doi:10.11959/j.issn.1000-436x.2017227

基于非线性对的车联网无证书批量匿名认证方案研究

宋成，张明月，彭维平，贾宗璞，刘志中，闫玺玺
（河南理工大学计算机科学与技术学院，河南 焦作 454000）

摘 要：针对当前车联网中匿名认证的安全性与效率问题，提出一种基于非线性对的车联网无证书批量匿名认证方案。通过可信中心与车辆协同生成公私钥对和假名，摆脱了系统安全对防篡改装置的依赖。分析表明，该方案能够实现可认证性、匿名性、可追踪性、不可链接性、前向与后向安全性等多种安全性能，并在随机预言模型下证实了该方案能够抵抗 Type I 与 Type II 攻击；该方案采用无证书的认证方式，有效减轻了系统存储负载，同时方案在非线性对运算基础上，实现消息的批量认证，有效提高了认证效率。因此，该方案在资源受限的物联网或嵌入式环境中，有着重要的理论意义与应用价值。

关键词：车载自组网；非线性对；无证书；匿名认证；随机预言模型
中图分类号：TP393 **文献标识码**：A

Research on pairing-free certificateless batch anonymous authentication scheme for VANET

SONG Cheng, ZHANG Ming-yue, PENG Wei-ping, JIA Zong-pu, LIU Zhi-zhong, YAN Xi-xi
(School of Computer Science and Technology, Henan Polytechnic University, Jiaozuo 454000, China)

Abstract: To solve the problem of security and efficiency of anonymous authentication in vehicular ad hoc network, a pairing-free certificateless batch anonymous authentication scheme was proposed. The public and private keys and pseudonyms were jointly generated by the trusted third party and vehicle, so the system security didn't depend on the tamper device. The scheme can realize authentication, anonymity, traceability, unforgeability, forward or backward security, and so on. Furthermore, under the random oracle model, the scheme can resist Type I and Type II attacks. Because there is no need to use certificates during authentication, the system storage load is effectively reduced. At the same time, the scheme realizes the batch message authentication on the basis of pairing-free operation, so the authentication efficiency is improved. Therefore, the scheme has important theoretical significance and application value in the resource-limited internet of things or embedded environment.

Key words: vehicular ad hoc network, pairing-free, certificateless, anonymous authentication, random oracle model

1 引言

随着车辆在现代社会的普及，停车难、交通拥堵、交通事故等一系列交通相关问题频频发生。交通管理、安全驾驶和交通信息交互等问题越来越受到人们的关注。近年来，在车辆管理方面，智能交通系统[1]（ITS）在国内外得到广泛的应用。为了构建下一代交通系统，基于移动 ad hoc 网络（MANET）[2]的车辆 ad hoc 网络[3]（VANET）得到企业和学术界的高度关注。在 VANET 中车辆能够与路侧单元进行通信进而获得实时的交通信息、天气信息、娱乐信息等，为人们提供了极大的便利。

然而，在 VANET 环境中存在一些安全威胁，一方面，VANET 的无线通信本质使数据极易被监

收稿日期：2017-05-17；**修回日期**：2017-09-09
通信作者：张明月，zhangmingyue0118@163.com
基金项目：国家自然科学基金资助项目（No.61300124, No.61300216）；河南省科技攻关计划基金资助项目（No.132102210123）
Foundation Items: The National Natural Science Foundation of China (No.61300124, No.61300216), The Science and Technology Research Program of Henan Province (No.132102210123)

测、篡改和伪造；另一方面，车辆通常位于开放的物理空间，隐私（如驾驶人的身份、车牌号、位置、行程）的泄露会给司机与乘客的生命与财产安全带来威胁。因此，VANET 环境中的数据安全与隐私保护问题[4]成为人们关注的焦点。匿名认证[5]是实现隐私保护的基本方法之一，然而，传统匿名认证算法设计复杂，计算量大，认证效率低。因此，在性能受限的 VANET 环境中，如何提高匿名认证的效率是当前人们研究的热点之一。

近年来，一些国内外学者针对 VANET 用户隐私保护问题做了大量的研究工作，并提出了一系列方案。Raya 等[6]首次提出一个基于别名证书的匿名认证协议，使用假名替代用户的真实身份实现用户的隐私保护。文献[7]提出了一个安全与隐私加强的批量认证协议 SPECS，该方案中，批量认证完成之后，任何 2 个车辆能够在无路侧单元（RSU）的参入下直接进行安全的通信。但 Horng 等[8]中证实 SPECS 方案存在伪装攻击的威胁。同时，在文献[8]中设计了一种新的批量匿名认证方案，RSU 为每辆车辆生成假名，通过假名进行通信，从而避免为每个车辆配备大量的公私钥对，但 RSU 的安全性难以得到保证。针对该问题，文献[9]中提出一种基于身份的匿名认证方案，将系统主密钥存储在车辆配备的防篡改装置中，车辆利用系统主密钥自己生成假名。文献[10]发现文献[9]方案的安全性过分依赖于防篡改装置，攻击者能够通过旁道攻击（如激光扫描与效率分析）获得隐秘信息。一旦防篡改装置中的系统主密钥遭到泄露，整个系统的安全将受到威胁。Wang 等[11]基于群签名提出了一种有效的身份隐私保护方案 ECPB，该方案中所有成员在加入群组之前需进行身份验证，并能实现批量认证。文献[12]采用非对称加密技术提出了一种基于身份的批量认证方案，每个消息的签名过程中使用的假名都是不同的，且能够实现可追踪性。Shao 等[13]基于群签名提出了一个能够实现批量认证的门限匿名认证协议，Lu 等[14]提出的方案 SPRING ，使用频繁更换的假名来保护用户的隐私，在可信认证中心（TA）的参与下提高认证效率。

为了进一步加强安全、提高效率，本文提出一种基于非线性对的车联网无证书批量匿名认证方案。该方案未涉及 PKI 证书，从而减少了系统车辆存储负担；通过分布式的方式生成系统公私钥对，且方案中未涉及计算复杂的双线性对运算，有效提高了认证效率。

2 VANET 网络模型

与传统的互联网不同，VANET 主要采用无线的通信方式，通信实体为车辆。系统模型包括 3 个部分：可信认证中心 TA、路侧单元 RSU 和车辆单元 OBU。通信方式主要有 2 种：车辆与路边单元 RSU 之间的通信和车辆与车辆之间的通信。VANET 网络模型如图 1 所示。

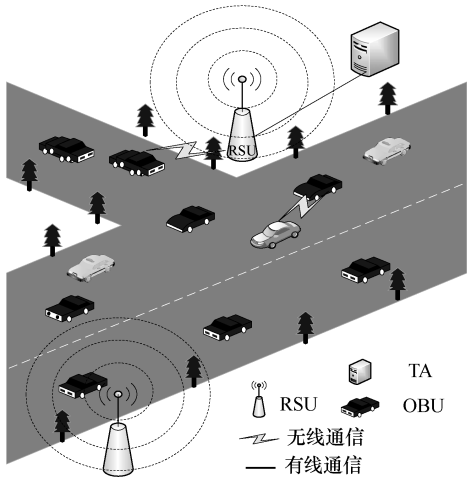

图 1 VANET 网络模型

1) TA

为了保证系统有条不紊的运行，通常需要一个可信的服务器 TA，负责存储所有认证的车辆用户的隐私信息，为系统生成公私钥对和系统参数。TA 通常为汽车制造商或交通管理部门。

2) RSU

RSU 是安装在道路两侧的基础设施，能够通过无线与车辆通信，类似无线传感网络的接入节点。RSU 与车辆之间使用 DSRC 协议[15]进行通信，通过该协议，RSU 能够对车辆发送的请求信息进行验证。

3) OBU

在 VANET 中每个车辆都配备了无线通信模块 OBU，通过 OBU 车辆能够与 RSU 或其他配备 OBU 的车辆进行通信，进而获得相应的服务。

3 本文方案

本文方案包括 4 个阶段：初始化阶段、密钥生成阶段、签名阶段和认证阶段。

3.1　初始化阶段

l 为 TA 的一个安全参数，TA 随机选择素数 p 和 q，满足 $q \mid p-1$，然后随机选取 g 属于有限域 Z_p^*（$g \neq 1$ 且 $g^q = 1 \bmod p$），x 属于有限域 Z_q^*，计算 $y = g^x \bmod p$。x 为系统的主密钥，$P_{\text{pub}} = y$ 作为 x 对应的公钥。选择 3 个散列函数：$H: \{0,1\}^* \to Z_q^*$，$H_1: \{0,1\}^* \to Z_q^*$，$H_2: \{0,1\}^* \to Z_q^*$，则系统公钥为 $(p, q, g, P_{\text{pub}}, H, H_1, H_2)$。

3.2　密钥生成阶段

Step1　设 ID_i 为车辆用户 V_i 的身份，V_i 随机选择 $(b_i, v_i) \in Z_q^*$，然后计算

$$B_i = g^{v_i} \bmod p \tag{1}$$

$$PID_{i_1} = b_i p \tag{2}$$

并将 (ID_i, PID_{i_1}, B_i) 通过安全信道发送给 TA。

Step2　TA 收到信息后，随机选择 $r \in Z_q^*$，计算部分公钥 PP_i 为

$$PP_i = g^r \bmod p \tag{3}$$

然后计算

$$PID_{i_2} = ID_i \oplus H(xPID_{i_1} \| PID_{i_1} \| t_1 \| P_{\text{pub}}) \tag{4}$$

假名 $PID_i = (PID_{i_1}, PID_{i_2}, t_1)$，其中，$t_1$ 为假名的有效时间。然后计算

$$s_i = H_1(PID_i \| B_i \| PP_i) \tag{5}$$

部分私钥为

$$PS_i = r - xs_i \bmod p \tag{6}$$

然后将 (PID_i, PP_i, PS_i) 发送给 V_i。

Step3　V_i 收到消息后，验证 $g^{PS_i} P_{\text{pub}}^{s_i} = PP_i \bmod p$ 是否成立，若成立，则执行 Step 4；否则，终止执行。

Step4　V_i 将

$$SK_i = V_i - PS_i \tag{7}$$

作为自身的私钥。令 $PK_{i_1} = B_i$，$PK_{i_2} = PP_i$，公钥为 $PK_i = (PK_{i_1}, PK_{i_2})$。

3.3　签名阶段

签名阶段指 V_i 对消息 m 进行签名。V_i 随机选择 $k \in Z_q^*$，计算

$$h_i = g^k \bmod p \tag{8}$$

$$u_i = H_2(PID_i \| m \| h_i) \tag{9}$$

$$e_i = k - SK_i u_i \bmod q \tag{10}$$

将 $\delta_i = (h_i, u_i, e_i)$ 作为 V_i 对消息 m 的签名，然后发送 (δ_i, m, PID_i) 给 RSU 或需要通信的车辆。

3.4　认证阶段

3.4.1　单车辆认证

单车辆认证指单个车辆请求 RSU 或其他车辆进行认证。当 RSU 或车辆收到需要认证的车辆 V_i 的消息签名 (δ_i, m, PID_i) 之后，首先，验证 t_1 的有效性，然后计算

$$s_i' = H_1(PID_i \| PK_{i_1} \| PK_{i_2}) \tag{11}$$

$$u_i' = H_2(PID_i \| m \| h_i) \tag{12}$$

令

$$\left(\frac{PK_{i_1} P_{\text{pub}}^{s_i'}}{PK_{i_2}} \right)^{u_i'} = \frac{h_i}{g^{e_i}} \bmod p \tag{13}$$

若式(13)成立，则验证通过，否则，拒绝接收该消息。

3.4.2　批量认证

设 n 个批量认证消息为 $(\delta_1, m_1, PID_1), (\delta_2, m_2, PID_2), \cdots, (\delta_n, m_n, PID_n)$，其中，$\delta_i = (h_i, u_i, e_i)$，$PID_i = (PID_{i_1}, PID_{i_2}, t_1)$，$i$=1,⋯,$n$。根据签名消息的来源不同，将批量认证分为 3 种类型。

1) 认证同一车辆的不同消息，即 n 个认证消息中，所有的 PID_i 是相同的。

2) 认证不同车辆的同一消息，即 n 个认证消息中，所有的 m 是相同的。

3) 认证不同车辆的不同消息。

无论消息来源于何种类型，均采用通用的认证方法。

当 RSU 或车辆收到批量认证消息后，RSU 或车辆首先针对每一认证消息 (δ_i, m_i, PID_i) 分别计算 $s_i' = H_1(PID_i \| PK_{i_1} \| PK_{i_2})$，$u_i' = H_2(PID_i \| m_i \| h_i)$。然后验证

$$(P_{\text{pub}})^{\sum_{i=1}^{n} s_i' u_i'} = \prod_{i=1}^{n} \left(\frac{h_i}{g^{e_i}} \left(\frac{PK_{i_2}}{PK_{i_1}} \right)^{u_i'} \right) \bmod p \tag{14}$$

如果式(14)成立，则认证通过；否则，终止。

如果消息来源为第一种类型，即认证消息来自与同一车辆，n 个认证的消息中的 PID_i 是相同的，

即 PK_{i_1}、PK_{i_2} 是相同的，进而 s_i' 也是相同的，验证式可以简化为

$$\left(\frac{PK_{i_1}P_{\text{pub}}^{\ s_i'}}{PK_{i_2}}\right)^{\sum_{i=1}^{n}u_i'}=\prod_{i=1}^{n}\frac{h_i}{g^{e_i}}\bmod p \tag{15}$$

4 方案分析

4.1 安全性分析

4.1.1 匿名性

方案中每个假名 PID_i 的生成过程中，用户随机选择的秘密值 b_i 和系统主密钥 x 均作为其输入参数。其中，秘密值 b_i 为车辆用户私有，系统主密钥 x 为 TA 私有，基于离散对数安全假设，攻击者无法知晓 x。因此，攻击者无法通过假名 PID_i 得到 V_i 的任何身份信息。

4.1.2 可追踪性

若某个车辆用户传递非正常信息，尽管其通过假名发布消息，TA 仍然能够对该恶意车辆进行追踪。由于 TA 拥有系统主密钥 x、系统公钥参数（包含 P_{pub}）和 $PID_i=(PID_{i_1},PID_{i_2},t_1)$，由 $PID_{i_2}=ID_i\oplus H(xPID_{i_1}\|PID_{i_1}\|t_1\|P_{\text{pub}})$ 可知，显然，$ID_i=PID_{i_2}\oplus H(xPID_{i_1}\|PID_{i_1}\|t_1\|P_{\text{pub}})$，因此，TA 可以通过计算得到 V_i 的真实身份 ID_i。

4.1.3 不可链接性

用户的不可链接性指的是攻击者不能够判断 2 个消息是否来自于同一车辆。通过链接游戏对本方案的不可链接性进行证明。本文方案记为 η，挑战者记为 A，B_0 与 B_1 表示 2 个忠实的车辆用户，签名者 RSU 记为 ζ。

定义 1 链接游戏

Step 1 挑战者由密钥生成算法 $KeyGen(k)$ 生成公私钥对 (SK,PK)，同时获得系统的公共参数 $(p,q,g,P_{\text{pub}},H,H_1,H_2)$。

Step 2 挑战者选取 2 个完全不同的消息 m_0、m_1。

Step 3 选取随机位 $b\in\{0,1\}$，然后，将 m_b 与 m_{1-b} 秘密发送给 B_0 与 B_1，b 对挑战者保密。

Step 4 签名者 ζ 分别与 B_0 与 B_1 执行本签名方案。

Step 5 B_0 与 B_1 输出 2 个有效的签名 δ_b 与 δ_{1-b} 分别与消息 m_0 与 m_1 相对应，然后，将 δ_b 与 δ_{1-b} 按照随机顺序发送给挑战者，否则，返回⊥给挑战者。

Step 6 挑战者猜测 δ_b 来自于 b'，如果 $b'=b$，则挑战者赢得这场游戏。

本文定义挑战者赢得游戏的优势为 $Adv_{\eta,\text{A}}^{\text{Link}}(\text{A})=|2\Pr[b'=b]-1|$，其中，$\Pr[b'=b]$ 表示 $b'=b$ 的概率。

定理 1 如果不存在挑战者 A 在多项式时间内以不可忽略的概率赢得该链接游戏，则称该方案满足不可链接性。

挑战者 A 如果在 Step5 中收到⊥，即 A 不能获得任何有用的信息，$b'=b$ 的概率为 $\frac{1}{2}$，这与抛硬币是等同的。

考虑另一种情况，假设攻击者 A 在执行完本方案的签名后得到了 2 个签名分别为 (δ_0,m_0,PID_0)、(δ_1,m_1,PID_1)。设 $j\in\{0,1\}$，j 表示该签名方案的一个实例，为了证明方案的不可链接性，对于 $(\delta_j,m_j,PID_j)\in\{(\delta_0,m_0,PID_0),(\delta_1,m_1,PID_1)\}$，在保证签名合法的情况下总能实现 $s_j'=H_1(PID_j\|PK_{j_1}\|PK_{j_2})$，$u_j'=H_2(PID_j\|m\|h_j)$，使 $\left(\frac{PK_{j_1}P_{\text{pub}}^{\ s_j'}}{PK_{j_2}}\right)^{u_j'}=\frac{h_j}{g^{e_j}}\bmod p$ 成立。所以挑战者是不能区别消息来自哪一个签名者，从而该方案能够满足不可链接性。

4.1.4 前向安全性与后向安全性

前向安全性与后向安全性保证车辆前后的认证信息不会相互影响。在本文方案中，若攻击者获得了签名消息 $\delta_i=(h_i,u_i,e_i)$，其中，$h_i=g^k\bmod p$，$u_i=H_2(PID_i\|m\|h_i)$，$e_i=k-SK_iu_i\bmod p$，k 具有随机性，每次签名所选择的 k 是不同的，因此，所有的签名不存在相关性，即攻击者无法通过当前的签名消息推断出之前或之后的签名消息。

4.1.5 抵抗 Type I 型攻击

Type I 型攻击是指外部攻击者能够替换合法用户的公钥。

定理 2 在基于离散对数安全性假设（DLP）前提下，所提方案能够在随机预言模型下实现存在性、不可伪造性以防止适应性选择消息攻击。

引理 1 如果 Type I 型攻击者 AI 能够通过 Game I 在 t 时间内向部分私钥提取预言机提出 q_{par} 查询，向公钥提取预言机发出 q_{pub} 查询，向公钥置换预言机提出 q_{pubr} 查询，向 H_1、H_2 随机预言机分

别提出 q_{H_1}、q_{H_2} 查询，并向签名预言机提出 q_{sig} 查询后以概率 ε 输出一个正确的签名，则存在一个算法 B 能够在

$$t < t' + (q_{\mathrm{pub}} + 3q_{\mathrm{pubr}} + 8q_{\mathrm{sig}})t_e + (2q_{\mathrm{pub}} + 3^{q_{\mathrm{pubr}}} + 6q_{\mathrm{sig}})t_m$$

时间内以概率

$$\varepsilon' > \left(\varepsilon - \frac{1}{2l}\right) \times \left(1 - \frac{1}{q_{\mathrm{par}}}\right)^{q_{\mathrm{par}}} \times \left(\frac{1}{2^{|p|}}\right)^{q_{\mathrm{pubr}}} \times \left(1 - \frac{1}{q_{\mathrm{par}}}\right)^{q_{\mathrm{pri}}} \times \frac{1}{q_{\mathrm{par}}}$$

解决 DLP 难题。其中，$|p|$ 表示位长，t_m 表示执行一次模乘运算所用的时间，t_e 表示的是一次模幂运算所用的时间。

下面通过随机预言模型证明存在一个算法 B 能够在 AI 的协助下解决 DLP 问题。

将一个 DLP 的随机挑战元组 (p,g,β) 作为算法 B 的输入参数，目标是输出 α，且满足 $g^{\alpha} = \beta \bmod p$，基于系统参数 $(p,q,g,P_{\mathrm{pub}},H,H_1,H_2)$，通过算法 B 对 AI 进行初始化，然后将 B 作为一个挑战者去完成 AI 的预言机询问。预言机查询阶段具体如下。

部分私钥提取查询。当 AI 以 PID_i 向此预言机进行询问时，B 通过列表 $L_{\mathrm{par}} = (PID_i, PS_i)$ 对 AI 与 B 之间的问答进行记录。如果 B 在 L_{par} 中查询到对应的 (PID_i, PS_i)，B 将 PS_i 返回给 AI，否则，B 随机选择 $c \in [1, q_{\mathrm{par}}]$ 。

1) 若 $i \neq c$，B 随机选择 $PS_i \in Z_q^*$，并将 PS_i 发送给 AI，然后将 (PID_i, PS_i) 保存到列表 L_{par} 中。

2) 若 $i = c$，B 令 $PID_i = PID^*$，输出“failure”并终止。

公钥提取查询。当 AI 以 PID_i 向此预言机进行询问时，挑战者通过列表 $L_{\mathrm{pub}} = (PID_i, PK_{i_1}, PK_{i_2}, s_i, v_i)$ 对 AI 与 B 之间的问答进行记录。如果 B 在 L_{pub} 中查询到对应的 $(PID_i, PK_{i_1}, PK_{i_2}, s_i, v_i)$ ，则 B 将 (PK_{i_1}, PK_{i_2}) 传送给 AI。否则，有以下 2 种情况。

1) 若 $PID_i = PID^*$，B 随机选择 $PK_{i_2} \in Z_p^*$ 计算 $s_i \in Z_p^*$，$PK_{i_1} = PK_{i_2} \beta^{-1} P_{\mathrm{pub}}^{-s_i} \bmod p$ ，将 (PK_{i_1}, PK_{i_2}) 发送给 AI，将 $(PID_i, PK_{i_1}, PK_{i_2}, s_i, \perp)$ 保存在列表 L_{pub} 中。

2) 若 $PID_i \neq PID^*$，B 通过 L_{par} 恢复出 (PID_i, PS_i)，如果 B 发现 (PID_i, PS_i) 不在 L_{par} 中，B 通过执行私钥提取查询得到新的 PS_i，然后 B 随机选择 $s_i \in Z_p^*$，$v_i \in Z_p^*$，计算 $PK_{i_2} = g^{PS_i} P_{\mathrm{pub}}^{s_i} \bmod p$，$PK_{i_1} = g^{v_i} \bmod p$ ，并将 (PK_{i_1}, PK_{i_2}) 发送给 AI，最后将 (PID_i, PS_i) 与 $(PID_i, PK_{i_1}, PK_{i_2}, s_i, v_i)$ 分别保存到列表 L_{par} 与 L_{pub} 中。

公钥替换查询。当 AI 以元组 $(PID_i, \widetilde{PK_{i_1}}, \widetilde{PK_{i_2}})$ 向公钥替换预言机进行查询，B 将从 L_{par} 恢复出 (PID_i, PS_i)，如果 B 没有从 L_{par} 中找到 (PID_i, PS_i)，B 执行私钥提取查询得到新的 PS_i，随后 B 验证等式 $g^{PS_i} P_{\mathrm{pub}}^{H_1(PID_i \| \widetilde{PK_{i_1}} \| \widetilde{PK_{i_2}})} = PK_{i_2} \bmod p$ 是否成立。若等式成立，B 输出“failure”并停止工作，否则，B 继续执行以下 2 个步骤。

1) 若 B 能够在 L_{pub} 列表中查询到 $(PID_i, PK_{i_1}, PK_{i_2}, s_i, v_i)$ ，B 令 $PK_{i_1} = \widetilde{PK_{i_1}}$ ，$PK_{i_2} = \widetilde{PK_{i_2}}$，然后将 $(PID_i, \widetilde{PK_{i_1}}, \widetilde{PK_{i_2}}, \perp, \perp)$ 保存在列表 L_{pub} 中。

2) 否则，B 以 PID_i 为输入执行公钥提取查询得到新的 PK_{i_1} 与 PK_{i_2}，然后令 $PK_{i_1} = \widetilde{PK_{i_1}}$ ，$PK_{i_2} = \widetilde{PK_{i_2}}$ ，并将 $(PID_i, \widetilde{PK_{i_1}}, \widetilde{PK_{i_2}}, \perp, \perp)$ 保存在列表 L_{pub} 中。

H_1 查询。当 AI 以 (PID_i, B_i, PP_i) 作为输入进行 H_1 查询，这里假定 AI 已经进行了公钥提取查询得到了 B_i 和 PP_i，即 PK_{i_1} 与 PK_{i_2}。因此，B 将在 L_{pub} 中查找对应的 $(PID_i, PK_{i_1}, PK_{i_2}, s_i, v_i)$，将 s_i 返回给 AI。

H_2 查询。当 AI 以 (PID_i, m_i, h_i) 作为输入进行 H_2 查询，B 用 (PID_i, m_i, u_i, h_i) 形式的列表 L_2 对 AI 与 B 之间的问答进行记录。如果 B 能够在 L_2 中查找到相应的 (PID_i, m_i, u_i, h_i)，则 B 将 u_i 返回给 AI。否则 B 随机选择 $u_i \in Z_q^*$ ，然后将 u_i 返回给 AI，并将 (PID_i, m_i, u_i, h_i) 存储在列表 L_2 中。

部分私钥提取查询。当 AI 以 PID_i 作为输入对此预言机进行查询时。

1) 若 $PID_i \neq PID^*$，B 输出“failure”并停止工作。

2) 否则，B 分别从 L_{par} 与 L_{pub} 中提取出相应的 (PID_i, PS_i) 与 $(PID_i, PK_{i_1}, PK_{i_2}, s_i, v_i)$，如果在 L_{par} 与 L_{pub} 中没有查找到对应的信息，B 将以 PID_i 作为输入分别执行部分私钥提取查询与公钥提取查询得到新的 PS_i 与 v_i，随后 B 将 $v_i - PS_i$ 传输给 AI，并将

(PID_i, PS_i) 与 $(PID_i, PK_{i_1}, PK_{i_2}, s_i, v_i)$ 分别存储在 L_{par} 与 L_{pub} 中。

签名查询。AI 以 (PID_i, m_i) 作为输入进行 H_2 查询，假定 PID_i 已经执行过询问。

1) 若 $PID_i \neq PID^*$，B 输出消息 m_i 对应的签名 δ_i，并将 δ_i 传送给 AI。

2) 否则，B 随机选择 $e_i, u_i \in Z_q^*$，在列表 L_{pub} 中恢复出相应的 $(PID_i, PK_{i_1}, PK_{i_2}, s_i, v_i)$ 并计算 $h_i = g^{e_i} PK_{i_1}^{u_i} P_{\text{pub}}^{s_i u_i} PK_{i_2}^{-u_i}$。$\delta_i = (u_i, h_i, e_i)$ 表示签名者 PID_i 对消息 m_i 的一个正确的签名。B 将 δ_i 返回给 AI 并将 (PID_i, m_i, u_i, h_i) 存储在 L_2 中。如果 (PID_i, m_i, h_i) 已经在 L_2 中被记录或者 PK_{i_1} 与 PK_{i_2} 已经被替换，B 将输出“failure”并停止模拟。

伪造。AI 停止查询并输出 $(\widehat{PID}, \widehat{m})$ 对应的正确签名 $(\hat{u}, \hat{h}, \hat{e})$。若 $\widehat{PID_i} \neq PID^*$，B 将输出“failure”并停止模拟。否则，B 通过相同方法重新运行，但 H_2 每次查询阶段的选择是不同的。B 能够得到另一个正确的签名 $(\hat{u}', \hat{h}', \hat{e}')$，并且这 2 个签名都要满足

$$g^{\hat{e}} PK_{i_1^*}^{\hat{u}} P_{\text{pub}}^{s\hat{u}} = \hat{h} PK_{i_2^*}^{\hat{u}} \text{ 与 } g^{\hat{e}'} PK_{i_1^*}^{\hat{u}'} P_{\text{pub}}^{s\hat{u}'} = \hat{h} PK_{i_2^*}^{\hat{u}'}$$

因此，B 能得到以下关系 $g^{\hat{e}-\hat{e}'} = \beta^{\hat{u}-\hat{u}'} \Leftrightarrow \log_g \beta = \dfrac{\hat{e}-\hat{e}'}{\hat{u}-\hat{u}'}$，则通过 $\dfrac{\hat{e}-\hat{e}'}{\hat{u}-\hat{u}'}$ 可以看出，B 能够解决 DLP 难题。

概率分析。下面将分析 B 赢得游戏的概率。由于 H_2 是一个随机查询预言机，AI 在没有进行 $H_2(\widehat{PID} \| \widehat{m} \| \hat{h})$ 询问的情况下生成 $(\widehat{PID}, \widehat{m})$ 对应的正确签名的概率至少为 $\dfrac{1}{2^l}$。在部分私钥提取询问阶段 B 没有停止模拟的概率为 $\left(1-\dfrac{1}{q_{\text{par}}}\right)^{q_{\text{pubr}}}$。在公钥置换阶段 B 没有停止模拟的概率为 $\left(1-\dfrac{1}{q_{\text{par}}}\right)^{q_{\text{pri}}}$。在 DLP 计算阶段 B 继续正常运行的概率为 $\dfrac{1}{q_{\text{par}}}$。因此，B 赢得游戏的概率至少为

$$\left(\varepsilon-\frac{1}{2l}\right)\times\left(1-\frac{1}{q_{\text{par}}}\right)^{q_{\text{par}}}\times\left(\frac{1}{2^{|p|}}\right)^{q_{\text{pubr}}}\times\left(1-\frac{1}{q_{\text{par}}}\right)^{q_{\text{pri}}}\times\frac{1}{q_{\text{par}}}$$

B 操作的时间最多为

$$t + (q_{\text{pub}} + 3q_{\text{pubr}} + 8q_{\text{sig}})t_e + (2q_{\text{pub}} + 3^{q_{\text{pubr}}} + 6q_{\text{sig}})t_m$$

4.1.6 抵抗 Type II 型攻击

Type II 型攻击者指能够获得系统主密钥的内部攻击者。

引理 2 如果 Type II 型攻击者 AII 能够通过 Game II 在 t' 内向部分私钥提取预言机提出 q_{par} 查询，向公钥提取预言机发出 q_{pub} 查询，向 H_1、H_2 随机预言机分别提出 q_{H_1}、q_{H_2} 查询，向私钥提取预言机发出 q_{pri} 查询，并向签名预言机提出 q_{sig} 查询后以概率 ε 输出一个正确的签名，则存在一个算法 B 能够在 $t' < t + (3q_{\text{pub}} + 8q_{\text{sig}})t_e + (3q_{\text{pub}} + 6q_{\text{sig}})t_m$ 时间内，以概率 $\varepsilon' > \left(\varepsilon - \dfrac{1}{2l}\right) \times \left(1 - \dfrac{1}{q_{\text{pub}}}\right)^{q_{\text{pri}}} \times \dfrac{1}{q_{\text{par}}}$ 解决 DLP 难题。其中，t_m 指执行一次模乘运算所用的时间，t_e 指的是一次模幂运算所用的时间。

下面，在随机预言模型下证明存在一个算法 B 能够在 AII 的协助下解决 DLP 问题。具体证明过程如下。

将一个 DLP 的随机挑战元组 (p, g, β) 作为算法 B 的输入，目标是输出 α，且满足 $g^\alpha = \beta \bmod p$，基于系统公开参数 $(p, q, g, p_{\text{pub}}, H_1, H_2)$ 和系统主密钥 x，通过算法 B 对 AII 进行初始化，然后将 B 作为一个挑战者去完成 AII 的预言机询问。预言机查询阶段具体如下。

公钥提取查询。当 AII 以 PID_i 向此预言机进行询问时，B 通过列表 $L_{\text{pub}} = (PID_i, PK_{i_1}, PK_{i_2}, PS_i, s_i, v_i)$ 对 AII 与 B 之间的问答进行记录。如果 B 在 L_{pub} 中查询到相应的 $(PID_i, PK_{i_1}, PK_{i_2}, PS_i, s_i, v_i)$，B 将 (PK_{i_1}, PK_{i_2}) 返回给 AII，否则，B 随机选择 $c \in [1, q_{\text{par}}]$。

1) 若 $i \neq c$，B 随机选择 $PS_i \in Z_q^*$，$s_i \in Z_p^*$，$v_i \in Z_p^*$，计算 $PK_{i_2} = g^{PS_i} P_{\text{pub}}^{s_i} \bmod p$，$PK_{i_1} = g^{v_i} \bmod p$，并将 (PK_{i_1}, PK_{i_2}) 发送给 AII，最后将 $(PID_i, PK_{i_1}, PK_{i_2}, PS_i, s_i, v_i)$ 保存在列表 L_{pub} 中。

2) 若 $i = c$，B 令 $PID_i = PID^*$，然后随机选择 $PS_i \in Z_q^*$，$s_i \in Z_p^*$，$v_i \in Z_p^*$，计算 $PK_{i_2} = g^{PS_i} P_{\text{pub}}^{s_i} \bmod p$，$PK_{i_1} = PK_{i_2} \beta^{-1} P_{\text{pub}}^{-s_i} \bmod p$，并将 (PK_{i_1}, PK_{i_2}) 传送给 AII，然后将 $(PID_i, PK_{i_1}, PK_{i_2}, PS_i, s_i, v_i)$ 保存

表 1　　**安全性能比较**

方案	可认证性	匿名性	不可链接性	前向安全性	后向安全性	可追踪性	Type Ⅰ	Type Ⅱ
文献[11]方案	√	√		√	√	√		
文献[12]方案	√	√				√		
文献[13]方案	√	√				√		
文献[14]方案	√	√				√		
文献[16]方案	√	√	√	√	√	√		
本文方案	√	√	√	√	√	√	√	√

到列表 L_{pub} 中。

H_1 查询。当 AII 以 (PID_i, B_i, PP_i) 作为输入进行 H_1 查询，这里，假定 AII 已经进行了公钥提取查询得到了 B_i 与 PP_i，即 PK_{i_1} 与 PK_{i_2}。因此，B 通过 L_{pub} 查询对应的 $(PID_i, PK_{i_1}, PK_{i_2}, PS_i, s_i, v_i)$，将 s_i 返回给 AII。

H_2 查询。当 AII 以 (PID_i, m_i, h_i) 作为输入进行 H_2 查询，B 以 (PID_i, m_i, u_i, h_i) 形式，通过列表 L_2 对 AI 与 B 之间的问答进行记录。如果 B 能够在 L_2 中查询到 (PID_i, m_i, u_i, h_i)，B 将 u_i 返回给 AII。否则，B 随机选择 $u_i \in Z_q^*$，然后将 u_i 返回给 AII，并将 (PID_i, m_i, u_i, h_i) 存储到列表 L_2 中。

私钥提取查询。当 AII 以 PID_i 向此预言机进行询问时，有以下 2 种情况。

1) 若 $PID_i = PID^*$，B 将输出“failure”并停止模拟。

2) 若 $PID_i \neq PID^*$，B 将从 L_{pub} 中查找对应的 $(PID_i, PK_{i_1}, PK_{i_2}, PS_i, s_i, v_i)$，如果 B 在 L_{pub} 中找不到对应的 $(PID_i, PK_{i_1}, PK_{i_2}, PS_i, s_i, v_i)$，B 以 PID_i 作为输入执行公钥提取查询得到新的 PS_i 与 v_i，之后将 $v_i - PS_i$ 发送送给 AII 并将 $(PID_i, PK_{i_1}, PK_{i_2}, PS_i, s_i, v_i)$ 保存到列表 L_{pub} 中。

签名查询。AII 以 (PID_i, m_i) 作为输入进行 H_2 查询，假定 PID_i 已经执行过询问。

1) 若 $PID_i \neq PID^*$，B 输出消息 m_i 相应的签名 δ_i，并将 δ_i 传送给 AII。

2) 否则，B 随机选择 $(e_i, u_i) \in Z_q^*$，在列表 L_{pub} 中恢复出相应的 $(PID_i, PK_{i_1}, PK_{i_2}, PS_i, s_i, v_i)$ 并计算 $h_i = g^{e_i} PK_{i_1}^{u_i} P_{\text{pub}}^{s_i u_i} PK_{i_2}^{-u_i} \bmod p$。$\delta_i = (u_i, h_i, e_i)$ 是签名者 PID_i 对消息 m_i 的一个正确的签名。B 将 δ_i 返回给 AII 并将 (PID_i, m_i, u_i, h_i) 存储到 L_2 中。注意到如果 (PID_i, m_i, h_i) 已经在 L_2 中被记录，B 将输出“failure”并停止模拟。

伪造与概率分析。在所有的询问都执行完之后，B 可以通过与引理 1 相似方法得到 $\dfrac{\hat{e}-\hat{e}'}{\hat{u}-\hat{u}'}$，从而能够解决 DLP 难题，并且，通过与引理 1 相同的方法得到 B 赢得游戏的概率至少为

$$\left(\varepsilon - \frac{1}{2l}\right) \times \left(1 - \frac{1}{q_{\text{par}}}\right)^{q_{\text{pri}}} \times \frac{1}{q_{\text{par}}}$$

B 的运行时间最多为

$$t + (3q_{\text{pub}} + 8q_{\text{sig}})t_e + (3q_{\text{pub}} + 6q_{\text{sig}})t_m$$

本文方案与现有方案的安全性能比较如表 1 所示。

4.2　效率分析

4.2.1　计算复杂度分析

为了便于方案计算复杂度的定性分析与比较，定义 T_{mul} 代表椭圆曲线上点乘运算，T_{par} 代表一次双线性对运算，T_{exp} 代表一次幂运算，T_{h} 代表一次 MapTopoint 散列函数运算。方案中其他的操作简单，运算时间极其微小，忽略不计。本文方案认证过程所消耗的时间与相关方案所消耗的时间对比结果如表 2 所示。

表 2　　**计算复杂度比较**

方案	认证一个消息	认证 n 个消息
文献[11]方案	$12T_{\text{exp}} + 5T_{\text{par}}$	$13nT_{\text{exp}} + 2T_{\text{par}}$
文献[12]方案	$T_{\text{mul}} + 2T_{\text{par}} + T_h$	$nT_{\text{mul}} + 2T_{\text{par}} + nT_h$
文献[13]方案	$4T_{\text{exp}} + 10T_{\text{par}}$	$4nT_{\text{exp}} + (n+6)T_{\text{par}}$
文献[14]方案	$11T_{\text{mul}} + 3T_{\text{par}}$	$11nT_{\text{mul}} + 3nT_{\text{par}}$
文献[16]方案	$2T_{\text{par}} + 5T_{\text{exp}}$	$(n+1)T_{\text{par}} + (4+n)T_{\text{exp}}$
本文方案	$6T_{\text{exp}}$	$(2n+4)T_{\text{exp}}$

如表 2 所示，无论是单个消息认证还是批量消息认证，本文方案均不存在计算复杂度较大的

双线性对运算，仅用到计算复杂度相对较小的幂运算。在文献[16]的实验中，选用 2 GHz CPU 4 GB RAM 处理器，在 100 个随机模拟运行中进行分析，得到平均结果 T_{exp} 运算时间为 0.6 ms，T_{par} 为 1.6 ms，T_{mul} 为 0.6 ms，T_h 为 2.7 ms。本文方案完成一个消息的认证过程仅需要 6 个 T_{exp} 运算，所需要的时间为 3.6 ms，其他所列方案使用的时间分别为 11 ms、6.5 ms、13.6 ms、6.2 ms、11.4 ms。因此，与其他方案相比，本文方案具有较低的运算成本，在同一时间段内，能够验证更多的消息。

图 2 显示了本文方案与对比方案在认证过程中批量认证的消息个数与所消耗的时间的关系。能够直观看到，随着 n 的增大，相比其他方案，本文方案更加高效。当需要认证的车辆达到 100 时，本文方案验证时间仅需要 100 ms 左右，其他方案都需要超过 200 ms。

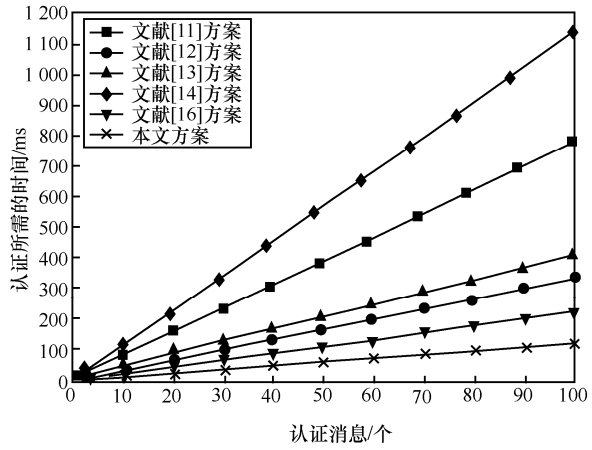

图 2 计算复杂度比较

因此，无论是单个消息认证还是批量消息认证，本文方案都具有一定的优势。

4.2.2 通信复杂度分析

通信复杂度是指通信过程所需的比特数。车联网认证方案中一次完整验证的通信开销通常主要由身份信息、签名、消息本身等组成。

设定原始消息的大小为 20 B，其中，文献[11]方案中消息的签名大小为 220 B，时间戳为 4 B，ID 所占空间为 2 B。在文献[12]中，传输数据分组中所包含的数据所占空间分别为：原始消息 20 B，签名 60 B，假名 40 B，时间戳 4 B，ID 所占空间为 4 B。文献[13]中，原始消息为 20 B，签名所占空间为 826 B，时间戳为 4 B，ID 所占空间为 3 B。在文献[14]中，传输数据分组中所包含的数据所占空间分别为：签名为 40 B，证书为 121 B，匿名密钥为 26 B，ID 所占空间为 2 B；在文献[16]中，原始消息所占的空间为 20 B，签名的大小为 20 B，公钥的大小为 20 B，匿名认证证书所占的空间为 180 B。在本文方案中，原始消息为 20 B，签名为 60 B，假名为 41 B，如表 3 所示。

表 3 通信复杂度比较

方案	通信复杂度/B
文献[11]方案	220+4+2=226
文献[12]方案	20+60+40+4+4=128
文献[13]方案	20+826+4+3=853
文献[14]方案	40+121+26+2=189
文献[16]方案	20+20+20+180=240
本文方案	20+60+41=121

通过比较分析可以发现，本文方案在通信复杂度方面也存在一定的优势。

5 结束语

本文针对车载自组织网络隐私保护过程中匿名认证效率较低的问题，提出了一种无证书无双线性对运算的批量匿名认证方案。分析表明，本文方案在正确性的前提下不仅能够确保可认证性、不可链接性、匿名性，前向与后向安全性等多种安全性能；并在随机预言模型下证明了方案能够抵抗 Type I 与 Type II 攻击。该方案采用分布式的方式生成所需的公私钥，有效地解决了对车内防篡改装置的依赖性问题；采用无证书无双线性对运算的批量认证方式，计算与存储开销较低。这对于存储空间非常有限的车辆节点和高动态的车载网络来有着重要的理论意义与应用价值。

参考文献：

[1] GIOVANNA C, GIUSEPPE M, ANTONIO P, et al. Transport models and intelligent transportation system to support urban evacuation planning process[J]. IET Intelligent Transport Systems, 2016, 10(4): 279-286.

[2] RIZVI M, PASHA S, TAMRAKAR S. MANET parameter analysis and its impact on next generation network[C]//International Conference on Recent Trends in Computer Science and Electronics Engineering. 2017.

[3] CHOUHAN P, KAUSHAL G, PRAJAPAT U. Comparative STudy MANET and VANET[J]. International Journal of Advanced Trends in Computer Science & Engineering, 2016.

[4] DIEP P T N, YEO C K. A trust-privacy framework in vehicular ad hoc networks (VANET)[C] //Wireless Telecommunications Symposium (WTS). 2016: 1-7.

[5] 刘方斌, 张琨, 李海,等. 无可信中心的门限追踪 ad hoc 网络匿名认证[J]. 通信学报, 2012, 33(8):208-213.
LIU F B, ZHANG K, LI H, et al. Threshold traceability anonymous authentication scheme without trusted center for ad hoc network[J]. Journal on Communications, 2012, 33(8): 208-213.
[6] RAYA M, HUBAUX J P. Securing vehicular ad hoc networks[J]. Journal of Computer Security, 2007, 15(1): 39-68.
[7] CHIM T W, YIU S M, HUI L C K, et al. SPECS: secure and privacy enhancing communications schemes for VANETs[J]. Ad Hoc Networks, 2011, 9(2):189-203.
[8] HORNG S J, TZENG S F, PAN Y, et al. b-SPECS+: batch verification for secure pseudonymous authentication in VANET[J]. IEEE Transactions on Information Forensics & Security, 2013, 8(11): 1860-1875.
[9] HORNG S J, TZENG S F, LI T, et al. Enhancing security and privacy for identity-based batch verification scheme in VANET[J]. IEEE Transactions on Vehicular Technology, 2017, PP(99).
[10] MAHANTA H J, AZAD A K, KHAN A K. Differential power analysis: attacks and resisting techniques[M]// Information Systems Design and Intelligent Applications. Springer India, 2015:349-358.
[11] WANG Y, ZHONG H, XU Y, et al. ECPB: efficient conditional privacy-preserving authentication scheme supporting batch verification for VANETs[J]. International Journal of Network Security, 2016, 18(2): 374-382.
[12] SHIM K A. Reconstruction of a secure authentication scheme for vehicular ad hoc networks using a binary authentication tree[J]. IEEE Transactions on Wireless Communications, 2013, 12(11):5386-5393.
[13] SHAO J, LIN X, LU R, et al. A threshold anonymous authentication protocol for VANETs[J]. IEEE Transactions on Vehicular Technology, 2016, 65(3):1-1.
[14] LU R, LIN X, SHEN X. SPRING: a social-based privacy-preserving packet forwarding protocol for vehicular delay tolerant networks[C]// Conference on Information Communications. 2010:632-640.
[15] TONG Z, LU H, HAENGGI M, et al. A stochastic geometry approach to the modeling of DSRC for vehicular safety communication[J]. IEEE Transactions on Intelligent Transportation Systems, 2016, 17(5):1-11.
[16] AZEES M, VIJAYAKUMAR P, DEBOARH L J. EAAP: efficient anonymous authentication with conditional privacy-preserving scheme for vehicular ad hoc networks[J]. IEEE Transactions on Intelligent Transportation Systems, PP(99):1-10.

作者简介：

宋成（1980-），男，河南信阳人，博士，河南理工大学讲师，主要研究方向为信息安全、密码学、可信计算等。

张明月（1992-），女，河北沧州人，河南理工大学硕士生，主要研究方向为信息安全、物联网安全等。

彭维平（1979-），男，湖北天门人，博士，河南理工大学副教授，主要研究方向为物联网安全及应用、数据防泄露等。

贾宗璞（1963-），男，河南邓州人，博士，河南理工大学教授，主要研究方向为物联网技术与应用、计算机网络技术、计算机测控技术、信息系统等。

刘志中（1981-），男，河南周口人，博士，河南理工大学讲师，主要研究方向为服务计算、物联网、群体智能算法。

闫玺玺（1985-），女，河南灵宝人，博士，河南理工大学讲师、硕士生导师，主要研究方向为数字版权管理、数字内容安全、计算机网络安全。