

Article

An optimal secure authenticated key exchange scheme for vehicular cloud computing using Schnorr signcryption with HECC

Rashid Ahmed¹, Riaz Shah², Mohsin Shah¹, Noor Ul Amin¹

¹Department of Telecommunication, Hazara University, Mansehra, KP, Pakistan

²Department of Computer Science, Hazara University, Mansehra, KP, Pakistan

E-mail: rashidyusufzai687@gmail.com, riazshah15654@gmail.com, syedmohsinshah@gmail.com, naminhu@hu.edu.pk

Received 27 September 2026; Accepted 11 October 2026; Published online 15 October 2026; Published 1 December 2026



Abstract

Vehicular Cloud Computing (VCC) combines vehicular ad hoc networking with cloud resources to support safety, traffic-management, infotainment, storage, and computation services. Because vehicles and roadside components communicate over dynamic wireless links, authentication, confidentiality, integrity, and resistance to impersonation and replay attacks are important requirements. This paper presents a secure authenticated key exchange scheme for VCC based on Schnorr signcryption and hyperelliptic curve cryptography (HECC). The scheme uses sender and receiver authentication phases and one-way hash operations to establish mutual authentication before data transfer. We evaluate the scheme using MATLAB and compares its computational cost with selected elliptic-curve and hyperelliptic-curve signcryption schemes. In the reported experiments, the proposed scheme requires 1.44 ms for signcryption and 1.92 ms for unsigncryption, giving a reported total of 3.36 ms. The paper also reports reduced key-size requirements for HECC relative to the ECC parameters used in its comparison. Security analysis in the source work addresses confidentiality, integrity, authenticity, and unforgeability. The results indicate a reduction in the reported computational overhead; however, the study is based on simulation and source-reported operation costs, so broader implementation and formal security validation are appropriate directions for future work.

Keywords vehicular cloud computing; VANET; Schnorr signcryption; hyper elliptic curve cryptography; authentication; key exchange; security; computational cost.

Selforganizology

ISSN 2410-0080

URL: <http://www.iaees.org/publications/journals/selforganizology/online-version.asp>

RSS: <http://www.iaees.org/publications/journals/selforganizology/rss.xml>

E-mail: selforganizology@iaees.org

Editor-in-Chief: WenJun Zhang

Publisher: International Academy of Ecology and Environmental Sciences

1 Introduction

Intelligent Transportation Systems (ITS) increasingly rely on wireless communication, distributed computing, and connected vehicles to exchange traffic and service information. Vehicular ad hoc networks (VANETs) provide vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication, while cloud computing

provides scalable storage and processing. Vehicular Cloud Computing (VCC) combines these capabilities so that vehicles, roadside infrastructure, edge resources, and remote cloud resources can cooperate to provide services to drivers, passengers, traffic authorities, and other users (Boukerche and Robson, 2018; Sheikh et al., 2020).

VCC applications include safety warnings, traffic information, route assistance, and non-safety services such as locating nearby facilities. The dynamic topology of VANETs, wireless transmission, changing vehicle density, and limited processing resources create security and performance challenges. Survey literature identifies threats including denial of service, eavesdropping, man-in-the-middle attacks, tunneling, malware, impersonation, and other attacks that can affect availability, confidentiality, integrity, and authentication (Gayathri and Gomathy, 2021; Masood et al., 2020).

Cryptographic authentication is therefore a central component of secure VCC communication. Existing approaches include pseudonymous authentication, group signatures, ECC-based authentication, and dynamic-key mechanisms. For VCC, reducing communication and computation overhead is particularly relevant because vehicle resources and wireless links may be constrained (Sharma et al., 2015). The paper proposes a key-exchange scheme that combines Schnorr signcryption with HECC and uses mutual sender/receiver authentication before communication.

The contribution of this paper is a concise research article presentation of that scheme, its authentication workflow, its stated security properties, and the performance results reported in our thesis.

2 Background and Related Work

2.1 Vehicular cloud computing

VCC extends VANET functionality by allowing vehicles and roadside or cloud infrastructure to contribute processing, storage, communication, and sensing resources. We describe temporary, permanent, and hybrid vehicular cloud architectures. In a temporary architecture, vehicles can form short-lived resource groups for a particular task; in a permanent architecture, participating vehicles maintain connectivity with cloud resources; and a hybrid architecture combines both models (Sheikh et al., 2020).

2.2 Security in VANETS and VCC

Security mechanisms in vehicular networks must authenticate communicating entities while protecting exchanged data against unauthorized modification and disclosure. Prior work discussed in the thesis includes dual authentication, pseudonymous authentication, certificate-based approaches, key-insulation techniques, and ECC-based authentication. These approaches demonstrate the importance of balancing security properties with the computation and communication cost imposed on vehicles.

2.3 Signcryption and elliptic-curve techniques

Signcryption combines message confidentiality and authentication functions in a single cryptographic procedure. The paper considers Schnorr signcryption and uses hyperelliptic curve operations for key generation and authentication. Earlier elliptic-curve signcryption schemes reported in the source include the approaches of Toorani and Beheshti (2010), Mohapatra (2010), and Elkamchouchi et al. (2017). A hyperelliptic-curve signcryption approach is also reported by Ullah et al. (2019).

2.4 Research gap

The literature reviewed indicates a continuing need for authenticated key establishment that provides the required security properties while limiting computation and communication overhead in VCC. Sharma et al. (2015), for example, proposed dynamic-key authentication for VCC using ECC. We identify computational and communication overhead as an area for further improvement and therefore replaces the ECC-based key-generation component with HECC in its proposed scheme.

3 System Model and Proposed Scheme

3.1 VCC architecture

The proposed architecture is organized into three processing perspectives: a vehicular processing layer, an edge processing layer, and a cloud processing layer. Vehicles provide local processing and communication resources and may form dynamic vehicular clouds. Edge nodes provide nearby processing and coordinate the resources of associated vehicles. The cloud layer supplies geographically remote but computationally powerful resources. The source architecture uses DSRC for V2V communication and Wi-Fi for vehicle-to-edge communication, with high-speed Ethernet/PON connectivity toward higher network levels.

3.2 Cryptographic notation

The notation below condenses the notation table in the thesis. The source document contains some formatting loss in the mathematical expressions; therefore, only symbols whose meanings are clear from the thesis are retained.

Symbol	Meaning
P	Large prime number; source specifies an order greater than 2^{80} .
Q	Prime number used with $P = QR + 1$ in the source notation.
D	Divisor of the hyperelliptic curve.
G	Primitive set used by the Schnorr procedure.
Spri / Spub	Sender private and public keys.
Rpri / Rpub	Receiver private and public keys.
h / KH	One-way hash / keyed one-way hash function.
R1 / R2	Intermediate values generated during sender authentication.
ω / μ	Hash-derived authentication values exchanged for verification.

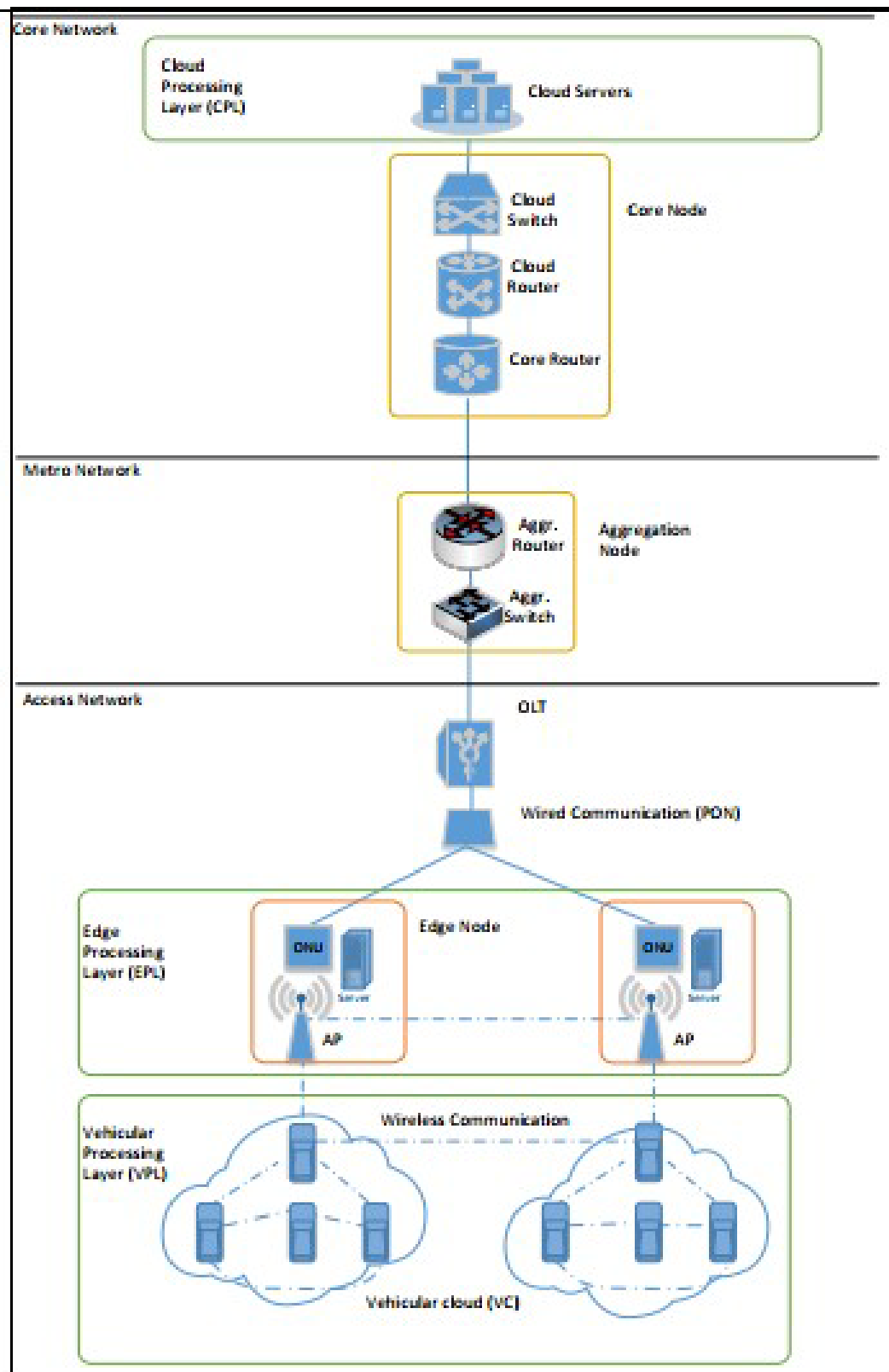


Fig. 1 Vehicular-cloud architecture (original architecture attributed there to Behbehani et al., 2021).

3.3 Sender authentication

The sender-authentication procedure begins with public-key verification for the sender and receiver. The receiver selects a value x_1 from the primitive set and computes R_1 using the divisor D . R_1 is shared with senders within the communication range. Each sender verifies R_1 , computes a hash value ω from the identifier and the sender private key, selects a second value x_2 , computes R_2 , and transmits the tuple (R_2, ω, id) to the receiver.

After receiving the tuple, the receiver verifies R_2 and computes a corresponding hash value ω' using the sender public key. The receiver accepts the sender when $\omega = \omega'$; otherwise, the connection is rejected.

3.4 Receiver authentication

The receiver-authentication phase provides the reverse verification. The receiver computes μ as a hash of the identifier and the product of R_2 with the receiver private key, and transmits μ to the sender. The sender computes μ' using R_2 and the receiver public key. If $\mu = \mu'$, the receiver is accepted; otherwise, the connection is terminated. The two phases therefore provide mutual authentication before data transfer.

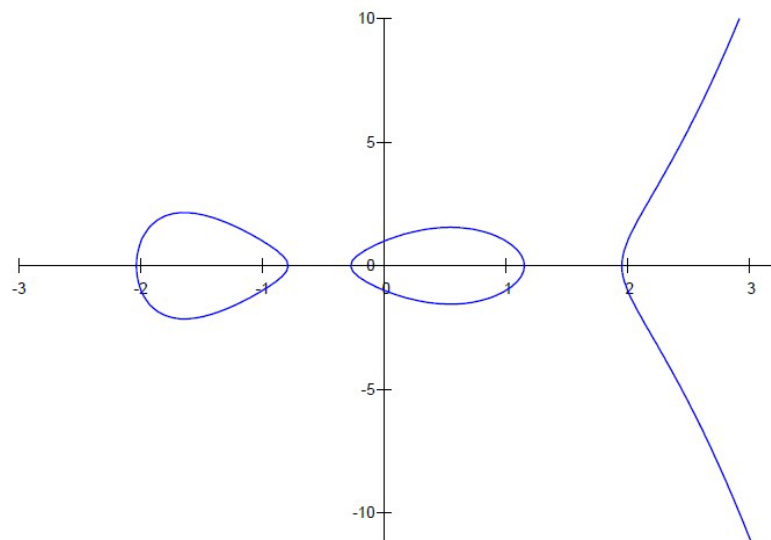


Fig. 2 Hyperelliptic-curve representation.

4 Security Analysis

The security analysis evaluates four principal properties. The discussion below reports those properties without extending the original claims into a formal proof.

4.1 Confidentiality

The paper argues that an adversary attempting to derive the private values underlying R_1 and R_2 would need to solve the discrete-logarithm problem associated with the underlying construction. Under the computational assumption adopted by the scheme, this is intended to prevent unauthorized recovery of the secret values.

4.2 Integrity

Integrity is supported by the hash-based verification values. The receiver checks ω against ω' and the sender checks μ against μ' . A modification that changes the authenticated inputs should therefore cause the corresponding verification values to differ and the connection to be rejected.

4.3 Authenticity

Mutual authenticity is provided through verification of sender and receiver public keys and the two authentication phases. The scheme is designed so that successful completion of both phases is required before

data transfer.

4.4 Unforgeability

The thesis argues that an eavesdropper cannot generate valid authentication values or keys without the relevant private values. This claim depends on the cryptographic hardness assumption of the underlying construction.

4.5 Threat coverage

The source work motivates the scheme against spoofing, man-in-the-middle, and replay attacks. The described use of one-way hashing, concatenation, public-key verification, and fresh intermediate values is intended to reduce exposure to these attacks. A formal adversarial proof or automated protocol-verification result should be considered future validation.

5 Performance Evaluation

We report MATLAB R2017b experiments on an Intel Core i3-6006U processor at 2.0 GHz with 4 GB RAM running Windows 10 Pro. The source compares signcryption and unsigncryption times for selected schemes and the proposed scheme.

Scheme	Signcryption (ms)	Unsigncryption (ms)	Total (ms)
Toorani and Beheshti (2010)	1.94	2.91	4.85
Mohapatra (2010)	2.91	1.91	4.82
Elkamchouchi et al. (2017)	2.91	3.88	6.79
Ullah et al. (2019)	1.92	1.92	3.84
Proposed scheme	1.44	1.92	3.36

The reported total execution time for the proposed scheme is 3.36 ms. Relative to the source-reported totals, this is lower than the four comparison values. Because these measurements are taken from originally stated simulation environment, they should be interpreted as source-reported results rather than independently reproduced results.

The paper also compares the number of elliptic-curve point multiplication (ECPM) and hyperelliptic-curve divisor multiplication (HCDM) operations. However, the source table contains formatting ambiguity: the proposed row lists one HCDM for signcryption and one HCDM for unsigncryption but reports a total of seven HCDM. To avoid silently changing the source data, that operation-count table is not reproduced as a numerical result here. The measured millisecond table above is retained because its values are internally presented as signcryption, unsigncryption, and total times.

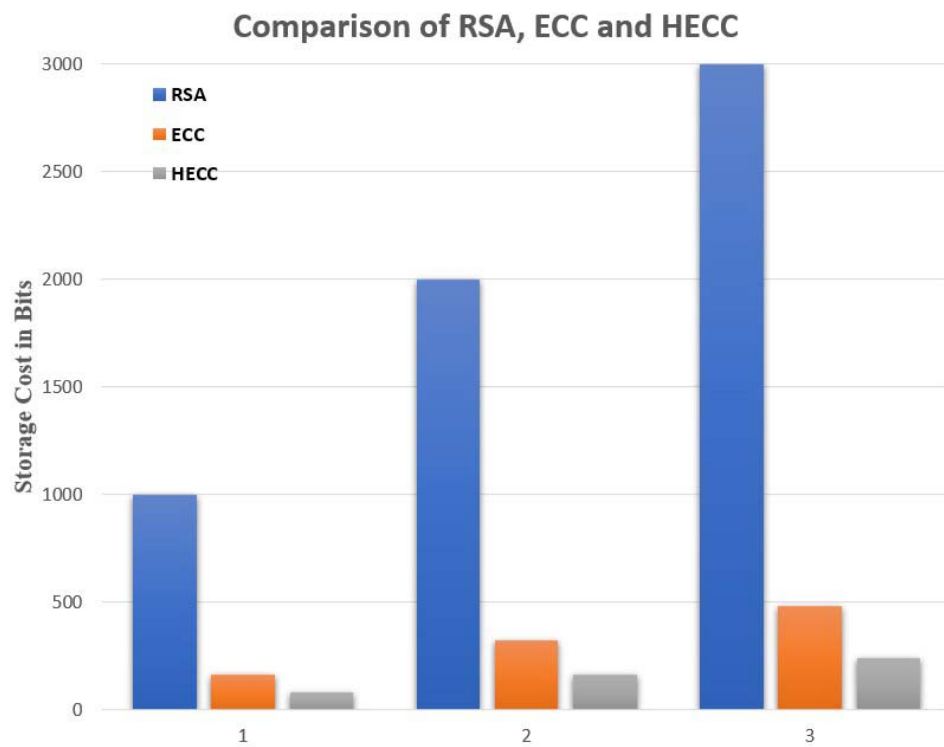


Fig. 3 Key-size comparison of RSA, ECC and HECC.

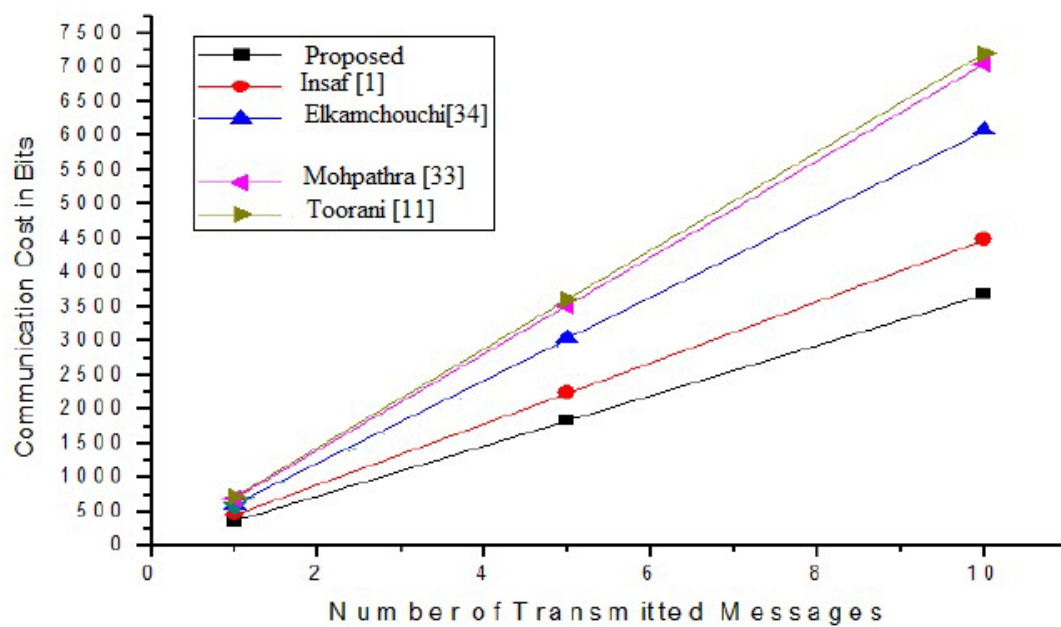


Fig. 4 Communication-cost comparison for different message counts.

6 Discussion

The source results support the paper's central design rationale: combining Schnorr signcryption with HECC is presented as a way to reduce the reported computational burden of authenticated key exchange in VCC. The proposed protocol also uses a two-phase mutual-authentication workflow, making the authentication state explicit before data transmission.

At the same time, several limitations should be considered. First, the evaluation is simulation-based and uses one hardware/software environment. Second, the communication-cost figure is presented graphically in the paper without a complete numerical table in the parsed source, limiting independent numerical comparison. Third, the source does not provide a formal security reduction, protocol-verification output, or a real vehicular testbed evaluation. Finally, the key-size and security-equivalence statements depend on the cryptographic parameters and assumptions adopted by the study. These limitations do not invalidate the reported experiment, but they define the scope within which the results should be read.

7 Conclusion and Future Work

This paper reformulates the MS thesis as a concise research article on secure authenticated key exchange for Vehicular Cloud Computing. The proposed construction uses Schnorr signcryption with HECC and performs sender and receiver authentication using hash-based verification values. It reports 1.44 ms signcryption time, 1.92 ms unsigncryption time, and 3.36 ms total computation time for the proposed scheme in its MATLAB-based evaluation. The source analysis also addresses confidentiality, integrity, authenticity, and unforgeability.

Future work should include implementation on vehicular or edge hardware, repeated experiments under varying vehicle density and network conditions, complete numerical communication-cost reporting, formal security proofs or automated protocol verification, and comparison with additional contemporary authentication schemes.

References

- Adnan M, Iqbal J, Waheed A, Amin NU, Zareei M, Umer A, Mohamed EM. 2021. Towards the design of efficient and secure architecture for software-defined vehicular networks. *Sensors*, 21(11): 3902
- Behbehani FS, Elgorashi T, Elmirghani JM. 2021. Power minimization in vehicular cloud architecture. *arXiv preprint arXiv:2102.09011*
- Boukerche A, Robson E. 2018. Vehicular cloud computing: Architectures, applications, and mobility. *Computer Networks*, 135: 171-189
- Elkamchouchi HM, El-Atiky MH, Abouelkheir E. 2017. A public verifiability signcryption scheme without pairings. *International Journal of Computer Applications*, 157(9)
- Gayathri M, Gomathy C. 2021. A deep survey on types of cyber-attacks in VANET. *Journal of Critical Reviews*, 8(1): 1029-1039
- Kanchan S, Singh G, Chaudhari NS. 2022. SPSR-VCP: Secure and privacy preserving SignReryption in vehicular cyber physical systems. *Journal of Ambient Intelligence and Humanized Computing*, 13(1): 1-20.
- Lu R, Lin X, Zhu H, Ho PH, Shen X. 2008. Efficient conditional privacy preservation protocol for secure vehicular communications. *IEEE INFOCOM*, 1229-1237. doi:10.1109/INFOCOM.2008.179.
- Masood A, Lakew DS, Cho S. 2020. Security and privacy challenges in connected vehicular cloud computing. *IEEE Communications Surveys & Tutorials*, 22(4): 2725-2764

- Mohapatra RK. 2010. Signcryption schemes with forward secrecy based on elliptic curve cryptography. Doctoral Thesis.
- Sharma MK, Bali RS, Kaur A. 2015. Dynamic key based authentication scheme for Vehicular Cloud Computing. 2015 International Conference on Green Computing and Internet of Things, 1059-1064. doi: 10.1109/ICGCIoT.2015.7380620
- Sheikh MS, Liang J, Wang W. 2020. Security and privacy in vehicular ad hoc network and vehicle cloud computing: A survey. *Wireless Communications and Mobile Computing*, 2020
- Studer A, Bai F, Bellur B, Perrig A. 2009. Flexible, extensible, and efficient VANET authentication. *Journal of Communications and Networks*, 11(6): 574-588. doi:10.1109/JCN.2009.6388411.
- Toorani M, Beheshti AA. 2010. An elliptic curve-based signcryption scheme with forward secrecy. *arXiv preprint arXiv:1005.1856*
- Ullah I, Amin NU, Khan J, Rehan M, Naeem M, Khattak H, et al. 2019. A novel provable secured signcryption scheme PSSS: A hyper-elliptic curve-based approach. *Mathematics*, 7(8): 686
- Zhong H, Huang B, Cui J, Xu Y, Liu L. 2018. Conditional privacy-preserving authentication scheme for VANETs. *IEEE Access*, 6: 17542-17554. doi:10.1109/ACCESS.2017.2782672.
- Zhou Y, Liu S, Xiao M, Deng S, Wang X. 2018. An efficient V2I authentication scheme for VANETs. *Mobile Information Systems*, 2018, Article 4070283. doi:10.1155/2018/4070283.