Computational Zero-Knowledge:

$$S^{(V^*)}(x) \stackrel{\sim}{=} [P \leftrightarrow V(x)]$$

View of the two are the same as msg of P and V^* with V^*'s randomness.

1 Commitment Protocol

Commitment Protocol: An interactive protocol that consists of the commitment phase and open phase satisfying two properties:

- Binding: After the commit protocol terminiates, the commiter can only open b in 1 way.
- Hiding: After the commit phases is over, any PPT receiver cannot predict bit better than $\frac{1}{2} + \text{negl}$

2 Graph 3-Coloring

Given a graph G, we say it is **3-colorable** if we can assign colors to each node such that for all $(u, v) \in E$, u and v are different colors.

2.1 ZK Proof for 3-Color

Given a graph G, we have the following protocol to demonstrate that $G \in$ 3-Color:

1. The prover P creates a random permutation shuffling the colors from one to another randomly. (exp. Red $\rightarrow$ Blue). The prover secretly commits to this new three coloring and sends commitments to V.
2. V selects a random edge $e = (u, v)$ and sends their selection back to P.
3. P decommits nodes u and v to V who can see that they are different colors.
4. This process is repeated k times.

Completeness: is clear from the inspection.
Soundness: Consider some $G \notin$ **3-Color**. Then, $\exists e = (u, v) \in E$ where (u, v) are the same color. Since V selects a random edge e', the probability

that they choose this edge is $\frac{1}{|E|}$. Therefore the probability that P can successfully fool the verifier is:

$$(1 - \frac{1}{|E|})^k$$

Which for $k = |E|$ is $1/e^{|E|}$.