第16讲

第16讲：课程总结与展望

牛温佳 教授

北京交通大学 · 网络空间安全学院

本讲内容

学习目标

系统回顾整个课程的核心知识点

巩固对量子类脑计算与智能汽车安全的理解

获取继续深入学习的资源和方法

16.1 课程核心知识点回顾

Section 16.1 课程核心知识点回顾

16.1 课程核心知识点回顾

模块一：量子计算基础（第1-4讲）

量子比特：信息的基本单位，可以处于|0⟩ 与|1⟩ 的叠加态，测量时坍缩到确定状态。

量子门与线路：在量子比特上进行操作的基本单元，所有量子门必须可逆（酉变换）。变分量子线路由编码、拟设（可训练线路）、测量三部分组成。

量子算法：Shor算法（因数分解）、Grover算法（非结构化搜索）、HHL算法（解线性方程组）。量子机器学习将量子计算的并行性与AI结合。

模块二：类脑计算基础（第5-7讲）

脉冲神经网络：第三代神经网络，通过离散的脉冲序列传递信息。LIF神经元模型模拟了生物神经元的积分-泄漏-发放过程。

16.1 课程核心知识点回顾（续）

类脑芯片：从硬件层面模拟神经网络，能效比传统芯片提升2-3个数量级。代表性芯片包括IBM TrueNorth、 Intel Loihi、清华"天机芯"。

模块三：智能汽车安全（第8-10讲）

自动驾驶分级：L0-L5共6个级别。核心技术栈包括感知、定位、决策规划、控制四大模块。

对抗攻击：通过微小扰动使AI模型出错。分为数字攻击和物理攻击，白盒攻击和黑盒攻击。物理攻击通过对抗补丁、对抗伪装等方式在真实世界实施。

防御策略：传统方法（数据增强、对抗训练、输入去噪）存在局限。需要从架构层面转变计算范式——利用量子-脉冲混合网络的不可微性和高维特征映射来对抗攻击。

16.1 课程核心知识点回顾（续）

模块四：交叉前沿（第11-13讲）

量子类脑融合：量子神经网络（QNN）的优势在于高维特征空间和并行性。量子-经典混合计算是最务实的当前路线。

3D深度欺骗攻击：从局部平面补丁升级为全表面三维伪装，通过可微渲染优化对抗纹理，可在多种天气和视角下保持攻击效果。

QSNN防御框架：脉冲编码+量子电路的双层防御，贡献约90%（SNN）+ 额外10%（PQC）的防御增益，实现攻击能量从目标区域向背景区域的重新分配。

模块五：实践与展望（第14-16讲）

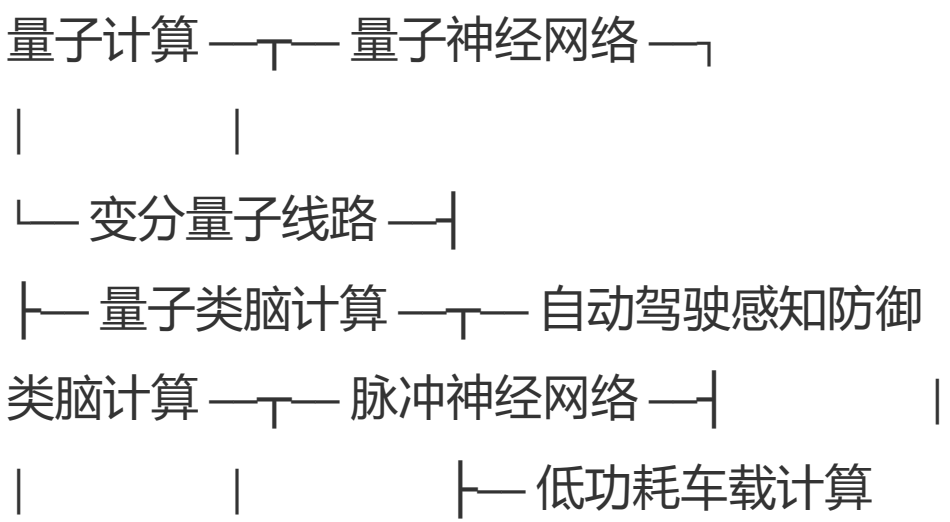
16.1 课程核心知识点回顾（续）

从产业案例（宝马×英伟达、路牌攻击等）到未来趋势，技术发展需要考虑伦理、社会影响和可持续发展的平衡。

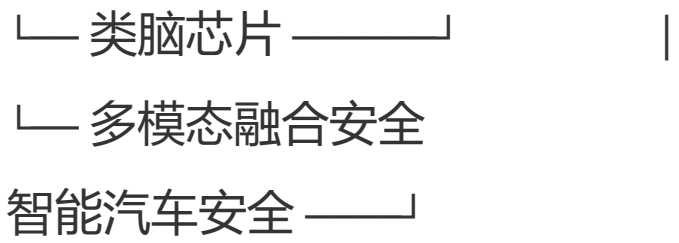
16.2 知识图谱

Section 16.2 知识图谱

16.2 知识图谱



16.2 知识图谱（续）



16.3 延伸学习资源

Section 16.3 延伸学习资源

16.3 延伸学习资源

在线课程

- IBM Quantum Learning: https://learning.quantum.ibm.com/

- 量子机器学习入门（PennyLane官方教程）

- CS231n: Deep Learning for Computer Vision（理解深度学习基础）

开源工具

- **PennyLane**：量子-经典混合编程框架

16.3 延伸学习资源（续）

- **SpikingJelly**：脉冲神经网络开发框架
- **Qiskit**：IBM量子计算框架

推荐书籍

1. 方滨兴. 人工智能安全. 电子工业出版社, 2020.

2. 姜楠. 量子机器学习: 基于Python的理论和实现. 清华大学出版社, 2024.

16.3 延伸学习资源（续）

3. 郭国平. 量子机器学习理论与实战. 人民邮电出版社, 2024.

4. Nielsen & Chuang. Quantum Computation and Quantum Information.

前沿追踪

- arXiv: quant-ph, cs.LG, cs.CV

- NeurIPS, ICML, CVPR 等顶会论文

16.3 延伸学习资源（续）

- 各大量子计算公司（IBM、Google、Xanadu）的技术博客

延伸阅读

📖选择一个你感兴趣的话题，写一篇科普短文或调研报告（约2000-3000字）：

📖1. 量子计算如何改变我们的生活?

📖2. 类脑芯片会是AI的下一个突破口吗?

📖3. 自动驾驶汽车真的安全吗?

📖4. 量子计算能保护AI不被攻击吗?

📖5. 从科幻到现实：我理想中的未来智能交通

📖6. 自选主题（需与课程内容相关）

结束语

Section 结束语

结束语

同学们，量子计算、类脑计算和智能汽车安全是当前最具活力和前景的三个前沿领域。它们各自的突破都足以改变世界，而当它们交叉融合时，可能会产生我们目前难以想象的创新。

希望这门课程能够：

- 为你打开一扇了解前沿科技的窗户
- 培养你跨学科思考的能力
- 激发你探索未知的热情
- 让你意识到科技发展必须与伦理责任同行

结束语（续）

谢谢大家！

📌本讲小结

- ✓ 16.1 课程核心知识点回顾
- ✓ 16.2 知识图谱
- ✓ 16.3 延伸学习资源
- ✓ 结束语
- ✓ 思考与讨论

感谢聆听

第16讲 · 课程总结与展望