PRAVEENSANKAR MANIMARAN

PHD RESEARCH FELLOW

♦ +919500552237 ♦ praveema@ifi.uio.no ♦ **LinkedIn:** 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. As part of the PhD, Praveen designed research projects, identified challenging research problems including privacy issues in VCs revocation, developed novel solutions, and built prototypes to showcase the feasibility.

EDUCATION

Ph.D. in Computer Science - University of Oslo, Norway (Oct 2020 - current)

- Research in **Verifiable Credentials, Zero-Knowledge Proofs, Blockchain Technologies**
- **Supervisors:** Roman Vitenberg, Leander Jehl
- **Collaborators:** Thiago Garrett, Mayank Raikwar, Arlindo F. Conceição
- 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).

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)

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 ***zkRevoke,*** a ZKP-based revocation protocol. ***zkRevoke*** is developed during my PhD.

PUBLICATIONS

1) 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]

- Studies Federated and Self-Sovereign Identity systems from a conceptual point-of-view.
- Proposes a generic framework for Identity systems and analyses the architectures and workings of (a) IOTA Id, (b) Indy, and (c) eIDAS v1.0.
- Highlights differences in decentralization and privacy strategies across these systems.

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

- *Prevoke* presents key privacy challenges in the revocation protocol and proposes a novel solution that utilizes Merkle Tree Accumulators, BBS Signatures, Bloom Filters and Smart Contract.
- *Prevoke* also proposes a two-phase verification protocol that optimizes the performance of verification. Most of the valid credentials go through fast verification. Only revoked and a handful of valid credentials would go through slow verification.

3) **Addressing traceability of revocation status of Verifiable Credentials** (Work in Progress)

- Formalize the privacy of holder's traceability in the verifiable credentials system.
- Proposes *zkRevoke*, a revocation protocol that uses a custom-built Zero-Knowledge Proof circuit.
- *zkRevoke* outperforms the existing protocols in terms of required bandwidth for issuers and holders.

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.

zkRevoke **- Proof of Concept implementation:**

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

WORK EXPERIENCE

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

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

WEBSITES, PORTFOLIOS, PROFILES

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

SKILLS

Zero-Knowledge Proofs	Verifiable Credentials
Blockchain	Research

REFERENCES

Dr. Roman Vitenberg, Professor, University of Oslo, Norway
romanvi@ifi.uio.no

Dr. Leander Nikolaus Jehl, Associate Professor, University of Stavanger, Norway

leander.jehl@uis.no