

# Suman Ghosh

---

## Curriculum Vitae

*"A person who never made a mistake never tried anything new." — Albert Einstein*

### Personal Information

D.O.B. August 6, 1997  
Gender Male  
Nationality Indian  
Mobile No +91 8250046839  
Email Id 2019mas1020@kgpian.iitkgp.ac.in, tukusg7654@gmail.com  
Address Junbedia, Bankura, West Bengal - 722155

### Education

2021–present **Joint M.Tech-Phd in Computer Science and Data Processing(2<sup>nd</sup> year)**, *Indian Institute of Technology Kharagpur*, Kharagpur, CGPA – 9.38.

2019–2021 **Master of Science(M.Sc.) in Mathematics**, *Indian Institute of Technology Ropar*, Punjab, CGPA – 8.86.

2016–2019 **Bachelor of Science(B.Sc.) in Mathematics**, *Bankura Christian College*, University of Burdwan, Percentage – 73.25%.  
Major in Mathematics with minor in Physics and Chemistry

2016 **Higher Secondary Examination**, *Bankura Christian Collegiate School*, WBCHSE, Percentage – 86.4%.

2014 **Secondary Examination(Madhyamik)**, *Bankura Christian Collegiate School*, WBBSE, Percentage – 84.85%.

### Academic Achievements

2021 **GATE(P.G. entrance) in Mathematics** Secured All India Rank 25

2021 **Obtained 3<sup>rd</sup> position in the final Master Degree Examination** Indian Institute of Technology Ropar

2019 **IIT JAM(M.Sc. entrance) in Mathematics** Secured All India Rank 547

2019 **Obtained 3<sup>rd</sup> position in the final Bachelor Degree Examination** University of Burdwan

## Research Experience

### Research Internship

August,2022– present **The Study of Scalable, Transparent Argument Systems**, supervised by Dr. Ratna Dutta, Indian Institute of Technology Kharagpur.

- Studied Fast Reed Solomon IOP of Proximity(FRI), some arithmetizations namely Algebraic Intermediate Representation(AIR), Algebraic Linking IOP(ALI) and Algebraic Placement and Routing(APR) reduction
- Studied construction of Scalable Transparent IOP of Knowledge(STIK)
- Studied Scalable Transparent Argument of Knowledge(STARK) as a realization STIK and corresponding zero knowledge versions zkSTIK and zkSTARK
- Implementing a STARK proof in C language

### M.Tech Thesis Project

May,2022– present **The Study of Transparent zkSNARK for R1CS**, supervised by Dr. Ratna Dutta, Indian Institute of Technology Kharagpur.

- Studied Interactive Oracle Proof(IOP), IOP of Proximity, Reed Solomon(RS) encoded IOP and Fast Fourier Transformation, Rank-1 Constraint Satisfaction, Merkle Tree
- Learned construction of RS encoded IOP for Lincheck, Rowcheck and Univariate Sumcheck Problem , Conversion of a RS encoded IOP to an arbitrary IOP and IOP for R1CS, Aurora-zkSNARK for R1CS
- Implementing an IOP for R1CS
- Studying other zkSNARKs Ligero,Bulletproof

### M.Sc. Thesis Project

August,2020– June,2021 **The Study of Algebraic Number Theory**, supervised by Dr. Balesh Kumar, Indian Institute of Technology Ropar.

- Studied Field Theory, Galois Theory, Unique factorization into prime ideals and Ramification Index
- Learned two algorithms to compute fundamental units
- Studied Dirichlet Unit Theorem and its application
- Studied Riemann Zeta Functions, Dedekind Zeta Functions, Dirichlet L-function and Dirichlet Class Number Formula

## Technical Skills

Programming Languages Python, C++, C, HTML(basics), CSS(basics)

Technical Softwares MATLAB, L<sup>A</sup>T<sub>E</sub>X

Others Microsoft Office, Microsoft Excel, Microsoft Powerpoint, Adobe Photoshop

Operating Systems Linux, windows

## Relevant Coursework

Theoretical Courses Cryptography and Network Security, Information and Coding Theory, Graph Theory, Theory of Computation

Courses with Lab Data Structure and Algorithms, Database Management System, Operating Systems, System Programming, Programming Language, Elements of Data Science

Mathematics Courses Linear Algebra, Abstract Algebra, Discrete Mathematics, Optimization Techniques, Probability and Stochastic Processes

## Presentation Skills

2022	<b>Introduction to Steganography</b>	<i>M.Tech 2<sup>nd</sup> semester</i>
2021	<b>Decision Tree</b>	<i>M.Tech 1<sup>st</sup> semester</i>
2020	<b>Introduction to Cryptography</b>	<i>M.Sc. 2<sup>nd</sup> semester</i>

## Lingual Skills

English	<b>Medium of education</b>	<i>Conversationally Intermediate TOEFL Score: 82/120 Reading: 22/30, Listening: 17/30 Speaking: 22/30, Writing: 21/30</i>
Bengali	<b>Fluent</b>	<i>mother tongue</i>
Hindi	<b>Intermediate</b>	<i>Conversationally fluent</i>

## Interests

Football	<i>Represented school several times in inter-school football matches</i>
Cricket, VolleyBall, Table Tennis, Carrom	<i>participated in intra-IIT competitions in IIT Ropar</i>
Photography	<i>Nature and Wildlife Photography</i>