

VANET 中基于无证书环签密的可认证隐私保护方案



赵楠 章国安

南通大学信息科学技术学院 江苏 南通 226019

(1054439272@qq.com)

摘要 针对车载自组织网络(Vehicular ad-hoc Network, VANET)中车辆用户隐私信息保护和通信消息传输安全的问题,提出了一种可认证的无证书环签密方案。车辆通过可信机构生成的伪身份通信,有且仅有可信机构可以根据车辆节点的原始注册信息和追踪密钥确定消息发送车辆的真实身份,保证了通信的匿名性和对恶意车辆身份的可追踪性;消息发送车辆和接收车辆基于所构建的可认证环签密模型分别执行签密和解签密算法,实现了签密车辆身份和所发送消息的可认证;在随机预言模型下证明了所提方案具有机密性和不可伪造性。将所提的隐私保护方案与现有的 VANET 隐私保护方案进行安全性能的比较,证明了所提方案的机密性、可认证性和可追踪性等安全性较完善。通过列表比较了所提方案中环签密和解签密算法中各项运算的数量。将两种算法中双线性运算和标量乘运算的开销之和作为所提方案的计算开销,列表并进行数值分析。仿真实验基于 Intel I7、3.07 GHz 的硬件平台和 MATLAB 软件。结果表明,所提方案的计算开销远小于其余 3 个方案。当车辆数量增大到适用范围的上限 100 时,所提方案的计算开销仍小于 150 ms。因此,该隐私保护方案满足了安全性和即时通信的要求,尤其适用于城市交通系统。

关键词 车载自组织网络;无证书密码体制;环签密;认证;隐私保护;可追踪性;效率

中图法分类号 TN918.4

Authenticated Privacy Protection Scheme Based on Certificateless Ring Signcryption in VANET

ZHAO Nan and ZHANG Guo-an

School of Information Science and Technology, Nantong University, Nantong, Jiangsu 226019, China

Abstract Aiming at the protection of vehicle users' privacy information and the security transmission of communication messages in the vehicle ad-hoc networks, an authenticated certificateless ring signcryption scheme was proposed. The vehicles communicated with others through their pseudo-identities generated by the trusted authority, and the real-identity of the vehicle can only be determined by the trusted authority according to the original registration information of the vehicle node and the tracing keys, which ensures the anonymity of the communication and traceability of the malicious vehicles. The signcryption and decryption algorithms are implemented respectively by message sending vehicle and receiving vehical based on the proposed authenticated certificateless ring signcryption model, which results in the achievement of the identity authentication of the signcryption vehicle and authentication of sending messages. The confidentiality and unforgeability of the proposed scheme can be proved under the random oracle model. Compared with the existing privacy-protection schemes of VANET, the security performance of the proposed scheme is more perfect in terms of confidentiality, authentication and traceability. Through the lists, the number of operations in the ring signcryption and decryption algorithms of the scheme are compared. The sum overhead of bilinear operations and scalar multiplications is treated as the computational overhead of the scheme, and is listed and analyzed numerically. The simulations of the scheme are based on Intel I7, 3.07 GHz hardware platform and MATLAB software. The results show that the computational overhead of the proposed scheme is far less than the other three. When the number of vehicles increases to 100, the upper limit of the applicable range, the computational overhead of the proposed scheme is still less than 150ms. Therefore, the proposed privacy protection scheme has satisfied the requirement of security and instant messaging, especially suitable for urban transportation systems.

Keywords Vehicular ad-hoc network, Certificateless public key cryptosystem, Ring signcryption, Authentication, Privacy protection, Traceability, Efficiency

到稿日期:2019-01-15 返修日期:2019-05-24 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:国家自然科学基金青年科学基金(61801249)

This work was supported by the Young Scientists Fund of the National Natural Science Foundation of China (61801249).

通信作者:章国安(gzhang@ntu.edu.cn)

1 引言

车载自组织网络^[1]是一种新型的多跳移动自组织网络,由路边基础设施和安装了具有通信和计算功能的移动传感器的车辆构成,主要包含两种通信模式^[2]:1)车与车的通信 V2V(Vehicle to Vehicle, V2V);2)车与路边基础设施的通信 V2I(Vehicle to Infrastructure, V2I)。随着智能交通系统^[3]的迅猛发展,传感、GPS、无线通信等智能技术被应用到 VANET 中,为人们提供了日益便捷、舒适的驾驶环境。但由于 VANET 的高移动性、较大网络规模以及开放的通信环境等特点,一系列安全问题(例如广播信息被篡改、通信消息被窃听、用户身份隐私信息被泄露)对 VANET 通信的安全可靠以及车辆用户的生命财产安全都产生了巨大的威胁,如何应对和解决 VANET 的隐私保护问题变得日益迫切。

目前,已经有许多学者对 VANET 中存在的隐私和隐私保护问题做了研究,大多数方案是根据基于身份的公钥密码体制^[4]而提出的。Zhang 等^[5]提出了一种用于 VANET 消息认证的隐私保护和可扩展方案,将基于身份的签密用于帮助车辆从 RSU 秘密地接收秘密成员的密钥,使车辆可以代表该组匿名发送消息;文献^[6]基于身份的签名(Identity-Based Signature, IBS)和基于身份的在线/离线签名(Identity-Based Online/Offline Signature, IBOOS)这两种方案对 V2R 通信双方的身份进行验证,以增强 VANET 通信的安全性;2016 年, Xie 等^[7]提出了一种有效的条件隐私保护认证方案,显著降低了消息签名阶段和消息验证阶段的计算成本;文献^[8]提出了一种新的双重认证方案,将指纹认证技术运用到哈希码的创建中,以避免恶意用户使用 VANET 中的用户密钥参与通信,提高了与网络通信的车辆的安全性。

近年来,无证书公钥密码体制^[9]的研究逐渐成为热点,许多研究者将数字签名与无证书密码体制相结合并应用于 VANET 隐私保护的方案设计中。Wang 等^[10]构造了一种新的无证书聚合签名算法,通过 RSU 生成的假名和车辆节点通信,从而实现 VANET 中车辆用户的隐私保护和通信节点间信息传输的安全认证;Yang 等^[11]提出了一种可证安全的 VANET 消息认证方案,认证中心 TA 利用代理重签名技术以 RSU 的签名代替 OBU 对消息的签名,大大降低了攻击者根据签名推测出车辆身份的可能性,满足了通信消息的匿名性要求。

签密打破了传统密码学采用的先签名后加密这种效率较低的方式,在一个逻辑算法中完成了用户对所发送消息的签名及加密^[12]。签密降低了计算开销,大大提高了计算效率,文献^[13-15]是部分无证书签密的实例。另外,许多特殊的数字签密方式^[16-19]也被不断提出并应用到 VANET 消息认证和隐私保护中。

近年来,环签密方式的研究不多,鉴于目前将环签密应用于 VANET 的实例较少,本文以无证书环签密^[20-22]为基础,构建了一个可认证的环签密算法模型,并提出了一种保护 VANET 车辆节点隐私和保密通信消息的可认证无证书环签密 CLRS(Certificateless Ring Signcryption)方案。该方案在匿名性、可认证性、可追踪性、机密性、不可伪造性等安全性能方面较完善,并且通过仿真实验比较发现,该方案的计算开销

较低,满足即时性要求,能较好地适用于城市交通通信系统。

2 基础知识

2.1 VANET 中的 CLRS 系统模型

典型的 VANET 系统一般包含以下 3 个部分。

(1)车辆节点:网络中每个车辆都安装了可与其他设备进行数据交互的车载单元(On Board Unit, OBU),OBU 一般是无线传感器,通过 LTE 4G/5G 与其他车载单元或路边单元通信。

(2)路边单元(Road Side Unit, RSU):RSU 通常部署在道路两侧和交叉路口,通过 LTE 4G/5G 与车辆节点通信,RSU 之间的通信则通过有线网路的安全通道进行。

(3)可信机构(Trust Authority, TA):通常由所处区域内的交通管理部门担任,负责车辆节点的初始注册,同时生成车辆用户的伪身份、发布系统参数,并通过有线信道与 RSU 通信,TA 一般默认是一个可信任的权威机构。

图 1 给出了无证书环签密下 VANET 的系统模型。环 R 中有 n 个车辆用户 $R = \{V_1, V_2, \dots, V_n\}$,假设环中某车辆有代表环中所有车辆对消息明文 m 签密的意愿并执行了环签密算法,环外一车辆接收到该密文后对应地执行解签密算法,从而获得消息。

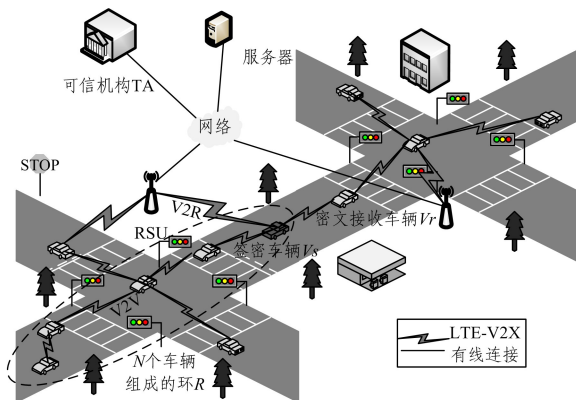


图 1 无证书环签密下 VANET 的系统模型

Fig. 1 System model of CLRS in VANET

2.2 双线性映射

$(G_1, +)$ 是生成元为 P 的 q 阶循环加法群, $(G_2, \cdot)$ 是同阶循环乘法群, q 为大素数, Z_q^* 是 $(q-1)$ 非 0 正整数循环群。设双线性映射 $e: G_1 \times G_1 \rightarrow G_2$ 满足以下 3 个性质。

(1)双线性性:对于 $\forall R, S, T \in G_1, x, y \in Z_q^*$, 有 $e(R, S+T) = e(R, S)e(R, T)$, $e(xR, yT) = e(xyR, T) = e(R, xyT) = e(R, T)^{xy}$ 。

(2)非退化性:存在 $R, T \in G_1$, 使 $e(R, T) \neq 1_{G_2}$ (1_{G_2} 表示群 G_2 的生成元)。

(3)可计算性:对于 $\forall R, T \in G_1$, $e(R, T)$ 可以由一个算法在多项式时间内计算出。

2.3 复杂性假设

定义 1(决策双线性 Diffie-Hellman (Decisional Bilinear Diffie-Hellman, DBDH)问题) 设 G_1 和 G_2 为 q 阶循环群,对于随机数 $a, b, c \in Z_q^*, w \in G_2$, 给定数组 $(P, aP, bP, cP, w) \in G_1^4 \times G_2$, 判断是否有 $w = (P, P)^{abc}$ 。

定义 2(计算 Diffie-Hellman (Computational Diffie-Hell-

man, CDH)问题) 设 G_1 为 q 阶循环群, 对于随机数 $a, b \in Z_q^*$, 给定数组 $(P, aP, bP) \in G_1^3$, 在 G_1 中计算出 abP 。

3 本文的可认证 CLRS 隐私保护方案

3.1 可认证的环签密算法模型

公钥密码体制中有加密和认证两种基本模型, 本文将这两个模型组合并与环签名相结合, 构建了一个新的可认证环签密算法模型, 其具备保密性和可认证性。假设 E 表示加密

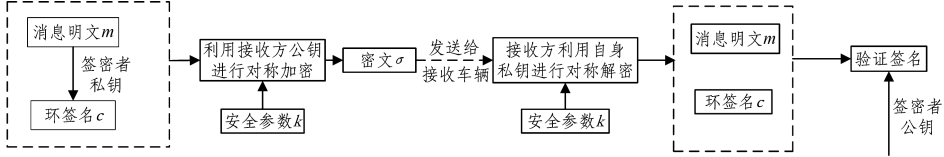


图2 可认证环签密算法模型

Fig. 2 Authenticated ring signcryption algorithm model

3.2 可认证 CLRS 隐私保护方案设计

在文献[23-24]和可认证环签密算法模型的基础上, 本文提出了一个适用于 VANET 隐私保护的、可认证的无证书环签密方案, 并且在环签密算法中设置了 3 个用于追踪签密车辆真实身份的追踪密钥。该方案满足了安全性、隐私性、可追踪性、机密性和不可伪造性。

本文方案包含 7 个子算法: 系统初始化、车辆注册、部分私钥提取、秘密值和车辆用户公钥生成、车辆用户完整私钥生成、环签密和解签密算法。

3.2.1 系统初始化

密钥生成中心 KGC 选择系统安全参数 k , G_1 是阶数为 q 的循环加法群, G_2 是同阶循环乘法群 (q 为素数且设置 $q = k$), P 是循环群 G_1 的一个生成元。假设双线性对 $e: G_1 \times G_1 \rightarrow G_2$ 。KGC 选择 4 个安全的单向散列函数 $H_1 - H_4$, 分别为 $H_1: \{0, 1\}^* \rightarrow G_1$, $H_2: G_2 \rightarrow \{0, 1\}^l \times G_1$, $H_3: \{0, 1\}^l \times G_1 \times G_2 \times \{0, 1\}^* \times G_1 \rightarrow Z_q^*$ 和 $H_4: \{0, 1\}^l \times Z_q^* \rightarrow Z_q^*$ 。其中, l 是消息明文 m 的长度。KGC 选择一个随机数 $s \in Z_q^*$ 作为系统的主密钥, 然后计算系统公钥 $P_{pub} = sP$ 。KGC 公开系统参数 $Params = \{q, e, G_1, G_2, P, P_{pub}, H_1, H_2, H_3, H_4\}$, 保密主密钥 s 。

3.2.2 车辆注册

交通管理中心 (Traffic Management Center, TMC) 执行这一操作。在 TMC 管理区域内的每一个车辆用户 V_i 都必须在 TMC 进行用户身份的初始注册, 车辆用户 V_i 的身份 $ID_{V_i} \in \{0, 1\}^*$ 。KGC 计算 $Q_i = H_1(ID_{V_i})$ 作为车辆 V_i 的伪身份, 车辆在与其它车辆通信中使用该伪身份进行数据匿名交互。

3.2.3 用户部分私钥提取

输入系统公共参数 $Params$ 、主密钥 s 和车辆 V_i 的伪身份 Q_i , KGC 计算车辆用户 V_i 的部分私钥 $psk_{V_i} = s \cdot Q_i$ 。

3.2.4 秘密值和车辆用户公钥的生成

输入系统公共参数 $Params$ 、车辆用户 V_i 的伪身份 Q_i , 车辆用户 V_i 选择随机数 $x_i \in_R Z_q^*$ 作为其秘密值, KGC 计算车辆用户公钥 PK_{V_i} 并通过安全通道将其发送给车辆 V_i 。

$$PK_{V_i} = (X_i, Y_i) = (x_i Q_i, x_i P_{pub}) \quad (1)$$

3.2.5 车辆用户完整私钥的生成

输入系统主密钥 s , 车辆用户 V_i 计算自身完整私钥:

(Encryption) 算法, D 表示解密 (Decryption) 算法。首先, 环中消息发送者 (签密车辆) V_s 用自身私钥 SK_{V_s} 对消息 m 进行加密, 得到签名 $c = E(SK_{V_s}, m)$; 然后, 利用环外消息接收车辆 V_r 的公钥 PK_{V_r} 进行二次加密, 得到环签密 $\sigma = E(PK_{V_r}, E(SK_{V_s}, m))$; V_r 收到环签密 σ 后, 利用自身私钥 SK_{V_r} 对密文解密, 再应用签密车辆的公钥 PK_{V_s} 进行二次解密; 最后, 利用公钥合法性验证解密的明文 $m = D(PK_{V_s}, D(SK_{V_r}, \sigma))$ 是否正确。可认证环签密算法的模型如图 2 所示。

$$SK_{V_i} = x_i \cdot psk_{V_i} = x_i \cdot s \cdot Q_i \quad (2)$$

3.2.6 环签密

假设环 R 中有 n 个车辆 $R = \{V_1, V_2, \dots, V_n\}$, 车辆用户 V_s 有代表环 R 中所有车辆对消息明文 m 签密的意愿。车辆用户 V_s 的身份为 ID_{V_s} , 其公钥为 PK_{V_s} , 私钥为 SK_{V_s} , 表达式分别为:

$$PK_{V_s} = (X_s, Y_s) = (x_s Q_s, x_s P_{pub}) \quad (3)$$

$$SK_{V_s} = x_s \cdot psk_{V_s} = x_s \cdot s \cdot Q_s \quad (4)$$

环签密 σ 的接收车辆 V_r 的身份为 ID_{V_r} , 其公钥为 $PK_{V_r} = (X_r, Y_r)$, 私钥为 SK_{V_r} 。签密车辆 V_s 执行以下步骤对消息 m 进行加密。

(1) 选择随机数 $\alpha \in_R Z_q^*$, 计算:

$$U = \alpha \cdot P \quad (5)$$

$$\omega = e(P_{pub}, X_r)^\alpha \quad (6)$$

(2) 对于任意的 $i \in \{1, 2, \dots, n\}$, 若 $i \neq s$, 选择 $\beta_i \in_R Z_q^*$, 计算:

$$R_i = \beta_i \cdot P \quad (7)$$

$$h_i = H_3(m, R_i, \omega, R, X_r) \quad (8)$$

若 $i = s$, 选择 $\beta_s \in_R Z_q^*$, 计算:

$$R_s = \beta_s \cdot X_s - \sum_{i=1, i \neq s}^n (R_i + h_i \cdot X_i) \quad (9)$$

$$h_s = H_3(m, R_s, \omega, R, X_r) \quad (10)$$

$$Z = (\beta_s + h_s) \cdot SK_{V_s} \quad (11)$$

(3) 对于任意的 $i \in \{1, 2, \dots, n\}$, 选择 $t_i \in_R Z_q^*$, 计算追踪密钥:

$$T_i = t_i \cdot P_{pub} \quad (12)$$

$$TK_i = t_i \cdot Y_i \quad (13)$$

$$T = x_s \cdot \sum_{i=1}^n T_i \quad (14)$$

(4) 计算密文:

$$c = (m \parallel Z) \oplus H_2(\omega) \quad (15)$$

因此, 消息明文 m 对应的环签密为 $\sigma = (c, U, R, R_1, \dots, R_n, T, T_1, \dots, T_n, TK_1, \dots, TK_n, Z)$ 。签密车辆 V_s 将环签密 σ 发送给接收车辆 V_r 。

3.2.7 解签密

接收车辆 V_r 的身份为 ID_{V_r} , 其公钥为 $PK_{V_r} = (X_r, Y_r)$, 私钥为 SK_{V_r} 。 V_r 收到环签密 σ 后用自身私钥 SK_{V_r} 对 σ 进行

解密,解密的具体过程如下。

(1)验证公钥的合法性:对于所有 $i \in \{1, 2, \dots, n\}$, 验证式(16)是否成立。若等式成立,则公钥合法,继续解密;否则,输出 $\perp$, 表示解密失败。

$$e(X_i, P_{\text{pub}}) = e(Q_i, Y_i) \quad (16)$$

(2)计算 $w' = e(U, SK_{V_r})$, 并通过计算式(17)得到 m' 和 Z' 。

$$(m' \parallel Z') = c \oplus H_2(w') \quad (17)$$

(3)对于任意 $i \in \{1, 2, \dots, n\}$, 计算式(18)并验证式(19)是否成立。若等式成立,则表明解密成功,输出解密后的消息 m' ; 否则,解密失败,输出 $\perp$ 。

$$h'_i = H_3(m', R_i, w', R, X_r) \quad (18)$$

$$e(P_{\text{pub}}, \sum_{i=1}^n (R_i + h'_i X_i)) = e(P, Z') \quad (19)$$

图3和图4分别给出了签密车辆 V_s 代表环 R 对消息明文 m 进行签密以及接收车辆 V_r 接收到环签密 σ 后对其进行解密的流程。

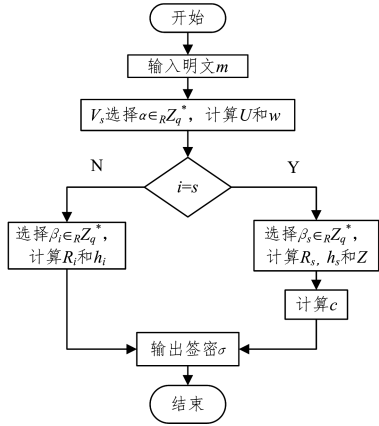


图3 环签密算法流程图

Fig. 3 Flow chart of ring signcrypt algorithm

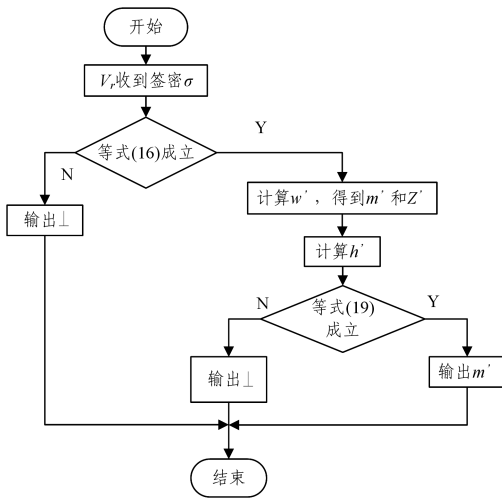


图4 解签密算法流程图

Fig. 4 Flow chart of ring decryption algorithm

4 方案分析

4.1 正确性

4.1.1 公钥合法性

证明:

$$e(X_i, P_{\text{pub}}) = e(x_i Q_i, P_{\text{pub}}) = e(Q_i, Y_i) \quad (20)$$

等式(20)成立。

4.1.2 签密正确性

证明:

$$\begin{aligned} e(P_{\text{pub}}, \sum_{i=1}^n (R_i + h'_i X_i)) &= e(P_{\text{pub}}, \sum_{i=1, i \neq s}^n (R_i + h'_i X_i)) e(P_{\text{pub}}, R_s + h'_s X_s) \\ &= e(P_{\text{pub}}, \sum_{i=1, i \neq s}^n (R_i + h'_i X_i)) e(P_{\text{pub}}, R_s) e(P_{\text{pub}}, h'_s X_s) \\ &= e(P_{\text{pub}}, \beta_s X_s) e(P_{\text{pub}}, h'_s X_s) \\ &= e(sP, (\beta_s + h'_s) X_s) \\ &= e(P, (\beta_s + h'_s) SK_{V_s}) \\ &= e(P, Z') \end{aligned} \quad (21)$$

等式(21)成立。

4.2 安全性

4.2.1 匿名性

本文方案实现了消息传递双方的匿名通信。

(1)发送车辆匿名

车辆在TMC注册后获得伪身份,并用该伪身份与其他车辆节点通信,签密车辆使用自身私钥产生签名标识 $Z = (\beta_s + h_s) \cdot SK_{V_s}$, 接收车辆通过验证等式(22):

$$\begin{aligned} e(Z, P) &= e((\beta_s + h_s) \cdot SK_{V_s}, P) \\ &= e((\beta_s + h_s) \cdot x_s \cdot Q_s, P_{\text{pub}}) \\ &= e(\beta_s X_s + h_s X_s, P_{\text{pub}}) \\ &= e(\sum_{i=1}^n (R_i + h_i X_i), P_{\text{pub}}) \end{aligned} \quad (22)$$

只能判断出签密车辆是环 R 中成员,无法推算出具体的签密车辆身份,因为由等式(23)可知,签密车辆 V_s 可以是环 R 中任意一个成员,密文接收车辆 V_r 无法通过收到的密文计算出该签密是由环 R 中哪一个车辆加密并发送的。另外,环外车辆判断出真实签密车辆的可能性至多为 $1/n$;即使是环内车辆,能够判断出哪一个车辆是代表整体对消息进行签密的可能性至多为 $1/(n-1)$ 。这一匿名方式有效保护了签密车辆用户的隐私信息,实现了发送车辆的匿名。

$$\begin{aligned} \sum_{i=1, i \neq s}^n (R_i + h_i X_i) + R_s + h_s X_s &= \sum_{i=1}^n (R_i + h_i X_i) \\ &= \sum_{i=1, i \neq j}^n (R_i + h_i X_i) + R_j + h_j X_j \end{aligned} \quad (23)$$

(2)接收车辆匿名

环签密密文 $\sigma = (c, U, R, R_1, \dots, R_n, T, T_1, \dots, T_n, TK_1, \dots, TK_n, Z)$ 中不包含接收车辆的身份信息,且通过式(6)、式(8)和式(10),将接收车辆公钥隐藏在式(15)计算的参数密文 c 中,攻击者无法通过截获的密文计算出接收车辆公钥、推测出接收车辆真实身份,从而实现了接收车辆的匿名。

综上,本文方案满足了车辆节点的匿名性要求。

4.2.2 可认证性

本文将公钥密码体制中的加密和认证两个模型相结合,提出了一个新的可认证的无证书环签密算法模型。签密过程中的每一个加密步骤与解密过程的每一个解密步骤都是对应的,即签密车辆 V_s 利用自身私钥 SK_{V_s} 对明文 m 进行加密,

再利用接收车辆 V_r 的公钥 PK_{V_r} 对 m 进行二次加密,接收车辆 V_r 在收到环签密 σ 后利用 SK_{V_r} 进行解密,再通过 V_s 的公钥进行二次解密,同时通过验证公钥合法性来验证密文是否合法。由于无证书密码体制下签密车辆 V_s 的私钥是由车辆自己随机选择的秘密值和 KGC 产生的部分私钥共同组成,保证了私钥的隐私性,因此在没有签密车辆私钥的情况下任何车辆都无法篡改 m ,从而实现了对于消息 m 的来源以及数据完整性的可认证。

4.2.3 可追踪性

环外车辆 V_r 接收到密文 σ 后,若发现签密车辆 V_s 有传递虚假信息或不诚实行为,欲找出环中签密车辆的真实身份,则可向 TA 提出仲裁申请。TA 通过以下步骤执行仲裁,确定签密车辆的真实身份。

(1)TA 的仲裁机构根据密文 σ 中的 TK_i 和环 R 的成员集合,向环中所有的车辆收集各自的 T_i , $T_i = TK_i \cdot x_i^{-1}$ 。

(2)仲裁机构集合齐所有的 T_i 后,通过计算判断式(24)成立,以验证 T_i 的有效性。若等式成立,则 T_i 有效。

$$e(TK_i, P_{\text{pub}}) = e(T_i, Y_i) \quad (24)$$

(3)若 T_i 有效,则计算 $L = \sum_{i=1}^n T_i$,通过逐一代入环中各车辆的 Y_i ,验证式(25),找出签密车辆的 Y_s ,从而确定签密车辆的真实身份,实现签密车辆的可追踪。

$$\begin{aligned} e(T, P_{\text{pub}}) &= e(x_s \cdot \sum_{i=1}^n T_i, P_{\text{pub}}) = e(\sum_{i=1}^n T_i, Y_i) \\ &= e(L, Y_i) \end{aligned} \quad (25)$$

4.2.4 机密性

定理 1 在随机预言模型和决策双线性 Diffie-Hellman 复杂性假设下,面对第 1 种类型敌手 A_I 的适应性选择密文攻击,本文的 CLRS 方案具有机密性(IND-CLRS-CCA2)。

证明:

在 DBDH 复杂性假设下,给定一个元组 (P, aP, bP, cP) ,挑战者 C_1 的挑战目标是利用 A_I 判断是否有 $w = (P, P)^{abc}$ 。设 H_1, H_2, H_3, H_4 是随机预言机, C_1 对 A_I 发起的询问作出如下回答。

(1)系统建立

挑战者 C_1 任选随机数 $a, b, \gamma \in_R Z_q^*$, 计算系统公钥 $P_{\text{pub}} = aP$, 发布系统参数 $Params$ 并将其发送给 A_I , 其中:

$$Params = \{q, e, G_1, G_2, P, P_{\text{pub}}, H_1, H_2, H_3, H_4\}$$

(2)询问

1) H_1 询问。 C_1 维护 H_1 列表 $L_1 = (ID_{V_i}, Q_i, \lambda_i)$, 列表初始状态为空。敌手 A_I 输入车辆身份 $ID_{V_i} \in \{0, 1\}^*$, C_1 检查列表 L_1 中已有的记录。当 $i=r$ 时, 计算 $Q_r = bP$, 输出 $\lambda_i = \perp$, 将元组 $(ID_{V_r}, Q_r, \perp)$ 添加到 L_1 并返回 Q_r ; 当 $i \neq r$ 时, C_1 选择随机数 $\lambda_i \in_R Z_q^*$, 计算 $Q_i = \lambda_i P$, 更新元组 $(ID_{V_i}, Q_i, \lambda_i)$ 到 L_1 并返回 Q_i 。

2) H_2 询问。 C_1 维护 H_2 列表 $L_2 = (w, \gamma)$, 列表初始状态为空。 C_1 查找 L_2 , 若存在元组 (w, γ) , 则返回 γ 给 A_I ; 否则, C_1 随机选择 $\gamma \in \{0, 1\}^l \times G_1$, 并将元组 (w, γ) 添加到 L_2 后返回 γ 。

3) H_3 询问。 C_1 维护 H_3 列表 $L_3 = (m_i, R_i, w, R, X_r, h_i)$, 列表初始状态为空。 C_1 查找 L_3 , 若列表中存在元组 $(m_i, R_i, w, R, X_r, h_i)$, 则返回 h_i 给 A_I ; 否则, C_1 随机选择 $h_i \in$

$_R Z_q^*$, 将元组 $(m_i, R_i, w, R, X_r, h_i)$ 添加到 L_3 后返回 h_i 。

4) H_4 询问。 C_1 维护 H_4 列表 $L_4 = (m_i, r_i, \beta_i)$, 列表初始状态为空。 C_1 查找 L_4 , 若列表中元组 (m_i, r_i, β_i) 存在, 则返回 β_i ; 否则, C_1 随机选择 $\beta_i \in_R Z_q^*$, 返回 β_i 并将元组 (m_i, r_i, β_i) 添加到 L_4 。

5) 部分私钥询问。 C_1 维护列表 L_{psk} , 列表初始状态为空。当敌手 A_I 询问车辆部分私钥 psk_{V_i} 时 C_1 查找列表 L_{psk} , 若 $i=r$, 则 C_1 挑战失败; 若 $i \neq r$, 则 C_1 查找 $L_1 = (ID_{V_i}, Q_i, \lambda_i)$, 将 Q_i 返回给 A_I 。

6) 公钥询问。 C_1 维护列表 $L_{PK} = (ID_{V_i}, x_i, PK_{V_i})$, 列表初始状态为空。敌手 A_I 向 C_1 询问车辆的公钥 PK_{V_i} , C_1 查找 L_{PK} , 若列表中已存在 PK_{V_i} , 则将其返回给 A_I ; 若没有记录, 则 C_1 选择随机数 $x_i \in_R Z_q^*$ 并计算公钥 $PK_{V_i} = (X_i, Y_i) = (x_i Q_i, x_i P_{\text{pub}})$, 然后将元组 $(ID_{V_i}, x_i, PK_{V_i})$ 添加到列表 L_{PK} 中并返回 PK_{V_i} 。

7) 公钥替换询问。敌手 A_I 发起公钥替换询问。 C_1 查找列表 L_{PK} 后, 令 $PK_{V_i} = PK_{V_i}', x_i = \perp$, 然后将更新的元组 $(ID_{V_i}, \perp, PK_{V_i}')$ 添加到 L_{PK} 。

8) 秘密值询问。 C_1 收到 A_I 的秘密值询问后查找 L_{PK} 中已有记录, 将 x_i 的值返回给 A_I ; 若列表中车辆的公钥已被替换, 则返回 $x_i = \perp$ 。

9) 环签密询问。 C_1 获得消息 $m_i \in \{0, 1\}^*$, 查找: ①列表 L_1 中存在身份为 ID_{V_i} 的车辆; ②该车辆在环 R 中。若不能同时满足这两个要求, C_1 挑战失败; 否则, C_1 按照环签密算法步骤计算消息 m 的签密并返回给 A_I 。

10) 解签密询问。收到身份为 ID_{V_i} 的接收车辆接收的环签密 σ 的解签密询问后, C_1 检查: ①车辆 V_i 的 $ID_{V_i} \in R$ 成立; ② ID_{V_i} 在列表 L_1 中; ③有一个元组 $(ID_{V_i}, Q_i, \lambda_i)$ 存在。当以上 3 个条件有 1 个不满足时, C_1 挑战失败; 否则, C_1 执行解签密算法步骤, 并将解签密结果返回给 A_I 。

(3)挑战

A_I 通过与 C_1 进行的模拟游戏获得两个等长的随机消息 m_0 和 m_1 。 C_1 选择一个比特 $\delta \in_R \{0, 1\}$, 执行签密算法得到消息 m_δ 的挑战密文 σ^* , 并将 σ^* 发送给 A_I 。收到密文 σ^* 后, A_I 与 C_1 重复上述模拟询问, 但 A_I 不能对 σ^* 进行解签密询问, 同时不能对 ID_{V_r} 的私钥进行部分私钥询问和秘密值询问。

(4)猜想

模拟游戏完成后, A_I 返回其猜想比特 δ^* 。由于密文 σ^* 的随机分布性以及 A_I 无法通过 σ^* 进行解签密询问, 因此 A_I 发现 σ^* 不是一个有效密文。然后, A_I 通过计算 $w = e(U^*, SK_{V_r})$ 对 $H_2(w)$ 询问, 其中, SK_{V_r} 是密文接收车辆的私钥。 C_1 选择随机数 $c \in_R Z_q^*$ 计算 $U^* = cP$, 因此有:

$$\begin{aligned} w &= e(U^*, SK_{V_r}) = e(cP, x_r \cdot \text{psk}_{V_r}) \\ &= e(cP, x_r \cdot a \cdot Q_r) = e(cP, x_r \cdot abP) \\ &= e(P, P)^{x_r abc} \end{aligned} \quad (26)$$

$$e(P, P)^{abc} = w^{1/x_r} \quad (27)$$

查找 L_{PK} , C_1 可以获得 x_r 的值, 因此 C_1 成功解决了 DBDH 问题。

假设敌手 A_I 进行了 $q_1 - q_4$ 次哈希询问, q_{psk} 次部分私钥

询问, q_{rpk} 次公钥替换询问, q_s 次环签密询问和 q_u 次解签密询问。假设敌手 A_1 可以在多项式时间 t 内完成全部询问后以不可忽略的概率 ϵ 区分密文, 则存在一个有效算法能以不可忽略的概率 ϵ' 解决 DBDH 问题。

C_1 成功解决 DBDH 问题的概率等价于以下 3 个事件同时发生的概率。

E_1 : C_1 在部分私钥询问和公钥替换询问阶段未被终止,

$$P(E_1) = \left(1 - \frac{q_{psk}}{q_1}\right) \left(1 - \frac{q_{rpk}}{q_1}\right);$$

E_2 : C_1 在对环签密 σ 的解签密阶段未被终止, $P(E_2 | E_1) =$

$$\frac{q_u}{q_1 - q_{psk} - q_{rpk}};$$

E_3 : C_1 在挑战阶段未被终止, $P(E_3 | E_1 E_2) = \epsilon \frac{q_s}{q_1}$ 。

因此,

$$\begin{aligned} \epsilon' &= P(E_1 E_2 E_3) \\ &= P(E_1) P(E_2 | E_1) P(E_3 | E_1 E_2) \\ &= \left(1 - \frac{q_{psk}}{q_1}\right) \left(1 - \frac{q_{rpk}}{q_1}\right) \cdot \frac{q_u}{q_1 - q_{psk} - q_{rpk}} \cdot \epsilon \frac{q_s}{q_1} \\ &\ll \epsilon \frac{q_s}{q_1} \end{aligned}$$

通过证明发现, 若假设敌手 A_1 能以不可忽略的概率区分密文, 则挑战者 C_1 解决 DBDH 问题的概率是可以忽略的, 与假设矛盾, 所以假设不成立。因此本文的 CLRS 方案具有机密性。

定理 2 在随机预言模型和 DBDH 复杂性假设下, 面对第 2 种类型敌手 A_{1I} 的适应性选择密文攻击, CLRS 方案具有机密性 (IND-CLRSC-CCA2) (证明过程与定理 1 类似, 不做赘述)。

综上所述, 本文的可认证 CLRS 方案具有适应性选择密文攻击下的机密性。

4.2.5 不可伪造性

定理 3 在随机预言模型和 CDH 计算 Diffie-Hellman 复杂性假设下, 面对第 1 种类型敌手 A_1 的适应性选择消息攻击, 本文的 CLRS 方案的存在性不可伪造 (EUF-CLRSC-CMA2)。

证明:

在 CDH 复杂性假设下, 给定一个元组 (P, aP, bP) , 挑战者 C_1 的挑战目标是利用 A_1 计算 abP 。设 H_1, H_2, H_3, H_4 是随机预言机, C_1 对 A_1 发起的询问作出如下回答。

(1) 系统建立: 与定理 1 相同。

(2) 询问: A_1 向挑战者 C_1 发起询问, C_1 作出回答。这里只对 H_1 询问 (不同于定理 1) 做详述, 其余询问参考定理 1。

1) H_1 询问。 C_1 维护列表 $L_1' = (ID_{V_i}, Q_i, \lambda_i)$, 列表初始为空。输入车辆身份 ID_{V_i} , C_1 查找 L_1' , 若该车辆身份 $ID_{V_i} \notin R$, 即该车辆不在环 R 中, 则 C_1 选择 $\lambda_i \in_R Z_q^*$, 计算 $Q_i = \lambda_i P$; 若 $ID_{V_i} \in R$, 则 C_1 计算 $Q_i = bP$, 最后返回 Q_i 。

(3) 伪造

A_1 输出一个由环 R 中某个签密车辆 V_s 发送给环外接收车辆 V_r 的消息明文 m^* 对应的伪造环签密 $\sigma^* = (c^*, U^*, R, R_1^*, \dots, R_n^*, T^*, T_1^*, \dots, T_n^*, TK_1^*, \dots, TK_n^*, Z^*)$ 。 C_1 查找列表 L_1' 中 ID_{V_r} 对应的元组 $(ID_{V_r}, Q_r, \lambda_r)$, 并利用 V_r 的私钥

SK_{V_r} 执行解签密算法。假设 σ^* 是一个由环中签密车辆 V_s 发送给接收车辆 V_r 的有效环签密, 则解签密算法执行完成后返回消息 m^* 。然后, C_1 应用分叉定理^[25]和预言重放技术, 生成消息 m^* 对应的两个有效环签密, 分别为 $\sigma' = (c', U', R, R_1', \dots, R_n', T', T_1', \dots, T_n', TK_1', \dots, TK_n', Z')$ 和 $\sigma'' = (c'', U'', R, R_1'', \dots, R_n'', T'', T_1'', \dots, T_n'', TK_1'', \dots, TK_n'', Z'')$, 即在不同哈希值下使用相同的随机磁带并重复运行图灵机, 从而得到 σ' 和 σ'' 。 C_1 对 σ' 和 σ'' 分别执行解签密算法, 可得到:

$$Z' = (x_r + h_{r'}) \cdot SK_{V_r} \quad (28)$$

$$Z'' = (x_r + h_{r''}) \cdot SK_{V_r} \quad (29)$$

其中, $h_{r'} \neq h_{r''}$ 。最后, 将签密车辆 V_s 的身份 ID_{V_s} 和消息明文 m 合并为伪造消息对 (ID_{V_s}, m) 。 A_1 返回两个有效签名 Z' 和 Z'' 。 C_1 计算:

$$\begin{aligned} (Z' - Z'')(h_{r'} - h_{r''})^{-1} &= (h_{r'} - h_{r''}) \cdot SK_{V_s} (h_{r'} - h_{r''})^{-1} \\ &= SK_{V_s} = x_r \cdot abP \end{aligned} \quad (30)$$

因此:

$$abP = \frac{1}{x_r} (Z' - Z'')(h_{r'} - h_{r''})^{-1} \quad (31)$$

C_1 成功解决了 CDH 问题。

假设敌手 A_1 进行了 $q_1 - q_4$ 次哈希询问, q_{psk} 次部分私钥询问, q_{rpk} 次公钥替换询问, q_s 次环签密询问和 q_u 次解签密询问。假设敌手 A_1 可以在多项式时间 t 内完成全部询问后以不可忽略的概率 ϵ 伪造签密, 则存在一个有效算法能以不可忽略的概率 ϵ' 解决 CDH 问题。

C_1 成功解决 CDH 问题的概率等价于以下 3 个事件同时发生的概率。

E_1 : C_1 在部分私钥询问和公钥替换询问阶段未被终止,

$$P(E_1) = \left(1 - \frac{q_{psk}}{q_1}\right) \left(1 - \frac{q_{rpk}}{q_1}\right);$$

E_2 : C_1 在对环签密 σ 的解签密阶段未被终止, $P(E_2 | E_1) =$

$$\frac{q_u}{q_1 - q_{psk} - q_{rpk}};$$

E_3 : C_1 成功伪造两个环签密, $P(E_3 | E_1 E_2) = \epsilon \frac{1}{9}$ 。

因此,

$$\begin{aligned} \epsilon' &= P(E_1 E_2 E_3) \\ &= P(E_1) P(E_2 | E_1) P(E_3 | E_1 E_2) \\ &= \left(1 - \frac{q_{psk}}{q_1}\right) \left(1 - \frac{q_{rpk}}{q_1}\right) \cdot \frac{q_u}{q_1 - q_{psk} - q_{rpk}} \cdot \epsilon \frac{1}{9} \ll \epsilon \frac{1}{9} \end{aligned}$$

经上述证明, 若假设敌手 A_1 能以不可忽略的概率伪造一个 CLRS 方案, 则挑战者 C_1 解决 CDH 问题的概率是可以忽略的, 与假设矛盾, 所以假设不成立。因此本文的 CLRS 方案的存在性不可伪造。

定理 4 在随机预言模型和 CDH 复杂性假设下, 面对第 2 种类型敌手 A_{II} 的适应性选择消息攻击, 本文 CLRS 方案的存在性不可伪造 (EUF-CLRSC-CMA2) (证明过程与定理 3 类似, 不做赘述)。

综上所述, 本文的可认证 CLRS 方案在适应性选择消息攻击下的存在性不可伪造。

通过上述安全性的分析, 表 1 列出了现有隐私保护方案和本文提出的方案的安全性能。对比可知, 本文方案的安全性能较好, 不仅消息传递过程安全可靠, 也保证了对恶意车辆节点的身份可追踪性。

表1 不同方案安全性能的对比

Table 1 Comparison of security performance of different schemes

	文献[29]	文献[30]	本文方案
匿名性	✓	✓	✓
机密性			✓
隐私性	✓	✓	✓
不可伪造性	✓	✓	✓
可认证性			✓
可追踪性	✓		✓

4.3 计算效率分析

本文选择计算开销作为不同方案下计算效率的参照。表2和表3分别列举了本文方案和其他3种CLRS方案中环签密算法、解签密算法的各项计算量,又因为各方案哈希运算和异或运算的数量相近且一次运算的时间足够小(相差3个数量级),因此在仿真比较时只考虑各方案中双线性运算和标量乘运算的计算开销,如表4所列。其中, P_B 表示一个双线性运算, S_m 表示一个标量乘运算, n 表示车辆用户数量。本文选用Intel I7、3.07GHz的硬件平台。通过实验结果可知:一个标量乘法运算 S_m 需要0.40ms,一个双线性运算 P_B 需要3.21ms。通过Matlab仿真实验对这3个CLAS方案和本文提出的可认证CLRS方案的计算开销进行对比,结果如图5所示。可以看出,本文所提方案的计算开销在4个方案中最少,且随着网络中车辆节点数的增加,所提方案的优越性逐渐提升,效率较高,因此本文方案尤其适用于车辆数量较大的城市交通系统。

表2 环签密算法的计算量

Table 2 Computational complexity of ring signcryption algorithms

运算类型	文献[26]	文献[27]	文献[28]	本文方案
双线性运算	$n+2$	$2n$	$2n$	1
哈希运算	$n+3$	$n+3$	$n+3$	$n+1$
XOR运算	3	2	3	1
标量乘运算	$2n+1$	$n+1$	$2n+1$	$2n+1$

表3 解签密算法的计算量

Table 3 Computational complexity of ring designcryption algorithms

运算类型	文献[26]	文献[27]	文献[28]	本文方案
双线性运算	4	$n+4$	4	5
哈希运算	$n+2$	$n+2$	$n+2$	$n+1$
XOR运算	3	2	3	1
标量乘运算	$2n-1$	$2n$	$2n$	n

表4 各CLRS方案的计算开销

Table 4 Computational overhead of different CLRS schemes

方案	计算开销
文献[26]	$(n+6)P_B+4nS_m$
文献[27]	$(3n+4)P_B+(3n+1)S_m$
文献[28]	$(2n+4)P_B+(4n+1)S_m$
本文方案	$6P_B+(3n+1)S_m$

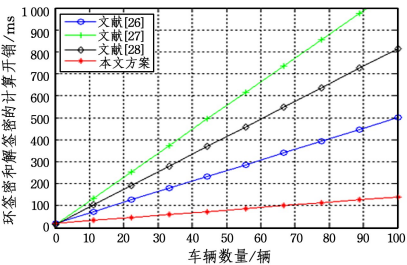


图5 不同CLRS方案计算开销的比较

Fig. 5 Comparison of computational overhead of different CLRS schemes

本文提出的CLRS方案一般应用在十字路口或某一段道路上一定数量的车辆之间的加密通信,对于超出限定范围的车辆来说,该加密消息不再具备实时性价值,因此,环 R 中的车辆数量 n 基本保持在60~80(一般不超过100)。从图5来看,当环中车辆数 $n=100$ 时,本文方案的计算开销不到150ms,符合即时通信的要求。另外,只有需要对签密车辆进行身份追踪时,才需要环中所有车辆与密文接收车辆协作,但这种情况发生频率不高,因此对本文方案的效率影响不大,这里不作考虑。

结束语 本文将公钥密码体制中的加密模型和认证模型组合,并结合环签密构建了一个新的可认证环签密算法模型,然后在此基础上提出了一个保护车载自组织网络中车辆用户隐私和通信安全的可认证无证书环签密方案。车辆节点使用在TMC注册的伪身份与其他节点和路边单元通信,环中其他车辆和密文接收车辆都无法确定密文发送车辆的身份,交管部门在车辆违规时还可以通过追踪密钥找出恶意车辆的真实身份,因此该方案满足了匿名性和可追踪性要求;签密和解密算法基于所提出的可认证环签密算法模型执行,实现了对通信消息来源完整性的可认证;另外,基于随机预言模型证明了本文的CLRS方案具有机密性且其存在性不可伪造。最后,通过仿真实验可知,本文方案总体的计算开销较低,在适用范围内符合即时通信的要求,能较好地适用于车流量较大的城市道路。

如何管理不同TMC管辖区域的车辆节点跨区域加入网络通信并对其进行有效的隐私保护是下一步的研究方向。

参考文献

[1] ZHONG H, HAN S S, CYI J, et al. Privacy-Preserving Authentication Scheme with Full Aggregation in VANET[J]. Information Sciences, 2019, 476: 211-221.

[2] JAEDUCK C, SOUHWAN J. Unified Security Architecture and Protocols Using Third Party Identity in V2V and V2I Networks [J]. Wireless Communications and Mobile Computing, 2012, 12(15): 1326-1337.

[3] YANG L. Big Data Technology and Its Analysis of Application in Urban Intelligent Transportation System[C]// 2018 International Conference on Intelligent Transportation, Big Data & Smart City (ICITBS). Xiamen: IEEE Press, 2018: 17-19.

[4] SHAMIR A. Identity-Based Cryptosystems and Signature Schemes[M]. Advances in Cryptology. Berlin: Springer, 1984: 47-53.

[5] ZHANG J. A Hybrid Authentication Protocol with ID-Based Signcryption for Vehicular Ad Hoc Networks[J]. Advanced Materials Research, 2013, 650: 465-469.

[6] VIJAYALAKSHMI N, SASIKUMAR R. An ID-Based Privacy Preservation for VANET [C] // International Conference on Computing & Communications Technologies. Chennai, IEEE Press, 2015: 164-167.

[7] XIE Y, WU L B, ZHANG Y B, et al. Efficient and Secure Authentication Scheme With Conditional Privacy-Preserving for VANETs[J]. Chinese Journal of Electronics, 2016, 25(5): 950-956.

[8] VIJAYAKUMAR P, AZESS M, KANNAN A, et al. Dual Au-

- thentication and Key Management Techniques for Secure Data Transmission in Vehicular Ad Hoc Networks[J]. IEEE Transactions on Intelligent Transportation Systems, 2016, 17(4): 1015-1028.
- [9] ALRIYAMI S S, PATERSON K G. Certificateless Public Key Cryptography[C]//Cryptology-ASIACRYPT. 2003:452-473.
- [10] WANG D X, TENG J K. Probably Secure Certificateless Aggregate Signature Algorithm for Vehicular Ad hoc Network[J]. Journal of Electronics & Information Technology, 2018, 40(1): 11-17.
- [11] YANG X D, YANG P, LI Y, et al. A Message Authentication Scheme for VANET Based on Certificateless Proxy Re-signature[J]. Computer Engineering & Science, 2018, 40(1): 40-44.
- [12] BARBOSA M, FARSHIM P. Certificateless Signcryption[C]//Proceedings of the 2008 ACM Symposium on Information, Computer and Communications Security. Tokyo: ACM, 2008(3): 18-20.
- [13] HOU C X. Certificateless Signcryption Scheme Without Random Oracles[J]. Chinese Journal of Electronics, 2018, 27(5): 1002-1008.
- [14] ZHANG Y J, ZHANG Y L, WANG C F. Certificateless Aggregate Signcryption Scheme with Internal Security and Const Pairings[J]. Journal of Electronics & Information Technology, 2018, 40(2): 500-508.
- [15] YU H F, YANG B. Low-computation Certificateless Hybrid Signcryption Scheme[J]. Frontiers of Information Technology & Electronic Engineering, 2017, 18(7): 928-941.
- [16] CUI J L, SUN H. An Efficient Certificateless Threshold Signcryption Scheme[J]. Journal of Xinyang University (Natural Science Edition), 2016, 29(2): 283-288.
- [17] ZHA W G. Certificateless Agent Signcryption Scheme without Bilinear Pairing[J]. Journal of East China Jiaotong University, 2015, 32(4): 110-116.
- [18] YU H F. Certificateless Proxy Signcryption Using Cyclic Multiplication Groups[C]//2018 14th International Conference on Computational Intelligence and Security (CIS). Hangzhou: IEEE Press, 2018: 426-429.
- [19] JIANG Z X. Design and Analyses of Certificateless Proxy Ring Signcryption Scheme[D]. Guangxi: Guangxi University, 2015.
- [20] SUN H, MENG K. Efficient Certificateless Ring Signcryption Scheme[J]. Computer Science, 2014, 41(11): 208-211, 238.
- [21] ZHU L J, ZHANG F T, MIAO S Q. A Provably Secure Parallel Certificateless Ring Signcryption Scheme[C]//International Conference on Multimedia Information Networking & Security. Nanjing: IEEE Press, 2010: 423-427.
- [22] HUANG Y Y, ZHANG J G, CHEN H Y. On the Security of ACertificateless Signcryption Scheme[C]//2014 IEEE Workshop on Electronics, Computer and Applications. Ottawa: IEEE Press, 2014: 664-667.
- [23] SHARMA G, BALA S, VERMA A K. An Identity-Based Ring Signcryption Scheme[C]//IT Convergence & Security. Lecture Notes in Electrical Engineering; Springer, Dordrecht, 2012: 151-157.
- [24] HONG D Z, XIE Q. Certificateless Ring Signcryption Scheme[J]. Computer Engineering and Application, 2011, 47(17): 107-110.
- [25] HERRANZ J, SAEZ G. Forking Lemmas for Ring Signature Schemes[J]. Journal of Management Studies, 2003, 2904(2): 266-279.
- [26] WANG L L, ZHANG G Y, MA C G. Verifiable Certificateless Ring Signcryption Scheme Based on Bilinear Pairings[J]. Computer Applications, 2007, 27(9): 2167-2169.
- [27] HOU H X, HE Y F. A New Certificateless Ring Signcryption Scheme[J]. Computer Technology and Development, 2012, 22(7): 151-153.
- [28] WANG L L, ZHANG G Y, MA C G. A Secure Ring Signcryption Scheme for Private and Anonymous Communication[C]//IFIP International Conference on Network & Parallel Computing Workshops. Liaoning: IEEE Computer Society, 2007: 107-111.
- [29] CUI Y Q, CAOL, ZHANGX Y, et al. Ring Signature Based on Lattice and VANET Privacy Preservation[J]. Journal of Computers, 2017, 40(169): 1-14.
- [30] 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 [C]//Advanced Big Data Analysis for Vehicular Social Networks. IEEE Access, 2018: 20209-20220.



ZHAO Nan, born in 1995, postgraduate. Her main research interests include data and communications security, privacy-protection of vehicular ad hoc network.



ZHANG Guo-an, born in 1965, Ph. D., professor, Ph. D supervisor. His main research interests include vehicular ad hoc network and wireless communication network theory and technology.