Curriculum Vitae

Dr. Sumit Kumar Debnath
Assistant Professor
Department of Mathematics
National Institute of Technology Jamshedpur
Jamshedpur-831014, Jharkhand, India
Mail id – sd.iitkgp@gmail.com, sdebnath.math@nitjsr.ac.in
Date of Birth- 25/11/1989
Sex(M/F)- M

Academic Qualification -

1. PhD in Cryptology and Network Security from Department of Mathematics, IIT Kharagpur in 2017. Topic: "Design of Privacy Preserving Secure Set Intersection Protocols".
2. M. Sc. in Mathematics (Specialization in Symmetric Key Cryptography) from IIT Kharagpur in 2012. Marks: 9.51 CGPA
3. B. Sc. in Mathematics Honours from University of North Bengal in 2010. Percentage of marks: 74.25 %.
4. Passed Higher Secondary (10+2) in 2007 from West Bengal Council of Higher Secondary Education in Science (School: Balurghat Khadimpur High School, Balurghat). Percentage of marks: 82.86 %.
5. Passed Madhyamik Examinations in 2005 from West Bengal Board of Secondary Education (School: Balurghat Khadimpur High School, Balurghat). Percentage of marks:74%.

Research Experience–

1. Joined in the Department of Mathematics, NIT Jamshedpur as Assistant Professor during June 2018.
2. Worked as Senior Research Fellow, Department of Mathematics, IIT Kharagpur, Kharagpur during June 2014 - July 2017.
   Field of Work: Survey on Electronic Voting, Secure Multi-party computations, Obfuscation, Constrained Pseudorandom Functions, Private Set Operations; Constructing Efficient Private Set Intersection Protocols and their variants; Security Analysis of the designed protocols in existing security models.

3. Worked as Junior Research Fellow, Department of Mathematics, IIT Kharagpur, Kharagpur during June 2012 - June 2014.
   Field of Work: Successful completion of one -year course work (2012-2013); Survey on Elliptic Curve, Edward Curve, Private Set Operations.

Teaching Experience–

1. Number Theory and Cryptography, Discrete Mathematics, Linear Algebra, Integral Transforms, Engineering Mathematics-I, Engineering Mathematics-II and Engineering Mathematics-III (July 2018- March 2021) at NIT Jamshedpur.
2. Mathematics –I as Teaching Assistant at IIT Kharagpur (Autumn 2014-2105).
3. Mathematics –II as Teaching Assistant at IIT Kharagpur (Spring 2014-2015).

Present Position- Assistant Professor, Department of Mathematics, NIT Jamshedpur, Jamshedpur- 831014

Awards-

1. Offered Research Assistant Position at IT Security and Cryptography, Flensburg University, Germany, 2018.
2. Offered Postdoc Researcher Position at School of Computer Science, Guangzhou University, China, 2017.
3. Senior Research Fellowship, Indian Institute of Technology Kharagpur, 2014.
4. Junior Research Fellowship, Indian Institute of Technology Kharagpur, 2012.
5. Qualified All India Gate exam in 2012.
6. Qualified CSIR-Net exam in June 2012.
7. Ranked 2nd in M.Sc. in Mathematics, Indian Institute of Technology Kharagpur, 2012.
8. Got silver medal for securing first class second position in B.Sc. from University of North Bengal, 2010.
9. Awarded University Rank-holder Scholarship by University Grants Commission, 2010.

Sponsored Projects/ Consultancies:

(a) DRDO ER & IPR Research Project (2020-2022) (**Principal Investigator**)
Title: Security Analysis & Development of Multivariate Post-Quantum Cryptography Schemes
Amount – 39.73 Lakhs
Status – On-going

List of Ongoing/Submitted/Awarded Ph.D. dissertations:

Sl. No.	Name of Research Scholar	Research Area	Single/Joint Guidance	Current Status
1	Tanmay Choudhury	Private Set Operations	Single	Thesis Submitted
2	Kunal Dey	Isogeny-Based Cryptography	Single	Ongoing
3	Vikas Srivastava	Multivariate Public Key Cryptography	Single	Ongoing
4	Tapaswini Mohanty	Quantum Cryptography	Single	Ongoing

List of Ongoing/ Submitted/Awarded M.Tech. / M.Sc. dissertations:

Sl. No.	Name of Scholar	Title of Dissertations	Research Area	Single/Joint Guidance	Current Status
1	Aniqua Sabri (M.Sc.)	Electronic Voting System using Blockchain Technology	Electronic Voting	Single	Completed
2	Debabrata Shaw (M.Sc.)	A Study on Quantum Key Distribution Protocols	Quantum Cryptography	Single	Completed
3	Arup Kumar Behera (M.Sc.)	Implementation of RSA Cryptosystem Using Python	RSA Cryptosystem	Single	Completed

Professional Activities:

1. Reviewer of papers for the journal IEEE Transactions on Circuits and Systems II: Express Briefs.
2. Reviewer of papers for the journal Advances in Mathematics of Communications, AIMS.
3. Reviewer of papers for the journal Security and Communication Networks, Wiley.
4. Reviewer of papers for the International Journal on Semantic Web and Information Systems (IJSWIS), IGI Global.
5. Guest Editor for the Special Issue entitled **"**Security and Privacy 2020" in the journal SN Computer Science, Springer.
6. Editor of the Proceedings of 1st International Conference on Security & Privacy (ICSP 2020), Lecture Notes in Electrical Engineering (LNEE), Series Volume 744, Springer: https://www.springer.com/gp/book/9789813367807

A. List of Publications –

Journal:

1. **Vikas Srivastava, Sumit Kumar Debnath*, Pantelimon Stanica and Saibal Kumar Pal:** A multivariate identity-based broadcast encryption with applications to the internet of things. Advances in Mathematics of Communications (accepted), AIMS (SCIE), 2021. Impact factor- 0.935

2. **Sumit Kumar Debnath, Tanmay Choudhury, Pantelimon Stanica, Kunal Dey and Nibedita Kundu*:** Delegating signing rights in a multivariate proxy signature scheme. Advances in Mathematics of Communications (accepted), AIMS (SCIE), 2021. Impact factor- 0.935

3. **Sumit Kumar Debnath, Sihem Mesnager,* Kunal Dey and Nibedita Kundu:** Post-quantum secure inner product functional encryption using multivariate public key cryptography. Mediterranean Journal of Mathematics, Springer (SCIE), 18(5), 1-15, 2021. Impact factor- 1.400

4. **Nibedita Kundu, Sumit Kumar Debnath and Dheerendra Mishra*:** A secure and efficient group signature scheme based on multivariate public key cryptography. Journal of Information Security and Applications, Elsevier (SCIE), 58, 102776, 2021. Impact factor- 3.872

5. **Sumit Kumar Debnath*, Kunal Dey, Nibedita Kundu and Tanmay Choudhury:** Feasible private set intersection in quantum domain. Quantum Information Processing, Springer (SCIE), 20 (1), 1-11, 2021. Impact factor- 2.349

6. **Sumit Kumar Debnath*, Tanmay Choudhury, Nibedita Kundu and Kunal Dey:** Post-quantum secure multi-party private set-intersection in star network topology. Journal of Information Security and Applications, Elsevier (SCIE), 58, 102731, 2021. Impact factor- 3.872

7. **Nibedita Kundu, Sumit Kumar Debnath and Dheerendra Mishra*:** 1-Out-of-2: Post-quantum oblivious transfer protocols based on multivariate public key cryptography. Sadhana, Springer (SCIE), 45(1), 1-12, 2020. Impact factor- 1.188

8. **Sumit Kumar Debnath*, Pantelimon Stanica, Tanmay Choudhury and Nibedita Kundu:** Post-quantum protocol for computing set intersection cardinality with linear complexity, IET Information Security, IET (SCIE), 14 (6), 661-669, 2020. Impact factor- 1.068

9. **Nibedita Kundu, Sumit Kumar Debnath*, Dheerendra Mishra, Tanmay Choudhury**: Post-quantum digital signature scheme based on multivariate cubic problem. Journal of Information Security and Applications, Elsevier (SCIE), 53, 102512, 2020. Impact factor- 3.872

10. **Sumit Kumar Debnath*, Pantelimon Stanica, Nibedita Kundu and Tanmay Choudhury**: Secure and efficient multiparty private set intersection cardinality. Advances in Mathematics of Communications, AIMS (SCIE), 15(2), 365-386, 2020. Impact factor- 0.935

11. **Sumit Kumar Debnath*, Nibedita Kundu and Tanmay Choudhury:** Efficient post-quantum private set intersection protocol. International Journal of Information and Computer Security (accepted), Inderscience (Scopus), 2019.

12. **Sumit Kumar Debnath*:** Provably secure private set intersection with constant communication complexity. International Journal of Cyber Warfare and Terrorism (IJCWT), IGI Global (Scopus), 9 (2), 39-64, 2019.

13. **Sumit Kumar Debnath* and Ratna Dutta:** Towards fair mutual private set intersection with linear complexity. Security and Communication Networks, Wiley (SCIE), 9(11), 1589-1612, 2016. Impact factor- 1.791

Conference:

1. **Vikas Srivastava and Sumit Kumar Debnath**: Cryptanalysis of LRainbow: The Lifted Rainbow Signature Scheme. In the Proceedings of 15th International Conference on Provable Security and Practical Security (ProvSec 2021), LNCS, Springer (accepted).

2. **Ratna Dutta, Sumit Kumar Debnath and Chinmoy Biswas**: Storage Friendly Provably Secure Multivariate Identity-Based Signature from Isomorphism of Polynomials Problem. In the Proceedings of the 18th International Conference on Security and Cryptography (SECRYPT 2021), CCIS, Springer (accepted).

3. **Sumit Kumar Debnath, Kouichi Sakurai, Kunal Dey and Nibedita Kundu**: Secure Outsourced Private Set Intersection with Linear Complexity. 2021 IEEE Conference on Dependable and Secure Computing (DSC), 1-8.

4. **Nibedita Kundu and Kunal Dey and Pantelimon Stanica and Sumit Kumar Debnath and Saibal Kumar Pal**: Post-Quantum Secure Identity Based Encryption from Multivariate Public Key Cryptography. Security and Privacy: Select Proceedings of ICSP 2020, 139, LNEE, Springer.

5. **Sumit Kumar Debnath and Ratna Dutta:** New Realizations of Efficient and Secure Private Set Intersection Protocols Preserving Fairness. In the Proceedings of the 19th International Conference on Information Security and Cryptology (ICISC 2016), LNCS, Volume 10157, Pages 254-284, Springer-Verlag.

6. **Sumit Kumar Debnath and Ratna Dutta:** How to Meet Big Data When Private Set Intersection Realizes Constant Communication Complexity. In the Proceedings of the 18th IEEE Information and Communications Security (ICICS 2016), LNCS, Volume 9977, Pages 445-454, Springer-Verlag.

7. **Sumit Kumar Debnath and Ratna Dutta:** Provably Secure Fair Mutual Private Set Intersection Cardinality Utilizing Bloom Filter. In the Proceedings of the 12th International Conference on Information Security and Cryptology (INSCRYPT 2016), LNCS, Volume 10143, Pages 505-525, Springer-Verlag.

8. **Sumit Kumar Debnath and Ratna Dutta:** Efficient Private Set Intersection Cardinality in the Presence of Malicious Adversaries. In the Proceedings of the 9th International Conference on Provable Security (ProvSec 2015),LNCS, Volume 9451, Pages 326-339, Springer-Verlag.

9. **Sumit Kumar Debnath and Ratna Dutta:** Secure and Efficient Private Set Intersection Cardinality Using Bloom Filter. In the Proceedings of the 18th International Information Security Conference (ISC 2015), LNCS,Volume 9290, Pages 209-226, Springer-Verlag.

10. **Sumit Kumar Debnath and Ratna Dutta:** A Fair and Efficient Mutual Private Set Intersection Protocol from a Two-way Oblivious Pseudorandom Function. In the Proceedings of the 17th International Conference on Information Security and Cryptology (ICISC 2014), LNCS, Volume 8949, Pages343-359, Springer-Verlag.

Book Chapter:

1. **Sumit Kumar Debnath:** Secure Computation of Private Set Intersection Cardinality with Linear Complexity. In Cryptographic Security Solutions for the Internet of Things, IGI Global (2018).

B. Conference/Seminar/Workshop Organized–

1. International Conference on Security & Privacy (ICSP 2020), Organized at the Department of Mathematics, NIT Jamshedpur during November 05-06, 2020. (Convener & Organizing Secretary- Dr. Sumit Kumar Debnath)

2. International Conference on Mathematical Analysis and Applications (MAA 2020), Organized at the Department of Mathematics, NIT Jamshedpur during November 02-04, 2020. (Chairman- Dr. Sumit Kumar Debnath)

3. Short term course on “Introduction to Modern Cryptography”, Organized at the Department of Mathematics, NIT Jamshedpur during July 01-06, 2019. (Coordinator- Dr. Sumit Kumar Debnath)

C. Conference/Seminar Attended –

1. Presented paper in the 2021 IEEE Conference on Dependable and Secure Computing, held in Japan, 2021.

2. Delivered lecture as invited speaker at Two-Day National Webinar on "Recent Development in Mathematics & Its Social Impact", organized by Department of Mathematics, Sukumar Sengupta Mahavidyalaya, Keshpur, West Bengal, during August 08-09, 2020.

3. Delivered lecture as invited speaker at TEQIP-KIT sponsored short term course on "Advanced Topics in Cryptography", organized by Department of Mathematics, IIT Kharagpur, during February 10-14, 2020.

4. Delivered lecture as invited speaker at National Seminar on Advances in Information Communication and Computing (AICC-2018), organized by Department of (CSC/ETC/MTC), GOVERNMENT AUTONOMOUS COLLEGE, Rourkela, on December 24, 2018.

5. Delivered lecture at TEQIP-II sponsored short term course on "Introduction to Cryptography", organized by Department of Mathematics, IIT Kharagpur, during January 27-31, 2017.

6. Attended the Workshop on Blockchain Technology, organized by ISI Kolkata, held in Kolkata, India, 2017.

7. Attended the 17^{th} International Conference on Cryptology (Indocrypt 2016), organized by ISI Kolkata, held in Kolkata, India, 2016.

8. Attended and Presented paper in the 18^{th}IEEE International Conference on Information and Communications Security (ICICS 2016), organized by NTU, held in Singapore, 2016.

9. Attended and Presented paper in the Seminar on Recent Advances in Mathematics, organized by Department of Pure Mathematics, University of Calcutta, India, 2016.

10. Attended and Presented paper in the Seminar on Recent Advances in Mathematics, organized by Department of Pure Mathematics, University of Calcutta, India, 2015.

11. Attended Winter School on Interplay Between Statistics and Cryptology 2014, Applied Statistics Units, ISI, Kolkata, India.

D. Research Interest –

- Quantum Cryptography, Private Set Operations, Secure Multi-party Computation
- Multivariate Public Key Cryptography, Isogeny Based Cryptography
- Lattice-based Cryptography, Post-Quantum Cryptography
- Identity Based Cryptography, Elliptic Curve Cryptography
- Functional Encryption, Crypto-currency, Electronic Voting