☙ CS6222 Cryptography ❧

Topic: Zero Knowledge Proofs Date: Nov 19, 2024
Lecturer: Wei-Kai Lin (TA: Arup Sarker) Scriber: Sadhika Dhanasekar and Chase Fickes

---

1 3 Coloring

If you have 3-coloring on this graph, you can permute the colors. In the given example of 6 vertices forming four triangles, there are 6 permutations of coloring. However, if you have a 4 vertex, complete graph, it would not be colorable unless we were to remove one of the edges.

Formal Definition Formally, x denotes a graph with n vertices and E edges: $x = ([n], E)$. The statement we are showing is $x \in L_{3-col}$. Other constraints are $w = (b_1, b_2, ...b_n)$, $b_i \in \{R, B, G\}$, $\forall (u, v) \in E$, $b_u \neq b_v$ if w is witness of $x \in L$.

Witness Addition Proving $x \in L$ can be difficult as 3-coloring in a NP complete problem. Let's say the prover is provided with the graph, x and a witness, w, that has a legitimate coloring of x and is selected from the set of all colorings for the graph, which is denoted by $w \in R_L(x)$ since each w may not be unique for a given x.

Interactive Proofs PPT ITM (P,V) is Zero Knowledge Proof (ZKP) for L if $\forall$ auxiliary $z \in \{\}^*$.

Complete: $\forall x \in L, \exists w \in \{0,1\}^*, \Pr[out_v[P(x,w) \leftrightarrow V(x,z) = 1] = ACC]$

Soundness: $\exists$ negl $\epsilon(\cdot), \forall x \notin L, \forall$ adverserial $P^*, \forall z, \Pr[out_v[P^*(x) \leftrightarrow V(x,z)] = Acc] \leq \epsilon(n) \forall n$
If the graph is not 3 colorable, there is no way to come up with any arbitrary algorithm, P^* that can prove the problem.

Zero-Knowledge: $\exists$ PPT simulator S such that $\forall x \in L, w \in R_L(x), \forall z$,
$\{view_v[P(x,w) \leftrightarrow V(x,z)]\}_n \approx \{S(x,z)\}_n$ The view is something you can create without knowing w where the view represents all transactions and messages sent between P and V.

This definition of zero-knowledge essentially means that the simulator does not need the witness, so the view with witness w is close to a simulation that does not know w. If the language is easy enough that V can solve the verify the statement in poly time without P, then it is zero-knowledge.

Sealed Envelope $\forall i \in [n], \pi \leftarrow$ Perm(3), meaning π is a permutation mapping to the 3 colors, $\{R, G, B\} \rightarrow \{R, G, B\}$. $c_1 =$ Com$(\pi(b_i); r_i)$. There is a sealed envelope that can only be opened by the seal, r_i. It has two purposes, hiding and binding. Prover sends this envelope storing a color for every vertex i to the verifier. The verifier then picks a uniformly random edge, $(u, v) \leftarrow E$, which is sent to the prover who opens the corresponding envelope. Given $(\pi(b_u); r_u)$ and $(\pi(b_v); r_v)$, the verifier receives $c_u =$ Com$(\pi(b_u); r_u)$ and $c_v =$ Com$(\pi(b_v); r_v)$. To verify the opening is correct, the verifier will recompute the commitment and check that the permuted color $b_u \neq b_v$, else it will reject. The commitment function, Com, is a function computable in polynomial time.

If a graph is not 3-colorable, there must exist two adjacent edges that are the same color. *Soundness:* $\exists (u^*, v^*) \in E$ *s.t.* c_{u^*}, c_{v^*} are some color.

Soundness Cont. If $(u, v) = (u^*, v^*)$, then V is rejected by binding of Com. $\Pr[out_v[...] = Acc] \leq 1 - \frac{1}{|E|}$. Repeat this protocol for $n * |E|$ times. $|Pr[] \leq (1 - \frac{1}{|E|})^{n*|E|} = e^{-n}$. This is negligible, so we have shown that this protocol fulfills the soundness requirement

Acknowledgement

Replace this with people who helped with this note. If any publication is used, cite them like this [**?**].

References