文章编号:1005-0523(2026)05-0055-08

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 330013;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.北京交通大学电子信息工程学院,北京 100044)

摘要:针对现有车载自组织网络(VANETs)中认证密钥协商方案面对量子计算威胁时存在的安全隐患,文章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,该方案能够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;相较代表性传统方案,计算与通信开销最高分别降低77.27%和63.76%。该方案在安全性与性能之间实现了良好平衡,具备广泛的应用前景与实际部署价值,可为VANETs在面临量子威胁时提供有效的安全保障。

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

中图分类号:TP309;TN918　　**文献标志码:**A

本文引用格式:廖龙霞,方禾,张青苗,等. 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[J]. 华东交通大学学报,2026,43(5):55-62.

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 agreement scheme in the existing vehicular ad-hoc networks (VANETs) under the threat of quantum computing, a novel authentication key agreement 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 agreement. 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 agreement. Performance evaluation shows that compared with the existing quantum cryptography scheme, the number of required quantum states is reduced, which improves the feasibility of realization; compared with the traditional classical scheme, the compu-

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

tation and communication overheads are reduced by 77.27% and 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

Citation format: Liao Longxia, Fang He, Zhang Qingmiao, et al. Authenticated key agreement scheme for VANETs based on classical-quantum hybrid cryptography[J]. Journal of East China Jiaotong University, 2026, 43(5): 55-62.

随着城市交通压力的不断增大，车载自组织网络（VANETs）作为智能交通系统（ITS）中的关键通信架构，已逐渐成为提升交通安全、缓解拥堵与优化出行体验的重要技术手段[1-2]。VANETs通过支持车与车之间（V2V）及车与基础设施之间（V2I）的信息交互，有效推动了ITS的发展。然而，由于通信环境的开放性和节点的高动态性，VANETs面临身份冒用、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，危及公众生命财产安全。因此，设计安全高效的认证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安全认证密钥协商（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（10 ms以内）。椭圆曲线密码学（ECC）方案[7-11]在计算复杂度与通信开销之间取得了一定平衡，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（NIST）预测，到2030年，量子计算机或将在数小时内破解2 048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了严峻挑战。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（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。此外，离散变量（DV）量子密码学方案对硬件设备要求较高，且抗干扰能力不足，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（CV）量子密码学的混合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，显著减少了系统开销。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；与传统方案相比，计算与通信开销最高分别降低了77.27%和63.76%，在安全性与性能之间取得了良好平衡，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3类实体组成：可信机构（TA）、半可信的路侧单元（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与车辆之间担任中

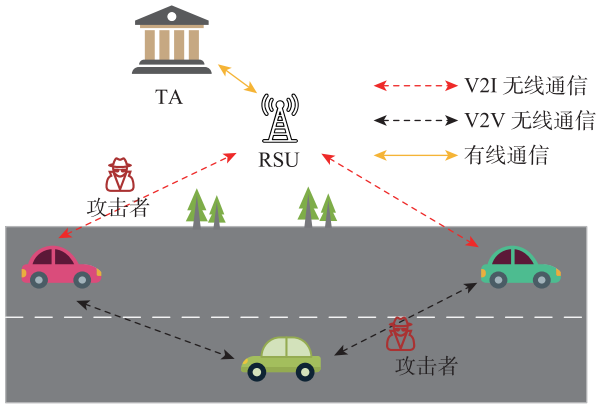


图1　系统模型
Fig. 1　System model

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，并内置量子处理单元。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。

本文所提方案主要关注理论层面的安全性与效率，暂不涉及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，能够发起被动或主动攻击。被动攻击包括监听通信以窃取隐私，而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，即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之间的安全通信；③ 抵御重放攻击、中间人攻击、假冒攻击等常见威胁。

2　方案设计

本文所提方案包括4个阶段：初始阶段、注册阶段、认证阶段和密钥协商阶段。

2.1　初始阶段

1）TA提前制备一些四模态CVGS。CVGS是与无向数学图相对应的纠缠多模量子态。无向图不存在环和两个顶点之间的多条边，它有一组有限的顶点和一组边，其中 v_i 表示第 i 个顶点，$e_{i,j}$ 表示连接顶点 v_i 和 v_j 的边。相应地，在CVGS中，每个顶点表示一个模态，而每条边表示两个模态之间的量子非破坏性测量（QND）耦合。CVGS是通过压缩态和线性光学器件产生的。首先，假设存在一个初始真空状态，其位置为 $\hat{x}_i$，动量为 $\hat{p}_i$。对初始真空态的位置和动量进行局部高斯运算（其中 r 为压缩参数）后，真空态的动量被压缩，同时位置被放大。表达式为

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

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

$$\begin{cases} \hat{x}_i = \hat{x}_i, \hat{p}_i = \hat{p}_i + a_{ij}\hat{x}_j \\ \hat{x}_j = \hat{x}_j, \hat{p}_j = \hat{p}_j + a_{ji}\hat{x}_i \end{cases} \tag{2}$$

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 $a_{ij}=a_{ji}=1$。由式（1）和式（2）可以得到

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

模态 $\hat{a}_i$ 和 $\hat{a}_j$ 相互纠缠，因此不可能完全确定它们各自的状态。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

$$\begin{cases} \hat{x}_1 = e^r \hat{X}_{\text{in}1}, \hat{p}_1 = e^{-r} \hat{P}_{\text{in}1} + e^r \hat{X}_{\text{in}2} \\ \hat{x}_2 = e^r \hat{X}_{\text{in}2}, \hat{p}_2 = e^{-r} \hat{P}_{\text{in}2} + e^r \hat{X}_{\text{in}1} + e^r \hat{X}_{\text{in}3} \\ \hat{x}_3 = e^r \hat{X}_{\text{in}3}, \hat{p}_3 = e^{-r} \hat{P}_{\text{in}3} + e^r \hat{X}_{\text{in}2} + e^r \hat{X}_{\text{in}4} \\ \hat{x}_4 = e^r \hat{X}_{\text{in}4}, \hat{p}_4 = e^{-r} \hat{P}_{\text{in}4} + e^r \hat{X}_{\text{in}3} \end{cases} \tag{4}$$

式中：下标in表示该模态为输入状态；模态的初始状态遵循高斯分布，即 $X_{\text{in}1}, X_{\text{in}2}, X_{\text{in}3}, X_{\text{in}4}, P_{\text{in}1}, P_{\text{in}2}, P_{\text{in}3}, P_{\text{in}4} \sim N(0, \sigma^2)$。在所设计方案中，利用CVGS的纠缠和量子隐形传态特性实现身份认证。

2）TA选择3个512位的安全哈希函数，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 F_V 和 F_R，用于存储与所有注册车辆（V）和RSU（R）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 I_{V_i}，$I_{V_i} \in Z_q^*$。TA选择随机数 m_{V_i} 并计算 V_i 的认证密钥 $k_{V_i} = I_{V_i} \oplus m_{V_i}$。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 $m_{V_i} = I_{V_i} \oplus k_{V_i}$ 获取共享密钥 m_{V_i}，随后将 k_{V_i} 和 m_{V_i} 安全地存储在其防篡改设备（TPD）中。q 为大素数，构成有限域 Z_q^* 的阶，Z^* 为正整数的集合。

2）同理，在部署路侧单元 R_j 时，操作员安全地将其真实身份 $I_{R_j}\in Z_q^*$ 传输给TA。TA选择随机数 n_{R_j}，计算 R_j 的认证密钥 $k_{R_j}=I_{R_j}\oplus n_{R_j}$。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 $n_{R_j}=I_{R_j}\oplus k_{R_j}$，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CVGS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CVGS，其位置和动量如式(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(IFT)运算，模态 $\hat{a}_2$ 和 $\hat{a}_4$ 的位置和动量变为

$$\begin{cases}\hat{x}_{R_2}=-\mathrm{e}^{-r}\hat{p}_{\mathrm{in}2}-\mathrm{e}^{r}\hat{X}_{\mathrm{in}1}-\mathrm{e}^{r}\hat{X}_{\mathrm{in}3},\hat{p}_{R_2}=\mathrm{e}^{r}\hat{X}_{\mathrm{in}2}\\ \hat{x}_{R_4}=-\mathrm{e}^{-r}\hat{p}_{R_4}-\mathrm{e}^{r}\hat{X}_{R_3},\hat{p}_{R_4}=\mathrm{e}^{r}\hat{X}_{R_4}\end{cases}\tag{5}$$

当 $r\to\infty$ 时，位置的关系为 $\hat{x}_1+\hat{x}_{\mathrm{T}2}+\hat{x}_3=0$，$\hat{x}_3+\hat{x}_4=0$，动量关系为 $\hat{p}_1-\hat{p}_{\mathrm{T}2}=0$，$\hat{p}_3-\hat{p}_{\mathrm{T}2}-\hat{p}_4=0$。下标T表示该模态为TA端模态。模态 $\hat{a}_1$，$\hat{a}_{\mathrm{T}2}$，$\hat{a}_3$，$\hat{a}_{\mathrm{T}4}$ 之间是纠缠的，存在很强的相关性。TA保留模态 $\hat{a}_{\mathrm{T}2}$ 和 $\hat{a}_{\mathrm{T}4}$，然后将模态 $\hat{a}_1$ 和模态 $\hat{a}_3$ 分别发送给 V_i 和 R_j。

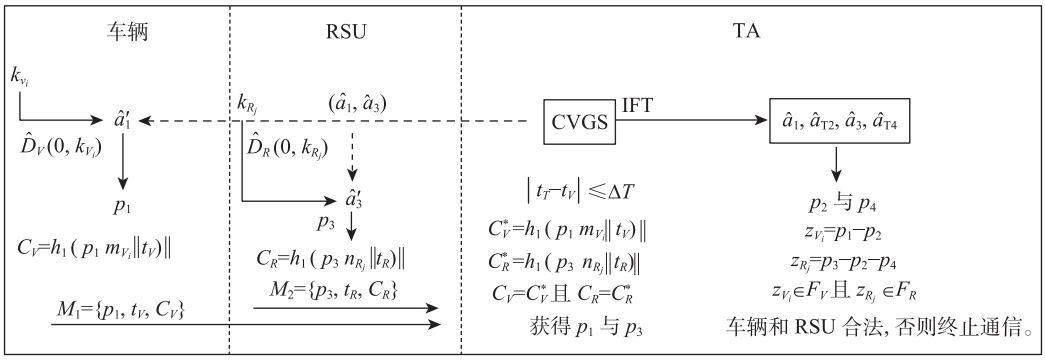


图2 身份认证过程

Fig. 2 Authentication process

步骤3：确认收到 $\hat{a}_1$，V_i 对模态 $\hat{a}_1$ 应用位移算子 $\hat{D}_{\mathrm{v}}\left(0,k_{V_i}\right)$，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

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

执行位移算子后，模态 $\hat{a}_1$ 的位置和动量变为 $\hat{x}_V=\mathrm{e}^{r}\hat{X}_{\mathrm{in}1}$ 和 $\hat{p}_V=\mathrm{e}^{-r}\hat{p}_{\mathrm{in}1}+\mathrm{e}^{r}\hat{X}_{\mathrm{in}2}+k_{V_i}$。$V_i$ 测量所持模态的动量，得到测量结果 p_1。随后，V_i 将测量结果 p_1 发送给TA。

V_i 计算测量结果 p_1 的MAC(消息认证码，记为 C_V)，得到 $C_V=h_1\left(p_1\middle\|m_{V_i}\middle\|t_V\right)$，其中 t_V 为当前时间戳。之后，V_i 将 $M_1=\{p_1,t_V,C_V\}$ 发送给TA。同理，收到 $\hat{a}_3$ 后，R_j 将位移算子 $\hat{D}_R\left(0,k_{R_j}\right)$ 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

$$\begin{cases}\hat{x}_R=e^{r}\hat{X}_{\mathrm{in}3}\\ \hat{p}_R=e^{-r}\hat{P}_{\mathrm{in}3}+e^{r}\hat{X}_{\mathrm{in}2}+e^{r}\hat{X}_{\mathrm{in}4}+k_{R_j}\end{cases}\tag{7}$$

然后，R_j 测量模态 $\hat{a}_R$ 的动量，得到 p_3。R_j 计算 p_3 的MAC值为 $C_R=h_1\left(p_3\middle\|n_{R_j}\middle\|t_R\right)$，其中 t_R 为当前时间戳。然后，R_j 将 $M_2=\{p_3,t_R,C_R\}$ 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 $|t_T-t_V|\leqslant\Delta T$ 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 $C_V^*=\mathrm{h}_1\left(p_1\middle\|m_{V_i}\middle\|t_V\right)$ 和 $C_R^*=\mathrm{h}_1\left(p_3\middle\|n_{R_j}\middle\|t_R\right)$。如果 $C_V^*=C_V$ 且 $C_R^*=C_R$，则消息来自可靠方且未被篡改。ΔT为系统允许的最大时间戳延迟阈值。

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 $z_{V_i}\in F_V$ 且 $z_{R_j}\in F_R$，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

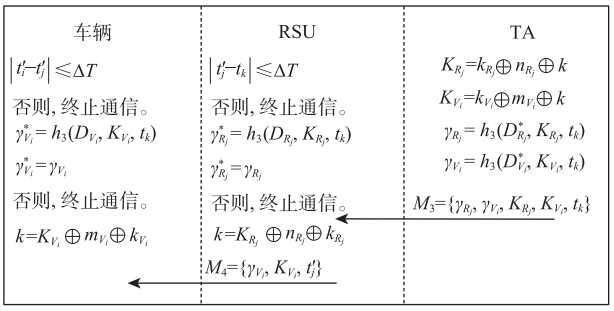


图3　密钥协商过程

Fig. 3　Key negotiation process

数协助 V_i 和 R_j 生成会话密钥，如图3所示，步骤如下。

1）TA生成确认信息（记为 A_{V_i}，A_{R_j}）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 $A_{V_i}=k_{V_i}\oplus m_{V_i}\oplus k$ 和 $A_{R_j}=k_{R_j}\oplus n_{R_j}\oplus k$。其次，TA计算验证消息完整性的 $\gamma_{R_j}=h_3\left(I_{R_j}^*,A_{R_j},t_k\right)$ 以及 $\gamma_{V_i}=h_3\left(I_{V_i}^*,A_{V_i},t_k\right)$，$t_k$ 为当前时间戳。最后，TA将验证消息 $M_3=\left\{\gamma_{V_i},\gamma_{R_j},A_{V_i},A_{R_j},t_k\right\}$ 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 $\left|t'_j-t_k\right|\leqslant\Delta T$ 是否成立。若成立，R_j 计算 $\gamma_{R_j}^*=h_3\left(I_{R_j},A_{R_j},t_k\right)$，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 $k=A_{R_j}\oplus m_{R_j}\oplus k_{R_j}$ 获取会话密钥。最后，R_j 将验证消息 $M_4=\left\{\gamma_{V_i},A_{V_i},t_k,t'_j\right\}$ 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 $\left|t'_i-t'_j\right|\leqslant\Delta T$ 是否成立。如果不成立，V_i 拒绝该信息。否则，V_i 计算 $\gamma_{V_i}^*=h_3\left(I_{V_i},A_{V_i},t_k\right)$ 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 $k=A_{V_i}\oplus n_{V_i}\oplus k_{V_i}$ 从而获取会话密钥 k。

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CVGS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。同时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 $\hat{D}_V\left(0,k_{V_i}\right)$ 和 $\hat{D}_R\left(0,k_{R_i}\right)$，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CVGS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实现无条件安全的身份验证。

在密钥协商阶段，方案使用512位哈希函数保障经典信息的传输。虽然Grover算法将哈希函数的暴力搜索复杂度从 $O(2^n)$ 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 $z_{V_i}\in F_V$ 且 $z_{R_j}\in F_R$，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 A_{R_j} 和 A_{V_i}。由于 $A_{V_i}=k_{V_i}\oplus m_{V_i}\oplus k$，$A_{R_j}=k_{R_j}\oplus n_{R_j}\oplus k$，$V_i$ 和 R_j 可以分别通过计算 $k=A_{V_i}\oplus n_{V_i}\oplus k_{V_i}$ 和 $k=A_{R_j}\oplus m_{R_j}\oplus k_{R_j}$ 来获得协商的会话密钥 k。

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。如果消息时延在可接受范围内，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，接收方将视其为过期信息。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2个量子信道和4个经典信道。认证阶段，经典测量结果的传输采用基于哈希的消息认证码（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与秘密信息无关，因此在经典信道中的拦截–发送攻击不会构成威胁。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 E 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 $\hat{x}_E=e^r\hat{X}_{\text{in1}}+e_1$ 和 $\hat{p}_E=e^{-r}\hat{P}_{\text{in1}}+e^r\hat{X}_{\text{in1}}+e_2$。然后，攻击者将测量结果 p_E 发送给TA。在步骤4中，TA测量所持模态后，计算校验变量 $z_E=p_E-p_2-e_2$。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。e_1,e_2 为攻击者执行位移算子时使用的任意位移参数。

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、RSU以及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）。总结如下。

1）密钥保密性：协议确保了车辆与RSU的密钥 k_{V_i} 和 k_{R_j} 不会被攻击者获取。query attacker查询结果均为not attacker，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，会话密钥查询结果也被满足，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进行了查询，结果返回未泄露，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[16-18]和经典密码学方案[7-8,20]进行比较分析。

3.3.1 与量子密码学方案比较

所提方案与文献[16-18]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。文献[16-18]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，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[16-17]。此外，在整个验证阶段，文献[16-17]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

Tab.1 Comparison with quantum cryptography schemes

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

3.3.2 与经典密码学方案的比较

所提方案与文献[7-8,20]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比特。椭圆曲线加密算法中，p 和 q 的长度均为20字节，椭圆曲线群 G 中元素长度为40字节。根据最新研究，量子态的生成与测量通常处于皮秒至微秒量级，其中连续变量图态纠缠态的平均制备时间一般不超过500 ns[21]。相较于经典密码算法（如SHA-512）的单轮哈希处理，量子操作在时间维度上并不构成显著瓶颈，因此其计算开销可在整体性能分析中予以忽略。

基于JPBC（Java Pairing-Based Cryptography）库和Paillier公钥加密（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 $T_{\text{sm}}=0.251$，拉格朗日插值运算 $T_{\text{li}}=0.004$，伪随机函数运算 $T_{\text{prf}}=0.007$，对称加密算法加密/解密 $T_{\text{e/d}}=0.026$，物理不可克隆函数 $T_{\text{puf}}=0.1$，单向哈希运算（SHA-256）$T_{\text{h}}=0.001$，单向哈希运算（SHA-512）$T_{\text{h}}^{*}=0.002$。

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4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）和文献[20]（0.82）。相比之下，所提方案的总计算开销分别减少了约26.05%、77.27%和51.22%。

2）通信开销。在所提方案中，认证阶段和密钥协商阶段共涉及4条消息的传输。在认证阶段，车辆和RSU将测量结果发送给TA，即 $M_1=\{p_1,t_V,C_V\}$ 和 $M_2=\{p_3,t_R,C_R\}$。在密钥协商阶段，TA发送

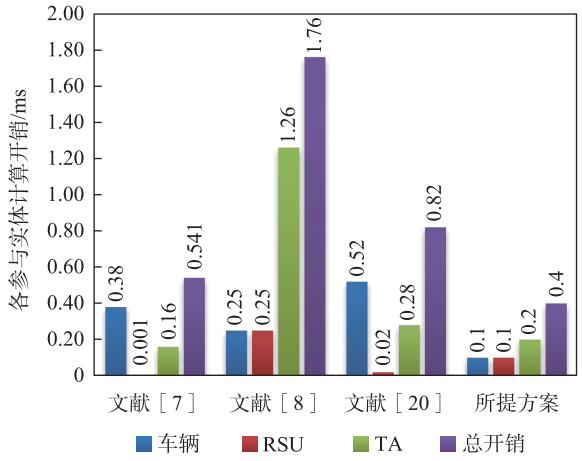


图4　计算开销对比

Fig. 4　Computation overhead comparison

$M_3=\{\gamma_{R_j},\gamma_{V_i},C_{R_j},C_{V_i},t_k\}$ 给RSU，RSU发送 $M_4=\{\gamma_{V_i},A_{V_i},t_k,t'_j\}$ 给车辆。因此，所提方案的总通信开销为：$10|Z_q^*|+4|T|$，即216字节。

图5展示了各对比方案中不同实体所消耗的通信开销。与文献[7-8,20]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%。

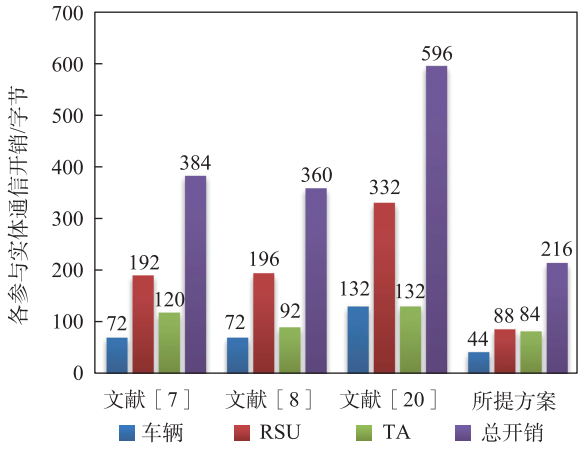


图5　通信开销对比

Fig. 5　Communication overhead comparison

4　结 论

本文将经典密码学与连续变量量子图态相结合，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高效的身份认证，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，从而提升了系统的安全性与鲁棒性。

3）性能分析显示，与现有量子密码学方案相比，该方案所需量子态数量较少，易于实际部署；与代表性传统密码学方案相比，其计算开销和通信开销分别最高降低了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 Junhui, Hu Huanhuan, Huang Fanwei, et al. Authentication technology in Internet of Things and privacy security issues in typical application scenarios[J]. Electronics, 2023, 12(8): 1812.

[3] Liao Longxia, Zhao Junhui, Hu Huanhuan, 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，等. 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, et al. 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，等. 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, et al. 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 Xiong, Ayub M F, et al. An efficient and physically secure privacy-preserving key-agreement pro-

tocol for vehicular ad-hoc network[J]. IEEE Transactions on Intelligent Transportation Systems, 2023, 24(9): 9940-9951.

[8] Awais S M, Wu Yucheng, 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, 25(12): 21107-21116.

[9] Liang Yangfan, Luo Entao, Liu Yining. 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 Qi, Zhang Ning, Ni Jianbing, 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 University, 2024, 41(1): 70-77.

[13] Cooper D A, Apon D C, Dang Q H, et al. Recommendation for stateful hash based signature schemes[R]. Gaithersburg: National Institute of Standards and Technology, 2020.

[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 Hailin, Chronopoulos A T, Zhang Zhongshan. An efficient security scheme for vehicular communication using a quantum secret sharing method[J]. IEEE Transactions on Vehicular Technology, 2020, 69(1): 1101-1105.

[16] Chen Zhiya, Zhou Kunlin, Liao Qin. Quantum identity authentication scheme of vehicular ad-hoc networks[J]. International Journal of Theoretical Physics, 2019, 58(1): 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(1): 4280617.

[18] Shi Qin, Yang Ze, Cheng Teng, et al. QKBAKA: a quantum-key-based authentication and key agreement scheme for Internet of vehicles[J]. IEEE Internet of Things Journal, 2024, 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), March 5-9, 2023, San Diego, CA, USA. New York: IEEE, 2023: 1-3.

[20] Wei Lu, Cui Jie, Zhong Hong, 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, 2023, 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，博士研究生，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。E-mail：junhuizhao@hotmail.com。

（责任编辑：姜红贵）