

## CURRICULUM VITAE

GERGELY BANA

In publications: Gergei Bana

Work: Department of Mathematics of IST, Technical University of Lisbon and Instituto de Telecomunicações

Av. Rovisco Pais , Lisboa 1049-001, Portugal

Tel.: +351 21 841 7140

Fax.: +351 21 841 7048

Webpage: <http://www.math.upenn.edu/~bana>

### EDUCATION:

1998-2004: University of Pennsylvania, Mathematics Department, Ph.D. studies (degree received in August 2004), advisors: Richard V. Kadison, Andre Scedrov; main focus on operator theory, quantum logic, probability, logics and probability in cryptographic protocols; thesis advisor: Andre Scedrov; thesis title: Soundness and Completeness of Formal Logics of Symmetric Encryption

2001-2003: Wharton School, M.A. studies in Statistics (M.A. degree received in August 2003), specialized in Financial Statistics; advisor: J. Michael Steele; masters paper: Risk-Free Internal Gains – Black and Scholes Re-Examined

1992-97 Faculty of Sciences of Eötvös University, Budapest; M.S. equivalent degree (DIPLOMA) in physics received in July 1997; main focus on quantum logic, quantum field theory; thesis title: Temperley-Lieb Algebras And Their Applications

1996 spring semester: Study abroad (TEMPUS fellowship) at the University of Copenhagen: general relativity, cosmology, operator algebras

SUMMER SCHOOLS: Complex Geometry summer school, Luminy Marseille, France, July 1999; “Cosmology” summer school at Les Houches, France, September 1997; “Functional Integration” NATO-sponsored school at Cargèse, Corsica, September 1996; “Space-time Models without Reference Frames” summer school, Óbánya, Hungary, 1994

### WORK EXPERIENCE:

Advanced Postdoctoral Researcher, Department of Mathematics of IST, Technical University of Lisbon and Instituto de Telecomunicações Jul 1, 2008 -

Visiting Assistant Professor, Tulane University, Department of Mathematics, New Orleans, Sep 1, 2007- Jun 31, 2008

Postdoctoral Researcher in Cryptography and Network Security at the University of California, Department of Computer Science, Davis Sep 1, 2005 – Aug 31, 2007

Postdoctoral Researcher in Cryptography and Network Security at the University of Pennsylvania, Department of Mathematics, 2004-05

Research Assistant in Cryptography and Network Security at the University of Pennsylvania, Department of Mathematics, 2003-04

Teaching Assistant (Fall 1998 – Spring 2002) at the University of Pennsylvania, Department of Mathematics

Research Assistant (1997-1998) at the Central Research Institute for Physics, Budapest

## **TEACHING EXPERIENCE**

Tulane University, Department of Mathematics (Fall 2007 - Spring 2008): Instructor of Graduate level “Mathematical Foundations of Computer Security”, Undergraduate “Calculus I-II”

University of Pennsylvania, Department of Mathematics (Summer 2001, 2002): Instructor of Undergraduate Honors’ “Linear Algebra” and “Ordinary Differential Equations”

University of Pennsylvania, Department of Mathematics (Fall 1998 – Spring 2002): Teaching Assistant of several introductory and upper level Undergraduate classes such as Calculus, Advanced Analysis

Tutoring college and high-school students in Mathematics and Physics (1993-present)

## **RECENT TALKS:**

“Recent approaches to computational semantics for first-order logical analysis of cryptographic protocols” Computational and Symbolic Proofs of Security, Spring School and French-Japanese collaboration workshop Atagawa Heights, Hashi Izu Peninsula, Japan Apr, 2009

“On the Relationship Between Symbolic and Computational Analysis of Security Protocols” Seminar talk at Laboratory of Cryptography and Information Security, University of Tsukuba, Japan, Jan 19, 2009

“Computational Semantics for First-Order-Logic-based Symbolic Analysis of Security Protocols” 4th Franco-Japanese Computer Security Workshop, Tokyo, Japan, Dec 2008

“Computational Semantics for First-Order-Logic-based Symbolic Analysis of Security Protocols” 3rd Franco-Japanese Computer Security Workshop, Nancy, France, Mar 2008

“Computational BPL - A Stochastic Approach” at 12<sup>th</sup> Annual Asian Computing Science Conference, Carnegie Mellon University, Doha Qatar, Dec 2007

“Computational Soundness of First Order Logic-based Symbolic Analysis of Cryptographic Protocols” at Tulane University, Theoretical Computer Science Seminar, Oct 2007

“Computational Semantics for Basic Protocol Logic” at Stanford Security Lunch, Stanford, April 2007

“Computational Semantics for Basic Protocol Logic” at Symposium on Proof Theory, Linear Logic, and Program Semantics, Keio University, March 2007

“Computational Soundness of Formal Indistinguishability Relations in Abadi-Rogaway-type Theories”, Keio University, June 2006

“Soundness of Formal Encryptions in the Presence of Key Cycles” at FCC Workshop on Formal and Computational Cryptography, ENS Paris, June 2005

“Soundness and Completeness of Expanded Abadi-Rogaway Logics of Formal Encryption” at Stanford Security Seminar, July 2004

“Computational and Information-Theoretic Soundness and Completeness of the Expanded Logics of Formal Encryption” at DIMACS Workshop on Security Analysis of Protocols, June 2004

“Computational and Information-Theoretic Soundness and Completeness of the Expanded Logics of Formal Encryption” Protocol Exchange Workshop, University of Maryland, May 2004

## **LANGUAGES:**

Fluent in English and Hungarian

Upper Intermediate Japanese

Basic skills in Russian and French

## **SPECIAL INTEREST:**

Music and piano playing. Completed various university level courses on music theory, ear training and history. Piano teachers include Simon Mulligan (Nov 2004-Jun2005), Meng-Chieh Liu (Feb 2005-Aug 2005), Lara Downes (Sep 2005-Aug 2007)

## PUBLICATIONS:

Koji Hasebe, Gergei Bana, Mitsuhiro Okada: Logical Verification Methods for Security Protocols (in Japanese), *Formal Approach to Information Security (collection of survey papers)*, Publisher: Kyoritsu Shuppan, Editors: Masami Hagiya and Yasuyuki Tsukada, 2009 (to appear)

Gergei Bana, Koji Hasebe, Mitsuhiro Okada: Computational Semantics for First-Order Logical Analysis of Cryptographic Protocols, *Formal to Practical Security: Papers issued from the 2005-2008 French-Japanese collaboration*, LNCS **5458**, Springer, 2009, pp33-56

Pedro Adão, Gergei Bana, Jonathan Herzog, Andre Scedrov: Soundness and Completeness of Formal Encryption: The Cases of Key-Cycles and Partial Information Leakage, accepted to *Journal of Computer Security*, special edition of selected papers from *Computer Security Foundations Workshop 2005*, in print

Gergei Bana, Koji Hasebe, Mitsuhiro Okada: Computational Semantics for Basic Protocol Logic - A Stochastic Approach, *Proceedings of 12<sup>th</sup> Annual Asian Computing Science Conference*, LNCS **4846**, Springer, 2007, pp86-94

Gergei Bana, Payman Mohassel, Till Stegers: Computational Soundness of Formal Indistinguishability Relations and Static Equivalence, *Proceedings of Asian 06, the 11<sup>th</sup> Annual Asian Computing Science Conference*, LNCS **4435**, 2006, Springer, pp182-196

Gergei Bana: A Note on Portfolios with Risk-Free Internal Gains, *Expositiones Mathematicae* **25/1** (2007) pp83-93

Pedro Adão, Gergei Bana, Jonathan Herzog, Andre Scedrov: Soundness of Formal Encryptions in the Presence of Key Cycles, *Proceedings of the 10<sup>th</sup> European Symposium on Research in Computer Security (ESORICS)*, LNCS **3679**, 2005, pp374-396

Pedro Adão, Gergei Bana, Andre Scedrov: Computational and Information-Theoretic Soundness and Completeness of Formal Encryption, *Proceedings of the 18th IEEE Computer Security Foundations Workshop (CSFW)*, 2005, pp170-184

Gergely Bana, Thomas Durt: Proof of Kolmogorovian Censorship, *Foundations of Physics*, **27** (1997), pp1355-1373

Please note that my name on recent publications is written phonetically, Gergei Bana, so for citations or web-search please try both forms of my name: Gergei or Gergely