CS6222 Cryptography

Topic: Zero-knowledge proofs
Lecturer: Wei-Kai Lin (TA: Arup Sarker)

Date: Nov 14, 2024
Scriber: Shiyu Li, Han Yang

---

1 Zero-Knowledge Proofs

What is proof? A proof is something that convince people the fact or the statement holds for everything.

- **Statement.** Well-defined.
- **Completeness.** If the statement is TRUE, $\exists$ a proof everyone can verify.
- **Soundness.** If the statement is FALSE, $\nexists$ a proof s.t. everyone can verify.

Interactive Proofs. In computer scientists' view, the proof can be interactive. For one theorem statement, the prover and the verifier can exchange messages many rounds until the verifier is satisfied and outputs accept or reject.

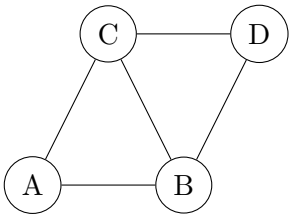
Compared with ancient proofs:

- More efficient. Use fewer number of bits in total communication.
- More statements.

Example. $x \in L$ is a statement, L is a problem/language.

- Ex. $L :=$ set of 3-colorable graphs.

  x is a graph as follow, which means x is 3-colorable.



- Fact: L is NP-complete. This means for all graph that is 3-colorable, there exits a witness that we can verify in polynomial time.

What is knowledge? If there is something we can obtain in almost no computation resources, it is less amount of knowledge. Knowledge takes us computational resources to obtain.

Go back to the 3-colorable graph. x is the statement. We concern about the witness, which is the coloring that the verifiers or others can not come up with easily. People need some time or memory to come up with the witness, then the witness has some knowledge. The prover knows the witness or the proof.

The whole purpose of zero knowledge is that the prover wants to convince the verifier the statement is true without revealing the knowledge.

ITM(P, V) is an interactive proof for language L if

- (Completeness) $\forall x \in L$, $\exists w\{0,1\}^*$ s.t. $\forall z$

$$\Pr[out_V[P(x,w) \leftrightarrow V(x,z)] = Acc] = 1,$$

  where out_V is output of V.

- (Soundness) $\exists$ negligible $\epsilon(\cdot)$ s.t. $\forall x \notin L$, $\forall$ adversarial P^*, $\forall z$

$$\Pr[out_V[P^*(x) \leftrightarrow V(x,z)] = Rej] \leq 1 - \epsilon(n),\ n := |x|.$$