车载网中可证安全的无证书聚合签名算法

王大星*① 滕济凯②
①(滁州学院数学与金融学院 滁州 239000)
②(青岛理工大学理学院 青岛 266555)

摘 要：为了实现车载自组织网络中车辆节点之间信息传输的安全认证，该文设计了一种无证书聚合签名方案。提出的方案采用无证书密码体制，消除了复杂的证书维护成本，同时也解决了密钥托管问题。通过路侧单元生成的假名与周围节点进行通信，实现了车辆用户的条件隐私保护。在随机预言模型下，证明了方案满足自适应选择消息攻击下的存在性不可伪造。然后，分析了方案的实现效率，并模拟实现了车载自组网(VANET)环境中车流密度与消息验证的时间延迟之间的关系。结果表明，该方案满足消息的认证性、匿名性、不可伪造性和可追踪性等性质，并且通信效率高、消息验证的时延短，更适合于动态的车载自组织网络环境。

关键词：车载自组网；聚合签名；无证书密码；随机预言模型
中图分类号：TP309; TN915 **文献标识码**：A **文章编号**：1009-5896(2018)01-0011-07
DOI: 10.11999/JEIT170340

Probably Secure Cetificateless Aggregate Signature Algorithm for Vehicular Ad hoc Network

WANG Daxing① TENG Jikai②
①(*School of Mathematics and Finance*, *Chuzhou University*, *Chuzhou* 239000, *China*)
②(*College of Science*, *Qingdao Technological University*, *Qingdao* 266555, *China*)

Abstract: In order to realize the security authentication of the information transmission between vehicle nodes in vehicular Ad hoc networks, a certificateless aggregate signature scheme is designed. The proposed scheme uses certificateless cryptography, which eliminates the complex maintenance cost of certificate and solves the problem of key escrow. Communicating through pseudonyms and nodes around the roadside units generated, the conditional privacy protection is achieved for vehicle users. In the random oracle model, the scheme is proved to be existentially unforgeable against adaptive chosen message attack. Then, the efficiency of the scheme is analyzed, and the relationship between the traffic density in Vehicular Ad hoc NETwork (VANETs) environment and the time delay of message verification is simulated. The results show that the scheme satisfies the message authentication, anonymity, unforgeability and traceability, as well as the higher communication efficiency and the shorter delay of message verification, which is more suitable for dynamic vehicular Ad hoc network environment.

Key words: Vehicular Ad hoc NETwork (VANET); Aggregate signature; Certificateless cryptosystem; Random oracle model

1 引言

车载自组织网络(Vehicular Ad hoc NETwork, VANET)是一种多跳并且高速移动的无线通信网络。作为未来智能交通的基础，VANET为车辆间的通信提供了一个重要的网络环境，可以有效解决道路安全、交通管理以及交通拥堵问题，是当前研究领域的一个热点方向。车载网络主要由安装在车辆上的车载单元(OnBoard Units, OBU)和部署在道路周围基础设施上的路侧单元(RoadSide Units, RSU)组成。用户通过车辆与车辆之间(Vehicle-to-Vehicle, V2V)、车辆与基础设施之间(Vehicle-to-Infrastructure, V2I)的通信，来共享信息和访问临近基础设施所提供的各种服务[1]。

然而，车载网络由于它自身的特点，如资源受限、节点的高速移动、通信延迟应足够短等，使得其安全问题变得很脆弱，包括窃听、篡改、跟踪用户的隐私等。较高的安全要求通常会导致认证效率

收稿日期：2017-04-17；改回日期：2017-09-05；网络出版：2017-11-01
*通信作者：王大星 daxingwang@126.com
基金项目：安徽高校自然科学研究项目(KJ2016A530)，高校优秀青年人才支持计划重点项目(gxyqZD2016330)，国家自然科学基金(61303256)
Foundation Items: The Projects of Natural Science Research of the Academic School of Anhui (KJ2016A530), The Key Projects of Support Program for Outstanding Young Talents of the Academic School (gxyqZD2016330), The National Natural Science Foundation of China (61303256)

低下，但由于车载网中车辆移动速度较快，必须保证消息认证的效率，否则安全消息得不到及时的认证，丢包率将会上升，从而导致通信效率低下。因此，减小消息验证的延迟是车载网对认证协议效率的一个关键要求。另一方面，车辆用户不希望他们的敏感信息如真实身份遭到非法追踪和恶意的分析。当发生交通事故或车主犯罪时，执法当局应该能够检索或跟踪车主的信息，以揭露他们的身份，这就是所谓的条件隐私保护。

数字签名能提供消息的认证性、完整性和不可否认性等性质。在交通密度很大的车载网的通信中，每个 RSU 或交通控制中心需要验证大量的车辆信息，将会导致大量的计算开销。但在很多情况下，这些计算必须在低带宽、低存储空间的资源受限环境中完成。聚合签名[2]是近年来被关注的一个热点，经常出现在顶级密码会议论文中，是一种有广阔前景的关键签名密码部件，对许多应用都有良好的支撑作用。聚合签名可以说是一种在数字签名领域的“批处理”和“压缩技术”：可以同时给多个消息和多个用户提供不可否认服务，可以把任意多个用户的签名压缩成一个签名。这大大减小了签名的存储空间，同时也降低了对网络带宽的要求；并且，把任意多个签名的验证简化到一次验证，大大减少了签名验证的工作量。因此，聚合签名在很大程度上提高了签名的验证与传输效率，这是聚合签名之所以被关注的主要原因。因此，VANET 中使用聚合签名可以大大减轻 RSU 的负担。

基于传统的公钥基础设施(Public Key Infrastructure, PKI)的签名是基于证书体制的，证书管理机构(Certificate Authority, CA)需要绑定用户和他的公钥，管理和维护证书的开销很大，不适合于车载网络中。基于身份的聚合签名[3,4]可以解决复杂的证书管理问题，可应用于无线网络等领域。然而，在基于身份的聚合签名方案中却存在密钥托管问题，密钥生成中心掌握着每个用户的私钥，存在着恶意伪造签名的安全问题。为了解决密钥托管问题，一些学者利用无证书密码体制[5]提出了无证书聚合签名体制[6−18]，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独立生成自己的公/私钥，从而保护了签名的安全。无证书密码体制既简化了公钥证书的管理问题，又解决了密钥托管问题，最近颇受密码学界的关注。近几年，一些有效的无证书聚合签名方案[6−11]被提出，在随机预言中是可证明安全的，但其较高的计算成本使得它并不适合于动态无线网络，如 VANETs。2014 年，He 等人[13]提出了无证书双方密钥协商协议，但双方的通信协议并不适合于规模庞大的车载自组网。2016 年，Nie 等人[18]提出了分布式无证书聚合签名方案，但它在 VANETs 中一直没有得到很好的应用，并且不能抵抗签名的伪造攻击[17]。因此，到目前为止，适合于车载网的认证方案还没有得到满意的解决。本文提出了一个适合于车载网的有效无证书聚合签名方案，车辆通过 RSU 生成一个假名，通过假名与周围节点进行通信。必要时，执法当局能够通过假名追踪车辆用户的真实身份。并且，本文的方案在随机预言模型中是可证明安全的。

2 无证书聚合签名方案的设计

一般的聚合签名由一个密钥管理中心(PKG)、n 个签名者、一个签名聚合器和一个签名验证者构成，方案由算法{Setup, PartialKeyGen, UserKey Gen, Sign, Aggregate, Aggregate Verify}构成，如图 1 所示。

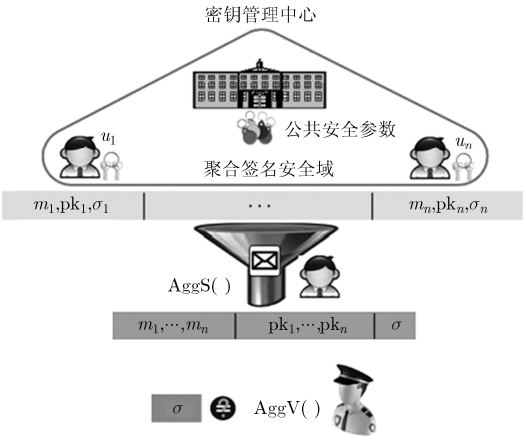

图 1 聚合签名原理图

本文设计的基于车载自组网的无证书聚合签名算法除了上述步骤以外，还包括车辆注册算法(Registration)、假名生成算法(PseudonymGen)和消息验证算法(Verify)，具体描述如下。

2.1 系统建立算法(Setup)

输入安全参数 l，密钥管理中心 KGC 选择阶为素数 q 的加法循环群 G_1 和乘法循环群 G_2，定义双线性映射 $e: G_1 \times G_1 \to G_2$，选择群 G_1 的生成元 $P \in G_1$，随机选择主密钥 $s \in Z_q^*$，计算 KGC 的公钥 $P_K = s \cdot P$，选择安全的 hash 函数 $H_1, H_2 : \{0,1\}^* \to Z_q^*$，消息集合 $M = \{0,1\}^*$。每个 RSU 选择其秘密值 $y_i \in Z_q^*$，计算公钥 $\overline{P}_i = y_i \cdot P$ 发送给 KGC。公开系统的参数列表 params，具体如下：

$$\text{params} = \{G_1, G_2, e, P, P_K, H_1, H_2, PR_i\}$$

2.2 车辆注册算法(Registration)

该算法由道路交通管理局(Road and Transport Authority, RTA)执行。对于身份信息为 ID_i 的每个车辆用户，为保护其隐私，RTA 生成他们的假身份 $\mathrm{ID}_i^{'}$。RTA 选择 hash 函数 $H_3:\{0,1\}^* \to G_1$，计算 $\mathrm{ID}_i^{'}=H_3(\mathrm{ID}_i)$。当执法机关要追查责任问题的车辆，那么 RTA 可以显示车辆的真实身份。

2.3 部分私钥生成算法(PartialKeyGen)

KGC 执行此算法，输入参数列表 params、主密钥 s 和身份 $\mathrm{ID}_i^{'}$，计算车辆用户的部分私钥 $p_i=s\cdot \mathrm{ID}_i^{'}$. 车辆用户可以通过验证等式 $e(p_i,P)=e\left(\mathrm{ID}_i^{'},P_K\right)$ 是否成立来确定正确性，这是因为

$$e(p_i,P)=e\left(s\cdot \mathrm{ID}_i^{'},P\right)=e\left(\mathrm{ID}_i^{'},s\cdot P\right)=e\left(\mathrm{ID}_i^{'},P_K\right)$$

2.4 用户密钥生成算法(UserKeyGen)

该算法生成VANETs中车辆用户的秘密值和公钥，并且车辆一旦行驶到某新的区域，新的 RTA 可更新用户的假身份。用户 U_i 随机选择秘密值 $x_i\in Z_q^*$，计算其公钥 $P_i=x_i\cdot P$。

2.5 假名生成算法(PseudonymGen)

该算法由路侧单元 RSU 执行。输入车辆用户 U_i 的身份 $\mathrm{ID}_i^{'}$ 和参数 params, RSU 随机选择 $a_i\in Z_q^*$，计算 $F1_i=a_i\cdot \mathrm{ID}_i^{'}$, $W_i=H_2(F1_i)$, $F2_i=a_i\cdot W_i$，输出假名 $F_i=F1_i+F2_i$。

2.6 签名算法(Sign)

车辆用户 U_i 要对发出的消息 m_i 签名，需要进行以下的计算过程：随机选择 $r_i\in Z_q^*$，计算

$$U_i=r_i\cdot P,\ h_i=H_1(m_i,F1_i,P_i,U_i)$$

$$V_i=p_i\cdot F2_i+h_i\cdot r_i\cdot P_K+h_i\cdot x_i\cdot \overline{P}_i,\ \sigma_i=(U_i,V_i)$$

输出消息签名 (m_i,σ_i)。

2.7 验证算法(Verify)

输入消息签名 (m_i,σ_i)、公钥 P_i、部分假名 $F1_i$ 以及参数 params，签名验证过程需要计算以下数值：

$$h_i=H_1(m_i,F1_i,P_i,U_i),\ W_i=H_2(F1_i)$$

$$e(V_i,P)\stackrel{?}{=}e(F1_i\cdot W_i+h_i\cdot U_i,P_K)e\left(h_i\cdot P_i,\overline{P}_i\right)$$

如果上式等号成立，则表明验证通过，否则表示该签名验证失败。其正确性证明如下：

$$\begin{aligned}e(V_i,P)&=e\left(p_i\cdot F2_i+h_i\cdot r_i\cdot P_K+h_i\cdot x_i\cdot \overline{P}_i,P\right)\\&=e(p_i\cdot F2_i,P)e(h_i\cdot r_i\cdot P_K,P)e\left(h_i\cdot x_i\cdot \overline{P}_i,P\right)\\&=e\left(s\cdot \mathrm{ID}_i^{'}\cdot a_i\cdot W_i,P\right)e(h_i\cdot r_i\cdot s\cdot P,P)\\&\quad\cdot e\left(h_i\cdot x_i\cdot y_i\cdot P,P\right)=e\left(a_i\cdot \mathrm{ID}_i^{'}\cdot W_i,s\cdot P\right)\\&\quad\cdot e\left(h_i\cdot r_i\cdot P,s\cdot P\right)e\left(h_i\cdot x_i\cdot P,y_i\cdot P\right)\\&=e\left(F1_i\cdot W_i,P_K\right)e\left(h_i\cdot U_i,P_K\right)e\left(h_i\cdot P_i,\overline{P}_i\right)\\&=e\left(F1_i\cdot W_i+h_i\cdot U_i,P_K\right)e\left(h_i\cdot P_i,\overline{P}_i\right)\end{aligned}$$

2.8 聚合签名算法(Aggregate)

输入 n 个车辆用户的签名 (m_i,σ_i)，聚合器计算并输出聚合签名 (m,σ)，其中，$m=\{m_1,m_2,\cdots,m_n\}$, $\sigma=(U_1,U_2,\cdots,U_n,V)$, $V=\sum_{i=1}^{n}V_i$。

2.9 聚合验证算法(Aggregate Verify)

RSU 收到 n 个用户的聚合签名，可以通过以下计算步骤验证如下：

$$h_i=H_1(m_i,F1_i,P_i,U_i),\ W_i=H_2(F1_i)$$

$$e(V,P)\stackrel{?}{=}e\left(\sum_{i=1}^{n}(F1_i\cdot W_i+h_i\cdot U_i),P_K\right)e\left(\sum_{i=1}^{n}(h_i\cdot P_i),\overline{P}\right)$$

如果上式等号成立，则表明验证通过，否则表示该签名验证失败。

3 安全性证明

定义 1 CDH 问题。设 G 是阶为素数 q 的加法循环群，随机选择 $a,b\in Z_q^*$，对于给定的 $P,aP,bP\in G$，计算 abP 是多项式时间内不能解决的困难问题。

定义 2 安全模型。无证书签名方案的设计要能抵御两种不同类型的攻击。第 1 类攻击者 A_1 不能得到 KGC 的主密钥，但可以替换其选择用户的公钥，从而可以得到任意签名者的部分私钥。第 2 类攻击者 A_2 可以访问 KGC 的主密钥，但不能替换用户的公钥。如果两个类型的攻击者成功伪造签名的概率是可忽略的，则认为无证书签名方案是自适应选择消息攻击下存在性不可伪造的。一般来说挑战者 C 维护一个列表包含车辆用户身份信息、秘密值、公钥等信息。攻击者 A 自适应地向挑战者 C 发起询问，并交互进行以下 6 个步骤。

(1)RevealPartialKey：攻击者 A 要求得到车辆用户 U_i 的部分私钥。挑战者 C 搜索他维护的列表 L，返回 U_i 相应的部分私钥 p_i。如果列表中没有，则返回 $\perp$ (符号 $\perp$ 表示该值未知)。

(2)RevealSecretKey：攻击者 A 要求得到用户 U_i 的秘密值 x_i。挑战者 C 以列表 L 中的 x_i 作为响应，如果列表中没有，则返回 $\perp$。

(3)RevealPublicKey：攻击者 A 要求得到用户 U_i 的公钥 P_i。挑战者 C 以列表 L 中的 P_i 作为响应，如果列表中没有，则返回 $\perp$。

(4)RevealPseudonym：攻击者 A 要求得到用户 U_i 的假名。挑战者 C 以列表 L 中的 F_i 作为响应，如果列表中没有，则返回 $\perp$。

(5)ReplacePublicKey：输入车辆用户 U_i 的身份信息 ID_i，攻击者 A 以他自己选择的 $P_i^{'}$ 替换 U_i 的真实公钥 P_i。如果列表中没有包含用户 U_i 的身份信息，则攻击者放弃这一步。

(6)Sign：输入消息 $m_i \in \{0,1\}^*$，攻击者 A 能够生成用户 U_i 的签名 σ_i。如果列表中包含用户 U_i，则挑战者 C 返回有效的签名和新的公钥 $P_i^{'}$ 和秘密值 $x_i^{'}$。如果列表中没有包含用户 U_i 的身份信息 ID_i，则返回 $\perp$。

攻击者 A_1 或 A_2 自适应地向挑战者 C 分别进行随机预言机查询，包括 RevealPartialKey, RevealSecretKey, RevealPublicKey, RevealPseudonym, ReplacePublicKey, Sign，最终输出用户 ID_i^* 的消息签名对 $\left(m_i^*,\sigma_i^*\right)$。其中，第 1 类攻击者 A_1 没有查询 ID_i 的部分私钥 p_i，第 2 类攻击者 A_2 没有查询 ID_i 的秘密值 x_i。

无证书聚合签名的安全模型中包含两类攻击者，分别是 A_1 和 A_2。在循环群 G_1 中给定一个随机的 CDH 问题实例 (P,aP,bP)，挑战者 C 与 A_1 或 A_2 进行交互，最终 C 利用 A_1 或 A_2 解决 CDH 问题，即计算出 abP。

定理 1 在随机预言模型下，如果存在敌手 A_1 能够在时间 t 内分别执行 $q_i(i=1,2,\cdots,8)$ 次 H_1 查询、H_2 查询、H_3 查询、RevealSecretKey 查询、RevealPublicKey 查询、RevealPseudonym 查询、ReplacePublicKey 查询、Sign 查询，然后以不可忽略的概率 ε 伪造出签名，那么存在一个算法 C_1，能够在时间 $t+O\left(\sum_{i=1}^{8} q_i\right)t_m$ 内以概率 $\varepsilon' \geq \dfrac{\varepsilon}{e(q_4+1)}$ 解决 CDH 问题，其中 t_m 表示 G_1 中的一个模乘运算的时间。

证明 首先，挑战者 C_1 输入安全参数 l 运行系统建立算法(Setup)，发送参数

$$\mathrm{params}=\left(G_1,G_2,e,P,P_K,H_1,H_2,\overline{P}\right)$$

给敌手 A_1，并且 C_1 维护一个列表 $L=(\mathrm{ID}_i,p_i,x_i,P_i,F_i)$，$L_{H_1}$，$L_{H_2}$ 和 L_{H_3}，初始值为空。C_1 随机选择 $c\in Z_q^*$，设 $P_K=X,\overline{P}=c\cdot P$。$A_1$ 开始自适应地向 C_1 进行以下询问。

H_1 询问：敌手 A_1 输入身份 ID_i，C_1 首先调出列表 L，如果列表中已有记录，则返回给 A_1。否则 C_1 执行抛币协议 $c_i=\{0,1\}$，概率 $P[c_i=0]=\eta$，$P[c_i=1]=1-\eta$。如果 $c_i=0$，C_1 随机选择 $\alpha_i\in Z_q^*$，计算 $Q_i=\alpha_i\cdot X$；如果 $c_i=1$，$H_1(\mathrm{ID}_i)=\alpha_i\cdot P$。$C_1$ 将 $(\mathrm{ID}_i,\alpha_i,c_i,Q_i)$ 添加到列表 L_{H_1} 中。

H_2 询问：敌手 A_1 发起询问 $H_2(m_i,F1_i,P_i,U_i)$，如果列表中已经存在该值，则返回该值。否则，C_1 随机选择 $h_i\in Z_q^*$，并添加 $(m_i,F1_i,P_i,U_i,h_i)$ 到列表 L_{H_2} 中，返回 h_i 给 A_1。

H_3 询问：敌手 A_1 询问 $H_3(F1_i)$，如果列表中已存在，则返回该值。否则，C_1 随机选择 $t_i\in Z_q^*$，并添加 $(F1_i,t_i)$ 到列表 L_{H_3} 中，返回 t_i 给 A_1。

RevealSecretKey 查询：如果列表 L 中包含 $(\mathrm{ID}_i,p_i,x_i,P_i,F_i)$，$C_1$ 检查 x_i 的值，如果 $x_i\neq\perp$，C_1 返回 x_i 给 A_1。否则，如果 $x_i=\perp$，C_1 随机选择 $v_i\in Z_q^*$，令 $x_i=v_i$，$P_i=v_i\cdot P$，将 x_i 发给 A_1，保存 (x_i,P_i) 到列表 L 中。如果列表 L 中不包含 $(\mathrm{ID}_i,p_i,x_i,P_i,F_i)$，$C_1$ 将 x_i 的置空，再按上述方法计算 (x_i,P_i)。

RevealPublicKey 查询：如果列表 L 中包含 $(\mathrm{ID}_i,p_i,x_i,P_i,F_i)$，$C_1$ 检查 P_i 的值，如果 $P_i\neq\perp$，C_1 返回 P_i 给 A_1。否则，如果 $P_i=\perp$，C_1 随机选择 $v_i\in Z_q^*$，令 $P_i=v_i\cdot P$，$x_i=v_i$，将 P_i 发给 A_1，保存 (P_i,x_i) 到列表 L 中。如果列表 L 中不包含 $(\mathrm{ID}_i,p_i,x_i,P_i,F_i)$，$C_1$ 将 P_i 的置空，再按上述方法计算 (P_i,x_i)。

RevealPseudonym 查询：如果 $(\mathrm{ID}_i,p_i,x_i,P_i,F_i)$ 包含在列表 L 中，C_1 检查 F_i 的值，如果 $F_i\neq\perp$，C_1 返回 F_i 给 A_1。否则，C_1 随机选择 $k_i\in Z_q^*$，计算 $F1_i=k_i\cdot Q_i$，$F2_i=k_i\cdot t_i$，并将 $F_i=F1_i+F2_i$ 发给 A_1，更新列表 L。如果 $(\mathrm{ID}_i,p_i,x_i,P_i,F_i)$ 不在列表 L 中，C_1 令 $F_i=\perp$，然后根据列表 L_{H_1} 和 L_{H_3} 中的信息计算 $F1_i=k_i\cdot Q_i$，$F2_i=k_i\cdot t_i$，并将 $F_i=F1_i+F2_i$ 发给 A_1，更新列表 L。

ReplacePublicKey 查询：假定 A_1 选择了用户 ID_i 新的公钥 $P_i^{'}$，C_1 搜索列表 L，如果列表中包含 $(\mathrm{ID}_i,p_i,x_i,P_i,F_i)$，$C_1$ 以 $P_i^{'}$ 替换 P_i，并将 x_i 置空，即 $x_i=\perp$。如果列表中不包含 $(\mathrm{ID}_i,p_i,x_i,P_i,F_i)$，$C_1$ 令 $P_i=P_i^{'},x_i=\perp,p_i=\perp$，并将 $(\mathrm{ID}_i,p_i,x_i,P_i,F_i)$ 增加到列表 L 中。

Sign 查询：当收到敌手 A_1 的签名查询，挑战者 C_1 执行如下步骤生成用户 ID_i 关于消息 m_i 的签名。

如果 $c_i=1$，并且发现列表 L 中包含 $(\mathrm{ID}_i,p_i,x_i,P_i,F_i)$，$C_1$ 检查 x_i，如果 $x_i=\perp$，C_1 执行 RevealPublicKey 查询，生成 $x_i=v_i,P_i=v_i\cdot P$。如果列表 L 中不包含 $(\mathrm{ID}_i,p_i,x_i,P_i,F_i)$，$C_1$ 执行 RevealPublicKey 查询，将 x_i 和 P_i 增加到列表 L 中。

当 $c_i=0$ 时，C_1 随机选择 $r_i,r_i\in Z_q^*$，令 $U_i=r_i\cdot P-h_i^{-1}\cdot F1_i\cdot t_i$，并计算

$$\begin{aligned}V_i&=p_i\cdot F2_i+h_i\cdot r_i\cdot P_K+h_i\cdot x_i\cdot\overline{P}\\&=h_i\cdot r_i\cdot X+h_i\cdot x_i\cdot\overline{P}\end{aligned}$$

输出签名 $\sigma_i=(U_i,V_i)$。

当 $c_i=1$ 时，C_1 随机选择 $r_i\in Z_q^*$，令 $U_i=r_i\cdot P$，$p_i=\alpha_i\cdot X$，$F2_i=k_i\cdot t_i$，$\overline{P}=c\cdot P$，并计算

$$V_i=\alpha_i\cdot X\cdot k_i\cdot t_i+h_i\cdot r_i\cdot X+h_i\cdot x_i\cdot c\cdot\overline{P}$$

敌手 A_1 通过 2 次 Sign 预言机查询，就可以得到两个有效签名：

$$V_i = p_i \cdot F2_i + h_i \cdot r_i \cdot P_K + h_i \cdot x_i \cdot \overline{P}$$

$$V_i^{'} = p_i \cdot F2_i + h_i^{'} \cdot r_i \cdot P_K + h_i^{'} \cdot x_i \cdot \overline{P}$$

然后，挑战者 C_1 就可以通过上式解出：

$$abP = \left((h_i)^{-1}V_i - \left(h_i^{'}\right)^{-1}V_i^{'}\right)\left(\alpha_i k_i t_i \left((h_i)^{-1} - \left(h_i^{'}\right)^{-1}\right)\right)^{-1}$$

因此，C_1 解决了 CDH 问题。

进一步，C_1 成功解决 CDH 问题的概率可转化为以下 3 个事件：

Y_1：敌手 A_1 的随机预言 Reveal SecretKey 查询过程没有使 C_1 终止交互；

Y_2：A_1 通过与 C_1 的交互，伪造了一个有效的聚合签名；

Y_3：A_1 输出一个伪造的签名没有使 C_1 终止交互。

$$P(Y_1 \wedge Y_2 \wedge Y_3) = P(Y_1)\cdot P(Y_2 \mid Y_1)\cdot P(Y_3 \mid Y_1 \wedge Y_2)$$
$$= (1-\eta)^{q_4}\cdot\varepsilon\cdot\eta$$

而 η 的最优值为 $1/(q_4+1)$，因此，

$$\varepsilon' \geq \eta(1-\eta)^{q_4}\cdot\varepsilon = \frac{\varepsilon}{q_4+1}\left(1-\frac{1}{q_4+1}\right)^{q_4}$$

又因为，$\lim\limits_{q_4\to+\infty}\left(1-\frac{1}{q_4+1}\right)^{q_4} = \frac{1}{e}$，因此，

$$\varepsilon' \geq \frac{\varepsilon}{e(q_4+1)}$$　　证毕

定理 2　在随机预言模型下，如果存在敌手 A_2 能够在时间 t 内分别执行 $q_i(i=1,2,\cdots,8)$ 次 H_1 查询、H_2 查询、H_3 查询、RevealPublicKey 查询、Reveal SecretKey 查询、RevealPseudonym 查询、Sign 查询，然后以不可忽略的概率 ε 伪造出签名，那么存在一个算法 C_1，能够在时间 $t+O\left(\sum_{i=1}^{7}q_i\right)t_m$ 内以概率 $\varepsilon' \geq \frac{\varepsilon}{e(q_4+1)}$ 解决 CDH 问题，其中 t_m 表示 G_1 中的一个模乘运算的时间。

证明过程与定理 1 相同，不再赘述。

4　安全性和效率对比

将本文提出的无证书聚合签名方案与目前几种效率较高的方案[7,9−11,18]相对比。相比之下，文献[7]的验证算法需要的计算成本较大，并且不能抵抗签名的伪造攻击。文献[9]和文献[18]的计算效率较高，但不满足签名的可追踪性，而且，文献[18]也不能抵抗签名的伪造攻击。文献[10]聚合验证算法中的双线性对运算次数随着签名人数的增长成正向的线性增长趋势，消耗的计算代价太大。文献[11]不满足签名的可追踪性，并且其通信传输模式也不适合于车载自组网。下面具体说明本文提出方案的安全性。

4.1 认证性和不可伪造性

本文提出的无证书聚合签名算法，已经严格证明了它满足自适应选择消息攻击下的存在性不可伪造，因此它满足消息的认证性和签名的不可伪造性。

4.2 匿名性

每一个车辆用户 U_i 都需要在道路交通管理局 RTA 处登记注册，RTA 利用 hash 函数 H_3 关联了用户的真实身份 ID_i 和假身份 $\mathrm{ID}_i^{'}$，而路侧单元 RSU 通过选择随机数 $a_i \in Z_q^*$ 为假身份 $\mathrm{ID}_i^{'}$ 生成了假名 F_i。所以，除了 RSU 任何人都不能关联用户的假身份 $\mathrm{ID}_i^{'}$ 和假名 F_i，除了 RTA 任何人都不能关联用户的真实身份 ID_i 和假身份 $\mathrm{ID}_i^{'}$，因此，本方案满足了车辆用户的匿名性。

4.3 可追踪性

在本文设计的签名方案中，一旦验证算法失败或者车辆用户犯罪时，RSU 就可以把车辆用户 U_i 的假身份 $\mathrm{ID}_i^{'}$ 递交给 RTA, RTA 查询车辆用户的注册信息，从而追踪到对应的真实身份 ID_i。在出现纠纷或疑义时，RTA 利用哈希函数的单向性质，通过计算 $\mathrm{ID}_i^{'} = H_3(\mathrm{ID}_i)$ 来证实恶意的车辆用户的真实身份，实现了非法车辆用户的可追踪性。表 1 给出了几种方案的安全性的比较，可以看出本文的方案具有上述优良性质。

表 2 给出了几种聚合签名方案的计算量比较，我们只选取了其中的双线性对的运算(简记为 P)和群 G_1 中的模乘运算(简记为 S)，这两种运算在 Intel i7 3.07 GHz 机器上运行时间大约分别是 3.21 ms 和 0.40 ms。可以看出，双线性对运算耗时属主要部分。其他运算如哈希函数运算时间非常微小，忽略不计。表中 Sync 表示正常的传输模式，Ad hoc 表示自组网传输模式，n 表示车辆用户的个数。

通过在 windows+OPNET IT Guru release 9.1.a 中模拟实现，图 2 比较了几种基于 VANET 的无证书聚合签名方案中驶入同一个路侧单元 RSU 的车流量与验证延迟时间的比较。可以看到，当交

表 1 安全性比较

	文献[7]	文献[9]	文献[10]	文献[11]	文献[18]	本文方案
通信方式	V2V	V2I	V2V	V2I	V2I	V2I
认证性	是	是	是	是	是	是
匿名性	是	是	是	是	是	是
可追踪性	是	否	是	否	否	是
抵抗伪造攻击	否	是	否	是	是	是

表 2 计算量比较

	类型	签名	验证	聚合签证
文献[7]	Sync	$5S$	$5P+2S$	$5P+2nS$
文献[9]	Ad hoc	$4S$	$4P+2S$	$4P+2nS$
文献[10]	Ad hoc	$3S$	$4P$	$(n+3)P$
文献[11]	Sync	$3S$	$4P+3S$	$4P+3nS$
文献[18]	Sync	$3S$	$4P+S$	$4P+nS$
本文方案	Ad hoc	$3S$	$3P+3S$	$3P+3nS$

通负荷增加时，我们的方案验证的签名数最多，也即信息的损失率最小。

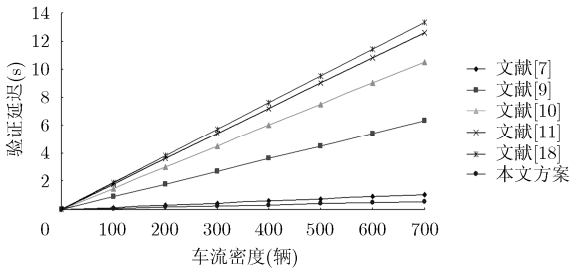

图 2 VANET 中车辆验证延迟

5 结论

聚合签名技术将许多不同用户的签名聚合成一个签名，只需对聚合后的签名进行验证即可判断收到的签名是否合法，大大提高了消息验证的效率，这一优点使其在车载自组织网络中有很好的应用价值。本文提出的安全有效的适合于车载网的无证书聚合签名方案具有无证书密码体制和聚合签名的双重优点，并在随机预言模型下是可证明安全的。本文的方案有效结合了车辆用户的隐私保护和非法用户的可追踪性质，即所谓的条件隐私保护。通过模拟实现的结果知道，相对于其他已存在的方案，本文的方案具有通信代价小、计算成本低和验证时延短等优点，因此更适合于类似车载自组织网络等资源受限的网络环境。

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 H. Insecurity of a certificateless aggregate signature scheme[J]. *Security & Communication Networks*, 2016, 9(11): 1547–1552. doi: 10.1002/sec.1447.

[3] 杜红珍. 一个适用于车载自组织网络的安全高效的聚合签名方案[J]. 河南科学, 2016, 34(4): 481–485.
DU Hongzhen. An efficient and secure aggregate signature scheme for vehicular Ad hoc network[J]. *Henan Science*, 2016, 34(4): 481–485.

[4] SHEN L, MA J, LIU X, *et al*. A provably secure aggregate signature scheme for healthcare wireless sensor networks[J]. *Journal of Medical Systems*, 2016, 40(11): 244–247. doi: 10.1007/s109 16-016-0613-3.

[5] SHEN L, MA J, LIU X, *et al*. A secure and efficient ID-based aggregate signature scheme for wireless sensor networks[J]. *IEEE Internet of Things Journal*, 2017, 4(2): 546–554. doi: 10.1109/JIOT.2016.2557487.

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

[7] ZHANG L, QIN B, WU Q, *et al*. Efficient many-to-one authentication with certificateless aggregate signatures[J]. *Computer Networks*, 2010, 54(14): 2482–2491. doi: 10.1016/ j.comnet.2010.04.008.

[8] 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 An International Journal*, 2015, 317(C): 48–66. doi: 10.1016/j.ins.2015.04.033.

[9] WANG H, QIN B, and DOMINGO-FERRER J. An improved binary authentication tree algorithm for vehicular networks[C]. IEEE International Conference on Intelligent Networking and Collaborative Systems, Princeton, 2012: 206–213. doi: 10.1109/iNCoS.2012.27.

[10] HORNG S J, TZENG S F, PAN, Y, *et al*. b-SPECS+: Batch verification for secure pseudonymous authentication in VANET[J]. *IEEE Transactions on Informaton Forensics and Security*, 2013, 8(11): 1860–1875. doi: 10.1109/TIFS.2013. 2277471.

[11] TU H, HE D, and HUANG B. Reattack of a certificateless aggregate signature scheme with constant pairing computations[J]. *The Scientific World Journal*, 2014(9): 1–10. doi: 10.1155/2014/343715.

[12] SHIM K A. On the security of a certificateless aggregate signature scheme[J]. *IEEE Communications Letters*, 2011, 15(10): 1136–1138. doi: 10.1109/LCOMM.2011.081011. 111214.

[13] HE D, TIAN M, and CHEN J. Insecurity of an efficient

certificateless aggregate signature with constant pairing computations[J]. *Information Sciences*, 2014, 268: 458–462. doi: 10.1016/j.ins.2013.09.032.

[14] 张玉磊, 李臣意, 王彩芬, 等. 无证书聚合签名方案的安全性分析和改进[J]. 电子与信息学报, 2015, 37(8): 1994–1999. doi: 10.11999/JEIT141635.
ZHANG Yulei, LI Chenyi, WANG Caifen, *et al*. Security analysis and improvements of certificate-less aggregate signature schemes[J]. *Journal of Electronics & Information Technology*, 2015, 37(8): 1994–1999. doi: 10.11999/JEIT 141635.

[15] 杜红珍, 黄梅娟, 温巧燕. 高效的可证明安全的无证书聚合签名方案[J]. 电子学报, 2013, 41(1): 72–76. doi: 10.3969/j.issn. 0372-2112.2013.01.014.
DU Hongzhen, HUANG Meijuan, and WEN Qiaoyan. Efficient and Provably-Secure certificateless aggregate signature scheme[J]. *Acta Electronica Sinica*, 2013, 41(1): 72–76. doi: 10.3969/j.issn.0372-2112.2013.01.014.

[16] SHEN H, CHEN J, SHEN J, *et al*. Cryptanalysis of a certificateless aggregate signature scheme with efficient verification[J]. *Security & Communication Networks*, 2016, 9(13): 2217–2221. doi: 10.1002/sec.1480.

[17] WANG L, CHEN K, LONG Y, *et al*. Cryptanalysis of a certificateless aggregate signature scheme[J]. *Security & Communication Networks*, 2016, 9(11): 1353–1358. doi: 10.1002/sec.1421.

[18] NIE H, LI Y, CHEN W, *et al*. NCLAS: A novel and efficient certificateless aggregate signature scheme[J]. *Security & Communication Networks*, 2016, 9(16): 3141–3151. doi: 10.1002/sec.1519.

王大星：　男，1980 年生，副教授，研究方向为密码学与信息安全.

滕济凯：　男，1980 年生，博士，研究方向为密码学与信息安全.