


 <b>FLORIDA ATLANTIC UNIVERSITY</b>	<b>NEW COURSE PROPOSAL</b> <b>Undergraduate Programs</b>		UUPC Approval <u>10/9/2023</u> UFS Approval _____ SCNS Submittal _____ Confirmed _____ Banner Posted _____ Catalog _____
	<b>Department</b> Mathematical Sciences  <b>College</b> Science <i>(To obtain a course number, contact <a href="mailto:erudolph@fau.edu">erudolph@fau.edu</a>)</i>		
<b>Prefix</b> MAD  <b>Number</b> 4475	<i>(L = Lab Course; C = Combined Lecture/Lab; add if appropriate)</i>  <b>Lab Code</b>	<b>Type of Course</b> <div style="border: 1px solid red; padding: 2px;">Lecture</div>	<b>Course Title</b> Post-Quantum Cryptography
<b>Credits</b> <i>(See Definition of a Credit Hour)</i> 3	<b>Grading</b> <i>(Select One Option)</i>  <b>Regular</b> <input checked="" type="radio"/>  <b>Sat/UnSat</b> <input type="radio"/>	<b>Course Description</b> <i>(Syllabus must be attached; see <a href="#">Template</a> and <a href="#">Guidelines</a>)</i>  This course provides an introduction to quantum-resistant cryptographic schemes: their underlying mathematical problems, formalisms, and constructions, with a focus on the computational aspects. Topics include code-based cryptography, lattice-based cryptography, isogeny-based cryptography, and multivariate-based cryptography.	
<b>Effective Date</b> <i>(TERM &amp; YEAR)</i> Spring 2024	<b>Prerequisites, with minimum grade*</b> MAS 2103 Matrix Theory and COP 2220 Programming I, with a grade of C or better.		<b>Corequisites</b>  <b>Registration Controls</b> <i>(Major, College, Level)</i>
<b>*Default minimum passing grade is D-. Prereqs., Coreqs. &amp; Reg. Controls are enforced for all sections of course</b>			
<b>WAC/Gordon Rule Course</b>  <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No  <small>WAC/Gordon Rule criteria must be indicated in syllabus and approval attached to proposal. See <a href="#">WAC Guidelines</a>.</small>		<b>Intellectual Foundations Program (General Education) Requirement</b> <i>(Select One Option)</i>  None  <small>General Education criteria must be indicated in the syllabus and approval attached to the proposal. See <a href="#">Intellectual Foundations Guidelines</a>.</small>	
<b>Minimum qualifications to teach course</b> Phd in Mathematics or related fields.			
<b>Faculty Contact/Email/Phone</b> Francesco Sica / sica@fau.edu / 561-297-3340		<b>List/Attach comments from departments affected by new course</b> Request for comments sent to Dept EECS on 9/20/2023	
<b>Approved by</b> Department Chair <u></u> College Curriculum Chair <u></u> College Dean <u></u> UUPC Chair <u>Korey Sorge</u> Undergraduate Studies Dean <u>Dan Meeroff</u> UFS President _____ Provost _____			<b>Date</b> _____ 09/21/2023 9/26/23 <u>9/26/23</u> 10/9/2023 10/9/2023 _____ _____

Email this form and syllabus to [mianning@fau.edu](mailto:mianning@fau.edu) seven business days before the UUPC meeting.

MAD 4475

**Post-Quantum Cryptography**

Tu 10:00 – 11:20, Th 10:00-11:20

3 credits

Spring, 2024

Dr. Shi Bai



TA name	Francesco Sica
Office	SE43- room xx
Office hours	TT xx:xx – xx:xx
Telephone	561-297-xxxx

### Course Description

This course provides an introduction to quantum-resistant cryptographic schemes: their underlying mathematical problems, formalisms, and constructions, and with a focus on the computational aspects. Topics include code-based cryptography, lattice-based cryptography, isogeny-based cryptography, and multivariate-based cryptography.

Most currently deployed cryptosystems will be vulnerable to powerful quantum computers. As a result, it is critical to base encryption on new mathematical problems that are resistant to quantum attackers. This course introduces post-quantum cryptography algorithms, covering the following topics:

- Mathematical foundations of cryptography
- Code-based cryptography
- Lattice-based cryptography
- Isogeny-based cryptography
- Multivariate-based cryptography

**Instructional Method:** In-Person

**Type of Course:** Lecture

**WAC/Gordon Rule Course:** No

**IFP course:** No

**Prerequisites/Corequisites:**

MAS 2103. Matrix Theory AND COP 2220 Programming I , with a grade of “C” or better. Or permission of the instructor.

**Course Objectives/Student Learning Outcomes**

The course provides an introduction to the mathematical foundations of post-quantum cryptography, as well as standard post-quantum cryptographic protocols. At the end of the course, students should be acquainted with the concepts of code-based cryptography, lattice-based cryptography, isogeny-based cryptography and multivariate-based cryptography.

**Required Textbook**

The course will not be based on a specific textbook. Course materials will be provided on Canvas for the class. We will also use some chapters of the following survey papers (which are freely available online) :

“A Decade of Lattice Cryptography” by Chris Peikert. <https://eprint.iacr.org/2015/939.pdf>

“A Survey on Code-Based Cryptography” by Violetta Weger, Niklas Gassner, Joachim Rosenthal. <https://arxiv.org/abs/2201.07119>

## Course Evaluation Method

The grade for the course will be determined by the following scheme:

Four Homework (20%), Mid-Term Exam (40%), Term Project (40%).

**Assignments:** There will be 4 homework for the course, each of which counts for 5% of the grade. Homework should be clearly handwritten or printed on paper or sent by email in PDF format. Late assignments will not be accepted and graded with 0 points.

**Mid-Term Exam:** Mid-Term exam counts for 40% of the final grade.

**Term Project:** A research project will be given for each student, which counts for 40% of the final grade. The purpose is to develop students' understanding of the current state-of-the-art of the research in post-quantum cryptography. In the beginning of the semester, a list of research papers will be given. Each student must choose one item in the list and study the paper. Additional research paper (other than from the given list) may be acceptable after discussion with the instructor, but each paper must be relevant to the course content. The evaluation of the project consists of two components:

- A report (e.g. 5-8 pages) summarizing the main techniques of the research paper. The report counts for 50% of the total grade.
- An oral exam (45 minutes). The examiners will ask questions on your report; on your understanding of the technical contents of the research paper; and also relevant materials that cover the topics taught during the semester. The oral

exam counts for 50% of the total grade. The time of the oral exam will be during the exam week. The report should be submitted prior to the oral exam.

### Grading scale

At the end of the semester, the following scale for FAU grade will be used.

Total Point s	87- 100	83- 86	77- 82	73- 76	70- 72	67- 69	63- 66	60- 62	57- 59	53- 56	50- 52	<50
Grade	A	A-	B+	B	B-	C+	C	C-	D+	D	D-	F

**Make-up Policies on Exams/Tests:** If you miss an exam, you must provide a written, verifiable excuse, if possible, in advance of the scheduled exam. Doctor notes, letters, emails from immediate family members are not accepted as proof of absence from any exams. Approval for a make-up exam must be obtained from your instructor.

**Special Course Requirements:** Students are expected to be familiar and comply with the standard university policies. In addition, the following policies on assignments should be confirmed.

**Collaboration policy on assignments:** Collaboration on the assignments is permitted for this course. If you do collaborate, your write-ups must be done independently, and you must acknowledge your collaborators in your write-up. Failure to do so constitutes plagiarism.

**Policy on the Recording of Lectures:** Students enrolled in this course may record video or audio of class lectures for their own personal educational use. A class lecture is defined as a formal or methodical oral presentation as part of a university course intended to present information or teach students about a particular subject. Recording class activities other than class lectures, including but not limited to student presentations (whether individually or as part of a group), class discussion (except when incidental to and incorporated within a class lecture), labs, clinical presentations such as

patient history, academic exercises involving student participation, test or examination administrations, field trips, and private conversations between students in the class or between a student and the lecturer, is prohibited. Recordings may not be used as a substitute for class participation or class attendance and may not be published or shared without the written consent of the faculty member. Failure to adhere to these requirements may constitute a violation of the University's Student Code of Conduct and/or the Code of Academic Integrity.

**Attendance Policy:** Students are expected to attend all of their scheduled University classes and to satisfy all academic objectives as outlined by the instructor. The effect of absences upon grades is determined by the instructor, and the University reserves the right to deal at any time with individual cases of non-attendance. Students are responsible for arranging to make up work missed because of legitimate class absence, such as illness, family emergencies, military obligation, court-imposed legal obligations or participation in University-approved activities. Examples of University-approved reasons for absences include participating on an athletic or scholastic team, musical and theatrical performances and debate activities. It is the student's responsibility to give the instructor notice prior to any anticipated absences and within a reasonable amount of time after an unanticipated absence, ordinarily by the next scheduled class meeting. Instructors must allow each student who is absent for a University-approved reason the opportunity to make up work missed without any reduction in the student's final course grade as a direct result of such absence.

### **Counseling and Psychological Services (CAPS) Center**

Life as a university student can be challenging physically, mentally and emotionally. Students who find stress negatively affecting their ability to achieve academic or personal goals may wish to consider utilizing FAU's Counseling and Psychological Services (CAPS) Center. CAPS provides FAU students a range of services – individual counseling, support meetings, and psychiatric services, to name a few – offered to help improve and maintain emotional well-being. For more information, go to <http://www.fau.edu/counseling/>

### **Disability Policy**

In compliance with the Americans with Disabilities Act Amendments Act (ADAAA), students who require reasonable accommodations due to a disability to properly execute coursework must register with Student Accessibility Services (SAS) and follow all SAS procedures. SAS has offices across three of FAU's campuses – Boca Raton, Davie and Jupiter – however disability services are available for students on all campuses. For more information, please visit the SAS website at [www.fau.edu/sas/](http://www.fau.edu/sas/).

### **Code of Academic Integrity**

Students at Florida Atlantic University are expected to maintain the highest ethical standards. Academic dishonesty is considered a serious breach of these ethical standards, because it interferes with the university mission to provide a high quality education in which no student enjoys an unfair advantage over any other. Academic dishonesty is also destructive of the university community, which is grounded in a system of mutual trust and places high value on personal integrity and individual responsibility. Harsh penalties are associated with academic dishonesty. For more information, see [University Regulation 4.001](#).

If your college has particular policies relating to cheating and plagiarism, state so here or provide a link to the full policy—but be sure the college policy does not conflict with the University Regulation.



## Course Tentative Outline

### Mathematical foundation of post-quantum cryptography

**Week 1:** mathematical background (linear algebra, algebraic structures)

**Week 2:** computational complexity and cryptography

**Week 3:** introduction to computational number theory

### Code-based cryptogrphay

**Week 4:** linear codes, random codes, intractable problems

**Week 5:** code-based schemes: McEliece, BIKE etc.

**Week 6:** cryptanalysis, information set decoding algorithms

### Lattice-based cryptogrphay

**Week 7:** lattices, worst-case hardness and average-case hardness problems

**Week 8:** trapdoors and applications

**Week 9:** lattice-based schemes, encryption and signature: Kyber, Dilithium etc.

### **Isogeny-based cryptography**

**Week 10:** basics on elliptic curves

**Week 11** supersingular isogeny Diffie-Hellman protocol

**Week 12:** bruteforce attack, Kani's theorem

### **Multivariate-based cryptography**

**Week 13:** multivariate quadratic problem

**Week 14:** encryption schemes, oil and vinegar (UOV) etc.

**Week 15:** cryptanalysis of multivariate problem