面向云服务的安全高效无证书聚合签名车联网认证密钥协商协议

张文芳,雷丽婷,王小敏,王 宇
(西南交通大学信息科学与技术学院,四川成都 610031)

摘 要: 针对目前车联网认证密钥协商协议效率低下以及车辆公私钥频繁更新的问题,提出一个基于无证书聚合签名的车联网匿名认证与密钥协商协议.本方案通过引入临时身份和预签名机制实现对车辆的隐私保护以及匿名认证,同时通过构建临时身份索引数据库,实现可信中心对可疑车辆的事后追查,满足车辆的条件匿名性要求.此外,本方案中车辆的公私钥不随其临时身份动态改变,有效避免了已有方案公私钥频繁更新带来的系统开销.同时,为了提供高效的批量认证,采用无双线性对的聚合签名技术,实现了车辆签名的动态聚合和转发,有效降低了签名传递的通信量和云服务器的验证开销.本文方案在eCK模型和CDH问题假设下被证明是形式化安全的.

关键词: 车联网;云服务;认证密钥协商;无证书;聚合签名;条件匿名性
中图分类号: TP393 **文献标识码:** A **文章编号:** 0372-2112 (2020)09-1814-10
电子学报URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2020.09.020

Secure and Efficient Authentication and Key Agreement Protocol Using Certificateless Aggregate Signature for Cloud Service Oriented VANET

ZHANG Wen-fang, LEI Li-ting, WANG Xiao-min, WANG Yu
(*School of Information Science and Technology, Southwest Jiaotong University, Chengdu, Sichuan* 610031, *China*)

Abstract: In order to solve low efficiency and frequent updates of vehicles' public keys and private keys, a certificateless aggregate signature authentication and key agreement scheme with anonymity in vehicular Ad-Hoc network (VANET) is proposed. In our scheme, by using temporary identity and pre-signature, vehicles' privacy protection and anonymity authentication can be realized. On the other hand, the suspected vehicles can be tracked by the trust authority with the index database of the temporary identity to satisfy conditional anonymity. Meantime, if the temporary identity is changed, it is not necessary to update vehicles' public keys and private keys in this scheme, so the cost of system can be reduced. Moreover, the pairing-free aggregate signature technology is used to improve the efficiency further, which makes the number of signatures and the verification cost of the server be decreased. It is shown that our protocol is provably secure in eCK model under the computational Diffie-Hellman (CDH) assumption.

Key words: vehicular Ad-Hoc network; cloud service; authentication and key agreement; certificateless; aggregate signature; conditional anonymity

1 引言

车联网(Vehicular Ad-hoc NETwork, VANET)作为物联网在交通领域的典型应用,通过实时收集路况信息,为车辆提供碰撞避免、警告提示等安全应用.为了进一步提升驾驶和乘车体验,车联网通过引入云平台,为车内乘客提供导航、多媒体娱乐等多种增值服务.研究并设计安全高效的车联网认证密钥协商协议以实现云服务器和车载单元之间的安全交互是亟待解决的热点问题.

收稿日期:2019-05-17; 修回日期:2019-09-20; 责任编辑:蓝红杰
基金项目:国家自然科学基金(No.61872302);四川省科技计划项目(No.2018GZ0195, No.2019YFH0097, No.2019YFG0502)

目前,针对车联网的认证密钥协商,主要分为以下几类:

(1)基于对称密码体制的认证方案[1~3]:主要采用 Hash 函数、消息认证码(MAC)或对称密码算法等轻量级运算,这类方案无法满足不可否认性要求.

(2)基于公钥基础设施(Public Key Infrastructure, PKI)的认证方案[4,5]:为实现对车辆的隐私保护,此类方案需要为每个 OBU 生成多个匿名公私钥对和证书,并预存于 OBU 防篡改装置,因此存储开销大,也增加了维护和管理复杂度.

(3)基于身份(ID-based)的认证方案[6~8,13~16]:这类方案虽然避免了 PKI 的证书管理问题,但往往需要进行耗时的双线性对运算,并且还引入了密钥托管. 此外,为了实现车辆的匿名认证,需要动态改变车辆的临时身份,导致 OBU 公私钥需要频繁更新,增加了系统开销.

(4)基于无证书密码体制(CL-based)的认证方案[11,12]:该类方案可避免 PKI 的证书管理以及基于身份体制的密钥托管问题,防止密钥生成中心(Key Generation Center,KGC)伪造车辆签名,但仍然无法避免双线性对运算和 OBU 公私钥频繁更新问题. 此外,上述各类方案缺少在高级安全模型下(如 eCK 模型)的形式化证明,难以抵抗临时私钥泄露等攻击.

为了解决上述问题,本文针对云服务下的车联网特殊需求,设计了一个基于无证书聚合签名的匿名认证密钥协商协议. 通过构建临时身份索引数据库实现对可疑车辆的追查,满足条件匿名性要求. 引入无对运算的聚合签名降低了签名验证的通信量和计算量. 通过验证可信中心为 OBU 临时身份签发的秘密签名实现云服务器对车辆的匿名认证,避免了因临时身份改变导致的公私钥频繁更新. 会话密钥由认证双方的临时私钥和长期私钥共同生成,即使临时私钥泄露,会话密钥的安全性仍可保证. 在 CL-eCK 模型和 CDH 困难假设下本方案被证明是形式化安全的.

2　车联网系统模型

本文将车联网(VANET)与云服务器结合,构建了云平台下的车联网系统模型,该系统模型如图 1 所示,主要包括 4 部分:可信任中心(TA)、路边设施单元(RSU)、车载单元(OBU)、云服务器(CS).

(1) 可信任中心(TA)由密钥生成中心(KGC)和注册追查中心(TRA)充当. KGC 负责系统建立以及系统成员部分密钥的生成,TRA 负责对车载单元 OBU 的注册申请颁发授权信息,并对可疑车辆执行事后追查.

(2) 路边设施单元(RSU)部署在道路周围,与车载单元 OBU 之间利用专用短程通讯协议(DSRC)进行无线通信. 在 RSU 区域内的车辆会按需发送服务请求,由诚实且可信的 RSU 动态聚合并转发签名等信息给 CS.

(3) 车载单元(OBU)发送注册申请,预先获得 TRA 对车辆临时身份颁发的授权信息,并利用该授权信息向 CS 发起认证请求,最后 OBU 利用与 CS 建立的会话密钥解密获得 CS 提供的服务.

(4) 云服务器(CS)可以满足用户的导航服务、娱乐服务等众多应用服务需求. 提供服务前,CS 与 OBU 需要执行认证密钥协商协议,确保 CS 只向合法的 OBU 提供保密的私有服务.

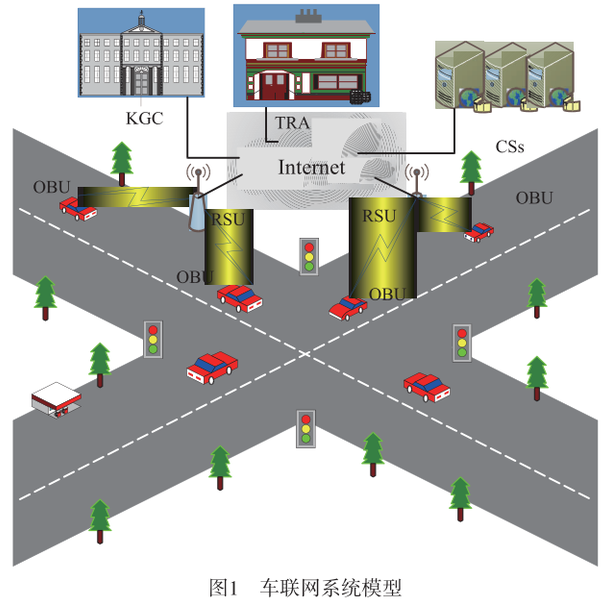


图1　车联网系统模型

3　安全模型

在无证书公钥密码体制中,拥有两种具备不同能力的敌手 A_1 和 A_2. A_1 模拟一个不诚实的用户,而 A_2 是一个半诚实的 KGC.

敌手 $\boldsymbol{A}_1$:此类敌手无法获取系统主密钥及用户部分私钥,但可替换用户的公钥和私有秘密值.

敌手 $\boldsymbol{A}_2$:此类敌手掌握系统主密钥,所以可获取用户的部分私钥,但不能代替用户的公钥和私有秘密值.

Lippold 等[9]利用传统的 eCK 模型扩展成无证书体制下的 CL-eCK 模型. 该模型通过挑战者 C 和敌手 $A \in \{A_1, A_2\}$ 之间的游戏来定义,每个参与者被模拟为多项式时间图灵机,可以并行地执行多项式通信会话, $\prod_{I,J}^{s_{id}}$ 表示参与者 I 和 J 的第 s_{id} 个会话. 无证书的 eCK 模型(CL-eCK)定义可参见文献[9,10].

4　车联网匿名认证与密钥协商方案

本节提出一个针对面向云服务的车联网认证密钥

协商方案. 该方案分为系统建立、注册与授权颁发、认证与密钥协商三个阶段,如图 2 所示.

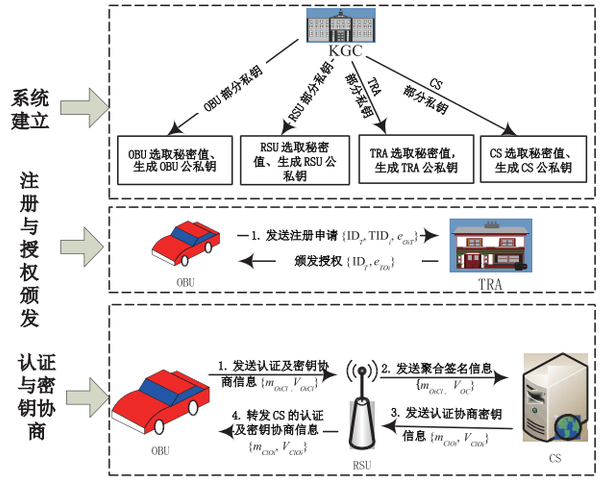


图2 本方案流程示意图

4.1 系统建立

(1)KGC 选取大素数 p 和 q,E/F_p 为有限域 F_p 上的椭圆曲线,选择 E/F_p 上阶为 q 的生成元 P,生成循环群 G;定义抗碰撞的安全散列函数:

$H_1:\{0,1\}^* \times G \rightarrow Z_q^*$,

$H_2:G \rightarrow Z_q^*$,

$H_3:\{0,1\}^* \times \{0,1\}^* \times \{0,1\}^* \times G \rightarrow Z_q^*$,

$H_4:\{0,1\}^* \times \{0,1\}^* \times G \times \{0,1\}^* \times G \times G \times \{0,1\}^* \rightarrow Z_q^*$,

$H_5:\{0,1\}^* \times G \times G \times \{0,1\}^* \rightarrow Z_q^*$;

选取 $x \in Z_q^*$ 作为系统主密钥,计算系统公钥 $P_{\text{pub}} = xP$ 和公开参数 Params $= \{p, q, E/F_q, P, G, H_1, H_2, H_3, H_4, H_5, P_{\text{pub}}\}$.

(2)KGC 为 OBU_i($i = 1,2,\cdots,n$)随机选取 $r_{Oi} \in Z_q^*$,计算 $R_{Oi} = r_{Oi}P$,$h_{Oi} = H_1(\text{ID}_{Oi}, R_{Oi})$,生成部分私钥 $s_{Oi} = r_{Oi} + xh_{Oi}$,对应的部分公钥为 $P_{Oi} = s_{Oi}P$,将(s_{Oi}, R_{Oi})由安全信道发至 OBU_i. OBU_i 收到后,验证公式 $s_{Oi}P = R_{Oi} + h_{Oi}P_{\text{pub}}$ 是否成立;若成立,选取 $r'_{Oi} \in Z_q^*$ 作为秘密值,计算 $R'_{Oi} = r'_{Oi}P$,OBU_i 的最终公私钥分别为(P_{Oi}, R'_{Oi})和(s_{Oi}, r'_{Oi}).

RSU_j($j \in \{1,2,\cdots,m\}$)、CS_l($l \in \{1,2,\cdots,k\}$)、TRA 执行与 OBU_i 相同过程生成对应公私钥,其公私钥分别表示为(P_{Rj}, R'_{Rj})和(s_{Rj}, r'_{Rj})、(P_{Cl}, R'_{Cl})和(s_{Cl}, r'_{Cl})、(P_T, R'_T)和(s_T, r'_T).

4.2 注册与授权颁发

RSU_j 转发 OBU_i 的注册申请至 TRA,TRA 对 OBU_i 进行身份认证并为其临时身份颁发秘密签名.

(1)$\text{OBU}_i \rightarrow$TRA:$\{\text{ID}_T, \text{TID}_i, e_{OiT}\}$

OBU_i 计算 $h'_{Oi} = H_1(\text{ID}_{Oi}, R'_{Oi})$,随机选取 $r_{OiT} \in Z_q^*$,得到临时身份 $\text{TID}_i = r_{OiT}(R'_{Oi} + h'_{Oi}P_{Oi})$,计算 $h'_T = H_1(\text{ID}_T, R'_T)$ 及与 TRA 的共享密钥 $K_{OiT} = H_2(r_{OiT}(r'_{Oi} + s_{Oi}h'_{Oi})(R'_T + h'_T R_T))$,产生消息 $m_{OiT} = \{\text{ID}_{Oi}, \text{ID}_T, r_{OiT}, T_{OiT}\}$. 其中,$\text{ID}_{Oi}$ 是 OBU_i 的真实身份,ID_T 为 TRA 的身份,T_{OiT} 为时戳. OBU_i 对 m_{OiT} 加密生成 $e_{OiT} = E_{K_{OiT}}(m_{OiT})$,并将$\{\text{ID}_T, \text{TID}_i, e_{OiT}\}$发给 TRA.

(2)TRA$\rightarrow \text{OBU}_i$:$\{\text{ID}_T, e_{OiT}\}$

TRA 计算 $h'_T = H_1(\text{ID}_T, R'_T)$ 及共享密钥 $K_{TOi} = H_2(\text{TID}_i(r'_T + s_T h'_T)) = K_{OiT}$,利用 K_{TOi} 解密 e_{OiT},检查时间戳 T_{OiT} 是否有效. 若有效,则计算 $h'_{Oi} = H_1(\text{ID}_{Oi}, R'_{Oi})$,并验证 $r_{OiT}(R'_{Oi} + h'_{Oi}P_{Oi}) \stackrel{?}{=} \text{TID}_i$,如果验证不通过,则终止协议;否则,将$\{\text{TID}_i, \text{ID}_{Oi}\}$保存于临时身份索引数据库 L_{OBU} 中,用于事后追踪,并生成消息 $m_{TOi} = \{\text{ID}_T, \text{TID}_i, T_{\text{end}i}\}$. 其中 $T_{\text{end}i}$ 为临时身份有效期,当 $T_{\text{end}i}$ 到期时,OBU_i 需再次申请身份授权,同时 TRA 更新 L_{OBU}.

随后 TRA 随机选取 $r_{TOi} \in Z_q^*$,计算 $R_{TOi} = r_{TOi}P$ 和 $h_{TOi} = H_3(m_{TOi}, R_{TOi})$,生成签名 $V_{TOi} = (r'_T + h'_T s_T)h_{TOi} + r_{TOi}$,并产生消息 $m'_{TOi} = \{m_{TOi}, V_{TOi}, R_{TOi}, T_{TOi}\}$,其中 T_{TOi} 为时戳. TRA 对 m'_{TOi} 加密得到 $e_{TOi} = E_{K_{TOi}}(m'_{TOi})$,将$\{\text{ID}_T, e_{TOi}\}$发给 OBU_i.

(3) OBU_i 利用 K_{OiT} 解密 e_{TOi},然后计算 $h_{TOi} = H_3(m_{TOi}, R_{TOi})$,验证时戳 T_{TOi} 和签名 $V_{TOi}P \stackrel{?}{=} (R'_T + h'_T P_T)h_{TOi} + R_{TOi}$ 有效性. 若验证通过,利用 TRA 的签名向 CS_l 请求认证并申请服务;否则,终止协议.

在上述密钥协商过程中,共享密钥 K_{OiT} 和 K_{TOi} 是由 CS 和 TRA 分别计算得到的,由 5.1 节正确性分析第(3)点易知 $K_{OiT} = K_{TOi}$. 共享密钥的生成同时用到了长期私钥和临时私钥,因此可有效抵抗临时私钥泄露攻击,证明详见 5.2 节.

注册与授权颁发协议过程如图 3 所示.

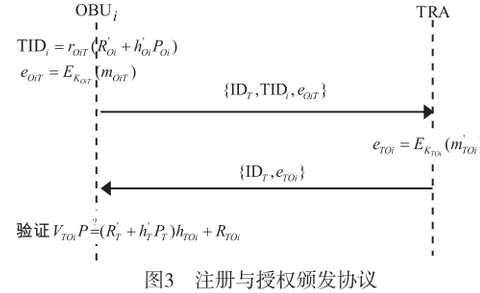


图3 注册与授权颁发协议

4.3 认证与密钥协商

当 OBU_i 向云服务器 CS_l 发起服务请求时,RSU_j 对 OBU_i($i \in \{1,2,\cdots,n\}$)的认证信息进行聚合并转发,实现 OBU_i 与 CS_l 之间高效的认证与会话密钥协商,该过程如图 4 所示,详细步骤如下.

(1)$\text{OBU}_i \rightarrow \text{RSU}_j$:$\{m_{OiCl}, V_{OiCl}\}$($i \in \{1,2,\cdots,n\}$)

OBU_i 随机选取 $r_{OiCl} \in Z_q^*$,计算 $R_{ClOi} = r_{ClOi}(r'_{Cl} +$

$s_{Cl}h'_{Cl})P$,产生消息 $m_{OiCl}=\{\mathrm{ID}_{Cl},m_{TOi},R_{TOi},R_{OiCl},T_{OiRj}\}$,其中 T_{OiRj}是时戳,ID_{Cl}为 CS_l的身份. OBU_i随后计算 $h_{OiCl}=H_4(m_{OiCl})$ 和 $V_{OiCl}=V_{TOi}+r_{OiCl}(r'_{Oi}+s_{Oi}h'_{Oi})h_{OiCl}$,并将 $\{m_{OiCl},V_{OiCl}\}$发至 RSU_j.

(2)$\mathrm{RSU}_j\rightarrow\mathrm{CS}_l$:$\{m_{OiCl},V_{OC},T_{RiCl}\}$ $(i\in\{1,2,\cdots,n\})$

当 RSU_j同时收到大量车辆的云服务请求时,首先验证 T_{OiRj}的新鲜性,若新鲜则对车辆的签名进行聚合,即 $V_{OC}=\sum_{i=1}^{n}V_{OiCl}$,然后将处理后的信息$\{m_{OiCl},V_{OC},T_{RjCl}\}$$(i\in\{1,2,\cdots,n\})$转发至对应的 CS_l.

(3)$\mathrm{CS}_l\rightarrow\mathrm{RSU}_j$:$\{m_{ClOi},V_{ClOi}\}$$(i\in\{1,2,\cdots,n\})$

CS_l首先验证 T_{RjCl}和 T_{endi}是否有效,若有效,计算$h'_T=H_1(\mathrm{ID}_T,R'_T)$,$h_{TOi}=H_3(m_{TOi},R_{TOi})$,$h_{OiCl}=H_4(m_{OiCl})$,$R_{TO}=\sum_{i=1}^{n}R_{TOi}$,然后验证聚合签名 $V_{OC}P\overset{?}{=}(R'_T+h'_TP_T)\sum_{i=1}^{n}h_{TOi}+R_{TO}+\sum_{i=1}^{n}R_{OiCl}h_{OiCl}$. 若验证通过,为每个 OBU_i随机选取 $r_{ClOi}\in Z_q^*$,计算 $R_{ClOi}=r_{ClOi}(r'_{Cl}+s_{Cl}h'_{Cl})P$ 和会话密钥$\mathrm{SK}_{ClOi}=H_2(r_{ClOi}(r'_{Cl}+s_{Cl}h'_{Cl})R_{OiCl})$;随后产生消息 $m_{ClOi}=\{\mathrm{ID}_{Cl},\mathrm{TID}_i,R_{ClOi},T_{ClOi}\}$,计算 $h_{ClOi}=H_5(m_{ClOi})$,$V_{ClOi}=r'_{ClOi}(r'_{Cl}+s_{Cl}h'_{Cl})+(r'_{Cl}+s_{Cl}h'_{Cl})h_{ClOi}$,并将$\{m_{ClOi},V_{ClOi}\}$ $(i\in\{1,2,\cdots,n\})$发送至 RSU_j.

(4)$\mathrm{RSU}_j\rightarrow\mathrm{OBU}_i$:$\{m_{ClOi},V_{ClOi}\}$$(i\in\{1,2,\cdots,n\})$

OBU_i验证 T_{ClOi}是否有效,若有效,计算 $h_{ClOi}=H_5(m_{ClOi})$和 $h'_{Cl}=H_1(\mathrm{ID}_{Cl},R'_{Cl})$,并验证等式 $V_{ClOi}P=R_{ClOi}+(R'_{Cl}+P_{Cl}h'_{Cl})h_{ClOi}$是否成立,若成立,则认证成功,于是计算会话密钥$\mathrm{SK}_{OiCl}=H_2(r_{OiCl}(r'_{Oi}+s_{Oi}h'_{Oi})R_{ClOi})$;否则,认证失败.

经过上述过程,云服务器 CS_l即可使用该会话密钥 SK_{OiCl}对 OBU_i申请的服务进行加密并发送至对应的车辆,保证该服务只能被授权车辆解密获取.

在本节的 OBU 认证过程中,OBU 签名 V_{OiCl}是对 TRA 签名 V_{TOi}进行随机化处理后得到的,由于 V_{TOi}只被 OBU_i所知,所以只有合法的 OBU_i才能生成有效的 V_{OiCl}. 由 5.1 节正确性分析可知,由 V_{OiCl}聚合后得到的签名 V_{OC}只需使用 TRA 的公钥(P_T,R'_T)进行验证,即可实现对 OBU 的匿名认证. 上述方法解除了车辆临时身份与 OBU 公私钥之间的绑定关系,避免了现有方案因车辆临时身份改变导致其公私钥频繁更新的问题. 此外,引入无对运算的聚合签名进一步降低了通信量和验证开销.

在密钥协商过程中,会话密钥 SK_{OiCl}和 SK_{ClOi}是由 OBU 和 CS 分别计算得到的,由 5.1 节正确性分析易知 $\mathrm{SK}_{OiCl}=\mathrm{SK}_{ClOi}$. 由于会话密钥的生成用到了实体的长期私钥和临时私钥,因此可有效抵抗临时私钥泄露攻击,证明详见 5.2 节.

认证密钥协商协议过程如图 4 所示.

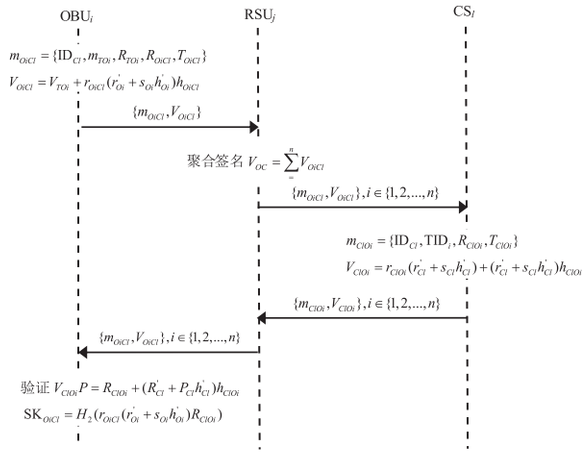


图4　认证与密钥协商协议

4.4　事后追查

注册与授权颁发过程中,TRA 会将注册时验证通过的 OBU 临时身份 R_{Oi}与其真实身份 ID_{Oi}进行绑定,并将$\{R_{Oi},\mathrm{ID}_{Oi}\}$以二元组的形式存储在临时身份索引数据库 L_{OBU}中. 当某车辆存在可疑或恶意行为需要追查其真实身份时,CS 将该车辆的服务申请消息$\{m_{OiCl},V_{OiCl}\}$发送至 TRA. TRA 从 m_{OiCl}中解析出该 OBU 的临时身份 TID_i,随后在 L_{OBU}中检索其对应的真实身份 ID_{Oi},完成对可疑车辆的事后追查. 系统可根据实际需要设置身份更新周期,当 OBU_i的临时身份有效期 T_{endi}到期时,需再次申请身份授权,同时 TRA 更新 L_{OBU}. 上述方法利用周期变化的临时身份有效保护了 OBU 的隐私,同时还可以实现必要的事后追查,满足车辆的条件匿名性保护需求.

5　方案分析

5.1　正确性分析

(1)OBU_i与 TRA 共享密钥 K_{OiT}和 K_{TOi}的一致性验证如下:

$$\begin{aligned}K_{TOi}&=H_2(\mathrm{TID}_i(r'_T+h'_Ts_T))\\&=H_2(r_{OiT}(R'_{Oi}+h'_{Oi}P_{Oi})(r'_T+h'_Ts_T))\\&=H_2(r_{OiT}(r'_{Oi}+h'_{Oi}s_{Oi})(R'_T+h'_TP_T))\\&=K_{OiT}\end{aligned}$$

(2)聚合签名 V_{OC}正确性推导过程如下:

$$V_{OC}=\sum_{i=1}^{n}V_{OiCl},R_{TO}=\sum_{i=1}^{n}R_{TOi}=\sum_{i=1}^{n}r_{TOi}P$$

$$\begin{aligned}V_{OC}P&=\sum_{i=1}^{n}(V_{TOi}+r_{Oi}(r'_{Oi}+h'_{Oi}s_{Oi})h_{OiCl})P\\&=\sum_{i=1}^{n}((r'_T+h'_Ts_T)h_{TOi}+r_{TOi}\\&\quad+r_{OiCl}(r'_{Oi}+h'_{Oi}s_{Oi})h_{OiCl})P\end{aligned}$$

$$= (R'_T + h'_T P_T) \sum_{i=1}^{n} h_{TOi} + R_{TO} + \sum_{i=1}^{n} R_{OiCl} h_{OiCl}$$

(3) OBU_i 与 CS_l 的会话密钥 SK_{OiCl} 和 SK_{ClOi} 一致性验证过程如下：

$$\begin{aligned} SK_{ClOi} &= H_2(r_{ClOi}(r'_{Cl} + h'_{Cl}s_{Cl})R_{OiCl}) \\ &= H_2(r_{ClOi}(r'_{Cl} + h'_{Cl}s_{Cl})r_{OiCl}(r'_{Oi} + h'_{Oi}s_{Oi})P) \\ &= H_2(r_{OiCl}(r'_{Oi} + h'_{Oi}s_{Oi})R_{ClOi}) \\ &= SK_{OiCl}. \end{aligned}$$

5.2 安全性证明

引理 1 在随机预言机模型下，假定 CDH 假设成立，本文协议对敌手 A_1 是安全的.

证明 假设敌手 A_1 在多项式时间 t 内以不可忽略的优势 $Adv_{A1}(k)$ 赢得游戏，则 A_1 有能力使得 C 解决 CDH 困难问题. C 随机选取 $x \in Z_q^*$，令 $P_{pub} = xP$，选择系统参数 $Params = \{q, E/F_p, P, G, H_1, H_2, H_3, P_{pub}\}$，并将 Params 发送给 A_1.

令 n_0 是每个用户发起的最大会话数，假设敌手 A_1 至多激活 n_1 个诚实用户，最多进行 n_2 次散列函数查询. A_1 完成 Test 查询后，仅有以下三种方法能区分真实的会话密钥和随机值.

(1) 猜测攻击：A_1 以 $O(\frac{1}{2^k})$ 的优势正确猜测出会话密钥，此优势是可忽略的.

(2) 密钥复制攻击：A_1 迫使参与者发起 Test 会话的非匹配会话，并拥有与 Test 会话相同的会话密钥. A_1 通过查询此非匹配会话来获得会话密钥. 由于 H_2 是随机预言机，并且针对不同的会话拥有不同的输入值，使得输出相同会话密钥是不可能的，即密钥复制攻击的优势是可忽略的.

(3) 伪造攻击：猜测攻击和密钥复制攻击的优势是可忽略的，因此，主要针对伪造攻击进行分析.

$\prod_{I,J}^{s_{id}}$ 作为 Test 会话，在某时刻，A_1 对参与者 I 和 J 之间的 Test 会话进行关于 (K_{IJ}) 的 H_3 查询，正确计算出 K_{IJ} 值.

挑战者 C 利用敌手 A_1 区分会话密钥和随机值的优势来解决 CDH 问题. 令 $Adv_C(k)$ 为 C 在安全参数 k 下解决 CDH 问题的优势，给定一个 CDH 挑战 $U = uP, V = vP$，其中 $u, v \in Z_q^*$，C 可以计算出 $CDH(U, V) = uvP$. C 模拟上述游戏，游戏期间，C 需响应 A_1 的所有查询.

C 随机选取两个不同的参与者 $I, J \in \{1, 2, \cdots, n_1\}$，$I \neq J$，$s \in \{1, \cdots, n_0\}$，令 $\prod_{I,J}^{s}$ 的匹配会话是 $\prod_{J,I}^{s}$，则 $\prod_{I,J}^{s}$ 是正确 Test 会话的可能性大于 $\frac{1}{n_0 n_1^2}$. 考虑下列两种情形：

Case1：存在诚实的用户拥有 Test 会话的匹配会话，根据 CL-eCK 模型定义，A_1 拥有以下 4 种选择：

(a) A_1 不能获得 I 的临时私钥和 J 的部分私钥；

(b) A_1 不能获得 J 的临时私钥和 I 的部分私钥；

(c) A_1 不能获得 I 和 J 的部分私钥；

(d) A_1 不能获得 I 和 J 的临时私钥.

Case 2：不存在诚实的用户拥有 Test 会话的匹配会话，根据 CL-eCK 模型定义，A_1 拥有以下 2 种选择：

(a) A_1 拥有 I 的完整私钥对，由新鲜性定义，敌手不能查询 I 的临时私钥；

(b) A_1 未获得 I 的完整私钥对，由新鲜性定义，敌手可以查询 I 的临时私钥.

引理 1 中的 Case1(a) 分析

A_1 不能获得 I 的临时私钥和 J 的部分私钥，C 回答 A_1 的如下查询：

Create(ID_i)：C 维护一个初始为空、记录格式为 $(ID_i, s_i, R_i, r'_i, R'_i)$ 的列表 L_C. 如果 $i = J$，C 随机选取两个随机数 $h_J, r'_J \in Z_q^*$，计算 $R_J = U - h_J P_{pub}$，$R'_J = r'_J P$，令 $H_1(ID_J, R_J) = h_J$，将 $(ID_J, \perp, R_J, r'_J, R'_J)$ 和 (ID_J, R_J, h_J) 分别记录于 L_C 和 L_{H1} 中；否则，C 随机选择 $s_i, h_i, r'_i \in Z_q^*$，计算 $R_i = s_i P - h_i P_{pub}$，$R'_i = r'_i P$，令 $h_i = H_1(ID_i, R_i)$，将 $(ID_i, s_i, R_i, r'_i, R'_i)$ 和 (ID_i, R_i, h_i) 分别记录于 L_C 和 L_{H1} 中.

$H_1(ID_i, R_i)$：C 维护一个初始为空、记录格式为 (ID_i, R_i, h_i) 的列表 L_{H1}. 若 (ID_i, R_i) 在列表 L_{H1} 中，则返回相应值 h_i；否则，C 随机选取 $h_i \in Z_q^*$，记录 (ID_i, R_i, h_i) 并将 h_i 返回.

$H_2(ID_i, R'_i)$：C 维护一个初始为空、记录格式为 (ID_i, R'_i, h'_i) 的列表 L_{H2}. 若 (ID_i, R'_i) 在列表 L_{H2} 中，则返回相应值 h'_i；否则，C 随机选取 $h'_i \in Z_q^*$，记录 (ID_i, R'_i, h'_i) 并将 h'_i 返回.

$H_3(K_{ij})$：C 维护一个初始为空、记录格式为 $(ID_i, ID_j, R_{ij}, R_{ji}, K_{ij}, SK_{ij})$ 的列表 L_{H3}. 若在 L_{H3} 中有记录，则返回对应 SK_{ij}；否则，C 根据下述操作返回查询值：

如果 $i = J$，C 在列表 L_{H3} 中查找对应元组 $(ID_i, ID_j, R_{ij}, R_{ji}, *)$. 若存在，计算 $\overline{K_{ij}} = K_{ij} - r_{ij} r_{ji} r'_i (r'_j + s_j h'_j) P$，其中 $h'_j = H_2(ID_j, R'_j)$，通过检查 $H_2(ID_i, R'_i)(R_i + H_1(ID_i, R_i)P_{pub})$、$r_{ij} R_{ji}$、$\overline{K_{ij}}$ 是否是 DDH 元组判断 K_{ij} 的正确性. 若是，则 K_{ij} 计算正确，在 L_{H3} 中记录元组 $(ID_i, ID_j, R_{ij}, R_{ji}, K_{ij}, SK_{ij})$，其中 SK_{ij} 取自于 L_S 中；否则，C 随机选取 $SK_{ij} \in \{0,1\}^k$，将元组记录于 L_{H3} 中.

如果 $i \neq J$，C 在列表 L_{H3} 中查找对应元组 $(ID_i, ID_j, R_{ij}, R_{ji}, *)$，若存在，在 L_{H3} 中记录元组 $(ID_i, ID_j, R_{ij}, R_{ji}, K_{ij}, SK_{ij})$，其中 SK_{ij} 取自于 L_S 中；否则，C 随机选取 $SK_{ij} \in \{0,1\}^k$，将元组记录于 L_{H3} 中.

RevealMasterKey:C 停止模拟.

RevealSessionKey($\prod_{i,j}^{s_{id}}$):如果 $\prod_{i,j}^{s_{id}}=\prod_{I,J}^{S}$ 或 $\prod_{i,j}^{s_{id}}=\prod_{J,I}^{S}$,$C$ 停止模拟.

RevealPartialPrivateKey(ID_i):若 $i=J$,则停止模拟;否则,返回对应部分私钥.

RevealSecretValue(ID_i):C 查找列表 L_C,若找到列表中存在对应项,C 发送 r_i'给 A_1;否则,执行 Create(ID_i)查询和返回 r_i'.

ReplacePublicKey(ID_i):C 针对 ID_i的元组查找列表 L_C,若找到,则利用 r'^* 和 R'^* 分别替换 r_i'和 R_i';否则,执行 Create(ID_i)并替换 r_i'和 R_i'为 A_1所选值.

ReavealEphemeralKey($\prod_{i,j}^{s_{id}}$):若 $\prod_{i,j}^{s_{id}}=\prod_{I,J}^{S}$,则 C 停止模拟;否则返回临时私钥给 A_1.

Send($\prod_{i,j}^{s_{id}}$,m):C 维护一个初始为空、记录格式为(ID_i,ID_j,R_{ij},R_{ji},SK_{ij})的列表 L_S,C 根据以下条件进行回答:

如果 $\prod_{i,j}^{s_{id}}=\prod_{I,J}^{S}$,则返回 $R_{ij}=V$.

如果 $i=J$,C 随机选取 $r_{ij},s_j\in Z_q^*$,计算 $\overline{K_{ij}}=K_{ij}-r_{ij}r_{ji}r_i'(r_j'+s_jh_j')P$,其中 $h_j'=H_2(\mathrm{ID}_j,R_j')$,检查 $H_2(\mathrm{ID}_i,R_i')(R_i+H_1(\mathrm{ID}_i,R_i)P_{pub})$、$r_{ij}R_{ji}$、$\overline{K_{ij}}$是否是 DDH 元组.若是,则 K_{ij}计算正确,在 L_S中记录元组(ID_i,ID_j,R_{ij},R_{ji},SK_{ij}),其中 SK_{ij}取自于 L_{H3}中.否则,C 随机选取$\mathrm{SK}_{ij}\in\{0,1\}^k$,将元组记录于 L_S中.

否则,按协议规定进行回答.

Test($\prod_{i,j}^{s_{id}}$):针对此查询,如果$\prod_{i,j}^{s_{id}}\neq\prod_{I,J}^{S}$,$C$ 停止模拟.否则,C 随机选取 $\xi\in\{0,1\}^k$,返回给 A_1.

若 A_1赢得此次游戏,则 A_1计算出正确的 K_{ij}. $K_{ij}=r_{ij}r_{ji}(r_i'+s_ih_i')(r_j'+s_jh_j')P=r_{ji}r_j'V+r_{ji}h_j'\mathrm{CDH}(U,V)$,其中 $h_i'=H_2(\mathrm{ID}_i,R_i')$ 和 $h_j'=H_2(\mathrm{ID}_j,R_j')$,由于 $U=s_jP$,$V=r_{ij}(r_i'+s_ih_i')P$,则 $\mathrm{CDH}(U,V)=(K_{ij}-r_{ji}r_j'V)(r_{ji}h_j')^{-1}$. C 能以$\frac{1}{n_2}$的概率在 L_{H3}中找到对应正确元组,即 C 解决 CDH 问题的优势为$\mathrm{Adv}_C(k)\geqslant\frac{1}{n_0n_1^2n_2}\mathrm{Adv}_{A1}(k)$,由于假定的 $\mathrm{Adv}_{A1}(k)$不可忽略,则 $\mathrm{Adv}_C(k)$也不可忽略,因此与 CDH 假设矛盾.

引理 1 中的 Case1(b)分析

A_1不能获得 J 的临时私钥和 I 的部分私钥,此过程是将 Case 1(a) 中 I 和 J 互换,参考 Case 1(a)的证明即可.

引理 1 中的 Case1(c)分析

A_1不能获得 I 和 J 的部分私钥,除了以下查询的回答不同,其余按照 Case 1(a)的规定执行.

Create(ID_i):C 维护一个初始为空、记录格式为(ID_i,s_i,R_i,r_i',R_i')的列表 L_C. 如果 $i=J$,按 Case 1(a)中 Create 查询执行;如果 $i=I$,C 随机选取两个随机数 $h_I,r_I'\in Z_q^*$,计算 $R_I=V-h_IP_{pub}$,$R_I'=r_I'P$,令 $H_1(\mathrm{ID}_I,R_I)=h_I$,将($\mathrm{ID}_I$,$\perp$,$R_I$,$r_I'$,$R_I'$)和($\mathrm{ID}_I$,$R_I$,$h_I$)分别记录于 L_C和 L_{H1}中;否则,C 随机选择 $s_i,h_i,r_i'\in Z_q^*$,计算 $R_i=s_iP-h_iP_{pub}$,$R_i'=r_i'P$,令 $h_i=H_1(\mathrm{ID}_i,R_i)$,将($\mathrm{ID}_i$,$s_i$,$R_i$,$r_i'$,$R_i'$)和($\mathrm{ID}_i$,$R_i$,$h_i$)分别记录于 L_C和 L_{H1}中.

$H_3(K_{ij})$:C 维护一个初始为空、记录格式为(ID_i,ID_j,R_{ij},R_{ji},K_{ij},SK_{ij})的列表 L_{H3}. 如果 $i=I$ 或 $i=J$,按照 Case 1(a)中 $H_3(K_{ij})$查询的 $i=J$ 时执行,其余按 Case 1(a)中 $H_3(K_{ij})$查询的具体规定执行.

RevealPartialPrivateKey(ID_i):若 $i=J$ 或 $i=I$,则停止模拟;否则,返回对应部分私钥.

Send($\prod_{i,j}^{s_{id}}$,m):C 维护一个初始为空、记录格式为(ID_i,ID_j,R_{ij},R_{ji},SK_{ij})的列表 L_S. 若 $i=J$ 或 $i=I$,按照 Case 1(a)中 Send 查询的 $i=J$ 时执行,其余按 Case 1(a)中 Send 查询的规定执行.

若 A_1赢得此次游戏,则 A_1计算出正确的 K_{ij}. $K_{ij}=r_{ij}r_{ji}(r_i'+s_ih_i')(r_j'+s_jh_j')P=r_{ij}r_{ji}(r_i'r_j'P+r_i'h_j'U+r_j'h_i'V+h_i'h_j'\mathrm{CDH}(U,V))$,其中 $h_i'=H_2(\mathrm{ID}_i,R_i')$ 和 $h_j'=H_2(\mathrm{ID}_j,R_j')$,由于 $U=s_jP$,$V=s_iP$,则 $\mathrm{CDH}(U,V)=(K_{ij}(r_{ij}r_{ji})^{-1}-r_i'r_j'P-r_i'h_j'U-r_j'h_i'V)(h_i'h_j')^{-1}$. C 能以$\frac{1}{n_2}$的概率在 L_{H3}中找到对应正确元组,即 C 解决 CDH 问题的优势为$\mathrm{Adv}_C(k)\geqslant\frac{1}{n_0n_1^2n_2}\mathrm{Adv}_{A1}(k)$,由于假定的 $\mathrm{Adv}_{A1}(k)$不可忽略,则 $\mathrm{Adv}_C(k)$也不可忽略,因此与 CDH 假设矛盾.

引理 1 中的 Case1(d)分析

A_1不能获得 I 和 J 的临时私钥,除了以下查询的回答不同,其余按照 Case 1(a)的规定执行.

Create(ID_i):C 维护一个初始为空、记录格式为(ID_i,s_i,R_i,r_i',R_i')的列表 L_C. C 随机选择 $s_i,h_i,r_i'\in Z_q^*$,计算 $R_i=s_iP-h_iP_{pub}$,$R_i'=r_i'P$,令 $h_i=H_1(\mathrm{ID}_i,R_i)$,将($\mathrm{ID}_i$,$s_i$,$R_i$,$r_i'$,$R_i'$)和($\mathrm{ID}_i$,$R_i$,$h_i$)分别记录于 L_C和 L_{H1}中.

$H_3(K_{ij})$:C 维护一个初始为空、记录格式为(ID_i,ID_j,R_{ij},R_{ji},K_{ij},SK_{ij})的列表 L_{H3}. 若在 L_{H3}中有记录,则返回对应 SK_{ij};否则,C 根据下述操作返回查询值:

C 在列表 L_S中查找对应元组(ID_i,ID_j,R_{ij},R_{ji},$*$).若存在,计算$\overline{K_{ij}}=(K_{ij}(r_{ij}r_{ji})^{-1}-r_i'r_j'P-r_i'h_j's_jP-r_j'h_i's_iP)(h_i'h_j')^{-1}$,其中 $h_i'=H_2(\mathrm{ID}_i,R_i')$,$h_j'=H_2(\mathrm{ID}_j,R_j')$,通过检

查 s_iP、s_jP、$\overline{K_{ij}}$是否是 DDH 元组来检查 K_{ij}的正确性. 若是,则 K_{ij}计算正确,在 L_{H3}中记录元组(ID_i,ID_j,R_{ij},R_{ji},K_{ij},SK_{ij}),其中 SK_{ij}取自于 L_S中;否则,C 随机选取 $I,J\in\{1,2,\cdots,n_1\}$,将元组记录于 L_{H3}中.

RevealPartialPrivateKey(ID_i):C 通过查找列表 L_C,返回部分私钥给 A_1.

ReavealEphemeralKey($\prod_{i,j}^{s_{\mathrm{id}}}$):若$\prod_{i,j}^{s_{\mathrm{id}}}=\prod_{i,j}^{S}$ 或者$\prod_{i,j}^{s_{\mathrm{id}}}=\prod_{J,I}^{S}$,则 C 停止模拟;否则返回临时私钥给 A_1.

Send($\prod_{i,j}^{s_{\mathrm{id}}}$,$m$):$C$ 维护一个初始为空、记录格式为(ID_i,ID_j,R_{ij},R_{ji},SK_{ij})的列表 L_S. 如果$\prod_{i,j}^{s_{\mathrm{id}}}=\prod_{i,j}^{S}$,则返回 $R_{ij}=U$;如果$\prod_{i,j}^{s_{\mathrm{id}}}=\prod_{J,I}^{S}$,则返回 $R_{ji}=V$;否则,按协议规定进行回答.

若 A_1赢得此次游戏,则 A_1计算出正确的 K_{ij}. $K_{ij}=r_{ij}r_{ji}(r'_i+s_ih'_i)(r'_j+s_jh'_j)P=\mathrm{CDH}(U,V)$,其中 $h'_i=H_2(\mathrm{ID}_i,R'_i)$和 $h'_j=H_2(\mathrm{ID}_j,R'_j)$,由于 $U=r_{ij}(r'_i+s_ih'_i)P$,$V=r_{ji}(r'_j+s_jh'_j)P$,则 $\mathrm{CDH}(U,V)=K_{ij}$. C 能以$\frac{1}{n_2}$的概率在 L_{H3}中找到对应正确元组,即 C 解决 CDH 问题的优势为$\mathrm{Adv}_C(k)\geqslant\frac{1}{n_0n_1^2n_2}\mathrm{Adv}_{A1}(k)$,由于假定的 $\mathrm{Adv}_{A1}(k)$不可忽略,则 $\mathrm{Adv}_C(k)$也不可忽略,因此与 CDH 假设矛盾.

引理 1 中的 Case2(a)和 Case 2(b)分析

Case2(a)和 Case 2(b)分别与 Case 1(a)和 Case 1(b)类似,同理可证明 C 解决 CDH 问题的优势为$\mathrm{Adv}_C(k)\geqslant\frac{1}{n_0n_1^2n_2}\mathrm{Adv}_{A1}(k)$,由于假定的 $\mathrm{Adv}_{A1}(k)$不可忽略,则 $\mathrm{Adv}_C(k)$也不可忽略,因此与 CDH 假设矛盾.

证毕.

引理 2 在随机预言机模型下,假定 CDH 假设成立,本文协议对敌手 A_2是安全的.

证明 假设敌手 A_2在多项式时间 t 内以不可忽略的的优势 $\mathrm{Adv}_{A2}(k)$赢得定义的游戏,则 A_2有能力使得 C 解决 CDH 困难问题. C 随机选取 $x\in Z_q^*$,令系统公钥 $P_{\mathrm{pub}}=xP$,选择系统参数 $\mathrm{Params}=\{q,E/F_p,P,G,H_1,H_2,H_3,P_{\mathrm{pub}}\}$,并将 Params 和主密钥 x 发送给敌手 A_2. 与引理 1 证明类似,针对伪造攻击进行分析,主要考虑 Case 1 和 Case 2 两种情形. 即:

Case 1:存在诚实的用户拥有 Test 会话的匹配会话,根据 CL-eCK 模型定义可分为以下 4 种情况:

(a) A_2不能获得 I 的临时私钥和 J 的秘密值;

(b) A_2不能获得 J 的临时私钥和 I 的秘密值;

(c) A_2不能获得 I 和 J 的临时私钥;

(d) A_2不能获得 I 和 J 的秘密值.

Case 2:不存在诚实的用户拥有 Test 会话的匹配会话,根据 CL-eCK 模型定义,A_2拥有以下 2 种选择:

(a)A_2拥有 I 的秘密值,由新鲜性定义,敌手不能查询 I 的临时私钥;

(b)A_2未获得 I 的秘密值,由新鲜性定义,敌手可以查询 I 的临时私钥.

上述 Case 1 和 Case 2 总共 6 种情况参照引理 1 的证明. 此处选择 Case 1(a)进行证明,其余情形同理可证其安全性,即可证明引理 2 成立.

引理 2 中的 Case1(a)分析

A_2不能获得 I 的临时私钥和 J 的秘密值,参照引理 1 证明中查询的回答,针对与引理 1 中 Case 1(a)查询回答的不同,按如下规定操作:

Create(ID_i):C 维护一个初始为空、记录格式为(ID_i,s_i,R_i,r'_i,R'_i)的列表 L_C. 如果 $i=J$,C 随机选取两个随机数 $r_J,h_J\in Z_q^*$,计算 $R_J=r_JP$,$R'_J=U$,$s_J=r_J+h_Jx$,令 $h_J=H_1(\mathrm{ID}_J,R_J)$,将($\mathrm{ID}_J$,$s_J$,$R_J$,$\perp$,$R'_J$)和($\mathrm{ID}_J$,$R_J$,$h_J$)分别记录于 L_C和 L_{H1}中;否则,C 随机选择 $r_i,h_i,r'_i\in Z_q^*$,计算 $R_i=r_iP$,$R'_i=r'_iP$,$s_i=r_i+h_ix$,令 $h_i=H_1(\mathrm{ID}_i,R_i)$,将($\mathrm{ID}_i$,$s_i$,$R_i$,$r'_i$,$R'_i$)和($\mathrm{ID}_i$,$R_i$,$h_i$)分别记录于 L_C和 L_{H1}中.

$H_3(K_{ij})$:C 维护一个初始为空、记录格式为(ID_i,ID_j,R_{ij},R_{ji},K_{ij},SK_{ij})的列表 L_{H3}. 若在 L_{H3}中有记录,则返回对应 SK_{ij};否则,C 根据下述操作返回查询值:

如果 $i=J$,C 在列表 L_{H3}中查找对应元组(ID_i,ID_j,R_{ij},R_{ji},$*$). 若存在,计算$\overline{K_{ij}}=K_{ij}r_{ij}^{-1}-s_ih'_iR_{ji}$,其中 $h'_i=H_2(\mathrm{ID}_i,R'_i)$,通过检查 R'_i、R_{ji}、$\overline{K_{ij}}$是否是 DDH 元组来检查 K_{ij}的正确性. 若是,则 K_{ij}计算正确,在 L_{H3}中记录元组(ID_i,ID_j,R_{ij},R_{ji},K_{ij},SK_{ij}),其中 SK_{ij}取自于 L_S中;否则,C 随机选取$\mathrm{SK}_{ij}\in\{0,1\}^k$,将元组记录于 L_{H3}中.

如果 $i\neq J$,C 在列表 L_{H3}中查找对应元组(ID_i,ID_j,R_{ij},R_{ji},$*$),若存在,在 L_{H3}中记录元组(ID_i,ID_j,R_{ij},R_{ji},K_{ij},SK_{ij}),其中 SK_{ij}取自于 L_S中;否则,C 随机选取$\mathrm{SK}_{ij}\in\{0,1\}^k$,将元组记录于 L_{H3}中.

RevealMasterKey:C 将主密钥返回.

RevealPartialPrivateKey(ID_i):C 返回部分私钥给 A_2.

RevealSecretValue(ID_i):如果 $i=J$,则 C 停止模拟;否则,C 查找列表 L_C,若找到列表中存在对应项,C 发送 r'_i给 A_2;否则,执行 Create(ID_i)查询和返回 r'_i.

Send($\prod_{i,j}^{s_{\mathrm{id}}}$,$m$):$C$ 维护一个初始为空、记录格式为

$(\mathrm{ID}_i,\mathrm{ID}_j,R_{ij},R_{ji},\mathrm{SK}_{ij})$的列表 L_S,C 根据以下条件进行回答:

如果 $\prod_{i,j}^{s_{\mathrm{id}}}=\prod_{i,j}^{S}$,则返回 $R_{ij}=V$.

如果 $i=J$,C 随机选取 $r_{ij}\in Z_q^*$,计算 $\overline{K_{ij}}=K_{ij}r_{ij}^{-1}-s_ih'_iR_{ji}$,其中 $h'_i=H_2(\mathrm{ID}_i,R'_i)$,检查 R'_i、R_{ji}、$\overline{K_{ij}}$是否是 DDH 元组. 若是,则 K_{ij}计算正确,在 L_S中记录元组$(\mathrm{ID}_i,\mathrm{ID}_j,R_{ij},R_{ji},\mathrm{SK}_{ij})$,其中 SK_{ij}取自于 L_{H3}中. 否则,C 随机选取 $\mathrm{SK}_{ij}\in\{0,1\}^k$,将元组记录于 L_S中.

否则,按协议规定进行回答.

若 A_2赢得此次游戏,则 A_2计算出正确的 K_{ij}. $K_{ij}=r_{ij}r_{ji}(r'_i+s_ih'_i)(r'_j+s_jh'_j)P=r_{ji}s_jh'_jV+r_{ji}\mathrm{CDH}(U,V)$,其中 $h'_i=H_2(\mathrm{ID}_i,R'_i)$和 $h'_j=H_2(\mathrm{ID}_j,R'_j)$,由于 $U=r'_jP$,$V=r_{ij}(r'_i+s_ih'_i)P$,则 $\mathrm{CDH}(U,V)=(K_{ij}-r_{ji}s_jh'_jV)r_{ji}^{-1}$. C 能以$\frac{1}{n_2}$的概率在 L_{H3}中找到对应正确元组,即 C 解决 CDH 问题的优势为$\mathrm{Adv}_C(k)\geqslant\frac{1}{n_0n_1^2n_2}\mathrm{Adv}_{A2}(k)$,由于假定的 $\mathrm{Adv}_{A2}(k)$不可忽略,则 $\mathrm{Adv}_C(k)$也不可忽略,因此与 CDH 假设矛盾.

证毕.

定理 1　本协议在 CDH 假设和 eCK 模型下是安全的.

证明　由上述引理 1 和引理 2 的证明,能够得出定理 1 成立.

证毕.

5.3　性能分析和比较

本节将本方案与文献[6,11~16]就安全性、计算开销以及通信开销等性能进行比较,结果如表 2 所示. 其中,T_M表示椭圆曲线上的倍点运算时间,T_P表示双线性对运算时间,T_E表示基于双线性对的乘法群上指数运算时间. 上述运算的仿真时间如表 1 所示,其中车载单元 OBU 由一部 4 核 2.45GHz 处理器的移动设备充当,服务器由部署了大数运算函数库(MIRACL)的 I5-4460S 2.90GHz CPU 的计算机充当. 符号"✓"和"×"表示是否满足某要求,符号"—"表示未涉及该性能. 此外,为了评估通信开销,我们对方案中涉及的参数长度进行如下定义:Hash 值、随机数的长度均为 160bits,时间戳的长度为 32bits,参与者身份的长度为 128bits,椭圆曲线上点的长度为 320bits.

表 1　运算操作的运行时间[17]

运算操作	运行时间(ms)	
	OBU	Server
T_P	32.713	5.427
T_E	2.249	0.339
T_M	3.335	0.538

表 2　性能比较

文献	匿名性	抗临时私钥泄露攻击	公私钥频繁更新	批认证	n 个 OBU 的认证密钥协商			
					通信量(bit)	OBUs 计算开销(ms)	Server 计算开销(ms)	总的计算开销(ms)
[6]	弱	×	×	×	$3776n$	$7nT_M=23.345n$	$6nT_M=3.228n$	$26.573n$
[11]	强	×	✓	×	$5504n$	$2nT_P+5nT_M=82.101n$	$2nT_P+4nT_M=13.006n$	$95.107n$
[12]	无	×	—	×	$5376n$	$2nT_P+6nT_M=85.436n$	$2nT_P+6nT_M=14.082n$	$99.518n$
[13]	强	✓	✓	×	$4096n$	$5nT_M=16.675n$	$8nT_M=4.304n$	$20.979n$
[14]	弱	✓	×	×	$3136n$	$2nT_M+2nT_E=14.503n$	$2nT_P+nT_M+3nT_E=12.409n$	$26.912n$
[15]	无	✓	—	×	$3456n$	$4nT_M=13.34n$	$4nT_M=2.152n$	$15.492n$
[16]	无	✓	—	×	$3072n$	$5nT_M=16.675n$	$5nT_M=2.69n$	$19.365n$
本文方案	强	✓	×	✓	$4640n+160$	$5nT_M=16.675n$	$(3n+3)T_M=1.614n+1.614$	$18.289n+1.614$

具体而言,在安全性方面,文献[15,16]未提供任何匿名性保护,文献[6,14]只具备弱匿名性,因此攻击者可以获得车载单元的真实身份并追踪车辆的具体位置. 文献[11]虽然具有强匿名性,但该方案的会话密钥仅由双方的临时私钥生成,因此无法抵抗临时私钥泄露攻击. 文献[13]虽然满足强匿名性并能抵抗临时私钥泄露攻击,但需要利用车辆公钥验证车辆临时身份的合法性,所以随着车辆临时身份的更新,系统需要为车辆动态生成新的公私钥,导致系统开销大幅增加. 与上述方案相比,本文方案借助临时身份不仅能够提供强匿名性保护,而且由于会话密钥由双方的长期私钥和临时私钥共同生成,能够抵抗临时私钥泄露攻击. 同时,在对车辆进行匿名认证的过程中,本文方案通过引入随机因子构建可信中心为车辆临时身份颁发的秘密签名,使得云服务器通过可信中心公钥和车辆的公开承诺即可验证该签名,无需车辆公钥参与验证,因此有效解决了因车辆临时身份改变导致其公私钥频繁更新的问题,减少了系统开销.

在计算量方面,由表 2 可以看出,面对 n 个 OBU 同时发起的认证及密钥协商请求,文献[6,11,12]相比于

本方案,OBU 需要执行更多的倍点运算和双线性对运算,因此本方案中 OBU 的计算量较低. 而且,本方案利用无对运算的聚合签名实现高效的批量认证,云服务器的计算开销从 $6nT_M$ 减少至 $(3n+3)T_M$,有效降低了云服务器的验证开销,比未采用批认证的方案[6,11~16]更加高效. 由以上分析可知,本方案的总计算效率比文献[6,11~14,16]具备一定优势,尤其在面对庞大数量的用户认证请求时,本方案的性能提升更明显,能够更好的满足车联网的实时性要求. 此外,虽然文献[15]的计算开销比本方案低,但该方案不具备对车辆的匿名性保护,难以实现 VANET 隐私保护要求.

在通信量方面,由于本文方案引入的临时身份不是随机数,且预签名信息中包含多个基于椭圆曲线的点参数,增加了部分通信量,但由于本方案通过路边设施单元(RSU)聚合和转发 OBU 的签名信息,在一定程度上又降低了签名传递的通信量. 总体而言,本文方案的通信开销处于各类方案的平均水平.

综上分析,本文方案虽然在通信量方面不具备明显优势,但在安全性上能够更好的满足车联网的认证需求,并且通过高效的批认证技术提升了方案的计算效率.

6 结论

本文面向云服务下的车联网提出一个基于无证书聚合签名的匿名认证与密钥协商方案. 方案采用无双线性对的聚合签名,有效降低了签名传递的通信量以及云服务器的验证开销,实现了高效的批认证. 同时,通过引入临时身份和预签名机制,实现了对车辆的隐私保护及条件匿名性保护. 在 eCK 模型和 CDH 假设下可证明本方案是形式化安全的,能够满足车联网的安全高效认证需求.

参考文献

[1] LIN X,SUN X,WANG X,et al. TSVC:timed efficient and secure vehicular communications with privacy preserving [J]. IEEE Transactions on Wireless Communications, 2008,7(12):4987 – 4998.

[2] ZHANG C,LIN X,LU R,et al. An efficient message authentication scheme for vehicular communications [J]. IEEE Transactions on Vehicular Technology,2008,57(6): 3357 – 3368.

[3] CHIM T W,YIU S M,HUI L C K,et al. Security and privacy issues for inter-vehicle communications in VANETs [A]. Sensor,Mesh and Ad Hoc Communications and Networks Workshops, 2009. SECON Workshops′09. IEEE Communications Society Conference on[C]. Rome,Italy: IEEE,2009. 1 – 3.

[4] WASEF A,SHEN X. EMAP:Expedite message authentication protocol for vehicular ad hoc networks [J]. IEEE Transactions on Mobile Computing,2013,12(1):78 – 89.

[5] WANG S B,YAO N M,GONG N,GAO Z G. A trigger-based pseudonym exchange scheme for location privacy preserving in VANETs [J]. Peer-to-Peer Networking and Applications,2018,11(3):548 – 560.

[6] 谢永,吴黎兵,张宇波,等. 面向车联网的多服务器架构的匿名双向认证与密钥协商协议[J]. 计算机研究与发展,2016,53(10):2323 – 2333.
XIE Yong,WU Li-bing,ZHANG Yu-bo,et al. Anonymous mutual authentication and key agreement protocol in multi-server architecture for VANETs [J]. Journal of Computer Research and Development, 2016, 53 (10): 2323 – 2333. (in Chinese)

[7] BAYAT M,BARMSHOORY M,RAHIMI M,et al. A secure authentication scheme for VANETs with batch verification[J]. Wireless Networks,2015,21(5):1 – 11.

[8] 宋成,张明月,彭维平,等. 基于双线性对的车联网批量匿名认证方案研究[J]. 通信学报,2017,38(06):49 – 57.
SONG Cheng,ZHANG Ming-yue,PENG Wei-ping,et al. Research on batch anonymous authentication scheme for VANET based on bilinear pairing[J]. Journal on Communications,2017,38(06):49 – 57. (in Chinese)

[9] LIPPOLD G,BOYD C,NIETO J G. Strongly secure certificateless key agreement [A]. Pairing-Based Cryptography-Pairing 2009[C]. Berlin:Springer,2009. 206 – 230.

[10] 苏航,刘建伟,陶芮. 无证书的层次认证密钥协商协议[J]. 通信学报,2016,37(7):161 – 171.
SU Hang, LIU Jian-wei, TAO Rui. Hierarchical certificateless authenticated key agreement protocol[J]. Journal on Communications, 2016, 37 (7): 161 – 171. (in Chinese)

[11] HAN M,HUA L,MA S. A self-authentication and deniable efficient group key agreement protocol for VANET [J]. KSII Transactions on Internet and Information Systems,2017,11(7):3678 – 3698.

[12] LI Y,CHEN W,CAI Z,et al. CAKA:a novel certificateless-based cross-domain authenticated key agreement protocol for wireless mesh networks[J]. Wireless Networks, 2016,22(8):2523 – 2535.

[13] 陈明. 强安全的匿名隐式漫游认证与密钥协商方案[J]. 计算机研究与发展,2017,54(12):2772 – 2784.
CHEN Ming. Strongly secure anonymous implicit authentication and key agreement for roaming service[J]. Journal of Computer Research and Development, 2017, 54 (12):2772 – 2784. (in Chinese)

[14] ODELU V,DAS A K,KUMARI S,et al. Provably secure authenticated key agreement scheme for distributed mobile

cloud computing services[J]. Future Generation Computer Systems,2017,68:74 – 88.

[15] TSENG Y,HUANG S,YOU M. Strongly secure ID-based authenticated key agreement protocol for mobile multi-server environments[J]. International Journal of Communication Systems,2017,30(11):1074 – 5351.

[16] 王真,马兆丰,罗守山. 基于身份的移动互联网高效认证密钥协商协议[J]. 通信学报,2017,38(08):19 – 27.
WANG Zhen, MA Zhao-feng, LUO Shou-shan. Identity-based efficient authentication and key agreement protocol for mobile Internet[J]. Journal on Communications, 2017,38(08):19 – 27. (in Chinese)

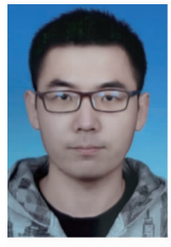
[17] HE D,ZEADALLY S,KUMAR N,et al. Efficient and anonymous mobile user Authentication protocol using self-certified public key cryptography for multi-server architectures[J]. IEEE Transactions on Information Forensicsand Security,2016,11(9):2052 – 2064.

作者简介

张文芳　女,1978 年 7 月出生于山西省太原市. 博士,西南交通大学副教授,硕士生导师. 主要研究领域为密码学和信息安全.
E-mail:wfzhang@ swjtu. edu. cn

雷丽婷　女,1993 年 6 月出生于贵州省贵阳市. 硕士. 主要研究方向为移动通信信息安全.
E-mail:306481334@ qq. com

王小敏(通讯作者)　男,1974 年 4 月出生于江西省萍乡市. 博士,西南交通大学教授,博士生导师. 主要研究领域为信息安全和轨道交通安全工程.
E-mail:xmwang@ swjtu. edu. cn



王　宇　男,1990 年 4 月出生于河北省石家庄市. 博士研究生. 主要研究方向为轨道交通信息安全.
E-mail:wy4324956@ my. swjtu. edu. cn