

车联网环境下多接收者匿名签密方案

邢丹丹, 曹素珍, 赵晓, 周大伟, 王正

(西北师范大学计算机科学与工程学院, 甘肃 兰州 730070)

摘要: 针对车联网中车辆的隐私泄露和恶意车辆提供虚假信息的问题, 提出一种适用于车联网环境的多接收者匿名签密方案。该方案使车辆能够向一组路侧单元(RSU)发送秘密信息。利用可信中心生成的长期伪身份和自己生成的短期伪身份保证车辆的强匿名性来提供有条件的隐私, 并避免造成发送者车辆的身份泄露。在签密的过程中将指定的一组接收者 RSU 的身份信息采用模多项式计算后添加到密文当中实现 RSU 之间的匿名。此外, 如果发现车辆有篡改和拦截消息等恶意行为, 它会被可信中心跟踪并撤销身份。在椭圆曲线离散对数问题和计算性 Diffie-Hellman 的基础上证明了所提方案在 ROM 下满足消息保密性、不可伪造性、匿名性、可撤销性等安全要求, 安全性证明和效率分析表明该方案具有较高的安全性。实验结果表明, 与对比方案相比, 该方案在车辆对消息进行签密的阶段中所用时间减少了 36.4%~54.7%, 总时间减少了 47.3%~56.7%, 同时, 该方案在解签密阶段是恒定数值, 具有较高的计算效率和实用性。

关键词: 车联网; 多接收者签密; 匿名性; 可追踪; 可撤销

中图分类号: TP309

文献标志码: A

DOI: 10.19678/j.issn.1000-3428.0068383

Multi-Receiver Anonymous Signcryption Scheme in IoV

XING Dandan, CAO Suzhen, ZHAO Xiao, ZHOU Dawei, WANG Zheng

(College of Computer Science and Engineering, Northwest Normal University, Lanzhou 730070, Gansu, China)

[Abstract] To address the issues of privacy leakage and false information from malicious vehicles in the Internet of Vehicle(IoV), this study proposes a multi-receiver anonymous signcryption scheme. This scheme enables a vehicle to send secret information to a set of Roadside Units(RSUs). The process involves two key steps. First, the use of a long-term pseudo-identity generated by the Trusted Authority(TA) and a short-term pseudo-identity generated by the vehicle itself ensure strong anonymity, providing conditional privacy and preventing leakage of the sender's identity. Second, during signcryption, the identity information of the specified group of recipient RSUs is calculated using a modular polynomial and incorporated into the ciphertext to maintain anonymity between RSUs. In addition, if a vehicle is detected tampering with or intercepting messages, it will be tracked and revoked by the TA. Based on the elliptic curve discrete logarithm problem and Computational Diffie-Hellman(CDH), the scheme's security properties, including message confidentiality, unforgeability, anonymity, and revocability, are proven. Security proofs and efficiency analysis show that the scheme offers high security. Experimental results show that, compared to related schemes, this scheme reduces the time required for the vehicle signcryption stage by 36.4%~54.7%, and the total time by 47.3%~56.7%. Furthermore, the scheme maintains a constant value in the decryption stage, providing high computational efficiency and practicability.

[Key words] Internet of Vehicles(IoV); multi-receiver signcryption; anonymity; traceable; revocable

0 引言

车联网(IoV)的网络拓扑结构变化快,对信息实时性要求高^[1-3],主要利用传感器数据采集、无线射频识别(RFID)以及专用短程通信(DSRC)^[4]等技术来实现车辆与车辆之间、车辆与路侧单元(RSU)之间的通信和信息交换^[5]。

然而在 IoV 的通信过程中,通信内容容易被恶

意攻击者修改、拦截和删除,甚至跟踪车辆并获取车辆隐私信息^[6-8]。因此,通信过程中存在一系列潜在的安全风险^[9-11]。传输的数据可能包含仅针对特定接收者的敏感信息,因此需要采取保密措施。而签密是在信息交换中提供身份验证、完整性和机密性的可靠手段^[12-13],尤其是在有多个接收者的情况下,与每个接收者协商并向其发送不同密文的传统方法相比显著提高了发送方的效率。

收稿日期: 2023-09-17 修回日期: 2023-12-15

基金项目: 国家自然科学基金(62262060,62362059);甘肃省教育厅产业支撑计划项目(2022CYZC-17,2023CYZC-09);甘肃省重点研发计划项目(23YFGA0081)。

通信作者 E-mail: 1563404753@qq.com

近年来,由于频频发生隐私泄露事件,用户有了越来越强的隐私保护意识,因此,验证用户的身份和保护消息完整性是通信过程中的必然要求。多接收者签密这种一对多的通信方式更适用于开放的 IoV 环境^[14-16],发送者和接收者都希望隐藏自己的真实身份。为了实现发送者匿名,文献[17]提出了一个隐藏发送者身份的多接收者签密方案,该方案将发送者的公钥与随机数相乘来隐藏发送者的身份。假名机制也可以保持车辆的匿名性,在恶意情况下仍能还原车辆真实身份^[18],真正实现接收者之间的匿名,文献[19]提出了一种新的模大素数多项式来混合和隐藏接收者的身份信息,这是目前最有效的方法之一。

文献[20]提出了一个基于身份的多签密和多接收者签密方案,解决了公钥证书管理的问题。文献[21]提出了一种基于身份的区块链聚合签密方案,但与文献[20]方案一样,该方案仍存在密钥托管问题。为了解决这一问题,许多研究人员提出了无证书签密方案。文献[22]提出了基于车联网的安全预警系统的隐私保护聚合认证方案,该方案与文献[21]方案一样,都使用了聚合签密这种多对一的通信模式,而多接收者签密是一种一对多的通信模式。文献[23]提出了一种用于智能社区管理系统的匿名无证书多接收器加密方案,该方案能够对恶意的发送者进行追踪,但无法撤销恶意的发送者,且在签密过程用到了计算复杂的双线性对,增加了运算时间。文献[24]提出了一种多密钥生成中心(KGC)通过公开信道的多接收者签密方案。文献[25]提出了一种应用区块链的多接收者多消息签密方案,该方案与文献[24]都是基于椭圆曲线密码体制,消除了双线性对,大大提高了计算效率,但并不具备追踪发送者的功能。

针对上述问题,本文提出适用于车联网环境的多接收者匿名签密方案,主要内容如下:

1) 基于无证书密码体制构造方案,通过无证书密码体制解决证书管理问题和密钥托管问题,有效降低 IoV 环境的通信负担。

2) 利用可信中心(TA)生成的长期伪身份和自己生成的短期伪身份保证车辆的强匿名性,避免造成发送者车辆的身份泄露。

3) 为实现 RSU 之间的匿名,在签密的过程中将指定的一组接收者 RSU 的身份信息采用模多项式计算后添加到密文中。

4) 当车辆有篡改和拦截消息等恶意行为时,可信中心可以追踪该车辆的真实身份,并由可信中心

撤销该用户。

5) 基于椭圆曲线离散对数困难问题构造高效的多接收者签密方案,方案在构造过程中不涉及双线性对运算,具有轻量化的优势,更适合 IoV 中快响应、低时延的计算需求。

1 预备知识

1.1 椭圆曲线

设满足方程 $y^2 = x^3 + ax + b \pmod{p}$ 上所有点的集合加上一个无穷远点 O 称为椭圆曲线,其中, p 是一个素数, a, b, x, y 都在 $E_p(a, b)$ 上取值,在给定的运算中, G 是集合中所有的点构成的 Abel 群。运算规则如下: 1) $p + O = p$; 2) 假设 p 的加法逆元是 $p^* = -p$, 则有 $p + p^* = O$; 3) 若有 n 个 p 相加, 则 $p + p + \dots + p = np$ 。

1.2 计算性 Diffie-Hellman(CDH)问题^[26]

给定一个阶为 q 的加法循环群 G , P 是 G 的生成元, 给定 $P, aP, bP \in G_q$, $a, b \in \mathbb{Z}_q^*$, 计算 $abP \in G_q$ 。CDH 假设如下:

定义算法 Ω , CDH 问题可以通过任意多项式时间算法求解的概率优势为: $A_{\Omega, \text{CDH}} = \Pr[\Omega(P, aP, bP) = abP]$ 。

1.3 椭圆曲线上的离散对数(ECDLP)问题^[26]

已知 $P, aP \in G_q$, 其中 $a \in \mathbb{Z}_q^*$, 求解满足条件的 a 。ECDLP 问题可以通过任意多项式时间算法求解的概率优势为: $A_{\Omega, \text{ECDLP}} = \Pr[\Omega(P, aP) = a]$ 。

1.4 符号说明

本文方案中的部分符号说明如表 1 所示。

表 1 符号说明

Table 1 Symbol description

符号	含义
T_{pub}	TA 的主公钥
K_{pub}	KGC 的主公钥
H_i	单向哈希函数
(x_i, y_i)	用户的完整私钥
E_k/D_k	对称加/解密算法
R_{ID_i}	车辆的真实身份
Q_{ID_i}	车辆的长期伪身份
P_{ID_i}	车辆的短期伪身份
P_{K_v}	车辆的公钥
P_{K_i}	RSU 的公钥
$f(\xi)$	RSU 身份信息的混合多项式
a_i	身份信息混合多项式 $f(\xi)$ 的系数
c	签密密文

2 本文方案

2.1 系统模型

本文方案主要由 4 个实体组成,即 TA、KGC、车辆(Vehicle)和 RSU。系统模型如图 1 所示。

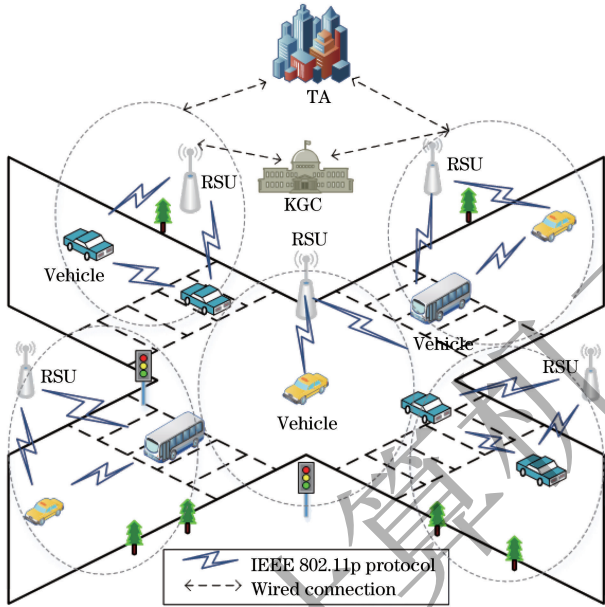


图 1 系统模型

Fig. 1 The system model

1)TA 是完全可信的实体,并拥有强大的计算能力和广泛的存储能力。因此,它们拥有车辆的真实身份列表,负责系统初始化、车辆注册、车辆假名以及恶意车辆的跟踪和撤销。

2)在系统中,KGC 是另一个拥有丰富计算和通信资源的可信实体。KGC 负责为系统中的车辆和 RSU 生成部分私钥。

3)每辆车都必须将真实的身份发送给 TA 进行注册。此外,车辆必须配备防篡改装置(TPD)和车载单元(OBU),TPD 具有高强度的安全特性,能够防止在各类环境下的信息泄露,以便安全地存储和处理敏感数据。通常,车辆收集实时交通数据,对信息进行签名加密,并将生成的密文发送到指定的一组 RSU。

4)RSU 是位于路边的无线基础设施,其主要任务是从附近的车辆接收已签密的密文,并对密文执行解签密以提取消息。在验证这些消息后,RSU 将继续为车辆提供服务。此外,RSU 可以向附近的车辆广播交通相关信息,并将相关反馈转发给 TA。

2.2 算法模型

在本小节中详细说明工作流程的 7 个阶段,即初始化、车辆注册、密钥生成、短期伪身份生成、签密、解签密、追踪和撤销。

1)初始化。TA 和 KGC 运行初始化算法以获得主密钥 s_1, s_2 和公共参数: $\{q, P, T_{pub}, K_{pub}, G_q, E_k, D_k, H_0, H_1, H_2, H_3, H_4, H_5\}$ 。

2)车辆注册。每辆车都需要在 TA 注册,才能获得其假名。首先,车辆发送真实身份 R_{ID_i} 。收到 R_{ID_i} 后,TA 运行长期假名生成算法以获取车辆的长期伪身份 Q_{ID_i} 。

3)密钥生成。将公共参数和车辆的身份信息 Q_{ID_i} 作为输入,车辆或 RSU 通过执行该算法可以得到自己的秘密值 x_i ,KGC 通过执行该算法可以得到车辆或 RSU 的部分私钥 y_i ,并得到车辆或 RSU 的公钥 P_{K_i} 。

4)短期伪身份生成。输入长期伪身份 Q_{ID_i} 和公共参数,TA 运行该算法为车辆生成短期伪身份 P_{ID_i} 。

5)签密。假设车辆 P_{ID_i} 需要向一组 $RSU = \{I_{D_1}, I_{D_2}, \dots, I_{D_n}\}$ 发送明文消息 M ,将系统参数等作为输入,车辆执行该算法得到签密密文: $(M, P_{ID_i}, P_{K_i}, S_{K_i}, \{I_{D_1}, I_{D_2}, \dots, I_{D_n}\})$ 。

6)解签密。在接收到相应的密文和车辆的假名 P_{ID_i} 后,运行该算法得到 M 。

7)追踪和撤销。一旦 RSU 发现任何车辆发送了虚假信息,它将向 TA 提交车辆的假名 P_{ID_i} ,TA 通过计算 $R_{ID_i} = P_{ID_i,1} \oplus H_2(s_1 P_{ID_i,1}, Q_{ID_i}, T_i)$ 来追踪车辆的真实身份并在列表 UL 中撤销车辆。

2.3 安全模型

本文方案是基于无证书的密码体制的,考虑 2 种不同的敌手,即第 1 类敌手 A_1 和第 2 类敌手 A_2 。2 类攻击者的特点比较如表 2 所示。

表 2 2 类攻击者的特点比较

Table 2 Comparison of the characteristics of two types of attackers

敌手	替换用户公钥	获得系统主密钥
A_1	✓	×
A_2	×	✓

2.3.1 消息保密性

方案的消息保密性即无证书多接收者签密在选择密文攻击下具有的密文不可区分性(IND-CLMS-CCA)。Game1 和 Game2 分别描述对抗敌手 A_1 和敌手 A_2 。

Game1 步骤如下:

初始化 挑战者 C 运行此算法生成系统主密钥和系统公共参数,然后将公共参数发送给 A_1 。 A_1 收到后输出一组目标身份 $RSU^* = \{I_{D_1}^*, I_{D_2}^*, \dots,$

$I_{D_n}^*$ }, 其中, n 是正整数, 然后将 RSU^* 发送给 C 。

哈希查询 A_1 要求 C 对方案 Ω 中使用的哈希函数进行一系列查询, C 向 A_1 响应相应的哈希值。

阶段 1 A_1 向 C 询问以下一系列询问, 然后 C 相应地做出响应:

1) 秘密值询问: 当 A_1 要求 C 对用户进行秘密值询问, 收到查询后, C 运行算法以获取用户的秘密值 x_{ID} , 并将其返回给 A_1 。

2) 部分私钥提取询问: 当 A_1 要求 C 对用户进行部分私钥提取询问, 收到查询后, C 运行算法以获取用户的部分私钥 y_{ID} , 并将其返回给 A_1 。

3) 设置公钥查询: 当 A_1 要求 C 对用户进行设置公钥询问, 收到查询后, C 运行算法以获取用户的公钥 $P_{K_{ID}}$, 并将其返回给 A_1 。

4) 设置私钥查询: 当 A_1 要求 C 对用户进行设置私钥询问, 收到查询后, C 运行算法以获取用户的私钥 $S_{K_{ID}}$, 并将其返回给 A_1 。

5) 公钥替换查询: 当 A_1 要求 C 对用户进行公钥替换询问, 收到查询后, C 运行算法将 $P_{K_{ID}}^*$ 作为用户的新公钥。

6) 签密询问: 当 A_1 要求 C 对明文 M 进行签密, C 运行签密算法并将密文 c 返回给 A_1 。

7) 解签密询问: 当 A_1 要求 C 对其选择的密文 c 进行设计解密时, C 运行解密算法并将 M 返回给 A_1 。

挑战 A_1 生成一对长度相等的明文 $\langle M_0, M_1 \rangle$ 并将其发送给 C 。 C 随机选择 $\beta \in \{0, 1\}$, 并计算 M_β 的密文 c^* , 然后将 c^* 返回给 A_1 。

阶段 2 A_1 要求 C 进行查询阶段所述的一系列查询, 但 A_1 无法对公钥已被替换的用户执行秘密值查询、部分私钥提取查询和设置私钥查询, 以及对密文 c^* 执行解签密查询。

猜测 A_1 猜测 $\beta^* \in \{0, 1\}$ 。如果 $\beta^* = \beta$ 成立, A_1 获胜, 否则失败。 A_1 获胜的优势被定义为: $A_{\Omega, \text{IND-CLMS-CCA}}(A_1) = |2\Pr[\beta^* = \beta] - 1|$ 。

如果对于选择密文攻击下的任何 A_1 , 在时间 τ 内获胜的概率优势满足 $A_{\Omega, \text{IND-CLMS-CCA}}(A_1) \leq \epsilon$, 则方案 Ω 安全, 其中, τ 是多项式运行时间, ϵ 是可忽略的概率优势。

Game2 步骤如下:

初始化 挑战者 C 运行算法生成系统公共参数, 然后将公共参数发送给 A_2 。 A_2 收到后输出一组目标身份 $RSU^* = \{I_{D_1}^*, I_{D_2}^*, \dots, I_{D_n}^*\}$, 其中, n 是正整数, 然后将 RSU^* 发送给 C 。

哈希查询 此步骤与 Game1 相同。

阶段 1 A_2 向 C 请求以下一系列查询, C 相应地做出响应:

1) 部分私钥提取询问: 当 A_2 要求 C 对用户进行部分私钥提取询问, 收到查询后, C 运行算法以获取用户的部分私钥 y_{ID} , 并将其返回给 A_2 。

2) 公钥替换询问: 当 A_2 要求 C 对用户进行公钥替换询问, A_2 要求 C 用自己选择的 $P_{K_{ID}}^*$ 替换用户的 $P_{K_{ID}}$ 时, C 将 $P_{K_{ID}}^*$ 保存为用户的新公钥。

挑战 A_2 生成长度相等的明文 (M_0, M_1) 并将其发送给 C 。 C 随机选择一个 $\beta \in \{0, 1\}$, 并计算 M_β 的密文 c^* , 然后将 c^* 返回给 A_2 。

阶段 2 A_2 要求 C 进行查询阶段所述的一系列查询, 但 A_2 无法对公钥已被替换的用户执行秘密值查询、部分私钥提取查询和设置私钥查询, 以及对密文 c^* 执行解签密查询。

猜测 A_2 猜测 $\beta^* \in \{0, 1\}$ 。如果 $\beta^* = \beta$ 成立, A_2 获胜, 否则失败。 A_2 获胜的优势被定义为: $A_{\Omega, \text{IND-CLMS-CCA}}(A_2) = |2\Pr[\beta^* = \beta] - 1|$ 。

如果对于选择密文攻击下的任何 A_2 , 在时间 τ 内获胜概率优势满足 $A_{\Omega, \text{IND-CLMS-CCA}}(A_2) \leq \epsilon$, 则方案 Ω 安全, 其中, τ 是多项式运行时间, ϵ 是可忽略的概率优势。

2.3.2 不可伪造性

方案的不可伪造性即无证书多接收者签密在选择明文攻击下的强存在不可伪造性(SUF-CLMS-CPA)。Game3 和 Game4 分别描述对抗敌手 A_1 和 A_2 。

Game3 步骤如下:

初始化 此步骤与 Game1 相同。

哈希查询 此步骤与 Game1 相同。

攻击 A_1 向 C 请求与 Game1 查询阶段相同的查询, C 相应地做出响应。

伪造 A_1 伪造密文 c^* 。如果密文 c^* 可以被任何接收者解密, 则 A_1 获胜, 否则失败。

如果对于选择明文攻击下的任何 A_1 , 在时间 τ 内获胜的概率优势满足 $A_{\Omega, \text{SUF-CLMS-CPA}}(A_1) \leq \epsilon$, 则方案安全, 其中, τ 是多项式运行时间, ϵ 是可忽略的概率优势。

Game4 的证明过程与 Game2 类似。

2.3.3 接收者匿名性

接收者匿名性即无证书多接收者签密在选择密文攻击下的接收者匿名性质的不可区分性(ANONRE-IND-CLMS-CCA)。Game5 和 Game6 分别描述对抗敌手 A_1 和 A_2 。

Game5 步骤如下:

初始化 挑战者 C 运行此算法生成系统公共参数,然后将公共参数发送给 A_1 。 A_1 收到后选择目标身份 $RSU^* = \{I_{D_0}^*, I_{D_1}^*\}$,然后将 RSU^* 发送给 C 。

哈希查询 此步骤与 Game1 相同。

阶段 1 此步骤与 Game1 相同。

挑战 A_1 选择明文 M 和一组 $RSU = \{I_{D_1}, I_{D_2}, \dots, I_{D_n}\}$ 。 C 随机选择 $e \in \{0, 1\}$,并用一组新的 $RSU^{**} = \{I_{D_e}^*, I_{D_2}, \dots, I_{D_n}\}$ 计算密文 c^* ,然后将密文 c^* 返回给 A_1 。

阶段 2 此步骤与 Game1 相同。

猜测 A_1 猜测 $e^* \in \{0, 1\}$ 。如果 $e^* = e$ 成立, A_1 获胜,否则失败。 A_1 获胜的优势被定义为:
 $A_{\Omega, \text{ANONRE-IND-CLMS-CCA}}(A_1) = |2\Pr[e^* = e] - 1|$ 。

如果对于 ANONRE-IND-CLMS-CCA 下的任何 A_1 , 在时间 τ 内获胜概率优势满足 $A_{\Omega, \text{ANONRE-IND-CLMS-CCA}}(A_1) \leq \epsilon$, 则方案安全,其中, τ 是多项式运行时间, ϵ 是可忽略的概率优势。

Game6 步骤如下:

初始化 挑战者 C 运行此算法生成公共参数,然后将公共参数发送给 A_2 。 A_2 选择目标身份 $RSU^* = \{I_{D_0}^*, I_{D_1}^*\}$,然后将 RSU^* 发送给 C 。

哈希查询 此步骤与 Game1 相同。

阶段 1 此步骤与 Game2 相同。

挑战 A_2 选择一个明文 M 和一组目标标识 $RSU = \{I_{D_1}, I_{D_2}, \dots, I_{D_n}\}$,然后发送给 C 。 C 随机选择 $e \in \{0, 1\}$ 并用一组新的目标标识 $RSU^{**} = \{I_{D_e}^*, I_{D_2}, \dots, I_{D_n}\}$ 计算密文 c^* ,然后将密文 c^* 返回给 A_2 。

阶段 2 此步骤与 Game2 相同。

猜测 A_2 猜测 $e^* \in \{0, 1\}$ 。如果 $e^* = e$ 成立, A_2 获胜,否则失败。 A_2 获胜优势被定义为:
 $A_{\Omega, \text{ANONRE-IND-CLMS-CCA}}(A_2) = |2\Pr[e^* = e] - 1|$ 。

如果对于 ANONRE-IND-CLMS-CCA 下的任何 A_2 , 在时间 τ 内获胜优势满足 $A_{\Omega, \text{ANONRE-IND-CLMS-CCA}}(A_2) \leq \epsilon$, 则方案安全,其中, τ 是多项式运行时间, ϵ 是可忽略的概率优势。

2.3.4 发送者匿名性

发送者匿名性即无证书多接收者签密在选择密文攻击下的匿名发送者的不可区分性(ANONSE-IND-CLMS-CCA)。Game7 和 Game8 分别描述对抗敌手 A_1 和 A_2 。

Game7 是挑战者 C 和敌手 A_1 之间的互动,步骤如下:

初始化 此步骤与 Game5 相同。

哈希查询 此步骤与 Game1 相同。

阶段 1 此步骤与 Game1 相同。

挑战 A_1 选择明文 M 和一组 $RSU = \{I_{D_1}, I_{D_2}, \dots, I_{D_n}\}$,然后发送给 C 。 C 随机选择 $e \in \{0, 1\}$,并用一组新的 $RSU^{**} = \{I_{D_e}^*, I_{D_2}, \dots, I_{D_n}\}$ 计算密文 c^* ,然后将密文 c^* 返回给 A_1 。

阶段 2 此步骤与 Game1 相同。

猜测 A_1 猜测 $e^* \in \{0, 1\}$ 。如果 $e^* = e$ 成立, A_1 获胜,否则失败。 A_1 成功的优势定义为:
 $A_{\Omega, \text{ANONSE-IND-CLMS-CCA}}(A_1) = |2\Pr[e^* = e] - 1|$ 。

如果对于 ANONSE-IND-CLMS-CCA 下的任何 A_1 , 在时间 τ 内赢得第一场比赛的概率优势满足 $A_{\Omega, \text{ANONSE-IND-CLMS-CCA}}(A_1) \leq \epsilon$, 则方案安全,其中, τ 是多项式运行时间, ϵ 是可忽略的概率优势。

Game8 是挑战者 C 和敌手 A_2 之间的互动,步骤如下:

初始化 此步骤与 Game6 相同。

哈希查询 此步骤与 Game1 相同。

阶段 1 此步骤与 Game2 相同。

挑战 A_2 选择明文 M 和一组目标标识 $RSU = \{I_{D_1}, I_{D_2}, \dots, I_{D_n}\}$,然后发送给 C 。 C 随机选择 $e \in \{0, 1\}$,并用一组新的目标标识 $RSU^{**} = \{I_{D_e}^*, I_{D_2}, \dots, I_{D_n}\}$ 计算密文 c^* 并返回给 A_2 。

阶段 2 此步骤与 Game2 相同。

猜测 A_2 猜测 $e^* \in \{0, 1\}$ 。如果 $e^* = e$ 成立, A_2 获胜,否则失败。 A_2 获胜的优势被定义为:
 $A_{\Omega, \text{ANONSE-IND-CLMS-CCA}}(A_2) = |2\Pr[e^* = e] - 1|$ 。

如果对于 ANONSE-IND-CLMS-CCA 下的任何 A_2 , 在时间 τ 内获胜的概率优势满足 $A_{\Omega, \text{ANONSE-IND-CLMS-CCA}}(A_2) \leq \epsilon$, 则方案安全,其中, τ 是多项式运行时间, ϵ 是可忽略的概率优势。

2.4 方案构造

1) 系统初始化。

G 是椭圆曲线上阶为 q 的加法循环群, P 是 G 的生成元。TA 随机选取 $s_1 \in \mathbb{Z}_q^*$ 作为其主密钥,并计算 $T_{\text{pub}} = s_1 P$ 。KGC 选择 $s_2 \in \mathbb{Z}_q^*$ 作为其主密钥,并计算 $K_{\text{pub}} = s_2 P$ 。定义 6 个密码学哈希函数:
 $H_0: \{0, 1\}^* \rightarrow \mathbb{Z}_q^*$, $H_1: \{0, 1\}^* \times \mathbb{Z}_q^* \times G_q \rightarrow \mathbb{Z}_q^*$,
 $H_2: \{0, 1\}^* \rightarrow G_q$, $H_3: G_q \times G_q \rightarrow \mathbb{Z}_q^*$, $H_4: \mathbb{Z}_q^* \times G_q \rightarrow \mathbb{Z}_q^*$, $H_5: \{0, 1\}^* \times G_q \times \mathbb{Z}_q^* \times \mathbb{Z}_q^* \times \dots \times \mathbb{Z}_q^* \rightarrow \mathbb{Z}_q^*$ 。

TA 选择对称加密函数 E_k 和相应的解密函数 D_k , 其中, k 是对称密钥。TA 和 KGC 公开参数为:
 $\{q, P, T_{\text{pub}}, K_{\text{pub}}, G_q, E_k, D_k, H_0, H_1, H_2, H_3, H_4, H_5\}$ 。

2) 车辆注册。

车辆将自己的真实身份信息 R_{ID_i} 发送给 TA。TA 首先检查真实的数据列表 UL, 如果该真实身份存在, 则 TA 为每辆车配备一个 TPD, 其中存储 R_{ID_i} 、系统私钥及参数, 随后随机选择 $t \in \mathbb{Z}_q^*$, 并计算长期伪身份 $Q_{ID_i} = tH_0(R_{ID_i})$ 存储于 TPD 之中, 用于隐藏车辆的真实身份, 并将长期伪身份 Q_{ID_i} 上传至 UL。只有在出现冲突时, TA 才能透露其真实身份。

3) 密钥生成。

车辆或 RSU 随机选择 $x_i \in \mathbb{Z}_q^*$ 作为其秘密值, 并计算公钥 $P_{K_i} = x_i P$ 。车辆发送 Q_{ID_i} 请求部分私钥时, KGC 检查 TA 通过安全通道发送的撤销列表来确认车辆是否被撤销, 若已经被撤销, KGC 将不再为车辆生成部分私钥, 若未被撤销, 计算 $r_i = H_1(Q_{ID_i}, P_{K_i}, s_2)$, KGC 为车辆或 RSU 生成部分私钥 $y_i = s_2 r_i$, $D_i = r_i^{-1} P$, 并将 y_i 和 D_i 通过安全信道发送给车辆或 RSU。车辆或 RSU 收到 y_i 和 D_i 后, 验证等式:

$$y_i D_i = K_{pub} \quad (1)$$

正确性证明如下:

$$y_i D_i = s_2 r_i r_i^{-1} P = s_2 P = K_{pub}$$

证毕。

若式(1)成立, 令 $S_{K_i} = (x_i, y_i)$ 为车辆或 RSU 的完整私钥, 否则算法终止。

4) 短期伪身份生成。

当车辆靠近 RSU 时, 车辆需要生成一个短期伪身份。车辆在 TPD 中输入车辆的长期伪身份 Q_{ID_i} , 随后进行验证, 验证通过则进行车辆短期伪身份的建立。TPD 随机选择 $\beta_i \in \mathbb{Z}_q^*$ 并计算 $P_{ID_i,1} = \beta_i P$, $P_{ID_i,2} = R_{ID_i} \oplus H_2(\beta T_{pub} \| Q_{ID_i} \| T_i)$ 。最后车辆获得短期伪身份 $P_{ID_i} = (P_{ID_i,1}, P_{ID_i,2}, T_i)$ 。

5) 签密。

为了确保消息的完整性和认证, 方案中设定接收者身份为 $RSU = \{I_{D_1}, I_{D_2}, \dots, I_{D_n}\}$, 车辆的公私钥分别为 P_{K_v} 和 $S_{K_v} = (x_v, y_v)$ 对消息 M 进行签密:

(1) 随机选择 $w \in \mathbb{Z}_q^*$, 计算 $K = wP$, $W_i =$

$$\begin{aligned} R_{ID_i} &= P_{ID_i,2} \oplus H_2(s_1 P_{ID_i,1} \| Q_{ID_i} \| T_i) = R_{ID_i} \oplus H_2(s_1 P_{ID_i,1} \| Q_{ID_i} \| T_i) \oplus H_2(\beta T_{pub} \| Q_{ID_i} \| T_i) = \\ &= R_{ID_i} \oplus H_2(s_1 P_{ID_i,1} \| Q_{ID_i} \| T_i) \oplus H_2(s_1 \beta P \| Q_{ID_i} \| T_i) = \\ &= R_{ID_i} \oplus H_2(s_1 \beta P \| Q_{ID_i} \| T_i) \oplus H_2(s_1 \beta P \| Q_{ID_i} \| T_i) = R_{ID_i} \end{aligned}$$

证毕。

3 安全性证明

定理 1 如果对于 IND-CLMS-CCA 下的任何

$$wy_v P_{K_i}, \alpha_i = H_3(K, W_i)。$$

(2) 随机选择 $\theta \in \mathbb{Z}_q^*$ 并构造 n 阶多项式:

$$f(\xi) = \prod_{i=1}^n (\xi - \alpha_i) + \theta \pmod{q} = a_0 + a_1 \xi + \dots + a_{n-1} \xi^{n-1} + \xi^n, \text{ 其中, } a_i \in \mathbb{Z}_q^*。$$

(3) 计算 $k = H_4(\theta, W)$, $J = E_k(M)$, $h = H_5(P_{ID_i}, M, \theta, W, T_i, a_0, a_1, \dots, a_{n-1})$, 随后, 车辆生成时间戳 T_i 。

(4) 构造密文 $c = (J, W, h, T_i, a_0, a_1, \dots, a_{n-1})$ 并向所有 RSU 发送。

6) 验证。

该阶段由 RSU 执行, 当接收到来自车辆的可疑消息时, 首先检查时间戳是否新鲜, 即判断当前时间值减去接收到的时间戳的时间值是否在误差范围内, 若在误差范围内则有效, 否则为无效的时间戳, 说明该消息为篡改后的虚假消息。

7) 解签密。

(1) 计算:

$$W = y_i x_i K \quad (2)$$

解签密算法正确性证明如下:

$$W_i = y_i x_i K = y_i x_i (wP) =$$

$$wy_i (x_i P) = wy_i P_{K_i} = W_i$$

证毕。

(2) 计算 $\alpha_i = H_3(K, W_i)$ 。利用密文 c 中包含的系数 $(a_0, a_1, \dots, a_{n-1})$ 恢复 n 阶多项式: $f(\xi) = a_0 + a_1 \xi + \dots + a_{n-1} \xi^{n-1} + \xi^n$, 然后计算 $\theta = f(\alpha_i) \pmod{q}$ 和 $k = H_4(\theta, W)$ 。

(3) 计算 $M' = D_k(J)$ 。

(4) 计算 $h' = H_5(P'_{ID_i}, M', \theta, W, a_0, a_1, \dots, a_{n-1})$, 并验证 $h = h'$, 若相等则表明接收者解密成功。

8) 追踪与撤销。

一旦 RSU 发现任何车辆发送了虚假信息, TA 即通过计算式(3)来追踪车辆的真实身份, 并在 UL 中删除该车辆的真实身份, 从而更新 UL。

$$R_{ID_i} = P_{ID_i,2} \oplus H_2(s_1 P_{ID_i,1} \| Q_{ID_i} \| T_i) \quad (3)$$

正确性证明如下:

A_1 , 以不可忽略的优势 ϵ 在时间 τ 内赢得游戏, A_1 最多可以进行 q_i 次 $H_i (i = 0, 1, 2, 3, 4, 5)$ 哈希查询、 q_u 次创建用户询问、 q_p 次公钥查询、 q_r 次公钥替换查询、 q_s 次签密询问和 q_d 次解签密查询, 挑战

者 C 可以通过在概率多项式时间 $\tau^* \leq \tau + (2q_u + q_d)T_{PM} + T_1$ 内以不可忽略优势:

$$A \geq \left(1 - \frac{q_0 q_u}{q}\right) \left(1 - \frac{q_1^2}{q}\right) \left(1 - \frac{q_2^2}{q}\right) \left(1 - \frac{q_3^2}{q}\right) \times \\ \left(1 - \frac{q_4^2}{q}\right) \left(1 - \frac{q_5^2}{q}\right) \left(1 - \frac{q_d}{q}\right) \epsilon$$

与敌手 A_1 交互来解决 CDH, 其中, T_{PM} 是用于执行椭圆曲线标量点乘法运算的时间, T_1 是用于执行模逆运算的时间。

证明 若 A_1 可以在多项式时间 τ 内以不可忽略的优势 ϵ 赢得游戏, 那么一定有一个挑战者 C 可以通过与 A_1 交互来解决 CDH 问题, 也就是说对于给定的 (P, aP, bP) , C 将输出 abP 。

初始化 挑战者 C 初始化系统公共参数: $\{q, P, T_{pub}, K_{pub} = aP, G_q, E_k, D_k, H_0, H_1, H_2, H_3, H_4, H_5\}$, 然后将公共参数返回给 A_1 。 A_1 收到后选择一组 $RSU^* = \{I_{D_1}^*, I_{D_2}^*, \dots, I_{D_n}^*\}$ 并将 RSU^* 发送给 C 。

哈希查询 A_1 向 C 请求以下一系列哈希查询, C 相应地做出响应:

1) H_0 查询。输入元组 I_{D_j} 向 C 请求 H_0 查询。 C 通过列表元组 $L_0 = (I_{D_j}, H_0(I_{D_j}))$ 对 A_1 和 C 的问答进行记录, 收到查询后, C 搜索列表 L_0 并响应 $H_0(I_{D_j})$ 到 A_1 , 否则 C 选择 $H_0(I_{D_j}) \in \mathbb{Z}_q^*$ 并发送给 A_1 , 然后将元组 $(I_{D_j}, H_0(I_{D_j}))$ 插入 L_0 。

2) H_1 查询。输入元组 $(Q_{ID_j}, P_{K_j}, s_{2,j})$ 向 C 请求 H_1 查询。 C 通过列表元组 $(Q_{ID_j}, P_{K_j}, s_{2,j})$ 对 A_1 和 C 的问答进行记录, 收到查询后, C 查询列表 L_1 , 若 $(Q_{ID_j}, P_{K_j}, s_{2,j}, r_j)$ 在列表 L_1 中, 则对 A_1 响应 r_j , 否则 C 选择 $r_j \in \mathbb{Z}_q^*$ 并对 A_1 响应 r_j , 然后将元组 $(Q_{ID_j}, P_{K_j}, s_{2,j}, r_j)$ 插入 L_1 。

3) H_2 查询。输入元组 (T_{pub}, Q_{ID_j}, T_i) 向 C 请求 H_2 查询。 C 通过列表元组 $L_2 = (T_{pub}, Q_{ID_j}, T_i, u_j)$ 对 A_1 和 C 的问答进行记录, 收到查询后, C 查询列表 L_2 , 若 $(T_{pub}, Q_{ID_j}, T_i, u_j)$ 在列表 L_2 中, 则对 A_1 响应 u_j , 否则 C 选择 $u_j \in \mathbb{Z}_q^*$ 并对 A_1 响应 u_j , 然后将元组 $(T_{pub}, Q_{ID_j}, T_i, u_j)$ 插入 L_2 。

4) H_3 查询。输入元组 (P_{ID_j}, K_j, W_j) 向 C 请求 H_3 查询。 C 通过列表元组 $L_3 = (P_{ID_j}, K_j, W_j, \alpha_j)$ 对 A_1 和 C 的问答进行记录, 收到查询后, C 查询列表 L_3 , 若 $(P_{ID_j}, K_j, W_j, \alpha_j)$ 在列表 L_3 中, 则对 A_1 响应 α_j , 否则 C 选择 $\alpha_j \in \mathbb{Z}_q^*$ 并对 A_1 响应 α_j , 然后将元组 $(P_{ID_j}, K_j, W_j, \alpha_j)$ 插入 L_3 。

5) H_4 查询。输入元组 $(P_{ID_j}, \theta_j, W_j)$ 向 C 请

求 H_4 查询。 C 通过列表元组 $L_4 = (P_{ID_j}, \theta_j, W_j, k_j)$ 对 A_1 和 C 的问答进行记录, 收到查询后, C 查询列表 L_4 , 若 $(P_{ID_j}, \theta_j, W_j)$ 在列表 L_4 中, 则对 A_1 响应 k_j , 否则 C 选择 $k_j \in \mathbb{Z}_q^*$ 并对 A_1 响应 k_j , 然后将元组 $(P_{ID_j}, \theta_j, W_j, k_j)$ 插入 L_4 。

6) H_5 查询。输入元组 $(P_{ID_j}, M_j, \theta_j, W_j, T_j, a_{j,0}, a_{j,1}, \dots, a_{j,n-1})$ 向 C 请求 H_5 查询。 C 通过列表元组 $L_5 = (P_{ID_j}, M_j, \theta_j, W_j, T_j, a_{j,0}, a_{j,1}, \dots, a_{j,n-1}, h_j)$ 对 A_1 和 C 的问答进行记录, 收到查询后, C 查询列表 L_5 , 若 $(P_{ID_j}, M_j, \theta_j, W_j, T_j, a_{j,0}, a_{j,1}, \dots, a_{j,n-1}, h_j)$ 在列表 L_5 中, 则对 A_1 响应 h_j , 否则 C 选择 $h_j \in \mathbb{Z}_q^*$ 并对 A_1 响应 h_j , 然后将元组 $(P_{ID_j}, M_j, \theta_j, W_j, T_j, a_{j,0}, a_{j,1}, \dots, a_{j,n-1}, h_j)$ 插入 L_5 。

阶段 1 C 询问一系列问题, C 相应地做出回应:

1) 创建用户查询。 A_1 向 C 请求查询, 收到查询后, C 检查元组 $(Q_{ID_j}, (x_j, y_j), P_{K_j})$ 是否在列 L_g 中。如果是, C 保留该元组, 否则 C 将执行以下操作:

(1) 如果 $Q_{ID_j} = Q_{ID_j}$, C 选择 $x_j, y_j, r_j \in \mathbb{Z}_q^*$, 设置 $P_{K_j} = x_j P$, $S_{K_j} = (x_j, \perp)$, 并更新列表 L_g 中的元组 $(Q_{ID_j}, (x_j, \perp), P_{K_j})$ 和列表 L_1 中的元组 $(Q_{ID_j}, P_{K_j}, s_{2,j}, r_j)$ 。

(2) 如果 $Q_{ID_j} \neq Q_{ID_j}$, C 选择 $x_j, y_j, r_j \in \mathbb{Z}_q^*$, 设置 $P_{K_j} = x_j P$, $S_{K_j} = (x_j, y_j)$, 并更新列表 L_g 中的元组 $(Q_{ID_j}, (x_j, y_j), P_{K_j})$ 和列表 L_1 中的元组 $(Q_{ID_j}, P_{K_j}, s_{2,j}, r_j)$ 。

2) 设置秘密值询问。 A_1 向 C 请求对 Q_{ID_j} 的秘密值查询。 C 通过列表元组 $L_g = (Q_{ID_j}, (x_j, y_j), P_{K_j})$ 对 A_1 和 C 的问答进行记录, 收到查询后 C 检查元组 $(Q_{ID_j}, (x_j, y_j), P_{K_j})$ 是否在列表 L_g 中。如果是, C 将 x_j 返回给 A_1 , 否则 C 请求创建用户查询以获得元组 $(Q_{ID_j}, (x_j, y_j), P_{K_j})$, 然后将 x_j 返回给 A_1 。

3) 部分私钥提取查询。 A_1 以 Q_{ID_j} 对此预言机进行查询。在接收到查询后, C 按照如下方式进行响应:

(1) 如果 $Q_{ID_j} = Q_{ID_j}$, 则 C 停止协议执行。

(2) 如果 $Q_{ID_j} \neq Q_{ID_j}$, C 检查在 L_g 中是否存在元组 $(Q_{ID_j}, (x_j, y_j), P_{K_j})$ 。如果是, C 将 y_j 返回给 A_1 , 否则 C 请求创建用户查询以获得元组 $(Q_{ID_j}, (x_j, y_j), P_{K_j})$, 然后将 y_j 返回给 A_1 。

4) 设置公钥查询。 A_1 要求 C 对身份 Q_{ID_j} 进行设置公钥查询。收到查询后, C 检查元组 $(Q_{ID_j},$

$(x_j, y_j), P_{K_j}$ 是否在 L_g 中。如果是, C 将 P_{K_j} 返回给 A_1 , 否则 C 请求创建用户查询以获得元组 $(Q_{ID_j}, (x_j, y_j), P_{K_j})$, 然后将 P_{K_j} 返回给 A_1 。

5) 设置私钥查询。 A_1 要求 C 对身份 Q_{ID_j} 进行设置私钥查询。在接收到查询后, C 按照如下方式进行响应:

(1) 如果 $Q_{ID_i} = Q_{ID_j}$, 则 C 停止协议执行。

(2) 如果 $Q_{ID_i} \neq Q_{ID_j}$, C 检查在列表 L_g 中是否存在元组 $(Q_{ID_j}, (x_j, y_j), P_{K_j})$ 。如果是, C 向 A_1 返回 $S_{K_j} = (x_j, y_j)$, 否则 C 请求创建用户查询以获得元组 $(Q_{ID_j}, (x_j, y_j), P_{K_j})$, 然后向 A_1 返回 $S_{K_j} = (x_j, y_j)$ 。

6) 公钥替换查询。如果 A_1 要求 C 用选择的 P'_{K_j} 替换 Q_{ID_j} 的 P_{K_j} , 则 C 查找 P_{K_j} 的列表 L_c , 并用 P'_{K_j} 替换 P_{K_j} , 然后更新列表 L_g 中的元组 $(Q_{ID_j}, (\perp, \perp), P_{K_j})$ 。

7) 签密查询。 A_1 选择明文 M , 发送者 P_{ID_j} 和一组接收者 $RSU = \{I_{D_1}, I_{D_2}, \dots, I_{D_n}\}$, 然后发送给 C , 收到查询后, C 判断 $(Q_{ID_j}, (x_j, y_j), P_{K_j})$ 是否在列表 L_g 中。如果是 C 执行以下步骤生成密文 c^* , 否则 C 执行创建用户查询以获得私钥 S_{K_v} 和公钥 P_{K_v} , 然后执行下列步骤来生成密文 c^* :

(1) 随机选择 $w \in \mathbb{Z}_q^*$, 计算 $K = wP$, $W_i = w y_v P_{K_i}$, $\alpha_i = H_3(K, W_i)$ 。

(2) 随机选择 $\theta \in \mathbb{Z}_q^*$, 并构造一个 n 阶多项式: $f(\xi) = \prod_{i=1}^n (\xi - \alpha_i) + \theta \pmod{q} = a_0 + a_1 \xi + \dots + a_{n-1} \xi^{n-1} + \xi^n$, 其中, $a_i \in \mathbb{Z}_q^*$ 。

(3) 计算 $k = H_4(\theta, W)$, $J = E_k(M)$ 和 $h = H_5(P_{ID_j}, M, \theta, W, T_i, a_0, a_1, \dots, a_{n-1})$ 。

(4) 随机选择 $t \in \mathbb{Z}_q^*$ 。

(5) 将密文 $c = (J, W, h, T_i, a_0, a_1, \dots, a_{n-1})$ 返回给 A_1 。

8) 解签密查询。构造密文 $c = (J, W, h, T_i, a_0, a_1, \dots, a_{n-1})$ 并选择一组接收者 $RSU = \{I_{D_1}, I_{D_2}, \dots, I_{D_n}\}$, 然后将它们发给 C , 请求解签密查询。收到查询后, C 执行以下操作:

(1) 在列表 L_5 中搜索元组 $(P_{ID_j}, M_j, \theta_j, W_j, T_j, a_{j,0}, a_{j,1}, \dots, a_{j,n-1}, h_j)$, 如果没有这样的元组, C 输出失败并中止游戏, 否则, C 从元组中获得 M 。

(2) 在列表 L_3 中搜索元组 $(P_{ID_j}, K_j, W_j, \alpha_j)$, 并设置多项式: $f(\xi) = \prod_{i=1}^n (\xi - \alpha_i) + \theta \pmod{q} = a_0 + a_1 \xi + \dots + a_{n-1} \xi^{n-1} + \xi^n$, 其中, $a_i \in \mathbb{Z}_q^*$ 。

(3) 在列表 L_1 中搜索元组 $(Q_{ID_j}, P_{K_j}, s_{2,j})$ 。如果没有这样的元组, C 输出失败并中止游戏, 否则 C 从元组 $(Q_{ID_j}, P_{K_j}, s_{2,j}, r_j)$ 中获得 $(Q_{ID_j}, P_{K_j}, s_{2,j})$ 。

(4) 从列表 L_3 中选择元组 $(I_{D_j}, K_j, W_j, \alpha_j)$, 并检查 (K_j, W_j) 是否为元组。

(5) 如果一些 (K_π, W_π) 是 CDH 元组, 计算 $\theta_\pi = f(\alpha_\pi)$ 和 $k_\pi = H_2(\theta_\pi, W_\pi)$, $M'_\pi = D_{k_\pi}(J_\pi)$ 。

(6) 测试方程 $M'_\pi = M_j$ 是否成立, 如果是, C 将 M_j 返回给 A_1 , 否则, 返回失败并中止游戏。

挑战 A_1 选择一对长度相等的明文 (M_0, M_1) , 并将其发送给 C 。在接收到 (M_0, M_1) 后, C 随机选择 $\beta \in \{0, 1\}$, 并用所选择的明文 M_β 计算密文 c^* , 如下所示:

1) 计算 $K = bP_{K_v}$, $W = b(P_{K_i} + K_{pub})$ 和 $\alpha_i = H_3(K, W_i)$ 。

2) 选择 $\theta \in \mathbb{Z}_q^*$ 并构造多项式: $f(\xi) = \prod_{i=1}^n (\xi - \alpha_i) + \theta \pmod{q} = a_0 + a_1 \xi + \dots + a_{n-1} \xi^{n-1} + \xi^n$, 其中, $a_i \in \mathbb{Z}_q^*$ 。

3) 计算 $k = H_4(\theta, W)$, $J = E_k(M)$, $h = H_5(P_{ID_j}, M, \theta, W, T_i, a_0, a_1, \dots, a_{n-1})$ 。

4) 将 $c^* = \langle J, W, h, t, a_0, a_1, \dots, a_{n-1} \rangle$ 返回给 A_1 。

阶段 2 A_1 要求 C 进行阶段 1 所述的一系列查询, 但 A_1 不能对公钥被替换的用户执行秘密值查询、部分私钥提取查询和设置私钥查询, 以及对密文 c^* 执行解签密查询。

猜测 A_1 猜测 $\beta^* \in \{0, 1\}$ 。如果 $\beta^* = \beta$ 成立, A_1 获胜, C 输出 $abP = W_i - K$ 作为 CDH 的解, 否则, C 失败。

通过以上步骤, 如果 A_1 在多项式时间 τ 内, 以不可忽略的优势 ϵ 获胜, 则 C 在概率多项式时间 $\tau^* \leq \tau + (2q_u + q_d)T_{PM} + T_1$ 内以不可忽视的概率优势:

$$A \geq \left(1 - \frac{q_0 q_u}{q}\right) \left(1 - \frac{q_1^2}{q}\right) \left(1 - \frac{q_2^2}{q}\right) \left(1 - \frac{q_3^2}{q}\right) \times \left(1 - \frac{q_4^2}{q}\right) \left(1 - \frac{q_5^2}{q}\right) \left(1 - \frac{q_d}{q}\right) \epsilon$$

解决 CDH 问题。

其他证明过程与上述过程类似, 篇幅所限, 不再赘述。

4 效率分析

4.1 功能分析

为证明本文方案的有效性, 将本文方案与文献[21-25]方案进行发送者匿名性、接收者匿名性、

可追踪、可撤销方面的对比实验,对比结果如表 3 所示。

表 3 功能对比
Table 3 Function comparison

方案	发送者 匿名性	接收者 匿名性	可追踪	可撤销
文献[21]方案	×	✓	×	×
文献[22]方案	✓	✓	✓	×
文献[23]方案	×	✓	✓	×
文献[24]方案	✓	✓	✓	×
文献[25]方案	✓	✓	×	×
本文方案	✓	✓	✓	✓

由表 3 可知:所有的方案都支持接收者匿名,除文献[21,23]方案外,其他方案都支持发送者匿名,但本文方案为车辆生成了短期伪身份与长期伪身份,实现了发送者车辆的强匿名,且文献[21]方案是基于身份的密码体制,存在密钥托管问题;文献[22-24]方案与本文方案都基于无证书密码体制,解决了证书管理和密钥托管问题,但文献[23]方案的理论基础是双线性对,相较于椭圆曲线来说计算较为复杂;文献[22-24]方案与本文方案都实现了发送者的可追踪,但文献[22]方案不满足多接收者签密一对多的通信模式;所有方案中只有本文方案同时实现了可追踪与可撤销;相比较而言,本文方案不仅可满足发送者的强匿名性以及实现接收者匿名,而且与其他方案相比,本文方案在降低用户开销方面具有更好的性能。

4.2 运算成本分析

将本文方案与同为多接收者签密的文献[23-25]方案在签密、解签密时间与总时间方面进行对比。为了便于重新标记每个方案的计算复杂性,定义了一些符号来表示不同计算操作所花费的时间,如表 4 所

示,表格数据来自文献[13]。未列出的其他计算操作花费的时间极少,可以忽略不计。

表 4 符号的定义
Table 4 Symbols definition

符号	含义
T_M	乘法运算的时间
T_I	逆运算操作的时间, $T_I \approx 11.6T_M$
T_E	幂运算的时间, $T_E \approx 240T_M$
T_B	双线性对运算的时间, $T_B \approx 87T_M$
T_{BE}	双线性配对幂运算的时间, $T_{BE} \approx 43.5T_M$
T_H	哈希函数运算的时间, $T_H \approx 29T_M$
T_{PA}	椭圆曲线上点加操作的时间, $T_{PA} \approx 0.12T_M$
T_{PM}	椭圆曲线上乘法运算的时间, $T_{PM} \approx 29T_M$

对文献[23-25]方案与本文方案进行各个阶段和总时间开销的分析,如表 5 所示,其中, n 表示接收者的数量。通过对比可以看出:本文方案签密需要进行 $n+2$ 次椭圆曲线乘运算,解签密只需要进行 1 次椭圆曲线乘运算,总的时间成本约为 $(29n+87)T_M$;文献[23]方案签密需要进行 $2n+3$ 次乘法运算以及 n 个双线性对运算,签密阶段的总成本为 $(2n+3)T_M+nT_B$,解签密需要 1 次乘法运算以及 1 次双线性对运算,解签密阶段的总成本为 T_M+T_B ,总的时间成本约为 $(89n+91)T_M$;文献[24]方案签密需要进行 $2n+1$ 次椭圆乘法运算以及 n 个乘法运算,签密阶段的总成本为 $(2n+1)T_{PM}+nT_M$,解签密需要 4 次椭圆曲线乘法运算,总的时间成本约为 $(59n+145)T_M$;文献[25]方案签密需要进行 $2n+1$ 次椭圆乘法运算,解签密需要 7 次椭圆曲线乘法运算,总的时间成本约为 $(58n+232)T_M$ 。综上可以得出,所有方案的解签密数值是恒定不变的,但 n 是可变的数值,签密时间和总时间随着 n 的增加而增加, n 的系数越小,时间成本就会越小,对比其他方案本,文方案在签密阶段的所需时间和总时间最少。

表 5 计算开销对比

Table 5 Computational cost comparison

方案	签密过程时间	解签密过程时间	总时间
文献[23]方案	$(2n+3)T_M+nT_B \approx (89n+3)T_M$	$T_M+T_B \approx 88T_M$	$(89n+91)T_M$
文献[24]方案	$(2n+1)T_{PM}+nT_M \approx (59n+29)T_M$	$4T_{PM} \approx 116T_M$	$(59n+145)T_M$
文献[25]方案	$(2n+1)T_{PM} \approx (58n+29)T_M$	$7T_{PM} \approx 203T_M$	$(58n+232)T_M$
本文方案	$(n+2)T_{PM} \approx (29n+58)T_M$	$T_{PM} \approx 29T_M$	$(29n+87)T_M$

4.3 实验分析

为了更直观展示本文方案的优势,将其与文献[23-25]方案进行数值模拟实验。使用 Windows 11 和 JDK Visual C++ 6.0 在 AMD Ryzen 5 5600H with Radeon Graphics 处理器和 16 GB RAM 进行了仿真实验。为方便分析,取接

收者的数量范围为[5,50],各方案在签密阶段的计算时间和总时间随接收者数量增加的变化如图 2 和图 3 所示。

图 2 是各方案在签密阶段随着接收者数量的增加,发送者在签密过程所需要的时间开销的对比。从图中可以看出,签密时间随着接收者数量的增多

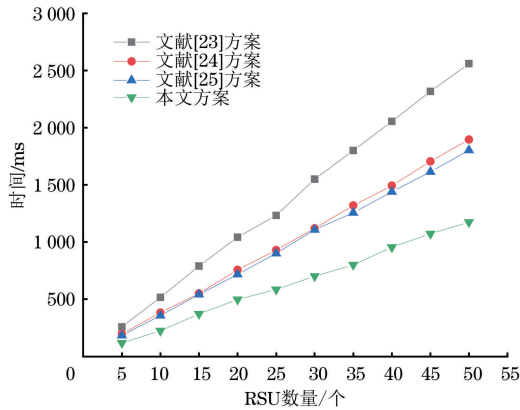


图 2 各方案签密阶段所用的计算时间对比

Fig.2 Comparison of computing time in signcryption phase of each scheme

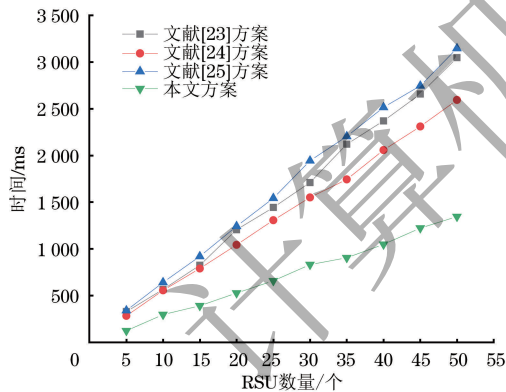


图 3 各方案所用总时间对比

Fig.3 Comparison of total time of each scheme

而增加,文献[24-25]方案在签密阶段的计算时间非常接近,且由于文献[23]方案在签密阶段使用到双线性对运算,运算时间对比其他方案增长幅度更明显,但本文方案的时间明显低于其他方案。

图 3 是各方案在解签密阶段随着接收者数量的增加,所需要的总的时间开销对比。总的时间是签密阶段的计算时间和解签密阶段的计算时间之和。从表 5 中可以看出:所有方案在解签密阶段的计算时间都是恒定的,所需要的时间不会随着接收者数量的增加而增加;文献[23-25]方案以及本文方案的解签密时间依次为 $88T_M$ 、 $116T_M$ 、 $203T_M$ 和 $29T_M$;本文方案的所需时间仍是最少的;各方案总时间是呈现增长的趋势,但本文的总时间开销明显小于其他方案,图 3 也体现了这一点。综上实验结果表明,本文在签密阶段、解签密阶段时间和总时间的比较上均具有一定的优势。

5 结束语

本文提出一种适用于车联网的多接收者匿名签密方案,实现了车辆和 RSU 的同时匿名,从而保护

双方的隐私,同时保持消息的身份验证、完整性和机密性。此外,本文方案提供了有条件的隐私保护,允许可信中心追踪和撤销恶意车辆,同时保护合法车辆的真实身份。本文方案安全高效且易于实现,与现有的多接收者方案相比有更高的效率。在未来的工作中,将继续提高车联网中多接收者签密方案的效率,同时将结合更安全和轻量级的技术,为车联网构建一个更有效的方案。

参考文献

- [1] IQBAL A, ZUBAIR M, KHAN M A, et al. An efficient and secure certificateless aggregate signature scheme for vehicular ad hoc networks[J]. Future Internet, 2023, 15(8): 266.
- [2] AHMED W, DI W, MUKATHE D. Blockchain-assisted privacy-preserving and context-aware trust management framework for secure communications in VANETs [J]. Sensors, 2023, 23(12): 5766.
- [3] 牛淑芬,闫森,吕锐曦,等. V2V 车联网中隐私保护性异构聚合签密方案[J]. 计算机工程, 2022, 48(9): 20-27, 36.
- [4] NIU S F, YAN S, LÜ R X, et al. Privacy-preserving heterogeneous aggregated signcryption scheme in V2V Internet of vehicles [J]. Computer Engineering, 2022, 48(9): 20-27, 36. (in Chinese)
- [5] XIONG H, CHEN J H, MEI Q, et al. Conditional privacy-preserving authentication protocol with dynamic membership updating for VANETs[J]. IEEE Transactions on Dependable and Secure Computing, 2022, 19(3): 2089-2104.
- [6] WEIL, CUI J, ZHONG H, et al. Proven secure tree-based authenticated key agreement for securing V2V and V2I communications in VANETs [J]. IEEE Transactions on Mobile Computing, 2022, 21(9): 3280-3297.
- [7] GONG Z Y, GAO T H, GUO N. PCAS: cryptanalysis and improvement of pairing-free certificateless aggregate signature scheme with conditional privacy-preserving for VANETs[J]. Ad Hoc Networks, 2023, 144: 103134.
- [8] YAO M T, GAN Q Q, WANG X M, et al. A key-insulated secure multi-server authenticated key agreement protocol for edge computing-based VANETs [J]. Internet of Things, 2023, 21: 100679.
- [9] LI M, ZHU L H, LIN X D. Privacy-preserving traffic monitoring with false report filtering via fog-assisted vehicular crowdsensing[J]. IEEE Transactions on Services Computing, 2021, 14(6): 1902-1913.
- [10] AL-SHAREEDA M A, MANICKAM S, MOHAMMED B A, et al. Provably secure with efficient data sharing scheme for fifth-generation (5G)-enabled vehicular networks without Road-Side Unit (RSU) [J]. Sustainability, 2022, 14(16): 9961.
- [11] 张海波,陈舟,黄宏武,等. VANET 系统中基于中国剩余定理的群内相互认证密钥协商协议[J]. 通信学报, 2022, 43(1): 182-193.
- [12] ZHANG H B, CHEN Z, HUANG H W, et al. Intra-group mutual authentication key agreement protocol based on Chinese remainder theorem in VANET system[J]. Journal on Communications, 2022, 43(1): 182-193. (in Chinese)
- [13] 杨吉云,姚锐冬,周洁,等. 基于切比雪夫混沌映射的车联网高效认证方案[J]. 计算机工程, 2021, 47(10): 34-42, 51.
- [14] YANG J Y, YAO R D, ZHOU J, et al. Efficient authentication scheme based on Chebyshev chaotic map for VANET[J]. Computer Engineering, 2021, 47(10): 34-42, 51. (in Chinese)
- [15] NIU S F, SHAO H L, SU Y, et al. Efficient heterogeneous

- signcryption scheme based on edge computing for industrial Internet of things [J]. *Journal of Systems Architecture*, 2023, 136: 102836.
- [13] LI H X, WU C H, PANG L J. Completely anonymous certificateless multi-receiver signcryption scheme with sender traceability [J]. *Journal of Information Security and Applications*, 2022, 71: 103384.
- [14] MING Y, YU X P, SHEN X Q. Efficient anonymous certificate-based multi-message and multi-receiver signcryption scheme for healthcare Internet of things[J]. *IEEE Access*, 2020, 8: 153561-153576.
- [15] ULLAH I, KHAN M A, KHAN F, et al. An efficient and secure multimessage and multireceiver signcryption scheme for edge-enabled Internet of vehicles[J]. *IEEE Internet of Things Journal*, 2022, 9(4): 2688-2697.
- [16] ZHONG H, ZHANG S, CUI J, et al. Broadcast encryption scheme for V2I communication in VANETs [J]. *IEEE Transactions on Vehicular Technology*, 2022, 71(3): 2749-2760.
- [17] PANG L J, YAN X X, ZHAO H Y, et al. A novel multi-receiver signcryption scheme with complete anonymity[J]. *PLoS One*, 2016, 11(11): e0166173.
- [18] LIANG Y F, LIU Y N, GUPTA B B. PPRP: preserving-privacy route planning scheme in VANETs [J]. *ACM Transactions on Internet Technology*, 2022, 22(4): 1-18.
- [19] TSENG Y M, HUANG Y H, CHANG H J. Privacy-preserving multireceiver ID-based encryption with provable security [J]. *International Journal of Communication Systems*, 2014, 27(7): 1034-1050.
- [20] 王新阳. 基于身份的多签密和多接收者签密算法研究[D]. 南京: 南京邮电大学, 2020.
- WANG X Y. Research on identity-based multi-signcryption and multi-receiver signcryption algorithms [D]. Nanjing: Nanjing University of Posts and Telecommunications, 2020. (in Chinese)
- [21] YANG Y, HE D B, VIJAYAKUMAR P, et al. An efficient identity-based aggregate signcryption scheme with blockchain for IoT-enabled maritime transportation system[J]. *IEEE Transactions on Green Communications and Networking*, 2022, 6(3): 1520-1531.
- [22] LIN X J. On the unforgeability of “privacy-preserving aggregation-authentication scheme for safety warning system in fog-cloud based VANET”[J/OL]. *IEEE Transactions on Information Forensics and Security*, 1[2023-08-10]. <http://doi.org/10.1109/TIFS.2024.3408055>.
- [23] DENG L Z. Anonymous certificateless multi-receiver encryption scheme for smart community management systems[J]. *Soft Computing*, 2020, 24(1): 281-292.
- [24] WANG L P, GUAN Z, CHEN Z, et al. Multi-receiver signcryption scheme with multiple key generation centers through public channel in edge computing [J]. *China Communications*, 2022, 19(4): 177-198.
- [25] 王利朋, 高健博, 李青山, 等. 应用区块链的多接收者多消息签密方案[J]. *软件学报*, 2021, 32(11): 3606-3627. WANG L P, GAO J B, LI Q S, et al. Blockchain-based multi-recipient multi-message signcryption scheme [J]. *Journal of Software*, 2021, 32(11): 3606-3627. (in Chinese)
- [26] LEE D H, KIM W B, SEO D, et al. An efficient public verifiable certificateless multi-receiver signcryption scheme for IoT environments[J]. *IEICE Transactions on Information and Systems*, 2021, E104.D(11): 1869-1879.

编辑 金胡考