·车联网通信性能优化与安全技术专题·

一种适用于车载自组织网络的无证书混合签密方案*

林峰[1,2]　罗镜明[1]　朱智勤[2]

（1.重庆邮电大学，通信与信息工程学院，重庆 400065；2.重庆邮电大学，自动化学院，重庆 400065）

【摘要】为提高车载自组织网络中消息认证的机密性，提出了一种可证安全性的高效无证书混合签密方案。基于车载自组织网络系统模型，在车辆进行注册后引入假名自生成算法，并在签密算法中采用混合签密计算方式。理论证明与试验验证结果表明，与现有无证书签密方案相比，该方案在保护车辆隐私信息的同时，降低了可信中心和路侧单元的计算量，计算开销与通信开销保持较低水平，最后，在随机预言模型中证明了该方案的不可伪造性和机密性，并且能够抵御各类攻击。

主题词：车载自组织网络　无证书签密　无双线性映射　随机预言模型

中图分类号：TN918　　**文献标志码：**A　　**DOI:** 10.19620/j.cnki.1000-3703.20230960

A Certificateless Hybrid Signcryption Scheme for Vehicular Ad-Hoc Networks

Lin Feng[1,2], Luo Jingming[1], Zhu Zhiqin[2]

(1. College of Communication and Information Engineering, Chongqing University of Posts and Telecommunications, Chongqing 400065; 2. College of Automation, Chongqing University of Posts and Telecommunications, Chongqing 400065)

【Abstract】In order to improve the confidentiality of message authentication in vehicle-mounted ad hoc networks, an efficient certificateless hybrid signcryption scheme with provable security is proposed. Based on the model of the vehicle-mounted ad hoc network system, a pseudonymous self-generation algorithm is introduced after the vehicle is registered, and a hybrid signcryption calculation method is adopted in the signcryption algorithm. Through theoretical proof and experimental verification, compared with the existing certificateless signcryption scheme, the proposed scheme not only protects the privacy information of the vehicle, but also reduces the computation cost of the trusted center and the roadside unit, and keeps the time overhead and communication overhead at a low level, which proves the unforgeability and confidentiality of the proposed scheme in the random oracle model, and can resist various attacks.

Key words: VANET, Certificateless signcryption, No bilinear mapping, Random prediction model

【引用格式】林峰, 罗镜明, 朱智勤. 一种适用于车载自组织网络的无证书混合签密方案[J]. 汽车技术, 2024(10): 56-62.

LIN F, LUO J M, ZHU Z Q. A Certificateless Hybrid Signcryption Scheme for Vehicular Ad Hoc Networks[J]. Automobile Technology, 2024(10): 56-62.

1　前言

车载自组织网络[1](Vehicular Ad-hoc NETwork，VANET)主要由车载单元(On Board Unit，OBU)和路侧单元(Road Side Unit，RSU)构成，在车辆行驶中，VANET能够实时共享车辆的运行状态及周边的交通信息，有效提升驾驶安全性及舒适度，优化驾驶体验。由于VANET传递的交通信息较为敏感，因而其信息安全问题备受关注。

VANET的通信方式可分为车辆对基础设施(Vehicle-to-Infrastructure，V2I)通信和车辆对车辆(Vehicle-to-Vehicle，V2V)通信。其中，V2V通信允许相邻车辆进行消息互换，减少交通拥堵，但入侵者可通过窃听、跟踪等方式对车辆发送的消息进行攻击，导致接收车辆无法鉴别信息的真实性和完整性，由此对车辆身份隐私造成危害[2]。

通常，VANET使用消息签密方法实现车辆身份、消息的机密性和消息的不可否认性验证[3]。为使无证书

*基金项目：重庆市教委“成渝地区双城经济圈建设”科技创新项目(KJCXZD2020028)。

通信作者：林峰(1973—)，男，正高级工程师，主要研究方向为5G-V2X车路协同控制与信息安全，linfeng@cqupt.edu.cn。

签密方案适用于VANET，Han等[4]提出了一种混合认证协议，通过使用双线性对运算实现各种安全要求，但未对车辆隐私进行有效保护；Islam等[5]提出了一种基于双线性配对的无证书签密方案，但并没有为车辆生成假名；Hong等[6]提出车联网环境下基于身份无配对的聚合签密方案，虽然取消了双线性对运算，降低了计算和通信成本，但无法抵抗公钥替换攻击；Dai等[7]提出在车载自组织网络中，无证书签密系统下的车辆与公钥基础设施（Public Key Infrastructure，PKI）下的车辆进行互认，并支持批量发送、验证消息，但方案中大量使用双线性配对算法，且无法抵御内部攻击；张文波等[8]提出了一种密钥自生成机制，实现了用户身份匿名与可追踪，但容易遭受消息重放攻击。

为保证车辆的隐私及信息安全，现有方案中消息签密的计算量仍然较大，且极易受到各种攻击。本文在前期研究工作的基础上，通过车辆向可信中心（Trusted Authority，TA）注册，生成终端私钥，再生成假名信息发送至TA，在签密过程中使用混合签密算法降低通信开销，并通过安全性能分析验证方案的不可伪造性和机密性。

2　相关理论

2.1　椭圆曲线离散对数难题

椭圆曲线离散对数难题[9-10]（Elliptic Curve Discrete Logarithm Problem，ECDLP）可定义为：取阶为大素数q的群G，p为群G中的一个生成元，已知p和Q，ECDLP的目标在于求得$k \in Z_q^*$，使得$Q=k \cdot p$成立，其中k为循环群Z_q^*中的元素。

2.2　计算性Diffie-Hellman问题

计算性Diffie-Hellman（Computational Diffie-Hellman，CDH）问题[11]可定义为：假设G为由椭圆曲线上的点构成的加法循环群Z_q^*，p为群G中的一个生成元，给定$ap \in G$、$bp \in G$，CDH问题的目标是在未知$a \in Z_q^*$、$b \in Z_q^*$的情况下，计算$abp \in G$。

2.3　高级加密标准对称加密算法

高级加密标准[12-13]（Advanced Encryption Standard，AES）算法使用同一密钥参与加密与解密过程，包括字节代换、行位移、列混淆和轮密钥的异或运算，其密钥长度可变，具有可逆性、高效性和完备的安全性。

AES对称加密算法由以下两个算法构成[14]：

a. 加密算法：$C=AES_e(Key,m)$，其中，明文m为输入，密文C为输出，e为加密标识符，对称密钥$Key \in K$，K为对称加密算法的密钥空间。

b. 解密算法：$m=AES_d(Key,C)$，其中，密文C为输入，明文m为输出，d为解密标识符，对称密钥$Key \in K$。

2.4　安全模型

为实现本文方案的安全性证明，依据文献[15]的随机预言模型，将方案归结为ECDLP和CDH难题。

在安全模型中，攻击者通常分为Ⅰ类型和Ⅱ类型：Ⅰ类型中，攻击者$A_Ⅰ$为第三方攻击者，不能访问系统中的主密钥s，但能读取或更改终端密钥y与其对应公钥Y；Ⅱ类型中，攻击者$A_Ⅱ$攻击能力更高，可以访问系统主密钥s，但无法获取终端密钥y与其对应公钥Y。

在$A_Ⅰ$和$A_Ⅱ$两类敌手的攻击下，无证书签密方案具有的适应性选择消息攻击下的不可伪造性和适应性选择密文攻击下的机密性，需经历以下阶段：

a. 阶段1：系统初始化，解决者C进行系统初始化，将参数发送至敌手A。

b. 阶段2：询问阶段，敌手A对解决者C进行有限次询问。

c. 阶段3：挑战阶段或猜测阶段，敌手A输出签密信息，若能够通过签密有效性验证或签密与预期值相等，则敌手A在博弈中获胜。

2.5　VANET系统模型

VANET系统模型主要由TA、OBU和RSU 3个部分构成，如图1所示：TA负责VANET的建立，通过建立绝对安全的有线信道与RSU通信，在系统中主要用于OBU和RSU的注册和密钥分发；OBU为安装在移动车辆上的处理单元，当车辆加入VANET前，须向TA申请注册，获得系统公共参数和相应的密钥，再将数据写入车辆防篡改设备中；RSU与OBU通信时，需对接收的消息签密密文进行验证后，再将信息集中转发至TA。

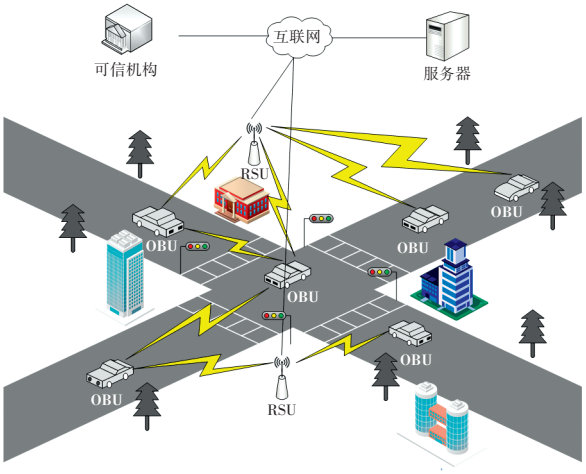

图1　车载自组织网络系统模型

3 本文方案

3.1 方案描述

本文基于文献[6]提出了一种适用于VANET的轻量级安全通信方案，通过使用椭圆曲线密码算法和AES对称加密算法，实现无证书混合签密流程，方案流程如图2所示。

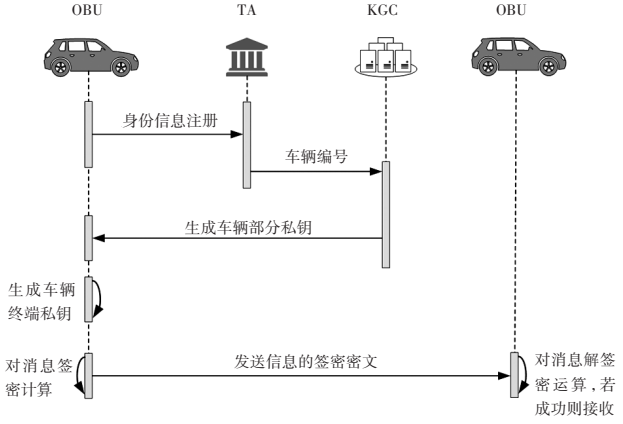

图2 方案流程

本文方案包括以下7个算法：

a. 系统初始化：首先，由密钥生成中心（Key Generation Center，KGC）选定参数并建立系统，随机选取大素数p和q，生成非奇异椭圆曲线$E_p(a,b):y^2=x^3+ax+b$，其中，$a,b\in F_p$，F_p为有限域，将点P作为加法群G中的生成元，群G均由$E_p(a,b)$上的点构成，P为G的阶。然后，随机选择系统主密钥$s\in Z_q^*$，则系统公钥$P_K=s\cdot P$，KGC选择4个系统哈希函数$H_1,H_2,H_3,H_4:\{0,1\}^*\rightarrow Z_q^*$。最后，KGC公布系统参数$S_{\text{para}}=\{E_p(a,b),p,q,G,P,P_K,H_1,H_2,H_3,H_4\}$。

b. 车辆注册算法：车辆的身份信息为ID，向TA进行身份信息注册，此时，TA生成其车辆编号$VD=H_1(ID,T)$，其中，T为当前注册时间，即(VD,ID,T)为注册消息组，并将VD发送给KGC。

c. 部分私钥生成算法：此算法由KGC执行，对于车辆部分密钥，综合系统参数S_{para}和对应车辆ID，选择一个随机数$n\in Z_q^*$，并计算部分私钥参数$N=n\cdot P$，$hv=H_2(P_K,VD,N)$，车辆的部分私钥$x=n\oplus hv\cdot s$，将车辆的部分私钥x通过安全信道发送给车辆ID，并将对应公钥$X=x\cdot P=N\oplus hv\cdot P_K$通过安全信道发送给其他车辆。

d. 终端密钥生成算法：车辆执行本算法生成公私钥对时，车辆ID随机选择私钥$y\in Z_q^*$，计算公钥$Y=y\cdot p$，并通过安全信道发送给其他车辆。

e. 假名生成算法：车辆注册后，车辆ID生成临时假名，输入当前时间参数T，计算假名参数$VH=H_3(Y,T)$，$P_{ID}=VD\oplus VH$，令$Q=(P_{ID},T)$为车辆假名，并通过安全信道发送给其他车辆。

f. 签密算法：车辆ID_A对于车辆ID_B，计算其公钥$PV_B=X_B\oplus Y_B$，输入当前时间参数T，选择随机数$k\in Z_q^*$，车辆ID_A对信息m执行签密运算：

$$\begin{cases} K=k\cdot P \\ U=k\cdot(X_B\oplus Y_B) \\ C=AES_e(U,m) \\ v=H_4(m,K,Q_A,PV_A,T) \\ R=v\cdot(x_A\oplus y_B)\oplus K \end{cases} \tag{1}$$

式中：K、U、v、R为签密参数，C为消息对称加密结果。

签密完成后，得到签密结果$\sigma=\{K,C,R,T\}$，车辆ID_A将σ发送给车辆ID_B。

g. 解签密算法：车辆ID_B进行解签密时执行本算法，输入签密密文σ，计算解签密私钥$pv_B=x_B\oplus y_B$，加载系统参数S_{para}、车辆ID_A公钥$PV_A=X_A\oplus X_B$、车辆ID_A假名Q_A，车辆ID_B对签密密文σ执行解签密运算：

$$\begin{cases} U'=pv_B\cdot K \\ m'=AES_d(U',C) \\ v'=H_4(m',K,Q_A,PV_A,T) \\ R\cdot P=v'\cdot PV_A\oplus K \end{cases} \tag{2}$$

检验$R\cdot P=v'\cdot PV_A\oplus K$是否成立，并判断时间戳$T$是否在有效期内，若通过检验，则选择接收信息$m'$。

3.2 正确性分析

对于接收明文信息m的正确性分析，由于接收车辆计算的U'与发送车辆的U间关系为：$U'=pv_B\cdot K=pv_B\,k\cdot P=k\cdot PV_B=k\cdot(X_B\oplus Y_B)=U$，并根据AES对称加密算法的特性，通过恒等变换可证明接收者的m'和发送者的m关系：

$$m'=AES_d(U',C)=AES_d(U,C)=AES_d(U,AES_d(U,m))=m \tag{3}$$

对于签密密文σ的有效性分析，可证明$R\cdot P=v'\cdot PV_A\oplus K$成立：

$$\begin{aligned} R\cdot P &= v\cdot(x_A\oplus y_A)\cdot P\oplus k\cdot P \\ &= H_4(m',K,QA,PVA,T)\cdot(n\oplus hv\cdot s\oplus y_A)\cdot P\oplus k\cdot P \\ &= v'(X_A\oplus Y_A)\oplus K \\ &= v'\cdot PV_A\oplus K \end{aligned} \tag{4}$$

因此，在签密密文$\sigma=\{K,C,R,T\}$进行传输时，若任意参数发生变化，都会使得$R\cdot P\neq v'\cdot PV_A\oplus K$，导致该签密密文无法通过有效性验证。

4 安全性分析

4.1 不可伪造性

假设攻击者A_{I-1}使用本文方案时，最多可进行q_2次h_2询问、q_n次创建用户询问、q_s次部分私钥询问、q_f次签密询问，若以优势ε成功伪造用户的签密密文，B_1为椭圆曲线离散对数问题的解决者，则该问题的输入为

$(s,P_K=s\cdot P)$，其中$s\in Z_q^*$，B_1的目标为计算s。B_1与$A_{\mathrm{I}-1}$的博弈交互包括系统初始化、询问阶段和挑战阶段。

4.1.1 系统初始化

由B_1构建系统，公开系统参数$S_{\mathrm{para}}=\{E_p(a,b),p,q,G,P,P_K,H_1,H_2,H_3,H_4\}$，并建立$L_1$、$L_2$、$L_3$、$L_4$、$L_{ID}$和$L_R$列表，分别用于跟踪$A_{\mathrm{I}-1}$对预言机$h_1$、$h_2$、$h_3$和$h_4$的询问，以及对用户创建和签密预言机的询问，其中，$B_1$选择$VD^*$作为被挑战者身份。

4.1.2 询问阶段

$A_{\mathrm{I}-1}$对B_1进行多项式有界次的询问如下：

a. h_1预言机查询：$A_{\mathrm{I}-1}$使用ID_i询问，若L_1列表中已存在，则将VD返回至$A_{\mathrm{I}-1}$；反之，则B_1随机选取$T\in Z_q^*$，计算$VD=H_1(ID_i,T)$，再将VD返回至$A_{\mathrm{I}-1}$。

b. h_2预言机查询：$A_{\mathrm{I}-1}$使用VD_i询问，若L_2列表中已存在，则将hv返回至$A_{\mathrm{I}-1}$；反之，则B_1先执行部分私钥查询，随机选取$n_i\in Z_q^*$，计算$N_i=n_i\cdot P$，$hv=H_2(P_K,VD_i,N_i)$，再将hv返回至$A_{\mathrm{I}-1}$。

c. h_3预言机查询：$A_{\mathrm{I}-1}$使用VD_i进行询问，若L_3列表中存在相应元组，则将VH返回给$A_{\mathrm{I}-1}$；反之，则进行终端密钥预言机查询，计算$VH=H_3(Y_i,T)$，并将VH返回至$A_{\mathrm{I}-1}$。

d. h_4预言机查询：$A_{\mathrm{I}-1}$使用(VD_i,C,K)询问，如果L_4中已经存在，则将v返回至$A_{\mathrm{I}-1}$；如果没有对应的Y_i，则执行终端密钥预言机查询；如果没有对应的X_i，则执行部分私钥预言机查询，再计算m_i和v，并将v返回至$A_{\mathrm{I}-1}$。其中：$m_i=AES_d(pv\cdot K,C)$，$v=H_4(m_i,K,Q,PV,T)$。

e. 用户创建预言机查询：$A_{\mathrm{I}-1}$使用VD_i进行查询，然后进行如下判断：

B_1查询L_{ID}，若不存在对应元组，当$VD_i=VD^*$时，B_1随机选择$n_i,y_i,hv\in Z_q^*$，计算$N_i=n_i\cdot P$，$Y_i=y_i\cdot P$，$x=\perp$；当$VD_i\neq VD^*$时，B_1随机选择$x_i,n_i,y_i,hv\in Z_q^*$，计算$Y_i=y_i\cdot P$，$N_i=x_i\cdot P-hv\cdot P_K$，最后将其加入相应的列表中；若列表中已存在相应元组，B_1再查询L_2列表，如果相应的元组(VD_i,P_K,N_i,hv)满足$hv=H_2(VD_i,P_K,N_i)$，则返回用户信息，否则，B_1结束本次博弈。

f. 终端密钥预言机查询：$A_{\mathrm{I}-1}$使用VD_i进行询问时，B_1查询L_{ID}列表，如果L_{ID}中已有对应元组，B_1返回(Y_i,y_i)至$A_{\mathrm{I}-1}$，否则，B_1随机选取$y_i\in Z_q^*$，计算$Y_i=y_i\cdot P$，并将(Y_i,y_i)返回至$A_{\mathrm{I}-1}$。

g. 部分私钥预言机查询：假定敌手$A_{\mathrm{I}-1}$最多只有q_s次查询次数。当$VD_i=VD^*$时，B_1输出$\perp$并结束博弈；当$VD_i\neq VD^*$，如果B_1查询L_{ID}列表存在对应元组，则计算$x_i=n_i\oplus hv\cdot s$，将x_i返回至$A_{\mathrm{I}-1}$，否则，B_1随机选择$n_i,x_i\in Z_q^*$，计算$N_i=n_i\cdot P$，将N_i保存在L_{ID}列表中，并将x_i返回至$A_{\mathrm{I}-1}$。

h. 公钥预言机查询：敌手$A_{\mathrm{I}-1}$使用VD_i询问时，B_1查询L_{ID}，如果L_{ID}中存在对应元组，B_1返回(N_i,Y_i)至$A_{\mathrm{I}-1}$，否则，B_1执行部分私钥预言机查询与终端密钥预言机查询，并将(N_i,Y_i)返回至敌手$A_{\mathrm{I}-1}$。

i. 签密预言机查询：敌手$A_{\mathrm{I}-1}$使用元组(VD_i,Q_i,N_i,K,m_i)进行查询，B_1计算$hv_i=H_2(VD_i,P_K,N_i)$，并将$\{N_i,hv_i\}$保存在L_2列表中。随机选择$R_i,v_i\in Z_q^*$，最后，将(m_i,Q_i,N_i,R_i,v_i)保存在列表L_R。

4.1.3 挑战阶段

敌手$A_{\mathrm{I}-1}$输出关于(VD^*,m_i)的伪签密密文，若$VD_i\neq VD^*$，B_1宣布攻击失败；否则，B_1从列表中查询到对应的签密信息(m_i,R_i,v_i)。当$A_{\mathrm{I}-1}$在博弈获胜，则输出$s=((R_i-k)/v_i-n_i-y_i)/hv_i$作为系统主密钥的有效解，表明解决ECDLP问题；反之，表明该问题未解决。

评估B_1解决ECDLP问题的优势，若$A_{\mathrm{I}-1}$执行VD^*的部分私钥查询，则B_1挑战失败。$A_{\mathrm{I}-1}$未执行该询问的概率为$P_r[\varepsilon_1]=(1-q_2/q)^{q_n}(1-1/q_n)^{q_s}(1-q_s/q)$，在问询阶段终止模拟的概率为$P_r[\varepsilon_2]=(1-\delta)^{q_s+q_f+1}$，在挑战阶段终止模拟的概率为$P_r[\varepsilon_3]=\delta$。因此，整个模拟过程中，$A_{\mathrm{I}-1}$不终止的概率为：$P_r[\varepsilon_1\wedge\varepsilon_2\wedge\varepsilon_3]=(1-\frac{q_2}{q})^{q_n}\cdot(1-\frac{1}{q_n})^{q_s}(1-\frac{q_s}{q})\delta(1-\delta)^{q_s+q_f+1}$。其中，$\delta=1/(q_s+q_f+1)$，若$(q_s+q_f)$足够大，则$(1-\delta)^{q_s+q_f+1}\to e^{-1}$。

因此，如果$A_{\mathrm{I}-1}$以优势ε成功伪造另一个签密密文，那么B_1就能够以ε'的优势解决椭圆曲线离散对数问题，其中，$\varepsilon'\geqslant(1-\frac{q_2}{q})^{q_n}(1-\frac{1}{q_n})^{q_s}(1-\frac{q_s}{q})\frac{\varepsilon}{e(q_s+q_f+1)}$。但这与ECDLP问题无法解决互相矛盾，说明敌手$A_{\mathrm{I}-1}$成功伪造一个签密密文的优势可被忽略，即本文方案可以抵抗敌手$A_{\mathrm{I}-1}$的伪造攻击，同理，$A_{\mathrm{II}-1}$型攻击同样可抵抗。

4.2 机密性

假设攻击者$A_{\mathrm{I}-2}$使用本方案时，最多可进行q_2次h_2询问、q_n次创建用户询问、q_s次部分私钥询问、q_f次签密询问，若以ε的优势成功破解一个签密密文，B_2是CDH问题的解决者，则该问题输入为$(P,k\cdot P,s\cdot P)$，B_2的目标是计算$k\cdot s\cdot P$。B_2与$A_{\mathrm{I}-2}$的博弈交互包括系统初始化、询问阶段、挑战阶段和猜测阶段。

4.2.1 系统初始化

由B_2构建系统，公开系统参数$S_{\mathrm{para}}=\{E_p(a,b),p,q,G,P,$

P_K,H_1,H_2,H_3,H_4}，并建立L_1、L_2、L_3、L_4、L_{ID}和L_m列表，分别用于跟踪$A_{\mathrm{I}-2}$对预言机h_2、h_3和h_4的询问，以及对用户创建和签密预言机的询问，同时，B_2选择VD^*作为被挑战者身份。

4.2.2 询问阶段

$A_{\mathrm{I}-2}$对B_2进行4.1节的h_2、h_3和h_4预言机查询，以及终端密钥、部分私钥、用户创建、公钥预言机查询。

解签密预言机查询：敌手$A_{\mathrm{I}-2}$使用元组(VD_i,σ,N_i,Y_i)进行查询，若$VD_i=VD^*$，B_1输出⊥并结束博弈；反之，B_2计算$hv=H_2(VD_i,P_K,N_i)$，并将$\{N_i,hv_i\}$保存在L_2列表中。随机选择$pv_i \in Z_q^*$，计算$U_i=pv_i \cdot K$，$m_i=AES_{\mathrm{d}}(pv_i,K,C)$，最后，将$(VD_i,\sigma,R_i,Y_i,U_i,m_i)$保存在列表$L_m$，并返回$m_i$至$A_{\mathrm{I}-2}$。

4.2.3 挑战阶段

敌手$A_{\mathrm{I}-2}$随机选择一对明文(m_0,m_1)及一对接受挑战者身份(VD_A,VD_B)，在阶段2不能对VD_B进行任何秘密值询问。此时，若$VD_B \neq VD^*$，则B_2结束博弈；否则，B_1将构造一个挑战密文。

B_2对VD_B执行公钥预言机查询，得到(VD_B,Y_B,N_B)。随机选取$\beta \in \{0,1\}$，选取随机数$R,k \in Z_q^*$，计算$K=k \cdot P$，$U=k(N_B \oplus hv_B \cdot P_K \oplus Y_B)$,$C=AES_e(U,m_\beta)$，$B_1$输出关于消息$m_\beta$的签密密文$\sigma^*=\{K,C,R,T\}$，并返回至$A_{\mathrm{I}-2}$。

4.2.4 猜测阶段

$A_{\mathrm{I}-2}$可对B_2进行多项式有界次的适应性询问，但不能对σ^*进行解签密询问。

此时，$A_{\mathrm{I}-2}$将输出β'作为对β的猜测，若$\beta'=\beta$，则B_1在已知$k \cdot P$和$s \cdot P$的情况下输出$(pv_B \cdot K-k \cdot Y_B-k \cdot N_B)/hv=k \cdot s \cdot P$，并将其作为CDH问题的解；否则，表明未解决CDH问题。

评估B_2解决CDH问题的优势，若$A_{\mathrm{I}-2}$执行VD^*的部分私钥查询，则B_2挑战失败；$A_{\mathrm{I}-2}$不执行该询问的概率为$P_r[\varepsilon_1]=(1-q_2/q)^{q_n}(1-1/q_n)^{q_r}(1-q_s/q)$，$A_{\mathrm{I}-2}$在问询阶段终止模拟的概率为$P_r[\varepsilon_2]=(1-\delta)^{q_s+q_f+1}$，$A_{\mathrm{I}-2}$在挑战阶段终止模拟的概率为$P_r[\varepsilon_3]=\delta$。最后，整个模拟过程中$A_{\mathrm{I}-2}$不终止的概率为$P_r[\varepsilon_1 \wedge \varepsilon_2 \wedge \varepsilon_3]=(1-\frac{q_2}{q})^{q_n} \cdot (1-\frac{1}{q_n})^{q_r}(1-\frac{q_s}{q})\delta(1-\delta)^{q_s+q_c+1}$。其中$\delta=1/(q_s+q_c+1)$，若$(q_s+q_c)$足够大，则$(1-\delta)^{q_s+q_c+1} \to e^{-1}$。

因此，如果$A_{\mathrm{I}-2}$以优势ε成功解密一个签密密文，那么B_2就能够以ε'的优势解决CDH问题，其中，$\varepsilon' \geqslant (1-\frac{q_2}{q})^{q_n}(1-\frac{1}{q_n})^{q_r}(1-\frac{q_s}{q})\frac{\varepsilon}{e(q_s+q_c+1)}$。但这与CDH问题无法解决互相矛盾，说明$A_{\mathrm{I}-2}$成功解密一个签密密文的优势能被忽略，即本文方案可抵抗$A_{\mathrm{I}-2}$的攻击，同理，$A_{\mathrm{II}-2}$型攻击同样可抵抗。

4.3 中间人攻击

当遭遇中间人攻击时，攻击者从公共信道截取签密密文$\sigma=\{K,C,R,T\}$，试图篡改该密文并生成新的有效签密密文σ^*。签密密文中$R=v(x_A \oplus y_A) \oplus k$，其中，$v$由$K$、$T$、$m(m=AES_{\mathrm{d}}(pv \cdot K,C))$等参数通过哈希计算得出。如果攻击者篡改$K$、$C$中任意参数，则$v' \neq v$，将导致签密密文无效。

若攻击者能够通过解决椭圆曲线离散对数难题而获得签密私钥x和y，计算出$R'=v'(x \oplus y) \oplus k$，生成签密密文$\sigma'=\{K',C',R',T\}$，则攻击者攻击成功；然而，椭圆曲线离散对数难题无解，因此，本文方案可以抵抗中间人攻击。

4.4 内部特权攻击

KGC特权人员能够直接访问车辆发送至TA的注册消息(VD,ID,T)及对应的部分私钥x，可读取系统私钥s，但无法获取车辆的终端密钥信息y。

在此条件下，当特权人员进行非法攻击时，由于缺少终端密钥信息，将无法计算车辆的完整私钥$pv=x \oplus y$，最终无法生成有效签密密文信息σ。因此，本文方案可成功抵御内部特权攻击。

4.5 重放攻击

车辆生成的签密密文为$\sigma=\{K,C,R,T\}$，密文包含发送消息的时间戳T，且R为时间戳T的相关签密计算参数。

当攻击者使用有效的签密密文进行重放攻击时，签密密文将无法通过时间戳检测，即使攻击者更新密文中T，密文被接收后仍无法通过有效性检测。因此，该方案能够抵御重放攻击。

对比本文方案与近年VANET方案的安全性，结果如表1所示，本文方案的安全性均优于其他方案。

表1 VANET安全性分析

方案	不可伪造性	机密性	中间人攻击	内部特权攻击	重放攻击
文献[5]	√	√	√	×	×
文献[6]	√	√	×	×	×
文献[7]	√	√	√	×	√
文献[8]	√	√	×	×	×
文献[16]	√	√	×	×	×
文献[17]	√	√	×	×	√
文献[18]	√	×	√	×	√
文献[19]	√	√	×	×	×
文献[20]	√	×	√	×	×
本文方案	√	√	√	√	√

注：√表示存在该性能；×表示未存在该性能。

5 性能分析

本文试验环境为Intel i5-8300H处理器，主频为2 666 MHz，内存为16 GB，该设备的操作系统为Ubuntu16.04。通过调用OPENSSL工具库，对各基础运算操作计算开销，测试结果如表2所示。

表2 各基础运算操作计算开销 ms

操作	计算开销	操作	计算开销
指数运算 T_e	0.263	双线性对点乘法运算 T_c	0.442
模逆运算 T_m	0.145	椭圆曲线点乘法运算 T_s	0.363
哈希运算 T_h	0.013	椭圆曲线点加法运算 T_a	0.002
双线性对操作 T_b	1.088		

5.1 计算开销分析

通过逐步分析各方案的算法步骤，对比各方案的时间开销，结果如表3所示。

表3 各方案计算开销

方案	签密开销	解签密开销	总开销/ms
文献[5]	T_e	T_e+2T_b	2.700
文献[6]	$4T_s$	$4T_s$	2.910
文献[7]	T_a+3T_s	$2T_a+4T_s$	2.542
文献[8]	$2T_a+3T_s$	$3T_a+3T_s$	2.183
文献[16]	$3T_s$	$3T_s$	2.175
文献[17]	$2T_c+T_e$	$2T_b+T_c$	3.764
文献[19]	T_m+2T_s	$2T_a+3T_s$	1.961
本文方案	$2T_h+3T_a+2T_s$	$2T_h+3T_a+3T_s$	1.872

在各方案的运算操作中，双线性对操作、双线性对点乘运算和椭圆曲线点乘运算为计算开销的主要来源，其中，双线性对操作的计算开销最大。而相较于文献[5]、文献[17]，本文方案无双线性对操作；与文献[6]~[8]及文献[16]相比，本文方案所需要椭圆曲线点乘运算操作次数最少；与文献[19]相比，本文无需模逆运算操作。因此，本文签密方案在时间开销上最低，操作更加高效。其中，AES_e和AES_d算法的时间开销约等于一次T_h。

5.2 通信开销分析

在通信开销方面，对本文方案和其他方案进行了签密密文分析，如表4所示。由于文献[5]、文献[17]方案包含双线性对运算，假设所有方案的时间戳长度$|T|$=32 bit，且$|Z_q^*|$=160 bit。在双线性对运算中，$|G_1|$=1 024 bit；在椭圆曲线密码运算中，$|G_q|$=320 bit。

由于本文方案未使用双线性对运算，因此，时间开销大幅降低；本文方案在通信开销上仅高于其他最低方案32 bit，因此，本文方案的通信开销可维持较低水平。

表4 各方案通信开销

方案	通信开销	密文长度/bit
文献[5]	$2\|G_1\|+\|G_q\|+\|Z_q^*\|$	2 528
文献[6]	$\|G_q\|+\|Z_q^*\|$	480
文献[7]	$\|G_q\|+\|Z_q^*\|$	480
文献[8]	$\|G_q\|+\|Z_q^*\|$	480
文献[16]	$\|G_q\|+\|Z_q^*\|$	480
文献[17]	$2\|G_1\|+\|T\|$	2 080
文献[19]	$\|G_q\|+2\|Z_q^*\|$	960
本文方案	$\|G_q\|+\|Z_q^*\|+\|T\|$	512

6 结束语

本文在VANET的无证书签密方案的基础上，结合车辆通信链路持续时间短的特点，采用椭圆曲线密码算法来构建签密计算，并且通过采用假名自生成算法减轻了TA和RSU的计算负担。通过签密计算，证明了本文方案满足车载自组网的安全需求，同时，对比各种无证书签密方案，本文方案的计算开销与通信开销均达到最低。未来，在保证VANET通信安全的同时，考虑在通信方案的轻量化方向开展进一步研究。

参 考 文 献

[1] MCHERGUI A, MOULAHI T, ZEADALLY S. Survey on Artificial Intelligence (AI) Techniques for Vehicular Ad-Hoc Networks (VANETs) [J]. Vehicular Communications, 2022, 34.

[2] AL-SHAREEDA M A, MANICKAM S, LAGHARI S A, et al. Replay-Attack Detection and Prevention Mechanism in Industry 4.0 Landscape for Secure SECS/GEM Communications[J]. Sustainability, 2022, 14(23).

[3] ZHAO Y, WANG Y, LIANG Y, et al. Identity-Based Broadcast Signcryption Scheme for Vehicular Platoon Communication[J]. IEEE Transactions on Industrial Informatics, 2022, 19(6): 7814-7824.

[4] 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. Beijing, China: Springer International Publishing, 2014: 218-226.

[5] ISLAM A, ALTAF F, MAITY S. Efficient Certificate-Less Signcryption Scheme for Vehicular Ad Hoc Networks[C]// Inventive Communication and Computational Technologies: Proceedings of ICICCT 2021. Springer Singapore, 2022: 927-942.

[6] DU H Z, WEN Q Y, ZHANG S S, et al. A Pairing-Free Certificateless Signcryption Scheme for Vehicular Ad Hoc Networks[J]. Chinese Journal of Electronics, 2021, 30(5): 947-955.

[7] DAI C, XU Z W. Pairing-Free Certificateless Aggregate Signcryption Scheme for Vehicular Sensor Networks[J]. IEEE Internet of Things Journal, 2022, 10(6): 5063-5072.

[8] 张文波, 黄文华, 冯景瑜. 基于无证书签密的车联社会网络安全通信机制[J]. 通信学报, 2021, 42(7): 128-136.
ZHANG W B, HUANG W H, FENG J Y. The Security Communication Mechanism of Social Network of Car Service Based on Non-Certificate Signcryption[J]. Journal of Communications, 2021, 42(7): 128-136.

[9] SHAO H, PIAO C. A Provably Secure Lightweight Authentication Based on Elliptic Curve Signcryption for Vehicle-to-Vehicle Communication in VANETs[J]. IEEE Transactions on Industrial Informatics, 2023, 20(3): 3738-3747.

[10] MA R, DU L Y. Attribute-Based Blind Signature Scheme Based on Elliptic Curve Cryptography[J]. IEEE Access, 2022, 10: 34221-34227.

[11] PAN J X, CHEN Q, RINGERUD M. Signed (Group) Diffie - Hellman Key Exchange with Tight Security[J]. Journal of Cryptology, 2022, 35(4): 26.

[12] PIAO J, WANG Z, WU Y, et al. In-Vehicle Flexray Network Security Based on Modified AES Encryption Algorithm[C]// The 2nd International Conference on Distributed Sensing and Intelligent Systems (ICDSIS 2021). London, UK: Institution of Engineering and Technology, 2021: 17-27.

[13] DAEMEN J, RIJMEN V. AES Proposal: Rijndael[J]. Computer Science, Mathematics, 1999.

[14] CARLSON A, GANG G, GANG T, et al. Evaluating True Cryptographic Key Space Size[C]// 2021 IEEE 12th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON). New York, USA: IEEE, 2021: 243-249.

[15] KASYOKA P, KIMWELE M, ANGOLO S M. Cryptanalysis of A Pairing-Free Certificateless Signcryption Scheme[J]. ICT Express, 2021, 7(2): 200-204.

[16] ULLAH I, KHAN M A, ALSHARIF M H, et al. An Anonymous Certificateless Signcryption Scheme for Secure and Efficient Deployment of Internet of Vehicles[J]. Sustainability, 2021, 13(19).

[17] ALI I, CHEN Y, ULLAH N, et al. Bilinear Pairing-Based Hybrid Signcryption for Secure Heterogeneous Vehicular Communications[J]. IEEE Transactions on Vehicular Technology, 2021, 70(6): 5974-5989.

[18] LIU X, WANG L, LI L, et al. A Certificateless Anonymous Cross-Domain Authentication Scheme Assisted by Blockchain for Internet of Vehicles[J]. Wireless Communications and Mobile Computing, 2022, 2022(1).

[19] CUI B B, LU W, WEI H. A New Certificateless Signcryption Scheme for Securing Internet of Vehicles in the 5G Era[J]. Security and Communication Networks, 2022, 2022(1).

[20] CUI J, XU W Y, HAN Y B, et al. Secure Mutual Authentication with Privacy Preservation in Vehicular Ad Hoc Networks[J]. Vehicular Communications, 2020, 21.

（责任编辑　瑞　秋）

修改稿收到日期为2024年1月30日。