HW0: Citation Graph Assignment

Brandon Hosley

2020 June 3

1 Reference Graph

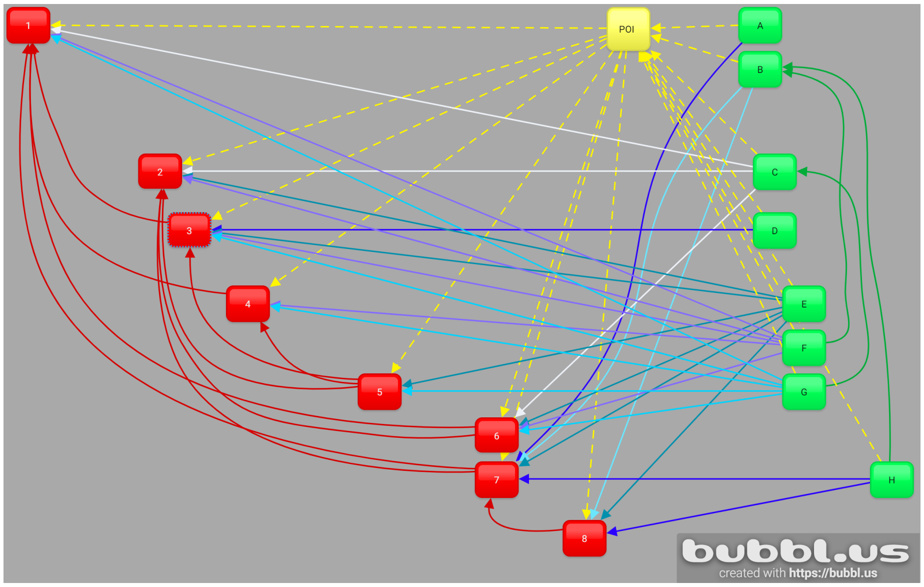

Figure 1: Reference Graph.

The papers in Figure 1 are positioned along the horizontal axis in relative chronological order (not to scale). The labels are keyed on the following page in ACM format. Red items are papers referenced by the Paper of Interest (POI). Green items reference the POI. Arrows point from one paper to another that it references.

2 References

Table 1: Documents used for Reference Graph

Label	Citation
1	Goldreich, O., Micali, S., and Wigderson, A. How to play ANY mental game. 218–229
2	Paillier, P. Public-key cryptosystems based on composite degree residuosity classes. In *International conference on the theory and applications of cryptographic techniques* (1999), Springer, pp. 223–238
3	Lindell, Y., and Pinkas, B. Privacy preserving data mining. In *Annual International Cryptology Conference* (2000), Springer, pp. 36–54
4	Goldreich, O. *Foundations of Cryptography.* No. January 2004. 2004
5	Laur, S., Lipmaa, H., and Mielikäihen, T. Cryptographically private support vector machines. *Proceedings of the ACM SIGKDD International Conference on Knowledge Discovery and Data Mining 2006* (2006), 618–624
6	Barni, M., Failla, P., Kolesnikov, V., Lazzeretti, R., Sadeghi, A. R., and Schneider, T. Secure evaluation of private linear branching programs with medical applications. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) 5789 LNCS*, July 2015 (2009), 424–439
7	Gentry, C. A Fully Homomorphic Encryption Scheme. *Dissertation*, September (2009), 169
8	Graepel, T., Lauter, K., and Naehrig, M. ML confidential: Machine learning on encrypted data. In *International Conference on Information Security and Cryptology* (2012), Springer, pp. 1–21
POI	Bost, R., Popa, R. A., Tu, S., and Goldwasser, S. Machine Learning Classification over Encrypted Data. In *NDSS* (2015), vol. 4324, p. 14

continues on next page

A Hunt, T., Zhu, Z., Xu, Y., Peter, S., and Witchel, E. Ryoan: A distributed sandbox for untrusted computation on secret data. *Proceedings of the 12th USENIX Symposium on Operating Systems Design and Implementation, OSDI 2016 35*, 4 (2016), 533–549

B Khedr, A., Gulak, G., and Vaikuntanathan, V. SHIELD: Scalable Homomorphic Implementation of Encrypted Data-Classifiers. *IEEE Transactions on Computers 65*, 9 (2016), 2848–2858

C Liu, J., Juuti, M., Lu, Y., and Asokan, N. Oblivious neural network predictions via MiniONN transformations. *Proceedings of the ACM Conference on Computer and Communications Security* (2017), 619–631

D Song, C., Ristenpart, T., and Shmatikov, V. Machine learning models that remember too much. *Proceedings of the ACM Conference on Computer and Communications Security* (2017), 587–601

E Li, T., Li, J., Liu, Z., Li, P., and Jia, C. Differentially private Naive Bayes learning over multiple data sources. *Information Sciences 444* (2018), 89–104

F zhi Gao, C., Cheng, Q., He, P., Susilo, W., and Li, J. Privacy-preserving Naive Bayes classifiers secure against the substitution-then-comparison attack. *Information Sciences 444* (2018), 72–88

G Sadegh Riazi, M., Songhori, E. M., Weinert, C., Schneider, T., Tkachenko, O., and Koushanfar, F. Chameleon: A hybrid secure computation framework for machine learning applications. *ASIACCS 2018 - Proceedings of the 2018 ACM Asia Conference on Computer and Communications Security* (2018), 707–721

H Yasumura, Y., Ishimaki, Y., and Yamana, H. Secure naïve bayes classification protocol over encrypted data using fully homomorphic encryption. *ACM International Conference Proceeding Series* (2019)