Question: Parallel Repetition of Binary Byzantine Agreement

April 23, 2017

Suppose that BBA is a binary Byzantine Agreement protocol. Consider the following proposal for Byzantine Agreement. Each party i gets as input some value $\mathsf{in}_i \in \{0,1\}^L$, written as $\mathsf{in}_i = \mathsf{in}_i[1], \ldots, \mathsf{in}_i[L]$. Each party must output a value $\mathsf{out}_i = \mathsf{out}_i[1], \ldots, \mathsf{out}_i[L]$ (or $\perp$).

- For each index $\ell = 1, \ldots, L$, do:
  - Run $\mathsf{BBA}(\mathsf{in}_\ell)$, and let $\mathsf{out}_i[\ell]$ be your output.
- If $\exists \ell$ such that $\mathsf{out}_i[\ell] = \perp$, return $\perp$.
- Else, return $\mathsf{out}_i = \mathsf{out}_i[1], \ldots, \mathsf{out}_i[L]$.

Question: Does it satisfy the notion of Byzantine Agreement in Definition 1 in *The Notion of Byzantine Agreement*?