DOI:10.19322/j.cnki.issn.1006-4710.2023.03.012 https://xuebao.xaut.edu.cn
引文格式:和斌涛,王尚平,刘丽华. VANETs中基于环签密和非交互式零知识证明的条件隐私保护方案[J]. 西安理工大学学报,2023,39(3):412-422.
HE Bintao, WANG Shangping, LIU Lihua. Conditional privacy protection scheme based on ring signcryption and non-interactive zero-knowledge proof in VANETs[J]. Journal of Xi'an University of Technology, 2023, 39(3): 412-422.

VANETs中基于环签密和非交互式零知识证明的条件隐私保护方案

和斌涛[1,2], 王尚平[1], 刘丽华[2]
(1. 西安理工大学 自动化与信息工程学院, 陕西 西安 710048;
2. 陕西理工大学 数学与计算机科学学院, 陕西 汉中 723001)

摘要: 针对车载自组织网络(VANETs)中现有环签名方案易陷入单点失败和追踪非法用户真实身份困难问题,提出了一种基于环签密和非交互式零知识证明的条件隐私保护方案。选用环签密方法来同时实现匿名认证和传递消息加密,采用分布式门限密钥生成方法来防止单点失败问题,利用非交互式零知识证明技术在环签密中增加追踪标签,使监管权威在必要时可以快速追踪用户的真实身份,实现了条件隐私保护的目标。与现有的几种环签密方案相比,本方案可以同时实现匿名性、机密性、可认证性、去中心化、防伪造性、不可链接性、可追踪性等安全性能。随着环成员数的增大,本方案在通信开销和计算开销两方面都表现出明显优势。

关键词: 环签密; 非交互式零知识证明; 条件隐私保护; 车载自组织网络; 可追踪性
中图分类号: TP309 **文献标志码**: A **文章编号**: 1006-4710(2023)03-0412-11

Conditional privacy protection scheme based on ring signcryption and non-interactive zero-knowledge proof in VANETs

HE Bintao[1,2], WANG Shangping[1], LIU Lihua[2]
(1. Faculty of Automation and Information Engineering, Xi'an University of Technology, Xi'an 710054, China;
2. School of Mathematics and Computer Science, Shaanxi University of Technology, Hanzhong 723001, China)

Abstract: In order to solve the problem that existing ring signature schemes in Vehicle Ad Hoc Networks (VANETs) are prone to fall into the single-point failure and difficult to trace the real identity of illegal users, a conditional privacy protection scheme based on the ring signcryption and non-interactive zero-knowledge proof is proposed. The ring signcryption method is used to realize anonymous authentication and message encryption at the same time. The distributed threshold key generation method is used to prevent the single-point failure problem, and the non-interactive zero-knowledge proof technology to add the tracking label in the ring signcryption, so that the trace authority can quickly track the real identity of the user when necessary, and can achieve the goal of conditional privacy protection. Compared with several existing ring signcryption schemes, this scheme can achieve anonymity, confidentiality, authentication, decentralization, anti-

收稿日期: 2022-09-19; **网络首发日期**: 2022-10-18
网络首发地址: https://kns.cnki.net/kcms/detail/61.1294.N.20221018.1604.004.html
基金项目: 国家自然科学基金资助项目(61572019);陕西省科技计划项目(2022GY-040)
第一作者: 和斌涛,男,博士生,讲师,研究方向为信息安全、网络安全。E-mail: hebintao@163.com
通信作者: 王尚平,男,博士,教授,博导,研究方向为信息安全、密码学。E-mail: spwang@mail.xaut.edu.cn

counterfeiting, unlinkability, traceability and so on simultaneously. With the increase of the number of ring members, the proposed scheme has obvious advantages in both communication overhead and computation cost.

Key words: ring signcryption; non-interactive zero-knowledge proof; conditional privacy protection; Vehicle Ad Hoc Networks; traceability

车载自组织网络(VANETs)是智能交通系统的重要组成部分。在 VANETs 中,每辆车都配备了车载单元(OBU),OBU 之间可以通过 V2V 模式进行通信交互,OBU 也可以与路边单元(RSU)等其他基础设施进行 V2I 模式通信交互[1-2]。VANETs 在给我们带来便利的同时也由于其支持无线通信而更容易遭受攻击,攻击者可以拦截、窃听、篡改通信消息,发布虚假信息,甚至泄露用户的身份隐私信息,危害驾驶人员安全。因此,在 VANETs 中设计安全高效的隐私保护方案非常重要。VANETs 中通常有四种隐私保护方法:基于证书的隐私保护方案[3]、基于群签名的隐私保护方案[4]、基于假名的隐私保护方案[5]、基于环签名的隐私保护方案[6-7]。

与证书方案相比,环签名方案不需要证书权威,无需存储大量的证书;与基于群签名的隐私保护方案相比,环签名成员地位平等,不需要管理员;虽然基于假名的隐私保护方案在单次使用时比较方便,但是假名的生成、更新和撤销过程都需要与可信中心进行大量的通信交互,大大增加了各方的存储和通信负担[8-9]。

由于环签名具有灵活性、自发性、匿名性和成员身份平等的优点,利用环签名可以在 VANETs 中设计出实用性较强的隐私保护方案[10]。环签名方案本身只能保护通信双方的身份隐私,并不能保证所传递信息的机密性,而环签密技术可以将环签名和加密功能集成到一起,在保护通信双方身份隐私的同时保证信息传递的机密性,只有信息接收者才有权对传递信息进行解密,环签密使得 VANETs 中的通信安全得到加强[11-12]。然而,环签密在保护合法用户身份隐私的同时,也给攻击者留下了可乘之机,由于所有成员的身份都是完全匿名的,即使敌手发送虚假或者非法信息也不会得到惩罚。为了杜绝这种完全匿名性所带来的安全隐患,赋予监管权威在必要时追踪用户真实身份的权利是非常必要的。条件隐私保护方案可以保证合法用户的身份隐私,必要时追踪非法用户的真实身份,同时实现匿名认证和可追踪特性[13-15]。

一般的环签密方案并不具有追踪功能,不能实现条件隐私保护,一些文献通过在环签密中增加追踪标签来实现对非法签密者真实身份的追踪。赵楠等[16]在 VANETs 中设计了基于环签密的可认证隐私保护方案,通过在环签密中加入追踪标签可以实现条件隐私保护,但其追踪标签和环成员数相关,随着环成员数的增加,追踪标签将大大增加环签密的通信开销和计算开销,而且追踪非法签密者真实身份的过程需要所有参与环签名成员进行诚实交互和计算,方案的实用性不强。2020 年,Cai 等[17]也利用环签密在 VANETs 中设计了条件隐私保护方案,在追踪时采用遍历算法对所有环成员的公钥进行排查,当环成员数较多时,需要付出较大的计算和通信开销。非交互式零知识证明可以在不泄露某个秘密值的情况下,无需多次交互就可以使验证者相信证明者掌握该秘密。文献[18]利用非交互式零知识证明来保证交易的有效性,大大提高了交易验证的效率。文献[19]利用非交互式零知识证明设计了可审计的隐私保护方案,减少了交易双方的通信开销。文献[20]利用非交互式零知识证明保证了自主生成假名过程的合法性。

区块链具有公开透明、防窜改、分布式等良好特性,区块链技术是实现去中心化的有力工具。2021 年,Tang 等[21]在智能电网中提出了基于区块链的多授权可追溯环签名方案,设计了多中心的分布式密钥生成方案,但该环签名未考虑对明文消息的加密,不满足传递信息的机密性。2022 年,黄丹[22]将区块链与环签密结合构造了电子证据认证方案,利用区块链设计了多中心的环签密方案,但该方案的密钥生成需要所有弱中心的同时参与,缺乏灵活性。沈华杰[23]用路边单元联盟维护的联盟区块链取代中心化的证书生成中心,采用了门限密钥生成方式,使得密钥生成过程更加灵活。

分析 VANETs 中现有的环签名方案不难发现,大部分环签名方案都需要完全可信的密钥生成中心,容易陷入单点失败问题。现有的环签名方案为了实现追踪功能,需要付出较多的通信开销和计算开销。为解决上述问题,基于文献[20]和[23],本文在 VANETs 中构造一个基于环签密和非交互式零知识证明的条件隐私保护方案。主要创新如下:

1) 针对现有环签名方案中心化的密钥生成方式容易陷入单点失败的问题,本文设计了联盟区块

链,用来记录和发布公钥及各种公开参数,由路边单元联盟为车载单元生成多个私钥份额,车载单元利用门限机制自行合成系统可验证的私钥,使得密钥生成过程更加安全和灵活。

2) 针对现有环签密方案中实现追踪功能所需的通信和计算开销较大的问题,本文首次将非交互式零知识证明和环签密相结合,利用非交互式零知识证明来生成追踪标签,只需较小的通信和计算开销即可实现对非法签密者真实身份的追踪。

3) 分析了所提方案的正确性、安全性以及通信和计算开销,并与相关方案进行比较。分析结果表明,所提方案比同类环签密方案安全性更好,由于引入了非交互式零知识证明,使得本方案在追踪上更加高效,和其他支持条件隐私保护的环签密方案相比,本方案在通信开销和计算开销两方面都具有优势。

1 预备知识

1.1 双线性映射

设 G_1,G_2 是两个阶为 q 的循环群,P 为群 G_1 的生成元,定义双线性映射 $e:G_1\times G_1\rightarrow G_2$ 满足如下性质:

1) 双线性:$\forall a,b\in Z_q^*$,$\forall P_1,P_2\in G_1$,有 $e(aP_1,bP_2)=e(bP_1,aP_2)=e(P_1,P_2)^{ab}$。

2) 非退化性:$\exists P_1,P_2\in G_1$,使得 $e(P_1,P_2)\neq 1_{G_2}$。

3) 可计算性:$\forall P_1,P_2\in G_1$,存在有效算法来计算 $e(P_1,P_2)$。

1.2 困难问题假设

定义 1 离散对数(DL)假设:给定元素 $P,Q\in G_1$,求整数 $a\in Z_q^*$,使 $a\cdot P=Q$ 是困难的。

定义 2 计算双线性 Diffie-Hellman(BDH)假设:已知 P、aP、bP、$cP\in G_1$,a、b、$c\in Z_q^*$,计算 $e(P,P)^{abc}$ 是困难的。

1.3 非交互式零知识证明

在零知识证明中,证明者 P 向验证者 V 证明其知道秘密 w 这一陈述,除了证明该陈述是真的之外,不会向验证者 V 透露任何关于 w 的内容。应用 Fiat-Shamir 非交互式零知识证明[24],证明者 P 可以通过给验证者 V 发送一个证明信息,不需多次交互就可以完成证明过程。

证明者选用与哈希(Hash)函数近似的模拟随机预言机,如图 1 所示,证明者 P 保持秘密 w,公开 $W=w\cdot P$,随机选择 r,生成承诺值 $com=r\cdot P$,计算 com 和 W 的哈希值 $c=hash(com,W)$,计算证据 $\pi=r+c\cdot w$,然后证明者 P 发送 c、π 给验证者 V,验证者 V 重新计算 $com_1=\pi\cdot P-c\cdot W$,$c_1=hash(com_1,W)$,判断 $c_1=c$ 是否成立。如果成立,则验证者 V 接受证明者 P 知道秘密 w 这一陈述。该非交互式零知识证明可以记作:$NIZK\{(w):W=w\cdot P\}$。

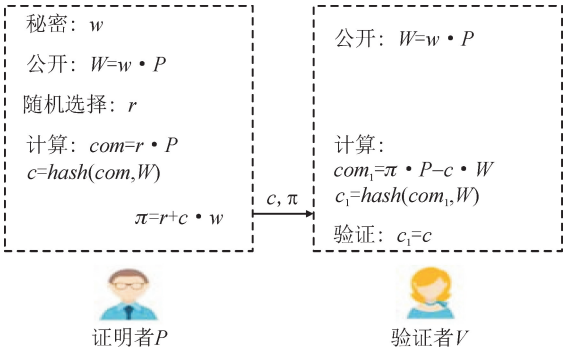

图 1 非交互式零知识证明

Fig. 1 Non-interactive zero-knowledge proof

2 系统模型

2.1 系统模型介绍

如图 2 所示,本方案主要包括 4 个实体:路边单元(RSU)、联盟区块链、车载单元(OBU)和监管权威(TRA)。

1) 路边单元(road side unit, RSU):RSU 是半可信的基础设施,安装在道路两侧,RSU 具有足够的处理性能、存储空间和良好的网络连接,RSU 之间通过无线通信的方式共同维护区块链。

2) 车载单元(on board unit, OBU):网络中的每辆车都配备了可与其他设备进行交互的车载单元,车载单元需要向系统进行注册,两个车载单元可以通过 V2V 的通信模式进行交互,或者与路边单元等其他基础设施进行 V2I 模式的通信。

3) 联盟区块链:本方案为了实现去中心化的目标,由 k 个 RSU 来初始化联盟区块链,共同商定系统参数设置,k 个 RSU 将自己的公钥和联合生成的系统公钥作为系统公共参数在区块链公开,监管权威的监管公钥也发布在区块链中,车载单元的真实身份信息和公钥之间的绑定关系也记录在联盟区块链中。

4) 监管权威(trace authority, TRA):监管权威负责监督路边单元联盟进行系统建立和维护。本文假定监管权威完全可信,监管权威不参与车载单元的注册、密钥生成及环签密过程,只有在必要时,监管权威才会对涉嫌非法签密者的真实身份进行追踪。

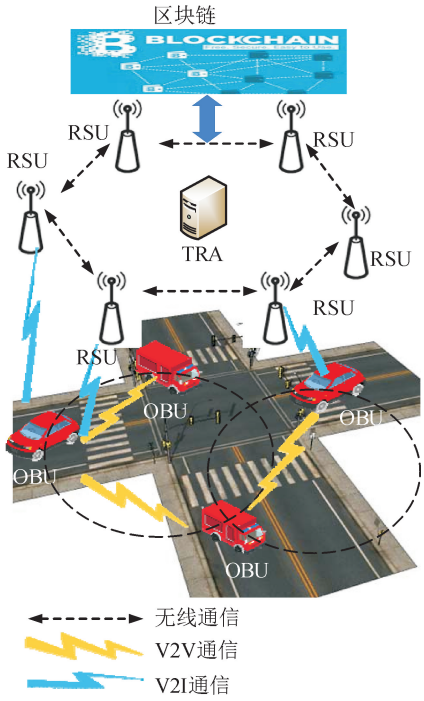

图 2 环签密系统模型

Fig. 2 System model of ring signcryption

2.2 系统安全性目标

1）匿名性：在正常通信情况下，消息发送者和消息接收者的真实身份都保持匿名，只有在必要时消息发送者的真实身份才能被追踪到。

2）机密性：通信双方以密文形式进行通信，只有消息接收者才有权对传递信息进行正确解密。

3）可认证性：系统成员身份的合法性、签密者追踪标签生成的正确性、传递消息的完整性、环签密的正确性都可认证。

4）去中心化：系统不需要密钥生成中心，由 k 个 RSU 共同确定系统的主密钥，OBU 私钥的第一项也是由 OBU 通过门限机制自行合成的。

5）防伪造性：敌手不能伪造 OBU 的身份进行通信，也不能伪造环签密来通过接收者的验证。

6）不可链接性：敌手不能从消息发送者的多次签密链接到同一签密者。

7）可追踪性：执法权威 TRA 在必要时有权追踪到涉嫌非法行为签密者的真实身份。

3 方案描述

3.1 系统建立

在监管权威 TRA 的监管下，设由 k 个路边单元 RSU 进行联盟区块链的初始化。设 G_1 为 q 阶的循环加法群，G_2 为同阶循环乘法群，P 为 G_1 的生成元，设双线性映射 $e:G_1\times G_1\rightarrow G_2$。选取 5 个安全的哈希函数分别为：$H_0:\{0,1\}^*\times G_1\rightarrow G_1$，$H_1:\{0,1\}^l\times G_1\times\{0,1\}^*\times G_1\times G_1\rightarrow Z_q^*$，$H_2:G_2\rightarrow\{0,1\}^*$，$H_3:\{0,1\}^*\times G_1\rightarrow\{0,1\}^l$，$H_4:G_1\times G_1\times G_1\times G_1\rightarrow\{0,1\}^*$。设监管权威 TRA 的私钥为 $tsk=v$，监管公钥为 $tpk=v\cdot P$，路边单元集合为 $\{RSU_1,RSU_2,\cdots,RSU_k\}$，第 i 个路边单元 RSU_i 的身份信息为 $SID_i\in\{0,1\}^*$。设 $RSU_i(i=1,2,\cdots,k)$ 随机选取 Z_q^* 上的秘密 S_i，并选择 Z_q^* 上 t 阶多项式 $f_i(x)$，令 $S_i=f_i(0)$，RSU_i 为其他 $k-1$ 个路边单元计算子密钥份额 $s_{i,j}=f_i(UID_j)$，并通过秘密通道发送 $s_{i,j}$ 给其他 RSU_j，RSU_i 自己计算并保留 $s_{i,i}=f_i(UID_i)$。当 RSU_i 收到来自其他 $k-1$ 个 RSU_j 发送的子密钥份额后，可以计算自己的私钥 $rsk_i=s_i=\sum_{j=1}^{k}s_{j,i}$，对应公钥为 $rpk_i=s_i\cdot P$。根据 Pedersen (t,k) 秘密共享方案[25]，至少需要 t 个 RSU 合作才能通过式(1)计算系统主密钥 sk：

$$sk=\sum_{i=1}^{t}\left(\prod_{j=1,j\neq i}^{t}\frac{SID_j}{SID_j-SID_i}\right)rsk_i \tag{1}$$

系统公钥可以通过式(2)计算：

$$pk=\sum_{i=1}^{t}\left(\prod_{j=1,j\neq i}^{t}\frac{SID_j}{SID_j-SID_i}\right)rpk_i \tag{2}$$

系统公钥 pk、监管公钥 tpk 和每个 RSU_i 的部分公钥 rpk_i 都作为公开参数公布到区块链中，则系统的公共参数为：$params=\{q,G_1,G_2,P,e,H_0,H_1,H_2,H_3,H_4,k,t,rpk_{i\{i=1,2,\cdots,k\}},pk,tpk\}$。

3.2 车载单元注册

每个车载单元 OBU_j 需要向 RSU 联盟进行注册以获得自己的公私钥对。

假定车载单元 OBU_j 的真实身份信息为 $UID_j\in\{0,1\}^*$，OBU_j 秘密选取 $w_j\in Z_q^*$，计算 $W_j=w_j\cdot P$，将 (UID_j,W_j) 发送给 RSU 联盟节点。每个 RSU_i 验证 OBU_j 提供的身份信息，且要求 (UID_j,W_j) 未在系统中使用过，这样就可确保 OBU_j 公钥的唯一性。若身份信息通过验证，RSU_i 将 (UID_j,W_j) 记录在区块链中，继续计算 $Q_j=H_0(UID_j,W_j)$，$psk_{i,j}=sk_i\cdot Q_j$，并通过安全通道发送 $(Q_j,psk_{i,j})$ 给 OBU_j。OBU_j 收到每个 RSU_i 返回的私钥份额后先验证式(3)：

$$e(psk_{i,j},P)=e(H_0(UID_j,W_j),rpk_i) \tag{3}$$

如果式(3)不成立，则要求 RSU_i 重新发送，如果式(3)成立，按照 Pedersen 秘密共享方案，当 OBU_j 收集到来自 RSU 联盟的 t 个私钥份额后，可以生成自己私钥的第一项：

$$usk_j=\sum_{i=1}^{t}\left(\prod_{j=1,j\neq i}^{t}\frac{SID_j}{SID_j-SID_i}\right)psk_{i,j}=sk\cdot Q_j \tag{4}$$

由此，OBU_j 的私钥为 (usk_j, w_j)，公钥为 (Q_j, W_j)。

3.3 环签密

设消息发送方 OBU_s 和消息接收方 OBU_r 的身份信息分别为 UID_s 和 UID_r。发送方 OBU_s 公钥为 (Q_s, W_s)，私钥为 (usk_s, w_s)，接收方 OBU_r 公钥为 (Q_r, W_r)，私钥为 (usk_r, w_r)。Q_s 和 usk_s 用于环签名的生成和验证；w_s、W_r 和 Q_r 用于对传递的明文消息 m 进行加密；W_s、usk_r 和 w_r 用于对环签名中的消息密文进行解密；W_s 加密后用于生成追踪标签；w_s 用于对 W_s 加密正确性的零知识证明。

环签密过程分为环签名准备、传递消息 m 加密、签密者的 W_s 加密、W_s 加密的零知识证明生成、完整环签密生成 5 个步骤。

1) 环签名准备

消息发送方 OBU_s 作为签密者选择公钥集合 $L=\{Q_1, Q_2, \cdots, Q_n\}$ 来进行环签名，$Q_s \in L$，设 OBU_s 发送消息 $m \in \{0,1\}^l$ 给接收者 OBU_r。OBU_s 首先随机选择 $r_0 \in Z_q^*$，计算 R_0：

$$R_0 = r_0 \cdot P \tag{5}$$

对任意的 $j \in \{1,2,\cdots,n\}$，若 $j \neq s$，OBU_s 随机选择 $r_j \in Z_q^*$，计算 U_j, h_j：

$$U_j = r_j \cdot P \tag{6}$$

$$h_j = H_1(m, U_j, L, R_0, Q_r) \tag{7}$$

若 $j=s$，OBU_s 选择 $\alpha \in Z_q^*$，计算 U_s、h_s 和 V：

$$U_s = \alpha \cdot Q_s - \sum_{j=1, j\neq s}^{n} (U_j + h_j \cdot Q_j) \tag{8}$$

$$h_s = H_1(m, U_s, L, R_0, Q_r) \tag{9}$$

$$V = (h_s + \alpha) usk_s \tag{10}$$

2) 传递消息 m 加密

为了保证传递消息的机密性，OBU_s 用自己的 w_s 和接收者的公钥 (Q_r, W_r)、系统公钥 pk 和参数 r_0 对明文消息 m 进行加密，得到明文消息 m 的密文 C。

$$R' = e(r_0 \cdot pk, Q_r) \tag{11}$$

$$b = H_2(R') \tag{12}$$

$$C = m \oplus H_3(b, w_s W_r) \tag{13}$$

3) 签密者的 W_s 加密

为了实现可追踪功能，OBU_s 需要对与其真实身份关联的 W_s 自觉进行加密，以便监管权威在必要时可以解密出 W_s，从而追踪到 OBU_s 的真实身份。为此，OBU_s 选择 $\rho \in Z_q^*$，选用 EL-Gamal 加密算法使用监管公钥 tpk 对 W_s 进行加密，得到 W_s 的密文 $C_s = (C_1, C_2)$，具体形式如下：

$$C_s = (\rho \cdot P, W_s + \rho \cdot tpk) \tag{14}$$

4) W_s 加密的零知识证明生成

为了向接收者证明 W_s 加密的真实性和正确性，OBU_s 采用非交互式零知识证明：$NIZK\{(w_s, \rho): C_1 = \rho \cdot P \wedge C_2 = W_s + \rho \cdot tpk\}$ 其中 $W_s = w_s \cdot P$。在不泄露 w_s 和 ρ 的情况下，OBU_s 向接收者证明确实选用了参数 ρ 和监管公钥 tpk 对 W_s 进行了正确加密，而且加密内容的确是和签密者 OBU_s 私钥中的 w_s 所对应的 W_s。该非交互式零知识证明过程如图 3 所示。

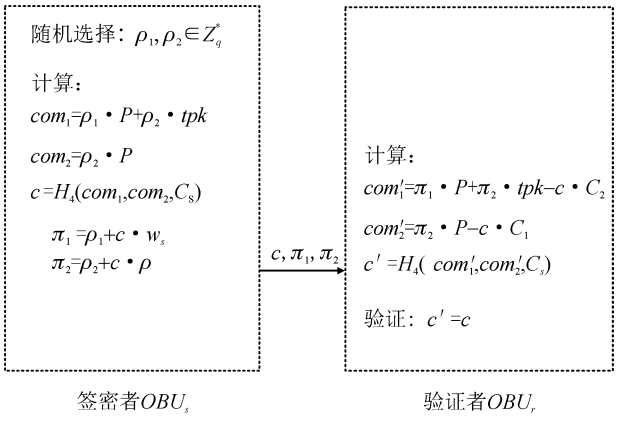

图 3 W_s 加密的非交互式零知识证明

Fig. 3 Non-interactive zero-knowledge proof of W_s encryption

签密者 OBU_s 作为非交互式零知识证明的证明人随机选择 $\rho_1, \rho_2 \in Z_q^*$，需要进行如下计算：

$$com_1 = \rho_1 \cdot P + \rho_2 \cdot tpk \tag{15}$$

$$com_2 = \rho_2 \cdot P \tag{16}$$

$$c = H_4(com_1, com_2, C_s) \tag{17}$$

$$\pi_1 = \rho_1 + c \cdot w_s \tag{18}$$

$$\pi_2 = \rho_2 + c \cdot \rho \tag{19}$$

式(18)可以向验证者证明签密者知道与 W_s 对应的私钥部分是 w_s，从而证明 EL-Gamal 加密的内容确实是 W_s。式(19)可以向验证者证明签密者知道 EL-Gamal 加密所选取的参数是 ρ，可以保证 EL-Gamal 加密过程是诚实执行的，没有欺诈行为。把该非交互式零知识证明过程生成的证明记做 $proof = (c, \pi_1, \pi_2)$，把 W_s 的密文 C_s 和对应的证明 $proof$ 进行绑定，生成追踪标签 tag：

$$tag = (C_s, proof) \tag{20}$$

5) 完整环签密生成

OBU_s 最终生成关于明文消息 m 的环签密 $\sigma = (C, L, R_0, \{U_j\}_{j=1,\cdots,n}, V, tag, T)$，其中 C 为明文消息 m 的密文，tag 为追踪标签，T 为签密当前时间戳，最后签密者 OBU_s 发送完整的签密 σ 给接收者 OBU_r，等待 OBU_r 对传递消息进行解密，并对环签密过程进行验证。

3.4 解签密

消息接收者 OBU_r 收到环签密 σ 后进行解签密操作。解签密过程分为签密时效性验证、W_s 加密的零知识证明验证、解密传递消息和环签密验证 4 个步骤。

1) 签密的时效性验证

消息接收者 OBU_r 接收到环签密 σ 后首先解析出签密时间戳 T,并判断 $|T-T_c|\leqslant \Delta T$ 是否成立,其中 T_c 为当前时间,ΔT 为消息有效的最大时间间隔。这样可以保证攻击者无法通过拦截重放带有新的时间戳的消息,可以实现抗重放攻击。

2) W_s 加密的零知识证明验证

OBU_r 作为图 3 中非交互式零知识证明的验证者,从签密 σ 中解析出追踪标签中的 $C_s=(C_1,C_2)$ 和 $proof=(c,\pi_1,\pi_2)$,并按照图 3 重新计算:

$$com'_1=\pi_1\cdot P+\pi_2\cdot tpk-c\cdot C_2 \tag{21}$$

$$com'_2=\pi_2\cdot P-c\cdot C_1 \tag{22}$$

$$c'=H_4(com'_1,com'_2,C_s) \tag{23}$$

OBU_r 判断 $c'=c$ 是否成立,若 $c'=c$,则可以确认签密者 OBU_s 是用监管公钥 tpk 对 W_s 进行了诚实加密,可保证监管权威在必要时能追踪到签密者 OBU_s 的真实身份。若 $c'\neq c$,则 OBU_r 拒绝接受签密消息。

3) 解密传递消息

OBU_r 用自己的私钥 (usk_r,w_r) 解密 σ 中所传递的密文 C,得到明文 m'。

$$b'=H_2(e(R_0,usk_r)) \tag{24}$$

$$m'=C\oplus H_3(b',W_sw_r) \tag{25}$$

4) 环签密验证

OBU_r 利用解密出的 m' 对签密 σ 进行验证,OBU_r 计算 h'_j 并验证式(27)。

$$h'_j=H_1(m',U_j,L,R_0,Q_r) \tag{26}$$

$$e(pk,\sum_{j=1}^{n}(U_j+h'_j\cdot Q_j))=e(P,V) \tag{27}$$

若式(27)成立,OBU_r 接受签密者的环签密,并确认 m' 就是签密者所发送的明文消息 m;若式(27)不成立,则解签密失败,拒绝接受签密内容。

3.5 身份追踪

当消息接收者 OBU_r 发现签密者 OBU_s 发送非法信息时,可以向监管权威申请追踪消息发送者的真实身份。监管权威从签密 σ 中提取追踪标签 tag,获取 W_s 的密文 C_s,并利用监管私钥 tsk 解密得到 W_s。

$$\begin{aligned}&W_s+\rho\cdot tpk-\rho\cdot P\cdot tsk=\\&W_s+\rho\cdot tpk-\rho\cdot tpk=W_s\end{aligned} \tag{28}$$

由于在注册时 OBU_s 的真实身份 UID_s 和 W_s 已经绑定,监管权威利用 W_s 就可以追踪到签密者的真实身份 UID_s。

4 方案分析

4.1 正确性分析

4.1.1 私钥份额的正确性

$$\begin{aligned}&e(psk_{i,j},P)=e(s_i\cdot H_0(UID_j,W_j),P)=\\&e(H_0(UID_j,W_j),s_i\cdot P)=\\&e(H_0(UID_j,W_j),rpk_i)\end{aligned} \tag{29}$$

4.1.2 传递消息的正确性

消息接收者 OBU_r 可以重新计算:

$$\begin{aligned}b'&=H_2(e(R_0,usk_r))=\\&H_2(e(r_0\cdot P,sk\cdot Q_r))=\\&H_2(e(r_0\cdot sk\cdot P,Q_r))=\\&H_2(e(r_0\cdot pk,Q_r))=b\end{aligned} \tag{30}$$

$$\begin{aligned}&m'=C\oplus H_3(b',w_r\cdot W_s)=\\&m\oplus H_3(b,w_s\cdot W_r)\oplus H_3(b',w_r\cdot W_s)=\\&m\oplus H_3(b,w_sw_rP)\oplus H_3(b',w_sw_rP)=m\end{aligned} \tag{31}$$

当 $b'=b$,$m'=m$ 时,传递消息正确。

4.1.3 W_s 加密的零知识证明正确性

$$\begin{aligned}&c'=H_4(com'_1,com'_2,C_s)=\\&H_4(\pi_1\cdot P+\pi_2\cdot tpk-c\cdot(W_s+\rho\cdot tpk),\\&\pi_2\cdot P-c\cdot(\rho\cdot P),C_s)=\\&H_4((\rho_1+cw_s)\cdot P+(\rho_2+c\rho)\cdot tpk-\\&c(W_s+\rho\cdot tpk),(\rho_2+c\rho)\cdot P-\\&c(\rho\cdot P),C_s)=\\&H_4(\rho_1\cdot P+c\cdot W_s+\rho_2\cdot tpk+c\rho\cdot tpk-\\&c\cdot W_s-c\rho\cdot tpk,\rho_2\cdot P+c\rho\cdot P-c\rho\cdot P,C_s)=\\&H_4(\rho_1\cdot P+\rho_2\cdot tpk,\rho_2\cdot P,C_s)=\\&H_4(com_1,com_2,C_s)=c\end{aligned} \tag{32}$$

4.1.4 环签密的正确性

$$\begin{aligned}&e(pk,\sum_{j=1}^{n}(U_j+h'_j\cdot Q_j))=\\&e(sk\cdot P,U_s+h'_s\cdot Q_s+\sum_{j=1,j\neq s}^{n}(U_j+h'_jQ_j))=\\&e(sk\cdot P,\alpha\cdot Q_s-\sum_{j=1,j\neq s}^{n}(U_j+h'_j\cdot Q_j)+\\&h'_s\cdot Q_s+\sum_{j=1,j\neq s}^{n}(U_j+h'_j\cdot Q_j))=\\&e(sk\cdot P,\alpha\cdot Q_s+h'_s\cdot Q_s)=\\&e(sk\cdot P,(\alpha+h'_s)\cdot Q_s)=\\&e(P,(\alpha+h'_s)\cdot sk\cdot Q_s)=\\&e(P,(\alpha+h'_s)\cdot usk_s)=e(P,V)\end{aligned} \tag{33}$$

4.2 安全性分析

4.2.1 匿名性

本方案可以保证信息交互双方的匿名通信。签

密者 OBU_s 利用自己的私钥和包括自身在内的 n 个环成员的公钥集合进行环签密。消息接收者只能通过验证确认签密者是环中的某一个成员，但无法通过签密内容来确定签密者的具体身份。随着环规模的增大，签密者的匿名性将得到不断增强。环签密 σ 中不透漏消息接收者 OBU_r 公钥的任何信息，只是通过式(11)和式(13)将消息接收者的公钥隐藏在消息的密文 C 中，攻击者无法通过截获 σ 来计算或者推测消息接收者 OBU_r 的真实身份，从而确保了消息接收者身份的匿名性。

4.2.2 机密性

通信双方所传递的消息 m 是以密文 C 的形式出现在环签密 σ 中，消息接收者 OBU_r 通过计算 b' 和 m' 来进行解密，得到明文 $m'=m$。本方案中只有同时拥有私钥 (usk_r,w_r) 两个部分的消息接收者才能正确解密出传递的明文信息，因此本方案可以确保环签密中消息传递的机密性。

4.2.3 可认证性

本方案中 OBU 私钥是由两部分组成，即 OBU 自己选择的秘密值和 RSU 联盟产生的私钥份额经 OBU 合成后的部分私钥。在注册时，联盟中的 RSU 可以对 OBU 身份的真实性进行认证，OBU 也可对 RSU 发送的部分私钥份额进行认证。消息接收者在收到环签密 σ 后可以通过验证 $c'=c$ 对签密者自觉加密 W_s 的正确性进行认证，通过计算 b'、m'、h'_j 和式(27)，对传递消息的完整性和环签密的正确性进行全面认证。环签密过程中，对其任何一项进行篡改都将无法通过验证。

4.2.4 去中心化

本方案的系统主密钥 sk 是由 RSU 联盟通过 Pedersen 秘密共享方案生成的，每个 RSU 只知道自己的部分私钥，都不掌握系统的主密钥，Pedersen (t,k) 门限方案使得系统最多可以容忍 $t-1$ 个 RSU 被腐化，与中心化的密钥生成方式相比，可以有效防止单点失败问题，增强了系统的安全性和可靠性。

图 4 展示了当 $k=12$ 时 Pedersen (t,k) 门限方案的安全性 $\sum_{j=0}^{t-1}C_k^j p^j(1-p)^{k-j}$，其中 p 为 RSU 联盟中一个 RSU 被腐化的概率，也可以认为是敌手的攻击能力，j 表示联盟中被腐化的 RSU 数量。可以看出，系统的安全性随 t 的增大而增大，当门限值 $t>4$，即门限值超过联盟成员总数的三分之一时，即使敌手的攻击能力 p 达到 0.3，系统的分布式密钥生成过程也被认为是安全的(系统的安全性大于 0.5)。

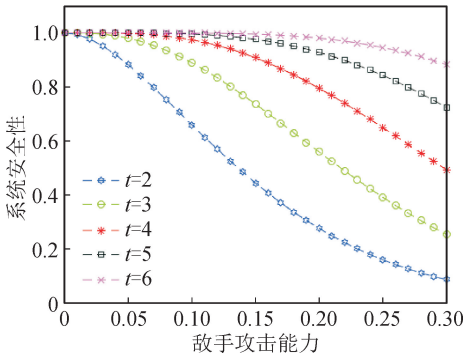

图 4 当 $k=12$ 时 Pedersen (t,k) 门限方案的安全性

Fig. 4 Security of Pedersen (t,k) threshold scheme when $k=12$

4.2.5 防伪造性

签密者的私钥 (usk_s,w_s) 由两部分组成，usk_s 需要 RSU 联盟认证才能生成，w_s 由签密者秘密选取，除了签密者自身，任何实体都不掌握 w_s，要从 W_s 计算出 w_s 属于离散对数困难问题，签密者在掌握 w_s 的前提下，使用非交互式零知识证明来展示对 W_s 加密的正确性，该零知识证明使用文献[26]中的随机预言模型，而攻击者只能通过伪造承诺的随机数来伪造零知识证明，在离散对数假设下，这种伪造发生的概率可以忽略不计。因此，敌手在不掌握签密者私钥的情况下，不可能伪造签密者的身份进行交互，也无法伪造出通过信息接收者验证的环签密。

4.2.6 不可链接性

在环签密过程中，签密者每次都会生成追踪标签 tag 。tag 中的 C_s 在进行 EL-Gamal 加密时会使用随机参数 $\rho\in Z_q^*$，在生成证据 π_1、π_2 以及哈希值 c 时，也会选用随机参数 $\rho_1,\rho_2\in Z_q^*$，所以每次生成的追踪标签都不相同，任何攻击者都无法从收集到的多个追踪标签链接到同一个签密者。

4.2.7 可追踪性

本方案在环签密 σ 中增加了追踪标签 $tag=(C_s,proof)$，$proof=(c,\pi_1,\pi_2)$。其中 C_s 为 W_s 在监管公钥 tpk 加密下的密文。π_1 为签密者 OBU_s 掌握 w_s 的证据，π_2 为签密者掌握加密选取参数 ρ 的证据，通过非交互式零知识证明来保证签密者是用监管公钥对关联签密者身份的 W_s 进行了诚实加密。接收者则通过 $c'=c$ 来验证签密者 OBU_s 对 W_s 加密的正确性，从而保证监管权威可以追踪到签密者的真实身份。

表 1 对几种方案的安全性进行了综合比较。文献[16]、[17]所提方案均需要可信中心，容易造成单点失败，文献[21]的方案没有对消息进行加密，不能保证消息的机密性。所有方案都可以实现匿名

性、可认证性、防伪造性、不可链接性和可追踪性。本方案同时具有上述所有安全特性，并实现了去中心化(由多个 RSU 通过分布式门限密钥生成方法共同决定系统的主密钥)，在保证安全性的同时，具有更好的灵活性。

表 1 不同方案的安全性能比较

Tab. 1 Comparison of security performance of different schemes

性能	文献[16]	文献[17]	文献[21]	本方案
匿名性	√	√	√	√
机密性	√	√	×	√
可认证性	√	√	√	√
去中心化	×	×	√	√
防伪造性	√	√	√	√
不可链接性	√	√	√	√
可追踪性	√	√	√	√

4.3 通信开销分析

对几种可追踪的环签密方案的通信开销进行分析和比较。设加法群 G_1 中的元素为 128 bytes，有限域 Z_q^* 中的元素为 64 bytes，一般哈希函数为 20 bytes，时间戳为 4 bytes。分析中不考虑消息 m 的固有长度和环公钥集合 L 的通信开销。表 2 计算了各方案的签密通信开销。

表 2 不同方案的签密通信开销比较

Tab. 2 Comparison of signcryption communication overhead of different schemes

方案	签密通信开销/bytes
文献[16]	$(3n+3)G_1 = 384n+384$
文献[17]	$(2n+1)G_1 + T = 256n+132$
文献[21]	$(2n+2)G_1 = 256n+256$
本方案	$(n+4)G_1 + 2Z_q^* + hash + T = 128n+664$

图 5 中，当环成员数 $n=4$ 时，本方案通信开销为 1 176 bytes，略高于文献[17]的 1 156 bytes，但小于其他两个方案的通信开销；当 $n=8$ 时，本方案环签密通信开销为 1 688 bytes，通信开销最小。

图 6 模拟了各方案的环签密通信开销随环成员数 n 的变化。从图 6 可以看出，从 $n>4$ 开始，本方案通信开销最小。本方案中环签密 σ 的通信开销主要包括 C、R_0、$\{U_j\}_{j=1,\cdots,n}$、V、tag 和 T 几个部分。本方案中传递消息的密文 C 和传递消息 m 的长度保持一致，没有增加额外的通信开销，R_0 属于 G_1 中的元素，V 属于 G_1 中的元素，追踪标签 $tag=(C_s, c, \pi_1, \pi_2)$ 中的 C_s 包含 G_1 中的两个元素，c 是长度为 20 bytes 的哈希值，π_1, π_2 属于 Z_q^* 中的两个元素，$\{U_j\}_{j=1,\cdots,n}$ 属于 G_1 中的 n 个元素，T 是时间戳。本方案的签密通信开销包括 G_1 中的 $n+4$ 个元素、Z_q^* 中的两个元素、一个哈希值 c 和一个时间戳 T。其中只有 $\{U_j\}_{j=1,\cdots,n}$ 的通信开销和环成员数 n 有关，其他部分的通信开销 $4G_1+2Z_q^*+hash+T$ 是固定的。而其他几个方案为了实现追踪功能，均需要在环签密中额外增加和环成员数 n 相关的参数，文献[16]中的通信开销为 $(3n+3)G_1=384n+384$ bytes，文献[17]为 $(2n+1)G_1+T=256n+132$ bytes，文献[21]为 $(2n+2)G_1=256n+256$ bytes，本方案通信开销为 $(n+4)G_1+2Z_q^*+hash+T=128n+664$ bytes。当 n 较小时，由于本方案中的 $4G_1+2Z_q^*+hash+T$ 这部分通信开销是固定的，无法避免，所以还未能显现出其在通信开销方面的优势；从 $n>4$ 开始，由于其他方案的通信开销和环成员数 n 都有着 $2n$ 甚至 $3n$ 的关系，因而本方案在通信开销方面的优势得以显现。

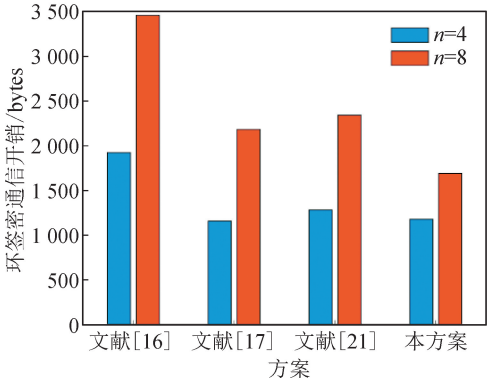

图 5 $n=4$ 和 $n=8$ 两种情况下各方案环签密通信开销

Fig. 5 Ring signcryption communication overhead of each scheme in the two cases of $n=4$ and $n=8$

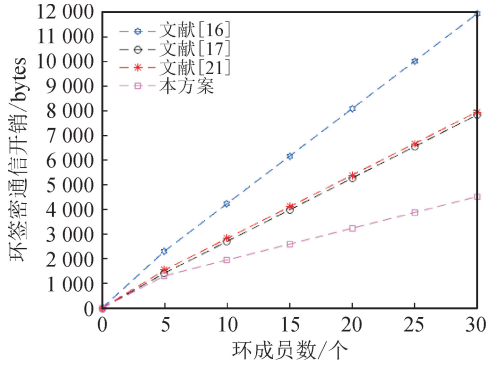

图 6 不同方案环签密通信开销随环成员数的变化

Fig. 6 Ring signcryption communication overhead of different schemes varies with the number of ring members

4.4 计算开销分析

本文所提方案在联盟区块链的初始化和密钥生成过程中计算开销都偏高,但由于系统初始化和密钥生成在一段时间内都只需执行一次,后续的多次环签密过程均无需额外的计算开销,因此本文只讨论签密、验证、追踪这三个阶段各方案所需的计算开销。在硬件为 Intel(R) Core(TM) i3-10100,主频为 3.60 GHz,内存 16GB,Windows 10 操作系统中,选用 PBC 代码库对常用的几种运算操作的耗时进行多次实验并取平均值,得到测试结果为 $T_{mul} \approx 1.85$ ms ,$T_p \approx 4.32$ ms,$T_h \approx 5.86$ ms。其中 T_{mul} 为群上的标量乘法计算耗时,T_p 为双线性映射的计算耗时,T_h 为映射到群中点元素的哈希函数计算耗时。相比其他运算,上述三种操作的耗时为主要计算开销,因此,本文通过对比这三种运算的耗时来评估各方案的计算开销,如表 3 所示。

表 3 各环签密方案计算开销对比

Tab. 3 Computational cost comparison of each ring signcryption scheme

方案	环签密/ms	解签密/ms	追踪/ms	总计算开销/ms
文献[16]	$(4n+2)T_{mul}+T_p+T_h \approx 7.4n+13.88$	$nT_{mul}+(2n+3)T_p+T_h \approx 10.49n+18.82$	$nT_{mul}+4nT_p \approx 19.13n$	$(6n+2)T_{mul}+(6n+4)T_p+2T_h \approx 37.02n+32.7$
文献[17]	$3nT_{mul}+T_p \approx 5.55n+4.32$	$nT_{mul}+3T_p \approx 1.85n+12.96$	$2nT_{mul} \approx 3.70n$	$6nT_{mul}+4T_p \approx 11.1n+17.28$
文献[21]	$(4n+3)T_{mul} \approx 7.4n+5.55$	$nT_{mul}+4T_p+T_h \approx 1.85n+23.14$	$nT_{mul}+4nT_p \approx 19.13n$	$(6n+3)T_{mul}+(4n+4)T_p+T_h \approx 28.38n+28.69$
本方案	$(2n+8)T_{mul}+T_p \approx 3.7n+19.12$	$(n+6)T_{mul}+3T_p \approx 1.85n+24.06$	$T_{mul} \approx 1.85$	$(3n+15)T_{mul}+4T_p \approx 5.55n+45.03$

1) 环签密计算开销

本方案环签密计算开销为 $(2n+8)T_{mul}+T_p$,约为 $3.7n+19.12$ ms。计算开销主要包括:计算消息密文 C 时需要的 2 次群上的标量乘法运算 $w_s \cdot W_r$ 、$r_0 \cdot pk$,一次双线性映射运算 $R' = e(r_0 \cdot pk, Q_r)$,计算 R_0 中需要的一次群上的标量乘法运算 $R_0 = r_0 \cdot P$,计算 $\{U_j\}_{j=1,\cdots,n}$ 中需要的 $2n-1$ 次群上的标量乘法运算,计算 V 中需要的一次群上的标量乘法运算,对 W_s 加密生成密文 C_s 需要的 2 次群上的标量乘法运算,生成零知识证明 $proof$ 需要的 3 次群上的标量乘法运算。其中只有计算 $\{U_j\}_{j=1,\cdots,n}$ 时的 $2n-1$ 次群上的标量乘法运算和环成员数 n 有关,其他的计算开销均为固定值。本方案在环签密阶段的固定计算开销约为 19.12 ms,而文献[17]的固定计算开销约为 4.32 ms,在环成员数较小时,文献[17]在本阶段计算开销最小,为 $3nT_{mul}+T_p \approx 5.55n+4.32$ ms。这是因为文献[17]在签密阶段的计算开销和环成员数 n 之间有着 $3nT_{mul}$ 的关系,而本方案在签密阶段的计算开销和环成员数 n 之间有着 $2nT_{mul}$ 的关系,故随着环成员数的增加,本方案固定开销较大的劣势将随着 n 的逐步增大而被抵消掉。从环成员数 $n=8$ 开始,本方案在环签密阶段的计算开销将逐步达到最小(相较其他几种方案),且环成员数越大,本方案的优势越明显。

2) 解签密计算开销

本方案解签密计算开销为 $(n+6)T_{mul}+3T_p$,约为 $1.85n+24.06$ ms。计算开销主要包括:零知识证明验证中需要的 5 次群上的标量乘法、解密所传递消息的密文时需要的 1 次群上的标量乘法和一次双线性映射运算、在验证环签名时需要的 n 次群上的标量乘法和 2 次双线性映射运算。文献[17]的解签密计算开销最小,为 $nT_{mul}+3T_p \approx 1.85n+12.96$ ms,相比文献[17],本方案多了 6 次群上的标量乘法运算。这是因为,在追踪 W_s 加密正确性的非交互式零知识证明过程中,多了 5 次群上的标量乘法运算,在解密传递消息时,多了 1 次群上的标量乘法运算。但文献[17]还有两次额外的异或运算未计算在内,且文献[17]在解签密阶段采用的是先验证环签名再进行解密明文消息的方法,其解密出的明文消息并未经过环签名验证流程的验证。

3) 追踪计算开销

在追踪阶段,文献[16]和文献[21]的计算开销都为 $nT_{mul}+4nT_p \approx 19.13n$ ms,追踪的计算开销较大,且追踪过程需要系统所有成员进行诚实交互。文献[17]追踪的计算开销为 $2nT_{mul} \approx 3.70n$ ms,需要采用遍历算法对所有环成员的公钥进行排查。随

着环成员数 n 的增加，其他几个方案的追踪开销都随着 n 线性增加。本方案在追踪阶段计算开销优势明显，只需要从追踪标签 tag 中提取密文 C_s，利用 EL-Gamal 解密就可以得到 W_s，从而确定签密者的真实身份，本方案追踪的计算开销为 $T_{mul} \approx 1.85$ ms，且追踪开销和环成员数 n 无关，因此在 VANETs 中，无论环成员数如何增加，当有用户发布虚假或者非法信息时，非法者的真实身份都可以在第一时间被监管权威快速追踪到。

4）总计算开销

图 7 展示了当 $n=8$ 时，各方案在环签密阶段、解签密阶段、追踪阶段的计算开销和总的计算开销。由图 7 可以看出，当 $n=8$ 时，本方案和文献[17]在签密阶段具有最小的计算开销，在追踪阶段本方案的计算开销优势明显，而且本方案有着最小的总计算开销。

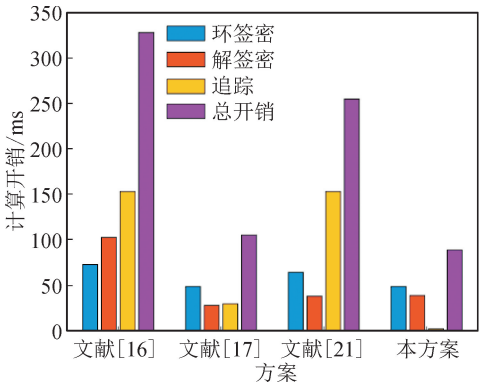

图 7 $n=8$ 时各签密方案不同阶段计算开销比较

Fig. 7 Computation cost comparison of each signcryption scheme in stages when $n=8$

图 8 模拟了几种方案的总计算开销随环成员数 n 的变化情况。由表 3 可知，文献[16]的总计算开销为 $(6n+2)T_{mul}+(6n+4)T_p+2T_h$，约为 $37.02n+32.7$ ms，文献[17]的总计算开销为 $6nT_{mul}+4T_p \approx 11.1n+17.28$ ms，文献[21]的总计算开销为 $(6n+3)T_{mul}+(4n+4)T_p+T_h$，约为 $28.38n+28.69$ ms，本文所提方案的总计算开销为 $(3n+15)T_{mul}+4T_p \approx 5.55n+45.03$ ms。由于本文方案中存在环签密阶段对 W_s 加密的零知识证明生成和解签密阶段对 W_s 加密的零知识证明验证以及追踪阶段对 W_s 的解密追踪，这些步骤的计算开销都是固定的，和环成员数 n 无关。当环成员数较少时，这些计算开销仍然存在，所以当环成员数 $n<5$ 时，本方案的计算开销略高于计算开销最小的文献[17]，但优于其他两个方案。除本方案之外，其他 3 个方案为了实现追踪功能，在环签密和追踪阶段都需要付出和环成员数 n 相关的计算开销，因而从 $n=5$ 开始，本方案总计算开销达到最优，而且随着环成员数 n 的增加，本方案的总计算开销的优势将会越来越显著，说明本方案更适用于车流量较大的 VANETs 环境。

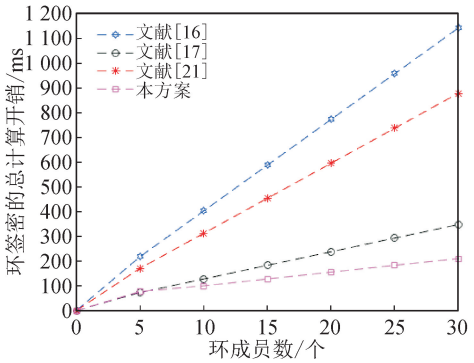

图 8 不同方案环签密总计算开销随环成员数的变化

Fig. 8 Total computation cost of ring signcryption for different schemes varying with the number of ring members

5 结 语

本文基于环签密和非交互式零知识证明技术，在 VANETs 中设计了条件隐私保护方案。非交互式零知识证明的引入保证了用户身份加密的正确性，并在环签密中实现了追踪功能，从而实现了条件隐私保护；同时，方案还具有防伪造性、去中心化、不可链接性、所有环节可认证等安全特性。相比同类方案，本方案具有较小的通信和计算开销。

本文只考虑了单一监管权威的情形，为了防止监管滥用，可以采用分布式密钥生成技术，由多个监管权威共享监管密钥来增强系统的安全性。

参考文献：

[1] HOSSEINI M B, RAHMANZADEH A, NAZEMI E. A self-organising organisational paradigm for using multi-agent systems in traffic control application of VANETs[J]. International Journal of Sensor Networks, 2022, 38(3): 143-153.

[2] WFAROOQS M, HUSSAIN S M S, USTUNT S. A survey of authentication techniques in vehicular ad-hoc networks[J]. IEEE Intelligent Transportation Systems Magazine, 2020, 13(2): 39-52.

[3] WANG Yimin, ZHONG Hong, XU Yan, et al. Enhanced security identity-based privacy-preserving authentication scheme supporting revocation for VANETs [J]. IEEE Systems Journal, 2020, 14(4): 5373-5383.

[4] ZHANG Chunhua, XUE Xiaoping, FENG Lijuan, et al. Group-signature and group session key combined safety message authentication protocol for VANETs [J]. IEEE Access, 2019, 7: 178310-178320.

[5] DENG Xinyang, GAO Tianhan, GUO Nan, et al. PCP: a pseudonym change scheme for location privacy preserving in VANETs[J]. Entropy, 2022, 24(5): 648.

[6] ZENG Shengke, HUANG Yuan, LIU Xingwei. Privacy-preserving communication for VANETs with conditionally anonymous ring signature[J]. International Journal of Network Security, 2015, 17(2): 135-141.

[7] LIU Feng, WANG Qi. IBRS: an efficient identity-based batch verification scheme for VANETs based on ring signature[C]//2019 IEEE Vehicular Networking Conference (VNC). IEEE, 2019: 1-8.

[8] BOUALOUACHE A, SENOUCI S M, MOUSSAOUI S. PRIVANET: an efficient pseudonym changing and management framework for vehicular ad-hoc networks [J]. IEEE Transactions on Intelligent Transportation Systems, 2019, 21(8): 3209-3218.

[9] LIU Zishan, LIU Zhenyu, ZHANG Lin, et al. MARP: a distributed MAC layer attack resistant pseudonym scheme for VANET[J]. IEEE transactions on dependable and secure computing, 2018, 17(4): 869-882.

[10] MUNDHE P, YADAV V K, SINGH A, et al. Ring signature-based conditional privacy-preserving authentication in VANETs[J]. Wireless Personal Communications, 2020, 114(1): 853-881.

[11] GUO Hui, DENG Lunzhi. Certificateless ring signcryption scheme from pairings[J]. International Journal of Network Security, 2020, 22(1): 102-111.

[12] SHARMA G, BALA S, VERMA A K. Pairing-free certificateless ring signcryption (PF-CLRSC) scheme for wireless sensor networks[J]. Wireless Personal Communications, 2015, 84(2): 1469-1485.

[13] Al-SHAREEDA M A, ANBAR M, HASBULLAH I H, et al. Efficient conditional privacy preservation with mutual authentication in vehicular ad hoc networks[J]. IEEE Access, 2020, 8: 144957-144968.

[14] 吴甜甜,杨亚芳,赵运磊. 一种面向车联网通信的条件隐私保护认证协议[J]. 计算机工程,2021,47(6):14-22,31.
WU Tiantian, YANG Yafang, ZHAO Yunlei. An authentication protocol with conditional privacy protection for IoV communication[J]. Computer Engineering, 2021, 47(6):14-22,31.

[15] SAMRA B, FOUZI S. New efficient certificateless scheme-based conditional privacy preservation authentication for applications in VANET[J]. Vehicular Communications, 2022, 34: 100414.

[16] 赵楠,章国安. VANET 中基于无证书环签密的可认证隐私保护方案[J].计算机科学,2020,47(3):312-319.
ZHAO Nan, ZHANG Guoan. Authenticated privacy protection scheme based on certificateless ring signcryption in VANET[J]. Computer Science, 2020, 47(3): 312-319.

[17] CAI Ying, ZHANG Hao, FANG Yuguang. A conditional privacy protection scheme based on ring signcryption for vehicular ad hoc networks[J]. IEEE Internet of Things Journal, 2020, 8(1): 647-656.

[18] MA Shunli, DENG Yi, HE Debiao, et al. An efficient NIZK scheme for privacy-preserving transactions over account-model blockchain[J]. IEEE Transactions on Dependable and Secure Computing, 2020, 18(2): 641-651.

[19] 赵艳琦. 基于区块链的认证与数据安全协议研究[D]. 西安:陕西师范大学,2021.
ZHAO Yanqi. Research on authentication and data security protocol based on blockchain[D]. Xi'an: Shaanxi Normal University, 2021.

[20] BOGATOV D, CARO A D, ELKHIYAOUI K, et al. Anonymous transactions with revocation and auditing in hyperledger fabric[C]//International Conference on Cryptology and Network Security. Springer, Cham, 2021: 435-459.

[21] TANG Fei, PANG Junjie, CHENG Kefei, et al. Multiauthority traceable ring signature scheme for smart grid based on blockchain[J]. Wireless Communications and Mobile Computing, 2021, 2021:1-9.

[22] 黄丹. 区块链与环签密结合的电子证据认证加密方案[J]. 重庆邮电大学学报:自然科学版,2022,34(1):16-23.
HUANG Dan. Authenticated encryption scheme of electronic evidence based on blockchain and ring signcryption [J]. Journal of Chongqing University of Posts and Telecommunications (Natural Science Edition), 2022, 34(1):16-23.

[23] 沈华杰. 车联网中基于联盟链的轻量级认证和隐私保护方案研究[D]. 上海:华东师范大学,2022.
SHEN Huajie. Research on lightweight certificate authority and privacy preserving scheme based on consortium blockchain in internet of vehicles [D]. Shanghai: East China Normal University, 2022.

[24] FIAT A, SHAMIR A. How to prove yourself: practical solutions to identification and signature problems [C]//Conference on the Theory and Application of Cryptographic Techniques. Springer, Berlin, Heidelberg, 1986: 186-194.

[25] PEDERSEN T P. A threshold cryptosystem without a trusted party[C]//Workshop on the Theory and Application of Cryptographic Techniques. Springer, Berlin, Heidelberg, 1991: 522-526.

[26] SCHNORR C P. Efficient signature generation by smart cards[J]. Journal of Cryptology, 1991, 4(3): 161-174.

(责任编辑 周 蓓)