·热点与综述·　　文章编号：1000-3428(2022)09-0020-08　　文献标志码：A　　中图分类号：TP309

V2V车联网中隐私保护性异构聚合签密方案

牛淑芬[1]，闫　森[1]，吕锐曦[2]，周思玮[1]，张美玲[1]

（1.西北师范大学 计算机科学与工程学院，兰州 730070；2.西北师范大学 数学与统计学院，兰州 730070）

摘　要：随着5G/6G移动通信技术的发展，车联网对于车辆对基础设施、车辆对车辆之间快速交换信息的要求明显提高。然而，在5G/6G网络切片技术中，不同的网络切片采用不同的密码体制，从而会形成异构网络通信。异构车联网可以实现车辆信息的即时共享，但开放的无线通信通道使车辆隐私信息易被泄露，这需要保证共享数据的机密性和完整性。提出一种隐私保护性异构聚合签密方案。该方案使用异构签密技术，在公钥基础设施和基于身份的密码系统(IBC)网络切片环境中可实现不同密码系统注册车辆之间的异构安全通信，同时采用聚合技术，在IBC环境中的车辆将接收到的密文消息进行聚合并对其解密。为确保解密后的密文消息完整，接收车辆对消息进行批量验证，以减少解签密过程所需的时间及传输量。在随机预言模型下，该方案对适应性选择密文攻击具有不可区分性，对适应性选择消息攻击具有存在性与不可伪造性。实验结果表明，相比基于边缘计算的无证书聚合签密方案与车联网高效签密方案，该方案在发送车辆对消息进行签密的阶段中所用时间减少了18.91%~63.12%，在接收车辆对密文进行解签密的阶段中所用时间减少了5.91%~33.66%，具有较高的计算效率。

关键词：车联网；公钥基础设施；基于身份的密码系统；异构聚合签密；5G/6G网络切片

开放科学（资源服务）标志码（OSID）：

中文引用格式：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.

英文引用格式：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.

Privacy-Preserving Heterogeneous Aggregated Signcryption Scheme in V2V Internet of Vehicles

NIU Shufen[1]，YAN Sen[1]，LÜ Ruixi[2]，ZHOU Siwei[1]，ZHANG Meiling[1]

（1.College of Computer Science and Engineering，Northwest Normal University，Lanzhou 730070，China；
2.College of Mathematics and Statistics，Northwest Normal University，Lanzhou 730070，China）

【Abstract】Owing to the emergence of 5G/6G mobile communication technology，the requirements of Internet of vehicles for the rapid exchange of information between Vehicle-to-Infrastructure（V2V），and between Vehicle-to-Increased（V2I）. However，in the 5G/6G network slicing technology，different network slices use different cryptosystems，thus affording heterogeneous network communication.Heterogeneous vehicle networking can realize the instant sharing of vehicle information. However，owing to open wireless communication channels，vehicle privacy information is easily leaked；as such，the confidentiality and integrity of information must be ensured.Hence，this paper proposes a privacy-preserving heterogeneous aggregated signcryption scheme.The proposed scheme uses heterogeneous signcryption technology to achieve heterogeneous secure communication between registered vehicles in different cryptographic systems in Public Key Infrastructure（PKI）and Identity-Based Cryptosystem（IBC）network slicing environments. Using aggregation technology，vehicles in the IBC aggregate and unsigncrypt the received ciphertext messages.To ensure that the unsigncrypted ciphertext message is complete，the receiving vehicle verifies the messages in batches，which obviates the requirement for determining the signcryption process time and transmission volume.When using a random oracle model，the scheme is indistinguishable to adaptively selected ciphertext attacks and existentially unforgeable to adaptively selected message attacks.The experimental results show that，compared with the certificateless aggregation signcrypting scheme based on edge computing and the efficient signcrypting scheme of Internet of vehicles，

基金项目：国家自然科学基金（61772022）。

作者简介：牛淑芬（1976—），女，副教授、博士，主研方向为网络隐私保护、云计算；闫　森，硕士研究生；吕锐曦，本科生；周思玮、张美玲，硕士研究生。

收稿日期：2021-12-06　　**修回日期：**2022-03-03　　**E-mail：**sfniu76@nwnu.edu.cn

计算机工程 www.ecice06.com

the time required by this scheme for signcrypting the message sent by the sending vehicle is 18.91%~63.12% less, and the time required by the receiving vehicle to decrypt the ciphertext is 5.91%~33.66% less, which proves the high computational efficiency of the algorithm.

【Key words】 Internet of vehicles; Public Key Infrastructure(PKI); Identity-Based Cryptosystem(IBC); heterogeneous aggregated signcryption; 5G/6G network slicing

DOI: 10. 19678/j. issn. 1000-3428. 0063450

0　概述

计算机系统和无线网络通信技术的快速发展扩大了智能交通系统的应用范围。车联网正在成为智慧交通的重要组成部分，车联网通过车载单元、路侧采集模块、车路通信单元等设备实现车辆运行数据的实时采集，进而搭建监测大规模车辆实时运行信息的数据平台，并提供各类数据服务。由于交通密度的增加，交通堵塞、事故的发生率也大幅增加，车联网已经成为道路安全和交通管理等特定应用的重要研究领域，它允许车辆和基础设施交换信息，确保道路安全和有效的交通管理。在车联网中，车辆对一切(V2X)的通信主要分为车辆对基础设施(Vehicle-to-Infrastructure，V2I)和车辆对车辆(Vehicle-to-Vehicle，V2V)[1]。V2I通信允许车辆在驾驶时向路边单元(Road-Side-Unit，RSU)发送消息，V2V通信可以实现相邻车辆之间的信息交换。V2V通信技术允许相邻车辆传输或交换信息，可以提高道路安全，减少交通拥堵，提供高效的交通管理。目前，V2V通信中存在的主要问题是如何提高数据交换的准确性和及时性。明文信息很容易被截获和篡改，车辆无法区分收到的信息是否真实，并且车辆更愿意相信经过认证的机密信息。因此，消息的认证和抗篡改成为V2V安全通信最重要的要求。

在车联网通信中最重要的是安全性要求，如机密性、车辆身份验证、消息的完整性和不可否认性。在一般情况下，机密性通过加密方案获得，车辆身份验证、完整性和不可否认性通过数字签名方案[2-4]获得。车载自组网(Vehicular Ad-hoc Networks，VANET)中的安全消息需要签名，但不需要加密。然而，在广播网络中，这样的消息可能会被窃取或截获。因此，需要确保恶意的第三方不能轻易获得该消息的内容。解决这个问题的一种方法是使用签名加密，它不仅按照传统方法的要求对消息进行签名，而且还对其进行加密。因此，在车联网中使用签密是必要的。签密作为一种新的密码原语于1997年由ZHENG[5]提出，它可以将数字签名和加密同时实现，其成本要比签名后加密或加密后签名的成本小得多。

随着移动通信行业的发展，5G/6G网络成为目前研究的热点。为满足5G/6G车联网的不同需求，人们引入网络切片技术[6-8]。由于不同的网络切片可能使用不同的密码系统和密码系统参数，研究人员提出了异构签密方案。2010年，SUN等[9]提出异构系统签密，并对其进行了安全性证明，但他们的方案容易受到内部攻击，并且也不能实现不可否认性。文献[10]提出一种针对内部攻击的异构签密方案。然而，该方案只允许基于身份的密码系统(IBC)中的车辆发送消息给公钥基础设施(PKI)中的接收车辆，并且没有考虑发送方的隐私。文献[11]提出两种异构签密方案来保证VANET中异构V2V通信的安全：一种方案是PKI中的车辆将消息发送给IBC中的车辆；另一种方案是将两者的身份进行互换。然而，在这两种方案中，发件人的隐私并没有得到保证。文献[12]提出了两个与文献[9]方案相似的签密方案，保证了VANET中异构V2V通信的安全，但不能保证车辆的隐私和可追溯性。此外，它们不支持对多个密文的批处理解签密。文献[13]提出了4种签密方案来保证异构V2I通信的安全，因为这些方案具有较大的计算量，并不适用于V2V网络。文献[14]提出基于边缘计算的无证书聚合签密方案，虽然无证书密码体制可以防止公钥替换攻击以及密钥托管问题，但其伪身份的产生、车辆与路边单元的传输都需要很长的计算时间，不能及时进行通信。文献[15]提出一种适用于车联网的高效签密方案，虽然没有使用双线性对运算，但采用大量的指数、乘法运算，并且该方案只考虑了一对一的通信，未考虑多个发送者的情况。

为满足车联网场景中对时延及可靠性的需求，本文将网络切片与车联网相结合，提出一种PKI和IBC公钥密码系统之间多对一的异构签密方案，确保在PKI密码体制网络中将多个车辆的消息传输到IBC网络中的车辆。该方案使用聚合签密技术对车辆的多个消息同时进行签密验证，以提高算法执行效率，降低通信和存储成本。

1　相关工作

1.1　V2X通信

车载自组网是一种移动自组织网络，它允许车辆和基础设施交换信息，确保道路安全和有效的交通管理。在VANET中，每辆车辆都与相邻的车辆以及RSU进行通信，这种通信类型通常被称为V2X通信，可以分为以下两种通信方式：

1)车辆与基础设施之间的通信。在V2I通信中，主要是RSU等基础设施与道路内的每辆车辆之间的通信，车辆将交通信息发送给RSU处理，RSU与其通信范围内的车辆进行通信。V2I系统模型如图1所示。

计算机工程 www.ecice.com

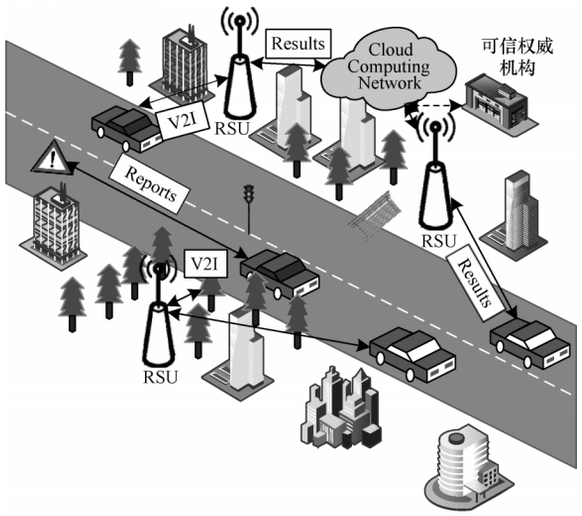

图1 V2I系统模型

Fig.1 V2I system model

2)车辆与车辆之间的通信。V2V通信支持道路状态信息广播,即使没有网络基础设施覆盖,车辆也可以进行通信,V2V系统模型如图2所示。车辆将自己的位置和方向发送给其他车辆,车辆也可以接收或交换交通信息,如位置信息、道路拥挤情况等。V2V通信不依赖于RSU的位置,更加灵活自由。

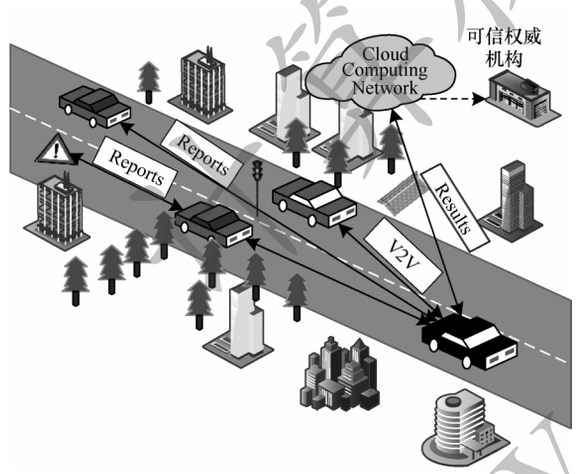

图2 V2V系统模型

Fig.2 V2V system model

1.2 5G/6G网络切片

网络切片是指利用软件定义网络(Software Designed Network,SDN)或网络功能虚拟化(Network Function Virtualizaiton,NFV)[16]等技术,将一个物理基础设施的计算和通信资源划分并优化为多个独立的逻辑网络,提供各种应用服务。NFV使用通用硬件实现网络功能的低成本需求,而SDN对控制平面与数据平面进行分离,以提供高效、灵活的资源管理[17]。因此,基于NFV和SDN的网络切片可以被认为是5G/6G网络中不可或缺的网络技术。一方面,网络切片可以挖掘和释放通信技术的潜力,提高效率,降低成本;另一方面,网络切片在车联网、智慧城市、工业制造等领域具有潜在的市场需求。

5G/6G网络切片可以分别满足车联网对超低时延、高可靠性与超长数据包、超高数据速率和超高可靠性等具体应用的要求[18-20]。从本质上讲,它将物理网络划分为多个虚拟网络,每个虚拟网络对应时延、带宽和安全性等业务需求中的一个,满足不同的网络应用场景。此外,随着网络切片代理[21]的引入,5G/6G网络切片技术可以实现网络资源的共享,将原本相互独立的网络资源进行整合和分配,从而实现相应特殊需求的网络资源的实时动态调度。

2 预备知识

2.1 双线性映射

设两个不同的循环群G_1和G_2分别为加法群和乘法群,其阶是相同素数p。设$e:G_1\times G_1\to G_2$为一个双线性对的函数,其中P是G_1的生成元,满足下列双线性对的性质[22-23]:

1)双线性。存在任意的$a,b\in\mathbb{Z}_p^*$,都有$e(aP,bQ)=e(P,Q)^{ab}$。

2)非退化性。存在$P,Q\in G_1$,使得$e(P,Q)\neq 1$。

3)可计算性。对于任意的$P,Q\in G_1$,存在有效的算法能够计算$e(P,Q)$。

2.2 困难问题

相关的困难问题主要有以下2点:

1)决策性Diffie-Hellman问题(DDHP)。在循环加法群G_1和其生成元P的基础下,给定(P,aP,bP,cP),其中$a,b,c\in\mathbb{Z}_p^*$,求解$ab=c \bmod p$。

2)离散对数问题(DLP)。给定$(P,\alpha P)$,在有限循环群G_1及其生成元P的基础上对$\alpha\in\mathbb{Z}_p^*$进行求解。

3 系统模型与安全模型

3.1 系统模型

本文考虑从PKI密码体制到IBC密码体制的V2V异构车辆通信模型,实体包括可信权威(TA)机构、路边单元(RSU)、车辆(V)、证书权威(CA)机构、密钥生成中心(PKG),如图3所示。从图3可以看出,实体可以通过不同的有线通信技术(如以太网)或无线替代技术(如DSRC协议[24])通信。

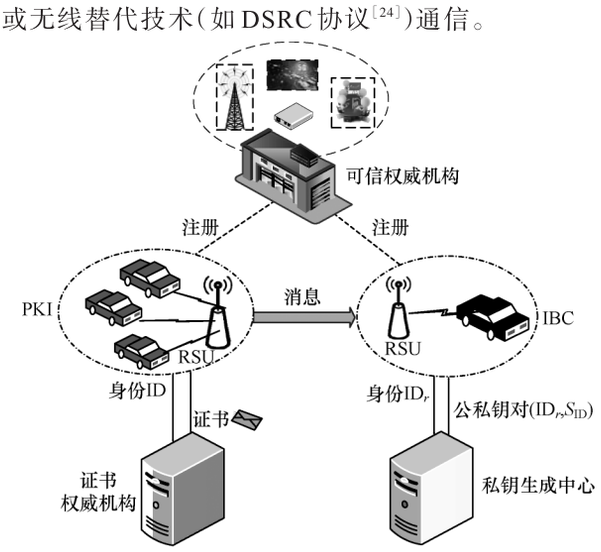

图3 本文系统模型

Fig.3 The system model of this paper

www.ecice06.com

可信权威（TA）机构：在VANET中，其生成和广播公共系统参数以及注册RSU和车辆。

路边单元（RSU）：通过无线信道与被覆盖区域内的车辆以及其他的RSU进行通信。RSU将车辆发送过来的信息进行验证，并将其发送给其他车辆。

车辆（V）：在每辆车辆上安装OBU等无线通信装置，捕捉附近车辆或路边传感器的信息。在PKI环境中的发送方车辆，向IBC环境中的邻近车辆和RSU发送消息。

证书权威（CA）机构：对PKI中的用户进行身份验证，并对用户的公钥和身份信息进行签名，产生公钥证书，将公钥证书发送给用户。

密钥生成中心（PKG）：根据用户的身份标识产生相对应的私钥，然后通过安全信道发送用户的公私钥对。

3.2　算法定义

本文算法定义如下：

系统建立：该算法由TA执行，将安全参数k输入，将系统参数params、系统公钥mpk和主密钥msk输出。

密钥生成：PKI系统中的用户随机选取私钥sk并计算对应的公钥pk。CA收到用户的身份和公钥后，对其进行签名并生成公钥证书。

密钥提取：IBC系统中的用户将身份ID_U发送给PKG，PKG根据身份信息计算相对应的私钥S_{ID_U}，而身份ID_U是用户的公钥pk。

签密算法：发送者根据系统参数params、消息m_i和接收者的公钥pk_r，使用自己的私钥sk_s生成密文σ_i。

聚合签密算法：接收者根据收到的密文σ_i和发送者的公钥pk_s，使用自己的公钥ID_r生成聚合签密密文σ。

聚合解签密算法：接收者通过给定的密文σ和发送者的公钥pk_s，用自己的私钥S_{ID_r}对σ解签密，输出明文m_i。

3.3　安全模型

为保证消息传输过程的安全性，方案必须满足以下需求及定义的两种安全模型。通过在多项式时间模拟敌手A和挑战者C之间的游戏来定义消息的机密性和不可伪造性。

游戏1（机密性）　通过使用挑战者C和敌手A分3个阶段进行游戏，证明适应性选择密文攻击具有不可区分性。

初始阶段：通过给定安全参数k，C可以获得系统参数，通过系统建立算法，同时执行密钥生成算法可以计算出n个发送者的公私钥对(pk_{s_i}, x_{s_i})，C将系统参数和发送者的公钥pk_{s_i}发送给A。

阶段1：C选择特定的目标身份为ID_r^*，将其发送给敌手A，A进行如下的询问。

密钥提取询问：敌手A对选择的身份ID进行询问，若$\mathrm{ID}_r \neq \mathrm{ID}_r^*$，C获得其私钥$S_{\mathrm{ID}}$并发送给A。

解签密询问：A将接收者身份ID_r和密文σ提交给C，若$\mathrm{ID}_r = \mathrm{ID}_r^*$，则输出$\perp$，否则C对密文$\sigma$运行解签密算法，将恢复的消息发送给A。

挑战阶段：在阶段1询问结束后，敌手A发起适应性预言询问，生成长度相同的明文m_0、m_1以及接收者的身份ID_r^*，但A不能通过询问获得目标身份的私钥，挑战者C随机选择$\beta \in \{0,1\}$，返回签密密文给A。

阶段2：A收到密文σ^*，发起适应性预言询问，并且A不能用ID_r^*和σ^*进行解签密询问来获取相对应的明文。

猜测阶段：当阶段2结束后，A通过输出一个比特β'来猜测β，若$\beta' = \beta$，那么A赢得游戏。

游戏2（不可伪造性）　通过使用挑战者C和敌手A分3个阶段进行游戏，证明在适应性选择消息攻击下具有存在性与不可伪造性。

初始阶段：挑战者C通过运行算法，输入安全参数k，将生成的系统公共参数params和n个发送者的公私钥对$\left(pk_{s_i}^*, sk_{s_i}^*\right)$发送给A。

攻击阶段：敌手A将接收者的身份ID_r和消息m_i通过发送给挑战者C并发起适应性预言询问，C对询问做出响应，得到密文σ_i，并将密文发送给A。

伪造阶段：A返回n个发送者的身份ID_i、1个接收者的身份ID_r^*和密文σ_i^*。若σ_i^*不是通过ID_i和ID_r^*相关的密钥询问产生，解签密询问输出的结果不为$\perp$，且接收者身份ID_r^*的签密询问没有被询问，则A获得比赛胜利。

4　本文方案

4.1　方案构造

系统建立：该方案由TA执行，输入安全参数1^k，TA执行3种算法。

1）输出两个阶为素数p的循环群G_1和G_2，其中G_1是加法群，其生成元为P，G_2是乘法群，TA随机选择一个主密钥$s \in Z_p^*$，计算系统公钥$P_0 = sP$。

2）选择3个单向哈希函数$H_1: \{0,1\}^* \to Z_p^*$，$H_2: \{0,1\}^* \times G_2 \to G_1$，$H_3: G_2 \to \{0,1\}^n$，$n$为签密消息的长度。

3）输出一个双线性映射$e: G_1 \times G_1 \to G_2$，计算$K = e(P,P)$，将$\{G_1, G_2, n, P, P_0, K, H_1, H_2, H_3\}$系统参数公开，并对主密钥$s$进行保密。

密钥生成：在PKI环境中，发送的车辆随机选择一个数$x_{s_i} \in \mathbb{Z}_p^*$为自己的私钥，计算对应的公钥$pk_{s_i} = x_{s_i}P$，将身份和公钥发送给CA验证生成公钥证书，并将证书发送给发送的车辆，其公私钥为$\left(pk_{s_i}, x_{s_i}\right)$。

密钥提取：在IBC环境中，PKG可以计算接收车辆的私钥$S_{\mathrm{ID}_r} = \dfrac{1}{H_1\left(\mathrm{ID}_r\right) + s}$，$P$通过其身份标识$\mathrm{ID}_r$，

计算机工程 www.ecice.com

将公私钥$(\mathrm{ID}_r, S_{\mathrm{ID}_r})$通过安全信道发送给接收的车辆。

签密算法：对发送的消息m_i，发送车辆的私钥$sk_{s_i}=x_{s_i}$，接收车辆的身份ID_r，该签密算法如下：

1）随机选取$x_i \in \mathbb{Z}_p^*$。

2）计算$r_i=K^{x_i}$。

3）计算$C_i=m_i \oplus H_3(r_i, H_1(ID_r))$。

4）计算$h_i=H_2(m_i, r_i)$。

5）计算$S_i=h_i x_{s_i}-x_i P$。

6）计算$T_i=x_i(H_1(ID_r)P+P_0)$。

发送车辆将签密密文$\sigma_i=(C_i, S_i, T_i)$发送给接收车辆。

聚合签密算法：接收车辆充当聚合者，收到消息m_i对应的签密密文$\sigma_i=(C_i, S_i, T_i)$，计算$S=\sum_{i=1}^{m} S_i$，则聚合密文为$\sigma=(C_i, S, T_i)$。

聚合解签密算法：接收车辆收到的密文σ_i与发送车辆的公钥pk_s，用自己的私钥对密文进行解密，该聚合解签密算法如下：

1）计算$r_i=e(T_i, S_{\mathrm{ID}_r})$。

2）恢复$m_i=C_i \oplus H_3(r_i, H_1(\mathrm{ID}_r))$。

3）恢复$h_i=H_2(m_i, r_i)$。

4）计算$R=\prod_{i=1}^{m} r_i$。

5）检查等式$R \cdot e(S, P)=e\left(\sum_{i=1}^{m} h_i, \sum_{i=1}^{m} pk_{s_i}\right)$是否成立，若等式成立，则接收消息$m_i$。

4.2 正确性证明

下面将对本文方案的正确性进行证明，当且仅当通过签密算法可以计算异构签密密文$\sigma_i=(C_i, S_i, T_i)$和异构聚合签密密文$\sigma=(C_i, S, T_i)$，即下列等式验证成立：

1）验证者检查等式$r_i \cdot e(S_i, P)=e(h_i, pk_{s_i})$，可以验证签密密文$\sigma_i=(C_i, S_i, T_i)$的正确性。

$$
\begin{aligned}
r_i \cdot e(S_i, P) &= r_i \cdot e(h_i x_{s_i}-x_i P, P)= \\
& r_i \cdot e(h_i x_{s_i}, P) \cdot e(-x_i P, P)= \\
& e(P, P)^{x_i} \cdot e(h_i, x_{s_i} P) \cdot e(P, P)^{-x_i}= \\
& e(h_i, x_{s_i} P)= \\
& e(h_i, pk_{s_i})
\end{aligned}
$$

2）验证该异构聚合签密方案的一致性。

$$
\begin{aligned}
e(T_i, S_{\mathrm{ID}_r}) &= e(x_i(H_1(\mathrm{ID}_r)P+P_0), S_{\mathrm{ID}_r})= \\
& e\left(x_i(H_1(\mathrm{ID}_r)+s)P, \frac{1}{H_1(\mathrm{ID}_r)+s} P\right)= \\
& e=K^{x_i}=r_i
\end{aligned}
$$

则：

$$
\begin{aligned}
R \times e(S, P) &= \prod_{i=1}^{m} r_i \times e\left(\sum_{i=1}^{m} S_i, P\right)= \\
& \prod_{i=1}^{m} r_i \times e\left(\sum_{i=1}^{m}(h_i x_{s_i}-x_i P), P\right)= \\
& \prod_{i=1}^{m} r_i \times e\left(\sum_{i=1}^{m} h_i x_{s_i}, P\right) \times e\left(-\sum_{i=1}^{m} x_i P, P\right)= \\
& \prod_{i=1}^{m} r_i \times e\left(\sum_{i=1}^{m} h_i, \sum_{i=1}^{m} x_{s_i} P\right) \times e(P, P)^{-\sum_{i=1}^{m} x_i}= \\
& K^{\sum_{i=1}^{m} x_i} \times e\left(\sum_{i=1}^{m} h_i, \sum_{i=1}^{m} x_{s_i} P\right) \times K^{-\sum_{i=1}^{m} x_i}= \\
& e\left(\sum_{i=1}^{m} h_i, \sum_{i=1}^{m} x_{s_i} P\right)=e\left(\sum_{i=1}^{m} h_i, \sum_{i=1}^{m} pk_{s_i}\right)
\end{aligned}
$$

5 安全性证明

本节基于决策性Diffie-Hellman问题以及离散对数问题假设，证明本文方案在随机预言模型下的机密性与不可伪造性。

5.1 机密性

定理1 在多项式时间t内，若敌手A能够以不可忽略的优势ε获得游戏1的胜利，则挑战者C能够解决DDHP困难问题。

初始阶段：挑战者C建立该算法，输入安全参数k，生成系统公共参数，同时C获取到n个发送者的公私钥对(x_{s_i}, pk_{s_i})，通过使用密钥生成算法，将系统公共参数和发送者的公钥pk_{s_i}发送给A。

阶段1：在这个阶段中，A进行多次询问，而C通过保存3张列表L_1、L_2、L_3，模拟A对随机预言机H_1、H_2、H_3的询问来回答A的询问，其中H_1的询问是不同的，并对目标身份ID_r^*进行H_1询问。具体询问如下：

H_1-询问：列表L_1由元组$\{\mathrm{ID}_r, \alpha_r, pk_r, sk_r, \mathrm{coin}\}$组成，当A使用$\mathrm{ID}_r$进行询问时，C检查$\{\mathrm{ID}_r, \alpha_r, pk_r, sk_r, \mathrm{coin}\}$是否在列表$L_1$中，若在列表$L_1$中，则$pk_r$返回A的值；否则C产生一个随机数$\mathrm{coin} \in \{0, 1\}$，使得$\Pr[\mathrm{coin}=0]=\delta$，$\Pr[\mathrm{coin}=1]=1-\delta$，若$\mathrm{coin}=1$，则C计算$pk_r=bP$，$\alpha_r=\perp$，$sk_r=\perp$；否则C随机选择$\alpha_i \in \mathbb{Z}_p^*$，计算$pk_r=\alpha_r P$，$sk_r=\alpha_r aP$，将其增加到列表$L_1$中，将$pk_r$发送到A中。

H_2-询问：元组(r_i, m_i)在列表L_2中，挑战者C判断元组(r_i, m_i, ρ_i)是否出现在列表L_2中，若列表L_2存在，则直接返回；否则，C选择$\rho_i \in \mathbb{Z}_p^*$，将$(r_i, m_i, \rho_i)$补充到列表$L_2$中。

H_3-询问：元组$\{C_i, pk_r, r_i\}$在列表L_3中，挑战者C判断元组(C_i, pk_r, r, ξ_i)是否出现在列表L_3中，若在表中则返回相应的ξ_i作为H_3的值；否则挑战者C随机选择整数$\xi_i \in \mathbb{Z}_p^*$，将元组(C_i, pk_r, r, ξ_i)存储在列表L_3中，返回ξ_i的值。

计算机工程 www.ecice06.com

密钥提取询问：当A对选择身份ID_r进行询问时，若$\mathrm{ID}_r \neq \mathrm{ID}_r^*$，则C需要执行$H_1$询问，从表$L_1$获得$\{\mathrm{ID}_r, \alpha_r, pk_r, sk_r, \mathrm{coin}\}$并返回私钥，否则输出$\perp$。

解签密询问：A把密文σ、发送者的公钥pk_{s_i}、接收者的身份ID_r发送给C。若$\mathrm{ID}_r \neq \mathrm{ID}_r^*$，则C对$\sigma$进行解签密，然后将结果发送给A，否则输出$\perp$。

挑战阶段：阶段1的结束时间由A决定。A产生2个等长的明文m_0、m_1和1个接收者的身份ID_r^*。注意：该ID_r^*不能在阶段1询问。C输出一个随机的比特$\beta' \in \{0,1\}$，并计算$\sigma^* = \mathrm{Signcrypt}\left(m_\beta, x_{s_i}, \mathrm{ID}_r^*\right)$。最后，$C$将$\sigma^*$发送给A。

阶段2：若A不对ID_r^*进行密钥提取询问，不提交通过对σ^*进行解签密询问获得的明文，那么A可以像阶段1一样进行适应性的询问。

猜测：当所有询问结束后，A得到一个$\beta' \in \{0,1\}$。如果$\beta' = \beta$，则A赢得这次游戏并且优势为$\mathrm{Adv}(A) = \left| \Pr[\beta' = \beta] - \frac{1}{2} \right|$。

5.2　不可伪造性

定理2　在随机预言模型下，假设DLP问题困难，通过使用Forking引理[25]来证明本文方案在适应性选择消息攻击下是存在性不可伪造的。

引理1　在多项式时间t内，如果敌手A赢得游戏2，那么挑战者C以不可忽略的概率ε'解决DLP困难问题。

证明　利用Forking引理来证明引理1。DLP问题挑战者C通过使用敌手A解决一个给定的DLP实例问题$(P, \alpha P)$，即计算α。

初始阶段：C首先运行系统并建立算法得到系统参数，密钥生成算法得到n个发送者的公钥$pk_{s_i}^*$，将其发送给敌手A。

攻击阶段：H_1、H_2、H_3询问中产生的数据被分别保存在列表L_1、L_2、L_3中，并且这些预言机被保持在C中，同时A可以对H_1、H_2、H_3进行适应性询问。

H_1-询问：若$H_1(\mathrm{ID}_i)$已经被询问过，则返回L_1的值；否则C返回一个随机数$h_{1,i} \in \mathbb{Z}_p^*$，在列表$L_1$增加$(\mathrm{ID}_i, h_{1,j})$。

H_2-询问：列表L_2由$(m_i, r_i, h_{2,i})$组成，当A对H_2与$h_{2,i}$进行询问时，如果$h_{2,i}$已经在列表L_2中并且被询问过，则直接返回；否则，C随机选择$h_{2,i} \in G_1$并将$(m_i, r_i, h_{2,i})$增添到列表L_2中。

H_3-询问：列表L_3由$(r_i, h_{3,i})$组成，A对H_3和$h_{3,i}$询问，如果从列表L_3已经询问到$h_{3,i}$，则直接返回到列表L_3；否则，C选择$h_{3,i} \in \{0,1\}^n$，在列表L_3中加入$(r_i, h_{3,i})$。

签密询问：A对消息进行签密询问时，将发送车辆和接收车辆的身份$(\mathrm{ID}_i, \mathrm{ID}_r)$以及两者之间传递的消息$m_i$发送给C。

C执行以下操作：

1）随机选择$\theta_i, t_i \in \mathbb{Z}_p^*$。

2）计算$h_i = t_i P$。

3）计算$S_i = \theta_i S_{\mathrm{ID}_r}$。

4）计算$T_i = \alpha t_i \left(H_1(\mathrm{ID}_r) P + P_0\right) - \theta_i P$。

5）计算$r_i = e\left(T_i, S_{\mathrm{ID}_r}\right)$。

6）计算$C_i = m_i \oplus H_3\left(r_i, H_1(\mathrm{ID}_r)\right)$。

7）返回$\sigma_i = (C_i, S_i, T_i)$给敌手A。

伪造阶段：A返回n个发送者的身份ID_i、接收者的身份ID_r^*、关于消息m_i的密文σ_i。当C收到密文$\sigma^* = (C_i^*, S^*, T_i^*)$时，如果$\mathrm{ID}_r = \mathrm{ID}_r^*$，则输出$\perp$；否则通过Forking引理，并同时输出另一个聚合密文$\sigma'^* = (C_i^*, S'^*, T_i^*)$，使得满足聚合签密等式，即有：

$$e\left(\sum_{j=1, j\neq i}^{m} h_j^* + h_i^*, pk_{s_i}^*\right) \cdot e\left(S^*, P\right)^{-1} = e\left(\sum_{j=1, j\neq i}^{m} h_j^* + h'^*_i, pk_{s_i}^*\right) \cdot e(S'^*, P)^{-1}$$

其中：$S^* = \sum_{j=1, j\neq i}^{m} S_j^* + S_i^*$；$S'^* = \sum_{j=1, j\neq i}^{m} S'^*_j + S'^*_i$。

可得到$\alpha = \left(h_i^* - h'^*_i\right)^{-1}\left(S_i^* - S'^*_i\right)$，使DLP困难问题得到解决。

6　性能分析

为分析本文方案的计算成本，将其与聚合签密方案[14]、签密方案[15]在签密阶段和解签密阶段进行比较。

6.1　理论分析比较

本文提出基于PKI密码系统传输与基于IBC密码系统的V2V异构聚合签密方案，而文献[14]提出了基于边缘计算的无证书V2I聚合签密方案，两者采用不同的密码体制和车联网环境；文献[15]方案与本文所提方案在本质上有所不同，本文提出的是多对一的聚合签密方案，而文献[15]没有使用聚合技术。本文和其他两个方案虽然采用的是相同的主密钥，但采用不同的系统参数，使得本文方案在计算成本、计算效率与安全性方面较优。现将本文方案所采用的指数运算(T_e)、哈希运算(T_h)、乘法运算(T_m)、双线性对运算(T_p)、加法运算(T_a)和文献[14-15]方案采用的运算进行对比，并对其进行理论分析。

表1是签密阶段的计算量比较，可以看出当传输消息时，各方案计算量由大到小依次为本文方案、文献[14-15]方案；在签密阶段，本文方案比文献[14]方案增加了指数计算，但减少了大量的乘法与加法运算，并且随着消息个数的增加，本文方案在乘法、加法计算量方面都远小于文献[14]方案。与文献[15]方案相比，本文方案采用聚合签密技术，在签密阶段需要对消息进行聚合，导致乘法与加法的效率有所降低，但减少了指数运算的计算量，总体上其计算效率较高。

计算机工程 www.ecice06.com

表1 签密阶段的计算量比较

Table 1 Computation comparison of signcryption stage

方案	1个消息	m个消息
文献[14]方案	$3T_h+7T_m+4T_a$	$3mT_h+7mT_m+(3m+2)T_a$
文献[15]方案	$3T_e+2T_h+2T_m+2T_a$	$3mT_e+2mT_h+2mT_m+2mT_a$
本文方案	$T_e+3T_h+4T_m+T_a$	$mT_e+(2m+1)T_h+(3m+1)T_m+(2+m)T_a$

表2是解签密阶段的计算量比较，当发送单个消息时，本文方案比文献[14]方案减少了5个乘法运算，解密速度较快；与文献[15]方案相比，本文使用了双线性对运算，减少了乘法运算。随着发送消息个数的增加，本文方案在双线性对、哈希、加法以及乘法运算的使用上都远远少于文献[15]方案。相比文献[14]方案，虽然本文方案采用运算时间较长的双线性对运算，但使用聚合签密技术减少了其运算量。

表2 解签密阶段的计算量比较

Table 2 Computation comparison of unsigncryption stage

方案	1个消息	m个消息
文献[14]方案	$3T_p+3T_h+6T_m+T_a$	$3mT_p+3mT_h+6mT_m+4mT_a$
文献[15]方案	$4T_e+2T_h+3T_m+T_a$	$4mT_e+2mT_h+3mT_m+mT_a$
本文方案	$3T_p+3T_h+T_m+T_a$	$(m+2)T_p+(2m+1)T_h+mT_m+3mT_a$

6.2 数值实验分析

本节对本文方案进行数值模拟实验。在双线性对密码[26]基础上使用C语言在2.9 GHz CPU、16 GB RAM PC机的Linux系统中进行数值模拟实验，如表3所示。

表3 系统配置和数学参数

Table 3 System configuration and mathematical parameters

配置	参数
CPU	AMD-Ryzen-7-4800H CPU@2.9 GHz
操作系统	Linux 和 Ubuntu 10.10
程序语言	C语言
程序库	Pairing-Based Cryptography
参数类型	Type A
基域/bit	512
椭圆曲线次数	2

1)本文方案的计算效率。由于消息个数影响签密与解签密算法的运行时间，在分别统计签密消息m为20、40、60、80、100时，执行整个算法、签密算法和解签密算法的时间如表4所示。

表4 本文方案的计算效率

Table 4 Computational efficiency of the proposed scheme s

m	算法时间	签密时间	解签密时间
20	0.449 1	0.180 1	0.166 4
40	0.922 1	0.378 4	0.372 4
60	1.316 3	0.541 4	0.552 0
80	1.753 2	0.673 3	0.717 9
100	2.213 8	0.935 2	0.958 8

2)比较分析。为减少实验环境因素导致的误差，将程序运行50次取其平均值作为其实验结果。对本文方案、文献[14-15]方案所提出的签密及解签密算法进行比较，结果分别如图4和图5所示。

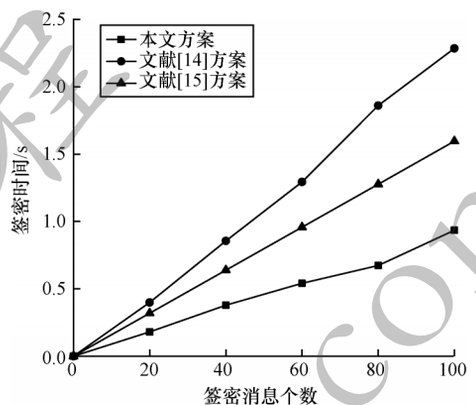

图4 不同方案签密阶段的时间成本

Fig.4 Time cost of signcryption stage for different schemes

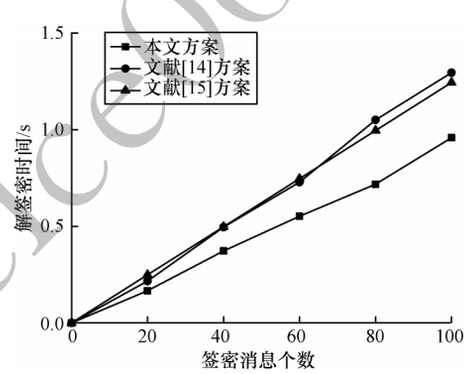

图5 不同方案解签密阶段的时间成本

Fig.5 Time cost of unsigncryption stage for different schemes

从图4可以看出，签密时间随着签密消息个数的增加而延长，但本文方案具有较短的时间。与文献[14]方案相比，两者的车联网环境不同，本文在V2V的车联网环境中进行签密，而文献[14]方案在V2I环境中，车辆与车辆之间的距离相对较短，两者的速度相对也比较低。因此，车辆与车辆在传输环境和传输速度方面优于RSU与车辆之间。虽然本文在签密阶段增加了指数运算，但大幅降低了加法与乘法运算的使用，导致接收车辆进行签密时所用时间更短。文献[15]方案是发送车辆来发送消息，为了公平比较，将其发送者进行倍乘，由于本文方案进行聚合签密，只用执行一次签密算法，而文献[15]方案的接收车辆执行签密算法的次数是根据发送车辆的数量来执行的，导致这个签密的时间比较长。因

计算机工程 www.ecice.com

此，本文方案的签密效率远高于[14-15]方案。

从图5可以看出，本文方案的解签密效率比文献[14-15]方案都要高，文献[14]提出一种基于边缘计算的无证书聚合签密方案，由于发送方与接收方都需匿名通信，导致在解签密时采用较多的乘法运算，使其在解签密阶段所用的时间较长，并且本文方案的传输效率比文献[14]方案要高，因为不用考虑RSU的地理位置，可以及时将信息传递到接收车辆，不用等待路边单元处理完的信息，而文献[15]方案接收车辆解签密的次数与消息的数量成正比，使方案的计算和传输效率都比较低。由于本文采用的是聚合签密，接收车辆可以进行批验证处理，并对接收到的密文进行聚合解签密，只用执行一次算法。

7　结束语

本文分析5G/6G车联网中消息传输的隐私问题与传输速率问题，将网络切片与车联网相结合，提出一种面向V2V车联网的隐私保护性异构聚合签密方案，以适用于多对一的应用场景。本文使用异构签密技术，确保基于PKI环境与IBC环境的5G/6G切片中车辆之间的安全通信，同时使用聚合签密，允许接收车辆同时对多个密文进行解密验证。实验结果表明，该方案在签密与解签密阶段的计算效率高于基于边缘计算的无证书聚合签密方案。下一步将在本文方案中加入边缘计算，以降低系统实体间通信时延，增强车联网的计算能力。

参考文献

[1] ZHOU J S, TIAN D X, WANG Y P, et al. Reliability-optimal cooperative communication and computing in connected vehicle systems[J]. IEEE Transactions on Mobile Computing, 2020, 19(5): 1216-1232.

[2] ALI I, GERVAIS M, AHENE E, et al. A blockchain-based certificateless public key signature scheme for vehicle-to-infrastructure communication in VANETs[J]. Journal of Systems Architecture, 2019, 99: 101636.

[3] ALI I, LAWRENCE T, LI F G. An efficient identity-based signature scheme without bilinear pairing for vehicle-to-vehicle communication in VANETs[J]. Journal of Systems Architecture, 2020, 103: 101692.

[4] ALI I, LI F G. An efficient conditional privacy-preserving authentication scheme for vehicle-to-infrastructure communication in VANETs[J]. Vehicular Communications, 2020, 22: 100228.

[5] ZHENG Y L. Digital signcryption or how to achieve cost (signature & encryption) ≪ cost (signature) +cost (encryption)[C]//Proceedings of CRYPTO'97. Berlin, Germany: Springer, 1997: 165-179.

[6] CAMPOLO C, MOLINARO A, IERA A, et al. 5G network slicing for vehicle-to-everything services[J]. IEEE Wireless Communications, 2017, 24(6): 38-45.

[7] KOTULSKI Z, NOWAK T W, SEPCZUK M, et al. Towards constructive approach to end-to-end slice isolation in 5G networks[J]. EURASIP Journal on Information Security, 2018(2): 1-23.

[8] FOUKAS X, PATOUNAS G, ELMOKASHFI A, et al. Network slicing in 5G: survey and challenges[J]. IEEE Communications Magazine, 2017, 55(5): 94-100.

[9] SUN Y X, LI H. Efficient signcryption between TPKC and IDPKC and its multi-receiver construction[J]. Science China Information Sciences, 2010, 53(3): 557-566.

[10] HUANG Q, WONG D S, YANG G M. Heterogeneous signcryption with key privacy[J]. The Computer Journal, 2011, 54(4): 525-536.

[11] LI F G, ZHANG H, TAKAGI T. Efficient signcryption for heterogeneous systems[J]. IEEE Systems Journal, 2013, 7(3): 420-429.

[12] LI Y P, QI Y J, LU L F. Secure and efficient V2V communications for heterogeneous vehicle ad hoc networks[C]//Proceedings of 2017 International Conference on Networking and Network Applications. Washington D. C., USA: IEEE Press, 2018: 93-99.

[13] ZHOU F, LI Y, DING Y. Practical V2I secure communication schemes for heterogeneous VANETs[J]. Applied Sciences, 2019, 9(15): 3131.

[14] RASHEED I, ZHANG L, HU F. A privacy preserving scheme for vehicle-to-everything communications using 5G mobile edge computing[J]. Computer Networks, 2020, 176: 107283.

[15] ELHABOB R, ADEL A, ELTAYIEB N, et al. An efficient signcryption scheme for vehicular satellite-based networks[J]. Journal of Karary University for Engineering and Science, 2021, 56(8): 1454-1461.

[16] TANG L, ZHAO G F, WANG C M, et al. Queue-aware reliable embedding algorithm for 5G network slicing[J]. Computer Networks, 2018, 146: 138-150.

[17] 侯建星，李少盈，祝宁. 网络切片在5G中应用分析[C]//中国通信学会信息通信网络技术委员会2015年年会论文集. 北京：中国通信学会普及与教育工作委员会，2015：179-185.
HOU J X, LI S Y, ZHU N. Network slices are analyzde in 5G application[C]//Proceedings of 2015 Annual Meeting of the Information and Communication Network Technology Committee of the China Communications Society. Beijing: Popularization and Education Committee of China Communication Society, 2015: 179-185. (in Chinese)

[18] CHEN M, ZHANG Y, HU L, et al. Cloud-based wireless network: virtualized, reconfigurable, smart wireless network to enable 5G technologies[J]. Mobile Networks and Applications, 2015, 20(6): 704-712.

[19] BEKTAS C, MONHOF S, KURTZ F, et al. Towards 5G: an empirical evaluation of software-defined end-to-end network slicing[C]//Proceedings of 2018 IEEE GLOBECOM Workshop. Washington D. C., USA: IEEE Press, 2018: 1-6.

[20] GUO H Z, ZHOU X Y, LIU J J, et al. Vehicular intelligence in 6G: networking, communications, and computing[J]. Vehicular Communications, 2022, 33: 100399.

[21] SAMDANIS K, COSTA-PEREZ X, SCIANCALEPORE V. From network sharing to multi-tenancy: the 5G network slice broker[J]. IEEE Communications Magazine, 2016, 54(7): 32-39.

（下转第36页）

计算机工程 www.ecr.com

（上接第27页）

[22] CHOON J C, HEE C J. An identity-based signature from gap diffie-Hellman groups[C]//Proceedings of International Workshop on Public Key Cryptography. Berlin, Germany: Springer, 2002: 18-30.

[23] BONEH D, FRANKLIN M. Identity-based encryption from the Weil pairing[C]//Proceedings of CRYPTO'01. Berlin, Germany: Springer, 2001: 213-229.

[24] JIANG D, TALIWAL V, MEIER A, et al. Design of 5. 9 GHz DSRC-based vehicular safety communication[J]. IEEE Wireless Communications, 2006, 13(5): 36-43.

[25] POINTCHEVAL D, STERN J. Security arguments for digital signatures and blind signatures[J]. Journal of Cryptology, 2000, 13(3): 361-396.

[26] The pairing-based cryptography library[EB/OL]. [2021-11-03]. https://crypto. stanford. edu/pbc/.

编辑　索书志