



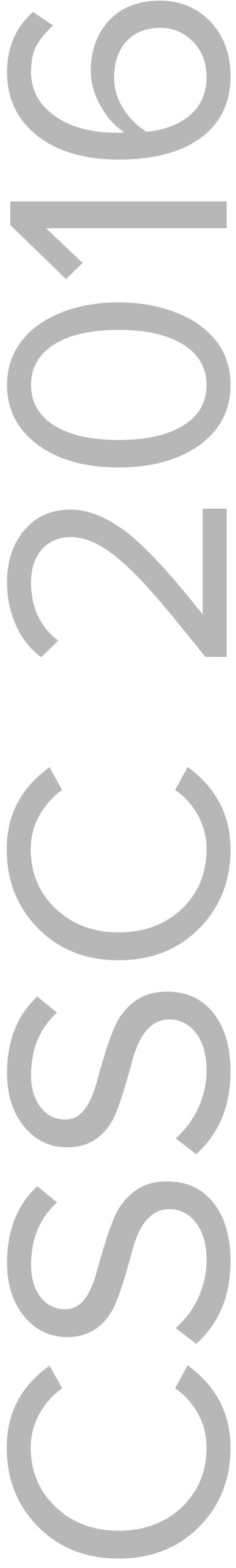
RESEARCH PRESENTATION

Abhinav Aggarwal

Student Union Building, Ballroom A

Thursday, April 7, 2016 10:30 am - 10:45 am

Secure one way interactive communication



Alice wants to communicate a message to Bob over a two-way interactive channel. However, an adversary, that cannot read bits on the channel from Bob to Alice (but is omniscient with unbounded resources otherwise), has decided to enter the scene with malicious intentions. The purpose of this report is to present an algorithm that establishes this one-way communication between Alice and Bob that succeeds with high probability and does not incur an extra cost that is much more than what the adversary pays, asymptotically. We do not assume any a priori knowledge about the adversary's budget T , however, the knowledge of the length L of the message with Alice and the error tolerance is assumed to be public. We use Reed-Solomon codes along with error correction on the symbols sent on the channels to protect against expensive defense, and the Naor-Naor hash functions along with AMD encoded randomized fingerprints to ensure a high probability of detecting tampering by the adversary. An important application of such an algorithm is to establish shared randomness between Alice and Bob, which may be used in other distributed protocols to achieve secrecy and authentication.