RJIT Research Journal of Information Technology

OPEN ACCESS

Executive Summary

PUF-Based Post-Quantum CAN-FD Framework for Vehicular Security

Ikram Ilahi

In high interconnectivity contexts with numerous delicate input and output sensors and drivers communicating, the Controller Area Network, or CAN, is a bus protocol that is frequently utilized. The bulk of functions of a vehicle's electronic components, known as Electronic Control Units (ECUs), which communicate through the differential bus, are one of the main applications of the Controller Area Network. Vehicle security frameworks only consider low-security cryptography for reduced ciphertext and resource utilization due to the resource limitations of the ECUs. However, with the quick adoption of CAN-FD (Flexible Data-rate), a more recent standard of the Controller Area Network, improved efficiency that supports up to eight times bigger payloads can be employed for cryptography and data transfer. The authors of this study suggest the PUF-PQC-CANFD, or PUF-Based Post-Quantum Cryptographic Framework.

Most of a vehicle's capabilities are controlled by hundreds of ECUs that are part of the electronic systems in vehicles. Vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), and vehicle-to-pedestrian (V2P) system integration is another feature of smart vehicles. The CAN bus's lack of security, however, gives enemies easy access to sensitive data, control, and the ability to easily impersonate any other node in the network. CAN is a standardized communication system that has command over crucial operations like brakes, steering, and acceleration. Performance and security of CAN messages are examined both qualitatively and quantitatively. There is also a review of how this framework compares to others in terms of how long data is transmitted over the CAN bus.

The use of CAN-FD is expanding as more cars, including smart vehicles, need quicker, larger buses to send more data. As a result, to defend against evolving threats, vehicle security must also make use of CAN-FD. Authors suggested PUF-PQC-CANFD, a PUF-using CAN-FD security framework with post-quantum security, in this study. By carefully addressing local public key storage and streamlining traffic, our architecture outperforms both pre-quantum and post-quantum frameworks in terms of bus performance.

To further investigate the aging/implementation of the PUF, as well as the energy, computational time, and area costs of this system compared to competing PQC-frameworks, implementation of this algorithm in hardware should also be finished.

Source: Information

KEYWORDS

Vehicular security; cybersecurity; controller area network; post-quantum; CAN-FD; authentication; physically unclonable function; SIDH; PUF-PQC-CANFD