Computing Node Clustering Coefficients Securely

Katchaguy Areekjseree, Yuzhe Tang and Sucheta Soundarajan
Department of Electrical Engineering and Computer Science, Syracuse University, NY USA.
{kareekij, ytang100, susounda}@syr.edu

Introduction
- Complex networks (e.g. social networks) gain a lot of interest from the researchers.
- To gain more insights, we can perform an analysis on this network.
- Some information may be leaked or shared with others when perform any analysis task.
  - E.g. number of friends and who they are.
  - However, some users are not willing to share their information.
- Secure multi-party computation (MPC) [1] allows individuals to jointly perform any computation without reveal individual’s input (convert any computation into a circuit of AND gates).
- **Long-term goal**: To develop a ‘library’ for performing graph operations securely.

Experimental Setup
- We consider 3 network properties that could computational cost
  - Average degree
  - Degree distribution
  - Clustering coefficient
- We generate 2000-node networks
  - ER (binomial) and LFR models[2] (power-law).

Cost of MPC
- Cost of MPC can be evaluated by the number of AND gates.
  - $C[PSIC] = (M_1 + M_2) \log(M_1 + M_2) (n^2 - n) / 2$
  - $C[PSU] = \sum_{i=1}^{n} M_i \log(M_i) (n^2 - n) / 2$
  - $C[SECSUM] = (n^3 - n^2) / 2$
  where $n$ is the number of parties and $M_i$ is the set cardinality.

Results
- (a) Results when varying average degree
- (b) Results when varying clustering coefficient

Key Observations
1. The computation cost increases as average degree increases, it highly depends on number of parties (u’s neighbors).
2. Clustering coefficient has little effect on the computation cost.
3. Computation costs do not seem to be dependent on degree distribution.

Conclusion
- We demonstrate how to design secure MPC algorithm.
- We proposed two high-level constructions (C1 and C2)
- Our long-term goal is to develop a library of secure graph primitives operations.
- This primitives operations will be building blocks for more sophisticated techniques.
  - e.g. community detection or link prediction.

References