M1-ISL
Option Initiation à la Recherche. TD2

Jean-François COUCHOT
couchot[arobase]femto-st[point]fr

18 janvier 2022

On considère les articles de recherche suivants :

1. Kairouz, P., Bonawitz, K., & Ramage, D. (2016, June). Discrete distribution estimation under local privacy. In International Conference on Machine Learning (pp. 2436-2444). PMLR.
2. Wang, T., Li, N., & Jha, S. (2018, May). Locally differentially private frequent itemset mining. In 2018 IEEE Symposium on Security and Privacy (SP) (pp. 127-143). IEEE.
3. Erlingsson, Ú., Pihur, V., & Korolova, A. (2014, November). Rappor : Randomized aggregatable privacy-preserving ordinal response. In Proceedings of the 2014 ACM SIGSAC conference on computer and communications security (pp. 1054-1067).
4. Vaidya, J., Shafiq, B., Basu, A., & Hong, Y. (2013, November). Differentially private naive bayes classification. In 2013 IEEE/WIC/ACM International Joint Conferences on Web Intelligence (WI) and Intelligent Agent Technologies (IAT) (Vol. 1, pp. 571-576). IEEE.
5. Lopuhaä-Zwakenberg, M., Alishahi, M., Kivits, J., Klarenbeek, J., van der Velde, G. J., & Zannone, N. (2021, July). Comparing classifiers' performance under differential privacy. In International Conference on Security and Cryptography (SECRYPT).

Exercice 0.1 (Evaluation des expérimentations au travers des codes disponibles).

1. *Récupérer chacun des articles précédents.*
2. *Les codes associés à ces travaux informatiques sont-ils disponibles en ligne ?*
3. *Que vous inspirent les expérimentations de ces articles ?*

Exercice 0.2 (Renforcement des expérimentations). *L'article 4 ne fournit pas d'algorithme mais uniquement un pseudo code.*

1. *Rechercher dans la référence 5 une implantation du code de l'article 4.*
2. *Remarquer aussi que la bibliothèque diffprivlib semble implanter l'algorithme.*
3. *Selon vous, quelle implantation semble la plus mature ? La plus fidèle ?*
4. *Sur Colab, rejouer l'expérimentation donnée à la figure 3.(c) en ne considérant aucune contrainte sur n.*
5. *Améliorer cette expérimentation en la rendant reproductible et en donnant des indicateurs de dispersion (absents dans l'article original).*