1163-68-1277 **Erica Blum**, **Jonathan Katz**, **Chen-Da Liu-Zhang** and **Julian Loss*** (lossjulian@gmail.com). *Asynchronous Byzantine Agreement with Subquadratic Communication.*

Byzantine agreement (BA) is a fundamental problem in distributed computing. In this context, n parties agree on a common output by running a distributed protocol. This should hold even if a powerful adversary adaptively corrupts some f of those parties and makes them deviate from the protocol description arbitrarily. As applications of BA typically involve large numbers of parties, it is critical to understand how the communication complexity of BA scales with n. Protocols with $o(n^2)$ communication complexity (CC) have been obtained under the assumption that all messages are delivered within some worst-case message delay. However, no solution exists for the asynchronous model where delays can be arbitrary, as long as messages are eventually delivered. This leads us to ask: Are there asynchronous BA protocols with $o(n^2)$ CC tolerating $f < n/3$ adaptive corruptions? We give the first positive and negative answers to this question: 1) We show asynchronous BA protocols with (expected) subquadratic CC tolerating an adaptive adversary that corrupts $f < n/3$ parties. Our protocol uses cryptographic setup by a trusted dealer. 2) We show that some form of setup is inherent for subquadratic BA tolerating $O(n)$ corrupted parties. (Received September 15, 2020)