



NATIONAL CENTER FOR TRANSPORTATION CYBERSECURITY AND RESILIENCY

A USDOT National Transportation Center

Project Title:	Secured Small-Key-Based Post Quantum Cryptographic Scheme for Blockchain-based VANET
PI Name and Contact:	Mizanur Rahman, Ph.D. Assistant Professor Department of Civil, Construction & Environmental Engineering 2007 Smart Communities and Innovation Building (SCIB) The University of Alabama, Tuscaloosa, AL Phone: (205) 348-1717 Email: mizan.rahman@ua.edu
Submission Date:	February 10, 2025
Version:	1.0
Project Performance Period	January 1, 2024 – December 31, 2024

Project Summary

The emergence of quantum computing presents significant challenges to traditional cryptographic algorithms used to secure data communication within Transportation Cyber-Physical Systems (TCPS). The vulnerabilities of traditional cryptographic schemes against quantum computing-based cyberattacks, with a particular focus on the data communication aspects of TCPS, are identified in this report. A case study has been conducted to analyze the vulnerabilities of a TCPS application from the Architecture Reference for Cooperative and Intelligent Transportation (ARC-IT) service package, i.e., Electronic Toll Collection, leveraging the Microsoft Threat Modeling tool. This case study highlights the cryptographic vulnerabilities of a TCPS application. In addition, this report, specifically, investigates the vulnerabilities of secured blockchain-based VANETs and presents an impersonation attack model utilizing Shor's algorithm implemented in a quantum computer to target the trust-based architecture of such networks. The findings reveal that an impersonation attack is feasible on a blockchain-based VANET, effectively compromising its trust chain. Consequently, this research underscores the critical need for a quantum-secured blockchain to enhance the security of VANETs and the urgency of transitioning to post-quantum cryptography (PQC) to mitigate these risks in TCPS. Thus, the standards and guidelines from the National Institute of Standards and Technology (NIST) PQC Standardization Process, analyzing the security properties and implementation considerations of various PQC families in TCPS, are reviewed. Finally, an experimental evaluation of CRYSTALS-Kyber assessed its performance across diverse TCPS communication scenarios, including both wired and wireless technologies. While CRYSTALS-Kyber proves effective in securing TCPS applications over high-bandwidth, low-latency Ethernet networks, this analysis highlights challenges in meeting the stringent latency requirements of safety-critical wireless applications within TCPS.

1. Data Description

Reports and data produced as part of this project are expected to include, but are not limited to, websites, publications, and archival-quality data curated from various sources. These reports will include technical documents with detailed figures such as tables, graphs, and scripts essential for analyzing and interpreting the data. The project will generate structured datasets and programming data. Structured datasets will include cryptographic algorithm performance metrics (key size, encryption times, and computational overhead), simulation logs from PQC integration into IEEE 1609.2 standards (latency, packet loss, and error rates), and federated learning outputs (model accuracy and robustness to adversarial attacks). Programming data will comprise scripts for cryptographic analysis, certificate segmentation algorithms, and federated learning models, developed in Python. Data will be collected through cryptanalysis platforms, simulation environments like OMNET++, and custom setups for real-world PQC testing.

2. Data format and metadata standards

Detailed data will be documented corresponding to each metadata set available in at least one of the following formats: XML, CSV, plain text, PDF, HTML, MS Word, or LaTeX. The aggregated data will be in plain text format and may be compressed for space-saving purposes. Programming scripts will be maintained in Python. Comprehensive metadata will accompany all datasets, including descriptions of variables, data collection procedures, and processing methods. Data dictionaries will be provided for all the related data, and standards

used for data and metadata format and content will be documented with proposed solutions and remedies. Metadata and data standards will align with the DCAT-US Schema v1.1 to support interoperability and compliance with federal data repositories like the USDOT Research Data Exchange (RDE). The data files will be stored and backed up in UA+BOX provided by the University of Alabama (UA). UA+Box provides a secure, managed, cloud-based toolset, and storage to facilitate collaboration and anywhere-access to active files and data. All data are encrypted both in transit and storage and are maintained on domestic servers. This storage is provided to UA faculty without charge.

3. Access Policies

Access to, sharing, and distributing of documentation will be via web sites and publishing and presenting in conferences, journals, and monographs. The data will be shared via the TraCR website and USDOT Repository & Open Science Access Portal enabling the research community to access and reproduce research activities. The Principal Investigator (PI) will coordinate with the UA Associate Director as well as TraCR's Director, Associate Directors and staff to oversee data management. Access to the raw data stored in UA+Box will require approval from the PI to ensure security and compliance. The reports produced from the proposed project will be maintained and available by TraCR.

4. Policies and Provisions for Re-use, Redistribution, derivatives

The author(s) and the researcher(s) reserve all rights of intellectual property. All sensitive personal information will be removed from the datasets before they are shared to avoid any ethical issues. Should any third-party data used, proper attribution will be provided, and licensing requirements will be strictly adhered to.

5. Plans for Archiving and Preservation of Access and Data Integrity

Data of long-term value includes cryptographic algorithm performance metrics, simulation logs, federated learning outputs, metadata, programming scripts, and project reports. The long-term strategy for maintaining, curating, and archiving the data is to seek support from the UA Office of Information (OIT). The OIT datacenter operates an enterprise-class Compellent SAN storage platform with daily replication/replay to a backup Compellent SAN located in our Atlanta Continuity of Operations facility, which is a highly secured Tier 2 disaster recovery facility. As needed, PI will ask the OIT data center to archive the data from this project for ten years.

6. Change Log

Version	Date	Description
1.0	February 10, 2025	Initial submission of the Data Management Plan.