We present a new model for (Asynchronous) Byzantine Reliable Broadcast to investigate the potentials of collusion between the honest players. To model the collusion, we assume that each honest player has k>1 distinct communication channels over which it can send an receive message. The adversary is (initially) oblivious, which channels belongs to which player. Only a protocol's message pattern can leak information on which channels belong to which player.

We show that if the system has n honest players and each player has exactly k channels, then the difference between honest and adversiarial players must be at at least n/2^k+ sqrt(xn/2^k) to succeed with probability 1/2^x. This even holds in the authenticated setting, i.e., if the players have access to a PKI that allows them to sign and verify messages. For this authenticated setting, we present a fast and simple asynchronous protocol that matches this lower bound within a small (additive) factor. Our protocols succeeds w.h.p. if the initial assignment of identities to players is picked uniformly at random.

Finally, we sketch how the protocol can be extended to the unauthenticated setting.