Centro de Informática
Centro de Ciências Exatas e da Natureza
Federal University of Paraíba,
João Pessoa, Paraíba CEP: 58.051-900, Brazil
+55 83 9613 8029
vivek.nigam@gmail.com
http://www.nigam.info
Nationality: Brazilian
Professor Adjunto *(Equivalent to Tenured Associate Professor)*

Vivek Nigam

Curriculum Vitae

Executive Summary

Research Projects: My research is centered in four different, but connected areas:

- **Formal Methods** being a specialist on the use of Maude and Statistical Model Checking. I have used formal methods for among other applications, the analysis of Denial of Service Attacks, Security Protocol Verification and Cyber-Physical Systems.
- **Foundations of Computer Security** being a specialist on protocol security and collaborative systems. I am interested now in Cyber-Physical security protocols, timed intruder models, and collaborative systems subject to regulations, such as Clinical Trials.
- **Denotational Semantics of Programming Languages** being a specialist on proving the soundness of proof transformations based on effect type systems. I am now interested in proving the equivalence of concurrent and probabilistic programs and their application to compiler and program verification.
- **Logical Frameworks** being a specialist on linear logical frameworks and the specification of systems with different notions of modalities, such as spatial, temporal and epistemic modalities.

In the last 5 years, I have co-authored publications appearing in major conferences (ESORICS, POST, POPL, LICS, IJCAR, CONCUR, LICS, ICLP) and leading journals (ToN, I&C, TCS, TPLP, JLC, JAR).

Research Projects: I am member of the project GT-ACTIONS (2014 - 2016) funded by the RNP – Brazilian agency responsible for the country's IP network. I am PI of the project "Regulated Collaborative Systems" (2014-2017) of the Brazilian Science without Borders program. I am awarded a a scholarship (once from 2013- 2016 and then from 2016 – 2019) for "High Productivity Researchers". I was supported by the prestigious Alexander von Humboldt foundation for two years (2010-2012) as a Postdoctorate researcher at LMU in Germany. During my PhD studies, I was supported by a French scholarship from Inria and during my Master studies, I was supported by the European Commission through the Alβan programme.

Teaching: At LMU and UFPB, I was responsible for 9 courses on 5 different areas with an average load between 10-12 hours per week. I am currently co-advising 10 students of which 4 Master and 6 Bachelor Students.

Academic Background

from 02/2017	***Researcher***, *fortiss*, João Pessoa, Brazil. (Equivalent to **Tenured Associate Professor**)
10/2012 – current (on leave)	***Professor Adjunto***, *Federal University of Paraíba*, João Pessoa, Brazil. (Equivalent to **Tenured Associate Professor**)
11/2010 - 10/2012	**Alexander von Humboldt Postdoctoral Researcher**, *Ludwig-Maximilians-Universität*, Munich, Germany. Supervisor: Martin Hofmann
11/2009 - 09/2010	**Postdoctoral Researcher**, *University of Pennsylvania*, Philadelphia, USA. Supervisors: Andre Scedrov and Boon Thau Loo
10/2006 - 09/2009	**PhD – Computer Science**, *École Polytechnique*, Paris, France. Supervisor: Dale Miller (Graduated with *Distinction*)
10/2004 - 09/2006	**M.Sc. in Computational Logic**, *Technische Universität Dresden and Universidade Nova de Lisboa*, Dresden, Germany and Lisbon, Portugal. Supervisor: João Leite (Graduated with *Distinction*)
01/1999 - 12/2003	**Bachelor in Electronic Engineering**, *Instituto Tecnológico de Aeronáutica*, São José dos Campos, Brazil.

Non-Academic Professional Experience

02/2005 - 07/2005	**Research Assistant**, *Fraunhofer Institute*, Dresden, Germany.
01/2004 - 09/2004	**Applications Engineer**, *SMAR*, Ribeirão Preto, Brazil.
01/2003 - 12/2003	**Intern of the Strategic Sourcing Practice**, *A.T. Kearney*, São Paulo, Brazil.

Grants / Awards / Certificates

08/2016 - 09/2016	Alexander von Humboldt Short-Term Research Stay at LMU.
03/2016 - 02/2019	CNPq Scholarship for High Productivity Researchers (*Pesquisador de Produtividade – Nível 2*)
10/2014 - 10/2016	Member of the project GT-ACTIONS: A Computational Framework for the Mitigation of Denial of Service Attacks. This project is funded by the *Rede Nacional de Ensino e Pesquisa* – the agency responsible for the Brazilian IP -Network. – 20% acceptance rate. Funding for traveling, equipments and student scholarships.
07/2014 - 09/2014	Alexander von Humboldt Short-Term Research Stay at LMU.
03/2014 - 03/2017	Science without Borders: Senior Visiting Professor for Carolyn Talcott
11/2013 - 10/2016	Project on Timed Collaborative Systems financed by CNPq - Universal Faixa A
07/2013	DAAD-Capes Scholarship for Short-Term Research Visit at LMU.
03/2013 - 02/2016	CNPq Scholarship for High Productivity Researchers (*Pesquisador de Produtividade – Nível 2*)
09/2010 – 11/2012	Alexander von Humboldt Research Fellowship for Postdoctoral Researchers.
07/2009	First place in the IPv6 challenge organized by G6 and sponsored by SFR.
10/2006 – 09/2009	PhD scholarship – INRIA/Mobius.
10/2004 - 09/2006	ALβAN scholarship – European Union Programme of High Level Scholarships for Latin America.

Skills

Languages	Portuguese, English: *Fluent* – German: *Advanced* – French: *Intermediate* – Hindi: *Basic*
Programming	C, Java, OCaml, Maude, Prolog, λ-Prolog, Answer-Set Programming, Linear Logic, LaTeX

References

Post-doc supervisor	Andre Scedrov, UPENN – `scedrov@math.upenn.edu`. Co-author in [31, 30, 28, 8, 26, 9, 24, 4, 17, 3, 12]
Collaborator	Carolyn Talcott, SRI-International – `clt@csl.sri.com`. Co-author in [42, 28, 26, 9, 17, 3, 13, 12, 11]
Post-doc supervisor	Martin Hofmann, LMU – `hofmann@ifi.lmu.de`. Co-author in [25, 21, 16]
Post-doc supervisor	Boon Thau Loo, UPENN – `boonloo@cis.upenn.edu`. Co-author in [30, 9, 8]
Ph.D Supervisor	Dale Miller, École Polytechnique – `dale@lix.polytechnique.fr`. Co-author in [34, 33, 32, 10]

Software

SeVen	A prototype with a selective defense for mitigating application-layer DDoS. See [18] for more details.
Clinical Trial Assistant – CTA	A prototype written in Maude and Java for real-time monitoring of Clinical Trials. See [42, 28, 26, 3] for more details.
TATU	A tool written in OCaml for checking automatically whether a proof system specified in Linear Logic with Subexponentials admits cut-elimination. See [1] for more details.
QUATI	A tool written in OCaml and Answer-Set Programming for checking automatically which rule permutations are always allowed. See [20, 23, 43] for more details.

Invited Speaker and Committee Membership

Invited Speaker / Panelist

- Invited Speaker at the Workshop Logic and Applications, Dubrovnik, Croatia, 2016
- Editorial Board on Computer and Network Security of the Frontiers journal (since 2014)
- Invited Speaker at the Workshop on Applied Mathematics of UnB, Brasília, Brazil 2013, 2016
- Invited Speaker at the DDoS Mitigation in the NREN Environment Workshop, Vienna, Austria, 2015
- Invited Speaker at the Shonan Meeting on Logic and Verification Methods for Security and Privacy, Japan, 2015
- Invited Speaker at Logical Frameworks and Meta-Languages (LFMTP), Berlin, Germany, 2015
- Panelist on Network/Information Security at the Workshop of the RNP (WRNP), Vitória, Brazil 2015
- Invited Speaker at the Alexander von Humboldt Kolleg on Proofs, Bern, Switzerland 2013
- Invited Speaker at Dagstuhl Meeting on Security and Rewriting, Dagstuhl, German, 2011.

Programme Committee

- **Steering Committee** of Logical and Semantic Frameworks with Applications (LSFA) 2016-2018
- Principles of Programming Languages (POPL) 2017 (External Reviewer)
- Workshop on Formal Techniques for Safety-Critical Systems, 2016
- Workshop on Linearity 2016
- Logic in Computer Science (LICS) 2016
- Workshop on Rewriting and its Applications (WRLA) 2016
- Formal Structures in Computation and Deduction (FSCD) 2016
- Logical and Semantic Frameworks with Applications (LSFA) 2016 (**co-chair**)
- International Joint Conference on Artificial Intelligence (IJCAI) 2015 (Extended PC)
- Workshop on Logic, Language, Information and Computation (WoLLIC) 2015
- International Colloquium on Theoretical Aspects of Computing (ICTAC) 2015
- Certified Programs and Proofs (CPP) 2015
- Logical and Semantic Frameworks with Applications (LSFA) 2011, 2012, 2014, 2015
- International Conference on Rewriting Techniques and Applications (RTA) joint with the International Conference on Typed Lambda Calculi and Applications (TLCA) 2014
- Intuitionistic Modal Logic and Applications (IMLA) 2013

Organizing Committee

- Shonan meeting on Logic and Verification Methods in Security and Privacy (2015)
- 18th Workshop on Logic, Language, Information and Computation (WoLLIC'2011)
- Intuitionistic Modal Logic and Applications 2013 (IMLA'13)

Hiring Committee

President of the hiring committee for a lecturer position on Theory and Design of Algorithms of the computer science department at the Federal University of Paraíba.

List of Publications

Journals

[1] Vivek Nigam, Elaine Pimentel, and Giselle Reis. An extended framework for specifying and reasoning about proof systems. *J. Log. Comput.*, 26(2):539–576, 2016. Special issue in honor of Roy Dyckhoff.

[2] Carlos Olarte, Elaine Pimentel, and Vivek Nigam. Subexponential concurrent constraint programming. *Theor. Comput. Sci.*, 606:98–120, 2015.

[3] Max Kanovich, Tajana Ban Kirigin, Vivek Nigam, Andre Scedrov, and Carolyn Talcott. A rewriting framework and logic for activities subject to regulations. *Mathematical Structures in Computer Science*, 2015. Published online.

[4] Max I. Kanovich, Tajana Ban Kirigin, Vivek Nigam, and Andre Scedrov. Bounded memory Dolev-Yao adversaries in collaborative systems. *Inf. Comput.*, 238:233–261, 2014.

[5] Elaine Pimentel, Carlos Olarte, and Vivek Nigam. A proof theoretic study of soft concurrent constraint programming. *TPLP*, 14(4-5):649–663, 2014.

[6] Max I. Kanovich, Tajana Ban Kirigin, Vivek Nigam, and Andre Scedrov. Bounded memory protocols. *Computer Languages, Systems & Structures*, 40(3-4):137–154, 2014.

[7] Vivek Nigam. A framework for linear authorization logics. *Theoretical Computer Science*, 536(0):21 – 41, 2014.

[8] Vivek Nigam, Limin Jia, Boon Thau Loo, and Andre Scedrov. Maintaining distributed logic programs incrementally. *Computer Languages, Systems & Structures*, 38(2):158–180, 2012.

[9] Anduo Wang, Limin Jia, Wenchao Zhou, Yiqing Ren, Boon Thau Loo, Jennifer Rexford, Vivek Nigam, Andre Scedrov, and Carolyn L. Talcott. Fsr: formal analysis and implementation toolkit for safe interdomain routing. *IEEE/ACM Trans. Netw.*, 20(6):1814–1827, 2012.

[10] Vivek Nigam and Dale Miller. A framework for proof systems. *J. Autom. Reasoning*, 45(2):157–188, 2010.

Refereed Conferences/Workshops

[11] Vivek Nigam, Carolyn Talcott, and Abraão Aires Urquiza. Towards the automated verification of cyber-physical security protocols: Bounding the number of timed intruders. In *European Symposium on Research in Computer Security (ESORICS)*, 2016.

[12] Max Kanovich, Tajana Ban Kirigin, Vivek Nigam, Andre Scedrov, and Carolyn Talcott. Timed multiset rewriting and the verification of time-sensitive distributed systems. In *14th International Conference on Formal Modeling and Analysis of Timed Systems (FORMATS)*, 2016.

[13] Carolyn Talcott, Vivek Nigam, Farhad Arbab, and Tobias Kappé. Formal specification and analysis of robust adaptive distributed cyber-physical systems. In *Formal Methods for the Quantitative Evaluation of Collective Adaptive Systems*, LNCS, pages 1–35. 2016. 16th edition in the series of Schools on Formal Methods (SFM), Bertinoro (Italy), 20-24 June 2016.

[14] Yuri Gil Dantas, Marcilio O. O. Lemos, Iguatemi Fonseca, and Vivek Nigam. Formal specification and verification of a selective defense for TDoS attacks. In *11th International Workshop on Rewriting Logic and its Applications (WRLA)*, 2016.

[15] Marcilio O. O. Lemos, Yuri Gil Dantas, Iguatemi Fonseca, Vivek Nigam, and Gustavo Sampaio. A selective defense for mitigating coordinated call attacks. In *34th Brazilian Symposium on Computer Networks and Distributed Systems (SBRC)*, 2016.

[16] Nick Benton, Andrew Kennedy, Martin Hofmann, and Vivek Nigam. Counting successes: Effects and transformations for non-deterministic programs. In *In Phil Wadler's Festschrift*, 2016.

[17] Max Kanovich, Tajana Ban Kirigin, Vivek Nigam, Andre Scedrov, and Carolyn Talcott. Discrete vs. dense times in the analysis of cyber-physical security protocols. In *Principles of Security and Trust - 4th International Conference, POST*, pages 259–279, 2015.

[18] Yuri Gil Dantas, Vivek Nigam, and Iguatemi E. Fonseca. A selective defense for application layer DDoS attacks. In *IEEE Joint Intelligence and Security Informatics Conference, JISIC 2014*, pages 75–82. IEEE, 2014.

[19] Carlos Olarte, Vivek Nigam, and Elaine Pimentel. Dynamic spaces in concurrent constraint programming. *Electr. Notes Theor. Comput. Sci.*, 305:103–121, 2014. In LSFA.

[20] Vivek Nigam, Giselle Reis, and Leonardo Lima. Quati: An automated tool for proving permutation lemmas. In *IJCAR*, pages 255–261, 2014.

[21] Nick Benton, Martin Hofmann, and Vivek Nigam. Abstract effects and proof-relevant logical relations. In Suresh Jagannathan and Peter Sewell, editors, *POPL*, pages 619–632. ACM, 2014.

[22] Vivek Nigam, Carlos Olarte, and Elaine Pimentel. A general proof system for modalities in concurrent constraint programming. In Pedro R. D'Argenio and Hernán C. Melgratti, editors, *CONCUR*, volume 8052 of *LNCS*, pages 410–424. Springer, 2013.

[23] Vivek Nigam, Giselle Reis, and Leonardo Lima. Checking proof transformations with ASP. *Theory and Practice of Logic Programming*, 13(4-5-Online-Supplement), 2013. Appearing at ICLP 2013.

[24] Max Kanovich, Tajana Ban Kirigin, Vivek Nigam, and Andre Scedrov. Bounded memory protocols and progressing collaborative systems. In *ESORICS*, volume 8135 of *LNCS*, pages 309–326. Springer, 2013.

[25] Nick Benton, Martin Hofmann, and Vivek Nigam. Proof-relevant logical relations for name generation. In Masahito Hasegawa, editor, *TLCA*, volume 7941 of *LNCS*, pages 48–60. Springer, 2013.

[26] Max I. Kanovich, Tajana Ban Kirigin, Vivek Nigam, Andre Scedrov, Carolyn L. Talcott, and Ranko Perovic. A rewriting framework for activities subject to regulations. In Ashish Tiwari, editor, *RTA*, volume 15 of *LIPIcs*, pages 305–322. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, 2012.

[27] Vivek Nigam. On the complexity of linear authorization logics. In *LICS*, pages 511–520. IEEE, 2012.

[28] Vivek Nigam, Tajana Ban Kirigin, Andre Scedrov, Carolyn Talcott, Max Kanovich, and Ranko Perovic. Towards an automated assistant for clinical investigations. In *IHI*, Second ACM SIGHIT International Health Informatics Symposium, 2012.

[29] Vivek Nigam, Elaine Pimentel, and Giselle Reis. Specifying proof systems in linear logic with subexponentials. *Electr. Notes Theor. Comput. Sci.*, 269:109–123, 2011. In LSFA.

[30] Vivek Nigam, Limin Jia, Boon Thau Loo, and Andre Scedrov. Maintaining distributed logic programs incrementally. In Peter Schneider-Kamp and Michael Hanus, editors, *PPDP*, pages 125–136. ACM, 2011.

[31] Max Kanovich, Tajana Ban Kirigin, Vivek Nigam, and Andre Scedrov. Bounded memory Dolev-Yao adversaries in collaborative systems. In *Formal Aspects in Security and Trust*, LNCS, pages 18–33, 2010.

[32] Vivek Nigam and Dale Miller. Algorithmic specifications in linear logic with subexponentials. In António Porto and Francisco Javier López-Fraguas, editors, *PPDP*, pages 129–140. ACM, 2009.

[33] Vivek Nigam and Dale Miller. Focusing in linear meta-logic. In *Proceedings of IJCAR: International Joint Conference on Automated Reasoning*, volume 5195 of *LNAI*, pages 507–522. Springer, 2008.

[34] Dale Miller and Vivek Nigam. Incorporating tables into proofs. In J. Duparc and T. A. Henzinger, editors, *CSL*, volume 4646 of *LNCS*, pages 466–480, 2007.

[35] Vivek Nigam and João Leite. Adding knowledge updates to 3APL. In Rafael H. Bordini, Mehdi Dastani, Jürgen Dix, and Amal El Fallah-Seghrouchni, editors, *PROMAS*, volume 4411 of *LNCS*, pages 165–181. Springer, 2006.

[36] Vivek Nigam and João Leite. A dynamic logic programming based system for agents with declarative goals. In Matteo Baldoni and Ulle Endriss, editors, *DALT*, volume 4327 of *LNCS*, pages 174–190. Springer, 2006.

[37] Alexander Kozlenkov, Rafael Peñaloza, Vivek Nigam, Loïc Royer, Gihan Dawelbait, and Michael Schroeder. Prova: Rule-based java scripting for distributed web applications: A case study in bioinformatics. In *EDBT Workshops*, volume 4254 of *LNCS*, pages 899–908. Springer, 2006.

[38] Vivek Nigam. Bloco flexível matemático. *Revista Controle e Instrumentação*, 94, 2004.

Thesis

[39] Vivek Nigam. *Exploiting non-canonicity in the Sequent Calculus*. PhD thesis, Ecole Polytechnique, sep 2009.

[40] Vivek Nigam. Dynamic logic programming and 3apl. Master's thesis, Technische Universität Dresden, Germany, and Universidade Nova de Lisboa, Portugal, sep 2006.

Unpublished Papers / Others

[41] Max Kanovich, Tajana Ban Kirigin, Vivek Nigam, Andre Scedrov, and Carolyn Talcott. Can we mitigate the attacks on distance-bounding protocols by using challenge-response rounds repeatedly? In *FCS*, 2016.

[42] Vivek Nigam and Carolyn Talcott. An executable formal model for specifying and verifying clinical trials. Draft.

[43] Vivek Nigam, Giselle Reis, and Leonardo Lima. Quati: From linear logic specifications to inference rules (extended abstract). In *Brazilian Logic Conference*, 2014.

[44] Vivek Nigam and Elaine Pimentel. Relating focused proofs with different polarity assignments. In *LFMTP*, 2013. Work in Progress.

[45] Vivek Nigam, Limin Jia, Boon Thau Loo, and Andre Scedrov. An operational semantics for network datalog. In *LAM*, 2010. A workshop affilitated to LICS'10.

[46] Max Kanovich, Tajana Ban Kirigin, Vivek Nigam, and Andre Scedrov. Progressing collaborative systems. In *FCS-PrivMod*, 2010.

[47] Juan A. Cordeiro, Ulrich Herberg, and Vivek Nigam. Reach everything from anywhere. In *online*, 2009. Obtained the first place in the IPv6 Challenge – *internet de demain*, organized by G6 and supported by SFR.

[48] Vivek Nigam. Using tables to construct non-redundant proofs. In *CiE 2008: Abstracts and extended abstracts of unpublished papers*, 2008.

[49] V. Nigam, C.L. Nasciment Jr., and L. F. C. Nascimento. Estudo comparativo da aplicação de técnicas de inteligência artificial para a previsão da faixa de peso de récem-nascidos. In *IX Encontro de Iniciação Científica e Pós-Graduação do ITA*, 2003. In Portuguese.

Teaching Experience

In the past years, I have been responsible for a number of courses in Bachelor and Masters Programs which are listed below. In most of these courses, I was responsible for the lectures, tutorials and evaluation of students.

2015.1 **Decoding the Coding Interview**, Undergraduate level course, Federal University of Paraíba. 4 hours per week. **Summary:** Coding interviews are normally used by major computer science companies, such as Google, Facebook, and Microsoft, in their hiring of software developers. In this class, I reviewed the major types of questions, training students to face such interviews, such as how to tackle a coding problem, write code on the whiteboard, and explore design alternatives.

2014.2 **Introduction to Protocol Security**, Master's level course, Federal University of Paraíba. 4 hours per week. **Summary:** Basics of cryptography; Protocol Security Properties; Logical Flaws of Existing Protocols; Principles of Protocol Design; Dolev-Yao intruder; Models for Specifying and Verifying Protocols; Tools for Protocol Verification.

2014.2, 2015.1 **Theoretical Computer Science**, Bachelor and Master's level course, Federal University of Paraíba. 4 hours per week. **Summary:** Mathematical Preliminaries; Regular Languages; Context-Free Languages; Turing Machines; Decidability; Computability; Reducibility; Church-Turing Thesis; Tractable Problems and Complexity.

2013.1, 2013.2, 2014.1 **Logic in Computer Science**, Bachelor level course, Federal University of Paraíba. 4 hours per week. **Summary:** Mathematical Preliminaries; Examples of Applications Logic in Computer Science; Propositional Logic Syntax and Semantics; Predicate Logic Syntax and Semantics; Proof Theory; Model Theory; Resolution and Logic Programming.

2012.2 **Research in Computer Science**, Bachelor-level, Federal University of Paraíba. 3 hours per week. **Summary:** Review Scientific Method; Critical Analysis of Scientific Papers; Scientific Writing; Introduction to LaTeX.

2012.1 **Protocol Security** (together with Ulrich Schöpp). Master's level course, Ludwig-Maximilians-Universität. 4 hours per week. **Summary:** Similar to the course Introduction to Protocol Security.

During these years, I introduced novel evaluation methods, such as oral exams (imported from Germany) to the Brazilian system. This experience was very successful for evaluating the level of student comprehension of the topics covered and for understanding how to improve my lectures and which topics to focus more on. I also experimented with other technologies in my lectures, such as automated judges for evaluating programming assignments, and teaching environments, namely Moodle. These technologies had a positive impact on the quality of classes as students could collaborate using the features in Moodle such as forums. The use of online judges to evaluate programming assignments established a uniform and unbiased evaluation method increasing the transparency of evaluations.

Besides the classes that I have been assigned, I have also started a number of initiatives to improve our Computer Science program. For our Bachelor program, I started a club for preparing students for Olympiads in Informatics and Programming Marathons. In this club, we discuss problems, solutions and ways to implement them. We also organize local Programming Marathons open to all students.

For our Master's Program, I started an Informatics Seminar, where other lecturers, visiting researchers and students can present their work. I am currently responsible for searching and inviting speakers. This initiative has been very fruitful as it established a forum where new collaborations can be formed. I myself started working on the project on DDoS attacks (described in Section on Grants / Awards / Certificates) because of this forum.

Finally, I am member of the commission for reformulating our Computer Science Bachelor's Program. The current program dates back almost 15 years and is seriously outdated. The commission is currently working together with the other lecturers to improve the program by focusing on the core areas of computer science.