

Brought to you by [INTERNATIONAL ISLAMIC UNIVERSITY MALAYSIA](#)

Scopus

[Back](#)

A Lightweight Post-Quantum Anonymous Attestation Framework for Traceable and Comprehensive Privacy Preservation in VANETs

[Journal of Cybersecurity and Privacy](#) • Article • [Open Access](#) • 2026 •

DOI: 10.3390/jcp6020044

[Agustina, Esti Rahmawati](#)^a ; [Ramli, Kalamullah](#)^a ; [Harwahyu, Ruki](#)^a ; [Gunawan, Teddy Surya](#)^b ; [Salman, Muhammad](#)^a ; [+2 authors](#)

^a Department of Electrical Engineering, Universitas Indonesia, Jawa Barat, Depok, 16424, Indonesia

[Show all information](#)

0

Citations

[View PDF](#)[Full text](#) [Export](#) [Save to list](#) [Document](#)[Impact](#)[Cited by \(0\)](#)[References \(60\)](#)[Similar documents](#)

Abstract

Vehicular ad hoc networks (VANETs) require authentication systems that balance privacy, scalability, and post-quantum security. While lattice-based V-LDAA offers quantum resistance, it faces challenges in signature size, traceability, and integration. We propose post-quantum traceable direct anonymous attestation (PQ-TDAA), combining National Institute of Standards and Technology (NIST)-standard Dilithium2 and Falcon-512 signatures with adapted Beullens-style blind signatures and Fiat–Shamir simplified Schnorr proofs, reducing proof size by 69.2% (8 kB vs. V-LDAA's 26 kB) and supporting European Telecommunications Standards Institute Technical Specification (ETSI TS) 102 941-compliant traceability through Road Side Unit (RSU)-assisted verification. Evaluated using SageMath, Python 3.11, and NS-3, PQ-TDAA-Falcon-512 achieves 8.1 ms and 49.7 ms end-to-end delays

at 10 and 20 vehicles, respectively, with 64.7 Mbps goodput on congested 802.11p channels, showing promise for densities of ≤ 50 vehicles and advantages over Dilithium2. Real-world validation on ARM Cortex-A76 (Raspberry Pi 5, emulating automotive OBUs) yields sub-0.5 ms V2V cycles within 100 ms beacon intervals, supporting practical embedded deployment. Future work will extend PQ-TDAA to emerging 5G and NR-V2X settings, integrate more realistic mobility and channel models through coupled NS-3 and SUMO co-simulation, and investigate side-channel resistance for enhanced scalability and robustness in real deployments. © 2026 by the authors.

Author keywords

anonymous attestation; lattice-based cryptography; post-quantum cryptography (PQC); privacy-preserving authentication; traceability; vehicular ad hoc networks (VANETs)

Corresponding authors

Corresponding
author

M. Salman

Affiliation

Department of Electrical Engineering, Universitas Indonesia, Jawa Barat,
Depok, 16424, Indonesia

Email address

muhammad.salman@ui.ac.id

© Copyright 2026 Elsevier B.V., All rights reserved.

Abstract

Author keywords

Corresponding authors

About Scopus

[What is Scopus](#)

[Content coverage](#)

[Scopus blog](#)

[Scopus API](#)[Privacy matters](#)

Language

[日本語版を表示する](#)[查看简体中文版本](#)[查看繁體中文版本](#)[Просмотр версии на русском языке](#)

Customer Service

[Help](#)[Tutorials](#)[Contact us](#)

ELSEVIER

[Terms and conditions](#) ↗ [Privacy policy](#) ↗ [Cookies settings](#)

All content on this site: Copyright © 2026 [Elsevier B.V.](#) ↗, its licensors, and contributors. All rights are reserved, including those for text and data mining, AI training, and similar technologies. For all open access content, the relevant licensing terms apply.

