Reading List

Information-Theory Measures and Applications:

- C. E. Shannon, "A mathematical theory of communication," The Bell System Technical Journal,, vol. 27, pp. 379–423 and 623–656, July/October 1948.
- N. Higham, M. Dennis, P. Glendinning, P. Martin, F. Santosa, and J. Tanner, Eds., The Princeton Companion to Applied Mathematics. Princeton University Press, 2015, ch. IV.36 Information Theory by Sergio Verdú.
- A. Rényi, "On measures of entropy and information," in Proceedings of the Fourth Berkeley Symposium on Mathematical Statistics and Probability, Volume 1: Contributions to the Theory of Statistics. University of California Press, 1961, pp. 547–561.
- L. Campbell, "A coding theorem and Rényi's entropy," Information and Control, vol. 8, no. 4, pp. 423 – 429, 1965.
- S. Verdú, "Error exponents and alpha-mutual information," Entropy, vol. 23, no. 2, 2021.
- Y. Shkel and S. Verdú, "A coding theorem for f-separable distortion measures," Entropy, vol. 20, no. 2, 2018.

Maximal Leakage:

- I. Issa, A. B. Wagner, and S. Kamath, "An operational approach to information leakage," IEEE Transactions on Information Theory, vol. 66, no. 3, pp. 1625–1657, 2020.
- B. Wu, A. B. Wagner, and G. E. Suh, "A case for maximal leakage as a side channel leakage metric," 2020.
- J. Liao, O. Kosut, L. Sankar, and F. du Pin Calmon, "Tunable measures for information leakage and applications to privacy-utility tradeoffs," IEEE Transactions on Information Theory, vol. 65, no. 12, pp. 8043–8066, 2019.
- C. Braun, K. Chatzikokolakis, and C. Palamidessi, "Quantitative notions of leakage for one-try attacks," Electronic Notes in Theoretical Computer Science, vol. 249, pp. 75–91, 2009, proceedings of the 25th Conference on Mathematical Foundations of Programming Semantics (MFPS 2009).

Differential Privacy:

- C. Dwork, K. Kenthapadi, F. McSherry, I. Mironov, and M. Naor, "Our data, ourselves: Privacy via distributed noise generation," in Advances in Cryptology - EUROCRYPT 2006, S. Vaudenay, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 2006, pp. 486–503.

- C. Dwork, F. McSherry, K. Nissim, and A. Smith, "Calibrating noise to sensitivity in private data analysis," in Proceedings of the Third Conference on Theory of Cryptography, ser. TCC'06. Berlin, Heidelberg: Springer-Verlag, 2006, pp. 265–284. [Online]. Available: http://dx.doi.org/10.1007/11681878 14

- C. Dwork, "Differential privacy," in Automata, Languages and Programming, M. Bugliesi, B. Preneel, V. Sassone, and I. Wegener, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2006, pp. 1–12.

- G. Barthe and F. Olmedo, "Beyond differential privacy: Composition theorems and relational logic for f-divergences between probabilistic programs," in Automata, Languages, and Programming, F. V. Fomin, R. Freivalds, M. Kwiatkowska, and D. Peleg, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013, pp. 49–60.

- S. Asoodeh, J. Liao, F. P. Calmon, O. Kosut, and L. Sankar, "Three variants of differential privacy: Lossless conversion and applications," IEEE Journal on Selected Areas in Information Theory, vol. 2, no. 1, pp. 208–222, 2021.

- P. Kairouz, S. Oh, and P. Viswanath, "The composition theorem for differential privacy," IEEE Transactions on Information Theory, vol. 63, no. 6, pp. 4037–4049, 2017.

- C. Dwork and A. Roth, "The algorithmic foundations of differential privacy," Foundations and Trendsà in Theoretical Computer Science, vol. 9, no. 3–4, pp. 211–407, 2014.

- D. Kifer and A. Machanavajjhala, "No free lunch in data privacy," in Proceedings of the 2011 ACM SIGMOD International Conference on Management of Data, ser. SIGMOD '11. New York, NY, USA: Association for Computing Machinery, 2011, pp. 193–204.

- I. Mironov, "Rényi differential privacy," 2017 IEEE 30th Computer Security Foundations Symposium (CSF), Aug 2017.

- G. Kamath and J. Ullman, "A primer on private statistics," 2020.

Differential Privacy and Machine Learning:

- M. Jagielski, J. Ullman, and A. Oprea, "Auditing differentially private machine learning: How private is private sgd?" 2020.

- D. Wang, M. Gaboardi, A. Smith, and J. Xu, "Empirical risk minimization in the non-interactive local model of differential privacy," Journal of machine learning research, vol. 21, no. 200, 2020.

- C. L. Canonne, G. Kamath, A. McMillan, A. Smith, and J. Ullman, "The structure of optimal private tests for simple hypotheses," in Proceedings of the 51st Annual ACM SIGACT Symposium on Theory of Computing, ser. STOC 2019.

Real-World Applications of Differential Privacy:

- U. Erlingsson, V. Pihur, and A. Korolova, "Rappor: Randomized aggregatable privacy-preserving ordinal response," in Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, ser. CCS '14. New York, NY, USA: Association for Computing Machinery, 2014, pp. 1054–1067. [Online]. Available: https://doi.org/10.1145/2660267.2660348

- Differential Privacy Team, "Learning with privacy at scale," https:fl//machinelearning.apple.com/ docs/learning-with-privacy-at-scale/flappledifferentialprivacysystem.pdf. [Online]. Available: https:fl/ /machinelearning.apple.com/docs/learning-with-privacy-at-scale/flappledifferentialprivacysystem.pdf

- B. Ding, J. Kulkarni, and S. Yekhanin, "Collecting telemetry data privately," in Proceedings of the 31st International Conference on Neural Information Processing Systems, ser. NIPS'17. Red Hook, NY, USA: Curran Associates Inc., 2017, pp. 3574–3583.

Other Topics:

- F. d. P. Calmon, A. Makhdoumi, M. M´edard, M. Varia, M. Christiansen, and K. R. Duffy, "Principal inertia components and applications," IEEE Transactions on Information Theory, vol. 63, no. 8, pp. 5011–5038, Aug 2017.

- Y. Y. Shkel, R. S. Blum, and H. V. Poor, "Secrecy by design with applications to privacy and compres- sion," IEEE Transactions on Information Theory, vol. 67, no. 2, pp. 824–843, 2021.

- K. Chatzikokolakis, G. Cherubin, C. Palamidessi, and C. Troncoso, "The bayes security measure," 2020.

- R. Shokri, G. Theodorakopoulos, J.-Y. Le Boudec, and J.-P. Hubaux, “Quantifying location privacy,” in 2011 IEEE Symposium on Security and Privacy, 2011, pp. 247–262.

- E. Sula and M. C. Gastpar, “Common information components analysis,” Entropy, vol. 23, no. 2, 2021.

Surveys:

- M. Bloch, O. Günlu¨, A. Yener, F. Oggier, H. V. Poor, L. Sankar, and R. F. Schaefer, “An overview of information-theoretic security and privacy: Metrics, limits and applications,” IEEE Journal on Selected Areas in Information Theory, vol. 2, no. 1, pp. 5–22, 2021.

- Wagner and D. Eckhoff, “Technical privacy metrics: A systematic survey,” ACM Comput. Surv., vol. 51, no. 3, Jun. 2018.