P2PMIXNOTE

lu562

June 2017

1.dinning cryptographers networks:https://en.wikipedia.org/wiki/Dining_cryptographers_problem

2.DiceMix requires 4+2f rounds in the presence of f malicious peers.

3.bulletin board: a server receiving messsages from each peer and broadcasting them to all other peers.(honest)

4.DiceMix built on synchronous settings. We can replace bulletin board using a reliable broadcast protocol.

5.the input messages must be fresh.(what if all honest nodes want to send messages at the same time, in this scenario all messages are not random)

6.termination is impossible to achieve against a malicious bulletin board, which can just block all communicaation.

7.3 needss: 1.key exchange mechanisms 2. all nodes publish a message simutaneously,3 encuring termination.

8.handling collisions:redundancy.building slots: $S_j = \sum m_i^j$

9.non-malleable commitment. preventing malicious peers from choosing their DC-net vectors depending on DC-net vectors of others. If bulletin board can be trusted then when can omit this.

10.KE-¿CM-¿DC-¿CF if everything OK.