



Dr. Angsuman Das

Assistant Professor
Department of Mathematics
Presidency University
86/1, College Street,
Kolkata - 700073, West Bengal, India

E-mail: angsuman.maths@presiuniv.ac.in

Webpage: <https://sites.google.com/site/angsumancrypto/>

1 Education:

Ph.D., Cryptography, 2014.

- Institute: Department of Pure Mathematics, University of Calcutta.
- Area of Specialization: *Public Key Cryptography, Secret Sharing Schemes*
- Thesis Proposal: *On Some Mathematical Aspects of Security Notions and Constructions of Public Key Cryptosystems and Secret Sharing Schemes.*
- Advisor: Dr. Avishek Adhikari

M.Sc., Pure Mathematics, 2008.

- Subject Specialization: *Primality & Cryptography, Non-commutative Rings & Modules*
- Institute: Department of Pure Mathematics, University of Calcutta.

B.Sc., Mathematics, 2006

- Subjects credited: *Mathematics, Physics, Chemistry*
 - Institute: St. Xavier's College, Kolkata, India.
-

2 Teaching and Research Experience:

- **Assistant Professor** September, 2018 to present
Department of Mathematics,
Presidency University, Kolkata
- **Assistant Professor** January, 2015 to August, 2018
Department of Mathematics,
St. Xavier's College, Kolkata
- **Assistant Professor** January, 2011 to December, 2014
Department of Mathematics and Statistics,
St. Xavier's College (Evening)

- **Senior Research Fellow** December 2010 to January 2011
Department of Pure Mathematics,
University of Calcutta
 - **Junior Research Fellow** December 2008 to November 2010
Department of Pure Mathematics,
University of Calcutta
 - **Junior Research Fellow** August 2008 to November 2008
Department of Mathematics,
Harish Chandra Research Institute
Allahabad, India.
-

3 Academic Publications: (*in reverse chronological order*)

3.1 Algebra and Graph Theory

3.1.1 Journal Publications

1. Manideepa Saha, **Angsuman Das**, Ece Yetkin Celikel & Cihat Abdioglu, Prime Ideal Sum Graph of a Commutative Ring, *To appear in **Journal of Algebra and its Applications***. (SCI Indexed Journal)
2. Manideepa Saha, Sucharita Biswas & **Angsuman Das**, On comaximal subgroup graph of \mathbb{Z}_n , *To appear in **International Journal of Group Theory***.
3. **Angsuman Das**. On Neighbourhood Graphs: Domination, Colouring and Other Properties. *To appear in **Discrete Mathematics, Algorithms and Applications***.
4. Sucharita Biswas, **Angsuman Das** & Manideepa Saha. Generalized Andrasfai Graphs. *To appear in **Discussiones Mathematicae - General Algebra and Applications***.
5. Ece Yetkin Celikel, **Angsuman Das** & Cihat Abdioglu, Ideal Based Quasi Zero Divisor Graph, **Hacetatepe Journal of Mathematics and Statistics**, Volume 50 (6), pp. 1658-1666, 2021.
6. Sucharita Biswas & **Angsuman Das**. A Family of Tetravalent Half-Arc-Transitive Graphs. **Proceedings - Mathematical Sciences**, Volume 131, Issue 2, Article 28, 2021, Springer. (SCI Indexed Journal)
7. K. Wahid, **Angsuman Das**, A. Rani, S. Amanat, M. Imran & Usman Ali. On Twin Preserving Spanning Subgraph, **Journal of Intelligent and Fuzzy Systems**, Volume 40, Number 5, pp. 9505-9513, 2021.
8. **Angsuman Das** & Arnab Mandal, Classification of Cayley Rose Window Graphs, **Theory and Applications of Graphs**, Volume 8, Issue 1, Article 7, 2021.

9. **Angsuman Das.** Connected Domination Value in Graphs. **Electronic Journal of Graph Theory and Applications**, Volume 9, Issue 1, pp. 113-123, 2021.
10. **Angsuman Das.** Triameter of Graphs. **Discussiones Mathematicae Graph Theory**, Volume 41, Issue 2, pp. 601-616, 2021. (SCI Indexed Journal)
11. Bedanta Bose & **Angsuman Das.** Graph Theoretic Representation of Rings of Continuous Functions. **Filomat**, Volume 34, Issue 10, pp. 3417-3428, 2020. (SCI Indexed Journal)
12. **Angsuman Das** & Manideepa Saha. Determining Number of Some Families of Cubic Graphs. **Journal of Algebra and Related Topics**, Volume 8, Number 2, pp. 39-55, 2020.
13. **Angsuman Das.** Paley-type graphs of order a product of two distinct primes. **Algebra and Discrete Mathematics**, Volume 28, Issue 1, pp. 44-59, 2019.
14. **Angsuman Das.** Partial Domination in Graphs. **Iranian Journal of Science and Technology, Transactions A: Science**, Springer, Volume 43, Issue 4, pp. 1713-1718, 2019. (SCI Indexed Journal)
15. Cihat Abdioglu, Ece Yetkin Celikel & **Angsuman Das.** The Armendariz Graph of a Ring. **Discussiones Mathematicae - General Algebra and Applications**, Volume 38, Issue 2, pp. 189-196, 2018.
16. **Angsuman Das** & Wyatt J. Desormeaux. Domination Defect in Graphs: Guarding with fewer Guards. **Indian Journal of Pure and Applied Mathematics**, Volume 49, Issue 2, pp. 349-364, June, 2018. (SCI Indexed Journal)
17. **Angsuman Das**, Renu C. Laskar and Nader J. Rad: On α -Domination in Graphs, **Graphs and Combinatorics**, Volume 34, Issue 1, 193-205, 2018. (SCI Indexed Journal)
18. **Angsuman Das.** On Perfectness of Intersection Graph of Ideals of Z_n . **Discussiones Mathematicae - General Algebra and Applications**, Vol 37, No. 2, 119-126, 2017.
19. **Angsuman Das.** On Subspace Inclusion Graph of a Vector Space, **Linear and Multilinear Algebra**, Taylor and Francis, Volume 66, Issue 3, 554 -564, 2018. (SCI Indexed Journal)
20. **Angsuman Das.** Infinite Graphs with Finite Dominating Sets. **Discrete Mathematics, Algorithms and Applications**, World Scientific, Volume 9, Issue 4, August 2017.
21. **Angsuman Das.** Coefficient of Domination in Graph. **Discrete Mathematics, Algorithms and Applications**, World Scientific, Volume 9, Issue 2, April 2017.
22. **Angsuman Das.** Non-zero Component Union Graph of a Finite Dimensional Vector Space. **Linear and Multilinear Algebra**, Volume 65, Issue 6, 1276-1287, 2017, Taylor and Francis. (SCI Indexed Journal)

23. **Angsuman Das.** On Non-zero Component Graph of Vector Spaces over Finite Fields. **Journal of Algebra and its Applications**, Volume 16, Issue 01, January 2017, World Scientific. (SCI Indexed Journal)
24. **Angsuman Das.** Subspace Inclusion Graph of a Vector Space. **Communications in Algebra**, Vol. 44, Issue 11, 2016, 4724-4731, Taylor and Francis. (SCI Indexed Journal)
25. **Angsuman Das.** Non-Zero Component Graph of a Finite Dimensional Vector Space. **Communications in Algebra**, Vol. 44, Issue 9, 3918-3926, 2016, Taylor and Francis. (SCI Indexed Journal)

3.1.2 Conference Publications

1. **Angsuman Das.** Determining Number of Generalized and Double Generalized Petersen Graph. In M. Changat and S. Das (eds), Algorithms and Discrete Applied Mathematics. *CALDAM 2020*, LNCS Volume 12016, Springer, pp. 131-140, 2020.
2. **Angsuman Das & Wyatt J. Desormeaux.** Connected Fair Domination in Graphs. In Giri D., Mohapatra R., Begehr H., Obaidat M. (eds) Mathematics and Computing. *ICMC 2017*, Communications in Computer and Information Science, Volume 655, 96-102. Springer, Singapore.
3. **Angsuman Das.** Quadratic Residue Cayley Graphs on Composite Modulus. *ICMC 2015*, Springer Proceedings in Mathematics and Statistics, Volume 139, pp. 277-287, 2015.

3.2 Cryptography

3.2.1 Journal Publications

1. **Angsuman Das, Avishek Adhikari & Kouichi Sakurai.** Plaintext Checkable Encryption with Designated Checker. **Advances in Mathematics of Communication**, Volume 9, Issue 1, pp. 37-53, 2015. (SCI Indexed Journal)
2. **Angsuman Das & Avishek Adhikari.** A Note on “On Ciphertext Undetectability”. **Tatra Mountains Mathematical Publications**, Volume 57, Issue 4, 119-121, 2013.
3. **Angsuman Das & Avishek Adhikari.** An efficient IND-CCA2 secure Paillier-based cryptosystem. **Information Processing Letters**, Volume 112, 2012, Pages 885-888, Elsevier. (SCI Indexed Journal)
4. **Angsuman Das & Avishek Adhikari.** An efficient multi-use multi-secret sharing scheme based on hash function. **Applied Mathematics Letters**, Volume 23, Issue 9, September 2010, Pages 993-996, 2010, Elsevier. (SCI Indexed Journal)

3.2.2 Conference Publications

1. **Angsuman Das** & Avishek Adhikari. Plaintext Checkable Signcryption. **ICISS 2015**, LNCS 9478, pp. 324-333, Springer, 2015.
2. Partha Sarathi Roy, **Angsuman Das** & Avishek Adhikari. Computationally Secure Cheating Identifiable Multi-Secret Sharing for General Access Structure. **ICDCIT 2015**, LNCS 8956, pp. 278-287, Springer, 2015.
3. **Angsuman Das**, Partha Sarathi Roy & Avishek Adhikari. Computationally Secure Robust Multi-Secret Sharing for General Access Structure. **ICMC 2015**, Springer Proceedings in Mathematics and Statistics, Volume 139, pp. 123-134, 2015.
4. **Angsuman Das** & Avishek Adhikari. Signcryption with Delayed Identification. **ICMC 2013**, Springer Proceedings in Mathematics and Statistics, Volume 91, pp. 23-39, 2014.
5. **Angsuman Das** & Avishek Adhikari. Signcryption from Randomness Recoverable PKE Revisited. **ICISS 2013**, LNCS 8303, pp. 78-90, Springer, 2013.
6. **Angsuman Das**, Sabyasachi Dutta & Avishek Adhikari. Indistinguishability against Chosen Ciphertext Verification Attack Revisited: The Complete Picture. **ProvSec 2013**, LNCS 8209, pp. 104-120, Springer, 2013.
7. **Angsuman Das** & Avishek Adhikari. An efficient multi-secret sharing scheme. in Proceedings of the *9th National Workshop on Cryptology 2009*, Benison Education, pp 20-22.

3.2.3 Book Chapter

1. **Angsuman Das** & Avishek Adhikari. On Constructions and Security Notions of Public-key Cryptosystems. In *Contemporary Topics in Mathematics and Statistics with Applications, Volume-1*, Asian Books Private Limited, (ISBN 81-8412132-6), 2013.

Submitted Papers/ Work in Progress

1. Angsuman Das and Arnab Mandal: *On Rose Window Graphs which are Cayley*.
2. Angsuman Das and Hiranya Kishore Dey: *On Determining Number of Kneser Graphs*.
3. Sucharita Biswas and Angsuman Das: *Generalized Pappus Graphs*.
4. Angsuman Das, Manideepa Saha and Saba Al-Kaseasbeh: *On Co-Maximal Subgroup Graph of a Group*.

4 Research:

4.1 Research Interests:

Graphs associated with Algebraic Structures, Domination in graphs, Vertex Transitive graphs, Automorphism Group of Graphs.

4.2 Doctoral Students

- Manideepa Saha (Ongoing)
- Sucharita Biswas (Ongoing)

4.3 Research Projects

- **Principal Investigator** in Startup Research Grant (SRG) for project entitled *Vertex transitive graphs and Cayley graphs: Polycirculant Conjecture, Automorphism groups and other problems*, funded by DST-SERB, Government of India, 2019-2021.
- **Co-Principal Investigator** in Major Research Project entitled “*Constructions and Analysis of Some Secret Sharing Schemes and Their Applications Using Mathematical and Statistical Tools*”, funded by *National Board of Higher Mathematics (NBHM), Department of Atomic Energy (DAE), Government of India*, 2014-2017.

4.4 Invited Talks:

- **Obsessed with \mathbb{Z}_n** , in *Analytica 2019*, St. Xavier’s College, Kolkata, India on 20th September, 2019.
- **On Polycirculant Conjecture**, in *International Conference on Discrete Mathematics, ICDM 2019*, Christ University, Bangalore on 9th June, 2019.
- **Groupifiability of Graphs**, in *Department of Mathematics, IIT Hyderabad* on 9th October, 2018.
- **Combinatorics: Random Thoughts**, in *In-Service Course for Post-Graduate Teachers (Mathematics)*, Kendriya Vidyalaya No.1, Saltlake, Kolkata, India on 22nd May, 2018.
- **Graphs defined over Vector Spaces**, in *International Conference on Discrete Mathematics and its Applications, ICDMA 2018, Department of Mathematics, Manonmaniam Sundaranar University, Tirunelveli* from 18-20th January, 2018.
- **Combinatorics: Adventures in Randomness**, in *In-Service Course for Post-Graduate Teachers (Mathematics)*, Kendriya Vidyalaya No.1, Saltlake, Kolkata, India on 28th December, 2017.
- **Coins, Numbers and Games: Random Thoughts on Randomness**, in *Department of Mathematics, Bangabasi Morning College, Kolkata* on 19th December, 2017.
- **Graph Connections: Graphs defined over Vector Spaces**, in *National Level Workshop on Graph Theory: Algebraic and Algorithmic Aspects (GTA3 2016), Department of Mathematics, Aliah University, Kolkata* from 19-24th December, 2016
- **Combinatorics for High School Students**, in *Post Graduate Teachers Training Course*, organized by *Kendriya Vidyalaya Sangathan, New Delhi* in *Kenriya Vidyalaya No. 1, Saltlake, Kolkata* on 20th May, 2017.

4.5 Awards, Grants and Fellowships:

- CIMPA-ICTP Scholarship for attending “Research School on Lattices and applications to cryptography and coding theory” organized by CIMPA-ICTP in HoChiMinh City, Vietnam from 1st August-12th August, 2016.
- DST-SERB Travel grant for attending “ProvSec 2013” organized by UTeM, Malaysia in Melaka, Malaysia from 23rd-25th October, 2013.

- Best Paper Award for a paper entitled “Signcryption with Delayed Identification” in ICMC 2013.
 - CIMPA-UNESCO Scholarship for attending “CIMPA-UNESCO-NEPAL School on Number Theory in Cryptography and its Applications” organized by Kathmandu University, Nepal in Dhulikhel, Nepal from 19th-31st July, 2009.
 - *Late Dr. N.C. Bose Majumder Memorial Best Paper Award* for a paper entitled “On Notions of Security for Group Homomorphic Public Key Cryptosystems” in NSRDMMS-2011.
 - NBHM (PhD) Senior Research Fellowship, 2010, National Board of Higher Mathematics (NBHM), Department of Atomic Energy, Govt. of India.
 - Junior Research Fellowship, Council of Scientific and Industrial Research (CSIR), Govt. of India in 2009.
 - Junior Research Fellowship, Harish Chandra Research Institute (HRI), Allahabad, India in 2008.
 - NBHM (PhD) Junior Research Fellowship, 2008, National Board of Higher Mathematics (NBHM), Department of Atomic Energy, Govt. of India.
 - NBHM (M.Sc) Scholarship, 2008, National Board of Higher Mathematics (NBHM), Department of Atomic Energy, Govt. of India.
 - Ramkrishna Ghosh Memorial Award, 2006, St. Xavier’s College, Kolkata.
-

5 Other Experiences

5.1 Teaching

- Guest Professor, Department of Mathematics, Presidency University, Kolkata (July, 2017 to August, 2018).
- Teaching Assistant for the courses
 - *Primality & Cryptography*, in 2009, 2010, 2012, 2013 & 2014, for M.Sc (2nd yr) students.
 - *Algebra-I*, in 2011, for M.Sc (1st yr) students.

both in Department of Pure Mathematics, University of Calcutta.

5.2 Reviewership of Journals

Mathematical Reviews (American Mathematical Society), *Linear Algebra and its Applications* (Elsevier), *Discrete Applied Mathematics* (Elsevier), *Linear Algebra and its Applications* (Elsevier), *Linear and Multilinear Algebra* (Taylor and Francis), *Journal of Algebra and its Applications* (World Scientific), *Bulletin of Malaysian Mathematical Society* (Springer), *Journal of Systems and Software* (Elsevier), *Computers and Mathematics with Applications* (Elsevier), *Applied Mathematics Letters* (Elsevier), *Security and Communication Networks* (Wiley), *Information Processing Letters* (Elsevier), *Designs, Codes and Cryptography* (Springer), *International Journal of Network Security*, *European Journal of Pure and Applied Mathematics*, *RAIRO - Operations Research*, *Afrika Matematika* (Springer), *Journal of Algebraic Systems*.

5.3 Technical Skills

Languages known: C;

Computing platforms: Sage; Mathematica;