information

MDPI

Article

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

Tyler Cultice and Himanshu Thapliyal *

Department of Electrical Engineering and Computer Science, University of Tennessee, Knoxville, TN 37996, USA
* Correspondence: hthapliyal@ieee.org

Abstract: The Controller Area Network (CAN) is a bus protocol widely used in Electronic control Units (ECUs) to communicate between various subsystems in vehicles. Insecure CAN networks can allow attackers to control information between vital vehicular subsystems. As vehicles can have lifespans of multiple decades, post-quantum cryptosystems are essential for protecting the vehicle communication systems from quantum attacks. However, standard CAN's efficiency and payload sizes are too small for post-quantum cryptography. The Controller Area Network Flexible Data-Rate (CAN-FD) is an updated protocol for CAN that increases transmission speeds and maximum payload size. With CAN-FD, higher security standards, such as post-quantum, can be utilized without severely impacting performance. In this paper, we propose PUF-Based Post-Quantum Cryptographic CAN-FD Framework, or PUF-PQC-CANFD. Our framework provides post-quantum security to the CAN network while transmitting and storing less information than other existing pre-quantum and post-quantum CAN frameworks. Our proposal protects against most cryptographic-based attacks while transmitting (at up to 100 ECUs) 25–94% less messages than existing pre-quantum frameworks and 99% less messages than existing post-quantum frameworks. PUF-PQC-CANFD is optimized for smaller post-quantum key sizes, storage requirements, and transmitted information to minimize the impact on resource-restricted ECUs.

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

Citation: Cultice, T.; Thapliyal, H. PUF-Based Post-Quantum CAN-FD Framework for Vehicular Security. *Information* **2022**, *13*, 382. https://doi.org/10.3390/info13080382

Academic Editors: Shingo Yamaguchi and Marco Baldi

Received: 1 July 2022
Accepted: 7 August 2022
Published: 9 August 2022

1. Introduction

The Controller Area Network, or CAN, is a bus protocol widely used in high interconnectivity environments where many sensitive input and output sensors and drivers communicate. One of the primary applications of the Controller Area Network is within vehicles, where the majority of functionalities of the vehicle's electronic systems, called Electronic Control Units (ECUs), communicate through the differential bus. Security of these multi-master and exposed communication systems has challenged researchers to develop frameworks capable of producing sufficient security on such low resources. Vehicular CAN security focuses on three principles, as explained by [1]:

- Minimizing performance and size cost.
- Maintaining the CAN protocol and standards.
- Minimize overhead in message transmission.

The resource constraints of the ECUs cause vehicular security frameworks to only consider low-security cryptography for smaller ciphertext and resource usage. However, with the rapid adaptation of a newer standard of the Controller Area Network, known as CAN-FD (Flexible Data-rate), higher efficiency that spans up to eight times larger payloads can be used for cryptography and information transfer.

1.1. Motivation

Due to the rise in wireless and IoT-based technologies, Controller Area Network's insecurities have become more exposed to remote attacks providing full control of sensitive information. Accompanying this, the development of quantum technology using Shor's Algorithm is estimated to break most existing asymmetric cryptography. Furthermore, non-volatile storage of private keys provides a huge risk to cryptography, as most non-volatile memory is insecure and vulnerable. Security frameworks centered around a reliably generated and unclonable signature are essential to providing a form of identification or verification of authenticity in cryptosystems. Physically Unclonable Functions, or PUFs, generate authenticity and cryptographic material with high-entropy, consistent responses and have observed strong usage in various existing pre-quantum frameworks [1]. However, existing frameworks utilizing lightweight, low security algorithms are not quantum-secure despite utilizing PUF technology. Additionally, post-quantum cryptography usually requires large memory and payload requirements, causing the need for CAN-FD and strong optimization. With these concerns in mind, the design of post-quantum CAN-FD frameworks are essential to minimizing performance overhead and mitigating future quantum security concerns.

1.2. Contribution

To mitigate these threats on the bus, we propose the use of post-quantum cryptography within a framework scheme utilizing optimized, high-speed CAN-FD frames. Our framework, "PUF-PQC-CANFD" or PUF-Based Post-Quantum Cryptographic CAN-FD Framework, utilizes post-quantum SIDH (197B) [2] and AES-256-GCM to validate authenticity of servers and nodes through challenge-responses. We demonstrate high security requirements while keeping memory and transmission requirements small for low-resource CAN ECUs. The framework provides for security from quantum attacks and other CAN threats, as shown in Figure 1. We also propose an authentication algorithm that verifies both the authenticity of the server and node based on pre-existing, locally stored public keys. Our message and storage requirements of authentication and standard communication are competitive to existing pre-quantum and post-quantum CAN frameworks. Thus, PUF-PQC-CANFD provides a storage and message optimized post-quantum approach to CAN security within vehicles.

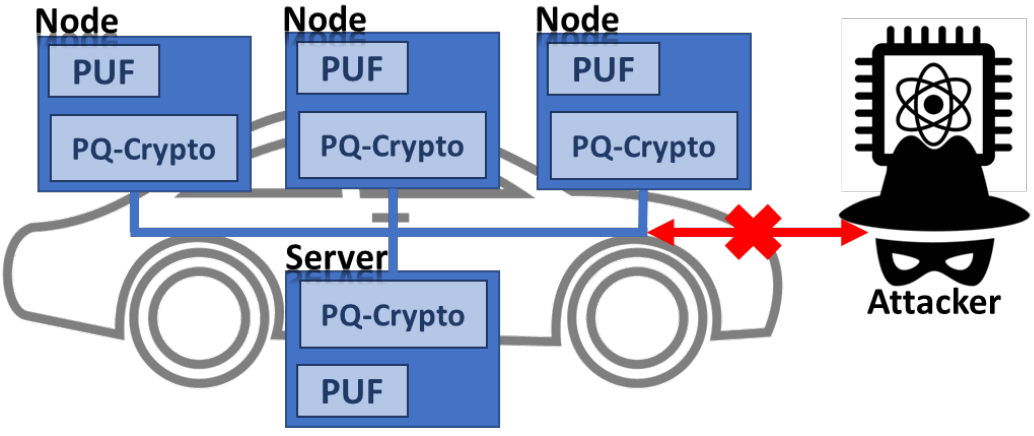

Figure 1. Injection and snooping attacks protected with Post-Quantum Vehicular Security on the CAN-FD Bus. By securing the vehicle's CAN bus and authenticating nodes within it, attackers that connect to the exposed bus are protected against it.

2. Background

Vehicular electronic systems contain hundreds of ECUs that control most functionalities within the vehicle. Smart vehicles also integrate with external surrounding devices, including vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), and vehicle-to-pedestrian

(V2P) systems [3]. However, the security of the CAN bus is minimal, which provides adversaries with sensitive information, control, and ability to spoof all other nodes within the network with ease. All messages are able to be spoofed or sniffed by any device with a connection to the bus, including malicious and compromised nodes. With the continued growth of CAN with wirelessly-enabled ECUs, the feasibility of conducting remote attacks on the CAN bus has become a strong concern. Previous research [4,5] has demonstrated CAN-related vehicle attacks that were capable of taking control of vital vehicular functions. Thus, exposed and unencrypted CAN buses with no authentication systems can risk the safety of drivers.

CAN is a standardized communication system with control over essential functions, such as acceleration, steering, and braking. The source-independent messages allow for control of vehicular functions to be easily given to additional systems, such as deep-learning neural networks or adversaries. Additional integrity features exist within the CAN frame, such as CRC and arbitration data, that provide frame length overhead that nearly doubles the transmission size of a CAN frame compared to the original data. This overhead can be observed in Figure 2. CAN is also popular in various robotics and physical systems. The CAN bus' architecture and features were expanded in an additional standard, Controller Area Network Flexible Data-Rate (CAN-FD), with higher transmit rates of data. This newer design is the basis of this proposal due to its ability to provide up to 8 times the payload size of CAN in comparatively faster transmission times. CAN frames consist of 111 bits to transmit, with only 64 bits of payload data. CAN-FD frames consist of similar sized arbitration with much larger data frames. Additionally, CAN-FD can transmit information at a significantly higher speed than standard CAN. Thus, CAN-FD's efficiency is significantly higher than its standard predecessor.

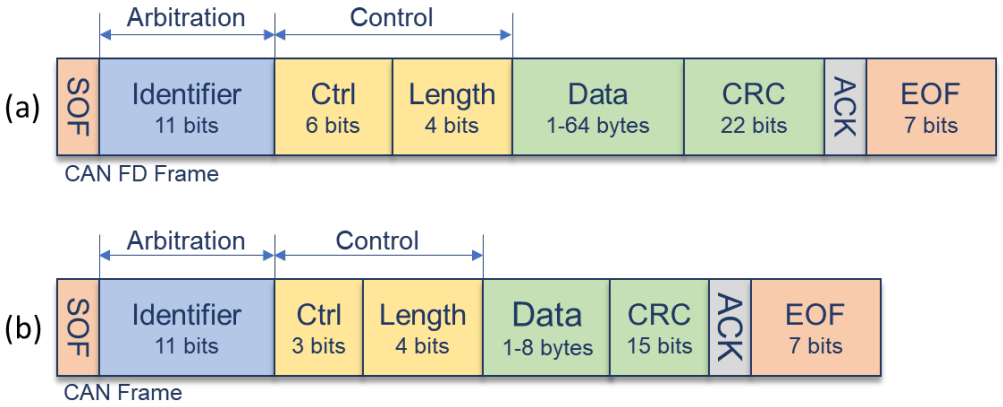

Figure 2. CAN and CAN-FD high-speed, standard data frame structure. (**a**) CAN frames consist of 111 bits to transmit. (**b**) CAN-FD frames consist of 572 total bits to transmit.

2.1. Post Quantum Cryptography

Post-quantum cryptography, or PQC, is a classification of cryptographic systems dedicated to being secure from cryptanalytic attacks by quantum computers. The PQC used in this paper is known as the Supersingular Isogeny Diffie–Hellman Key Exchange, or SIDH [2], which replaces elliptic curve mathematics with a supersingular isogeny graph. Similarly to the Elliptic Curve Diffie–Hellman (ECDH), SIDH establishes secret keys through insecure channels (such as CAN). By utilizing a private, sensitive key and another party's public key, one can generate a secure key without transmitting any vital information. Afterwards, symmetric encryption can be used to securely transmit information encrypted with the shared secret key. While key sizes of SIDH are larger than ECDH, the key sizes of sufficient security are much smaller than alternatives used in Post-Quantum Cryptographic vehicular security, such as NewHope, Kyber (>800 B), and Dilithium (>1312 B) [6]. However, our design allows for a flexible selection of possible key-establishment algorithms that can be used while maintaining many benefits.

2.2. Related Work

Many prior PUF frameworks have been proposed in pre-quantum vehicular security. Labrado et al. [1] discusses the use of PUF in a lightweight key-exchange-based authentication framework featuring a similar session key distribution system. The lightweight behavior allowed for minimal messages on standard CAN frames with sufficient security. Furthermore, Siddiqui et al. [7] provides a similar standard-encryption based PUF framework, but suffers from extremely high message requirements due to the algorithm's "transmit all public-key" design alongside moderately sized cryptographic primitives. Cloud-reliant PUF verification frameworks, such as Easy-Sec [8], also utilize PUFs in a public-key-based authentication scheme with smart vehicle networks (i.e., V2I). These verify PUF and vehicle information through the cloud, rather than within the vehicle. Some PUF-based CAN frameworks change contents of the CAN packet to provide additional space [9], but these designs do not follow the ISO 11898 standard. Additionally, LASAN_M, a Post-Quantum security framework, proposed by Ravi et al. [10], discussed the use of Kyber for key exchange and Dilithium for digital signatures. LASAN_M does not use PUFs and relies on generated signatures, similar to the Transport Layer Security (TLS). The system utilizes digital certificates/signatures and a central communication or root-of-trust security module to authenticate ECUs and handle all communication. A central authority (CA) would digitally sign the vehicles that the vehicular ECUs would use to validate themselves. However, the message requirement of signature data (thousands of bytes) alongside storage requirements is LASAN_M's trade-off for extremely strong security. A popular CAN framework, TESLA [11], also repurposed their framework with post-quantum security parameters (128 bit quantum and classical security) in mind, but suffers the same trade-off as LASAN_M.

These frameworks provide specific features that focus on different applications and optimizations. Labrado et al. [1] focuses on providing lightweight, but sufficient security (PRESENT-80) to small, fast CAN systems. Additionally, Siddiqui et al.'s [7] design provides a framework more "plug-and-play" with more common 128-bit security. In LASAN_M, smaller cryptographic data is traded away for strong, fast post-quantum security for CAN-FD. However, some applications may require post-quantum security with a significantly lower amount of messages, as for larger counts of nodes can become extremely vulnerable to self denial-of-service (or significant transmission slowdowns). Thus, there is a need for a post-quantum secure framework that transmits few messages but stores smaller cryptographic information. PUF-PQC-CANFD aims to fill this gap in PUF-based CAN frameworks by providing focus on smaller post-quantum cryptographic information size and, as a result, required message count.

3. Proposed PUF-Based CAN-FD Post Quantum Framework

We propose a design for a vehicular security framework designed for use in CAN-FD utilizing PUF responses and post-quantum security. The structure of the CAN network is shown in Figure 3. While the size of most cryptographic ciphertext is overwhelming for standard CAN, our design demonstrates that a CAN-FD framework is capable of post-quantum security with performance comparable to other designs. While some CAN security designs repurpose arbitration fields in the data frame [9], our proposal adheres to the CAN-FD standards and uses only the data field for ciphertext information.

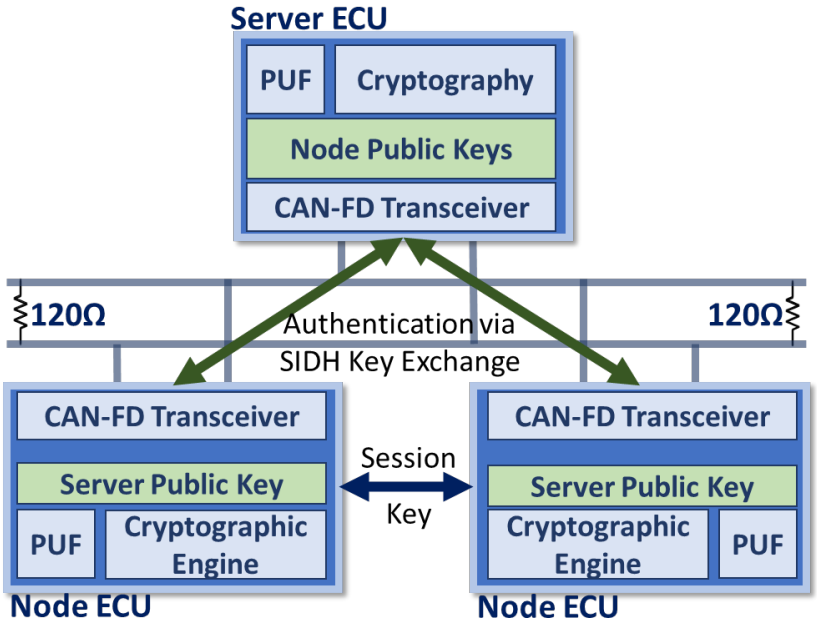

Figure 3. PUF-Based Post-Quantum Cryptographic CAN-FD Framework's generalized structure. SIDH key exchange is used to authenticate and transmit session keys that are then used by ECUs for normal node-to-node traffic encryption. All information is transmitted over a single CAN bus.

3.1. Design

The design of PUF-PQC-CANFD features a challenge-response validation system with an additional ECU defined as a "server". The server ECU maintains a large database of all valid node public keys (loaded when ECU is installed to system) to generate the shared keys used in authentication upon initialization. The vehicle ECUs, defined as "nodes", will generate a shared key using their PUF response and the locally stored public key material of the valid server. This shrinks storage costs in resource-limited nodes quadratically compared to storing all public keys observed in [7]. While the public keys are safe to store in non-volatile memory, the PUF provides a consistent private key material without requiring storage in insecure, non-volatile memory. These keys are unique to their nodes and will be used for authentication purposes to the server through dedicated message IDs. A two-way authentication through challenge-responses is performed by the server. The server transmits a uniquely encrypted challenge to nodes and the nodes reply with both the response and a reverse-challenge. The server must generate and transmit the correct response for the node to accept the session key and whitelist from the server. To minimize message costs, the challenge-responses are conducted alongside increasingly sensitive cryptographic information (i.e., session key, whitelist, etc.). Responses should be known on the challenger side for validation and can be generated from any type of function with a sufficient value space (i.e., hash, PUF response, or even a simple addition). Afterwards, valid nodes are provided a temporary session key for node-to-node encryption and a whitelist containing verified ECUs. If the server's response to the challenge is invalid, the session key will not be used and an error will be issued. Therefore, the SIDH key is only used periodically for communication with the server and authentication while the session keys are used for communication between nodes. Furthermore, the exposure of the SIDH key is much less frequent than the temporary ephemeral session key, thus providing strong security alongside the PQC key. A more detailed algorithm of the authentication scheme is defined in Algorithm 1.

Algorithm 1 PUF-PQC-CANFD: Server-Node Authentication Scheme.

Require: Server S, $NodeCount > 0$
  $S : Private_S \leftarrow PUFResponse(PUF_S)$
  for $\{N : Public_N\}$ in NodeList **do**
    $N : Private_N \leftarrow PUFResponse(PUF_N)$
    $S : Shared_N \leftarrow SIDHShared(Private_S, Public_N)$
    $N : Shared_S \leftarrow SIDHShared(Private_N, Public_S)$
  end for
  while $N_{Validated} < N_{Total}$ or not TimedOut **do**
    for N in $N_{Remaining}$ **do**
      S: Create Challenge C_S
      S: Transmit $Encrypt(C_S)$ to N
      N: $R_S \leftarrow Func(Decrypt(C_S))$
      N: Create Challenge C_N
      N: Transmit $Encrypt(R_S||C_N)$ to S
      if $R_S == R_{Expected}$ **then**
        S: N added to $N_{Validated}$
      end if
    end for
  end while
  while True **do** ▷ Repeated every M messages
    if $numMessagesSent > M$ **then**
      Generate Random 32-byte Session Key K_S
      for N in $N_{Validated}$ **do**
        S: $R_N \leftarrow Func(Decrypt(C_N))$
        S: $C_N \leftarrow R_N$
        S: $List_N \leftarrow N_{Validated}$
        S: Transmit $Encrypt(K_S||List_N||R_N)$ to N
        if $R_N == R_{Expected}$ **then**
          N: Uses K_S for Node-To-Node Encryption
        end if
      end for
    end if
  end while

Normal communication should utilize the inherent AES-GMAC/CTR of GCM mode for all communication to secure and prevent replay attacks and random/garbage injection attacks. The system should redistribute new symmetric session keys for normal communication of every M messages, where M is selected per application. Additionally, a new challenge-response validation should occur each session key by using the previous response as the next challenge. Our scheme scales linearly with the node count, as it uses significantly less messages than other PQC frameworks. Furthermore, parallelization may provide additional performance benefits, and the hardware acceleration of cryptography may remove computational overhead of larger cryptographic primitives. Additionally, new public keys should be re-flashed into relevant ECUs when nodes/servers are replaced. The process of re-flashing is implementation-specific and should be secure and tailored to the CAN system utilized. This decision to tie servers and nodes together allows local public key storage and provides additional security by using the public key as a signature for the correct server or node.

3.2. Post-Quantum Cryptography

The selection of cryptography in this framework aims to provide a sufficient level of security to quantum attacks while limiting message and memory cost of the cryptography. Thus, we selected a compressed SIDH [2] key exchange and AES-256 with GCM mode (for replay prevention and authentication). SIDH provides a relatively small key compared to

other NIST post-quantum standard finalists with long-term usage in mind. Additionally, a secure hashing algorithm, such as SHA-256, should be used to hash the generated shared key. For additional security, one may also decide to hash responses from the PUF.

AES-256 is also considered quantum safe with 128-bits of security, as per Grover's Algorithm. Additionally, message requirements of PUF-PQC-CANFD account for the additional IV and other information for AES256-GCM required. The IV should be randomly selected and included alongside the messages, as the available space in each CAN message is generally more than enough to transmit in a single frame. Furthermore, the GMAC feature of GCM mode should be utilized as well for message source authenticity.

4. Security Analysis

A qualitative and quantitative analysis of CAN-message performance and security are discussed. Additionally, a discussion of the impact of this framework compared to others on the transmission time over the CAN bus is provided. These comparisons are theoretical and calculated and do not include the overhead time of cryptographic computation. These comparisons frame the benefits of our proposed design and the message cost on transmitting such large amounts of information. These comparisons help to demonstrate our alternative solution to CAN security, focusing on post-quantum protection and low-storage/transmission requirements. The results assume standard-ID and high-speed CAN-FD. While the max bitrate of CAN-FD can be up to 15 Mbits/s (or higher), beyond 5 Mbits/s is likely prone to issues [12]. This shrinks data bitrate to approximately 4.2 Mbits/s when factoring in overhead.

4.1. Attack Protection and Security

PUF-PQC-CANFD focuses on providing additional security and post-quantum cryptography without significantly impacting message cost. An overview of the defenses and security features compared to existing pre-quantum and post-quantum frameworks are shown in Table 1. The use of GCM mode prevents replay and random injection attacks in our framework. Counters (AES-CTR), an inherent feature of AES-GCM, ensure that no two messages are the same, even with the same plaintext information (stopping replay attacks). By maintaining the public key of the server or nodes internally, the ECUs can verify that the server/node has not been replaced by another seemingly "valid" ECU, a feature missing in some compared frameworks. By using a session key system, our framework does not require all communication to be passed through the security module such as [10]. Additionally, by frequently refreshing session keys, we can avoid creating point-to-point keys between nodes such as in [7]. Furthermore, our system uses post-quantum cryptography, including post-quantum Diffie–Hellman keys for authentication and session information. Individual keys for point-to-point encryption would provide stronger security; however, the security of the post-quantum authentication and ephemeral session keys are adequate to provide long-term safety to the CAN network. While all mentioned frameworks protect against many cryptography-based attacks, they do not protect against denial-of-service (DoS) attacks. DoS attacks may selectively/indefinitely delay ECUs from receiving certain information. Overall, this proposal provides strong defense against attacks and other security features that sufficiently protect against quantum and traditional threats.

Table 1. Security/Feature overview comparison of proposed vs. existing [1,7,10] frameworks. As our framework is designed around providing adequate security to all fronts of attacks, we are capable of defending against most modern and future CAN threats.

	CAN/CAN-FD Frameworks			
Criteria	**PUF-PQC-CANFD**	**Labrado [1]**	**Siddiqui [7]**	**LASAN [10]**
Replay Defense	✔	✔	✘	✔
Sender Authenticity	✔	✘	✘	✔
Snooping Defense	✔	✔	✔	✔
Spoofing Defense	✔	✔	✔	✔
Node Blacklists	✔	✘	✔	✔
Post-Quantum	✔	✘	✘	✔
Server Verification	✔	✔	✘	✘
DoS Defense	✘	✘	✘	✘

4.2. Post-Quantum Authentication

CAN-FD frames provide much larger payloads to transmit more encrypted information without the need of splitting data into multiple messages. Alongside this, our system stores the server's public key within the local data of each ECU. This is for validation purposes and removes the need to transmit any public keys during authentication. These benefits combined provide results with similar message counts to lightweight pre-quantum algorithms despite the difference in key sizes. Additionally, the data transmission requires only $3n$ messages for authentication, where n is the number of nodes in the system. This is comparable to Labrado et al.'s [1] $4n$, and much lower than Siddiqui et al.'s [7] $3n^2 + 2n$ messages. Moreover, it is significantly lower than post-quantum framework LASAN_M's [10] $321n$ messages. These can be observed in tabular form in Table 2 for both initial authentication and reauthentication (when applicable).

Table 2. Messages, as functions of n nodes, sent in authentication compared between various CAN/CAN-FD Frameworks. All frameworks assume use of CAN-FD packet sizes (64 bytes) with their proposed structures. Initial is authentication that occurs upon the initialization of vehicle, while repeat (only applicable to frameworks that reauthenticate) is the authentication procedure when reauthenticating nodes during operation.

Transmitted	**Message/Byte Count per Node**			
Message	**Proposal**	**Labrado [1]**	**Siddiqui [7]**	**LASAN_M [10]**
Authentication (initial)	$3n$	$4n$	$3n^2 + 2n$	$321n$
Authentication (repeat)	$1n$	$4n$	N/A	N/A

The estimated time taken to transmit the frames based on message costs using CAN-FD @ 5Mbps for these frameworks are shown in Figure 4 and Table 3. PUF-PQC-CANFD takes approximately 75% , 4%, and 1% of the time required to transmit authentication frames at 25 ECUs compared to [1], [7], and [10], respectively. Comparison with 50, 75, and 100 ECUs are also provided to compare more to real world ECU counts of 50 to 100 ECUs [13]. This time difference continues to grow as the number of ECUs increases. The time taken during authentication should be accounted for upon vehicle start up and reauthentication/re-keying. During this period, this stage will disable electronics in the vehicle temporarily. In addition, this framework provides 128-bits of post-quantum security with comparable results to lightweight CAN frameworks. Our proposal can send larger ciphertext with less risk of self-inflicting a DoS attack, a problem frequently discussed for standard CAN with large counts of ECUs.

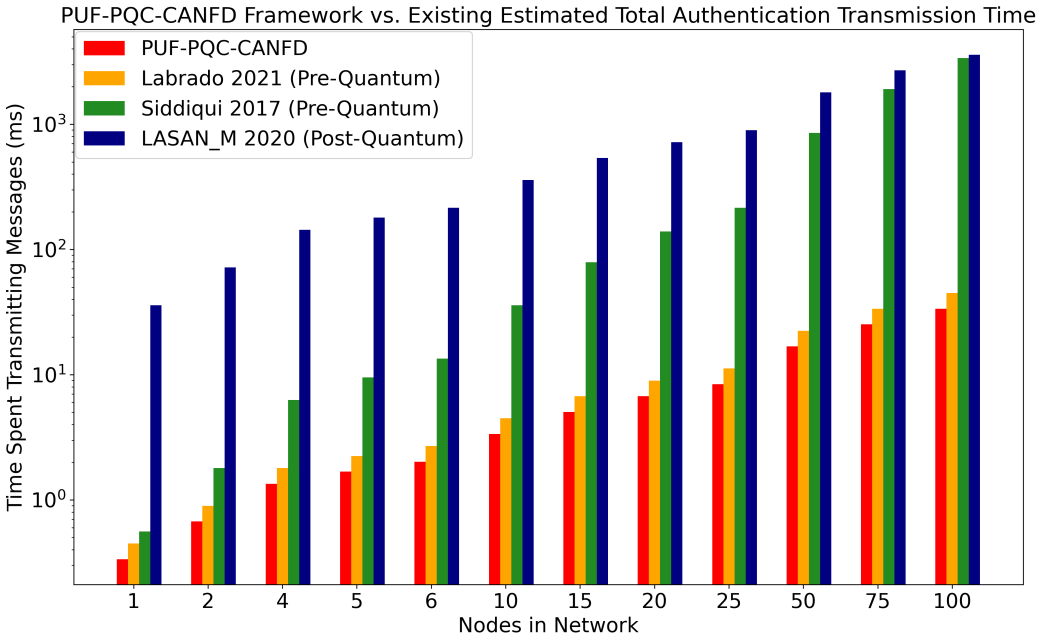

Figure 4. Time required to transmit all authentication information over the CAN network in $log_{10}(milliseconds)$ between PUF-PQC-CANFD, Labrado 2021 [1], Siddiqui 2017 [7], and LASAN_M 2020 [10]. The values are theoretical, and do not describe the computational/time cost of cryptography. Additionally, the times are estimated on the framework's message costs based on their specified CAN configurations. Higher values mean more time is taken to transmit all required information between nodes. Tabular results are shown in Tables 2 and 3.

Table 3. Estimated time frameworks would spend transmitting authentication messages: PUF-PQC-CANFD vs. Existing Pre-Quantum [1,7] and Post-Quantum [10] frameworks. Time estimations are based from their message values using their specified CAN configurations and only includes time the CAN network would be busy/transmitted on. Graphical results are shown in Figure 4.

	Number of ECUs to Authenticate							
Framework	**5**	**10**	**15**	**20**	**25**	**50**	**75**	**100**
PUF-PQC-CANFD	1.68 ms	3.36 ms	5.04 ms	6.72 ms	8.4 ms	16.8 ms	25.2 ms	33.6 ms
Labrado [1]	2.24 ms	4.48 ms	6.72 ms	8.96 ms	11.2 ms	22.4 ms	33.6 ms	44.8 ms
Siddiqui [7]	9.52 ms	35.84 ms	78.96 ms	138.87 ms	215.6 ms	851.2 ms	1906.8 ms	3382.4 ms
LASAN_M [10]	179.62 ms	359.24 ms	538.86 ms	718.48 ms	898.1 ms	1796.2 ms	2694.3 ms	3592.4 ms

4.3. Area and Computational Cost

It is important to also account for computation time and area of the SIDH algorithm. While a software implementation of SIDH would include a large time overhead during the key-exchange computation, recent research in FPGA-based implementations of SIDH demonstrated key-exchanges in only 31.6 ms with less resources than some other post-quantum algorithms [14]. Computations of SIDH are comparatively slower than cryptography used by other frameworks (i.e., ECDH, Kyber). However, lower key sizes with post-quantum allows for smaller non-volatile/volatile storage hardware requirements on low-resource nodes than other implementations. This trade-off allows for more SIDH hardware optimizations in the future to greatly benefit our framework, as the storage requirements and number of messages transmitted remain generally constant. Additionally, a design of an AES256-GCM hardware acceleration crypto-core was proposed by [15] that is sized and optimized for IoT/embedded security applications such as this framework.

5. Conclusions and Future Work

The use of CAN-FD is rising as more vehicles require faster and larger buses to transmit more data, such as smart vehicles. Thus, vehicle security must also utilize CAN-FD to protect against rising threats by utilizing these improved protocols. In this paper, we proposed PUF-PQC-CANFD, a PUF-utilizing CAN-FD security framework with post-quantum security. By optimizing traffic and carefully considering local public key storage, our design performs similarly or better over the bus than both existing pre-quantum and post-quantum frameworks. In this work, we utilized SIDH for the post-quantum cryptography and authentication. Due to recently demonstrated attacks on SIDH [16], the exploration of alternatives may provide security benefits that outweigh the memory/size efficiency of our chosen cryptography. The framework's design is independent of the post-quantum cryptosystem. Thus, replacement of SIDH will still provide low message cost, and security benefits remain regardless of the cryptosystem. For example, the NIST standardization winner, CRYSTALS-Kyber [17], could replace SIDH, as it would provide strong, standardized security with the cost of larger keys. Our design is optimized for small storage requirements and low-traffic, especially in authentication. As standards for communication and ECU systems progress, vehicular security must adapt and evolve to mitigate new threats.

Implementation of this algorithm in hardware should also be completed to further explore the aging/implementation of the PUF, along with the energy, computational time, and area costs of this system compared to other PQC-frameworks. Physical implementation using proposed PUF designs will provide further insight into the effectiveness of minimizing traffic and key sizes. Exploration into other post-quantum systems in this framework will also demonstrate the robustness and flexibility. Additionally, exploration into DoS protection would prove useful in preventing adversaries from selectively disabling certain features of the vehicle by flooding the CAN bus. By layering denial-of-service protection alongside this CAN-FD framework, authentication can be used to validate and deny CAN bus access to malicious nodes potentially performing a DoS attack.

Author Contributions: Conceptualization, T.C. and H.T.; Data curation, T.C.; Formal analysis, T.C.; Funding acquisition, H.T.; Investigation, T.C. and H.T.; Methodology, T.C. and H.T.; Project administration, H.T.; Resources, H.T.; Software, T.C.; Supervision, H.T.; Validation, T.C.; Writing—original draft, T.C.; Writing—review & editing, H.T. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Labrado, C.; Thapliyal, H.; Mohanty, S.P. Fortifying Vehicular Security through Low Overhead Physically Unclonable Functions. *J. Emerg. Technol. Comput. Syst.* **2021**, *18*, 3442443. [CrossRef]
2. Moody, D.; Alagic, G.; Apon, D.; Cooper, D.; Dang, Q.; Kelsey, J.; Liu, Y.K.; Miller, C.; Peralta, R.; Perlner, R.; et al. *Status Report on the Second Round of the NIST Post-Quantum Cryptography Standardization Process*; NIST: Gaithersburg, MD, USA, 2020. [CrossRef]
3. Chen, S.; Hu, J.; Shi, Y.; Peng, Y.; Fang, J.; Zhao, R.; Zhao, L. Vehicle-to-Everything (v2x) Services Supported by LTE-Based Systems and 5G. *IEEE Commun. Stand. Mag.* **2017**, *1*, 70–76. [CrossRef]
4. Moore, M.R.; Bridges, R.A.; Combs, F.L.; Anderson, A.L. Data-driven extraction of vehicle states from can bus traffic for cyberprotection and safety. *IEEE Consum. Electron. Mag.* **2019**, *8*, 104–110. [CrossRef]
5. Jo, H.J.; Choi, W. A Survey of Attacks on Controller Area Networks and Corresponding Countermeasures. *IEEE Trans. Intell. Transp. Syst.* **2021**, *23*, 6123–6141. [CrossRef]
6. George, T.; Li, J.; Fournaris, A.P.; Zhao, R.K.; Sakzad, A.; Steinfeld, R. *Performance Evaluation of Post-Quantum TLS 1.3 on Embedded Systems*; Cryptology ePrint Archive, Paper 2021/1553; ACM: New York, NY, USA, 2021. Available online: https://eprint.iacr.org/2021/1553 (accessed on 5 August 2022).

7. Siddiqui, A.S.; Gui, Y.; Plusquellic, J.; Saqib, F. A Secure Communication Framework for ECUs. *Adv. Sci. Technol. Eng. Syst. J.* **2017**, *2*, 1307–1313. [CrossRef]
8. Sadhu, P.K.; Yanambaka, V.P.; Mohanty, S.P.; Kougianos, E. Easy-Sec: PUF-Based Rapid and Robust Authentication Framework for the Internet of Vehicles. *arXiv* **2022**, arXiv:2204.07709.
9. Woo, S.; Jo, H.J.; Lee, D.H. A Practical Wireless Attack on the Connected Car and Security Protocol for In-Vehicle CAN. *IEEE Trans. Intell. Transp. Syst.* **2015**, *16*, 993–1006. [CrossRef]
10. Ravi, P.; Sundar, V.K.; Chattopadhyay, A.; Bhasin, S.; Easwaran, A. Authentication Protocol for Secure Automotive Systems: Benchmarking Post-Quantum Cryptography. In Proceedings of the 2020 IEEE International Symposium on Circuits and Systems (ISCAS), Sevilla, Spain, 12–14 October 2020; pp. 1–5. [CrossRef]
11. Alkim, E.; Bindel, N.; Buchmann, J.; Dagdelen, Ö.; Eaton, E.; Gutoski, G.; Krämer, J.; Pawlega, F. Revisiting TESLA in the Quantum Random Oracle Model. In Proceedings of the Post-Quantum Cryptography, Utrecht, The Netherlands, 26–28 June 2017; Lange, T., Takagi, T., Eds.; Springer International Publishing: Cham, Switzerland, 2017; pp. 143–162.
12. Schreiner, M.; Donat, L.; Köngeter, S. Introduction of CAN FD into the next generation of vehicle E/E architectures. *IEEE Int. Conf. Commun.* **2017**.
13. Möller, D.P.; Haas, R.E. *Guide to Automotive Connectivity and Cybersecurity*; Springer: Berlin/Heidelberg, Germany, 2019.
14. Koziel, B.; Azarderakhsh, R.; Kermani, M.M. A High-Performance and Scalable Hardware Architecture for Isogeny-Based Cryptography. *IEEE Trans. Comput.* **2018**, *67*, 1594–1609. [CrossRef]
15. Sung, B.Y.; Kim, K.B.; Shin, K.W. An AES-GCM authenticated encryption crypto-core for IoT security. In Proceedings of the 2018 International Conference on Electronics, Information, and Communication (ICEIC), Honolulu, HI, USA, 24–27 January 2018; pp. 1–3. [CrossRef]
16. Castryck, W.; Decru, T. *An Efficient Key Recovery Attack on SIDH (Preliminary Version)*; Cryptology ePrint Archive, Paper 2022/975; ACM: New York, NY, USA, 2022. Available online: https://eprint.iacr.org/2022/975 (accessed on 5 August 2022).
17. Bos, J.; Ducas, L.; Kiltz, E.; Lepoint, T.; Lyubashevsky, V.; Schanck, J.M.; Schwabe, P.; Seiler, G.; Stehlé, D. CRYSTALS-Kyber: A CCA-secure module-lattice-based KEM. In Proceedings of the 2018 IEEE European Symposium on Security and Privacy (EuroS&P), London, UK, 24–26 April 2018; IEEE: Hoboken, NJ, USA, 2018; pp. 353–367.