计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.190400119

VANET 中基于 RSU 辅助签名环形成的方案

张 浩 蔡 英 夏红科
北京信息科技大学计算机学院 北京 100101
(1639490356@qq.com)

摘 要 车辆自组织网络(Vehicular Ad-hoc Network,VANET)使交通系统更加智能和高效。信道的开放性以及车辆移动的高速性等特点,导致 VANET 存在诸如身份、传输数据以及位置等隐私信息泄露问题。目前,针对 VANET 的身份隐私泄露问题,越来越多的学者采用基于环签名的方案,但是车辆如何在行驶过程中与周围车辆组成签名环一直是一个难解决的问题。针对基础设施部署较完善地区,文中提出一种基于 RSU(Road-Side Unit)辅助签名环形成的方案。该方案通过 RSU 收集覆盖区域内车辆的公钥并广播公钥集,从而确定区域内车辆的签名环,并利用双线性对映射实现 RSU 与车辆间消息传输的基于身份加密的过程。安全分析和实验证明,所提方案在基础设施较完善地区能够拥有较好的效率和安全性。

关键词:车辆自组织网络;RSU;签名环形成;双线性对映射;基于身份加密
中图法分类号 TP309

RSU-based Assisting Ring Formation Scheme in VANET

ZHANG Hao,CAI Ying and XIA Hong-ke
School of Computer,Beijing Information Science & Technology University,Beijing 100101,China

Abstract A vehicular ad-hoc network (VANET) makes the transportation system more intelligent and efficient. But due to the open wireless channel and the high-speed movement of vehicles,VANET has privacy leakage issues such as identity,transmission data and location. For the issue of identity privacy leakage of VANET,the existing researches use ring signature increasingly. However,how the vehicle forms a ring with the surrounding vehicles has always been a difficult issue to solve during the moving of vehicles. Therefore as for the area where the infrastructure is deployed well,a RSU-based assisting ring formation scheme is proposed. The public keys of the vehicles in the coverage area are collected by the RSU,thus determining the public key set and broadcasteds it to the vehicles in the area. And the use of bilinear pair mapping achieves the identity-based encryption process of the message transmission between RSU and vehicles. According to security analysis and experiments,the scheme can have better efficiency and security in areas with better infrastructure.

Keywords Vehicular ad-hoc network,RSU,Ring formation,Bilinear pair mapping,Identity-based encryption

1 引言

车辆自组织网络是移动自组织网络在道路交通方面的应用,是一种特殊的移动自组织网络[1-2]。在 VANET 中,载有车载单元(On-Board Unit,OBU)的车辆作为移动节点,可以与其他车辆以及路边单元(RSU)进行通信,实时感知道路交通状况,既能帮助驾驶员有效避免车辆碰撞和追尾等交通事故,又有助于避免交通拥堵等情况[3-5]。VANET 的应用可分为两类:1)安全类应用,包括碰撞避免、追尾警告、危险区域警告等;2)非安全类应用,包括基于位置的服务、互联网访问以及听歌和看电影等娱乐性服务。

VANET 在提供上述服务的同时,由于无线信道的开放性以及车辆高速移动等特点,其隐私极易遭受攻击[6]。攻击者可在无线信道中截获车辆发送的数据包,从而非法获取车辆的身份隐私信息、驾驶路线、位置隐私信息等。车辆相互通信时,需要确认发送方的真实身份并实现消息认证,在认证过程中,发送方的身份、位置等隐私信息同样面临威胁。车辆的身份隐私信息一旦被泄露,将会对车辆用户的财产安全以及人身安全等造成威胁,所以 VANET 的身份隐私保护是至关重要的[7-8]。

已有的解决 VANET 身份隐私问题的方案大致可分为 4 类:匿名证书、假名、群签名以及环签名。其中,基于环签名的身份隐私保护方案是目前解决车联网身份隐私保护问题的研究热点。相对于匿名证书,环签名不需要时刻保持与分发中

到稿日期:2019-04-19 返修日期:2019-07-12 本文已加入开放科学计划(OSID),请扫描上方二维码获取补充信息。
基金项目:国家自然科学基金(61672106);中央引导地方科技发展专项(Z171100004717002)
This work was supported by the National Natural Science Foundation of China (61672106) and Special Program for Guiding Local Science and Technology Development by the Central Government (Z171100004717002).
通信作者:蔡英(ycai@bistu.edu.cn)

心的联系，更加灵活；相对于群签名，环签名的环中成员地位平等，不需要群管理者的角色，更加安全；环签名虽然没有假名方案的简便性，但是具有更高的安全性。2001 年，Rivest 等第一次提出环签名的概念[9]，并介绍了环签名的匿名性与自发性的特性。Petzoldt 等[10]提出了一种基于多元多项式的新阈值环签名方案。Rajabzadeh 等[11]提出了基于 RSA 假设的第一个可证明安全的基于身份的短代理环签名方案。Han 等[12]提出了一种双重保护的环签名算法，通过安全传输保护消息的发送和接收过程。Liu 等[13]提出了第一个基于格的双重认证环签名的 VANET 隐私保护方案，为量子计算机提供了安全保障。

已有的环签名方案虽然在一定程度上实现了 VANET 的身份隐私保护，但是车辆在行驶过程中如何与周围车辆组成签名环一直是一个难解决的问题。本文针对 VANET 中基础设施建设完备的地区，提出了一种基于 RSU 辅助签名环形成的方案。该方案通过 RSU 收集覆盖区域内车辆的公钥并广播公钥集，从而确定区域内车辆的签名环。其中，车辆与 RSU 之间采用基于身份的加密和签名方案进行消息传输，既保障了车辆与 RSU 之间消息传输的安全性，又提高了 VANET 中车辆组环的效率。

2 预备知识

2.1 VANET 模型

VANET 由信任机构(Trust Authority，TA)、RSU 以及 OBU 车辆组成，其中车辆与车辆、车辆与 RSU 之间都是通过专用短程通信技术(Dedicated Short Range Communications，DSRC)进行通信，如图 1 所示。

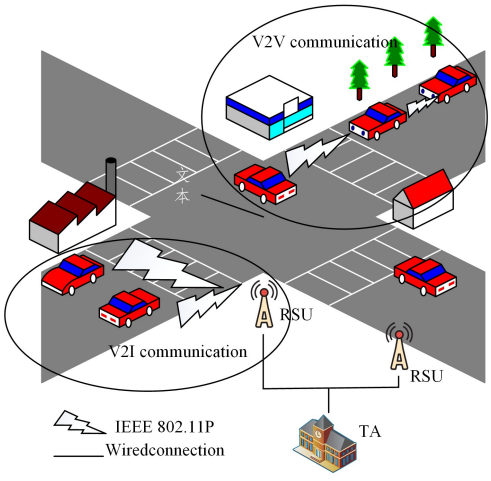

图 1 VANET 模型

Fig. 1 VANET model

TA：负责 RSU 和 OBU 车辆的登记注册，为 RSU 和 OBU 车辆生成公私钥对，并将生成的系统参数以及公私钥对写入车辆和 RSU 的防篡改设备中。

RSU：部署在路边的基础设施。担任 TA 与车辆之间的沟通桥梁，同时作为网关接入点，车辆可通过 RSU 连入 Internet 网络。在本文中，RSU 还辅助 VANET 中的车辆组成签名环。

OBU 车辆：作为 VANET 中的移动节点，具有与其他 OBU 车辆、RSU 通信的能力，能够以一定的频率向 RSU 广播道路交通状况以及车辆行驶信息(位置、行驶速度、方向、驾驶状态等)[14-15]。

DSRC：基于 IEEE 802.11p 无线电技术的 DSRC 距离在 300 m 左右。车辆通过 DSRC 可与其他车辆以及 RSU 进行通信。

2.2 双线性对映射

双线性映射[16]及双线性对映射的困难问题[17]已在 OSID 附件详细描述。

2.3 基于身份的加密体制

基于身份的加密体制[18]可以简化用户身份信息与其公钥的关联关系。不同于传统的密码体制，基于身份的加密体制可直接通过用户身份信息计算出用户的公钥，克服了传统密码体制存在的存储空间和计算资源开销大的问题，简化了密钥管理，缓解了系统压力。

基于身份的加密体制的主要算法见 OSID 附件。

3 基于 RSU 辅助签名环形成的方案

本文方案适用于 VANET 中基础设施建设完备的地区，通过基于身份加密和签名的技术，RSU 收集覆盖区域内车辆的公钥，确定并广播签名环公钥集。方案包括 7 个部分，具体流程如图 2 所示，方案中的符号说明如表 1 所列。

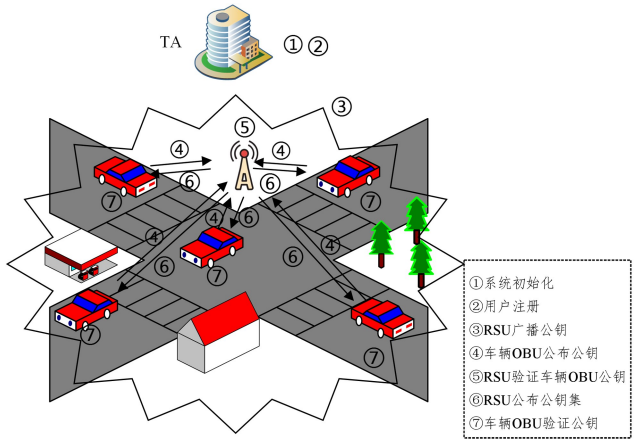

图 2 基于 RSU 辅助环形成方案过程图

Fig. 2 Process diagram of RSU-based assisting ring scheme

表 1 参数描述

Table 1 Parameters description

参数	描述
G_1，G_2	加法群、乘法群
q	G_1 和 G_2 阶大素数
P	G_1 的生成元
e：$G_1\times G_1\rightarrow G_2$	双线性映射
H_1，H_2	哈希函数
s	TA 主密钥
P_{pub}	TA 公钥
VID_i	车辆的真实身份
$QVID_i$	车辆的公钥
$DVID_i$	车辆的私钥
R_{ID_i}	RSU 的真实身份
$QRID_i$	RSU 的公钥
$DRID_i$	RSU 的私钥
V_i	第 i 辆车辆
σ，σ_1	签名

(1)系统初始化

TA 随机选取安全参数 q(q 为大质数)，q 为加法群 G_1 和乘法群 G_2 的阶数，P 是 G_1 的生成元，双线性映射 $e:G_1\times G_1\rightarrow G_2$。TA 随机选取 $s\in Z_q$ 作为主密钥，系统公钥 $P_{pub}=sP$，主密钥 s 秘密保存在 TA 中，RSU 与 OBU 车辆都不可得知。本文方案需要用到的安全 hash 函数有：$H_1:\{0,1\}^*\rightarrow G_1$，$H_2:\{0,1\}^*\times G_1\rightarrow Z_q^*$，$H_3:G_2\rightarrow\{0,1\}^*$，$H_4:\{0,1\}^*\rightarrow\{0,1\}^*$。

(2)用户注册

所有的 OBU 车辆和 RSU 加入 VANET 之前，都需要到 TA 进行登记注册。TA 负责检查 OBU 车辆和 RSU 身份信息的真实性，通过审核之后为其注册。OBU 车辆身份信息为 VID_i，TA 计算 OBU 车辆的公钥 $QVID_i=H_1(VID_i)$ 和私钥 $DVID_i=sQVID_i$，并将公私钥对写入 OBU 车辆的防篡改设备中。RSU 身份信息为 R_{ID_i}，TA 计算 RSU 的公钥 $QRID_i=H_1(RID_i)$ 和私钥 $DRID_i=sQRID_i$，并同样将公私钥对存储到 RSU 的防篡改设备中。

(3)RSU 广播公钥

RSU 向其覆盖区域内的 OBU 车辆广播其公钥 $QRID_i$，即 $RSU\xrightarrow[QRID_i]{}V_i$，$i\in\{0,1,\cdots,n\}$。

(4)OBU 车辆公布公钥

OBU 车辆用自己的私钥对公钥签名，签名的具体过程如下所示：

1)随机选取 $l\in Z_q^*$，并计算签名 σ 中的第一个元素 $X=lQVID_i$；

2)计算 $g=H_2(QVID_i,X)$；

3)计算签名 σ 中的第二个元素 $Y=(l+g)DVID_i$；

4)输出签名 $\sigma=(X,Y)$。

输出签名 σ 后，用 RSU 的公钥将签名和公钥信息加密并发送给 RSU，即 $OBU\xrightarrow[c]{}RSU$。加密的具体过程如下所示：

1)令 $m=QVID_i\parallel\sigma$；

2) 随机选取 $r\in Z_q^*$，计算 $h=H_2(r,m)$；

3)计算 $o=e(P_{pub},QRID_i)$；

4)令 $F=hP$，$J=r\oplus H_3(o^r)$，$W=m\oplus H_4(r)$，则输出密文 $c=\langle F,J,W\rangle$。

(5)RSU 验证 OBU 车辆的公钥

RSU 接收到 OBU 车辆发送的消息后，首先用私钥 $DRID_i$ 进行解密，即 $De(DRID_i,c)$。RSU 解密消息的具体过程如下所示：

1)计算 $o'=e(F,DRID_i)$；

2)计算 $r=J\oplus H_3(o')$；

3)计算 $m=W\oplus H_4(r)$；

4)计算 $h=H_2(r,m)$，如果 $F\neq hP$，则放弃密文，否则返回明文 m。

接着，验证 OBU 车辆发送的公钥信息的真实性，即 $Verify(QVID_i,\sigma)$。验证的具体过程如下所示：

1)计算 $g=H_2(QVID_i,X)$；

2)双线性对计算 $e(P_{pub},X+gQVID_i)$。

验证 $e(P,Y)$ 和 $e(P_{pub},X+gQVID_i)$，若 $e(P,Y)=e(P_{pub},X+gQVID_i)$，则将 OBU 车辆的公钥提取出来加入到公钥集 θ，否则丢弃该信息。

(6)RSU 公布公钥集

RSU 在覆盖区域内收集 OBU 车辆公布的公钥之后，确定收集的公钥集 θ 内公钥的数量 $num(\theta)$，若 $num(\theta)>N$(N 为阈值)，则 RSU 向覆盖区域内的 OBU 车辆公布公钥集 θ。

若经过时间 t，$num(\theta)<N$，则 RSU 用先前公布的公钥集来填充公钥集 θ，然后公布给覆盖区内的 OBU 车辆。RSU 公布公钥集的具体过程如下所示：

1)RSU 随机选择 $c\in Z_q^*$，并计算签名 σ_1 的第一个元素 $M=c\theta$，其中 $\theta=\{QVID_1,QVID_2,\cdots,QVID_n\}$；

2)计算 $d=H_2(\theta,M)$，其中 $\theta=\{QVID_1,QVID_2,\cdots,QVID_n\}$；

3)计算 $U=(c+d)DRID_i$；

4)输出签名 $\sigma_1=(M,U)$。

输出签名 σ_1 后，RSU 在其覆盖区域内向 OBU 车辆广播签名 σ_1 和公钥信息，即 $RSU\xrightarrow[\{\theta,\sigma_1\}]{}OBU$。

(7)OBU 车辆验证公钥

OBU 车辆接收到 RSU 公布的公钥集和签名之后，验证公钥集的真实性，即 $Verify(\theta,\sigma_1)$。OBU 车辆验证公钥的具体过程如下所示：

1) 利用公钥集 θ 和签名 σ_1 进行验证，其中 $\theta=\{QVID_1,QVID_2,\cdots,QVID_n\}$；

2)计算 $d=H_2(\theta,M)$；

3)双线性对计算 $e(P_{pub},M+d\theta)$。

若 $e(P,M)=e(P_{pub},M+d\theta)$，则 OBU 车辆用此环签发消息，否则丢弃该信息。

4　安全性分析

本节将从正确性、匿名性、不可伪造性、可认证性、机密性这 5 个方面对本文提出的方案进行安全性分析。

(1)正确性：OBU 车辆或 RSU 对公钥信息生成的签名，其他车辆或 RSU 可以通过验证算法进行验证。

证明：

$$\begin{aligned}e(P_{pub},X+gQVID_i)&=e(s\cdot P,X+gQVID_i)\\&=e(s\cdot P,l\cdot QVID_i+gQVID_i)\\&=e(s\cdot P,(l+g)QVID_i)\\&=e(P,(l+g)\cdot s\cdot QVID_i)\\&=e(P,(l+g)DVID_i)\\&=e(P,Y)\end{aligned}$$

经计算可得 $e(P,Y)=e(P_{pub},X+gQVID_i)$，所以验证算法具有正确性。

(2)匿名性：本文方案中 OBU 车辆向所在区域内的 RSU 发送自己的公钥具有匿名性。

证明：在 OBU 车辆向所在区域的 RSU 发送公钥信息时，由于区域内聚集了众多车辆，RSU 以及攻击者成功将加密处理后的公钥信息与 OBU 车辆的真实身份关联起来的概率可忽略。

(3)不可伪造性：签名车辆的自身私钥未泄露前，该方案满足不可伪造性。

证明：1)本方案是基于身份的签名方案，攻击者想通过

OBU 车辆的公钥以及系统参数计算出 OBU 车辆的私钥，无异于解决椭圆曲线离散对数问题，成功概率可忽略。

2)签名过程中，OBU 车辆随机选取 $l \in Z_q^*$，其他车辆以及 RSU 不可得知，所以攻击者想通过 OBU 车辆的签名以及公钥计算其私钥的概率可忽略。

3)由于攻击者无法得到 OBU 车辆的私钥，因此攻击者伪造 OBU 车辆签名的概率可忽略。

(4)可认证性：本文方案在签名的过程中具有可认证性。

证明：由于攻击者伪造 OBU 车辆签名的概率是可忽略的，因此验证者可通过 OBU 车辆的公钥验证等式 $e(P,Y)=e(P_{pub},X+gQVID_i)$ 是否成立，若成立，则签名合法，否则将该签名丢弃。

(5)机密性：本文方案中 OBU 车辆向 RSU 发送公钥信息具有机密性。

证明：OBU 车辆向 RSU 发送的公钥信息是通过 RSU 的公钥 $QRID_i$ 进行加密的，攻击者无法得知存储在 TA 的主密钥 s，所以无法计算得出 RSU 的私钥 $DRID_i$，即攻击者无法得知 OBU 车辆发送的消息内容。

5 性能分析

本实验是在虚拟机 VMware Workstation Pro 上通过搭建 Veins 框架实现的。Veins 是基于 OMNeT++离散事件仿真环境，通过 TraCI 接口查询和调度 SUMO 中的车辆运动状态。本实验采用 SUMO 的 0.32.0 版本和 OMNET 的 5.3 版本，其中 SUMO 集成了车辆的行驶规律、驾驶员的驾驶习惯等重要内容，并通过 Traci 拓展包与 OMNET++进行通信，将 SUMO 中车辆的行驶轨迹输入到 OMNET++中，然后由 OMNET++进行网络仿真。其中，基于身份的加密和签名操作通过 Stanford 大学开发的开源库 Pairing Based Crypto(PBC) library 实现。主要的仿真参数如表 2 所列，部署有 RSU 的十字路口交通场景如图 3 所示。

表 2 仿真参数

Table 2 Simulation parameters

参数	值
仿真时间/s	200
仿真移动节点数	50
仿真移动节点速度/(km/h)	≤70
移动节点的通信距离/m	300
RSU 的通信距离/m	1000
RSU 数量	1
信道频段/MHz	10
标准消息大小/byte	200
经加密的消息大小/byte	364

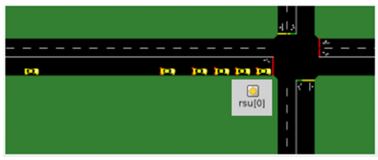

图 3 十字路口的交通模拟图

Fig. 3 Traffic simulation of crossroad

本实验评估了 RSU 在辅助车辆组成签名环的过程中 RSU 收集车辆公钥集引起的计算开销，同时评估了车辆在生成公钥信息签名以及验证公钥信息期间产生的计算开销。在 RSU 辅助车辆组成签名环的过程中，RSU 和车辆所需的双线对计算次数，以及测试 100 次所花费的平均时间开销如表 3 所列。实验完成的主要任务包括：

(1)分析基于 RSU 辅助车辆组成签名环的组环时延与路口车辆密度的关系；

(2)当车辆密度一定时，分析基于 RSU 辅助车辆组成签名环的组环概率与公钥集阈值大小的关系；

(3)分析车辆密度极大时，对于基于 RSU 辅助车辆组成签名环的方案的组环概率影响。

表 3 方案的计算开销

Table 3 Computational cost of proposed protocol

	加密、签名开销	时间/s
RSU	N 次双线性对签名验证过程	$N*0.005$
	1 次双线性对签名过程	0.0006
	N 次双线性对解密过程	$N*0.007$
车辆	1 次双线性对签名过程	0.0006
	1 次双线性对验证过程	0.005
	1 次双线性对加密过程	0.004

图 4 反映了基于 RSU 辅助签名环形成的方案所耗费的时间随着路口车辆密度的变大而缩短；但当车辆密度增长到某个程度后，本文方案的组环时延趋于平稳。实际生活中，城市路口的红灯时间约为 30～90 s。仿真实验中，当路口聚集的车辆数量达到 20 后，本文方案的组环时延将低于 10 s；当路口的车辆数量达到 40 辆以上时，本文方案的组环延迟仅为 2～3 s，远低于红灯持续时间。因此，在路口处，基于 RSU 辅助环形成的方案可有效为车辆组成签名环。

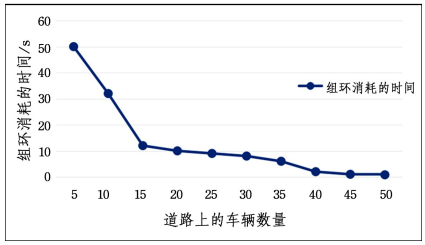

图 4 道路车辆密度对组环时延的影响

Fig. 4 Vehicle density's impact on delay of ringing

组环概率指路口处组环成功的车辆数量占总车辆数量的比例。图 5 的仿真结果表明，当公钥集的阈值一定时，随着车辆密度的增加，基于 RSU 辅助环形成的方案的组环概率变大。因为本文方案中 RSU 在收集车辆公钥时，随着道路上车辆数量的增长，车辆数量远大于组环的阈值，所以方案的组环概率增大。

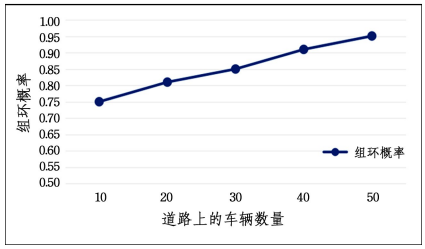

图 5 道路上车辆的数量对组环概率的影响

Fig. 5 Vehicle density's impact on probability of ringing

图 6 的仿真结果表明，当车辆密度一定时，随着公钥集阈值的增大，本文方案的组环概率变小。因为本文方案中 RSU 在收集公钥时，公钥集阈值的增大使得车辆数量与阈值间的差值变小，从而导致部分车辆无法组环；当阈值大于车辆数量时，环将无法形成，所以组环概率会变小。

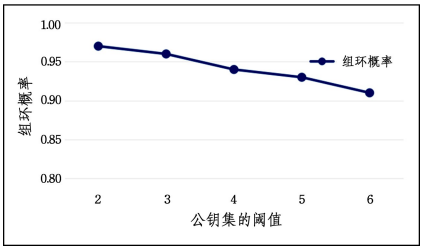

图 6　公钥集的阈值大小对组环概率的影响

Fig. 6　Threshold size's of the public key set impact on delay of ringing

结束语　本文针对基于环签名的 VANET 身份隐私保护方案签名环的形成，提了一种安全、高效的基于 RSU 辅助签名环形成的方案，该方案主要适用于路边基础设施比较完善的地区。方案中 OBU 车辆将自己的公钥信息安全地发送给 RSU，RSU 收集到公钥信息后将向覆盖范围内的车辆进行发送。针对方案的安全性分析和仿真实验结果表明，基于 RSU 辅助签名环形成的方案不仅具有可抵御攻击的安全性，还具有较高的效率。但是，该方案对基础设施的依赖性较强，这将迫使我们加大对基础设施不完善情况下的环形成方案的研究力度，从而为后续基于环签名的 VANET 身份隐私保护的研究做好基础工作。

参 考 文 献

[1] ZEADALLY S, HUNT R, CHEN Y S, et al. Vehicular ad hoc networks (VANETS): status, results, and challenges[J]. Telecommunication Systems, 2012, 50(4): 217-241.

[2] TOOR Y, MUHLETHALER P, LAOUITI A, et al. Vehicle Ad Hoc networks: applications and related technical issues[J]. IEEE Communications Surveys & Tutorials, 2008, 10(3): 74-88.

[3] HE D, ZEADALLY S, XU B, et al. An Efficient Identity-based Conditional Privacy-preserving Authentication Scheme For Vehicular Ad-hoc Networks[J]. IEEE Transactions on Information Forensics and Security, 2015, 10(12): 2681-2691.

[4] CHIM T, YIU S, HUI L, et al. VSPN: VANET-based Secure and Privacy-preserving Navigation[J]. IEEE Transactions on Computers, 2014, 63(2): 510-524.

[5] RAJPUT U, ABBAS F, OH H. A Hierarchical Privacy Preserving Pseudonymous Authentication Protocol for VANET[J]. IEEE Access, 2016, PP(99): 7770-7784.

[6] DHAMGAYE A, CHAVHAN N. Survey on security challenges in VANET 1[J]. International Journal of Computer Science & Network, 2013, 2(1): 88-96.

[7] WANG F, XU Y, ZHANG H, et al. 2FLIP: A two-factor lightweight privacy-preserving authentication scheme for VANET [J]. IEEE Transactions on Vehicular Technology, 2016, 65(2): 896-911.

[8] VIJAYAKUMAR P, AZEES M, DEBORAH L J. CPAV: Computationally Efficient Privacy Preserving Anonymous Authentication Scheme for Vehicular Ad Hoc Networks[C]// IEEE International Conference on Cyber Security & Cloud Computing. IEEE, 2016.

[9] RIVEST R L, SHAMIR A, TAUMAN Y. How to leak a secret [C]// Advances in Cryptology-ASIACRYPT. 2001: 552-565.

[10] PETZOLDT A, BULYGINS S, BUCHMANN J. A multivariate based threshold ring signature scheme[J]. Applicable Algebra in Engineering, Communication and Computing, 2013, 24: 255-275.

[11] RAJBZADEH A, MARYAM S, MAHMOUD S, et al. A short identity-based proxy ring signature scheme from RSA[J]. Computer Standards & Interfaces, 2015, 38: 144-151.

[12] HAN Y, XUE N N, WANG B Y, et al. Improved Dual-Protected Ring Signature for Security and Privacy of Vehicular Communications in Vehicular Ad-hoc Networks[J]. IEEE Access, 2018, 6: 9-20.

[13] LIU J, YU Y, JIA J, et al. Lattice-based double-authentication-preventing ring signature for security and privacy in vehicular Ad-Hoc networks[J]. Tsinghua Science and Technology, 2019, 24(5): 575-584.

[14] SYFULLAH M, LIM M Y. Data broadcasting on Cloud-VANET for IEEE 802.11p and LTE hybrid VANET architectures [C]// International Conference on Computational Intelligence & Communication Technology. IEEE, 2017: 1-6.

[15] GREESHMA T P, ROSHINI T V. A Review on Privacy Preserving Authentication in VANETs[C]// 2018 International Conference on Control, Power, Communication and Computing Technologies (ICCPCCT). Kannur, 2018: 235-238.

[16] CAI Y, FAN Y, WEN D. An Incentive-Compatible Routing Protocol for Two-Hop Delay-Tolerant Networks[J]. IEEE Transactions on Vehicular Technology, 2015, 65(1): 266-277.

[17] XIONG H, BEZNOSOV F, QIN Z. Efficient and Spontaneous Privacy-preserving Protocol for Secure Vehicular Communication[C]// Proceedings of ICC 2010. Cape Town, South Africa, 2010: 1-6.

[18] SHAMIR A. Identity-based cryptosystems and signature schemes[C]// Workshop on the Theory and Application of Cryptographic Techniques. Springer Berlin Heidelberg, 1984: 47-53.

ZHANG Hao, born in 1995, master. His research field includes identity privacy protection of VANETs and so on.

CAI Ying, Ph. D, professor, supervisor. Her main interests include cryptographic algorithms and computer security, social networking and privacy protection, connected cars and edge computing, etc.