COT 6427 Secret Sharing Protocols

Credits: 3 credits

Textbook, Title, Author, and Year: Core academic articles on secret sharing constructions (started from 1979). Plus some other supplementary journals and conference papers.

Reference Materials:

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.

Specific Course Information

Catalog 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.

Prerequisites: Graduate level status or permission of the instructor

Specific Goals for The Course: 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.

Brief List of Topics to Be Covered:

Introduction, Terminologies, and Preliminary Technical Materials

Standard Model: TSS: Threshold Secret Sharing (1979), VSS: Verifiable Secret Sharing (1985), GSS: Generalized Secret Sharing (1987), WSS: Weighted Secret Sharing (1988), GMS: Geometric Secret Sharing (1988), DSS: Dynamic Secret Sharing (1991), VIS: Visual Secret Sharing (1994), MSS: Multistage Secret Sharing (1994), PSS: Proactive Secret Sharing (1995), QSS: Quantum Secret Sharing (1999)

Interdisciplinary Model: RSS: Rational Secret Sharing (2004), SSS: Social Secret Sharing (2010), SRS: Socio-Rational Secret Sharing (2012)

Hierarchical Model: DJS: Disjunctive Secret Sharing (1988), CJS: Conjunctive Secret Sharing (2004), SQS: Sequential Secret Sharing (2015)