Course Project

Instructor: Mehrdad Nojoumian
Course: Secret Sharing Protocols

Deadline: End of April

(1) Programming: implement a secret sharing scheme (with my confirmation) with all required components (e.g., generating a large prime number, etc) using a programming language that you are comfortable with. Here is the guideline:

1. You may use existing crypto packages for some parts.
2. It is better to use C++ or Java for this program (you can also use Maple or Matlab).
3. The minimum size of your numbers should be 128 bits.
4. It would be great if you create a GUI (Graphical User Interface) for your program.
5. Finally, prepare one-page description regarding the architecture of your code.

Please put all your source files (and also the executable file if you use C++) along with the one-page description in a zip file and submit it to the related assignment section on Canvas.

Or

(2) Essay: prepare a technical essay on secret sharing schemes. You have four options:

1. **Comprehensive Survey:** prepare a survey on a specific application of secret sharing schemes, e.g., sealed-bid auctions, secure MPC, distributed systems, etc.

2. **Educational Project:** design fascinating games and puzzles to teach a set of secret sharing protocols to high school students.

3. **Improvement:** modify (or completely change) existing secret sharing constructions to improve their computational and communication complexities.

4. **New Construction:** come up with a completely new idea, e.g., a novel secret sharing construction or a new application of secret sharing schemes.

This is an alternative option for those who are not interested in programming or implementation. You are required to provide a 10~15-page essay (**1** inch margin, **10 Arial** font, **1.15** line spacing) with the following structure:

1. Abstract/Content of the Research.
2. Introduction and Your Contributions.
3. Preliminary/Background Materials.
4. Content/Main Body/Techniques.
5. Discussion and Concluding Remarks.

Subsequently, you must submit your essay to the related assignment section on Canvas. You can work in a team of 2 students if your project is large enough.