

MÁSTER EN NUEVAS TECNOLOGÍAS ELECTRÓNICAS Y FOTÓNICAS

TRABAJO DE FIN DE MÁSTER - CURSO 2026-2027

PROPUESTA

Título:	<i>Técnicas de control basadas en Inteligencia Artificial para Sistemas de Distribución Cuántica de Claves (QKD)</i>
Título en inglés:	<i>Artificial Intelligence-Based Control Techniques for Quantum Key Distribution (QKD) Systems</i>
Tutor/es:	<i>Adrián Llanos Velasco, Pablo Arteaga Díaz</i>
Correos-e:	<i>adrian.llanos@qddynamics.es, pablo.arteaga@qddynamics.es</i>
Lugar de realización:	<i>Tres Cantos, Madrid</i>

Resumen:

La Distribución Cuántica de Claves (QKD, Quantum Key Distribution) permite a dos partes establecer una clave secreta compartida cuya seguridad se fundamenta en las leyes de la mecánica cuántica, y constituye una de las tecnologías más maduras para proteger las comunicaciones frente a la amenaza que supone la computación cuántica. Sin embargo, su despliegue fuera del laboratorio se ve limitado por la inestabilidad de los sistemas reales: la deriva de polarización y de fase en la fibra óptica, las variaciones de temperatura, las fluctuaciones de la potencia láser, la desalineación temporal entre emisor y receptor o el envejecimiento de los detectores de fotón único degradan la tasa de error cuántico (QBER) y reducen la tasa de clave secreta, llegando a interrumpir la generación de clave.

Tradicionalmente estas perturbaciones se corrigen mediante lazos de control clásicos (PID, algoritmos de búsqueda por gradiente o barridos periódicos) que requieren interrumpir la transmisión, consumen fotones de la propia clave y responden con lentitud ante cambios rápidos del canal. El objetivo de este Trabajo de Fin de Máster es estudiar, diseñar y evaluar técnicas de control basadas en Inteligencia Artificial — aprendizaje automático supervisado, redes neuronales para predicción de series temporales y aprendizaje por refuerzo— capaces de estabilizar de forma autónoma los parámetros críticos de un sistema QKD y de optimizar en tiempo real sus parámetros de operación (intensidades de los estados señuelo, probabilidades de elección de base, umbrales de detección, etc.).

El trabajo incluirá el análisis de datos de telemetría del sistema, el entrenamiento y la comparación de distintos controladores inteligentes frente a los métodos clásicos, y, en la medida de lo posible, su validación con datos experimentales o sobre el hardware QKD disponible en el centro de realización (Tres Cantos, Madrid). Se espera obtener controladores que reduzcan el tiempo de inactividad del enlace, mantengan el QBER por debajo del umbral de seguridad y aumenten la tasa de clave secreta efectiva.

Metodología:

El trabajo se desarrollará en las siguientes fases:

- **Revisión bibliográfica:** estudio a nivel de sistema del funcionamiento de un enlace QKD y de sus subsistemas ópticos y electrónicos, de las fuentes de inestabilidad en sistemas reales y del estado del arte en la aplicación de técnicas de IA a su control y optimización.
- **Adquisición y análisis de datos:** adquisición y preprocesado de registros de

telemetría del sistema QKD (QBER, tasas de detección, señales de los actuadores, temperatura, etc.), identificando variables relevantes, correlaciones y escalas temporales de las derivas, que servirán como base para el entrenamiento y la evaluación de los controladores.

- **Diseño de controladores:** implementación de un controlador de referencia clásico (PID o búsqueda por gradiente) y de controladores basados en IA: (i) modelos supervisados y redes recurrentes (LSTM/GRU) para predecir la deriva y compensarla de forma anticipada; (ii) agentes de aprendizaje por refuerzo (p. ej. DQN, PPO o SAC) que actúen sobre los actuadores del sistema (controladores de polarización, moduladores de fase, líneas de retardo) maximizando una recompensa ligada a la tasa de clave y al QBER; (iii) regresores ligeros para la predicción de parámetros óptimos del protocolo.
- **Evaluación:** comparación cuantitativa de los controladores en términos de QBER medio, tasa de clave secreta, tiempo de recuperación ante perturbaciones, fracción de tiempo útil del enlace, robustez frente a condiciones no vistas en el entrenamiento y coste computacional, prestando atención a que el control no comprometa las hipótesis de seguridad del protocolo.
- **Validación experimental y documentación:** según disponibilidad, integración del mejor controlador en el sistema experimental o en un banco de pruebas hardware-in-the-loop, y redacción de la memoria con el análisis de resultados y las líneas futuras.

Las herramientas previstas son Python (NumPy, SciPy, PyTorch, Gymnasium/Stable-Baselines3) y, en su caso, las interfaces de control del equipamiento óptico del laboratorio.

Conocimientos previos recomendados:

Es suficiente con una base sólida de óptica y de electrónica/control. En concreto, se recomienda:

- Fundamentos de óptica y fotónica: polarización de la luz, interferometría, fibra óptica y detección de señales ópticas.
- Electrónica y teoría de control: sistemas realimentados, control PID, estabilidad e identificación de sistemas.
- Se valorará positivamente la experiencia previa en Inteligencia Artificial (regresión, redes neuronales o aprendizaje por refuerzo), aunque no es imprescindible: los conceptos necesarios se adquirirán durante el desarrollo del trabajo.
- Programación en Python y manejo de librerías de cálculo científico y aprendizaje profundo (NumPy, SciPy, PyTorch o TensorFlow).
- Nivel de inglés suficiente para la lectura de artículos científicos.

Bibliografía:

- [1] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in Proc. Int. Conf. Computers, Systems and Signal Processing, Bangalore, India, 1984, pp. 175–179. Reimpreso en Theor. Comput. Sci., vol. 560, pp. 7–11, 2014. doi: 10.1016/j.tcs.2014.05.025.
- [2] N. Gisin, G. Ribordy, W. Tittel and H. Zbinden, "Quantum cryptography," Rev. Mod. Phys., vol. 74, no. 1, pp. 145–195, 2002.
- [3] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus and M. Peev, "The security of practical quantum key distribution," Rev. Mod. Phys., vol. 81, no. 3, pp. 1301–1350, 2009.
- [4] H.-K. Lo, X. Ma and K. Chen, "Decoy state quantum key distribution," Phys.

- Rev. Lett., vol. 94, 230504, 2005.
- [5] F. Xu, X. Ma, Q. Zhang, H.-K. Lo and J.-W. Pan, "Secure quantum key distribution with realistic devices," *Rev. Mod. Phys.*, vol. 92, 025002, 2020.
 - [6] S. Pirandola et al., "Advances in quantum cryptography," *Adv. Opt. Photon.*, vol. 12, no. 4, pp. 1012–1236, 2020.
 - [7] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, 10th anniversary ed. Cambridge University Press, 2010.
 - [8] W. Wang and H.-K. Lo, "Machine learning for optimal parameter prediction in quantum key distribution," *Phys. Rev. A*, vol. 100, 062334, 2019. doi: 10.1103/PhysRevA.100.062334.
 - [9] W. Liu, P. Huang, J. Peng, J. Fan and G. Zeng, "Integrating machine learning to achieve an automatic parameter prediction for practical continuous-variable quantum key distribution," *Phys. Rev. A*, vol. 97, 022316, 2018.
 - [10] M. Young, H. Duan, S. Pirandola and M. Lucamarini, "A comparison of optimisation algorithms for electronic polarisation control in quantum key distribution," *Applied Sciences*, vol. 16, no. 5, 2568, 2026. doi: 10.3390/app16052568.
 - [11] K. Purohit and A. K. Vyas, "Quantum key distribution through quantum machine learning: a research review," *Front. Quantum Sci. Technol.*, vol. 4, 1575498, 2025. doi: 10.3389/frqst.2025.1575498.
 - [12] A. Al-Kuwari, S. Alqrinawi, L. Al-Amir, A. Mollazehi and S. Al-Kuwari, "Machine learning techniques for enhancing quantum key distribution," *arXiv preprint arXiv:2603.07384*, 2026.
 - [13] R. S. Sutton and A. G. Barto, *Reinforcement Learning: An Introduction*, 2nd ed. MIT Press, 2018.
 - [14] I. Goodfellow, Y. Bengio and A. Courville, *Deep Learning*. MIT Press, 2016.
 - [15] K. J. Åström and R. M. Murray, *Feedback Systems: An Introduction for Scientists and Engineers*, 2nd ed. Princeton University Press, 2021.