doi:10.11959/j.issn.1000-436x.2017112

基于双线性对的车联网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 454003）

摘 要：为解决当前车联网中匿名认证的效率问题，利用椭圆曲线上的双线性对的性质，提出一种批量匿名认证方案。通过路侧单元节点（RSU）与车辆共同生成签名，有效减轻了 VANET 认证中心的负担进而提高认证效率，并且增加了攻击者提取密钥的难度，并在随机预言模型中给出其安全性证明。分析表明，该方案能够满足多种安全需求，计算开销明显降低，认证效率得到有效提高。因此，该方案在计算性能受限的物联网（IoT, Internet of things）环境中，有着重要的理论意义与应用价值。

关键词：双线性对；匿名认证；隐私保护；车联网；随机预言模型
中图分类号：TP393 **文献标识码**：A

Research on batch anonymous authentication scheme for VANET based on bilinear pairing

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 454003, China)

Abstract: To solve the problem of efficiency of anonymous authentication in vehicular ad hoc network, a batch anonymous authentication scheme was proposed by using bilinear pairing on elliptic curves . The signature was generated by the roadside unit node (RSU) and the vehicle together. Thus, the burden of VANET certification center was reduced and the authentication efficiency was proved. Meanwhile, the difficulty of the attacker to extract the key was increased. Furthermore, security proofs were given to the scheme in the random oracle model. Analysis shows that the proposed scheme can meet the needs of many kinds of security requirements, the computational overhead is significantly reduced, and the authentication efficiency is improved effectively too. Therefore, the scheme has important theoretical significance and application value under computational capability constrained Internet of things (IoT) environment.

Key words: bilinear pairing, anonymous authentication, privacy protection, vehicular network, 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、交通事故等一系列相关的交通问题频频发生。交通管理、安全驾驶和交通信息交换等问题越来越受到人们的关注。车辆自组织网络（VANET）作为智能交通系统的重要组成部分，是缓解和解决现有交通问题的关键。VANET 网络是一种节点为车辆的特殊移动自组织网络（MANET）[1]，车辆配备了车载单元（OBU, on board unit），通过无线通信设备实现车辆与车辆（V2V）以及车辆与路侧单元（RSU，road side unit）（V2I）相互交流。在 VANET 中车辆可以获得交通信息、娱乐信息，提高驾驶的安全性，进而提高驾驶体验。近年来，车辆自组织网络的许多应用与增值服务给人们带来了方便。

然而，VANET 面临着独特的安全挑战，一方面，VANET 无线通信的本质使数据极易被监测、改变和伪造；另一方面，车辆都位于开放的物理空间，隐私（如驾驶人的身份、车牌号、位置和行程）的泄露会给司机与乘客的生命与财产安全

收稿日期：2016-12-07；修回日期：2017-03-29
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)

带来威胁，因此，VANET 安全问题逐渐引起重视。VANET 用户隐私保护的最基本方法是用户身份匿名认证。传统的匿名身份认证算法复杂，计算量大，认证效率相对较低。然而，尽管相对于 MANET，VANET 中的车辆不受严格的能量、空间和计算能力限制[2,3]，但是，由于 VANET 中车辆的高动态性，即时通信体系与通信的安全性是目前 VANET 的重要需求。因此，通信开销是 VANET 匿名认证过程中必须考虑的问题，在确保安全的基础上提高匿名认证效率也是当前 VANET 面临的重要挑战之一。

到目前为止，许多学者已经提出了 VANET 匿名认证方案[4~6]，但它们大多数都是基于公钥基础设施（PKI, public key infrastructure）的传统数字签名技术来验证消息，这些协议的计算和存储开销大，对 VANET 性能要求较高。为了解决 VANET 中匿名认证方案通信与计算开销大的问题，近年来，批量认证的思想在 VANET 应用中引起了高度关注。研究者们提出了基于批量认证的方案提高认证效率。文献[7]提出了一种有效的批量验证方案，用于 RSU 与 OBU 之间通信，此方案能够实现 RSU 同时对多个车辆进行验证，总验证时间有所减少，但是该方案过分依赖于车辆的防篡改装置。SPECS 方案[8]介绍了一种安全与隐私加强的批量验证协议，在完成批量验证之后一车辆可以同任意车辆形成群组，并且可以在无 RSU 的参与下彼此之间进行安全通信。但文献[9]证实 SPECS 方案是不能抵抗伪装攻击的，并且攻击者可以伪装成合法车辆发布假消息甚至能假冒合法车辆与其他车辆进行安全通信。

针对现有方案存在的不足，本文利用椭圆曲线上的双线性对性质，提出一种改进的安全高效的车联网批量匿名认证方案。本文对方案的正确性、匿名性、抗中间人攻击、前向和后向私密性等相关安全性质进行了理论证明，并利用随机预言模型证明了其不可伪造性。最后，与现有方案执行效率的比较分析结果表明，本文方案具有更高的认证效率。

2 预备知识

2.1 VANET 网络模型

如图 1 所示，系统模型包括 3 个部分：可信服务中心（TA，trust agency）、路侧单元（RSU）和车载单元（OBU）。每部分的具体职责如下。

1) TA 可以是汽车制造商或运输管理部门，负责生成系统的全局安全参数并发布公共/私有密钥给所有参与者。

2) RSU 是安装在道路两侧的通信设备，类似于无线传感网络的接入节点。RSU 与车辆之间使用 DSRC 协议[10]进行通信。

3) 在 VANET 中，每个车辆都配备了 OBU，OBU 与 RSU 或其他 OBU 之间通过 DSRC 协议进行通信。

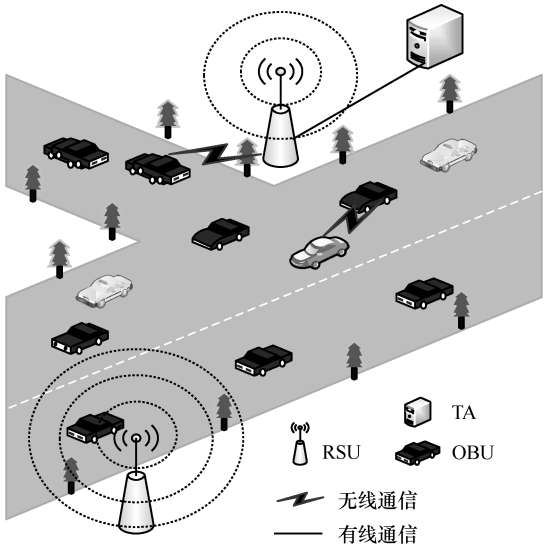

图 1 VANET 网络模型

2.2 双线性对

双线性对[11]理论是本文方案的基础。

设 G_1 是阶为素数 q 的加法循环群，G_2 是阶为素数 q 的乘法循环群，双线性对 $e:G_1\times G_1\to G_2$ 满足以下性质。

双线性：$\forall P,R,Q\in G_1,\forall a,b\in Z_q$，有

$$\begin{cases} e(aP,bQ)=e(P,Q)^{ab} \\ e(P,Q+R)=e(P,Q)e(P,R) \\ e(P+Q,R)=e(P,R)e(Q,R) \end{cases}$$

非退化性：$\exists P,Q\in G_1$，满足 $e(P,Q)\neq 1$。

可计算性：$\forall P,Q\in G_1$，存在算法能够在多项式时间内计算 $e(P,Q)$。

对称性：$\forall P,Q\in G_1, e(P,Q)=e(Q,P)$。

2.3 批量认证

假设方案中各步骤都正常进行，则对于 $i\in(1,n)$，有认证参数 $Verify(s_i,m_i,C_i)$，其中，s_i 为最终签名信息，m_i 为消息，C_i 为随机化参数，

则批量认证参数为 $BatchVerify((s_1,m_1,C_1),(s_2,m_2,C_2)\cdots(s_n,m_n,C_n))$。若 $Verify(s_i,m_i,C_i)=0$，则 $BatchVerify((s_1,m_1,C_1)(s_2,m_2,C_2)\cdots(s_n,m_n,C_n))=0$。即若 n 个签名中每个签名都合法，则批量验证通过；若此 n 个签名中有一个或多个签名不合法，则批量验证不通过。

文献[12]将批量验证分为 3 种类型。

类型 1：对同一用户的不同消息进行批量认证。

类型 2：对不同用户的同一消息进行批量认证。

类型 3：对不同用户的不同消息进行批量认证。

3　基于双线性对的匿名认证方案

针对车辆自组网的特点，为了满足 VANET 通信过程中的安全与隐私保护需求，本文基于椭圆曲线上双线性对的性质，设计了一种安全高效的车联网批量匿名认证方案。方案包括 5 个阶段：注册阶段、初始化阶段、签名阶段、验证阶段和更新阶段。

3.1　注册阶段

车辆节点 OBU 与路侧单元节点 RSU 在 TA 处进行注册登记，TA 为其颁发相应的认证信息，并生成系统参数。具体步骤如下。

Step 1　TA 随机生成一个 $m\times n$ 维的矩阵 $\boldsymbol{A}$ ($2\leqslant m<n$)和一个 m 维的列向量 $\boldsymbol{w}$，满足线性方程组 $\boldsymbol{Ad}=\boldsymbol{w}$ 有无穷多解，即系数矩阵 $\boldsymbol{A}$ 的秩等于增广矩阵 $\overline{\boldsymbol{A}}$ 的秩，$R(\boldsymbol{A})=R(\overline{\boldsymbol{A}})$ 且 $R(\boldsymbol{A})<n$。

Step 2　TA 为每个合法车辆节点生成唯一的 n 维列向量 $\boldsymbol{d}_i$，且 $\boldsymbol{d}_i$ 满足 $\boldsymbol{Ad}_i=\boldsymbol{w}$，即 $\boldsymbol{d}_i$ 为线性方程组 $\boldsymbol{Ad}=\boldsymbol{w}$ 的一个解。TA 将向量 $\boldsymbol{d}_i$ 发给相应的车辆节点 V_i 作为其真实身份信息，TA 随机选取一个 m 维列向量 $\boldsymbol{D}$，然后计算 V_i 的身份

$$ID_i=\boldsymbol{D}^{\mathrm{T}}\boldsymbol{d}_i \tag{1}$$

TA 将 $\boldsymbol{A}$、$\boldsymbol{D}$ 和 $\boldsymbol{w}$ 作为 RSU 与 TA 之间的共享秘密通过安全信道发送给 RSU。

Step 3　设 P 是群 G 的生成元，RSU 在素数模 q 的单位群、有限域 Z_q^* 中生成自身的私钥 x_1，并计算另一私钥 x_2

$$x_2=(\boldsymbol{D}^{\mathrm{T}}\boldsymbol{w})\bmod q \tag{2}$$

对应的公钥为 $PK_1=x_1P$、$PK_2=x_2P$，$H:\{0,1\}^*\rightarrow G_1$ 为单向散列函数。

Step 4　系统的公共参数为 $(q,H,G_1,G_2,e,P,PK_1,PK_2)$。

3.2　初始化阶段

初始化阶段，RSU 对车辆节点进行身份验证，为随后对车辆的消息签名做准备。具体步骤如下。

Step 1　当车辆 V_i 需要与其他车辆通信时，车辆向签名者 RSU 发送签名请求信号。

Step 2　当 RSU 收到车辆 V_i 发来的签名请求信号后，随机选择 $k\in Z_q^*$，计算认证参数 $\boldsymbol{R}$ 和 $\boldsymbol{s}$。

$$\boldsymbol{R}=k\boldsymbol{A} \tag{3}$$

$$\boldsymbol{s}=k\boldsymbol{w} \tag{4}$$

发送认证信息 $(t_1,\boldsymbol{R},H(\boldsymbol{s}\,\|\,ID_{R_p}\,\|\,t_1)$ 给车辆用户 V_i，其中，ID_{R_p} 是 RSU 的身份标识符，t_1 是与消息发送时间有关的时间数。

Step 3　V_i 收到 RSU 发来的消息，首先计算

$$\boldsymbol{r}=\boldsymbol{Rx}_i \tag{5}$$

然后验证 $h(\boldsymbol{r}\,||\,ID_{R_p}\,||\,t_1)=h(\boldsymbol{s}\,\|\,ID_{R_p}\,\|\,t_1)$ 是否成立，若相等，则发送 $(t_2,H(\boldsymbol{r}\,||\,ID_{R_p}\,||\,t_1\,\|\,t_2))$ 给 RSU，t_2 是与消息发送时间有关的时间数。

Step 4　RSU 收到消息后验证 $h(\boldsymbol{r}\,\|\,ID_{R_p}\,\|\,t_1\,\|\,t_2)=h(\boldsymbol{s}\,\|\,ID_{R_p}\,\|\,t_1\,\|\,t_2)$ 是否成立。验证成功则继续与 V_i 之间的通信。选取随机参数 $y_i\in Z_q^*$，并且计算 $\rho_i=y_iP$，将参数 ρ_i 发送给车辆用户。

在同一 RSU 的通信范围内，车辆首次与 RSU 通信时需要进行身份验证才能够完成之后的消息签名，此次认证是双向匿名认证。首次认证完成之后，当车辆与其他车辆进行通信需要 RSU 协助以生成签名时，车辆与 RSU 之间不再需要进行认证过程，减少了整个通信过程的通信与计算消耗。

3.3　签名阶段

在消息的签名阶段，RSU 与 OBU 共同生成用于车辆之间进行认证的消息签名。具体步骤如下。

Step 1　车辆 V_i 选取随机参数 u_i、r_{i1}、r_{i2}，设置随机化参数 $C_i=u_i\rho_i$、假名 $RID_i=ID_it_2$，计算中间参数

$$\beta_i=r_{i1}H(RID_i\,\|\,C_i\,\|\,M_i)+r_{i2}P \tag{6}$$

$$\gamma_i=r_{i1}u_i(\bmod q) \tag{7}$$

车辆用户将 (β_i,γ_i) 发送给签名者 RSU。

Step 2　签名者 RSU 在接收到 (β_i,γ_i) 之后，对其进行签名，计算签名

$$T_i=x_1\beta_i+x_2y\gamma_iP \tag{8}$$

然后发送给车辆用户。

Step 3 车辆用户收到签名者 RSU 发送来的签名 T_i，计算最终签名信息

$$S_i = r_{i1}^{-1}(T_i - r_{i2}PK_1) \tag{9}$$

获得签名者 RSU 对消息 M_i 的签名 $\sigma_i=(S_i,C_i,RID_i,M_i)$。签名阶段消息交互流程如图 2 所示。

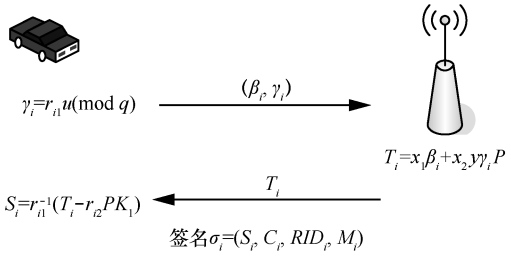

图 2 签名阶段消息交互流程

3.4 验证阶段

在验证阶段，车辆之间完成认证，分为单车辆验证和批量验证。

1) 单车辆验证

车辆用户将自己的签名 σ_i 发送给需要进行通信的车辆进行验证，计算

$$e(S_i,P)=e(H(RID_i\|C_i\|M_i),PK_1)e(C_i,PK_2) \tag{10}$$

若式(10)成立，验证通过，说明车辆身份是合法的，接收消息 M_i；否则，拒绝接收该消息。验证阶段消息交互流程如图 3 所示。

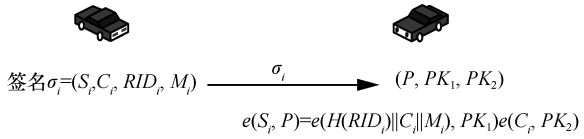

图 3 验证阶段消息交互流程

2) 批量验证

Fiat[13]基于 RSA 方案设计了一种批量验证方案，Harn[14]提出了基于 DSA 的批量验证方案。然而，以上 2 种方案都适用于类型 1。文献[12]基于离散对数的困难性问题提出的批量验证方案同样只适用于类型 1。

本文方案完全适用于批量验证所有类型。由于签名过程是由 RSU 与 V_i 共同完成，RID_i 是 V_i 随机生成的，C_i 是 RSU 生成的随机属性，S_i 是最终生成的签名，每次签名消息都会不同，不会因为车辆身份或消息的不同而影响验证等式关系的成立。具体认证过程如下。

V_j 接收到 $\sigma_1=(S_1,C_1,RID_1,M_1)$，$\sigma_2=(S_2,C_2,RID_2,M_2)$，…，$\sigma_i=(S_i,C_i,RID_i,M_i)$，…，$\sigma_n=(S_n,C_n,RID_n,M_n)$（其中，$M_1,M_2,\cdots,M_n$ 可能相同，也可能不同），有

$$e(\sum_{i=1}^{n}S_i,P)=e(\sum_{i=1}^{n}H(RID_i\|C_i\|M_i),PK_1)e(\sum_{i=1}^{n}C_i,PK_2) \tag{11}$$

若式(11)成立则接受该签名。

3.5 更新阶段

若有成员退出群组，则公钥 PK_2 将发生改变。已知

$$\begin{cases}\boldsymbol{Ad}_1=\boldsymbol{w}\\ \boldsymbol{Ad}_2=\boldsymbol{w}\\ \quad\vdots\\ \boldsymbol{Ad}_n=\boldsymbol{w}\end{cases} \tag{12}$$

当已知 $\boldsymbol{d}_1,\boldsymbol{d}_2,\cdots,\boldsymbol{d}_n$ 时，求新的 $\boldsymbol{A}$ 与 $\boldsymbol{w}$，$\boldsymbol{A}$ 是 $m\times n$ 阶矩阵，$\boldsymbol{w}$ 是 m 维列向量，所以有 $mn+m$ 个未知数，但只有 m 个等式，所以 $\boldsymbol{A}$ 与 $\boldsymbol{w}$ 不是唯一的，若有成员撤销或新成员加入，可以利用已有的车辆节点 $\boldsymbol{d}_i$，由注册服务器重新计算 $\boldsymbol{A}$ 与 $\boldsymbol{w}$。然后发送给 RSU，由 RSU 节点重新计算 PK_2，然后公布给群成员。当成员撤销以后，$e(S_i,P)=e(H(RID_i\|C_i\|M_i),PK_1)e(C_i,PK_2)$ 和 $e(\sum_{i=1}^{n}S_i,P)=e(\sum_{i=1}^{n}H(RID_i\|C_i\|M_i),PK_1)e(\sum_{i=1}^{n}C_i,PK_2)$ 中的 PK_2 都将进行更新，撤销用户的签名消息不能通过认证，并且撤销用户也不能完成对其他车辆的认证。更新阶段消息交互流程如图 4 所示。

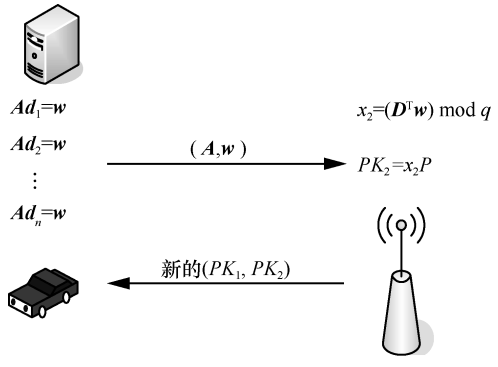

图 4 更新阶段消息交互流程

4 方案分析

下面，主要从方案的正确性、安全性和效率这

3 个方面进行分析。

4.1 正确性分析

证明过程包括单个认证的正确性与批量认证的正确性。

在单车辆验证过程中，通过验证式(10)是否成立来确定签名者的合法身份。因此，对于单车辆认证的正确性证明，通过验证等式 $e(S_i,P)=e(r_{i1}^{-1}(T_i-r_{i2}PK_1),P)$ 是否成立来实现。因为

$$\begin{aligned}e(S_i,P)&=e(r_{i1}^{-1}(x_1\beta_i+x_2y\lambda_iP-r_{i2}PK_1),P)\\&=e(x_1H(RID_i\|C_i\|M_i)+x_2yuP,P)\\&=e(x_1H(RID_i\|C_i\|M_i),P)e(x_2yuP,P)\\&=e(H(RID_i\|C_i\|M_i),x_1P)e(yuP,x_2P)\\&=e(H(RID_i\|C_i\|M_i),PK_1)e(C_i,PK_2)\end{aligned}\tag{13}$$

所以正确性成立。

在批量验证过程中，通过验证式(11)是否成立来确定签名的合法性。因此，对于批量认证的正确性证明，通过验证等式 $e(\sum_{i=1}^{n}S_i,P)=e(\sum_{i=1}^{n}H(RID_i\|C_i\|M_i),PK_1)e(\sum_{i=1}^{n}C_i,PK_2)$ 是否成立来实现，因为

$$\begin{aligned}e(\sum_{i=1}^{n}S_i,P)&=e(r_{i1}^{-1}(T_1-r_{i2}PK_1)+r_{i1}^{-1}(T_2-r_{i2}PK_1)+\cdots+\\&\quad r_{i1}^{-1}(T_n-r_{i2}PK_1),P)\\&=e(r_1^{-1}(x_1\beta_1+x_2y\lambda_1P-r_2PK_1)+\\&\quad r_1^{-1}(x_1\beta_2+x_2y\lambda_2P-r_2PK_1)+r_2PK_1)+\cdots+\\&\quad r_1^{-1}(x_1\beta_n+x_2y\lambda_nP-r_2PK_1),P)\\&=e(x_1H(RID_1\|C_1\|M_1)+\\&\quad x_1H(RID_2\|C_2\|M_2)+\cdots+\\&\quad x_1H(RID_n\|C_n\|M_n)+x_2y_1u_1P+\\&\quad x_2y_2u_2P+\cdots+x_2y_nu_nP,P)\\&=e(x_1\sum_{i=1}^{n}H(RID_i\|C_i\|M_i),P)e(\sum_{i=1}^{n}x_2y_iu_iP,P)\\&=e(\sum_{i=1}^{n}H(RID_i\|C_i\|M_i),x_1P)e(\sum_{i=1}^{n}y_iu_iP,x_2P)\\&=e(\sum_{i=1}^{n}H(RID_i\|C_i\|M_i),PK_1)e(\sum_{i=1}^{n}C_i,PK_2)\end{aligned}\tag{14}$$

所以正确性成立。

4.2 安全性分析

4.2.1 匿名性

本文的认证方案记为 η，攻击者记为 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　攻击者由密钥生成算法 $KeyGen(k)$ 生成公私钥对 (SK,PK)，同时获得系统的公共参数 $(q,H,G_1,G_2,e,P,PK_1,PK_2)$。

Step 2　攻击者选取 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 对于攻击者是不公开的。

Step 4　签名者 ζ 分别与 B_0 与 B_1 执行本文的签名方案。

Step 5　如果 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，则将 δ_b 与 δ_{1-b} 按照随机顺序发送给攻击者；否则，返回 $\perp$ 给攻击者。

Step 6　攻击者对 δ_b 的来源进行分析，输出 b 的一个猜想 b'，$b'\in\{0,1\}$，如果 $b'=b$，则攻击者赢得这场游戏。

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

定理 1　如果攻击者 A 使用签名方案在链接游戏中以不可忽略的概率赢得游戏，则该方案满足不可链接性即匿名性。

A 作为在定义 1 中链接游戏的攻击者，如果在 Step 5 中收到的是 $\perp$，那么说明 A 不能获得任何有用的信息，得到 b 的概率为 $\frac{1}{2}$，这与 b 的随机猜测是相同的。

考虑另一种情况，假设攻击者 A 在执行完本文方案的签名后得到了 2 个签名分别为 (S_0,C_0,RID_0,M_0) 和 (S_1,C_1,RID_1,M_1)。设 $j\in\{0,1\}$，j 表示该签名方案的一个实例，其中，$(y_jP,\beta_j,\gamma_j,T_j)$ 表示交互过程中的参数。为了证明方案的不可链接性，对于 $\{(S,C,RID,M)\}\in\{(S_0,C_0,RID_0,M_0),(S_1,C_1,RID_1,M_1)\}$ 和任意的 $(y_jP,\beta_j,\gamma_j,T_j)$，$j\in\{0,1\}$，总存在 (r'_{j_1},r'_{j_2},u'_j)，使 $C=u'_jy_jP$，$\beta_j=r'_{j1}H(RID_i\|C_i\|M_i)+r_{j2}P$，$\gamma_j=r'_{j1}u'_j(\text{mod}q)$，$T_j=x_1\beta_j+x_2y\gamma_jP$，可得

$$\begin{aligned}S_i&=r_{j_1}'^{-1}(T_j-r'_{j_2}PK_1)\\&=r_{j_1}'^{-1}(x_1\beta_j+x_2y_j\gamma_jP-r'_{j_2}PK_1)\\&=r_{j_1}'^{-1}(x_1r'_{j_1}H(RID_i\|C_i\|M_i)+x_2y_jr'_{j_1}u'_jP)\\&=x_1H(RID_i\|C_i\|M_i)+x_2y_ju'_jP)\\&=x_1H(RID_i\|C_i\|M_i)+x_2C\end{aligned}$$

因此

$$e(S,P)=e(r_{i1}^{-1}(x_1\beta_i+x_2y\lambda_iP-r_{i2}PK_1),P)$$
$$=e(x_1H(RID_i\|C_i\|M_i)+x_2yuP,P)$$

4.2.2 抵抗中间人攻击

在中间人攻击中，攻击者同时与相互通信的双方保持通信连接，并且使相互通信的双方相信彼此在一个安全的连接中进行信息交互，从而获得有用信息达到攻击目的。在本文方案中，RSU 与 V_i 每次通信过程中都会首先通过随机数建立链接。因为攻击者与 RSU、攻击者与 V_i 以及 RSU 与 V_i 之间建立的连接使用的随机数是不同的，所以攻击者无法通过中间人攻击与合法用户建立通信连接以达到攻击目的。

4.2.3 抵抗共谋攻击

1) n 个车辆共谋获取另一车辆的身份信息

假设 V_i 与同一有限域内的 n 个车辆进行了通信，这 n 个车辆都得到了 V_i 对消息的签名。依据实际情况共谋攻击可以分为 2 种。

情况 1 V_i 与每辆车传送的为同一消息。在这种情况下每个签名中的消息 M 是相同的，假设签名分别 (S_1,C_1,RID_1,M)，(S_2,C_2,RID_2,M)，$\cdots$，$(S_j,C_j,RID_j,M),\cdots,(S_n,C_n,RID_n,M)$，其中，$j\in 1,\cdots,n$ 指的是与车辆 $1,2,\cdots,n$ 的共 n 次通信，其中，$S_j=r_{j1}^{-1}(T_j-r_{j2}PK_1)$，$C_j=u_j\rho_j$。

由于 r_{j1}、r_{j2}、u_j 是车辆在每次签名过程中随机生成的参数，各个随机参数之间没有任何联系，并且，RSU 每次为车辆生成的 ρ_j 也是不同的，所以，根据各个车辆与 V_i 验证过程中生成的签名并不能得到任何有用信息，进而得知 V_i 的真实身份。

情况 2 V_i 与不同的车辆传送的是不同的消息。在这种情况下每个签名当中的消息 M 是不同的，假设签名分别为 (S_1,C_1,RID_1,M_1)，(S_2,C_2,RID_2,M_2)，$\cdots$，(S_j,C_j,RID_j,M_j)，$\cdots$，(S_n,C_n,RID_n,M_n)，其中，$j\in 1,\cdots,n$ 指的是与车辆 $1,\cdots,n$ 的共 n 次通信，$S_j=r_{j1}^{-1}(T_j-r_{j2}PK_1)$，$C_j=u_j\rho_j$。与情况 1 相同，由于签名的组成部分中每一部分的生成都有随机数的参与，并且随机数分别来源于 RSU 与 V_i，这保证了每次签名的随机性，即使将 n 个签名综合分析，即 n 个车辆进行共谋，也不能得到有用信息进而得到 V_i 的真实身份。

2) n 个 RSU 共谋以追踪车辆的真实身份

因为 V_i 与 RSU 的通信过程中始终传递的是 V_i 的临时身份公钥 RID_i，并且每次签名过程中 RID_i 都是随机生成的，通信参数中没有出现与车辆真实身份相关的任何信息，所以，即使 n 个 RSU 进行合谋也无从求解出车辆的真实身份。

综上，本匿名认证方案是可以抵抗共谋攻击的。

4.2.4 不可伪造性

随机预言模型[15]：满足下列性质的散列函数 $H:\{0,1\}^*\rightarrow\{0,1\}^n$ 称为随机预言机。

1) 均匀性。预言机的输出在 $\{0,1\}^n$ 上呈均匀分布。

2) 确定性。对于相同的输入，H 的输出值是相同的。

3) 有效性。给定一个输入 x，H 的计算可以在关于 x 长度的低阶多项式时间内完成。

利用随机预言机的以上 3 个性质证明密码体制的安全性模型被称为随机预言模型。

在随机预言模型中，如果攻击者能在多项式时间 t 内以不可忽略的概率 ε 伪造一个合法的签名，则存在一个多项式时间算法，能够解决 CDH 困难假设。

定义 2 多一伪造性[16]

存在一个签名方案，对于任意的整数 l，存在 $l=polynomial(k)$，其中，$polynomial$ 表示一个概率多项式随机算法 k 是一个安全参数，$(l,l+1)-$伪造指的是存在一个概率多项式时间算法能够在与签名者进行 l 次交互后，以不可忽略的概率计算出 $l+1$ 个有效的签名。

定义 3 选择目标的 CDH 假设[17]（chosen-target CDH 假设）

P 是阶为 q 的群 G 的生成元，给定攻击者 $A(P,aP)$，随机参数 $a\in Z_q$，并且 A 可以向以下 2 种预言机进行询问。

1) 目标预言机

① 在 G 上随机选择 Z。

② 将 Z 作为输出。

2) 帮助预言机

① 以给定的元素 $Z\in G$ 作为输入，计算 $V=aZ$。

② 将 V 作为输出。

经过 q_t 次目标询问与 q_h 次帮助询问，攻击者 A 输出 l 对元组 $\{(V_1,Z_1),(V_2,Z_2),\cdots,(V_l,Z_l)\}$，

$q_h < l \leqslant q_t$ 并且满足 $V_i = aZ_i$（q_h 与 q_t 分别表示对帮助预言机和目标预言机的询问次数），则 A 赢得游戏。

假设证明，不存在一个概率多项式时间算法能使 A 以不可忽略的概率解决 CDH 难题。

下面，将证明本文方案在选择目标的随机盲签名方案下是安全的。

证明　假设攻击者 A 能在本文方案中解决选择目标 CDH 假设难题，假设另一个攻击者 F 与 A 具有相同的能力，场景描述如下。

初始化阶段。设 $(q,H,G_1,G_2,e,P,Pub_1,Pub_2)$ 是本文方案的系统参数，$Pub_1 = aP$，(P,aP) 是选择目标 CDH 假设的一个攻击目标，并且，攻击者 F 拥有参数 x_2，且 $Pub_2 = x_2P$。攻击者 F 能够对选择目标 CDH 假设下的目标预言机 T_1 与帮助预言机 H_2 进行询问。

预言机查询阶段。F 能查询目标预言机获得随机参数 $Z \in G_1$，并且查询 H_2，通过输入 $Z \in G_1$，得到输出 aZ。随后将模拟 O_h 与 O_s 这 2 种预言机查询。

攻击者 A 进行 2 种查询，通过 O_h 进行散列查询，通过 O_s 进行签名查询，详细过程如下。

1) 检测 (m,RID,c)

检测是用来检查在列表 L_h 中是否存在一个前缀列表为 (m,RID,c) 作为输入的记录程序。

如果存在以 (m,RID,c) 为前缀列表则的记录，返回 1；否则，返回 0。

2) 查询 O_h

攻击者 A 向预言机 O_h 查询 (m,RID,c) 的散列值，F 将会启用检测 (m,RID,c)，核实 (m,RID,c) 是否被查询过。

如果 (m,RID,c) 被询问过，将 (m,RID,c) 作为索引在列表 L_h 中检索 Z。

否则，F 将会通过查询问 T_1，获得随机参数 $Z \in G_1$，并将 (m,RID,c,Z) 存储在 L_h 列表中以保持一致性。

将 Z 返回给 A。

3) 查询 O_s

为了得到签名，攻击者 A 将 β_1、γ_1 作为输入，F 将 β_1 作为 H_2 的输入得到输出 $T_1 = a\beta_1$。

F 计算 $T = T_1 + x_2 y \gamma_1 P$。

将 T 作为输出发送给 A。

伪造性和问题的解决。分别完成向 O_h 与 O_s 的 q_r 和 q_s 次询问，如果攻击者 A 能够输出 l 个有效的签名 (S_1,C_1,RID_1,m_1)，(S_2,C_2,RID_2,m_2)，…，(S_l,C_l,RID_l,m_l)，$q_s < l \leqslant q_r$，则可以计算得到 $V_i = S_i - x_2C_i = aZ_i, 1 \leqslant i \leqslant l$，输出选择目标 CDH 假设下的 l 个有效签名 $(V_1,Z_1),(V_2,Z_2),\cdots,(V_l,Z_l)$ 且 $q_h = q_s < l \leqslant q_r = q_t$。这与选择目标 CDH 假设相矛盾，所以本文方案能够满足不可伪造性，以实现可认证性。

4.2.5　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。前向保密性是指攻击者即使获得了当前认证的秘密信息，也不能推测出之前认证消息的相关信息。后向保密性与前向保密性恰恰相反，攻击者即使获得了当前认证的相关信息也不能推测出之后的认证信息，从而追踪车辆之后的认证过程。也就是说，用户当前的认证信息不会揭露用户之前与之后的认证信息。

方案中认证信息的生成取决于车辆与 RSU 在签名方案中引入了随机属性，保证了每一次认证消息的生成都会有随机值的参与，$C_i = u_i\rho_i$ 在每次认证信息的生成中都是不相同的，所以，即使恶意攻击者获得了当前签名认证过程的任何信息，都不能推断出之前的认证信息或之后的认证信息。

将本文方案的安全性与现有方案（文献[18]、文献[19]和文献[20]）进行了对比分析，结果如表 1 所示。

通过分析可以发现，本文方案使车联网匿名认证的安全性得到进一步提高，同时解决了现有方案存在的中间人攻击、前向与后向安全性等多种安全隐患。

表 1　　**安全性能比较**

方案	可认证性	匿名性	抵抗中间人攻击	抗共谋攻击	不可伪造性	可更新性	前向安全性	后向安全性
文献[18]方案	√	√						
文献[19]方案	√	√			√	√		
文献[20]方案	√	√		√	√			
本文方案	√	√	√	√	√	√	√	√

4.3 效率分析

4.3.1 计算复杂度分析

本文方案所消耗的时间仅与代表性方案（文献[18]、文献[19]和文献[20]）进行比较。其中，定义 T_{mul} 代表一次椭圆曲线上点乘运算，T_{par} 代表一次双线性对运算，T_{exp} 代表一次乘方运算。由于其他运算比较简单，消耗时间较短，可忽略不计。根据文献[21]，选用 Intel i7 3.07 GHz 的处理器，应用 MIRACL 加密数据库运行安全的 80 bit 椭圆曲线上的循环子群，依据处理时间，得到 T_{mul} 为 0.39 ms，T_{par} 为 3.21 ms。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[18]方案	$3T_{\text{mul}}$	$(2n+1)T_{\text{mul}}$
文献[19]方案	$10T_{\text{par}}+4T_{\text{exp}}$	$(n+6)T_{\text{par}}+4nT_{\text{exp}}$
文献[20]方案	$2T_{\text{par}}+2T_{\text{mul}}$	$2T_{\text{par}}+(n+1)T_{\text{mul}}$
本文方案	$3T_{\text{par}}$	$3T_{\text{par}}$

如表 2 所示，与其他方案进行比较，在进行单个消息认证时本文认证方案的认证负载有着明显的优势，随着批量认证消息的增加，本文方案的优势越来越明显，其认证延迟不随着消息的增多而加大，始终是一个常数。需要特别说明的是，文献[19]验证表明，随着认证消息的增多，所需的计算量是逐渐减少的而不是呈正比例增长的，最后稳定在 $(n+6)T_{\text{par}}+4nT_{\text{exp}}$ 上。

4.3.2 通信复杂度分析

与计算复杂度不同的是，通信复杂度不考虑计算效率，而仅考虑通信的比特数。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，在文献[18]中，传输数据分组中所包含的数据所占空间如下。原始消息占 20 B，签名占 40 B，假名占 40 B，时间戳占 4 B。在文献[19]中，原始消息占 20 B，签名占 826 B，时间戳占 4 B，ID 占 3 B。在文献[20]中可恢复消息的签名大小为 21+32=53 B，假名大小为 42 B。在本文方案中消息所占大小为 20 B，签名所占大小为 60 B。各方案通信复杂度比较如表 3 所示。

本文方案是基于椭圆曲线密码体制的签名方案而设计的，与传统的基于大数分解和离散对数的数字签名体制相比，签名长度相对较短，通过表 3 可以看出，本文方案与其他方案在通信复杂度方面相比较，明显存在一定的优势。

表 3 通信复杂度比较

方案	所占空间/B
文献[18]方案	$20+40+40+4=104$
文献[19]方案	$20+826+4+3=853$
文献[20]方案	$53+42=95$
本文方案	$20+60=80$

5 结束语

本文针对车联网隐私保护过程中匿名认证安全与效率较低的问题，基于椭圆曲线上双线对的性质，提出一种改进的车联网匿名认证方案。本文方案通过批量匿名认证的方式解决车联网中的隐私保护问题进而提高认证效率。通过方案分析，本文方案在正确性的前提下不仅可以确保不可伪造性、匿名性、可撤销性、前向与后向安全性，还能抵抗中间人攻击、共谋攻击等，同时，摆脱了批量认证类型的限制，能够安全高效地实现 3 种类型的批量认证。因此，与现有方案相比，本文方案安全性明显加强，并且在计算复杂度和空间复杂度上也存在一定的优势，这对资源受限的车联网在交通领域中的应用研究具有重要的意义和价值。

参考文献：

[1] ZHANG D, CHEN M, et al. Mobility prediction in telecom cloud using mobile calls[J]. IEEE Wireless Communications, 2014, 21(1): 26-32.

[2] ZHANG D, ZHANG D, XIONG H, et al. BASA: building mobile ad hoc social networks on top of Android[J]. IEEE Network, 2014, 28(1):4-9.

[3] KUMARI S V, PARAMASIVAN B. Defense against Sybil attacks and authentication for anonymous location-based routing in MANET[J]. Wireless Networks, 2016:1-12.

[4] ZHANG J, SUN Z, LIU S, et al. On the security of a threshold anonymous authentication protocol for VANETs[C]// Security, Privacy, and Anonymity in Computation, Communication, and Storage. 2016.

[5] YAO L, LIN C, WU G, et al. An anonymous authentication scheme in data-link layer for VANETs[J]. International Journal of Ad Hoc & Ubiquitous Computing, 2016, 22(1):1-13.

[6] JIANG S, ZHU X, WANG L. An efficient anonymous batch authentication scheme based on HMAC for VANETs[J]. IEEE Transactions on Intelligent Transportation Systems, 2016, 17(8):2193-2204.

[7] ZHANG C, LU R, LIN X, et al. An efficient identity-based batch verification scheme for vehicular sensor networks[C]//IEEE INFOCOM. 2008:246-250.

[8] 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.

[9] HORNGORNG 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.
[10] 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): 1448-1458.
[11] LAM T, RIETSCH K. Total positivity, schubert positivity, and geometric Satake[J]. Journal of Algebra, 2016, 460:284-319.
[12] 赵臻, 陈杰, 张跃宇, 等. VANET 中高效撤销的批量验证群签名方案[J]. 密码学报, 2016, 3(3):292-306.
ZHAO Z, CHEN J, ZHANG Y Y, et al. Efficient revocable group signature scheme with batch verification in VANET[J]. Journal of Cryptologic Research, 2016, 3(3): 292-306.
[13] FIAT A. Batch RSA[C]//International Cryptology Conference on Advances in Cryptology. 1989:175-185.
[14] HARN L. Batch verifying multiple DSA-type digital signatures[J]. Electronics Letters, 1998, 34(9): 870-871.
[15] HAITNER I, OMRI E, ZAROSIM H. Limits on the usefulness of random oracles[J]. Journal of Cryptology, 2016, 29(2):283-335.
[16] POINTCHEVAL D, STEM J. Provably secure blind signature schemes[C]//Advances in Cryptology ASIACRYPT'96. 1996: 252-265.
[17] 刘哲, 刘建伟, 伍前红,等. 车载网络中安全有效分布式的假名生成[J]. 通信学报, 2015, 36(11):33-40.
LIU Z, LIU J W, WU Q H, et a1. Secure and efficient distributed pseudonym generation in VANET[J]. Journal on Communications, 2015, 36(11): 33-40.
[18] HUANG J L, YEH L Y, CHIEN H Y. ABAKA: an anonymous batch authenticated and key agreement scheme for value-added services in vehicular ad hoc networks[J]. IEEE Transactions on Vehicular Technology, 2011, 60(1):248-262.
[19] SHAO J, LIN X, LU R, et al. A threshold anonymous authentication protocol for VANETs[J]. IEEE Transactions on Vehicular Technology, 2016, 65(3): 1711-1720.
[20] LIU Y, HE Z, ZHAO S, et al. An efficient anonymous authentication protocol using batch operations for VANETs[J]. Multimedia Tools & Applications, 2016:1-21.
[21] SHIM K A. An efficient conditional privacy-preserving authentication scheme for vehicular sensor networks[J]. IEEE Transactions on Vehicular Technology, 2012, 61(4):1874-1883.

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，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。