EE 465: Cryptocurrency and Blockchain Technologies (Autumn 2018)
Instructor: Saravanan Vijayakumaran
Indian Institute of Technology Bombay

Endsem Exam : 24 points November 22, 2018

1. Answer the following questions in the context of the Bitcoin protocol.

   (a) (1 point) What is the cause of transaction malleability in pre-SegWit transactions? Why is it not present in SegWit transactions?

   (b) (1 point) In the Bitcoin micropayments protocol, what can go wrong if initial transaction transferred funds to a 1-of-2 multisig output instead of the 2-of-2 multisig output?

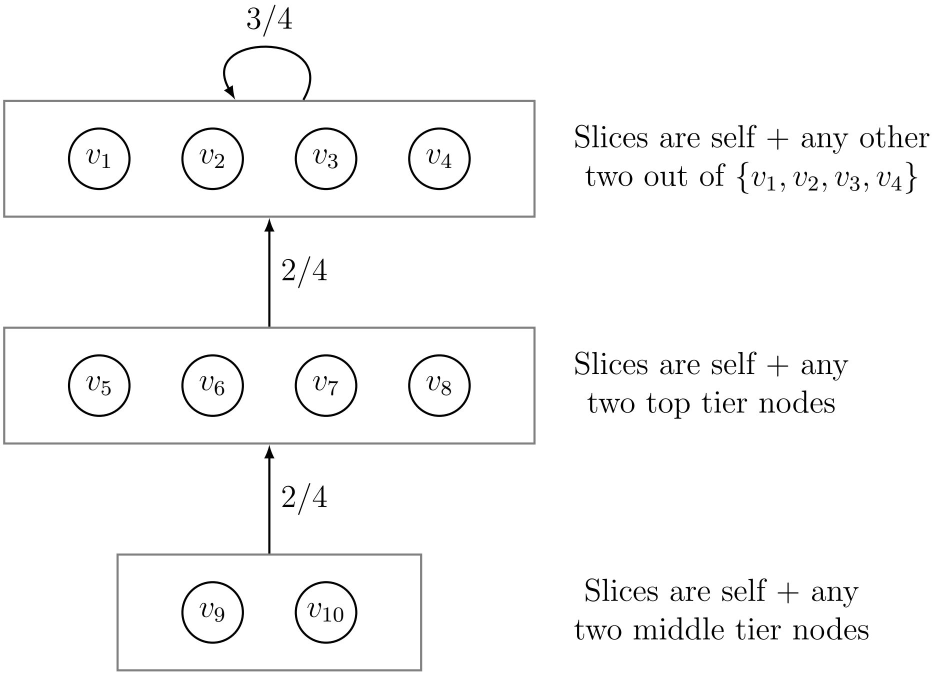
2. The FBAS shown in the below figure enjoys quorum intersection.

   (a) (1 point) Find the smallest quorum containing v_6 and v_9. Justify your answer by specifying the quorum slice for each member which is contained in the quorum you found.

   (b) (2 points) Show that $\{v_1\}$ is a DSet.

   (c) (2 points) Show that $\{v_5, v_6\}$ is not a DSet.

   (d) (1 point) Find the smallest DSet containing $\{v_5, v_6\}$.


3/4
v_1
v_2
v_3
v_4
Slices are self + any other two out of $\{v_1, v_2, v_3, v_4\}$
2/4
v_5
v_6
v_7
v_8
Slices are self + any two top tier nodes
2/4
v_9
v_{10}
Slices are self + any two middle tier nodes

3. Answer the following questions in the context of the Monero system.

   (a) (1 point) Suppose you created a Pedersen commitment C to an amount a. Without revealing the blinding factor x used to create C, how can you prove to someone that C is in fact a commitment to the amount a and not to some amount $a' \neq a$?

   (b) (2 points) Give an example illustrating the need for range proofs on Pedersen commitments in the Monero protocol.

   (c) (3 points) In an elliptic curve group of cardinality l with generator G, a Diffie-Hellman triple is a triple (A, B, C) of the form (aG, bG, abG) where $a, b \in \mathbb{Z}_l$. Suppose you have access to a genie who can tell you if a given triple is a Diffie-Hellman triple or not. Show how such a genie can be used to identify the signer in a LSAG signature, i.e. given an LSAG signature over the public keys $P_0, P_1, \ldots, P_{n-1}$ you should use the genie to identify the public key P_j whose corresponding private key x_j was used to create the LSAG signature.

4. A zero knowledge proof for the existence of an isomorphism $\phi : G_1 \mapsto G_2$ between graphs $G_1 = (V_1, E_1)$ and $G_2 = (V_2, E_2)$ proceeds as follows:

   - Prover picks a random permutation π from the set of permutations of V_2
   - Prover calculates $F = \{(\pi(u), \pi(v) \mid (u, v) \in E_2\}$ and sends the graph $G' = (V_2, F)$ to verifier
   - Verifier picks $\sigma \in \{1, 2\}$ randomly and sends it to prover
   - If $\sigma = 2$, then prover sends π to the verifier. Otherwise, it sends $\pi \circ \phi$ to the verifier where $(\pi \circ \phi)(v)$ is defined as $\pi(\phi(v))$
   - If the received mapping is an isomorphism between G_σ and G', the verifier accepts. Otherwise, it rejects

   (a) (2 points) If $\sigma = 2$, the prover sends π which is independent of ϕ. This does not seem to prove any knowledge regarding ϕ. What can go wrong if the verifier always sent $\sigma = 1$ to the prover?

   (b) (2 points) Instead of the first step above, suppose the prover begins by picking a random permutation from the set of permutations of V_1. Modify the remaining steps to obtain a zero knowledge proof of graph isomorphism.

5. (2 points) Suppose a Hyperledger Fabric network requires an application to get **three** endorsements before a transaction proposed by it is added to the blockchain. Explain the steps involved starting from the transaction proposal by the application to the addition of the transaction in the blockchain. Assume there are four peers P_1, P_2, P_3, P_4 connected by the same channel who can endorse a transaction.

6. (1 point) Prove the Schwartz-Zippel lemma.

7. Suppose Bob chooses a random polynomial $a(x) = a_0 + a_1x + a_2x^2 + \cdots + a_dx^d$ with coefficients from a prime field $\mathbb{F}_q$ and keeps it secret. Let $G = \langle g \rangle$ be a group of order q in which discrete logarithms are hard to find and the d-PKE assumption holds. Alice chooses a random point t from $\mathbb{F}_q$.

   (a) (1 point) Suppose Bob behaves honestly. Without revealing t to Bob, how can Alice get Bob to calculate $g^{a(t)}$?

   (b) (2 points) Suppose Bob can behave maliciously. Describe a protocol (which does **not** use bilinear pairing operations) by which Bob can convince Alice that he has evaluated his secret polynomial at the point t without revealing the polynomial to Alice.