D8. Research Opportunity and Performance Evidence (ROPE)—Publication list

Bibliometrics retrieved May 28, 2018: citation counts from Google Scholar; A*,A,B,C conference rankings from CORE2018; A*,A,B,C journal rankings from ERA2010 and 2015 5-year impact factors from Thomson Reuters. Project ID and years funded are included for papers supported by an ARC grant.

Authored Books

1. Joseph, Anthony D., Blaine Nelson, Benjamin I. P. Rubinstein and J. D. Tygar. *Adversarial Machine Learning*. in press. Cambridge University Press, 2018.
2. Verkade, Heather, Terrence D. Mulhern, Jason M. Lodge, Kristine Elliott, Simon Cropper, Benjamin I. P. Rubinstein, Allen Espinosa, Michelle Livett, Laura Dooley, Sarah Frankland and Raoul Mulder. *Misconceptions as a trigger for enhancing student learning in higher education: A handbook for educators*. Published by The University of Melbourne, 2017. ISBN: 978 0 7340 5410 4.

Book Chapters

3. Rubinstein, J. Hyam, Benjamin I. P. Rubinstein and Peter L. Bartlett. "Bounding embeddings of VC classes into maximum classes". In: *Measures of Complexity*. Ed. by V. Vovk, H. Papadopoulos and A. Gammerman. Springer, 2015, pp. 303–325. **(5 citations)**
4. Biggio, Battista, Igino Corona, Blaine Nelson, Benjamin I. P. Rubinstein, Davide Maiorca, Giorgio Fumera, Giorgio Giacinto and Fabio Roli. "Security evaluation of support vector machines in adversarial environments". In: *Support Vector Machines Applications*. Ed. by Y. Ma and G. Guo. Springer, Feb. 2014, pp. 105–153. **(28 citations)**
5. Nelson, Blaine, Marco Barreno, Fuching Jack Chi, Anthony D. Joseph, Benjamin I. P. Rubinstein, Udam Saini, Charles Sutton, J. D. Tygar and Kai Xia. "Misleading learners: Co-opting your spam filter". In: *Machine Learning in Cyber Trust: Security, Privacy, and Reliability*. Springer, 2009, pp. 17–51. **(49 citations)**

Refereed Journal Articles

6. Fanaeepour, Maryam and Benjamin I. P. Rubinstein. "Differentially private counting of users' spatial regions". In: *Knowledge and Information Systems* 54.1 (Jan. 2018), pp. 1–28.
7. Lyu, Lingjuan, Karthik Nandakumar, Benjamin I. P. Rubinstein, Jiong Jin, Justin Bedo and Marimuthu Palaniswami. "PPFA: Privacy-Preserving Fog-enabled Aggregation in Smart Grid". In: *IEEE Transactions on Industrial Informatics* (Feb. 2018). in press.
8. Marchant, Neil G. and Benjamin I. P. Rubinstein. "In Search of an Entity Resolution OASIS: Optimal Asymptotic Sequential Importance Sampling". In: *Proceedings of the VLDB Endowment* 10.11 (Feb. 2017), pp. 1322–1333. **(1 citation)**
9. Dimitrakakis, Christos, Blaine Nelson, Zuhe Zhang, Aikateirni Mitrokotsa and Benjamin I. P. Rubinstein. "Differential privacy for Bayesian inference through posterior sampling". In: *Journal of Machine Learning Research* 18.11 (Mar. 2017), pp. 1–39. **(7 citations)**
10. Lau, Lawrence, Yamuna Kankanige, Benjamin Rubinstein, Robert Jones, Christopher Christophi, Vijayaragavan Muralidharan and James Bailey. "Machine-learning algorithms predict graft failure after liver transplantation". In: *Transplantation* 101.4 (Apr. 2017), pp. 125–132. **(3 citations)**
11. Han, Yi, Tansu Alpcan, Jeffrey Chan, Christopher Leckie and Benjamin I. P. Rubinstein. "A game theoretical approach to defend against co-resident attacks in cloud computing: Preventing co-residence using semi-supervised learning". In: *IEEE Transactions on information Forensics and Security* 11.3 (Mar. 2016), pp. 556–570. **(18 citations)**
12. Zhang, Duo, Benjamin I. P. Rubinstein and Jim Gemmell. "Principled graph matching algorithms for integrating multiple data sources". In: *IEEE Transactions on Knowledge and Data Engineering* 27.10 (Apr. 2015), pp. 2784–2796. **(6 citations)**
13. Fanaeepour, Maryam, Lars Kulik, Egemen Tanin and Benjamin I. P. Rubinstein. "The CASE histogram: Privacy-aware processing of trajectory data using aggregates". In: *GeoInformatica* 19.4 (Jul. 2015), pp. 747–798. **(7 citations)**

14. Zhao, Bo, Benjamin I. P. Rubinstein, Jim Gemmell and Jiawei Han. “A Bayesian approach to discovering truth from conflicting sources for data integration”. In: *Proceedings of the VLDB Endowment* 5.6 (Feb. 2012), pp. 550–561. **(234 citations)**

15. Rubinstein, Benjamin I. P. and Aleksandr Simma. “On the stability of empirical risk minimization in the presence of multiple risk minimizers”. In: *IEEE Transactions on Information Theory* 58.7 (Jul. 2012), pp. 4160–4163. **(2 citations)**

16. Nelson, Blaine, Benjamin I. P. Rubinstein, Ling Huang, Anthony D. Joseph, Steven J. Lee, Satish Rao and J. D. Tygar. “Query strategies for evading convex-inducing classifiers”. In: *Journal of Machine Learning Research* 13.May (2012), pp. 1293–1332. **(59 citations)**

17. Rubinstein, Benjamin I. P. and J. Hyam Rubinstein. “A geometric approach to sample compression”. In: *Journal of Machine Learning Research* 13.Apr (2012), pp. 1221–1261. **(31 citations)**

18. Rubinstein, Benjamin I. P., Peter L. Bartlett, Ling Huang and Nina Taft. “Learning in a large function space: Privacy-preserving mechanisms for SVM learning”. In: *Journal of Privacy and Confidentiality* 4.1 (Aug. 2012). Special Issue on Statistical and Learning-Theoretic Challenges in Data Privacy, pp. 65–100. **(117 citations)**

19. Barth, Adam, Benjamin I. P. Rubinstein, Mukund Sundararajan, John C Mitchell, Dawn Song and Peter L. Bartlett. “A learning-based approach to reactive security”. In: *IEEE Transactions on Dependable and Secure Computing* 9.4 (Jul. 2012), pp. 482–493. **(14 citations)**

20. Rubinstein, Benjamin I. P., Peter L. Bartlett and J. Hyam Rubinstein. “Shifting: One-inclusion mistake bounds and sample compression”. In: *Journal of Computer and System Sciences* 75.1 (2009), pp. 37–59. **(35 citations)**

21. Rubinstein, Benjamin I. P., Blaine Nelson, Ling Huang, Anthony D. Joseph, Shing-hon Lau, Satish Rao, Nina Taft and J. D. Tygar. “Stealthy poisoning attacks on PCA-based anomaly detectors”. In: *ACM SIGMETRICS Performance Evaluation Review* 37.2 (2009), pp. 73–74. **(34 citations)**

22. Rubinstein, Benjamin I. P., Jon McAuliffe, Simon Cawley, Marimuthu Palaniswami, Kotagiri Ramamohanarao and Terence P. Speed. “Machine learning in low-level microarray analysis”. In: *ACM SIGKDD Explorations Newsletter* 5.2 (2003). Special Issue on Microarray Data Mining, pp. 130–139. **(22 citations)**

Fully-Refereed Conference Proceedings

23. Fanaeepour, Maryam and Benjamin I. P. Rubinstein. “Histogramming Privately Ever After: Differentially-Private Data-Dependent Error Bound Optimisation”. In: *Proceedings of the 34th International Conference on Data Engineering*. ICDE. IEEE. 2018.

24. Aye, Zay Maung Maung, Kotagiri Ramamohanaro and Benjamin I. P. Rubinstein. “Fast Manifold Landmarking with Locality Sensitive Hashing”. In: *22nd Pacific-Asia Conference on Knowledge Discovery and Data Mining*. PAKDD. accepted. Feb. 2018.

25. Han, Yi and Benjamin I. P. Rubinstein. “Adequacy of the Gradient-Descent Method for Classifier Evasion Attacks”. In: *AAAI-18 Workshop on Artificial Intelligence for Cyber Security*. AICS. Jan. 2018.

26. Rubinstein, Benjamin I. P. and Francesco Alda. “Pain-Free Random Differential Privacy with Sensitivity Sampling”. In: *Proceedings of the 34th International Conference on Machine Learning*. ICML. PMLR. May. 2017, pp. 2950–2959. **(1 citation)**

27. Alda, Francesco and Benjamin I. P. Rubinstein. “The Bernstein mechanism: Function release under differential privacy”. In: *Proceedings of the 31st AAAI Conference on Artificial Intelligence*. AAAI. Feb. 2017.

28. Liu, Xunyun, Aaron Harwood, Shanika Karunasekera, Benjamin Rubinstein and Rajkumar Buyya. “E-storm: Replication-based state management in distributed stream processing systems”. In: *46th International Conference on Parallel Processing*. ICPP. IEEE. 2017, pp. 571–580. **(1 citation)**

29. Verkade, Heather, Jason M. Lodge, Kristine Elliott, Terrence D. Mulhern, Allen A. Espinosa, Simon J. Cropper and Benjamin I. P. Rubinstein. “Exploring misconceptions as a trigger for enhancing student learning”. In: *Higher Education Research and Development Society of Australasia*. HERDSA. Apr. 2017.

30. Zhang, Zuhe, Benjamin I. P. Rubinstein and Christos Dimitrakakis. “On the differential privacy of Bayesian inference”. In: *Proceedings of the 30th AAAI Conference on Artificial Intelligence*. AAAI. Feb. 2016, pp.

2365–2371. **(24 citations)**

31. He, Jiazhen, Benjamin I. P. Rubinstein, James Bailey, Rui Zhang, Sandra Milligan and Jeffrey Chan. “MOOCs meet measurement theory: A topic-modelling approach”. In: *Proceedings of the 30th AAAI Conference on Artificial Intelligence*. AAAI. Feb. 2016, pp. 1195–1201. **(5 citations)**

32. Fanaeepour, Maryam and Benjamin I. P. Rubinstein. “Beyond points and paths: counting private bodies”. In: *2016 IEEE 16th International Conference on Data Mining*. ICDM. IEEE. Dec. 2016, pp. 131–140. **(3 citations)**

33. Alpcan, Tansu, Benjamin I. P. Rubinstein and Christopher Leckie. “Large-scale strategic games and adversarial machine learning”. In: *2016 IEEE 55th Conference on Decision and Control*. CDC. IEEE. Dec. 2016, pp. 4420–4426.

34. Aye, Zay Maung Maung, Kotagiri Ramamohanarao and Benjamin I. P. Rubinstein. “Large Scale Metric learning”. In: *2016 International Joint Conference on Neural Networks*. IJCNN. IEEE. Jul. 2016, pp. 1442–1449.

35. Sanchez, Ivan, Zay Maung Maung Aye, Benjamin I. P. Rubinstein and Kotagiri Ramamohanarao. “Fast trajectory clustering using Hashing methods”. In: *2016 International Joint Conference on Neural Networks*. IJCNN. IEEE. Jul. 2016, pp. 3689–3696. **(3 citations)**

36. Milligan, Sandra, Jiazhen He, James Bailey, Rui Zhang and Benjamin I. P. Rubinstein. “Validity: a framework for cross-disciplinary collaboration in mining indicators of learning from MOOC forums”. In: *Proceedings of the Sixth International Conference on Learning Analytics & Knowledge*. LAK. ACM. Apr. 2016, pp. 546–547. **(2 citations)**

37. He, Jiazhen, James Bailey, Benjamin I. P. Rubinstein and Rui Zhang. “Identifying At-Risk Students in Massive Open Online Courses”. In: *Proceedings of the 29th AAAI Conference on Artificial Intelligence*. AAAI. 2015, pp. 1749–1755. **(46 citations)**

38. Lim, Zhe and Benjamin I. P. Rubinstein. “Sub-Merge: Diving Down to the Attribute-Value Level in Statistical Schema Matching.” In: *Proceedings of the 29th AAAI Conference on Artificial Intelligence*. AAAI. Jan. 2015, pp. 1791–1797.

39. Dimitrakakis, Christos, Blaine Nelson, Aikaterini Mitrokotsa and Benjamin I. P. Rubinstein. “Robust and private Bayesian inference”. In: *25th International Conference on Algorithmic Learning Theory*. ALT. Springer. Oct. 2014, pp. 291–305. **(43 citations)**

40. Dimitrakakis, Christos, Aikaterini Mitrokotsa and Benjamin I. P. Rubinstein. “Proceedings of the 7th Workshop on Artificial Intelligence and Security (AISec)”. In: *Proceedings of the 2014 ACM Conference on Computer and Communications Security*. CCS. ACM Press, 2014, pp. 1–124.

41. Negahban, Sahand N., Benjamin I. P. Rubinstein and Jim Gemmell. “Scaling multiple-source entity resolution using statistically efficient transfer learning”. In: *Proceedings of the 21st ACM International Conference on Information and Knowledge Management*. CIKM. ACM. Oct. 2012, pp. 2224–2228. **(6 citations)**

42. Cardenas, Alvaro A., Blaine Nelson and Benjamin I. P. Rubinstein. “Fifth ACM Workshop on Artificial Intelligence and Security (AISec)”. In: *Proceedings of the 2012 ACM Conference on Computer and Communications Security*. CCS. ACM. Oct. 2012, pp. 1–110.

43. Huang, Ling, Anthony D. Joseph, Blaine Nelson, Benjamin I. P. Rubinstein and J. D. Tygar. “Adversarial machine learning”. In: *Proceedings of the 4th ACM Workshop on Security and Artificial Intelligence*. ACM. Oct. 2011, pp. 43–58. **(269 citations)**

44. Narayanan, Arvind, Elaine Shi and Benjamin I. P. Rubinstein. “Link prediction by de-anonymization: How we won the Kaggle social network challenge”. In: *The 2011 International Joint Conference on Neural Networks*. IJCNN. IEEE. Feb. 2011, pp. 1825–1834. **(121 citations)**

45. Cardenas, Alvaro A., Rachel Greenstadt and Benjamin I. P. Rubinstein. “Proceedings of the 4th Workshop on Artificial Intelligence and Security (AISec)”. In: *Proceedings of the 2011 ACM Conference on Computer and Communications Security*. CCS. ACM Press, Oct. 2011, pp. 1–116.

46. Nelson, Blaine, Benjamin I. P. Rubinstein, Ling Huang, Anthony D. Joseph, Shing-hon Lau, Steven J. Lee, Satish Rao, Anthony Tran and J. Doug Tygar. “Near-Optimal Evasion of Convex-Inducing Classifiers.” In: *Proceedings*

of the Thirteenth International Conference on Artificial Intelligence and Statistics. AISTATS. 2010, pp. 549–556. **(39 citations)**

47. Barth, Adam, Benjamin I. P. Rubinstein, Mukund Sundararajan, John C. Mitchell, Dawn Song and Peter L. Bartlett. “A learning-based approach to reactive security”. In: *Proceedings of the Fourteenth International Conference on Financial Cryptography and Data Security*. FC. 2010, pp. 192–206. **(28 citations)**

48. Nelson, Blaine, Benjamin I. P. Rubinstein, Ling Huang, Anthony D. Joseph and J. D. Tygar. “Classifier evasion: Models and open problems”. In: *International Workshop on Privacy and Security Issues in Data Mining and Machine Learning*. PSDML. 2010, pp. 92–98. **(31 citations)**

49. Ghosh, Arpita, Benjamin I. P. Rubinstein, Sergei Vassilvitskii and Martin Zinkevich. “Adaptive bidding for display advertising”. In: *Proceedings of the 18th International Conference on World Wide Web*. WWW. ACM. 2009, pp. 251–260. **(60 citations)**

50. Rubinstein, Benjamin I. P., Blaine Nelson, Ling Huang, Anthony D. Joseph, Shing-hon Lau, Satish Rao, Nina Taft and J. D. Tygar. “ANTIDOTE: Understanding and defending against poisoning of anomaly detectors”. In: *Proceedings of the 9th ACM SIGCOMM Internet Measurement Conference*. IMC. ACM. 2009, pp. 1–14. **(138 citations)**

51. Rubinstein, J. Hyam and Benjamin I. P. Rubinstein. “Geometric & Topological Representations of Maximum Classes with Applications to Sample Compression”. In: *Proceedings of the 21st Annual Conference on Learning Theory*. COLT. 2008, pp. 299–310. **(7 citations)**

52. Rubinstein, Benjamin I. P., Blaine Nelson, Ling Huang, Anthony D. Joseph, Shing-hon Lau, Nina Taft and J. Doug Tygar. “Evading anomaly detection through variance injection attacks on PCA”. In: *Proceedings of the 11th International Symposium on Recent Advances in Intrusion Detection*. RAID. 2008, pp. 394–395. **(16 citations)**

53. Nelson, Blaine, Marco Barreno, Fuching Jack Chi, Anthony D. Joseph, Benjamin I. P. Rubinstein, Udam Saini, Charles A. Sutton, J. Doug Tygar and Kai Xia. “Exploiting Machine Learning to Subvert Your Spam Filter.” In: *First USENIX Workshop on Large-scale Exploits and Emergent Threats*. LEET. 2008, pp. 1–9. **(107 citations)**

54. Barreno, Marco, Peter L. Bartlett, Fuching Jack Chi, Anthony D. Joseph, Blaine Nelson, Benjamin I. P. Rubinstein, Udam Saini and J. Doug Tygar. “Open problems in the security of learning”. In: *Proceedings of the 1st ACM Workshop on Artificial Intelligence & Security*. AISec. ACM. 2008, pp. 19–26. **(39 citations)**

55. Rubinstein, Benjamin I. P., Peter L. Bartlett and J. Hyam Rubinstein. “Shifting, one-inclusion mistake bounds and tight multiclass expected risk bounds”. In: *Advances in Neural Information Processing Systems 19*. NIPS. 2007, pp. 1193–1200. **(11 citations)**

56. Rubinstein, Benjamin I. P. “Evolving quantum circuits using genetic programming”. In: *Proceedings of the 2001 Congress on Evolutionary Computation*. CEC. IEEE. 2001, pp. 144–151. **(66 citations)**

Other Publication Outputs

Edited Proceedings

57. Fanaeepour, Maryam and Benjamin I. P. Rubinstein. “Histogramming Privately Ever After: Differentially-Private Data-Dependent Error Bound Optimisation”. In: *Proceedings of the 34th International Conference on Data Engineering*. ICDE. IEEE. 2018.

58. Aye, Zay Maung Maung, Kotagiri Ramamohanaro and Benjamin I. P. Rubinstein. “Fast Manifold Landmarking with Locality Sensitive Hashing”. In: *22nd Pacific-Asia Conference on Knowledge Discovery and Data Mining*. PAKDD. accepted. Feb. 2018.

59. Han, Yi and Benjamin I. P. Rubinstein. “Adequacy of the Gradient-Descent Method for Classifier Evasion Attacks”. In: *AAAI-18 Workshop on Artificial Intelligence for Cyber Security*. AICS. Jan. 2018.

60. Rubinstein, Benjamin I. P. and Francesco Alda. “Pain-Free Random Differential Privacy with Sensitivity Sampling”. In: *Proceedings of the 34th International Conference on Machine Learning*. ICML. PMLR. May. 2017, pp. 2950–2959. **(1 citation)**

61. Alda, Francesco and Benjamin I. P. Rubinstein. “The Bernstein mechanism: Function release under differential privacy”. In: *Proceedings of the 31st AAAI Conference on Artificial Intelligence*. AAAI. Feb. 2017.

62. Liu, Xunyun, Aaron Harwood, Shanika Karunasekera, Benjamin Rubinstein and Rajkumar Buyya. "E-storm: Replication-based state management in distributed stream processing systems". In: *46th International Conference on Parallel Processing*. ICPP. IEEE. 2017, pp. 571–580. **(1 citation)**

63. Verkade, Heather, Jason M. Lodge, Kristine Elliott, Terrence D. Mulhern, Allen A. Espinosa, Simon J. Cropper and Benjamin I. P. Rubinstein. "Exploring misconceptions as a trigger for enhancing student learning". In: *Higher Education Research and Development Society of Australasia*. HERDSA. Apr. 2017.

64. Zhang, Zuhe, Benjamin I. P. Rubinstein and Christos Dimitrakakis. "On the differential privacy of Bayesian inference". In: *Proceedings of the 30th AAAI Conference on Artificial Intelligence*. AAAI. Feb. 2016, pp. 2365–2371. **(24 citations)**

65. He, Jiazhen, Benjamin I. P. Rubinstein, James Bailey, Rui Zhang, Sandra Milligan and Jeffrey Chan. "MOOCs meet measurement theory: A topic-modelling approach". In: *Proceedings of the 30th AAAI Conference on Artificial Intelligence*. AAAI. Feb. 2016, pp. 1195–1201. **(5 citations)**

66. Fanaeepour, Maryam and Benjamin I. P. Rubinstein. "Beyond points and paths: counting private bodies". In: *2016 IEEE 16th International Conference on Data Mining*. ICDM. IEEE. Dec. 2016, pp. 131–140. **(3 citations)**

67. Alpcan, Tansu, Benjamin I. P. Rubinstein and Christopher Leckie. "Large-scale strategic games and adversarial machine learning". In: *2016 IEEE 55th Conference on Decision and Control*. CDC. IEEE. Dec. 2016, pp. 4420–4426.

68. Aye, Zay Maung Maung, Kotagiri Ramamohanarao and Benjamin I. P. Rubinstein. "Large Scale Metric learning". In: *2016 International Joint Conference on Neural Networks*. IJCNN. IEEE. Jul. 2016, pp. 1442–1449.

69. Sanchez, Ivan, Zay Maung Maung Aye, Benjamin I. P. Rubinstein and Kotagiri Ramamohanarao. "Fast trajectory clustering using Hashing methods". In: *2016 International Joint Conference on Neural Networks*. IJCNN. IEEE. Jul. 2016, pp. 3689–3696. **(3 citations)**

70. Milligan, Sandra, Jiazhen He, James Bailey, Rui Zhang and Benjamin I. P. Rubinstein. "Validity: a framework for cross-disciplinary collaboration in mining indicators of learning from MOOC forums". In: *Proceedings of the Sixth International Conference on Learning Analytics & Knowledge*. LAK. ACM. Apr. 2016, pp. 546–547. **(2 citations)**

71. He, Jiazhen, James Bailey, Benjamin I. P. Rubinstein and Rui Zhang. "Identifying At-Risk Students in Massive Open Online Courses". In: *Proceedings of the 29th AAAI Conference on Artificial Intelligence*. AAAI. 2015, pp. 1749–1755. **(46 citations)**

72. Lim, Zhe and Benjamin I. P. Rubinstein. "Sub-Merge: Diving Down to the Attribute-Value Level in Statistical Schema Matching." In: *Proceedings of the 29th AAAI Conference on Artificial Intelligence*. AAAI. Jan. 2015, pp. 1791–1797.

73. Dimitrakakis, Christos, Blaine Nelson, Aikaterini Mitrokotsa and Benjamin I. P. Rubinstein. "Robust and private Bayesian inference". In: *25th International Conference on Algorithmic Learning Theory*. ALT. Springer. Oct. 2014, pp. 291–305. **(43 citations)**

74. Dimitrakakis, Christos, Aikaterini Mitrokotsa and Benjamin I. P. Rubinstein. "Proceedings of the 7th Workshop on Artificial Intelligence and Security (AISec)". In: *Proceedings of the 2014 ACM Conference on Computer and Communications Security*. CCS. ACM Press, 2014, pp. 1–124.

75. Negahban, Sahand N., Benjamin I. P. Rubinstein and Jim Gemmell. "Scaling multiple-source entity resolution using statistically efficient transfer learning". In: *Proceedings of the 21st ACM International Conference on Information and Knowledge Management*. CIKM. ACM. Oct. 2012, pp. 2224–2228. **(6 citations)**

76. Cardenas, Alvaro A., Blaine Nelson and Benjamin I. P. Rubinstein. "Fifth ACM Workshop on Artificial Intelligence and Security (AISec)". In: *Proceedings of the 2012 ACM Conference on Computer and Communications Security*. CCS. ACM. Oct. 2012, pp. 1–110.

77. Huang, Ling, Anthony D. Joseph, Blaine Nelson, Benjamin I. P. Rubinstein and J. D. Tygar. "Adversarial machine learning". In: *Proceedings of the 4th ACM Workshop on Security and Artificial Intelligence*. ACM. Oct. 2011, pp. 43–58. **(269 citations)**

78. Narayanan, Arvind, Elaine Shi and Benjamin I. P. Rubinstein. “Link prediction by de-anonymization: How we won the Kaggle social network challenge”. In: *The 2011 International Joint Conference on Neural Networks*. IJCNN. IEEE. Feb. 2011, pp. 1825–1834. **(121 citations)**

79. Cardenas, Alvaro A., Rachel Greenstadt and Benjamin I. P. Rubinstein. “Proceedings of the 4th Workshop on Artificial Intelligence and Security (AISec)”. In: *Proceedings of the 2011 ACM Conference on Computer and Communications Security*. CCS. ACM Press, Oct. 2011, pp. 1–116.

80. Nelson, Blaine, Benjamin I. P. Rubinstein, Ling Huang, Anthony D. Joseph, Shing-hon Lau, Steven J. Lee, Satish Rao, Anthony Tran and J. Doug Tygar. “Near-Optimal Evasion of Convex-Inducing Classifiers.” In: *Proceedings of the Thirteenth International Conference on Artificial Intelligence and Statistics*. AISTATS. 2010, pp. 549–556. **(39 citations)**

81. Barth, Adam, Benjamin I. P. Rubinstein, Mukund Sundararajan, John C. Mitchell, Dawn Song and Peter L. Bartlett. “A learning-based approach to reactive security”. In: *Proceedings of the Fourteenth International Conference on Financial Cryptography and Data Security*. FC. 2010, pp. 192–206. **(28 citations)**

82. Nelson, Blaine, Benjamin I. P. Rubinstein, Ling Huang, Anthony D. Joseph and J. D. Tygar. “Classifier evasion: Models and open problems”. In: *International Workshop on Privacy and Security Issues in Data Mining and Machine Learning*. PSDML. 2010, pp. 92–98. **(31 citations)**

83. Ghosh, Arpita, Benjamin I. P. Rubinstein, Sergei Vassilvitskii and Martin Zinkevich. “Adaptive bidding for display advertising”. In: *Proceedings of the 18th International Conference on World Wide Web*. WWW. ACM. 2009, pp. 251–260. **(60 citations)**

84. Rubinstein, Benjamin I. P., Blaine Nelson, Ling Huang, Anthony D. Joseph, Shing-hon Lau, Satish Rao, Nina Taft and J. D. Tygar. “ANTIDOTE: Understanding and defending against poisoning of anomaly detectors”. In: *Proceedings of the 9th ACM SIGCOMM Internet Measurement Conference*. IMC. ACM. 2009, pp. 1–14. **(138 citations)**

85. Rubinstein, J. Hyam and Benjamin I. P. Rubinstein. “Geometric & Topological Representations of Maximum Classes with Applications to Sample Compression”. In: *Proceedings of the 21st Annual Conference on Learning Theory*. COLT. 2008, pp. 299–310. **(7 citations)**

86. Rubinstein, Benjamin I. P., Blaine Nelson, Ling Huang, Anthony D. Joseph, Shing-hon Lau, Nina Taft and J. Doug Tygar. “Evading anomaly detection through variance injection attacks on PCA”. In: *Proceedings of the 11th International Symposium on Recent Advances in Intrusion Detection*. RAID. 2008, pp. 394–395. **(16 citations)**

87. Nelson, Blaine, Marco Barreno, Fuching Jack Chi, Anthony D. Joseph, Benjamin I. P. Rubinstein, Udam Saini, Charles A. Sutton, J. Doug Tygar and Kai Xia. “Exploiting Machine Learning to Subvert Your Spam Filter.” In: *First USENIX Workshop on Large-scale Exploits and Emergent Threats*. LEET. 2008, pp. 1–9. **(107 citations)**

88. Barreno, Marco, Peter L. Bartlett, Fuching Jack Chi, Anthony D. Joseph, Blaine Nelson, Benjamin I. P. Rubinstein, Udam Saini and J. Doug Tygar. “Open problems in the security of learning”. In: *Proceedings of the 1st ACM Workshop on Artificial Intelligence & Security*. AISec. ACM. 2008, pp. 19–26. **(39 citations)**

89. Rubinstein, Benjamin I. P., Peter L. Bartlett and J. Hyam Rubinstein. “Shifting, one-inclusion mistake bounds and tight multiclass expected risk bounds”. In: *Advances in Neural Information Processing Systems 19*. NIPS. 2007, pp. 1193–1200. **(11 citations)**

90. *Proceedings of the Second Australian Students’ Computing Conference*. AUSCC. 175 pages. 2004. ISBN: 0-975-71730-8.

91. *Proceedings of the First Australian Undergraduate Students’ Computer Conference*. AUSCC. 126 pages. 2003. ISBN: 0-646-42751-2.

92. Rubinstein, Benjamin I. P. “Evolving quantum circuits using genetic programming”. In: *Proceedings of the 2001 Congress on Evolutionary Computation*. CEC. IEEE. 2001, pp. 144–151. **(66 citations)**

Technical Reports

93. Barth, Adam, Saung Li, Benjamin I. P. Rubinstein and Dawn Song. *How Open Should Open Source Be?* technical report UCB/EECS-2011-98. Department of Electrical Engineering & Computer Sciences, UC Berkeley, Aug. 2011. **(6 citations)**

94. Gemmell, Jim, Benjamin I. P. Rubinstein and Ashok K. Chandra. *Improving entity resolution with global constraints*. technical report MSR-TR-2011-100. Microsoft Research, Aug. 2011. **(10 citations)**

95. Rubinstein, Benjamin I. P., Blaine Nelson, Ling Huang, Anthony D. Joseph, Shing-hon Lau, Nina Taft and Doug Tygar. *Compromising PCA-based anomaly detectors for network-wide traffic*. technical report UCB/EECS-2008-73. EECS Department, University of California, Berkeley, 2008. **(23 citations)**

96. Culnane, Chris, Benjamin I. P. Rubinstein and Vanessa Teague. *Options for encoding names for data linking at the Australian Bureau of Statistics*. Feb. 2018. arXiv: 1802.07975 [cs.CR].

97. Fish, Benjamin, Lev Reyzin and Benjamin I. P. Rubinstein. *Sublinear-Time Adaptive Data Analysis*. Sep. 2017. arXiv: 1709.09778 [cs.LG]. **(1 citation)**

98. Culnane, Chris, Benjamin I. P. Rubinstein and Vanessa Teague. *Privacy Assessment of De-identified Opal Data: A report for Transport for NSW*. May. 2017. arXiv: 1704.08547 [cs.CR]. **(2 citations)**

99. Culnane, Chris, Benjamin I. P. Rubinstein and Vanessa Teague. *Vulnerabilities in the use of similarity tables in combination with pseudonymisation to preserve data privacy in the UK Office for National Statistics' Privacy-Preserving Record Linkage*. 2017. arXiv: 1712.00871 [cs.CR]. **(1 citation)**

100. Culnane, Chris, Benjamin I. P. Rubinstein and Vanessa Teague. *Health Data in an Open World*. Dec. 2017. arXiv: 1712.05627 [cs.CY]. **(1 citation)**

101. He, Jiazhen, Benjamin I. P. Rubinstein, James Bailey, Rui Zhang and Sandra Milligan. *TopicResponse: A Marriage of Topic Modelling and Rasch Modelling for Automatic Measurement in MOOCs*. 2016. arXiv: 1607.08720 [cs.LG].