# Very Simple and Efficient Byzantine Agreement

Silvio Micali

**CSAIL, MIT, Cambridge, USA**
silvio@csail.mit.edu

## Abstract

We present a very simple, cryptographic, binary Byzantine-agreement protocol that, with $n \geq 3t+1 \geq 3$ players, at most $t$ of which are malicious, halts in expected 9 rounds.

**1998 ACM Subject Classification** C2.2 Network Protocols, F.0 General

**Keywords and phrases** Byzantine Agreement

**Digital Object Identifier** 10.4230/LIPIcs.ITCS.2017.6

## 1 Set Up

The players communicate, in rounds, in a synchronous, point-to-point network with full connectivity. Each player $i$ has a public key $PK_i$, and a corresponding secret key $SK_i$, of a verifiable random function. (For simplicity, we may rely on a unique-signature digital signature scheme and a hash-function $H$ modelled as a random oracle. This way, $i$ univocally associates to each message $m$ the random string $H(SIG_i(m))$.) There is also a random string $R$, independent of the $n$ public keys. The players, their public keys, and the string $R$ are common knowledge to all players.

## 2 Adversarial Model

A honest player follows all his protocol instructions. Initially all players are honest, and remain so until he made malicious (corrupted) by a polynomial-time Adversary. At the start of *any round*, the Adversary may secretly corrupt *any player* he wants, provided that he corrupts less than $n/3$ players in total. The Adversary totally controls, and perfectly coordinates, the actions of all corrupted players, who thus may arbitrarily deviate from their protocol instructions. At each round, the Adversary immediately learns all messages sent by the honest players, and then chooses the messages sent in the same round by all currently corrupted players. However, the Adversary cannot interfere (block, alter, etc.) the messages the currently honest players send to each other. In addition, since he is computationally bounded, he cannot successfully forge the digital signature of an honest player, except with negligible probability.

## 3 Further Information

For more details, see https://people.csail.mit.edu/silvio/Selected Scientific Papers Distributed Computation.

Also, the author and Vinod Vikuntanathan have modified the protocol so as as to work also when the Adversary corrupt any number of players less than $n/2$. Stay tuned!

8th Innovations in Theoretical Computer Science Conference (ITCS 2017).
Editor: Christos H. Papadimitriou; Article No. 6; pp. 6:1–6:1
Leibniz International Proceedings in Informatics
LIPICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany