GRAND : GRAPH RECONSTRUCTION FROM POTENTIAL PARTIAL ADJACENCY AND NEIGHBORHOOD DATA

Are Your Secure Graph Computations Really Safe?

AUTHORS

Sofiane Azogagh, Zelma Aubin Birba, Josée Desharnais,
Sébastien Gambs, Marc-Olivier Killijian and Nadia Tawbi

PARTNERS

UQÀM Université du Québec à Montréal

UNIVERSITÉ LAVAL

DEEL DEpendable & Explainable Learning

1.CONTEXT

Collaborative ecosystems like social media platforms often seek to enhance user experience by recommending new connections (friends, followers, content). To do this without directly sharing user data, they may rely on **secure multi-party computation** to compute statistics like the **number of common neighbors** [1, 2] (e.g., mutual friends between users across networks).

2.PROBLEM STATEMENT

- Distributed graph protocols (e.g., secure computation of common neighbors) are used to preserve privacy.
- However, an adversary observing only the matrix of common neighbors (i.e., G^2) may reconstruct the original graph—possibly leaking sensitive structure.
- **What can an attacker learn from just the number of mutual friends?**

3. ADVERSARY MODELS

Model	**Knows** G2	**Knows part of** G
Uninformed	✅	❌
Informed	✅	✅ (Existing and absent edges)

4. METHODOLOGY

4.1. TOPOLOGICAL ATTACKS

From the common neighbors matrix and the partial knowledge, direct inferences can be made on the existence/non-existence of some edges.

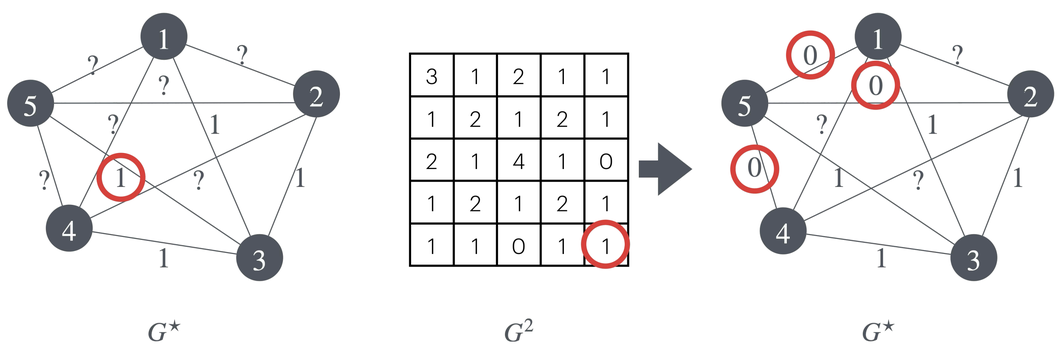


illustration of the DegreeMatchingAttack (cf paper@5.1)

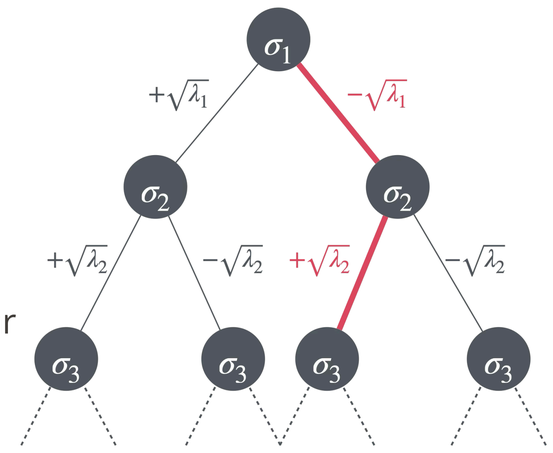
4.2. SPECTRUM-BASED RECONSTRUCTION

$$G = U\Sigma U^\intercal$$

$$G^2 = (U\Sigma U^\intercal)^2 = U\Sigma^2 U^\intercal = U\Lambda U^\intercal$$

Singular Value Decompositions of G and G^2

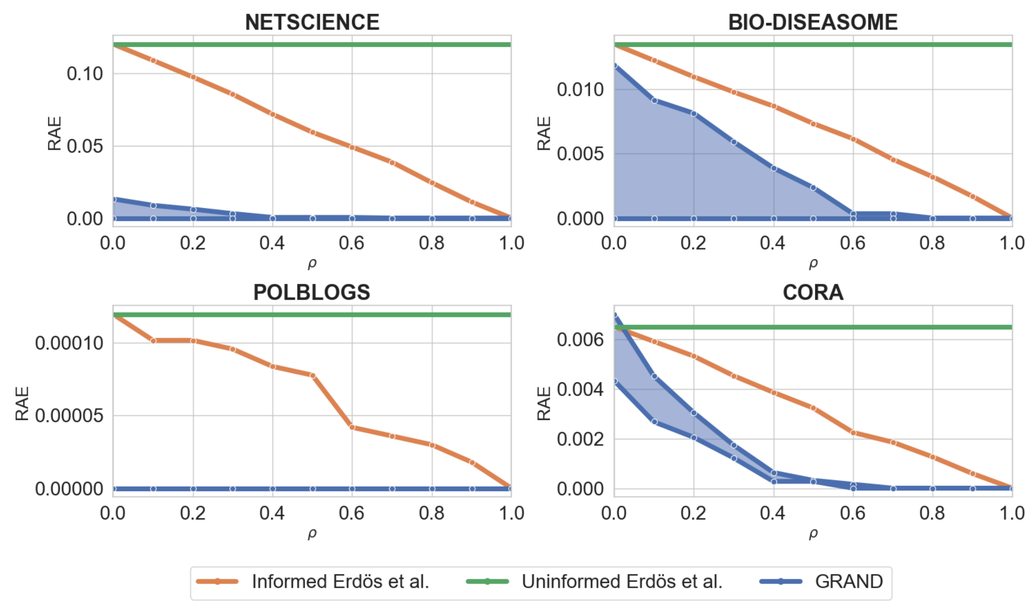
- The singular values of G^2 are the squares of the ones of G.
- Our method chooses the singular values of G that minimize its Frobenius distance with the known adjacency information
- Exploration space is reduced from **exponential** to **linear** number of possibilities.



Exploration space for spectral reconstruction. At each level, the red path yields an adjacency matrix which is close to the known adjacency information.

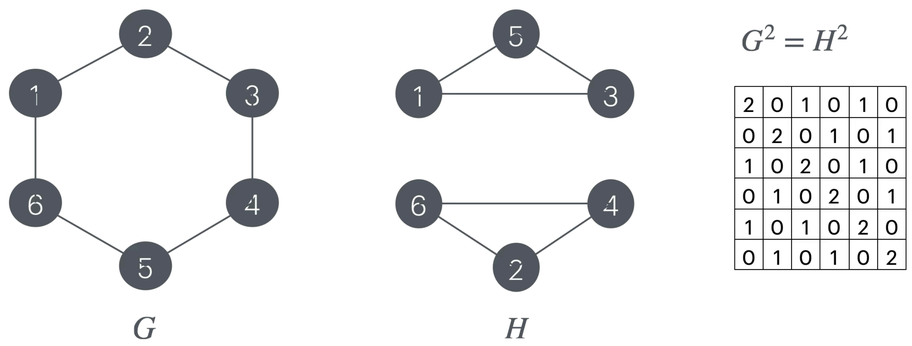
5. KEY FINDINGS

5.1. GRAPHS CAN BE PERFECTLY RECONSTRUCTED



Reconstruction performance compared to state of the art (Erdös et al. [3])

5.2. NEW GRAPH EQUIVALENCE : COSQUARENESS



6.TAKEAWAYS

- Common neighbors matrix does leak a lot of information about the initial graph
- Partial knowledge further improves graph reconstruction
- Different graphs can have the same common neighbors matrix.

REFERENCES

[1] Sofiane Azogagh, Zelma Aubin Birba, Sébastien Gambs, Marc-Olivier Killijian (2024). Crypto'Graph: Leveraging Privacy-Preserving Distributed Link Prediction for Robust Graph Learning. Scheduled to appear at CODASPY24

[2] Didem Demirag, Mina Namazi, Erman Ayday, and Jeremy Clark (2023). Privacy-Preserving Link Prediction. In Data Privacy Management, Cryptocurrencies and Blockchain Technology.

[3] Dora Erdös, Rainer Gemulla Evimaria Terzi (2012). Reconstructing Graphs from Neighborhood Data. In 2012 IEEE 12th International Conference on Data Mining.