Bren Cavallo

Education:

- CUNY Graduate Center, Mathematics, Ph.D., 2015
  Adviser: Delaram Kahrobaei
- Vassar College, Mathematics and Italian, B.A., 2011.

Research Interests

- Computational/Combinatoria Group Theory
- Cryptography, Theoretical Computer Science, Computational Complexity

Research Grants and Fellowships

- **Office of Naval Research Grant**, Research Fellowship through a grant of D.Kahrobaei and V.Shpilrain, Research on Applications of Group Theory in Information Security, Summer 2012 -
- **PSC CUNY Research Foundation**, Research Fellowship through a grant of D.Kahrobaei Research on Generic Case Complexity of Algorithmic Problems in Polycyclic Groups, Summer 2013-
- **Center for Logic Algebra Computation** (NYCCT, CUNY) Research Assistantship. Director: D.Kahrobaei, Fall 2012-
- **Science Fellowship**, CUNY Graduate Center, Fall 2012
- **Mary Evelyn Wells - Gertrude Smith Prize for Mathematics**, Vassar College, May 2011
- **REU Research Fellowship**, Kent State University, Summer 2010

Publications

(1) B. Cavallo, J. Delgado, D. Kahrobaei, E. Ventura, *Algorithmic Recognition of Infinite-Cyclic-Extentions*, Journal of Pure and Applied Algebra, Elsevier, (*to appear*).

(2) B. Cavallo, G. Di Crescenzo, D. Kahrobaei, V. Shpilrain, *Efficient and Secure Delegation of Group Exponentiation to a Single Server*, International Workshop on Radio Frequency Identification: Security and Privacy Issues. Springer International Publishing, 156-173 (2015).

(3) 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).

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

Patents

- B. Cavallo, D. Kahrobaei, V. Shpilrain, *Decoy-based secure delegation of computation, with application to RSA encryption*, patent number: 3071140 US01 (2014).

Visiting Positions

- January 2014: Institute Henri Poincare, Paris, France.
- June/November 2013: Universitat Politecnica de Catalunya, Barcelona.
- October 2013- : Center for Logic, Algebra, and Computation, New York City College of Technology (CUNY), Mathematics Department. Research Assistant (Adviser: D. Kahrobaei)

Invited Conference Talks

(1) **2015 Joint Mathematics Meetings**, Special Session on Groups, Algorithms, Cryptography San Antonio, TX, *Decoy-Based Secure Delegation of Computation, With Application to RSA*, January 11, 2015

(2) **GAGTA 8: Geometric and Asymptotic Group Theory with Applications**, University of Newcastle, Newcastle, Australia, *A family of polycyclic groups over which the uniform conjugacy problem is NP-complete*, July 22, 2014

(3) **CANT: Combinatorial and Additive Number Theory:** CUNY Graduate Center, New York, NY, *The subset sum problem and the conjugacy problem in polycyclic groups*, May 30, 2014

(4) **GAGTA 7: Geometric and Asymptotic Group Theory with Applications**, City College of New York, New York, NY, *Secret Sharing Using Non-Commutative Groups and the Shortlex Ordering*, May 30, 2013

(5) **American Mathematical Society Eastern Sectional Meeting**, AMS Special Session on Algorithmic Problems of Group Theory and Applications in Cryptography, Boston College, MA, *Secret Sharing Using Non-Commutative Groups and the Shortlex Order*, April 7, 2013

Invited Seminar and Colloquium Talks

- **Algebra and Cryptography Seminar**, CUNY Graduate Center, New York, NY
  (6) *Decoy-Based Secure Delegation of Computation, With Application to RSA*, October 10, 2014
  (7) *Secret Sharing using the Shortlex Ordering*, April 26, 2013
  (8) *Secret Sharing*, February 1, 2013
- **New York Algebra Colloquium**, CUNY Graduate Center, New York, NY
  (9) *The Conjugacy Problem Over Families of Polycyclic Groups*, October 10, 2014
  (10) *A Tits Alternative for the Automorphism Group of a Rigid Poly-Z Group*, May 9, 2014
- **Vassar College Mathematics Colloquium**, Vassar College, Poughkeepsie, NY
  (11) *An Introduction to Computational Group Theory*, October 7, 2014
  (12) *Eigenvectors of Nearly Normal Matrices*, November 11, 2010
- **Seminari de Teoria de Grups**, CRM- Centre de Recerca Matematica, Bellaterra, Spain
  (13) *Secret Sharing Using Non-Commutative Groups and the Shortlex Ordering*, June 21, 2013

Expository Seminar Talks

- **City Tech Undergraduate Mathematics Seminar**, New York City College of Technology, New York, NY
  (14) *Random Walks on Integer Lattices*, March 13, 2014
- **NYU Undergraduate Mathematics Seminar**, New York University, New York, NY
  (15) *Perfectly Secret Encryption*, April 4, 2014
- **GC Student Cryptography Seminar**, CUNY Graduate Center, New York, NY,
  (16) *The Leftover Hash Lemma*, September 19, 2014
  (17) *Delegation of Exponentiation With Application to RSA*, September 12, 2014
  (18) *Conjugacy in Polycyclic Groups and Lengths of Words*, April 25, 2014
  (19) *Subset Sum Problems*, February 28, 2014
  (20) *The Millionaires Problem*, September 20, 2013
  (21) *Amplification of Undecidable Problems*, April 19, 2013
  (22) *Orbit-Stabilizer Problem in Polycyclic Groups, Part III*, March 1, 2013
  (23) *Orbit-Stabilizer Problem in Polycyclic Groups, Part II*, February 22, 2013
  (24) *Orbit-Stabilizer Problem in Polycyclic Groups, Part I*, February 15, 2013
  (25) *On Various Secret Sharing Schemes, Part II*, October 19, 2012
  (26) *On Various Secret Sharing Schemes, Part I*, October 12, 2012

Conference Organization

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

Seminar Organization

- Co-organizer of the GC Student Cryptography Seminar (with Ha Lam and Bianca Sosnovski) CUNY Graduate Center (Fall 2012 - Spring 2015) `https://sites.google.com/site/gccryptostudents/` Faculty Adviser: Delaram Kahrobaei

Teaching Experience

- Adjunct Lecturer, City College of New York, Fall 2011 - Spring 2015
  – Courses Taught: Introduction to Arithmetic, College Algebra, Precalculus, Calculus I.

Professional Membership

- **AMS,** American Mathematical Society
- **Sigma Xi,** Sciences Honor Society
- **NYAS,** New York Academy of Sciences

Additional Information

- **Languages:** English (native), Italian (conversational), Spanish (reading)
- **Programming Languages:** Python, GAP (Groups Algorithms Programming), Java
- **Additional:** Freelance Jazz Pianist

References

- Professor Delaram Kahrobaei (The New York College of Technology, Graduate Center, City University of New York, Mathematics/Computer Science Department)
- Professor Vladimir Shpilrain (The City College of New York, Graduate Center, City University of New York, Mathematics Department)
- Professor Enric Ventura Capell (Universitat Politecnica de Catalunya, Mathematics Department)