面向6G车联网的自适应抗量子密码学：基于上下文感知的优化

Poushali Sengupta Mayank Raikwar Sabita Maharjan Frank Eliassen Yan Zhang 奥斯陆大学 奥斯陆大学 奥斯陆大学 奥斯陆大学 奥斯陆大学 poushals@ifi.uio.no mayankr@ifi.uio.no sabita@ifi.uio.no frank@ifi.uio.no yanzhang@ifi.uio.no

arXiv:2602.01342v1 [cs.CR] 1 Feb 2026

摘要—**未来强大的量子计算机或许能够破解车辆与其他设备之间通信所采用的安全机制（车联万物，简称 V2X）。称为后量子密码学的新型安全方法有助于保护这些系统，但通常需要更多计算能力，还可能拖慢通信速度，这对高速 6G车联网构成了挑战。本文提出一种自适应后量子密码学（PQC）框架，该框架可预测短期移动性和信道变化，并利用预测型多目标进化算法（APMOEA）动态选择适当的基于格、基于编码或基于哈希的后量子密码配置，以满足车联网时延和安全约束。然而，在动态车载环境中频繁进行密码配置重构，会在算法切换期间引入新的攻击面。安全的单调升级协议可防止切换期间发生降级、重放和失步攻击。理论结果表明，在预测误差有界时决策具有稳定性，在移动性漂移下时延有界，并且在预测噪声较小时能够保证正确性。这些结果展现了未来 6G车联网实现抗量子密码学的一条可行路径。通过基于真实移动性数据（LuST）、天气数据（ERA5）和 NR-V2X 信道轨迹开展的大量实验，我们表明，该框架最多可将端到端时延降低 27%，将通信开销降低 65%，并利用强化学习有效稳定密码切换行为。此外，在所评估的对抗场景中，单调升级协议成功防止了降级、重放和失步攻击。**

I. 引言

随着大规模量子计算机日益普及，它们对现代车辆通信系统的安全性构成了严重威胁。目前，车与万物（V2X）通信的安全措施大多依赖椭圆曲线和基于 RSA 的公钥基础设施等技术。遗憾的是，这些方法难以有效抵御诸如 Shor算法 [1] 之类的攻击。对于未来 6G车联网中的关键应用，安全与可靠性至关重要，因此必须转向抗量子安全。

标准化的后量子密码算法包括基于格的方案（例如 Kyber 和 Dilithium） [2]–[4], 基于编码的方案（例如 Classic McEliece） [5], [6], 以及基于哈希的签名（例如, SPHINCS+) [7]。尽管后量子密码算法潜力巨大，但在车联网系统中直接部署后量子密码仍面临挑战。许多后量子密码算法需要更大的密钥、更多的处理能力和更长的计算时间，导致通信时延增加 [8], [9],，这可能会妨碍碰撞规避和协作式车辆通信等实时需求。此外，传统的后量子密码实施模型往往忽视车联网情境 [10], [11]的动态特性。车辆面临不断变化的条件，包括移动性变化、天气对通信质量的影响，以及计算资源的波动。根据这些条件，需求可能从紧急安全通知到常规数据传输不等。静态的后量子密码配置无法同时满足所有车联网运行条件：过于保守的选择会造成不必要的时延，而轻量级配置在严峻或对抗性场景下可能无法提供充分的安全性。车联网链路具有较大的多普勒扩展、频繁的波束失准和快速的信道变化 [12], [13],，导致不同后量子密码类别之间的瞬时成本差异。基于编码的方案因其鲁棒性，在深衰落期间表现出色 [14],；而基于格的方案在中等信噪比、低延迟场景下性能更佳 [15], [16]。由于这些波动发生在 100 毫秒以内 [17], ，静态分配后量子密码可能造成时延或安全性开销，这凸显了对预测性、上下文感知密码层的需求，以优化后量子密码选择并满足超可靠低时延通信合规性 [18]。

为解决这些问题，我们提出了一种专为 6G车联网设计的上下文感知自适应后量子密码框架（CAAP）。与传统的固定式后量子密码部署不同，CAAP 利用实时感知和预测分析，根据当前状况动态选择最佳密码算法。该框架由四个主要组件构成：(1) 上下文感知管道，用于收集车辆速度、通信质量、天气状况和消息紧急程度，并将其整合为统一的上下文向量；(2) 短期预测器，用于预测未来 100–200ms 时间窗口内的上下文变化；(3) 自适应预测多目标进化算法（*APMOEA*），通过在基于格、基于编码或基于哈希的签名之间进行选择，权衡时延、计算成本、通信开销和抗量子能力；(4) 安全转换协议，通过经认证的版本单调协商，防范降级、重放和上下文操纵攻击，其遵循与 TLS 1.3 和 QUIC [19], [20] 类似的原则。

下一代网络安全与隐私研讨会（FutureG） 2026年 2026年2月 23日，美国加利福尼亚州圣迭戈 ISBN 979-8-9919276-9-7
https://dx.doi.org/10.14722/futureg.2026.23xxx
www.ndss-symposium.org

APMOEA 的核心是利用强化学习持续进行自适应，在最大限度保障安全性的同时，降低处理和通信延迟。通过从实时性能和历史性能中学习，该算法能够在多样化的车载环境中有效地制定后量子密码决策。我们对这一自适应层进行了严格分析，推导出上下文感知决策的稳定性条件、移动性漂移下的有界时延，以及预测误差较小时后量子密码选择的正确性。通过在现实条件下进行广泛测试，包括 LuST 移动性轨迹、ERA5 天气数据、符合 3GPP 标准的 NR-V2X 信道模型以及汽车计算模型，我们的自适应框架实现了时延降低 27%、完全抵抗降级攻击，并且相较于 NSGA-II 和仅强化学习基线方案具有更强的鲁棒性。本文的主要贡献如下:

- **面向车载约束的后量子密码选择自适应规划。我们提出 APMOEA，这是一种预测型多**目标规划机制，可在严格的超可靠低时延通信时延、计算、通信和安全约束下，动态选择后量子密码配置方案、计算、通信和安全约束。
- **通过单调PQC转换实现安全执行**。 我们设计了一种轻量级的认证转换协议，可在重新配置期间强制执行单调PQC升级，并防止降级、重放和失步攻击。
- **稳定性与有界时延的形式化保证**。我们提供理论分析，证明在预测误差有界时决策稳定性得以保持，相对于预言机选择器的正确性得以保证，并且在现实的车载移动性和信道漂移条件下，端到端时延有界。
- **基于真实车联网轨迹的主张驱动评估。我们**使用 LuST 移动性、ERA5 天气数据、NR-V2X 信道模型和汽车级计算配置开展实验，结果表明时延最高可降低 27%，并且在对抗性上下文操纵下表现稳健。

我们强调，本研究并未引入新的密码学原语。相反，本研究主要针对在严格的车载超可靠低时延通信（*URLLC*）约束下，自适应选择并安全转换后量子密码（*PQC*）机制的问题。尽管系统设计上兼容新兴的面向6G的V2X环境，但核心贡献在于上下文感知密码自适应，而非对未来6G网络进行详细的物理层建模。多目标优化和强化学习被用作实现这一自适应安全目标的使能机制，以确保其高效且稳定。由于完整标准化的6G车载通信协议栈尚不可用，我们采用面向*6G*的视角。具体而言，我们对体现预期6G特征的车载通信进行建模，例如超可靠低时延通信、高移动性和密集连接，同时保持与现有 NR-V2X抽象的兼容性。

PQC部署范围：CAAP在应用层采用后量子密码学，保护通过已建立的5G连接传输的V2V数据通信。PQC方案对车辆之间交换的安全关键消息和协同感知消息进行加密和认证。这与5G-AKA和EAP-TLS提供的网络层安全性有所不同，但又相辅相成；后两者负责车辆与5G网络基础设施之间的初始认证和安全连接建立。

II. 背景、相关工作与威胁模型

本节介绍背景、既有研究以及对手假设，这些内容说明了为何车联网系统需要采用自适应后量子密码学。

A. 背景与相关工作

基于 5G 及 6G 之后的技术开发的新一代车载网络服务，需要超可靠低时延通信（URLLC），时延要求为 5 至 20 毫秒，同时还要具备高可靠性，并能在快速变化的移动性和信道条件下有效运行 [21], [22]。基于椭圆曲线密码学（ECC）和 RSA 的传统安全方法容易受到量子计算威胁，因此，采用后量子密码对于未来的实现至关重要 [23]，[24]。然而，在当今的经典车载硬件上部署时，与传统公钥密码学相比，后量子密码方案通常会带来更大的密钥长度、更高的验证成本和更多的计算开销；这些因素都可能随信噪比、分组差错率（PER）、CPU负载及移动性变化而显著波动 [13], [15], [25]。因此，在严格的运行条件下，静态 PQC 配置往往会违反 URLLC 时延限制；而在低风险场景下，则会引入本可避免的计算和通信开销。

目前针对车联网系统中后量子密码的研究提案，大多是在固定条件下评估 Kyber、Dilithium 和 McEliece 等算法 [16], [26]。这些评估未考虑车辆快速移动、3GPP 所描述的衰落过程，或可用计算资源的变化。其他基准测试研究 [25], [27]进一步表明，没有任何一种后量子密码方法能在所有运行场景中胜过其他方法。这凸显了开发能够基于预测和上下文感知进行自适应的后量子密码层的必要性。尽管面向物联网和嵌入式系统 [28], [29]的自适应、资源感知型密码策略会根据负载或能源可用性调整经典密钥强度，但这些方法既无法应对后量子密码参数的大幅变化，也无法防范后量子密码迁移期间可能发生的降级、回滚或上下文强制攻击。TLS 1.3 和 QUIC 等协议 [30], [31] 提供了抵御降级攻击的机制，但它们假定客户端-服务器环境稳定，这与车联网场景中的动态条件不同，后者涉及不可预测的时延。关于检测降级 [19] 和协商 QUIC 版本 [32] 的既有研究指出了在恶意网络环境中防止回滚所面临的挑战，但尚未整合实时上下文感知自适应。据我们所知，CAAP 首次将具备降级防护能力的后量子密码迁移与强化学习引导的预测型优化器相结合，专门

针对 6G 车联网运行需求量身设计。本研究并未提出新的后量子密码原语，而是着重于根据快速变化的车联网情境，自适应地编排标准化后量子密码机制（例如 Kyber、Dilithium、SPHINCS+）。

B. 威胁模型

我们考虑一个能够访问 V2X 无线通信的强大对手，它可以注入、重放、延迟或修改数据包 [30], [31]。攻击者可能伪造信噪比或分组错误率等上下文特征，以影响后量子密码选择 [29], , 重放过时的版本计数器以触发降级攻击 [32],, 或操纵消息传递以引发同步故障 [19]。对手的目标包括削弱后量子密码强度、增加时延、破坏迁移稳定性，或诱使系统采用速度较慢或安全性较低的配置。实际上，后量子安全依赖于协调配合的密码机制，而非单一原语。因此，每个候选动作都代表一个后量子密码配置档案，包含 (i) 用于会话密钥建立的密钥封装机制 (KEM)，以及 (ii) 用于认证和完整性保护的数字签名方案。例如，配置可以将用于密钥交换的 Kyber 与用于认证的 Dilithium 或 SPHINCS+ 结合使用。我们假设采用标准化的 NIST 推荐后量子密码原语，且不修改底层密码算法。此外，对手可能降低信道质量 [13]。车辆和路侧单元 (RSU)。5G NR-V2X 或未来的 6G架构并不要求部署 RSU。我们的框架完全支持直接车车通信，并将 RSU 视为可选的边缘基础设施，在可用时可降低时延。假设车辆和路侧单元具备可信硬件，用于安全存储长期密钥并维护可靠的版本计数器 [33], , 且后量子密码实现不存在侧信道泄漏。车载传感器数据（例如速度和环境信号）被视为可信数据，而网络可观测指标则可能遭到操纵。CAAP 强制执行 (i) 机密性，(ii) 消息完整性和真实性，(iii) 单调、不可逆的后量子密码升级，以及 (iv) 通信端点之间一致的后量子密码迁移。

我们针对车联网安全中的强大对手模型展开研究，该模型包括具备量子能力的攻击者、主动网络对手、上下文操纵攻击者以及降级攻击者。尽管 CAAP 依赖受信任的车辆硬件，但其运行于不受信任的通信介质之上，即使面对这些威胁，也能确保抗量子机密性、完整性和可靠升级。本工作的主要目标是通过减少时延来增强 PQC方案。然而，理解安全威胁至关重要，原因有二。首先，自适应密码系统可能成为攻击者的目标，攻击者或许会操纵其环境，迫使系统使用更弱的算法。其次，在密码方法之间切换是一个关键过程；如果攻击者破坏这一过程，就可能同时危及安全性和性能。因此，必须针对潜在攻击评估优化引擎和安全转换协议，以确保低时延PQC框架在6G车联网环境中的可靠性。

表 I: 系统假设与对手能力。

类别	描述
假设	• 可信硬件信任根（安全密钥存储、单调计数器）、经认证的启动，以及正确的PQC实现。车辆器件）、经过身份验证的启动以及正确的PQC实现。车辆且路侧单元未遭到攻陷。 •无线信道不可信，且实际上由对手控制。 • 用于生成上下文（速度、信噪比、移动性）的《传感器》存在噪声，但并未遭到恶意攻陷。
对手能力	• 具备量子能力的攻击者，能够破解经典密码系统（椭圆曲线数字签名算法/ECDH/RSA）。允许先收集后解密。 • 主动网络攻击者，能够注入、修改、重放、干扰或丢弃车联网消息。 • 上下文操纵攻击者，诱使人为信道退化或丢包，以影响后量子密码选择。 • 操纵转换消息以强制使用较弱的后量子密码。

III. 上下文感知自适应后量子密码（CAAP）框架

我们提出了 CAAP，该系统根据车辆当前所处的情况调整所使用的 PQC方案类型。该系统由四个相互协作的组件组成：(i) **上下文提取**，用于提取移动性、信道和工作负载指标；(ii) 使用轻量级预测对上下文演变进行**短期预测**；(iii) **APMOEA**，用于选择最优的后量子密码算法；以及 (iv) **安全转换协议**，用于强制执行经过身份验证的单调版本升级。上下文每 20–50ms 更新一次，预测时间跨度为 100–200 ms，并且 PQC转换可在一次车联网往返通信内完成。车辆会主动监测一系列影响密码处理过程成本和速度的因素。这些因素包括移动性特征（如速度和连接时长）、信道条件（如 SNR 和分组错误率）、环境因素（包括天气和能见度）、计算负载（指中央处理器和图形处理器资源），以及消息紧急程度（区分关键安全通信和紧迫性较低的消息）。这些不同的输入经过标准化处理后，发送至下一个模块进行处理。为防止快速变化导致密码方法发生不稳定的切换，我们采用短期预测建模。该过程使用简单的滤波器和回归模型来预测接下来可能发生的情况（例如预期时延、SNR 和处理能力）。这种预测既能为决策提供稳定的数据，又能保持较低的计算需求。决策引擎确定每次通信会话期间应使用的最佳后量子密码算法。候选算法包括：**1. 基于格的方案**（如 Kyber 和 Dilithium），兼顾速度与强大**2. 基于编码的方案**（如 Classic McEliece），适合在通信条件较差时使用，以及**3. 基于哈希的签名**（例如 SPHINCS+），其轻量且无需维护状态。每种算法都会根据多维成本向量进行评估，从而做出有依据的选择，以满足具体情境的需求，具体如下：

$$C_{\text{alg}} = (T_{\text{enc}},\ T_{\text{dec}},\ S_{\text{key}},\ S_{\text{ct}},\ E_{\text{comp}},\ S_{\text{sig}}), \tag{1}$$

分别表示加密和解密时间、密钥长度、密文大小、计算能耗和签名长度。这些向量是第四节所述优化过程的输入。

关于评估范围的说明：在本研究中，我们分别评估加密/密钥封装方案（Kyber、Classic McEliece）和数字签名方案（Dilithium、SPHINCS+），以评估它们在车对车网络约束下的实际可行性和稳健性。我们承认，实际部署需要两种机制协同工作——加密用于防范窃听，签名用于防止主动中间人攻击。虽然目前我们的自适应选择针对单个原语进行，但该框架旨在支持混合配置。

A. 与*MAPE-K* 自适应循环的关系

所提出的后量子密码升级机制并不修改现有密码标准；它在协议编排层面运行，使用标准化的、NIST推荐的PQC算法，并遵循与TLS 1.3和QUIC类似的降级保护原则。对应用吞吐量的影响通过超可靠低时延通信约束下的通信开销和端到端时延间接体现。尽管在车联网场景中进行了评估，该框架并非固有地特定于某一领域，也可扩展到其他时延敏感系统。

CAAP遵循经典的基于知识的监控-分析-规划-执行（*MAPE-K*）控制回路，该回路广泛应用于自适应和自治系统 [34]。图1展示了按照MAPE-K控制回路组织的CAAP，将其用作一种组织抽象以提高可解释性。分布式**知识库（K）**包含离线后量子密码成本概况、强化学习反馈以及协议状态（例如版本计数器和上下文哈希），以支持稳健的自适应。本研究并不提出新的自适应架构；相反，它贡献了一种具有稳定性保证的后量子密码选择预测性多目标规划公式，以及一种可防止降级和失步的安全单调执行协议——这些能力是通用自适应框架所不具备的。

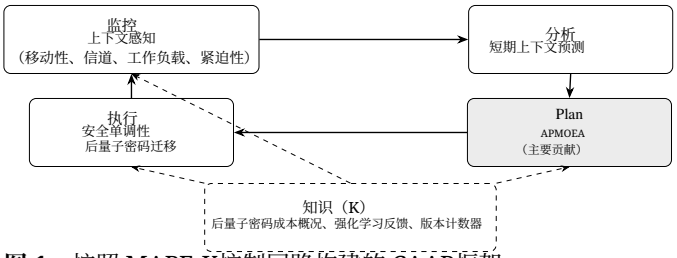


图 1：按照 MAPE-K控制回路构建的 CAAP框架。

*B. V2X*系统模型与车辆动力学

向量 C_{alg} 描述了特定PQC配置档案固有且与上下文无关的成本特征，这些特征通过离线基准测试获得。在运行时，这些算法层面的属性会映射为与上下文相关的目标，以反映车载通信条件、系统负载和消息紧迫性。因此，优化引擎基于派生的多目标函数运行，而非直接基于C_{alg}。我们考虑一种车载通信环境

该环境基于NR-V2X抽象，并在超可靠低时延通信（URLLC）约束下运行。在高移动性和信道条件快速变化的情况下，车辆与路侧单元（RSU）及相邻车辆交换周期性消息和事件驱动消息。车载移动性由随时间变化的速度 $v(t)$和加速度 $a(t)$表征，两者共同影响多普勒扩展和信道相干时间。为在不进行显式物理层建模的情况下捕捉短期链路稳定性，我们引入连通时限 τ_c，表示通信链路在发生显著拓扑或信道变化前预计能够保持可靠的时长。令 $\mathcal{A} = \{a_1, a_2, \ldots, a_n\}$表示系统可用的候选密码动作集合。每个动作 $a \in \mathcal{A}$ 对应一个有效的PQC配置档案，而非单个密码原语。消息分为若干紧急类别$\mathcal{M}$={：安全消息、控制消息和遥测消息}。安全消息对时延极为敏感，必须满足严格的时延限制，而控制消息和遥测消息能够容忍更高的密码开销。每类消息都关联一个紧急度权重 $u \in \{u_s, u_c, u_t\}$，该权重会影响后量子密码选择决策。

C. 上下文模型与符号说明

转换协议依赖于来自车辆周围环境、无线连接和设备处理状态的实时信息。我们使用如下定义的上下文向量来表示这些信息：

$$X_t = (\text{SNR}, \text{PER}, v_s, v_a, \tau_c, u, \text{CPU}_{\text{load}}, \ldots). \tag{2}$$

连通时限 τ_c 和紧急度权重 u 使优化器能够考虑车载移动性和安全关键消息语义，而无需进行详细的物理层仿真。此上下文向量包含信号强度（信噪比）、分组差错率（分组错误率）、车辆速度（v_s）、加速度（v_a）、能见度条件、环境温度（T_{amb}）、当前 CPU负载以及消息的紧急程度等关键因素。这些要素全面展现了车辆的物理运动、无线连接质量、环境条件、处理能力以及待传输消息的重要性。此外，APMOEA 优化器中的所有代价函数相对于这些特征均为利普希茨连续。这意味着即使上下文发生微小变化，系统仍会保持一致且可预测的行为。每种 PQC配置档案都会产生不同的计算、通信和时延开销，这些开销在车载超可靠低时延通信场景中尤为关键。例如，基于哈希的签名方案能够提供强大的安全保障，但代价是签名长度增加；而基于格的方案时延较低，但依赖不同的计算假设。所提出的自适应框架根据实时车载上下文、消息紧急程度和资源可用性，在这些配置档案中进行选择。

D. 安全*PQC*迁移协议

在不同的PQC配置之间切换时，迁移过程中可能会产生额外的安全风险。

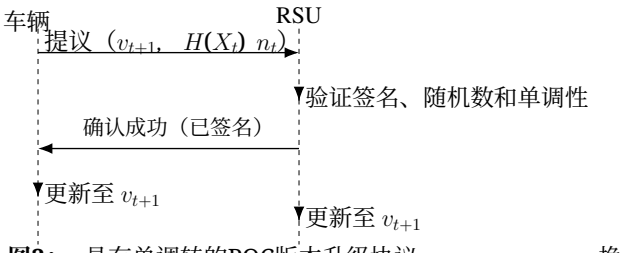


图2： 具有单调转的PQC版本升级协议 换。

为降低这些风险，我们实施了一种安全协商协议，其关键特性如下：通过经过身份验证的信令消息验证消息来源；采用单调版本控制，防止回滚到安全性较低的配置；通过原子转换确保更新一致地进行；使用唯一标识符提供重放保护；并借助决策一致性机制，确保通信双方对选定的PQC配置达成一致。这些措施共同防范过渡阶段攻击，并保障安全通信。如图2所示，安全PQC迁移协议协调车辆与路侧单元之间的平滑版本升级和安全协商。该过程包括收集实时数据、预测短期状况、运行优化算法以确定最佳加密选项、选择最优后量子密码算法、安全协商新参数，以及持续监控情况。这一自适应框架在提供抗量子安全性的同时，仍能满足延迟要求和资源约束；这些都是6G-V2X网络的关键特性。

IV. APMOEA优化算法

APMOEA作为核心决策引擎，在动态车联网情境下，依据时延、计算与安全性约束进行自适应PQC配置选择。为在快速变化的条件下提高决策稳定性并加速收敛，强化学习（RL）反馈被作为内部机制集成到优化循环中。对于每个候选PQC配置档案 $a \in \mathcal{A}$，我们定义一个多目标代价向量：

$$f(a) = (T_{\text{lat}}(a),\ C_{\text{comp}}(a),\ S_{\text{comm}}(a),\ \sigma_{\text{sec}}(a)), \tag{3}$$

其中， $T_{\text{lat}}(a)$ 是端到端签名/验证延迟，$C_{\text{comp}}(a)$ 是计算成本（CPU 周期）， $S_{\text{comm}}(a)$ 捕捉密钥和载荷大小开销，$\sigma_{\text{sec}}(a)$ 则表示密码强度（比特安全性）。形式上，目标向量 $f(a)$ 是根据当前状态 X_t 对 C_{alg} 进行上下文感知变换后计算得出的。APMOEA 旨在实时约束下寻找帕累托最优解集。第三节中的预测上下文变量（例如信道质量、处理能力可用性）被纳入作为动态权重。优化器遵循一系列核心步骤：首先，根据上下文特征初始化一个 PQC 配置种群。然后，运用变异和交叉技术探索设计空间并生成候选配置。接着，使用传统的上下文加权适应度（效用）函数形式对这些候选配置进行排序，适应度(a) $=$ $w_1 T_{\text{lat}} + w_2 C_{\text{comp}} + w_3 S_{\text{comm}} - w_4 \sigma_{\text{sec}}$，该函数综合了多种因素例如时延、计算成本、通信成本和安全性。最后，强化学习智能体会监控所选算法的性能，并调整变异率和权重参数，以提高稳定性并尽量减少 PQC 算法选择的波动。考虑一个旨在提升道路安全和效率、负责管理车联网通信的智能交通系统。在此场景中，一支自动驾驶车辆车队持续相互通信，并与交通基础设施通信，以便实时做出决策。

1) 状态向量初始化：每辆车辆收集构成状态向量 s_t的数据。例如，车辆的状态可能包括 T_{lat}， C_{comp}，信噪比，移动性，CPU 负载

2) 决策与奖励系统：车辆运行时会持续评估自身所处的上下文。例如，高时延（T_{lat} ）会对运行产生负面影响，导致奖励分数降低（ R_t），尤其是在频繁切换通信信道时（ N_{switch}）。相反，时延较低且信噪比较高的稳定连接会带来更高的奖励。此外，密码安全性较高的车辆也会获得额外奖励（σ_{sec}）。

3) 调整策略：车辆会根据观察到的奖励调整其通信行为；当时延增加时，它可能会调整传输参数，或选择其他后量子密码配置方案以提升性能。

4) 持续学习过程：车辆会持续适应各种道路状况、交通状况和环境变化，并根据反馈不断完善策略，以便在交通拥堵或天气恶劣时仍保持高效。

我们采用如下奖励函数，以最小化时延、惩罚过于频繁的切换和较差的信噪比状况，并鼓励选择安全性更高的后量子密码配置：

$$R_t = -T_{\text{lat}} - \alpha \cdot N_{\text{switch}} + \beta \cdot \text{SNR} + \gamma \cdot \sigma_{\text{sec}}. \tag{4}$$

我们采用表格型 Q 学习方法，以避免基于神经网络的强化学习所带来的计算开销。APMOEA 通过根据预测条件调整动态权重、利用强化学习反馈惩罚振荡性决策，并在稳定的适应度模式逐渐显现时逐步减少探索，从而收敛到稳定解。这些特性使算法能够在车载环境快速变化的情况下，持续生成后量子密码建议。算法 1 对自适应优化过程进行了形式化描述。APMOEA 纳入短期上下文预测，在适应度评估前动态调整时延、计算、通信和安全目标的相对权重。在每一代中，算法都会评估固定规模的候选PQC配置文件种群，从而确保计算成本有界且可预测。对于四种后量子密码类别且种群规模小于 40 的情况，该优化算法在汽车级 CPU 上的运行时间不到 1 毫秒，可在车载环境中实现实时密码算法选择。

在 APMOEA 中，种群由候选后量子密码配置档案组成。每个档案指定一种标准化PQC原语（例如 Kyber、Dilithium、McEliece 或 SPHINCS+）

算法 1 自适应预测多目标进化算法

输入： 当前上下文 X_t，预测上下文 X_{t+1}，后量子密码算法集合 $\mathcal{A}$**输出：** 为当前上下文选定的后量子密码算法 a_t 1：通过从 $\mathcal{A}$ 中抽取候选算法，初始化种群 P_0 2：**对于** $t = 1$ 到 T **执行**
3 a $a \in P_t$ ：为每个候选项计
4 算多目标代价向量 **f( )**：根据预测上下文 $\hat{}$ X_{t+1} 更新动态权重 w_i 5：使用加权代价计算所有候选项的适应度分数6：通过锦标赛选择（对随机抽取的候选项进行两两比较）选出父代候选项7：通过交叉和变异生成子代8：强化学习智能体调整变异率和权重参数，以降低不稳定性9：由父代和子代构成下一代种群 P_{t+1} 10：**结束循环**11：确定帕累托最优候选（不被任何其他候选项支配），并将其作为a_t输出**注意：** 锦标赛选择是指随机抽取一小部分候选项，并从中选出适应度最高者作为父代。帕累托最优解是指不存在其他算法能在所有目标上同时表现更好的候选项。

同时还包含一个权重向量，用于体现时延、计算成本、通信开销和安全性的重要性差异。优化过程中，进化算子会作用于这些配置。交叉操作将表现良好的配置中的权重向量组合起来，形成新的权衡方案；变异操作则引入小幅随机变化，以进一步探索相近的偏好。这些操作不会生成新的密码方案，而是生成新的偏好配置，用于引导从现有后量子密码原语中进行选择。这使优化器能够随着车载条件的变化，自适应地选择最合适的PQC配置，同时保持底层密码算法的正确性和完整性。

算法2 安全PQC迁移协议

输入： 当前版本 v_t，提议版本 v_{t+1}，上下文哈希 $H(X_t)$
输出： 各方更新至版本 v_{t+1}
1：发送方构造转换消息：

$$M = (v_{t+1},\ H(X_t),\ \text{随机数})$$

2：发送方使用当前方案对 M 签名 v_t
3：接收方验证签名并检查：
- $v_{t+1} \geq v_t$ (单调性检查)
- $H(X_t)$ 与其本地上下文哈希匹配
- 随机数此前未被使用

4: **如果**任何检查失败**则**
5: 拒绝转换并恢复至 v_t
6: **否则**
7: 接收方通过签名确认予以确认
8: 双方更新至版本 v_{t+1}
9: **结束条件判断**

安全PQC迁移协议使车辆和路侧单元（RSU）能够安全升级到新的后量子密码配置，而不会面临降级、重放或失步攻击的风险。在每次更新时，发送方会提出一个新的后量子密码版本，并附上上下文哈希和新的随机数，然后使用当前启用的后量子密码方案对该消息进行签名。接收方会验证所提议的版本不低于当前版本、上下文哈希与本地视图相符，且随机数是新的。如果任何一项检查未通过，则拒绝此次迁移，双方继续使用现有配置；否则，双方交换签名确认，并同时切换到新版本。

V. 理论保证

本节分析 CAAP 的稳定性、鲁棒性和安全性。我们展示了 APMOEA 在动态车载条件下能够持续选择适当的后量子密码配置方案，而安全转换协议则增强了重新配置过程中的密码学保证。观察到的端到端时延增加仍有界，并处于与车辆动力学相关的超可靠低时延通信预算范围内，包括信道相干时间和移动性引起的变化。此外，只要短期移动性和信道预测误差保持在适中范围内，优化器就能维持稳健的选择行为。令 X_t 表示时刻的上下文ˆ特征向量 t，并令 X_{t+1} 为其预测值。APMOEA 通过以下方式选择后量子密码算法： $a_t = \arg\min_{a \in \mathcal{A}} L_t(a)$，其中加权代价为： $L_t(a)$ =

$$w_1\, T_{\text{lat}}(a, X_t) + w_2\, C_{\text{comp}}(a, X_t) + w_3\, S_{\text{comm}}(a) - w_4\, \sigma_{\text{sec}}(a). \quad (5)$$

我们假设：**(A1)** 所有成本项关于上下文X_t均为 L-利普希茨；**(A2)** 移动性和信道漂移满足 $\|X_{t+1} - X_t\| \leq \delta$；ˆ **(A3)** 预测误差满足 $\|X_{t+1} - \hat{X}_{t+1}\| \leq \varepsilon$；**(A4)** PQC 候选项之间的最小损失间隔为 $\Delta_{\min} > 0$。令$\Delta_{\min}$ 为任意两个后量子密码算法之间的最小损失间隔。**定理的证明见附录**。

定理 V.1 (决策稳定性)。若 $K\varepsilon < \Delta_{\min}$，则在上下文稳定区间内，对所有 t，*APMOEA* 均选择相同的算法 a_t 。此处，K 表示损失函数的利普希茨常数，ε 表示上下文预测误差，$\Delta_{\min}$表示任意两个后量子密码算法之间的最小损失间隔。

该协议可防止由传感器噪声或较小的预测误差导致的不稳定 PQC 切换，有助于维持车辆运行稳定。当预测误差足够小时，优化器会做出一致的决策，且所选的 PQC 配置会随时间保持稳定。形式上，当 $K\varepsilon < \Delta_{\min}$ 时，稳定性成立。我们评估了协议针对回滚尝试、消息丢失、版本计数器篡改和同步错误的鲁棒性，表 II 总结了相应的防御措施。

表 II： 后量子密码转换协议的故障模式分析。

攻击场景	缓解机制	结果
旧版本重放	随机数 + 上下文哈希	已检测
消息丢失	原子两阶段确认	无部分更新
非对称更新	相互确认	安全回滚至 v_t
计数器篡改	签名不匹配	数据包丢弃
强制降级	单调版本检查	不可能

表 II 中的缓解机制在协议层实现，且独立于 APMOEA 选定的具体后量子密码配置。底层后量子密码原语无需修改即可使用。重新配置期间的安全性通过协议机制得到保障，例如经认证的版本计数器、上下文哈希、新鲜度随机数和原子确认步骤，这些机制可防止重放、降级和失步攻击。APMOEA 负责选择后量子密码配置方案，而转换协议则安全地管理不同方案之间的切换。降级尝试会通过版本不匹配被检测到，从而确保合法升级成功接受，并

对降级攻击予以拒绝。令 v_t 表示时间 t 的当前后量子密码版本， v_{t+1} 表示拟议版本；所有转换消息均包含经过身份验证的版本信息、上下文哈希和新鲜度随机数，以确保安全转换。

定理 V.2 (单调升级安全性)。 令 v_t 表示当前后量子密码版本， v_{t+1} 表示协商的目标版本。在采用版本计数器、上下文哈希和相互确认的认证信令下，任何概率多项式时间对手都无法诱使系统转换到任何 $v < v_{t+1}$ ，也无法造成端点去同步。

这里， v_t 是当前使用的后量子密码版本， v_{t+1} 是升级过程中提议的新版本。任何篡改都会破坏经过签名且与随机数绑定的转换记录，导致双方立即拒绝，因此降级无法成功。这消除了混合后量子密码迁移期间最严重的风险。端到端后量子密码时延建模如下：

$$T_{\text{lat}}(a, X_t) = T_{\text{enc}}(a) + T_{\text{dec}}(a) + T_{\text{net}}(a, X_t), \tag{6}$$

其中， T_{net} 涵盖信噪比、带宽和负载相关效应。

定理 V.3 (时延有界性)。令 X_t 表示时间 t时的上下文。假设在一个决策区间内，车辆和信道变化均有界：

$|v_{t+1} - v_t| \le \Delta v, \qquad |\gamma_{t+1} - \gamma_t| \le \Delta\gamma$，其中 v_t 表示车辆速度，γ_t 表示链路信噪比（或信道质量代理）。*APMOEA*所选*PQC*配置的时延满足

$$T_{\text{lat}}(a_t, X_t) \le \max_{a \in \mathcal{A}} T_{\text{lat}}(a, X_t) + O(\Delta v + \Delta\gamma). \tag{7}$$

此处， X_t 表示时刻 t的上下文向量， δ 限制相邻步骤之间上下文的变化幅度， a_t 表示 APMOEA 选定的后量子密码算法， $\mathcal{A}$ 表示所有后量子密码算法的集合，而 $T_{\text{lat}}(\cdot)$ 表示端到端时延。由于上下文的小幅变化只会引起时延的小幅波动，并且 APMOEA 从不选择劣于可行最大值的候选项，因此时延始终有界。因此，即使在高速移动性下，由后量子密码引起的时延仍符合超可靠低时延通信要求。令预言最优算法为。这里的“预言最优”是指：如果系统能够在没有任何预测误差的情况下，准确获知下一个上下文，那么它会选择的理想后量子密码算法。在真实的下一个上下文下，该算法为 $a^\star = \arg\min_{a \in \mathcal{A}} L_{t+1}(a)$。

VI. 实验评估

我们针对贡献中提出的主张评估 CAAP。我们通过在真实的 NR-V2X 移动性、信道、天气和计算轨迹下，将 APMOEA 与静态后量子密码基线进行比较，评估 (C1) 时延降低；通过对安全转换协议实施重放、回滚和上下文操纵攻击，评估 (C2) 抵御降级和失步的能力；通过引入可控的预测噪声并测量后量子密码切换行为，评估 (C3) 决策稳定性；并通过分析其对异构信道条件和汽车计算配置的敏感性，评估 (C4) 鲁棒性。

1. 实验设置所有实验均旨在直接评估一项或多项所述主张。我们考虑四种经 NIST 标准化的后量子密码方案：Kyber-768 和 Dilithium-3（基于格）、Classic McEliece-348864（基于代码）和 SPHINCS+-128s（基于哈希）。它们的计算和通信特性汇总于表 III。我们将 APMOEA 与车联网系统中常用的三种静态基线进行比较：Static-Lattice、Static-Code 和 Static-Hash。评估聚焦于四项指标：端到端时延、计算开销、通信开销和安全一致性（即不存在降级或不同步）。上下文信号经过时间对齐；预测、优化和后量子密码切换均在一台车规级 800 MHz 中央处理器模拟器上运行。相同的上下文演变确保了比较的公平性。

2. 结果与讨论

实验采用 LuST 移动性轨迹、ERA5 天气数据和 NR-V2X 信道模型，并基于 NIST 后量子密码参考实现及汽车级中央处理器配置文件推导密码学成本。

时延与超可靠低时延通信合规性：与静态 PQC 配置相比，自适应 PQC 选择始终能够降低端到端密码学时延（表 IV）；通过在不利条件下避免使用计算密集型方案，CPU 使用率降低约 22–40%。经典密码学（ECDH/ECDSA）由于密钥较小且验证开销较低，时延更低；然而，固定的 PQC 配置经常无法满足 V2X 安全流量的 5–20 ms URLLC 预算。相比之下，CAAP 在动态上下文中始终将时延控制在 URLLC 限值内，展现了后量子安全在车联网系统中的实际可行性。

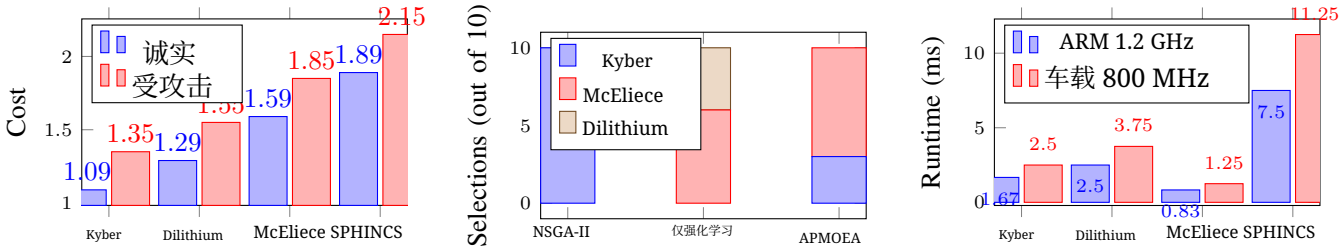
上下文操纵下的鲁棒性：图 3(a) 显示，对上下文信号进行对抗性操纵会增加 PQC 配置的绝对成本，但其相对排序保持不变。这表明有界扰动不会导致密码算法选择出现不稳定或受对手控制的情况，从而支持成本模型和优化过程所依据的鲁棒性假设。

选择行为与决策稳定性：图 3(b) 比较了 NSGA-II、仅强化学习和基于 APMOEA 的策略的选择行为。NSGA-II 表现出有限的自适应能力，并收敛到一种主导配置，而仅强化学习方法在低信噪比条件下反应过度，频繁选择开销较高的基于 McEliece 的方案。相比之下，APMOEA 通过联合优化时延、计算、通信和安全性，在后量子密码类别之间实现了均衡选择。强化学习进一步稳定了决策，将 PQC 切换频率从每分钟 14.2 次降至 4.3 次，并将峰值时延降低了 75% 以上（表 IV）。

硬件可行性：图 3(c) 评估了汽车级硬件的运行时敏感性。尽管 McEliece 的原始计算时间较短，但其较大的通信开销使其不适用于超可靠低时延通信流量。相比之下，由于验证成本较高，SPHINCS+ 对中央处理器频率表现出更高的敏感性。自适应规划器会权衡这些因素，并选择能在 800MHz 车载 CPU 上的毫秒级限制内运行的配置，从而支持实时部署。

表 III：后量子密码配置方案的计算成本、通信开销、动态选择频率和对抗敏感性对比。

算法	计算成本（毫秒）			通信开销（KB）		动态选择		上下文攻击成本	
	Enc	Dec	验证	公钥大小	签名/密文	选择百分比	触发器	诚实	攻击
SPHINCS+-128s	0.90	–	1.10	0.05	17.00	69.1%	无状态 / 不稳定性下的回退机制	1.89	2.15
Kyber-768	0.25	0.35	0.15	1.18	1.08	26.9%	低延迟且计算高效运行	1.09	1.35
Dilithium-3	0.40	0.45	0.30	1.50	2.70	4.0%	高保障认证阶段	1.29	1.55
McEliece-348864	0.05	0.06	–	240.00	0.13	<1%	极端噪声下的罕见使用	1.59	1.85



(a) 上下文操纵效应　(b) NSGA-II 与强化学习与 APMOEA　(c) 不同硬件上的运行时敏感性

图 3：(a) 对抗性上下文操纵下的后量子密码成本，(b) NSGA-II、仅强化学习和 APMOEA 的选择行为，以及 (c) ARM 1.2GHz 和车规级 800 MHz CPU 上的硬件相关运行时变异性（以毫秒为单位）。

表 IV：真实 NR-V2X 条件下的时延性能、切换稳定性和降级攻击鲁棒性。

方案 / 设置	密钥大小（KB）	端到端时延（毫秒）	切换次数 / 60 秒	安全结果
ECDH / 椭圆曲线数字签名算法（经典）	0.09	4.1	–	经典基线
Kyber-768	1.18	9.3	–	后量子密码（静态）
Dilithium-3	1.50	10.8	–	后量子密码（静态）
McEliece-348864	240.00	8.7	–	后量子密码（静态）
SPHINCS+-128s	0.05	17.4	–	后量子密码（静态）
自适应后量子密码（APMOEA，无强化学习）	–	7.8	14.2	升级已接受；检测到降级
自适应后量子密码（APMOEA + 强化学习）	–	**7.2**	**4.3**	**升级已接受；检测到降级**

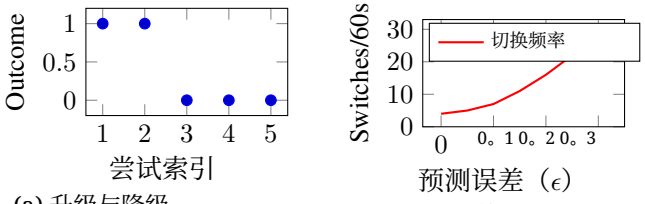
表 V：上下文操纵与硬件运行时。

算法	诚实成本	受攻击成本	ARM 1.2GHz（秒）	车辆 800MHz（秒）
Kyber	1.09	1.35	0.00167	0.00250
Dilithium	1.29	1.55	0.00250	0.00375
McEliece	1.59	1.85	0.00083	0.00125
SPHINCS+	1.89	2.15	0.00750	0.01125

密码学迁移的安全性：安全转换协议成功防止了降级和重放攻击，同时允许合法的后量子密码升级（表 IV，图 4）。即使丢包增加且上下文噪声加剧，强化学习仍能稳定规划决策，防止有害或不一致的转换。此外，即使预测误差达到 $\varepsilon \leq 0.10$，后量子密码选择仍保持稳定，这与第 V 节推导出的理论稳定性保证一致。

3. 局限性与未来范围：由于目前尚无 6G 系统，我们的实验采用了基于轨迹的 NR-V2X 信道模型和汽车计算配置。CAAP 支持现有的 5G NR-V2X，并可通过最小改动过渡到 6G。其局限性包括依赖时钟同步、对预测准确性敏感，以及缺乏实际部署验证。未来的工作将通过 6G 感知集成、对强化学习辅助自适应进行形式化验证，以及在基于解决方案的测试平台（例如硬件在环或小规模车联网配置）上进行端到端部署来解决这些问题，从而验证运行时行为、集成开销，以及超越基于轨迹建模的系统级交互。

未来的工作将扩展 CAAP，使其能够联合优化加密和签名方案，从而更好地体现实际后量子安全的要求：单靠任何一种机制都不足以满足安全需求。



(a) 升级与降级　(b) 预测误差的影响

图 4：(a) 降级攻击拒绝（1=成功，0=已拒绝）和 (b) 预测误差驱动的切换频率。

VII. 结论

我们提出了一种面向6G车联网的自适应后量子密码框架 CAAP，该框架联合预测移动性和信道动态，通过 APMOEA选择最优PQC方案，并强制执行安全的单调升级。该框架将时延降低了27%，能够防止降级攻击，并且对上下文操纵、硬件可变性和预测噪声具有稳健性。理论分析证明了在现实漂移条件下的决策稳定性和有界时延，展示了实现量子安全车联网的可行路径。

参考文献

[1] P. W. Shor，《量子计算机上进行素因数分解和离散对数运算的多项式时间算法》，《SIAM计算杂志》，1997年。[2] NIST，《NIST后量子密码学第三轮报告》，https://csrc.nist.gov，2022年。[3] L. Ducas等，《CRYSTALS-Dilithium：基于模格的数字签名》，2020年。[4] J. Bos 等，《 CRYSTALS-Kyber：算法规范》，2020 年。[5] R. McEliece，《一种基于代数编码理论的公钥密码系统》，《DSN进展报告》，1978年。[6] N. Sendrier，《基于编码的密码学：现状与展望》，载于IEEE信息论国际研讨会，2011年。[7] D. Bernstein等，《 SPHINCS+：提交至NIST后量子密码标准化项目》，2019年。[8] A. Paul和E. Lorenzen，《面向汽车和车联网应用的后量子密码学评估》，《IEEE车辆技术汇刊》，2022年。[9] Y. Pan和H. Li，《用于安全车载自组网通信的NIST后量子密码算法性能评估》，《IEEE车辆技术汇刊》，第72卷第8期，第10412–10425页，2023年。[10] J. Ha等，《自动驾驶中的车联网通信：综述》，《IEEE通信调查与教程》，2020年。[11] Q. Liu和N. Mahyuddin，《面向5G及后续技术的低时延可靠车联网》，《IEEE Access》，2021年。[12] 3第三代合作伙伴计划，《3GPP TR 38.885 V16.0.0：新空口车联网研究》，《技术报告》，2019年。[13] A. Ali、M. I. Baig和S. Hussain，《毫米波车联网通信：挑战与机遇》，《IEEE通信杂志》，2020年。[14] Z. Chen和Q. Li，《衰落和干扰信道上的McEliece型密码系统性能》，《IEEE信息取证与安全汇刊》，2020年。[15] D. Jao、M. Albrecht和S. Bai，《基于格的后量子密码算法性能评估》，《ACM隐私与安全汇刊》，2022年。[16] Z. Pan和M. Li，《面向下一代车联网的后量子密码增强认证》，《IEEE车辆技术汇刊》，2023年。[17] S. Khattak、A. Maaref和A. Yongacoglu，《高移动性下的快速时变车联网信道》，《IEEE车辆技术汇刊》，2019年。[18] V. Gounder和S. Srinivasan，《面向嵌入式系统和物联网平台的噪声感知自适应密码学》，《传感器》，2020年。[19] E. Rescorla，《传输层安全协议（TLS）1.3版》，RFC 8446，2018年。[20] J. Iyengar和M. Thomson，《QUIC：一种用于HTTP/3的安全可靠传输协议》，《ACM Queue》，2021年。[21] 3第三代合作伙伴计划，《3GPP TR 22.886：增强3GPP对5G车联网服务的支持研究》，《技术报告》，2020年。[22] Y. Liu、M. Chen和Y. Zhang，《6G车联网：迈向超可靠低时延车载通信》，《IEEE网络》，2022年。[23] P. Shor，《量子计算机上进行素因数分解和离散对数运算的多项式时间算法》，《SIAM计算杂志》，1997年。[24] NIST，《NIST后量子密码标准化：最终标准（Kyber、Dilithium）》，美国国家标准与技术研究院，技术报告，2022年。[25] L. Chen、D. Moody和A. Patrick，《NIST后量子密码第三轮入围者：性能评估》，美国国家标准与技术研究院，技术报告，2021年。[26] Y. Chen、R. Kumar和T. Abdelzaher，《面向车载自组网安全的后量子密码学评估》，《IEEE物联网杂志》，2022年。[27] J. Almeida、D. Hofheinz和E. Kiltz，《NIST后量子密码候选算法的性能与安全性比较》，《ACM隐私与安全汇刊》，2024年。[28] X. Sun和X. Du，《面向资源受限无线系统的自适应密码框架》，《IEEE移动计算汇刊》，2018年。[29] A. Rahman和K. Cabaj，《面向物联网设备的上下文感知密码自适应》，《IEEE Access》，2020年。[30] E. Rescorla，《传输层安全协议（TLS）1.3版》，RFC 8446，2018年。[31] J. Iyengar和M. Thomson，《QUIC：一种基于用户数据报协议的安全可靠传输协议》，载于IEEE计算机通信会议（INFOCOM），2020年。[32] M. Thomson和J. Iyengar，《QUIC传输协议中的版本协商》，互联网草案，互联网工程任务组，技术报告，2021年。[33] M. Wolf和A. Weimerskirch，《面向车联网安全的硬件信任根》，《IEEE车辆通信》，2019年。

[34] J. O. Kephart 和 D. M. Chess，“自主计算的愿景”，*Computer*，第 36 卷，第 1 期，第 41–50 页，2003 年。

附录

A. 决策稳定性的证明

证明。令 $L_t(a)$ 表示算法 a 在时刻 t 的加权损失，令 $\hat{} L_{t+1}(a)$ 表示根据 $\hat{} X_{t+1}$ 计算得到的预测损失。根据假设 (A1)，每个成本项关于上下文均为 L-利普希茨：

$$|L(a, X) - L(a, X')| \le K\|X - X'\|, \tag{8}$$

其中某个常数 K 由 L 所有组件的利普希茨常数组合确定。根据 (A3)，预测误差满足 $\| \hat{} X_{t+1} - X_{t+1}\| \le \varepsilon$。因此，$|\hat{} L_{t+1}(a) - L_{t+1}(a)| \le K\varepsilon.$令 $\Delta_{\min}$ 表示任意两个后量子密码算法之间的最小损失间隔：

$$\Delta_{\min} = \min_{a \neq b} |L_{t+1}(a) - L_{t+1}(b)|. \tag{9}$$

若 $K\varepsilon < \Delta_{\min}$，则预测误差引起的扰动不足以改变所有 $a \in \mathcal{A}$ 上 $L_{t+1}(a)$ 的排序。因此，最小化者的身份保持不变：

$$\arg\min_a \hat{L}_{t+1}(a) \;=\; \arg\min_a L_{t+1}(a). \tag{10}$$

由于 APMOEA 根据预测损失进行选择，因此它返回的算法与使用真实上下文的预言机相同。因此，对于满足损失差条件的任意区间内的所有 t，决策都保持稳定，从而证明了该结论。

□

B. 单调升级安全性的证明

证明。设 v_t 为当前正在使用的后量子密码版本，$v_{t+1} > v_t$ 为优化器提出的版本。每条转换消息都包含一个经过身份验证的版本计数器 ctr、一个上下文哈希 $H(X_t)$、一个新鲜度随机数 N_t，以及在端点的可信硬件中计算的数字签名。我们证明，任何概率多项式时间（PPT）对手都无法导致降级或失步。重放的消息包含旧随机数 $N_{t'}$ 和旧版本计数器 $v_{t'} < v_{t+1}$。新鲜度检查会拒绝任何随机数已过期的消息。如果对手将 $(v_{t'},\ N_{t'})$ 改写为任意一对 $(v,\ N)$，签名将无法通过验证。因此，重放攻击无法导致降级。若要强制降级，对手必须生成一条版本计数器为 $v < v_t$ 的消息。由于版本计数器包含在签名载荷中，修改 v 会破坏签名，从而导致消息立即被拒绝。根据对后量子密码签名方案安全性的假设，任何 PPT 对手都无法伪造有效签名。两阶段协议要求相互确认：每个端点只有在收到来自对等端的有效且带有新鲜签名的确认消息后，才会转换到 v_{t+1}。对手丢弃、延迟或篡改任何消息都会导致不匹配，进而触发回滚至 v_t。因此，任何一个端点都无法单独推进。降级需要接受某个 $v < v_{t+1}$。两个端点都会执行单调版本检查：$v_{\text{received}} \ge v_t$？无论消息内容如何，任何 $v < v_t$ 都会被拒绝。因此，即使成功伪造旧消息的签名，也无法导致降级。由于对手的所有策略都无法生成可行的交互记录来导致

转至 $v < v_{t+1}$ 或导致端点状态不一致，因此，所有可接受转移都严格单调且同步。 □

C. 时延有界性的证明

证明。令 $T_{\text{lat}}(a, X_t)$ 表示上下文 X_t 下的端到端时延。假设 (A2) 指出，车辆动力学满足：$\|X_{t+1} - X_t\| \le \delta$. T_{lat} 的每个分量关于上下文变量（加密时间、解密时间、网络时延和信噪比相关效应）均为连续函数。因此，T_{lat} 本身是利普希茨连续的：$|T_{\text{lat}}(a, X_{t+1}) - T_{\text{lat}}(a, X_t)| \le C\delta$，其中 $C > 0$ 为某个常数。令 $a_t = \arg\min_{a \in \mathcal{A}} L_t(a)$ 为 APMOEA 选出的算法，该算法保证 a_t 位于时刻 t 可行集的帕累托前沿上或附近。那么，对于任意 $a \in \mathcal{A}$，根据最大值的定义，$T_{\text{lat}}(a_t, X_t) \le \max_{a' \in \mathcal{A}} T_{\text{lat}}(a', X_t)$。在时刻 $t+1$，我们有 $T_{\text{lat}}(a_t, X_{t+1}) \le T_{\text{lat}}(a_t, X_t) + C\delta$。因此，

$$T_{\text{lat}}(a_t, X_t) \le \max_{a' \in \mathcal{A}} T_{\text{lat}}(a', X_t) + O(\delta), \tag{11}$$

这证明只要上下文漂移有界，时延增长就保持有界。在车载环境中，δ 对应于一个优化间隔（20–50ms）内移动性、衰落和负载的变化，这些变化都很小。因此，后量子密码的时延仍符合超可靠低时延通信的要求。 □

D. 小预测误差下的鲁棒性

引理 A.1(小预测误差下的鲁棒性)。 如果预测误差满足稳定性条件 $K\varepsilon < \Delta_{\min}$，则 *APMOEA* 会选择 $a_t = a^\star$。

在可接受的预测噪声下，APMOEA 选择的最优后量子密码与预言机的选择一致，并按照算法2进行安全迁移和检测。

证明。令 $a^\star = \arg\min_{a \in \mathcal{A}} L_{t+1}(a)$ 为真实下一时刻上下文 X_{t+1} 下预言机选出的最优后量子密码算法。APMOEA 计算：$a_t = \text{argmin}_a \hat{} L_{t+1}(a)$，其中，$\hat{} L_{t+1}(a)$ 使用预测上下文 $\hat{} X_{t+1}$ 计算。根据 (A3)，$\| \hat{} X_{t+1} - X_{t+1} \| \le \varepsilon$. 根据利普希茨连续性，$|\hat{} L_{t+1}(a) - L_{t+1}(a)| \le K\varepsilon$. 如果 $K\varepsilon < \Delta_{\min}$（稳定性条件），则损失的扰动不足以改变最小化器的选择。因此，

$$\arg\min_a \hat{L}_{t+1}(a) = \arg\min_a L_{t+1}(a) = a^\star. \tag{12}$$

因此，当预测误差相对于损失间隔较小时，APMOEA 的决策与预言机一致。这保证了在可容许噪声下能够正确选择后量子密码。 □

E. 表格和图表旨在展示的内容

表 III 总结了与车载部署相关的四类 NIST 后量子密码在计算、通信和鲁棒性方面的特性。表 IV 报告了端到端时延和切换稳定性，凸显了相较于静态基线，自适应 PQC 选择带来的超可靠低时延通信优势，以及强化学习的稳定作用。图 3 通过以下方面评估鲁棒性：(a) 有界上下文操纵下的代价稳定性；(b) NSGA- II、仅强化学习和 APMOEA 之间的选择行为对比；以及 (c) 硬件可变性下的运行时可行性。图 4 通过拒绝降级尝试证实了安全转换，并说明预测误差增大将导致切换频率升高。

F. 结果中使用的操作性定义

端到端时延。 时延定义为密码学处理与网络时延之和，$T_{\text{e2e}}(a, X_t) = T_{\text{crypto}}(a, \text{中央处理器}_t) + T_{\text{net}}(\text{信噪比}_t, \text{分组错误率}_t)$。密码学时延根据 NIST 参考实现和车载 CPU性能剖面计算；网络时延则采用依赖信噪比/分组错误率的 NR-V2X 模型，并对 200 次蒙特卡洛运行取平均。结果根据 5–20 毫秒的 URLLC时延预算进行评估。

上下文操纵下的成本。 “诚实”成本反映标称上下文演化，而“受攻击”成本则对信噪比和计算负载等信号施加有界扰动，以模拟传感器噪声或恶意上下文注入。这些扰动不会改变密码学原语，只用于检验选择鲁棒性。

切换稳定性。 切换频率用于衡量在固定时间窗口内（例如每 60 秒的切换次数）PQC配置发生变化的频率。切换次数越少，表示运行越稳定、可靠。

抗降级能力。 降级防护通过协议层的单调版本检查、上下文一致性、nonce新鲜性和原子确认来强制实施。只有所有检查均通过，才会接受转换，从而防止降级和失步攻击。