BIBLIOGRAPHY

1. Agrawal R, and Srikant R, “Privacy-Preserving Data Mining”, *proceedings of the 2000 ACM SIGMOD on management of data*, Dallas, TX USA, 439-450, May 15-18 2000.
2. Atallah M J and Du W, “Secure multi-party computational geometry”, *proceeding of the Seventh International Workshop on Algorithms and Data Structures*,165-179, 2001.
3. Agrawal R, Evfimievski A, and Srikant R, “Information Sharing Across Private Databases”, *proceedings of the ACM SIGMOD, International Conference on Management of Data*, San Diego, CA, 2003.
4. Brickell J and Shmatikov V, “Privacy-Preserving Graph Algorithms in the Semi-honest Model”, *ASIACRYPT 2005, LNCS 3788*, 236–252, 2005.
5. Bryant R, Katz R, and Lazowska E D, "Big- Data Computing: Creating Revolutionary Breakthroughs in Commerce, Science and Society”, *http://www.cra.org/ccc/initiatives*, 1-15, 2008.
6. Barni M, Failla P, Lazzeretti R, “Efficient Privacy-Preserving Classification Of ECG Signals”, *Information Forensics and Security, WIFS*, First IEEE International Workshop, 91 – 95, 6-9, December 2009.
7. Bogetoft P, Christensen D, *et al.* “Secure multiparty computation goes live”, *Financial Cryptography and Data Security (FC '09), Springer-Verlag*, 325-343, 2009.
8. Barni M, Pierluigi F, Riccardo L, Sadeghi A, and Schneider T, "Privacy-preserving ECG classification with branching programs and neural networks." *Information Forensics and Security*, IEEE Transactions 6(2), 452-468, 2011.
9. Bogdanov D, Riivo T, and Willemson J, "Deploying secure multi-party computation for financial data analysis", *Financial Cryptography and Data Security*. Springer Berlin Heidelberg, 57-64, 2012.
10. Bogdanov D, “Sharemind: programmable secure computations with practical applications”, Ph.D. thesis, University of Tartu, http://hdl. handle.net/10062/29041, 2013.

11. Clifton C, Kantarcioglu M, Vaidya, X. Lin, and M. Y. Zhu, “Tools for Privacy-Preserving Distributed Data Mining,” *J. SIGKDD Explorations, Newsletter,* 4(2), *ACM Press*, 28-34, December, 2002.
12. *Chowdhury S, “Data Mining and Beyond”, proceeding of Journal of American Academy of Business, Cambridge, 576-580, March, 2003.*
13. *Chowdhry S, “Trends in Databases Tools and Technologies”, “the Business Review”, Cambridge, 7, 20-25, 2007.*
14. Dorothy E D and Denning P J, “Data Security”, *ACM Computing Surveys 11(3),* ISSN: 0360-0300, 227 – 249, September, 1979.
15. Du W and Atallah M J, “Protocols for Secure Remote Database Access with Approximate Matching”, *7th ACM Conference on Computer and Communications Security (ACMCCS 2000), the First Workshop on Security and Privacy in E-Commerce*, Athens, Greece, November, 2000.
16. Du W, and Atallah M J, “Privacy-Preserving Cooperative statistical analysis,” *14th IEEE Computer Security Foundations Workshop*, Nova Scotia, Canada, 273–282, June, 2001.
17. Du W and Atallah M J, “Secure multi-party computation problems and their applications: A review and open problem”, in *New Security Paradigms Workshop, Cloudcroft*, New Mexico, USA, 11-20, 11-13, September, 2001.
18. Dalhli M, “Lecture notes on Secure Multi-party Computation”, *an advance course in computer and network security*, Hebrew University, Springer, 2002.
19. Datta S, Bhaduri K, Giannella C, and Wolff R, “Distributed data mining in peer-to-peer networks”, *IEEE Internet Computing special issue on distributed data mining*, 10(4), 18–26, 2006.
20. Dinh T, Tuan A, Thanh V, and Datta A, "Delegated secure sum service for distributed data mining in multi-cloud settings", *CoRR*, 2012.
21. Dunning L A, and Ray K, "Privacy Preserving Data Sharing With Anonymous ID Assignment" Information Forensics and Security”, *IEEE Transactions on Information Forensics and Security,* 8(2), 402-413, 2013.
22. Even S, Goldreich O, and Lempel A, “A randomized protocol for signing contracts”, *Communications of the ACM,* 28(6), 637-647, 1985.
23. Erman A, Raisaro J L, McLaren P J, Fellay J, and Hubaux J P, "Privacy-Preserving Computation of Disease Risk by Using Genomic, Clinical, and

Environmental Data", *proceedings of USENIX Security Workshop on Health Information Technologies* (HealthTech), 2013.

24. Fournet C, Kohlweiss M, and Danezis G, and Luo Zhengqin, "ZQL: A compiler for privacy-preserving data processing", *USENIX Security*, 163-178, 2013.
25. Goldreich O, Micali S, and Wigderson A, "How to play any mental game - a completeness theorem for protocols with honest majority", *19th ACM Symposium on the theory of Computing*, 218-229, 1987.
26. Goldwasser S., "Invited talk: multi-party computation past and present", *MIT laboratory for computer Science*, USA, 1996.
27. Jurczyk P, Xiong L, and Goryczka S, "Dobjects+: enabling privacy-preserving data federation services", *International Conference on Data Engineering (ICDE)*, IEEE 28th, 1325-1328, 2012.
28. Kalle L, "Different perspectives on information system problem and solution", *ACM computing surveys (CSUR)*, 19(1), 5-46, March, 1987.
29. Karr A, Xiaodong L, Sanil A P, and Reiter J, **"**Secure Regression on Distributed Databases", *American Statistical Association, Institute of Mathematical Statistics, and Interface Foundation of North America Journal of Computational and Graphical Statistics*, 14(2), 263–279, 2005.
30. Kargupta H, Das K, and Liu K, "A game theoretic approach toward multi-party privacy preserving distributed data mining," *Technical Report TR_CS_01_07*, 24 April, 2007.
31. Kamara S, Payman M, and Raykova M, "Outsourcing Multi-Party Computation", *IACR Cryptology ePrint Archive*, 272, 2011.
32. Kui R, Wang C, and Wang Q, "Security challenges for the public cloud", *Internet Computing IEEE*, 16(1), 69-73, 2012.
33. Kolesnikov V, Sadeghi A, and Schneider T, "A systematic approach to practically efficient general two-party secure function evaluation protocols and their modular design", *Journal of Computer Security*, 21(2), 283-315, 2013.
34. Lindell Y, and Pinkas B, "Privacy preserving data mining", *Journal of cryptology*, 15(3), 177-206, 2002.
35. Liu K, Kargupta H, and Ryan J, "Random projection-based multiplicative data perturbation for privacy preserving distributed data mining", *IEEE transactions on knowledge and data engineering (TKDE)*, 18(1), 92–106, January, 2006.

36. Lindell Y and Pinkas B, “An efficient protocol for secure two-party computation in the presence of malicious adversaries”, *proceedings of the 26th annual international conference on Advances in Cryptology (Eurocrypt '07)*, Springer-Verlag, Berlin, Heidelberg, 52-78, 2007.
37. Lindell Y, Pinkas B, and Smart N, “Implementing two-party computation efficiently with security against malicious adversaries”, *proceedings of the 6th international conference on Security and Cryptography for Networks (SCN '08), Springer-Verlag*, Berlin, Heidelberg, 2-20, 2008.
38. Lindell Y and Pinkas B, "Secure multiparty computation for privacy-preserving data mining." *Journal of Privacy and Confidentiality*, 1(1), 1-39, 2009.
39. Maurer U, “Keynote talk: The role of cryptography in database security”, *proceeding of the ACM SIGMOD 04, International conference on management of data*, Paris, France, 29-35, 13-18 June, 2004.
40. Mishra D K, and Chandwani M, "Anonymity enabled secure multi-party computation for Indian BPO", *proceedings of the TENCON 2007,* IEEE Region 10 Conference, 1-4, 2007.
41. Mishra D K and Chandwani M, “Extended Protocol for Secure Multiparty Computation using Ambiguous Identity”, *WSEAS Transaction on Computer Research*, 2(2), February, 2007.
42. Mishra D K, and Chandwani M, "A zero-hacking protocol for secure multiparty computation using multiple TTP", *TENCON 2008-IEEE Region 10 Conference*, 2008.
43. Mishra D K, Koria N, Kapoor N and Bahety R, “A Secure Multi-Party Computation Protocol for Malicious Computation Prevention for Preserving Privacy during Data Mining,” *International Journal of Computer Science and Information Security*, 3(1), 2009.
44. Miyaji A, and Rahman M S, "Privacy-preserving Two-party Rational Set Intersection Protocol." *Informatica (Slovenia)*, 36(3), 277-286, 2012.
45. Nergiz M E, Abdullah E C¸ Pedersen T B, and Saygin Y, "A look-ahead approach to secure multiparty protocols", *Knowledge and Data Engineering*, IEEE Transactions, 24(7), 1170-1185, 2012.
46. Omote K, and Miyaji A, “A practical English auction with one-time registration”, *proceeding of fifth Australasian conference on information*

security and privacy, *ACISP 2000,* Brisbane, Australia, 427-442, 10-12 July, 2000.

47. Oleshchuk V and Zadorozhny V, (2007), "Secure Multi-Party Computations and Privacy Preservation: Results and Open Problems", *Telektronikk: Telenor's Journal of Technology,* 103(2), 2007.
48. Pinkas B, Schneider T, Smart N, and Williams S, "Secure two-party computation is practical*", Advances in Cryptology - ASIACRYPT '09, Springer-Verlag*, 250-267, 2009.
49. Padwalkar A, Pande P and Dave V, "Secure Multi-Party Computation Protocol: Basic Buidling Block Methods**",** *National Conference on Innovations in IT and Management: 2014*, SIMCA, Pune, India, ISBN: 978-81-927230-0-*6*, 128-131, February, 2014.
50. Qingkai M, Wei H, I-Ling Y, and Bastani F, "Multiparty computation with full computational power and reduced overhead", *proceeding of eighth IEEE international symposium on high assurance system engineering*, 241-248, 25-26 March, 2004.
51. Rabin M, "How to exchange secrets by oblivious transfer", *Tech. Report Memo TR-81, Aiken Computation Laboratory,* 1981.
52. Ronald C, Ivan D, "Multi-party computation: an introduction", *Lecture Notes, 2004*.
53. Raymond W, Jiuyong L, WaiChee A and Wang K, "(α, k)-anonymity: an enhanced k-anonymity model for privacy preserving data publishing", *proceedings of the 12th ACM SIGKDD international conference on Knowledge discovery and data mining*, 2006.
54. Rane S, Wang Y, Draper S, and Ishwar P, "Secure Biometrics: Concepts, Authentication Architectures and Challenges", *arXiv preprint arXiv:1305.4832,* 2013.
55. Srivatsava R, Kasiviswanathan S P, and Smith A, "Composition attacks and auxiliary information in data privacy", *proceedings of the 14th ACM SIGKDD international conference on Knowledge discovery and data mining*, 2008.
56. Sheikh R, Kumar B, and Mishra D K, "Privacy-Preserving k-Secure Sum Protocol", *International Journal of Computer Science and Information Security,* 6(2), 184-188, November, 2009.

57. Sheikh R, Kumar B, and Mishra D K, "Changing Neighbors k Secure Sum Protocol for Secure Multi Party Computation", *arXiv preprint arXiv:1002.2409*, 2010.
58. Sadeghi A, Schneider T, and Winandy M, "Token-based cloud computing." *Trust and Trustworthy Computing. Springer Berlin Heidelberg*, 417-429, 2010.
59. Sheikh R, Kumar B, and Mishra D K, "A distributed k-secure sum protocol for secure multi-party computations", *arXiv preprint arXiv:1003.4071*, 2010.
60. Sheikh R, Kumar B, and Mishra D K, "A Modified ck-Secure Sum Protocol for Multi-Party Computation", *arXiv preprint arXiv:1002.4000*, 2010.
61. Sheikh R, Kumar B, and Mishra D K, "Secure Multiparty Computation: From Millionaires Problem to Anonymizer", *Information Security Journal A Global Perspective*, 2011.
62. Trevathan J, "Security anonymity and trust in electronic auctions," *Crossroad archive, ACM Press,* 11(3), May, 2005.
63. Teo S G, Vincent L, and Shuguo H, "A Study of Efficiency and Accuracy of Secure Multiparty Protocol in Privacy-Preserving Data Mining", *Advanced Information Networking and Applications Workshops (WAINA)*, IEEE 26th International Conference, 85-90, 2012.
64. Verykios V S, Elmagarmid A K, Elisa B, Saygin Y, and Elena D, "Association rule hiding", in *IEEE transactions on knowledge and data engineering*, 15(3), May/June, 2003.
65. Verykios V S, Bertino E, *et al.*, "State-of-the-art in Privacy Preserving Data Mining", *proceeding of SIGMOD Record*, 33(1), 50-57, March, 2004.
66. Wahlstrom K, and John F, "On the impact of knowledge discovery and data mining", *proceeding of ACM international conference proceeding series,* 7, 22-27, 2000.
67. Williams P, Vincent E, *et al.*, "Prime III: Where Usable Security and Electronic Voting Meet", *USES'07, www.usablesecurity.org*, 2007.
68. Yao A, "Protocols for secure computations", *IEEE Symposium on Foundations of Computer Science (FOCS '82)*, IEEE Computer Society, 160-164, 1982.
69. Yao A, "How to generate and exchange secretes", *proceeding twenty seventh IEEE symposium on foundation of computer science*, 162-167, 1986.

70. Zhan Z, and Wenliang D, “Privacy-preserving data mining using multi-group randomized response techniques”, 1(2), 2004.