

## Bibliographie

- [1] Fatima Meskine, Safia Nait Bahloul, Mustapha Kamel Rahmouni intitulé “Privacy Preserving K-means Clustering: A Survey Research“ , papier accepté dans “The 4th International Symposium on Information Security (IS'09)”, Vilamoura, Algarve-Portugal, Proceedings publié par Springer LNCS, Nov 02-03, 2009.
- [2] Anil K. JAIN and Richard C. DUBES, Algorithms for clustering data, Prentice Hall, 1988.
- [3] L. Kaufman and P. J Rousseeuw, Finding Groups in data, An introduction to cluster analysis, John Wiley & Sons, New York, 1990.
- [4] Anil K. Jain, M.N Murty, P.J Flynn, Data Clustering: A review, ACM Computing Surveys, Vol 31, N° 3, Septembre 1999.
- [5] J. C. Dunn, "A Fuzzy Relative of the ISODATA Process and Its Use in Detecting Compact Well-Separated Clusters", Journal of Cybernetics, vol 3, pp 32-57, 1973.
- [6] A. C. Yao. How to generate and exchange secrets. In Proc. of the 27th IEEE Symposium on Foundations of Computer Science, pages 162–167. IEEE, 1986.
- [7] O. Goldreich, S. Micali et A. Wigderson, How to play any mental game, a completeness theorem for protocols with honest majority, 19<sup>th</sup> STOC, pp 218-229, 1987.
- [8] O. Goldreich, Foundations of cryptography, volume 2, Draft of a chapter on General Protocols, July 2, 2003.
- [9] Cabena Peter, Pablo Hadjnian, Rolf Stadler, Jaap Verhees and Alessandro Zanasi, Discovering Data Mining: From Concept to Implementation, Prentice Hall, 1997.
- [10] Y. Peng, G. Kou, Y. Shi, Z. Chen, "A Descriptive Framework for the Field of Data Mining and Knowledge Discovery ", International Journal of Information Technology and Decision Making, Volume 7, pp 639 – 682, 2008.
- [11] Nisbet, Robert, John Elder, Gary Miner, 'Handbook of Statistical Analysis & Data Mining Applications, Academic Press/Elsevier, 2009.
- [12] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. *Official Journal of the European Communities*, No L(281):31-50, Oct. 24 1995.
- [13] Standard for privacy of individually identifiable health information. Federal Register, 67(157):53181-53273, Aug. 14 2002.
- [14] M. Feingold, M. Corzine, M. Wyden, and M. Nelson. Data Mining Moratorium Act of 2003. U.S. Senate Bill (proposed), Jan. 16 2003.
- [15] Kantardzic Mehmed, Data Mining: Concepts, Models, Methods, and Algorithms, John Wiley & Sons, 2003.

- [16] M. J. Atallah, H. G. Elmongui, V. Deshpande, and L. B. Schwarz. Secure supply-chain protocols. In *IEEE International Conference on E-Commerce*, pages 293-302, Newport Beach, California, June 24-27 2003.
- [17] S. D. Warren and L. D. Brandeis. The Right to Privacy. *Harvard Law Review*, 4(5):193-220, 1890.
- [18] A. F. Westin. *The Right to Privacy*, Atheneum, 1967.
- [19] F. D. Schoeman. *Philosophical Dimensions of Privacy*, Cambridge Univ. Press, 1984.
- [20] S. Garfinkel. *Database Nation: The Death of the Privacy in the 21st Century*. O'Reilly & Associates, Sebastopol, CA, USA, 2001.
- [21] A. Rezgur, A. Bouguettaya, and M. Y. Eltoweissy. Privacy on the Web: Facts, Challenges, and Solutions. *IEEE Security & Privacy*, 1(6):40-49, Nov-Dec 2003.
- [22] Merriam-Webster online dictionary.
- [23] M. Ackerman, L. Cranor, and J. Reagle. Privacy in E-Commerce: Examining User Scenarios and Privacy Preferences. In *Proc. of the ACM Conference on Electronic Commerce*, pages 1-8, Denver, Colorado, USA, November 1999.
- [24] P. Jefferies. Multimedia, Cyberspace & Ethics. In *Proc. of International Conference on Information Visualisation (IV2000)*, pages 99-104, London, England, July 2000.
- [25] S. Cockcroft and P. Clutterbuck. Attitudes Towards Information Privacy. In *Proc. of the 12<sup>th</sup> Australasian Conference on Information Systems*, Australia, 2001.
- [26] C. Clifton, M. Kantarcioglu, and J. Vaidya. Defining Privacy For Data Mining. In *Proc. of the National Science Foundation Workshop on Next Generation Data Mining*, pages 126-133, Baltimore, MD, USA, November 2002.
- [27] S. R. M. Oliveira and O. R. Zaïane. Toward Standardization in Privacy-Preserving Data Mining. In *Proceedings of the 3rd. Workshop on Data Mining Standards (DM-SSP 2004)*, in conjunction with KDD 2004. Seattle, WA, USA. August, 2004.
- [28] E. Turban and J. E. Aronson. *Decision Support Systems and Intelligent Systems*. Prentice-Hall, New Jersey, USA, 2001.
- [29] P. Samarati. Protecting Respondents' Identities in Microdata Release. *IEEE Transactions on Knowledge and Data Engineering*, 13(6):1010-1027, 2001.
- [30] C. Clifton, M. Kantarcioglu, J. Vaidya, X. Lin, and M. Y. Zhu. Tools For Privacy Preserving Distributed Data Mining. *SIGKDD Explorations*, 4(2):28-34, 2002.
- [31] V. S. Verykios, E. Bertino, I. N. Fovino, L. P. Provenza, , Y. Saygin, , and Y. Theodoridis. State-of-the-art in privacy preserving data mining. *SIGMOD Rec.* 33, 1 (Mar. 2004), 50-57, 2004.

- [32] Charu. C. Aggarwal and Philip S.YU: A General Survey of Privacy-Preserving Data Mining Models and Algorithms, In Privacy-Preserving Data Mining and Algorithms book, volume 34, pp 11-52, Springer US edition, 2008.
- [33] Jaideep Vaidya, Chris Clifton, Michael Zhu, Privacy preserving data mining book, Springer US edition, 2006.
- [34] J. Vaidya, A survey A Survey of Privacy-Preserving Methods Across Vertically Partitioned Data, In Privacy-Preserving Data Mining and Algorithms book, volume 34, pp 337-358, Springer US edition, 2008.
- [35] B. Pinkas, Cryptographic Techniques for Privacy-Preserving Data Mining, SIGKDD Explorations, the newsletter of the ACM Special Interest Group on Knowledge Discovery and Data Mining, January 2003.
- [36] Agrawal R., Srikant R. Privacy-Preserving Data Mining. *Proceedings of the ACM SIGMOD Conference*, 2000, USA, pp 439-450, ACM, 2000.
- [37] Agrawal D. Aggarwal C. C. On the Design and Quantification of Privacy- Preserving Data Mining Algorithms. *ACM PODS Conference*, 2002.
- [38] Samarati P.: Protecting Respondents' Identities in Microdata Release. *IEEE Trans. Knowl. Data Eng.* 13(6): 1010-1027, 2001.
- [39] Machanavajjhala A., Gehrke J., Kifer D., and Venkitasubramaniam M.: l-diversity: Privacy Beyond k-Anonymity. *ICDE*, 2006.
- [40] Verykios V. S., Elmagarmid A., Bertino E., Saygin Y., Dasseni E.: Association Rule Hiding. *IEEE Transactions on Knowledge and Data Engineering*, 16(4), 2004.
- [41] Moskowitz I., Chang L.: A decision theoretic system for information downgrading. *Joint Conference on Information Sciences*, 2000.
- [42] Adam N., Wortmann J. C.: Security-Control Methods for Statistical Databases: A Comparison Study. *ACM Computing Surveys*, 21(4), 1989.
- [43] Elisa Bertino, Dan Lin and Wei Jiang. A Survey of Quantification of Privacy Preserving Data Mining Algorithms. In *Advances in Database Systems*, vol. 34, Springer US, 183-205, 2008.
- [44] David Wai-Lok Cheung, Vincent Ng, Ada Wai-Chee Fu, and Yongjian Fu. Efficient mining of association rules in distributed databases. *Transactions on Knowledge and Data Engineering*, 8(6):911{922, December 1996.
- [45] Rong Chen, Krishnamoorthy Sivakumar, and Hillol Kargupta. Distributed web mining using bayesian networks from multiple data streams. In *The 2001 IEEE International Conference on Data Mining*. IEEE, November 29 - December 2, 2001.
- [46] G. Jagannathan and R. Wright. "Privacy-Preserving Distributed k-means Clustering over Arbitrarily Partitioned Data", *KDD'05*, 593-599. 2005.

- [47] Y. Lindell and B. Pinkas. Privacy-preserving data mining. Advances in Cryptography (CRYPTO'00), volume 1880 of Lecture Notes in Computer science, 36-53. Springer-Verlag, 2000.
- [48] J. Ross Quinlan, Introduction of Decision trees, Machine learning 1(1), 81-106, 1986.
- [49] T. Mitchell, Machine Learning. McGraw Hill, 1997.
- [50] G. Piatetsky-Shapiro, Discovery, analysis, and presentation of strong rules, in G. Piatetsky-Shapiro & W. J. Frawley, eds, 'Knowledge Discovery in Databases', AAAI/MIT Press, Cambridge, MA, 1991.
- [51] R. Agrawal; T. Imielinski; A. Swami: *Mining Association Rules Between Sets of Items in Large Databases*", SIGMOD Conference, pp 207-216, 1993
- [52] Jochen Hipp, Ulrich Güntzer, and Gholamreza Nakhaeizadeh. Algorithms for association rule mining - A general survey and comparison. SIGKDD Explorations, 2(2):1-58, 2000.
- [53] G. Fung, A comprehensive overview of basic clustering algorithms, 2001.
- [54] P. Berkhin, Survey Of Clustering Data Mining Techniques, Rapport technique, San Jose, CA, Accrue Software, 2002.
- [55] J. MacQueen , Some methods for classification and analysis of multivariate observations, Proceedings of the Fifth Berkeley Symposium on Mathematical statistics and probability, pp. 281 – 297, Berkeley, 1967.
- [56] J. C. Bezdek , "Pattern Recognition with Fuzzy Objective Function Algorithms", Plenum Press, New York, 1981.
- [57] G. Cleuziou , L. Martin et C. Vrain . PoBOC : un algorithme de "soft-clustering" Applications à l'apprentissage de règles et au traitement de données textuelles, EGC'2004, pp. 217-228, Clermont-Ferrand, janvier 2004.
- [58] W.M Rand Objective Criteria for the evaluation of Clustering Methods. Journal of the American Statistical Association, vol.66, pp. 846-850, 1971.
- [59] P. Jaccard The distribution of the flora in the alpine zone. New Phytol, vol.11, pp. 37-50, 1912.
- [60] S.Z Slim, M.A ISMAIL, K-means-type algorithms: a generalized convergence theorem and characterization of local optimality, IEEE Transactions on Pattern Analysis and Machine Intelligence PAMI 6, pp 81-87, 1984.
- [61] G.H Ball et D.J Hall, A novel method of data analysis and pattern classification, Rapport technique, Menlo Park, CA, Stanford Research Insitute, 1965.

- [62] L. Kaufman et P.J. Rousseeuw, Clustering by means of medoids In Dodge, Y. (Ed.) Statistical Data Analysis based on the L1 Norm, pp. 405-416, 1987.
- [63] E. Diday La méthode des nuées dynamiques. Rev. Stat. Appliquées, vol.XIX, N° 2, pp. 19-34, 1975.
- [64] Y. Lindell, Composition of secure multi-party computation protocols: A comprehensive study, Springer LNCS 2815, 2003.
- [65] R. Canetti, Security and composition of multiparty cryptographic protocols, Journal of cryptology, vol 13, pp 143-202, 2000.
- [66] S. Goldwasser et L. Levin, Fair computation of general functions in presence of immoral majority, Crypto'90, Springer Verlag, LNCS 537, pp 77-93, 1990.
- [67] D. Beaver, Foundations of secure Interactive Computing, CRYPTO'91, Springer Verlag LNCS 576, pp. 377-391, 1991.
- [68] S. Micali et P. Rogaway, Secure computation, unpublished manuscript, 1992, preliminary version in CRYPTO'91, Springer-Verlag, LNCS 576, pp 392-404, 1991.
- [69] J. N Gray, Notes on database operating systems, Operating systems: An advanced course, Springer-Verlag LNCS 60, chapitre 3.F, pp465, 1978.
- [70] R. Cleve, Limits on the security of coin flips when half the processors are faulty , 18<sup>th</sup> STOC, pp 364+369, 1986.
- [71] R. Ostravsky et M. Tung, How Withstand Mobile Virus Attacks, in 10th PODC, pp 51-59, 1991.
- [72] R. Canetti et A. Herzberg, Maintaining security in the presence of transient faults, CRYPTO'94, Springer-Verlag LNCS 839, pp 425-438, 1994.
- [73] M. Ben-Or, S. Goldwasser et A. Wigderson, Completeness Theorems for Non-Cryptographic Fault-Tolerant Distributed Computation, 20<sup>th</sup> STOC, pp 1-10, 1988.
- [74] D. Chaum, C. Crepeau et I. Damgard, Multi-party Unconditionally Secure Protocols, 20th STOC, pp 11-19, 1988.
- [75] S. Golwasser, S. Micali et R.L. Rivest, A digital signature scheme secure against adaptative chosen-message attacks, SIAM Journal on Computing, vol 17, pp 281-308, 1988.
- [76] T. Rabin et M. Ben-Or, Verifiable Secret sharing and Multi-party Protocols with Honest Majority , 21st STOC, pp 73-85, 1989.
- [77] O. Goldreich, secure multi-party computation, Manuscript, v.1.4, 2002.
- [78] A. C. Yao. Protocols for secure computations (extended abstract). In 23<sup>rd</sup> Symposium on Foundations of Computer Science. IEEE, 1982.

- [79] S. Goldwasser et S. Micali, Probabilistic encryption & how to play mental poker keeping secret all partial information, Proceedings of 14<sup>th</sup> Annual ACM Symposium on Theory of Computing, 1982.
- [80] S. Goldwasser et S. Micali, Probabilistic encryption. Journal of Computer and System Sciences, vol 28, pp.270-299, 1984.
- [81] M. Bellare et P. Rogaway. Optimal Asymmetric Encryption- How to Encrypt with RSA. Advances in Cryptology, Proceedings of Eurocrypt'94, LNCS 950, Springer-Verlag, pp. 92-111, 1995.
- [82] J.C. Benaloh. Verifiable Secret-Ballot Elections. PhD Thesis, Yale University, 1988.
- [83] D. Naccache et J. Stern. A New Cryptosystem based on Higher Residues. Proceedings of the CCCS, ACM Press, pp.59-66, 1998
- [84] T. Okamoto et S. Uchiyama. A new Public key Cryptosystems as Secure as Factoring. Advances in Cryptology, Proceedings of Eurocrypt'98, LNCS 1403, Springer-Verlag, pp.308-318, 1998
- [85] P. Paillier. "Public Key Cryptosystems Based on Composite Degree Residuosity Classes." Advances in Cryptology EURO- CRYPT '99 Proceedings, LNCS 1592, pp. 223-238. 1999.
- [86] Jaideep Vaidya and Chris Clifton. Privacy Preserving Association Rule Mining in Vertically Partitioned Data. In Proceedings of The 8th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, pages 639–644, Edmonton, Alberta, Canada, July 23–26 2002.
- [87] Wenliang Du and Mikhail J. Atallah. Privacy-Preserving Statistical Analysis. In Proceedings of the 17th Annual Computer Security Applications Conference, pages 102–110, New Orleans, Louisiana, USA, December 10–14, 2001.
- [88] B. Goethals, S. Laur, H. Lipmaa and T. Mielikainen. "On Private Scalar Product Computation for Privacy-Preserving Data Mining" ICISC, LNCS 3506, pp. 104-120. 2004.
- [89] A. Shamir: How to share a secret. Communications of the ACM, 22(11), 612-613, November 1979.
- [90] T. Pedersen, E. Savas, Y. Saygin, Secret sharing vs encryption-ensembled techniques for privacy-preserving datamining, Joint UNECE/Eurostat work session on statistical data confidentiality, Manchester, UK, 17-19 December 2007.
- [91] Clifton, C., Kantarcioglu, M., Vaidya, J., Lin, X., and Zhu, M. Y. Tools for privacy preserving data mining. *SIGKDD Explorations*, 4(2) pp 28–34, 2002
- [92] J. Vaidya, C. Clifton: Privacy-preserving k-means clustering over vertically partitioned data. In Proc. of the 19th ACM SIGKDD international conference on Knowledge discovery and data mining, 206-215, 2003.

- [93] Samet, A. Miri, L. Orozco-Barbosa: Privacy-preserving k-means clustering in Multi-party environment, International Conference on Security and Cryptography, SCRYPT 2007.
- [94] Clifton, C., Kantarcioglu, M., Vaidya, J., Lin, X., and Zhu, M. Y. Tools for privacy preserving data mining. *SIGKDD Explorations*, 4(2) pp 28–34, 2002.
- [95] M. C. Doganay, T. B. Pederson, Y. Saygin, E. Savas: A. Levi, Distributed Privacy Preserving Clustering with Additive Secret Sharing, In Proceeding of the 2008 international workshop on Privacy and anonymity in information society table, ACM Conferences, Nantes, France.
- [96] Selim Volkan Kaya. Toolbox for Privacy Preserving Data Mining. Master's thesis, Sabanci University, Istanbul, TURKEY, July 2007.
- [97] S. Jha, L. Kruger and P. Mc Daniel: Privacy-Preserving Clustering, European Symposium on research in computer security, 397-417, 2005.
- [98] Naor, M. and Pinkas, B. Efficient oblivious transfer protocols. In Proc. of the 12th annual ACM-SIAM symposium on Discrete algorithms, pages 448–457, 2001.
- [99] Xiao, M.-J., Huang, L.-S., Luo, Y.-L., and Shen, H. Privacy preserving ID3 algorithm over horizontally partitioned data. In *Parallel and Distributed Computing, Applications and Technologies*, pages 239–243. 2005.
- [100] J. Bar-Ilan and D. Beaver, Non cryptographic fault-tolerant computing in constant number of rounds of interaction, In 18<sup>th</sup> ACM Proceeding , Symposium on Principales of Distributed Computing, pp 201-209, ACM Press, 1989.
- [101] C. Su, F. Bao, J. Zhou, T. Takagi, K. Sakurai: Privacy-Preserving Two party K-means Clustering via secure approximation, 21<sup>st</sup> Inter. Conf. on advanced Information Networking and Applications Workshops, 385-391. 2007.
- [102] E. Kiltz, G. Leander and J. Malone-Lee. *Secure Computation of the Mean and Related Statistics*. Theory of Cryptography Conference, 2005.
- [103] P. Bunn, R. Ostrovsky: Secure Two Party k-means clustering, CCS'07, Alexandria, Virginia, USA, October 29 – November 2, 2007.
- [104] J. Sakuma and S. Kobayashi, Large-scale k-means Clustering with User-Centric Privacy Preservation, volume 5012 of Lecture Notes in Computer science, 320-322. Springer, 2008.
- [105] W. Kowalczyk and N. Vlassis, Newcast EM, NIPS 17, MIT Press, 2005.