Security Specification

System Goals:

- A Client wants to learn the secret (m1 * m2) + m3 mod p
- Implementing Multi-Party Computation (MPC) to compute the secret
- The protocol is a combination of MPC and an Algorand smart contract which will allows the Client to learn the secret only if he pays.

Scheme:

- The keys for encryption and decryption are generated using the ElGamal algorithm.
- The messages m1, m2, and m3 are sent to the ElGamal algorithm for encryption.
- The ElGamal algorithm returns encrypted messages, public key, and private key.
- The protocol creates three shares of the private key.
- The individual encrypted message and one private key share are shared with each party by the Dealer.
- The Trusted Party reconstructs the private key and uses it to decrypt each of the party's messages.
- Trusted Party runs the input gadget, multiplication gadget, and addition gadget to compute the secret.
- The secret is then encrypted using One Time Pad (OTP) and put on the Algorand ledger.
- The smart contract only shares the key with the Client when it verifies that he has paid. The Client can then use the key to decrypt the message.

Computational Assumptions:

- As given, one of the parties is semi-honest; that is, it is passively corrupted.
- All communications happen through secure channels.
- The adversary cannot attack the protocol or the messages shared within it.

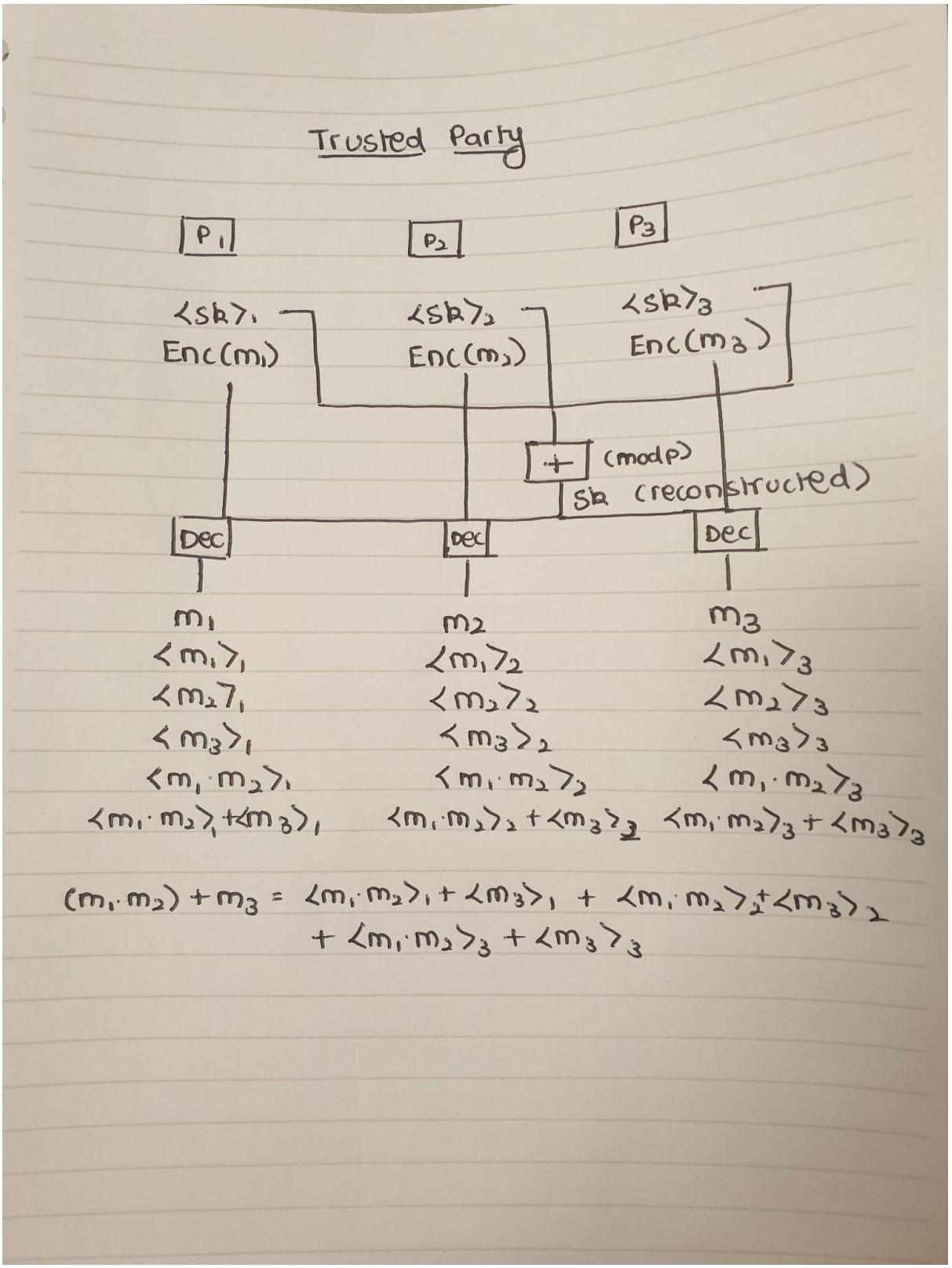
Specifications:

- Every party P_i sends its input Enc(m_i),$< sk >_i \in Z_m$ to the trusted party T
- T computes the secret $(m_1 * m_2) + m_3$
- As the adversary type is semi-honest, the number of parties is equal to three, and corrupted parties are equal to one, the corruption bound is t<n/2. Hence security is defined as Information Theoretic (IT).
- As there are secure channels and t<n/2, the adversary learns nothing more than what he already knows. The adversary needs (t+1) points to reconstruct

the secret, which he does not; hence we define this as the privacy property of the protocol.

- Based on whatever inputs the parties get from the dealer, on running the protocol, they get the correct values only (as computational assumption states that the adversary cannot attack the network). This is the definition of the correctness property of the protocol.

Circuit:



GitHub Repo Link: https://github.com/anushree-vaidya-11/CS555-Project-ANP
Default Branch: Anhsirk6khaos-Encryption+MPC