12]的方案通信开销跟本文一致，但是以降低认证效率为代价的。

5　结束语

本文提出了一种VANET中不使用双线性对的无证书批认证方案，解决了传统认证方案中存在的密钥托管问题；方案在RO模型中可以抵抗自适应选择消息和身份攻击，并能实现匿名通信、有条件的隐私通信，可以抵抗假冒攻击、更改攻击和重放攻击等，满足VANET中的安全通信要求。分析表明，与其他3个认证方案相比，本文所提出的方案的认证效率最高提升了88.66%，且消息数目越大，性能提升越明显，故该方案适合于要求认证时延低、计算开销小和隐私保护的车载自组网环境中。

表 2　不同方案的计算开销(ms)

方案	签名生成	认证1条消息	认证n条消息
文献[15]	$5T_{\mathrm{mul}\text{-}G1}+1T_{\mathrm{pa}\text{-}G1}+1T_{\mathrm{mtp}}$=12.9581	$T_{\mathrm{mul}\text{-}G1}+3T_{\mathrm{exp}}+T_{\mathrm{mtp}}$=18.7480	$nT_{\mathrm{mul}\text{-}G1}+3T_{\mathrm{exp}}+nT_{\mathrm{mtp}}$=5.1120$n$+12.6117
文献[17]	$4T_{\mathrm{mul}\text{-}G1}+1T_{\mathrm{pa}\text{-}G1}+2T_{\mathrm{mtp}}+1T_{\mathrm{h}}$=15.6552	$2T_{\mathrm{par}}+2T_{\mathrm{mul}\text{-}G1}+1T_{\mathrm{pa}\text{-}G1}+1T_{\mathrm{mtp}}+1T_{\mathrm{h}}$=8.4273	$2T_{\mathrm{exp}}+2\mathrm{n}T_{\mathrm{mul}\text{-}G1}+nT_{\mathrm{pa}\text{-}G1}+\mathrm{n}T_{\mathrm{mtp}}+nT_{\mathrm{h}}$ =7.8312n+8.422
文献[12]	$5T_{\mathrm{exp}}+3T_{\mathrm{h}}$= 0.0253	$T_{\mathrm{exp}}+2T_{\mathrm{par}}+3T_{\mathrm{h}}$=8.4273	$(n+1)T_{\mathrm{par}}+nT_{\mathrm{exp}}+3nT_{\mathrm{h}}$=4.2163$n$+4.2110
本文	$4T_{\mathrm{mul}\text{-}G}+2T_{\mathrm{pa}\text{-}G}+3T_{\mathrm{h}}$=1.7666	$4T_{\mathrm{mul}\text{-}G}+3T_{\mathrm{pa}\text{-}G}+3T_{\mathrm{h}}$=1.7737	$(2n+2)T_{\mathrm{mul}\text{-}G}+3nT_{\mathrm{h}}+(2n+1)T_{\mathrm{pa}\text{-}G}$= 0.8879$n$+0.8858

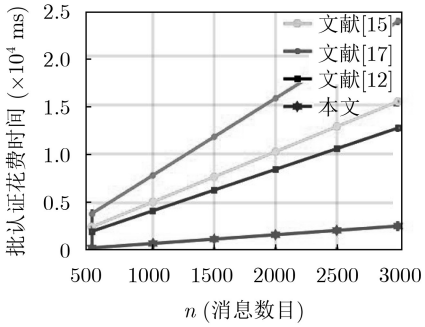

图 2 方案总的认证计算开销

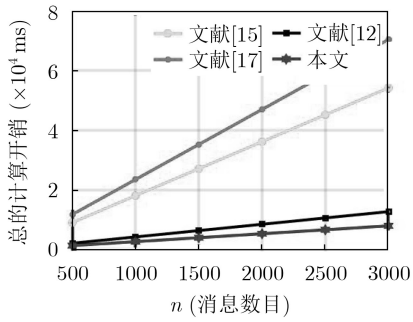

图 3 批认证时间开销

表 3 不同方案的通信开销(Byte)

方案	发送1条消息	发送n条消息
本文	144	144n
文献[17]	384	384n
文献[15]	388	388n
文献[12]	144	144n

参 考 文 献

[1] KENNEY J B. Dedicated short-range communications (DSRC) standards in the United States[J]. *Proceedings of the IEEE*, 2011, 99(7): 1162–1182. doi: 10.1109/jproc.2011.2132790.

[2] 张春花, 臧海娟, 薛小平, 等. 车联网轨迹隐私保护研究进展[J]. 计算机应用, 2017, 37(7): 1921–1925, 1942. doi: 10.11772/j.issn.1001-9081.2017.07.1921.
ZHANG Chunhua, ZANG Haijuan, XUE Xiaoping, *et al*. Research progress in internet of vehicles trajectory privacy protection[J]. *Journal of Computer Applications*, 2017, 37(7): 1921–1925, 1942. doi: 10.11772/j.issn.1001-9081.2017.07.1921.

[3] 李馥娟, 王群, 钱焕延. 车联网安全威胁综述[J]. 电子技术应用, 2017, 43(5): 29–33, 37.
LI Fujuan, WANG Qun, and QIAN Huanyan. Survey on security threats of Internet of vehicles[J]. *Application of Electronic Technique*, 2017, 43(5): 29–33, 37.

[4] QU Fengzhong, WU Zhihui, WANG Feiyue, *et al*. A security and privacy review of VANETs[J]. *IEEE Transactions on Intelligent Transportation Systems*, 2015, 16(6): 2985–2996. doi: 10.1109/tits.2015.2439292.

[5] LI Jie, LU Huang, and GUIZANI M. ACPN: A novel authentication framework with conditional privacy-preservation and non-repudiation for VANETs[J]. *IEEE Transactions on Parallel and Distributed Systems*, 2015, 26(4): 938–948. doi: 10.1109/tpds.2014.2308215.

[6] WANG Fei, XU Yongjun, ZHANG Hanwen, *et al*. 2FLIP: A two-factor lightweight privacy-preserving authentication scheme for VANET[J]. *IEEE Transactions on Vehicular Technology*, 2016, 65(2): 896–911. doi: 10.1109/tvt.2015.2402166.

[7] ZHONG Hong, WEN Jingyu, CUI Jie, *et al*. Efficient conditional privacy-preserving and authentication scheme for secure service provision in VANET[J]. *Tsinghua Science and Technology*, 2016, 21(6): 620–629. doi: 10.1109/tst.2016.7787005.

[8] HE Debiao, ZEADALLY S, XU Baowen, *et al*. An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks[J]. *IEEE Transactions on Information Forensics and Security*, 2015, 10(12): 2681–2691. doi: 10.1109/TIFS.2015.2473820.

[9] ZHANG Yaling, YANG Liang, and WANG Shangping. An efficient identity-based signature scheme for vehicular communications[C]. The 2015 11th International Conference on Computational Intelligence and Security, Shenzhen, China, 2015: 326–330. doi: 10.1109/cis.2015.86.

[10] SHIM K A. *CPAS*: An efficient conditional privacy-preserving authentication scheme for vehicular sensor networks[J]. *IEEE Transactions on Vehicular Technology*, 2012, 61(4): 1874–1883. doi: 10.1109/tvt.2012.2186992.

[11] SHAO Jun, LIN Xiaodong, LU Rongxing, *et al*. A threshold anonymous authentication protocol for VANETs[J]. *IEEE Transactions on Vehicular Technology*, 2016, 65(3): 1711–1720. doi: 10.1109/tvt.2015.2405853.

[12] ZHANG Lei, WU Qianhong, DOMINGO-FERRER J, *et al*. Distributed aggregate privacy-preserving authentication in VANETs[J]. *IEEE Transactions on Intelligent Transportation Systems*, 2017, 18(3): 516–526. doi: 10.1109/tits.2016.2579162.

[13] LIU Zhicai, XIONG Ling, PENG Tu, *et al*. A realistic distributed conditional privacy- preserving authentication scheme for vehicular ad hoc networks[J]. *IEEE Access*, 2018, 6: 26307–26317. doi: 10.1109/ACCESS.2018.2834224.

[14] CUI Jie, TAO Xuefei, ZHANG Jing, *et al*. HCPA-GKA: A hash function-based conditional privacy-preserving authentication and group-key agreement scheme for VANETs[J]. *Vehicular Communications*, 2018, 14: 15–25. doi: 10.1016/j.vehcom.2018.09.003.

[15] BAYAT M, BARMSHOORY M, RAHIMI M, *et al*. A secure authentication scheme for VANETs with batch verification[J]. *Wireless Networks*, 2015, 21(5): 1733–1743. doi: 10.1007/s11276-014-0881-0.

[16] LO N W and TSAI J L. An efficient conditional privacy-preserving authentication scheme for vehicular sensor networks without pairings[J]. *IEEE Transactions on Intelligent Transportation Systems*, 2016, 17(5): 1319–1328. doi: 10.1109/tits.2015.2502322.

[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. doi: 10.1016/j.ins.2015.04.033.

[18] GAYATHRI N B, THUMBUR G, REDDY P V, *et al*. Efficient pairing-free certificateless authentication scheme with batch verification for vehicular ad-hoc networks[J]. *IEEE Access*, 2018, 6: 31808–31819. doi: 10.1109/ACCESS.2018.2845464.

[19] KARATI A, ISLAM S H, and KARUPPIAH M. Provably secure and lightweight certificateless signature scheme for IIoT environments[J]. *IEEE Transactions on Industrial Informatics*, 2018, 14(8): 3701–3711. doi: 10.1109/tii.2018.2794991.

[20] ZHANG Bo, ZHU Tianqing, HU Chengyu, *et al*. Cryptanalysis of a lightweight certificateless signature scheme for IIOT environments[J]. *IEEE Access*, 2018, 6: 73885–73894. doi: 10.1109/access.2018.2883581.

[21] 吴涛, 景晓军. 一种强不可伪造无证书签名方案的密码学分析与改进[J]. 电子学报, 2018, 46(3): 602–606. doi: 10.3969/j.issn.0372-2112.2018.03.013.

WU Tao and JING Xiaojun. Cryptanalysis and improvement of a certificateless signature scheme with strong unforgeability[J]. *Acta Electronica Sinica*, 2018, 46(3): 602–606. doi: 10.3969/j.issn.0372-2112.2018.03.013.

[22] 谢永, 李香, 张松松, 等. 一种可证安全的车联网无证书聚合签名改进方案[J]. 电子与信息学报, 2020, 42(5): 1125–1131. doi: 10.11999/JEIT190184.

XIE Yong, LI Xiang, ZHANG Songsong, *et al*. An improved provable secure certificateless aggregation signature scheme for vehicular ad hoc NETworks[J]. *Journal of Electronics & Information Technology*, 2020, 42(5): 1125–1131. doi: 10.11999/JEIT190184.

曾　萍：女，1969年生，教授，研究方向为通信与网络安全、物联网安全.

郭瑞芳：女，1994年生，硕士生，研究方向为物联网安全.

马英杰：女，1979年生，副教授，研究方向为混沌密码通信.

高　原：女，1979年生，讲师，研究方向为区块链应用.

赵　耿：男，1964年生，教授，博士生导师，研究方向为混沌密码通信.

责任编辑：余　蓉