

Biographical Sketch –DELARAM KAHROBAEI

Mathematics Department, New York City College of
Technology (CUNY) 300 Jay St. Brooklyn, NY 11201
Doctoral Program in Computer Science Department
CUNY Graduate Center, 365 Fifth Avenue, NY, NY 10016

E-mail: dkahrobaei@gc.cuny.edu
E-mail: dkahrobaei@citytech.cuny.edu
Tel: (646)318-8520
Webpage: <https://wfs.gc.cuny.edu/DKahrobaei/www/>

PROFESSIONAL DEVELOPMENT

Ph.D. in Mathematics, CUNY GRADUATE CENTER (City University of New York: CUNY) (2004) Advisor: G. Baumslag

Masters of Computer Science, The City College of New York, School of Engineering (CUNY)(2004)

Masters of Mathematics, Claremont Graduate University, Claremont Colleges (1999)

BS of Mathematics and Computer Science, SHARIF UNIVERSITY OF TECHNOLOGY, Iran (1998)

APPOINTMENTS

Assistant Professor in Mathematics (IT) (since 2006) NEW YORK CITY COLLEGE OF TECHNOLOGY (CUNY)

Doctoral Faculty in Computer Science, CUNY Graduate Center, Doctoral Program in Computer Science (2008—Present)

Lecturer in Pure Mathematics, UNIVERSITY OF ST ANDREWS, MATHEMATICAL INSTITUTE (SCOTLAND, UK) (2004 —2006)

Adjunct Lecturer, HUNTER COLLEGE, DEPARTMENT OF MATHEMATICS, CUNY (2000 — 2004)

Research Assistant in Combinatorial Group Theory, NEW YORK GROUP THEORY COOPERATIVE (2001—2004)

Research Assistant in Computational Group Theory and Cryptologic Application (2002—2003)

CENTER FOR ALGORITHMIC AND INTERACTIVE SCIENTIFIC SOFTWARE (CAISS), City College of New York, CUNY

PUBLICATIONS

1. *A Simple Proof of a Theorem of Karrass and Solitar*, **American Math Soc. Contemporary Mathematics**, Vol. 372, 107-108 (2005)
2. *A Non-Commutative Generalization of the ElGamal Key Exchange using Polyyclic Groups* (with B.Khan) **Proceeding of IEEE** (2006)
3. *The True Prosoluble Completion of a Group: Examples and Open Problems* (with P.de la Harpe, G.Arzhantseva, Z.Sunik)
Journal of Geometriae Dedicata, Springer Netherlands, Vol. 124, No.1, 5-26 (2007)
4. *A Graphical Generalization of Arithmetic* (with K.Bhutani and B.Khan)
Integers: Electronic Journal of Combinatorial Number Theory, Vol. 7, A12, 31 pp. (2007)
5. *Doubles of Residually Solvable groups*
Aspects of Infinite Group Theory, Algebra and Discrete Mathematics, World Scientific, Vol.1, 7 pp (2008)
6. *A Problem Concerning Decision versus Search Arising in Group- Based Cryptography* (with M.Anshel)
Journal of Groups, Complexity, Cryptology, Heldermann Verlag, 8 pp(2009)
7. *On Residual Solvability of Generalized Free Products of Finitely Generated Nilpotent Groups*, Accepted, **Communications in Algebra**, 10 pp
8. *A Note on Residual Solvability of One-Relator Groups* (with A.Douglas) 8 pp (2009) **Linus Publication**
9. *A survey and open problems in non-commutative cryptography* (with B.Fine, M.Habeeb, G.Rosenberger)
Submitted to **Cambridge University Press in the London Mathematical Society Lecture Note Series** (27 pages) (2009)
10. Expository Paper: Applications of Group Theory in Cryptography (with M. Anshel)
Accepted to **International Journal of Pure and Applied Mathematics** (2009)
11. *On Growth Rate of an Endomorphism of a Group* (with K.Falconer, B.Fine)(Preprint), 21 pp, (2009)
12. *Polyyclic Groups: A New Platform for Cryptology?* (with B.Eick) **math.GR/0411077**, 7 pp (2004)
13. *Residual Solvability of Generalized Free Products*, **CUNY Graduate Center PhD Thesis**, 194 pp (2004)
14. Book Project: Group Theory and application to Cryptography (with S.Shahriari) (In preparation)(99 pages so far)
15. *The complexity of Decision and Search for Nilpotent Groups* (with M.Anshel) (in preparation, 2009)
16. *Generalizing Discrete Log Problem using polyyclic groups* (with M.Habeeb, V.Shpilrain) (in preparation 2009)
17. *Some Residually Solvable One-relator Groups* (with A.Douglas, K. Bencsath)(Preprint 2009)

ACADEMIC AND PROFESSIONAL HONORS/AWARDS

NSF Grant, National Science Foundation, PI, Award No. DMS-0758054, 2008-2009 (\$12,800)

NSF Grant, National Science Foundation, co-PI, ADVANCE-IT START proposal, HRD-0811192, 2008— 2010 (\$195,000)

Faculty Fellowship Publication Award, City University of New York, Spring 2009

PSC-CUNY Grant, CUNY Research Foundation Grant, 2007— 2010

EMS Grant, Edinburgh Mathematical Society Grant, UK, 2006

LMS Grant, London Mathematical Society Collaborative Small Grant, UK, 2005, 2006

KTH Visiting Fellow Grant, Kungl Tekniska Hogskolan, Matematiska Institutionen, Sweden, November 2005

Isaac Newton Institute for Mathematical Sciences Visiting Fellow Grant, Cambridge, UK, July 2005

FIM-ETHZ Travel Grant, FIM, ETH Zurich, Université de Genève, Switzerland, June 29-July 6 2005

IHES Visiting Fellow Grant, Institute des Hautes Etudes Scientifiques, France, November 2004

Swiss National Fund Research Grant, Université de Genève, Switzerland, Three months in 2005

IPM Visiting Fellow Grant, Institute for Studies in Theoretical Physics & Math, Iran, Dec. 2004-Jan 2005

Graduate A Fellowship, Hunter College, CUNY, NY, US, 2003— 2004

Research Fellowship, CUNY Research Foundation, The City College of New York (2001-2003), Hunter College (Summer 2002)

CUNY Graduate Center (Fall 2000); **Science Fellowship**, CUNY Graduate Center, 1999 — 2001, **PSC-CUNY Award**, CUNY

Graduate Center, 2002 — 2003; **University Fellowship**, CUNY Graduate Center, 2001 — 2002

INVITED VISITING POSITIONS

IHES-Institute des Hautes Etudes Scientifiques (France) Invited Visiting Professor (November 2004)

IPM-Institute for studies in Theoretical Physics and Mathematics (Iran) Invited Visiting Scholar (December 2004- January 2005)

Université de Genève (Switzerland) Invited Visiting Scholar (Hosts: G. Arzhantseva, P.de la Harpe) (Jan, Jun 2005, Jan 2006)

FIM, ETH, Université de Genève, Invited Participant (Program in Lie Groups: Topology to Arithmetic) (Switzerland)

In memory of Armand Borel (Host: M.Burger)(June29 –July 7 2005)

Kungl. Tekniska Hogskolan, (Sweden) Invited Visiting Scholar, Host: E. Shahgholian, Nov 2005

Isaac Newton Institute for Mathematical Sciences (Cambridge, UK) Invited Participant, Program in Model Theory; Applications in

Algebra-Analysis)(July 2005)

Ecole Polytechnique Fédérale de Lausanne (Switzerland) Invited Visiting Scholar (Host: L.Bartholdi) (December 2005)

AIM- American Institute of Mathematics (Palo Alto, CA, USA) Invited Participant (Host: V. Shpilrain) (August 2007)

INVITED LECTURES : INTERNATIONAL AND NATIONAL (MORE THAN 50 TALKS)

United States: International Conference on Geometric and Combinatorial Methods in Group Theory and Semi-group Theory (John Meakin 60th Birthday)(Nebraska) (2009), 2009 Joint Mathematics Meeting-Algebraic Cryptography & Generic Case Complexity Special Session(Washington DC), Geometric and Asymptotic Group Theory with Applications Conference (Stevens Institute of Technology, Hoboken, NJ) (2009), American Mathematical Society Meeting-Mathematical aspects of Cryptography Special Session (2007), Geometric Group Theory conference in the Gulf in Florida(2008), Zassenhaus Group Theory Conference in Pennsylvania(2009), New York Group Theory (Magnus) Seminar(2008), Rutgers Mathematics Colloquium(2008), CUNY Graduate Center Cryptography Seminar(2008), New York University(2004), Rutgers University(2004), SUNY Albany Group Theory Conference (2003), CUNY Graduate Center Algebra and Cryptography Seminar(2006), New York Logic Workshop (2004), New York City College of Technology Colloquium(2007), New York City College of Technology Research Conference (2008), Medgar Evers College of CUNY Colloquium (2007), Bronx Community College of CUNY Colloquium (2008)

Canada: Third Annual Meeting of the Prairie Network for Research in Mathematical Sciences University of Saskatchewan (2009), Université du Québec à Montréal Colloquium (2009), McGill University (2009)

England: British Mathematics Colloquium in Liverpool 2005(Contributed), Oxford University 2005, University of Warwick 2004 Isaac Newton Institute for Mathematical Sciences (2005, Contributed), University of Nottingham (2006)

Groups St Andrews (University of Bath)(2009 contributed)

Scotland: University of Glasgow (2005), University of Edinburgh (2005), University of St Andrews (2006, 2005, 2004)

Switzerland: Université de Genève (2005), Ecole Polytechnique Fédérale de Lausanne (2005)

France: IHES Institute des Hautes Etudes Scientifiques (2004)

Spain: First Meeting of the Spanish Mathematical Society 2005), Centre de Recerca Matemàtica, Barcelona (2005)

Sweden: The Royal Institute of Technology in Stockholm (2005)

Ireland: Queens University Belfast (2005)

Iran: IPM Institute for studies in Theoretical Physics and Mathematics (2006, 2005, 2004), Sharif U. of Technology (2004)

SYNERGISTIC ACTIVITIES

Organizer of **American Mathematical Society Meeting**, 2010 Eastern Spring Special Session, “Groups, Computations, Applications”

Co-founder of **NYWIMN**, New York Women in Mathematics Network, with Victoria Gitman (since 2006)

Co-organizer of **THE NYWIMN FIRST and SECOND CONFERENCES**, The City University of New York,

(CUNY Graduate Center-December 9, 2006) (City Tech-May 2, 2008) (with Victoria Gitman)

Director of C-LAC, Center for Logic, Algebra and Computation (Since 2008)

Member of the Editorial Board of **International Journal of Open Problems in Computer Science and Mathematics**

Panel Member for the research projects of the **PSC CUNY Grants**, Research Foundation of City University of New York(since 2009)

Referee for the research projects of the **PSC CUNY Grants**, Research Foundation of City University of New York(since 2008)

Book Reviewer for **Springer-Verlag** (UK)

Referee for the **Journal of Algebra**, Referee for **Journal of Groups, Complexity, Cryptology (Heldermann Verlag, Germany)**

Co-founder & Co-organizer of **New York Algebra Colloquium**, CUNY Graduate Center (Since Fall 2008) (with A.Douglas)

Leading and Lecturing Research Seminar in **Combinatorial Group Theory and Cryptography**, Interdisciplinary Seminar in

Mathematics and Computer Science Department, CUNY Graduate Center (Since Spring 2008)(with M.Anshel, K.Boklan)

Co-founder and Co-organizer of **Mathematics Seminar Series**, NYCCT, CUNY (Since September 2007) (with Hans Schoutens)

Co-founder and Co-organizer of C-LAC Seminars, City Tech (CUNY) (Since Fall 2008) (with A.Douglas, V.Gitman)

Organizer of **Polycyclic Groups and Cryptologic Applications Seminar**, University of St Andrews (2004-2005)

Supervising **PhD student research** project in CUNY Graduate Center in Mathematics Department: M. Habeeb (since 2009)

External **PhD Examiner** in Mathematics, **Rutgers University**: Leigh Cobbs, Lattice Subgroups of Kac-Moody Groups(July 2009)

PhD Examiner in Computer Science, CUNY **GC**: C.Chum, Hash functions, Latin Squares, Security Sharing Schemes (May 2009)

Supervising **MSc student research** project in CUNY Graduate Center in Mathematics Department: H.Lam (Since summer 2009)

Supervising **MSc student research** project in CUNY Graduate Center in Mathematics Department: S.Sze (Since Fall 2009)

Supervising student research project in New York City College of Technology, City University of New York:

Fall 2007-2008: K.Islam [Public key encryption] Supported by Emerging Scholar Fellowship, He is now working in DHS

Spring 2007: O.Davy [RSA encryption Scheme] Supported by LSAMP

Spring 2008: W.Guo [Life and Work of Sarah Rees on complexity of Word Problem in Group Theory]

Spring and Summer 2008: F.Fung [A topic in Applications of Combinatorial Group Theory in Cryptography]

2008-2009: S.Scott [Digital Signatures] Supported by NSF-LSAMP and emerging scholar fellowship

Fall 2008: R.Li [Comparing security in different key exchange problems] Supported by Emerging Scholar Fellowship

Spring 2009: D. Morales, P vs NP supported by Emerging Scholar fellowship

Fall 2009: M.Dupas and R.Dambreville, Computational Group Theory and Cryptography, supported by NSF-LSAMP

Supervising student research project from Brooklyn College: 2009: E. Baidoo, Digital Signatures supported by NSF-LSAMP

Supervising MSc student research project in University of St Andrews: A. Ferguson [on Algebraic Cryptography](2005)

Mentor for the Association for Women in Mathematics Mentor Network (Since Spring 2008)

Member of ACC, **Algebraic Cryptography Center**, Stevens Institute of Technology (Since 2007)

Member of CIRCA, **Center for Interdisciplinary Research in Computational Algebra**, University of St Andrews (2004-06)

COLLABORATORS

University of Geneva (Switzerland): P. de la Harpe, G.Arzhantseva, **Texas A&M University:** Z.Sunik

Catholic University of America: K. Bhutani, **Technische Universität Braunschweig(Germany):** B. Eick

City University of New York: B.Khan(J.Jay, GC), V.Gitman & A.Douglas(City Tech), M.Anshel(CUNY , GC), M.Habeeb(GC),

V.Shpilrain, **Fairfield University:** B.Fine, **University of St Andrews:** K.Falconer, **TU Dartmund(Germany):** G.Rosenberger