DANILO BAZZANELLA
Co-founder and Head of the group CrypTO – Cryptography and Number Theory
https://crypto.polito.it

CURRICULUM VITAE

Position

Aggregate Professor at the Department of Mathematical Science of Politecnico di Torino, Scientific Sector MAT/02 - Algebra.

Web site: https://crypto.polito.it/danilo_bazzanella

Education

- Master's degree with honors in Mathematics (1989 Univ. Genova) with the thesis: "Codici a Chiave Pubblica ed Algoritmi di Fattorizzazione" (tutor Prof. A. Perelli).

- Ph. D. in Mathematics (1995 Univ. Genova) with the thesis: "Metodo delle Coppie di Esponenti e applicazioni" (tutor Prof. A. Perelli).

Teaching activities

- I was and still I am in charge of numerous teaching courses for the bachelor's degree, for the master's degree and for the Ph. D. program, including Cryptography, Blockchain and Cryptoeconomy, Mathematical Analysis 1, Mathematical Analysis 2, Analytic Number Theory, Complex Analysis, Mathematical Methods for Engineering and Theory of Probability and Statistics.

- I was tutor of numerous theses in the fields of Cryptography and Number Theory.

- I was and still I am supervisor of various Ph. D. students: Carlo Sanna (31 cycle - Title of the thesis: "Arithmetic Properties of Linear Recurrences and Other Topics in Number Theory"), Simone Dutto (34 cycle), Guglielmo Morgari and Andrea Gangemi (35 cycle), Matteo Rossi, Gessica Alecci, Giuseppe D'Alconzo and Edoardo Signorini (36 cycle), Giuliano Romeo (37 cycle), Enrico Guglielmino and Federico Accossato (38 cycle) and Lorenzo Romano (39 cycle).

- Teaching Books: "Serie di Funzioni e Trasformate" D. Bazzanella, P. Boieri, L. Caire, A. Tabacco, CLUT (2001).

- I was a member of the selection committee for the admission to the Ph. D. program in Pure and Applied Mathematics of Politecnico di Torino e Università di Torino.

- I am a tutor of the student team BitPolito (https://www.bitpolito.it), dedicated to dissemination, research, and development on the subject of Bitcoin and Blockchain.

- Teacher and member of the scientific committee of the Executive Master in Decentralized Finance, Blockchain, Fintech (SAA - School of Management) (https://www.saamanagement.it/formazione-executive/finanza-decentralizzata-blockchain-fintech/)

Politecnico di Torino – Corso Duca degli Abruzzi 24, 10129 - Torino, Italy
danilo.bazzanella@polito.it – https://crypto.polito.it/danilo_bazzanella
www.linkedin.com/in/danilobazzanella

DANILO BAZZANELLA
Co-founder and Head of the group CrypTO – Cryptography and Number Theory
https://crypto.polito.it

Management activities

- I was a member of the Academic Senate of Politecnico di Torino (2011-2012), as a representative of assistant professors. In that role I was a member of the Research Strategy Commission and the Commission for the Statute of the University.

- I was a member of the Board of Governors (2013-2020). During my tenure I was a member of the Strategic Plan Commission, Student Project and University Fees Commission, Budget Commission, Commission for Monitoring Researchers and Fellows, Staff Planning Commission, Interdepartmental Centers Commission, Commission for Teaching Strategies, Commission for Research Strategies and the General Regulation Commission.

- I am currently a member of the Academic Senate of Politecnico di Torino.

- I am the coordinator of the Commission for the Website of the Department of Mathematical Sciences of Politecnico di Torino.

- I am the co-founder and actually the head of the research group CrypTO (https://crypto.polito.it/), the research group of Cryptography and Number Theory of the Department of Mathematical Sciences of Politecnico. The activities of the group concern teaching (courses for the master's degree, for the Ph. D., thesis, student teams...), research (Symmetric and Asymmetric Cryptography, Post-Quantum Cryptography, Cryptanalysis, Blockchain, Number Theory...), dissemination (series of seminars and conferences) and technology transfer (projects in collaboration with technology companies).

- I am a founding member of the association De Componendis Cifris - Italian Association of Cryptography (https://www.decifris.it).

Scientific activities

My research field is Number Theory and its application to Cryptography. In the early years my research was mainly oriented towards the distribution of prime numbers and additive diophantine problems with primes.

In recent years I have shifted my attention to the applications of Number Theory to Cryptography and in particular to Post-Quantum Cryptography, Cryptanalysis and the Blockchain technology.

I am a member of UMI (Italian Mathematical Union) and of "Cryptography and codes" UMI group (https://umi.dm.unibo.it/gruppi-umi-2/gruppo-umi-crittografia-e-codici/).

I am a member of GNSAGA – Gruppo Nazionale per le Strutture algebriche, geometriche e le loro applicazioni of INDAM - Istituto Nazionale di Alta Matematica "Francesco Severi".

I am a co-founder and a member of the De Componendis Cifris – Associazione nazionale di crittografia (https://www.decifris.it).

Politecnico di Torino – Corso Duca degli Abruzzi 24, 10129 - Torino, Italy
danilo.bazzanella@polito.it – https://crypto.polito.it/danilo_bazzanella
www.linkedin.com/in/danilobazzanella

DANILO BAZZANELLA
Co-founder and Head of the group CrypTO – Cryptography and Number Theory
https://crypto.polito.it

I am a director of the node CrypTO of the Cybersecurity National Lab (https://cybersecnatlab.it).

I am a member of the scientific committee of Book series "Crittografia" (https://www.aracneeditrice.eu/it//collana/crittografia-book-series.html).

I am a referee of various Number Theory and Cryptography Journals.

Research projects

- Name of the project: "Crittografia Post-Quantum per applicazioni cloud"
Company: Telsy SpA (TIM Group) - https://www.telsy.com/

- Name of the project: "Cryptanalysis of ARX ciphers"
Company: DarkMatter - https://www.darkmatter.ae

- Name of the project: "Cryptanalysis of multivariate-based cryptosystems and Machine learning applied to cryptanalysis"
Company: TII - Technology Innovation Institute - https://tii.ae

- Name of the project: " Design and cryptanalysis of post-quantum signature schemes and Automatic methods for key recovery attacks in symmetric ciphers "
Company: TII - Technology Innovation Institute - https://tii.ae

- Name of the project: "Design di piattaforme decentralizzate user-rewarding"
Company: SEA Soluzioni Eco Ambientali - https://www.seaeco.it

- Name of the project: "Design di piattaforme decentralizzate user-rewarding"
Company: SEA Soluzioni Eco Ambientali - https://www.seaeco.it

- Name of the project: "Applicazioni della tecnologia blockchain in ambito industriale"
Company: TurinTech - https://www.turintech.it/

- Cryptanalysis of Post-Quantum Digital Signatures Candidates and Automated Cryptanalysis of Symmetric Primitives - TII (Technology Innovation Institute) - https://tii.ae

- QUBIP (Quantum-oriented Update to Browsers and Infrastructure for the PQ Transition) - Horizon Europe Framework Programme (HORIZON)

- STRIDE (Secure and TRaceable Identities in Distributed Environments) - Partenariato Esteso PNRR - Spoke 5 del progetto Cybersecurity, nuove tecnologie e tutela dei diritti Security and Rights in the CyberSpace (SERICS) - https://serics.eu

Politecnico di Torino – Corso Duca degli Abruzzi 24, 10129 - Torino, Italy
danilo.bazzanella@polito.it – https://crypto.polito.it/danilo_bazzanella
www.linkedin.com/in/danilobazzanella

DANILO BAZZANELLA
Co-founder and Head of the group CrypTO – Cryptography and Number Theory
https://crypto.polito.it

I have research and dissemination collaborations with various companies: Telsy SpA, Quadrans Foundation, Foodchain, INRiM - Istituto Nazionale di Ricerca Metrologica, Young Platform, Thales - Alenia Space, ST Microelectronics… (https://crypto.polito.it/en/partners).

I was a member of the following PRIN projects:

- Geometria Algebrica - Coordinator: Pedrini C. (1998-2000)
- Funzioni L e Numeri Primi - Coordinator: Perelli A. (2000-2003)
- Funzioni L e Problemi Diofantei Additivi - Coordinator: Perelli A. (2002-2004)
- Funzioni L e Problemi Diofantei Additivi - Coordinator: Perelli A. (2004-2006)
- Teoria Analitica dei Numeri e Funzioni L - Coordinator: Zannier U. (2007-2009)
- Funzioni L e Problemi Analitici in Teoria dei Numeri - Coordinator: Zannier U. (2010-2012)
- Geometria Algebrica Aritmetica e Teoria dei Numeri - Coordinator: Chiarellotto B. (2013-2016)

Dissemination

- Conference "CrypTO Conference – Torino 2023" (https://crypto.polito.it/conference).

- Periodic conferences named "Number Theory Meeting" (http://ntmeeting.polito.it), dedicated to number theory and its applications, in years 2016-2023. Next event scheduled for September 2024.

- Conference "CrypTO Conference – Torino 2021" (https://crypto.polito.it/crypto_conference/crypto_conference_2021).

- "Cryptography and Coding Theory", Annual Conference of UMI Group Cryptography and Coding Theory (https://sites.google.com/view/crittografiaecodici/convegno-2021)

- Series of seminars "CRYPTOGRAPHY: From Theory to Applications", in collaboration with Telsy SPA, a company of the TIM group specialized in cybersecurity (https://crypto.polito.it/en/eventi/crittografia_dalla_teoria_alle_applicazioni).

- Series of seminars "De Cifris Augustae Taurinorum", in collaboration with the national cryptography association De Componendis Cifris, Telsy SpA and Quadrans Foundation (https://crypto.polito.it/en/eventi/seminari_di_de_cifris_augustae_taurinorum).

- I was one of the organizers of the "Second Symposium on Analytic Number Theory" - Cetraro, 8-12 July 2019 (https://www.dima.unige.it/ant/symposium/).

Pubblications

- D. Bazzanella "Codici a Chiave Pubblica ed Algoritmi di Fattorizzazione", Master's Degree Thesis (1989 Univ. Genova) - Tutor: Prof. A. Perelli.
- D. Bazzanella "Primes in almost all short intervals",Boll. U.M.I.(7), 9-B (1995), 233-249.
- D. Bazzanella "Il Metodo delle Coppie di Esponenti ed Applicazioni", Ph. D. Thesis (1995 Univ. Genova) - Tutor: Prof. A. Perelli.
- D. Bazzanella, A. Perelli "The exceptional set for the number of primes in short intervals", Journal of Number Theory 80 (2000) n.1, 109-124.
- D. Bazzanella, A. Languasco "On the asymptotic formula for Goldbach numbers in short intervals",

DANILO BAZZANELLA
Co-founder and Head of the group CrypTO – Cryptography and Number Theory
https://crypto.polito.it

Stud. Sci. Math. Hung. 36 (2000) n.1-2, 185-199.
- D. Bazzanella "Primes in almost all short intervals II", Boll. U.M.I. (8) 3-B (2000), 717-726.
- D. Bazzanella "Primes between consecutive squares", Arch. Math. (Basel) 75 (2000) n.1, 29-34.
- D. Bazzanella, P. Boieri, L. Caire, A. Tabacco "Serie di Funzioni e trasformate" CLUT (2001).
- D. Bazzanella "Prime numbers between squares",Riv. Mat. Univ. Parma (7) 3* (2004), 159-164.
- D. Bazzanella "The exceptional set for the distribution of primes between consecutive powers", Acta Math. Hungar. 116 (3) (2007), 197-207.
- D. Bazzanella "A note on primes in short intervals", Arch. Math. (Basel) 91 (2008) n. 2, 131-135.
- D. Bazzanella "Primes between consecutive powers", Rocky Mountain J. Math. 39 (2009), n. 2, 413-421.
- D. Bazzanella "A note on primes between consecutive powers", Rend. Semin. Mat. Univ. Padova 121 (2009) 223-231.
- D. Bazzanella "Prime numbers in intervals starting at a fixed power of the integers", J. Australian Math. Soc. 87 (2009) 83-99.
- D. Bazzanella, A. Languasco, A. Zaccagnini "Prime numbers in logarithmic intervals", Transactions of the American Mathematical Society 362 (2010), n. 5, 2667-2684.
- D. Bazzanella "Two conditional results about primes in short intervals", Int. J. Number Theory 7 (2011), n. 7, 1753-1759.
- D. Bazzanella "On the divisor function in short intervals", Arch. Math. (Basel) 97 (2011), n. 5, 453-458.
- D. Bazzanella "Some conditional results on primes between consecutive squares", Funct. Approx. Comment. Math. 45, n. 2 (2011), 255-263.
- D. Bazzanella "Primes between consecutive squares and the Lindelöf hypothesis", Period. Math. Hungar. 66, n. 1 (2013), 111-117.
- D. Bazzanella "Conditional results about primes between consecutive powers", Riv. Mat. Univ. Parma 4, n. 1 (2013), 61-69.
- D. Bazzanella "A note on integer polynomials with small integrals", Acta Math. Hungar. 141 (2013), n. 4, 320-328.
- D. Bazzanella, R. Camerlo "The class of the exceptional sets for a general asymptotic formula", Funct. Approx. Comment. Math. 51 (2014), n. 2, 347-362.
- D. Bazzanella "A note on integer polynomials with small integrals. II", Acta Math. Hungar. 149 (2016), n. 1, 71-81.
- D. Bazzanella "Integer polynomials with small integrals", Riv. Mat. Univ. Parma, vol 7 (2016), n. 1, 165-179.
- D. Bazzanella, C. Sanna "Least common multiple of polynomial sequences", Rendiconti del Seminario Matematico, vol. 78 (2020), n. 1, 21-25.
- D. Bazzanella, A. Di Scala, S. Dutto, N. Murru "Primality tests, linear recurrent sequences and the Pell equation", The Ramanujan Journal (2021).
- D. Bazzanella, S. Bettin, A. Perelli, A. Zaccagnini, "Proceedings of Second Symposium on Analytic Number Theory" Cetraro (2021).
- D. Bazzanella, T. Serra, A. Tagliaferro, "Integers in a Rational Sequence", Rendiconti Sem. Mat. Univ. Pol. Torino Vol. 79, 2021 (2021), 25-29.
- S. Barbero, D. Bazzanella, E. Bellini, "Rotational cryptanalysis in the presence of constants applied to ChaCha stream cipher", Symmetry (2022).
- S. Barbero, D. Bazzanella, L. Capuano, A. Mori, N. Murru, C. Sanna, "Proceedings of 5th Number Theory Meeting" Torino (2022).
- D. Bazzanella, A. Gangemi, "Bitcoin: a new proof-of-work system with reduced variance", Financial Innovation 9, 91 (2023).