could you use a Dark DAO-like paradigm to break MPC-based computations?

everyone sends their share to an SGX machine, which only releases the info/bribes if enough shares are collected?