Cycle Counting under Local Differential Privacy for Degeneracy-bounded Graphs

Quentin Hillebrand, Vorapong Suppakitpaisarn, Tetsuo Shibuya

The University of Tokyo

STACS, March 2025

State of the Art of Private Cycle Counting

Model	Lower Bound	Upper Bound
Non-interactive	$\Omega(n^2)$	$\mathcal{O}\left(n^2\right)$
Interactive	$\Omega(n^{1.5})$	$\mathcal{O}\left(n^2\right)$

Table 1: State of the art ℓ_2-error for triangle counting [Imola et al., USENIX 2022] and [Eden et al., ICALP 2023]

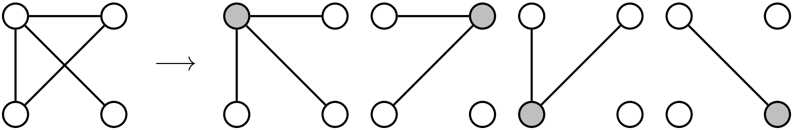
ℓ_2-error of our algorithm for triangles: $\mathcal{O}\left(n\right)$

Model	Lower Bound	Upper Bound
Non-interactive	$\Omega(n^{k-1})$	$\mathcal{O}\left(n^{k-1}\right)$
Interactive	$\Omega(n^{k-1.5})$	$\mathcal{O}\left(n^{k-1}\right)$

Table 2: Bounds on the ℓ_2-error for graphlets of size k [Suppakitpaisarn et al., AISTATS 2025]

ℓ_2-error of our algorithm for odd k-cycles: $\mathcal{O}\left(n^{\frac{k-1}{2}}\right)$

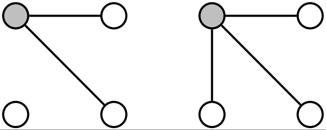
Local Differential Privacy[1] for Graph Statistics



Definition (ε-edge local differentially privacy [Qin et al., SIGSAC 2017])

Let $\varepsilon > 0$. A randomized algorithm $\mathcal{R}$ is ε-edge local differentially private on the node ν_i if, for all adjacency vectors differing by 1 bit $a \sim a'$, and for all S

$$\mathbb{P}[\mathcal{R}(a) \in S] \leq e^{\varepsilon} \cdot \mathbb{P}[\mathcal{R}(a') \in S].$$



- This definition is robust to **post-processing**
- The **composition** of 2 private mechanisms yields a private mechanism

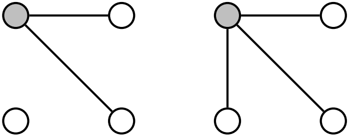
[1] Kasiviswanathan et al., "What can we learn privately?", 2011, SIAM Journal on Computing

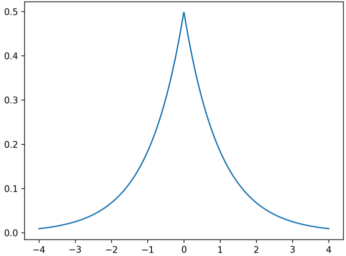
Building Block 1: Laplace Mechanism

With the **Laplace Mechanism** [Dwork et al., TCC 2006] one can privately publish **numbers**.

Global Sensitivity of function f

$$\Delta_f = \max_{a \sim a'} |f(a) - f(a')|$$





Publishing $f(x) + \mathrm{Lap}(\Delta_f/\varepsilon)$ provides ε edge local differential privacy

Building Block 2: Randomized Response

With **Randomized Response** [Warner, Journal of the American Statistical Association 1965] one can privately publish vectors of bits and thus **adjacency lists**.

1 1 0 1 1 1 1 1 0 0 0 0 0 1 1 0 0 0 0 1

$$\downarrow$$

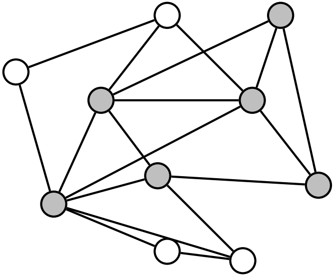
1 1 0 1 0 1 1 1 0 1 1 0 0 1 1 0 1 0 0 1

$$\mathbb{P}[\mathsf{RR}(b) = 1] = \begin{cases} \frac{e^{\varepsilon}}{1+e^{\varepsilon}} & \text{if } b = 1 \\ \frac{1}{1+e^{\varepsilon}} & \text{if } b = 0. \end{cases}$$

Degeneracy

Definition (Degeneracy [Lick and White, Canadian Journal of Mathematics 1970])

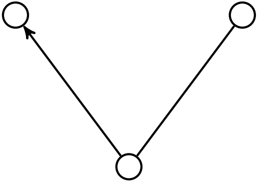
The degeneracy of a graph G is the small number $\delta(G)$ such that any subgraph of G, contains at least one node with induced degree at most $\delta(G)$ in this subgraph.



- Real-world graph tend to present an exponential degree distribution and are thus not degree-bounded [Barabási and Albert, Science 1999].
- On the other hand the degeneracy stays small in most graph irrespective of its size [Shin et al., ICDM 2016].
- Moreover, preferential attachment naturally creates degeneracy-bounded graphs [Barabási and Albert, Science 1999].

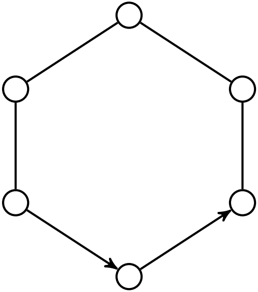
Bounds on Subgraphs Counts

S_2^* is the number of forks such that one of the node on the extremity has a higher degree than the central node.



$$S_2^* = \mathcal{O}\left(\delta^2 n\right)$$ [2]

C_{2k}^* is the number of cycles of length $2k$ such that at least 3 consecutive nodes have a monotonous degree.

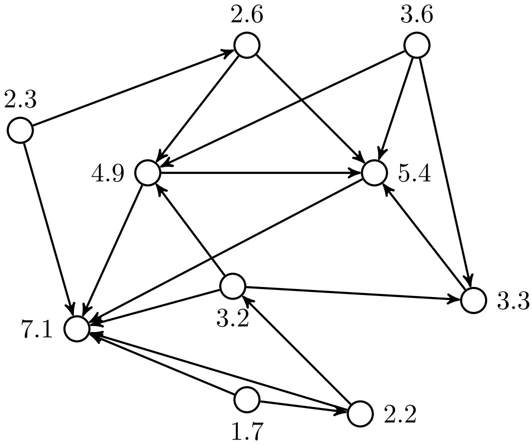


Corollary 18 of this work

$$C_{2k}^* = \mathcal{O}\left(\delta^{k+1} n^{k-1}\right)$$

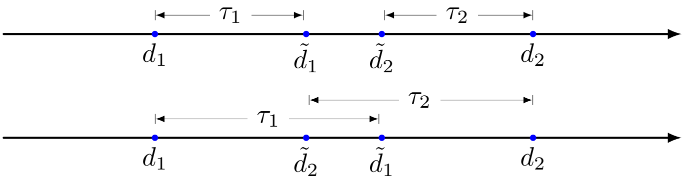
[2] Chiba and Nishizeki, "Arboricity and Subgraph Listing Algorithms", 1985, SIAM journal of computing

Preprocessing: Private Vertex Ordering



- Publish user's degree with Laplace Mechanism (building block 1)
- Orient the edges from lowest degree to highest degree

Error on the Laplace Publication

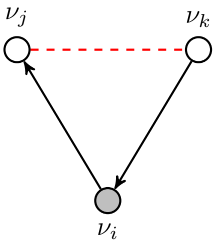


- The value of the minimum or maximum of 2 degrees is only changed if the sum of the 2 noises is larger than the gap between the 2 degrees
- The error on the minimum or maximum is never larger than the sum of the noises

Optimized Algorithm

The algorithm adapts the **2-step mechanism** described in Imola et al., USENIX 2021.

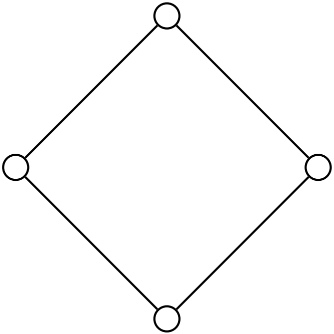
- Each user **publishes its degree** with the Laplace mechanism (building block 1)
- Those noisy degrees are used to **privately reorder the graph**
- **Each user publishes its neighbors** using Randomized Response (building block 2)
- The **central server aggregates the graph** and sends it back to all the users
- Using the graph sent by the central server, each user **locally computes the number of oriented triangles** it is involved in and publishes it with the Laplace mechanism
- The central server outputs the **sum of all of those publications**

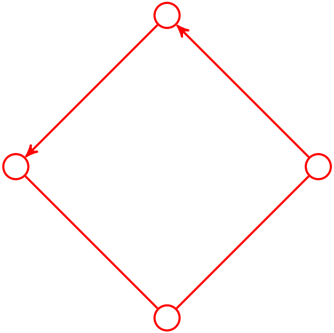


Accuracy of Private Triangle Counting

Error of **state of the art** triangle counting algorithms depend on the number of C_4.

Error of **the proposed** triangle counting algorithms depend on the number of C_4^*.





This gives a L2-error of our algorithm bounded by $\mathcal{O}(\delta^{1.5}n^{0.5} + \delta^{0.5}d_{max}^{0.5}n^{0.5})$.

Conclusion

- We introduce a light weight and efficient preprocessing step to privately reorder a graph.
- We show how this preprocessing can be used to design a triangle counting algorithm for degeneracy bounded graphs.
- The algorithm can be extended to the private estimation of the number of odd-length cycles.

Thank you for your attention!

References I

Imola, Jacob, Takao Murakami, and Kamalika Chaudhuri. "{Communication-Efficient} triangle counting under local differential privacy". In: *31st USENIX security symposium (USENIX Security 22)*. 2022, pp. 537–554.

Eden, Talya et al. "Triangle counting with local edge differential privacy". In: *arXiv preprint arXiv:2305.02263* (2023).

Suppakitpaisarn, Vorapong et al. "Counting Graphlets of Size k under Local Differential Privacy". In: *The 28th International Conference on Artificial Intelligence and Statistics*. 2025. URL: https://openreview.net/forum?id=rAvvANgQoh.

Qin, Zhan et al. "Generating synthetic decentralized social graphs with local differential privacy". In: *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*. 2017, pp. 425–438.

Kasiviswanathan, Shiva Prasad et al. "What can we learn privately?" In: *SIAM Journal on Computing* 40.3 (2011), pp. 793–826.

References II

- Dwork, Cynthia et al. "Calibrating noise to sensitivity in private data analysis". In: *Theory of Cryptography: Third Theory of Cryptography Conference*. TCC 2006. New York, NY, USA: Springer, Mar. 2006, pp. 265–284.
- Warner, Stanley L. "Randomized response: A survey technique for eliminating evasive answer bias". In: *Journal of the American Statistical Association* 60.309 (1965), pp. 63–69.
- Lick, Don R and Arthur T White. "k-Degenerate graphs". In: *Canadian Journal of Mathematics* 22.5 (1970), pp. 1082–1096.
- Barabási, Albert-László and Réka Albert. "Emergence of scaling in random networks". In: *science* 286.5439 (1999), pp. 509–512.
- Shin, Kijung, Tina Eliassi-Rad, and Christos Faloutsos. "Corescope: Graph mining using k-core analysis—patterns, anomalies and algorithms". In: *2016 IEEE 16th international conference on data mining (ICDM)*. IEEE. 2016, pp. 469–478.

References III

Chiba, Norishige and Takao Nishizeki. "Arboricity and Subgraph Listing Algorithms". In: *SIAM J. Comput.* 14.1 (1985), pp. 210–223. DOI: 10.1137/0214017. URL: https://doi.org/10.1137/0214017.

Imola, Jacob, Takao Murakami, and Kamalika Chaudhuri. "Locally differentially private analysis of graph statistics". In: *30th USENIX security symposium (USENIX Security 21)*. 2021, pp. 983–1000.