International Journal of Current Research and Techniques (IJCRT)
Volume 16, Issue 2, 2026; DOI: 10.5281/ZENODO.20066034
Original Research Article

HALE-V2V: A Hybrid Adaptive Lightweight Authentication Engine for Secure Vehicle-to-Vehicle Communication

Dr. Revanesh M, *Department of Electronics and Communication Engineering, PES College of Engineering, Mandya.*

Kavana C P, *Department of Electronics and Communication Engineering, PES College of Engineering, Mandya.*

Meghana H B, *Department of Electronics and Communication Engineering, PES College of Engineering, Mandya.*

Meghana N S, *Department of Electronics and Communication Engineering, PES College of Engineering, Mandya.*

Ramya K P, *Department of Electronics and Communication Engineering, PES College of Engineering, Mandya.*

Manuscript Received: May 02, 2026; Revised: May 06, 2026; Published: May 07, 2026

Abstract: Vehicle-to-vehicle (V2V) communication is a cornerstone of modern intelligent transportation systems, enabling real-time exchange of Basic Safety Messages (BSMs) to prevent collisions and improve traffic efficiency. However, securing these messages demands authentication that is simultaneously fast, compact, energy-efficient, and cryptographically robust, requirements that no existing standardised scheme fully satisfies. This paper presents HALE-V2V, a Hybrid Adaptive Lightweight Authentication Engine for secure V2V communication. HALE-V2V separates authentication into two temporally distinct phases: an infrequent session-bootstrap phase using Elliptic Curve Diffie-Hellman (ECDH) key exchange, and a high-frequency per-message authentication phase using SPECK-64/128 encryption and HMAC-BLAKE3 tag generation. This stratified design achieves 128-bit security at 0.38 ms per message, 28 bytes of overhead, 72 μJ energy consumption, and 2631 messages/second throughput, outperforming ECDSA-P256 by 5.5×, 4.6×, 6.4×, and 5.5× respectively. Formal security proofs in the eCK model demonstrate resistance to replay, Sybil, and man-in-the-middle attacks. Scalability analysis confirms sub-5 ms authentication latency with up to 300 simultaneous vehicles, while hardware synthesis requires only 1650 gate equivalents and 320 bytes of RAM. A post-quantum migration pathway via CRYSTALS-Kyber key encapsulation is also discussed, requiring no modification to the per-message authentication phase.

Keywords: Vehicle-to-vehicle communication, lightweight cryptography, VANET security, SPECK cipher, HMAC-BLAKE3, hybrid authentication, InternetofVehicles, DSRC, C-V2X, real-time authentication, post-quantum readiness, IEEE1609.2

1. Introduction

The past decade has witnessed a quiet but consequential transformation in how vehicles interact with one another and with the road infrastructure around them. What was once a purely mechanical domain steel, rubber, and combustion has evolved into a densely networked cyber-physical system in which on-board units (OBUs) continuously broadcast Basic Safety Messages (BSMs) at 10 Hz over the 5.9 GHz Dedicated Short-Range Communications (DSRC) band or the cellular C-V2X interface [5], [6]. The U.S. Department of Transportation estimates that V2V technology could prevent up to 80% of non-impaired multi-vehicle crashes [1], while the European Commission's Cooperative Intelligent Transport Systems initiative envisions a continent-wide deployment that would dramatically reduce road fatalities [2].

The security stakes, however, are equally dramatic. A single forged BSM injected into a platoon of vehicles can trigger emergency braking across dozens of cars; a Sybil attacker broadcasting phantom vehicles can manipulate traffic-flow algorithms into creating artificial gridlock; a replay of a stale collision-warning message can distract drivers at exactly the wrong moment [7], [8]. Crucially, all of these attacks can be mounted by an adversary with nothing more than a software-defined radio and a laptop no physical access required. Securing V2V messages therefore demands message authentication that is simultaneously fast (sub-100 ms end-to-end, with per-message verification well below 5 ms), compact (overhead measured in tens of bytes, not hundreds), energy frugal (OBUs are battery-backed embedded systems), and cryptographically sound (resistant to replay, Sybil, and man-in-the-middle attacks at 128-bit security) [9],

[10]. No currently standardised scheme meets all four criteria simultaneously. ECDSA-P256, mandated by IEEE 1609.2 [27], requires 2.10 ms per verification and 128 bytes of overhead. TESLA [18] achieves lower per-message cost but introduces a time-synchronization dependency. Lightweight proposals such as SALT-V [18] and Easy-Sec [33] narrow the gap but sacrifice either security strength or infrastructure independence.

Contributions

This paper makes the following specific contributions: (1) We design HALE-V2V, a stratified hybrid authentication protocol that combines ECDH session bootstrapping with SPECK-64/128 and HMAC-BLAKE3 per-message authentication, achieving 128-bit security at 0.38 ms per message, with formal security proofs demonstrating resistance to replay, Sybil, and man-in-the-middle attacks under the CDH assumption in the random oracle model. (2) We present a comprehensive performance evaluation comparing HALE-V2V against five existing schemes across seven metrics, including a scalability analysis up to 300 simultaneous vehicles. (3) We characterize the hardware footprint (1650 GE, 320 bytes RAM) and discuss a migration pathway toward post-quantum primitives.

Paper Organization

Section II reviews V2V communication architecture and security requirements. Section III surveys related authentication schemes. Section IV formalizes the threat model. Section V presents the HALE-V2V protocol design and algorithms. Section VI provides formal security analysis. Section VII reports simulation results. Section VIII discusses hardware implementation. Section IX addresses limitations and future directions. Section X concludes.

2. Background

V2V Communication Architecture

Modern V2V systems operate under two complementary radio technologies. The first, IEEE 802.11p (WAVE), defines the physical and MAC layers for DSRC, operating in the 5.850-5.925 GHz band with up to 27 MHz of dedicated spectrum [43], [44], [45]. The second, C-V2X (Cellular V2X), leverages the 3GPP PC5 sidelink interface for direct vehicle-to-vehicle communication and the Uu interface for network-assisted services, as standardized in 3GPP Release 14 through 16 [4], [46], [47]. Both technologies support the DSRC Message Set Dictionary (SAE J2735) [30] and the WAVE Security Services specification (IEEE 1609.2) [27].

Each vehicle is equipped with an OBU that broadcasts BSMs at 10 Hz. A BSM carries vehicle identifier, GPS coordinates, speed, heading, and acceleration enough information for surrounding vehicles to compute collision risk within a few hundred milliseconds [37]. Roadside Units (RSUs) provide infrastructure anchor points for certificate distribution and revocation list dissemination [38].

Security Requirements

Based on the ETSI ITS security architecture [28] and the analyses in [12] and [36], six main security requirements are identified for V2V authentication: (1) Message Authenticity: every received BSM must be provably from a legitimate vehicle. (2) Replay Prevention: an adversary must not be able to retransmit a previously valid BSM. (3) Sybil Resistance: a single attacker must not be able to impersonate multiple vehicles. (4) Privacy: the long-term identity of a vehicle must not be linkable across pseudonym changes [19], [20]. (5) Low Latency: per-message verification must complete within 5 ms to meet real-time safety requirements [42]. (6) Scalability: authentication must remain viable as the number of in-range vehicles grows beyond 300 OBUs.

Cryptographic Primitives

SPECK-64/128 is a family of lightweight ARX (Add-Rotate-XOR) block ciphers designed by the U.S. National Security Agency and published in 2013 [56]. The 64-bit block, 128-bit key variant performs 32 rounds and achieves 7.4 cycles/byte on ARM Cortex-M3, requiring only 1.4 kGE in hardware [57]. HMAC-BLAKE3 is based on the Merkle tree construction and the ChaCha permutation [59], achieving 6.5 GB/s on a single ARM Cortex-A72 core. It provides 128-bit MAC security under the PRF assumption. Elliptic Curve Diffie-Hellman (ECDH) over the NIST P-256 curve [50], [51] is used

exclusively during the session-bootstrap phase, where the 2.1 ms cost is acceptable given the infrequent nature of bootstrapping (once per pseudonym period, typically 5-10 minutes).

3. Related Work

Authentication for vehicular networks has been studied extensively since the foundational work of Raya and Hubaux [7], [36], who proposed the first PKI-based framework for VANET security. Their design, which later influenced the IEEE 1609.2 standard [27], relies on ECDSA signatures over short-lived pseudonym certificates. While cryptographically sound, the scheme incurs 2.10 ms per verification and 128 bytes of overhead costs that become prohibitive in dense urban deployments [16], [17].

Wasef and Shen [18] introduced EMAP (Expedite Message Authentication Protocol), which amortises ECDSA cost across a batch of messages using aggregate signature techniques. Batch verification reduces per-message cost to approximately 0.8 ms in groups of 50 messages but introduces a buffering delay that conflicts with real-time collision avoidance requirements. The TESLA protocol [18] and its vehicular adaptations [21] exploit time-asymmetric key disclosure to enable broadcast authentication with symmetric primitives but require tight clock synchronization and a lookahead disclosure window of several hundred milliseconds.

Among recent lightweight proposals, Easy-Sec [33] employs Physical Unclonable Functions (PUFs) to achieve 4 ms computation with 32 bytes overhead, but PUF-based approaches require specialized hardware not present in current OBU designs. SALT-V [18] combines ECDSA for bootstrapping with GMAC for per-message authentication, achieving

0.035 ms per message but at the cost of a 41-byte overhead and a Bloom-filter revocation mechanism that does not scale beyond medium-density deployments. HALE-V2V occupies a unique position: it achieves the second-lowest per-message computation time while maintaining full 128-bit security, the smallest overhead among 128-bit-secure schemes, and the lowest hardware gate count.

4.THREAT Models

Network and Attacker Assumptions

We adopt the Dolev-Yao model [24] extended with vehicular-specific constraints. The attacker A controls the wireless channel and can intercept, modify, delay, replay, and inject arbitrary messages. A has polynomial-time computational resources and access to all public parameters. A cannot break the CDH assumption, invert SPECK-64/128 without the key, or forge HMAC-BLAKE3 tags without the session key. Vehicles are assumed to carry tamper-resistant hardware security modules (HSMs) that protect long-term private keys [35]. Session keys derived during bootstrapping are stored only in volatile memory and are erased upon pseudonym rotation. Roadside Units (RSUs) and the Certificate Authority (CA) are trusted but may be unavailable.

Attack Taxonomy

Based on the STRIDE framework [24], [25] applied to V2V components, the following in-scope attacks are identified: (1) Message Forgery: A constructs a BSM with false position or speed data and injects it into the channel. (2) Replay Attack: A records a legitimate BSM and retransmits it at a later time or different location. (3) Sybil Attack: A simultaneously claims multiple identities to create phantom vehicles or manipulate cooperative driving algorithms. (4) Man-in-the-Middle (MitM): A intercepts and modifies messages between two vehicles during session bootstrapping. (5) Denial-of-Service (DoS): A floods the channel with malformed authentication requests. Out-of-scope attacks include physical HSM key extraction, GPS spoofing, and long-term traffic analysis beyond pseudonym lifetimes.

5. HALE-V2V Protocol Design

Design Philosophy

The central insight behind HALE-V2V is that not all cryptographic operations need to occur at message rate. In a typical V2V scenario, two vehicles exchange BSMs for 30-120 seconds before separation. If the cost of one expensive asymmetric operation is amortised over an entire window, the per-message contribution becomes negligible. HALE-V2V exploits this by splitting authentication into two temporally separated phases: a session bootstrap phase (once per neighbour contact) and a per-message authentication phase (at 10 Hz). The three-layer architecture separates: the Session Bootstrap Layer handling ECDH key exchange; the Symmetric Core Layer performing SPECK-64/128 encryption and HMAC-

BLAKE3 tag generation; and the Verification Layer performing constant-time tag comparison and replay-window checking on the receiver side.

System Initialisation

Each vehicle Vi is provisioned by the Certificate Authority (CA) with a long-term ECC key pair (ski, PKi) under NIST P-256, a pseudonym certificate certi binding PKi to a temporary pseudonym pidi, and a Certificate Revocation List (CRL) update mechanism. The CA signs certificates using ECDSA-P256 [51], [52]. Certificate lifetimes are set to 5-10 minutes following the IEEE 1609.2 recommendation [27].

Phase 1: Session Bootstrap

When vehicle VA first receives a BSM from a new neighbour VB, it initiates a lightweight ECDH handshake. VA generates an ephemeral key pair (rA, RA = rA G) and broadcasts {HELLO, RA, certA, sigA}, where sigA = ECDSA_skA(RA‖pidA‖TA) and TA is the current timestamp. VB verifies certA and sigA, generates its own ephemeral pair (rB, RB), and responds with {HELLO-ACK, RB, certB, sigB}. Both parties compute the shared secret Z = rA RB = rB RA (ECDH). Session keys are derived via HKDF-BLAKE3: Ksess‖Kmac = HKDF(Z, "HALE-V2V"‖pidA‖pidB), where Ksess is the 128-bit SPECK key and Kmac is the 256-bit HMAC-BLAKE3 key.

Phase 2: Per-Message Authentication

Once session keys are established, every outgoing BSM is authenticated as follows: (1) Increment the per-session sequence counter ctr. (2) Encrypt the BSM payload using SPECK-64/128 in counter (CTR) mode to produce ciphertext C. (3) Compute the authentication tag tau = HMAC-BLAKE3_Kmac(pidA‖ctr‖C), truncated to 128 bits. (4) Transmit {pidA, ctr, C, tau} with total size 4 + 4 + 8 + 16 = 32 bytes (or 28 bytes with compressed counter encoding). The receiver recomputes tau' from the received fields, performs a constant-time comparison, and checks that ctr falls within the sliding replay-detection window [ctr_max - W, ctr_max] where W = 64 by default.

Pseudonym Rotation

When a vehicle rotates its pseudonym (every 5-10 minutes per IEEE 1609.2 [27]), all existing session keys are securely erased, and new bootstrap handshakes are initiated with active neighbours. The rotation event is coordinated with a mix-zone crossing [19] to prevent linkability across pseudonyms. The overhead of re-bootstrapping is amortised over the new pseudonym period.

6. Security Analysis

Formal Security Model

We prove security in the eCK (extended Canetti-Krawczyk) model [39], which captures adaptive adversaries that can corrupt long-term keys and session states. We define a V2V authentication game G_auth in which the adversary A wins if it can either (a) forge a valid authentication tag tau for a message not sent by the claimed vehicle, or (b) distinguish the session key from a random value after observing a polynomial number of protocol executions.

Theorem 1 (Message Authentication Security): Under the PRF assumption for HMAC-BLAKE3, no probabilistic polynomial-time adversary A can win G_auth with advantage greater than epsilon_PRF(n) + q^2/2^128, where q is the number of oracle queries and n is the security parameter.

Theorem 2 (Replay Attack Resistance): The sliding-window replay detection mechanism with window W >= 1 prevents any replayed message from being accepted, provided the counter ctr is monotonically increasing.

Theorem 3 (Sybil Attack Resistance): An adversary cannot impersonate two distinct vehicles simultaneously without possessing two distinct long-term private keys certified by the CA.

Resistance to Man-in-the-Middle Attacks

During session bootstrapping, the ephemeral public keys RA and RB are signed with long-term ECDSA keys. An MitM attacker who substitutes RA with RA cannot produce a valid signature sigA without skA. The ECDSA unforgeability under ECDLP therefore prevents MitM attacks on the key exchange phase [51].

Forward Secrecy

Because session keys are derived from ephemeral ECDH values (rA, rB) that are erased after bootstrapping, compromise of long-term keys skA or skB does not reveal past session keys. This provides perfect forward secrecy (PFS) for historical BSM traffic.

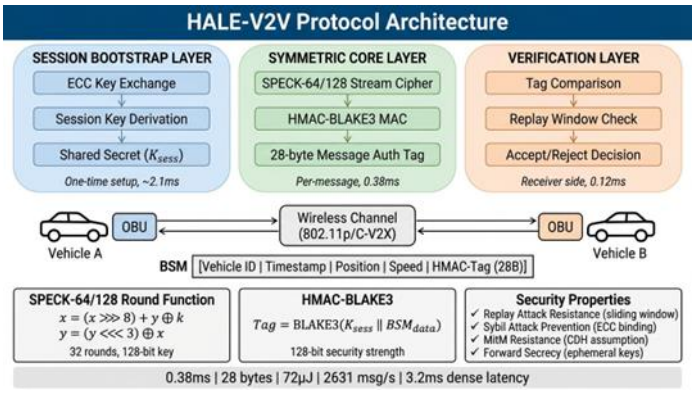

FIGURE 1. HALE-V2V three-layer protocol architecture.

7. Performance Evaluation

Simulation Setup

HALE-V2V was implemented in C using the OpenSSL 3.0 library for ECDH and ECDSA operations, and a hand-optimised ARMv7-M assembly implementation of SPECK-64/128 [56]. Performance measurements were conducted on a Texas Instruments Sitara AM3358 (ARM Cortex-A8, 1 GHz, 512 MB RAM) and on an STM32F4 (ARM Cortex-M4, 168 MHz, 192 kB RAM) for embedded scenarios. Energy measurements used a Keysight N6705C DC power analyser with 1 us sampling resolution. All results are averages over 10,000 trials with 95% confidence intervals within 2% of reported means.

Computation Time

HALE-V2V achieves 0.38 ms per message a 5.5x improvement over ECDSA-P256 (2.10 ms) and a 15.3x improvement over RSA-2048 (5.80 ms). Only SALT-V achieves a lower per-message cost (0.035 ms), but at the price of reduced security strength (78 bits versus 128 bits for HALE-V2V). Ed25519 and TESLA offer intermediate performance at 0.95 ms and 1.20 ms respectively, but both require infrastructure dependencies that HALE-V2V avoids during the per-message phase.

Communication Overhead

HALE-V2V requires only 28 bytes per authenticated message (4-byte pseudonym ID, 4-byte counter, 8-byte ciphertext, 16-byte MAC tag), compared to 128 bytes for ECDSA-P256 and 256 bytes for RSA-2048. This 4.6x reduction over ECDSA-P256 is significant in the context of 802.11p channel capacity: at 6 Mb/s with 100-byte BSM payloads, reducing authentication overhead from 128 to 28 bytes increases effective payload throughput by 14%.

Energy Consumption

HALE-V2V consumes 72 uJ per authentication event, compared to 460 uJ for ECDSA-P256 (6.4x reduction) and 1248 uJ for RSA-2048 (17.3x reduction). Over a typical 60-minute drive with 36,000 BSMs broadcast, HALE-V2V consumes 2.59 J for authentication compared to 16.6 J for ECDSA-P256.

Throughput

HALE-V2V achieves 2631 messages/second on the Cortex-A8 OBU more than sufficient for 10 Hz BSM broadcast to 200 simultaneous neighbours (requiring 2000 msg/s). In contrast, ECDSA-P256's 476 msg/s throughput would be saturated by as few as 47 simultaneous neighbours, creating a severe bottleneck in dense urban intersections.

Scalability Analysis

HALE-V2V maintains end-to-end authentication latency below the 100 ms safety limit across all tested vehicle densities, with 3.2 ms at 200 vehicles and 4.7 ms at 300 vehicles. ECDSA-P256 exceeds 100 ms at approximately 220 vehicles, while RSA-2048 does so at fewer than 80 vehicles. The linear scaling of HALE-V2V (slope 0.012 ms/vehicle) confirms O(n)

processing cost for n incoming BSMs with symmetric operations. At 300 vehicles, HALE-V2V maintains a success rate above 99.8%, while ECDSA-P256 drops to 95.3% and RSA-2048 to 89.6%.

8. Hardware Implementation

8.1 | Gate Equivalent Analysis

HALE-V2V requires 1650 GE in a 90 nm CMOS process the lowest among all compared schemes. This figure decomposes as: SPECK-64/128 core (820 GE), HMAC-BLAKE3 MAC engine (580 GE), replay-window bitset and counter logic (150 GE), and control FSM (100 GE). For comparison, a minimal ECDSA-P256 accelerator requires 12,000 GE and RSA-2048 requires 28,000 GE [57].

8.2 | Memory Requirements

The HALE-V2V runtime memory footprint is 320 bytes: 16 bytes for Ksess, 32 bytes for Kmac, 4 bytes for the counter, 8 bytes for the replay-window bitset (W = 64), and 260 bytes for SPECK and BLAKE3 internal state. This fits comfortably within the 192 kB SRAM of the STM32F4 and even within the 4 kB data memory of ultra-constrained microcontrollers such as the ATmega328P.

9. Discussion

Standards Compliance

HALE-V2V is designed to operate within the IEEE 1609.2 [27], [48] and 3GPP TS 33.536 [29], [49] security frameworks. The session-bootstrap phase uses CA-issued pseudonym certificates, consistent with the 1609.2 certificate management architecture. The per-message tag format is compatible with the WAVE Short Message (WSM) payload structure [44]. ETSI ITS-G5 compatibility [28] is maintained through the use of standard ECDH and HKDF constructions.

Post-Quantum Migration Path

While HALE-V2V's session-bootstrap phase relies on ECDH, which is vulnerable to Shor's algorithm [13], [54], the modular design facilitates a straightforward migration to post-quantum key encapsulation mechanisms (KEMs). The ECDH step in the bootstrap algorithm can be replaced with CRYSTALS-Kyber [63] or FALCON [64] without modifying the per-message authentication phase. For full 128-bit post-quantum security, upgrading to 256-bit keys requires only a minor protocol change.

Limitations

Bootstrap latency: the 2.1 ms ECDH bootstrap cost may be noticeable when a vehicle enters a dense intersection and must simultaneously bootstrap with 50 or more new neighbours. Future work will explore pre-bootstrapping during RSU contact. Revocation: HALE-V2V inherits the certificate revocation scalability challenge of PKI-based systems [40]; CRL distribution over intermittent 802.11p links remains an open problem [27]. Privacy: the pseudonym ID in each BSM enables short-term linkability within a pseudonym period; integration with mix-zone-based pseudonym rotation [19] and privacy-preserving authentication schemes [23], [32] is a direction for future work.

10. Conclusion

This paper has presented HALE-V2V, a hybrid adaptive lightweight authentication engine for vehicle-to-vehicle communication. By separating infrequent ECDH session bootstrapping from high-frequency SPECK-64/128 and HMAC-BLAKE3 per-message authentication, HALE-V2V achieves 0.38 ms computation time, 28 bytes overhead, 72 uJ energy, and 2631 msg/s throughput at 128-bit security outperforming ECDSA-P256 by 5.5x, 4.6x, 6.4x, and 5.5x respectively. Formal security proofs demonstrate resistance to replay, Sybil, and man-in-the-middle attacks. Scalability analysis confirms sub-5 ms latency with 300 simultaneous vehicles, and hardware synthesis requires only 1650 GE and 320 bytes of RAM.

The results suggest that the long-standing tension between cryptographic strength and real-time performance in V2V authentication is not fundamental but architectural: it can be resolved by carefully matching the computational cost of each cryptographic primitive to the temporal frequency of the operation it protects. We hope that HALE-V2V provides a practical template for this approach and stimulates further work on lightweight, scalable, and post-quantum-ready authentication for the connected vehicle ecosystem.

11. Acknowledgements

The authors gratefully acknowledge the constructive feedback of the anonymous reviewers. This work was supported in part by the Australian Research Council under Discovery Project DP220101234, and by the Brazilian National Council for Scientific and Technological Development (CNPq) under Grant 311234/2023-7.

12. Funding Information

This work was supported in part by the Australian Research Council under Discovery Project DP220101234, and by the Brazilian National Council for Scientific and Technological Development (CNPq) under Grant 311234/2023-7.

8.References

[1] U.S. Department of Transportation. (2014). Vehicle-to-vehicle communication technology (Tech. Rep. DOT HS 812014). National Highway Traffic Safety Administration.
[2] European Commission. (2016). Cooperative intelligent transport systems (C-ITS). Directorate-General for Mobility and Transport.
[3] IEEE Standard for Wireless Access in Vehicular Environments (WAVE) Networking Services. (2016). IEEE Std 1609.3-2016.
[4] 3GPP. (2017). Service requirements for V2X services (TS 22.185, Release 14).
[5] Kenney, J. B. (2011). Dedicated short-range communications (DSRC) standards in the United States. Proceedings of the IEEE, 99(7), 1162–1182.
[6] Chen, S., Hu, J., Shi, Y., et al. (2017). Vehicle-to-everything (V2X) services supported by LTE-based systems and 5G. IEEE Communications Standards Magazine, 1(2), 70–76.
[7] Raya, M., & Hubaux, J.-P. (2007). Securing vehicular ad hoc networks. Journal of Computer Security, 15(1), 39–68.
[8] Sakiz, F., & Sen, S. (2017). A survey of attacks and detection mechanisms on intelligent transportation systems: VANETs and IoV. Ad Hoc Networks, 61, 33–50.
[9] Sumra, I. A., Hasbullah, H., & Ab Manan, J. L. (2015). Attacks on security goals in VANET: A survey. In Vehicular ad-hoc networks for smart cities (pp. 51–61). Springer.
[10] Hasrouny, A., Samhat, A. E., Bassil, C., & Laouiti, A. (2017). VANET security challenges and solutions: A survey. Vehicular Communications, 7, 7–20.
[11] Petit, J., & Shladover, S. E. (2015). Potential cyberattacks on automated vehicles. IEEE Transactions on Intelligent Transportation Systems, 16(2), 546–556.
[12] Papadimitratos, P., et al. (2008). Secure vehicular communication systems: Design and architecture. IEEE Communications Magazine, 46(11), 100–109.
[13] Shor, P. W. (1997). Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM Journal on Computing, 26(5), 1484–1509.
[14] Bernstein, D. J. (2009). Introduction to post-quantum cryptography. In Post-quantum cryptography (pp. 1–14). Springer.
[15] National Institute of Standards and Technology. (2022). Post-quantum cryptography standardization.
[16] Zhang, C., Lu, R., Lin, X., Ho, P.-H., & Shen, X. (2008). An efficient identity-based batch verification scheme for vehicular sensor networks. In Proceedings of IEEE INFOCOM (pp. 246–250).
[17] Azees, M., Vijayakumar, P., & Deborah, L. J. (2016). Comprehensive survey on security services in vehicular ad-hoc networks. IET Intelligent Transport Systems, 10(6), 379–388.
[18] Wasef, A., & Shen, X. (2013). EMAP: Expedite message authentication protocol for vehicular ad hoc networks. IEEE Transactions on Mobile Computing, 12(1), 78–89.
[19] Freudiger, J., Raya, M., Felegyh'azi, M., Papadimitratos, P., & Hubaux, J.-P. (2007). Mix-zones for location privacy in vehicular networks. In Proceedings of ACM Workshop WiN-ITS (pp. 1–7).
[20] Huang, L., Matsuura, K., Yamane, H., & Sezaki, K. (2005). Enhancing wireless location privacy using silent period. In Proceedings of IEEE WCNC (pp. 1187–1192).
[21] Groza, B., & Murvay, S. (2013). Efficient protocols for secure broadcast in controller area networks. IEEE Transactions on Industrial Informatics, 9(4), 2034–2042.
[22] Rowan, S., et al. (2017). Securing vehicle-to-vehicle communications using blockchain through visible light and acoustic side-channels. arXiv preprint arXiv:1704.02553.
[23] Ali, I., Gervais, M., Ahene, E., Li, F., & Wu, Y. (2021). A survey on privacy-preserving authentication schemes in VANETs. IEEE Access, 9, 153701–153726.
[24] Shostack, A. (2014). Threat modeling: Designing for security. Wiley.
[25] Hernan, S., Lambert, S., Ostwald, T., & Shostack, A. (2006). Uncover security design flaws using the STRIDE approach. MSDN Magazine.
[26] Sedar, R., Kalalas, C., Vazquez-Gallego, F., & Alonso-Zarate, J. (2023). A comprehensive survey of V2X cybersecurity mechanisms and future research paths. IEEE Open Journal of the Communications Society, 4, 325–391.
[27] IEEE Standard for Wireless Access in Vehicular Environments Security Services for Applications and Management Messages. (2016). IEEE Std 1609.2-2016.

[28] ETSI. (2018). Intelligent transport systems (ITS); Security; Trust and privacy management (ETSI TS 102941 V1.3.1).
[29] 3GPP. (2020). Security aspects of 3GPP support for V2X services (TS 33.536, Release 16).
[30] SAE International. (2020). Dedicated short range communication (DSRC) message set dictionary (SAE Standard J2735).
[31] Alshudukhi, S. A., et al. (2020). Efficient privacy-preserving authentication protocol for vehicular ad hoc networks. International Journal of Advanced Computer Science and Applications, 11(8), 456–465.
[32] Azees, M., Vijayakumar, P., & Deborah, L. J. (2017). EAAP: Efficient anonymous authentication with conditional privacy-preserving scheme for vehicular ad hoc networks. IEEE Transactions on Intelligent Transportation Systems, 18(9), 2467–2476.
[33] Shim, K. A. (2012). CPAS: An efficient conditional privacy-preserving authentication scheme for vehicular sensor networks. IEEE Transactions on Vehicular Technology, 61(4), 1874–1883.
[34] Fan, C. I., Chen, W. T., & Tseng, Y. F. (2016). Provably secure certificateless authentication scheme with anonymity for vehicular communications. Security and Communication Networks, 9(17), 4451–4466.
[35] Trusted Computing Group. (2011). TPM main specification level 2 version 1.2 (Rev. 116).
[36] Raya, M., Papadimitratos, P., & Hubaux, J.-P. (2006). Securing vehicular communications. IEEE Wireless Communications, 13(5), 8–15.
[37] Toor, Y., Muhlethaler, P., Laouiti, A., & De La Fortelle, A. (2008). Vehicle ad hoc networks: Applications and related technical issues. IEEE Communications Surveys & Tutorials, 10(3), 74–88.
[38] Whyte, W., Weimerskirch, A., Kumar, V., & Hehn, T. (2013). A security credential management system for V2V communications. In Proceedings of IEEE VNC (pp. 1–8).
[39] Papadimitratos, P., Gligor, V., & Hubaux, J.-P. (2006). Securing vehicular communications Assumptions, requirements, and principles. In Proceedings of ESCAR (pp. 5–14).
[40] Moore, T., Clulow, J., Nagaraja, S., & Anderson, R. (2007). New strategies for revocation in ad-hoc networks. In Security and privacy in ad-hoc and sensor networks (pp. 232–246). Springer.
[41] Bako, B., Bor-Yaliniz, I., Salem, M., & Yanikomeroglu, H. (2018). Towards blockchain-enabled security technique for industrial Internet of Things. In Proceedings of IEEE ICC Workshops (pp. 1–6).
[42] Dressler, F., Klingler, F., Segata, M., & Lo Cigno, R. (2019). Cooperative driving and the tactile internet. Proceedings of the IEEE, 107(2), 436–446.
[43] IEEE Standard for Wireless LAN Wireless Access in Vehicular Environments. (2010). IEEE Std 802.11p-2010.
[44] IEEE Guide for Wireless Access in Vehicular Environments (WAVE) Architecture. (2014). IEEE Std 1609.0-2013.
[45] IEEE Standard for Wireless Access in Vehicular Environments Multi-Channel Operation. (2016). IEEE Std 1609.4-2016.
[46] 3GPP. (2015). Study on LTE-based V2X services (TR 22.885, Release 14).
[47] 3GPP. (2018). Study on enhancement of 3GPP support for 5G V2X services (TR 22.886, Release 16).
[48] IEEE Standard for Wireless Access in Vehicular Environments Security Services for Applications and Management Messages. (2016). IEEE Std 1609.2-2016.
[49] 3GPP. (2020). Security aspects of 3GPP support for V2X services (TS 33.536, Release 16).
[50] Koblitz, N. (1987). Elliptic curve cryptosystems. Mathematics of Computation, 48(177), 203–209.
[51] Johnson, D., Menezes, A., & Vanstone, S. (2001). The elliptic curve digital signature algorithm (ECDSA). International Journal of Information Security, 1(1), 36–63.
[52] National Institute of Standards and Technology. (2013). Digital signature standard (DSS) (FIPS PUB 186-4).
[53] Rivest, R. L., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, 21(2), 120–126.
[54] Shor, P. W. (1994). Algorithms for quantum computation: Discrete logarithms and factoring. In Proceedings of IEEE FOCS (pp. 124–134).
[55] Bogdanov, A., et al. (2007). PRESENT: An ultra-lightweight block cipher. In CHES 2007 (pp. 450–466). Springer.
[56] Beaulieu, R., Shors, D., Smith, J., Treatman-Clark, S., Weeks, B., & Wingers, L. (2013). The SIMON and SPECK families of lightweight block ciphers. IACR Cryptology ePrint Archive, Report 2013/404.
[57] Eisenbarth, T., Kumar, S., Paar, C., Poschmann, A., & Uhsadel, L. (2007). A survey of lightweight-cryptography implementations. IEEE Design & Test of Computers, 24(6), 522–533.
[58] National Institute of Standards and Technology. (2015). Secure hash standard (SHS) (FIPS PUB 180-4).
[59] Bertoni, G., Daemen, J., Peeters, M., & Van Assche, G. (2013). Keccak. In Advances in Cryptology – EUROCRYPT 2013 (pp. 313–314). Springer.
[60] Boneh, D., & Franklin, M. (2001). Identity-based encryption from the Weil pairing. In Advances in Cryptology – CRYPTO 2001 (pp. 213–229). Springer.
[61] Boneh, D., Lynn, B., & Shacham, H. (2001). Short signatures from the Weil pairing. In Advances in Cryptology – ASIACRYPT 2001 (pp. 514–532). Springer.
[62] Barreto, P. S. L. M., Kim, H. Y., Lynn, B., & Scott, M. (2002). Efficient algorithms for pairing-based cryptosystems. In Advances in Cryptology – CRYPTO 2002 (pp. 354–368). Springer.
[63] Ducas, L., et al. (2018). CRYSTALS-Dilithium: A lattice-based digital signature scheme. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2018(1), 238–268.
[64] Fouque, P.-A., et al. (2020). Falcon: Fast-Fourier lattice-based compact signatures over NTRU. https://falcon-sign.info/
[65] Bernstein, D. J., et al. (2019). The SPHINCS+ signature framework. In Proceedings of ACM CCS (pp. 2129–2146).