车联网中具有多密文等值测试的在线/离线异构签密方案

周美贤，范馨月
（重庆邮电大学通信与信息工程学院，重庆 400065）

摘　要：针对车联网（Internet of vehicles，IoV）中异构加密体制通信问题，提出了一种支持多密文等值测试的在线/离线异构签密方案，实现了无证书密码体制到公钥基础设施的安全通信。所提方案基于椭圆曲线加密（elliptic curve cryptosystem，ECC）构建，利用在线/离线签密机制降低车辆端的计算开销。在云端进行多密文等值测试使接收者只须从云端下载一次重复密文，减轻接收者负担。安全性方面，在随机预言机模型（random oracle model，ROM）下证明不可伪造性和机密性。再采用ProVerif和Scyther工具验证，ProVerif结果表明该方案能够保证消息机密性、身份匿名性与签名正确性，Scyther结果显示未发现有效的攻击路径。性能分析表明，与现有方案相比，该方案在计算与通信开销上更具优势，在密文数量较大时优势更明显，适用于车联网环境。

关键词：车联网；椭圆曲线加密；异构签密；在线/离线；多密文等值测试
中图分类号：TP393；TN918
文献标志码：A
doi: 10.11959/j.issn.1000−0801.2026032

Online/offline heterogeneous signcryption scheme with multi-ciphertext equality test in Internet of vehicles

Zhou Meixian, Fan Xinyue
School of Communication and Information Engineering, Chongqing University of Posts and Telecommunications, Chongqing 400065, China

Abstract: To address the heterogeneous cryptographic communication problem in the Internet of vehicles (IoV), an online/offline heterogeneous signcryption scheme supporting multiple ciphertext equality tests was proposed to achieve secure communication from a certificateless cryptosystem to a public key infrastructure. The scheme was constructed based on elliptic curve cryptosystem (ECC), and the online/offline signcryption mechanism was employed to reduce the computational overhead on vehicles. A multiple ciphertext equality test was performed in the cloud so that the receiver only needed to download the duplicate ciphertext once, thereby reducing the receiver's burden. In terms of security, the scheme was proven under the random oracle model (ROM) to satisfy non-repudiation and confidentiality security. Furthermore, the scheme was formally verified using ProVerif and Scyther tools. The ProVerif results

收稿日期：2025−08−21；**修回日期：**2025−09−15
通信作者：周美贤，S230101220@stu.cqupt.edu.cn
基金项目：国家自然科学基金资助项目（No. 62271096）
Foundation Item: The National Natural Science Foundation of China (No. 62271096)

show that message confidentiality, identity anonymity, and signature correctness are guaranteed, while the Scyther results show that no effective attack paths are found. Performance analysis demonstrates that the scheme achieves lower computational and communication overhead compared with the existing schemes, and the advantages become more significant with an increasing number of ciphertexts, making it suitable for IoV environments.

Key words: IoV, ECC, heterogeneous signcryption, online/offline, multi-ciphertext equality test

0　引言

车联网[1]是基于物联网和智能交通系统的车载网络架构。随着通信技术的发展，特别是5G和蜂窝车到万物通信（cellular-vehicles to everything，C-V2X）技术[2]的成熟，该技术被广泛应用于缓解交通拥堵、快速处理交通事故等突发事件，有效地提升了出行体验和交通效率。车联网技术提升了交通便捷性，但也带来了诸多安全与隐私挑战[3]。车辆通过无线网络与其他车辆及路侧单元（road side unit，RSU）通信。由于无线通信的开放性，数据在传输过程中易被恶意攻击者窃取或篡改，从而引发严重的安全问题[4]。明文传输虽具备实时性优势，但极易遭受中间人攻击，导致敏感信息泄露和数据被篡改[5]。而传统加密机制虽能有效保障数据的机密性，却无法使接收方在不解密的情况下验证数据的真实性与完整性，从而存在潜在的信任问题。同时，车联网中广泛存在基于不同密码体制的车辆与RSU的通信。这种异构性主要源于不同制造商在硬件平台、通信协议以及安全机制上的不一致。当车辆需要向使用不同密码体制的RSU传输消息时，车辆与RSU之间的通信就是异构通信[6]。目前已有许多关于车联网中异构通信的研究[7-9]，该问题也成为当前车联网研究的重要方向。

为了在保证数据真实性与完整性的基础上，同时实现通信内容的机密保护，许多学者将签密技术应用到不同的密码体制中以保证车联网中的安全通信。1997年，Zheng[10]首次提出了签名加密技术，该技术将数字签名和公钥加密结合到一个逻辑步骤中，以更高效的方式实现了机密性、认证、完整性和不可否认性。随后，Li等[11]设计了基于公钥基础设施（public key infrastructure，PKI）的签密方案，尽管满足了安全通信的关键要求，但由于复杂的证书管理问题，该方案在计算和通信开销方面效率较低，因此限制了其在资源受限节点（如车辆）中的实际应用。为了避免证书管理的开销，研究人员提出了基于身份加密（identity-based cryptography，IBC）的签密方案[12]，然而，IBC体系中由于所有用户私钥均由密钥生成中心（key generation center，KGC）生成，因此存在密钥托管问题。为克服IBC体系的这一缺陷，2003年，Al-riyami和Paterson[13]提出了无证书密码体制（certificateless public key cryptography，CLC）的概念。在CLC中，密钥由两部分组成，一部分由权威机构生成，另一部分由用户自主生成，权威机构不掌握用户的完整私钥。鉴于CLC体系在安全性和效率方面的优势，近年来被广泛应用于车联网等安全通信场景。2024年，Huang等[14]采用数论研究单位算法，在保持抗量子安全的同时实现了无证书聚合签密，显著地降低了验签开销。但格参数导致公钥、签名偏大，签名侧计算开销仍然过大。

在实际车联网应用中，通信双方可能处于不同的密码体系中。为实现异构密码体制间的有效通信，Sun和Li[15]提出了一种支持PKI和IBC间双向异构的签密方案，该方案还被拓展以支持多接收者场景。然而，该方案只能实现外部安全，无法满足内部安全的要求，且无法满足不可否认

性这一安全要求。为提升隐私保护与通信效率，Ali等[16]提出了一种异构聚合签密方案，采用聚合技术以减少解签密过程所需的时间及传输量。为进一步降低计算复杂度，Ali等[17]设计了一种CLC与IBC间的在线/离线异构签密协议，通过将签密过程划分为离线阶段和在线阶段，在离线阶段预先完成复杂的点乘运算，在线阶段只须执行轻量级操作，显著地降低了在线计算开销。但是该方案的离线签密阶段有接收者的信息，导致在线/离线签密不灵活。Elkhalil等[18]提出了基于区块链的异构在线/离线签密体系，借助区块链上数据难以篡改和可追溯性来实现异构通信，但区块链共识机制的依赖导致通信时延增加，链上数据存储成本较高且存在隐私信息暴露风险。针对车辆须频繁发生跨域交互的情况，Chen等[19]将区块链和短群签名结合，部署仅有读和写的智能合约以降低共识交互和开销，但链上的元数据易被攻击者关联分析，导致车辆跨域轨迹存在重识别风险。尽管上述研究在支持异构密码体系签密方面取得了显著的进展，但普遍未考虑如何高效地在车辆网云服务器中对加密数据进行检索，导致云端密文利用率较低。

车联网中车载单元在计算与存储能力方面有限，设备通常将密文上传到云服务器存储。为提高密文的可用性与检索效率，国内外学者针对密文搜索问题提出了多种解决方案，主要包括可搜索加密技术[20-21]和密文等值测试技术[22-27]。Boneh等[20]和Omala等[21]提出的可搜索加密方案只能对使用相同公钥加密的密文进行检索，不适用于多密钥环境。为克服该限制，2010年Yang等[22]首次提出了公钥加密等值测试技术。该技术在无须解密密文的前提下，可判断由不同公钥加密的密文是否对应相同明文。Zhao等[23]提出将基于属性加密与多密文等值测试技术融合，在实现细粒度访问控制的同时支持密文的检索，但该方案访问策略配置与用户撤销管理流程较为复杂，缺乏在标准模型下的全面安全性分析。He等[24]基于格密码体制实现密文等值测试功能，实现了量子安全，但在密文等值测试过程中存在侧信道信息泄露风险。Xiong等[25]将等值测试功能集成到异构签密方案中，使授权服务器能在不泄露明文的情况下进行等值测试并返回检索结果。文献[25]仅支持两个密文间的等值测试，Yang等[26]提出具有多密文等值测试签密方案，利用范德蒙矩阵对多个密文进行等值检测，提高了密文检索效率。利用同样的多密文等值检测方法，Yang等[27]还实现了从PKI到IBC的异构签密通信，但该方案使用双线性配对，计算开销较大。

尽管上述方案能够满足车联网通信的基本安全要求，但计算开销和通信开销较大，难以适应实时通信等对时延敏感的应用场景[28]。主要原因是这些方案普遍依赖双线性配对及基于双线性配对的点运算，计算复杂度较高，进而增加了签密、解签密和密文等值测试的整体开销。例如，双线性配对运算的计算开销约为椭圆曲线点乘的10倍，同时基于双线性配对的点乘运算开销约为椭圆曲线点乘的4倍。

针对上述问题，本文提出了一种基于ECC、支持多密文等值测试的在线/离线异构签密方案，以实现车联网中异构密码体系间的高效通信，满足车联网对低时延与高可靠性的实际需求，本文具体贡献如下。

（1）本文方案结合异构签密机制与多密文等值测试技术，实现CLC与PKI体系间的安全通信。通过RSU生成陷门信息，并由云服务器（cloud server，CS）基于该陷门信息完成多密文等值测试，使云端在不解密的前提下对密文进行批量验证和复用，避免重复计算和存储，有效地提高了云端密文的利用率。同时，接收方只须从云服务器上下载一次重复密文，减轻接收者通信与存储负担。

（2）本文方案基于ECC设计，避免了双线性

配对操作，显著地减轻了计算开销与整体通信开销。同时，该方案引入在线/离线签密技术，离线阶段仅进行随机数生成和系统参数运算，生成对所有接收者通用的中间结果，从而降低在线签密阶段的计算压力。离线签密中不包含接收者身份和公钥信息，即使对手获取到离线签名结果，也无法推导出明文和接收者信息。

（3）在随机预言机模型（random oracle model，ROM）下完成不可伪造性和机密性安全性证明。再采用 ProVerif 和 Scyther 工具验证，ProVerif结果表明所提方案能够保证消息机密性、身份匿名性与签名正确性，Scyther结果显示在多轮攻击模拟中未发现有效的攻击路径。

1　理论知识

1.1　椭圆曲线密码学

1985年，Miller[29]首次将椭圆曲线应用于密码学，之后ECC就广泛应用于加密协议中。设F_p为一个有限域，阶为素数p。在F_p上定义一条椭圆曲线E：$y^2\equiv x^3+ax+b \bmod p$，$4a^3+27b^2\neq 0$，其中，$a$，$b\in F_p$。椭圆曲线加法群$G$由曲线上的点和无穷点$O$构成，具有如下性质。

（1）点加：假设$(P,Q)\in G$，当$P\neq Q$且$P+Q=R$时，R为P和Q所在直线与椭圆曲线的交点；当$P=Q$且$P+Q=R$时，R为P或Q的切线与椭圆曲线的交点；当$P+Q=O$时，则$Q=-P$。

（2）标量乘法：假设$W\in G$，标量乘法$lW=\underbrace{W+W+\cdots+W}_{l}$表示将点$W$重复相加$l$次，其中，$l\in \mathbf{Z}_q^*$且$l>0$。

1.2　困难问题假设

本文所提方案的安全性依赖于以下两个经典的计算难题。

（1）椭圆曲线离散对数问题（elliptic curve discrete logarithm problem，ECDLP）：给定椭圆曲线上的两个点$(P,Q)\in G$，对于$Q=aP$，其中，$a\in \mathbf{Z}_q^*$，在已知P、Q情况下求出a是困难的。

（2）椭圆曲线计算迪菲–赫尔曼问题（elliptic curve computational Diffie-Hellman problem，ECCDHP）：给定椭圆曲线上的点$\{P,Q=aP,R=bP\}\in G$，其中，$(a,b)\in \mathbf{Z}_q^*$，求解$abP\in G$是困难的。

2　系统模型

2.1　系统框架

系统框架如图1所示，车辆采用CLC体制，由KGC和追踪管理机构（trace authority，TRA）

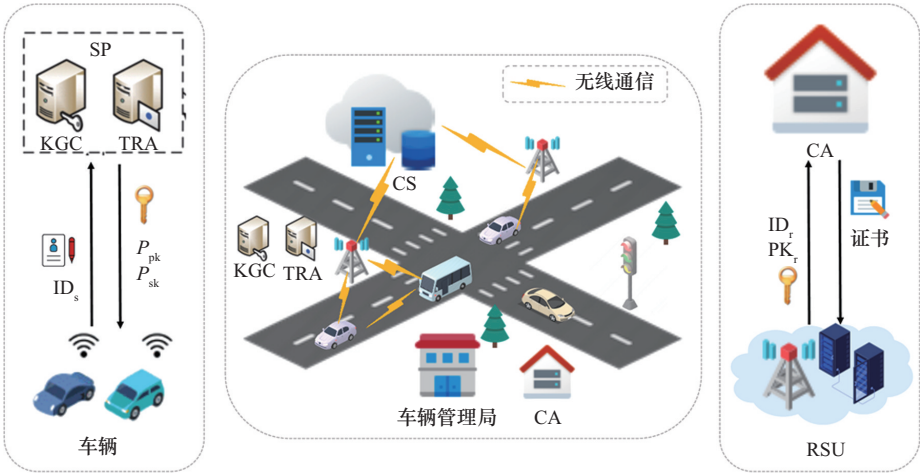


图1　系统框架

生成假名和部分密钥；RSU采用PKI体制，由证书颁发机构（certificate authority，CA）为公钥颁发证书。由无线通信技术连接车辆与其他设施，实现异构密码体制间的通信。

2.2 安全模型

在ROM下，本文所提方案须满足两个核心安全性要求：不可伪造性和机密性。车辆作为发送方处于CLC体系，该方案的不可伪造性需要考虑两类攻击者。第1类攻击者$\mathcal{A}_{\mathrm{I}}$：具有替换用户公钥的能力，但无法获得系统主私钥。第2类攻击者$\mathcal{A}_{\mathrm{II}}$：能够获得系统主私钥，但不能替换用户公钥。

定义1 如果没有敌手$\mathcal{A}_{\mathrm{I}}$在概率多项式时间（probabilistic polynomial time，PPT）内具有至少ε的优势破解ECDLP，则本文所提方案满足针对第1类攻击者的自适应性选择消息攻击下的不可伪造性（existential unforgeability against chosen messages attacks，EUF-CMA-type-I）。

定义2 如果没有敌手$\mathcal{A}_{\mathrm{II}}$在PPT内具有至少$\varepsilon$的优势破解ECDLP，则本文所提方案满足EUF-CMA-type-II。

定义3 如果没有敌手$\mathcal{A}$在PPT时间内具有至少优势ε破解ECCDHP，则本文所提方案满足自适应选择密文攻击下$\mathcal{A}_{\mathrm{I}}$的不可区分性（indistinguishability against adaptive chosen ciphertext attacks，IND-CCA2）。

3 方案设计

3.1 方案框架

系统流程如图2所示，主要由服务提供商（service provider，SP）、CA、车辆、RSU、CS组成。SP由KGC和TRA组成，KGC为车辆分发部分公私钥对，TRA为车辆生成假名。CA负责PKI体系中RSU的注册与认证。车辆负责对消息进行签密，并将签密后的密文上传到CS。RSU负责将部分私钥作为陷门信息上传到CS，并具备从云端下载密文并执行解签密操作的能力。CS负责密文的集中存储与管理，支持多密文等值测试功能。

本节将详细介绍方案的具体设计，该方案由7个阶段组成：系统初始化阶段、车辆注册阶段、

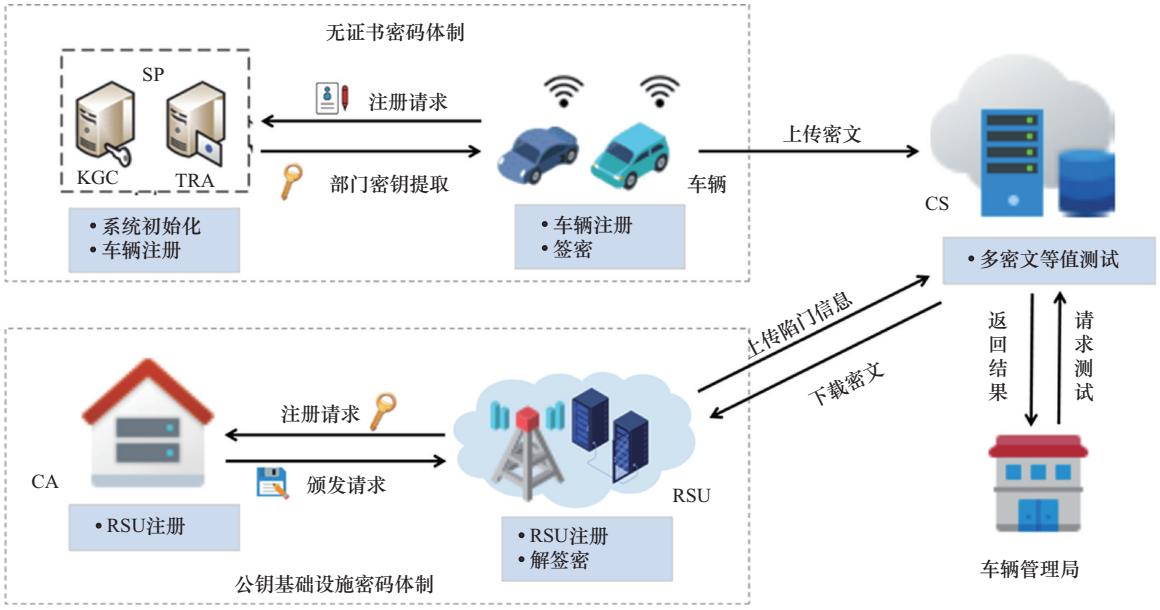


图2 系统流程

RSU注册阶段、陷门生成阶段、签密阶段、多密文等值测试阶段、解签密阶段。符号定义见表1。

表 1　符号定义

符号	定义
k	系统主密钥
G,P	椭圆曲线加法循环群和其生成器
$\mathrm{ID_s}$	车辆的身份标识
$\mathrm{PID_s}$	车辆的假名
$(P_{\mathrm{pk}},P_{\mathrm{sk}})$	车辆的部分公私钥
$(\mathrm{PK_s},\mathrm{SK_s})$	CLC中车辆完整公私钥
$(\mathrm{PK_r},\mathrm{SK_r})$	PKI中RSU的公私钥
$H_i(i=1,2,3,4,5,6)$	单向哈希函数
M	明文消息
CT	密文
n	进行等值测试的密文个数
$T_i,\Delta T$	当前时间戳和有效期
$\|,\oplus$	级联和异或

3.2　系统初始化

输入安全参数λ，KGC和TRA选择一个素数阶为q的椭圆曲线加法群G，生成元为P。随机选取主密钥$k\in_R\mathbf{Z}_q^*$，计算系统公钥$P_{\mathrm{pub}}=k\cdot P$，其中，$Z_q^*$表示模$q$的乘法可逆元集合，$Z$是“整数集合”的符号，下标$q$表示“除以$q$后余数的集合”，上标*表示“乘法可逆元的子集”，符号$\in_R$表示“随机选取”。定义了6个单向哈希函数：$H_1,H_2,H_5:G\to\mathbf{Z}_q^*$，$H_3\to\{0,1\}^*\times\{0,1\}^*\times G^3\to\mathbf{Z}_q^*$，$H_4,H_6:\{0,1\}^*\to\mathbf{Z}_q^*$。KGC和TRA公布系统参数$\mathrm{params}=\{G,q,P,k,P_{\mathrm{pub}},\ H_1,H_2,H_3,H_4,H_5,H_6\}$。

3.3　签密

签名功能是本文方案的重要部分，主要负责车辆消息的安全传输与匿名保护。该功能模块主要由4个子过程构成：车辆注册、RSU注册、陷门生成、车辆签密。其中，车辆签密过程如算法1所示。

（1）车辆注册

车辆处于CLC中，首先车辆向TRA提交身份标识符$\mathrm{ID_s}$发起注册请求，TRA在收到请求后生成随机数$w_{\mathrm{s}}\in_R\mathbf{Z}_q^*$，计算其公共参数$W_{\mathrm{s}}=w_{\mathrm{s}}P$，再结合主密钥$k$生成车辆假名$\mathrm{PID_s}=\mathrm{ID_s}\oplus H_1(W_{\mathrm{s}}k)$。TRA存储假名并将$\mathrm{PID_s}$发送给KGC。KGC收到假名后生成随机数$\alpha\in_R\mathbf{Z}_q^*$，计算部分私钥$P_{\mathrm{sk}}=(\alpha+k\mathrm{PID_s})$，部分公钥$P_{\mathrm{pk}}=P_{\mathrm{sk}}P$。KGC将$\{\mathrm{PID_s},P_{\mathrm{sk}},P_{\mathrm{pk}}\}$返回车辆。然后，车辆本地生成随机数$V_{\mathrm{sk}}\in_R\mathbf{Z}_q^*$作为车辆部分的私钥，公共值$V_{\mathrm{pk}}=V_{\mathrm{sk}}P$作为车辆部分的公钥。最终车辆得到$\delta_1$，$\delta_2\in_R Z_q^*$完整私钥$\mathrm{SK_s}=(V_{\mathrm{sk}},P_{\mathrm{sk}})$，完整公钥$\mathrm{PK_s}=(V_{\mathrm{pk}},P_{\mathrm{pk}})$。

（2）RSU注册

RSU处于PKI中，由RSU生成公私钥。RSU生成随机数，分别生成私钥$\mathrm{SK}_{r,1}=1/\delta_1$，$\mathrm{SK}_{r,2}=1/\delta_2$，对应的公钥分别是$\mathrm{PK}_{r,1}=\delta_1P$，$\mathrm{PK}_{r,2}=\delta_2P$。得到RSU完整私钥$\mathrm{SK}_r=(\mathrm{SK}_{r,1},\mathrm{SK}_{r,2})$，完整公钥$\mathrm{PK}_r=(\mathrm{PK}_{r,1},\mathrm{PK}_{r,2})$。RSU向CA发送$(\mathrm{ID}_r,\mathrm{PK}_r)$，CA为RSU颁发数字证书。其中，$\mathrm{ID}_r$是RSU在PKI中唯一的身份标识，RSU将自身$\mathrm{ID}_r$和生成的公钥一起提交给CA（证书机构），CA基于$\mathrm{ID}_r$验证RSU的合法身份，并为其生成的公钥签发数字证书，才能让其他通信方相信，公钥确实属于该RSU。

（3）陷门生成

RSU将部分私钥$\mathrm{SK}_{r,2}$发送给CS作为陷门信息$\mathrm{td}=\mathrm{SK}_{r,2}$。

（4）车辆签密

本文所提方案中签密过程分为离线签密和在线签密。离线签密生成随机数r_1，$r_2\in_R\mathbf{Z}_q^*$，再计算$R=r_1P$，$Q=r_2P$。得到离线密文$\sigma_{\mathrm{off}}=(r_1,r_2,R,Q)$，在离线密文基础上对消息$m\in\{0,1\}^*$进行在线签密，在线签密过程如下。

① 根据离线密文计算$C_1=r_1\mathrm{PK}_{r,1}$，$C_2=r_2\mathrm{PK}_{r,2}$，$C_3=H_2(R)\oplus m$，$C_4=\varphi^{-1}(P_{\mathrm{sk}}+V_{\mathrm{sk}})+r_1$，其中，$\varphi=H_3(m,\mathrm{PID_s},\mathrm{PK_s},R,Q,T)$，$T$为当前时间戳。

② 计算$f_0=H_4(m\|n)$，$f_1=H_4(m\|n\|f_0)$，…，$f_{n-1}=H_4(m\|n\|f_0\|f_1\|\cdots\|f_{n-2})$，其中，$n$为进行多密文等值测试的密文个数。

③ 消息发送者车辆随机生成$D\in_R\mathbf{Z}_q^*$，计算$f(D)=f_0+f_1D+f_2D^2+\cdots+f_{n-1}D^{n-1}$，$C_5=H_5(Q)\oplus D$，$C_6=H_6(n\|C_1\|C_2\|\cdots\|C_5\|Q\|f_0\|f_1\|\cdots\|f_{n-1})$，最终得到完整密文$\mathrm{CT}=(n,T,f(D),C_1,C_2,C_3,C_4,C_5,C_6)$。

算法1 车辆签密过程

输入 消息m，车辆假名$\mathrm{PID_s}$，车辆完整私钥$\mathrm{SK_s}$，RSU完整公钥$\mathrm{PK_r}$，密文个数n，当前时间戳T

输出 完整密文

//离线阶段

（1）随机生成r_1，$r_2\in_R\mathbf{Z}_q^*$；

（2）计算$R=r_1P$，$Q=r_2P$，得到离线密文$\sigma_{\mathrm{off}}=(r_1,r_2,R,Q)$；

//在线阶段

（3）计算$C_1=r_1\mathrm{PK}_{\mathrm{r},1}$，$C_2=r_2\mathrm{PK}_{\mathrm{r},2}$，$C_3=H_2(R)\oplus m$，$\varphi=H_3(m,\mathrm{PID_s},\mathrm{PK_s},R,Q,T)$，$C_4=\varphi^{-1}(P_{\mathrm{sk}}+V_{\mathrm{sk}})+r_1$；

（4）计算$f_0=H_4(m\|n)$；

（5）**for** i=1:1:$n-1$

（6） $f_i=H_4(m\|n\|f_{i-1})$；

（7）**end for**

（8）随机生成$D\in_R\mathbf{Z}_q^*$；

（9）计算$f(D)=f_0+f_1D+f_2D^2+\cdots+f_{n-1}D^{n-1}$，$C_5=H_5(Q)\oplus D$，$C_6=H_6(n\|C_1\|C_2\|\cdots\|C_5\|Q\|f_0\|f_1\|\cdots\|f_{n-1})$；

（10）车辆生成签名$\mathrm{CT}=(n,T,f(D),C_1,C_2,C_3,C_4,C_5,C_6)$

3.4 多密文等值测试

多密文等值测试功能实现在不泄露明文和车辆密钥的前提下，判断一批密文是否对应同一明文。多密文等值测试算法如算法2所示。

CS上接收不同车辆发送的n个密文$\mathrm{CT}_1,\mathrm{CT}_2,\cdots,\mathrm{CT}_n$和其对应的$n$个陷门信息$\mathrm{td}_1,\mathrm{td}_2,\cdots,\mathrm{td}_n$，每个密文表示为$\mathrm{CT}_i=(n_i,T_i,f(D_i),C_{i,1},C_{i,2},C_{i,3},C_{i,4},C_{i,5},C_{i,6})$，$i\in\{1,2,\cdots,n\}$，$n_1=n_2=\cdots=n_n=n$，结合陷门信息$\mathrm{td}_i=\mathrm{SK}_{i-r,2}$，可计算$D_i=C_{i,5}\oplus H_5(C_{i,2}\cdot\mathrm{SK}_{i-r,2})$，$f(D_i)=f_0'+f_1'D_i+f_2'D_i^2+\cdots+f_{n-1}'D_i^{n-1}$，列出以下方程组：

$$\begin{cases}f(D_1)=f_0'+f_1'D_1+\cdots+f_{n-1}'D_1^{n-1}\\f(D_2)=f_0'+f_1'D_2+\cdots+f_{n-1}'D_2^{n-1}\\\quad\vdots\\f(D_n)=f_0'+f_1'D_n+\cdots+f_{n-1}'D_n^{n-1}\end{cases}\tag{1}$$

根据方程组可得范德蒙矩阵如下：

$$\boldsymbol{V}=\begin{bmatrix}1&D_1&D_1^2&\cdots&D_1^{n-1}\\1&D_2&D_2^2&\cdots&D_2^{n-1}\\\vdots&\vdots&\vdots&\cdots&\vdots\\1&D_n&D_n^2&\cdots&D_n^{n-1}\end{bmatrix},\quad\det(\boldsymbol{V})=\prod_{1\le i<j\le m}(D_i-D_j)\tag{2}$$

因为D_i为$\mathbf{Z}_q^*$内的随机数，所以$\det(\boldsymbol{V})\neq0$，根据克拉默法则可知存在一组唯一解$f_0',f_1',\cdots,f_{n-1}'$，通过式（3）验证每一个密文$\mathrm{CT}_i$中的明文$m_i$是否相等。若所有的$C_{i,6}$均验证成功，则$m_1=m_2=\cdots=m_n$；否则验证失败。

$$C_{i,6}\overset{?}{=}H_6(n_i\|C_{i,1}\|C_{i,2}\|\cdots\|C_{i,5}\|Q_i\|f_0'\|f_1'\|\cdots\|f_{n-1}')\tag{3}$$

式（3）正确性证明如下：

$$\begin{aligned}&D_i=C_{i,5}\oplus H_5(C_{i,2}\cdot\mathrm{SK}_{i-r,2})=\\&C_{i,5}\oplus H_5(r_{i,2}\mathrm{PK}_{i-r,2}\cdot\mathrm{SK}_{i-r,2})=\\&C_{i,5}\oplus H_5(r_{i,2}\delta_{i,2}P\cdot(1/\delta_{i,2}))=\\&C_{i,5}\oplus H_5(Q)\end{aligned}\tag{4}$$

算法2 多密文等值测试算法

输入 密文集合$\{\mathrm{CT}_1,\mathrm{CT}_2,\cdots,\mathrm{CT}_n\}$，陷门集合$\{\mathrm{td}_1,\mathrm{td}_2,\cdots,\mathrm{td}_n\}$

输出 判定标志$b\in\{0,1\}$（“1”表示验证成功，“0”表示验证失败）

（1）**for** i=1:1:n

（2） 计算$D_i=C_{i,5}\oplus H_5(C_{i,2}\cdot\mathrm{SK}_{i-r,2})$，$f(D_i)=f_0'+f_1'D_i+f_2'D_i^2+\cdots+f_{n-1}'D_i^{n-1}$；

（3）**end for**

（4）构造范德蒙矩阵$\boldsymbol{V}\in\mathbf{Z}_q^{n\times n}$；

（5）根据克拉默法则求出唯一解$f_0',f_1',\cdots,f_{n-1}'$；

（6）**for** i=1:1:n

（7）　**if**　$C_{i,6}\neq H_6(n_i\|C_{i,1}\|C_{i,2}\|\cdots\|C_{i,5}\|Q_i\|f_0'\|f_1'\|\cdots\|f_{n-1}')$

（8）　$b=0$；

（9）　**break**

（10）　**end if**

（11）**end for**

（12）全部成立返回$b=1$

3.5　解签密

当RSU收到密文CT时，生成当前时间戳T'，计算$|T'-T|\leqslant\Delta T$是否成立，ΔT为假名有效期。若成立，则验证签密信息。RSU计算$R'=C_1\cdot\mathrm{SK}_{\mathrm{r},1}$，$Q'=C_2\cdot\mathrm{SK}_{\mathrm{r},2}$，根据$R'$可恢复明文。

$$m'=C_3\oplus H_2(R') \tag{5}$$

$$R'\stackrel{?}{=}C_4P-\varphi^{-1}(V_{\mathrm{pk}}+P_{\mathrm{pk}}) \tag{6}$$

其中，$\varphi=H_3(m,\mathrm{PID_s},\mathrm{PK_s},R',Q',T)$，通过式（6）验证签密的合法性，验证成功则说明$m'=m$，否则验证失败。式（6）正确性证明如下：

$$R'=C_1\cdot\mathrm{SK}_{\mathrm{r},1}=r_1\cdot\mathrm{PK}_{\mathrm{r},1}\cdot\mathrm{SK}_{\mathrm{r},1}=r_1\cdot\delta_1P\cdot(1/\delta_1)=r_1P=R \tag{7}$$

$$Q'=C_2\cdot\mathrm{SK}_{\mathrm{r},2}=r_2\cdot\mathrm{PK}_{\mathrm{r},2}\cdot\mathrm{SK}_{\mathrm{r},2}=r_2\cdot\delta_2P\cdot(1/\delta_2)=r_2P=Q \tag{8}$$

$$\begin{aligned}R'&=C_4P-\varphi^{-1}(V_{\mathrm{pk}}+P_{\mathrm{pk}})=\\&(\varphi^{-1}(V_{\mathrm{sk}}+P_{\mathrm{sk}})+r_1)P-\varphi^{-1}(V_{\mathrm{pk}}+P_{\mathrm{pk}})=\\&\varphi^{-1}(V_{\mathrm{sk}}+P_{\mathrm{sk}})P+r_1P-\varphi^{-1}(V_{\mathrm{pk}}+P_{\mathrm{pk}})=\\&r_1P=R\end{aligned} \tag{9}$$

4　安全分析

4.1　基于ROM的安全证明

本节对所提方案的不可伪造性和机密性进行安全性证明。

定理1　在ROM中基于ECDLP假设，方案可以实现EUF-CMA安全。定理1由引理1和引理2证明。

引理1　假设存在攻击者$\mathcal{A}_{\mathrm{I}}$在PPT内以至少ϵ的优势破坏EUF-CMA-type-I安全性，则挑战者$\mathcal{C}$能以优势$\varepsilon'\geqslant\epsilon/q_h^2\left(1-q_{\mathrm{psk}}/q_h\right)\left(1-q_{\mathrm{sk}}/q_h\right)\left(1-q_{\mathrm{sc}}/2^l\right)$破解ECDLP[30]，其中，$q_h$、$q_{\mathrm{psk}}$、$q_{\mathrm{sk}}$、$q_{\mathrm{sc}}$分别代表哈希查询、车辆部分私钥查询、车辆完整私钥查询、签密查询的次数，l表示密钥的位数。

证明　该证明主要描述挑战者$\mathcal{C}$如何在攻击者$\mathcal{A}_{\mathrm{I}}$的帮助下破解ECDLP。假设$\mathcal{C}$收到一个ECDLP实例（$P,S=sP$），$\mathcal{C}$的任务是求解$s\in_R\mathbf{Z}_q^*$，攻击者$\mathcal{A}_{\mathrm{I}}$与$\mathcal{C}$进行如下交互。

系统建立阶段：输入安全参数λ，$\mathcal{C}$运行系统初始化和RSU注册算法，生成系统主密钥k、系统参数params和接收方的公私钥对$(\mathrm{PK_r'},\mathrm{SK_r'})$，并将params、$\mathrm{PK_r'}$发送给$\mathcal{A}_{\mathrm{I}}$。

攻击：$\mathcal{A}_{\mathrm{I}}$执行以下查询，为避免非连续应答，$\mathcal{C}$维护初始为空的列表$\{L_{\mathrm{H}_1},L_{\mathrm{H}_2},L_{\mathrm{H}_3},L_{\mathrm{H}_4},L_{\mathrm{H}_5},L_{\mathrm{H}_6},L_{\mathrm{pk}}\}$分别用于存储$H_1\sim H_6$的预言模拟和公钥信息。

（1）$H_1\sim H_6$查询：$\mathcal{C}$收到$\mathcal{A}_{\mathrm{I}}$关于$\mathrm{PID_s}$的查询，$\mathcal{C}$检查$\mathrm{PID_s}$是否在$\{L_{\mathrm{H}_1},L_{\mathrm{H}_2},L_{\mathrm{H}_3},L_{\mathrm{H}_4},L_{\mathrm{H}_5},L_{\mathrm{H}_6}\}$中，若存在则返回相应哈希值给$\mathcal{A}_{\mathrm{I}}$，否则$\mathcal{C}$返回随机值$h\in_R\mathbf{Z}_q^*$，并存入对应的列表中。

（2）部分私钥查询：$\mathcal{A}_{\mathrm{I}}$向$\mathcal{C}$发送关于$\mathrm{PID_s}$的部分私钥查询，若$\mathrm{PID_s}=\mathrm{PID_s'}$则查询终止。否则$\mathcal{C}$选取随机数$x\in_R\mathbf{Z}_q^*$返回$\mathcal{A}_{\mathrm{I}}$。

（3）私钥查询：$\mathcal{A}_{\mathrm{I}}$向$\mathcal{C}$发送关于$\mathrm{PID_s}$的私钥查询，若$\mathrm{PID_s}=\mathrm{PID_s'}$，则查询终止。否则，$\mathcal{C}$可以获得部分私钥$P_{\mathrm{sk}}=x$，并且遍历列表$L_{\mathrm{pk}}$检查其中是否有元组$\{\mathrm{PID_s},s,\mathrm{PK_s}\}$，若有则返回$\mathrm{SK_s}=\{s,x\}$作为$\mathcal{A}_{\mathrm{I}}$的私钥，否则选择随机数$s\in_R\mathbf{Z}_q^*$，并将$\mathrm{SK_s}=\{s,x\}$返回$\mathcal{A}_{\mathrm{I}}$。

（4）公钥查询：$\mathcal{A}_{\mathrm{I}}$向$\mathcal{C}$发送关于$\mathrm{PID_s}$的公钥查询，若$\mathrm{PID_s}=\mathrm{PID_s'}$，则查询终止。否则$\mathcal{C}$遍历列表$L_{\mathrm{pk}}$检查其中是否有元组$\{\mathrm{PID_s},s,\mathrm{PK_s}\}$，若有则返回$\mathrm{PK_s}$，否则选择两个随机数$(s,x)\in_R\mathbf{Z}_q^*$，计算$P_{\mathrm{pk}}=xP$，$V_{\mathrm{pk}}=sP$，返回$\mathrm{PK_s}=(V_{\mathrm{pk}},P_{\mathrm{pk}})$给$\mathcal{A}_{\mathrm{I}}$。

（5）公钥替换查询：$\mathcal{A}_{\mathrm{I}}$向$\mathcal{C}$发送关于$\{\mathrm{PID_s},\mathrm{PK_s}\}$的公钥替换查询，$\mathcal{C}$用来自$\mathcal{A}_{\mathrm{I}}$的特定

值替换PK_s，并将$\{PID_s, PK_s, \perp\}$存入L_{pk}，其中，$\perp$是一个未知值。

（6）签密查询：$\mathcal{A}_I$向$\mathcal{C}$提供消息m和PID_s，$\mathcal{C}$执行签密算法以响应查询。

伪造阶段：$\mathcal{A}_I$是一个伪造者，根据分叉引理[31]创建一个拉斯维加斯算法$\mathcal{A}_I'$，可以分别伪造两条签名消息$\{m, \varphi, C_4\}$，$\{m, \varphi', C_4'\}$。其中，$C_4=\varphi^{-1}(s+x)+r_1 \bmod q$，$C_4'=\varphi'^{-1}(s+x)+r_1 \bmod q$，由$C_4-C_4'$可得：

$$\begin{aligned} &C_4-C_4'=[\varphi^{-1}(s+x)+r_1]-[\varphi'^{-1}(s+x)+r_1] \bmod q= \\ &\varphi^{-1}\cdot s-\varphi'^{-1}\cdot s+\varphi^{-1}\cdot x-\varphi'^{-1}\cdot x \bmod q= \\ &(\varphi^{-1}-\varphi'^{-1})(s+x) \bmod q, \\ &\frac{C_4-C_4'}{\varphi^{-1}-\varphi'^{-1}}-x=s \bmod q \end{aligned} \tag{10}$$

$\mathcal{C}$将$(C_4-C_4')/(\varphi^{-1}-\varphi'^{-1})-x$作为ECDLP的解，但是ECDLP在PPT内无法解决，所以$\mathcal{A}_I$伪造的签名信息不合法，该方案满足EUF-CMA-type-I安全性。

证毕。

引理2 假设存在攻击者$\mathcal{A}_{II}$在PPT内以至少ϵ的优势破坏EUF-CMA-type-II安全性，则挑战者$\mathcal{C}$能以优势$\varepsilon' \geqslant \epsilon / q_h^2\left(1-q_{sk}/q_h\right)\left(1-q_{sc}/2^l\right)$破解ECDLP。

证明 该证明主要描述挑战者$\mathcal{C}$如何在$\mathcal{A}_{II}$的帮助下破解ECDLP。假设$\mathcal{C}$收到一个ECDLP实例（$P, S=sP$），$\mathcal{C}$的任务是求解$s \in_R \mathbf{Z}_q^*$，$\mathcal{A}_{II}$与$\mathcal{C}$进行如下交互。

引理2的证明与引理1类似，进行$H_1 \sim H_6$哈希查询、公钥查询、私钥查询、签密查询。$\mathcal{A}_{II}$不能进行公钥替换查询，但是可以获取主密钥，因此不用进行部分私钥查询。最后根据分叉引理证明因为$\mathcal{C}$无法破解ECDLP，所以$\mathcal{A}_{II}$伪造的签名信息不合法，该方案满足EUF-CMA-type-II安全性。

证毕。

定理2 在ROM中，假设存在攻击者$\mathcal{A}$以至少ϵ的优势针对本方案的IND-CCA2安全性，$\mathcal{A}$在PPT内执行$H_1 \sim H_6$哈希查询，私钥查询，公钥查询，解签密查询（解签密查询次数表示为q_{usc}），查询结果帮助挑战者$\mathcal{C}$求解ECCDHP，$\mathcal{C}$破解问题的优势$\varepsilon' \geqslant \left[\varepsilon/(q_{h_2}+q_{h_3})\right]\left[1-(q_{usc}/2^{\lambda})\right]$。

证明 该证明主要描述$\mathcal{C}$如何在$\mathcal{A}$的帮助下破解ECCDHP。假设$\mathcal{C}$收到一个ECCDHP实例$(P, \phi K, r_1 S) \in G$，$\mathcal{C}$需要求出$\phi r_1 P \in \mathbf{Z}_q^*$，$\mathcal{A}$与$\mathcal{C}$进行如下交互。

系统建立阶段：输入安全参数λ，$\mathcal{C}$运行系统初始化和RSU注册算法，生成系统主密钥k、系统参数params和接收方的公私钥对(PK_r', SK_r')，选择挑战身份ID_r'，并将params、PK_r'发送给$\mathcal{A}$。

阶段1：与引理1类似，进行哈希查询、公钥查询、私钥查询、解签密查询。

解签密查询：对密文CT执行解签密查询，若$PID_s = PID_s'$，查询终止，否则$\mathcal{C}$执行解签密算法，将查询结果返回$\mathcal{A}$。

挑战：完成阶段1后$\mathcal{A}$为挑战者ID_r'选择两条等长的消息m_1和m_2。$\mathcal{C}$选择(μ_1, μ_2)，$C_3', C_4' \in_R \mathbf{Z}_q^*$，计算$C_1'=\mu_1 P$，$C_2'=\mu_2 P$，将$CT_1'=(C_1', C_2', C_3', C_4')$返回$\mathcal{A}$。

阶段2：$\mathcal{A}$执行与阶段1相同的查询，但是不能对CT_1'进行解签密查询。

猜测：$\mathcal{C}$从列表L_{H_2}或L_{H_3}随机选取$\{PID_s, R, h_2\}$或$\{PID_s, M, PK_s, R, Q, \varphi\}$，得到$R=r_1 P$的概率为$1/(q_{h_2}+q_{h_3})$，$\mathcal{C}$给出$\phi R=\phi r_1 P$作为ECCDHP的解。但已知ECCDHP在PPT内无法解决，可知本方案具有IND-CCA2安全性。

证毕。

综上所述，本文所提方案在ROM模型下完成了EUF-CMA和IND-CCA2的安全性证明。尽管ROM是一种理想化模型，实际中哈希函数并不完全等价于随机预言机模型，但该模型在密码学设计领域仍具有实践参考价值，大量的密码学协议依赖ROM模型进行安全性分析。并且本文进一步在第4.2节和第4.3节中分别使用ProVerif

与 Scyther 工具对协议进行形式化验证，ProVerif 结果表明协议满足机密性与认证性等安全性质，Scyther 结果显示在多实例并发下未发现任何攻击轨迹，进一步增强了协议安全性的可信度。

4.2　基于 ProVerif 的安全分析

ProVerif 是一种基于 Dolev-Yao 模型[32]的自动化分析工具，用于验证密码协议的安全性。假设攻击者具备 Dolev-Yao 攻击能力，即能够完全控制通信信道，任意截获、篡改、重放和伪造消息，但无法破解安全的密码原语。本文在 ProVerif 中对会话密钥 k、车辆私钥 V_{sk}、明文消息 m 等敏感数据进行机密性查询（query secret <变量>），对车辆真实身份 ID_s 进行匿名性查询（query attacker<变量>），并通过事件关系验证了协议的可认证性（query event<事件 1> ==> event<事件 2>）。

ProVerif 运行结果如图 3 所示，攻击者无法获取 m、V_{sk}、P_{sk}、k，说明所提方案实现了隐私信息的保密性；并且攻击者不能根据假名推测出车辆的 ID_s，证明所提方案实现了对车辆身份的条件隐私保护；再通过验证签名成功的条件，说明解密过程的正确性。以上结果说明在 Dolev-Yao 攻击模型下，协议能够有效地保障机密性、身份匿名性与消息完整性，能抵抗伪造消息、重放攻击、身份冒充等常见主动攻击。

```
--------------------------------------------------------------
Verification summary:

Query secret m_2,m_1 is true.

Query secret Vsk is true.

Query secret Psk_1,Psk is true.

Query secret k_1 is true.

Query not attacker(ID[]) is true.

Query event(verify_signature_success) ==> event(decrypt_success(m[])) is true.

--------------------------------------------------------------
```

图 3　ProVerif 运行结果

4.3　基于 Scyther 的安全分析

为进一步验证协议在实际执行过程中的抗攻击能力，本文使用协议验证工具 Scyther 进行仿真验证。Scyther 同样基于 Dolev-Yao 攻击模型，能够自动搜索出在有限轮数内的所有可能攻击路径，并检查协议是否满足弱同步性、强同步性、存活性、协商一致性等安全属性。指定车辆 V、CS、RSU 作为协议安全验证的角色，设置高级选项运行本文协议 100 次，以便为每个请求查找潜在攻击的多种模式。Scyther 运行结果如图 4 所示，结果表明，未能找到任何有效的攻击路径。表明协议可以有效地抵御中间人攻击、重放攻击、会话劫持、身份伪造、会话不同步攻击等威胁，进一步增强协议的安全性与可信度。

Scyther results : verify

Claim				Status		Commen
V2GHybrid	V	V2GHybrid,wagree	Weakagree	Ok	Verified	No attacks.
		V2GHybrid,Valive	Alive	Ok	Verified	No attacks.
		V2GHybrid,Vagree	Niagree	Ok	Verified	No attacks.
		V2GHybrid,Vsync	Nisynch	Ok	Verified	No attacks.
	CS	V2GHybrid,CS1	Weakagree	Ok	Verified	No attacks.
		V2GHybrid,CS2	Alive	Ok	Verified	No attacks.
		V2GHybrid,CS3	Niagree	Ok	Verified	No attacks.
		V2GHybrid,CS4	Nisynch	Ok	Verified	No attacks.
	RSU	V2GHybrid,RSU1	Weakagree	Ok	Verified	No attacks.
		V2GHybrid,Ralive	Alive	Ok	Verified	No attacks.
		V2GHybrid,Ragree	Niagree	Ok	Verified	No attacks.
		V2GHybrid,Rsync	Nisynch	Ok	Verified	No attacks.

Done.

图 4　Scyther 运行结果

5　性能分析

本节从功能特性、计算开销和通信开销 3 个方面对所提方案进行性能分析，选择该领域中具有代表性、与本文研究场景高度相关的对比方案[16, 25-27]，以分析所提方案的有效性和实用性。

5.1　功能分析

功能对比结果见表 2。本文所提方案克服了文献[26]仅支持同一密码体制通信的局限，更适合车联网异构环境的需求。与文献[16]相比，本文所提方案增加了多密文等值测试功能。文献[25]中等值测试只能同时判断两个密文，本文所提方案可以同时判断多个密文。文献[27]虽实现功能与本文相同，但本文在计算和通信开销上相较于文献[27]有明显优势。

表 2　功能对比结果

方案	异构签密	密文等值测试	多密文等值测试
文献[26]	×	√	√
文献[16]	√	×	×
文献[25]	√	√	×
文献[27]	√	√	√
本文方案	√	√	√

5.2　计算开销

设置安全级别为80位，$\bar{p}$、p、q是3个大素数。选择对称双线性配对$\hat{e}:G_1\times G_1\to G_2$，$G_1$是椭圆曲线$\bar{E}\equiv(x^3+x)\bmod\bar{p}$上点$\bar{P}$生成的阶为$q$的加法群，其中，$\bar{p}=512$ bit，$q=160$ bit。选择加法循环群为G的q阶椭圆曲线，其中，$p=160$ bit。

利用上述设置，基于Linux操作系统Ubuntu20.04.6LTS，搭载Intel(R) Core(TM) i5-8265U CPU @ 1.60 GHz处理器和8.0 GB内存的计算平台，采用MIRACL密码库对相关加密操作进行运算。加密操作中异或运算处理时间可忽略不计。加密操作时间见表3。

表 3　加密操作时间

运算操作	定义	执行时间/ms
T_{BP}	双线性映射	4.211 0
T_{PM-BP}	双线性映射点乘运算	1.709 2
T_{EX_1-BP}	G_1中的幂运算	4.400 0
T_{EX_2-BP}	G_2中的幂运算	1.603 1
T_{PM-ECC}	椭圆曲线点乘运算	0.442 5
T_{PA-ECC}	椭圆曲线点加运算	0.001 8
T_H	哈希运算	0.000 8

计算开销对比见表4。文献[25, 27]基于双线性映射，核心运算涉及映射和指数运算，开销较大。本文所提方案和文献[16, 26]是基于椭圆曲线加密，避免了高代价的配对运算。并且本文所提方案将签密过程中不需要接收者信息和在线消息的部分计算预先在离线阶段完成，本文所提方案的签密计算成本只考虑在线签密的开销。虽然算法中哈希运算较多，但哈希运算的时间开销非常小，对方案整体的计算开销影响不大。

为量化本文所提方案的性能，在Linux操作系统Ubuntu20.04.6LTS环境下，搭载Intel(R) Core(TM) i5-8265U CPU @ 1.60 GHz处理器和8.0 GB内存的计算平台进行模拟实验。将密文数量分别设置为10、20、30、40、50、60、70、80、90和100，重复测试1 000次并取平均值来确定执行时间，单位为ms。签密算法计算开销、解签密算法计算开销、等值测试计算开销和通信开销分别如图5~图8所示。

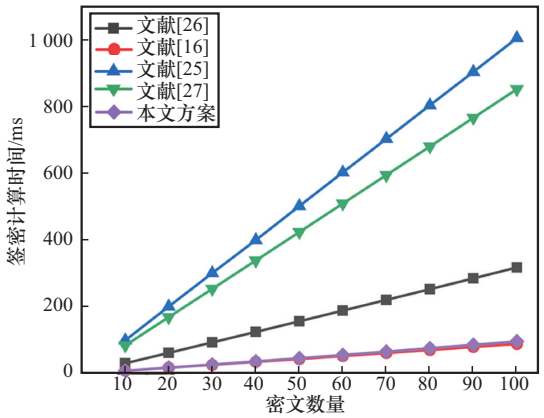


图 5　签密算法计算开销

由图5和图6可知，基于双线性映射的文献[25, 27]计算开销明显高于使用椭圆曲线的方案，本文所提方案的签密和解签密计算开销略高

表 4　计算开销对比

方案	签密	解签密	等值测试
文献[26]	$7T_{PM-ECC}+(n+3)T_H$	$6T_{PM-ECC}+(n+3)T_H$	$3nT_{PM-ECC}+2nT_H$
文献[16]	$2T_{PM-ECC}+T_H$	$2T_{PM-ECC}+2T_H+T_{PA-ECC}$	—
文献[25]	$4T_{PM-BP}+2T_{EX_2-BP}+4T_H$	$2T_{PM-BP}+T_{EX_2-BP}+3T_{BP}+4T_H$	$(n-1)(2T_{PM-BP}+2T_{BP}+2T_H)$
文献[27]	$4T_{PM-BP}+T_{EX_2-BP}+(n+4)T_H$	$3T_{PM-BP}+T_{EX_2-BP}+2T_{BP}+5T_H$	$nT_{BP}+2nT_H$
本文方案	$(2T_{PM-ECC})_{off}+(2T_{PM-ECC}+(n+4)T_H)_{on}$	$3T_{PM-ECC}+T_{PA-ECC}+2T_H$	$nT_{PM-ECC}+2nT_H$

于文献[16]，但本文增加了多密文等值测试功能，签密和解签密时需要计算用于等值测试的密文，并且高出的计算时间在几毫秒，属于可接受范围。由图7可知，在进行密文等值测试时，具备多密文等值测试功能的本文所提方案和文献[26-27]相比优势明显，无须两两进行等值测试。本文所提方案和文献[27]多密文等值测试均使用椭圆曲线，但本文所提方案减少了椭圆曲线点乘运算次数，所以具有更低的计算开销。在密文数量为90时，本文所提方案耗时仅为39.97 ms，相比文献[27]的119.62 ms，计算开销降低约66%，并且随着密文数量的增大优势继续扩大。综合分析签密、解签密和密文等值测试3方面的计算成本，本文所提方案的性能优势更明显。

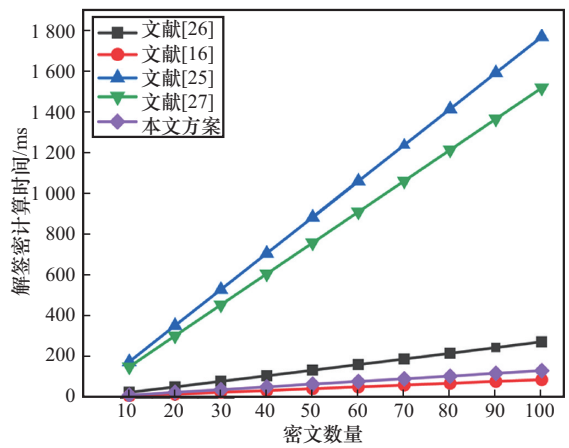


图 6　解签密算法计算开销

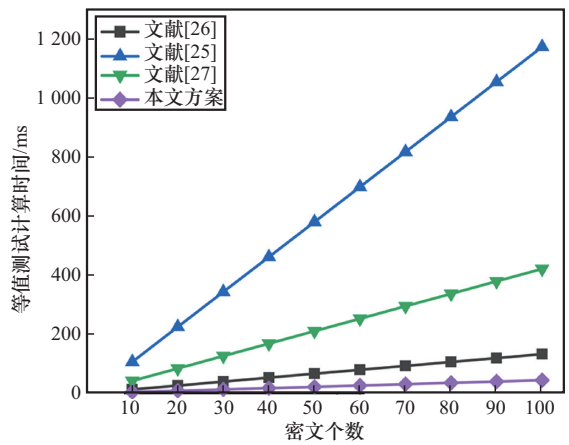


图 7　等值测试计算开销

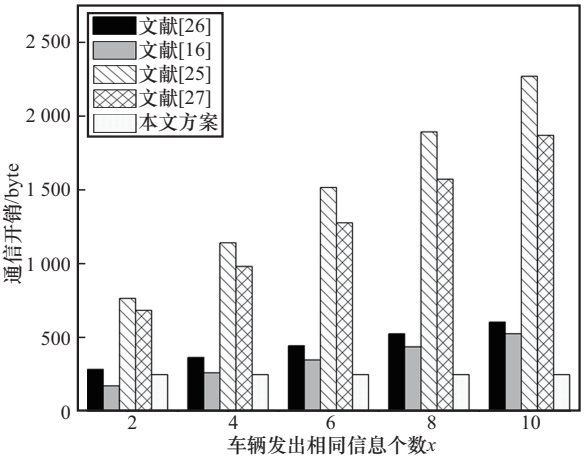


图 8　通信开销

5.3　通信开销

根据实验配置计算本文所提方案和对比文献的通信开销，各方案的通信开销对比见表5。根据设置，$\bar{p}$ 和 p 的大小分别为64 byte和20 byte，所以 G_1、G_2 中的元素为(64×2) byte =128 byte，G 中元素为(20×2) byte =40 byte。$\mathbf{Z}_q^*$ 中的元素、时间戳 T、身份标识符ID的大小分别为20 byte、4 byte和20 byte。密文长度是影响通信性能的主要原因。

表 5　各方案的通信开销对比

方案	通信开销
文献[26]	$4\|G\|+(2+2x)\|\mathbf{Z}_q^*\|$= (200+40$x$) byte
文献[16]	$2\|G\|+2x\|\mathbf{Z}_q^*\|+x\|T\|$= (80+44$x$) byte
文献[25]	$x\|G_1\|+3\|G_2\|+2x\|\mathbf{Z}_q^*\|+x\|ID\|$= (384+188$x$) byte
文献[27]	$(3+x)\|G_1\|+x\|\mathbf{Z}_q^*\|$= (786+168$x$) byte
本文方案	$2\|G\|+8\|\mathbf{Z}_q^*\|+\|T\|$= 244 byte

在车联网应用场景中，车辆需要多次将同一消息发送给RSU，以确保消息可靠送达。假设车辆向RSU发送同一消息 x 次，由表5可知，由于本文方案先在云端进行多密文等值测试，RSU只须下载一次重复的密文进行解密，通信开销为常数。其他对比方案则须对所有车辆密文进行解密，所以其通信开销都是 x 的一次函数，取决于 x 的大小。由图8可知，本文方案相较于文献[25, 27]

大幅地减少了重复解密带来的计算开销。当x=2时，文献[16]的通信开销低于本文所提方案，但随着x的增加，文献[16]的通信开销迅速累积并超过本文所提方案。所以，在车联网实际应用场景中，本文所提方案的通信开销具有明显优势。

6 结束语

针对车联网异构密码体系通信的隐私安全问题，本文提出了具有多密文等值测试的在线/离线异构签密方案，实现了CLC与PKI体系的安全通信，并在云服务器实现了多密文等值测试以提升密文利用率、降低接收端开销。结合椭圆曲线加密和在线/离线签密技术，有效地降低了在线签密的计算开销。本文所提方案在ROM下证明了具有EUF-CMA和IND-CCA2安全性。经过ProVerif验证了方案的正确性、不可链接性和保密性，Scyther结果显示未发现任何攻击轨迹。性能分析表明本文所提方案具有较小的计算开销和通信开销，适配资源受限车联网中复杂环境的应用需求。但本文所提方案未考虑量子计算威胁，缺乏抗量子能力，下一步计划将格基密码等抗量子算法融入现有框架，设计抗量子异构签密方案，同时保留原方案的低开销优势。

参考文献：

[1] Leng Y, Zhao L. Novel design of intelligent internet-of-vehicles management system based on cloud-computing and internet-of-things[C]//Proceedings of the 2011 International Conference on Electronic & Mechanical Engineering and Information Technology. Piscataway: IEEE Press, 2011, 6: 3190-3193.

[2] Elhabob R, Zhao Y, Hassan A, et al. PKE-ET-HS: public key encryption with equality test for heterogeneous systems in IoT[J]. Wireless Personal Communications, 2020, 113(1): 313-335.

[3] Song L, Sun G, Yu H, et al. FBIA: a fog-based identity authentication scheme for privacy preservation in Internet of vehicles[J]. IEEE Transactions on Vehicular Technology, 2020, 69(5): 5403-5415.

[4] Nyangaresi V O, Rodrigues A J, Taha N K. Mutual authentication protocol for secure VANET data exchanges[C]//Proceedings of the International Conference on Future Access Enablers of Ubiquitous and Intelligent Infrastructures. Cham: Springer International Publishing, 2021: 58-76.

[5] Xie Z, Chen Y, Ali I, et al. Efficient and secure certificateless signcryption without pairing for edge computing-based Internet of vehicles[J]. IEEE Transactions on Vehicular Technology, 2022, 72(5): 5642-5653.

[6] Zheng K, Zheng Q, Chatzimisios P, et al. Heterogeneous vehicular networking: a survey on architecture, challenges, and solutions[J]. IEEE Communications Surveys & Tutorials, 2015, 17(4): 2377-2396.

[7] Niu S, Shao H, 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.

[8] Wang Y, Jia X, Bao Y, et al. Efficient and provably secure offline/online heterogeneous signcryption scheme for VANETs[J]. IEEE Internet of Things Journal, 2024, 11(24): 41248-41260.

[9] Ullah I, Khan M A, Kumar N, et al. A conditional privacy preserving heterogeneous signcryption scheme for Internet of vehicles[J]. IEEE Transactions on Vehicular Technology, 2022, 72(3): 3989-3998.

[10] Zheng Y. Digital signcryption or how to achieve cost (signature & encryption)≪ cost (signature)+ cost (encryption)[C]//Proceedings of the Annual International Cryptology Conference. 1997: 165-179.

[11] Li C K, Yang G, Wong D S, et al. An efficient signcryptionscheme with key privacy and its extension to ring signcryption[J]. Journal of Computer Security, 2010, 18(3): 451-473.

[12] Karati A, Islam S K H, Biswas G P, et al. Provably secure identity-based signcryption scheme for crowdsourced industrial Internet of things environments[J]. IEEE Internet of Things Journal, 2017, 5(4): 2904-2914.

[13] Al-Riyami S S, Paterson K G. Certificateless public key cryptography[C]//Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security. Berlin, Heidelberg: Springer Berlin Heidelberg, 2003: 452-473.

[14] Huang Y, Xu G, Song X, et al. A quantum-secure certificateless aggregate signature protocol for vehicular ad hoc networks[J]. Vehicular Communications, 2024, 47: 100775.

[15] 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.

[16] Ali I, Chen Y, Pan C, et al. ECCHSC: computationally and bandwidth efficient ECC-based hybrid signcryption protocol for secure heterogeneous vehicle-to-infrastructure communications[J]. IEEE Internet of Things Journal, 2021, 9(6): 4435-

4450.

[17] Ali I, Chen Y, Li J, et al. Efficient offline/online heterogeneous-aggregated signcryption protocol for edge computing-based internet of vehicles[J]. IEEE Transactions on Intelligent Transportation Systems, 2023, 24(12): 14506-14519.

[18] Elkhalil A, Zhang J, Elhabob R. An efficient heterogeneous blockchain-based online/offline signcryption systems for Internet of vehicles[J]. Cluster Computing, 2021, 24(3): 2051-2068.

[19] Chen B, Wang Z, Xiang T, et al. BCGS: blockchain-assisted privacy-preserving cross-domain authentication for VANETs[J]. Vehicular Communications, 2023, 41: 100602.

[20] Boneh D, Di Crescenzo G, Ostrovsky R, et al. Public key encryption with keyword search[C]//Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques. Berlin, Heidelberg: Springer Berlin Heidelberg, 2004: 506-522.

[21] Omala A A, Ali I, Li F. Heterogeneous signcryption with keyword search for wireless body area network[J]. Security and Privacy, 2018, 1(5): e25.

[22] Yang G, Tan C H, Huang Q, et al. Probabilistic public key encryption with equality test[C]//Proceedings of the Cryptographers' Track at the RSA Conference. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010: 119-131.

[23] Zhao M, Chen H, Yao Y, et al. Lattice-based ABE with multi-ciphertext equality test in cloud computing[J]. Journal of King Saud University Computer and Information Sciences, 2025, 37(3): 38.

[24] He J, Ye Q, Yang Z, et al. A compact public key encryption with equality test for lattice in cloud computing[J]. Scientific Reports, 2025, 15(1): 27426.

[25] Xiong H, Hou Y, Huang X, et al. Heterogeneous signcryption scheme from IBC to PKI with equality test for WBANs[J]. IEEE Systems Journal, 2021, 16(2): 2391-2400.

[26] Yang X, Luo X, Liu R, et al. Certificateless aggregate signcryption scheme with multi-ciphertext equality test for the Internet of vehicles[J]. PLoS One, 2025, 20(5): e0322185.

[27] Yang X, Li S, Li M, et al. Heterogeneous signcryption scheme from PKI to IBC with multi-ciphertext equality test in Internet of vehicles[J]. IEEE Internet of Things Journal, 2023, 11(8): 14178-14191.

[28] Cheng J, Yuan G, Zhou M C, et al. A fluid mechanics-based data flow model to estimate VANET capacity[J]. IEEE Transactions on Intelligent Transportation Systems, 2019, 21(6): 2603-2614.

[29] Miller V S. Use of elliptic curves in cryptography[C]//Proceedings of the Conference on the Theory and Application of Cryptographic Techniques. Berlin, Heidelberg: Springer Berlin Heidelberg, 1985: 417-426.

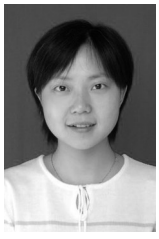
[30] Liu J, Zhang L, Sun R, et al. Mutual heterogeneous signcryption schemes for 5G network slicings[J]. IEEE Access, 2018, 6: 7854-7863.

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

[32] Dolev D, AC YAO. On the security of public key protocols[J]. IEEE Transactions on Information Theory, 1981, 29(2): 198-208.

[作者简介]

周美贤（2000– ），女，重庆邮电大学通信与信息工程学院硕士生，主要研究方向为车联网隐私保护和认证协议。



范馨月（1979– ），女，重庆邮电大学通信与信息工程学院副教授，主要研究方向为网络信息安全、信号处理。