Jerome Wiesemann
PhD Student in Quantum Information

Waterloo, ON, Canada
jwiesemann@uwaterloo.ca
jeromewiesemann.com

EDUCATION

PhD in Physics (Quantum Information)
05/25 – Exp. 04/29

University of Waterloo, Institute for Quantum Computing — *Waterloo, Canada*

- Research on quantum communication, photonic devices and photonic quantum error correction (QEC), supervised by Prof. N. Lütkenhaus
- Co-president of the IQC Graduate Student Association (2025-2026)

M.Sc. Physics, Technische Universität Berlin
10/22 – 12/24

GPA: 4.0/4.0 — *Berlin, Germany*

- Master's thesis: "Security implications of device imperfections in quantum key distribution," supervised by Prof. H. Weimer and Dr. N. Walenta, in collaboration with Fraunhofer HHI
- Modeling realistic photonic devices, analyzing vulnerabilities, developing security proofs and hacking implementations to enhance the security of quantum key distribution (QKD)

B.Sc. Physics, Technische Universität Berlin
10/19 – 09/22

GPA: 3.9/4.0 — *Berlin, Germany*

- Bachelor's thesis: "Iterative computation of individual Floquet states," supervised by Prof. A. Eckardt
- Mentor for first-year physics students

AWARDS

Physik-Studienpreis, German Physical Society
07/25

Awarded to eight students across Berlin and Brandenburg for outstanding academic achievement for the M.Sc. and B.Sc. in physics

Merit Scholarship, Bourse au Mérite
09/19

Awarded for highest distinction in the French Baccalauréat

RESEARCH & INDUSTRY EXPERIENCE

R&D Internship
02/25 – 04/25

ID Quantique — *Geneva, Switzerland*

- Characterized commercial QKD transmitters and receivers to assess and mitigate implementation security risks
- Developed and applied a framework to internally evaluate and increase the resilience of QKD systems against side-channel attacks

Student Researcher
11/22 – 01/25

Fraunhofer Heinrich Hertz Institute — *Berlin, Germany*

- Conducted experimental research on QKD systems with a focus on security proofs, implementation of photonic devices and certification
- **European Project Nostradamus:** Developed novel attack strategies (Trojan-horse and injection-locking attacks) for Europe's first QKD evaluation lab
- **German Project QuNet+BlueCert:** Led development of an attack matrix for German QKD certification trials with national certification labs and metrology institutes

Research Stay
06/24 (1 month)

Vigo Quantum Communication Center, Universidade de Vigo — *Vigo, Spain*

- Collaboration with Fraunhofer HHI under the EU project Nostradamus, developing novel experimental methods to evaluate injection-locking attacks in QKD transmitters
- Findings published in *APL Photonics* (2025)

Teaching Assistant
10/22 – 03/24

Technische Universität Berlin — *Berlin, Germany*

- Preparation of tutorials, one-on-one office hours, grading of homework assignments and exams in theoretical physics

Publications & Talks

Evaluation of quantum key distribution systems against injection-locking attacks
J. Wiesemann, F. Grünenfelder, A. Blázquez, N. Walenta, D. Rusca
APL Photonics, 10, 066112, 10.1063/5.0260685 (June 2025)

A consolidated and accessible security proof for finite-size decoy-state quantum key distribution
J. Wiesemann, J. Krause, D. Tupkary, N. Lütkenhaus, D. Rusca, N. Walenta
Preprint on *arXiv*, arXiv:2405.16578 (Dec. 2024), under review at *Quantum*

Invited talk: "A security proof for BB84," *Quantum Communication Symposium Germany*, Nov. 2024

Invited talk: "Current state of security in QKD," *German Federal Printing Office (Bundesdruckerei)*, Dec. 2024

Invited talk on QKD security at the steering committee meeting of Germany's national quantum communication initation (*QuNET*), 2024

Technical Skills

Programming: Python (NumPy, SciPy, pandas, Matplotlib, etc.), C++ (built >10k lines OpenGL graphics engine), C, MATLAB
Languages: German (native), French (native), English (fluent, TOEFL C2)