COURSE SYLLABUS

1 ECE 8481 - Post-Quantum Cryptographic Engineering

2 Meeting Information

3 credits, 3 contact hours One 150-minute lecture

a. **Section 001:**
Lecture: Mfrom 06:15 pm to 08:45 pm in Drosdick Hall ., **CEER 212**

b. **Section DL1:**
Lecture: Mfrom 06:15 pm to 08:45 pm in Online SYN.,

3 Course Instructor(s), TA(s)

a. **Section 001:**

Class Instructor:	Jiafeng Xie
Office Hours:	Thursday 2-4PM, or by appt.
TA:	None

b. **Section DL1:**

Class Instructor:	Jiafeng Xie
Office Hours:	Thursday 2-4PM, or by appt.
TA:	None

4 Textbook

This course does not have a prescribed textbook

a. **Other Supplemental Materials:**
Recommended:

Lattice-Based Public-Key Cryptography in Hardware, S. Roy and I. Verbauwhede, Springer, 2019 (ebook downloadable).

References:

Hardware Implementation of Finite Field Arithmetic, Jean P. Deschamps et. al., McGraw, 2009.

Introduction to Post-Quantum Cryptography, Post-quantum cryptography, D. Bernstein, 2009 (ebook downloadable).

Course slides (important)

5 Specific Course Information

a. **Catalog Description**
Basic foundation of the post-quantum crypotographic engineering and recent advances in the field; introduces design and implementation techniques for the arithmetic unit and overall post-quantum cryptography on both hardware and software platforms, and side-channel attack skills.

b. **Prerequisites:** None; **Co-requisites:** None

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

6 Learning Objectives

a. Be able to understand the basic foundation of the post-quantum cryptography and recent advances in the field; equip the learners with the ability to design and implement simple version of the basic arithmetic unit (post-quantum cryptography) on both hardware and software platforms. More importantly, prepare course participants for their future career in the coming quantum era. Specifically,

1. Be able to collaborate and communicate with classmates for projects and tasks.

2. Be able to familiar with basic post-quantum cryptosystem design process: use both hardware and software synthesis tools to design the main post-quantum cryptographic arithmetic operations.

3. Be able to understand the idea of system constraints and requirements like processing time, resource occupation & cost, and size along with the possible trade-off considerations

7 List of Covered Topics

1. Introduction of pre- and post-quantum cryptography
2. Introduction of lattice-based scheme (arithmetic operations)
3. Introduction of cryptographic hardware circuits: polynomial multiplication
4. Other components within lattice-based scheme
5. Implementation of simple post-quantum scheme (sampler and modular reduction)
6. Lattice-based Ring-LWE scheme (data flow optimization)
7. Post-quantum cryptoprocessor (introduction-I)
8. Post-quantum cryptoprocessor (introduction-II)
9. System-level building & testing
10. Unified processor
11. Introduction of digital signature scheme
12. Introduction of side-channel attacks

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**

Month	Week/Date	Course Topic	Assignment
August	Week-1 8/28	Introduction	
September	Week-2 9/11	Arithmetic operations	HW 1: point-wise multiplier
September	Week-3 9/18	Hardware polynomial multiplication	Paper review
September	Week-4 9/25	Other components	Project 1: hardware NTT
October	Week-5 10/2	Mid-term exam	
October	Week-6 10/9	Break	
October	Week-7 10/16	Sampler and reduction	Project 2: sampler
October	Week-8 10/23	Data flow optimization	
October	Week-9 10/30	Cryptoprocessor-I	HW 2: system-level data flow
November	Week-9 11/6	Cryptoprocessor-II	
November	Week-10 11/13	System-level building	Final project: PQCryptoprocessor
November	Week-11 11/20	Unified processor	
November	Week-12 11/27	Digital signature scheme	
December	Week-13 12/4	Side-channel attacks	
December	Week-14 12/11	Recent advances	

9 Grading Policy

Your final grade will be determined from the following:

- Project/homework assignment: 60% (4 project/homework assignments, each 15 points)
- Paper review: 10% (2 technical paper review assignments, each 5 points)
- Mid-Term Exam: 10%
- Final Project: 20%

Letter grade scale: A(90–100), A–(87–89), B+(83–86), B(80–82), B–(77–79), C+(73–76), C(70–72), C–(67–69), D+(63–66), D(61–62), D–(60)F(<60)

10 HW Assignment and Laboratory Report Submission Policy

Homework and Project must be submitted according to the designated timeline. LATE SUBMISSION WILL NOT BE ACCEPTED. Your homework should be neat and with your full name on.

11 Attendance Policy

General Rules

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.

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

Personal Days

Personal Days are NOT allotted for laboratory sessions and courses that meet once a week. For all other courses that meet at least twice a week, students are entitled to excused absences for any reason that may contribute to their personal wellness. The following rules apply.

Students must advise the instructor by email *before* class of their intent to utilize a Personal Day as the reason for their absence. A Personal Day will not be approved retroactively. Students may, but are not required, to provide additional information regarding their absence. A Personal Day does not grant an automatic extension for items due. Students remain responsible for all assignments, exams, presentations, etc. due on that date. The instructor may apply her/his discretion on a case-by-case basis to determine whether an extension on a deliverable item is appropriate.

For classes that meet thrice a week (50 mins $\times$ 3), TWO personal days are allowed in the semester. These personal days may not be used ...

1. on consecutive class days
2. in the same week
3. immediately preceding or following a University holiday or break period, and
4. on days when exams, presentations or other major assignments are scheduled.

For classes that meet twice a week (75 mins $\times$ 2), ONE personal day is allowed in the semester. This personal day may not be used ...

1. immediately preceding or following a University holiday or break period, and
2. on days when exams, presentations or other major assignments are scheduled.

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 when you are not talking so as 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.