Simran Tinani

IT Security Analyst

Contact

- simran.tinani@gmail.com
- +41 76 618 82 71
- Workplace Homepage
- Personal Homepage
- LinkedIn
- GitHub

Personal Information

- DOB: 15 August 1995
- Nationality: Indian

Languages

- English – Native
- German – B2 Proficiency
- Hindi – Mother tongue
- Punjabi – Mother tongue

Teaching and Mentorship

- UZH: Taught courses on Algebra, Elliptic Curves, Convolutional Codes, Cryptography.
- UZH: Co-supervised a master's thesis on uniform hypergraphs and cryptographic secret-sharing access structures.
- Hashbrown: Mentored interns on existing projects, their business impact and relevant knowledge and skills.

Volunteering

- PhD Representative – UZH ZGSM
- President – IISER Alumni Association
- Animal Welfare – SPCA, Chandigarh
- Math Camps – IISER

Other interests

- Literature & Poetry
- Swimming, badminton, hiking
- Writing

References

Available upon request.

Experience

IT Security Analyst
Sep'23 – Present

cnlab security AG

- Design, planning, coordination, documentation of security reviews
- Conceptual and practical aspects of security protocols and cryptographic primitives integrated in IT systems
- Research on post-quantum cryptography, standardization, implementation efforts; authored a comprehensive guide (to be published soon)
- Analysis of web applications— architectural soundness, data flow, authentication and authorization mechanisms
- Source-code level security audits of smart contracts
- Configuration analysis of configurations of infrastructure components including web servers, reverse proxies, and application firewalls
- Analysis of vulnerabilities in accordance with CVE's, CVSS
- Application of standards and regulations: RFC's, NIST, BSI, PCI-DSS
- Development of an internal AI strategy concept; demo on basics of LLM prompting at the cnlab 2024 annual conference https://www.cnlab.ch/fileadmin/documents/Publikationen/2024/cnlab_KI-und-Sicherheit_Prompting_web.pdf

PhD Student and Teaching Assistant
Sep'19 – Aug'23

University of Zürich

- Authored nine research papers, delivered five research talks, served as reviewer, participated in multiple research conferences.
- Collaborated with cryptography department of VBS and Cyber Defence Campus for research.

Coordinator, Cybersecurity Community
Jan'22 – Aug'23

Digital Society Initiative

- Organised and coordinated events and activities, managed member database and website.

Data Scientist
Aug'18 – Jun'19

Hashbrown Systems, India

- Developed a deep learning object detection and tracking model for counting vehicles in a live video feed (White Paper) https://hashbrown.com/blog/ooh/vehicular-counting-using-object-detection-and-object-tracking.
- Developed a model for estimation of advertisement views based on demographic distribution, recalibratable with real data.
- Analyzed stock price trends and developed automated trading models.

Education

DAS in Cybersecurity
Jan'24 – Present

ETH Zürich

Two-year long continuing education degree, pursued with 20% load
Selected courses: Network Security, System Security, Formal Methods in Information Security
Selected projects: Programming the infrastructure (client, server) for automated certificate procurement with ACME (Let's Encrypt); Formal security analysis and proofs of the OTR and PACE protocols using Tamarin Prover

PhD in Mathematics
Sep'19 – Jun'23

University of Zürich

Thesis: *A Study of Algebraic Methods in Asymmetric Cryptography link*.
Successfully defended on 9 June 2023
Advisor: Prof. Joachim Rosenthal

BS-MS Dual Degree in Mathematics
Aug'13 – May'18

IISER Mohali

Cumulative Index: 9.8/10 *Summa Cum Laude*. Master's Thesis: *A Study of Quadratic Number Fields* link

Contact

- simran.tinani@gmail.com
- +41 76 618 82 71
- Workplace Homepage
- Personal Homepage
- LinkedIn
- GitHub

Personal Information

- DOB: 15 August 1995
- Nationality: Indian

Languages

- English – Native
- German – B2 Proficiency
- Hindi – Mother tongue
- Punjabi – Mother tongue

Teaching and Mentorship

- UZH: Taught courses on Algebra, Elliptic Curves, Convolutional Codes, Cryptography.
- UZH: Co-supervised a master's thesis on uniform hypergraphs and cryptographic secret-sharing access structures.
- Hashbrown: Mentored interns on existing projects, their business impact and relevant knowledge and skills.

Volunteering

- PhD Representative – UZH ZGSM
- President – IISER Alumni Association
- Animal Welfare – SPCA, Chandigarh
- Math Camps – IISER

Other interests

- Literature & Poetry
- Swimming, badminton, hiking
- Writing

References

Available upon request.

Contact

- simran.tinani@gmail.com
- +41 76 618 82 71
- Workplace Homepage
- Personal Homepage
- LinkedIn
- GitHub

Personal Information

- DOB: 15 August 1995
- Nationality: Indian

Languages

- English – Native
- German – B2 Proficiency
- Hindi – Mother tongue
- Punjabi – Mother tongue

Selected Academic Achievements

- **CYD Doctoral Fellowship Grant — Cyber Defense Campus** Sep'19
  Funding for two years' of PhD salary (~ CHF 170,000)
- **Qualified CSIR-NET (Mathematics)** Jun'18
  All-India Rank 83
- **Award of Excellence — IISER Mohali** May'18
  Best Overall Academic Performance (Mathematics)
- **Six Certificates of Excellence — IISER Mohali** Aug'14 – May'18
  Awards for Best Semester-Wise Academic Performance (Mathematics)
- **INSPIRE Scholarship — Dept. of Science & Tech, India** Aug'13 – May'18
  Scholarship for higher studies in basic sciences

Programming and Tools

- **Python**: Several years of experience: machine learning, computer vision, cryptographic utilities, backend systems development
- **SageMath**: Conducting experiments and verifying theoretical results in cryptography research
- **BurpSuite**: Basic proficiency
- **nmap, sslyze**: Basic proficiency
- **Shell Scripting**: Basic proficiency
- **R**: Intermediate proficiency. Data analysis, forecasting, visualization, machine learning algorithms
- **LaTeX, Office (Excel, Word, PowerPoint)**: Scientific documentation, writing papers, and preparing presentations
- **Hugo**: Static site generator for building personal website and resume.
- **HTML, CSS**: Working proficiency. Used in building and customizing static site with Hugo.

Selected Publications (full list with links)

- **Cryptanalysis of a System Based on Twisted Dihedral Group Algebras**
  Simran Tinani — *Transactions on Mathematical Cryptology (TMC)* , 2022
- **A Deterministic Algorithm for the Discrete Logarithm Problem in a Semigroup**
  Simran Tinani, Joachim Rosenthal — *Journal of Mathematical Cryptology, vol. 16, no. 1, pp. 141–155* , 2022
- **Complexity of Conjugacy Search in Some Polycyclic and Matrix Groups**
  Simran Tinani, Carlo Matteotti, Joachim Rosenthal — *arXiv preprint* , 2022
- **A Number Theoretic Approach to Cycles in LDPC Codes**
  Julia Lieb, Simran Tinani — *IFAC-PapersOnLine, Proceedings of 25th International Symposium on Mathematical Theory of Network Systems (MTNS)* , 2022
- **Existence and Cardinality of k-Normal Elements in Finite Fields**
  Simran Tinani, Joachim Rosenthal — *Theoretical Computer Science and General Issues, Springer International Publishing* , 2021

Selected Talks

- **A Number Theoretic Approach to Cycles in LDPC Codes**
  25th International Symposium on Mathematical Theory of Network Systems (MTNS) — *Bayreuth, Germany* (September 2022)
- **Methods for Attacks in Non-Commutative Cryptography**
  Cyber Security Track, Cyber Alp Retreat — *Cyber-Defence Campus, Switzerland* (July 2022)
- **Complexity of Conjugacy Search in some Platform Groups**
  International Workshop on Coding Theory and Cryptography, WCC — *Rostock, Germany* (March 2022)

Teaching and Mentorship

- UZH: Taught courses on Algebra, Elliptic Curves, Convolutional Codes, Cryptography.
- UZH: Co-supervised a master's thesis on uniform hypergraphs and cryptographic secret-sharing access structures.
- Hashbrown: Mentored interns on existing projects, their business impact and relevant knowledge and skills.

Volunteering

- PhD Representative – UZH ZGSM
- President – IISER Alumni Association
- Animal Welfare – SPCA, Chandigarh
- Math Camps – IISER

Other interests

- Literature & Poetry
- Swimming, badminton, hiking
- Writing

References

Available upon request.

Contact

- simran.tinani@gmail.com
- +41 76 618 82 71
- Workplace Homepage
- Personal Homepage
- LinkedIn
- GitHub

Personal Information

- DOB: 15 August 1995
- Nationality: Indian

Languages

- English – Native
- German – B2 Proficiency
- Hindi – Mother tongue
- Punjabi – Mother tongue

Teaching and Mentorship

- UZH: Taught courses on Algebra, Elliptic Curves, Convolutional Codes, Cryptography.
- UZH: Co-supervised a master's thesis on uniform hypergraphs and cryptographic secret-sharing access structures.
- Hashbrown: Mentored interns on existing projects, their business impact and relevant knowledge and skills.

Volunteering

- PhD Representative – UZH ZGSM
- President – IISER Alumni Association
- Animal Welfare – SPCA, Chandigarh
- Math Camps – IISER

Other interests

- Literature & Poetry
- Swimming, badminton, hiking
- Writing

References

Available upon request.