
PRAVEENSANKAR MANIMARAN

PHD RESEARCH FELLOW

+919500552237 ♦ praveema@ifi.uio.no ♦ **LinkedIn:** [linkedin.com/in/praveen000/](https://www.linkedin.com/in/praveen000/) ♦ **WWW:** <https://praveen.xyz/>

PROFESSIONAL SUMMARY

Praveensankar Manimaran is a PhD Research Fellow at the University of Oslo, Norway working on Verifiable Credentials and Zero-Knowledge Proofs (ZKPs). As part of the PhD, Praveen worked on challenging research problems including privacy issues in VCs revocation, developed novel solutions using ZKPs, and built prototypes to showcase the feasibility.

EDUCATION

M.Tech. in Computer Science And Engineering - National Institute of Technology Puducherry, India
(June 2020)

- CGPA: 9.82, Gold Medalist.

B.E. in Computer Science And Engineering - PSG College of Technology, India (May 2016)

WORK EXPERIENCE

Ph.D. Research Fellow - University of Oslo, Norway (Oct 2020 - current)

- Research in **Verifiable Credentials, Zero-Knowledge Proofs, Blockchain Technologies**
- Worked as a teaching assistant for the following courses: IN5020 - Distributed Systems (2022, 2023), IN5420 - Distributed Blockchain Technologies (2022, 2023).
- Installed and maintained Norway's EBSI pilot node (2022-2023).
- **Advisors:** Roman Vitenberg, Leander Jehl

Software Engineer - Accolite Software India Pvt Ltd (July 2016 - March 2017)

- Worked on web development using technologies associated with .NET frameworks and angularjs.

RESEARCH ADOPTION

EBIP: Secure Privacy-Preserving Revocation of Verifiable Credentials [<https://hub.ebsi.eu/ebips>]

- Presents a security vulnerability in EBSI's Dynamic Status List, a revocation protocol for verifiable credentials that addresses the privacy issue of holder's traceability.
- Adopts *Untrace*, a ZKP-based revocation protocol that I developed during my PhD.

PUBLICATIONS

1) *Untrace: Addressing holder's privacy in Verifiable Credentials using ZKPs* (Work in Progress)

2) *Decentralization Trends in Identity Management: From Federated to Self-Sovereign Identity Management Systems*. (Computer Science Review, Volume 58).

[<https://www.sciencedirect.com/science/article/pii/S1574013725000528>]

3) *Prevoke: Privacy-Preserving Configurable Method for Revoking Verifiable Credentials*. 2024 IEEE International Conference on Blockchain (Blockchain). [doi: 10.1109/Blockchain62396.2024.00053]

PROJECTS

***Prevoke* - Proof of Concept implementation:**

- Implemented *Prevoke*, and integrated *Prevoke* into an inbuilt VC ecosystem.
- **Languages:** Golang, Solidity,
- **Github repo:** <https://github.com/praveensankar/Prevoke>.

***Untrace* - Proof of Concept implementation:**

- Implemented, and integrated *Untrace* into an inbuilt VC ecosystem.
- Built a custom ZKP circuit based on groth16 ZKP scheme using the gnark library.
- Benchmarked the performance of *Untrace*.
- **Languages:** Golang, Solidity
- The GitHub repository will be shared upon request, as the research paper is not yet published.

WEBSITES, PORTFOLIOS, PROFILES

- <https://github.com/praveensankar>
- <https://scholar.google.com/citations?user=oyTr15UAAAAJ>

SKILLS

Zero-Knowledge Proofs

Verifiable Credentials

Blockchain

Research