CSC 8980 Cryptography

Final Project

1. Project Description

The final project focuses on the implementations and applications of cryptosystems, aiming at understanding their advantages, disadvantages, and cryptanalysis. The **topics of interests include, but not limited to:**

- Applications of crypto algorithms, i.e., apply existing crypto algorithms to some real-world applications.
- Security analysis of crypto algorithms, including confidentiality, authenticity, integrity, and etc.
- Implementations of attacks, such as analytic attack, side-channel attack, substitution attack, and so on, for breaking crypto algorithms.

2. Project Requirements

The requirements of the final project are listed as follows:

- Every student or group that contains at most 2 students should select a project topic and report the project information, including the project topic and participant(s), to the instructor via email by Mar. 31, 2018.
- Every student or group should complete the final project and submit the project report by April 15, 2018.
- Every project should be presented in class. The presentation schedule will be announced later.

3. Project Grading Policy

The grades consist of the following three parts:

- Project Report (45 points), which will be judged in terms of project novelty, project organization, and writing.
- Project Presentation (45 points), which will be judged in terms of slides quality, time allocation, response to questions, and speaking.
- Discussion Participation (10 points), which will be judged from the questions a student raises/discusses during other's project presentation in class.

Note: for a project group, each group member (i.e., project participant) will deserve the same points for Project Report and Project Presentation for the team work.