COMP6453 Tutorial Week 10

1 Zero Knowledge Proof for Equal Plaintexts

For this exercise, review what an *sigma protocol*.

Suppose Alice has an ElGamal ciphertext (v_0, e_0) that encrypts a message m under Bob's public key u_0, and another (v_1, e_1), that encrypts the same message m under Bill's public key u_1. She wants to convince Charlie that this is the case, without revealing anything else. For example, some protocols may require that Alice broadcast the same message to Bob and Bill. How would you use Sigma Protocols for this problem that allows Alice to do this, while keeping her message encrypted, but proving that she really did encrypt the same message.

2 BLS with multiple signers

Consider BLS signatures that you have studied in class. You explored aggregate signatures where you can aggregate multiple signatures by the same singer resulting in efficient verification. Answer the following questions.

- Instead of one signer, there are now multiple signers. Write a new version of BLS aggregation with multiple signers, where there are n signers and i-th signer signs message m_i.
- Discuss the efficiency of this algorithm. What happens when each of the signers sign the same message m?
- Is this signature aggregation scheme secure? If no, then write an attack on this scheme. How can you change your scheme to make it secure.