适于车载网安全通信的高效签密方案

张 宇[1,2],陈 晶[1],杜瑞颖[1],周 庆[2],郑明辉[3]
(1.武汉大学计算机学院,湖北武汉 430072;2.信息保障技术重点实验室,北京 100072;3 湖北民族学院 445000,湖北恩施)

摘 要: 针对车载自组织网络的特点,该文利用双线性对提出了一个新的基于身份的签密方案,并在随机预言模型中给出了安全性证明.在假设 Bilinear Diffie-Hellman 问题是困难的条件下,该方案被证明是安全的.与已有的基于身份的签密方案相比,该方案计算量和传输代价小,适合用于车载网安全通信.

关键词: 车载自组织网络;基于身份的签密;双线性对;可证明安全
中图分类号: TP309 **文献标识码:** A **文章编号:** 0372-2112 (2015)03-0512-06
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2015.03.015

An Efficient Signcryption Scheme for Secure Communication of VANET

ZHANG Yu[1,2], CHEN Jing[1], DU Rui-ying[1], ZHOU Qing[2], ZHENG Ming-hui[3]
(1. *School of Computer, Wuhan University, Wuhan, Hubei* 430072, *China*; 2. *Science and Technology on Information Assurance Laboratory, Beijing* 100072, *China*; 3. *Hubei Institute for Nationalities, Enshi, Hubei* 445000, *China*)

Abstract: According to the characteristics of vehicular networks, this paper presents a identity-based signcryption scheme using the bilinear pairings and proves its security in the random oracle model. The proposed scheme is proved to be secure assuming that the Bilinear Diffie-Hellman problem is hard. Compared with the existing identity based signcryption schemes, the new scheme has lower computation cost and communication overhead. It is suitable for secure communication of vehicular networks.

Key words: vehicular ad hoc networks; identity-based signcryption; bilinear pairing; provable security

1 引言

车载自组织网络(Vehicular Ad hoc NETwork, VANET,简称车载网)是一种特殊的无线自组织网络,以短距离无线通信(DSRC)标准、车辆环境无线接入(WAVE)标准和802.11p为基础[1,2].典型的VANET结构通常包含服务中心、路边单元(RSU)以及车载通信单元(OBU)3个部分[3].OBU安装在每一辆车上,可以进行车间通信(V2V)和对RSU通信(V2R),RSU部署在道路两侧或十字路口.这种移动自组网络参与节点多、规模大、拓扑变化频繁、路径寿命短,有严格的低时延要求.

车载网作为未来智能交通系统的基础,为车间通信创建了一个重要的平台,可以实现事故告警、辅助驾驶、道路交通信息查询、乘客间通信和Internet信息服务等应用.这些信息会通过多跳方式在大范围车辆间传递[4].由于无线网络本身的脆弱性和开放性,车载网很容易受到攻击和破坏.因此,车载自组网的部署和实施必须充分考虑信息的保密性、认证性等安全需求.设计高效可靠的安全机制是当前车载自组织网络的研究重点之一[5,6].

密码学的传统方法是以"先签名后加密"的方式来同时实现保密性和认证性的.它所需的代价是签名和加密所需的代价之和,因而效率较低.为了提高效率,Zheng在文献[7]中提出了签密的概念.签密能够在一个合理的逻辑步骤内同时完成数字签名和公钥加密两项功能,而其计算量和通信成本都要低于传统的"先签名后加密",因而它是实现既保密又认证地传输消息的较为理想的方法.

基于身份密码体制是一种特殊的公钥密码体制,它的设计思想最早由Adi Shamir在1984年提出[8],其设计目标是在无需第三方提供认证服务的情况下,实现公钥与身份绑定,简化密钥管理.在基于身份的密码体制中,用户的公钥直接从其身份信息(如姓名、身份证号、E-mail地址、车牌号等)得到,而私钥则是由一个称为私钥生成中心(PKG)的可信方生成.

收稿日期:2013-09-16;修回日期:2014-06-16;责任编辑:梅志强
基金项目:信息保障技术重点实研室开放基金(No.KJ-13-104)

2002 年,文献[9]定义了基于身份的签密方案.基于身份的签密方案综合了基于身份密码体制与签密体制的优点,计算量和通信成本低,密钥管理简单.因此,基于身份的签密方案是车载网环境下保证信息的保密性与认证性的理想方案[10~12].近年来,基于身份的签密方案的研究取得了一系列成果[9,13~23].

文献[9]定义了基于身份的签密方案的安全模型,并利用双线性对构造了第一个基于身份的签密方案.该文献中定义的安全模型能处理消息的保密性和签名的不可伪造性,但构造的签密方案不是语义安全的[14].文献[15]提出的方案,验证过程需要用到接收方的私钥,因此不能满足公开验证性.文献[16]设计了一个能同时满足公开验证性和前向安全性的签密方案,然而他们的方案需要两个私钥,一个用于签密,一个用于解签密,密钥管理比较复杂.文献[17]给出了一个安全的签密方案,但计算效率较低.文献[18]提出了一个高效的签密方案,但该签密方案不是语义安全的[19,20],也不满足不可伪造性[20].文献[21]提出了目前为止计算效率最高的基于身份的签密方案,但该方案不满足前向安全性与公开验证性[24].

车载网具有拓扑结构变换快、信道不稳定、带宽不足等特点[25],已有的基于身份的签密方案不能很好地适应该环境的需求.本文利用双线性对提出了一个高效的基于身份的签密方案,并在随机预言模型[26]中给出了安全性证明.该方案中,签密与解签密操作总共仅需 2 次双线性对运算,计算效率只略低于文献[21]的方案,相对于已有的其他基于身份的签密方案均有大幅提高,能够较好的适应车载网环境.

2　预备知识

2.1　基于身份签密方案的组成

文献[9]中给出了基于身份的签密方案的形式化定义,包含系统建立(setup),密钥提取(extract),签密(signcrypt)和解签密(unsigncrypt)四种操作.

2.2　基于身份签密方案的安全性定义

一个基于身份的签密方案需要满足保密性,不可伪造性,公开验证性,不可否认性,前向安全性[18].

文献[14]通过敌手和挑战者之间的游戏给出了基于身份签密方案的保密性和不可伪造性的形式化定义,具体请参阅文献[14].

2.3　双线性对及相关困难问题

本文提出的签密方案是基于双线性映射的[27].双线性映射 e 可以通过有限域上超椭圆曲线上的 Tate 对或 Weil 对来构造.

本文提出的签密方案安全性依赖于 Bilinear Diffie-Hellman (BDH)问题[27]和椭圆曲线上的离散对数(ECDL)[28]问题.具体请参阅文献[27,28].

3　本文方案

3.1　网络结构

本文采用典型的 VANET 结构,如图 1 所示.服务中心在系统中充当完全可信的角色,拥有最高管理权限,负责系统的初始化与维护,对 RSU 和 OBU 进行登记管理,以及私钥的生成、分发等.服务中心通过有线信道与 RSU 通信.RSU 是 VANET 的重要基础设施.RSU 与 OBU 之间,OBU 与 OBU 之间通过无线信道相互通信.

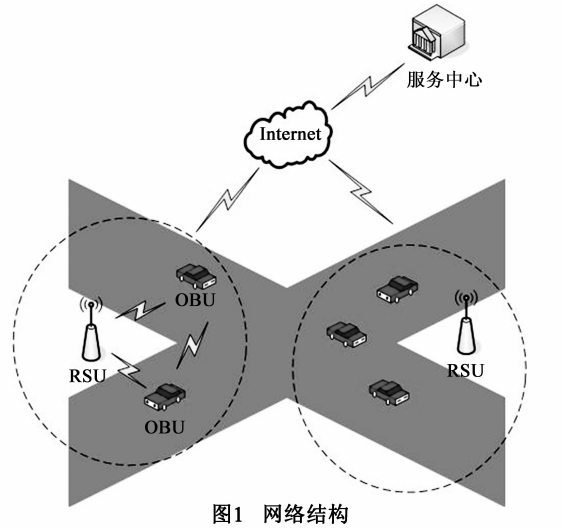

图1　网络结构

3.2　签密方案

本节提出一个适用于车载网安全通信的签密方案,具体如下:

初始化系统:输入安全参数 z,服务中心选择两个素数 q 阶($q>2^z$)群 G_1 和 G_2.其中,G_1 为循环加法群,生成元为 P.G_2 为循环乘法群.定义双线性对映射 e:$G_1\times G_1\rightarrow G_2$.选取安全的对称密码算法$(E,D)$.定义安全的 Hash 函数 $H_1:\{0,1\}^*\rightarrow G_1$,$H_2:\{0,1\}^*\rightarrow Z_q$,$H_3:Z_q\times G_1\rightarrow Z_q$,$H_4:G_2\rightarrow\{0,1\}^l$.其中,$l$ 为对称密码算法(E,D)的密钥长度.服务中心随机选择主密钥 $s\in Z_q^*$,计算 $P_{pub}=sP$.服务中心公开系统参数$\{z,G_1,G_2,e,q,P,P_{pub},E,D,H_1,H_2,H_3,H_4\}$,保密 s.公开参数嵌入到所有的 OBU 及 RSU 中.

密钥提取:OBU 或 RSU(在此,统称为通信单元)在接入网络前,都需要进行登记.登记时,输入身份 ID$\in\{0,1\}^*$,服务中心计算 $Q_{ID}=H_1(ID)$,$S_{ID}=sQ_{ID}$.其中 Q_{ID}为该通信单元的公钥,S_{ID}为该通信单元的私钥.服务中心通过安全方式将私钥发送给通信单元.流程如图 2 所示.在此,设通信单元 A 的身份为 ID_A,公钥为 Q_A,私钥为 S_A;通信单元 B 的身份为 ID_B,公钥为 Q_B,私钥为 S_B.

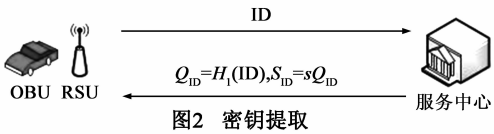

图2 密钥提取

签密:为了发送消息 m 给通信单元 B,通信单元 A 需执行以下步骤:

(1)随机选择 $r\in Z_q^*$.

(2)计算 $R=rP$, $h_1=H_2(m)$, $h_2=H_3(h_1,R)$, $S=\frac{r}{h_2+S_A}$.

(3)计算 $\omega=e(P_{pub},Q_B)^r$, $k=H_4(\omega)$,计算 $c=E_k(S\parallel m)$.

(4)发送密文 $\sigma=\{c,R\}$给通信单元 B.

解签密:收到密文 σ,通信单元 B 执行以下步骤:

(1)计算 $\omega=e(R,S_B)$, $k=H_4(\omega)$,恢复消息 $S\parallel m=D_k(c)$.

(2)计算 $h_1=H_2(m)$,计算 $h_2=H_3(h_1,R)$.

(3)验证 $R=S(h_2P+Q_AP_{pub})$.如果成立,通信单元 B 接受这个消息,否则认为 σ 不合法.

容易得知,根据双线性对的性质等,方案的正确性可以得到保证:

$$\omega=e(P_{pub},Q_B)^r=e(sP,Q_B)^r=e(R,S_B)$$

$$R=rP=S(h_2+S_A)P=S(h_2P+Q_AP_{pub})$$

特别说明:在计算 $S=\frac{r}{h_2+S_A}$ 和 $R=S(h_2P+Q_AP_{pub})$时,需要将 G_1 上的点 S_A 和 Q_A 转换为 Z_q^* 中的数[29].

4 安全性分析

由下列定理 1~定理 3 可知,本文提出的签密方案满足基于身份的签密方案的安全要求.

定理 1 在随机预言模型中,针对本文提出的签密方案,若存在一个敌手 A 能够在 t 时间内,以 ξ 的优势赢得文献[14]中定义 1 的游戏(最多能进行 q_i 次 H_i 询问($i=1,2,3,4$), q_e 次 extract 询问, q_s 次 signcrypt 询问, q_u 次 unsigncrypt 询问),则存在一个区分者 C,能够在 $t'<t+(q_s+q_u)t_e$ 时间内,以优势 $\xi'\geq\frac{2\xi}{q_4*q_1}$解决 BDH 问题.其中, t_e 表示计算一次双线性对运算所需的时间.

证明 C 接收了一个随机的 BDH 问题实例(P, P_1, P_2, P_3) = (P, aP, bP, cP),他的目标是计算出 $e(P,P)^{abc}$. C 将攻击者 A 作为他的子程序使用. A 扮演游戏的敌手, C 扮演游戏的挑战者.游戏一开始, C 将系统参数发送给 A.其中, $P_{pub}=cP$(C 无法得知 c, c 扮演主密钥). C 维护 L_1, L_2, L_3, L_4 四张列表,这些列表初始状态为空, L_1, L_2, L_3, L_4 分别用于跟踪 A 对预言机 H_1, H_2, H_3, H_4 的询问.下面解释这些列表的建立.

H_1 询问:输入参数为 ID_U. C 首先从$\{1,2,\cdots q_1\}$中随机选取 i_1.此处不妨假设 A 不会做重复的询问.对于 A 的第 i 次询问,如果 $i\neq i_1$,从 Z_q^* 中随机选择 L_1 中未出现过的 x_i,计算 $H_1(ID_U)=Q_U=x_iP$,计算 $S_U=x_iP_{pub}$,并将(ID_U, Q_U, S_U, x_i)添加到 L_1 中.如果 $i=i_1$,令 $ID_b=ID_U$,返回 $H_1(ID_U)=bP$.

H_2 询问:输入参数为 m.如果(m, h_1)已经在表 L_2 中,返回 h_1;否则从 Z_q^* 中随机选择 L_2 中未出现过的 h_1,将(m, h_1)添加到 L_2 中,返回 h_1.

H_3 询问:输入参数为 h_1, R.如果(h_1, R, h_2)已在表 L_3 中,则返回 h_2;否则从 Z_q^* 中随机选择 L_3 中未出现过的 h_2,将(h_1, R, h_2)添加到 L_3 中,返回 h_2.

H_4 询问:输入参数为 ω.如果(ω, k)已在表 L_4 中,则返回 k;否则从$\{0,1\}^l$中随机选择 L_4 中未出现过的 k,将(ω, k)添加到 L_4 中,返回 k.

Extract 询问:假设 A 在对 ID_U 执行 Extract 询问前已经执行过 H_1 询问.如果 $ID_U=ID_b$,终止模拟;否则在表 L_1 中查找 ID_U 对应的组合(ID_U, Q_U, S_U, x_i),并返回 S_U.

Signcrypt 询问: A 输入(m, ID_1, ID_2).假设 A 在执行 Signcrypt 之前已经执行过 $H_1(ID_1)$和 $H_1(ID_2)$询问了.分两种情况进行讨论.

(1) $ID_1\neq ID_b$

在 L_1 表中查找组合(ID_1, Q_1, S_1, x_1).

随机选择 $r\in Z_q^*$,计算 $R=rP$.

输入参数 m,通过 H_2 询问获取 h_1.

输入参数 h_1, R,通过 H_3 询问获取 h_2.

计算 $S=\frac{r}{h_2+S_1}$.

计算 $\omega=e(P_{pub},Q_2)^r$.

输入参数 ω,通过 H_4 询问获取 k.

计算 $c=E_k(S\parallel m)$.

返回(c, R).

(2) $ID_1=ID_b$

输入参数 m,通过 H_2 询问获取 h_1.

随机选择 $h_2\in Z_q^*$, $S\in Z_q^*$.

计算 $R=S(h_2P+Q_1P_{pub})$.

查询 L_3 中是否已经有三元组(h_1, R, h_2'),并且 $h_2\neq h_2'$.如果存在这样的三元组,重新随机选择 $h_2\in Z_q^*$, $S\in Z_q^*$,重复上述过程,直到找到三元组的前两元并未在 L_3 中出现过,并将条目(h_1, R, h_2)加入 L_3.

在 L_1 表中查找组合(ID_2, Q_2, S_2, x_2).

计算 $\omega = e(R, S_2)$.

通过 H_4 询问获取 k.

计算 $c = E_k(S \| m)$.

返回密文 $\sigma = \{c, R\}$.

Unsigncrypt 询问:A 输入$(\sigma, \mathrm{ID}_1, \mathrm{ID}_2)$.假设 A 在进行 Unsigncrypt 询问之前已经执行过 $H_1(\mathrm{ID}_1)$和 $H_1(\mathrm{ID}_2)$询问了.分两种情况考虑.

(1)$\mathrm{ID}_2 \neq \mathrm{ID}_b$

在表 L_1 中查找条目$(\mathrm{ID}_2, Q_2, S_2, x_2)$.

计算 $\omega = e(R, S_2)$.

如果 $\omega \notin L_4$,返回符号"⊥";否则查询 L_4 获取 k 并计算 $S \| m = D_k(c)$.

如果 $m \notin L_2$,返回符号"⊥";否则通过查询 L_2 获取 h_1.

如果$(h_1, R, h_2) \notin L_3$,返回符号"⊥";

如果 $R \neq S(h_2 P + Q_1 P_{\mathrm{pub}})$,返回符号"⊥";

否则返回 m.

(2)$\mathrm{ID}_2 = \mathrm{ID}_b$

如果 $\mathrm{ID}_1 \notin L_1$,返回"⊥".

如果 $R \notin L_3$,返回"⊥".

按照以下步骤遍历 L_4 中的条目(ω, k).

计算 $S \| m = D_k(c)$.

如果 $m \notin L_2$,转到 L_4 的下一条目并重新开始.

根据 m 查询 L_2 获取条目(m, h_1).如果$(h_1, R) \notin L_3$,转到 L_4 的下一条目并重新开始.

根据(h_1, R)查询 L_3 获取 h_2.

验证 $R = S(h_2 P + Q_1 P_{\mathrm{pub}})$.如果成立,返回 m;否则转到 L_4 中的下一条目并重新开始.

如果遍历完 L_4 中所有的条目还是没有消息返回,返回"⊥".

经过多项式有界次上述询问后,A 输出两个希望挑战的身份$\{\mathrm{ID}_1^*, \mathrm{ID}_2^*\}$和两个长度均为 L 的明文$\{m_0, m_1\}$.此处,ID_2^* 不能被执行过 Extract 询问.如果 $\mathrm{ID}_2^* \neq \mathrm{ID}_b$,$C$ 终止这个模拟;否则令 $R^* = aP$,随机选择 $c^* \in \{0,1\}^n$(n 为当明文长度为 L,对称加密算法 E 输出密文的长度),令 $\sigma^* = (c^*, R^*)$,提交密文 σ^* 给 A.

A 开始第二轮的询问.这些询问与第一阶段相同,但不能对 ID_2^* 执行 Extract 询问,也不能对 c^* 执行 Unsigncrypt询问.在模拟结束时,A 输出 $u' \in \{0,1\}$作为对明文 m_u 中 u 的猜测.此时,C 从 L_4 中随机选择条目(ω_i, k_i),输出 ω_i 作为 BDH 问题的解答.

下面计算 C 成功的概率.

在挑战阶段,如果 $\mathrm{ID}_2^* \neq \mathrm{ID}_b$,$C$ 将失败.C 不在挑战阶段失败的概率为$\frac{1}{q_1}$.按照游戏规则,如果 A 在挑战阶段选择 $\mathrm{ID}_2^* = \mathrm{ID}_b$,那么 A 在询问过程中未对 ID_b 执行 Extract 询问.

令 D 代表该 BDH 问题的正确解答,令 Ω 代表事件 A 在上述模拟过程中对 D 进行了 $H_4(D)$询问.容易理解,Ω 等价于事件 D 出现在 L_4 中.文献[27]中已经证明,如果 A 以概率 ξ 赢得游戏,那么 $\Pr[\Omega] \geq 2\xi$.

C 从 L_4 的 q_4 个条目中随机选择一个,恰好选中 D 所在条目的概率为$\frac{1}{q_4}$.

综上,$\Pr[C \text{ succeed}] \geq \frac{1}{q_1} * 2\xi * \frac{1}{q_4} = \frac{2\xi}{q_4 * q_1}$

在 C 的计算时间方面,每次 signcrypt 询问最多需要 1 次双线性对运算,每次 unsigncrypt 询问最多需要 1 次双线性对运算.故 C 的计算时间 $t' < t + (q_s + q_u) t_e$.证毕.

定理 2　假设椭圆曲线上离散对数问题是困难的,那么在随机预言模型下,本文提出的签密方案在适应性选择消息攻击下能抗存在性伪造.

证明　假设一个敌手能伪造一个本签密方案中的签名,那么他就能伪造文献[29]中椭圆曲线上的短签名 SECDSSl.SECDSS1 是将文献[7]中的签名方案 SDSSl 移植到椭圆曲线密码体制中的形式.文献[7]指出在离散对数困难问题下,如果将散列函数视为随机函数,那么,SDSSl 是在适应性选择消息攻击下存在性不可伪造的.

综上,可以得出结论:假设椭圆曲线上离散对数问题是困难的,那么在随机预言机模型下,本文提出的签密方案是适应性选择消息攻击下存在性不可伪造的.证毕.

定理 3　本文提出的签密方案满足公开验证性、不可否认性、前向安全性.

证明　当通信双方产生争议时,只需提交$(R, S, h_1. h_2)$给第三方验证者,验证者检验等式 $R = S(h_2 P + Q_A P_{\mathrm{pub}})$和 $h_2 = H_3(h_1, R)$是否都成立即可.此过程不需要接收者的私钥,也不需要访问明文,满足公开验证性的同时保证了保密性.

由定理 2 得知,本文提出的签密方案在适应性选择消息攻击下能抗存在性伪造.如果发送方确实签密过一个消息,就无法否认.

假设发送方的私钥泄露,第三方得到了发送方的私钥 S_A.但即使如此第三方也无法计算会话密钥 $\omega = e(R, S_B)$或 $\omega = e(P_{\mathrm{pub}}, Q_B)^r$.所以本文提出的签密方案满足前向安全性.证毕.

5　效率分析

从计算量和通信成本两个方面来评价本文提出的

签密方案.为了简便,用 E,M,P 分别表示 G_2 中的指数运算次数,G_1 中的标量乘运算次数和双线性对运算次数.$x(+y)$表示需要 x 次双线性对运算,y 次双线性对预计算.$|G_1|$表示 G_1 中一个元素的长度,$|q|$表示有限域 Z_q 中一个元素的长度,$|m|$表示明文长度,|ID|表示身份 ID 的长度.

本方案的签密过程中,需要 1 次指数运算,1 次标量乘运算,1 次双线性对运算;解签密过程中,不需要指数运算,需要 2 次标量乘运算,1 次双线性对运算.本文的方案需要传输的信息是 $\sigma=\{c,R\}$,传输量是 $|c|+|R|=|G_1|+|q|+|m|$.

表 1 给出了本文所提的方案与目前已有的几个重要的基于身份的签密方案的对比.通过对比可以看出,本文的方案效率仅略低于文献[21]的方案,与其他方案相比均有明显的提高.但经过分析可知,文献[21]的方案并不提供前向安全性及公开验证性[24].本文提出的方案同时满足保密性、不可伪造性、公开验证性、不可否认性、前向安全性.

表 1 本文提出的方案与已有的重要签密方案的性能对比

方案	签密			解签密			密文长度
	P	M	E	P	M	E	
文献[9]	0(+1)	3	0	3(+1)	0	1	$2\|G_1\|+\|m\|$
文献[17]	0(+1)	3	0	3	1	0	$2\|G_1\|+\|ID\|+\|m\|$
文献[18]	0(+1)	4	1	2(+2)	0	2	$2\|G_1\|+\|m\|$
文献[21]	0(+1)	1	0	0(+1)	2	0	$2\|q\|+\|m\|$
文献[30]	0(+1)	3	1	2(+2)	0	2	$2\|G_1\|+\|ID\|+\|m\|$
文献[31]	0	2	2	2	1	1	$2\|G_1\|+\|G_2\|+\|ID\|+\|m\|$
本文方案	0(+1)	1	1	1	2	0	$\|G_1\|+\|q\|+\|m\|$

6 结束语

VANET 拓扑结构变化快、节点通信实时性强,如何保证通信的保密性与认证性是 VANET 研究中一项具有挑战性的课题.签密作为同时实现保密性和认证性的重要密码工具,对解决车载网络目前面临的安全问题具有重要意义.本文提出了一种适用于车载网环境下安全通信的基于身份的签密方案,并在随机预言模型下证明了该协议的安全性.通过与已有的基于身份签密方案的比较表明,新签密方案的计算量和通信成本较低,能适应车载网络安全通信的要求.研究适合于车载网络安全通信的签密方案,并将研究成果用于保证车载网络安全是必须予以足够重视的一个重要方向,这不仅是密码学应用研究的需要,也是车载网络广泛应用的迫切需要.

参考文献

[1] Martinez FJ, Toh C-K, Cano J-C, et al. Emergency services in future intelligent transportation systems based on vehicular communication networks [J]. Intelligent Transportation Systems Magazine, IEEE, 2010, 2(2): 6 – 20.

[2] Papadimitratos P, La Fortelle A, Evenssen K, et al. Vehicular communication systems: Enabling technologies, applications, and future outlook on intelligent transportation[J]. Communications Magazine, IEEE, 2009, 47(11): 84 – 95.

[3] Papadimitratos P, Buttyan L, Holczer T, et al. Secure vehicular communication systems: design and architecture[J]. Communications Magazine, IEEE, 2008, 46(11): 100 – 109.

[4] 吴磊,刘明,王晓敏,等.移动分布感知的车载自组网络数据分发[J].软件学报,2011,22(07):1580 – 1596
Wu L, Liu M, Wang X-M, et al. Mobile distribution-aware data dissemination for vehicular ad hoc networks [J]. Journal of Software, 2011, 22(7): 1580 – 1596. (in Chinese)

[5] Mishra B, Nayak P, Behera S, et al. Security in vehicular adhoc networks: a survey[A]. Proceedings of the 2011 International Conference on Communication, Computing & Security [C]. Odisha, India: ACM, 2011. 590 – 595.

[6] 田锐,孙利民,刘燕, et al. COBRA:车载网络中基于协作的大数据传输增强机制[J].计算机研究与发展,2009,46(12):2076 – 2084.
Tian Rui, Sun Limin, Liu Yan, et al. COBRA: A collaboration based reinforcement mechanism for mass transmission in VANETs[J]. Journal of Computer Research and Development, 2009, 46(12): 2076 – 2084. (in Chinese)

[7] Zheng Y. Digital signcryption or how to achieve cost (signature & encryption) << cost (signature) + cost (encryption)[A]. Advances in Cryptology—CRYPTO'97[C]. USA: Springer, 1997. 165 – 179.

[8] Shamir A. Identity-based cryptosystems and signature schemes [A]. Advances in Cryptology[C]. Heidelberg: Springer, 1985. 47 – 53.

[9] Malone-Lee J. Identity-based Signcryption[OL]. http://eprint.iacr.org, 2002.

[10] 刘辉.车载自组织网络信息认证和隐私保护机制的研究[D]:西安:西安电子科技大学,2012.

[11] Zhang L, Wu Q, Solanas A, et al. A scalable robust authentication protocol for secure vehicular communications[J]. Vehicular Technology, IEEE Transactions on, 2010, 59(4): 1606 – 1617.

[12] Kamat P, Baliga A, Trappe W. An identity-based security framework for VANETs[A]. Proceedings of the 3rd International Workshop on Vehicular Ad hoc Networks[C]. Los Angeles, USA: ACM, 2006. 94 – 95.

[13] 张秋璞,叶顶锋.对一个基于身份的多重签密方案的分析和改进[J].电子学报,2011,39(12):2713 – 2720.
Zhang Qiupu, Ye Dingfeng. Cryptanalysis and improvement of an identity-based multi-signcryption scheme [J]. Acta Electronica Sinica, 2011, 39(12): 2713 – 2720. (in Chinese)

[14] Libert B, Quisquater J-J. A new identity based signcryption scheme from pairings[A]. Information Theory Workshop 2003 Proceedings[C]. Paris, France: IEEE, 2003. 155 – 158.

[15] Nalla D, Reddy K C. Signcryption Scheme for Identity-based Cryptosystems[OL]. http://eprint.iacr.org, 2003.

[16] Chow SS, Yiu S-M, Hui LC, et al. Efficient forward and provably secure ID-based signcryption scheme with public verifiability and public ciphertext authenticity[A]. Information Security and Cryptology-ICISC 2003[C]. Seoul, Korea: Springer, 2004. 352 – 369.

[17] Chen L, Malone-Lee J. Improved identity-based signcryption [A]. Public Key Cryptography-PKC 2005[C]. Les Diablerets, Switzerland: Springer, 2005. 362 – 379.

[18] 李发根,胡予濮,李刚.一个高效的基于身份的签密方案[J].计算机学报,2006,29(9):1641 – 1647.
Li Fagen, Hu Yupu, Li Gang. An efficient identity-based signcryption scheme[J]. Chinese Journal of Computers, 2006, 29(9):1641 – 1647. (in Chinese)

[19] 张明武,杨波,周敏,张文政.两种签密方案的安全性分析及改进[J].电子与信息学报,2010,32(07):1731 – 1736.
Zhang M-W, Yang B, Zhou M, et al. Analysis and improvement of two signcryption schemes[J]. Journal of Electronics and Information Technology, 2010, 32(7):1731 – 1736. (in Chinese)

[20] 张键红.两种签密方案的安全分析[J].东南大学学报(自然科学版),2007,37(S1):29 – 33.
Zhang Jianhong. Security analysis of two signcryption schemes [J]. Journal of Southeast University (Natural Science Edition), 2007:37(S1):29-33. (in Chinese)

[21] 张串绒,张玉清,李发根,等.适于 ad hoc 网络安全通信的新签密算法[J].通信学报,2010,31(3):19 – 24.
Zhang Chuanrong, Zhang Yuqing, Li Fagen, et al. New signcryption algorithm for securecommunication of ad hoc networks[J]. Joumal on Communications. 2010, 31(3):19 – 24. (in Chinese)

[22] 黄欣沂,张福泰,伍玮.一种基于身份的环签密方案[J].电子学报,2006,34(2):263 – 266.
HUANG Xin-yi, ZHANG Fu-tai, WU Wei. An identity-based ring signcryption scheme[J]. Acta Electronica Sina, 2006, 34(2):263 – 266. (in Chinese)

[23] 张串绒,肖国镇.一个可公开验证签密方案的密码分析和改进[J].电子学报,2006,34(1):177 – 179.
Zhang Chuanrong, Xiao Guozhen. Cryptanalysis and improvement of a signcryption scheme with public verifiability[J]. Acta Electronica Sinica, 2006, 34(1):177 – 179. (in Chinese)

[24] 肖鸿飞,刘长江.一种基于身份的改进高效签密方案[J].计算机工程,2011,37(24):126 – 128.
Xiao H-F, Liu C-J. Improvedefficient identity-based signcryption scheme[J]. Computer Engineering, 2011, 37(24):126 – 128. (in Chinese)

[25] 李晋国,林亚平,李睿,等.车载自组织网络中基于椭圆曲线零知识证明的匿名安全认证机制[J].通信学报,2013,34(5):52 – 61.
Li Jinguo, Lin Yaping, Li Rui, et al. Secure anonymous authentication scheme based on elliptic curve and zero-knowledge proof in VANET[J]. Joumal on Communications, 2013, 34(5):52 – 61. (in Chinese)

[26] 冯登国.可证明安全性理论与方法研究[J].软件学报,2005,16(10):1743 – 1756.
Feng Dengguo. Research on theory and approach of provable security[J]. Journal of Software, 2005, 16(10):1743 – 1756. (in Chinese)

[27] Boneh D, Franklin M. Identity-based encryption from the Weil pairing[J]. SIAM Journal on Computing, 2003, 32(3):586 – 615.

[28] Odlyzko AM. Discrete logarithms in finite fields and their cryptographic significance[A]. Advances in Cryptology[C]. Berlin Heidelberg: Springer, 1985. 224 – 314.

[29] Zheng Y, Imai H. How to construct efficient signcryption schemes on elliptic curves[J]. Information Processing Letters, 1998, 68(5):227 – 233.

[30] Yu G, Ma X, Shen Y, et al. Provable secure identity based generalized signcryption scheme[J]. Theoretical Computer Science, 2010, 411(40):3614 – 3624.

[31] Kushwah P, Lal S. An efficient identity based generalized signcryption scheme[J]. Theoretical Computer Science, 2011, 412(45):6382 – 6389.

作者简介

张　宇　男,1984 年生于山东泰安.现为武汉大学计算机学院博士研究生.研究方向为网络安全.
E-mail:zy168612@qq.com

陈　晶(通信作者)　男,1981 年生于湖北武汉.武汉大学计算机学院副教授、博士生导师.研究方向为网络安全、无线网络.
E-mail:chenjing@whu.edu.cn

杜瑞颖　女,1964 年生于河南新乡.武汉大学计算机学院教授、博士生导师.研究方向为网络安全、无线网络.

周　庆　男,1974 年生于江苏泰兴,信息保障技术重点实验室高级工程师.研究方向为信息安全技术.

郑明辉　男,1974 年生于湖北嘉鱼.湖北民族学院教授.研究方向为信息安全.