**Distributed Computing Made Secure - A Graph Theoretic Approach**

**Merav Parter, Weizmann Institute**

**Abstract**
In the area of distributed graph algorithms a number of network's entities with local views solve some computational task by exchanging messages with their neighbors. Quite unfortunately, an inherent property of most existing distributed algorithms is that throughout the course of their execution, the nodes get to learn not only their own output but rather learn quite a lot on the inputs or outputs of many other entities. This leakage of information might be a major obstacle in settings where the output (or input) of network's individual is a private information (e.g., distributed networks of selfish agents, decentralized digital currency such as Bitcoin).

In this paper, we introduce a new framework for secure distributed graph and provide the first general compiler that takes any "natural" non-secure distributed algorithm that runs in $r$ rounds, and turns it into a secure algorithm that runs in $\widetilde{O}(r \cdot D \cdot poly(\Delta))$ rounds where $\Delta$ is the maximum degree in the graph and $D$ is its diameter. A "natural" distributed algorithm is one where the local computation at each node can be performed in polynomial time. An interesting advantage of our approach is that it allows one to decouple between the price of locality and the price of security of a given graph function $f$. The security of the compiled algorithm is information-theoretic but holds only against a semi-honest adversary that controls a single node in the network.

The main technical part of our compiler is based on a new cycle cover theorem: We show that the edges of every bridgeless graph $G$ of diameter $D$ can be covered by a collection of cycles such that each cycle is of length $\widetilde{O}(D)$ and each edge of the graph $G$ appears in $\widetilde{O}(1)$ many cycles, existentially this is optimal, up to polylogarithmic terms.

Joint work with Eylon Yogev.