基于无证书签密的车联社会网络安全通信机制

张文波[1,2]，黄文华[1,2]，冯景瑜[1,2]
（1. 西安邮电大学网络空间安全学院，陕西 西安 710121；2. 西安邮电大学无线网络安全技术国家工程实验室，陕西 西安 710121）

摘 要：针对车联社会网络（VSN）的通信安全问题，提出了一种高效的无证书签密方案，在随机预言模型下基于计算性 Diffie-Hellman 和椭圆曲线离散对数困难性问题证明了所提方案的安全性，为 VSN 成员间的通信提供了机密性和不可伪造性保护。采用假名机制解决 VSN 中的隐私保护问题时，在不需要安装额外防篡改装置的条件下，提出了一种车辆假名及其密钥的自生成机制。性能分析表明，所提方案可有效减少通信量，并可显著减少密钥生成中心的计算负担。

关键词：车联社会网络；车载自组网；隐私保护；无证书密码体制；签密
中图分类号：TN393
文献标识码：A
DOI: 10.11959/j.issn.1000−436x.2021144

Secure communication mechanism for VSN based on certificateless signcryption

ZHANG Wenbo[1,2], HUANG Wenhua[1,2], FENG Jingyu[1,2]
1. School of Cyberspace Security, Xi'an University of Posts and Telecommunications, Xi'an 710121, China
2. National Engineering Laboratory for Wireless Security, Xi'an University of Posts and Telecommunications, Xi'an 710121, China

Abstract: To solve the communication security problems of vehicular social network (VSN), an efficient certificateless signcryption scheme was proposed. The proposed scheme was proven secure in the random oracle model based on the computational Diffie-Hellman problem and elliptic curve discrete logarithm problem, which provided confidentiality and unforgeability protection for VSN members. In addition, when the pseudonym mechanism was used to solve the privacy protection problem in VSN, without installing tamper-proof device, a self-generation mechanism for vehicle pseudonyms and their keys was proposed. The performance analysis shows that the proposed scheme can decrease communication cost, and significantly reduce the computation overhead of the key generation center.

Keywords: VSN, VANET, privacy protection, certificateless cryptography, signcryption

1 引言

车联社会网络（VSN, vehicular social network）是在出行过程中具有相同兴趣爱好或者相同目的地的人员相互联系、沟通而形成的虚拟移动网络[1]，是一种引入社交属性的车载自组网（VANET, vehicular ad hoc network）。VSN 部署在 VANET 之上，除了能够提供道路安全预警、提升车辆驾驶体验等行车安全服务外，还可以满足社交娱乐、即时通信、合作式行驶等基于社会关系的非安全服务需求。随着自媒体行业的发展和 5G 通信网络的逐步覆盖，VSN 将为用户提供更个性化、更便捷的行车和娱乐服务，以及更加精准的数据投递服务。

典型的 VSN 结构如图 1 所示，包含 3 类实体，即可信中心（TA, trusted authority）、路边单元（RSU, roadside unit）和车辆；2 类通信模式，即车辆−基

收稿日期：2021−01−14；修回日期：2021−03−10
基金项目：国家自然科学基金资助项目（No.61802302）；陕西省自然科学基础研究计划基金资助项目（No.2019JM-442）
Foundation Items: The National Natural Science Foundation of China (No.61802302), The Natural Science Basic Research Program of Shaanxi (No.2019JM-442)

础设施通信（V2I/V2R, vehicle-to-infrastructure/RSU）和车辆−车辆通信（V2V, vehicle-to-vehicle）。VSN 中的应用在通信过程中既需要经常访问用户的实际位置、个人偏好、社会关系等隐私信息，又要频繁地进行基于社会关系的信息交流，因此，VSN 中的隐私保护和通信安全变得至关重要[2]。

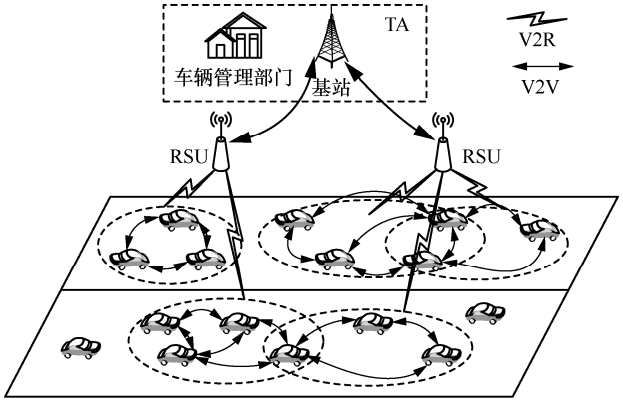


图 1　VSN 结构示意

针对以上 2 类通信模式，学者已经提出了许多消息认证和隐私保护的解决方案。文献[3]基于身份的签名方法构造了用于 V2I 安全通信的消息认证方案，使用假名代替真实身份实现了条件隐私保护，与以前的方案相比在性能上提升了近 1/5。文献[4]提出了基于身份的条件隐私保护认证方案，假名及其密钥由防篡改装置（TPD, tamper-proof device）生成，由于采用椭圆曲线密码体制（ECC, elliptic curve cryptography），与文献[3]相比具有更高的计算效率。文献[5]设计了基于身份签名方法的消息认证方案，为车辆与 RSU 之间的消息传输提供安全的认证过程，分别支持 RSU 和车辆的批量消息验证，提高了 RSU 的消息处理能力，并在随机预言模型（ROM, random oracle model）下证明了方案的安全性。为了解决基于身份的密码方案所具有的密钥托管问题，文献[6-7]为 V2I 安全通信构造了无双线性对运算的无证书认证方案，在避免密钥托管问题的同时，还支持 RSU 的批量消息验证。

以上的 V2I 安全通信解决方案大多是通过数字签名的方式实现 TA 与车辆或者 RSU 与车辆之间的消息认证。然而，完善的车联网络生态除了 RSU 和车辆之间的通信，更多的还应该是车与车之间的 V2V 通信，形成“人→车→RSU→车辆管理部门→人”的闭环，最终形成车辆社交生态圈。文献[8]为实现 V2V 通信过程中的隐私保护和消息认证，采用椭圆曲线密码体制为车联网构建了基于身份的消息认证方案，也解决了基于双线性对的认证方案计算效率偏低的问题。与文献[4]类似，文献[8]的方案也由 TPD 负责随机假名及其密钥的生成。文献[9]为 V2V 安全通信设计了基于身份的无双线性对运算的消息认证方案，当车辆向 TA 申请注册时，由 TA 为其生成假名标识和密钥以实现通信过程中的隐私保护。文献[10]为了在 VSN 中减少生成假名的数量，将已有的假名序列组成一个假名环轮流使用，但性能分析表示仅当假名数量为 7～9 时，才具有较高的效率，并且需要 TA 和 RSU 合作才能从假名获取实身份。

社交驾驶和即时通信是 VSN 的两大特色[11]，也是其与 VANET 的不同之处，而在社交和即时通信过程中传输的消息往往较敏感，因此，通信内容的私密性保护是 VSN 的安全挑战之一。文献[12]为了保证 VANET 中消息传输的安全，提出了一种混合认证协议，但该协议并未对车辆隐私进行有效保护。文献[13]提出了具有隐私保护功能的签密方案，由 TA 和私钥生成器分别生成车辆的假名和密钥，但与文献[12]同样采用了双线性对运算，计算效率较低。文献[14]提出的基于签密的条件隐私保护认证方案中，通过签名验证消息的完整性，以对称加密算法保护通信内容的机密性，其中对称加密时的密钥由假名信息及私钥计算得到。方案基于椭圆曲线密码体制构建，因而计算消耗相对较低，但方案未给出完备的安全性证明。

上述方案均是在 TA 或 RSU 生成多个假名后，依次向密钥生成中心（KGC, key generation center）申请生成对应的公私钥对，大大增加了密钥生成中心的工作量和通信量。根据文献[15]的描述，为了使假名达到隐私保护的预期效果，其更新策略建议每隔 2 min 或 1 km 就更新一次假名。即使采用假名环的更新方式[10]，每辆车所需的假名数量也将非常多。随着 5G 通信信号的覆盖，依托现有的通信基站或加油站作为 RSU，可以使 RSU 管辖范围内的车辆数量至少增加一个数量级。当 TA 或 RSU 管辖的车辆为数以万计时，假名及其密钥的生成将给 TA 和 RSU 带来巨大的负担和挑战。文献[4, 7-8]通过在车辆上安装 TPD 来生成假名及其密钥，可以在一定程度上减少 TA 的工作量，但由于部分 TPD 中已预加载 TA 的密钥，易引起恶意攻击者

关注，遭受侧信道攻击[16-17]，增加的设备成本也可能阻碍 VANET 的发展。虽然文献[18-19]通过周期性地更新存储于TPD中的信息来防止恶意攻击者获取有用信息，但并不能从根本上解决信息泄露的问题。

本文提出一种 VSN 环境下的基于无证书签密的安全通信机制，主要工作及创新如下。

1) 设计了适用于V2V通信的基于ECC的无证书签密方案，避免了密钥托管问题，在 ROM 模型下证明了方案的安全性，并采用假名机制保护通信双方的真实身份。与已有的消息签名方案相比，所提方案在实现车辆与车辆之间通信的不可伪造性与隐私保护的同时，可提供消息机密性保护。

2) 提出了一种车辆假名及其密钥的自生成机制。车辆注册时与可信中心秘密保存的参数生成假名，并利用系统公开参数和自身公私钥对生成其密钥。与已有方案中由TA或RSU辅助生成方式相比，所提机制可以把计算工作量分摊给车辆，显著降低了 TA 或 RSU 的工作负担。

3) 从安全性、计算效率和通信量三方面与已有方案进行了对比，在具备各项安全特性的基础上还具有较短的密文长度和较低的计算量，尤其在假名生成阶段不需要 TA 的参与，密钥生成阶段也仅需 KGC 参与一次，有效地减少了通信量。

2 预备知识

2.1 相关困难性问题及其假设

计算性 Diffie-Hellman（CDH, Computation- al Diffie-Hellman）问题定义如下。设 G 是由椭圆曲线上的点构成的加法循环群，P 是 G 的一个生成元。给定 $aP, bP \in G$，CDH 问题的目标是在 $a, b \in Z_q^*$ 未知的情况下，计算 abP。

椭圆曲线离散对数问题（ECDLP, elliptic curve discrete logarithm problem）定义如下。设 G 是由椭圆曲线上的点构成的加法循环群，P 是 G 的一个生成元。对于 $\forall a \in Z_q^*$，给定 $P, aP \in G$，ECDLP 问题的目标是计算 a。

2.2 签密方案的形式化定义

用于 VSN 安全通信的无证书签密方案包含 4 个参与者：KGC、交通管理中心（TMA, traffic management authority）、签密者（标识为 ID_A）和接收者（标识为 ID_B），分为 3 个阶段，共由 6 个算法构成。

1) 注册阶段

系统参数生成。输入安全参数 ℓ，KGC 生成系统主密钥 msk，输出系统公开参数 params。

部分密钥生成。输入 params、msk 和实体身份标识 ID，KGC 输出实体的部分公私钥，并安全传送给实体。

2) 密钥生成阶段

实体密钥生成。输入 params、ID、部分公私钥，实体输出完整密钥。

假名密钥生成。输入 params、ID、实体密钥以及可信中心的公钥，实体输出假名标识 PID 及假名密钥。假名密钥与真实身份密钥在形式上具有一致性。

3) 消息签密阶段

签密。输入消息 m、ID_A 及其密钥、ID_B 及其公钥，签密者输出对 m 的签密密文 σ。

解签密。输入签密密文 σ、ID_A 及其公钥、ID_B 及其密钥。如果验证通过，接收者输出明文消息 m；否则，拒绝接收消息。

2.3 安全模型

无证书签密方案存在 2 种类型的攻击者 A_I 和 A_{II}，具体说明如下。

1) A_I 类攻击者模拟恶意用户，可以获取用户公钥并能够任意替换合法用户的公钥，但不掌握系统主密钥。该类攻击者包含攻击敌手 $A_{I\text{-}1}$ 和 $A_{I\text{-}2}$，其中，$A_{I\text{-}1}$ 用于攻击方案的机密性，$A_{I\text{-}2}$ 用于攻击方案的不可伪造性。

2) A_{II} 类攻击者模拟不诚实的 KGC，掌握系统主密钥，但无法替换合法用户的公钥。该类攻击者包含攻击敌手 $A_{II\text{-}1}$ 和 $A_{II\text{-}2}$，其中，$A_{II\text{-}1}$ 用于攻击方案的机密性，$A_{II\text{-}2}$ 用于攻击方案的不可伪造性。

关于无证书签密方案安全模型的具体描述可参考文献[20-21]，本文不再赘述。

3 本文方案

本节对提出的用于 VSN 安全通信的无证书签密方案进行描述，相关符号的意义如表 1 所示。

3.1 方案描述

1) 注册阶段

系统参数生成。输入安全参数 ℓ，KGC 生成 2 个大素数 p 和 q，q 为循环群 G 的阶。令 P 为 G 的一个生成元。选取安全哈希函数：$H_1 : \{0,1\}^* \times G \times$

$G \to Z_q^*$，$H_2:\{0,1\}^* \times\{0,1\}^* \times G \times G \times G \to Z_q^*$，$H_3:G \to \{0,1\}^*$。随机选取 $z \in Z_q^*$ 为主密钥，计算系统公钥 $P_{\text{pub}} = zP$。KGC 秘密保存主密钥 z，公开系统参数 $\text{params} = (p, q, P, P_{\text{pub}}, H_1, H_2, H_3)$。

表 1　　参数说明

参数	含义
z	KGC 的主密钥
P_{pub}	系统公钥
H_x	哈希函数，其中 x = 1, 2, 3
ID_i	实体 V_i 的标识
SK_i	ID_i 对应的私钥
PK_i	ID_i 对应的公钥
PID_i	V_i 的假名标识集合
$\text{PID}_{i,j}$	V_i 的第 j 个 PID
w_i	TMA 与 ID_i 之间的秘密信息，用于生成 PID_i
m	明文消息
sig	消息 m 的签名
C	消息 m 的密文

部分密钥生成。实体（RSU、车辆等）选取 $x_i, w_i \in Z_q^*$，计算 $X_i = x_i P$，将 (ID_i, X_i, w_i) 通过安全渠道传送给 TMA 进行注册。TMA 审核无误后，秘密保存 w_i，并将二元组 $<\text{ID}_i, w_i>$ 添加到实体信息表（EIT, entity information table）中，然后将 (ID_i, X_i) 发送给 KGC。KGC 选取 $d_i \in Z_q^*$，计算部分公钥 $K_i = d_i P$，部分私钥 $k_i = z + d_i h_1^i$，$h_1^i = H_1(\text{ID}_i, X_i, K_i)$，将 K_i 和 k_i 通过安全渠道传送给实体。

2) 密钥生成阶段

实体密钥生成。实体可以通过计算等式 $k_i P = P_{\text{pub}} + h_1^i K_i$ 是否成立来判断部分私钥是否有效。若有效，则实体的公私钥分别为 $\text{PK}_i = (X_i, K_i)$ 和 $\text{SK}_i = (x_i, k_i)$。TMA 的密钥也由 KGC 生成，公私钥分别为 $\text{PK}_{\text{TMA}} = (X_{\text{TMA}}, K_{\text{TMA}})$ 和 $\text{SK}_{\text{TMA}} = (x_{\text{TMA}}, k_{\text{TMA}})$。

假名密钥生成。为使车辆实体的假名密钥与真实身份密钥在形式上具有一致性，车辆按照 KGC 为其生成密钥的方式为每一个假名生成公私钥。设假名标识为 $\text{PID}_{i,j}$，随机选取 $x_{P_i}, \gamma_{P_i} \in Z_q^*$，计算 $X_{P_i} = x_{P_i} P$，$K_{P_i} = \gamma_{P_i} P + h_1^i K_i$，其中，$h_1^i = H_1(\text{ID}_i, X_i, K_i)$。那么 $\text{PID}_{i,j}$ 的公钥为 $\text{PK}_{P_i} = (X_{P_i}, K_{P_i})$，私钥为 $\text{SK}_{P_i} = (x_{P_i}, k_{P_i})$，其中 $k_{P_i} = \gamma_{P_i} + k_i$。

3) 消息签密阶段

签密。车辆 V_{A} 首先在假名集合中按照预先设定的策略选取一个 PID_{A}，其私钥为 $\text{SK}_{\text{PA}} = (x_{\text{PA}}, k_{\text{PA}})$，公钥为 $\text{PK}_{\text{PA}} = (X_{\text{PA}}, K_{\text{PA}})$，车辆 V_{B} 的假名公钥为 $\text{PK}_{\text{PB}} = (X_{\text{PB}}, K_{\text{PB}})$。$V_{\text{A}}$ 与 V_{B} 间使用假名签密的过程如下。

① V_{A} 随机选取 $r \in Z_q^*$，计算 $R = rP$

② $h_2 = H_2(X_{\text{PA}}, K_{\text{PA}}, R, \text{PID}_{\text{A}}, m)$

③ $\text{sig} = h_2 r + x_{\text{PA}} + k_{\text{PA}}$

④ $Y = r(X_{\text{PB}} + h_1^{\text{PB}}(K_{\text{PB}} + P_{\text{pub}}))$

⑤ $C = H_3(Y) \oplus m$

其中，$h_1^{\text{PB}} = H_1(\text{PID}_{\text{B}}, X_{\text{PB}}, K_{\text{PB}})$。$V_{\text{A}}$ 发送 $\sigma = < R, \text{sig}, C >$ 给车辆 V_{B}。

解签密。V_{B} 收到签密消息 σ 后，使用相应的私钥 $\text{SK}_{\text{PB}} = (x_{\text{PB}}, k_{\text{PB}})$ 和 V_{A} 的公钥 $\text{PK}_{\text{PA}} = (X_{\text{PA}}, K_{\text{PA}})$ 进行解签密。计算过程如下。

① $Y' = (x_{\text{PB}} + h_1^{\text{PB}} k_{\text{PB}})R$

② $m = H_3(Y') \oplus C$

③ $h_2' = H_2(X_{\text{PA}}, K_{\text{PA}}, R, \text{PID}_{\text{A}}, m)$

④ $\text{sig}P = h_2' R + X_{\text{PA}} + K_{\text{PA}} + P_{\text{pub}}$

通过步骤②恢复出明文消息 m。如果步骤④成立，签名有效，接受消息 m；否则拒绝该消息。

3.2　车辆假名自生成过程

对于任意车辆，选取哈希函数 $H_P:\{0,1\}^* \times G \times G \to Z_q^*$，假名标识的生成过程如下。

随机选取 $\varphi \in Z_q^*$，计算

① $\text{pid}_{j_1} = \varphi P$

② $\text{pid}_{j_2} = H_P(t, \text{pid}_{j_1}, \varphi X_{\text{TMA}}) \oplus w_i$

车辆的第 j 个假名为 $\text{PID}_{i,j} = \{\text{pid}_{j_1}, \text{pid}_{j_2}, t\}$，其中，$t$ 是该假名的有效时间。那么，车辆的所有假名集合为 $\text{PID}_i = \{\text{PID}_{i,j} \mid j = 1, 2, \cdots, n\}$，$n$ 表示所拥有的假名的数量。

3.3　正确性分析

通过式(1)可得 $Y' = Y$，据此可正确解密出明文消息 $m = H_3(Y') \oplus C$。

$$
\begin{aligned}
&Y' = (x_{\text{PB}} + h_1^{\text{PB}} k_{\text{PB}})R = \\
&(x_{\text{PB}} + h_1^{\text{PB}}(\gamma_{\text{PB}} + k_B))R = \\
&r(x_{\text{PB}} + h_1^{\text{PB}}\gamma_{\text{PB}} + h_1^{\text{PB}}(d_B h_1^B + z))P = \\
&r(X_{\text{PB}} + h_1^{\text{PB}}(\gamma_{\text{PB}} + h_1^B d_B)P + h_1^{\text{PB}} zP) = \\
&r(X_{\text{PB}} + h_1^{\text{PB}}(K_{\text{PB}} + P_{\text{pub}})) = Y
\end{aligned} \tag{1}
$$

签名的有效性验证如式(2)所示。

$$\begin{aligned}&\mathrm{sig}P=(h_2'r+x_{\mathrm{PA}}+k_{\mathrm{PA}})P=\\&h_2'rP+x_{\mathrm{PA}}P+(\gamma_{\mathrm{PA}}+k_{\mathrm{A}})P=\\&h_2'R+X_{\mathrm{PA}}+(\gamma_{\mathrm{PA}}+d_{\mathrm{A}}h_1^{\mathrm{A}}+z)P=\\&h_2'R+X_{\mathrm{PA}}+K_{\mathrm{PA}}+P_{\mathrm{pub}}\end{aligned}\tag{2}$$

3.4 安全性证明

本节描述了在 2 种类型的攻击者攻击下方案的机密性和不可伪造性安全证明过程（参考文献[20-21]的证明方法）。

1) 机密性

定理 1 $\mathrm{A_{I\text{-}1}}$类敌手攻击下的机密性。

在预言机模型中，若存在一个敌手 $\mathrm{A_{I\text{-}1}}$能够在多项式时间内以不可忽略的优势 $\varepsilon_{\mathrm{I\text{-}1}}$赢得以下模拟过程（假设最多可进行 q_i 次 H_i 查询、q_{SK} 次私钥生成查询和 q_S 次签密查询），则存在一个算法 Q 能够在多项式时间内以不可忽略的优势 $\left(1-\frac{q_{\mathrm{SK}}}{2^{\lambda}}\right)\left(1-\frac{q_3}{2^{\lambda}}\right)\frac{\varepsilon_{\mathrm{I\text{-}1}}}{\mathrm{e}(q_S+q_{\mathrm{SK}})}$解决 CDH 问题。

证明 假设算法 Q 是CDH困难问题的解决者，其输入是 (P,aP,bP)，目标是在 $a,b\in Z_q^*$ 且未知的情况下计算出 abP。Q 充当此次模拟的挑战者。当模拟开始后，设 $P_{\mathrm{pub}}=aP$（a 为系统主密钥），Q 运行系统参数生成算法，发送 params 给 $\mathrm{A_{I\text{-}1}}$，并维护列表 $L_1,L_2,L_3,L_{\mathrm{SK}},L_{\mathrm{PK}}$ 用于跟踪 $\mathrm{A_{I\text{-}1}}$ 对预言机 H_1、H_2 和 H_3 的询问，以及对私钥提取和公钥提取的询问。初始时每个列表均为空。

阶段 1 询问阶段。敌手 $\mathrm{A_{I\text{-}1}}$进行下述多项式有界次询问。

H_1 询问。当 Q 收到 $\mathrm{A_{I\text{-}1}}$对 H_1 的询问时，若 L_1 中存在 $(\mathrm{ID}_i,X_i,K_i,h_1)$，则返回相应的值；否则，对 ID_i 进行公钥提取询问，得到相应的 h_1。

H_2 询问。当 Q 收到 $\mathrm{A_{I\text{-}1}}$对 H_2 的询问时，若 L_2 中存在 $(X_i,K_i,R,\mathrm{ID}_i,m,h_2)$，则返回相应的值；否则，随机选取 $h_2\in Z_q^*$ 且 $h_2\notin L_2$，添加元组 $(X_i,K_i,R,\mathrm{ID}_i,m,h_2)$ 到 L_2 中，并返回 h_2。

H_3 询问。当 Q 收到对 H_3 的询问时，若 L_3 中存在 (Y,h_3)，返回对应的值；否则，随机选取 $h_3\in\{0,1\}^*$ 且 $h_3\notin L_3$，添加 (Y,h_3) 到 L_3 中，并返回 h_3。

公钥提取询问。当 Q 收到对 PID_i（此处表示其中的一个假名）的公钥生成询问时，执行下列操作。若 $(\mathrm{PID}_i,X_i,K_i,c)$ 存在于 L_{PK} 中，返回相应的值，其中 $c\in\{0,1\}$，$\Pr[c=1]=\delta=1/(q_{\mathrm{SK}}+q_S+1)$；否则，从 c 中随机选取一个值。如果 $c=0$，选取 $x_{P_i},k_{P_i},h_1\in Z_q^*$，计算 $X_{P_i}=x_{P_i}P$，$\gamma_{P_i}=k_{P_i}-k_i$ 以及 $K_{P_i}=k_{P_i}P-P_{\mathrm{pub}}$，将 $(\mathrm{PID}_i,x_{P_i},k_{P_i})$ 添加到 L_{SK}、$(\mathrm{PID}_i,X_{P_i},K_{P_i},h_1)$ 添加到 L_1，并将 $(\mathrm{PID}_i,X_{P_i},K_{P_i},c)$ 添加到 L_{PK} 中，返回 $\mathrm{PK}_{P_i}=(X_{P_i},K_{P_i})$ 给 $A_{\mathrm{I\text{-}1}}$。如果 $c=1$，令 $X_{P_i}=x_{P_i}^*P$，$K_{P_i}=\gamma_{P_i}^*P+h_1^iK_i$，其中 Q 掌握 $x_{P_i}^*,\gamma_{P_i}^*\in Z_q^*$，选取满足 $h_1\notin L_1$ 的 $h_1\in Z_q^*$，将 $(\mathrm{PID}_i,X_{P_i},K_{P_i},h_1)$ 添加到 L_1 中，然后将 $(\mathrm{PID}_i,X_{P_i},K_{P_i},c)$ 添加到 L_{PK} 中，并返回 PK_{P_i}。

私钥提取询问。当 Q 收到对身份 ID_i（或 PID_i）的私钥生成询问时，查找 L_{SK}，若存在 (ID_i,x_i,k_i)，则返回私钥 $\mathrm{SK}_i=(x_i,k_i)$ 给 $\mathrm{A_{I\text{-}1}}$；否则，执行公钥提取询问，获得相应的元组 $(\mathrm{ID}_i,X_i,K_i,c)$。如果 $c=0$，返回在公钥提取询问中向 L_{SK} 添加的 SK_i；若 $c=1$，结束询问并终止模拟。

公钥替换。对于 ID_i，$A_{\mathrm{I\text{-}1}}$ 可选择任一新公钥 $\mathrm{PK}_i'=(X_i',K_i')$ 替换原有公钥 PK_i。

签密询问。Q 在 L_{PK} 中查找 $(\mathrm{ID_A},X_{\mathrm{A}},K_{\mathrm{A}},c)$。若 $c=1$，结束询问并终止该模拟过程；否则，查找 L_{PK} 和 L_{SK}，获取相应的私钥 $\mathrm{SK_A}$ 和公钥 $\mathrm{PK_B}$，对 $(\mathrm{ID_A},\mathrm{ID_B},m)$ 执行签密算法，得到 $\sigma=<R,\mathrm{sig},C>$，并将 σ 返回给 $\mathrm{A_{I\text{-}1}}$。

解签密询问。当 Q 收到 $\mathrm{A_{I\text{-}1}}$的解签密询问时，在 L_{PK} 查询 ID_B 对应的元组 $(\mathrm{ID_B},X_{\mathrm{B}},K_{\mathrm{B}},c)$，执行如下操作。

① 若 $(\mathrm{ID_B},X_{\mathrm{B}},K_{\mathrm{B}},c)$ 存在且 $c=0$，则在 L_{SK} 中查询对应的私钥 $\mathrm{SK_B}$，对 σ 执行解签密算法得到 m 和 $h_2=H_2(X_{\mathrm{A}},K_{\mathrm{A}},R,\mathrm{ID_A},m)$；若 $c=1$，查询 L_2 和 L_3 得到 h_2 和 h_3，计算 $m=h_3\oplus C$。如果 $\mathrm{sig}P=h_2R+X_A+K_A+P_{\mathrm{pub}}$ 成立，则返回 m，否则终止模拟。

②若 $(\mathrm{ID_B},X_{\mathrm{B}},K_{\mathrm{B}},c)$ 不存在，表示公钥已被替换，Q 查询 L_1，L_2 和 L_3，得到 $(\mathrm{ID_A},X_{\mathrm{A}}',K_{\mathrm{A}}',h_1')$、$(X_{\mathrm{A}}',K_{\mathrm{A}}',R,\mathrm{ID_A},m,h_2')$ 和 (Y,h_3')，计算 $m=h_3'\oplus C$，如果 $\mathrm{sig}P=h_2'R+X_{\mathrm{A}}'+K_{\mathrm{A}}'+P_{\mathrm{pub}}$ 成立，则返回 m，否则终止模拟。

阶段 2 挑战阶段。

$\mathrm{A_{I\text{-}1}}$给出 2 个接受挑战的身份 $\mathrm{PID_A}$ 和 $\mathrm{PID_B}$，以及 2 个等长度的明文消息 m_0,m_1。Q 对 $\mathrm{PID_B}$ 执行公钥询问得到 $(\mathrm{PID_B},X_{\mathrm{PB}},K_{\mathrm{PB}},c)$。若 $c=0$，则终止

模拟；若 $c=1$，则随机选取 $\beta\in\{0,1\}$，以及 $b,s^*,h_2^*\in Z_q^*$，计算 $R=bP$，$s^*=h_2^*r+x_{\mathrm{PA}}+k_{\mathrm{PA}}$；$Q$ 选取 $Y^*\in G$，查询 L_3 获取 h_3^*，计算 $C^*=h_3^*\oplus m_\beta$，将挑战密文 $\sigma^*=<R^*,s^*,C^*>$ 返回给 $\mathrm{A_{I\text{-}1}}$。

$\mathrm{A_{I\text{-}1}}$ 进行概率多项式有界次询问，当询问终止时，输出 β' 作为对 β 的猜测，若 $\beta'=\beta$，Q 输出 $(Y^*-x_{\mathrm{PB}}^*R)/h_1^{\mathrm{PB}}-(\gamma_{\mathrm{PB}}^*+h_1^Bd_{\mathrm{B}}^*)R=abP$ 作为 CDH 问题的解；否则，未解决 CDH 问题。

若 $\mathrm{A_{I\text{-}1}}$ 执行了 $\mathrm{PID_B}$ 的私钥生成询问，则 Q 挑战失败，而它不执行该询问的概率为 $\Pr[\varepsilon_1]=1-q_{\mathrm{SK}}/2^\lambda$，其中，$2^\lambda$ 是密钥空间大小；若 $\mathrm{A_{I\text{-}1}}$ 在挑战阶段执行了 H_3 询问，则挑战失败，它不执行该询问的概率为 $\Pr[\varepsilon_2]=1-q_3/2^\lambda$；$Q$ 在询问阶段未终止模拟的概率为 $\Pr[\varepsilon_3]=(1-\delta)^{q_S+q_{\mathrm{SK}}+1}$；$Q$ 在挑战阶段未终止模拟的概率为 $\Pr[\varepsilon_4]=\delta$。最后，顺利模拟以上过程的概率为 $\Pr[\varepsilon_1\wedge\varepsilon_2\wedge\varepsilon_3\wedge\varepsilon_4]=(1-q_{\mathrm{SK}}/2^\lambda)\cdot(1-q_3/2^\lambda)\delta(1-\delta)^{q_S+q_{\mathrm{SK}}+1}$，其中，$\delta=1/(q_{\mathrm{SK}}+q_S+1)$ 且当 $q_{\mathrm{SK}}+q_S$ 足够大时，$(1-\delta)^{q_S+q_{\mathrm{SK}}+1}\to \mathrm{e}^{-1}$。

综上所述，敌手 $\mathrm{A_{I\text{-}1}}$ 若能以不可忽略的概率 $\varepsilon_{\mathrm{I\text{-}1}}$ 攻破方案的机密性，那么 Q 将以不可忽略的概率 $\left(1-\frac{q_{\mathrm{SK}}}{2^\lambda}\right)\left(1-\frac{q_3}{2^\lambda}\right)\frac{\varepsilon_{\mathrm{I\text{-}1}}}{\mathrm{e}(q_S+q_{\mathrm{SK}})}$ 解决 CDH 问题。证毕。

定理 2　$\mathrm{A_{II\text{-}1}}$ 类敌手攻击下的机密性。

证明方法与定理 1 相似，不再赘述。

2) 不可伪造性

定理 3　$\mathrm{A_{I\text{-}2}}$ 类敌手攻击下的不可伪造性。

在预言机模型中，若存在一个敌手 $\mathrm{A_{I\text{-}2}}$ 能够在多项式时间内以不可忽略的优势 $\varepsilon_{\mathrm{I\text{-}2}}$ 赢得以下模拟过程（假设最多可进行 q_i 次 H_i 查询、q_{SK} 次私钥生成查询和 q_S 次签密查询），则存在一个算法 Q 能够在多项式时间内以不可忽略的优势 $\left(1-\frac{q_{\mathrm{SK}}}{2^\lambda}\right)\frac{\varepsilon_{\mathrm{I\text{-}2}}}{\mathrm{e}(q_S+q_{\mathrm{SK}})}$ 解决 ECDLP 问题。

证明　假设算法 Q 是 ECDLP 困难问题的解决者，其输入是 (a,aP)，目标是在 $a\in Z_q^*$ 且未知的情况下计算出 a。算法 Q 以 $\mathrm{A_{I\text{-}2}}$ 为子程序并充当此次模拟的挑战者。当模拟开始后，设 $P_{\mathrm{pub}}=aP$（a 为系统主密钥），Q 运行系统参数生成算法，发送 params 给 $\mathrm{A_{I\text{-}2}}$，并维护列表 $L_1,L_2,L_{\mathrm{SK}},L_{\mathrm{PK}}$ 用于跟踪 $\mathrm{A_{I\text{-}2}}$ 对预言机 H_1、H_2，私钥提取和公钥提取的询问。初始时每个列表均为空。

阶段 1　询问阶段。敌手 $\mathrm{A_{I\text{-}2}}$ 进行定理 1 中的 H_1 和 H_2 询问，以及公钥提取、私钥提取和公钥替换询问。签名及验证询问描述如下。

签名询问。当 Q 收到 $\mathrm{A_{I\text{-}2}}$ 对 $(m,\mathrm{ID_A})$ 的签名询问时，在 L_{PK} 中查找 $(\mathrm{ID_A},X_{\mathrm{A}},K_{\mathrm{A}},c)$。若 $c=1$，结束询问并终止该模拟过程；否则，查找 L_{SK}，获取私钥 $\mathrm{SK_A}$，执行签密算法，得到签名 $\sigma=<R,\mathrm{sig},C>$，并将 σ 返回给 $\mathrm{A_{I\text{-}2}}$。

签名验证询问。Q 在 L_{PK} 中查询 $\mathrm{PK_A}=(X_{\mathrm{A}},K_{\mathrm{A}})$ 对应元组，并执行如下操作。

①若存在且 $c=0$，计算 $h_2=H_2(X_{\mathrm{A}},K_{\mathrm{A}},R,\mathrm{ID_A},m)$，若 $\mathrm{sig}P=h_2R+X_{\mathrm{A}}+K_{\mathrm{A}}+P_{\mathrm{pub}}$ 成立，则签名正确，返回 m，否则终止模拟；若 $c=1$，查询 L_2 获取 h_2'，如果 $\mathrm{sig}P=h_2'R+X_{\mathrm{A}}+K_{\mathrm{A}}+P_{\mathrm{pub}}$ 成立，则返回 m，否则终止模拟。

②若不存在，表示公钥已被替换，Q 查询 L_1 和 L_2，得到 $(\mathrm{ID_A},X_{\mathrm{A}}',K_{\mathrm{A}}',h_1')$、$(X_{\mathrm{A}}',K_{\mathrm{A}}',R,\mathrm{ID_A},m,h_2)$，如果 $\mathrm{sig}P=h_2'R+X_{\mathrm{A}}'+K_{\mathrm{A}}'+P_{\mathrm{pub}}$ 成立，则将 m 返回给 $\mathrm{A_{I\text{-}2}}$，否则终止模拟。

阶段 2　挑战阶段。

Q 对身份 $\mathrm{PID_A}$ 执行公钥查询得到 $(\mathrm{PID_A},X_{\mathrm{PA}},K_{\mathrm{PA}},c)$。若 $c=0$，则终止模拟；否则，随机选取 $r,s^*\in Z_q^*$，计算 $R=rP$，$h_2^*=H_2(X_{\mathrm{PA}},K_{\mathrm{PA}},R,\mathrm{ID_{PA}},m)$，输出伪造的签名 $\sigma^*=<R,s^*,m>$。若签名伪造成功，输出 $s^*-(h_2^*r+x_{PA}^*+\gamma_{PA}^*+d_A^*h_1)=a$ 作为 ECDLP 问题的解；否则，未解决 ECDLP 问题。

若 $\mathrm{A_{I\text{-}2}}$ 执行了 $\mathrm{PID_A}$ 的私钥生成询问，则 Q 挑战失败，而它不执行该询问的概率为 $\Pr[\varepsilon_1]=1-q_{\mathrm{SK}}/2^\lambda$；$Q$ 在询问阶段未终止模拟的概率为 $\Pr[\varepsilon_2]=(1-\delta)^{q_S+q_{\mathrm{SK}}+1}$；$Q$ 在挑战阶段未终止模拟的概率为 $\Pr[\varepsilon_3]=\delta$。最后，顺利模拟以上过程的概率为 $\Pr[\varepsilon_1\wedge\varepsilon_2\wedge\varepsilon_3]=(1-q_{\mathrm{SK}}/2^\lambda)\delta(1-\delta)^{q_S+q_{\mathrm{SK}}+1}$。

综上所述，敌手 $A_{\mathrm{I\text{-}2}}$ 若能以不可忽略的概率 $\varepsilon_{\mathrm{I\text{-}2}}$ 攻破方案的不可伪造性，那么 Q 将以不可忽略的概率 $\left(1-\frac{q_{\mathrm{SK}}}{2^\lambda}\right)\frac{\varepsilon_{\mathrm{I\text{-}2}}}{\mathrm{e}(q_S+q_{\mathrm{SK}})}$ 解决 ECDLP 问题。证毕。

定理 4　$A_{\mathrm{II\text{-}2}}$ 类敌手攻击下的不可伪造性。

证明方法与定理 3 相似，不再赘述。

4　方案分析

本节将从安全性、计算效率和通信效率三方面

对本文方案与其他签密方案及车联网络环境下的认证方案进行比较。

4.1 安全性分析

1) 可追踪性

当 TMA 接收到车辆的 $\mathrm{PID}_{i,j}$ 后，提取其中的 pid_{j_1}，计算 $w_i = H_P(t_i, \mathrm{pid}_{j_1}, x_{\mathrm{TMA}}\mathrm{pid}_{j_1}) \oplus \mathrm{pid}_{j_2}$。通过查询 EIT 中 $< \mathrm{ID}_i, w_i >$ 的对应关系即可获取车辆的真实身份 ID_i。其中，$x_{\mathrm{TMA}}\mathrm{pid}_{j_1}$ 的计算需要 TMA 的私钥 x_{TMA}，因此，仅 TMA 能够正确解析出车辆的真实身份。

2) 通信双方的匿名性

车辆在通信时均秘密保存真实身份，并以假名作为其身份标识来确保通信过程中的匿名性。通过已有的假名获取车辆的真实身份，需要计算出 w_i 值，而计算 w_i 时需要获得 TMA 的私钥 x_{TMA}。然而，在 x_{TMA} 未知的情况下计算出它的值属于 ECDLP 困难问题。

3) 不可链接性

车辆的各个 PID 之间无相关性，攻击者无法通过已知的 PID 推断出车辆的真实身份，有效地保证了身份信息的安全。车辆生成 PID 的公私钥时，均是在整数域中选取随机数，各个公钥之间不具有相关性，也无法通过多个公钥信息来确定多个 PID 是否来自同一车辆。

本文方案与近几年车联网络环境下消息认证与隐私保护方案在消息的不可伪造性、通信消息的机密性、身份匿名性、真实身份可追踪性及假名的不可链接性等方面的对比如表 2 所示。其中，身份匿名性是可追踪性及不可链接性的前提，即如果一个方案不具有匿名性，也就无法比较可追踪性及不可链接性，如文献[12]方案。

4.2 性能分析

在进行计算效率分析时，主要统计椭圆曲线上耗时较长的点乘和点加运算，而不考虑异或、Z_q^* 上的运算以及映射到 Z_q^* 上的哈希运算，具体的比较结果如表 3 所示。其中，T_{em} 和 T_{ea} 分别表示点乘和点加运算时间。

为了定量分析不同方案的性能，通过实验测定了 T_{em} 和 T_{ea} 的具体数值分别为 0.484 7 ms 和 0.002 1 ms。实验环境如下：Intel G630，主频 2.7 GHz，内存 4 GB（DDR3-1600 MHz），Windows 7 操作系统。方案中使用的椭圆曲线 $E: y^2 = x^3 + ax + b \bmod p$ 中的 p 和群 G 的阶 q 均为 160 bit。从图 2 所示的计算耗时可以看出，文献[22]方案在签密与解签密总时间上与本文方案接近，而与其他方案相比，本文方案在总的计算时间上有一定的优势。

表 2 车联网络环境下不同方案的安全特性比较

方案	不可伪造性	机密性	身份匿名性	可追踪性	不可链接性	消除密钥托管
文献[4]方案	√	×	√	√	√	×
文献[5]方案	√	×	√	√	√	×
文献[6]方案	√	×	√	√	√	√
文献[7]方案	√	×	√	√	√	√
文献[9]方案	√	×	√	√	√	×
文献[10]方案	√	√	√	×	√	×
文献[12]方案	√	√	×	—	—	×
文献[13]方案	√	√	√	√	√	×
文献[14]方案	√	√	√	√	√	×
文献[19]方案	×	√	√	√	√	×
本文方案	√	√	√	√	√	√

注：√表示满足该项安全特性，×表示不满足。

表 3 不同方案的性能对比

方案	签密	解签密	密文长度
文献[20]方案	$3T_{\mathrm{em}}+2T_{\mathrm{ea}}$	$5T_{\mathrm{em}}+3T_{\mathrm{ea}}$	$2\lvert Z_q^*\rvert$
文献[22]方案	$2T_{\mathrm{em}}$	$4T_{\mathrm{em}}+2T_{\mathrm{ea}}$	$\lvert Z_q^*\rvert + \lvert G\rvert$
文献[23]方案	$5T_{\mathrm{em}}+T_{\mathrm{ea}}$	$6T_{\mathrm{em}}+7T_{\mathrm{ea}}$	$\lvert Z_q^*\rvert+2\lvert G\rvert+\lvert\mathrm{Delegation}\rvert$
文献[24]方案	$4T_{\mathrm{em}}+3T_{\mathrm{ea}}$	$3T_{\mathrm{em}}+4T_{\mathrm{ea}}$	$2\lvert Z_q^*\rvert + 2\lvert G\rvert$
文献[25]方案	$3T_{\mathrm{em}}+2T_{\mathrm{ea}}$	$4T_{\mathrm{em}}+2T_{\mathrm{ea}}$	$\lvert Z_q^*\rvert + \lvert G\rvert$
本文方案	$3T_{\mathrm{em}}+2T_{\mathrm{ea}}$	$3T_{\mathrm{em}}+3T_{\mathrm{ea}}$	$\lvert Z_q^*\rvert + \lvert G\rvert$

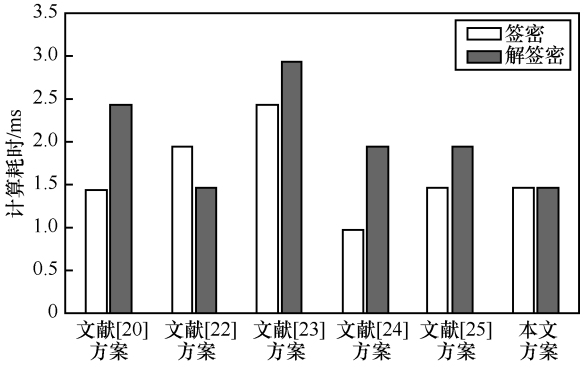


图 2 不同方案的计算耗时对比

表 3 中的密文长度表示各个方案的通信开销程度。文献[23]方案发送的密文中包含代理信息 Delegation，因此密文长度最长，文献[20]方案的通

信开销最小，仅为 $2|Z_q^*|$=320 bit。文献[22, 25]方案与本文方案具有相同的通信开销$|Z_q^*|+|G|$=480 bit，是文献[20]方案通信开销的 1.5 倍。

车联网络环境下不同假名生成方案在生成 n 个不同 PID 及其密钥时的计算耗时对比如表 4 所示，其中，T_{bm} 表示基于双线性对方案中椭圆曲线上的点乘运算时间，T_{h} 表示哈希函数运算时间。除了文献[13]方案中使用了耗时较高的双线性对运算外，其他方案的 PID 生成总时间均相同。由于本文方案为了消除密钥托管问题，在密钥生成时增加了额外的点乘运算，导致计算耗时上的优势并不明显。然而，本文方案的 PID 生成不需要 TMA 的参与，对每辆车而言也仅需 KGC 参与一次，当 n 较大时，本文方案可以显著减轻 TMA 和 KGC 的负担。

表 4　不同方案中 PID 和密钥生成效率对比

方案	PID 生成		密钥生成	
	TA/TMA	车辆	KGC	车辆
文献[4]	$n(2T_{\mathrm{em}}+T_{\mathrm{h}})$	–	nT_h	nT_{em}
文献[5]	$n(T_{\mathrm{em}}+T_{\mathrm{h}})$	nT_{em}	$n(T_{\mathrm{em}}+T_{\mathrm{h}})$	—
文献[6]	$n(2T_{\mathrm{em}}+2T_{\mathrm{h}})$	—	$n(T_{\mathrm{em}}+T_{\mathrm{h}})$	nT_{em}
文献[7]	$n(2T_{\mathrm{em}}+T_{\mathrm{h}})$	—	$n(T_{\mathrm{em}}+T_{\mathrm{h}})$	nT_{em}
文献[9]	$n(T_{\mathrm{em}}+T_{\mathrm{h}})$	nT_{em}	$n(T_{\mathrm{em}}+T_{\mathrm{ea}}+T_{\mathrm{h}})$	—
文献[13]	$n(T_{bm}+T_{\mathrm{h}})$	nT_{bm}	$n(T_{\mathrm{bm}}+T_{\mathrm{h}})$	—
文献[14]	$n(2T_{\mathrm{em}}+T_{\mathrm{h}})$	—	$n(T_{\mathrm{em}}+T_{\mathrm{h}})$	—
本文方案	—	$n(2T_{\mathrm{em}}+T_{\mathrm{h}})$	$2T_{\mathrm{em}}$	$n(2T_{\mathrm{em}}+T_{\mathrm{ea}})$

5　讨论

为实现 VSN 中 V2V 的安全通信，本文提出了高效的无双线性对的无证书签密方案，各个成员的消息在得到签名验证的同时，增加了机密性保护。鉴于学者已经提出许多用于 V2I/V2R 通信的认证方案，因此，本文未考虑该类通信方式。如果对本文方案进行一定调整，也可用于此类通信。但是，由于增加了消息机密性保护，与已有仅提供消息认证功能的方案相比，在计算效率方面相对较低。

假名机制是 VANET 和 VSN 中较常用的隐私保护方法。传统的假名机制是由 TA 或 RSU 辅助生成假名，并由 KGC 提前生成一系列密钥，优点是能够有效地控制假名使用范围。当网络规模较大时，会对 TA 和 KGC 形成较大的负担。本文提出的车辆假名及其密钥的自生成机制可显著减少 TMA 和 KGC 的计算量，然而，应用本文的假名及其密钥自生成机制时，恶意车辆可能会过度生成假名，造成假名的滥用。

6　结束语

VSN 是未来车联网的发展趋势之一，在组建车辆社交生态的同时，呈现出一些新的安全问题。本文为 VSN 中车辆−车辆间通信的私密性和不可伪造性提出一种高效的签密方案，并采用假名机制保证车辆信息的隐私。车辆假名及其密钥均由车辆自身生成，但因特殊原因需要获取车辆真实身份时，必须由 TMA 根据假名计算得到。与已有假名生成方案相比，对于每辆车而言只需 KGC 参与一次密钥生成即可，显著减少了生成大量假名和密钥给 TMA 和 KGC 带来的工作负担。

随着人工智能和无人驾驶技术的发展，驾驶人员将逐步解放出来，拥有更多的时间用于社交、娱乐活动，进一步促进 VSN 的发展，也必将会带来更多的安全挑战。

参考文献：

[1] QIU T, CHEN B C, SANGAIAH A K, et al. A survey of mobile social networks: applications, social characteristics, and challenges[J]. IEEE Systems Journal, 2018, 12(4): 3932-3947.

[2] 王翔, 冷甦鹏, 张可, 等. 车联社会网络综述[J]. 通信学报, 2015, 36(1): 203-214.
WANG X, LENG S P, ZHANG K, et al. Vehicular social network: a survey[J]. Journal on Communications, 2015, 36(1): 203-214.

[3] SHIM K. CPAS: an efficient conditional privacy-preserving authentication scheme for vehicular sensor networks[J]. IEEE Transactions on Vehicular Technology, 2012, 61(4): 1874-1883.

[4] HE D B, ZEADALLY S, XU B W, 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.

[5] LO N W, 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.

[6] 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.

[7] MING Y, CHENG H L. Efficient certificateless conditional privacy-preserving authentication scheme in VANET[J]. Mobile Information Systems, 2019, 2019: 1-19.

[8] 吴黎兵, 谢永, 张宇波. 面向车联网高效安全的消息认证方案[J]. 通信学报, 2016, 37(11): 1-10.
WU L B, XIE Y, ZHANG Y B. Efficient and secure message authentication scheme for VANET[J]. Journal on Communications, 2016,

37(11): 1-10.

[9] ALI I, LAWRENCE T, LI F G. An efficient identity-based signature scheme without bilinear pairing for vehicle-to-vehicle communication in VANET[J]. Journal of Systems Architecture, 2020, 103: 692-705.

[10] GAO T H, DENG X Y, LI Q S, et al. APPAS: a privacy-preserving authentication scheme based on pseudonym ring in VSN[J]. IEEE Access Special Section on Advanced Big Data Analysis for Vehicular Social Networks, 2019, 7: 69936-69946.

[11] VEGNI A M, LOSCRÍ V. A survey on vehicular social networks[J]. IEEE Communications Surveys & Tutorials, 2015, 17(4): 2397-2419.

[12] HAN Y, FANG D, YUE Z, et al. SCHAP: the aggregate signcryption based hybrid authentication protocol for VANET[C]//International Conference on Internet of Vehicles- Technologies and Services. Berlin: Springer, 2014: 218-226.

[13] HONG Z, TANG F, LUO W J. Privacy-preserving aggregate signcryption for vehicular ad hoc networks[C]//Proceedings of the 2nd International Conference on Cryptography, Security and Privacy. New York: ACM Press, 2018: 72-76.

[14] LU M, WU Y, XU Y W, et al. SACP: a signcryption-based authentication scheme with conditional privacy preservation for VANET[C]//The 2018 International Conference on Wireless Algorithms, Systems, and Applications. Berlin: Springer, 2018: 773-779.

[15] SAE. J2735v: Dedicated short-range communications (DSRC) message set dictionary[S]. SAE Standard, 2016.

[16] MANIVANNAN D, MONI S, ZEADALLY S. Secure authentication and privacy-preserving techniques in vehicular ad-hoc networks (VANET)[J]. Vehicular Communications, 2020, 25: 1-18.

[17] DEWANGAN R, ALTAF F, MAITY S. Certificateless aggregate message authentication for hierarchical trusted authority based VANET[C]//2019 3rd International Conference on Computing Methodologies and Communication. Piscataway: IEEE Press, 2019: 429-434.

[18] ZHANG L, WU Q H, DOMINGO-FERRER J, et al. Distributed aggregate privacy-preserving authentication in VANET[J]. IEEE Transactions on Intelligent Transportation Systems, 2017, 18(3): 516-526.

[19] CUI J, XU W, HAN Y B, et al. Secure mutual authentication with privacy preservation in vehicular ad hoc networks[J]. Vehicular Communications, 2020, 21: 1-9.

[20] 周彦伟, 杨波, 王青龙. 安全的无双线性映射的无证书签密机制[J]. 软件学报, 2017, 28(10): 2757-2768.
ZHOU Y W, YANG B, WANG Q L. Secure certificateless signcryption scheme without bilinear pairing[J]. Journal of Software, 2017, 28(10): 2757-2768.

[21] 牛淑芬, 牛灵, 王彩芬, 等. 标准模型下可证明安全的无证书广义签密[J]. 通信学报, 2017, 38(4): 35-45.
NIU S F, NIU L, WANG C F, et al. Certificateless generalized signcryption scheme in the standard model[J]. Journal on Communications, 2017, 38(4): 35-45.

[22] KASYOKA P, KIMWELE M, ANGOLO S M. Cryptanalysis of a pairing-free certificateless signcryption scheme[J]. ICT Express, 2021, 7(2): 200-204.

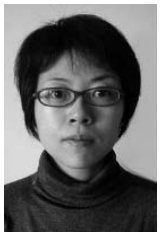
[23] QI Y F, TANG C M, LOU Y, et al. Certificateless proxy identity-based signcryption scheme without bilinear pairings[J]. China Communications, 2013, 10(11): 37-41.

[24] 方光伟. 一种可证安全无对运算的签密方案分析与改进[J]. 计算机应用研究, 2020, 37(11): 3422-3427.
FANG G W. Security analysis and improvement of provable security certificateless signcryption scheme[J]. Application Research of Computers, 2020, 37(11): 3422-3427.

[25] KARATI A, FAN C N, HUANG J J. An efficient pairing-free certificateless signcryption without secure channel communication during secret key issuance[J]. Procedia Computer Science, 2020, 171: 110-119.

[作者简介]

张文波（1983− ），男，山东聊城人，博士，西安邮电大学讲师，主要研究方向为物联网安全、隐私保护等。



黄文华（1980− ），女，江苏江阴人，西安邮电大学副教授、硕士生导师，主要研究方向为隐私保护、网络安全风险评估等。

冯景瑜（1984− ），男，甘肃陇南人，博士，西安邮电大学副教授、硕士生导师，主要研究方向为物联网安全、频谱共享和隐私保护等。