

ELEC5703: Introduction to Quantum Communications**Introduction**

This is an engineering minded course in quantum communications. Students coming in are not assumed to know much quantum mechanics. By the end of the course they should be able to treat a quantum link the way they would treat any other communications link: write a channel model, budget the impairments, compute an error rate and decide whether a protocol still works.

The conceptual core of the offerings of this course are as follows: orthogonality and incompatible measurements, Bell states and Bell inequalities, entanglement, teleportation, BB84 and E91. Further we will discuss and learn post-processing, side-channels, measurement-device-independent QKD (MDI-QKD) and secret-key rate versus distance.

The term is organized into three blocks:

- **Photons as signals.** Polarization qubits, optical hardware, and a lossy, noisy photonic channel, including a first signal-to-noise and quantum-bit-error-rate (QBER) calculation.
- **Entanglement as a resource.** Bell states, CHSH, teleportation, and entanglement swapping, including the detection loophole and why a classical optical amplifier cannot extend a quantum link.
- **QKD as a communication system.** BB84, E91, information reconciliation and privacy amplification, source and detector side-channels, decoy-state and MDI-QKD, then repeaters and rate versus distance.

Course Description and Requirements

Course Description: The course will emphasize core concepts, technical implementations, and practical limits of real-world quantum communications. A list of the majority of topics covered in this course are as follows: Polarization qubits and the linear algebra required to use them; optical waveplates, polarizing beam splitters, and single-photon detection; fibre loss, detector efficiency, dark counts, and QBER; entanglement, Bell inequalities, teleportation, and entanglement swapping; BB84 and E91; sifting, information reconciliation, and privacy amplification; decoy-state and measurement-device-independent QKD; linear-optics Bell-state analysis; quantum repeaters and secret-key rate versus distance.

Prerequisite(s): None

Lectures: 3 hours per week.

Laboratory and problem analysis: 0 hours per week

Instructor

Professor: Connor Kupchak

Email: connorkupchak@cunet.carleton.ca

Course Webpage: on Brightspace

Textbooks and Resources:

1) Quantum Physics: An Introduction Based on Photons. A.I. Lvovsky Springer ISBN-13: 978-3662565827 ebook: \$54.99 USD (**Mandatory**)

2) Quantum Communications <https://arxiv.org/pdf/2311.02367> M. Hajdusek and R. Van Meter Free (Mandatory)

Recommended (not required but excerpts will be posted when used)

- N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," Rev. Mod. Phys. 74, 145 (2002). QBER, dark counts, and practical BB84.
- A. K. Ekert, "Quantum cryptography based on Bell's theorem," Phys. Rev. Lett. 67, 661 (1991). E91.
- H.-K. Lo, X. Ma, and K. Chen, "Decoy-state quantum key distribution," Phys. Rev. Lett. 94, 230504 (2005).
- H.-K. Lo, M. Curty, and B. Qi, "Measurement-device-independent quantum key distribution," Phys. Rev. Lett. 108, 130503 (2012).
- S. Pirandola et al., "Fundamental limits of repeaterless quantum communications," Nat. Commun. 8, 15043 (2017). PLOB bound.
- Instructor notes and in-class exercises (Brightspace).

A laptop with Python or MATLAB is required for the modelling project and is useful on assignments. No specialized lab hardware is required.

Lecture Outline

Lectures are Wednesday and Friday, 11:35 am - 12:50 pm, in SA 308.

The first lectures are Wednesday 9 September and Friday 11 September. Friday 11 December follows a Monday schedule, so this course does not meet that day. The last lecture is Wednesday 9 December.

Week	Dates (2026)	Topics	Assessment
1	9, 11 Sep	Course framing: a quantum link as a communications system. Polarization qubits, Dirac notation, inner products, orthogonality, the measurement postulate.	
2	16, 18 Sep	Unitary operations. Waveplates and the polarizing beam splitter as hardware. Pauli and Hadamard implementations. Mixed states as a model of noise.	
3	23, 25 Sep	Single-photon sources in practice: attenuated lasers (Poisson statistics, $g(2)$), SPDC, heralding. Why a laser pulse is the wrong qubit and still the usual source.	
4	30 Sep, 2 Oct	The photonic channel. Fibre attenuation (dB/km and Beer's law), coupling, detector efficiency, dark counts, coincidence windows. Link budget. SNR as true counts versus dark counts. First implementation of QBER.	Assignment 1 due Fri 9 Oct 11:59pm
5	7, 9 Oct	Tensor products, Bell states, local measurement, remote state preparation.	
6	14, 16 Oct	Bell inequality and CHSH. Visibility, the detection loophole, and detector efficiency. Entanglement as a consumed network resource. CHSH here is the E91 abort condition later.	Assignment 2 due Fri 23 Oct 11:59pm
-	26-30 Oct	Fall break. No classes.	
7	21, 23 Oct	Teleportation, no-cloning, entanglement swapping. Why an erbium-doped fibre amplifier is indistinguishable from an eavesdropper. Linear-optics Bell measurement preview (two of four Bell states).	
8	4, 6 Nov	Midterm in class (4 Nov). BB84: one-time pad, sifting, intercept-resend (~25% QBER), the 11% security	Midterm Wed 4 Nov

		threshold. Loss does not by itself break security; errors do. Dark counts versus true counts.	
9	11, 13 Nov	E91: entanglement-based QKD, overlapping bases for key generation versus CHSH, monogamy, abort if $S \leq 2$. Information reconciliation and privacy amplification named. Worked use of published rates (fibre and satellite) as a calculation, not only a citation.	
10	18, 20 Nov	QKD post-processing and side-channels (restored from Winter 2025). Sifting to QBER estimate to LDPC reconciliation to privacy amplification. $I(A:B) = 1 - h_2(e)$, including $f(e)$. Multi-photon / photon-number-splitting and Trojan-horse attacks. Decoy-state BB84 as the source-side fix.	Assignment 3 due Fri 27 Nov 11:59pm
11	25, 27 Nov	MDI-QKD, taught together with the Bell-state analyzer. Detector side-channels (blinding) mean Bob's detectors cannot be trusted. MDI-QKD places an untrusted BSA at Charlie. Protocol, sifting, and how BSA success and loss set the rate. Secret-key rate versus distance and the PLOB ceiling, now with $1 - h_2(e)$ already in hand.	
12	2, 4, 9 Dec	MDI-QKD wrap if needed. Quantum repeaters: link architectures (including meet-in-the-middle, which students have just seen in MDI-QKD), memory retrieval efficiency, wait time versus direct transmission. Optional: entanglement purification. Student presentations. Last class is Wednesday 9 December.	Modelling project due Fri 4 Dec. 11:59pm Presentations

Self-Declaration form and Deferred Term work

Students who claim illness, injury or other extraordinary circumstances beyond their control as a reason for missed term work are held responsible for immediately informing the instructor concerned and for submitting a self-declaration form no later than three (3) days after the date/deadline of term work including test/midterm, labs, assignments. Any alternate arrangements made with the instructor for submission of term work should be made as soon as possible but within 3 days of the missed due date. If this is not possible after discussion with the instructor, alternate arrangements must be made before the last day of classes in the term as published in the academic schedule.

Instructors can require (or not) the student to submit the self-declaration form. Include the following statement if you require the student to submit a completed self-declaration form:

Consult with the instructor no later then 3 days after any missed course work or midterm examination.

or

Contact the instructor with the completed self-declaration form no later than 3 days after the date/deadline of term work including test/midterm, labs, assignments.

Evaluation and Grading Scheme

Assignments (3): 25%

Midterm (1): 20%

Modeling Project: 10%

Class Presentation: 10%

Final Exam: 35%

Assignments

Submit a single PDF on Brightspace by 23:59 on the due date. A penalty of 10% per calendar day applies for up to three days; after three days the assignment is not accepted. Computational work (Python or MATLAB) must include the commands or a short script and the numerical output.

- **Assignment 1.** Polarization algebra on $|H\rangle$, $|V\rangle$, $|+\rangle$, $|-\rangle$ plus a first link budget: received rate and $SNR = R_{\text{signal}}/R_{\text{dark}}$ at several distances. Due Friday 9 October.
- **Assignment 2.** Waveplates, tomography, and a QBER contribution from finite alignment error, combined with the detector/dark-count model from Assignment 1. Due Friday 23 October.
- **Assignment 3.** E91/CHSH on a non-ideal Bell pair (or the "wrong" Bell state), plus either a $1 - h_2(e)$ secret-key estimate or a repeater wait time with a 50% Bell-state analyzer. Due Friday 27 November.

Modelling Project

Each student (or a pair, at the instructor's discretion) models $R(L)$ for a stated fibre QKD or repeater link. Required elements: (i) a table of physical parameters with units and sources; (ii) $QBER(L)$ and Rate on the same plot; (iii) identification of the impairment that inhibits the link; (iv) one paragraph on what hardware or protocol change would move the drop off point (decoy-state BB84, MDI-QKD, or an extra repeater node are acceptable answers). Due Friday 4 December.

In Class Presentation

All students present. Topics are claimed on Brightspace so there is no overlap. You will not be expected to be an expert about the entire protocol. You are expected to understand the main concept of the protocol and relate it to the topics covered in class, and to include a quantitative noise or rate discussion. Presentations are scheduled in week 12.

You are encouraged to relate what we have learned in this course and try to apply it to the concept of the protocol. Presentations will be 12-15 minutes long. Use this time wisely. Most of all, treat this as an opportunity for yourself in trying to learn something new and how to explain it to others (and yourself!).

Rubric:

- Use of visual aids, including at least one plot or resource budget table. 30%
- Organization, including a clear statement of the engineering bottleneck. 40%
- Clarity of the delivery and engagement with audience. 30%

Midterm and Final Examinations

The midterm is held in lecture on Wednesday 4 November 2026 (80 minutes). A missed midterm without a documented reason receives zero. With a valid self-declaration or accommodation, the midterm weight is moved to the final examination.

Both examinations permit a non-programmable calculator and one double-sided page of personal notes. Electronic devices are not permitted. Evidence of unauthorized collaboration will be treated as an academic-integrity offence.

Learning Outcomes

Upon successful completion of this course, students will be able to:

1. Represent polarization qubits in Dirac and matrix notation, identify orthogonal (incompatible) measurement bases, and implement Pauli and Hadamard operations with waveplates and a polarizing beam splitter.

2. Build a photonic link budget of the form $\eta = 10^{-\frac{\alpha L}{10}} \cdot \eta_{\text{coupling}} \cdot \eta_{\text{det}}$ and convert it into a received photon rate and a signal-to-noise ratio (true detections versus dark counts in a coincidence window).
3. Assemble a QBER budget from misalignment, dark counts, and multi-photon pulses and determine the distance at which a QKD link crosses a security threshold (including the 11% intercept-resend bound for BB84 and the CHSH abort condition $S \leq 2$ for E91).
4. Explain BB84 sifting and intercept-resend, and explain why E91 remains secure even if Eve holds the entanglement source, using monogamy of entanglement and a CHSH test on unused basis pairs.
5. Carry a sifted key through information reconciliation and privacy amplification and compute a simplified secret-key length from $I(A:B) = 1 - h_2(e)$ (including a non-ideal reconciliation factor $f(e)$).
6. State why an attenuated laser enables photon-number-splitting, what decoy states buy back, and why detector side-channels (including blinding) motivate measurement-device-independent QKD.
7. Describe MDI-QKD as an untrusted Bell-state measurement in the middle, relate its success probability to a linear-optics Bell-state analyzer (at most 50%), and compare its engineering role to BB84 (prepare-and-measure) and E91 (entanglement-based).
8. Describe teleportation and entanglement swapping, and compute a simplified repeater wait time including fibre loss, BSA success probability and memory retrieval efficiency. Compare a repeaterless rate to a PLOB-type ceiling.

Academic Integrity and Plagiarism

a) Please consult the Faculty of Engineering and Design information page about the Academic Integrity policy and our procedures: <https://carleton.ca/engineering-design/current-students/fed-academic-integrity>. Violations of the Academic Integrity Policy will result in the assignment of a penalty such as reduced grades, the assignment of an F in a course, a suspension or, expulsion.

b) One of the main objectives of the Academic Integrity Policy is to ensure that the work you submit is your own. As a result, it is important to write your own solutions when studying and preparing with other students and to avoid plagiarism in your submissions. The University Academic Integrity Policy defines plagiarism as “presenting, whether intentionally or not, the ideas, expression of ideas or work of others as one’s own.” This includes reproducing or paraphrasing portions of someone else’s published or unpublished material, regardless of the source, and presenting these as one’s own without proper citation or reference to the original source.

Examples of violations of the policy include, but are not limited to:

- Any submission prepared in whole or in part, by someone else;
- Using another’s data or research findings without appropriate acknowledgment;
- Submitting a computer program developed in whole or in part by someone else, with or without modifications, as one’s own;
- Failing to acknowledge sources of information through the use of proper citations when using another’s work and/or failing to use quotations marks; and
- Unless explicitly permitted by the instructor in a specific course, the use of generative AI and similar tools to produce assessed content (such as text, code, equations, images, summaries, videos, etc.).

The instructor understands the benefits of AI use in learning and development. However, use of AI for the full generation of documents and text is not permitted. Students are required to disclose any AI use in their submitted use. Acceptable examples include: grammar and spelling checks, sentence clarity and obtaining deeper insight into course material that is justified by the student.

As our understanding of the uses of AI and its relationship to student work and academic integrity continue to evolve, students are required to discuss their use of AI in any circumstance not described here with the course instructor to ensure it supports the learning goals for the course.

Academic Accommodations

You may need special arrangements to meet your academic obligations during the term. For an accommodation request the processes are as follows:

Pregnancy obligation: Contact us with any requests for academic accommodation during the first two weeks of class, or as soon as possible after the need for accommodation is known to exist. For accommodation regarding a formally-scheduled final exam, you must complete the Pregnancy Accommodation Form ([click here](#)).

Religious obligation: Contact us with any requests for academic accommodation during the first two weeks of class, or as soon as possible after the need for accommodation is known to exist. For more details [click here](#).

Academic Accommodations for Students with Disabilities: The Paul Menton Centre for Students with Disabilities (PMC) provides services to students with Learning Disabilities (LD), psychiatric/mental health disabilities, Attention Deficit Hyperactivity Disorder (ADHD), Autism Spectrum Disorders (ASD), chronic medical conditions, and impairments in mobility, hearing, and vision. If you have a disability requiring academic accommodations in this course, please contact PMC at 613-520-6608 or pmc@carleton.ca for a formal evaluation. If you are already registered with the PMC, contact your PMC coordinator to send us your Letter of Accommodation at the beginning of the term, and no later than two weeks before the first in-class scheduled test or exam requiring accommodation (if applicable). After requesting accommodation from PMC, contact us, if needed, to ensure that accommodation arrangements are made.

You should request your academic accommodations in the [Ventus Student Portal](#), for each course at the beginning of every term. For in-term tests or midterms, please request accommodations at least two (2) weeks before the first test or midterm.

Please consult the [PMC website](#) for the deadline to request accommodations for formally-scheduled exams (if applicable).

Survivors of Sexual Violence: As a community, Carleton University is committed to maintaining a positive learning, working and living environment where sexual violence will not be tolerated, and where survivors are supported through academic accommodations as per Carleton's Sexual Violence Policy. For more information about the services available at the university and to obtain information about sexual violence and/or support, visit: <https://carleton.ca/equity/sexual-assault-support-services>

Accommodation for Student Activities: Carleton University recognizes the substantial benefits, both to the individual student and for the university, that result from a student participating in activities beyond the classroom experience. Reasonable accommodation will be provided to students who compete or perform at the national or international level. Contact us with any requests for academic accommodation during the first two weeks of class, or as soon as possible after the need for accommodation is known to exist: <https://carleton.ca/senate/wp-content/uploads/Accommodation-for-Student-Activities-1.pdf>