Curriculum Vitae

Marina Blanton

Contact Information

Marina Blanton (née Bykova)
Computer Science and Engineering Department
University at Buffalo, The State University of New York, Buffalo, NY
Email: mblanton@buffalo.edu
WWW: http://www.buffalo.edu/~mblanton

Research Interests

My research interests centrally focus on applied cryptography, information security, and privacy. Specific topics include privacy-preserving computation and outsourcing, integrity of outsourced computation and storage, private biometric and genomic computation, authentication, and anonymity.

Education

Aug. 2007	PhD in CS, Purdue University. GPA: 4.00. Advisor: Mikhail Atallah
Dec. 2004	MS in CS, Purdue University. GPA: 4.00.
Mar. 2002	MS in EECS, Ohio University. GPA: 3.93. Advisor: Shawn Ostermann
Jun. 1999	BS in CS with Honors, Tyumen State Oil and Gas University, Russia. GPA: 4.00. Advisor: Mikhail Karatun

Work Experience

Jan. 2017 – present	Associate Professor, Computer Science and Engineering Department, University at Buffalo (SUNY), Buffalo, New York
May 2021 – present	Faculty Director, Women in Science and Engineering (WiSE), University at Buffalo (SUNY), Buffalo, New York
Dec. 2014 – present	Senior Scientist, Interrupt Sciences, Pendleton, New York
Aug. 2007 – Jun. 2016	Assistant Professor, Department of Computer Science and Engineering, University of Notre Dame, Notre Dame, Indiana
May 2012 – Jun. 2012	Research Scientist, Air Force Research Laboratory, Rome, New York
Aug. 2002 – Jul. 2007	Teaching/Research Assistant, Department of Computer Science, Purdue University, West Lafayette, Indiana
Sep. 2001 – Jun. 2002	Network Engineer, Communications Network Services, Ohio University, Athens, Ohio
Sep. 1999 – Aug. 2001	Software Designer, Communications Network Services, Ohio University, Athens, Ohio
Sep. 1999 – Jun. 2001	Graduate/Teaching Assistant, School of Electrical Engineering and Computer Science, Ohio University, Athens, Ohio

Aug. 1998 – Aug. 1999	Systems Engineer, Sibnefteprovod, JSC, Tyumen, Russia
Dec. 1997 – Jun. 1998	System Coordinator Helper, Facilities Management, Ohio University, Athens, Ohio

Awards and Recognitions

Aug. 2023	Noteworthy Reviewer for USENIX Security 2023
Aug. 2022	2022–2023 ELATES Fellow
Mar. 2022	SEAS JEDI (Justice, Equity, Diversity, and Inclusion) Award, University at Buffalo
Dec. 2021	CSE Senior Faculty Teaching Award, University at Buffalo
Dec. 2020	CSE Outstanding Faculty Service Award, University at Buffalo
Feb. 2019	Google Faculty Research Award
May 2016	Named IEEE Senior Member
Nov. 2015	Named ACM Senior Member
Oct. 2015	2015 ACM CCS Test of Time Award (awarded to two papers of significant impact on security field published 10 years ago in a flagship conference ACM CCS)
Jan. 2013	AFOSR Young Investigator Award
Oct. 2007	Nominated for the ACM Doctoral Dissertation Award by Purdue University
Apr. 2007	Siemens scholarship in recognition of research achievements
Mar. 2007	Diamond Award (annual award for outstanding academic achievement, awarded to one graduating Ph.D. student), Center for Education and Research in Information Assurance and Security (CERIAS), Purdue University
May 2006	UCLA Institute for Pure and Applied Mathematics (IPAM) Award for participation in the Securing Cyberspace (SC'06) Program (core participant, fall 2006)
Apr. 2006	Intel Foundation Ph.D. Fellowship Award for 2006–2008 academic years (second year declined)
Apr. 2004	Purdue Research Foundation (PRF) Summer Research Scholarship (support for summer 2004)
Mult. years	Winner of university-wide and participant of regional programming contests and olympiads in physics

Publications

Advisees are underlined.

Books

1. M. Atallah and M. Blanton (Editors), "Algorithms and Theory of Computation Handbook. Volume I: General Concepts and Techniques," *Chapman & Hall/CRC*, Nov. 2009.

2. M. Atallah and M. Blanton (Editors), "Algorithms and Theory of Computation Handbook. Volume II: Special Topics and Techniques," *Chapman & Hall/CRC*, Nov. 2009.

In Books

3. M. Blanton, "Authentication," Regular Entry in *Encyclopedia of Database Systems*, second edition, L. Liu and M. Özsu (Editors), Springer, 2018.

4. M. Blanton, "Hash Functions," Short Entry in *Encyclopedia of Database Systems*, second edition, L. Liu and M. Özsu (Editors), Springer, 2018.

5. M. Blanton, "Message Authentication Codes," Short Entry in *Encyclopedia of Database Systems*, second edition, L. Liu and M. Özsu (Editors), Springer, 2018.

6. M. Blanton and P. Gasti, "Secure and Efficient Iris and Fingerprint Identification," Chapter 9 in *Biometric Security*, pp. 274–311, D. Ngo, A. Teoh, and J. Hu (Editors), Cambridge Scholars Publishing, Jan. 2015.

7. E. Aguiar, Y. Zhang, and M. Blanton, "An Overview of Issues and Recent Developments in Cloud Computing and Storage Security," Chapter in *High Performance Cloud Auditing and Applications*, B.-Y. Choi, K. Han, and S. Song (Editors), Springer, 2014.

8. M. Blanton, "Authentication," Regular Entry in *Encyclopedia of Database Systems*, L. Liu and M. Özsu (Editors), Springer, 2009.

9. M. Blanton, "Hash Functions," Short Entry in *Encyclopedia of Database Systems*, L. Liu and M. Özsu (Editors), Springer, 2009.

10. M. Blanton, "Message Authentication Codes," Short Entry in *Encyclopedia of Database Systems*, L. Liu and M. Özsu (Editors), Springer, 2009.

In Refereed Journals

11. M. Blanton, D. Murphy, and C. Yuan, "Efficiently Compiling Secure Computation Protocols From Passive to Active Security: Beyond Arithmetic Circuits," *Proceedings on Privacy Enhancing Technologies (PoPETs)*, Vol. 2024, No. 1, 2024. Also in *Privacy Enhancing Technologies Symposium (PETS)*, Jul. 2024.

12. M. Blanton, M. Goodrich, and C. Yuan, "Secure and Accurate Summation of Many Floating-Point Numbers," *Proceedings on Privacy Enhancing Technologies (PoPETs)*, Vol. 2023, No. 3, 2023. Also in *Privacy Enhancing Technologies Symposium (PETS)*, Jul. 2023. (accept. rate 25%)

13. A. Baccarini, M. Blanton, and C. Yuan, "Multi-Party Replicated Secret Sharing over a Ring with Applications to Privacy-Preserving Machine Learning," *Proceedings on Privacy Enhancing Technologies (PoPETs)*, Vol. 2023, No. 1, 2023. Also in *Privacy Enhancing Technologies Symposium (PETS)*, Jul. 2023. (accept. rate 25%)

14. M. Samadani, M. Berenjkoob, and M. Blanton, "Secure Pattern Matching based on Bit Parallelism," *International Journal of Information Security (IJIS)*, Vol. 18, No. 3, pp. 371–391, 2019.

15. Z. Shan, K. Ren, M. Blanton, and C. Wang, "Practical Secure Computation Outsourcing: A Survey," *ACM Computing Surveys*, Vol. 51, No. 2, Article 31, 40 pages, 2018.

16. Y. Zhang, M. Blanton, and G. Almashaqbeh, "Implementing Support for Pointers to Private Data in a General-Purpose Secure Multi-Party Compiler," *ACM Transactions on Privacy and Security (TOPS)*, Vol. 21, No. 2, Article 6, 34 pages, 2018.

17. M. Aliasgari, M. Blanton, and F. Bayatbabolghani, "Secure Computation of Hidden Markov Models and Secure Floating Point Arithmetic in the Malicious Model," *International Journal of Information Security (IJIS)*, Vol. 16, No. 6, pp. 577–601, 2017.

18. M. Blanton and E. Aguiar, "Private and Oblivious Set and Multiset Operations," *International Journal of Information Security (IJIS)*, Vol. 15, No. 5, pp. 493–518, Oct. 2016.

19. M. Blanton and F. Bayatbabolghani, "Efficient Server-Aided Secure Two-Party Function Evaluation with Applications to Genomic Computation," *Proceedings on Privacy Enhancing Technologies (PoPETs)*, No. 4, 2016. Also in *Privacy Enhancing Technologies Symposium (PETS)*, pp. 144–164, Jul. 2016.

20. Y. Zhang and M. Blanton, "Efficient Dynamic Provable Possession of Remote Data via Update Trees," *ACM Transactions on Storage (TOS)*, Vol. 12, No. 2, Article 9, 45 pages, Feb. 2016.

21. Y. Zhang, M. Blanton, and G. Almashaqbeh, "Secure Distributed Genome Analysis for GWAS and Sequence Comparison Computation," *BMC Medical Informatics and Decision Making*, Vol. 15, Suppl. 5, Article S4, 12 pages, Dec. 2015.

22. M. Blanton, Y. Zhang, and K. Frikken, "Secure and Verifiable Outsourcing of Large-Scale Biometric Computations," *ACM Transactions on Information and System Security (TISSEC)*, Vol. 16, No. 3, Article 11, 35 pages, Nov. 2013.

23. M. Blanton and M. Aliasgari, "Analysis of Reusability of Secure Sketches and Fuzzy Extractors," *IEEE Transactions on Information Forensics and Security (TIFS)*, Vol. 8, No. 9, pp. 1433–1445, Sep. 2013.

24. T. R. Hoens, M. Blanton, A. Steele, and N. Chawla "Reliable Medical Recommendation Systems with Patient Privacy," *ACM Transactions on Intelligent Systems and Technology (TIST)*, Vol. 4, No. 4, 31 pages, Sep. 2013.

25. M. Blanton and M. Aliasgari, "Secure Outsourced Computation of Iris Matching," *Journal of Computer Security (JCS)*, Vol. 20, No. 2–3, pp. 259–305, 2012.

26. V. Deshpande, L. Schwarz, M. Atallah, M. Blanton, and K. Frikken, "Outsourcing Manufacturing: Secure Price-Masking Mechanisms for Purchasing Component Parts," *Production and Operations Management (POMS)*, Vol. 20, No. 2, pp. 165–180, Mar. 2011.

27. S. Byun, C. Ruffini, J. Mills, A. Douglas, M. Niang, S. Stepchenkova, S. K. Lee, J. Loutfi, J.-K. Lee, M. Atallah, and M. Blanton, "Internet Addiction: Metasynthesis of 1996–2006 Quantitative Research," *CyberPsychology & Behavior*, Vol. 12, No. 2, pp. 203–207, Apr. 2009.

28. M. Atallah, M. Blanton, N. Fazio, and K. Frikken, "Dynamic and Efficient Key Management for Access Hierarchies," *ACM Transactions on Information and System Security (TISSEC)*, Vol. 12, No. 3, Article 18, pp. 1–43, Jan. 2009.

29. A. Douglas, J. Mills, M. Niang, S. Stepchenkova, S. Byun, C. Ruffini, S. K. Lee, J. Loutfi, J.-K. Lee, M. Atallah, and M. Blanton, "Internet Addiction: Meta-Synthesis of Qualitative Research for the Decade 1996–2006," *Computers in Human Behavior*, Vol. 24, No. 6, pp. 3027–3044, Sep. 2008.

30. M. Blanton and M. Atallah, "Succinct Representation of Flexible Privacy-Preserving Access Rights," *Special Issue (Privacy-Preserving Data Management) of the International Journal on Very Large Data Bases (VLDBJ)*, Vol. 15, No. 4, pp. 334–354, Nov. 2006.

31. R. Balupari, B. Tjaden, S. Ostermann, M. Bykova, and A. Mitchell, "Real-Time Network-Based Anomaly Intrusion Detection," *Special Issue (Real Time Security) of the Journal of Parallel and Distributed Computing Practices*, Vol. 4, No. 2, Jun. 2001.

In Refereed Magazines

32. M. Blanton and F. Bayatbabolghani, "An Approach to Improving Security and Efficiency of Private Genomic Computation using Server Aid," *IEEE Security and Privacy*, Vol. 15, No. 5, pp. 20–28, Sep./Oct. 2017.

In Refereed Conference Proceedings

Acceptance rate included where known.

33. M. Blanton and C. Yuan, "Binary Search in Secure Computation," *Network and Distributed System Security Symposium (NDSS)*, 18 pages, 2022. (accept. rate: 16.2%)

34. M. Blanton, A. Kang, and C. Yuan, "Improved Building Blocks for Secure Multi-Party Computation based on Secret Sharing with Honest Majority," *International Conference on Applied Cryptography and Network Security (ACNS)*, pp. 377-397, 2020. (accept. rate: 21%)

35. M. Blanton and M. Jeong, "Improved Signature Schemes for Secure Multi-Party Computation with Certified Inputs," *European Symposium on Research in Computer Security (ESORICS'18)*, pp. 438–460, Sep. 2018. (accept. rate: 20%)

36. Y. Zhang, M. Blanton, and B. Bayatbabolghani, "Enforcing Input Correctness via Certification in Garbled Circuit Evaluation,", *European Symposium on Research in Computer Security (ESORICS'17)*, pp. 552–569, Sep. 2017. (accept. rate: 15.9%)

37. A. Shahbazi, F. Bayatbabolghani, and M. Blanton, "Private Computation with Genomic Data for Genome-Wide Association and Linkage Studies," *International Workshop on Genomic Privacy and Security (GenoPri'16)*, Nov. 2016.

38. M. Blanton and S. Saraph, "Secure and Oblivious Maximum Bipartite Matching Size Algorithm with Applications to Secure Fingerprint Identification," *European Symposium on Research in Computer Security (ESORICS'15)*, pp. 384–406, Sep. 2015. (accept. rate: 20.1%)

39. Y. Zhang and M. Blanton, "Efficient Secure and Verifiable Outsourcing of Matrix Multiplications," *International Conference on Information Security (ISC'14)*, pp. 158–178, Oct. 2014. (accept. rate: 17.2%)

40. Y. Zhang, A. Steele, and M. Blanton, "PICCO: A General-Purpose Compiler for Private Distributed Computation," *ACM Conference on Computer and Communications Security (CCS'13)*, pp. 813–826, Nov. 2013. (accept. rate: 19.8%)

41. M. Aliasgari and M. Blanton, "Secure Computation of Hidden Markov Models," *International Conference on Security and Cryptography (SECRYPT'13)*, pp. 242–253, Jul. 2013. (accept. rate: 13%)

42. Y. Zhang and M. Blanton, "Efficient Dynamic Provable Possession of Remote Data via Balanced Update Trees," *ACM Symposium on Information, Computer and Communications Security (ASIACCS'13)*, pp. 183–194, May 2013. (accept. rate for full papers: 16.2%)

43. M. Blanton, A. Steele, and M. Aliasgari, "Data-Oblivious Graph Algorithms for Secure Computation and Outsourcing," *ACM Symposium on Information, Computer and Communications Security (ASIACCS'13)*, pp. 207–218, May 2013. (accept. rate for full papers: 16.2%)

44. M. Aliasgari, M. Blanton, Y. Zhang, and A. Steele, "Secure Computation on Floating Point Numbers," *Network and Distributed System Security Symposium (NDSS'13)*, 18 pages, Feb. 2013. (accept. rate: 18.8%)

45. M. Blanton, M. Atallah, K. Frikken, and Q. Malluhi, "Secure and Efficient Outsourcing of Sequence Comparisons," *European Symposium on Research in Computer Security (ESORICS'12)*, pp. 505–522, Sep. 2012. (accept. rate: 20%)

46. M. Blanton and E. Aguiar, "Private and Oblivious Set and Multiset Operations," *ACM Symposium on Information, Computer and Communications Security (ASIACCS'12)*, 12 pages, May 2012. (accept. rate for full papers: 22%)

47. M. Blanton, "Achieving Full Security in Privacy-Preserving Data Mining," *IEEE International Conference on Information Privacy, Security, Risk and Trust (PASSAT'11)*, pp. 925–934, Oct. 2011. (accept. rate for long papers: 8%)

48. M. Blanton, Y. Zhang, and K. Frikken, "Secure and Verifiable Outsourcing of Large-Scale Biometric Computations," *IEEE International Conference on Information Privacy, Security, Risk and Trust (PASSAT'11)*, pp. 1185–1991, Oct. 2011. (accept. rate for poster papers: 18%)

49. M. Blanton and P. Gasti, "Secure and Efficient Protocols for Iris and Fingerprint Identification," *European Symposium on Research in Computer Security (ESORICS'11)*, pp. 190–209, Sep. 2011. (accept. rate: 23.2%)

50. M. Blanton and M. Aliasgari, "On the (Non-)Reusability of Fuzzy Sketches and Extractors and Security in the Computational Setting," *International Conference on Security and Cryptography (SECRYPT'11)*, pp. 68–77, Jul. 2011. (accept. rate for full papers: 13%)

51. T. R. Hoens, M. Blanton, and N. Chawla, "Reliable Medical Recommendation Systems with Patient Privacy," *ACM International Health Informatics Symposium (IHI'10)*, pp. 173–182, Nov. 2010. (accept. rate for presented papers: 17.1%)

52. P. Gasti, G. Ateniese, and M. Blanton, "Deniable Cloud Storage: Sharing Files via Public-Key Deniability," *ACM Workshop on Privacy in the Electronic Society (WPES'10)*, pp. 31–42, Oct. 2010. (accept. rate for full papers: 20.8%)

53. M. Blanton and K. Frikken, "Efficient Multi-Dimensional Key Management in Broadcast Services," *European Symposium on Research in Computer Security (ESORICS'10)*, pp. 424–440, Sep. 2010. (accept. rate: 20.9%)

54. T. R. Hoens, M. Blanton, and N. Chawla, "A Private and Reliable Recommendation System for Social Networks,," *IEEE International Conference on Information Privacy, Security, Risk and Trust (PASSAT'10)*, pp. 816–825, Aug. 2010. (accept. rate: 11%)

55. M. Blanton and M. Aliasgari, "Secure Outsourcing of DNA Searching via Finite Automata," *Annual IFIP Conference on Data and Applications Security (DBSec'10)*, pp. 49–64, Jun. 2010. (accept. rate for full papers: 29.5%)

56. T. Raeder, M. Blanton, N. Chawla, and K. Frikken, "Privacy-Preserving Network Aggregation," *Pacific-Asia Conference on Knowledge Discovery and Data Mining (PAKDD'10)*, pp. 198–207, Jun. 2010. (accept. rate for short papers: 23.3%)

57. M. Blanton and W. Hudelson, "Biometric-Based Non-Transferable Anonymous Credentials," *International Conference on Information and Communications Security (ICICS'09)*, pp. 165–180, Dec. 2009. (accept. rate for full papers: 19.1%)

58. K. Frikken, M. Blanton, and M. Atallah, "Robust Authentication Using Physically Unclonable Functions," *Information Security Conference (ISC'09)*, pp. 262–277, Sep. 2009. (accept. rate for full papers: 27.6%)

59. M. Blanton, "Improved Conditional E-Payments," *Applied Cryptography and Network Security (ACNS'08)*, pp. 188–206, Jun. 2008. (accept. rate: 22.9%)

60. M. Atallah, K. Frikken, M. Blanton, and Y. Cho, "Private Combinatorial Group Testing," *ACM Symposium on Information, Computer and Communications Security (ASIACCS'08)*, pp. 312–320, Mar. 2008. (accept. rate for full papers: 17.6%)

61. M. Blanton, "Online Subscriptions with Anonymous Access," *ACM Symposium on Information, Computer and Communications Security (ASIACCS'08)*, pp. 217–227, Mar. 2008. (accept. rate for full papers: 17.6%)

62. M. Atallah, M. Blanton, and K. Frikken, "Incorporating Temporal Capabilities in Existing Key Management Schemes," *European Symposium on Research in Computer Security (ESORICS'07)*, pp. 515–530, Sep. 2007. (accept. rate: 23.8%)

63. M. Atallah, M. Blanton, M. Goodrich, and S. Polu, "Discrepancy-Sensitive Dynamic Fractional Cascading, Dominated Maxima Searching, and 2-d Nearest Neighbors in Any Minkowski Metric," *Workshop on Algorithms and Data Structures (WADS'07)*, pp. 114–126, Aug. 2007. (accept. rate: 26.7%)

64. M. Atallah, M. Blanton, and K. Frikken, "Efficient Techniques for Realizing Geo-Spatial Access Control," *ACM Symposium on Information, Computer and Communications Security (ASIACCS'07)*, pp. 82–92, Mar. 2007. (accept. rate: 18.9%)

65. G. Ateniese, M. Blanton, and J. Kirsch, "Secret Handshakes with Dynamic and Fuzzy Matching," *Network & Distributed System Security Symposium (NDSS'07)*, pp. 159–177, Feb. 2007. (accept. rate: 15.3%)

66. M. Atallah, M. Blanton, V. Deshpande, K. Frikken, J. Li, and L. Schwarz, "Secure Collaborative Planning, Forecasting, and Replenishment (SCPFR)," *Multi-Echelon/Public Applications of Supply Chain Management Conference*, Jun. 2006. (accept. rate: 16%)

67. M. Atallah, M. Blanton, and K. Frikken, "Key Management for Non-Tree Access Hierarchies," *ACM Symposium on Access Control Models and Technologies (SACMAT'06)*, pp. 11–18, Jun. 2006. (accept. rate: 30.5%)

68. M. Atallah, M. Blanton, K. Frikken, and J. Li, "Efficient Correlated Action Selection," *Financial Cryptography and Data Security (FC'06)*, LNCS 4107, pp. 296–310, Feb. 2006. (accept. rate for full papers: 19.8%)

69. M. Atallah, K. Frikken, and M. Blanton, "Dynamic and Efficient Key Management for Access Hierarchies," *ACM Conference on Computer and Communications Security (CCS'05)*, pp. 190–201, Nov. 2005. (accept. rate: 15.3%)

70. M. Atallah, M. Blanton, V. Deshpande, K. Frikken, J. Li, and L. Schwarz, "Secure Collaborative Planning, Forecasting, and Replenishment (SCPFR)," *Manufacturing and Service Operation Management (M&SOM)*, Jun. 2005.

71. M. Blanton and M. Atallah, "Provable Bounds for Portable and Flexible Privacy-Preserving Access Rights," *ACM Symposium on Access Control Models and Technologies (SACMAT'05)*, pp. 95–101, Jun. 2005. (accept. rate: 21.1%)

72. K. Frikken, M. Atallah, and M. Bykova, "Remote Revocation of Smart Cards in a Private DRM System," *Australasian Information Security Workshop (AISW'05), Digital Rights Management*, pp. 169–177, Jan. 2005. (accept. rate: 37.1%)

73. M. Atallah, M. Bykova, J. Li, K. Frikken, and M. Topkara, "Private Collaborative Forecasting and Benchmarking," *ACM Workshop on Privacy in the Electronic Society (WPES'04)*, pp. 103–114, Oct. 2004. (accept. rate for full papers: 23.3%)

74. M. Atallah and M. Bykova, "Portable and Flexible Document Access Control Mechanisms," *European Symposium on Research in Computer Security (ESORICS'04)*, LNCS 3193, pp. 193–208, Sep. 2004. (accept. rate: 17.0%)

75. M. Bykova and M. Atallah, "Succinct Specifications of Portable Document Access Policies," *ACM Symposium on Access Control Models and Technologies (SACMAT'04)*, pp. 41–50, Jun. 2004. (accept. rate: 28.1%)

76. M. Bykova and S. Ostermann, "Statistical Analysis of Malformed Packets and Their Origins in the Modern Internet," *ACM Internet Measurement Workshop (IMW'02)*, pp. 83–88, Nov. 2002.

77. M. Bykova, S. Ostermann, and B. Tjaden, "Detecting Network Intrusions via a Statistical Analysis of Network Packet Characteristics," *IEEE Southeastern Symposium on System Theory (SSST'01)*, pp. 309–314, Mar. 2001.

78. B. Tjaden, L. Welch, S. Ostermann, D. Chelberg, R. Balupari, M. Bykova, A. Mitchell, and L. Tong, "SECURE-RM: Security and Resource Management for Dynamic Real-Time Systems," *Real-Time System Security Minisymposium, Southern Conference on Computing (SCC'00)*, Oct. 2000.

79. B. Tjaden, L. Welch, S. Ostermann, D. Chelberg, R. Balupari, M. Bykova, A. Mitchell, D. Lissitsyn, L. Tong, M. Masters, P. Werme, D. Marlow, B. Chapell, and P. Irey, "INBOUNDS: The Integrated Network-Based Ohio University Network Detective Service," *World Multiconference on Systemics, Cybernetics, and Informatics (SCI'00)*, Jul. 2000.

Tutorials

80. F. Bayatbabolghani and M. Blanton, "Secure Multi-Party Computation," presented at *ACM Conference on Computer and Communications Security (CCS)*, pp. 2157–2159, 2018.

Theses

81. M. Blanton, "Key Management in Hierarchical Access Control Systems," *Ph.D. Thesis*, Purdue University, Aug. 2007.

82. M. Bykova, "Statistical Analysis of Malformed Packets and Their Origins in the Modern Internet," *Master's Thesis*, Ohio University, Mar. 2002.

Significant Software Products

83. "PICCO: A General-Purpose Compiler for Private Distributed Computation," `https://github.com/applied-crypto-lab/picco`, 2023.

Selected Technical Reports

Only technical reports that correspond to unpublished work, work under submission, or full versions with major differences from published work are listed.

84. A. Rathore, M. Blanton, M. Gaboardi, L. Ziarek, "A Formal Model for Secure Multiparty Computations," *arXiv Report 2306.00308*, 2023.

85. A. Baccarini, M. Blanton and S. Zou, "Understanding Information Disclosure from Secure Computation Output: A Study of Average Salary Computation," *arXiv Report 2209.10457*, 2022.

86. M. Blanton, A. Kang, S. Karan, and J. Zola, "Privacy Preserving Analytics on Distributed Medical Data," *arXiv Report 1806.06477*, 2018.

87. F. Bayatbabolghani, M. Blanton, M. Aliasgari, and M. Goodrich, "Secure Fingerprint Alignment and Matching Protocols," *arXiv Report 1702.03379*, 2017.

88. J. DeBenedetto and M. Blanton, "Optimizing Secure Statistical Computations with PICCO," *arXiv Report 1612.08678*, 2016.

89. M. Blanton and S. Saraph, "Secure and Oblivious Maximum Bipartite Matching Size Algorithm with Applications to Secure Fingerprint Identification," *Cryptology ePrint Archive Report 2014/596*, IACR, Aug. 2014.

90. Y. Zhang and M. Blanton, "Efficient Secure and Verifiable Outsourcing of Matrix Multiplications," *Cryptology ePrint Archive Report 2014/133*, IACR, Feb. 2014.

91. M. Blanton and M. Aliasgari, "On the (Non-)Reusability of Fuzzy Sketches and Extractors and Security Improvements in the Computational Setting," *Cryptology ePrint Archive Report 2012/608*, IACR, Oct. 2012.

92. N. Chawla, T. Raeder, M. Blanton, and K. Frikken, "Modeling the Product Space as a Network," *NET Institute Working Paper No. 08–18*, SSRN, Oct. 2008.

93. M. Atallah, M. Blanton, and K. Frikken, "Incorporating Temporal Capabilities in Existing Key Management Schemes," *Cryptology ePrint Archive Report 2007/245*, IACR, Jun. 2007.

94. M. Blanton, "Empirical Evaluation of Secure Two-Party Computation Models," *CERIAS Technical Report TR 2005–58*, Purdue University, Aug. 2005.

95. M. Bykova, "What Should a Good Security Model Be?" *CERIAS Technical Report TR 2004–38*, Purdue University, Sep. 2004.

Patents

- S. Bopardikar, A. Speranzo and M. Blanton, "Query-Aware Privacy for Access Control Data Analytics," US patent application No. 16/382,303, published Nov. 2019.

Research Grants

- "SaTC: TTP: Small: Experimental Platform for Rapid Prototyping and Deployment of Secure Multi-Party Protocols," National Science Foundation (NSF), PI: Marina Blanton, 7/15/2022–6/30/2025, $599,982.

- Center for Identification Technology Research (CITeR) project "Privacy-Preserving Biometric-Based Authentication using Secure Multi-Party Computation," National Science Foundation (NSF), PI: Marina Blanton, 6/15/2020–6/14/2021, $50,000.

- Buffalo BlueSky Project "Formal System Modeling in Security Applications," PI: Marina Blanton, co-PIs: Lukasz Ziarek and Matthew Bolton, 3/1/2020–2/28/2022, $15,000.

- Google Faculty Research Award "Efficient Tools for Privacy-Preserving Data Analysis," PI: Marina Blanton, 3/1/2019–2/29/2020, $49,066.

- REU Supplement for NSF grant "TWC: Small: A General-Purpose Compiler for Private Distributed Computation and Outsourcing," PI: Marina Blanton, 5/1/2017–8/31/2017, $8,000.

- "TWC: Small: A General-Purpose Compiler for Private Distributed Computation and Outsourcing," National Science Foundation (NSF), PI: Marina Blanton, 9/01/2013–8/31/2017, $147,652.

- "A Comprehensive Toolset for General-Purpose Private Computing and Outsourcing," Air Force Office of Scientific Research (AFOSR) Young Investigator Program, PI: Marina Blanton, 03/01/2013–08/31/2016, $360,018.

- "TWC: Small: Protecting Privacy of Biometric Data throughout Computation," National Science Foundation (NSF), PI: Marina Blanton, 12/01/2012–11/30/2016, $350,207.

- REU Supplement for NSF grant "TWC: Small: Protecting Privacy of Biometric Data throughout Computation," PI: Marina Blanton, 5/1/2013–8/31/2013, $8,000.
- "A Comprehensive Toolset for General-Purpose Private Computing and Outsourcing," Air Force Research Laboratory (ARFL) Extension Grant, PI: Marina Blanton, 09/01/2012–12/31/2012, $10,000.
- "Techniques for Secure and Reliable Computational Outsourcing," Air Force Office of Scientific Research (AFOSR), PI: Mikhail Atallah, co-PI: Marina Blanton, 03/15/2009–11/30/2012, $377,000.
- "Incorporating Privacy Protection into Social and Health Networks," Notre Dame Faculty Scholarship Award Program (FSAP), PI: Marina Blanton, 01/01/2010–12/31/2010, $9,965.

Student Supervision

Current PhD advisees:

1. Dennis Murphy (expected graduation 2024)
2. Alessandro Baccarini (expected graduation 2024)

Graduated PhDs:

3. Chen Yuan, 2022 (currently at Facebook)
4. Myoungin Jeong, 2018 (currently at Korea Military Academy)
5. Fattaneh Bayatbabolghani, 2017 (currently Software Engineer at Google)
6. Yihua Zhang, 2015 (currently Security Engineer at Lacework, previously Senior Software Engineer at Google)
7. Mehrdad Aliasgari, 2013 (currently Department Chair and Associate Professor at California State University, Long Beach)

Graduated MS students:

8. Everaldo Aguiar, 2012 (currently Senior Engineering Manager at PagerDuty)

Other former graduate advisees:

9. Ghada Almashaqbeh (currently Assistant Professor at University of Connecticut)
10. Ali Shahbazi (currently Research Scientist Fellow at National Institute of Health)
11. Gursimran Singh
12. Aaron Steele
13. T. Ryan Hoens, co-advised with Nitesh Chawla (currently Senior Machine Learning Engineer at Boosted.ai)

Former pre-doctoral research associates:

14. Mohammad Samadani

Former post-doctoral advisees:

1. Ah Reum Kang (currently at Soonchunhyang University)
2. Yihua Zhang (currently Security Engineer at Lacework)

Undergraduate students involved in research:

1. Thomas Behrens
2. Breanna Devore-McDonald
3. Victoria Dib
4. Benjamin Gunning
5. Phil Hudelson
6. Dominique Hightower
7. Nicholas Pellegrino
8. Amy Pritchard
9. Siddharth Saraph
10. William Stewart
11. Cassandra Ware

MS students involved in research:

1. Tarun Bhuthapuri
2. Gursimran Singh

Examination committees for the following students:

1. Andrew Blaich (Ph.D.)
2. Michael Chappel (Ph.D.)
3. Gian Pietro Farina (Ph.D.)
4. Karen Hollingsworth (Ph.D.)
5. Qi Liao (Ph.D.)
6. Ewa Misiolek (Ph.D.)
7. Amy Pritchard (Ph.D.)
8. Troy Raeder (M.S.)
9. Zihao Shan (Ph.D.)
10. Frank Tsai (Ph.D.)
11. Dirk Van Bruggen (Ph.D.)
12. Haitao Wang (Ph.D.)
13. Li Yu (Ph.D.)

Courses Taught

At the University of Notre Dame:

CSE 30151 Theory of Computing

CSE 40567/60567 Computer Security

CSE 40622/60622 Cryptography and Data Security

At the University at Buffalo:

CSE 199 Internet, Computing, and Society

CSE 565 Computer Security

CSE 664 Applied Cryptography and Computer Security

CSE 701 Privacy Enhancing Technologies

CSE 704 Security and Privacy in Blockchain

CSE 708 Security and Privacy in IoT

Outreach and Extra-Curriculum Activities

- Participated (2008–2012) as a speaker in the Expanding Your Horizons in Science and Mathematics (EYH) career conference that brings hundreds of middle school girls to university campus in the spring of each year. During the day on campus, female faculty from science and engineering fields give workshops to the girls in the hope that these presentations will encourage the attendees to choose a career path in science or engineering.
- Participated as a regional judge in Siemens Competition in Math, Science & Technology for high school students. This competition is a very prestigious national event that each year selects and honors the brightest individual and team high school participants in math, science, and engineering in the hope to stimulate interest in these fields in young individuals who will be our future work force.
- Organized (2013–2015) student knowledge exchanges for graduate students from nearby universities. This event brings together students working on various technical aspects of privacy for a day of presentations and discussions with the goal of learning about research of their peers, building a network, and forming a global view of the field.
- Organized a summer school in May 2016 for graduate students and postdoctoral scholars on secure and oblivious computation and outsourcing. The summer school's presentations covered the latest research developments as well as included discussions of open problems and future research directions.
- Participated (2022–2023) in design and execution of a year-long outreach program through WiSE that paired up female high school students with female college students in STEM disciplines and provided mentoring and college shadowing experience to the high school students. The program involved 5 high schools in the Buffalo area.

Research Citations

All numbers are from Google Scholar (collected on October 21, 2023).

Citations	5,805
h-index	33
i10-index	55

Invited Talks

Conference Keynote Speeches

Dec. 2019 **Keynote speaker**, International Conference on Information Security and Cryptology (Inscrypt) 2019, Nanjing, China

Invited Conference and Workshop Speeches

Jan. 2020	Invited speaker, Workshop on Teaching Secure Computation, George Washington University, Washington DC
Jun. 2019	Invited speaker, Theory and Practice of Multi-Party Computation (TPMPC) Workshop 2019, Bar-Ilan University, Israel
Sep. 2018	Panelist, Great Lakes Security Day, Rochester Institute of Technology, Rochester, NY
Aug. 2014	Successful PI talk, NSF/DIMACS Workshop for Aspiring PIs in Secure and Trustworthy Cyberspace, San Diego, CA
Jun. 2012	Cyber and Information Challenges 2012 Conference, Utica, NY

Invited Seminar and Colloquium Talks

Oct. 2023	CrySP Speaker Series, School of Computer Science, University of Waterloo, Waterloo, ON, Canada
Jul. 2023	Cybersecurity Seminar, Delft University of Technology, Delft, Netherlands
Sep. 2022	Security Seminar, Department of Computer Science, Boston University, Boston, MA
Mar. 2018	Department of Biomedical Informatics Grand Rounds, University at Buffalo, Buffalo, NY
Oct. 2015	CSE Seminar, University at Buffalo, Amherst, NY
Oct. 2015	Dagstuhl Seminar on Genomic Privacy, Wadern, Germany
Aug. 2015	United Technologies Research Center, East Hartford, CT
Mar. 2015	University of Texas at Dallas, Richardson, TX
Mar. 2014	CERIAS Seminar, Purdue University, West Lafayette, IN
Oct. 2013	SAP Research, Karslruhe, Germany
Mar. 2013	University of Illinois at Chicago, Chicago, IL
Jun. 2012	Air Force Research Laboratory, Rome, NY
Mar. 2012	Benedictine University, Lisle, IL
Sep. 2011	University of California, Irvine, CA
Sep. 2011	Microsoft Research, Redmond, WA
Jul. 2011	Center for Advanced Security Research Darmstadt (CASED), Technical University Darmstadt, Darmstadt, Germany
Jun. 2011	Qatar University, Doha, Qatar
Dec. 2010	CSSE Colloquium, Miami University, Oxford, OH
Jul. 2009	REU Seminar, University of Notre Dame, Notre Dame, IN
Nov. 2008	Science Today Seminar, SUNY at Oswego, Oswego, NY
Sep. 2008	SPAR Seminar, Johns Hopkins University, Baltimore, MD
Apr. 2007	CS Seminar, Texas A&M University, College Station, TX
Apr. 2007	EECS Seminar Series, Case Western Reserve University, Cleveland, OH
Mar. 2007	ECE Seminar, Iowa State University, Ames, IA
Mar. 2007	CSE Seminar Series, University of Notre Dame, Notre Dame, IN

Mar. 2007	DCS Colloquium, Rutgers University, Piscataway, NJ
Mar. 2007	IBM T. J. Watson Research Center, Hawthorne, NY
Feb. 2007	CS Colloquium, Florida State University, Tallahassee, FL
Feb. 2007	Center for Applied Cybersecurity Research (CACR) Seminar, Indiana University, Bloomington, IN
Jan. 2007	CS Seminar, California Institute of Technology, Pasadena, CA
Jan. 2007	Security Seminar, University of Illinois at Urbana-Champaign, Urbana, IL
Oct. 2006	CSE Colloquium, the Pennsylvania State University, University Park, PA
Mar. 2006	CERIAS Security Seminar, Purdue University, West Lafayette, IN
Oct. 2004	Guest lecture at Database Security CS 590S, Purdue University, West Lafayette, IN
Sep. 2004	INRIA, the French National Institute for Research in Computer Science and Control, Rocquencourt, France
Jul. 2001	NASA Glenn Research Center, Cleveland, OH

Editorial Activities

May 2006 – Nov. 2009	M. Atallah and M. Blanton (Editors), *"Algorithms and Theory of Computation Handbook. Volume I: General Concepts and Techniques."*
May 2006 – Nov. 2009	M. Atallah and M. Blanton (Editors), *"Algorithms and Theory of Computation Handbook. Volume II: Special Topics and Techniques."*

Professional Service

Journal Editorial Boards

Jan. 2021 – present	Associate Editor of IEEE Transactions on Dependable and Secure Computing (TDSC)
Jan. 2020 – Mar. 2023	Associate Editor of International Journal of Information Security (IJIS)
Jan. 2017 – Jun. 2021	Associate Editor of IEEE Transactions on Information Forensics and Security (TIFS)
Jan. 2013 – Dec. 2015	Associate Editor of EURASIP Journal on Information Security

Conference Committees

- Program committee member, ACM Conference on Data and Application Security and Privacy (CODASPY) 2024
- Program committee member, USENIX Security Symposium 2023
- Program committee member, USENIX Security Symposium 2022
- Program committee member, European Symposium on Research in Computer Security (ESORICS) 2021
- Program committee member, European Symposium on Research in Computer Security (ESORICS) 2020
- Program committee member, IEEE Symposium on Security and Privacy (S&P) 2020

- Program committee member, European Symposium on Research in Computer Security (ESORICS) 2019
- Program committee member, IEEE Symposium on Security and Privacy (S&P) 2019
- Program committee member, Network and Distributed System Security Symposium (NDSS) 2019
- Program committee member, International Conference on Information Security (ISC) 2018
- Program committee member, International Conference on Applied Cryptography and Network Security (ACNS) 2018
- Program committee member, IEEE Symposium on Security and Privacy (S&P) 2018
- Program committee member, EAI International Conference on Security and Privacy in Communications Networks (SECURECOMM) 2017
- Program committee member, IEEE Symposium on Privacy-Aware Computing (PAC) 2017
- Program committee member, Annual IFIP WG 11.3 Conference on Data and Applications Security and Privacy (DBSec) 2017
- Program committee member, Innovative CyberSecurity and Privacy for Internet of Things: Strategies, Technologies, and Implementations (WICSPIT) 2017
- Program committee member, ACM Conference on Computer and Communications Security (CCS) 2016
- Program committee member, IEEE International Conference on Cloud Computing (CLOUD) 2016
- Program committee and editorial board member, Privacy Enhancing Technologies Symposium (PETS) 2015/2016
- Program committee member, ACM Conference on Computer and Communications Security (CCS) 2015
- Program committee member, International Conference on Information Security (ISC) 2015
- Program committee member, International Conference on Information Security (ISC) 2014
- Program committee member, ACM Conference on Computer and Communications Security (CCS) 2014
- Program committee member, European Symposium on Research in Computer Security (ESORICS) 2014
- Program committee member, Annual IFIP WG 11.3 Working Conference on Data and Applications Security (DBSec) 2014
- Program committee member, ACM Workshop on Privacy in the Electronic Society (WPES) 2013
- Program committee member, International Conference on Information and Communications Security (ICICS) 2013
- Program committee member, European Symposium on Research in Computer Security (ESORICS) 2013
- Program committee member, Annual IFIP WG 11.3 Working Conference on Data and Applications Security (DBSec) 2013
- Program committee member, International Conference on Network and System Security (NSS) 2013

- Program committee member (cloud computing track), International Symposium on Stabilization, Safety, and Security of Distributed Systems (SSS) 2012
- Program committee member, International Conference on Network and System Security (NSS) 2012
- Program committee member, European Symposium on Research in Computer Security (ESORICS) 2012
- Program committee member, Annual IFIP WG 11.3 Working Conference on Data and Applications Security (DBSec) 2012
- Program committee member, International Conference on Applied Cryptography and Network Security (ACNS) 2012
- Program committee member, ACM Workshop on Privacy in the Electronic Society (WPES) 2011
- Program committee member, International Conference on Network and System Security (NSS) 2011
- Program committee member, ACM SIGKDD Conference on Knowledge Discover and Data Mining (KDD) 2011
- Program committee member, International Conference on Security and Cryptography (SECRYPT) 2011
- Program committee member, Annual IFIP WG 11.3 Working Conference on Data and Applications Security (DBSec) 2011
- Program committee member, International Conference on Trust and Trustworthy Computing (TRUST) 2011
- Program committee member, Information Security Conference (ISC) 2010
- Program committee member, International ICST Conference on Security and Privacy in Communication Networks (SecureComm) 2010
- Program committee member, International Conference on Security and Cryptography (SECRYPT) 2010
- Program committee member, Annual IFIP WG 11.3 Working Conference on Data and Applications Security (DBSec) 2010
- Program committee member, Financial Cryptography and Data Security (FC) 2010
- Program committee member, Workshop on Data Privacy Management (DPM) 2009
- Program committee member, Information Security Conference (ISC) 2009
- Program committee member, International Conference on Advanced Information Networking and Applications (AINA) 2009, Security, Privacy and Trust track
- Program committee member, International Conference on Information Security and Cryptology (Inscrypt) 2008
- Program committee member, IEEE/IFIP International Symposium on Trust, Security and Privacy for Pervasive Applications (TSP) 2008
- Program committee member, ACM Workshop on Privacy in the Electronic Society (WPES) 2008
- Program committee member, European Symposium on Research in Computer Security (ESORICS) 2008

- Publicity chair, International Conference on Information Systems Security (ICISS) 2007

Grant Proposal Review

- Panelist and ad-hoc reviewer for National Science Foundation (multiple years and programs)
- Reviewer for Czech Science Foundation

Advisory Boards

2008–present Ohio University EECS Advisory Board

University Service

University-level service

2021–present	**Women in Science and Engineering (WiSE) Faculty Director**, University at Buffalo
2022–2023	University Committee on the Future of Computer Science and Computing, University at Buffalo
2000–2001	Electronic Theses and Dissertations Committee, Ohio University

School-level service

2021–present	SEAS Tenure and Promotion Committee, School of Engineering and Applied Sciences, University at Buffalo
2020–present	DivTech Faculty Advisor, University at Buffalo
2018–2019	Ad Hoc Committee on Sexual Harassment, School of Engineering and Applied Sciences, University at Buffalo
2017–2018	Teaching Faculty Personnel Ad Hoc Committee, School of Engineering and Applied Sciences, University at Buffalo
2004–2005	Grade Appeal Committee, School of Science, Purdue University

Department-level service

2018–present	**Co-chair** of Diversity Committee, Department of Computer Science and Engineering, University at Buffalo
2021–2022	**Chair** of Graduate Admissions Automation Committee, Department of Computer Science and Engineering, University at Buffalo
2017–2021	Faculy Search Committee, Department of Computer Science and Engineering, University at Buffalo
2017–2021	Graduate Admissions Committee, Department of Computer Science and Engineering, University at Buffalo
2013–2014	Graduate Studies Committee, Department of Computer Science and Engineering, University of Notre Dame
2007–2011	Graduate Studies Committee, Department of Computer Science and Engineering, University of Notre Dame
2004–2006	Graduate Student Board, Department of Computer Science, Purdue University

2004–2005 Graduate Committee, Department of Computer Science, Purdue University

Other Professional Service

- Evaluation committee member for the CRA-W/ACSA Scholarships for Women Studying Information Security (SWSIS) Program 2017 – present
- Organizing committee chair for Great Lakes Security Day (GLSD), Sep. 2019
- Privacy Enhancing Technologies (PET) Awards Committee (for Caspar Bowden Award), 2018
- Organizing committee member for DIMACS Workshop on Outsourcing Computation Securely, Jul. 2017

Refereeing for Conferences/Journals

- ACM Computing Surveys
- ACM Conference on Computer and Communications Security (CCS)
- ACM Symposium on Access Control Models and Technologies (SACMAT)
- ACM Symposium on High Performance and Distributed Computing (HPDC)
- ACM Symposium on Principles of Database Systems (PODS)
- ACM Transactions on Information and System Security (TISSEC)
- ACM Transactions on Internet Technology (TOIT)
- ACM Transactions on the Web (TWeb)
- Annual Computer Security Applications Conference (ACSAC) (On the 2006 reviewer committee)
- Applied Cryptography and Network Security (ACNS)
- Conference on Integer Programming and Combinatorial Optimization (IPCO)
- Elsevier Computer Networks (COMNET)
- Elsevier Computer Standards & Interfaces (CSI)
- Elsevier Computers & Security
- Elsevier Journal of Systems and Software (JSS)
- Elsevier Theoretical Computer Science (TCS)
- ETRI Journal
- EURASIP Journal on Wireless Communications and Networking (JWCN)
- European Journal of Operational Research (EJOR)
- ICTACT Journal on Communication Technology (IJCT)
- IEEE/ACM International Conference on High Performance Computing (HiPC)
- IEEE/ACM Transactions on Computational Biology and Bioinformatics (TCBB)
- IEEE Communications Letters
- IEEE Conference on Electronic Commerce (CEC)
- IEEE INFOCOM

- IEEE Internet Computing
- IEEE Network and Distributed System Security Symposium (NDSS)
- IEEE Security and Privacy (S&P)
- IEEE Transactions on Computers (TC)
- IEEE Transactions on Dependable and Secure Computing (TDSC)
- IEEE Transactions on Information Forensics & Security
- IEEE Transactions on Information Theory
- IEEE Transactions on Knowledge and Data Engineering (TKDE)
- IEEE Transactions on Software Engineering
- Information and Software Technology, International Journal
- Information Processing Letters (IPL)
- International Conference on Distributed Computing Systems (ICDCS)
- International Conference on Information and Communications Security (ICICS)
- International Conference on Information Security and Cryptology (ICISC)
- International Journal of Information Security (IJIS)
- International Symposium on Algorithms and Computation (ISAAC)
- Journal of Information Science and Engineering (JISE)
- Journal of Logical and Algebraic Methods in Programming (JLAMP)
- Journal of Latin American Applied Research (LAAR)
- Privacy Enhancing Technologies Symposium (PETS)
- Workshop on Privacy Enhancing Technologies (PET)
- Workshop on Selected Areas in Cryptography (SAC)