Byzantine Agreement on Steroids

Silvio Micali

MIT

Abstract. As insightfully defined by Pease, Shostak, and Lamport, Byzantine agreement (BA) has rightfully received enormous attention, and is one of the most demanding and compelling notions in fault-tolerant and secure computation. Yet, BA protocols are too slow for most practical applications, and often satisfy conditions much weaker than those originally envisaged.

We put forward an extremely efficient, cryptographic, and probabilistic BA protocol working in a variety of networks. No matter what the number of players might be, so long as more than 2/3 of them are honest, the new protocol halts and reaches agreement in (at most!) expected 9 steps, in each of which a player sends a single message to all other players. Furthermore, our protocol satisfies a new and very surprising property, *player replaceability*, enabling one to dramatically and securely *reduce* the number of players actually running the protocol.