Beyond Computation: A Fragmentation-Aware Performance Analysis of Cryptographic Schemes for Real-Time C-V2X Cooperative Perception

Mason Minear, Mike Haggart, and Junaid Khan
Western Washington University, WA, USA
minearm, haggarm, junaid.khan@wwu.edu

***Abstract*—Securing cooperative perception messages in Cellular Vehicle-to-Everything (C-V2X) networks creates a conflict between cryptographic overhead and stringent low-latency requirements. Traditional performance analyses often focus on computational cost, overlooking network-layer impacts like packet fragmentation. This paper evaluates AES, ECC, RSA, and Homomorphic Encryption (HE) through high-fidelity simulations under network congestion. We demonstrate a critical finding: while computationally feasible in some regards, HE's massive ciphertext expansion leads to packet fragmentation and catastrophic end-to-end latency, rendering it unsuitable for real-time applications. Our results establish that network-layer constraints, not just computational cost, are the primary limiting factor for deploying advanced cryptography in vehicular networks.**

***Index Terms*—Vehicular Networks, C-V2X, Cooperative Perception, Cybersecurity, Performance Evaluation, Latency, Homomorphic Encryption, MTU Fragmentation.**

I. Introduction

The evolution of intelligent transportation systems hinges on the transition from isolated vehicle autonomy to cooperative mobility. Connected and Autonomous Vehicles (CAVs) leverage next-generation communication technologies like Cellular Vehicle-to-Everything (C-V2X) to share sensor data, enabling Cooperative Perception (CP) [1]. By fusing data from neighboring vehicles—communicated via direct sidelink channels—CAVs can build a comprehensive environmental model. This extended perception allows vehicles to perceive hazards beyond their direct line-of-sight and sensor range, drastically improving situational awareness and preventing accidents.

The effectiveness of CP, however, is predicated on the timely and reliable delivery of high-frequency messages. For safety-critical functions such as collision avoidance, C-V2X standards aim for ultra low end-to-end latency. This reliance on open-channel wireless communication introduces significant security vulnerabilities. Malicious actors can intercept, modify, or inject false messages to compromise vehicle behavior, cause collisions, or track user movements [2]. Therefore, implementing robust cryptographic measures to ensure confidentiality, integrity, and authenticity is not optional.

However, cryptography introduces computational and communication overhead, creating a fundamental tension between security requirements and performance constraints. This overhead manifests in two ways: (1) computational delay for encryption and decryption operations, and (2) communication delay from increased packet size due to ciphertext, padding, and metadata. This second factor is particularly critical in C-V2X, where radio resources are shared and packet size directly impacts channel load and transmission time.

While numerous studies have evaluated standard encryption algorithms for vehicular networks [3], emerging privacy-preserving techniques introduce new challenges. Homomorphic Encryption (HE), for example, offers the powerful capability to perform computations on encrypted data. This feature is attractive for privacy-preserving aggregation by third parties in a C-V2X architecture. [4] However, the practical implications of HE's significant data expansion on a congested, real-time network stack are not well understood. Most analyses focus on computational complexity in isolation, overlooking the cascading effects at the network layer [5].

This paper addresses this critical gap by ana-

lyzing how cryptographic overhead impacts C-V2X network performance, particularly under congestion and subject to practical constraints like the Maximum Transmission Unit (MTU). We hypothesize that for advanced schemes, the network transmission cost associated with large ciphertexts far outweighs the computational cost. Our contributions are:

1) A C-V2X Simulation Framework for Cryptographic Analysis in ns-3 representing a dense urban grid with progressive network load, designed specifically to isolate and measure the impact of encryption-induced packet size changes on network latency.
2) Comparative Performance Analysis to evaluate four distinct cryptographic schemes (AES, RSA, ECC, and Homomorphic Encryption) across varying message payloads, quantifying computational overhead and end-to-end latency.
3) Identification of Fragmentation Bottleneck through simulation data that Homomorphic Encryption's massive ciphertext expansion forces extensive packet fragmentation to comply with standard network MTU limits.

II. Related Work

The performance of standard cryptographic primitives in vehicular networks is well-understood. Literature confirms Elliptic Curve Cryptography (ECC) offers superior efficiency over RSA for asymmetric operations like digital signatures [4], [3]. AES is also accepted as highly efficient for symmetric payload encryption.

The motivation for exploring advanced cryptography stems from the known limitations of standard privacy mechanisms. Pseudonym-based schemes [6] are vulnerable to spatio-temporal tracking attacks, driving research toward techniques like Homomorphic Encryption (HE). However, existing research on HE in V2X primarily focuses on non-real-time data aggregation tasks where latency constraints are relaxed. These analyses often overlook the practical network-layer implications of HE's significant data expansion on a congested, real-time network stack.

This gap is particularly critical because not all HE schemes are alike. Modern HE research has focused on mitigating ciphertext expansion through two primary avenues: (1) Lightweight or Compact Schemes designed for specific, limited operations [7], and (2) Batching (or 'packing') Techniques [8], where multiple plaintexts are encrypted into a single ciphertext. These state-of-the-art approaches are designed to amortize the high overhead of HE, but are infeasible in real time C-V2X communication of cooperative perception messages with stringent latency and information completeness requirements.

This paper, therefore, addresses a critical gap. Before evaluating complex, batched, or lightweight schemes, it is essential to first establish a quantitative baseline for a general-purpose, non-batched HE scheme. This allows us to isolate and measure the fundamental network-layer bottleneck, providing a crucial reference point for the V2X community and motivating the need for network-aware designs in any future HE implementation

III. Methodology and Simulation Setup

A. Threat Model

We assume a C-V2X environment where malicious actors can conduct network-level attacks. The primary threats considered are (i) Eavesdropping (Confidentiality) where an attacker on the sidelink channel can intercept and read the contents of unencrypted cooperative perception messages. This is addressed by payload encryption (e.g., AES). (ii) Message Falsification (Integrity/Authenticity) where an attacker can inject false or modified messages to cause collisions or disrupt traffic flow. This is typically addressed by digital signatures (e.g., ECC-based). (iii) Spatio-temporal Tracking (Privacy) where an attacker can link messages over time, even if they are pseudonymously signed, to track a vehicle's movements. This threat is the primary motivation for exploring privacy-preserving computation like Homomorphic Encryption.

Our analysis evaluates the performance cost of cryptographic countermeasures (AES, ECC, RSA, HE) against these distinct threats.

To evaluate the performance trade-offs of the cryptographic schemes, we established a controlled and reproducible simulation environment using ns-3.

B. Network Topology and Environment

The simulation scenario involved 200 static nodes arranged in a uniform 20x10 grid. The choice of

a static grid eliminates variables associated with mobility (planned as future work), allowing for a focused analysis on the performance impact of cryptographic overhead under congestion. Nodes were positioned with uniform spacing: 20 meters along the x-axis and 4 meters along the y-axis, emulating vehicles in multiple lanes of a dense urban environment. The communication range for each node is set to 200 meters.

C. C-V2X Network Model and Traffic Generation

We modeled the communication stack based on C-V2X specifications. A critical parameter for our analysis is the Maximum Transmission Unit (MTU), which was set to 1420 bytes, a standard value for packet-based services over modern cellular networks. Any IP packet larger than this size must be fragmented by the network layer before transmission.

To analyze performance under varying network loads, we implemented a progressive congestion model. Nodes transmitted messages with payload sizes ranging from 100 to 1000 bytes, increasing in 100-byte increments across separate simulation runs. In each run, every node transmitted a burst of 40 packets at a high rate (inter-packet interval of 0.005 seconds), producing a total transmission time of 0.2 seconds per node. This rapid transmission design forces the network state to evolve quickly from uncongested to highly congested.

D. Cryptographic Formulations and Implementation Models

We evaluated four schemes, each with distinct mathematical foundations that influence performance.

1) AES (Advanced Encryption Standard): AES is a symmetric block cipher based on substitution-permutation networks. Its efficiency stems from highly optimized round operations (SubBytes, ShiftRows, MixColumns, AddRoundKey).

2) RSA (Rivest-Shamir-Adleman): RSA is an asymmetric algorithm whose security relies on factoring large integers $n = pq$. To encrypt a plaintext message m, the ciphertext c is calculated as $c = m^e \pmod{n}$. Decryption reverses this process: $m = c^d \pmod{n}$.

3) ECC (Elliptic Curve Cryptography): ECC's security leverages the hardness of the elliptic curve discrete logarithm problem ($P = kG$). For key exchange (ECDH), users with private keys k_A and k_B exchange public keys $P_A = k_A \cdot G$ and $P_B = k_B \cdot G$ to independently calculate a shared secret $S = k_A \cdot P_B = k_B \cdot P_A$.

4) Homomorphic Encryption (HE): HE allows computation on encrypted data. Many HE schemes rely on lattice-based cryptography and the Learning With Errors (LWE) problem. To manage noise inherent in the process, ciphertext parameters must be large, which leads to significant data expansion. We used PALISADE (Practical Lattice Cryptography for Advanced Security Applications and Data Encryption) [9]. A library for advanced cryptographic techniques, including homomorphic encryption, to achieve scalability and real-time applications.

E. Performance Metrics and Measurement Strategy

KPIs were collected using a custom V2xKpi module integrated with a SQLite database. The primary metrics were computational overhead and end-to-end latency. For fragmented messages, latency was specifically defined as the total duration from the transmission of the first fragment to the successful reception and reassembly of the final fragment at the destination.

IV. Performance Evaluation and Results

Our analysis first investigates computational overhead before moving to network latency. The results reveal performance profiles that are not apparent from a high-level comparison alone.

A. Computational Overhead Analysis

1) AES Efficiency Profile: The computational cost of AES is negligible. Both encryption and decryption complete in exceptionally short timeframes, measured in microseconds. While a slight positive correlation between message length and processing time exists, the absolute increase is insignificant for this application context. This establishes AES as the baseline for minimal computational impact.

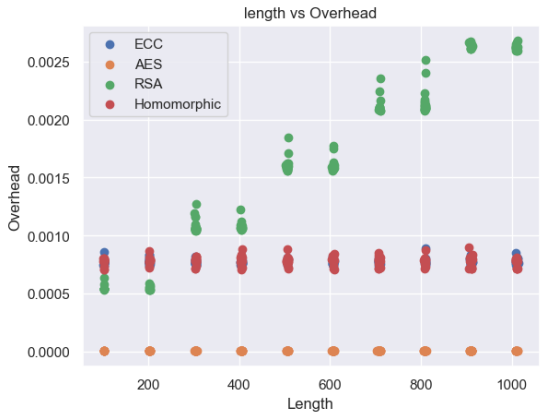
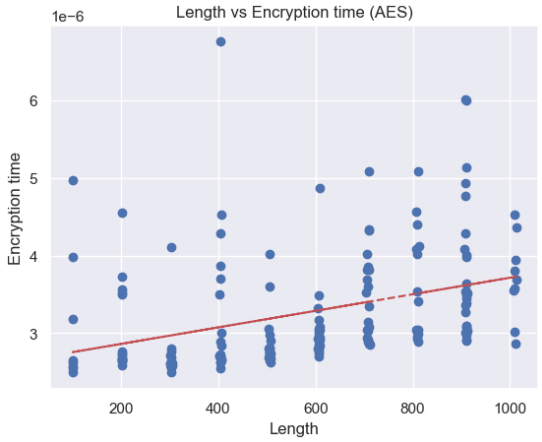
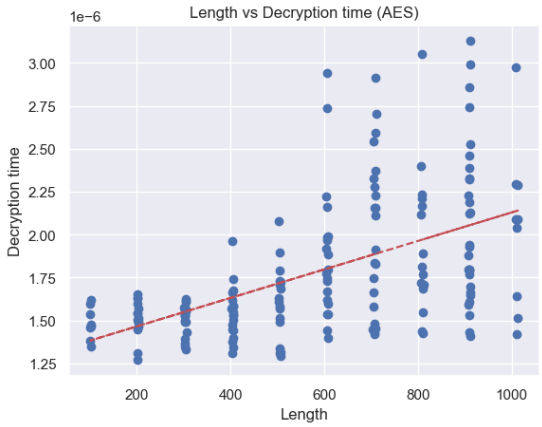


Fig. 1: Overhead comparison



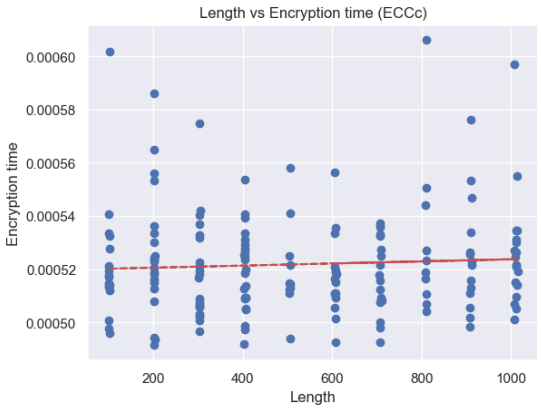
(a) AES Encryption



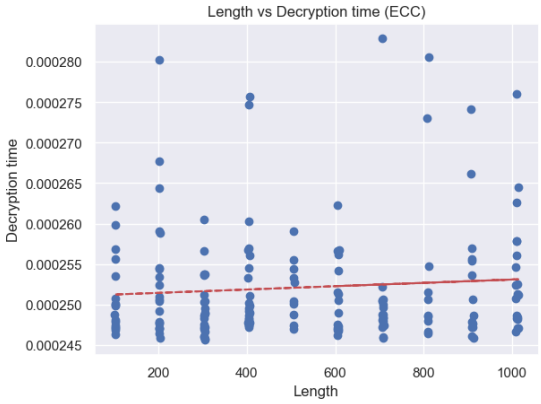
(b) AES Decryption

Fig. 2: AES Encryption and Decryption time

2) ECC Performance Characteristics: The computational demands for ECC are significantly higher than for AES, with processing times measured in hundreds of microseconds. However, performance remains stable and predictable across all message lengths. This predictability makes ECC suitable for periodic, high-security operations like key exchanges.



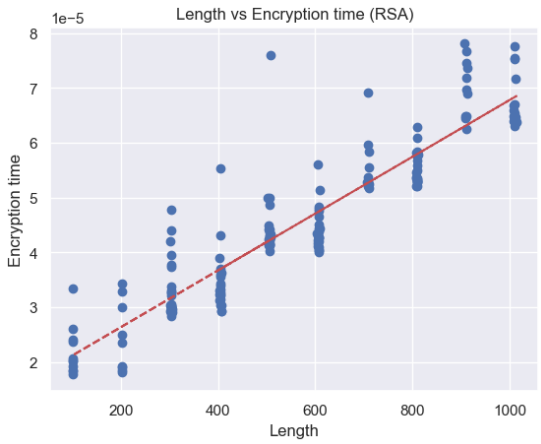
(a) ECC Encryption



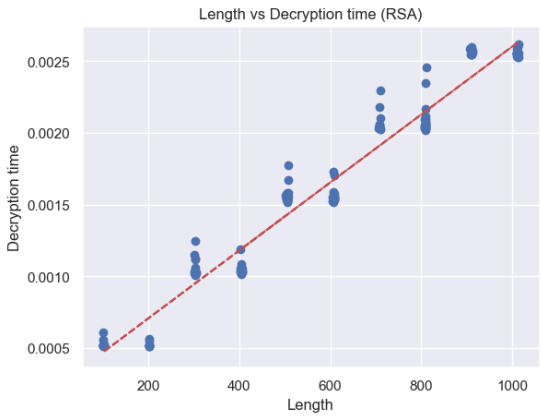
(b) ECC Decryption

Fig. 3: ECC Encryption and Decryption time

3) RSA Asymmetry and Bottlenecks: RSA exhibits critical performance asymmetries. RSA encryption time exhibits a distinct **step function**, where processing time increases sharply at specific message size thresholds (e.g., every 256 bytes), corresponding to its block-based processing nature. Conversely, RSA decryption time shows a strong positive correlation with message length and is significantly higher than encryption time, confirming decryption as a major computational bottleneck.

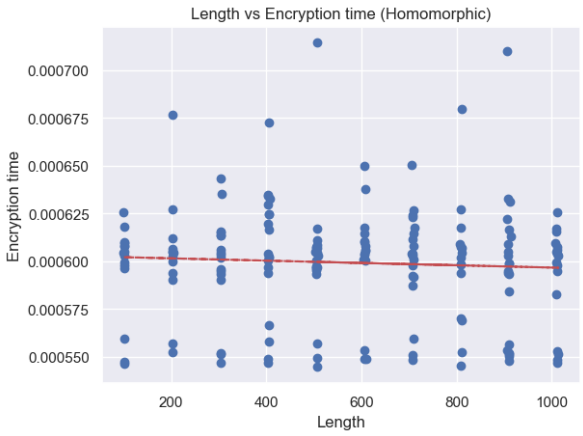


(a) RSA Encryption

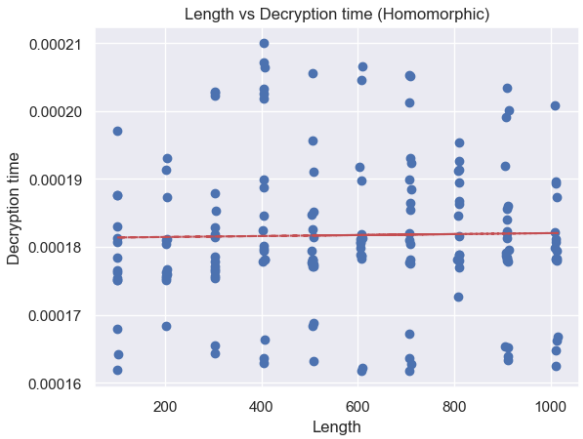


(b) RSA Decryption

Fig. 4: RSA Encryption and Decryption time



(a) HE Encryption



(b) HE Decryption

Fig. 5: Homomorphic Encryption and Decryption time

4) Homomorphic Encryption Computational Profile: A counter-intuitive finding is that HE's computational cost, while higher than AES, is surprisingly comparable in magnitude to ECC's. Both encryption and decryption times are relatively stable. This crucial observation demonstrates that for single encryption/decryption operations, processing cost itself is not the primary barrier for HE. This allows us to definitively conclude that HE's failure point lies elsewhere.

B. Network Latency and Ciphertext Expansion

Network latency provides a more practical measure of performance, as it incorporates both processing time and communication overhead.

1) Baseline Latency: The latency profile for AES-encrypted packets is nearly identical to the non-encrypted baseline, proving that its minimal size overhead has no discernible impact on network transmission time. ECC introduces a moderate overhead (100 bytes), resulting in a small but consistent increase in latency.

2) Impact of RSA Packet Size: Due to its larger packet size increase (adding over 256 bytes even for small messages), RSA's latency is consistently higher than AES and ECC. This gap widens for larger original message sizes, demonstrating how fixed overhead disproportionately increases network contention under load.

C. A Network-Layer Failure Case for Homomorphic Encryption

The most significant finding of this study concerns Homomorphic Encryption. While computa-

tionally comparable to ECC, HE's ciphertext size was measured to be over **88,000 bytes**. Given the 1420-byte MTU of our simulated C-V2X network, transmitting a single HE-encrypted message required fragmentation into approximately **62 packets**.

This resulted in a catastrophic increase in latency. We term this phenomenon a **fragmentation cascade failure**. The extreme delay is caused by the high probability of failure during the reassembly process in a congested network. The loss or delay of even a single fragment stalls the reassembly of the entire original message. This fragility makes HE fundamentally unusable for real-time safety applications in its current form.

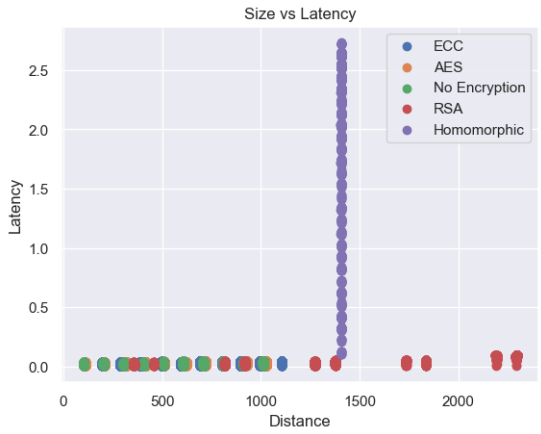


Fig. 6: Latency performance collapse of Homomorphic Encryption due to network fragmentation.

V. Discussion and Implications

The results of our analysis present critical insights into the practical deployment of cryptographic protocols in real-time vehicular networks.

A primary takeaway from this study is that evaluating cryptographic protocols solely on computational overhead is insufficient for network-bound systems.

The catastrophic latency observed for HE warrants a deeper examination of the underlying mechanism. The loss of even a single fragment forces the entire reassembly process to stall, awaiting retransmission, rendering the concept of real-time communication impossible.

Based on these findings, we propose practical recommendations for engineers designing secure C-V2X systems to prioritize Low Data Expansion and Adopt a Hybrid Approach combining different schemes based on need

VI. Conclusion

We presented a fragmentation-aware performance analysis of cryptographic schemes for securing cooperative perception messages in C-V2X networks. We show using high-fidelity simulations that HE's massive ciphertext expansion leads to extensive packet fragmentation, causing an increase in end-to-end latency that renders it unsuitable for any safety-critical, real-time application. The findings underscore a critical lesson for the V2X community: designing secure and efficient systems requires a cross-layer approach, where protocol performance must be considered in the context of network constraints.

References

[1] Guiyang Luo, Chongzhang Shao, Nan Cheng, Haibo Zhou, Hui Zhang, Quan Yuan, and Jinglin Li. Edgecooper: Network-aware cooperative lidar perception for enhanced vehicular awareness. *IEEE Journal on Selected Areas in Communications*, 2023.

[2] Shunli Ren, Zixing Lei, Zi Wang, Mehrdad Dianati, Yafei Wang, Siheng Chen, and Wenjun Zhang. Interruption-aware cooperative perception for v2x communication-aided autonomous driving. *IEEE Transactions on Intelligent Vehicles*, 9(4):4698–4714, 2024.

[3] Mahmood A Al-Shareeda, Mohammed Anbar, Selvakumar Manickam, Ayman Khalil, and Iznan Husainy Hasbullah. Security and privacy schemes in vehicular ad-hoc network with identity-based cryptography approach: A survey. *IEEE Access*, 9:121522–121531, 2021.

[4] Xiaoqiang Sun, F Richard Yu, Peng Zhang, Weixin Xie, and Xiang Peng. A survey on secure computation based on homomorphic encryption in vehicular ad hoc networks. *Sensors*, 20(15):4253, 2020.

[5] Seiya Jumonji, Kazuya Sakai, Min-Te Sun, and Wei-Shinn Ku. Privacy-preserving collaborative filtering using fully homomorphic encryption. *IEEE Transactions on Knowledge and Data Engineering*, 35(3):2961–2974, 2021.

[6] Mahmood A Al-Shareeda, Mohammed Anbar, Selvakumar Manickam, and Iznan H Hasbullah. A secure pseudonym-based conditional privacy-preservation authentication scheme in vehicular ad hoc networks. *Sensors*, 22(5):1696, 2022.

[7] Songzhan Lv and Yining Liu. Plva: privacy-preserving and lightweight v2i authentication protocol. *IEEE Transactions on Intelligent Transportation Systems*, 23(7):6633–6639, 2021.

[8] Donghwan Kim, Jaiyoung Park, Jongmin Kim, Sangpyo Kim, and Jung Ho Ahn. Hyphen: A hybrid packing method and its optimizations for homomorphic encryption-based neural networks. *IEEE Access*, 12:3024–3038, 2023.

[9] Palisade homomorphic encryption library, 2025.