Department of Electrical Engineering
UNIST

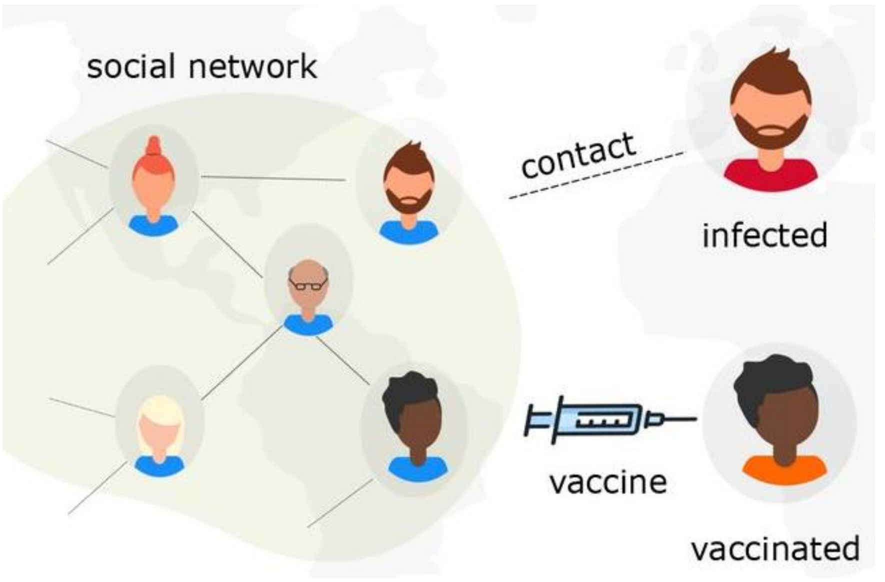
EEE490 Undergraduate Research

Degree-Preserving Local Differential Privacy for Analyzing Coreness of Decentralized Social Networks

Jiwon Sung, and **Sung Whan Yoon** (Advisor)

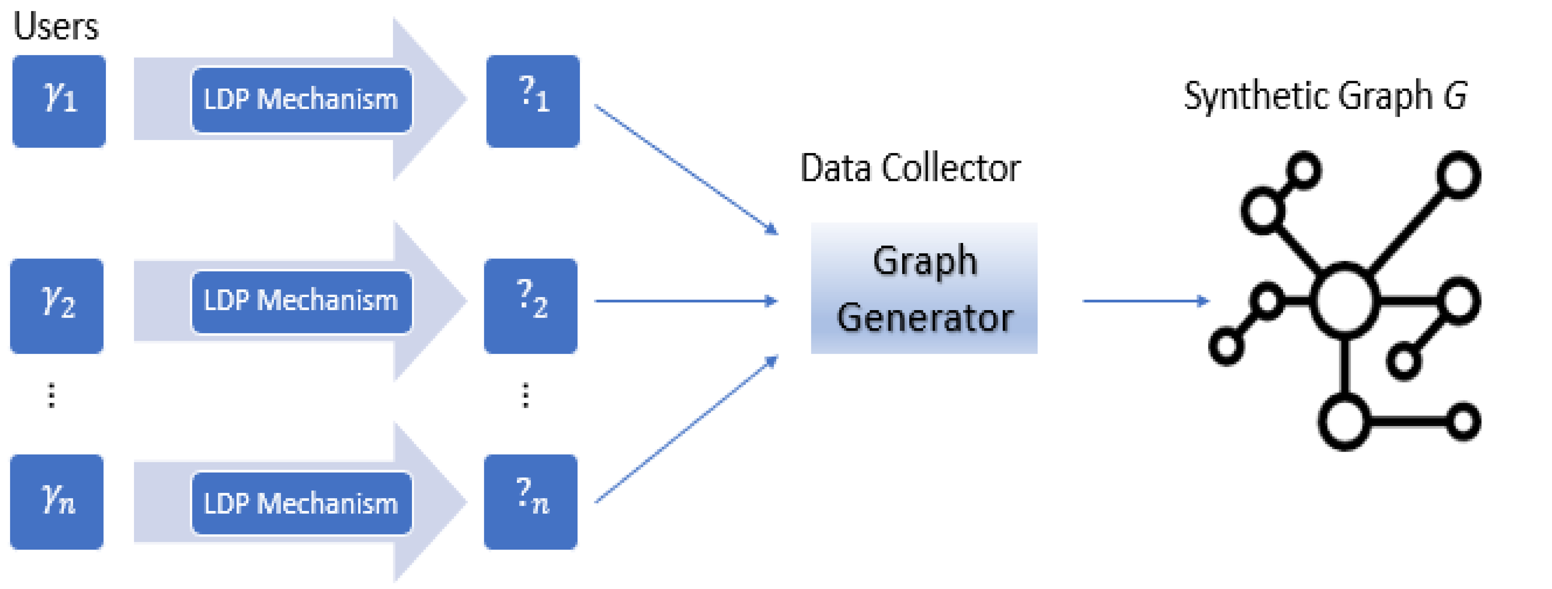
*The following research was initially conducted during my internship at InfoLab, KAIST

1. Introduction



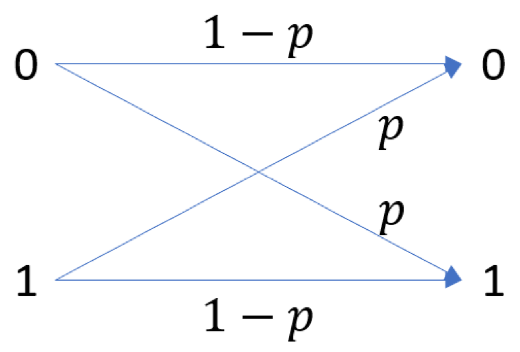
A randomized mechanism $\mathcal{M}$ satisfies ϵ-edge LDP if and only if for any two adjacency vectors $\boldsymbol{\gamma}$ and $\boldsymbol{\gamma}'$ that only differ in one bit, and for any $\boldsymbol{s} \in \text{range}(\mathcal{M})$, we have

$$\frac{\Pr[\mathcal{M}(\boldsymbol{\gamma}) = s]}{\Pr[\mathcal{M}(\boldsymbol{\gamma}') = s]} \le e^{\epsilon}$$

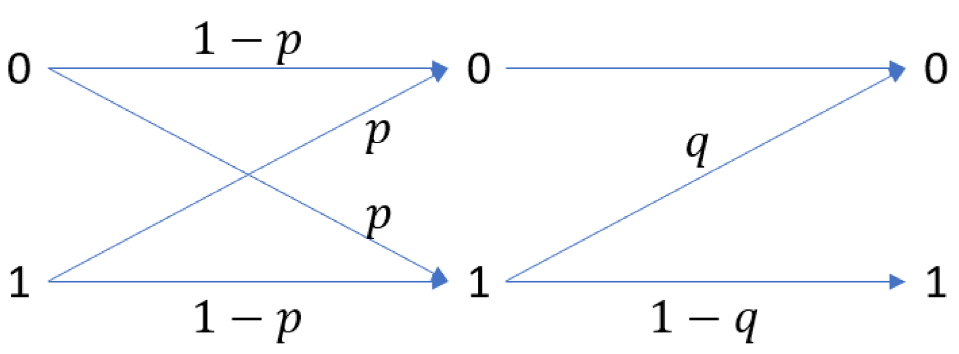


2. Prior Works & Our Proposed Method

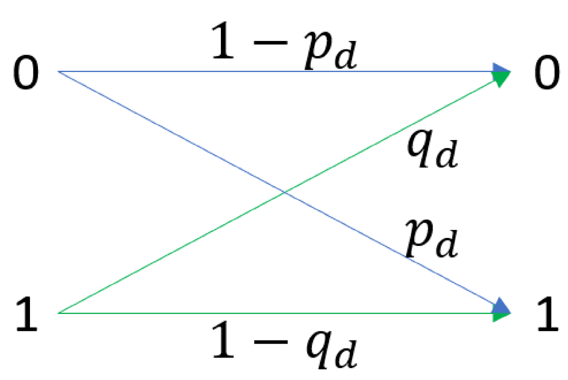
Randomized Response (**RR**)



Degree-Preserving Randomized Response (**DPRR**)



Degree-Preserving Asymmetric Bit Flipping (**DPABF, proposed**)



Degree constraint $\quad d = (n-d)p_d + d(1-q_d)$

Edge-LDP constraint $\quad e^{-\epsilon} \le \frac{1-p_d}{q_{d+1}} \le e^{\epsilon}, \quad e^{-\epsilon} \le \frac{p_d}{1-q_{d+1}} \le e^{\epsilon}$

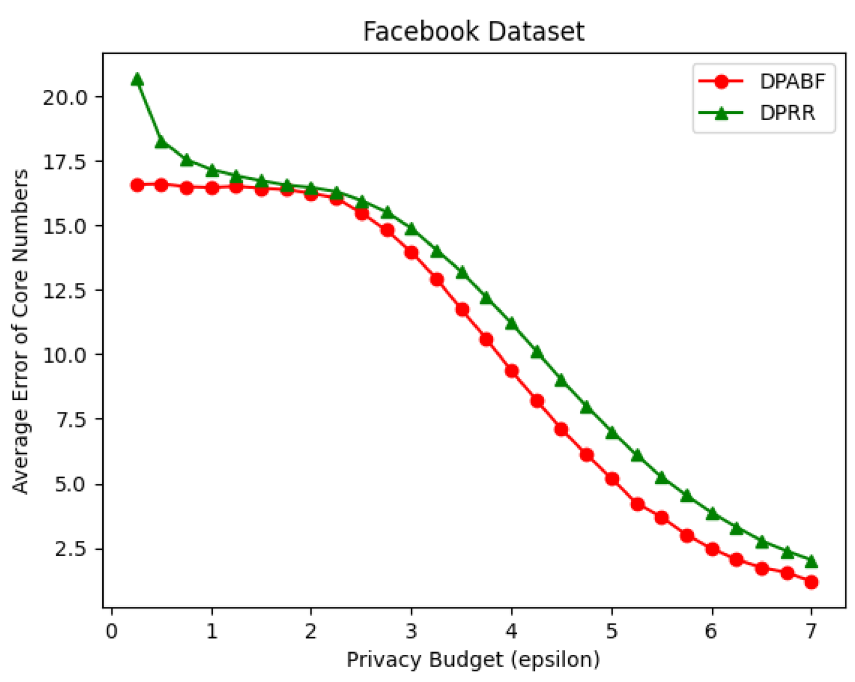
$$\text{minimize } L(\boldsymbol{A}) = \sum_{d=1}^{\lfloor \frac{n}{2} \rfloor} Var\{\deg(M(\boldsymbol{a}_d)|d)\} = \sum_{d=1}^{\lfloor \frac{n}{2} \rfloor} q_d(1-q_d) + p_d(1-p_d)$$

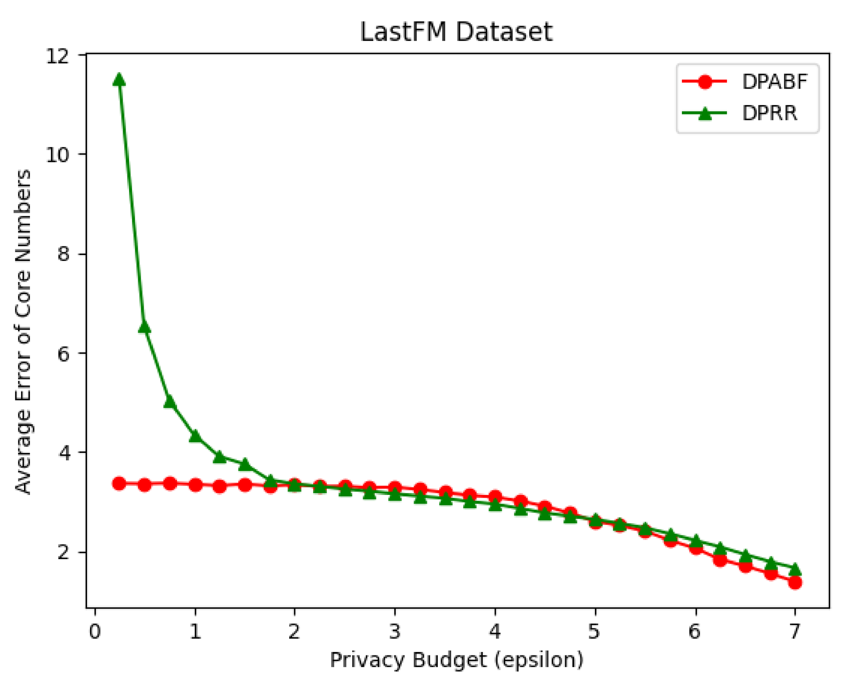
Concave, not convex!

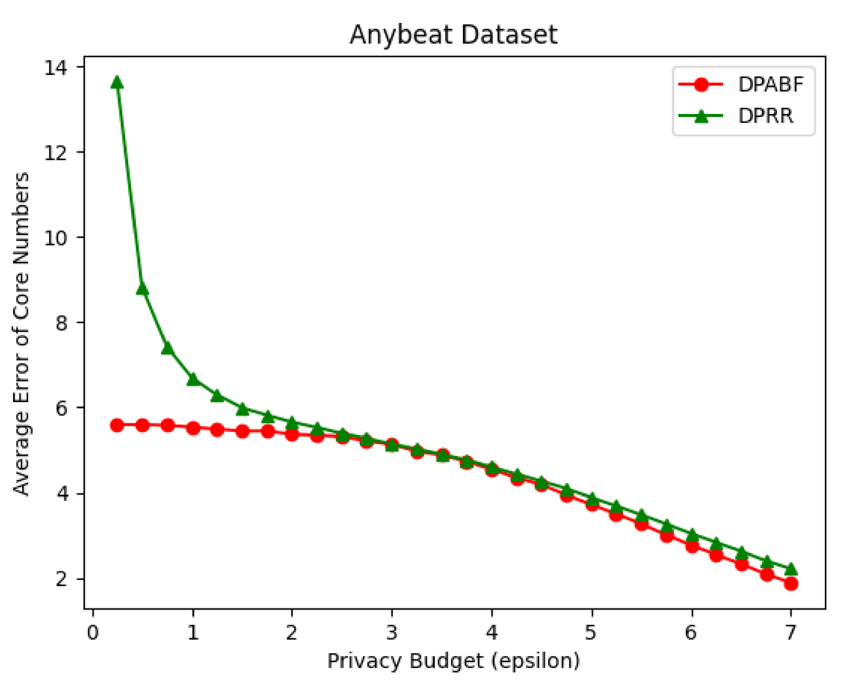
Soften the degree constraint.
Let $p_d \approx p_{d+1}$ for $1 \le d \le n-2$.
Then, $q_{d+1} = \frac{n-(d+1)}{d+1} p_{d+1} \approx \frac{n-(d+1)}{d+1} p_d$.
Thus, under the assumption that $d \le \lfloor \frac{n}{2} \rfloor$,

$$p_d = \frac{1}{e^{\epsilon} + \frac{n-(d+1)}{d+1}}, \qquad q_d = \frac{n-(d+1)}{n+1} p_d$$

3. Simulation Results



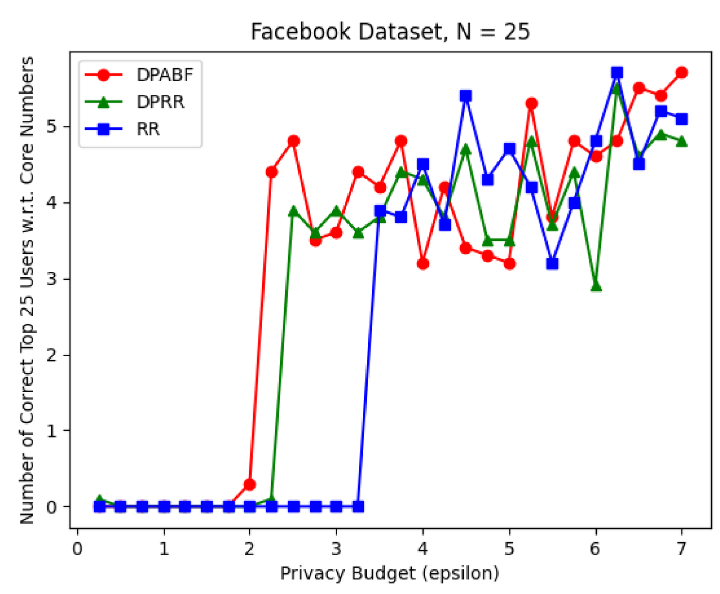


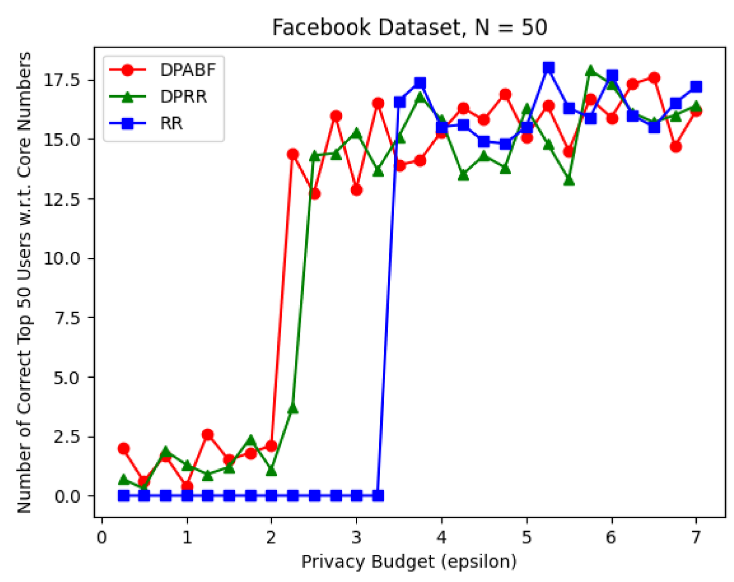


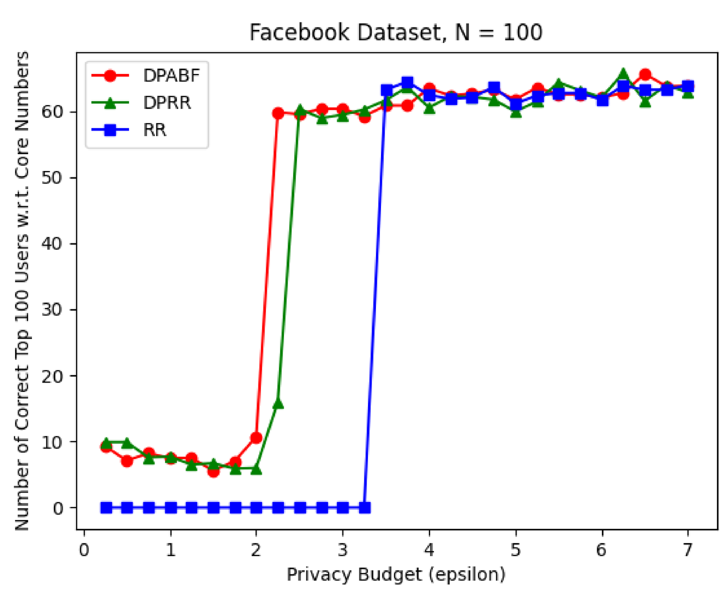
Facebook dataset
$(V, E) = (4039, 88234)$

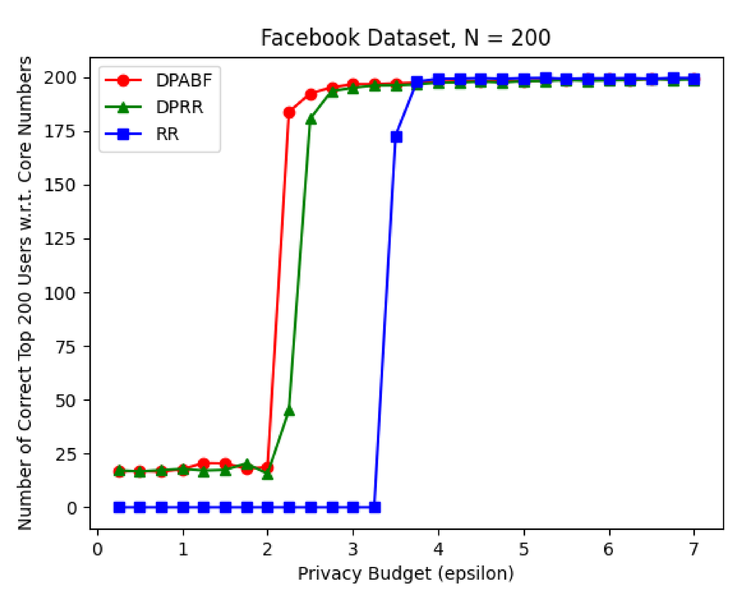
LastFM dataset
$(V, E) = (7624, 27806)$

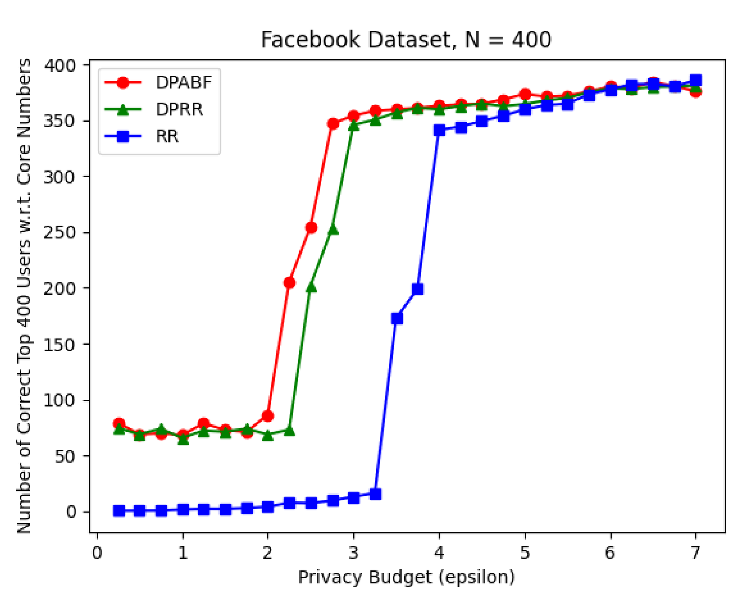
Anybeat dataset
$(V, E) = (12645, 67.1K)$











4. Conclusion

- Our proposed model can retain users' coreness more accurately in comparison to DPRR especially in high privacy regions.
- Our method doesn't split up and allocate the privacy budget to the adjacency vectors and degree values, but instead fully utilizes the whole budget to the adjacency vectors.
- We chose $p_d \approx p_{d+1}$ over $q_d \approx q_{d+1}$ because adjacent vectors of social networks are generally sparse.

References

1. S. L. Warner 1965, "Randomized Response: A Survey Technique for Eliminating Evasive Answer Bias", Journal of the American Statistical Association, vol. 60, p.63-69.
2. S. Hidano, T. Murakami 2023, "Degree-Preserving Randomized Response for Graph Neural Networks under Local Differential Privacy".
3. P. M. Pardalos, S. A. Vavasis 1991, "Quadratic programming with one negative eigenvalue is NP-hard", Journal of Global Optimization **1**: 15-22.