***Curriculum Vitae***

Dr. Sugata Gangopadhyay

Associate Professor

Department of Computer Science and Engineering

Indian Institute of Technology Roorkee

Personal details: Date of birth: 3rd February 1970; Indian; Male.

Phone: +91 9411153198 (Mobile).

Email: [gsugata@gmail.com](mailto:gsugata@gmail.com), [sugatfma@iitr.ac.in](mailto:sugatfma@iitr.ac.in)

***Education***

* 1998. Ph.D.Indian Institute of Technology, Kharagpur.

Area of research: Algebra.

Title of the Ph.D. thesis: “On Units in Group Rings”.

* 1993. M.Sc. (Mathematics)Indian Institute of Technology, Kharagpur.
* 1991. B.Sc. (Mathematics honours)

St. Xavier's College, University of Calcutta.

***Awards***

1. Awarded Silver Medal and General Proficiency Prize by IIT Kharagpur in the year 1993 for securing 1st position in M.Sc. Mathematics.
2. Outstanding Teacher Award, 2016, IIT Roorkee.

***Professional Experience***

* 2013, 27 September, till date. Department of Computer Science and Engineering, Indian Institute of Technology Roorkee, Associate Professor.
* 2012, 23 October 2012, 26 September. Department of Mathematics, Indian Institute of Technology Roorkee, Associate Professor.
* 2012 January to 22 October 2012. Computer Science Unit, Indian Statistical Institute, Chennai Centre, Associate professor.(On leave with service continuity from IIT Roorkee)
* 2004, 9 July to 2012, 22 October. Department of Mathematics, Indian Institute of Technology Roorkee, Assistant Professor.
* 2004 March to June. Department of Mathematics, Indian Institute of Technology, Kharagpur, Assistant Professor.
* 1999 to 2003. Birla Institute of Technology and Science,Pilani,IndiaLecturer in Mathematics.
* 1997, November to 1998, December, Harish Chandra Research Institute, Allahabad, Visiting Fellow.

***Publications in Journals***

1. Mandal, B., Gangopadhyay, S. and Stanica, P., International Journal of Computer Mathematics: Computer Systems Theory, DOI 10.1080/23799927.2017.1304453.
2. Gangopadhyay, S., Pasalic, E., Stanica, P. and Datta, A note on non-splitting -bent functions, Information Processing Letters 121(2017) 1 - 5.
3. Pasalic, E., Muratovic-Ribic, A., Hodzic, S. and Gangopadhyay, S., On derivatives of polynomials over finite fields through integration, Discrete Applied Mathematics, 217(2017) 294 - 303.
4. Gangopadhyay, S., Kar Gangopadhyay, A.,Pollatos, S. and Stanica, P., Cryptographic Boolean functions with biased inputs, Cryptography and Communications – Discrete Structures, Boolean functions and Sequences 9(2): 301-314(2017).
5. Gangopadhyay, S., Singh, B. and Vetrivel, V., Investigations on cubic rotation symmetric bent functions, Electronic Notes in Discrete Mathematics 56(2016) 15 - 19.
6. Mandal, B., Stanica, P., Gangopadhyay, S., Pasalic, E., An Analysis of Class of Bent Functions, Fundamenta Informaticae, 146(3) (2016) 271 - 292.
7. Gangopadhyay, S., and Mandal, B., Second-Order Nonlinearity Bounds of Cubic MMF Bent-Negabent Functions Constructed by Using Feistel Functions, in special issue for “Cryptology and Cyber-Security”, the IPSI BgD Transactions on Advanced Research, vol. 11, no. 1, 13 – 19 (2015).
8. Gangopadhyay, S., and Sharma, D., A Note on the Structure of 6-Variable Bent Functions, inspecial issue for “Cryptology and Cyber-Security”, the IPSI BgDTransactions on Advanced Researchvol. 11, no. 1, 20 – 24 (2015)
9. Bajric, S., Pasalic, E., Ribic-Muratovic, A. and Gangopadhyay, S., On generalized bent functions with Dillon’s exponents, Information Proc. Letters, 114: 222 – 227 (2014).
10. Artamonov, V. A., Chakrabarti, S. Gangopadhyay, S and Pal, S. K., On Latin squares of polynomially complete quasigroups generated by shifts, Quasigroups and related systems 21: 117 – 130 (2013).
11. Gangopadhyay, S., Pasalic, E. and Stanica, P., A note on generalized bent criteria for Boolean functions, IEEE Trans. Inform. Theory 59(5):3233 – 3236 (2013).
12. Gangopadhyay, S., Affine inequivalence of cubic Maiorana--McFarland type bent functions, Discrete Applied Mathematics 161(7-8): 1141–1146 (2013).
13. Gangopadhyay S., Joshi A., Leander G. and Sharma R. K., A new construction of bent functions based on -bent functions, Des. Codes Cryptogr. 66(1-3): 243 – 256 (2013).
14. Stanica P, Martinsen T., Gangopadhyay S. and Singh B. K.,Bent and generalized bent Boolean functions,Des. Codes Cryptogr. 69(1):77 – 94(2013).
15. Mihaljevic M., Gangopadhyay S., Paul G. and Imai H.,Internal State Recovery of Keystream Generator LILI-128 Based on aNovel Weakness of the Employed Boolean Function Information Processing Letters, 112(21):805 – 810 (2012).
16. Mihaljevic M., Gangopadhyay S., Paul G. and Imai H., Generic Cryptographic Weakness ofk-normal Boolean Functions in Certain Stream Ciphersand Cryptanalysis of Grain-128, Periodica Mathematica Hungarica 65(2):39 – 61 (2012).
17. Stanica P., Gangopadhyay S., Chaturvedi A., Kar Gangopadhyay A. and MaitraS., Investigations on bent and negabent functions via the nega-Hadamard transform, IEEE Trans. Inform. Theory 58(6):4064 – 4072 (2012).
18. Gangopadhyay S. and Singh B. K.,On second-order nonlinearities of some type bent functions, Fundamenta Informaticae 114(3 – 4):271 – 285 (2012).
19. Mihaljevic M., Gangopadhyay S., Paul G. and Imai H., Internal State Recovery of Grain-v1 Employing Normality Order of the Filter Function, IET Information Security 6(2): 55 – 64 (2012).
20. Garg M. and Gangopadhyay S., A lower bound of the second-order nonlinearities of Boolean bent functions, Fundamenta Informaticae 111(4): 413 – 422 (2011).
21. Gode R. and Gangopadhyay S., On lower bounds of second-order nonlinearities of cubic bent functions constructed by concatenating Gold functions, International Journal of Computer Mathematics 88(15):3125 – 3135 (2011).
22. Canright D., Gangopadhyay S., Maitra S. and Stanica P., Laced Boolean functions and subset sum problem in finite fields, Discrete Applied Mathematics 159 (11): 1059 – 1188 (2011).
23. Gode R. and Gangopadhyay S., Third-order nonlinearities of a subclass of Kasami functions, Cryptography and Communications - Discrete Structures, Boolean Functions and Sequences2: 69 – 83 (2010).
24. Gode R. and Gangopadhyay S., On higher-order nonlinearities of monomial partial spreads type Boolean functions, Journal of Combinatorics, Information and System Sciences 35(3 – 4): 341 – 360 (2010).
25. Gangopadhyay S., Sarkar S. and Telang R., On the lower bounds of second order nonlinearities of some Boolean functions, Information Sciences 180: 266--273 (2010).
26. Gangopadhyay S., Sharma D., Sarkar S., MaitraS.,On Affine (Non) Equivalence of Bent Functions, Computing85: 37 – 55 (2009).
27. Maitra S., Subba Rao Y. V., Stanica P., GangopadhyayS.,Non trivial solutions to cubic seive congruence problems: , Special Issue on Applied Cryptography \& Data Security, Journal of “Computacion y Sistemas”, 12(3): 253 – 266 (2009).
28. Gangopadhyay S., Sharma D.,On construction of non-normal Boolean functions,Australasian journal of combinatorics38: 267 – 272 (2007).
29. Gangopadhyay S., Keskar P. H., MaitraS.,Patterson - Wiedemann construction revisited, Discrete MathematicsVol. 306, Issue 14, pp. 1540 – 1556, 2006.
30. Sharma R. K., GangopadhyayS.,On congruence subgroups and units in ,Communications in Algebra 32(2): 663 – 668 (2004).
31. Gangopadhyay S., A note on character sums with polynomial arguments,Finite Fields and Their Applications 9(4): 449 – 457 (2003).
32. Sharma R. K., Gangopadhyay S., On Units in , Pan American MathematicalJournal 2(1): 1 – 9 (2001).
33. Sharma R. K., Gangopadhyay S., On Chains in Units of , Mathematical Sciences Research Hotline 4(9): 1 – 33 (2000).
34. Sharma R. K., Gangopadhyay S., On Units in , Mathematical Sciences Research Hotline 4(8): 13 – 29 (2000).
35. Sharma R. K., Gangopadhyay S., V. Vetrivel, On Units in Communications in Algebra 25(7): 2285 – 2299 (1997).

***Papers presented in conferences***

1. Gangopadhyay S., Singh B. and Vetrivel V, Investigations on cubic rotation symmetric bent

functions, 1st IMA Conference on Theoretical and Computational Discrete Mathematics, 22

-23 March 2016, University of Derby UK.

1. Gangopadhyay S.,Pasalic E. and Singh B. K., On upper bounds on algebraic immunity of some and Niho bent functions, 8th International Conference on Communications and Networking in China, August 14 – 16, 2013, Guilin, People’s Republic of China.
2. GangopadhyayS., Gowers norm of cubic bent Boolean functions, Fq11, The 11th International Conference on Finite Fields and their Applications, Magdeburg, Germany, July 22 – 26, 2013.
3. Mihaljevic M. J., Gangopadhyay S., Paul G. and Imai H., An Algorithm for the Internal State Recovery ofGrain-v1, presented in the 11th Central European Conference on Cryptology, Debrecen, Hungary, 30 June to 2 July, 2011.
4. Gangopadhyay, S., Joshi A,, Leander G. and Sharma R. K., A new construction of bent functions based on -bent functions. In: the proceedings of ``The Seventh International Workshop on Coding and Cryptography 2011". April 11 - 15, 2011, Paris, France, pp. 153 – 162.
5. Mihaljevic M. J., Gangopadhyay S., Paul G. and Imai H., A Generic Weakness of the $k$-normal Boolean FunctionsExposed to Dedicated Algebraic Attack, 2010 Int. Symp. OnInform. Theory and its Appl. - ISITA 2010, Taichung,Taiwan, Oct. 17-20, 2010, IEEE Proceedings, pp. 911-916.(IEEE Catalog Number: CFP 10767-USB, ISBN: 078-1-4244-6014-4,ISSN: 1943-7439)
6. Stanica P., Gangopadhyay S., ChaturvediA. GangopadhyayA. andMaitra S., Nega –Hadamard Transform, Bent and NegabentFunctions, SETA 2010, LNCS 6338, 2010, pp. 359 – 372.
7. Gangopadhyay, S., Singh, B. K. On second-order nonlinearities of some type bent functions, presented in 10th Central European Conference on Cryptology, Bedlewo Poland, 10–12 June, 2010, Pages 17–18.
8. Gangopadhyay S. and Sharma D., A note on the structure of 6-variable bent functions,IMST 2009 - FIM XVIII, Jaypee University of InformationTechnology, Waknaghat, Solan, H.P., India, August 2 - 4, 2009, page 42.
9. Telang R. and Gangopadhyay S., On higher-order nonlinearity of monomialpartial-spreads type Boolean functions,IMST 2009 - FIM XVIII, Jaypee University of InformationTechnology, Waknaghat, Solan, H.P., India, August 2 - 4, 2009, page 79.
10. KarGangopadhyay A., Kulshreshtha P., Gangopadhyay, S, Estimation of regression coefficientsof the selected populations with an application to portfolio theory of corporate finance, IMST 2009 - FIM XVIII, Jaypee University of InformationTechnology, Waknaghat, Solan, H.P., India, August 2 - 4, 2009, page 68.
11. Sarkar S. and GangopadhyayS.,On the Second Order Nonlinearity of a Cubic Maiorana-McFarland Bent Function,Finite Fields and their Applications, Fq 9, Dublin, Ireland, July 13 – 17, 2009.
12. Gangopadhyay S., Sharma D., Sarkar S., MaitraS.,On Affine (Non) Equivalence of Bent Functions, 8th Central European Conferenceon Cryptography, Graz, Austria, July 2 – 4, 2008.

<http://www.math.tugraz.at/\~~cecc08/abstracts/cecc08\_abstract\_25.pdf>

1. Gangopadhyay S., Sharma D.,On a new invariant of Boolean functions, The fourteenth International Conferenceof the Forum for Interdisciplinary Mathematics, Chennai, India, January 6 – 8, 2007, page108.
2. Carlet C., Gangopadhyay S., Maitra S.,Crosscorrelation spectra of Dillon type functions,The second international workshop on sequence design and its applicationin communications IWSDA'05, Shimonoseki, Yamaguchi, Japan, October 10 – 14, 2005, pp. 24 – 28.
3. Gangopadhyay S., MaitraS.,Further results related to Generalized Nonlinearity,Third International Conference on Cryptology in India, INDOCRYPT 2002,Hyderabad, India, December 16-18, 2002. Published inLecture Notes in Computer Science, (Springer-Verlag), Vol. 2551, 2002, pp. 260 – 274.
4. Gangopadhyay S., Keskar, P. H., Maitra S., Patterson-Wiedemann construction revisited,R.C. Bose Centenary Symposium on Discrete Mathematics and Applications, Kolkata, India, December 20 – 23, 2002. Electronic notes in Discrete Mathematics - Elsevier, Vol. 15.

***Invited talks:***

1. India-Russia workshop on Number Theory, Combinatorics, Cryptology Moscow State University 15 – 17 October 2014.
2. Guest lecture entitled “Normality of Boolean functions and its impact on stream cipher cryptanalysis” in a workshop under the Information Security and Education and Awareness at the department of Computer Science and Engineering, Indian School of Mines, Dhanbad, 15 March 2014.
3. Three lectures entitled “Boolean and Vectorial Boolean Functions, Cryptographically strong Boolean Functions and Strong S-Box Design” in CEP course between 24 to 28 September 2012 atSAG DRDO New Delhi.
4. “Construction of bent functions based on Z-bent functions”in Coding and Cryptography Research Group (CCRG) seminar series in the School of Physical and Mathematical Sciences, Nanyang Technological University.
5. “Boolean functions in cryptology” in the tutorial workshop “Many Facets of Cryptology”, jointly organized by the Department of Computer Science & Engineering, JadavpurUniversity and the Centre of Excellence in Cryptology, Indian Statistical Institute, to be held during October 14-15, 2011, in the TEQIP building inside the Jadavpur University main campus.
6. “On Dillon and Patterson-Wiedemann type Boolean functions” in1st Indo-French Workshop on Cryptography and Related Topics (IFW), June 11, 2007, Paris, France, organized by the Indo-French Centre for the Promotion of Advanced Research under the Department of Science and Technology (DST), Government of India and the Ministry of Foreign Affairs, Government of France.
7. “Lightweight LFSR based stream ciphers” in Workshop on "Modernisation of Cryptograpahy - Road Ahead" during 27-28 Nov 08 at Center for Artificial Intelligence and Robotics Bangalore for their users (Army, Navy and Airforce).
8. “On Affine Equivalence of Bent Functions” in the workshop on Cryptology – 2008and participated in Cipher Retreat II during 5 - 8 December 2008 in Institute of MathematicalApplications Bhubaneswar.

***Academic visits***

1. 7 to 21 May 2014, Applied Mathematics Department, Naval Postgraduate School, Monterey, California, USA.
2. 20 November to 20 December 2013, Applied Mathematics Department, Naval Postgraduate School, Monterey, California, USA.
3. 23 to 30 March 2013, Research Institute of Secure Systems, National Instituteof Advanced Science and Technology, Tsukuba, Japan.
4. 12 to 23 May 2012,Faculty of Mathematics Natural Sciences and Information Technologies(FAMNIT), University of Primorska, Slovenia.
5. 18 to 23 March 2012, School of Physical and Mathematical Sciences, NanyangTechnological University, Singapore.
6. 5 to 12 November 2011, Faculty of Mathematics Natural Sciences and Information Technologies(FAMNIT), University of Primorska, Slovenia.
7. 2 to 9 October 2011, Research Center for Information Security,National Institute of Advanced Industrial Science and Technology, Tokyo, Japan.
8. 27 February to 7 March 2010, Research Center for Information Security,National Institute of Advanced Industrial Science and Technology, Tokyo, Japan.
9. 1 June 2010 to 19 July 2010, Projet Secret, Institut National deRechercheenInformatiqueetenAutomatique (INRIA) Rocquencourt, France.
10. 1 June 2009 to 20 July 2009, Research Center for Information Security,National Institute of Advanced Industrial Science and Techlogy, Tokyo, Japan.
11. 23 May 2008 to 20 July 2008, Projet Secret, Institut National deRechercheenInformatiqueetenAutomatique (INRIA) Rocquencourt, France.
12. November 2003 to February 2004, Department of Information Technology,University of Lund, Sweden.
13. August 2003 to November 2003, Visiting Scientist, Applied Statistics Unit, Indian Statistical Institute Kolkata.

***Ph.D. Theses Supervised***

1. Deepmala Sharma. Title of the thesis: “On Affine Equivalence of Cryptographically Significant Boolean Functions” (Awarded in 2009).
2. RuchiGode. Title of the thesis: “On Higher-Order NolinearitiesofBoolean Functions” (Awarded in 2011).
3. Manish Garg. Title of the thesis: “Some Results on Lower Bounds of Higher-Order Nonlinearities of Boolean Functions”(Awarded in 2012).
4. Brajesh Kumar Singh. Title of the thesis:”Problems on Boolean Functions and Their Generalization”(Awarded in 2012).
5. AnkitaChaturvedi. Title of the thesis: “Nega-Hadamard Transforms on Boolean and Generalized Boolean Functions” (Awarded 2013).
6. Anand B. Joshi. Title of the thesis: “On Boolean Functions in the Context of Coding Theory and Cryptography” (Awarded 2013).

***Projects:***

1. Project Leader (Indian Side): India-Japan Cooperative Research Project: “Security Evaluation and Design of Components and Cryptographic Primitives for RFID and Sensor Networks”. Funding Agency: Department of Science and Technology (India) and Japan Science and Technology. Indian side financial outlay: INR. 2.9 million.(2009 – 2013 )
2. Project Leader (Indian side): “Cryptographically Significant Boolean Functions with Application in Stream and Block Ciphers”. Funded by - Department of Science and Technology (India), Ministry of Higher Education, Science and Technology Slovenia and Slovenian Research Agency. (2011--2013) Indian side financial outlay: INR. 0.8 million. (2011 – 2014)
3. Project Leader (Indian Side): Indo-Japanese joint research project entitled “Lightweight Encryption Techniques for Cyber Security Applications”, funded by DST - JSPS. Financial outlay: INR. 0.6 million.