## FLORIDA ATLANTIC UNIVERSITY

### Graduate Programs — NEW COURSE PROPOSAL

<table>
<thead>
<tr>
<th>RECOMMENDED COURSE IDENTIFICATION:</th>
<th>COLLEGE: COLLEGE OF ENGINEERING AND COMPUTER SCIENCE</th>
</tr>
</thead>
<tbody>
<tr>
<td>PREFIX: COT</td>
<td></td>
</tr>
<tr>
<td>COURSE NUMBER: 6116</td>
<td></td>
</tr>
<tr>
<td>LAB CODE (L or C)</td>
<td></td>
</tr>
<tr>
<td>(TO OBTAIN A COURSE NUMBER, CONTACT <a href="mailto:imaldonado@fau.edu">imaldonado@fau.edu</a>)</td>
<td></td>
</tr>
<tr>
<td>COMPLETE COURSE TITLE: Secret Sharing Protocols</td>
<td></td>
</tr>
<tr>
<td><strong>EFFECTIVE DATE</strong></td>
<td></td>
</tr>
<tr>
<td>(first term course will be offered)</td>
<td></td>
</tr>
<tr>
<td>SPRING 2016</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CREDITS:</th>
<th>TEXTBOOK INFORMATION:</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>Core academic articles on secret sharing constructions (started from 1979)</td>
</tr>
<tr>
<td></td>
<td>Plus some other supplementary journals and conference papers</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>GRADING (SELECT ONLY ONE GRADING OPTION):</th>
<th>REGISTRATION CONTROLS (MAJOR, COLLEGE, LEVEL)*:</th>
</tr>
</thead>
<tbody>
<tr>
<td>REGULAR</td>
<td></td>
</tr>
<tr>
<td>Satisfactory/Unsatisfactory</td>
<td></td>
</tr>
</tbody>
</table>

| COURSE DESCRIPTION, NO MORE THAN THREE LINES: |
| Core secret sharing constructions along with their properties (symmetric/non-symmetric) and applications are discussed in three different models: (1) Standard: threshold, verifiable, generalized, weighted, geometric, dynamic, visual, multistage, proactive and quantum, (2) Interdisciplinary: rational, social and socio-rational, and (3) Hierarchical: disjunctive, conjunctive and sequential. |

<table>
<thead>
<tr>
<th>PREREQUISITES *:</th>
<th>COREQUISITES*:</th>
</tr>
</thead>
<tbody>
<tr>
<td>GRADUATE LEVEL STATUS OR PERMISSION OF THE INSTRUCTOR</td>
<td>N/A</td>
</tr>
</tbody>
</table>

* PREREQUISITES, COREQUISITES AND REGISTRATION CONTROLS WILL BE ENFORCED FOR ALL COURSE SECTIONS.

| MINIMUM QUALIFICATIONS NEEDED TO TEACH THIS COURSE: |
| Member of the graduate faculty of FAU and has a terminal degree in the subject area (or a closely related field) |

Faculty contact, email and complete phone number: Mehrdad Nojoumian
mnojoumian@fau.edu, 561-297-3411

Please consult and list departments that might be affected by the new course and attach comments. Mathematical Sciences (College of Science)

**Approved by:**

Department Chair: [Signature]

College Curriculum Chair: [Signature]

College Dean: [Signature]

UGPC Chair: [Signature]

Graduate College Dean: [Signature]

UFS President: [Signature]

Provost: [Signature]

Date: 10/13/2015


3. Consent from affected departments (attach if necessary)

Email this form and syllabus to UGPC@fau.edu one week before the University Graduate Programs Committee meeting so that materials may be viewed on the UGPC website prior to the meeting.

FAUniverseGrad Revised November 2014
1. Course title/number, number of credit hours

<table>
<thead>
<tr>
<th>Secret Sharing Protocols</th>
<th>3 credit hours</th>
</tr>
</thead>
<tbody>
<tr>
<td>COT 6116</td>
<td></td>
</tr>
</tbody>
</table>

2. Course prerequisites, corequisites, and where the course fits in the program of study

Prerequisites:
Graduate level status or permission of the instructor

3. Course logistics

Term: Spring 2016
Class location and time: TBA, Tuesdays and Thursdays: 12:30 - 13:50

4. Instructor contact information

<table>
<thead>
<tr>
<th>Instructor's name</th>
<th>Mehrdad Nojoumian</th>
</tr>
</thead>
<tbody>
<tr>
<td>Office address</td>
<td>EE96, Room 530</td>
</tr>
<tr>
<td>Office Hours</td>
<td>TBA</td>
</tr>
<tr>
<td>Contact telephone number</td>
<td>561.297.3411</td>
</tr>
<tr>
<td>Email address</td>
<td><a href="mailto:mnojoumian@fau.edu">mnojoumian@fau.edu</a></td>
</tr>
</tbody>
</table>

5. TA contact information

<table>
<thead>
<tr>
<th>TA's name</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Office address</td>
<td></td>
</tr>
<tr>
<td>Office Hours</td>
<td></td>
</tr>
<tr>
<td>Contact telephone number</td>
<td></td>
</tr>
<tr>
<td>Email address</td>
<td></td>
</tr>
</tbody>
</table>

6. Course description

Core secret sharing constructions along with their properties (symmetric or non-symmetric) and applications are discussed in three different models: (1) Standard: threshold, verifiable, generalized, weighted, geometric, dynamic, visual, multistage, proactive and quantum, (2) Interdisciplinary: rational, social and socio-rational, and (3) Hierarchical: disjunctive, conjunctive and sequential.

Knowledge of linear algebra, number theory and computer programming would be of great help. The instructor also reviews the necessary background materials.

7. Course objectives/student learning outcomes/program outcomes

**Course objectives**

This course enables the students to learn the fundamental concepts and the mathematical aspects of "secret sharing" as one of the most important components of cryptographic constructions and security protocols. Furthermore, it enables the students to utilize these schemes in distributed secure systems as well as other cryptographic tools such as secure multiparty computation.

8. Course evaluation method

<table>
<thead>
<tr>
<th>Evaluation Method</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Presentation</td>
<td>20%</td>
</tr>
<tr>
<td>Projects</td>
<td>30%</td>
</tr>
<tr>
<td>Homework, Midterm/Quizzes</td>
<td>20%</td>
</tr>
<tr>
<td>Final Examination</td>
<td>30%</td>
</tr>
</tbody>
</table>

**Project:** students are supposed to select one of the following options: (a) develop new modes and protocols, (b) improve the existing constructions, (c) implement the existing protocols, or (d) prepare a survey on...
9. Course grading scale

Grading Scale:


10. Policy on makeup tests, late work, and incompletes

All assignments are due at 11:00 am on the due date. Late assignments will lose 10% of the total points for each day they are late. They will not be accepted after three days. However, appropriate accommodations will be made for students having a valid medical excuse. Unless there exists an evidence of medical or emergency situation, incomplete grades will not be given. Plagiarism will not be tolerated. Any copying and pasting without attribution and a reference will be considered plagiarism.

11. Special course requirements

N/A

12. Classroom etiquette policy

University policy requires that in order to enhance and maintain a productive atmosphere for education, personal communication devices, such as cellular phones and laptops, are to be disabled in class sessions.

13. Disability policy statement

In compliance with the Americans with Disabilities Act, students who require special accommodations due to a disability to properly execute coursework must register with the Office for Students with Disabilities (OSD) located in Boca Raton campus, SU 133 (561) 297-3880 and follow all OSD procedures.

14. Honor code policy

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 unfair advantage over any other. Academic dishonesty is also destructive of the university community, which is grounded in a system of mutual trust and place high value on personal integrity and individual responsibility. Harsh penalties are associated with academic dishonesty. See University Regulation 4.001 at [http://www.fau.edu/regulations/chapter4/4.001_Code_of_Academic_Integrity.pdf](http://www.fau.edu/regulations/chapter4/4.001_Code_of_Academic_Integrity.pdf)

15. Required texts/reading

Core academic articles on secret sharing constructions (started from 1979)
Plus some other supplementary journals and conference papers

16. Supplementary/recommended readings

Introduction to Modern Cryptography (2nd edition), Katz and Lindell, Chapman & Hall/CRC.
Cryptography Theory and Practice (3rd edition), Stinson, Chapman & Hall/CRC.
Handbook of Applied Cryptography, Menezes, Oorschot, Vanstone, Chapman & Hall/CRC.
Core secret sharing schemes along with their properties (symmetric or non-symmetric) and applications are discussed in three different models:

<table>
<thead>
<tr>
<th>Weekly Schedule</th>
<th>Topics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Week 01</td>
<td>Introduction and Terminologies</td>
</tr>
<tr>
<td>Week 02</td>
<td>Preliminary Technical Materials</td>
</tr>
<tr>
<td>Week 03</td>
<td>Preliminary Technical Materials</td>
</tr>
</tbody>
</table>
| Week 04: Assig-01 | Standard Model:  
  TSS: Threshold Secret Sharing (1979)  
  VSS: Verifiable Secret Sharing (1985) |
| Week 05 | GSS: Generalized Secret Sharing (1987)  
  MSS: Multistage Secret Sharing (1994) |
| Week 09 | Spring Break |
| Week 10 | Interdisciplinary Model:  
| Week 11: Assig-04 | Hierarchical Model:  
| Week 12 | Symmetric Properties: Computational vs Unconditional, Synch vs Asynch, Interactive vs Non-Interactive, Ideal vs Non-Ideal, Perfect vs Imperfect |
| Week 13: Assig-05 | Non-Symmetric Properties: Ramp, Homomorphic, Weak, Linear, Multiplicative, Cumulative Schemes |
| Week 14 | Applications: Distributed Secure Systems, Sealed-Bid Auctions, Secure Electronic Voting, Multiparty Computation, Threshold Cryptography |
| Week 15 | Presentation and Project Report |
| Week 16 | Reading Week |
| Week 17 | Final Exam |
References

Secret Sharing Schemes:


Non-Symmetric Properties:


Supplementary Resources:


COT 6116: Secret Sharing Protocols
Spring 2016
Mehrdad Nojoumian


Note: this list may be updated in the future.
Re: Request for approval -- new courses

Rainer Steinwandt [srainer@math.fau.edu]

To:  
Cc: Yuan Wang, Nurgun Erdol

Monday, October 12, 2015 4:28 PM

Good afternoon,

Thank you for your email. Both courses look very fine, and there are no objections from the Department of Mathematical Sciences.

Kind regards,
Rainer

From: "Mihaela Cardei" <mcardei@fau.edu>
To: "Rainer Steinwandt" <srainer@math.fau.edu>
Cc: "Yuan Wang" <YWANG@fau.edu>, "Nurgun Erdol" <erdol@fau.edu>
Sent: Monday, October 12, 2015 9:27:37 AM
Subject: Request for approval -- new courses

Dear Dr. Steinwandt,

The Department of Computer & Electrical Engineering and Computer Science (CEECs) is proposing 2 new courses:
COT 6116 - Secret Sharing Protocols
CTS 6319 - Cyber Security: Measurement and Data Analysis

Please find attached the syllabi and cover pages.

We need your approval that the Department of Mathematical Sciences supports these course proposals. Could you please review the material and email me your approval decision?

Thank you,

Mihaela Cardei, PhD
Professor
Computer & Electrical Engineering and Computer Science Department
College of Engineering and Computer Science
Florida Atlantic University
http://www.cse.fau.edu/~mhiela