基于经典-量子混合密码学的车载自组织网络认证密钥协商方法

廖龙霞[1]，方禾[2]，张青苗[1]，赵军辉[3]

（1.华东交通大学信息与软件工程学院，江西 南昌 330001；2.福建师范大学计算机与网络空间安全学院，福建 福州 350007；3.北京交通大学信息与工程学院，北京 100080）

摘要：针对现有车载自组织网络（VANETs）中认证密钥协商方案在量子计算威胁下的安全隐患，提出一种融合经典密码学与连续变量量子密码学的新型认证密钥协商方案。该方案利用连续变量量子图态（CVGS）的量子隐形传态特性实现车辆与路侧单元的身份认证，并结合安全哈希函数完成密钥协商。安全性分析表明，该方案可在短期内有效抵御量子计算攻击，满足身份认证与密钥协商的安全需求。性能评估显示，与现有量子密码学方案相比，所需量子态数量更少，提升了实现可行性；相较传统经典方案，计算与通信开销分别降低77.27%和63.76%。该方案在安全性与性能之间实现良好平衡，具备广泛的应用前景与实际部署价值，可为VANETs在面对量子威胁时提供有效安全保障。

关键词：车载自组织网络；认证密钥协商；经典-量子混合密码学；连续变量量子图态；量子隐形传态；安全哈希函数；量子计算攻击

中图分类号：TP309；TN918　　**文献标志码：**A

Authenticated Key Agreement Scheme for VANETs Based on Classical-Quantum Hybrid Cryptography

Liao Longxia[1], Fang He[2], Zhang Qingmiao[1], Zhao Junhui[3]

(1. School of Information and Software Engineering, East China Jiaotong University, Nanchang 330013, China; 2. School of Computer and Cyberspace Security, Fujian Normal University, Fuzhou 350007, China; 3. School of Electronic and Information Engineering, Beijing Jiaotong University, Beijing 100044, China)

Abstract: Aiming at the security risks of the authentication key negotiation scheme in the existing vehicular ad-hoc networks (VANETs) under the threat of quantum computing, a novel authentication key negotiation scheme integrating classical cryptography and continuous variable quantum cryptography is proposed. The scheme utilizes the quantum teleportation property of continuous variable quantum graph state (CVGS) to realize the authentication between vehicles and roadside units, and combines with secure hash function to complete the key negotiation. The security analysis shows that the scheme can effectively resist quantum computing attacks in a short period of time and satisfy the security requirements of authentication and key negotiation. Performance evaluation shows that compared with the existing quantum cryptography scheme, the number of required quantum states is reduced by half, which improves the feasibility of realization; compared with the traditional classical scheme, the computation and communication overheads are reduced by 77.27%和 63.76%, respectively. This scheme achieves a good balance between security and performance, and has a wide range of application prospects and practical deployment value, which can provide effective security for VANETs in the face of quantum threats.

Key words: vehicular ad-hoc networks; authentication key agreement; classical-quantum hybrid cryptography; continuous-variable quantum graph states; quantum teleportation property; secure hash functions; quantum computing attacks

收稿日期：2025-06-16
基金项目：国家重点研发计划（2020YFB1807204）.

随着城市交通压力的不断加剧，车载自组织网络（vehicular ad-hoc networks，VANETs）作为智能交通系统（intelligent transportation system, ITS）中的关键通信架构，已成为提升交通安全、缓解拥堵与优化出行体验的重要技术手段[1-2]。VANETs 通过支持车间（vehicle-to-vehicle, V2V）及车与基础设施间（vehicle-to-infrastructure, V2I）的信息交互，有效推动了 ITS 的发展。然而，由于其通信环境的开放性和节点的高动态性，VANETs 面临着身份冒用、信息窃取、篡改与伪造等严重安全威胁，甚至可能引发交通事故，威胁公众生命财产安全。因此，设计安全高效的认证与密钥协商机制已成为保障 VANETs 安全通信的核心任务[3-5]。

目前，国内外学者在 VANETs 安全认证与密钥协商（authentication key agreement, AKA）领域已提出多种方案。例如，基于双线性对的匿名认证方案可提供较强的安全性与隐私保护能力[6]，但认证延迟较高，难以满足 VANETs 对实时性的苛刻要求（10ms 以内）。椭圆曲线密码学（elliptic curve cryptography, ECC）方案[7-11]在计算复杂度与通信开销上取得了一定平衡，适合资源受限的车载终端[12]，但其安全性仍建立在椭圆曲线离散对数难题上，难以抵御量子计算威胁。据美国国家标准与技术研究所预测，到 2030 年，量子计算机或将在数小时内破解 2000 位 RSA 密钥[13]，这对以大数因子分解为基础的传统公钥体制构成严峻挑战。尽管后量子密码学算法在抗量子攻击方面展现出前景，但其计算复杂度通常是 ECC 的 2-4 倍[14]，难以完全适配车载高动态环境。与此同时，具有信息论安全特性的量子密码学也成为研究热点。以离散变量（discrete variable, DV）量子态为基础的认证方案[15-18]在提升安全性方面已有所突破，然而其匿名性欠佳、交互复杂，且系统实现难度较大，限制了其在实际车载环境中的应用。

在现有研究成果的基础上，VANETs 认证与密钥协商仍面临以下关键挑战：一方面，如何在保证系统安全性的前提下，降低认证与密钥协商过程中的计算与通信开销，确保协议在高动态、低延迟的车载环境下稳定运行；另一方面，如何有效应对量子计算发展带来的安全威胁，避免现有基于公钥体制的密码学算法失效。同时，DV 量子密码学方案对硬件设备要求高、抗干扰能力不足，限制了其在实际车载场景中的应用。因此，设计一种兼具高安全性、低开销与良好可实现性的认证密钥协商方案，成为 VANETs 安全研究亟需突破的重要课题。

针对上述问题，本文提出一种融合经典密码学与连续变量（continuously variable, CV）量子密码学的新型混合 AKA 方案。该方案充分利用连续变量量子图态（CVGS）的量子隐形传态特性，实现车辆与路侧单元之间的高效身份认证，并结合经典安全哈希函数完成密钥协商，有效降低了消息交互次数与计算复杂度，显著降低系统开销。安全性分析表明，该方案能够有效抵御量子计算相关攻击，满足身份认证与密钥协商的多项安全要求。性能评估显示，与现有量子密码方案相比，实际可行性更高；与传统经典方案相比，计算与通信开销分别降低了 77.27%和 63.76%，在安全性与性能之间取得良好平衡，为未来 VANETs 中的实用部署提供了可行路径。

1 系统模型

VANETs 系统主要由三类实体组成：可信的信任机构（trust authority, TA）、半可信的路侧单元（road side unit, RSU）和不可信的车辆，如图 1 所示。TA 负责系统中所有实体的注册与身份认证，并掌握车辆的真实身份信息；RSU 作为固定基础设施，提供服务并在 TA 与车辆间充当中介角色；车辆内置车载单元及

防篡改设备，用于存储敏感信息如会话密钥。所有实体均具备量子通信能力，内置量子处理单元）。尽管当前连续变量量子设备多处于实验室应用阶段，但已有研究展示了其芯片级集成和室温稳定运行能力[19]，为未来在 RSU 和车载终端中部署奠定了基础。

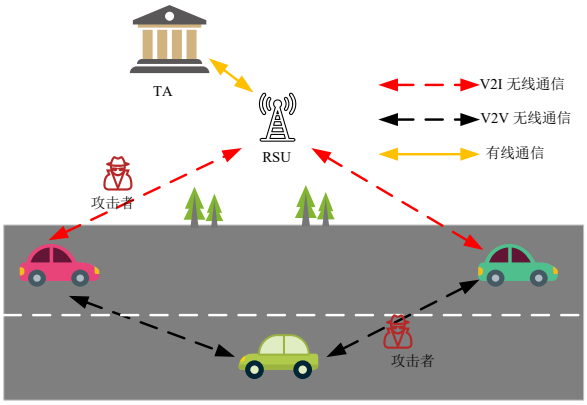

图 1　系统模型图

Fig.1 System model

本文提出的方案主要关注理论层面的安全性与效率，暂不涉及如 CVGS 稳定传输和量子纠缠实时分发等工程性挑战。在安全模型中，攻击者可能为车辆或 RSU，可发起被动或主动攻击。被动攻击包括监听通信以窃取隐私，主动攻击则涉及信息篡改与伪造。

本方案的安全目标包括：1）抗量子攻击能力，在量子计算威胁下短期内保护通信隐私；2）完成经过身份验证的会话密钥协商，实现车辆与 RSU 间的安全通信；3）抵御重放攻击、拦截－发送攻击、假冒攻击等常见威胁。

2　方案设计

本文所提方案包括四个阶段：初始阶段、注册阶段、认证阶段和密钥协议阶段。

2.1 初始阶段

1）TA 提前制备一些四模态 CVGSs。CVGS 是与无向数学图 $G=(V,E)$ 相对应的纠缠多模量子态。无向图不存在循环和两个顶点之间的多条边，它有一组有限的 n 个顶点 $V=\{v_i\}$ 和一组度数 $E=\{e_{i,j}=(v_i,v_j)\}$，其中 v_i 表示顶点 i，$e_{i,j}$ 表示连接顶点 v_i 和 v_j 的边。相应地，在 CVGS 中，每个顶点 $v_i\in V$ 表示一个模态 $\hat{a}_i$，而每条边 $e_{i,j}\in E$ 表示模态 $\hat{a}_i$ 和 $\hat{a}_j$ 之间的量子非破坏性测量（quantum non-demolition, QND）耦合。CVGS 是通过压缩态和线性光学产生的。首先，假设有 n 个初始真空状态，其位置为 $x_i^{(0)}$，动量为 $p_i^{(0)}(i=1,2,...n)$，随机变量 $x_i^{(0)}$ 和 $p_i^{(0)}$ 满足标准高斯分布。对初始真空态 $\hat{a}_i$ 和 $\hat{a}_j$ 进行局部高斯运算 $S(r)=\exp[r(\hat{x}\hat{p}+\hat{p}\hat{x})/2]$（$r$ 为压缩参数）后，真空态的动量被压缩，同时位置被放大。

$$\hat{x}_i=e^r\hat{x}_i^{(0)},\hat{p}_i=e^{-r}\hat{p}_i^{(0)}\quad(1)$$

之后，对模态 $\hat{a}_i$ 和 $\hat{a}_j$ 进行 QND 耦合操作后，对应模态的位置和动量变化为

$$\begin{aligned}\hat{x}_i&=\hat{x}_i,\hat{p}_i=\hat{p}_i+a_{ij}\hat{x}_j\\ \hat{x}_j&=\hat{x}_j,\hat{p}_j=\hat{p}_j+a_{ji}\hat{x}_i\end{aligned}\quad(2)$$

此处只考虑无向图状态，因此 QND 相互作用的强度是相同的，即 $a_{ij}=a_{ji}=1$。由（1）和（2）可以得到

$$\begin{aligned}&\hat{x}_i = e^r \hat{x}_i^{(0)}, \hat{p}_i = e^{-r} \hat{p}_i^{(0)} + e^r \hat{x}_j^{(0)} \\ &\hat{x}_j = e^r \hat{x}_j^{(0)}, \hat{p}_j = e^{-r} \hat{p}_j^{(0)} + e^r \hat{x}_i^{(0)}\end{aligned} \tag{3}$$

模态 $\hat{a}_i$ 和 $\hat{a}_j$ 相互纠缠，因此不可能完全确定它们的状态。当 $r \to \infty$ 时，有 $\hat{p}_i - \hat{x}_j \to 0$， $\hat{p}_j - \hat{x}_i \to 0$。

在 TA 生成的单个四模态 CVGS 中， $\hat{a}_1, \hat{a}_2, \hat{a}_3, \hat{a}_4$ 的位置和动量分别表示为：

$$\begin{aligned}&\hat{x}_1 = e^r \hat{X}_{in1}, \hat{p}_1 = e^{-r} \hat{P}_{in1} + e^r \hat{X}_{in2} \\ &\hat{x}_2 = e^r \hat{X}_{in2}, \hat{p}_2 = e^{-r} \hat{P}_{in2} + e^r \hat{X}_{in1} + e^r \hat{X}_{in3} \\ &\hat{x}_3 = e^r \hat{X}_{in3}, \hat{p}_3 = e^{-r} \hat{P}_{in3} + e^r \hat{X}_{in2} + e^r \hat{X}_{in4} \\ &\hat{x}_4 = e^r \hat{X}_{in4}, \hat{p}_4 = e^{-r} \hat{P}_{in4} + e^r \hat{X}_{in3}\end{aligned} \tag{4}$$

其中，模态的初始状态遵循高斯分布，即 $X_{in1}, X_{in2}, X_{in3}, X_{in4}, P_{in1}, P_{in2}, P_{in3}, P_{in4} \sim N(o, \sigma^2)$。在所设计方案中，利用 CVGSs 的纠缠和量子远程传态特性实现身份认证。

2）TA 选择三个 512-bits 的安全哈希函数，以确保信息的安全传输。此外，TA 初始化两个空的身份布谷鸟过滤器（identity cuckoo filter, ICF），分别表示为 ICF_v 和 ICF_r，用于存储与所有注册车辆和 RSU 相对应的指纹。

2.2 注册阶段

1）对于每辆车 V_i，制造商通过安全、预先建立的渠道（例如，在工厂配置期间）向 TA 提交其真实身份 $RID_{v_i} \in Z_q^*$。TA 选择随机数 m_{v_i} 并计算 V_i 的认证密钥 $k_{v_i} = RID_{v_i} \oplus m_{v_i}$。TA 秘密存储 k_{v_i}，并通过秘密信道将 k_{v_i} 传输给 V_i。收到 k_{v_i} 后， V_i 通过计算 $m_{v_i} = RID_{v_i} \oplus k_{v_i}$ 获取共享密钥 m_{v_i}，随后将 k_{v_i} 和 m_{v_i} 安全地存储在其 TPD 中。

2）同理，在部署路边单元 R_j 时，操作员安全地将其真实身份 $RID_{r_j} \in Z_q^*$ 传输给 TA。 TA 选择随机 n_{r_j} 数，计算 R_j 的认证密钥 $k_{r_j} = RID_{r_j} \oplus n_{r_j}$。然后，TA 秘密存储 k_{r_j}，并通过秘密信道将 k_{r_j} 传输给 R_j。 R_j 计算 $n_{r_j} = RID_{r_j} \oplus k_{r_j}$，并秘密存储 k_{r_j} 和 n_{r_j}。

2.3 认证阶段

车辆 V_i 在 R_j 的范围内行驶时， V_i 发送认证请求给 R_j。同时， R_j 将请求转发给 TA。TA 利用 CVGSs 的量子隐形传态特性对 V_i 和 R_j 进行身份验证，如图 2 所示，具体步骤如下。

步骤 1：TA 选择四模态 CVGSs，其位置和动量如公式（4）所示。

步骤 2：TA 对模态 $\hat{a}_2$ 和 $\hat{a}_4$ 进行反傅里叶变换运算，模态 $\hat{a}_2$ 和 $\hat{a}_4$ 的位置和动量变为：

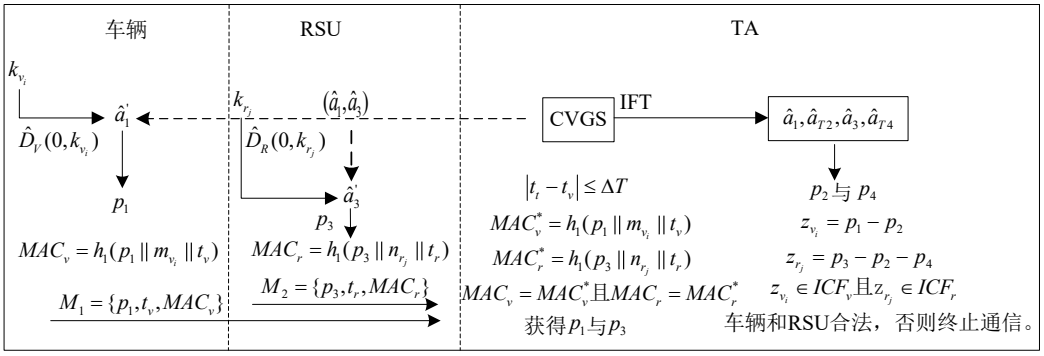

图 2 身份认证过程

Fig.2 Authentication process

$$\begin{aligned}&\hat{x}_{T2}=-e^{-r}\hat{p}_{in2}-e^{r}\hat{X}_{in1}-e^{r}\hat{X}_{in3},\hat{p}_{T2}=e^{r}\hat{X}_{in2}\\&\hat{x}_{T4}=-e^{-r}\hat{p}_{in4}-e^{r}\hat{X}_{in3},\hat{p}_{T4}=e^{r}\hat{X}_{in4}\end{aligned}\quad(5)$$

当 $r\to\infty$ 时，位置的关系为 $\hat{x}_1+\hat{x}_{T2}+\hat{x}_3=0$，$\hat{x}_3+\hat{x}_4=0$，动量关系为 $\hat{p}_1-\hat{p}_{T2}=0$，$\hat{p}_3-\hat{p}_{T2}-\hat{p}_4=0$。因此，模态 $\hat{a}_1,\hat{a}_{T2},\hat{a}_3,\hat{a}_{T4}$ 之间是纠缠的，存在很强的相关性。TA 保留模态 $\hat{a}_{T2}$ 和 $\hat{a}_{T4}$，然后将模态 $\hat{a}_1$ 和模态 $\hat{a}_3$ 分别发送给 V_i 和 R_j。

步骤 3：确认收到 $\hat{a}_1$ 后，V_i 对模态 $\hat{a}_1$ 应用位移算子 $\hat{D}_v(0,k_{v_i})$，将车辆的认证密钥 k_{v_i} 隐秘地编码到模态 $\hat{a}_1$ 上。位移算子定义如下

$$\hat{D}(\alpha,\beta)=\begin{cases}\hat{x}\to\hat{x}+\alpha\\\hat{p}\to\hat{p}+\beta\end{cases}\quad(6)$$

执行位移算子后，模态 $\hat{a}_1$ 的位置和动量变为 $\hat{x}_{V'}=e^{r}\hat{X}_{in1}$ 和 $\hat{p}_{V'}=e^{-r}\hat{p}_{in1}+e^{r}\hat{X}_{in2}+k_{v_i}$。$V_i$ 测量所持模态的动量，得到 p_1。随后，V_i 将测量结果 p_1 发送给 TA。

利用量子密钥分发或量子数字签名技术传输经典测量结果，可以有效抵御量子计算攻击。然而，使用这两种方法都不可避免地会增加整体开销，使系统变得更加复杂。因此，本方案使用基于哈希的消息认证码（hash-based message authentication code, HMAC）来保障测量结果的安全传输。

V_i 计算测量结果 p_1 的消息认证码，得到 $MAC_v=h_1(p_1\|m_{v_i}\|t_v)$，其中 t_v 为当前时间。之后，V_i 将 $M_1=\{p_1,t_v,MAC_v\}$ 发送给 TA。同理，收到 $\hat{a}_3$ 后，R_j 将位移算子 $\hat{D}_R(0,k_{r_j})$ 应用于模态 $\hat{a}_3$，从而将其转化为模态 $\hat{a}_R$。模态 $\hat{a}_R$ 的位置和动量表示如下：

$$\begin{aligned}&\hat{x}_R=e^{r}\hat{X}_{in3}\\&\hat{p}_R=e^{-r}\hat{P}_{in3}+e^{r}\hat{X}_{in2}+e^{r}\hat{X}_{in4}+k_{r_j}\end{aligned}\quad(7)$$

然后，R_j 测量模式 $\hat{a}_R$ 的动量，得到 p_3。R_j 计算 p_3 的 MAC 值为 $MAC_r=h_1(p_3\|n_{r_j}\|t_r)$，其中 t_r 是时间戳。然后，R_j 将 $M_2=\{p_3,t_r,MAC_r\}$ 发送给 TA。

步骤 4：收到 M_1 和 M_2 后，TA 获取当前时间戳 t_t 并通过检查 $|t_t-t_v|\le\Delta T$ 是否成立来检查消息的新鲜度。若成立，TA 验证收到信息的可靠性和完整性。TA 使用其存储的验证密钥 m_{v_i} 和 n_{r_j} 计算 $MAC_v^*=h_1(p_1\|m_{v_i}\|t_v)$ 和 $MAC_r^*=h_1(p_3\|n_{r_j}\|t_r)$。如果 $MAC_v^*=MAC_v$ 且 $MAC_r^*=MAC_r$，则消息来自可靠方且未被篡改。

TA 测量保留模态的动量，得到经典结果 p_2 和 p_4。然后，TA 计算 $z_{v_i}=p_1-p_2$ 和 $z_{r_j}=p_3-p_2-p_4$。若，$z_{v_i}\in ICF_v$ 且 $z_{r_j}\in ICF_r$，表明 $z_{v_i}=k_{v_i}$ 和 $z_{r_j}=k_{r_j}$。TA 确认 V_i 和 R_j 为合法参与者。否则，将推断出存在攻击者或未经授权的参与者，并终止通信。

2.4 密钥协商阶段

如果 V_i 和 R_j 都是合法的，TA 利用安全哈希函数协 V_i 和 R_j 生成会话密钥，如图 3 所示，步骤如下：

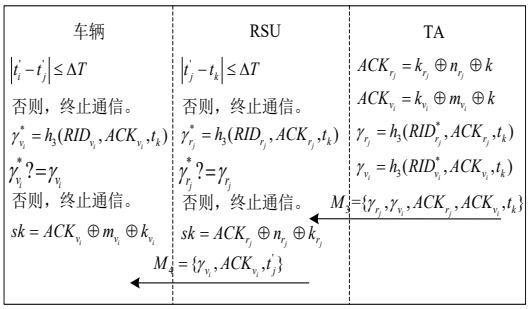

图 3 密钥协商过程

Fig.3 Key negotiation process

1）TA 生成确认信息 M_3 并发送给 R_j。首先，TA 随机选择会话密钥 k 且 $k\in Z_q^*$，并计算 $ACK_{v_i}=k_{v_i}\oplus m_{v_i}\oplus k$ 和 $ACK_{r_j}=k_{r_j}\oplus n_{r_j}\oplus k$。其次，TA 计算验证消息完整性的 $\gamma_{r_j}=h_3(RID_{r_j}^{*},ACK_{r_j},t_k)$ 以及 $\gamma_{v_i}=h_3(RID_{v_i}^{*},ACK_{v_i},t_k)$。最后，TA 将验证消息 $M_3=\{\gamma_{v_i},\gamma_{r_j},ACK_{v_i},ACK_{r_j},t_k\}$ 发送给 R_j。

2）R_j 获取会话密钥。收到 M_3 后，R_j 获取当前时间戳 $t_j^{'}$，并检查 $|t_j^{'}-t_k|\le\Delta T$ 是否成立。若成立，R_j 计算 $\gamma_{r_j}^{*}=h_3(RID_{r_j},ACK_{r_j},t_k)$，并判定 $\gamma_{r_j}^{*}=\gamma_{r_j}$ 是否成立。若不成立，则终止通信。否则，R_j 通过计算 $sk=ACK_{r_j}\oplus m_{r_j}\oplus k_{r_j}$ 获取会话密钥。最后，R_j 将验证消息 $M_4=\{\gamma_{v_i},ACK_{v_i},t_k,t_j^{'}\}$ 发送给 V_i。

3）V_i 获取会话密钥。收到 M_4 后，V_i 获取当前时间戳 $t_i^{'}$ 并检查 $|t_i^{'}-t_j^{'}|\le\Delta T$ 是否成立。如果不成立，V_i 拒绝该信息。否则，V_i 计算 $\gamma_{v_i}^{*}=h_3(RID_{v_i},ACK_{v_i},t_k)$ 并判断 $\gamma_{v_i}^{*}=\gamma_{v_i}$ 是否成立。若不成立，则终止通信。否则，V_i 通过计算 $sk=ACK_{v_i}\oplus n_{v_i}\oplus k_{v_i}$ 从而获取会话密钥 sk。

3 安全性和性能分析

本文对所提方案的安全和隐私需求满足情况进行了分析，并利用形式化验证工具 ProVerif 对协议进行了验证。同时，将方案与量子密码学及经典密码学方案进行了比较。

3.1 安全和隐私需求满足情况

1）抗量子计算攻击。所提方案使用 CVGSs 实现车辆和 RSU 的身份验证，以确保认证密钥的安全性，从而抵御量子计算攻击。利用安全哈希函数保障经典信息的安全传输。

验证阶段，TA 生成将模态 $\hat{a}_1$ 和模态 $\hat{a}_3$ 并分别发送给 V_i 和 R_j。随后，V_i 和 R_j 对各自的模态进行位移操作 $\hat{D}_v(0,k_{v_i})$ 和 $\hat{D}_r(0,k_{r_j})$，将各自的认证密钥隐秘地编码到 TA 的模态 $\hat{a}_{T2}$ 和 $\hat{a}_{T4}$。根据 CVGSs 的动量-位置纠缠关系，TA 通过测量结果可以完成参与方合法性验证。这一过程利用量子态的不可分割性来实现无条件安全的身份验证。

在密钥协商阶段，方案使用 512-bits 哈希函数保障经典信息的传输。虽然 Grover 算法将哈希函数的蛮力搜索复杂度从 $O(2^n)$ 降低到 $O(2^{n/2})$，但 512 位密钥仍然提供了 $O(2^{256})$ 的等效安全强度。这种量子经典混合架构有助于平衡现有经典技术与未来量子技术之间的过渡。

2）身份认证：TA 通过计算 $z_{v_i}=p_1-p_2$ 和 $z_{r_j}=p_3-p_2-p_4$ 来判定参与者的合法性。若，$z_{v_i}\in ICF_v$ 且 $z_{r_j}\in ICF_r$，表明 V_i 和 R_j 为合法参与者。否则，将推断出存在攻击者或未经授权的参与者，并终止通信。

3）会话密钥协议：TA 验证 V_i 和 R_j 的真实身份后，向 R_j 返回确认信息 ACK_{r_j} 和 ACK_{v_i}。由于 $ACK_{v_i}=k_{v_i}\oplus m_{v_i}\oplus k$，$ACK_{r_j}=k_{r_j}\oplus n_{r_j}\oplus k$，$V_i$ 和 R_j 可以分别通过计算 $sk=ACK_{v_i}\oplus n_{v_i}\oplus k_{v_i}$ 和

$sk = ACK_{r_j} \oplus m_{r_j} \oplus k_{r_j}$ 来获得协商的会话密钥 sk 。

4）抵御重放攻击：接收方收到信息后，首先要检查信息的新鲜度。如果消息时延在接受范围内，接收方将检查报文的完整性，确保传送的报文未被修改。否则，接收方将把它视为过期信息。因此，本文提出的方案可确保防止重放攻击。

5）抵御拦截-发送攻击：所提方案的验证过程中，有两个量子信道和四个经典信道。认证阶段，经典测量结果的传输采用 HMAC 实现安全传输。在认证阶段，经典测量结果的传输采用 HMAC 实现安全传输。在密钥协商阶段，经典信息的传输采用安全哈希函数。由于在经典信道中传输的信息是公开的或独立于秘密信息的，因此在经典信道中的拦截-发送不会构成威胁。量子信道中，为获取认证密钥信息，拦截-发送攻击者截获 TA 在步骤 2 中发送的模态 $\hat{a}_1$ 和 $\hat{a}_3$，对其进行测量后发送给 RSU。由于模态与认证密钥无关，攻击者测量后无法获得有用信息。此外，量子不可克隆定理表明，攻击者对模态的测量将导致量子态坍缩。

6）抵御假冒攻击：假设攻击者伪装成合法车辆，试图通过接收到的模态 $\hat{a}_1$ 发动攻击，企图通过认证。攻击者对模态 $\hat{a}_1$ 执行位移算子 $\hat{D}_E(e_1,e_2)$，模态 $\hat{a}_1$ 变为 $\hat{a}_E$，其位置和动量分别为：$\hat{x}_E = e^r \hat{X}_{in1} + e_1$ 和 $\hat{p}_E = e^{-r} \hat{P}_{in1} + e^r \hat{X}_{in1} + e_2$。然后，攻击者将测量结果 p_e 发送给 TA。在步骤 5 中，TA 测量所持模态后，计算 $z_e = p_e - p_2 - e_2$。由于攻击者没有正确的 k_{v_i}，TA 查找不到 z_e，认证过程将失败。

3.2 形式化验证

为验证所提出协议的安全性，本文使用形式化验证工具 ProVerif 2.05 对协议进行建模与分析。在建模过程中，考虑了车辆（Vehicle）、路侧单元（RSU）以及可信机构（TA）三方实体，并在 Dolev-Yao 攻击模型下假设攻击者可以完全控制通信信道，但无法破解密码学原语（如哈希函数和异或运算）。在安全性验证中，重点关注以下安全属性：

为评估所提协议的安全性，本文采用验证工具 ProVerif 2.05 进行形式化分析，该工具基于 Dolev-Yao 攻击者模型。验证结果如图 4 所示，总结如下：

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

Query not attacker(kv[]) is true.

Query not attacker(kr[]) is true.

Query event(endAuthVehicle) ==> event(beginAuthVehicle) is true.

Query event(endAuthRSU) ==> event(beginAuthRSU) is true.

Query event(acceptSessionKey) ==> event(endAuthVehicle) is true.

Query not attacker(k[]) is true.

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

图 4 ProVerif 2.05 的输出结果

Fig. 4 The output of ProVerif 2.05

1）密钥保密性：协议确保了车辆与路侧单元（RSU）的密钥 k_{v_i} 和 k_{r_j} 不会被攻击者获取。query attacker(kv) 和 query attacker(kr) 查询结果均为 not attacker(kv)和 not attacker(kr)，表明密钥未被泄露，攻击者无法获取相关密钥信息。

2）双向认证性：通过 query event(endAuthVehicle) ==> event(beginAuthVehicle) 和 query event(endAuthRSU) ==> event(beginAuthRSU) 两条认证性查询，对车辆与 RSU 双方的认证过程进行了验证，结果均满足查询条件，说明认证过程安全可靠，未被冒充或中断。此外，query event(acceptSessionKey) ==> event(endAuthVehicle) 查询结果也被满足，表明会话密钥仅在车辆完成认证后才被接受使用。

3）会话密钥保密性：针对生成的会话密钥 k，执行了 query attacker(k) 查询，结果返回 not attacker(k)，说明攻击者无法窃取会话密钥，其安全性得以保障。

综上所述，形式化安全性分析结果表明，所提协议在机密性、双向认证性以及会话密钥安全性方面均能够满足安全需求，能够有效抵御多种典型网络安全威胁。

3.3 性能分析

本节将所提方案分别与量子密码学方案[16]、[17、[18]和经典密码学方案[7]、[8]、[20]进行比较分析。

1）与量子密码学方案比较

所提方案与文献[16]、[17]和[18]中的方案在量子态类型、通信轮数和量子态制备次数方面进行了比较，如表 1 所示。[16]、[17]和[18]基于 DV 量子态，在实际应用中面临多个设计挑战，如量子比特质量、纠错和量子比特控制。在建立基于 DV 量子计算的认证协议时，生成门操作和复杂指令对高质量量子比特的要求不容忽视。当量子比特用于任何计算时，它们往往会产生不正确的结果。在通信轮数方面，本文所提方案的经典信息传输轮数低于文献[18]中的方案，而量子信息传输次数低于文献[16]和[17]。此外，在整个验证阶段，文献[16]和[17]需要进行 2 次 DV 量子态的准备，而我们的方案只需要生成 1 次 CVGS 量子态。如上所述，我们的方案更具优势。

表 1 与量子密码学方案的比较

Table 1 Comparison with quantum cryptography schemes

方案	量子态类型	通信轮数（次数）	量子态制备次数
文献[16]	DV	2（量子）	2
文献[17]	DV	2（量子）+2（经典）	2
文献[18]	DV	0（量子）+5（经典）	4
所提方案	CV	1（量子）+2（经典）	1

2）与经典密码学方案比较

所提方案与文献[7]、文献[8]和文献[20]中的方案在计算和通信开销方面进行了对比分析。为便于比较，系统安全级别设为 80-bit 级。椭圆曲线加密算法中，p 和 q 的长度均为 20 字节，椭圆曲线组G的大小为 40 字节。根据最新研究，量子态的生成与测量普遍处于皮秒至微秒量级，其中 CVGS 纠缠态的平均制备时间通常不超过 500 纳秒[21]。相较于经典密码算法（如 SHA-512）的一轮哈希处理，量子操作在时间维度上并不构成显著瓶颈，故其计算开销可在整体性能分析中忽略不计。

基于 JPBC 库和 Pallier PKE，使用 Java 编程计算不同加密算法执行 100 次的平均耗时如下：标量乘法运算 $T_{sm}=0.251$，拉格朗日插值运算 $T_{li}=0.004$，伪随机函数运算 $T_{prf}=0.007$，对称加密算法加密/解密 $T_{e/d}=0.026$，物理不可克隆函数 $T_{puf}=0.1$，单向哈希运算 (SHA-256) $T_h=0.001$，单向哈希运算 (SHA-512) $T_h^*=0.002$。

① 计算开销

对比计算开销时，主要分析了认证阶段和密钥协商阶段的计算开销。如图 5 所示，所提方案的总计算开销远低于文献[7]（0.541）、文献[8]（1.76）与文献[20]（0.82）。相较而言，所提方案在总计算开销上分别减少了约 26.05%、77.27%和 51.22%。

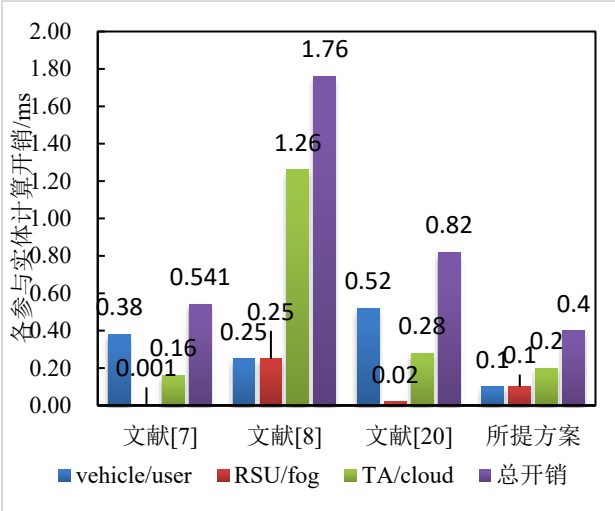

图 5 计算开销对比

Fig.5 Computation overhead comparison

② 通信开销

在所设计的方案中，认证阶段和密钥协商阶段共涉及 4 条消息的传输。认证阶段，车辆和 RSU 将测量结果发送给 TA，即 $M_1=\{p_1,t_v,MAC_v\}$ 和 $M_2=\{p_3,t_r,MAC_r\}$。在密钥协商阶段，TA 发送 $M_3=\{\gamma_{r_j},\gamma_{v_i},MAC_{r_j},MAC_{v_i},t_k\}$ 给 RSU，RSU 发送 $M_4=\{\gamma_{v_i},ACK_{v_i},t_k,t_j^{'}\}$ 给车辆。因此，所提方案的总通信开销为：$10\left|Z_q^*\right|+4|T|$，即 216 字节。

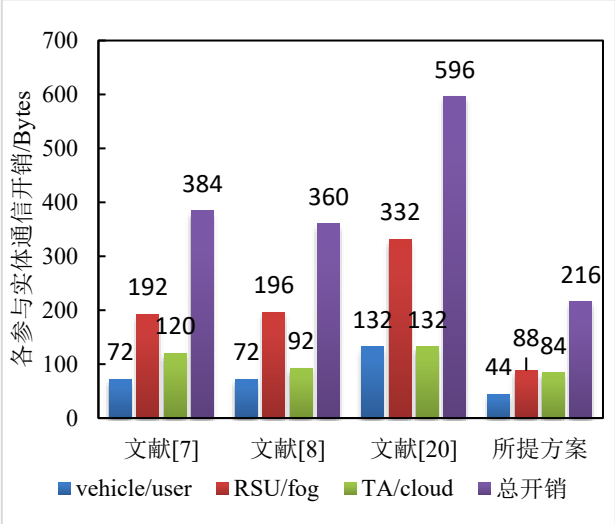

图 6 通信开销对比

Fig.6 Communication overhead comparison

图 6 是各对比方案中不同实体所消耗的通信开销。与文献[7]、文献[8] 和文献[20] 中方案相比，所提方案在通信开销上分别降低了 43.75%、40.00% 和 63.76%。

4 结论

本文采用经典密码学与连续变量量子图态相结合的方法，对车载自组织网络中的认证密钥协商方案进行了研究，得出以下结论：

1）利用连续变量量子图态的量子隐形传态特性实现了高效的身份认证，结合经典安全哈希函数完成了密钥协商，有效降低了认证过程中的消息交互次数和计算复杂度。

2）安全性分析表明，所提出的混合认证密钥协商方案能够在短期内抵御量子计算相关攻击，满足身份认证、密钥协商等多项安全要求，提升了系统的安全性与鲁棒性。

3）性能分析显示，相较现有量子密码学方案，该方案所需量子态数量少，易于实际部署；相较传统经典密码学方案，计算和通信开销分别降低了 77.27%和 63.76%，展现出良好的安全性与性能平衡。

参考文献：

[1] Khezri E, Hassanzadeh H, Yahya R O, et al. Security challenges in internet of vehicles (IoV) for ITS: A survey[J]. Tsinghua Science and Technology, 2025, 30(4): 1700-1723.

[2] Zhao J H, Hu H H, Huang F W, et al. Authentication technology in internet of things and privacy security issues in typical application scenarios[J].Electronics, 2023, 12(8): 1812.

[3] Liao L L, Zhao J H, Hu H H, et al. Secure and efficient message authentication scheme for 6G-enabled VANETs[J].Electronics, 2022, 11(15): 2385.

[4] 张晗,陈立全,杨波,方瑞琦.5G 工业互联网下的轻量级数据使用安全方案[J].东南大学学报(自然科学版),2024,54(3):772-780.
Zhang Han,Chen Liquan,Yang Bo,Fang Ruiqi.Secure lightweight data using scheme in 5G industrial Internet systems[J].Journal of Southeast University (Natural Science Edition),2024,54(3):772-780.

[5] 张海波, 兰凯, 黄宏武, 王汝言, 邹灿. 车联网中可证安全的分布式匿名高效边缘认证协议[J]. 电子与信息学报, 2023, 45(8): 2902-2910.
ZHANG Haibo, LAN Kai, HUANG Hongwu, WANG Ruyan, ZOU Can. Provably Secure Distributed Efficient Edge Authentication Protocol with Anonymity in Internet of Vehicles[J]. Journal of Electronics & Information Technology, 2023, 45(8): 2902-2910.

[6] Azees M, Vijayakumar P, Deboarh L J.EAAP: Efficient anonymous authentication with conditional privacy preserving scheme for vehicular ad hoc networks[J].IEEE Transactions on Intelligent Transportation Systems, 2017, 18(9): 2467-2476.

[7] Saleem M A, Li X, Ayub M F, et al. An efficient and physically secure privacy-preserving key-agreement protocol for vehicular ad-hoc network[J]. IEEE Transactions on Intelligent Transportation Systems, 2023, 24(9): 9940-9951.

[8] Awais S M, Yucheng W, Mahmood K, et al. Provably secure and lightweight authentication and key agreement protocol for fog-based vehicular ad-hoc networks[J]. IEEE Transactions on Intelligent Transportation Systems, 2024, 12(25):21107 - 21116.

[9] Liang Y F, Luo ET, Liu Y N. Physically secure and conditional-privacy authenticated key agreement for VANETs[J].IEEE Transactions on Vehicular Technology, 2023, 72(6): 7914-7925.

[10] Rajkumar Y, Kumar S V N S. An elliptic curve cryptography based certificate-less signature aggregation scheme for efficient authentication in vehicular ad hoc networks[J]. Wireless Networks, 2024, 30(1): 335-362.

[11] Jiang Q, Zhang N, Ni J B, et al. Unified biometric privacy preserving three-factor authentication and key agreement for cloud-assisted autonomous vehicles[J].IEEE Transactions on Vehicular Technology, 2020, 69(9): 9390-9401.

[12] 周天清,王博博. UDN 中面向安全卸载的多目标联合优化算法研究[J].华东交通大学学报, 2024,41(1):70-77.
Zhou Tianqing, Wang Bobo. Research on Multi-Objective Joint Optimization Algorithm for Secure Offloading in UDN[J]. JOURNAL OF EAST CHINA JIAOTONG UNIVERSTTY, 2024,41(1):70-77.

[13] Cooper D, Apon D, Dang Q, et al. NIST Special Publication 800-208: Recommendation for stateful hash based signature schemes (2020)[EB/OL].

[14] Dam D T, Tran T H, Hoang V P, et al. A survey of post quantum cryptography: Start of a new race[J].Cryptography, 2023, 7(3): 40.

[15]Xiao H L, Chronopoulos A T, Zhang Z S. An efficient security scheme for vehicular communication using a quantum secret sharing method[J].IEEE Transactions on Vehicular Technology, 2019, 69(1): 1101-1105.

[16]Chen Z Y, Zhou K L, Liao Q. Quantum identity authentication scheme of vehicular ad-hoc networks[J].International Journal of Theoretical Physics, 2019, 58: 40-57.

[17]Prateek K, Altaf F, Amin R, et al. A privacy preserving authentication protocol using quantum computing for V2I authentication in vehicular ad hoc networks[J].Security and Communication Networks, 2022, 2022(1): 4280617.

[18]Shi Q, Yang Z, Cheng T, et al. Qkbaka: a quantum key based authentication and key agreement scheme for internet of vehicles[J].IEEE Internet of Things Journal, 2023, 11(7): 12292-12306.

[19]Piétri Y, Vidarte L T, Schiavon M, et al. CV-QKD receiver platform based on a silicon photonic integrated circuit[C]//2023 Optical Fiber Communications Conference and Exhibition (OFC). IEEE, 2023: 1-3.

[20]Wei L, Cui J, Zhong H, et al. A lightweight and conditional privacy-preserving authenticated key agreement scheme with multi-TA model for fog-based VANETs[J].IEEE Transactions on Dependable and Secure Computing, 2021, 20(1): 422-436.

[21]Tornow C, Kanazawa N, Shanks W E, et al. Minimum quantum run-time characterization and calibration via restless measurements with dynamic repetition rates[J].Physical Review Applied, 2022, 17(6): 064061.

第一作者：廖龙霞（1989—），女，博士生，实验师，研究方向为无线网络信息安全。E-mail：liaolxcl@163.com。

通信作者：赵军辉（1973—），男，教授，博士，博士生导师，研究方向为宽带移动通信系统与专用移动通信、通信工程、人工智能、新一代电子信息技术无线和移动通信及相关应用。E-mail：junhuizhao@hotmail.com。