COURSE SYLLABUS

1 ECE 5170 - Introduction to Post-Quantum Computing

2 Meeting Information

3 credits, 3 contact hours Example: (Two 75-minute lectures)

a. **Section 001:**
Lecture: TR from 01:00 pm to 02:15 pm in Tolentine Hall 310A., **Tolentine Hall 310A**

3 Course Instructor(s), TA(s)

a. **Section 001:**
Class Instructor: Jiafeng Xie
Office Hours: Tuesday 3 to 5:00 PM or by appointment, conducted either in-person or by zoom (https://villanova.zoom.us/j/5501866845), or by appt.
TA: None

4 Textbook

This course does not have a prescribed textbook

a. **Other Supplemental Materials:** Introduction to Post-Quantum Cryptography (Chapters 1 and 2), D. Bernstein, 2009 (ebook).
Lattice-Based Public-Key Cryptography in Hardware (Chapters 2, 4, and 5), S. Roy and I. Verbauwhede, Springer, 2019 (ebook).

5 Specific Course Information

a. **Catalog Description**
Introduction to fundamental knowledge and skills related to quantum and post-quantum computing, basic and hands-on projects on different post-quantum cryptography schemes, brief introduction of emerging lightweight post-quantum techniques.

b. **Prerequisites:** ECE 2042 Fundamentals of CPE I (ECE 3450 Embedded Systems-II): VHDL or equivalent; ECE 1620 EGR Prog. And Applic. (C or equivalent); **Co-requisites:**

c. For CPE/EE undergraduate seniors (or similar level) who are interested in post-quantum computing

6 Learning Objectives

a. In light of the rapid advancement of quantum computing, this course is designed for students to be able to understand the fundamental knowledge related to quantum and post-quantum computing; learn the basic and hands-on projects based on different components (and extended to the whole system) of a lightweight post-quantum cryptography scheme on both software and hardware platforms; and catch up the trend of emerging post-quantum techniques., this course will also prepare the participants' future career in quantum/post-quantum field. Specifically,

1. Be able to collaborate and communicate with classmates for related projects.
2. Be able to familiar with basic working mechanism and operational feature of post-quantum schemes.
3. Be able to use coding languages (such as C and VHDL) to design a lightweight post-quantum cryptographic scheme on both software and hardware platforms.

b.

ABET Student Outcomes						
1	2	3	4	5	6	7
		X				

The above student outcomes are defined by the Accreditation Board for Engineering and Technology (ABET) as:

3. an ability to communicate effectively with a range of audiences

7 List of Covered Topics

1. Introduction to traditional cryptography
2. Introduction of quantum computing development
3. Post-quantum computing
4. Post-quantum lattice-based scheme (and a lightweight variant)
5. Implementation of post-quantum lightweight scheme (both software and hardware)
6. Future direction

8 Tentative Schedule

Tentative schedules for all sections follow. Be sure to refer to the schedule for your specific section, if more than one is provided.

Tentative Schedule for **All Sections**

Week	Topics	Assignment
1	Recall of traditional cryptography	1 paper review (tutorial
2	Introduction of quantum computing	1 paper review (tutorial
3	Post-quantum computing: theory and scheme foundation	1 paper review (tutorial
4	Binary Ring Learning-with-Errors: modular arithmetic, string, and rings	Homework 1: Software a
5	Matrix-vector product, polynomial ring, polynomial modular, and coefficient modular	Project 1: Software cod
6	Binary Binary Ring Learning-with-Errors based post-quantum encryption scheme	
7	Mid-term review and mid-term exam	
8	Hardware design technique, accumulation kernel	Project 2: Hardware co
9	Sign processing, sparse polynomial multiplier	Project 2: processing co
10	Arithmetic component and sign control-I	Project 3: Sign processi
11	Arithmetic component and sign control-II	
12	Module Learning-with-Errors, input processing component	Final Project: Input/ou
13	Output processing, polynomial addition, component connection, broken PQC	
14	Overall processing arithmetic, side-channel attacks, speed flexibility	

9 Grading Policy

Grading policy here

Letter grade scale: A(93–100), A–(90–92), B+(87–89), B(83–86), B–(80–82), C+(77–79), C(73–76), C–(70–72), D+(67–69), D(63–66), D–(60–62), F(<60)

Project/homework assignment: 45Paper review: 15Mid-Term Exam: 15Final Project: 20Attendance: 5

10 HW Assignment and Laboratory Report Submission Policy

The submission deadlines of assignments and project reports will be announced by the instructor. A late submission of an assignments will be not accepted unless the communication with the instructor. All the assignment submissions need to go through the Blackboard link.

11 Attendance Policy

The full version of the official Villanova class attendance policy is posted at https://live-villanova-catalog.cleancatalog.io/class-attendance, but the main points are as follows.

Class and laboratory attendance for first-year students is mandatory. A first-year student will receive a grade of "Y" (failure) whenever the number of unexcused absences in a course exceeds twice the number of weekly class meetings for the course. State here if attendance is mandatory or not for your class. Provide a description of what it means to be present (seated and ready to go, just in the room, camera on if virtual, be explicit).

Where possible, students should inform their instructors if they plan to be late or absent from class. In all cases, students should be prepared to provide documentation to petition for excused absences to the Associate Dean for Student and Strategic Programs, Dr. Stephen Jones. Students should use the form for requesting an excused absence. Excused absences do not count toward a failure in the course for first year students. Absence from class does not release the student from work assigned. Students who miss an in-class obligation (exam, presentation, etc.) due to an excused absence will not be penalized - the instructor may offer a make-up test, arrange an alternative time for a presentation, exempt a student from the assignment, or provide another arrangement. In the case of illness or injury, the form must be submitted within 24 hours of missing class.
The University's list of excused absences for all students includes the following:
• participation in NCAA athletic competitions
• participation in special academic events (e.g., conferences, field trips, project competitions)
• participation in official university business (e.g., student representatives attending meetings related to university governance)
• attendance at significant events involving the immediate family (e.g., funerals, weddings)
• religious holidays - see the University's policy on Religious Holidays
• college-approved participation in placement activities (e.g., job interviews, graduate school interviews, attending job fairs)
• legally required absence (jury duty, court appearance, short-term military service)
• documented serious illness, such as COVID, or disability

Whenever possible, students should inform the instructor if they plan to be late or absent from class. In all cases, documentation is required to petition for *excused* absences to the Associate Dean for Student and Strategic Programs, Dr. Stephen Jones. The excused absence form is posted at: https://forms.office.com/r/H2kbHKLUmw.

Excused absences do not count towards a failure in the course for first year students. Absence from class does not release the student from assigned work. Students who miss an in-class obligation such as an exam, a presentation, etc., due to an excused absence will not be penalized - the instructor may offer a make-up test, arrange an alternative time for a presentation, exempt a student from the assignment, or provide another arrangement. In the case of illness or injury, the form must be submitted within 24 hours of missing a class. The University's list of excused absences for all students includes the following:

1. Participation in NCAA athletic competitions
2. Participation in special academic events such as: conferences, field trips, project competitions, etc., and in official university business such as student representatives attending meetings related to university governance
3. Attendance at significant events of the immediate family such as: funerals, weddings, etc.
4. Religious holidays - see the University's policy on Religious Holidays
5. College-approved participation in placement activities such as: job interviews, graduate school interviews, job fairs
6. Legally required absence such as: jury duty, court appearance, short-term military service
7. Documented serious illness or disability

12 Examination Policy

The College of Engineering has adopted the following general examination guidelines:

1. Students must arrive before the start of the examination. Under exceptional circumstances a student may need to arrive late, but he/she can enter the examination room no later than five (5) minutes after the start of the exam.
2. Cell phones must be turned off until the student exits the examination room.
3. The official Villanova class attendance policy must be followed when requesting excuses for absences or lateness to an examination.
4. Each student must write and sign the following statement, "I have neither given nor received any unauthorized assistance in the completion of this examination."
5. For online examinations, the instructor may implement video proctoring or other measures to ensure academic integrity. For consent purposes, the instructor will inform students in advance if (s)he plans to use any form of video-proctoring and whether the examination will be recorded.

13 Academic Integrity Policy

The College of Engineering is committed to creating an environment of academic integrity and ethical decision-making that we hope is reflected in the actions of our students and graduates. As Villanova students, integrity is central to the University mission. As engineers, our code of conduct requires us to place honor and integrity at the forefront of everything we do. As engineering students, it is expected that you will begin to adopt these values and instill them into your work habits. Students violating the academic integrity policy will receive a zero on that assignment or exam and the violation will be reported to the Associate Dean for Academic Affairs. The University's academic integrity policy can be found on the following web page:
https://live-villanova-catalog.cleancatalog.io/academic-integrity-0.

14 Adherence to the Student Code of Conduct

Students are expected to act in a professional and respectful manner to their fellow students, faculty, and staff. Students should become acquainted with and understand the responsibilities set forth in the Student Handbook, especially those in the sections on Policy and Regulations. Adherence to university regulations is expected and required for successful completion of the program of studies. Enforcement within the classroom of policies regarding classroom behavior is the responsibility of the faculty member. All other discipline problems are to be referred to the Dean of Students.

15 Inclusive Classroom

This classroom is a place where you will be treated with respect; we welcome individuals of all ages, backgrounds, beliefs, ethnicities, gender, gender identities and expressions, sexual orientation, and other visible and non-visible differences. All members of this class are expected to contribute to a respectful, welcoming, and inclusive environment to allow all among us to learn and flourish.

16 Students with Disabilities

It is the policy of the university to make reasonable academic accommodations for qualified individuals with disabilities. If you are a person with a disability (non-physical) please register with the office of Learning Support Services (LSS) by emailing Learning.support.services@villanova.edu

or by phoning 610-519-5176 as soon as possible. Registration is *required* in order to receive accommodations. In addition, please contact the instructor during office hours in order to make the appropriate arrangements.

The Office of Disability Services (ODS) collaborates with students, faculty, staff, and community members to create diverse learning environments that are usable, equitable, inclusive and sustainable. The ODS provides Villanova University students with physical the necessary support to successfully complete their education and participate in activities available to all students. If you have a diagnosed disability and plan to utilize academic accommodations, please contact and register with Gregory Hannah, advisor to students with disabilities at 610-519-3209 or visit the office on the second floor of the Connelly Center.

17 Tutoring Services

Villanova's tutoring services include The Writing Center, The Learner's Studio, and The Center for Speaking and Presentation. These services are offered free of charge to students. Drop in as-needed or book a regular weekly session to supercharge your academic success. Sessions can be 30 or 60 minutes in length.

Register for an account and book sessions in advance at villanova.mywconline.com. If you don't see your class listed, request a tutor for a missing subject at: tutorrequest.villanova.edu For more information, contact Juliana Struder at juliana.studer@villanova.edu or at 610-519-5862.

18 Online Expectations

Some or all sessions of this class may be recorded for educational purposes and for later playback. In order to foster a professional environment, please wear appropriate clothes, refrain from eating, mute your microphone if you are not talking to eliminate background noise and select an appropriate setting free of distractions. You may turn off your webcam for privacy reasons unless explicitly instructed not to do so by the instructor (such as during the conduct of online examinations).

19 Electronics Policy

The use of electronic devices, such as phones, laptops, tablets, calculators, etc., during class is generally allowed, unless their use causes a disturbance to others. During examinations, the use of any electronic device is prohibited, unless it is expressly authorized by the instructor.

Students are prohibited from making any audio or visual recordings (including taking photographs) of lectures, discussions, or other classroom activities, unless a student (1) has written permission in advance from the instructor, or (2) is permitted to record under terms and conditions as approved by the University's Office of Disability Services or Learning Support Services. Students who have received approval to record classes as an academic accommodation must provide supporting documentation from the Office of Disability Services or Learning Support Services in advance of any recording. Students may use authorized recordings only for the purposes of individual study in the course, and may not disseminate or share them with a wider audience without explicit permission.

20 Copyright Policy

The materials used in Villanova University courses ("Course Materials") generally represent the intellectual property of course instructors, third parties and/or the university which may not be disseminated or reproduced in any form for public distribution (e.g., sale, exchange, etc.) without

the written permission of the course instructor. Course materials include all written or electronic documents and materials, including syllabi, current and past examination questions/answers, and presentations such as lectures, videos, slides, etc., provided by a course instructor. Course materials may only be used by students enrolled in the course for academic (course-related) purposes.

Published course readings (book chapters, articles, reports, etc.) available in "Blackboard" are copyrighted materials. These works are made available to students through licensed databases or fair use. They are protected by copyright law, and may not be further disseminated or reproduced in any form for distribution (e.g. uploading to websites, sale, exchange, etc.) without the permission of the copyright owner.

Follow these links for more information on Intellectual Property, Copyright, and Computer Acceptable Use.

21 Professorial Duties

It is important to note that teaching is one of the many duties that professors perform as part of their job responsibilities. In addition to teaching, professors perform research, advise graduate students, edit journals and review journal articles, serve on committees for the university and professional societies, travel to conferences to remain abreast of current developments and to present their results... to name just a few commitments.