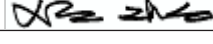


 FLORIDA ATLANTIC UNIVERSITY	NEW COURSE PROPOSAL Graduate Programs		UGPC Approval _____ UFS Approval _____ SCNS Submittal _____ Confirmed _____ Banner _____ Catalog _____	
	Department Mathematics and Statistics College Science (To obtain a course number, contact erudolph@fau.edu)			
Prefix MAD Number 6515	(L = Lab Course; C = Combined Lecture/Lab; add if appropriate) Lab Code	Type of Course Lecture	Course Title Mathematical Foundations of Post-Quantum Cryptography	
Credits (See Definition of a Credit Hour) 3	Grading (Select One Option) Regular ☒ Sat/UnSat ☐	Course Description (Syllabus must be attached; see Template and Guidelines) This course explores the field of post-quantum cryptography, focusing on cryptographic algorithms designed to resist quantum attacks. The curriculum covers a selection of the following main areas of post-quantum cryptography: lattice-based, code-based, isogeny-based, multivariate, and hash-based cryptography, with a strong emphasis on their mathematical foundations.		
Effective Date (TERM & YEAR) Spring 2026				
Prerequisites Graduate standing or permission of instructor <i>Prerequisites, Corequisites and Registration Controls are enforced for all sections of course.</i>		Academic Service Learning (ASL) course ☐ Academic Service Learning statement must be indicated in syllabus and approval attached to this form.		
		Corequisites	Registration Controls (For example, Major, College, Level)	
Minimum qualifications needed to teach course: Member of the FAU graduate faculty and has a terminal degree in the subject area (or a closely related field).		List textbook information in syllabus or here Post-quantum cryptography, Daniel J. Bernstein, Johannes Buchmann, Erik Dahmen. Springer, 2009. ISBN: 978-3-540-88701-0 Supplementary notes will be provided weekly.		
Faculty Contact/Email/Phone Veronika Kuchta / vkuchta@fau.edu		List/Attach comments from departments affected by new course Department of Electrical Engineering and Computer Science		

Approved by Department Chair  College Curriculum Chair  College Dean  UGPC Chair _____ UGC Chair _____ Graduate College Dean _____ UFS President _____ Provost _____	Date 09/22/2025 9/22/2025 9/22/2025 _____ _____ _____ _____ _____
--	--

Email this form and syllabus to UGPC@fau.edu 10 days before the UGPC meeting.



MAD 6515
Mathematical Foundations of Post-Quantum Cryptography

Department of Mathematics and Statistics
Spring 2026
3 Credit Hours

Instructor:
Office Location:
Office Hours:
Phone Number:

Course Description

This course explores the field of post-quantum cryptography, focusing on cryptographic algorithms designed to resist quantum attacks. The curriculum covers a selection of the following main areas of post-quantum cryptography: lattice-based cryptography, code-based cryptography, isogeny-based cryptography, multivariate cryptography, and hash-based cryptography, with a strong emphasis on their mathematical foundations.

Instructional Method

In-person.

Prerequisites/Corequisites

Mathematical maturity appropriate to fourth year undergraduate or first year graduate student status.

Course Objectives/Student Learning Outcomes

Upon successful completion of this course, students will be able to:

1. Understand the challenges quantum computing poses to existing cryptographic methods.

2. Analyze the mathematical foundations of lattice-based, code-based, multivariate, and hash-based cryptographic schemes.
3. Learn how to construct quantum resistant cryptographic schemes.
4. Evaluate the security and efficiency trade-offs of PQC algorithms.
5. Critically read and analyze cryptographic research writing.

Required Texts/Readings

Textbook: *Post-quantum cryptography*, Daniel J. Bernstein, Johannes Buchmann, Erik Dahmen, Springer, 2009. ISBN: 978-3-540-88701-0

The book was published during a pivotal time when quantum computing was gaining momentum. Authored by renowned experts, it helped define the mathematical challenges and directions for future research. It remains a foundational text for understanding how mathematics is used to build quantum-resistant systems.

Supplementary/Recommended Readings

Supplementary reading material will be provided on a weekly basis.

Course Topical Outline

Week #	Lecture content
Week 1	Overview of public-key cryptography and attacks on discrete logarithm problem and factorization (Shor's and Grover's algorithm, NIST competition)
Week 2	Introduction to post-quantum cryptography
Week 3	Lattice-based cryptography: mathematical background (linear algebra, Gaussian distribution, lattices)
Week 4	Lattice-based cryptography: lattice-based hard problems (SIS, LWE)
Week 5	Lattice-based cryptography: Regev encryption, ring-SIS, ring LWE
Week 6	Lattice-based cryptography: signature scheme, fully homomorphic encryption, security analysis
Week 7	Code-based cryptography: mathematical background (linear codes, finite fields, and error-correcting codes.)
Week 8	Code-based cryptography: code-based hard problems,
Week 9	Code-based cryptography: code-based cryptosystems, McEliece cryptosystem, security analysis
Week 10	Code-based cryptography: HQC cryptosystem, security analysis
Week 11	Multivariate public key cryptography: mathematical background (polynomial systems, multivariate quadratic (MQ) problem)
Week 12	Multivariate public key cryptography: hard problems and cryptographic constructions (UOV cryptosystem), security analysis
Week 13	Multivariate public key cryptography: cryptographic constructions, Rainbow cryptosystem, security analysis

Week 14	Hash-based cryptography: one-time signature
Week 15	Hash-based cryptography: Merkle signature (XMSS)

Course Evaluation Method

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

Quizzes (25%), Midterm Exam (30%), Project (15%), Final Exam (30%).

Quizzes: Regular quizzes are conducted weekly, lasting 15-20 minutes, covering specific topics for that week. They count for 25% of the final grade.

Midterm Exam: The midterm exam counts for 30% of the final grade.

Group Project: A research project on post-quantum cryptography, conducted in groups of up to 5 students. Each group selects one research paper from a provided list. Papers outside the list may be considered after instructor's approval, provided they are relevant to the course.

Components of the Project:

-*Report* (e.g. 5-10 pages) summarizing the main techniques of the research paper.

-*Group presentation (20-30 minutes)*. After the presentation, the examiner will ask questions on your report, on your understanding of the technical content of the research paper.

The group project counts for 15% of the final grade.

Final exam: The final exam will cover the totality of the syllabus. It counts for 30% of the final grade.

Bonus Opportunity: Active participation in class (e.g., volunteering to go to the board or helping peers with exercise solutions) can earn up to **5% bonus points** toward the final course grade.

Grading scale

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

Total points	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 a quiz, 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 quizzes. Approval for a make-up quiz 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 group project is permitted and recommended for this course.

Policy on the Recording of Lectures

Because of a new Florida Statute in 2021, the following model language is suggested for inclusion in course syllabi, at the discretion of individual faculty: 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/.

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.

Subject: Re: a few items
From: Hari Kalva <hkalva@fau.edu>
Date: 9/8/2025, 2:00 PM
To: Yuan Wang <YWANG@fau.edu>

Hi Yuan, we support all the three proposed items:

- a revision of the Math track of the Cyber Security Graduate Certificate by adding a few elective courses in the Math course list
- a proposal of new graduate course Mathematical Foundation of Post-Quantum Cryptography
- a proposal of new graduate course Mathematics for Artificial Intelligence (primary audience will be teachers in mathematics)

I will take care of CAP 5768 for Spring 26.

Thank you.

From: Yuan Wang <YWANG@fau.edu>
Sent: Sunday, September 7, 2025 2:50 PM
To: Hari Kalva <hkalva@fau.edu>
Subject: Re: a few items

Dear Hari,

I'm very sorry, but I attached in my previous email a wrong version the course proposal for Math Foundation of Post-Quantum Cryptograhpy so the syllabus was missing. Please use the file in this email.

For your convenience, I'm including the other two attached files in this email.

Thank you.
Yuan

On 9/7/2025 1:59 PM, Yuan Wang wrote:

Dear Hari,

I hope all has been going well with you.

I have a few items for your attention:

- For Spring 2026, we do not plan to offer a section of CAP 5768. Could you please

cancel or hold CAP 5768-001, under Chang? We plan to offer a section in Spring 2027. I hope this is okay with you.

- I'm seeking your support on the following:
 - a revision of the Math track of the Cyber Security Graduate Certificate by adding a few elective courses in the Math course list
 - a proposal of new graduate course Mathematical Foundation of Post-Quantum Cryptography
 - a proposal of new graduate course Mathematics for Artificial Intelligence (primary audience will be teachers in mathematics)

The proposals, including the course syllabus, are attached. Your feedback and support would be greatly appreciated!

Thank you.

Yuan