Secret Sharing Protocols
Course Syllabus

1. Course title/number, number of credit hours	
Secret Sharing Protocols COT 6427	3 credit hours
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 2017 *Class location and time*: Online Lectures and CM 128, Tuesdays and Thursdays: 12:30 ~ 01:50	
4. Instructor contact information	
Instructor's name *Office address* *Office Hours* *Contact telephone number* *Email address*	Mehrdad Nojoumian EE96, Room 530 Tuesdays and Thursdays: 10:00 ~ 12:00 561.297.3411 mnojoumian@fau.edu
5. TA contact information	
TA's name *Office address* *Office Hours* *Contact telephone number* *Email address*	N/A
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	
Subject to changes: Homework & Participation: Bonus up to 10% Presentation: 20% Final Project: 30% Midterm & Final Exams: 50%	**Project:** students are supposed to select one of the following options: (a) develop new models and protocols, (b) improve existing constructions, (c) implement existing protocols, or (d) prepare a survey on applications of secret sharing schemes.

9. Course grading scale

Grading Scale:
90 and above: "A", 87-89: "A-", 83-86: "B+", 80-82: "B", 77-79 : "B-", 73-76: "C+", 70-72: "C", 67-69: "C-", 63-66: "D+", 60-62: "D", 51-59: "D-", 50 and below: "F."
Note: The minimum grade required to pass the course is D.

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 and 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

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.

17. Course topical outline, including dates for exams/quizzes, papers, completion of reading

Core secret sharing schemes along with their properties (symmetric or non-symmetric) and applications are discussed in three different models:

Weekly Schedule	Topics
Week 01	Introduction and Terminologies
Week 02	Preliminary Technical Materials
Week 03	Preliminary Technical Materials
Week 04: **Assig-01**	Standard Model: TSS: Threshold Secret Sharing (1979) VSS: Verifiable Secret Sharing (1985)
Week 05	GSS: Generalized Secret Sharing (1987) WSS: Weighted Secret Sharing (1988)
Week 06: **Assig-02**	GMS: Geometric Secret Sharing (1988) DSS: Dynamic Secret Sharing (1991)
Week 07	VIS: Visual Secret Sharing (1994) MSS: Multistage Secret Sharing (1994)
Week 08: **Assig-03**	PSS: Proactive Secret Sharing (1995) QSS: Quantum Secret Sharing (1999)
Week 09	Spring Break
Week 10	Interdisciplinary Model: RSS: Rational Secret Sharing (2004) SSS: Social Secret Sharing (2010) SRS: Socio-Rational Secret Sharing (2012)
Week 11: **Assig-04**	Hierarchical Model: DJS: Disjunctive Secret Sharing (1988) CJS: Conjunctive Secret Sharing (2004) SQS: Sequential Secret Sharing (2015)
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:

1. Adi Shamir. How to Share a Secret. Communications of the ACM, 22(11): 612–613, **1979**.
2. Benny Chor, Shafi Goldwasser, Silvio Micali, and Baruch Awerbuch. Verifiable Secret Sharing and Achieving Simultaneity in the Presence of Faults. 26th Annual Symposium on Foundations of Computer Science, FOCS'85, pages 383–395, IEEE, **1985**.
3. Mitsuru Ito, Akira Saito, and Takao Nishizeki. Secret Sharing Scheme Realizing General Access Structure. Global Telecommunications Conference, GLOBECOM'87, pages 99–102, IEEE, **1987**.
4. Josh Cohen Benaloh and Jerry Leichter. Generalized Secret Sharing and Monotone Functions. 8th International Cryptology Conference, CRYPTO'88, vol 403 of LNCS, pages 27–35, Springer, **1988**.
5. Gustavus J. Simmons. How to (Really) Share a Secret. 8th Annual International Cryptology Conference, CRYPTO'88, vol 403 of LNCS, pages 390–448, Springer, **1988**.
6. Gustavus J Simmons. An Introduction to Shared Secret and/or Shared Control Schemes and Their Application. Contemporary Cryptology: The Science of Information Integrity, pages 441–497, **1991**.
7. Moni Naor and Adi Shamir. Visual Cryptography. International Conference on the Theory and Applications of Cryptographic Tech, EUROCRYPT'94, vol 950 of LNCS, pages 1–12, Springer, **1994**.
8. J. He and E. Dawson. Multistage Secret Sharing Based on One-Way Function. Electronics Letters, 30(19): 1591–1592, **1994**.
9. Amir Herzberg, Stanislaw Jarecki, Hugo Krawczyk, and Moti Yung. Proactive Secret Sharing or: How to Cope with Perpetual Leakage. 15th Annual International Cryptology Conference, CRYPTO'95, vol 963 of LNCS, pages 339–352, Springer, **1995**.
10. Mark Hillery, Vladimir Buzek, and Andre Berthiaume. Quantum Secret Sharing. Physical Review A, 59:1829–1834, **1999**.
11. Joseph Y. Halpern and Vanessa Teague. Rational Secret Sharing and Multiparty Computation: Extended Abstract. 36th ACM Symposium on Theory of Computing, STOC'04, pages 623–632, **2004**.
12. Mehrdad Nojoumian, Douglas R. Stinson, and Morgan Grainger. Unconditionally Secure Social Secret Sharing Scheme. IET Information Security (IFS), Special Issue on Multi-Agent and Distributed Information Security, 4(4): 202–211, **2010**.
13. Mehrdad Nojoumian and Douglas R. Stinson. Socio-Rational Secret Sharing as a New Direction in Rational Cryptography. 3rd International Conference on Decision and Game Theory for Security (GameSec), vol 7638 of LNCS, pages 18–37, Springer, **2012**.
14. Gustavus J. Simmons. How to (Really) Share a Secret. 8th Annual International Cryptology Conference, CRYPTO'88, vol 403 of LNCS, pages 390–448, Springer, **1988**.

15. Tamir Tassa. Hierarchical Threshold Secret Sharing. 1st Theory of Cryptography Conference, TCC'04, vol 2951 of LNCS, pages 473–490, Springer, **2004**.

16. Mehrdad Nojoumian and Douglas R. Stinson. Sequential Secret Sharing as a New Hierarchical Access Structure. Journal of Internet Services and Information Security (JISIS), Special Issue on Next Generation Networks and Systems Security, 5(2): 24–32, **2015**.

Non-Symmetric Properties:

17. G. R. Blakley and Catherine Meadows. Security of Ramp Schemes. 4th Annual International Cryptology Conference, CRYPTO'84, vol 196 of LNCS, pages 242–268, Springer, **1984**.

18. Josh Cohen Benaloh. Secret sharing homomorphisms: Keeping Shares of a Secret Sharing. 6th International Cryptology Conference, CRYPTO'86, vol 263 of LNCS, pages 251–260, Springer, **1986**.

19. Tal Rabin and Michael Ben-Or. Verifiable Secret Sharing and Multiparty Protocols with Honest Majority. 21st Annual ACM Symposium on Theory of Computing, STOC'89, pages 73–85, **1989**.

20. Mauricio Karchmer and Avi Wigderson. On Span Programs. In 8th Annual Structure in Complexity Theory Conference, pages 102–111, IEEE, **1993**.

21. Yvo Desmedt, Giovanni Di Crescenzo, and Mike Burmester. Multiplicative Non-Abelian Sharing Schemes and Their Application to Threshold Cryptography. 4th International Conference on the Theory and Application of Cryptology and Information Security, ASIACRYPT'94, vol 917 of LNCS, pages 21–32, Springer, **1994**.

22. Hossein Ghodosi, Josef Pieprzyk, Reihaneh Safavi-Naini, and Huaxiong Wang. On Construction of Cumulative Secret Sharing Schemes. 3rd Australasian Conference on Information Security and Privacy, ACISP'98, vol 1438 of LNCS, pages 379–390, Springer, **1998**.

Supplementary Resources:

23. G. R. Blakley. Safeguarding Cryptographic Keys. In National Computer Conference, NCC'79, pages 313–317, AFIPS Press, **1979**.

24. Michael Ben-Or, Shafi Goldwasser, and AviWigderson. Completeness Theorems for Non-Cryptographic Fault-Tolerant Distributed Computation. 20th Annual ACM Symposium on Theory of Computing, STOC'88, pages 1–10, **1988**.

25. David Chaum, Claude Crepeau, and Ivan Damgard. Multiparty unconditionally secure protocols. 20th Annual ACM Symposium on Theory of Computing, STOC'88, pages 11–19, **1988**.

26. Tal Rabin and Michael Ben-Or. Verifiable Secret Sharing and Multiparty Protocols with Honest Majority. 21st Annual ACM Symposium on Theory of Computing, STOC'89, pages 73–85, **1989**.

27. Donald Beaver. Multiparty Protocols Tolerating Half Faulty Processors. 9th Annual International Cryptology Conference, CRYPTO'89, vol 435 of LNCS, pages 560–572, Springer, **1989**.

28. Michael Harkavy, J. D. Tygar, and Hiroaki Kikuchi. Electronic Auctions with Private Bids. 3rd Conference on USENIX Workshop on Electronic Commerce, WOEC'98, pages 61–74. USENIX, **1998**.

29. Douglas R. Stinson and Ruizhong Wei. Unconditionally Secure Proactive Secret Sharing Scheme with Combinatorial Structures. 6th Annual International Workshop on Selected Areas in Cryptography, SAC'99, vol 1758 of LNCS, pages 200–214, Springer, **1999**.

30. Rosario Gennaro, Yuval Ishai, Eyal Kushilevitz, and Tal Rabin. The Round Complexity of Verifiable Secret Sharing and Secure Multicast. 33th Annual ACM Symposium on Theory of Computing, STOC'01, pages 580–589, **2001**.

31. Mehrdad Nojoumian and Timothy C. Lethbridge. A New Approach for the Trust Calculation in Social Networks. 3rd International Conference on e-Business (ICE-B), pages 257–264, INSTICC Press, **2006**.

32. S. Dov Gordon and Jonathan Katz. Rational Secret Sharing, Revisited. 5th International Conference on Security and Crypto for Networks, SCN'06, vol 4116 of LNCS, pages 229–241, Springer, **2006**.

33. Mehrdad Nojoumian and Timothy C. Lethbridge. A New Approach for the Trust Calculation in Social Networks. In E-business and Telecommunication Networks: 3rd International Conference on E-Business, Best Papers, vol 9 of CCIS, pages 64–77, Springer, **2008**.

34. Mehrdad Nojoumian and Douglas R. Stinson. Brief Announcement: Secret Sharing Based on the Social Behaviors of Players. 29th ACM Symposium on Principles of Distributed Computing (PODC), pages 239–240, **2010**.

35. Mehrdad Nojoumian. Novel Secret Sharing and Commitment Schemes for Cryptographic Applications. PhD Thesis, Department of Computer Science, University of Waterloo, Canada, **2012**.

36. Mehrdad Nojoumian and Douglas R. Stinson. On Dealer-Free Dynamic Threshold Schemes. Advances in Mathematics of Communications (AMC), 7(1): 39–56, **2013**.

37. Mehrdad Nojoumian. Generalization of Socio-Rational Secret Sharing with a New Utility Function. 12th IEEE International Conference on Privacy, Security and Trust, PST'14, pages 338–341, **2014**.

38. Mehrdad Nojoumian and Douglas R. Stinson. Efficient Sealed-Bid Auction Protocols Using Verifiable Secret Sharing. 10th International Conference on Information Security Practice and Experience, ISPEC'14, vol 8434 of LNCS, pages 302–317, Springer, **2014**.

39. Sriram Krishnamachari, Mehrdad Nojoumian, and Kemal Akkaya. Implementation and Analysis of Dutch-Style Sealed-Bid Auctions: Computational vs Unconditional Security. 1st International Conference on Information Systems Security and Privacy, ICISSP'15, pages 106–113, **2015**.

40. Mehrdad Nojoumian. Trust, Influence and Reputation Management Based on Human Reasoning. 4th AAAI Workshop on Incentives and Trust in E-Communities, WIT-EC'15, pages 21–24, **2015**.

Note: this list may be updated in the future.