一种可证安全的车联网无证书聚合签名改进方案

谢 永[①] 李 香[①] 张松松[①] 吴黎兵*[②]

[①](青海大学计算机技术与应用系 西宁 810016)

[②](武汉大学计算机学院 武汉 430072)

摘 要：车联网(VANETs)是组织车－X(X：车、路、行人及互联网等)之间的无线通信和信息交换的大型网络，是智慧城市重要组成部分。其消息认证算法的安全与效率对车联网至关重要。该文分析王大星等人的VANETs消息认证方案的安全不足，并提出一种改进的可证安全的无证书聚合签名方案。该文方案利用椭圆曲线密码构建了一个改进的安全无证书聚合认证方案。该方案降低了密码运算过程中的复杂性，同时实现条件隐私保护功能。严格安全分析证明该文方案满足VANETs的安全需求。性能分析表明该文方案相比王大星等人方案，较大幅度地降低了消息签名、单一验证以及聚合验证算法的计算开销，同时也减少了通信开销。

关键词：车联网；聚合签名；无证书体制；椭圆曲线密码；条件隐私保护

中图分类号：TN915; TP309 **文献标识码**：A **文章编号**：1009-5896(2020)05-1125-07

DOI: 10.11999/JEIT190184

An Improved Provable Secure Certificateless Aggregation Signature Scheme for Vehicular Ad Hoc NETworks

XIE Yong[①] LI Xiang[①] ZHANG Songsong[①] WU Libing[②]

[①](*Department of Computer Technology and Application*, *Qinghai University*, *Xining* 810016, *China*)

[②](*Computer School*, *Wuhan University*, *Wuhan* 430072, *China*)

Abstract: Vehicular Ad hoc NETworks (VANETs) which is an important part of smart cities are large networks that organize wireless communication and information exchange between vehicles and X (X: cars, roads, pedestrians, and the Internet). The security and efficiency of the message authentication algorithm are crucial to the VANETs. After analyzing the security shortage of Wang Daxing *et al* VANETs message authentication scheme, an improved provable secure certificateless aggregation signature scheme for VANETs is proposed. The scheme constructs a secure certificateless aggregation authentication scheme by using Elliptic Curve Cryptography (ECC) and reduces the complexity of the cryptographic operation process, while achieving user's conditional privacy protection. Rigid security analysis proves that the scheme satisfies the security requirements of VANETs. The performance analysis shows the proposed scheme considerably reduces the computational cost of message signature, single verification and aggregation verification algorithm, and reduces the communication cost when compared with Wang schemes.

Key words: Vehicular Ad hoc NETworks (VANETs); Aggregated signature; Certificateless system; Elliptic Curve Cryptography (ECC); Conditional privacy protection

1 引言

近年来，人们的生活水平日益提高，以车代步的出行也更加便捷，人们对更加安全、高效、舒适驾驶的需求越来越迫切。这种形势下，车辆自组织网络(Vehicular Ad-hoc NETworks, VANETs)越来越受到相关研究人员的关注，并且已成为政府和汽车制造商共同关注的热点研究方向。VANETs是一种新型的多跳移动无线通信网络，一般由一个可信密钥生成中心(Key Generation Center, KGC)，具有车载单元(On Board Unit, OBU)的车辆以及路侧单元(Road Side Unit, RSU)组成。KGC负责OBU和RSU的注册与管理。用户通过车辆的OBU与车辆进行V2V (Vehicle-to-Vehicle)的通

收稿日期：2019-03-26；改回日期：2019-09-28；网络出版：2020-01-20
*通信作者： 吴黎兵 wu@whu.edu.cn
基金项目：国家自然科学基金(61862052)，青海省基金(2017-ZJ-959Q, 2019-ZJ-7065)

Foundation Items: The National Natural Science Foundation of China (61862052), The Science and Technology Foundation of Qinghai Province (2017-ZJ-959Q, 2019-ZJ-7065)

信，与RSU进行V2I (Vehicle-to-Infrastructure)的通信。车辆将所感知的信息通过V2V或V2I的无线通信方式传输给RSUs，并由RSUs通过有线传输方式发送给对应服务器，车辆就能通过RSUs获得各种应用服务[1]。

VANETs是一种快速移动的网络，因其自身的网络特点，到目前为止依然面临着通信稳定性欠缺、易被追踪、易受攻击等安全问题。无法解决安全问题，VANETs的发展也会受到严重限制。近几年来，越来越多的研究人员开始致力于VANETs的安全性研究。然而，追求安全性则会增加网络中的通信以及计算开销，使得消息认证效率下降。因此，一个安全且高效的VANETs所具备的条件必须包含如下3个：(1)通信协议可以保证消息的可认证性；(2)车辆在通信过程中保持匿名，但在发生交通事故时，可以追踪到车辆的真实身份，实现条件隐私保护；(3)协议的计算与通信开销要尽量小，以满足VANETs苛刻的低延迟要求。

消息签名与认证技术是保证信息可认证性的关键，VANETs中消息认证也采用消息签名的方法，为了降低VANETs的通信负担，一些学者提出了聚合签名[2]的方案。聚合签名算法可以实现将多个用户的签名压缩成1个签名进行处理，提高了消息认证效率。聚合签名分为基于传统公钥基础设施的聚合签名[3]与基于身份的聚合签名[4]两类。前者是基于证书体制的，管理和维护证书会造成很大开销，因此不太适用于VANETs。后者是基于身份的，无需托管证书，适用于VANETs这类无线通信网络。但后者存在密钥托管问题，用户私钥可能会被恶意的密钥生成中心利用，这会对系统安全产生极大威胁。为了解决密钥托管问题，一些学者利用无证书密码体制提出了无证书聚合签名方案[5–7]，密钥生成中心只生成用户的部分私钥，用户随机选取一个秘密值和他的部分私钥一起生成自己独立的公/私钥，从而确保签名安全[8]。

近年来，一些学者为VANETs消息认证提出了许多认证方案。文献[5]提出了一种基于身份的结构化聚合签名方案，但其计算成本过高不适用于VANETs。文献[6,7]以及文献[9]所提出的方案中涉及许多双线性对运算，文献[10]提出双线性对运算是十分复杂的，因此它们都不适用于VANETs。文献[11]提出了一个在VANETs中可以应用的无证书的批量认证方案，极大地提高了消息认证效率，但文献[12]指出其不能抵抗重放攻击和假扮攻击。并在文献[11]的基础上提出了一种新的面向V2I通信的认证方案，但是该方案不能抵抗篡改攻击[13]。文献[14]在文献[11]的基础上提出了改进方案，既可以保护VANETs用户的隐私，又可以降低计算开销，但是被文献[15]指出该方案不能有效抵抗假扮攻击。

针对车辆在通信过程中的隐私保护问题，文献[16]基于公钥设施基础提出了隐私保护认证方案，旨在实现车辆匿名性。但文献[17]指出文献[16]在跟踪车辆真实身份时，管理证书是一个很大的负担，不适用于VANETs，并提出了一种在签名阶段利用预先计算的方法来减少通信开销的隐私保护认证方案，比较适用于VANETs。为了保护用户隐私以及提高通信网络的安全性，王大星等人[8]提出了一种利用RSU为车辆生成临时假名的无证书消息聚合认证方案。然而经我们分析发现该方案不能抵抗恶意的KGC安全攻击，且条件隐私保护的可操作性并不理想。

为了解决当前车联网的安全性与效率不足的情况，本文在王大星等人[8]方案的基础上提出了一种改进的具有条件隐私保护功能的可证安全的无证书聚合签名方案。总结起来，本文主要有3个创新点：(1)本文方案采用椭圆曲线构建了简易安全的无证书聚合认证方案；(2)本文方案采用更安全可靠的随机匿名机制来保护用户隐私，并给出了严格的安全性证明，且条件隐私保护的可操作性较强；(3)与王大星等人的方案以及Zhong等人[17]方案的性能比较表明，本文方案在计算与通信方面的开销显著减少了。

本文余下部分安排如下：第2节分析王大星等人的CLAS方案，第3, 4节提出改进方案及其安全性分析与证明，第5, 6节是性能分析与全文总结。

2 王大星等人的CLAS方案及分析

2.1 王大星等人[8]的CLAS方案简述

王大星等人[8]的方案可简述为如下9个算法

(1) 系统建立算法(setup): KGC建立加法循环群G_1和乘法循环群G_2，其阶为素数q。定义双线性映射$e:G_1\times G_1\to G_2$，P为群G_1的生成元。设$s\in {}_RZ_q^*$为系统主密钥，则系统公钥为$P_K=s\cdot P$。令$H_1,H_2:\{0,1\}^*\to Z_q^*$为安全的Hash函数，消息$M=\{0,1\}^*$。每个RSU设立各自的秘密值$y_i\in {}_RZ_q^*$，则其公钥为$\overline{P}_i=y_i\cdot P$，并发送给KGC。最后，KGC公开系统参数列表：$\text{paras}=\{G_1,G_2,e,P,P_K,H_1,H_2,\overline{P_i}\}$。

(2) 车辆注册算法(registration)：可信注册中心(Trusted Authority, TA)完成车辆注册算法。令车辆的身份信息为ID_i, TA生成假身份$\text{ID}_i'=H_3(\text{ID}_i)$以实现隐私保护目的。

(3) 部分私钥生成算法(PartialKeyGen)：KGC输入paras, s和$\mathrm{ID}_i^{'}$，依据$p_i = s \cdot \mathrm{ID}_i^{'}$计算出车辆部分私钥。

(4) 用户密钥生成算法(UserKeyGen)：车辆执行本算法，生成其秘密值和公钥。车辆ID_i选择$x_i \in {}_RZ_q^*$，则公钥为$P_i = x_i \cdot P$。

(5) 假名生成算法(PseudonymGen)：RSU为车辆执行本算法，生成车辆的临时假名。RSU选择$a_i \in {}_RZ_q^*$，计算$F1_i = a_i \cdot \mathrm{ID}_i^{'}$, $W_i = H_2(F1_i)$, $F2_i = a_i \cdot W_i$，令$F_i = (F1_i, F2_i)$为车辆假名。

(6) 签名算法(sign)：设消息为m_i，车辆选择$r_i \in {}_RZ_q^*$，求$U_i = r_i \cdot P$，$h_i = H_1(m_i, F1_i, P_i, U_i)$，$V_i = p_i \cdot F2_i + h_i \cdot r_i \cdot P_K + h_i \cdot x_i \cdot \overline{P}$，$\sigma_i = (U_i, V_i)$。

(7) 验证算法(verify)：RSU输入消息和签名(m_i, σ_i)、车辆公钥P_i、假名F_i以及paras，计算$h_i = H_1(m_i, F1_i, P_i, U_i)$, $W_i = H_2(F1_i)$，并且验证$e(V_i, P) = e(F1_i \cdot W_i + h_i \cdot U_i, P_K) e(h_i \cdot P_i, \overline{P})$是否成立。若成立，则接受消息，反之丢弃。

(8) 聚合签名算法(aggregate)：RSU输入n个消息签名(m_i, σ_i)，计算聚合签名$V = \sum_{i=1}^{n} V_i$，聚合消息即为$\{\{m_i\}_{i=1}^n, \{U_i\}_{i=1}^n, V\}$。

(9) 聚合验证算法(aggregate verify)：TA或数据中心执行本算法。输入从某一个RSU(其公钥为$\overline{P}$)发送过来的n个消息的聚合签名$\{\{m_i\}_{i=1}^n, \{U_i\}_{i=1}^n, V\}$，对每个单一消息$m_i$计算$h_i = H_1(m_i, F1_i, P_i, U_i)$，$W_i = H_2(F1_i)$，并验证：$e(V, P) = e\left(\sum_{i=1}^{n} (F1_i \cdot W_i + h_i \cdot U_i), P_K\right) \cdot e\left(\sum_{i=1}^{n} (h_i \cdot P_i), \overline{P}\right)$。

2.2 王大星等人的CLAS方案的安全问题

本节分析王大星等人方案无法抵抗恶意KGC的攻击、无法实现隐私保护，并且身份追踪性不足等问题。

(1) 恶意KGC攻击：恶意的KGC监听到某一有效消息$(m_i, F_i, P_i, \sigma_i = (U_i, V_i))$。由于KGC已知$s$，能计算出$p_i = s \cdot \mathrm{ID}_i^{'}$。

伪造虚假消息：令$h_i^{-1} = (H_1(m_i, F1_i, P_i, U_i))^{-1}$, $T = \left(r_i \cdot P_K + x_i \cdot \overline{P}\right) = h_i^{-1} \cdot (V_i - p_i \cdot F2_i)$。设伪造消息为$m'$，则$h = H_1(m^{'}, F1_i, P_i, U_i)$ $V' = p_i \cdot F2_i + h \cdot T = p_i \cdot F2_i + h \cdot (r_i \cdot P_K + x_i \cdot \overline{P})$，即攻击者可成功伪造消息签名。

(2) 无法实现车辆隐私保护：当注册车辆ID_i到达某一个RSU的通信区域中，为了获得临时假名F_i，向RSU发送由TA所分配的假身份$\mathrm{ID}_i^{'}$，这是以明文方式发送，在一定程度上泄露车辆信息。另外，每一次消息发送过程，必须向验证者提供车辆公钥P_i，方案的P_i则为一成不变的，这会成为敌手在追踪车辆时的重要信息。

(3) 方案提供的身份追踪功能可操作性不强：当注册车辆ID_i到达某一个RSU的通信区域内，为了获得临时假名F_i，向RSU发送由TA所分配的假身份$\mathrm{ID}_i^{'}$，然后RSU选择$a_i \in {}_RZ_q^*$，计算，$W_i = H_2(F1_i)$, $F2_i = a_i \cdot W_i$,令$F_i = (F1_i, F2_i)$为车辆假名。

一般来说，虚假消息无法在短时间内被甄别出来，具有一定的滞后性。一个RSU在短时间内车辆加入与退出数量庞大，车辆的临时假名更新频繁且数据量大的惊人。RSU的存储量有限，无法存储与$\mathrm{ID}_i^{'}$所对应的a_i及$F1_i = a_i \cdot \mathrm{ID}_i^{'}$。若所有RSU的数据都存储到后台数据库中，则成了海量数据，查询时工作量繁重。因此，车辆真实身份的追踪功能的可操作性并不可观。

3 改进的方案

为了克服王大星等人的CLAS方案的不足，本节提出一种改进的无证书聚合签名方案。本方案共包含9个算法。

(1) 系统建立算法(setup)：KGC选取一个椭圆曲线$E_p(a, b)$: $y^2 = x^3 + ax + b \bmod p$，其中$p$为一个大素数，$a, b \in F_p$。同时选取一个$E_p(a, b)$的点$P$作为群$G$的生成元，设$G$的阶为$q$, G也包含了无穷远点Q。设$s \in {}_RZ_q^*$为系统主密钥，则系统公钥为$P_K = s \cdot P$。本算法选取了5个可证安全的$h_1, h_2, h_3, h_4, h_5 : \{0,1\}^* \to Z_q^*$作为系统Hash函数。

每个RSU设立各自的秘密值$y_k \in {}_RZ_q^*$，则其公钥为$\overline{P}_k = y_k \cdot P$，并发送给KGC。最后，KGC公开系统的参数列表：$\mathrm{paras} = \{E_p(a, b), p, q, G, P, P_K, h_1, h_2, h_3, h_4, h_5, \overline{P_i}\}$。

(2) 车辆注册算法(registration)：令车辆的真实身份信息为RID_i, TA生成其假身份$\mathrm{ID}_i = h_1(\mathrm{RID}_i, T_{\mathrm{reg}})$，这里$T_{\mathrm{reg}}$为注册时间，保存$\{\mathrm{RID}_i, \mathrm{ID}_i, T_{\mathrm{reg}}\}$，并将$\mathrm{ID}_i$发送给KGC。

(3) 部分私钥生成算法(PartialKeyGen)：本算法由KGC执行。KGC输入paras, s和ID_i，随机选取$u_i \in {}_RZ_q^*$，并计算$U_i = u_i \cdot P$, $h_{ui} = h_2(U_i, P_K)$, $s_{vi} = u_i + h_{ui} s \bmod q$，并且将$\{U_i, s_{vi}\}$通过安全方式传给车辆$\mathrm{ID}_i$，车辆部分私钥为$s_{vi}$。

(4)用户密钥生成算法(UserKeyGen)：车辆执行本算法，生成其秘密值和公钥。车辆ID_i选择$x_i \in {}_RZ_q^*$，公钥为$X_i = x_i \cdot P$。

(5) 假名生成算法(PseudonymGen): RSU(其公私钥为$(\overline{P}_k, y_k)$)为车辆执行本算法，生成车辆的临时假名。RSU使用当前时间T_i，计算$\mathrm{ID}_i^* = \mathrm{ID}_i \oplus h_3(y_k \cdot X_i, T_i)$，并令$F_i = (\mathrm{ID}_i^*, T_i)$为车辆假名，发送给车辆。

(6)签名算法(sign)：本算法为车辆消息m_i签名。车辆ID$_i$令$r_i \in {}_RZ_q^*$，并且计算$R_i = r_i \cdot P$, $h_i = h_4(m_i, F_i, X_i, U_i, R_i)$ ， $h_{xi} = h_5(m_i, U_i, F_i, R_i, X_i)$ ，$v_i = r_i + h_i s_{vi} + h_{xi} x_i \bmod q$，令$\sigma_i = (R_i, v_i)$为消息的签名。

(7) 验证算法(verify): RSU执行本算法。输入消息及其签名(m_i, σ_i)、车辆公钥P_i、假名F_i以及系统参数paras，计算$h_i = h_4(m_i, F_i, X_i, U_i, R_i)$, $h_{xi} = h_5(m_i, U_i, F_i, R_i, X_i)$, $h_{ui} = h_2(U_i, P_K)$，验证下式是否成立：

$v_i \cdot P = R_i + h_i \cdot U_i + h_i h_{ui} \cdot P_K + h_{xi} \cdot X_i$， 若成立，则接受该消息，否则，丢弃该消息。

证明如下：

$$\begin{aligned} L.H.S &= v_i \cdot P \\ &= (r_i + h_i s_{v_i} + h_{xi} x_i) \cdot P \\ &= r_i \cdot P + h_i s_{v_i} \cdot P + h_{xi} x_i \cdot P \\ &= R_i + h_i (u_i + h_{ui} s) \cdot P + h_{xi} \cdot X_i \\ &= R_i + h_i u_i \cdot P + h_i h_{ui} s \cdot P + h_{xi} \cdot X_i \\ &= R_i + h_i \cdot U_i + h_i h_{ui} \cdot P_K + h_{xi} \cdot X_i \\ &= R.H.S \end{aligned}$$

(8) 聚合签名算法(aggregate): RSU执行本算法。输入n个消息签名(m_i, σ_i)，计算签名的聚合为$v = \sum_{i=1}^{n} v_i$，然后聚合消息为$\{\{m_i, F_i, X_i, U_i, R_i\}_{i=1}^n, v\}$。

(9) 聚合验证算法(aggregate verify): TA或数据中心执行本算法。输入从某一个RSU(其公钥为$\overline{P}_K$)发送过来的n个消息的聚合签名$\{\{m_i, F_i, X_i, U_i, R_i\}_{i=1}^n, v\}$，对每个单一消息$m_i$计算，$h_{ui} = h_2(U_i, P_K)$, $h_i = h_4(m_i, F_i, X_i, U_i, R_i)$, $h_{xi} = h_5(m_i, U_i, F_i, R_i, X_i)$，然后通过下式验证：

$$\begin{aligned} v \cdot P = &\sum_{i=1}^{n} R_i + \sum_{i=1}^{n} h_i \cdot U_i + \left(\sum_{i=1}^{n} h_i h_{ui}\right) \\ &\cdot P_K + \sum_{i-1}^{n} h_{xi} \cdot X_i \end{aligned}$$

4 安全性分析

4.1 安全模型

本文改进的认证方案借鉴了无证书公钥签名思想，依据文献[18]定义的安全攻击模型，本文方案的安全性考虑两类不同级别的攻击敌手：

普通敌手$\mathcal{A}_{\mathcal{I}}$：$\mathcal{A}_{\mathcal{I}}$表示了普通的第三攻击者，不能够获取系统主密钥$s$，但可以获取或更改用户私有密钥$x$与其对应公钥$X$。

超级敌手$\mathcal{A}_{\mathcal{II}}$：$\mathcal{A}_{\mathcal{II}}$代表具有更高级别的攻击能力，能够攻陷KGC，获取系统主密钥s，但不能够获得与更改用户私有密钥x。

4.2 安全性证明

定理1 假定敌手$\mathcal{A}_{\mathcal{I}}$在攻击游戏中经过多项式次随机预言机询问，能够成功伪造一个签名的优势为ε，在多项式时间内的优势为

$$\begin{aligned} \varepsilon' \geq &\left(1 - \frac{q_{h2}}{q}\right)^{q_c} \left(1 - \frac{1}{q_c}\right)^{q_k} \left(1 - \frac{q_{h3}}{q}\right) \\ &\cdot \left(1 - \frac{q_{h4}}{q}\right) \left(1 - \frac{q_{h5}}{q}\right) \frac{1}{q_c} \varepsilon \end{aligned}$$

其中q_{hi}表示对应h_i预言机查询次数，q_c表示创建用户预言机查询次数，q_k表示部分私钥查询次数。

证明 假设一个敌手$\mathcal{A}_{\mathcal{I}}$在本文方案中能以优势$\varepsilon$成功伪造目标用户ID$_i$的有效签名。设给定一个挑战者$\mathcal{C}$，利用可以解决ECDLP问题$(P, Q = s \cdot P)$。$\mathcal{C}$与$\mathcal{A}_{\mathcal{I}}$进行如下游戏交互。

初始化阶段：$\mathcal{C}$构建系统，并令$Q = P_K$，并公开系统参数paras，建立并维护5个列表，分别是L_{h2}列表$(\mathrm{ID}, U, \mathrm{PK}, \tau_{h2})$, L_{h3}列表$(\mathrm{ID}, X, \tau_{h3})$, L_u列表$(\mathrm{ID}, m, F, X, U)$以及$L_s$的列表$(\mathrm{ID}, m,\ F, X, U, \tau_{h4}, \tau_{h5}, R, v)$。

预言机查询阶段：在本阶段，$\mathcal{A}_{\mathcal{I}}$与$\mathcal{C}$之间进行预言机交互。

h_2预言机查询：当$\mathcal{A}_{\mathcal{I}}$询问ID，若$L_{h2}$中已有，则返回$\tau_{h2}$给$\mathcal{A}_{\mathcal{I}}$；若没有，则$\mathcal{C}$先执行部分私钥预言机查询，并随机选取$u \in Z_q^*$，计算$U = u \cdot P$，然后计算$\tau_{h2} = h_2(U_i, P_K)$，并返回$\tau_{h2}$给$\mathcal{A}_{\mathcal{I}}$。

h_3预言机查询：当$\mathcal{A}_{\mathcal{I}}$以ID进行询问，若$L_{h3}$中已有相应元组，则返回$\tau_{h3}$给$\mathcal{A}_{\mathcal{I}}$；若没有$X$，则先执行用户秘密值预言机查询，并随机选择$a \in Z_q^*$，然后计算$\tau_{h3} = h_3(a \cdot X, T_i)$，并返回$\tau_{h3}$给$\mathcal{A}_{\mathcal{I}}$。

h_4预言机查询：当$\mathcal{A}_{\mathcal{I}}$询问$(\mathrm{ID}, m)$，若$L_u$中已有，则返回$\tau_{h4}$给$\mathcal{A}_{\mathcal{I}}$；若没有对应的$X$，则先执行用户密钥预言机查询，部分私钥预言机查询，然后计算$\tau_{h4} = h_4(m, F, X, U, R)$，并返回$\tau_{h4}$给$\mathcal{A}_{\mathcal{I}}$。

h_5预言机查询：当$\mathcal{A}_{\mathcal{I}}$询问$(\mathrm{ID}, m)$，若$L_s$中已有，则返回$\tau_{h5}$给$\mathcal{A}_{\mathcal{I}}$；若无，则先执行用户密钥预言机查询，部分私钥预言机查询，然后计算$\tau_{h5} = h_5(m_i, U_i, F_i, R_i, X_i)$，并返回$\tau_{h5}$给$\mathcal{A}_{\mathcal{I}}$。

用户创建预言机查询：当$\mathcal{A}_{\mathcal{I}}$以(ID)进行询问时，$\mathcal{C}$查询$L_u$，若无对应的元组，则进行如下操作：若ID = ID$_t$时，$\mathcal{C}$随机选择$u, \tau_{h2}, x \in Z_q^*$，计算$U = u \cdot P$, $X = x \cdot P$, $s_v = \perp$；当ID $\neq$ ID$_t$时，$\mathcal{C}$随机选择$s_v, u, \tau_{h2}, x \in Z_q^*$，计算$X = x \cdot P$, $U = s_v \cdot P - \tau_{h2} \cdot Q$，然后将其加到相应列表中。若有相应元组，$\mathcal{C}$查询$L_{h2}$，若存在相应的$(\mathrm{ID}, U, \tau_{h2})$，验证是否满足$\tau_{h2} \leftarrow h_2(U, Q)$，不满足，$\mathcal{C}$结束本次游戏；否则返回用户信息。

用户秘密值预言机查询：当$\mathcal{A}_{\mathcal{I}}$以ID进行此询问时，$\mathcal{C}$查询$L_u$，若$L_u$中已有对应元组，$\mathcal{C}$返回

(X,x)给$\mathcal{A}_{\mathrm{I}}$，否则，$\mathcal{C}$随机选择$x\in Z_q^*$，计算$X=x\cdot P$，并将(X,x)返回给$\mathcal{A}_{\mathrm{I}}$。

部分私钥预言机查询：假设游戏$\mathcal{A}_{\mathrm{I}}$最多进行q_k次本询问。当$\mathrm{ID}=\mathrm{ID}_t$时，$\mathcal{C}$输出“$\perp$”并结束游戏。当$\mathrm{ID}\neq\mathrm{ID}_t$时，$\mathcal{C}$查询$L_u$，若$L_u$中已有对应元组，$\mathcal{C}$返回$(U,s_v)$给$\mathcal{A}_{\mathrm{I}}$，否则，$\mathcal{C}$随机选择$u,s_v\in Z_q^*$，计算$U=u\cdot P$，并将$(U,s_v)$返回给$\mathcal{A}_{\mathrm{I}}$。

公钥预言机查询：当$\mathcal{A}_{\mathrm{I}}$以ID进行此询问时，$\mathcal{C}$查询L_u，若L_u中已有对应元组，$\mathcal{C}$返回(U,X)给$\mathcal{A}_{\mathrm{I}}$，否则，$\mathcal{C}$执行部分私钥预言机查询与用户秘密值预言机查询，并将U,X返回给$\mathcal{A}_{\mathrm{I}}$。

签名预言机查询：当$\mathcal{A}_{\mathrm{I}}$以$(\mathrm{ID}_i,U_i,m_i,F_i)$进行查询时，$\mathcal{C}$随机选择$v_i,h_i,h_{xi}\in Z_q^*$，计算$\tau_{h2i}=h_2(U_i,P_K)$，并将$\{U_i,\tau_{h2i}\}$加入到$L_{h2}$中。令：$R_i=v_i\cdot P-h_iU_i-h_i\tau_{h2i}Q-\tau_{h5i}X_i$，将$(m_i,R_i,v_i,U_i)$插入到$L_s$与$L_u$中。

输出阶段：最后，$\mathcal{A}_{\mathrm{I}}$输出(ID,U,m)的一个伪造签名。若$\mathrm{ID}_i\neq\mathrm{ID}_t$, $\mathcal{C}$宣布失败；否则，$\mathcal{C}$从预言机查询列表中找到相应签名信息：$(m_i,\sigma_i=(U_i,v_i),R_i,X_i,F_i)$。若$\mathcal{A}_{\mathrm{I}}$赢得了该游戏，则有

$$v_i\cdot P=R_i+h_i\cdot U_i+h_i\tau_{h2i}\cdot Q+h_{xi}\cdot X_i \tag{1}$$

依据分叉引理[19]，$\mathcal{A}_{\mathrm{I}}$能够在多项式时间内以不同的v_i与h_i重新构造消息的另一个有效签名$(m_i,\sigma_i^*=(U_i,v^*),R_i^*,X_i,F_i)$，即满足

$$v_i^*\cdot P=R_i^*+h_i^*\cdot U_i+h_i^*\tau_{h2i}\cdot Q+h_{xi}\cdot X_i \tag{2}$$

依据式(1)与式(2), $\mathcal{C}$可以计算出

$$(v_i-v_i^*)\cdot P=(h_i-h_i^*)\tau_{h2i}\cdot Q=(h_i-h_i^*)\tau_{h2i}s\cdot P \tag{3}$$

由式(3)得出$s=\dfrac{(v_i-v_i^*)}{(h_i-h_i^*)\tau_{h2i}}\bmod q$，即$\mathcal{C}$解决了ECDLP问题。

接下来，评估$\mathcal{C}$成功解决ECDLP问题的优势问题。

E_1: $\mathcal{C}$并没有终止过游戏。

E_2: v_i^*是一个关于消息(ID_t,m_t)的有效签名。

即优势为：$\varepsilon'=\Pr[E_1\wedge E_2]=\Pr[E_1]Pr[E_2|E_1]$，其中，$Pr[E_2|E_1]=\varepsilon$。依据游戏分析，可以得到：

$$\Pr[E_1]\geq\left(1-\frac{q_{h2}}{q}\right)^{q_c}\left(1-\frac{1}{q_c}\right)^{q_k}\left(1-\frac{q_{h3}}{q}\right)\cdot\left(1-\frac{q_{h4}}{q}\right)\left(1-\frac{q_{h5}}{q}\right)\frac{1}{q_c}$$

。因而，可以得到下述不等式：

$$\varepsilon'=\Pr[E_1\wedge E_2]\geq\left(1-\frac{q_{h2}}{q}]\right)^{q_c}\left(1-\frac{1}{q_c}\right)^{q_k}\cdot\left(1-\frac{q_{h3}}{q}\right)\left(1-\frac{q_{h4}}{q}\right)\left(1-\frac{q_{h5}}{q}\right)\frac{1}{q_c}\varepsilon$$

显然，若敌手$\mathcal{A}_{\mathrm{I}}$具有成功伪造一个签名的优势ε，那$\mathcal{A}_{\mathrm{I}}$就能够解决ECDLP问题，这与在随机预言机模型下ECDLP问题为困难问题相冲突。即可证明定敌手的优势ε是不存在，本文方案可以抵抗敌手$\mathcal{A}_{\mathrm{I}}$的伪造攻击。　　证毕

定理2　假定敌手$\mathcal{A}_{\mathrm{II}}$在攻击游戏中经过多项式次随机预言机询问，能成功伪造目标ID_t一个有效签名优势为ε，在多项式时间内的优势满足不等式：

$$\varepsilon'\geq\left(1-\frac{q_{h2}}{q}\right)^{q_c}\left(1-\frac{1}{q_c}\right)^{q_x}\left(1-\frac{1}{q_c}\right)^{q_r}\cdot\left(1-\frac{q_{h3}}{q}\right)\left(1-\frac{q_{h4}}{q}\right)\left(1-\frac{q_{h5}}{q}\right)\frac{1}{q_c}\varepsilon$$

其中q_{hi}表示对应h_i预言机查询次数，q_c表示创建用户预言机查询次数，q_x表示用户秘密值查询次数，q_r表示用户公钥查询次数。

通过本定理的证明，可以说明本文方案能够抵抗$\mathcal{A}_{\mathrm{II}}$的安全攻击。此定理的证明过程在此不再陈述。

5　性能分析

5.1　计算开销分析

对于VANETs来讲，在保证网络安全性的前提下，认证产生的计算开销量和通信开销量是衡量这个认证方案的最重要的指标之一。本节在计算和通信开销方面对本文方案以及王大星等人[8]方案和Zhong等人[17]方案做性能分析。

王大星等人方案以及Zhong等人方案采用双线性算法构建了签名方案，本文方案采用运算量更少的椭圆曲线密码构建了签名方案。为了更合理地比较3个方案的性能，本文同时构建了2个安全级别均为80 bit的密码运算方案。其一为双线性对密码运算方案：$e:G_1\times G_1\to G_2$, G_1是一个阶为$\bar{q}$的加法群，生成元为$\bar{P}$, $\bar{P}$是度为2的超奇异曲线$E:y^2=x^3+ax+b \bmod \bar{p}$上的点，$\bar{p}$, $\bar{q}$分别是512 bit, 160 bit的素数；其二为椭圆曲线运算方案：以P构建一个阶为q的非超奇异曲线$\bar{E}:y^2=x^3+ax+b \bmod p$的加法群$G$，其中$p$, q均为160 bit的素数，$a,b\in Z_q^*$。参照文献[15]的性能评估方法，本文利用 MIRACL库，在Win7的操作系统，2.4 GHz的CPU主频，以及4 GB内存的环境下，实现了2种密码运算方案中的密码运算，并记录了各个密码运算的执行时间。表1是密码运算对应缩写及执行时间[15]。

根据表1中密码运算的执行时间，可以得到在王大星等人的方案中，签名算法过程包括4个T_{dm}, 2个T_{da}和1个T_{h}，总开销为$4T_{\mathrm{dm}}+2T_{\mathrm{da}}+T_{\mathrm{h}}$；单一验证算法过程包含3个$T_{\mathrm{d}}$, 3个$T_{\mathrm{dm}}$, 1个$T_{\mathrm{da}}$和2个$T_{\mathrm{h}}$，总开销为$3T_{\mathrm{d}}+3T_{\mathrm{dm}}+T_{\mathrm{da}}+2T_{\mathrm{h}}$；聚合验证算法过程中，包括3个$T_{\mathrm{d}}$, $3n$个T_{dm}, $3n$–2个T_{da}和$2n$个T_{h}，总开销为$3T_{\mathrm{d}}+3nT_{\mathrm{dm}}+(3n-2)T_{\mathrm{da}}+2nT_{\mathrm{h}}$。同样可

表 1 密码运算的执行时间(ms)

运算操作名称	
双线性对	双线性对运算，e
	乘法运算，$x \cdot P$
	加法运算，$P+Q$
椭圆曲线	乘法运算，$x \cdot Q$
	加法运算，$P+Q$
单向Hash运算	

以得到Zhong等人方案的3个算法的计算开销，如表2所示。

在本文方案中，签名算法过程包括1个T_{em}和2个T_{h}，总开销为$T_{\mathrm{em}}+2T_{\mathrm{h}}$；单一验证算法过程，主要包含4个$T_{\mathrm{em}}$、3个$T_{\mathrm{ea}}$和3个$T_{\mathrm{h}}$，总开销为$4T_{\mathrm{em}}+3T_{\mathrm{ea}}+3T_{\mathrm{h}}$；聚合签名算法过程包括$2n$+2个$T_{\mathrm{em}}$、$3n$个$T_{\mathrm{ea}}$和$3n$个$T_{\mathrm{h}}$，总开销为$(2n+2)T_{\mathrm{em}}+3nT_{\mathrm{ea}}+3nT_{\mathrm{h}}$。

根据表2中给出的3种方案在3个过程中所需的计算开销可以看到，在签名阶段，本文方案相较于王大星等人方案以及Zhong等人的方案在计算开销上减少了约93%，在单一验证阶段，本文方案的计算开销比王大星等人方案减少了约89%，比Zhong等人的方案减少了87%，而在聚合验证阶段下，3种方案的计算开销都随消息数量增加而呈线性增长。由图1可见，在消息数量增加过程中，本文方案的计算开销增长率远小于另外两种方案。

由以上分析知，从计算开销的层面上看，本文提出的方案要远优于王大星等人的方案以及Zhong等人的方案。

5.2 通信开销分析

在5.1节的分析中，$\bar{p}$和p所占的字节数分别为64 Byte和20 Byte，那么，群G_1和群G内元素所占的字节数为128 Byte和40 Byte。假定VANETs中车辆假名生成的时间T_i所占的字节数为4 Byte。表3给出了3种方案所需要额外增加的通信开销。相比王大星等人以及Zhong等人的方案，本文方案通信开销量分别减少了约75%和80%。可见，本文方案更适用VANETs。

表 2 计算开销比较(ms)

	签名算法	验证算法	聚合验证算法
Wang方案	$4T_{\mathrm{dm}}+2T_{\mathrm{da}}+T_{\mathrm{h}}\approx 10.605$	$3T_{\mathrm{d}}+3T_{\mathrm{dm}}+T_{\mathrm{da}}+2T_{\mathrm{h}}\approx 27.1959$	$3T_{\mathrm{d}}+3nT_{\mathrm{dm}}+(3n-2)T_{\mathrm{da}}+2nT_{\mathrm{h}}\approx 7.9759n+19.22$
Zhong方案	$4T_{\mathrm{dm}}+2T_{\mathrm{da}}+2T_{\mathrm{h}}\approx 10.6052$	$3T_{\mathrm{d}}+2T_{\mathrm{dm}}+T_{\mathrm{da}}+2T_{\mathrm{h}}\approx 24.5376$	$3T_{\mathrm{d}}+2nT_{\mathrm{dm}}+(2n-1)T_{\mathrm{da}}+2nT_{\mathrm{h}}\approx 5.3174n+19.2346$
本文方案	$T_{\mathrm{em}}+2T_{\mathrm{h}}\approx 0.7362$	$4T_{\mathrm{em}}+3T_{\mathrm{ea}}+3T_{\mathrm{h}}\approx 2.9558$	$(2n+2)T_{\mathrm{em}}+3nT_{\mathrm{ea}}+3nT_{\mathrm{h}}\approx 1.4842n+1.4716$

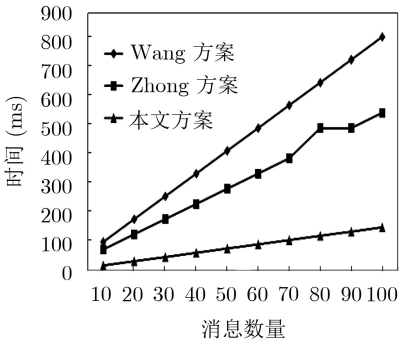

图 1 认证开销与消息数量的关系

表 3 通信开销比较

方案	消息	通信开销(Byte)
Wang方案	$\{m_i,\delta_i=(U_i,V_i),$ $P_i,F_i=(F1_i,F2_i)\}$	576
Zhong方案	$\left\{\begin{array}{c} m_i,\mathrm{PID}_i,\mathrm{vpk}_i,\\ t_i,\sigma_i=(R_i,T_i)\end{array}\right\}$	724
本文方案	$\{m_i,\delta_i=(U_i,v_i),$ $P_i,F_i=(\mathrm{ID}_i^*,T_i)\}$	140

6 结束语

本文分析了王大星等人提出的VANETs无证书聚合签名方案的不足，并提出了一种改进的可证安全的无证书聚合方案。本文方案采用了椭圆曲线密码构建了聚合签名与认证算法，摒弃了复杂的双线对密码运算却达到了更高安全级别要求，并且给出了严格的安全性分析，证明本文方案满足VANETs对各种安全的需求。与王大星等人以及Zhong等人方案的性能分析对比表明，本文方案在签名、单一消息验证和聚合消息验证算法的计算开销减少许多，同时降低了方案的通信开销。

车联网对于消息签名与认证效率有着极高的要求，因而下一步的工作是研究面向车联网的轻量级认证方案。

参 考 文 献

[1] 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. doi: 10.11959/j.issn.1000-436x.2015253.
LIU Zhe, LIU Jianwei, WU Qianhong, *et al*. Secure and efficient distributed pseudonym generation in VANET[J]. *Journal on Communications*, 2015, 36(11): 33–40. doi: 10.11959/j.issn.1000-436x.2015253.

[2] ZHANG Hui. Insecurity of a certificateless aggregate

signature scheme[J]. *Security and Communication Networks*, 2016, 9(11): 1547–1552. doi: 10.1002/sec.1447.

[3] HA J. An efficient and robust anonymous authentication scheme in global mobility networks[J]. *International Journal of Security and Its Applications*, 2015, 9(10): 297–312. doi: 10.14257/ijsia.2015.9.10.27.

[4] SHEN Limin, MA Jianfeng, LIU Ximeng, *et al*. A provably secure aggregate signature scheme for healthcare wireless sensor networks[J]. *Journal of Medical Systems*, 2016, 40(11): No. 244. doi: 10.1007/s10916-016-0613-3.

[5] IWASAKI T, YANAI N, INAMURA M, *et al*. Tightly-secure identity-based structured aggregate signature scheme under the computational Diffie-Hellman assumption[C]. The 30th IEEE International Conference on Advanced Information Networking and Applications, Crans-Montana, Australia, 2016: 669–676. doi: 10.1109/AINA.2016.99.

[6] HORNG S J, TZENG S F, HUANG P H, *et al*. An efficient certificateless aggregate signature with conditional privacy-preserving for vehicular sensor networks[J]. *Information Sciences*, 2015, 317: 48–66. doi: 10.1016/j.ins.2015.04.033.

[7] 宋成, 张明月, 彭维平, 等. 基于非线性对的车联网无证书批量匿名认证方案研究[J]. 通信学报, 2017, 38(11): 35–43. doi: 10.11959/j.issn.1000-436x.2017227.

SONG Cheng, ZHANG Mingyue, PENG Weiping, *et al*. Research on pairing-free certificateless batch anonymous authentication scheme for VANET[J]. *Journal on Communications*, 2017, 38(11): 35–43. doi: 10.11959/j.issn.1000-436x.2017227.

[8] 王大星, 滕济凯. 车载网中可证安全的无证书聚合签名算法[J]. 电子与信息学报, 2018, 40(1): 11–17. doi: 10.11999/JEIT170340.

WANG Daxing and TENG Jikai. Probably secure cetificateless aggregate signature algorithm for vehicular ad hoc network[J]. *Journal of Electronics & Information Technology*, 2018, 40(1): 11–17. doi: 10.11999/JEIT170340.

[9] BAYAT M, BARMSHOORY M, RAHIMI M, *et al*. A secure authentication scheme for VANETs with batch verification[J]. *Wireless Networks*, 2014, 21(5): 1733–1743. doi: 10.1007/s11276-014-0881-0.

[10] CHEN L, CHENG Z, and SMART N P. Identity-based key agreement protocols from pairings[J]. *International Journal of Information Security*, 2007, 6(4): 213–241. doi: 10.1007/s10207-006-0011-9.

[11] ZHANG Chenxi, LU Rongxing, LIN Xiaodong, *et al*. An efficient identity-based batch verification scheme for vehicular sensor networks[C]. The 27th IEEE Conference on Computer Communications, Phoenix, USA, 2008: 246–250. doi: 10.1109/INFOCOM.2008.58.

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

[13] LEE C C and LAI Yanming. Toward a secure batch verification with group testing for VANET[J]. *Wireless Networks*, 2013, 19(6): 1441–1449. doi: 10.1007/s11276-013-0543-7.

[14] 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. doi: 10.1016/j.adhoc.2010.05.005.

[15] 吴黎兵, 谢永, 张宇波, 等. 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. doi: 10.11959/j.issn.1000-436x.2016211.

WU Libing, XIE Yong, ZHANG Yubo, *et al*. Efficient and secure message authentication scheme for VANET[J]. *Journal on Communications*, 2016, 37(11): 1–10. doi: 10.11959/j.issn.1000-436x.2016211.

[16] LU Rongxing, LIN Xiaodong, ZHU Haojin, *et al*. ECPP: Efficient conditional privacy preservation protocol for secure vehicular communications[C]. The 27th Conference on Computer Communications, Phoenix, USA, 2008: 1229–1237. doi: 10.1109/INFOCOM.2008.179.

[17] ZHONG Hong, HAN Shunshun, CUI Jie, *et al*. Privacy-preserving authentication scheme with full aggregation in VANET[J]. *Information Sciences*, 2019, 476: 211–221. doi: 10.1016/j.ins.2018.10.021.

[18] JIA Xiaoying, HE Debiao, LIU Qin, *et al*. An efficient provably-secure certificateless signature scheme for internet-of-things deployment[J]. *Ad Hoc Networks*, 2018, 71: 78–87. doi: 10.1016/j.adhoc.2018.01.001.

[19] POINTCHEVAL D and STERN J. Security proofs for signature schemes[C]. International Conference on the Theory and Applications of Cryptographic Techniques, Saragossa, Spain, 1996: 387–398.

谢　永：男，1978年生，博士，副教授，硕士生导师，研究方向为物联网、通信与安全、密码学等.

李　香：女，1996年生，硕士生，研究方向为车联网、同态加密、密码学等.

张松松：女，1994年生，硕士生，研究方向为口令安全、信息安全、密码学等.

吴黎兵：男，1972年生，博士，教授，博士生导师，研究方向为车联网，通信安全，分布式计算等.