Biographical Sketch : Delaram Kahrobaei

E-mail: delaram.kahrobaei61@gc.cuny.edu, delaram.kahrobaei@qc.cuny.edu
kahrobaei@ihes.fr, dk2572@nyu.edu, delaram.kahrobaei@york.ac.uk
U.S. Citizen
Exceptional Talent Tier 1 Resident of U. K.

Professional Preparation:

- Cornell University, Cornell SC Johnson College of Business, Women in Leadership, Certificate, 2020.
- The National Science Foundation, Entrepreneurship, Certificate, 2014.
- CUNY Graduate Center, Mathematics, Ph.D. 2004. Advisor: G. Baumslag.
- The City College of New York, Computer Science, M.A. 2004.
- Claremont Graduate University, Applied Mathematics, M.S. 2004.
- Sharif University of Technology, Mathematics and Computer Science, B.S. 1998.

Appointments:

- 2021 – current : Full Professor with tenure, Computer Science Department, Queens College, The City University of New York, USA.
- 2021 – current : Full Professor with tenure, Mathematics Department, Queens College, The City University of New York, USA.
- 2021 – current : 2021 – 2024: Honorary Chair of Cyber Security, 2024 – current: Visiting Honorary Professor, Department of Computer Science, University of York, UK.
- 2023 – current : Member of Board of Directors, Friends of IHES-Institut des Hautes Études Sciéntifiques.
- 2018 – 2021 : Chair of Cyber Security, (equivalent to Distinguished Professor with tenure), Department of Computer Science, University of York, UK.
- 2019 – 2021: Founder and Director of the York Interdisciplinary Centre for Cyber Security, University of York.
- 2024 : CARMIN Professor, IHES-Institut des Hautes Études Sciéntifiques, Paris, France.
- 2013, 2016 – current : Adjunct Professor of Computer Science, New York University.
- 2022– current : Member of Scientific Advisory Board: Feynmann Foundation, Quantum for Humanity, Brussels, Belgium
- 2022 – current : External Advisor, NSF funded Accelerating impact through Partnerships, Center for Data Driven Drug Development and Treatment Assessment (DATA), University of Michigan.
- 2019 – current : External Advisor QUASAR (Quantum Security via Algebras and Representation Theory) based in University of Ottawa (Canada).
- 2022 – current : Advisory Board, nodeQ: Development of High-Performance Quantum Networks, US-UK Company
- 2021 – 2022 : University Dean for Research, The City University of New York
- 2008– 2021 : Doctoral Faculty, PhD Program in Computer Science, CUNY Graduate Center, (PhD Thesis Advisor to 4 Math, 3 CS graduated PhD students, 2 Postdocs).
- 2015 – 2018 : Full Professor with tenure, 2011 – 2015 : Associate Professor, 2006 – 2010 : Assistant Professor, Department of Mathematics, The City University of New York, NYCCT
  (On sabbatical fellowship leave 2015–2016).
- 2017 – 2021 : Graduate Faculty, M.S. Program in Data Science, CUNY Graduate Center.
- 2018 : Graduate Faculty, M.S. Program in Data Analysis and Visualization, CUNY GC.
- 2016; 2017: Visiting Professor, Sorbonne University, LIP6, Quantum Information lab, PolSys lab, Paris, France.
- 2014, 2016, 2017, 2018, 2024: Visiting Professor, IHP-Institut Henri Poincaré, Paris, France.
- 2015 – 2018: Advisory board, CUNY Hub for Innovation and Entrepreneurship.
- 2015 – 2018 : Member of the Faculty Advisory Board Data Science @CUNY.

- 2012 – 2018 : Co-Founder, President, University Start-up Infoshield, Inc., NY (This was sold in 2021)
- 2016 – current : Member of the board of advisory at LifeNome Inc. Security Advisor.
- 2008 – 2018 : Director and Founder, Center for Logic Algebra, Computation.
- 2013: Visiting Professor, Universitat Politecnica de Catalunya, Barcelona, Spain.
- 2011: Visiting Professor, University of Toronto, Canada.
- 2004 – 2006 : Assistant Professor in Pure Mathematics, University of St Andrews, Scotland.
- 2005/2006: Visiting Professor, Universite de Geneve, Switzerland.
- November 2004, January 2023: Visiting Professor, IHES-Institute des Hautes Etudes Scientifiques, Paris, France.
- 2000 – 2004 : Lecturer, Mathematics and Statistics Department, Hunter College, CUNY.

Grants, Awards

Research Grants (ONR, NSF, AAAS, NSA, NASA, IHP, AWM, NFRFE, LMS, EMS, SNF, INdAM, RF-CUNY, HIMR)

- ONR, *New Directions in Post-Quantum Cryptography (PQC) and Quantum Key Distribution (QKD)*, PI at CUNY: Delaram Kahrobaei (USA), PI at Sorbonne: Ludovic Perret (France), PI at York: Timothy Spiller (UK), $\sim$ \$0.5M, 2023–2026.
- NSF, The National Science Foundation, Conference Support for the Trimester Post-quantum Algebraic Cryptography at IHP France, Co-PI, \$20K, 2024.
- Mentioned as one of the distinguished Women scientists at IHES as inspiring role-models in the article *Reflecting on how to tackle the gender gap from an institutional perspective: the example of IHES (Institut des Hautes Etudes Scientifiques, France)*, By: Giulia Foffano, development officer at IHES ; Claire Lenz, director of development and communications at IHES ; Emmanuel Ullmo, director at IHES, the Notices of American Mathematical Society, 2023.
- New Frontiers in Research Fund–Exploration, Canadian Government, Co-Principal Investigator, *Algebraic Techniques for Quantum Security*, with A. Broadbent (PI), M. Nevins, H. Salmasian, \$250, 000.00, 2019–2022.
- York Maastricht Partnership Investment Fund, Co-Principal Investigator at York, *Responsible Data Science by Design*, PI at York: D. Kolovos, PI at Maastricht: M. Dumontier, €956,754.00,(2019–2022)
- Institut Henri Poincaré, IHP Trimester *Post-quantum Algebraic Cryptography*, Program leader, €200,000.00, 2024 (with J-C. Faugère, L. Perret, V. Shpilrain)
- ONR Research Grant, Office of Naval Research, Principal Investigator, *Practical Fully Homomorphic Encryption and Applications* (\$448, 000.00) with V. Shpilrain, 2015–2019.
- ONR Research Grant, Office of Naval Research, Principal Investigator, *New Approaches to Information Security Based on Group Theory* (\$448, 962.00) with V. Shpilrain, 2012–2015.
- **Industrial Innovation and Partnership Grants**: National Science Foundation, NSF, I-Corps, Principal Investigator, Secure and efficient outsourcing of computation on private data (\$50, 000.00) with H. Lam, K. Ramaswamy, V. Shpilrain, 2014.
- American Association for the Advancement of Science (AAAS) Women's International Research Collaborations (WIRC), Principal Investigator, (\$20, 000.00), 2012–2013.
- Institut Henri Poincare, IHP, Research in Paris Grant (RiP), with J-C. Faugère, K. Horan, L. Perret, *A Fully Homomorphic Encryption Scheme with noise Using Rings*, 2018.
- National Security Agency (NSA) grant, Co-principal Investigator, support for International Symposium of Symbolic and Algebraic Computation, ISSAC 2018, with PI: A. Ovchinikov, A. Hulpke, \$20, 096.00, 2018.
- London Mathematical Society (LMS), Principal Investigator, Scheme 7, with K. Mallahi-Karai, 2019.
- Heilbronn Institute for Mathematical Research, *York Workshop in Quantum Information, Complexity & Cryptography*, with R. Colbeck, P. Farshim, R. Santhanam, T. Spiller, £5300 (2020)
- York Institute for Future Health, CFHRR10, *A platform for fully encrypted health data analysis*, 2019.

- Risk, Evidence, and Decision-Making Theme priming to support the York Interdisciplinary Workshop on Cyber Security (2019).
- INdAM-GNSAGA (Instituto Nazionale di Alta Matematica, Gruppo Nazionale per le Strutture Algebriche, Geometriche e le loro Applicazioni) research grant, with A. Tortora, M. Tota, Italy, 2018.
- National Science Foundation, PI, DMS-0758054, $12,852.00, To organize International Research Conference for Women in Mathematics on Algebra, Logic, Theoretical Computer Science, with Gitman, 2008–2009.
- PSC-CUNY Grant, CUNY Research Foundation Grant, Principal Investigator, Between $4000.00 to $6000.00 per year, 2007–2011, Traditional B ($6,000.00 each year): 2012–2014, 2015–2017, 2018–2019, 2023–2024. (For teaching course release time and travel/visitors)
- National Science Foundation, through Institut Henri Poincare (Paris), Nexus of Computation Semester (Winter 2016). Analysis in Quantum Information (Fall 2017). Random Walks on Groups (January 2014).
- CUNY Chancellor's "Salute to Scholar" Award, 2008, 2012, 2014, 2016.
- CUNY Fellowship Leave Award, 2015–2016.
- NSF-AWM award, Association of Women in Mathematics, 2011.
- Faculty Fellowship Publication Award, City University of New York, Spring 2009.
- EMS Grant, Principal Investigator, Edinburgh Math. Society-Graphic Generalization of Arithmetic, UK, 2006.
- LMS Grant, Principal Investigator, London Mathematical Society Collaborative Small Grant-Questions concerning True Prosoluble Completion of a group, UK, 2006.
- LMS Grant, Principal Investigator, London Mathematical Society Collaborative Small Grant, Genericity of Residual Solvability of Generalized Free Products, UK, 2005.
- SNF Travel Grant, Swiss National Foundation, January 2005, June 2005, January 2006.
- City Tech Foundation Award to support Center for Logic, Algebra, Computation, PI (2010–2018).
- Faculty Travel Grant for Research, Research Foundation of CUNY (2017)
- Faculty Travel Grant, City Tech Foundation (2006–2017)
- Research assistantship, Research Foundation of CUNY (2001–2004)
- Science Fellowship, CUNY Graduate Center (1999–2001)
- IPM Research Assistantship (1996–1998)

Educational Grants

- NSF Grant, National Science Foundation, Principal Investigator at CUNY, Collaborative Project: Building Cybersecurity Capacity, DUE1128869 ($99,000.00) Total amount of $398,000.00 Joint with NYU, PI at NYU: N. Memon, (2011–2013).
- National Aeronautics and Space Administration (NASA)/Goddard Space Flight Center, Internal Research and Development (IRAD), Co-Principal Investigator, Educational NASA Computational and Scientific Case Studies (enCOMPASS), PI at NASA: N. Memarsadeghi (2012)

Institutional Grants

- NSF Grant, National Science Foundation, Co-Principal Investigator, ADVANCE-IT START proposal, HRD-0811192, 2008– 2011, $195,000.00, PI at NYCCT: Provost August, Co-PIs: Associate Provost Brown, V. Gitman.
- National Science Foundation, NSF-FORWARD to Professorship Grant, Principal Investigator, ($15,000.00), (with Associate Provost Brown) 2011–2013.

Editorial Activities

- Associate Editor of SIAM Journal on Applied Algebra and Geometry (SIAGA), The Society for Industrial and Applied Mathematics, since 2019
  https://www.siam.org/publications/journals/siam-journal-on-applied-algebra-and-geometry-siaga.
- Associate Editor of the Advances in Mathematics of Communications (AMC), American Institute of Mathematical Sciences, https://www.aimsciences.org/journal/1930-5346 since 2019
- Chief Editor of the International Journal of Computer Mathematics: Computer Systems Theory, Taylor and Francis, https://www.tandfonline.com/toc/tcom20/3/3?nav=tocList Since 2019.
- Associate Editor, Journal of Mathematical Cryptology, De Gruyter, https://www.degruyter.com/journal/key/jmc/html?lang=en, since 2022.
- Associate Editor, La Matematica, Springer Nature Group, Official Journal of the Association for Women in Mathematics, Section: Mathematics of Quantum Computing, Cryptography, and Artificial Intelligence, https://www.springer.com/journal/44007, since 2022.
- Editor of the Tbilisi Mathematical Journal, http://tcms.org.ge/Journals/TMJ/ Since 2019.

Research Interests

- Post-Quantum Cryptography (PQC), Quantum Computation, Applied Algebra, Mathematics of Artificial Intelligence (AI), AI for PQC

Selected Books, Publications, Patents:

Books

(118) D. Kahrobaei, R. Flores, M. Noce, M. Habeeb, C. Battarbee, *Book: Applications of Group Theory in Cryptography: Post-quantum Group-based Cryptography*, The Mathematical Surveys and Monographs series of the American Mathematical Society, Volume: 278, pp. 141, ISBN: 978-1-4704-7469-0 (2024)

(117) Handbook: K. Najarian, D. Kahrobaei, E. Dominguez, R. Soroushmehr, *Artificial Intelligence in Health care and Medicine*, CRC Press, Taylor and Francis, 300 pages, ISBN-10: 0367619172, ISBN-13 : 978-0367619176 (2022)

(116) Handbook: D. Kahrobaei, L. Perret, *Post-quantum Cryptography*, To be published in Springer, Information Security and Cryptography book series, (Forthcoming 2025)

NIST PQC Standardization Competition

(115) L. Bettale, D. Kahrobaei, L. Perret, J. Verbel, *Biscuit: Shorter MPC-based Signature from PoSSo*, biscuit-pqc.org, Accepted First Round, NIST Post-quantum Cryptography, Digital Signature Schemes, Competition (2023)

Publications

(114) L. Bettale, D. Kahrobaei, L. Perret, J. Verbel, *Biscuit: New MPCitH Signature Scheme from Structured Multivariate Polynomials*, Applied Cryptography and Network Security. ACNS 2024. Lecture Notes in Computer Science, vol 14583, Springer, Cham, 457– 486 (2024)

(113) C. Battarbee, D. Kahrobaei, L. Perret, S. F. Shahandashti, *A Subexponential Quantum Algorithm for the Semidirect Discrete Logarithm Problem*, PQCrypto 2024, University of Oxford, Springer Lecture Notes in Computer Science, 15th International Conference on Post-quantum Cryptography, volume 14771, 202—226, (2024)

(112) R. Flores, D. Kahrobaei, T. Koberda, *Expanders and right-angled Artin groups*, Journal of Topology and Analysis, World Scientific, 16, no. 2, 155–179 (2024).

(111) R. Flores, D. Kahrobaei, T. Koberda, C. Le Coz, *Right-angled Artin groups and the cohomology basis graph*, Proc. of the Edinburgh Math Society, Cambridge University Press, accepted https://arxiv.org/abs/2309.05495, 1–17, (2024)

(110) C. Le Coz, C. Battarbee, R. Flores, T. Koberda, D. Kahrobaei, *Post-quantum hash functions using $SL_n(\mathbb{F}_p)$*, Advances of Mathematics of Communication, accepted, arXiv:2207.03987, 1–18 (2024).

(109) D. Kahrobaei, M. Noce, E. Rodaro, *Applications of Automata Groups in Cryptography*, https://doi.org/10.1080/23799927.2024.2335157, 1–10, International Journal of Computer Mathematics: Computer System Theory (2024).

(108) D. Kahrobaei, C. Monetta, Perret, M. Tota, M. Vigorito, *Cryptanalysis of protocols using (Simultaneous) Conjugacy Search Problem in certain Metabelian Platform Groups,* https://arxiv.org/abs/2309.13928, Under revision, Journal of Mathematical Cryptology, De Gruyter, 1–12 (2024)

(107) K. Mallahi-Karai, D. Kahrobaei, *Secret sharing and representation theory of p-groups*, De Gruyter, Book Chapter in "Finitely Presented Groups. With Applications in Post-Quantum Cryptography and Artificial Intelligence", 165–173, DOI: 10.1515/9783111473574-010 (2024)

(106) M. Cumplido, D. Kahrobaei, M. Noce, *The root extraction problem in braid group-based cryptography*, https://doi.org/10.1007/s44007-024-00117-x, La Matematica, Springer Nature, 1–11, (2024).

(105) D. Kahrobaei, L. Perret, M. Vigorito, *Security Analysis of ZK PoK based on MQ problem in the Multi-Instance Setting*, 1–7, CIFRIS (2024)

(104) J-C. Faugère, K. Horan, D. Kahrobaei, M. Kaplan, E. Kashefi, L. Perret, *Fast Quantum algorithm for solving system of multivariate system of equations*, Quantum Information and Computation, Rinton Press, 1–25, https://arxiv.org/abs/1712.07211, Under Revision (2024)

(103) C. Battarbee, D. Kahrobaei, Perret, S. F. Shahandashti, *SPDH-Sign: towards Efficient, Post-quantum Group-based Signature*, PQCrypto 2023, The 14th International Conference on Post-Quantum Cryptography, 113–138, Lecture Notes in Computer Science, Springer, **14154**, 14th International Conference on Post-quantum Cryptography (2023)

(102) D. Kahrobaei, M. Stanojkovski, *Cryptographic multilinear maps using pro-p groups*, Advances in Mathematics of Communications, American Institute of Mathematics, Volume 17, Issue 5: 1101–1114 (2023).

(101) H. Gray, C. Battarbee. S. Shahandashti, D. Kahrobaei, *A Novel Attack on McEliece's Cryptosystem*, International Journal of Computer Mathematics: Computer Systems Theory, Taylor & Francis, 8:3, 178–191 (2023).

(100) G. Di Crescenzo, M. Khodjaeva, T. Chen, R. Krishnan, D. Shur, D. Kahrobaei, V. Shpilrain, *On Single-Server Delegation of RSA*, SECITC 2022 (15th International Conference Innovative Security Solutions for Information Technology and Communications) LNCS, Springer Lecture Notes in Computer Science, **13809**, 81–101(2023)

(99) C. Battarbee, D. Kahrobaei, L. Perret, S. F. Shahandashti, *A Subexponential Quantum Algorithm for the Semidirect Discrete Logarithm Problem*, Fourth Post-quantum PQC Standardization Conference, (National Institute of Stardardization and Technology NIST), 1–27 (2022)
https://csrc.nist.gov/csrc/media/Events/2022/fourth-pqc-standardization-conference/documents/paper-a-subexpoenential-quantum-algorithm-pqc2022.pdf .

(98) C. Battarbee, D. Tailor, D. Kahrobaei, S. Shahandashti, *On the efficiency of a general attack against the MOBS cryptosystem*, Journal of Mathematical Cryptology, De Gruyter, vol. 16, no. 1, 289–297 (2022).

(97) C. Battarbee, D. Kahrobaei, S. F. Shahandashti *Cryptanalysis of Semidirect Product Key Exchange Using Matrices Over Non-Commutative Rings*, MathCrypt 2021, Mathematical Cryptology 1(2): 2–9. 2022.

(96) D. Kahrobaei, A. Tortora, M. Tota, *A Closer Look at the Multilinear Maps Using Nilpotent Groups*, International Journal of Computer Mathematics: Computer Systems Theory, **7**, Taylor & Francis, 63–67 (2022)

(95) G. Di Crescenzo, M. Khodjaeva, D. Kahrobaei, V. Shpilrain, *On Single-Server Delegation of RSA Decryption*, CFAIL, Affiliated Workshop of CRYPTO 2022,1–8 (2022).

(94) D. Kahrobaei, V. Shpilrain, *Fully homomorphic encryption of real-life data*, International Journal of Computer Mathematics: Computer Systems Theory, Taylor & Francis, Vol 6, Issue 4, 381–385 (2021)

(93) G. Di Crescenzo, M. Khodjaeva, V. Shpilrain, D. Kahrobaei, R. Krishnan, *Single-Server Delegation of Ring Multiplications from Quasilinear-time Clients*, SIN 2021 (14th International Conference on Security of Information and Networks), IEEE, 1–8, doi: 10.1109/SIN54109.2021.9699330. (2021).

(92) R. Flores, D. Kahrobaei, T. Koberda, *Hamiltonicity via cohomology of right-angled Artin groups*, Linear Algebra and its Applications, Elsevier, Volume 631, 94–110 (2021).

(91) R. Flores, D. Kahrobaei, T. Koberda, *An algebraic characterization of k–colorability*, The Proceedings of the American Mathematical Society, **149** (2021), 2249–2255.

(90) G. Di Crescenzo, M. Khodjaeva, D. Kahrobaei, V. Shpilrain, *Delegating a Product of Group Exponentiations with Application to Signature Schemes*, Journal of Mathematical Cryptology, De Gruyter **14**, no. 1, 438–459 (2021).

(89) S. Isaac, D. Kahrobaei, *A closer look at Tropical Cryptography*, International Journal of Computer Mathematics: Computer Systems Theory 6, Taylor & Francis, no. 2, 137–142 (2021)

(88) G. Di Crescenzo, M. Khodjaeva, D. Kahrobaei, V. Shpilrain, *Secure and Efficient Delegation of Elliptic-Curve Pairing*, 45–68, ACNS 2020, Applied Cryptography and Network Security, Lecture Notes Computer Science **12146**, 45?-66 (2020)

(87) G. Di Crescenzo, M. Khodjaeva, D. Kahrobaei, V. Shpilrain, *Secure and Efficient Delegation of Pairings with Online Inputs*, CARDIS 2020, 19th Smart Card Research and Advanced Application Conference, Springer Lecture Notes in Computer Science (LNCS) **12609** (2021), 84—98 (2020)

(86) J. Gryak, R. Haralick, D. Kahrobaei, *Solving the Conjugacy Decision Problem via Machine Learning*, Experimental Mathematics, Taylor & Francis **29**, no. 1, 66–78 (2020).

(85) A. Yohannis, A. de la Vega, D. Kahrobaei, M. D. Kolovos, *Towards Model-Based Development of Decentralised Peer-to-Peer Data Vaults*, SecureMDE, ACM/IEEE 23rd International Conference on Model Driven Engineering Languages and Systems, Montreal, Canada, 1–8 (2020)

(84) G. Di Crescenzo, M. Khodjaeva, D. Kahrobaei, V. Shpilrain, *Efficient and Secure Delegation to a Single Malicious Server: Exponentiation over Non-Abelian Groups*, Mathematics in Computer Science, Springer **14**, no. 3, 641–656 (2020)

(83) D. Kahrobaei, A. Tortora, M. Tota, *Multilinear Cryptography Using Nilpotent Groups*, De Gruyter Proceedings in Mathematics, 127–133, DOI:10.1515/9783110638387-013 (2020)

(82) R. Flores, D. Kahrobaei, T. Koberda, *A Cryptographic Application of the Thurston norm*, International Journal of Computer Mathematics: Computer Systems Theory, Taylor & Francis, 5:1, 15–24 (2020).

(81) R. Flores, D. Kahrobaei, T. Koberda, *Algorithmic Problems in right-angled Artin groups: Complexity and Applications*, Journal of Algebra, Elsevier **519**, 111–129 (2019)

(80) D. Kahrobaei, K. Mallahi-Karai, *Some applications of arithmetic groups in cryptography*, Groups Complexity, Cryptology, De Gruyter **11**, no. 1, 25–33 (2019).

(79) A. Wood, V. Shpilrain, K. Najarian, D. Kahrobaei, *Private Naive Bayes Classification of Personal Biomedical Data: Application in Cancer Data Analysis*, Elsevier, Computers in Biology and Medicine, **105**, 144–150 (2019).

(78) A. Gribov, J. Gryak, K. Horan, V. Shpilrain, R. Souroush, K. Najarian, D. Kahrobaei, *Medical diagnostic based on encrypted medical data*, Springer, BICT 2019, 11th EAI International Conference on Bio-inspired Information and Communications Technologies, Carnegie Mellon University, Springer-Cham, 98-111 (2019).

(77) G. Di Crescenzo, M. Khodjaeva, D. Kahrobaei, V. Shpilrain, *Practical and Secure Delegation of RSA-type Group Exponentiation to a Single Malicious Server*, 5th IEEE Workshop on Security and Privacy in the Cloud, Washington DC, SPC 2019, 1–9, (2019).

(76) G. Di Crescenzo, M. Khodjaeva, D. Kahrobaei, V. Shpilrain, *Delegating a Product of Group Exponentiations with Application to Signature Schemes*, Conference Proceedings of the Number-Theoretic Methods in Cryptology Conference (University of Sorbonne, Paris), `http://nutmic2019.imj-prg.fr/confpapers/DelegateExp.pdf`, 1–23 (2019).

(75) J. Gryak, D. Kahrobaei, C. Martinez-Perez, *On the conjugacy problem in certain metabelian groups*, Glasgow Mathematical Journal, Cambridge University Press **61**, Issue 2, 251–269 (2019).

(74) A. Gribov, D. Kahrobaei, V. Shpilrain, *Practical Private-key Fully Homomorphic Encryption in Rings*, Groups Complexity Cryptology, De Gruyter, **10**, 17–27, no. 1 (2018).

(73) A. Wood, V. Shpilrain, K. Najarian, A. Mostashari, D. Kahrobaei, *Private-Key Fully Homomorphic Encryption for Private Classification*, Springer Lecture Notes in Computer Science **10931**, 475–481 (2018)

(72) K. Horan, D. Kahrobaei, *Hidden Subgroup Problem and Post-quantum Group-based Cryptography*, Springer Lecture Notes in Computer Science **10931**, 218–226 (2018)

(71) L. Barthelemy, D. Kahrobaei, G. Renault, Z. Sunic, *Quadratic Time Algorithm for Inversion of Binary Permutation Polynomials*, Springer Lecture Notes in Computer Science **10931**, 19–27 (2018)

(70) A. Wood, R. Soroushmehr, N. Farzaneh, D. Fessell, K. R. Ward, J. Gryak, D. Kahrobaei, K. Najarian, *Fully Automated Spleen Localization and Segmentation Using Machine Learning and 3D Active Contours*, IEEE Engineering in Medicine and Biology Conference (EMBC'18) 53–56 (2018).

(69) G. Di Crescenzo, M. Khodjaeva, D. Kahrobaei, V. Shpilrain, *Efficient and Secure Delegation to a Single Malicious Server: Exponentiation over Non-Abelian Groups*, Springer Lecture Notes in Computer Science **10931**, 137–146 (2018)

(68) I. Chatterji, D. Kahrobaei, N. Y. Lu, *Cryptosystems Using Subgroup Distortion*, Theoretical and Applied Informatics **29**, 14–24 (2017).

(67) G. Di Crescenzo, D. Kahrobaei, M. Khodjaeva, V. Shpilrain, *Practical and Secure Delegation of Exponentiations over Discrete-Log Groups to a Single Malicious Server*, CCSW '17 Proceedings of the 2017 on Cloud Computing Security Workshop, Association for Computing Machinery (ACM), 17–28 (2017).

(66) G. Di Crescenzo, D. Kahrobaei, M. Khodjaeva, V. Shpilrain, *Computing Multiple Exponentiations: From Batch Verification to Batch Delegation*, IEEE Conference on Communications and Network Security IEEE CNS 2017, the Third IEEE Workshop on Security and Privacy in the Cloud (SPC) 531–539 (2017).

(65) B. Cavallo, J. Delgado, D. Kahrobaei, E. Ventura, *Algorithmic Recognition of Infinite-Cyclic-Extentions*, Journal of Pure and Applied Algebra, Elsevier, **221** (2017) 2157–2179.

(64) S. Molaei, K. Horan, B. Nallamothu, D. Kahrobaei, M. Shiri, K. Najarian *Deep Convolutional Neural Networks for Left Ventricle Segmentation*, Conference proceeding, IEEE Engineering in Medicine and Biology Society conference (EMBC'17) 668–671 (2017).

(63) R. Flores, D. Kahrobaei, *Cryptography with Right-angled Artin Groups*, Theoretical and Applied Informatics **28** (2016), no. 3, pp. 8–16.

(62) D. Kahrobaei, V. Shpilrain, *Invited Paper: Using semidirect product of (semi)groups in public key cryptography*, Computability in Europe 2016, Lecture Notes in Computer Science, Springer, LNCS **9709**, Pursuit of the Universal, 132–141 (2016).

(61) D. Garber, D. Kahrobaei, H. T. Lam, *Length Based attack for Polycyclic Groups*, Journal of Mathematical Cryptology, De Gruyter, 33-44 (2015).

(60) B. Cavallo, G. Di Crescenzo, D. Kahrobaei, V. Shpilrain, *Efficient and Secure Delegation of Group Exponentiation to a Single Server*, RFIDsec 2015, Springer Lecture Notes Computer Science **9440** (2015), 156–173.

(59) D. Kahrobaei, C. Koupparis, and V. Shpilrain, *A CCA secure cryptosystem using matrices over group rings*, Contemporary Mathematics **633**, American Mathematical Society, 73–80 (2015).

(58) B. Cavallo, D. Kahrobaei, *Secret sharing using the Shortlex order and non-commutative groups*, Contemporary Mathematics **633**, American Mathematical Society, 1–8, (2015).

(57) B. Cavallo, D. Kahrobaei, *A Polynomial Time Algorithm For The Conjugacy Decision and Search Problems in Free Abelian-by-Infinite Cyclic Groups*, Reports@SCM **1**, No. 1, Electronic Journal of the Societat Catalana de Matematiques, 55–61 (2014).

(56) D. Kahrobaei, H. T. Lam, *Heisenberg groups as platform for the AAG key-exchange protocol*, 2014 IEEE 22nd International Conference on Network Protocols (ICNP), IEEE, 660–664 (2014).

(55) M. Habeeb, D. Kahrobaei, C. Koupparis, and V. Shpilrain, *Public key exchange using semidirect product of (semi)groups*, in: ACNS 2013, Applied Cryptography and Network Security, Lecture Notes Comp. Sc. **7954** (2013), 475–486.

(54) A. Douglas, D. Kahrobaei, and J. Repka, *A Classification of Embedding of Abelian Extensions of D_n into E_{n+1}*, Journal of Pure and Applied Algebra, Elsevier, **217** (2013), 1942-1954.

(53) D. Kahrobaei, C. Koupparis, and V. Shpilrain, *Public key exchange using matrices over group rings*, Groups, Complexity, and Cryptology **5** (2013), 97–115.

(52) D. Kahrobaei, C. Koupparis, *Non-commutative digital signatures using non-commutative groups*, Groups, Complexity, Cryptology **4** (2012), 377–384. skip

(51) M. Habeeb, D. Kahrobaei, and V. Shpilrain, *A Secret Sharing scheme based on group-presentation and word problem*, Contemporary Mathematics, American Mathematical Society **582** (2012), 143–150.

(50) D. Kahrobaei, S. Majewicz, *Residual Solvability of Generalized Free Products of Solvable Groups*, Discrete Mathematics and Theoretical Computer Science, France, **13**, No 4 (2012), 45-50.

(49) D. Kahrobaei, E. Vidaurre, *Publicly verifiable secret sharing using non-abelian groups*, Contemp. Math., **582**, Amer. Math. Soc., 175–179 (2012).

(48) D. Kahrobaei, On Residual Solvability of Generalized Free Products of Finitely Generated Nilpotent Groups, Communications in Algebra, Taylor and Francis Publication, **39** (2011), 647–656.

(47) K. Falconer, B. Fine, D. Kahrobaei, *On Growth Rate of an Endomorphism of a Group*, Groups, Complexity, Cryptology, De Gruyter Publication, **3**, Issue 2 (2011), 285–300.

(46) K. Bencsath, A. Douglas, D. Kahrobaei, *Some Residually Solvable One-relator Groups*, Bulletin of the Irish Mathematical Society **65** (2010), 23–31.

(45) M. Habeeb, D. Kahrobaei, V. Shpilrain, *A new Public Key Using Semi-Direct Products*, Proceedings of the Second International Conference on Symbolic Computation and Cryptography, Royal Holloway University of London, (2010), 137–142.

(44) D. Kahrobaei, M. Anshel, *Decision and Search in non-abelian Cramer Shoup*, Groups, Complexity, Cryptology, De Gruyter Publication, 1 (2009), 217–225.

(43) D. Kahrobaei, *Book Chapter: Doubles of Residually Solvable groups*, Aspects of Infinite Group Theory, Algebra and Discrete Math, World Scientific Publication, **1** (2008), 192–200.

(42) G. Arzhantseva, P. de la Harpe, D. Kahrobaei, *The True Prosoluble Completion of a Group: Examples and Open Problems*, Geometriae Dedicata, Springer Netherlands, **124**, No.1 (2007), 5–26. (Appendix by G. Arzhantseva, Z. Sunic).

(41) K. Bhutani, B. Khan, D. Kahrobaei, *A Graphic Generalization of Arithmetic*, Integers: Electronic Journal of Combinatorial Number Theory, **7**, A12 (2007), 1–31.

(40) D. Kahrobaei, B. Khan, *A Non-Commutative Generalization of the El Gamal Key Exchange using Polycyclic Groups*, Proceeding of IEEE, GLOBECOM (2006), 1–5.

(39) D. Kahrobaei, *A Simple Proof of a Theorem of Karrass and Solitar*, Contemporary Mathematics, American Mathematical Society, **372** (2005), 107–108.

Survey Papers

(38) C. Battarbee, D. Kahrobaei, S. Shahandashti, *Semidirect Product Key Exchange: the State of Play*, Journal of Algebra and Applications, World Scientific, Special Issue on Recent Advances in Coding Theory and Cryptography, `https://doi.org/10.1142/S0219498825500665` , 1–12 (2024).

(37) M.I.Gonzalez Vasco, D. Kahrobaei, E. McKemmie, *Applications of Simple Groups in Cryptography in the quantum Era*, La Matematica, Springer Nature, `https://doi.org/10.1007/s44007-024-00096-z`, 1–16 (2024)

(36) D. Kahrobaei, R. Flores, M. Noce, Invited Paper: *Group-based Cryptography in the Quantum Era*, The Notices of American Mathematical Society, Volume 70, Number 5, 752–763 (2023)

(35) G. Di Crescenzo, M. Khodjaeva, D. Kahrobaei, V. Shpilrain, Invited Paper: *A Survey on Delegated Computation*, Proceedings of The 26th International Conference Developments in Language Theory (DLT-2022) Tampa, FL, USA, Springer Lecture Notes in Computer Science, LNCS **13257**, 33-53 (2022)

(34) A.Wood, K. Najarian, D. Kahrobaei, *Homomorphic Encryption for Machine Learning in Medicine and Bioinformatics*, Association for Computing Machinery (ACM), Computing Surveys, DOI:10.1145/3394658, Vol. 53, No. 4, Article 70, 1–35 (2021).

(33) D. Kahrobaei, M.L. Noce, *Algorithmic Problems in Engel Groups and Cryptographic Applications*, International Journal of Group Theory,Volume 9, Issue 4, 231—250 (2020).

(32) J. Gryak, D. Kahrobaei, *The Status of the Polycyclic Group-Based Cryptography: A Survey and Open Problems*, Groups Complexity Cryptology, De Gruyter, Volume **8**, Issue 2, 171–186 (2016).

(31) B. Fine, M. Habeeb, D. Kahrobaei, G. Rosenberger *Aspects of non-abelian group-based cryptography: A survey and open problems*, JP Journal of Algebra and Number Theory **21** (2011), 1–41.

(30) S. Sze, D.Kahrobaei, R.Dambreville, M. Dupas , *Finding n-root in nilpotent groups and applications in cryptography*, IJAM, 1-20 (2011)

Patents

(29) K. Najarian, A. Wood, C. Minoccheri, E. Wittrup, J. Gryak, R. Wilson, D. Kahrobaei, *Systems and Methods for Classifying Encrypted Data Using an Encrypted Machine Learning Model*, under submission for Full US Patent Application. (2024)

(28) C. Le Coz, C. Battarbee, R. Flores, T. Koberda, D. Kahrobaei, *Post-quantum hash functions using* $SL_n(\mathbb{F}_p)$, pending Provisional US Patent 2023.

(27) D. Kahrobaei, V. Shpilrain, H. T. Lam, *System and Method for Private-Key Fully Homomorphic Encryption and Private Search Between Rings* US Patent 10,396,976 (2019)

(26) D. Kahrobaei, B. Cavallo, V. Shpilrain, *Method and apparatus for secure delegation of computation*, U.S. Patent 9,825,926 (2017)

Books

(25) D. Kahrobaei, K. Bencsath, Book: *Group products and residual solvability*, 128 pp, ISBN-10: 3843368465, ISBN-13: 9783843368469 (2010)

Edited Books

(24) D. Kahrobaei, M. Khodjaeva, *Mathematical Aspects of Cryptography and Coding Theory*, Accepted by La Matematica, Springer Nature (2024)

(23) J.-F. Biasse, C. Carlet, G. Di Crescenzo, M. I. Gonzalez Vasco, D. Kahrobaei, S. Mesnager, Edited Book: *Mathematics of Cryptography and Coding in the Quantum Era*, International Journal of Computer Mathematics: Computer Systems Theory, Taylor & Francis `https://www.tandfonline.com/toc/tcom20/6/4` 243–404 (2021).

(22) D. Kahrobaei, B. Cavallo, D. Garber, *Algebra and Computer Science*, American Mathematical Society, Contemporary Mathematics, **677**, ISBN-13 978-1-4704-2303-2 (2016).

(21) D. Kahrobaei, V. Shpilrain, *Algorithmic Problems in Group Theory, Their Complexity and applications in Information Security*, American Mathematical Society, Contemporary Mathematics **633**, ISBN 978-0–8218–9859–8, (2015).

(20) B. Fine, D. Kahrobaei, and G. Rosenberger, *Computational and Combinatorial Group Theory and Cryptography*, American Mathematical Society, Contemporary Mathematics, **582**, ISBN-10: 0-8218-7563-9, ISBN-13: 978-0-8218-7563-6 (2012), 1–199.

(19) D. Kahrobaei, *Groups, Complexity, Cryptology*, De Gruyter Publication **3**, Issue 1, ISSN 1869-6104 (2011).

Extended Abstracts

(18) D. Kahrobaei, *The Impact of the Semidirect Discrete Logarithm Problem (SDLP) in Post-quantum Cryptography (PQC)* DOI: `https://doi.org/10.69091/koine/vol-1-W20`, DE CIFRIS KOINE, 124–126 (2024)

(17) A. Wood, V. Shpilrain, K. Najarian, D. Kahrobaei, *Applications of Fully Homomorphic Encryption for Private Analytics in Healthcare*, Conference Proceedings of the Second Annual Symposium on Business Analytics, New York (2018)

(16) A. Gribov, J. Gryak, K. Horan, D. Kahrobaei, V. Shpilrain, R. Souroush, K. Najarian, *Medical Diagnostics Based on Encrypted Medical Data*, Conference Proceedings of the Second Annual Symposium on Business Analytics, New York (2018)

(15) J-C. Faugère, K. Horan, D. Kahrobaei, M. Kaplan, E. Kashefi, L. Perret, Extended Abstract-presented as a poster, *Fast Quantum Algorithms for Solving Multivariate Quadratic Equations over Finite Fields*, QCrypt, 8th International Conference on Quantum Cryptography (2018).

Thesis

(14) D. Kahrobaei, *Residual Solvability of Generalized free products*, PhD Thesis, CUNY Graduate Center, (2004), 1–194.

Diversity, Equity, Inclusion Article

(13) P. Brown, D. Kahrobaei, *Metropolitan Mentors: Building a Network of Women in Mathematics and Computer Science across New York City*, Book chapter in : *Forward to Professorship in STEM: Inclusive Faculty Development Strategies that Work.* Mavriplis, C. and Heller, R., eds. Elsevier Publishing. ISBN: 978-0-12-800855-3 (2015).

Submitted Articles

(12) D.Kahrobaei, A. Malik, D. Savchuk, *Analysing Heuristic Solutions of the Conjugacy Search Problem in Contracting Self-similar Groups*, 1–24, Under Submission (2024)

(11) C. Battarbee, G. Borin, R. Cartor, N. Heninger, D. Jao, D. Kahrobaei, L. Maddison, E. Persichetti, A. Robinson, D. Smith-Tone, R. Steinwandt, *On the Semidirect Discrete Logarithm Problem in Finite Groups*, Submitted to Asiacrypt'24. `https://eprint.iacr.org/2024/905.pdf`, 1–24.

(10) G. Di Crescenzo, M. Khodjaeva, D. Kahrobaei, V. Shpilrain, *Batch Delegation of Exponentiation in Discrete Log and RSA Groups*, `https://shpilrain.ccny.cuny.edu/journal-v8_submit.pdf`, Under submission, 1–22 (2024).

Preprints

(9) D. Kahrobaei, H. T. Lam, V. Shpilrain, *Public key exchange using extensions by endomorphisms and matrices over a Galois field*, Preprint, 1–10, `http://www.sci.ccny.cuny.edu/~shpil/semi_galois.pdf` (15 citations on google scholar) (2014).

(8) M. Habeeb, D. Kahrobaei, V. Shpilrain, *A semidirect Product Key-Exchange Protocol Using Free metabelian Groups*, Preprint, 2012.

(7) B. Eick, D. Kahrobaei, *Polycyclic Groups: A New Platform for Cryptology?*, `math.GR/0411077`, Preprint (2004), 1–7. (92 citations on google scholar)

Newspapers and Magazines

(6) Y. Antolin, D. Kahrobaei, *Trenzas matematicas para guardar secretos*, El Pais, https://elpais.com/elpais/2019/05/06/ciencia/1557136645_167329.html (2019)

(5) D. Kahrobaei (Interviewed), Bloomberg Law, *AI Watermarking Tools Emerging to Tag Machine-Made Content*, https://news.bloomberglaw.com/privacy-and-data-security/ai-watermarking-tools-emerging-to-tag-machine-made-content (August 7, 2023)

(4) D. Kahrobaei (Interviewed), Fortune Magazine, *Quantum computers threaten to end digital security. Here's what's being done about it*, https://fortune.com/2020/09/11/post-quantum-encryption-algorithm-nist/ (2020)

(3) D. Kahrobaei (Interviewed), *VPN*, The Wall Street Journal, https://www.wsj.com/articles/what-is-a-vpn-do-i-need-to-us (August 2022).

(2) D. Kahrobaei (Interviewed), DNA Ancestry Kits: The Risks to Consider Before You Spit PBS Public Broadcasting Service, Twin Cities, https://www.tpt.org/post/from-rewire-risks-with-dna-ancestry-kits/, February 8, 2019.

(1) D. Kahrobaei, A. Mostashari, *How Adversarial Artificial Intelligence is Threatening Our Digital Future*, News Week Expert Forum, https://www.newsweek.com/how-ai-quantum-computing-are-challenging-security-our-digital-future-182562 (September 2023)

Graduate Advisors and Postdoctoral Sponsors: G. Baumslag (CUNY Graduate Center)

Ph.D. Thesis and Postdoctoral Advisor (Internal/External):

(51) Ph.D. Thesis Advisor to Maggie Habeeb (Ph.D. in Mathematics 2012, CUNY Graduate Center), Currently tenured full professor Pennwest California University (since 2024).

(50) Ph.D. Thesis Advisor to Charalambous Koupparis (Ph.D. in Mathematics 2012,CUNY Graduate Center), Former Director, Head of Data Science, Strategy & Analytics, Quant, Royal Bank of Canada Capital Markets, Currently Managing Director, Techniques Two Sigma, New York, USA

(49) Ph.D. Thesis Advisor to Ha T. Lam (Ph.D. 2014 in Mathematics, CUNY Graduate Center), Postdoc at CUNY Graduate Center, then CTO at Infoshield, Inc., then Postdoc at Ericsson, then Security Engineer at Oblong Industries in Los Angeles, CA, Currently Senior Applied Cryptographer at Oracle, California.

(48) Ph.D. Thesis Advisor to Bren Cavallo (Ph.D. 2015 in Mathematics, CUNY Graduate Center), Currently Research Data Scientist, Meta AI, New York.

(47) Ph.D. Thesis Advisor to Jonathan Gryak (Ph.D. in Computer Science 2017, (2014–2017) CUNY Graduate Center), Currently Tenure-Track Assistant Professor Queens College, CUNY, Former Research Scientist (a research faculty position) in the Michigan Institute for Data Science University of Michigan, Senior Research Supervisor at University of Michigan (Ann Arbor) in Computational Medicine and Bioinformatic Department (2017–2022).

(46) Ph.D. Thesis Advisor to Matluba Khodjaeva (Ph.D. in Computer Science 2017, (2016–2017), CUNY Graduate Center, Currently tenure track assistant professor at the City University of New York, Senior college: John Jay College, Doctoral Faculty CUNY Graduate Center)

(45) Ph.D. Thesis Advisor to Alexander Wood (Ph.D. in Computer Science September 2018, (2015–2018) CUNY Graduate Center, Currently artificial Intelligence Engineer at MITRE, highly selective National Security Accelerator Program (NSAP), Previously postdoctoral fellow at University of Michigan in Ann Arbor (2017–2021), Intern (summer 2017) then Research Scientist, at University of Michigan in Ann Arbor, Computational Medicine Department

(44) Ph.D. Thesis Advisor to Christopher Battarbee, Ph.D. in Computer Science, University of York, UK (2020–2023), Postdoctoral Fellow Sorbonne University starting October 2023. with S. Shahandashti

(43) PhD Thesis Advisor, Martina Vigorito, PhD in Mathematics, University of Salerno, Italy, Co-supervised with M. Tota and P. Longobardi (Since 2022)

(42) PhD Thesis Supervisor: Juan Vieira, PhD in Physics, University of York, UK (2023–2026) Primary supervisor: T. Spiller.

(41) Postdoctoral Advisor to Alfa Yohannis (Postdoc in Computer Science, University of York, March 2020-March 2022; Co-supervising with Professor Kolovos, and Dr. Matragkas)

(40) PhD Thesis External Examiner, École Normale Superieur Paris, France, Aisling Connolly, Department of Mathematics, Advisor: David Naccache, September 13, 2019.

(39) PhD Thesis External Examiner, University of Sorbonne, France, Olive Chakraborty, Multivariate Post-quantum Cryptography, Advisors: Ludovic Perret, Jean-Charles Faugére, December 2020.

(38) President of the Jury of the PhD Thesis Committee, Sorbonne University, Paris Cité, France, Emmanuel Rauzy, Department of Mathematics, Perspectives on an effective theory of groups, Advisor: Andrzej Zuk, June 24, 2022.

(37) Member of Jury of the PhD Thesis Defence, The University of Paris VIII, France, Department of Mathematics, Ruikai CHEN, Contributions algebriques a des polynomes specifiques sur des corps finis pour la theorie des codes et la cryptographie (Algebraic contributions to some specific polynomials over finite fields for coding theory and cryptography), Advisor: Sihem Mesnager, June 2024.

(36) PhD Thesis Examiner, CUNY Graduate Center, Shervin Parsi, Unification of generative and classifier models in machine learning, Department of Physics, Advisor: David Schwab, May 2022, August 15, 2023.

(35) PhD Thesis External Examiner, University of Birmingham, UK, Any Muanalifah, Modifying the tropical version of Stickel's protocol, Department of Mathematics, Advisor: Sergey Sergeev, March 7, 2022.

(34) PhD Thesis External Examiner, University of Passau, Germany, Ange Salome Messeng Ekossono, On some contributions to the algebraic cryptoanalysis of elliptic curve cryptosystems, Department of Mathematics, Advisor: Martin Kreuzer, 2024.

(33) PhD Thesis External Examiner, CUNY Graduate Center, Haripriya Chakraborty, Mechanism Design and Modeling to Analyze Complex Social Systems for Public Policy, Advisor: Liang Zhao, 2021

(32) PhD Thesis External Examiner, CUNY Graduate Center, USA, Nur Dean, Game Dynamics in Complex Networks, Advisor: Shweta Jain, June 24, 2020.

(31) Postdoctoral Advisor to Armin Weiβ (Postdoc in Computer Science, summer 2015, CUNY Graduate Center)

(30) Postdoctoral Advisor to Alexey Gribov (Postdoc in Computer Science, October 2015– January 2017, CUNY Graduate Center)

(29) PostdocAdvisor to Christopher Battarbee, Sorbonne University, France, with L. Perret, 2023–2006.

(28) Advisor of the Visiting Postdoctoral Fellow, Maria Cumplido, University of Seville, Spain (April 2022)

(27) Advisor of the Visiting Postdoctoral Fellow, Eilidh McKemmie, Rutgers University (Spring 2023)

(26) Advisor of the Visiting Postdoctoral Fellow, Marialaura Noce, Gottingen University Germany and University of Salerno Italy (January 2022)

(25) Advisor of the Visiting Postdoctoral Fellow, Mima Stajonovski, Max Planck Institute Germany, (February 2020)

(24) Advisor of the Visiting Postdoctoral Fellow, Corentin Le Coz, Technion Institute of Technology, Israel (March 2022)

(23) Jordi Delgado (Visiting PhD student in Mathematics from UPC Barcelona, CUNY Graduate Center, Summer/Fall 2015)

(22) External PhD Thesis Examiner in Mathematics, University of Newcastle: Jack Aiston, Homomorphic Encryption and Quantum Computation (2020) Advisor: Andrew Duncan.

(21) Chair of Committee of the Ph.D. Dissertation Proposal for Kelsey Horan (Ph.D. in Computer Science December 2018.)

(20) External PhD Thesis Examiner in Mathematics, Rutgers University: Leigh Cobbs, Lattice Subgroups of Kac-Moody Groups (July 2009) Advisor: Lisa Carbone.

(19) External PhD Thesis Examiner in Computer Science, CUNY Graduate Center: Xiaodong Yan, Preconditioning methods for Matrix Computation (January 2015) Advisor: Victor Pan.

(18) Ph.D. Thesis Examiner in Computer Science, CUNY Graduate Center: C.Chum, Hash functions, Latin Squares, Secret Sharing Schemes (May 2009, 2010), Advisor: Sean Zhang.

(17) Ph.D. Thesis Examiner in Computer Science, CUNY Graduate Center: M.Chen, Monte Carlo RFID Library Location System (November, 2010 for the Proposal and April 2013 for the defense) Advisor: Sean Zhang.

(16) Committee member of the Ph.D. Oral Exam in Computer Science, Priya Chakraborty, September 13, 2017, Model Compression in Deep Neural Networks, Advisor: Victor Pan.

(15) Ph.D. Thesis Proposal Examiner in Computer Science, CUNY Graduate Center, Yunqi Xue, April 9th 2015, In search of Homo Sociologicus, Advisor: Rohit Parikh.

(14) Committee member of the Ph.D. Oral Exam in Mathematics, CUNY Graduate Center: Gabrielle Zapata, Group-Based Cryptography, November 6, 2015. Advisor: Vladimir Shpilrain.

(13) Committee member of the Ph.D. Oral Exam in Mathematics, CUNY Graduate Center: Lisa Bromberg, May 18, 2012. Advisor: Vladimir Shpilrain.

(12) Committee member of the Ph.D. Oral Exam in Computer Science, CUNY Graduate Center: Qi Luan, Low-rank Approximation and Finding Large Volume Sub-matrices through Randomized Dimensionality Reduction, August 30, 2016. (Advisor Victor Pan)

(11) Committee member of the Ph.D. Oral Exam in Computer Science, CUNY Graduate Center: V. Zaderman, Approximating roots of polynomials, August 30, 2016. (Advisor: Victor Pan)

(10) Committee member of the Ph.D. Oral Exam in Mathematics, CUNY Graduate Center: Bianca Sosnovski, September 2010. Committee member of the Ph.D. Thesis Exam in Mathematics, CUNY Graduate Center, April 8, 2016. (Advisor: Vladimir Shpilrain)

(9) Chair of committee of PhD Oral Exam in Computer Science, Ni Yen Lu, CUNY Graduate Center, February 2017.

(8) Chair of committee of PhD Oral Exam in Computer Science Severin Fanja Ngnosse, CUNY Graduate Center, September 2015.

(7) Committee member of the Ph.D. Oral Exam in Mathematics, CUNY Graduate Center: Eli Amzallag, Cryptography with Tropical Algebra, December 2013. (Advisor: Alexey Ovchinnikov)

(6) Ph.D. Thesis Proposal Examiner in Computer Science, CUNY Graduate Center: Mohamed Ayed, October 2019. *Network embedding of chemical bioactivity* (Advisor: Lei Xie)

(5) Supervised NSF-LS-AMP for minority PhD student at CUNY Graduate Center in Mathematics Department: Elizabeth Vidaurre (Fall 2011, Spring 2012)

(4) Supervised NSF-LS-AMP for minority PhD student at CUNY Graduate Center in Mathematics Department: Bianca Sosnovski (2012)

(3) Supervised a Research Project, CUNY Graduate Center in Mathematics Department PhD student Sandra Sze (2011)

(2) MSc Thesis External Examiner, University of Sorbonne, Paris 7, France, Antoine Goldsborough, Groupes aléatoire, Advisor: Andrzej Zuk, June 15, 2020.

(1) Supervised summer research project of M.Sc. student at University of St Andrews, Scotland, Mathematics Department: Andrew Furgeson (2005), PhD Warwick University, Postdoc at Bristol University.

Selected Invited Visiting Positions:

- April 21–24, 2024, University of Michigan, USA.
- September 12–15, 2023, Sorbonne University, France.
- July 26–28, 2023, Constructor University (formerly Jacob University of Bremen), Germany.
- July 18–July 23, 2023, University of Seville, Spain.
- July 10–16, 2023, University of Salerno, Italy
- June 13–17, 2023, University of South Florida, USA.
- June 5–10, 2023, University of California San Diego, UCSD, USA.
- August 8–11, 2022, Cornell University, Communication in Mathematics, Ithaca.
- January 27–February 3, 2022, IHES, Paris, France.
- April 16–21, 2023, Schloss Dagstuhl – Leibniz-Zentrum fur Informatik, Pushing the Limits of Computational Combinatorial Constructions, Germany.
- July 25–28, 2022, International Centre for Mathematical Sciences, Foundations and Applications of Lattice-based Cryptography, Edinburgh, Scotland.
- February 24–28, 2020, Universidad Rey Juan Carlos Campus de Mostoles (Madrid), Spain
- December 9–12, 2019, University of Almeria, Spain
- September 16–21, 2019, State University of Yerevan, Armenia.
- August 5–10, 2019, University of Ottawa, Canada.
- March 18–20, 2019, Universidad Autonoma de Madrid, Spain.
- August 24–29, 2018, September 7–11, 2015, University of Nice, France.
- May 2018, University of Salerno, Italy.
- May 22–26, 2017: International Center for Mathematical Sciences, Program on "Braids in algebra, geometry and topology", Edinburgh, Scotland.
- January 13–17, 2016: University of South Florida, Tampa.
- January 4–8, 2016: University of Michigan, Ann Arbor.
- October 2–6, 2014, November 12–19, 2015, University of Nebraska in Lincoln.
- October 7–10, 2015, University of Bilbao in Basque Country, Spain.
- September 24– October 6, 2015, University of Zaragoza, Spain.
- September 14–18, 2015, CIRM (Centre International de Rencontres Mathematiques), Luminy, Marseilles, France.
- August 31–September 4, 2015, Technische Universiteit Eindhoven, Netherlands.
- June 1–7, 2015: ENS Paris, France.
- January 19–26, 2015: University of Florence, Italy.
- August 25–29: RWTH Aachen University, Germany.
- March 31–April 5, 2014: Erwin Shrodinger International Institute, University of Vienna, Austria.
- August 1–6, 2011: ICERM-Institute of Computational and Experimental Mathematics, Brown University.
- November 16–20, 2005, July 18–24, 2010: University of Warwick, England, UK.

- August 30–September 6, 2010: CRM-The Centre de Recherches Mathematiques, Montreal, Canada.
- August 13–17, 2007: AIM- American Institute of Mathematics, Palo Alto, USA.
- December 15–23, 2005: Ecole Polytechnique Federale de Lausanne, Switzerland.
- July 8–16, 2005: Isaac Newton Institute for Mathematical Sciences, Cambridge University, England, UK.
- June 28–July 7, 2005: Forschungsinstitut fur Mathematik, ETH Zurich, Switzerland.

Synergistic Activities:

- Review Panel, The Swiss National Science Foundation and the National Foundation for Science and Technology Development (NAFOSTED) in Vietnam, 2024.
- Committee member for selection of CARMIN Professor, IHES, Institute des Hautes Etudes Scientifiques, 2024.
- Launching Planning Grant, CUNY, 2021–2022.
- Launching Interdisciplinary Research Grant, CUNY, 2021–2022.
- Chair of Review Panel: Planning Grant, CUNY, 2021–2022.
- Review panelist, The CUNY Green Energy grants, 2021.
- Panelist for Canadian Banff International Research Station, workshop proposal, 2023
- Panelist for CHIST-ERA, European Union and French National Foundation. It is a consortium of research funding organisations in Europe and beyond supporting use-inspired basic research in Information and Communication Technologies (ICT) or at the interface between ICT and other domains. The CHIST-ERA consortium is itself supported by Horizon Europe within the European Innovation Council?s Pathfinder programme. CHIST-ERA promotes novel and multidisciplinary research with the potential to lead to significant technology breakthroughs in the long term. 2023.
- Served as a panelist for the Knowledge Foundation, a major Swedish research foundation supporting research projects carried out in collaboration between academia, industry, and other organisations. The foundation is endowed and created by the Swedish government, Sweden, 2022.
- Served as a panelist for the National Centre for Cyber Security (NCSC), UK, 2020, 2021.
- Served as a panelist for the EPSRC, The Engineering and Physical Sciences Research Council, UK, 2020, 2021, 2022.
- Served as a panelist for the The Dutch Research Council (NWO), Cyber Security Programme, Netherlands, 2020.
- Served as a panelist for the New Frontiers in Research Fund, the Exploration 2020 multidisciplinary review panel, Canada, 2020.
- Served as a panelist for the Royal Academy of Engineering, Research Fellowship, UK, 2020, 2021.
- Served as a panelist for the National Science Foundation, Research, Educational, Institutional grants (2010, 2012, 2013, 2015, 2016, 2021)
- Served as a panelist for the ANR, Agence Nationale de la Recherche, QuantERA, Supporting European research projects in Quantum Technologies, France (2019)
- Served as a panelist for the NSERC, Natural Sciences and Engineering Research Council of Canada, Mathematical, Environmental and Physical Sciences Division (2017)
- Served as a panelist for the American Association for the Advancement of Science, Research Grants. (2013, 2014, 2015, 2016, 2017)
- Invited Judge NYC Regional Business Plan Competition - March 18, 2022.
- Member of the Research Committee at the CUNY Graduate Center (2015–2018)

- Peer Reviewer, The Research Foundation of The City University of New York (RFCUNY) Peer Review Program (2018)
- Founder of the New York Women in Mathematics and Computing Network.
- Reviewer of Henslow Research Fellowship 2022 (Sciences), Selwyn College, Cambridge University (UK), 2022.
- Co-organizer of the New York Applied Algebra Colloquium at the CUNY Graduate Center (2008–2018).
- Co-organizer of the Algebra and Cryptography seminar at the CUNY Graduate Center. (2010–current)
- Organizer of the Mathematical Aspects of Cryptography Student Seminar at CUNY Graduate Center.
- Co-organized 2 summer bootcamps for female high school teachers in cybersecurity. These teachers trained 22 female high school students for the cybersecurity competition at NYU.
- Developed several new interdisciplinary graduate courses on Group-based Cryptography at the CUNY Graduate Center.
- Developed several new courses in Data Science at the CUNY Graduate Center.
- Reviewer for Mathematical Reviews, American Mathematical Society (2007–2017)
- Computing Reviewer for The Association for Computing Machinery
- Panel Member for the research projects of the PSC CUNY Grants in Computer Science, Research Foundation of City University of New York (2011 – 2018)
- Panel Member for the research projects of the PSC CUNY Grants in Mathematics, Research Foundation of City University of New York (2010)
- Book Reviewer for Springer-Verlag
- Elected to chair of AMS committee of teaching assistants and part time instructors (February 2012-January 2013) Served on the committee (2010-2013)
- Mentor for the Association for Women in Mathematics Mentor Network, (2008–2018)
- Voting Member of Graduate Council, CUNY Graduate Center, PhD Program in Computer Science Department representative, (2010–2018).
- Chair of Grants and Research Committee in the School of Arts and Sciences, NYCCT, CUNY, 2009-2010, 2011-2012, 2013-2014, 2014-2015.
- Member of the Advisory Council at the New York City College of Technology, (2014–2018)
- Supervising Summer Research Project Funded by the NCSC, National Cyber Security Centre UK, Clara Simons, University of York, with S. Shahandashti, 2019.
- Supervising Summer Research Project Funded by the NCSC, National Cyber Security Centre UK, Edward Barrett, University of York, with R. Wilson, 2020.
- Supervising 6 Masters and Undergraduate Thesis Projects, University of York, UK (2020)
- Supervising research project of 30 undergraduate students at the City University of New York (2006–2016).
- External Evaluator, Department of Mathematics and Computer Science, York College, The City University of New York, October 2019.

Collaborators and Co-Editors: B. August (CUNY, USA), M. Anshel (City College of New York, CUNY, USA), Y. Antolin (Madrid, Spain). G. Arzhantseva (University of Vienna, Austria), L. Barthelemy (Paris, France), K. Bencsath (Manhattan College, USA), K. Bhutani(Catholic University of America, USA), JF Biasse (University of South Florida, USA), A. Broadbent (University of Ottawa, Canada), P. Brown (CUNY, USA), B. Cavallo (Facebook New York, USA), I. Chatterji (University of Nice, France), P. de la Harpe (University of Geneva, Switzerland), M. Dumontier,(University of Maastricht, Netherlands), J. Delgado (University of Basque Country, Spain), A. Douglas (CUNY Graduate Center,

USA), G. Di Crescenzo (Applied Communication Sciences and New York University, USA), B. Eick (Technische Universitat Braunschweig, Germany), K. Falconer (University of St Andrews, Scotland), J.-C. Faugere (INRIA, LIP6, University of Sorbonne, Pierre et Marie Curie, France), B. Fine (Fairfield University, USA), R. Flores (University of Seville, Spain), D. Garber (Holon University, Israel), M.I.Gonzalez Vasco(Madrid, Spain), J. Gryak (university of Michigan, Ann Arbor, USA), V. Gitman (CUNY Graduate Center, USA), M. Habeeb (California University in Pennsylvania, USA), R. Haralick (CUNY Graduate Center, USA), A. Gribov (Symbiont.io, USA), M. Kaplan (VeriQloud Company, France), B. Khan (University of Nebraska, Lincoln, USA), E. Kashefi (CNRS, Quantum Information Lab, LIP6, University of Pierre et Marie Curie, Paris, France and University of Edinburgh, Scotland), M. Khodjaeva (CUNY, GC), T. Koberda (University of Virginia), D. Kolovos(University of York, UK), C. Koupparis (Royal Bank of Canada in New York), H.T. Lam (Oblong Security Company, LA), N. Y. Lu (CUNY GC), S. Majewicz (CUNY, USA), K. Mallahi (Jacobs University of Bremen, Germany), C. Martinez-Perez (University of Zaragoza, Spain), N. Memarsadeghi (NASA, USA), N. Memon (New York University, USA), S. Molaye (Harvard University), A. Mostashari (LifeNome, Inc., USA), K. Najarian (University of Michigan, Ann Arbor), M. Nevins (University of Ottawa, Canada), ML Noce (University of Bath, UK), L. Perret (LIP6, University of Sorbonne, France), G. Renault (University of Sorbonne, France), J. Repka (University of Toronto, Canada), G. Rosenberger (Hamburg University, Germany), H. Salmasian (University of Ottawa, Canada), D. Savchuk (University of South Florida, USA), S.Shahandashti (University of York, UK), V. Shpilrain (City College of New York, USA), R. Soroushmehr (University of Michigan, Ann Arbor, USA), M. Stanojkovski (Max Planck Institute, Germany), Z. Sunic (Texas A&M University, USA), S. Sze (CUNY Graduate Center, USA), A. Tortora (University of Salerno, Italy), M. Tota (University of Salerno), E. Ventura (University of Politecnica Catalunya), Alexander Wood (University of Michigan, Ann Arbor, USA).

Invited Conference Talks

(298) Invited Speaker, Workshop 2: Emerging topics in design and cryptanalysis of post-quantum schemes, Institut Henri Poincare, Paris, France, November 4–8, 2024

(297) Invited speaker, Introductory summer school for Post-quantum Algebraic Cryptography, Institut d'Etudes Scientifiques, Cargese (Corsica), France, September 9–13, 2024.

(296) Invited Workshop Speaker, Friends of Institut des Hautes Etudes Scientifiques, IHES, September 2024.

(295) (Canceled due conflicting Schedule) Invited Speaker, 9th European Congress of Mathematics, Groups and Applications to Cryptography Special Session, Seville, July 19, 2024.

(294) Plenary Speaker and Group Leader, Swiss-VT: Coding Theory and Cryptography Summer School and Collaboration Workshop at the Virginia Tech Steger Center, Riva San Vitale, Switzerland, July 1–5, 2024.

(293) Plenary Speaker, Ischia Group Theory Conference, Italy, April 8–13, 2024

(292) Invited Speaker, American Mathematical Society, Spring 2024 AMS Eastern Sectional Meeting, special session on Post-Quantum Cryptography, Washington DC, April 6–7, 2024

(291) Invited Speaker, Internet Policy and Politics Conference, Policy Studies Organization (PSO), University of Oxford, UK, January 27, 2024.

(290) (Cancelled due to conflicting another conference at Oxford Invited Speaker), Conference on connections between group theory, logic, and computer science, Stevens Institute of Technology, June 12–14, 2024.

(289) Invited Speaker, Cryptography conference CIFRIS23 De Componendis Cifris Association, Special Session, New Trends in Group-based Cryptography, December 14–15 Dec 2023, Rome, Italy.

(288) (Declined due to conflicting talk) Plenary Speaker, Fairfield Algebra Regional Meeting (FARM), December 2, 2023.

(287) Invited Speaker, 1 hour talk, The AWM 2023 Research Symposium (Association for Women in Mathematics), Quantum Algorithms Special Session, Atlanta, September 30 –October 2, 2023

(286) Invited Speaker, Conference in Applied Algebra in Data Science, Osnabruck, Germany, September 7, 2023.

(285) Invited Career Panelist, Conference in Applied Algebra in Data Science, Osnabruck, Germany, September 7, 2023.

(284) Invited Speaker, Geometric and Asymptotic Group Theory with Applications (GAGTA) 2023: Groups and Dynamics, Erwin Schrodinger International Institute for Mathematics and Physics, Vienna, Austria, July 17-21, 2023

(283) Invited Speaker, 7th Biennial International Group Theory Conference, South Africa, NWU (Potchefstroom Campus), 7–11 August 2023.

(282) Invited Speaker, The Canadian Mathematical Society, Special Session on Theory and Applications of Finite Fields, Ottawa, Canada, June 4–5, 2023.

(281) Invited speaker, American Mathematical Society, Spring Eastern Sectional Meeting, Special Session Cybersecurity and Cryptography, virtually April 1–3, 2023

(280) Invited Speaker, Internet Policy and Politics Conference, Policy Studies Organization (PSO), University of Oxford, UK, January 21, 2023.

(279) Featured speaker, CUNY Graduate Center, Women in Mathematics Seminar, Association for Women in Mathematics Chapter, November 11, 2022.

(278) Plenary Speaker, 4th BYMAT Conference, Bringing Young Mathematicians Together, on Mathematics and Gender, Workshop on How to rise and thrive in your career as a successful mathematician belonging to an underrepresented (visible/invisible) minority group? Universitat Politécnica de Valencia, Spain, November 9–11, 2022.

(277) Plenary speaker, ENYGMMa, Women in Mathematics Conference, SUNY Stony Brook, October 7, 2022.

(276) Invited Chair, Public Sector Cyber Security and Data Protection Conference, UK Government Event, London , UK, September 20, 2022.

(275) Plenary Speaker, 2022 European Women in Mathematics Meeting, Special Session on Groups from Theory to computation and applications, University of Aalto, Finland, August 22–26, 2022.

(274) Invited speaker, 2022 Combinatorics, Computing, Group Theory and Applications in South Florida, Boca Raton, Florida, August 17–21, 2022.

(273) Invited Plenary Speaker, Young Cryptographers Summer Camp at Florida Atlantic University, July 25–29, 2022.

(272) Plenary Speaker (4 hours), Contemporary algebraic and geometric techniques in coding theory and cryptography, Universita degli Studi della Campania Luigi Vanvitelli Italy, (online) July 18–22, 2022.

(271) Speaker, AMS-SMF-EMS Joint International Meeting, American Mathematical Society-Société mathématique de France, European Mathematical Society, Special Session on Group theory, Algorithms and Applications, July 18-20, 2022,

(270) Speaker, Coding theory and cryptography, conference, A conference in honour of Joachim Rosenthal's 60th birthday, July 11–15, 2022, Zurich, Switzerland

(269) Invited Speaker, International Congress of Mathematicians 2022, ICM Satellite Conference, Mathematical Aspects of Post-quantum Cryptography, 2022 (postponed)

(268) Plenary Speaker, Ischia Group Theory Conference, Italy, June 20–25, 2022.

(267) Speaker, Association for Women in Mathematics Research Symposium, University of Minnesota, June 16–19, 2022.

(266) Invited International Conference Speaker, DLT 2022: 24th International Conference on Developments in Language Theory, University of South Florida, May 9–13, 2022.

(265) Panelist, Quantum Sciences and Post-quantum Cryptography Workshop, Panel on Future of Quantum Information, CUNY Graduate Center, May 16, 2022.

(264) Chair Panelist, Defence and Intelligence Research Forum, The Future of Defence-Related Research Grants Programs, CUNY Advanced Science Research Center, May 6, 2022,

(263) Panelist, Women in STEM Career Panel, CUNY Guttman CC, March 30, 2023.

(262) Invited Speaker, Applied Algebra connections to AI, Quantum Communication and Cyber Security, Applied Mathematics Program at CUNY, CUNY Research Foundation, April 8, 2022.

(261) Invited speaker, American Mathematical Society Spring Eastern, Tufts University, Special Session on Mathematics in Security and Defense, March 19–20, 2022.

(260) The featured speaker at IHES voices of Women in Mathematics for the United Nations as the International Day of Women and Girls in Science Institut des Hautes Etudes Scientifiques, `https://friendsofihes.ihes.fr/index.php/2022/02/11/voices-of-women-at-ihes-delaram-kahrobaei/`, February 11, 2022.

(259) Panelist Leadership panel, CUNY Women in STEM Network, December 9, 2021.

(258) Featured Woman in Fundamental Research at IHES among top 6 women mathematicians, `https://www.ihes.fr/en/givingtuesday2021-2/`, 2021.

(257) Keynote Speaker, New York City College of Technology, Research Day, November 29, 2021.

(256) Plenary Speaker, The International Conference on Security & Privacy (ICSP 2021), India, online, November 16–17, 2021.

(255) Invited guess lecturer, Entrepreneurship and Innovation for CUNY STEM students, October 21, 2021.

(254) Invited Speaker, CUNY Postdoctoral Association Town Hall, September 22, 2021.

(253) Featured Speaker at Al Jazeera News Channel, Can bitcoin be Trusted, `https://www.aljazeera.com/program/inside-story/2021/6/8/can-bitcoin-be-trusted`, June 8, 2021.

(252) Invited Speaker, Pro-finite Groups and Application, London Mathematical Society, June 2, 2021.

(251) International Invited Speaker, Max Planck Institute, Workshop on Applied Algebra in Data Science, Leipzig, Germany, September 17–19, 2022. (Cancelled due Covid)

(250) Plenary Speaker, Ischia Group Theory Conference, Italy, March 26, 2021.

(249) Keynote Speaker, 3rd Women in Research Conference, University of York, March 10, 2021.

(248) Invited International Speaker, The American Mathematical Society, Mathematics in Security and Defence, January 6–9, 2021, Washington DC, USA.

(247) (Cancelled Due Covid) Invited International Speaker, Tbilisi WAMS School On Algebra And Cryptography, The University of Georgia, Tbilisi, Georgia, June 22–June 30, 2021.

(246) Keynote speaker, IEEE International Workshop on Information Forensics and Security, New York University, USA, December 6-11, 2020.

(245) Data Markets: Remedying Internet Business Models or Creating New Beasts?, York-Maastricht University Workshop, December 4, 2020.

(244) Keynote speaker, Royal Air Force, Signal Unit 90 event, Yorkshire, UK, December 5, 2019.

(243) Invited Speaker, The London Mathematical Society, Computer Science Colloquium, Annual Theme: Mathematics of Security, De Morgan House, London, UK, November 13, 2019

(242) Invited International speaker, Board on Mathematical Sciences and Analytics (BMSA) within the National Academies of Sciences, Engineering, and Medicine, Mathematical Frontiers, Quantum Encryption, November 12, 2019.

(241) Keynote Conference Speaker, Women in Mathematics: Opportunities for the future Conference at University of Bristol, November 5, 2019.

(240) Invited International Conference Talk (1 hour talk), The American Mathematical Society, Special Session on What's New in Group Theory, University of Binghamton, October 12–13, 2019.

(239) Invited Speaker, Royal Society of Statistics, Statistics in Cyber Security, London, October 3, 2019.

(238) Invited International Speaker, Conference on Semigroups and Groups, Automata, Logics (SandGAL19), Politecnico di Milano, Italy, June 10–13, 2019

(237) Invited Panel member, Cyber Security in the Public Sector: An exchange of ideas, Joint event New States Man Newspaper (UK) and Cisco, Chatham House, London, May 30.

(236) Invited Speaker, Applied Algebra and Geometry Research Network, UK, May 30, 2019

(235) Invited Panel Member, Internet of Things and the ever changing privacy landscape, Persian Women in Tech Event, Reed Smith LLP in London, May 22, 2019.

(234) Invited Round Table Attendee: Tech: Comparison & Cooperation between the US & UK, Joint event Parliamentary Internet, Communications and Technology Forum (London) in partnership with Global Women's Innovation Network (DC), At the House of Commons, UK Parliament, Westminster Hall, London, April 16, 2019.

(233) Invited International Conference Talk, The American Mathematical Society, Special Session on Mathematical Cryptology, University of Connecticut Hartford, April 13-14, 2019. (Cancelled due to conflict of Schedule with interview panel at York)

(232) Invited International Conference Speaker, Groups, Automata, Graphs, Technische Universitat Graz, Austria, February 12–13, 2019.

(231) Invited International Conference Talk, Asia-Australia Algebra Conference, Sydney, Australia, January 21–25, 2019. (Cancelled due to conflict of Schedule)

(230) Invited International Conference Talk, Geometry, Analysis and Groups, Euler International Mathematical Institute (EIMI), Saint Petersburg, Russia, October 1–5, 2018.

(229) Invited Conference Talk, Elementary Theory of Groups and Group Rings and Related Topics, 70th Birthday of Benjamin Fine and Memory of Gilbert Baumslag, New York, November 1–2, 2018. (Cancelled due to Conflicting Schedule moving to New job at UK)

(228) National Conference Talk, The American Mathematical Society, University of Michigan, Ann Arbor, Special Session on Interactions between Algebra, Machine Learning and Data Privacy, October 2018.

(227) Conference Talk, Second Symposium on Business Analytics, The Paul H. Chook Department of Information Systems and Statistics, Baruch College, City University of New York, October 12, 2018.

(226) International Conference Talk, ICMS 18, Post-quantum Group-based Cryptography Session, University of Notre Dame, July 24–27, 2018.

(225) National Talk, American Mathematical Society, Special Session on Algorithmic Group Theory and Applications, April 21–22, 2018, Northeastern University, Boston.

(224) Invited Talk, Defense and Intelligence Research Forum, at the Research Foundation of the City University of New York, April 20, 2018.

(223) Invited International Conference Talk, The workshop on Mealy machines, automaton (semi)groups, decision problems and random generation, University Paris Diderot, July 12, 2017.

(222) Invited International Conference Talk, 13th Computability in Europe, CiE 2017, Special Session in Cryptography and Information Theory, Turku, Finland, June 12, 2017.

(221) Invited Sectional Conference Talk, American Mathematical Society, Hunter College, CUNY, Special Session on Cryptography, May 6–7, 2017.

(220) Invited International Conference Talk, XXI Coloquio Latinoamericano de Algebra, Buenos Aires, Argentina, July 25–29. 2016.

(219) Invited plenary lecture at the CiE conference (Computability in Europe 2016), The University Paris 7, June 27 – July 1, 2016.

(218) Invited Plenary Lecture at the CiE 2016-Women in Computability Workshop, The University of Paris 7, June 28 2016.

(217) Invited International conference Talk, Cybersecurity Workshop, Sponsored by ICERM, University of Wisconsin Madison, June 15–17, 2016.

(216) Conference Talk, GAGTA, Stevens Institute of Technology, NJ, June 13–17, 2016.

(215) Conference Talk, Zassenhaus Group Theory Conference, Adelphi University, Long Island, New York, June 10–12, 2016.

(214) Conference Talk, Applied Algebra Day Conference, University of Wisconsin Madison, April 29–May 1, 2016.

(213) Invited conference lecture, Institut Henri Poincare, Nexus of Information and Computation Theories, Paris, France, March 2016.

(212) National Conference Talk, Geometric and Probabilistic Methods in Group Theory and Dynamical Systems, Texas A&M University, College Station, November 9–12, 2015.

(211) Invited International Conference Talk, The German Mathematical Society (Deutsche Mathematiker Vereinigung, DMV), Mini-symposia on Algebraic Aspects of Cryptology, September 21–25, 2015.

(210) International Conference Talk, GAGTA, CIRM (Centre International de Rencontres Mathematiques), Luminy, Marseilles, France, September 14–18, 2015.

(209) Invited International Conference Talk, American, European, and Portuguese Mathematical Societies Meeting, Special Session on Algebra and Computer Science, Porto, Portugal, June 10–13, 2015

(208) National Conference Talk 2015 Zassenhaus Group Theory Conference, Binghamton University, May 22–24, 2015

(207) Invited plenary Talk, Group Theory Conference on the honor of Gerhard Rosenberger, Fairfield University, April 23-24, 2015

(206) Invited National Conference Talk, American Mathematical Society Joint Meeting, Special Session on What's New in Group Theory, San Antonio, TX, January 13, 2015.

(205) Invited National Conference Talk, Special Session on Groups, Algorithms, Cryptography at the 2015 Joint Mathematics Meetings in San Antonio, TX, January 10, 2015

(204) Invited International Conference Talk, Spanish Group Theory Conference, Seville, Spain, October 23-25, 2014.

(203) International Conference Talk, GAP Days 2014 (Groups Algorithm Programming), RWTH Aachen University, Germany, August 26, 2014. Conjugacy Problem in Polycyclic Groups in GAP.

(202) Invited workshop speaker, DIMACS Workshop on Multicore and Cryptography, Center for Discrete Mathematics and Theoretical Computer Science, Stevens Institute of Technology, NJ, July 21–23, 2014.

(201) Invited International Conference Talk, Geometric and Asymptotic Group Theory and Applications Conference, Newcastle, Australia, July 21–25 2014. (cancelled due conflicting schedule)

(200) Invited International Conference Talk, Workshop on New Directions in Cryptography, Satellite workshop of 9th Computer Science in Russia, Moscow, Russia, June 6–12, 2014.

(199) Invited International Conference Talk, The Second Joint Meeting American Mathematical Society with the Israel Mathematical Union Meeting, Special Session in Applications of Algebra in Cryptography, Tel-Aviv University, Israel (June 16–19, 2014)

(198) Invited International Conference Talk, The 11th KAIST Geometric Topology Fair, Korea Advance Institute of Science and Technology, Jeonju, South Korea, August 12–17, 2013

(197) Invited International Conference Talk, Eighth Barcelona Weekend in Group Theory Conference, Universitat Politecnica de Catalunya and CRM-Centre de Recerca Matematica, Barcelona, April 26–27 2013

(196) Invited International Conference Talk Geometric and Asymptotic Group Theory and Applications Conference, Dusseldorf University, Germany, July 26 – August 4, 2012.

(195) Invited International Conference Talk, Canadian Mathematical Society Meeting, Special Session in Groups and Algorithms, Ottawa, Canada, December 6–9, 2013.

(194) Invited International Conference Talk Workshop on post-quantum cryptography in St. Petersburg, Russia, Russian Academy of Science, Steklov Institute, June 12–13, 2011.

(193) Invited Conference Talk National Joint American Mathematical Society 2013 meeting, AMS Special Session on Algorithmic Problems of Group Theory and Their Complexity, San Diego, January 9, 2013.

(192) Invited Conference Talk, American Mathematical Society Eastern meeting, AMS Special Session on Algorithmic Problems of Group Theory and Applications in Cryptography, April 6–7, 2013, Boston College, MA

(191) Invited International Conference Talk Geometric and Asymptotic Group Theory and Applications Conference, City College of New York and CUNY Graduate Center, New York, May 28–31, 2013.

(190) Combinatorial and Additive Number Theory (CANT 2013) Conference, CUNY Graduate Center, New York, May 21–24, 2013, Searching for a secure platform for cryptology: Number Theoretic Problems vs Group Theoretic Problems

(189) Invited Conference panel member, Association for Women in Mathematics-Society for Industrial and Applied Mathematics-Computational Mathematics and Engineering, Boston, February 25–March 1, 2013

(188) Invited Panel Member, CUNY Central, Inspiring Women in Science Conference Series, Women and Entrepreneurship, April 29, 2014.

(187) Invited Panel Member, Princeton University, Work-Life Balance for Women in Mathematics, May 17, 2013

(186) Invited Panel Member, Science Online Teen, New York, April 13, 2013 (cancelled due to illness)

(185) Invited Conference Talk Keynote speaker, The Women in Science and Mathematics Conference in Pennsylvania, April 8, 2014, cancelled due to conflicting schedule.

(184) Invited Panel Member, Association for Women in Mathematics, Joint National Mathematics Meeting, American Mathematics Society Meeting, Building a Research Career in Mathematics, January 15, 2014

(183) Invited Conference Talk Group Theory, Combinatorics, and Computing conference, Florida Atlantic University, Boca Raton, Florida, October 3–8, 2012.

(182) Invited Conference Talk The 31st Ohio State-Denison Mathematics Conference, Ohio State University, Columbus, May 25, 2012.

(181) Invited Conference Talk Infinite Possibilities Conference for Women in Mathematics, University of Maryland, Baltimore, Invited Panel Member on Writing successful grant strategies, March 31, 2012

(180) Invited Conference Talk Infinite Possibilities Conference for Women in Mathematics, University of Maryland, Baltimore, Invited Panel Member on Rising and Thriving in your current profession, March 30, 2012

(179) Invited Conference Talk Zassenhaus Group Theory Conference, Towson University, Baltimore, May 27, 2011

(178) Invited Conference Talk American Mathematical Society Conference, University of Utah, Salt Lake City, Special session on Geometric, Combinatorial, and Computational Group Theory, October 22–23, 2011.

(177) Invited Conference Talk American Mathematical Society Meeting, University of Nebraska-Lincoln, Special Session on Algorithmic and Geometric Properties of Groups and Semigroups, October 14–16, 2011.

(176) Invited Conference Talk AWM Anniversary Conference at ICERM: "40 Years and Counting: AWM's Celebration of Women in Mathematics" Brown University, September 17–18, 2011.

(175) Invited Conference Talk International conference Approaches to Group Theory, Cornell University, October 9–11, 2010.

(174) International workshop on Complexity and Group Based Cryptography, The Centre de Recherches Mathamatiques (CRM) (Montreal, Canada) September 2nd, 2010.

(173) Invited Conference Talk Combinatorics, Groups, Algorithms, and Complexity Conference in honor of Babai's 60th birthday (Ohio State University, Columbus, Ohio)(March 20, 2010)

(172) Invited Conference Talk Manhattan Group Theory Day, CUNY Graduate Center, December 4th 2009

(171) Invited Conference Talk National American Mathematical Society-MAA Joint Mathematics Meetings in Washington DC, Special session on Generic Case Complexity and Algebraic Cryptography, A new Gateway for Group-based Cryptography, January 7 2009

(170) Invited Conference Talk International Conference on Geometric and Combinatorial Methods in Group Theory and Semi-Group Theory (John Meakin 60th Birthday) (Nebraska), May 2009.

(169) Invited Conference Talk Geometric and Asymptotic Group Theory with Applications Conference, Stevens Institute of Technology, NJ, March 12 2009.

(168) Invited Conference Talk Zassenhaus Group Theory Conference, Pennsylvania, May 29–31, 2009.

(167) Invited Conference Talk American Mathematical Society meeting, Stevens Institute of Technology, NJ, Non-commutative key exchange problems, April 15, 2007

(166) Invited Conference Talk Geometric Group Theory Conference on the Gulf, Pensacola Beach, Florida, Prosoluble Completion of a Group, March 23, 2008

(165) Invited Conference Talk Tensor Scholar Conference for Women in Mathematics, York College, City University of New York, March 12, 2011

(164) International Conference Talk Third Annual Meeting of the Prairie Network for Research in Mathematical Sciences, University of Saskatchewan, Canada, April 2009.

(163) Conference Talk American Mathematical Society-MAA Joint Mathematics Meetings in Washington DC, Contributed Talks in Group Theory special session, Residual Solvability of One-relator groups, January 8, 2009

(162) International Conference Talk Group St Andrews International Conference, University of St Andrews, Scotland, August 3–11, 2013

(161) International Conference Talk Group St Andrews International Conference, Bath University, England, UK, August 2, 2009.

(160) International Conference Talk Second International Conference on Symbolic Computation and Cryptography, Royal Holloway, University of London, UK June 23–25, 2010.

(159) Invited International Conference Talk First Meeting of the Spanish Mathematical Society, Special session on Theory of Groups and Representations, Valencia, Spain, January 31, 2005

(158) International Conference Talk British Mathematics Colloquium 2005, Number Theory Splinter, Liverpool, England, UK, April 5 2005

(157) International Conference Talk British Mathematics Colloquium 2005, Liverpool, England, UK, April 6, 2005.

(156) International Conference poster Presentation Isaac Newton Institute for Mathematical Sciences, Workshop on Model Theory, Algebraic and Analytical, Geometry, Cambridge, UK (July 10–16 2005)

(155) Conference presentation, MSRI Geometric Group Theory: Connection for Women, Mathematical Sciences Research Institute, Berkeley, CA USA, August 23–24, 2007 (presented a poster)

(154) Conference Talk Albany Group Theory Conference, SUNY, State University of New York, October 18, 2003.

Invited Seminar and Colloquium Talks (International and National)

(153) Invited Seminar Speaker, Mathematics Colloquium, University of Pittsburgh, March 14, 2025

(152) Invited Seminar Speaker, Italian Cryptography and Codes Group Seminar, October 2024.

(151) Invited Colloquium Speaker, Oxford Mathematics Colloquium, Oxford University, June 14, 2024

(150) Invited Colloquium Speaker, UCL University College London, Department of Computer Science, June 13, 2024

(149) Invited Seminar Talk organized by IHES, Qube Research and Technologies, Paris, France, June 2024.

(148) Invited Speaker, CUNY Research Scholars Program Tech Fellows AI Lecture series, CUNY Central Office of Research, March 15, 2024

(147) Invited Seminar Speaker, ACCESS: Algebraic Coding and Cryptography Seminar Series, February 20, 2024

(146) Invited Speaker, Florida Atlantic University, February 16, 2024.

(145) Invited Colloquium Speaker, Pure Mathematics, University of Southampton, UK, January 26, 2024.

(144) Invited Speaker, University of Bristol, UK, January 25, 2024.

(143) Invited panelist, Generative AI, Queens College CUNY, November 13, December 4, 2023.

(142) Invited Speaker, New York: UK-US Quantum Collaboration Meeting, British General Consulate, November 17, 2023

(141) Invited speaker, Telecom Paris, Cryptography Seminar, France, September 14, 2023.

(140) Invited Speaker, Mathematics Colloquium, University of South Florida, June 16, 2023.

(139) Invited Speaker, University of Salerno, Italy, July 2023.

(138) Invited Speaker, Queens College Computer Science Colloquium, May 3, 2023.

(137) Invited Speaker, Princeton University, Discrete Mathematics Seminar, Mathematics Department, February 23, 2023

(136) Invited Speaker at École Normale Supérieure Group Theory Monthly Seminar, Ulm Paris, France, January 10, 2023

(135) Invited Speaker, Biomedical Engineering Colloquium, NYU, New York University, Tandon School of Engineering, September 2023.

(134) Featured speaker, CUNY Graduate Center, Women in Mathematics Seminar, Association for Women in Mathematics Chapter, November 10, 2022

(133) Invited guest lecturer, Post-quantum Cryptography, University of Seville, Spain, October 28, 2022.

(132) Invited Speaker, New York Group Theory Seminar, April 29, 2022.

(131) Panelist for Research Experience for Undergraduates, University of Virginia, June 2021, June 2022.

(130) Invited panel speaker, Critical Infrastructure/Cyber-Physical, The City College of New York, CUNY, March 3, 2022.

(129) Invited Guest Lecturer, University of Manchester, Digital Futures Trust, UK, May 6, 2020.

(128) Invited International Seminar Talk, University of Zurich-Neuchatel, Applied Algebra and Cryptography Seminar, Zurich, Switzerland, April 22, 2020.

(127) Invited Colloquium Talk, Universidad Rey Juan Carlos Campus de Mostoles (Madrid), Spain, February 25, 2020.

(126) Invited Seminar Talk, University of York, Computer Science Seminar, UK, February 12, 2020.

(125) Invited Seminar Talk, University of York, QUFIT Seminar, UK Quantum Technologies Hub for Quantum Communications, York, UK, February 4, 2020.

(124) Invited Seminar Talk, University of Harriott Watt, Scotland, UK, January 29, 2020.

(123) Invited Colloquium Talk, University of St Andrews, UK, January 28, 2020.

(122) Invited Seminar Talk, University of Almeria, Spain, December 11, 2019.

(121) Invited Colloquium Talk, University of Aberdeen, Scotland, UK, November 20, 2019.

(120) Invited Seminar Talk, University of Durham, UK, November 19, 2019.

(119) Invited Colloquium Talk, University of Bristol, UK, November 4, 2019.

(118) Invited Lecture, Yerevan State University, Armenia, September 17, 2019.

(117) Invited Seminar Speaker, University of Ottawa, Canada, August 5, 2019.

(116) Invited lecture, Lazard Financial Firm, New York, July 1, 2019.

(115) Invited Seminar Talk, University of Kent, UK, March 29, 2019.

(114) Invited Seminar Talk, Group Theory Seminar, Universidad Autonoma de Madrid, Spain, March 19, 2019.

(113) Invited lecturer, Mini-course in Group-based Cryptography II (2 hours), Universidad Autonoma de Madrid, Spain, March 20, 2019.

(112) Invited lecturer, Mini-course in Group-based Cryptography I (2 hours), Universidad Autonoma de Madrid, Spain, March 18, 2019.

(111) Invited Colloquium Talk, Jacobs University, Bremen, Germany, February 14, 2019.

(110) Invited Seminar Talk, University of York, Semigroup Seminar, UK, February 6, 2019.

(109) Invited Seminar Talk, University of Newcastle, UK, January 29, 2019.

(108) Invited Seminar Talk, University of Royal Holloway, UK, January 24, 2019.

(107) Invited International Colloquium Talk, University of Ottawa, Mathematics Colloquium, October 12, 2018.

(106) Invited International Mini-course: Post-quantum Group-based Cryptography I (2 hours), University of Nice, France, August 27, 2018.

(105) Invited International Mini-course: Post-quantum Group-based Cryptography II (2 hours), University of Nice, France, August 28, 2018.

(104) Invited International Seminar Talk, idalab GmbH Seminar, Berlin, Germany, July 13, 2018.

(103) Invited International Mini-course (1.5 hour), Group-based Cryptography, University di Napoli Federico II, Italy, 2018.

(102) Invited International Mini-course (4 hours), Group-based Cryptography, University of Salerno, Italy, 2018.

(101) Invited International Seminar Talk, Politecnico of Milano, Italy, March 8, 2018.

(100) Invited International Distinguished lecture, Computational Foundry series, Swansea University, Wales, March 5, 2018.

(99) Invited International Seminar talk at Information Security and Privacy research group at University of McMaster, Ontario, Canada, February 12, 2018.

(98) Invited International Colloquium Talk, Tutte Colloquium, Optimization and Combinatorics Department, University of Waterloo, Canada, February 9, 2018

(97) Invited International Seminar Talk, Ecole Politechnique University, Paris, January 22, 2018.

(96) Invited International Seminar Talk, University of Porto, Portugal, January 8, 2018.

(95) Invited International Seminar Talk, University of Politectica Catalunia, Barcelona, November 17. 2017.

(94) Invited Colloquium Talk, Helen Barton Lecture Series in Computational Mathematics, University of North Carolina Greensboro, October 20, 2017.

(93) Invited Seminar Talk, spamhaus, Courant Institute, New York University, September 13, 2017.

(92) Invited International Seminar Talk, Sorbonne University, PolSys, LIP6, Paris, France, July 13, 2017.

(91) Invited Colloquium Talk, NASA: National Aeronautics and Space Administration, The Goddard Information Science and Technology Colloquium Series, May 17, 2017.

(90) Invited Seminar Talk, University of Salerno, Italy, May 29, 2017

(89) Invited Seminar Talk, Quantum and Post-quantum Computation Seminar, CUNY Graduate Center, Initiative for Theoretical Sciences, March 2017.

(88) Invited Seminar Talk, Joint Seminars: Distinguished Speakers - Oxford Women in Computer Science, Oxford University, Women in Computing Seminar, and OASIS: The Oxford Advanced Seminar on Informatic Structures, England, UK, October 11, 2016.

(87) Invited Seminar Talk, Colorado State University, Rocky Mountain Algebraic Combinatorics Seminar, Fort Collins, Colorado, September 16, 2016.

(86) Invited Seminar Talk, University of California, Irvine, Computer Science Department, April 15, 2016.

(85) Invited Colloquium Talk, Jacob University, Bremen, Germany, Mathematics Colloquium, March 7, 2016.

(84) Invited Seminar Talk, University of Seville, Spain, February 11, 2016.

(83) Invited Seminar Talk, University of Neuchatel, Switzerland, February 29, 2016.

(82) Invited Colloquium Talk, University of South Florida, Tampa, January 15, 2016.

(81) University of Michigan, Computational Medicine and Bioinformatics Department, Ann Arbor, January 8, 2016.

(80) University of Michigan, Computational Medicine and Bioinformatics Department, Ann Arbor, January 7 2016.

(79) University of Michigan, Computational Medicine and Bioinformatics Department, Ann Arbor, January 6, 2016.

(78) Invited Seminar Talk, Florida Atlantic University, January 12, 2016.

(77) Invited Seminar Talk, University of Nebraska in Lincoln, Semigroup, Groups and Topology Seminar, November 17, 2015.

(76) Seminar Talk, CUNY Graduate Center, Mathematical Aspect of Cryptography Student Seminar, November 3, 2015.

(75) Invited International Seminar Talk, University of Basque Country, Bilbao, Spain, Algebra Seminar, October 8, 2015.

(74) Invited International Seminar Talk, University of Zaragoza, Spain, Algebra Seminar, September 30, 2015.

(73) Invited Seminar Talk, University of Nice, France, Algebra and Topology Seminar, September 10, 2015.

(72) Invited Seminar Talk, Technical University of Eindhoven, Netherlands, Cryptography Seminar, September 2, 2015.

(71) Invited Panel member, How to Succeed in NSF I-Corps (Innovative Corporation), at CUNY Hub for Innovation and Entrepreneurship, June 15, 2015

(70) Invited International Talk, University NOVA in Lisbon, Algebra and Logic Seminar, June 8, 2015.

(69) Invited Seminar Talk, CRM-Centre de Recerca Matematica, Seminari de Teoria de Grups, Barcelona, May 26, 2015

(68) Invited Panel member, CUNY Hub for Innovation and Entrepreneurship (CUNY iHub), May 19, 2015

(67) Invited Seminar Talk, Topology and Geometric Group Theory Seminar, Cornell University, May 5, 2015.

(66) Invited Seminar Talk, The Bernstein Seminar, Cornell University, May 5, 2015.

(65) Invited Seminar Talk, Geometric Group Theory Seminar, Tufts University, February 24, 2015.

(64) Invited International Seminar Talk, University of Florence, Italy, January 23, 2015.

(63) Invited International Seminar Talk, University of Zaragoza, Spain, October 21, 2014.

(62) Invited International Seminar Talk, Universidad Autonoma de Madrid, Spain, October 17, 2014.

(61) Invited Seminar Talk, Center for Logic, Algebra, Computation, NYCCT, October 14, 2014.

(60) Invited Seminar Talk, Groups, Semigroups, Topology, University of Nebraska in Lincoln, October 3, 2014.

(59) Invited Seminar Talk, Applied Communication Science Company, NJ, September, 2014.

(58) Invited Seminar Talk, State University of New York, Binghamton University, Algebra Seminar, September 9, 2014.

(57) Invited Seminar Talk, CUNY Graduate Center, Algebra Cryptography Seminar, November 15, 2013.

(56) Invited Colloquium Speaker, Leipzig University, Computer Science Department, Germany, March 26, 2013

(55) Invited Colloquium Talk, CUNY Graduate Center, Computer Science Colloquium, November 29th, 2012

(54) Invited Seminar Talk, UC Berkeley, October 2013 (Cancelled due to Hurricane Sandy in New York)

(53) Invited Seminar Talk, Rutgers University New Brunswick, Algebra Seminar, September 4, 2013.

(52) Invited Colloquium Talk, Smith College, MA, September 12, 2013.

(51) Invited Seminar Talk, Columbia University, Theory of Computation Seminar, New York, February 8, 2013

(50) Invited Seminar Talk, CUNY Graduate Center, Algebra Cryptography seminar, April 20, 2012

(49) Invited Colloquium Talk, Rensselaer Polytechnic Institute (RPI), Computer Science Colloquium, December 6, 2012

(48) Invited International Seminar Talk, University Paris VII, Mathematics Institute, France, November 23, 2012

(47) Invited International Seminar Talk, Sorbonne University, Laboratoire d'informatique de Paris 6 (LIP6), PolSys Seminar, France, November 23, 2012

(46) Invited International Seminar Talk University d'Orleans, France, November 22, 2012

(45) Invited International Seminar Talk University of Toronto, GANITA seminar, Interdisciplinary seminar whose main focus is on geometry, algebra, number theory and applications, July 12, 2011.

(44) Invited Colloquium Talk Brooklyn College, Computer Science Colloquium, March 23, 2011

(43) Invited Seminar Talk, New York Algebra Colloquium, Graduate Center CUNY, September 16, 2011.

(42) Invited Seminar Talk University of Texas (Austin), Algebra, Number Theory, Combinatorics Seminar, March 2010.

(41) Invited International Colloquium Talk University du Quebec in Montreal Colloquium, Canada February 13, 2009

(40) Invited International Seminar Talk McGill University, Geometric Group Theory Seminar, Canada, February 11 2009.

(39) Invited Colloquium Talk Rutgers University, Mathematics Colloquium, New Brunswick, NJ, November 7 2008.

(38) Invited Seminar Talk Graduate Center CUNY, New York Group Theory Seminar (Magnus Seminar) October 17 2008

(37) Invited Seminar Talk Non-commutative Cryptography, an Introduction, CUNY Graduate Center, Mathematical Aspects of Cryptography Series of talks, February 1, 2008.

(36) Invited Seminar Talk Non-commutative protocols, CUNY Graduate Center, Mathematical Aspects of Cryptography Series of talks, February 8, 2008

(35) Invited Seminar Talk Complexity of Decision Problems in Polycyclic Groups (February 15, 2008), CUNY Graduate Center, Mathematical Aspects of Cryptography Series of talks

(34) Invited Seminar Talk On Unsolvability of Group Theoretic Decision Problems (February 29, 2008), CUNY Graduate Center, Mathematical Aspects of Cryptography Series of talks

(33) Invited Seminar Talk On solvability of Group Theoretic Decision Problems, CUNY Graduate Center, Mathematical Aspects of Cryptography Series of talks, March 7, 2008.

(32) Invited Colloquium Talk Bronx Community College Mathematics Colloquium (March 25, 2008)

(31) Invited Colloquium Talk NYCCT, City University of New York, Mathematics and Physics Colloquium, January 6, 2007

(30) Invited Colloquium Talk Medgar Evers College, Mathematics Colloquium, City University of New York, November 28, 2007

(29) Invited Seminar Talk CUNY Graduate Center Algebra and Cryptography Seminar, Graduate Center, City University of New York, NY, US, November 3 2006

(28) Invited International Seminar Talk Nottingham Pure Mathematics Colloquium, University of Nottingham, UK, March 3 2006

(27) Invited International Seminar Talk IPM Combinatorics Seminar, Institute for studies in Theoretical Physics and Mathematics, Iran, January 4 2006.

(26) Invited International Seminar Talk, KTH Algebra-och Geometti seminarier, The Royal Institute of Technology in Stockholm, Sweden, November 16 2005.

(25) Invited International Seminar Talk CRM Math Seminar, Centre de Recerca Matematica, Barcelona, February 3 2005.

(24) Invited International Seminar Talk Universite de Geneve Seminaires d'Algebre et de Geometrie Section de Mathematiques, Switzerland, January 14 2005.

(23) Invited International Colloquium Talk Ecole Polytechnique Federale de Lausanne IGAT Colloquium, Institute of Geometry, Algebra, Topology, Lausanne, Switzerland, January 134h 2005.

(22) Invited International Seminar Talk Universite de Geneve Seminaires d Algebre et de Geometrie, Section de Mathematiques, Switzerland, January 11, 2005.

(21) Invited International Seminar Talk IPM Mathematics Colloquium, Institute for studies in Theoretical Physics and Mathematics, Iran, Jan. 3 2005.

(20) Invited International Seminar Talk IPM Mathematics Colloquium, Institute for studies in Theoretical Physics and Mathematics, Iran, January 1, 2005.

(19) Invited International Seminar Talk St Andrews Analysis Seminar, Mathematical Institute, Scotland, UK, November 29 2005.

(18) Invited International Seminar Talk Oxford Topology Seminar, Oxford University, England, UK, October 24 2005.

(17) Invited International Colloquium Talk St Andrews Pure Mathematics Colloquium, Mathematical Institute, Scotland, UK, March 24, 2005.

(16) Invited International Seminar Talk Glasgow Algebra Seminar, University of Glasgow, Scotland, UK, February 16, 2005.

(15) Invited International Colloquium Talk Queens Belfast Mathematics Colloquium, Queen's University, Belfast, Ireland, UK, February 11 2005.

(14) Invited International Seminar Talk Edinburgh-Heriot-Watt Algebra Seminar, University of Edinburgh, Scotland, UK, February 8, 2005.

(13) Invited International Colloquium Talk IHES Mathematics Colloquium, Institute des Hautes Etudes Scientifiques, France, November 12, 2004.

(12) Invited International Seminar Talk Ecole Normale Superieure de Lyon, Unite de Mathematiques Pures et Appliquees, France, Informal Talk, November 14, 2004.

(11) Invited Seminar Talk New York Logic Workshop, Graduate Center CUNY, New York, NY, US, September 10, 2004.

(10) Invited Seminar Talk NYU Cryptography Seminar, Courant Institute of Mathematical Science, New York University, July 16, 2004.

(9) Invited Seminar Talk Rutgers Group Theory Seminar, Rutgers University, New Brunswick, NJ, USA, March 10th 2004, Residual Solvability of Generalized Free Products

(8) Invited International Seminar Talk Warwick Algebra Seminar, University of Warwick, Mathematics Institute, England, UK, November 18, 2004

(7) Invited International Seminar Talk IPM Mathematics Colloquium, Institute for studies in Theoretical Physics and Mathematics, Iran, December 29, 2004 Residual Solvability of Generalized Free Products

(6) Invited International Colloquium Talk Sharif Mathematics Colloquium, Sharif University of Technology, Tehran, Iran, December 22, 2004.

(5) Invited International Colloquium Talk St Andrews Pure Mathematics Colloquium, Mathematical Institute, Scotland, UK, October 10, 2004.

(4) Invited International Seminar Talk Undergraduate Analysis Seminar, University of St Andrews, Scotland, UK, May 3, 2005.

(3) Invited International Seminar Talk Polycyclic Groups and Cryptologic Applications Seminar, University of St Andrews, Scotland, December 15, 2004.

(2) Invited International Seminar Talk Polycyclic Groups and Cryptologic Applications Seminar, University of St Andrews, Scotland, November 4, 2004.

(1) Seminar Presentation, Mathematical Aspects of Cryptology Student Seminar, CUNY Graduate Center, November 9, 2012.

Conferences organization

(67) Program Leader, IHP Trimester *Post-quantum Algebraic Cryptography*, €200,000.00, (with Perret, Faugère, Shpilrain) September–December 2024.

(66) Co-organizer, IES, Cargese, *Summer School in Post-quantum Algebraic Cryptography*, September 6–10, 2024, Corsica, France

(65) Co-organizer, IHP, Institut Henri Poincare, *Deployment of Post-quantum Cryptography*, 7–11 October 2024, Paris, France.

(64) Co-organizer, IHP, Institut Henri Poincare, *Emerging topics in design and cryptanalysis of post-quantum schemes* , November 4–8, 2024, Paris, France.

(63) Co-organizer, IHP, Institut Henri Poincare, *Quantum technologies for Cryptography*, December 2–6, 2024, Paris, France.

(62) Program Committee, Cryptography conference CIFRIS24 De Componendis Cifris Association, September 2024, Rome, Italy.

(61) Co-organizer, Universita degli Studi di Palermo, Post-quantum Group-based Cryptography Special Session, at the 2nd Joint Meeting Unione Matematica Italiana (UMI) and the American Mathematical Society (AMS), July 23 – July 26, 2024

(60) Co-organizer, CiE 2024, The 20th Computability Conference, Special Session on Quantum Computation, University of Amsterdam, Netherlands, with M. Sadrzadeh, July 8–10, 2024.

(59) Co-organizer, AIM Workshop, American Institute of Mathematics, CalTech, CA, *Post-quantum Group-based Cryptography*, with L. Perret, April 29–May 4, 2024.

(58) Program Committee, Cryptography conference CIFRIS23 De Componendis Cifris Association, December 14–15 Dec 2023, Rome, Italy.

(57) Co-organizer, SIAM 1st Annual NY-NJ-PA, minisymposium Computational and Applied Group Theory, NJIT, October 20–21, 2023

(56) Program Committee, Computability in Europe July 2023.

(55) Faculty advisor of ENYGMMa (Empowering New York Gender Minority Mathematicians), Joint conferences in Columbia University, SUNY Stony Brook, CUNY Graduate Center, Organized for PhD students, October 7, November 4, 2022, February 10, 2023.

(54) Program Committee, The International Conference on Cryptology, Coding Theory and Cybersecurity (I4CS'22), 26–28 October 2022 , Casablanca, Morocco

(53) Scientific Committee, *2022 Combinatorics, Computing, Group Theory and Applications in South Florida*, Boca Raton, Florida, August 14–21, 2022.

(52) AMS-SMF-EMS Joint International Meeting, American Mathematical Society-Société mathématique de France, European Mathematical Society, Special Session on Group theory, Algorithms and Applications, July 18-20, 2022, with F. Dahmani, I. Chatterji, M. Deraux, University of Grenoble, France.

(51) Program Committee, The International Workshop on the Arithmetic of Finite Fields, WAIFI 2022, Chengdu, China. August 29–September 2, 2022.

(50) Program committee, The First International Conference on Cryptography, Codes, and Cyber Security (I4CS), University of Casablanca, Morocco, July 14–16, 2022.

(49) Co-organizer, Association for Women in Mathematics, AWM in Minneapolis, Minnesota for the 2022 Research Symposium, The Institute for Mathematics and its Applications, in partnership with the University of Minnesota, *Mathematics of Cryptography*, June 16 –19, 2022. with M. Khodjaeva.

(48) Co-organizer, Quantum Workshop, CUNY Graduate Center, with A. Alu, May 16, 2022

(47) Co-Organizer Machine Learning and Artificial Intelligence Workshop, CUNY Graduate Center, April 8, 2022

(46) Co-organizer of Defence and Intelligence Forum, May 6, 2022 (with J. Tsapogas, J. Brumberg).

(45) Co-organizer, CUNY Women in STEM Network, December 9, 2021, with A. Gray,.

(44) Programme Committee, 18th IMA conference on Cryptography and Coding, University of Oxford, UK, December 2021.

(43) 24th International Symposium on Mathematical Theory of Networks and Systems (MTNS 2020), Special Session on Mathematical Aspects of Coding and Cryptography, with S. Mesnager, 23–27 August 2021, University of Cambridge, UK.

(42) Scientific Committee, Tbilisi WAMS School On Algebra And Cryptography, The University of Georgia, Tbilisi, Georgia, June 22–June 30, 2022.

(41) York Workshop in Quantum Information, Complexity & Cryptography, with R. Colbeck, P. Farshim, R. Santhanam, T Spiller, 2022.

(40) Co-organizing Interdisciplinary Workshop on Aspects of Cyber Security, University of York, UK, June 20–21, 2019. (with S. Braunstein, S. Pirandola, S. F. Shahandashti, T. Spiller, V. Vasilakis)

(39) Program Committee, WAHC'18-6th Workshop on Encrypted Computing and Applied Homomorphic Cryptography, Toronto, Canada, October 2018.

(38) Co-organizer, American Mathematical Society, Special Session on Interactions between Algebra, Machine Learning, Data Privacy, October 20–21, 2018, University of Michigan, Ann Arbor (with J. Gryak, K. Horan, K. Najarian, R. Soroushmehr, A. Wood)

(37) Co-organizer, 6th International Congress on Mathematical Software, ICMS 2018, Notre Dame, Special Session on Post-quantum Group-based Cryptography, 24–27 July 2018 (with V. Shpilrain).

(36) Local Arrangement Committee, The 43rd International Symposium on Symbolic and Algebraic Computation (ISSAC), CUNY Graduate Center, July 16–19, 2018 (with A. Ovchinnikov, V. Pan).

(35) Co-organizer, American Mathematical Society, Special Session on Algorithmic Group Theory and Applications, April 21–22, 2018, Northeastern University, Boston (with A. Tortora)

(34) Co-organizer of MAD, Manhattan Algebra Day 9, CUNY G.C. (December 8th, 2017)
(with A. Miasnikov, O. Kharlampovich, V. Shpilrain, S. Ushakov)

(33) Co-organizer of Defence and Intelligence Forum, Research Foundation CUNY, April 2018 (with J. Tsapoga, J. Brumberg).

(32) Co-organizer, Mathematical Congress of the Americas 2017 (MCA2017), Montreal, Canada, Special Session on Computations in Groups and Applications, July 24 – 28, 2017 (with I. Bumagina)

(31) Co-organizer, Computability in Europe 2017, Special Session on Cryptography and Information Theory, Turko, Finland, June 12–16, 2017 (with H. Lipmaa)

(30) Co-organizer, New York Multidisciplinary Symposium on Security and Privacy, New York University, February 25, 2017, (with N. Memon, Q. Zhu).

(29) Co-organizer American Mathematical Society Eastern meeting, AMS Special Session on Infinite permutation groups, totally disconnected locally compact groups, and geometric group theory (May 6–7, 2017) (with S. Smith) Hunter College, CUNY, New York.

(28) Co-organizer of Manhattan Algebra Day 8, CUNY G.C. (December 9th 2016)
(with A. Miasnikov, O. Kharlampovich, V. Shpilrain, S. Ushakov)

(27) Co-organizer, American, European, and Portuguese Mathematical Societies Meeting, Special Session on Algebra and Computer Science, Porto, Portugal, June 10 –13, 2015 (with C. Carvalho)

(26) Co-organizer, Special Session on Groups, Algorithms, Cryptography at the 2015 Joint Mathematics Meetings in San Antonio, TX, January 10–13, 2015 (with B. Cavallo)

(25) Co-organizer, Association for Women in Mathematics Panel, Breaking the Glass Ceiling Permanently. at the 2015 Joint Mathematics Meeting in San Antonio, TX, January 10, 2015 (with C. Sormani, B. Anne Case, K. Leonard)

(24) Co-organizer, Panel Discussion, THE INTRINSIC VALUE PROJECT 1: A meeting at the crossroads - science, performance and the art of possibility, Part of undergroundzero festival, New York, July 9-10, 2014 (with H. Deyner)

(23) Co-organizer The Second Joint Meeting American Mathematical Society with the Israel Mathematical Union Meeting, Special Session in Applications of Algebra in Cryptography, Bar-Ilan University, Ramat-Gan and Tel-Aviv University, Tel Aviv, Israel (June 16-19, 2014) (with D. Garber)

(22) Co-organizer National Joint American Mathematical Society 2013 meeting, AMS Special Session on Algorithmic Problems of Group Theory and Their Complexity (January 9-12, 2013) (with V. Shpilrain) San Diego, CA

(21) Co-organizer American Mathematical Society Eastern meeting, AMS Special Session on Algorithmic Problems of Group Theory and Applications in Cryptography (April 6-7, 2013) (with V. Shpilrain) Boston College, MA

(20) Co-Organizer National Joint American Mathematical Society 2012 Meeting, Special Session on Groups, Algorithm, Complexity and Theory of Security (January 4-7, 2012) (with M. Habeeb) Boston, MA

(19) Co-organizer of AWM Anniversary Conference at ICERM: "40 Years and Counting: AWM's Celebration of Women in Mathematics" Brown University (September 17-18, 2011) Special Session in Geometric Group Theory with Moira Chas

(18) Co-Organizer of American Mathematical Society 2011 Fall Eastern Sectional Meeting, Special Session on Mathematical Aspects of Cryptography and Cyber Security (September 10-11, 2011) (with Ben Fine, Gerhard Rosenberger) at Cornell University, Ithaca

(17) Co-Organizer American Mathematical Society 2011 Spring Western Sectional Meeting, Special Session on Computer Algebra, Group and Applications (April 30-May1, 2011) (with Ben Fine and Gerhard Rosenberger) Las Vegas, USA

(16) Organizer of American Mathematical Society 2011 National Joint Meeting (New Orleans, January 6-9, 2011), Special Session on Groups, Geometry, Applications

(15) Organizer of American Mathematical Society Meeting, 2010 Eastern Spring Special Session, Groups, Computations, Applications, New Jersey Institute of Technology, Newark (May 2010)

(14) Co-organizer of Manhattan Group Theory Day I, CUNY G.C. (December 4th 2009)
(with G. Baumslag, A.Miasnikov, V.Shpilrain, S.Ushakov)

(13) Co-organizer of Manhattan Group Theory Day II, CUNY G.C. (December 3rd 2010)
(with G. Baumslag, A. Miasnikov, V. Shpilrain, S. Ushakov)

(12) Co-organizer of Manhattan Algebra Day III, CUNY G.C. (December 9th 2011)
(with G. Baumslag, O. Kharlampovich, A. Miasnikov, V. Shpilrain, S. Ushakov)

(11) Co-organizer of Manhattan Algebra Day IV, CUNY G.C. (December 7th 2012)
(with G. Baumslag, A. Miasnikov, O. Kharlampovich, V. Shpilrain, S. Ushakov)

(10) Co-organizer of Manhattan Algebra Day V, CUNY G.C. (December 6th 2013)
(with G. Baumslag, A. Miasnikov, O. Kharlampovich, V. Shpilrain, S. Ushakov)

(9) Co-organizer of Manhattan Algebra Day VI, CUNY G.C. (December 5th 2014)
(with G. Baumslag, A. Miasnikov, O. Kharlampovich, V. Shpilrain, S. Ushakov)

(8) Co-organizer of Manhattan Algebra Day VI, CUNY G.C. (December 4th 2015)
(with A. Miasnikov, O. Kharlampovich, V. Shpilrain, S. Ushakov)

(7) Co-Organizer of New York Women in Mathematics and Computing Network conference, May 10, 2013 at NYCCT (CUNY) Forward to Professorship II (with Provost P. Brown)

(6) Co-Organizer and Founder of New York Women in Mathematics and Computing Network conference, March 3, 2012 at NYCCT (CUNY) Forward to Professorship (with Associate Provost P. Brown)

(5) Co-Organizer and Founder of New York Women in Mathematics and Computing Network conference series, Leadership in Higher Education, April 27, 2012 at CUNY Graduate Center (with Associate Provost P. Brown)

(4) Co-Organizer of New York Women in Mathematics and Computing Network workshop, Communicating in a male dominated field, November 30, 2012 at New York City College of Technology (CUNY) (with Associate Provost Pamela Brown)

(3) Co-organizer and moderator of the panel session, The Training and Professional Development of Teaching Assistants 2013 Joint Mathematics Meetings, San Diego, CA

(2) Co-organizer and Co-founder of the New York Women in Mathematics Network, Conference at The City University of New York CUNY Graduate Center-December 9, 2006 (with Victoria Gitman)

(1) Co-organizer of the New York Women in Mathematics, Interdisciplinary Research in Group Theory, Logic and Theoretical Computer Science, NYCCT, CUNY, May 2 2008 (with V.Gitman)

Seminar and Colloquium organization

(9) Co-organizer and co-founder of the York Cyber Security Seminar, University of York (UK), with S. Shahandashti, `https://sites.google.com/york.ac.uk/cybersec/seminars` (2018-2020)

(8) Co-organizer of the Algebra-Cryptography Seminar, CUNY Graduate Center (Since Spring 2013) (with V.Shpilrain, A.Miasnikov, R.Gilman) `www.sci.ccny.cuny.edu/~shpil/algcryp.html`

(7) Co-founder and Co-organizer of Quantum and Post-quantum Computation Seminar, CUNY Graduate Center, Initiatives for Theoretical Sciences (Spring 2017) (with M. Hillery, V. Oganasyan) (A joint seminar: Computer Science, Mathematics, Physics Departments at CUNY)
`https://sites.google.com/view/gcpostquantumseminar/`

(6) Co-founder and Co-organizer of New York Applied Algebra Colloquium, CUNY Graduate Center (Fall 2008–2018) (with A.Douglas, S. Smith, B. Steinberg) `https://sites.google.com/site/nyalg2/`

(5) Organizer of the Mathematical Aspects of Cryptography Student Seminar at CUNY Graduate Center (partly with Michael Anshel 2009-2010) (2009–2018) `https://sites.google.com/site/gccryptostudents/`

(4) Leading and Lecturing Research Seminar in Combinatorial Group Theory and Cryptography, Interdisciplinary Seminar in Mathematics and Computer Science Department, CUNY Graduate Center (2008-2009)(with M. Anshel, K. Boklan)

(3) Co-founder and Co-organizer of Mathematics Seminar Series, NYCCT, CUNY, Brooklyn (September 2007–Spring 2015) (with Hans Schoutens)

(2) Co-founder and Co-organizer of C-LAC Seminars, City Tech (CUNY) (Fall 2008–Spring 2015) (with A.Douglas) `c-lac.org`

(1) Organizer of Polycyclic Groups and Cryptologic Applications Seminar, University of St Andrews (2004–2005).

Courses taught at the University of York in Computer Science Department

- Supervised 10 Masters and Undergraduate Thesis (2019–2021)
- MSc Module Lead, Privacy and Security (2021)
- MSc Module, Wider Aspects of Cyber Security (2021)

Courses taught at the CUNY Graduate Center, PhD Program in Mathematics

- PhD Thesis Supervision in Mathematics, CUNY Graduate Center (Fall 2010, Spring and Fall 2011, Spring and Fall 2012, Spring and Fall 2013, Spring 2014)
- Independent Studies with four PhD students in Mathematics, CUNY Graduate Center (Spring 2010, Spring 2011, Spring 2012)

Courses taught at the CUNY Graduate Center, PhD Program in Computer Science

- Algorithms for Big Data Analysis (Fall 2017)
- Algebraic Cryptography (Fall 2016)
- Cryptography and Network Security (Fall 2014)
- Mathematical Aspects of Algebraic Cryptography (Fall 2013)
- Combinatorial Group Theory and Cryptography (Spring 2013)
- Computational Group Theory and applications to Cryptography (Spring 2012)
- Aspects of Non-Abelian Group-Based Cryptography: A New Approach to Modern Cryptography (Spring 2011)
- Group Theory, Finite Fields and their applications in Computer Science (Spring 2009)
- PhD Thesis Supervision in Computer Science, CUNY Graduate Center (Fall 2014, Spring 2015, Spring 2016, Fall 2016, Spring 2017, Fall 2017)
- Independent Studies in Computer Science, CUNY Graduate Center (Spring 2016, Spring 2017, Fall 2017)

Graduate courses taught at New York University, Computer Science Department

- Design and Analysis of Algorithms (both in class and online, Fall 2016, Spring 2020, Fall 2022, Spring 2023, Spring 2024)
- The Foundations of Computer Science (2017 – 2018, Both in class and online courses)
- Modern Cryptography (Fall 2013)

Courses taught at the CUNY Graduate Center, MS Program in Data Analysis and Visualization, For Liberal Arts, Humanities and Social Sciences Students

- Working With Data: Fundamentals (Fall 2018)

Courses taught at CUNY Queens College

- Discrete Structures, Algorithms, Post-quantum Cryptography.

Courses taught at NYCCT, City University of New York

- Discrete Structures and Algorithm, Finite Fields and Cryptography, Discrete Mathematics, Mathematical Modelling, Differential Equations, Linear Algebra, Calculus I, Precalculus, Probability and Statistics.

Courses taught at University of St Andrews in Scotland

- Group Theory, Linear Algebra.

Courses taught at Hunter College

- Finite Mathematics, Linear Algebra, Calculus I

University Service, University of York, UK

- Interview Panel member for recruitment committee Research Theme Champions, Technologies for the Future (2020)
- Interview Panel member for hiring committee Chair/Distinguished Professor of Quantum Computing (2020)
- Interview Panel member for hiring committee Chair/Distinguished Professor of Engineering (Electronic Engineering) (2019)
- Interview Panel member for hiring committee permanent assistant professor/lecturer in Cyber Security (2019)
- Interview Panel member for hiring committee permanent assistant professor/lecturer in Electrical Engineering (2019)
- Interview Panel member for hiring committee Research Development Manager, Information and communications technology and Electronics (2019)
- Interview Panel member for hiring committee 4 permanent assistant professors/lecturers in Computer Science (2019)
- Member of the Industrial Advisory Board (2018–2021)
- Interview Panel member for hiring committee 2 Research Associate/Fellow of Assuring Autonomy International Programme (2020)
- Member of University of York Women's Forum, Diversity and Equality Committee (2020–2021)
- April 2021 – August 2021 : The Head of Department of Computer Science Advisory Team

Queens College (CUNY) Service

- Hiring Committee member for Two Tenure-Track Assistant Professorship in Computer Science, 2022.
- Member of Campus Working Group on COACHE: Collaborative on Academic Careers in Higher Education, Office of Provost, `https://www.qc.cuny.edu/provost/coache/`, Since 2023.
- Member of Generative AI team, Center for Excellence in Teaching, Learning, and Leadership (CETLL), Since 2023.
- Mentoring junior faculty, Since 2022.

Departmental Service, Mathematics Department, NYCCT, CUNY

- Mentoring junior faculty (2011–2018)
- Member of the Research and Grants committee (2008–2018)
- Co-Chair of Student committee and faculty advisor to the Student Math Club (2012–2015)
- Co-Chair of Website Committee (2008–2015)
- CUNY Campaign Captain in the Mathematics Department (2006–2015)