Course code and number, Fall 2011

UNIVERSITY OF CALGARY
DEPARTMENT OF PHYSICS and ASTRONOMY
COURSE OUTLINE

1. Phys 697, Topics in Contemporary Physics (Quantum Cryptography)

Lecture Sections:

L01: TuTh, 12:30-13:45, SS 105 **Wolfgang Tittel,** Office SB 315 Tel. No. 220-4760, wtittel@ucalgary.ca,
Office Hours: We 10:00-11:00, or after appointment

Departmental Office SB605, Tel. No. 220-5385, office@phas.ucalgary.ca

2. PREREQUISITES: N/A (Quantum Mechanics and linear Algebra, or consent of Instructor)

3. GRADING: The University policy on grading and related matters is described sections F.1 and F.2 of the online University Calendar. In determining the overall grade in the course the following weights will be used:

Assignments (10)	30%	
Midterm test (1)	20%	(Date will be communicated on the PHYS575 Blackboard site later in the term)
Presentation (1)	20%	
Final Examination (Oral)	30%	

Percentage grades will be given for all elements of term work and examinations. A weighted course percentage will be calculated for each student after the final exam. A table of conversion from final course percentage to final course letter grade will be published on the course Blackboard site later in the term.

4. Missed Components of Term Work. The regulations of the Faculty of Science pertaining to this matter are found in the Faculty of Science area of the Calendar in section 3.6: **http://www.ucalgary.ca/pubs/calendar/current/sc-3-6.html**. It is the student's responsibility to familiarize himself/herself with these regulations. See also **http://www.ucalgary.ca/pubs/calendar/current/e-3.html**.

5. REGULARLY SCHEDULED CLASSES HAVE PRECEDENCE OVER ANY OUT-OF-CLASS-TIME-ACTIVITY. If you have a clash with this out-of-class-time-activity, please inform your instructor as soon as possible so that alternative arrangements may be made for you.

6. TEXTBOOK: M.A. Nielsen & I.L. Chuang, Quantum Computation and Quantum Information, Cambridge University Press
Other reading:

- N. Gisin, G. Ribordy, W. Tittel , and H. Zbinden, Quantum Cryptography, Rev. Mod. Phys. 74, pp 145-195 (2002)
- V. Scarani, S. Iblisdir, and N. Gisin, Quantum Cloning, Rev. Mod. Phys. 77, pp. 1225-1256 (2005)
- Additional support will be provided during the lectures

7. EXAMINATION POLICY: [Statement regarding aids allowed on tests and examinations (e.g., calculator, open book, etc.).]
Students are encouraged to read the Calendar, Section G, on Examinations:
http://www.ucalgary.ca/pubs/calendar/current/g.html.

Department Approval_____ **Date**_____

Associate Dean's Approval for
out of regular class-time activity: _____ **Date:**_____

11. OTHER IMPORTANT INFORMATION FOR STUDENTS:

(a) ACADEMIC MISCONDUCT (cheating, plagiarism, or any other form) is a very serious offence that will be dealt with rigorously in all cases. A single offence may lead to disciplinary probation or suspension or expulsion. The Faculty of Science follows a zero tolerance policy regarding dishonesty. Please read the sections of the University Calendar under K. Student Misconduct (**http://www.ucalgary.ca/pubs/calendar/current/k.html**) to inform yourself of definitions, processes and penalties

(b) ASSEMBLY POINTS in case of emergency during class time. Be sure to FAMILIARIZE YOURSELF with the information at http://www.ucalgary.ca/emergencyplan/assemblypoints.

(c) ACADEMIC ACCOMMODATION POLICY. Students with documentable disabilities are referred to the following links:

Calendar entry on students with disabilities: **http://www.ucalgary.ca/pubs/calendar/current/b-1.html**
Disability Resource Centre: **http://www.ucalgary.ca/drc/**

(d) SAFEWALK: Campus Security will escort individuals day or night (**http://www.ucalgary.ca/security/safewalk/**). Call **220-5333** for assistance. Use any campus phone, emergency phone or the yellow phones located at most parking lot pay booths.

(e) FREEDOM OF INFORMATION AND PRIVACY: This course will be conducted in accordance with the Freedom of Information and Protection of Privacy Act (FOIPP). As one consequence**, students should identify themselves on all written work by placing their name on the front page and their ID number on each subsequent page**. For more information see also **http://www.ucalgary.ca/secretariat/privacy.**

(f) STUDENT UNION INFORMATION: VP Academic **Phone**: 220-3911 **Email**: suvpaca@ucagary.ca.
SU Faculty Rep. **Phone:** 220-3913 **Email:** sciencerep@su.ucalgary.ca Website **http://www.su.ucalgary.ca/home/contact.html**.
Student Ombudsman: **http://www.su.ucalgary.ca/services/student-services/student-rights.html**

(i) INTERNET and ELECTRONIC COMMUNICATION DEVICE Information. You can assume that in all classes that you attend, **your cell phone should be turned off**. Also, communication with other individuals, via laptop computers, Blackberries or other devices connectable to the Internet is not allowed in class time unless specifically permitted by the instructor. If you violate this policy you may be asked to leave the classroom. Repeated abuse may result in a charge of misconduct.

Course Syllabus

PHYS 697 - COURSE SYLLABUS

Quantum key distribution (QKD)

• Introduction to communication security, cryptography, and ciphers

• A brief review of quantum mechanics, including the description of single qubit states and composite systems (state and density matrix representation) and projection measurements

• Quantum key distribution, including error correction and privacy amplification

• Introduction to classical and quantum information theory, including Shanon and von Neuman entropy, mutual information

• Quantum cloning

• Eavesdropping (individual and coherent attacks)

• Implementations of QKD based on faint laser pulses or entangled states of light

• Side-channel attacks

• Squashing and device-independent QKD

If time permits: other (quantum) cryptographic primitives

• quantum bit commitment and coin flipping

• quantum private queries