Dr. Sugata Gangopadhyay
Associate Professor
Department of Mathematics
Indian Institute of Technology Roorkee

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

Postal Address: Indian Institute of Technology Roorkee
Roorkee - 247667, INDIA
Email: gsugata@gmail.com, sugo@isichennai.res.in

Publications in Journals:

1. Mihaljević M., Gangopadhyay S., Paul G. and Imai H., Internal State Recovery of Keystream Generator LILI-128 Based on a Novel Weakness of the Employed Boolean Function, Information Processing Letters. DOI: 10.1016/j.ipl.2012.07.013.

2. Gangopadhyay S., Joshi A., Leander G. and Sharma R. K., A new construction of bent functions based on $\mathbb{Z}$-bent functions, Des. Codes Cryptogr. DOI 10.1007/s10623-012-9687-1.

3. Mihaljević M., Gangopadhyay S., Paul G. and Imai H., Generic Cryptographic Weakness of k-normal Boolean Functions in Certain Stream Ciphers and Cryptanalysis of Grain-128, Periodica Mathematics Hungarica, vol. 65(2), 2012, pp. 39–61.

4. Stănică P., Gangopadhyay S., Chaturvedi A., Kar Gangopadhyay A. and Maitra S., Investigations on bent and negabent functions via the nega–Hadamard transform, IEEE Trans. Inform. Theory, vol. 58, no. 6, pp. 4064–4072, 2012.

5. Gangopadhyay S. and Singh B. K., On second-order nonlinearities of some $\mathcal{D}_0$ type bent functions, Fundamenta Informaticae, vol. 114(3–4), pp. 271–285, 2012.

6. Stănică P, Martinsen T., Gangopadhyay S. and Singh B. K., Bent and generalized bent Boolean functions, Des. Codes Cryptogr. DOI 10.1007/s10623-012-9622-5.

7. Mihaljević M., Gangopadhyay S., Paul G. and Imai H., Internal State Recovery of Grain-v1 Employing Normality Order of the Filter Function, IET Information Security, vol. 6, no. 2, June 2012.

8. Garg M. and Gangopadhyay S., A lower bound of the second-order nonlinearities of Boolean bent functions, Fundamenta Informaticae, 111(4), pp. 413-422, 2011.

9. 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), pp. 3125-3135, 2011.

10. Canright D., Gangopadhyay S., Maitra S. and Stanica P., Laced Boolean functions and subset sum problem in finite fields, Discrete Applied Mathematics, 159 (11), pp. 1059–1188, 2011.

11. Gode R. and Gangopadhyay S., Third-order nonlinearities of a subclass of Kasami functions, Cryptography and Communications - Discrete Structures, Boolean Functions and Sequences, Vol. 2, pp. 69–83, 2010.

12. Gode R. and Gangopadhyay S., On higher-order nonlinearities of monomial partial spreads type Boolean functions, Journal of Combinatorics, Information and System Sciences, Vol. 35, nos. 3–4, pp. 341–360, 2010.

13. Gangopadhyay S., Sarkar S. and Telang R., On the lower bounds of second order nonlinearities of some Boolean functions, Information Sciences, Vol. 180 pp. 266–273, 2010.

14. Gangopadhyay S., Sharma D., Sarkar S., Maitra S., On Affine (Non) Equivalence of Bent Functions, Computing, Vol. 85, pp. 37–55, 2009.

15. Maitra S., Subba Rao Y. V., Stanica P., Gangopadhyay S., Non trivial solutions to cubic seive congruence problems: $x^3 \equiv y^2 z \mod p$, Special Issue on Applied Cryptography & Data Security, Journal of "Computacion y Sistemas", Vol. 12, No. 3, pp. 253–266, 2009.

16. Gangopadhyay S., Sharma D., On construction of non-normal Boolean functions, Australasian journal of combinatorics, Vol. 38, pp. 267–272, 2007.

17. Gangopadhyay S., Keskar P. H., Maitra S., Patterson - Wiedemann construction revisited, Discrete Mathematics, Vol. 306, Issue 14, pp. 1540–1556, 2006.

18. Sharma R. K., Gangopadhyay S., On congruence subgroups and units in $\mathbb{Z}S_4$, Communications in Algebra, Vol. 32, No. 2, pp. 663–668, 2004.

19. Gangopadhyay S., A note on character sums with polynomial arguments, Finite Fields and Their Applications, Vol. 9, No. 4, pp. 449–457, 2003.

20. Sharma R. K., Gangopadhyay S., On Units in $\mathbb{Z}D_8$, Pan American Mathematical Journal, Vol. 2, No. 1, pp. 1–9, 2001.

21. Sharma R. K., Gangopadhyay S., On Chains in Units of $\mathbb{Z}A_4$, Mathematical Sciences Research Hotline, Vol. 4, No. 9, pp. 1–33, 2000.

22. Sharma R. K., Gangopadhyay S., On Units in $\mathbb{Z}A_4$, Mathematical Sciences Research Hotline, Vol. 4, No. 8, pp. 13–29, 2000.

23. Sharma R. K., Gangopadhyay S., V. Vetrivel, On Units in $\mathbb{Z}S_3$, Communications in Algebra, Vol. 25, No. 7, pp. 2285–2299, 1997.

Papers presented in conferences:

1. Mihaljevic M. J., Gangopadhyay S., Paul G. and Imai H., An Algorithm for the Internal State Recovery of Grain-v1, presented in the 11th Central European Conference on Cryptology, Debrecen, Hugary, 30 June to 2 July, 2011. (Soft copy of the extended abstracts distributed).

2. Gangopadhyay, S., Joshi A,, Leander G. and Sharma R. K., A new construction of bent functions based on $\mathbb{Z}$-bent functions. In: the proceedings of "The Seventh International Workshop on Coding and Cryptography 2011". April 11 - 15, 2011, Paris, France, pp. 153–162.

3. Mihaljevic M. J., Gangopadhyay S., Paul G. and Imai H., A Generic Weakness of the k-normal Boolean Functions Exposed to Dedicated Algebraic Attack, 2010 Int. Symp. on Inform. 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)

4. Stanica P., Gangopadhyay S., Chaturvedi A. Gangopadhyay A. and Maitra S., Nega–Hadamard Transform, Bent and Negabent Functions, SETA 2010, LNCS 6338, 2010, pp. 359–372.

5. Gangopadhyay, S., Singh, B. K. On second-order nonlinearities of some D_0 type bent functions, presented in 10th Central European Conference on Cryptology, Bedlewo Poland, 10–12 June, 2010, Pages 17–18.

6. Gangopadhyay S. and Sharma D., A note on the structure of 6-variable bent functions, IMST 2009 - FIM XVIII, Jaypee University of Information Technology, Waknaghat, Solan, H.P., India, August 2 - 4, 2009, page 42.

7. Telang R. and Gangopadhyay S., On higher-order nonlinearity of monomial partial-spreads type Boolean functions, IMST 2009 - FIM XVIII, Jaypee University of Information Technology, Waknaghat, Solan, H.P., India, August 2 - 4, 2009, page 79.

8. Kar Gangopadhyay A., Kulshreshtha P., Gangopadhyay, S, Estimation of regression coefficients of the selected populations with an application to portfolio theory of corporate finance, IMST 2009 - FIM XVIII, Jaypee University of Information Technology, Waknaghat, Solan, H.P., India, August 2 - 4, 2009, page 68.

9. Sarkar S. and Gangopadhyay S., 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. (Soft copy of the collection of the abstracts distributed).

10. Gangopadhyay S., Sharma D., Sarkar S., Maitra S., On Affine (Non) Equivalence of Bent Functions, 8th Central European Conference on Cryptography, Graz, Austria, July 2-4, 2008. http://www.math.tugraz.at/˜ cecc08/abstracts/cecc08_abstract_25.pdf

11. Gangopadhyay S., Sharma D., On a new invariant of Boolean functions, The fourteenth International Conference of the Forum for Interdisciplinary Mathematics, Chennai, India, January 6-8, 2007, page108,

12. Carlet C., Gangopadhyay S., Maitra S., Crosscorrelation spectra of Dillon type functions, The second international workshop on sequence design and its application in communications IWSDA'05, Shimonoseki, Yamaguchi, Japan, October 10-14, 2005, pp. 24-28.

13. Gangopadhyay S., Maitra S., Further results related to Generalized Nonlinearity, Third International Conference on Cryptology in India, INDOCRYPT 2002, Hyderabad, India, December 16-18, 2002. Published in Lecture Notes in Computer Science, (Springer-Verlag), Vol. 2551, 2002, pp. 260–274.

14. 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.