**PHY 599**

**General Information**

* *Course title*: Quantum and Post Quantum Cryptography
* *Semester*: Spring 2022
* *Credit hours*: 3
* *Meeting time and location*: Physical Science – Room 111
* *Instructor*: Bertrand Cambou
* *Instructor email*: bertrand.cambou@nau.edu
* *Office location*: SICCS building, Room 110
* *Office hours*: Open – call 1(408)2031648 when absent

**Course Prerequisites**

One of the following: Elements of cryptography, nanotechnologies for cybersecurity, quantum physics and computing.

**Academic Catalog Description**

Study of emerging methods, techniques, and research areas in cryptography that use quantum effects for key distribution, and the study of novel asymmetrical cryptographic methods currently under development to protect cyber physical systems, which will mitigate attacks from quantum computers.

**Course Purpose**

This project-based course provides a study for graduate-level students interested in learning the limitations of asymmetrical cryptography, along with how post quantum cryptographic (PQC) algorithms have the potential to secure cyber physical systems, and government assets. The course is particularly appropriate as an elective for students in the APMS, MSEE, MSCS, and PHDINF programs. The program includes weekly lectures, lab hours, in-class discussion, in-class assignments, reading assignments, homework assignments, literature review of research projects, research project implementation and assessment, and research project papers and presentations. The first segment of the course’s objective is to introduce post quantum cryptography, an overview of quantum computing and quantum computers, Shor algorithm, and quantum key distribution (BB84, and multi-bit distribution). The second segment of the class presents the main PQC algorithms, and provides an update on the Post Quantum Cryptography effort driven by the National Institute of Standards and Technologies. Examples of algorithms are: lattice-based cryptography (NTRU, LWE, LWR,…); and code-based, and multivariate algorithms. By the end of the course, students will develop a better understanding of the challenges offered by PQC, hardware and software implementations, as well as the respective strengths and weaknesses of the various cryptographic methods when subject to attacks. The students will be able to engage in research efforts related to the emerging cryptographic methods presented in the course, in a variety of applications, in other research areas of interest in computer science, electrical engineering, informatics, and applied mathematics. This class encourage inter-discipline partnership, and teamwork.

**Student Learning Outcomes**

Upon successful completion of this course, students will be able to demonstrate the following advanced competencies:

* Analyze, evaluate, and articulate the general uses of emerging cryptographic methods in strengthening cybersecurity.
* Evaluate, select, and apply these emerging cryptographic algorithms to design and develop cybersecurity solutions for a variety of application domains; and
* The acquisition of a general understanding of the field to contribute to open research areas in cybersecurity.

As the future of quantum computers is speculative in nature, PQC algorithms will most likely replace the asymmetrical algorithms developed in the 80’s such as RSA, and ECC, therefore, the prime objective of PHY 599 is to prepare the students to thrive in such a fast moving technological environment.

**Course Structure**

This offering of PHY 599 will consist of lectures, lab hours, in-class assignments, homework assignments, scholarly literature reading assignments, and a multi-part development projects.

**Required Materials and Readings**

Recent technical publications on quantum computing, post quantum cryptography, and quantum key distribution will be provided.

**Recommended background information**

*Understanding Cryptography: A Textbook for Students and Practitioners* by Christof Paar, Jan Pelzl.(ISBN: 9783642041013).

**Course Outline**

For a more detailed outline, check the course schedule.

The course will start with the positioning of post quantum cryptography (PQC) as a potential replacement of mainstream asymmetrical cryptography, and will discuss the potential value of PQC even if quantum computers are not powerful enough to attack mainstream cryptographic schemes, such as RSA which are 40 year old, and to complex for ultra-light IoTs. As part of this positioning, the course will introduce the objectives of the PQC initiative of the National Institute of Standard and Technologies (NIST). The status of the development of quantum computers (QC), both in hardware and in software, will be presented, as well as examples of algorithms breaking mainstream asymmetrical cryptography such as the factoring algorithm developed by Peter Shor. Various Quantum Key Distribution (KQD) schemes using optical qubits will be studied such as BB84, and the schemes transmitting multiple quabit such as E91. Examples of research work done at NAU in the area of KQD will be discussed in the classroom. The course will then present in more detail the benchmark driven by NIST to evaluate various PQC algorithms (hash, code-based, multivariate, lattice, isogenies,..) for encryption, digital signature, and key encapsulation. Elements of mathematics needed for Lattice-based cryptography will also be presented (NTRU, LWE, ring-LWE, LWR) with an emphasis on encryption, and key encapsulation. As time permit, the course will summarize other PQC algorithms such as code-based, and multivariate. Finally, the respective figures of merits of PQC algorithms will be discussed: possibility to leverage software-hardware co-implementation and look up tables; efficiency of the algorithms in term of latency, and computing power; potential weaknesses when subject to crypto-analysis.

The agenda covered during the semester should be similar than the following (weekly schedules are approximate, and subject to minor changes):

1- Introduction to post quantum physics (week 1)

2- Overview quantum computing (week 2-3)

3- Crypto-analysis with QC (week 3)

4- Quantum key distribution (week 4-5)

5- Overview PQC (week 6)

6- Elements of mathematics for lattices (week 7)

7- Introducing lattice cryptography (week 8)

9- NTRU cryptography (week 9)

8- LWE cryptography (week 10-11)

9- Other PQC (week 12)

10- PUF-enhanced PQC (week 14-…)

**Assessment of Student Learning Outcomes**

Two types of methods are used to assess the learning of the students, the first one based on attendance, in-class and homework assignments represents 10% weight, the second that is based on student research projects represents 65%. The ability to prepare scientific reports represents 25% weight. In-class and reading assignments assess expertise in articulating and evaluating emerging cryptographic techniques; and homework assignments will assess student’s abilities to apply cryptographic and embedded software techniques. The multi-stage research project assesses the ability to identify, interpret, and explain open research questions in emerging cryptographic methods as well as the ability to design and apply solutions in developing secure systems.

**Grading System**

The weight of each course component toward your final grade is:

|  |  |
| --- | --- |
| **Assignment** | **Grade Weight %** |
| Homework assignments (To be presented within two working weeks) | 10% |
| Research project #1: Demonstrate understanding of the basic concepts | 30% |
| Research project #2: Demonstrate understanding of the advanced concepts | 35% |
| Final report on the projects | 15% |
| Final report on guest speakers | 10% |

Homework:

The students will have the opportunity to prepare homework asssignments. The objectives of the homework assignments are to summarize, and practice elements directly related to the class. This could be some mathematical computations, detailing examples presented in class, or finding additional examples similar to the ones presented. A good student should try to prepare most of the proposed homework.

Projects:

The first project assesses the student’s ability to select, describe, synthesize, and present material related to what is presented in class on a topic of their choice. Examples of successful projects include; programing a small example of Peter Shor factoring algorithm, or the development of a method showing how LWE (Learning With Errors) works. The students will be encouraged to present their projects in class, and to prepare small tutorials explaining the context, and bigger picture, of their projects. The objective of the second project will be to study a topic in more detail, present it in class, and prepare a final report on it. On demand, and when relevant, the students will have access to the cybersecurity lab to work on their projects. The students will have the latitude to pick their projects in line with their general area of expertise, and a list proposed by the instructor. The outcome could combine some programming work, and literature work demonstrating their understanding of the subject.

Grades will be awarded on the following scale:

|  |  |
| --- | --- |
| **Percentage Grade** | **Letter Grade** |
| 90% or above | A |
| 80% through 89% | B |
| 70% through 79% | C |
| 60% through 69% | D |
| 59% or below | F |

There is no "curve;" your grade is completely up to you and is not affected by the grades of your classmates. Extra credit opportunities may present themselves throughout the semester and be announced during class meetings. If you feel a mistake has been made in grading your assignment, please address your concerns during office hours.

*Northern Arizona University*

**Policy Statements for course syllabi**

[**http://nau.edu/Curriculum-and-Assessment/\_Forms/Curricular-Policy/Syllabus\_Policy\_Statements/**](http://nau.edu/Curriculum-and-Assessment/_Forms/Curricular-Policy/Syllabus_Policy_Statements/)