CSE5014: Cryptography and Network Security
2023 Spring Semester Project (Optional) Description
Due: Jun. 18th, 2023

The goal of this optional project is for you to explore more interesting topics in cryptography and its applications in various related areas. You are required to give a self-contained report, together with possible supplementary materials (demo, codes, etc.). The project is *optional.*

You are assumed to work individually. The project report is due on **June 18th, 2023**. Each student may submit **a report directly to the homepage on sakai.sustech.edu.cn**. *Please indicate* **clearly** *the references in your report. All your submissions will be evaluated individually based on your own project (work load, scope, clarity and organization of your report, etc.). In your project report, a good formulation of the protocol and formal security analysis are highly valuable.*

The suggested list of topics includes but not limited to the following:

- *Design of "Good" (high-dimensional) pseudorandom number generators. Show the security properties via proof using the language we have learned in the course, or by simulation. Give an implementation of "random" generators, and find possible applications. For instance, random groups generator, online "red envelope" generator, etc.*
- *Survey the implementation, and existing attacks of real cryptographic schemes, e.g., RSA, SHA-256, AES, etc. Give also your own implementation if possible.*
- *A network protocol in the real world (e.g., SSL, IPSec), survey the application of cryptography therein, and analyze the security. You are encouraged to explore and choose a protocol that is closely related to your field of specialty and interest.*
- *Survey the usage of cryptography in TEEs (trusted execution environment), e.g., Intel SGX, ARM Trustzone, Risc-v Keystone, etc.*
- *More advanced applications of cryptography, for example, privacy-preserving data mining, secure multi-party computation, verifiable computation, etc.*