Cryptology ePrint Archive: Report 2011/313

Error-free Multi-valued Broadcast and Byzantine Agreement with Optimal Communication Complexity

Arpita Patra

Abstract: In this paper we present first ever error-free, asynchronous broadcast (called as A-cast) and Byzantine Agreement (called as ABA) protocols with optimal communication complexity and fault tolerance. Our protocols are multi-valued, meaning that they deal with ℓ bit input and achieve communication complexity of $O(n\ell)$ bits for large enough ℓ for a set of $n \geq 3t+1$ parties in which at most t can be Byzantine corrupted.

In synchronous settings, Fitzi and Hirt (PODC'06) proposed probabilistically correct multi-valued broadcast (BC) and Byzantine Agreement (BA) protocols with optimal complexity of $O(n\ell)$ bits. Recently, Liang and Vaidya (PODC'11) achieved the same deterministically, i.e. without error probability. In asynchronous settings, Patra and Rangan (Latincrypt'10, ICITS'11) reported similar protocols with error probability. Here we achieve optimal complexity of $O(n\ell)$ bits for asynchronous error-free case.

Following all the previous works on multi-valued protocols, we too follow reduction-based approach for our protocols, meaning that our multi-valued protocols are designed given existing A-cast and ABA protocols for small message (possibly for single bit). However compared to existing reductions, our reductions are simple and elegant. More importantly, our reductions run in constant expected time, in contrast to $O(n)$ of Patra and Rangan (ICITS'11). Furthermore our reductions invoke less or equal number of instances of protocols for single bit in comparison to the reductions of Patra and Rangan.

In synchronous settings, while the reduction of Fitzi and Hirt is constant-round and invokes $O(n(n+\kappa))$ (κ is the error parameter) instances of protocols for single bit, the reduction of Liang and Vaidya calls for round complexity and number instances that are in fact function of the message size, $O(\sqrt{\ell} + n^2)$ and $\calO(n^2\sqrt{\ell} + n^4)$, respectively where $\ell = \Omega(n^6)$. By adapting our techniques from asynchronous settings, we present new {\it error-free} reduction in synchronous world that is constant-round and calls for only $O(n^2)$ instances of protocols for single bit which is at least as good as Fitzi and Hirt.

Category / Keywords: cryptographic protocols / Asynchronous, Multi-valued, A-cast, Byzantine Agreement, Communication Complexity

Date: received 13 Jun 2011

Contact author: arpita at cs au dk, arpitapatra10@gmail com