Praveensankar Manimaran

PhD Research Fellow

praveema@ifi.uio.no +919500552237 https://praveen.xyz/

github.com/praveensankar/ linkedin.com/in/praveen000/

Bio

Praveensankar Manimaran is a PhD Research Fellow at the University of Oslo, Norway, working on Verifiable Credentials and Zero-Knowledge Proofs. Praveen has expertise in developing new research directions, designing, developing, and implementing solutions for complex research problems.

Education

Ph.D. - Informatics, *University of Oslo* 2020 Oct – Present

M.Tech. - Computer Science and Engineering, 2018 Jul – 2020 Jun
National Institute of Technology Puducherry
- CGPA: 9.82, **Gold Medalist**

B.E. - Computer Science and Engineering, 2012 Jul – 2016 May
PSG College of Technology

Professional Experience

PhD Research Fellow, *University of Oslo, Norway* 2020 Oct – 2024 Oct
- 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
- **Collaborators:** Thiago Garrett, Mayank Raikwar, Arlindo F. Conceição

Software Engineer, *Accolite Software India Pvt Ltd* 2016 Jul – 2017 Mar
- Worked on web development and used technologies associated with the .NET framework.

Publications

Addressing traceability of revocation status of Verifiable Credentials,
(https://arxiv.org/html/2509.11934v1)
- 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 existing protocols in terms of required bandwidth for issuers and holders.

Decentralization Trends in Identity Management: From Federated to Self-Sovereign Identity Management Systems, *(Computer Science Review, Volume 58, 2025)*

- Reviews Federated and Self-Sovereign Identity systems from a conceptual point of view.
- Proposes a generic framework for Identity systems and analyzes 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.

Prevoke: Privacy-Preserving Configurable Method for Revoking Verifiable Credentials, *2024 IEEE International Conference on Blockchain (Blockchain)*

- *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.

Research Adoption

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

- Discloses 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.

Projects

zkRevoke, *Implementation* 2024 Aug – 2025 May

- 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.

Prevoke, *Implementation* 2023 Aug – 2024 Jul

- Implemented *Prevoke*, and integrated *Prevoke* into an inbuilt VC ecosystem.
- **Workflows:** 1) issuance, 2) revocation, 3) VP construction and sharing, and 4) VP verification.
- In addition, Smart Contract is deployed on a Private Blockchain using Ganache, hosted in NREC.
- The entities are hosted as servers and geographically distributed via NREC.
- **Results:** Analyzed the performance, latency, and cost of Prevoke for different workloads.
- **Languages:** Golang, Solidity, Python
- **Github repo:** https://github.com/praveensankar/Prevoke .