Publications

TRANSACTIONS AND JOURNALS

Published

1. **Sikarwar H**, Das D, SecEdge: Secure Edge-Computing Based Hybrid Approach for Data Collection and Searching in IoV, **IEEE Transactions on Network and Service Management**, 2023 Jul 27. **IF: 5.3**

2. **Sikarwar H**, Das D, A novel MAC-based authentication scheme (NoMAS) for internet of vehicles (IoV), **IEEE Transactions on Intelligent Transportation Systems**, 2023 Feb 10. **IF: 8.5**

3. **Sikarwar H**, Das D, Towards lightweight authentication and batch verification scheme in IoV, **IEEE Transactions on Dependable and Secure Computing**, 2021. **IF: 7.3**

4. **Sikarwar H**, Vasudev H, Das D, Conti M, SECURE: Secure and efficient protocol using randomness and edge computing for drone-assisted internet of vehicles, **IEEE Transactions on Network and Service Management**, 2024. **IF: 5.3**

Revision Submitted

5. **Sikarwar H**, Nahar A, Das D, DyBatch: Message prioritization and priority-driven batch verification in large-scale IoV networks, **IEEE Transactions on Vehicular Technology**, 2023. **IF: 6.8 [R4 Submitted.]**

6. Nahar A, **Sikarwar H**, Das D and Mishra Sudip, MRMH: Multi-constraint routing optimization using hybrid metaheuristics in vehicular ad-hoc networks, **IEEE Transaction on Network Science and Engineering**, 2024. **IF: 6.6 [R1 Submitted.]**

Under Review

7. **Sikarwar H**, Vasudev H, Das D, Conti M, AAPEC: Anonymous Authentication using PUF-based Edge Computing for IoVs, **IEEE Transactions on Mobile Computing**, 2025. **IF: 7.3 [Under Review].**

8. **Sikarwar H**, K K Mondal, Das D., Towards Nonce-Reuse Resilience in Authenticated Encryption: A PUF-Based Hardware Cryptography Framework In **IEEE Transactions on Consumer Electronics**, 2025. **IF: 4.3 [Under Review]**.

9. K K Mondal, **Sikarwar H**, Das D., Secure IoT Communications with Optimized AES-128 and Dynamic Threat Modeling on Embedded ESP32, **IEEE Transactions on Consumer Electronics**, 2024. **IF: 4.3 [Under Review]**

10. Nagar M, **Sikarwar H** and Das D, Enhancing Cross-User Generalization in Human Activity Recognition with Adaptive Noise Scheduling and Linear Attention, **IEEE Transactions on Human-Machine Systems**, 2025. **IF: 3.5 [Under Review]**

CONFERENCES PROCEEDINGS

1. Nahar A, **Sikarwar H**, Jain S, Das D, CacheIn: A Secure Distributed Multi-layer Mobility-Assisted Edge Intelligence based Caching for Internet of Vehicles, In **IEEE/ACM 23rd International Symposium on Cluster, Cloud and Internet Computing (CCGrid) 2023 May 1, Bangalore, India (pp. 437-446) Core Ranking: A**.

2. **Sikarwar H**, Das D. SMMAP: Secure MAC-based Mutual Authentication Protocol for IoV. In **Proceedings of the 24th International Conference on Distributed Computing and Networking 2023 Jan 4, Kharagpur, India (pp. 330-335) Core Ranking: B**.

3. **Sikarwar H**, Das D, EECAAP: Efficient Edge-Computing based Anonymous Authentication Protocol for IoV, In **IEEE 29th International Conference on High Performance Computing, Data, and Analytics (HiPC) 2022 Dec 18, Bangalore, India (pp. 302-307) Core Ranking: B**.

4. Nahar A, **Sikarwar H**, Das D. AlcFier: Adaptive self-learning classifier for routing in vehicular ad-hoc network. In **2022 IEEE 47th conference on local computer networks (LCN) 2022 Sep 26, Canada (pp. 311-314). Core Ranking: B**.

5. **Sikarwar H**, Nahar A, Das D. LAAS: Lightweight Anonymous Authentication Scheme for Universal Internet of Vehicles (UIoV). In **International Wireless Communications and Mobile Computing (IWCMC) 2022 May 30, Dubrovnik, Croatia (pp. 859-864). Core Ranking: B**.

6. Nahar A, **Sikarwar H**, Das D. CSBR: A cosine similarity based selective broadcast routing protocol for vehicular ad-hoc networks. In **IFIP networking conference (networking) 2020 Jun 22, Paris, France (pp. 404-412). Core Ranking: A**.

7. **Sikarwar H**, Das D. A lightweight and secure authentication protocol for WSN. In **International Wireless Communications and Mobile Computing (IWCMC) 2020 Jun 15, Limassol, Cyprus (pp. 475-480). Core Ranking: B**.

8. **Sikarwar H**, Nahar A, Das D, LABVS: Lightweight authentication and batch verification scheme for universal internet of vehicles (UIoV), In **IEEE Vehicular Technology Conference (VTC2020-Spring) 2020 May 25, Belgium (pp. 1-6) Core Ranking: B**.

9. **Sikarwar H**, Das D, Kalra S. Efficient authentication scheme using blockchain in IoT devices. In **Advanced Information Networking and Applications: Proceedings of the 34th International Conference on Advanced Information Networking and Applications (AINA-2020), Caserta, Italy (pp. 630-641). Core Ranking: B**.

10. **Sikarwar H**, and Das D An Efficient Lightweight Authentication and Batch Verification Scheme for Universal Internet of Vehicles (UIoV). In **International Wireless Communications and Mobile Computing (IWCMC), 2020. Core Ranking: B**.

References

[1] Juan Contreras-Castillo, Sherali Zeadally, and Juan Antonio Guerrero-Ibañez. "Internet of vehicles: architecture, protocols, and security". In: *IEEE internet of things Journal* 5.5 (2017), pp. 3701–3709.

[2] Saleh Yousefi, Mahmoud Siadat Mousavi, and Mahmood Fathy. "Vehicular ad hoc networks (VANETs): challenges and perspectives". In: *2006 6th international conference on ITS telecommunications*. IEEE. 2006, pp. 761–766.

[3] Khadige Abboud, Hassan Aboubakr Omar, and Weihua Zhuang. "Interworking of DSRC and cellular network technologies for V2X communications: A survey". In: *IEEE transactions on vehicular technology* 65.12 (2016), pp. 9457–9470.

[4] Sajjad Hussain Shah and Ilyas Yaqoob. "A survey: Internet of Things (IOT) technologies, applications and challenges". In: *2016 IEEE Smart Energy Grid Engineering (SEGE)* (2016), pp. 381–385.

[5] Omprakash Kaiwartya et al. "Internet of vehicles: Motivation, layered architecture, network model, challenges, and future aspects". In: *IEEE access* 4 (2016), pp. 5356–5373.

[6] Aidil Redza Khan et al. "DSRC technology in vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) IoT system for intelligent transportation system (ITS): A review". In: *Recent Trends in Mechatronics Towards Industry 4.0: Selected Articles from iM3F 2020, Malaysia* (2022), pp. 97–106.

[7] Olof Liberg et al. *Cellular Internet of things: technologies, standards, and performance*. Academic Press, 2017.

[8] Wei Duan et al. "Emerging technologies for 5G-IoV networks: applications, trends and opportunities". In: *IEEE Network* 34.5 (2020), pp. 283–289.

[9] Bin Yu, Lisheng Xu, and Yongxu Li. "Bluetooth Low Energy (BLE) based mobile electrocardiogram monitoring system". In: *2012 IEEE International Conference on Information and Automation*. IEEE. 2012, pp. 763–767.

[10] Chia-Chin Chong, Fujio Watanabe, and Hiroshi Inamura. "Potential of UWB technology for the next generation wireless communications". In: *2006 IEEE Ninth International Symposium on Spread Spectrum Techniques and Applications*. IEEE. 2006, pp. 422–429.

[11] Ching-Hsien Hsu, Amir H Alavi, and Mianxiong Dong. *Introduction to the Special Section on Cyber Security in Internet of Vehicles*. 2023.

[12] Himani Sikarwar, Ankur Nahar, and Debasis Das. "LABVS: Lightweight authentication and batch verification scheme for universal internet of vehicles (UIoV)". In: *2020 IEEE 91st Vehicular Technology Conference (VTC2020-Spring)*. IEEE. 2020, pp. 1–6.

[13] Benjamin Kwapong Osibo et al. "Security and privacy in 5G internet of vehicles (IoV) environment". In: *Journal on Internet of Things* 3.2 (2021), p. 77.

[14] Fatih Sakiz and Sevil Sen. "A survey of attacks and detection mechanisms on intelligent transportation systems: VANETs and IoV". In: *Ad Hoc Networks* 61 (2017), pp. 33–50.

[15] Hamideh Taslimasa et al. "Security issues in Internet of Vehicles (IoV): A comprehensive survey". In: *Internet of Things* (2023), p. 100809.

[16] Yunchuan Sun et al. "Attacks and countermeasures in the internet of vehicles". In: *Annals of Telecommunications* 72 (2017), pp. 283–295.

[17] Tanvi Garg et al. "A survey on security and privacy issues in IoV." In: *International Journal of Electrical & Computer Engineering (2088-8708)* 10.5 (2020).

[18] Tej Tharang Dandala, Vallidevi Krishnamurthy, and Rajan Alwan. "Internet of Vehicles (IoV) for traffic management". In: *2017 International conference on computer, communication and signal processing (ICCCSP)*. IEEE. 2017, pp. 1–4.

[19] Jawaher Abdulwahab Fadhil and Qusay Idrees Sarhan. "Internet of Vehicles (IoV): A survey of challenges and solutions". In: *2020 21st International Arab Conference on Information Technology (ACIT)*. IEEE. 2020, pp. 1–10.

[20] Youcef Djenouri et al. "A Secure Intelligent System for Internet of Vehicles: Case Study on Traffic Forecasting". In: *IEEE Transactions on Intelligent Transportation Systems* (2023).

[21] Yunxin Li. "An overview of the DSRC/WAVE technology". In: *Quality, Reliability, Security and Robustness in Heterogeneous Networks: 7th International Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness, QShine 2010, and Dedicated Short Range Communications Workshop, DSRC 2010, Houston, TX, USA, November 17-19, 2010, Revised Selected Papers 7*. Springer. 2012, pp. 544–558.

[22] Aneesh Paul et al. *Advanced driver assistance systems*. Tech. rep. SAE Technical Paper, 2016.

[23] Ehsan Moradi-Pari et al. "DSRC versus LTE-V2X: Empirical performance analysis of direct vehicular communication technologies". In: *IEEE Transactions on Intelligent Transportation Systems* 24.5 (2023), pp. 4889–4903.

[24] MK Priyan and G Usha Devi. "A survey on internet of vehicles: applications, technologies, challenges and opportunities". In: *International Journal of Advanced Intelligence Paradigms* 12.1-2 (2019), pp. 98–119.

[25] Shadi Al-Sarawi et al. "Internet of Things (IoT) communication protocols". In: *2017 8th International conference on information technology (ICIT)*. IEEE. 2017, pp. 685–690.

[26] Weigang Wu, Zhiwei Yang, and Keqin Li. "Internet of Vehicles and applications". In: *Internet of Things*. Elsevier, 2016, pp. 299–317.

[27] Arif Hakimi et al. "A survey on internet of vehicle (iov): A pplications & comparison of vanets, iov and sdn-iov". In: *ELEKTRIKA-Journal of Electrical Engineering* 20.3 (2021), pp. 26–31.

[28] Asif Faisal et al. "Understanding autonomous vehicles". In: *Journal of transport and land use* 12.1 (2019), pp. 45–72.

[29] Samira El Madani, Saad Motahhir, and Abdelaziz El Ghzizal. "Internet of vehicles: concept, process, security aspects and solutions". In: *Multimedia Tools and Applications* 81.12 (2022), pp. 16563–16587.

[30] Ashish Nanda et al. "Internet of autonomous vehicles communications security: overview, issues, and directions". In: *IEEE Wireless Communications* 26.4 (2019), pp. 60–65.

[31] Kashif Naseer Qureshi et al. “Internet of vehicles: Key technologies, network model, solutions and challenges with future aspects”. In: *IEEE Transactions on Intelligent Transportation Systems* 22.3 (2020), pp. 1777–1786.

[32] Himani Sikarwar, Ankur Nahar, and Debasis Das. “LAAS: lightweight anonymous authentication scheme for universal internet of vehicles (UIOV)”. In: *2022 International Wireless Communications and Mobile Computing (IWCMC)*. IEEE. 2022, pp. 859–864.

[33] Haoxuan Yang, Tao Feng, Yan Yan, et al. “Implementing efficient attribute encryption in IoV under cloud environments”. In: *Computer Networks* 218 (2022), p. 109363.

[34] Chanchal Maurya and Vijay Kumar Chaurasiya. “Efficient Anonymous Batch Authentication Scheme With Conditional Privacy in the Internet of Vehicles (IoV) Applications”. In: *IEEE Transactions on Intelligent Transportation Systems* (2023).

[35] Grant Kelly, Bruce McKenzie, et al. “Security, privacy, and confidentiality issues on the Internet”. In: *Journal of Medical Internet Research* 4.2 (2002), e861.

[36] Spyridon Samonas and David Coss. “The CIA strikes back: Redefining confidentiality, integrity and availability in security.” In: *Journal of Information System Security* 10.3 (2014).

[37] Loren Kohnfelder and Praerit Garg. “The threats to our products (1999)”. In: *URL: https://adam. shostack. org/microsoft/The-Threats-To-Our-Products. docx* (2021).

[38] Nishant Sharma, Naveen Chauhan, and Narottam Chand. “Security challenges in Internet of Vehicles (IoV) environment”. In: *2018 First International Conference on Secure Cyber Computing and Communication (ICSCCC)*. IEEE. 2018, pp. 203–207.

[39] Himani Sikarwar and Debasis Das. “An Efficient Lightweight Authentication and Batch Verification Scheme for Universal Internet of Vehicles (UIoV)”. In: *2020 International Wireless Communications and Mobile Computing (IWCMC)*. IEEE. 2020, pp. 1266–1271.

[40] Myrto Arapinis, Vincent Cheval, and Stéphanie Delaune. “Composing security protocols: from confidentiality to privacy”. In: *International Conference on Principles of Security and Trust*. Springer. 2015, pp. 324–343.

[41] Upstream Security. *Automotive cybersecurity incidents surged dramatically in 2019*. Accessed: 2024-07-09. 2020. URL: https://www.helpnetsecurity.com/2020/01/06/automotive-cybersecurity-incidents/.

[42] Himani Sikarwar and Debasis Das. “A novel MAC-based authentication scheme (NoMAS) for Internet of Vehicles (IoV)”. In: *IEEE Transactions on Intelligent Transportation Systems* 24.5 (2023), pp. 4904–4916.

[43] Huu Phuoc Dai Nguyen and Rajnai Zoltán. “The current security challenges of vehicle communication in the future transportation system”. In: *2018 IEEE 16th International Symposium on Intelligent Systems and Informatics (SISY)*. IEEE. 2018, pp. 000161–000166.

[44] Mohamed Eltoweissy, Stephan Olariu, and Mohamed Younis. “Towards Autonomous Vehicular Clouds”. In: *Ad Hoc Networks. Second International Conference, ADHOCNETS 2010, Victoria, BC, Canada, August 18-20, 2010, Revised Selected Papers*. Springer, Berlin, Heidelberg. 2012, pp. 1–16. DOI: 10.1007/978-3-642-17994-5_1.

[45] Himani Sikarwar and Debasis Das. “SecEdge: Secure Edge-Computing Based Hybrid Approach for Data Collection and Searching in IoV”. In: *IEEE Transactions on Network and Service Management* (2023).

[46] Yiliang Liu, Liangmin Wang, and Hsiao-Hwa Chen. "Message authentication using proxy vehicles in vehicular ad hoc networks". In: *IEEE Transactions on vehicular technology* 64.8 (2014), pp. 3697–3710.

[47] Majid Bayat et al. "A secure authentication scheme for VANETs with batch verification". In: *Wireless networks* 21 (2015), pp. 1733–1743.

[48] J Jenefa and EA Mary Anita. "An enhanced secure authentication scheme for vehicular Ad Hoc networks without pairings". In: *Wireless Personal Communications* 106 (2019), pp. 535–554.

[49] Jun Shao et al. "A threshold anonymous authentication protocol for VANETs". In: *IEEE Transactions on vehicular technology* 65.3 (2015), pp. 1711–1720.

[50] Ming-Chin Chuang and Jeng-Farn Lee. "TEAM: Trust-extended authentication mechanism for vehicular ad hoc networks". In: *IEEE systems journal* 8.3 (2013), pp. 749–758.

[51] Muhammad Naveed Aman, Uzair Javaid, and Biplab Sikdar. "A privacy-preserving and scalable authentication protocol for the internet of vehicles". In: *IEEE Internet of Things Journal* 8.2 (2020), pp. 1123–1139.

[52] Himani Sikarwar and Debasis Das. "SMMAP: Secure MAC-based Mutual Authentication Protocol for IoV". In: *Proceedings of the 24th International Conference on Distributed Computing and Networking*. 2023, pp. 330–335.

[53] Trupil Limbasiya and Debasis Das. "VCom: Secure and efficient vehicle-to-vehicle message communication protocol". In: *IEEE Transactions on Network and Service Management* 18.2 (2020), pp. 2365–2376.

[54] Rajkumar Singh Rathore et al. "In-vehicle communication cyber security: challenges and solutions". In: *Sensors* 22.17 (2022), p. 6679.

[55] Himani Sikarwar and Debasis Das. "Towards lightweight authentication and batch verification scheme in IoV". In: *IEEE Transactions on Dependable and Secure Computing* 19.5 (2021), pp. 3244–3256.

[56] Alfonso Martínez-Cruz et al. "Security on in-vehicle communication protocols: Issues, challenges, and future research directions". In: *Computer Communications* 180 (2021), pp. 1–20.

[57] Gonzalo De La Torre, Paul Rad, and Kim-Kwang Raymond Choo. "Driverless vehicle security: Challenges and future research opportunities". In: *Future Generation Computer Systems* 108 (2020), pp. 1092–1111.

[58] Palak Bagga et al. "Authentication protocols in internet of vehicles: Taxonomy, analysis, and challenges". In: *Ieee Access* 8 (2020), pp. 54314–54344.

[59] Randhir Kumar et al. "P2SF-IoV: A privacy-preservation-based secured framework for Internet of Vehicles". In: *IEEE Transactions on Intelligent Transportation Systems* 23.11 (2021), pp. 22571–22582.

[60] Christina Tikkinen-Piri, Anna Rohunen, and Jouni Markkula. "EU General Data Protection Regulation: Changes and implications for personal data collecting companies". In: *Computer Law & Security Review* 34.1 (2018), pp. 134–153.

[61] Yanbing Liu, Yuhang Wang, and Guanghui Chang. "Efficient privacy-preserving dual authentication and key agreement scheme for secure V2V communications in an IoV paradigm". In: *IEEE Transactions on Intelligent Transportation Systems* 18.10 (2017), pp. 2740–2749.

[62] Farhan Ahmad et al. “Vehicular cloud networks: Architecture, applications and security issues”. In: *2015 IEEE/ACM 8th International Conference on Utility and Cloud Computing (UCC)*. IEEE. 2015, pp. 571–576. DOI: 10.1109/UCC.2015.103.

[63] Zhaolong Ning et al. “Mobile edge computing-enabled internet of vehicles: Toward energy-efficient scheduling”. In: *IEEE Network* 33.5 (2019), pp. 198–205.

[64] Georg T. Becker, Alexander Wild, and Tim Güneysu. “Security analysis of index-based syndrome coding for PUF-based key generation”. In: *2015 IEEE International Symposium on Hardware Oriented Security and Trust (HOST)*. 2015, pp. 20–25. DOI: 10.1109/HST.2015.7140230.

[65] Muhammad Arif et al. “A survey on security attacks in VANETs: Communication, applications and challenges”. In: *Vehicular Communications* 19 (2019), p. 100179.

[66] Kazuhide Fukushima, Shinsaku Kiyomoto, and Yutaka Miyake. “Software protection combined with tamper-proof device”. In: *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences* 95.1 (2012), pp. 213–222.

[67] Charles Herder et al. “Physical unclonable functions and applications: A tutorial”. In: *Proceedings of the IEEE* 102.8 (2014), pp. 1126–1141.

[68] Sergio M Tornell et al. “A novel On-Board Unit to accelerate the penetration of ITS services”. In: *2016 13th IEEE annual consumer communications & networking conference (CCNC)*. IEEE. 2016, pp. 467–472.

[69] Andreas Pfitzmann and Marit Hansen. *A terminology for talking about privacy by data minimization: Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management*. 2010.

[70] Yevgeniy Dodis and John Steinberger. “Message authentication codes from unpredictable block ciphers”. In: *Advances in Cryptology-CRYPTO 2009: 29th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 16-20, 2009. Proceedings*. Springer. 2009, pp. 267–285.

[71] Douglas R Stinson. “Some observations on the theory of cryptographic hash functions”. In: *Designs, Codes and Cryptography* 38 (2006), pp. 259–277.

[72] Jie Cui et al. “An efficient message-authentication scheme based on edge computing for vehicular ad hoc networks”. In: *IEEE Transactions on Intelligent Transportation Systems* 20.5 (2018), pp. 1621–1632.

[73] Geong Sen Poh et al. “Searchable symmetric encryption: Designs and challenges”. In: *ACM Computing Surveys (CSUR)* 50.3 (2017), pp. 1–37.

[74] David Bernstein, Nino Vidovic, and Sohrab Modi. “A cloud PAAS for high scale, function, and velocity mobile applications-with reference application as the fully connected car”. In: *2010 Fifth International Conference on Systems and Networks Communications*. IEEE. 2010, pp. 117–123. DOI: 10.1109/ICSNC.2010.37.

[75] Rasheed Hussain et al. “Rethinking Vehicular Communications: Merging VANET with Cloud Computing”. In: *4th IEEE International Conference on Cloud Computing Technology and Science Proceedings*. IEEE. 2012, pp. 606–609. DOI: 10.1109/CloudCom.2012.6427481.

[76] Rong Yu et al. “Toward cloud-based vehicular networks with efficient resource management”. In: *IEEE Network* 27.5 (2013), pp. 48–55. DOI: 10.1109/MNET.2013.6616110.

[77] Tesnim Mekki et al. “Vehicular cloud networks: Challenges, architectures, and future directions”. In: *Vehicular Communications* 9 (2017), pp. 268–280. DOI: 10.1016/j.vehcom.2017.07.001.

[78] Roland HC Yap et al. “Extending BAN logic for reasoning with modern PKI-based protocols”. In: *2008 IFIP International Conference on Network and Parallel Computing*. IEEE. 2008, pp. 190–197.

[79] Ran Canetti, Abhishek Jain, and Alessandra Scafuro. “Practical UC security with a global random oracle”. In: *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*. 2014, pp. 597–608.

[80] Ravikanth Pappu et al. “Physical one-way functions”. In: *Science* 297.5589 (2002), pp. 2026–2030.

[81] Roel Maes and Ingrid Verbauwhede. “Physically unclonable functions: A study on the state of the art and future research directions”. In: *Towards Hardware-Intrinsic Security: Foundations and Practice* (2010), pp. 3–37.

[82] Phillip Rogaway. “Authenticated-encryption with associated-data”. In: *Proceedings of the 9th ACM Conference on Computer and Communications Security*. 2002, pp. 98–107.

[83] Nhat-Phuong Tran et al. “High throughput parallelization of AES-CTR algorithm”. In: *IEICE TRANSACTIONS on Information and Systems* 96.8 (2013), pp. 1685–1695.

[84] Neil Cameron. “ESP32 Microcontroller”. In: *ESP32 Formats and Communication: Application of Communication Protocols with ESP32 Microcontroller*. Springer, 2023, pp. 1–54.

[85] I Arun Faisal, T Waluyo Purboyo, and A Siswo Raharjo Ansori. “A review of accelerometer sensor and gyroscope sensor in IMU sensors on motion capture”. In: *J. Eng. Appl. Sci* 15.3 (2019), pp. 826–829.

[86] Marko Wolf and Timo Gendrullis. “Design, implementation, and evaluation of a vehicular hardware security module”. In: *Information Security and Cryptology-ICISC 2011: 14th International Conference, Seoul, Korea, November 30-December 2, 2011. Revised Selected Papers 14*. Springer. 2012, pp. 302–318.

[87] Bum Han Kim et al. “Anonymous and traceable communication using tamper-proof device for vehicular ad hoc networks”. In: *2007 International Conference on Convergence Information Technology (ICCIT 2007)*. IEEE. 2007, pp. 681–686.

[88] Mubashir Husain Rehmani and Yasir Saleem. “Network simulator NS-2”. In: *Encyclopedia of Information Science and Technology, Third Edition*. IGI Global, 2015, pp. 6249–6258.

[89] Bruno Blanchet et al. “ProVerif 2.00: automatic cryptographic protocol verifier, user manual and tutorial”. In: *Version from* (2018), pp. 05–16.

[90] Annette Bleeker and Lambert Meertens. “A semantics for BAN logic”. In: *Proceedings of the DIMACS workshop on design and formal verification of security protocols*. 1997.

[91] Maria Sommerhalder. “Hardware Security Module”. In: *Trends in Data Protection and Encryption Technologies* (2023), pp. 83–87.

[92] Mario Stipčević and Çetin Kaya Koç. “True random number generators”. In: *Open problems in mathematics and computational science*. Springer, 2014, pp. 275–315.

[93] Miguel Herrero-Collantes and Juan Carlos Garcia-Escartin. “Quantum random number generators”. In: *Reviews of Modern Physics* 89.1 (2017), p. 015004.

[94] Stathis Mavrovouniotis and Mick Ganley. “Hardware security modules”. In: *Secure Smart Embedded Devices, Platforms and Applications*. Springer, 2013, pp. 383–405.

[95] FIPS Pub. “Standards for security categorization of federal information and information systems”. In: *NIST FIPS* 199 (2004), p. 122.

[96] Eun-Hee Nah et al. “International organization for standardization (ISO) 15189”. In: *Annals of laboratory medicine* 37.5 (2017), pp. 365–370.

[97] Chan-Ho Han. “International electrotechnical commission”. In: *Electric Engineers Magazine* (2007), pp. 29–34.

[98] Yimin Wang et al. “ECPB: efficient conditional privacy-preserving authentication scheme supporting batch verification for VANETs.” In: *Int. J. Netw. Secur.* 18.2 (2016), pp. 374–382.

[99] SK Hafizul Islam et al. “A robust and efficient password-based conditional privacy preserving authentication and group-key agreement protocol for VANETs”. In: *Future Generation Computer Systems* 84 (2018), pp. 216–227.

[100] Maria Azees, Pandi Vijayakumar, and Lazarus Jegatha Deboarh. “EAAP: Efficient anonymous authentication with conditional privacy-preserving scheme for vehicular ad hoc networks”. In: *IEEE Transactions on Intelligent Transportation Systems* 18.9 (2017), pp. 2467–2476.

[101] Jing Zhang et al. “PA-CRT: Chinese remainder theorem based conditional privacy-preserving authentication scheme in vehicular ad-hoc networks”. In: *IEEE Transactions on Dependable and Secure Computing* 18.2 (2019), pp. 722–735.

[102] Jie Li, Huang Lu, and Mohsen Guizani. “ACPN: A novel authentication framework with conditional privacy-preservation and non-repudiation for VANETs”. In: *IEEE transactions on parallel and distributed systems* 26.4 (2014), pp. 938–948.

[103] Avleen Malhi and Shalini Batra. “Privacy-preserving authentication framework using bloom filter for secure vehicular communications”. In: *International Journal of Information Security* 15 (2016), pp. 433–453.

[104] Himani Sikarwar and Debasis Das. “EECAAP: Efficient Edge-Computing based Anonymous Authentication Protocol for IoV”. In: *2022 IEEE 29th International Conference on High Performance Computing, Data, and Analytics (HiPC)*. 2022, pp. 302–307.

[105] Aydin Aysu et al. “End-to-end design of a PUF-based privacy preserving authentication protocol”. In: *Cryptographic Hardware and Embedded Systems–CHES 2015: 17th International Workshop, Saint-Malo, France, September 13-16, 2015, Proceedings 17*. Springer. 2015, pp. 556–576.

[106] Prosanta Gope, Jemin Lee, and Tony QS Quek. “Lightweight and practical anonymous authentication protocol for RFID systems using physically unclonable functions”. In: *IEEE Transactions on Information Forensics and Security* 13.11 (2018), pp. 2831–2843.

[107] Prosanta Gope et al. “Lightweight and physically secure anonymous mutual authentication protocol for real-time data access in industrial wireless sensor networks”. In: *IEEE transactions on industrial informatics* 15.9 (2019), pp. 4957–4968.

[108] Urbi Chatterjee et al. “Building PUF based authentication and key exchange protocol for IoT without explicit CRPs in verifier database”. In: *IEEE transactions on dependable and secure computing* 16.3 (2018), pp. 424–437.

[109] Jiankuo Dong et al. “EC-ECC: Accelerating elliptic curve cryptography for edge computing on embedded GPU TX2”. In: *ACM Transactions on Embedded Computing Systems (TECS)* 21.2 (2022), pp. 1–25.

[110] Hongwei Li et al. “Security and privacy of connected vehicular cloud computing”. In: *IEEE Network* 32.3 (2018), pp. 4–6.

[111] Jaya Dofe, Jonathan Frey, and Qiaoyan Yu. “Hardware security assurance in emerging IoT applications”. In: *2016 IEEE International Symposium on Circuits and Systems (ISCAS)*. IEEE. 2016, pp. 2050–2053.

[112] Chun Guo et al. “Authenticated encryption with nonce misuse and physical leakage: definitions, separation results and first construction”. In: *Progress in Cryptology–LATINCRYPT 2019: 6th International Conference on Cryptology and Information Security in Latin America, Santiago de Chile, Chile, October 2–4, 2019, Proceedings 6*. Springer. 2019, pp. 150–172.

[113] Anil Kumar Sutrala et al. “On the design of conditional privacy preserving batch verification-based authentication scheme for internet of vehicles deployment”. In: *IEEE Transactions on Vehicular Technology* 69.5 (2020), pp. 5535–5548.

[114] Mohammad Wazid et al. “Design of lightweight authentication and key agreement protocol for vehicular ad hoc networks”. In: *IEEE Access* 5 (2017), pp. 14966–14980.

[115] Mohammad Wazid et al. “Design and analysis of secure lightweight remote user authentication and key agreement scheme in internet of drones deployment”. In: *IEEE Internet of Things Journal* 6.2 (2018), pp. 3572–3584.

[116] Palak Bagga et al. “On the design of mutual authentication and key agreement protocol in internet of vehicles-enabled intelligent transportation system”. In: *IEEE Transactions on Vehicular Technology* 70.2 (2021), pp. 1736–1751.

[117] Xiaodong Lin et al. “TSVC: Timed efficient and secure vehicular communications with privacy preserving”. In: *IEEE transactions on wireless communications* 7.12 (2008), pp. 4987–4998.

[118] Chen Lyu et al. “PBA: Prediction-based authentication for vehicle-to-vehicle communications”. In: *IEEE transactions on dependable and secure computing* 13.1 (2015), pp. 71–83.

[119] Fei Wang et al. “2FLIP: A two-factor lightweight privacy-preserving authentication scheme for VANET”. In: *IEEE Transactions on Vehicular Technology* 65.2 (2015), pp. 896–911.

[120] Farshad Rahimi Asl and Reza Samavi. “SyNORM: Symmetric non repudiated message authentication in vehicular ad hoc networks”. In: *2017 IEEE 86th Vehicular Technology Conference (VTC-Fall)*. IEEE. 2017, pp. 1–5.

[121] Xincheng Li, Yali Liu, and Xinchun Yin. “An anonymous conditional privacy-preserving authentication scheme for VANETs”. In: *2019 IEEE 21st International Conference on High Performance Computing and Communications; IEEE 17th International Conference on Smart City; IEEE 5th International Conference on Data Science and Systems (HPCC/SmartCity/DSS)*. IEEE. 2019, pp. 1763–1770.

[122] Chenxi Zhang, Pin-Han Ho, and Janos Tapolcai. “On batch verification with group testing for vehicular communications”. In: *Wireless Networks* 17 (2011), pp. 1851–1865.

[123] Cheng-Chi Lee and Yan-Ming Lai. “Toward a secure batch verification with group testing for VANET”. In: *Wireless networks* 19 (2013), pp. 1441–1449.

[124] Shiang-Feng Tzeng et al. “Enhancing security and privacy for identity-based batch verification scheme in VANETs”. In: *IEEE Transactions on Vehicular Technology* 66.4 (2015), pp. 3235–3248.

[125] Trupil Limbasiya and Debasis Das. “ESCBV: energy-efficient and secure communication using batch verification scheme for vehicle users”. In: *Wireless Networks* 25.7 (2019), pp. 4403–4414.

[126] Tao Jing et al. “Timeliness Improvement of Information Interaction for IoVs Using Mini-Batch Identification Strategy”. In: *2022 IEEE 25th International Conference on Intelligent Transportation Systems (ITSC)*. IEEE. 2022, pp. 2101–2106.

[127] Yili Jiang et al. “Anonymous and efficient authentication scheme for privacy-preserving distributed learning”. In: *IEEE Transactions on Information Forensics and Security* 17 (2022), pp. 2227–2240.

[128] Xiaotong Zhou et al. “Efficient certificateless conditional privacy-preserving authentication for VANETs”. In: *IEEE Transactions on Vehicular Technology* 71.7 (2022), pp. 7863–7875.

[129] Fan Wu et al. “Batch-assisted verification scheme for reducing message verification delay of the vehicular ad hoc networks”. In: *IEEE Internet of Things Journal* 7.9 (2020), pp. 8144–8156.

[130] Huei-Wen Ferng et al. “Messages classification and dynamic batch verification scheme for vanets”. In: *IEEE Transactions on Mobile Computing* 20.3 (2019), pp. 1156–1172.

[131] Lei Zhang et al. “Hybrid and hierarchical aggregation-verification scheme for VANET”. In: *IEEE Transactions on Vehicular Technology* 71.10 (2022), pp. 11189–11200.

[132] Qi Tao et al. “B-DSPA: A Blockchain-based Dynamically Scalable Privacy-Preserving Authentication Scheme in Vehicular Ad-hoc Networks”. In: *IEEE Internet of Things Journal* (2023).

[133] Jingwei Liu et al. “CPAHP: Conditional Privacy-Preserving Authentication Scheme With Hierarchical Pseudonym for 5G-Enabled IoV”. In: *IEEE Transactions on Vehicular Technology* (2023).

[134] Chenxi Zhang et al. “An efficient identity-based batch verification scheme for vehicular sensor networks”. In: *IEEE INFOCOM 2008-The 27th Conference on Computer Communications*. IEEE. 2008, pp. 246–250.

[135] NB Gayathri et al. “Efficient pairing-free certificateless authentication scheme with batch verification for vehicular ad-hoc networks”. In: *IEEE Access* 6 (2018), pp. 31808–31819.

[136] Debiao He et al. “An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks”. In: *IEEE Transactions on Information Forensics and Security* 10.12 (2015), pp. 2681–2691.

[137] Mingming Cui, Dezhi Han, and Jun Wang. “An efficient and safe road condition monitoring authentication scheme based on fog computing”. In: *IEEE Internet of Things Journal* 6.5 (2019), pp. 9076–9084.

[138] Reza Curtmola et al. “Searchable symmetric encryption: improved definitions and efficient constructions”. In: *Proceedings of the 13th ACM conference on Computer and communications security*. 2006, pp. 79–88.

[139] Seny Kamara, Charalampos Papamanthou, and Tom Roeder. “Dynamic searchable symmetric encryption”. In: *Proceedings of the 2012 ACM conference on Computer and communications security*. 2012, pp. 965–976.

[140] David Cash et al. “Dynamic searchable encryption in very-large databases: Data structures and implementation”. In: *Cryptology ePrint Archive* (2014).

[141] Shi-Feng Sun et al. “An efficient non-interactive multi-client searchable encryption with support for boolean queries”. In: *Computer Security–ESORICS 2016: 21st European Symposium on Research in Computer Security, Heraklion, Greece, September 26-30, 2016, Proceedings, Part I 21*. Springer. 2016, pp. 154–172.

[142] Qi Jiang et al. “Three-factor authentication protocol using physical unclonable function for IoV”. In: *Computer Communications* 173 (2021), pp. 45–55.

[143] Muhamed Turkanović, Boštjan Brumen, and Marko Hölbl. "A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the Internet of Things notion". In: *Ad Hoc Networks* 20 (2014), pp. 96–112.

[144] Mohammad Sabzinejad Farash et al. "An efficient user authentication and key agreement scheme for heterogeneous wireless sensor network tailored for the Internet of Things environment". In: *Ad Hoc Networks* 36 (2016), pp. 152–176.

[145] Sravani Challa et al. "Secure signature-based authenticated key establishment scheme for future IoT applications". In: *Ieee Access* 5 (2017), pp. 3028–3043.

[146] Jongho Won, Seung-Hyun Seo, and Elisa Bertino. "Certificateless cryptographic protocols for efficient drone-based smart city applications". In: *IEEE Access* 5 (2017), pp. 3721–3749.

[147] Muhammad Asghar Khan et al. "A provable and privacy-preserving authentication scheme for UAV-enabled intelligent transportation systems". In: *IEEE Transactions on Industrial Informatics* 18.5 (2021), pp. 3416–3425.

[148] Sajid Hussain et al. "Designing secure and lightweight user access to drone for smart city surveillance". In: *Computer Standards & Interfaces* 80 (2022), p. 103566.

[149] Fan Wu et al. "A novel authentication scheme for edge computing-enabled Internet of Vehicles providing anonymity and identity tracing with drone-assistance". In: *Journal of Systems Architecture* 132 (2022), p. 102737.

[150] Shehzad Ashraf Chaudhry et al. "A lightweight authentication scheme for 6G-IoT enabled maritime transport system". In: *IEEE Transactions on Intelligent Transportation Systems* 24.2 (2021), pp. 2401–2410.

[151] Yevgeniy Dodis, Leonid Reyzin, and Adam Smith. "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data". In: *Advances In Cryptology-EUROCRYPT 2004: International Conference On The Theory And Applications Of Cryptographic Techniques, Interlaken, Switzerland, May 2-6, 2004. Proceedings 23*. Springer. 2004, pp. 523–540.

[152] Russell Housley. *Using AES-CCM and AES-GCM authenticated encryption in the cryptographic message syntax (CMS)*. Tech. rep. 2007.

[153] Andrey Bogdanov et al. "ALE: AES-based lightweight authenticated encryption". In: *Fast Software Encryption: 20th International Workshop, FSE 2013, Singapore, March 11-13, 2013. Revised Selected Papers 20*. Springer. 2014, pp. 447–466.

[154] Kosei Sakamoto et al. "Rocca: an efficient AES-based encryption scheme for beyond 5G". In: *IACR Transactions on Symmetric Cryptology* (2021), pp. 1–30.

[155] Cuauhtemoc Mancillas-López and Brisbane Ovilla-Martínez. "An Ultra-Fast Authenticated Encryption Scheme with Associated Data Using AES-OTR". In: *Journal of Circuits, Systems and Computers* 31.09 (2022), p. 2250167.

[156] Yusuke Naito, Yu Sasaki, and Takeshi Sugawara. "Aes-lbbb: Aes mode for lightweight and bbb-secure authenticated encryption". In: *IACR Transactions on Cryptographic Hardware and Embedded Systems* (2021), pp. 298–333.

[157] Ronaldo Serrano et al. "ChaCha20–Poly1305 Authenticated Encryption with Additional Data for Transport Layer Security 1.3". In: *Cryptography* 6.2 (2022), p. 30.

[158] Muhammad Ghulam Ghouse et al. “i-AEGIS-128: an improved authenticated encryption based on AEGIS-128”. In: *2021 7th International Conference on Optimization and Applications (ICOA)*. IEEE. 2021, pp. 1–7.

[159] Jeroen Delvaux et al. “Helper Data Algorithms for PUF-Based Key Generation: Overview and Analysis”. In: *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems* 34.6 (2015), pp. 889–902. DOI: 10.1109/TCAD.2014.2370531.

[160] Venkata P Yanambaka et al. “PMsec: Physical unclonable function-based robust and lightweight authentication in the internet of medical things”. In: *IEEE Transactions on Consumer Electronics* 65.3 (2019), pp. 388–397.

[161] Krishna Prasad Satamraju and B. Malarkodi. “A PUF-based Mutual Authentication Protocol for Internet of Things”. In: *2020 5th International Conference on Computing, Communication and Security (ICCCS)*. 2020, pp. 1–6. DOI: 10.1109/ICCCS49678.2020.9276868.

[162] Hassan N. Noura, Reem Melki, and Ali Chehab. “Secure and Lightweight Mutual Multi-Factor Authentication for IoT Communication Systems”. In: *2019 IEEE 90th Vehicular Technology Conference (VTC2019-Fall)*. 2019, pp. 1–7. DOI: 10.1109/VTCFall.2019.8891082.

[163] Konstantinos Goutsos and Alex Bystrov. “Lightweight PUF-based Continuous Authentication Protocol”. In: *2019 International Conference on Computing, Electronics and Communications Engineering (iCCECE)*. 2019, pp. 229–234. DOI: 10.1109/iCCECE46942.2019.8941608.

[164] C. Gouvêa and J. C. López-Hernández. “High Speed Implementation of Authenticated Encryption for the MSP430X Microcontroller”. In: (2012), pp. 288–304. DOI: 10.1007/978-3-642-33481-8_16.

[165] Dang Khoa Nguyen, Leonardo Lanante, and Hiroshi Ochi. “High Throughput–Resource Saving Hardware Implementation of AES-CCM for Robust Security Network”. In: *Journal of Automation and Control Engineering Vol* 1.3 (2013).

[166] Soufiane Oukili and Seddik Bri. “Hardware implementation of AES algorithm with logic S-box”. In: *Journal of Circuits, Systems and Computers* 26.09 (2017), p. 1750141.

[167] Paul Burciu. “An efficient (low resources) modular hardware implementation of the AES algorithm”. In: *Journal of Electrical Engineering, Electronics, Control and Computer Science* 5.3 (2019), pp. 1–10.

[168] Safiullah Khan, Wai-Kong Lee, and Seong Oun Hwang. “Scalable and Efficient Hardware Architectures for Authenticated Encryption in IoT Applications”. In: *IEEE Internet of Things Journal* 8.14 (2021), pp. 11260–11275. DOI: 10.1109/JIOT.2021.3052184.

[169] Paweł Morawiecki et al. “ICEPOLE v1”. In: *submitted to the CAESAR competition* (2015).

[170] Vincent Grosso et al. “SCREAM & iSCREAM side-channel resistant authenticated encryption with masking”. In: *Submission to CAESAR* (2014).

[171] C. Dobraunig et al. *Ascon v1, CAESAR submissions*. 2014. URL: http://competitions.cr.yp.to/round1/asconv1.pdf.

[172] T. Iwata et al. *Cloc: Compact low-overhead CFB*. CAESAR submissions. 2014.

[173] F. Abed et al. *The Poet Family of On-line Authenticated Encryption Schemes*. CAESAR Submissions. CAESAR. 2014. URL: https://competitions.cr.yp.to/round1/poetv101.pdf.

[174] J. Jean, I. Nikolić, and T. Peyrin. *Deoxys v1*. CAESAR submissions. 2014. URL: http://competitions.cr.yp.to/round1/deoxysv1.pdf.

[175] A. Biryukov and D. Khovratovich. *Paeq v1, CAESAR submissions*. Available: http://competitions.cr.yp.to/round1/paeqv1.pdf. 2014. URL: http://competitions.cr.yp.to/round1/paeqv1.pdf.

[176] Athena Research Group. *FPGA and ASIC Implementations of Authenticated Ciphers*. http://cryptography.gmu.edu/athenadb/fpga_auth_cipher/rankings_view.

[177] Chien-Ming Chen et al. "A secure authentication protocol for internet of vehicles". In: *Ieee Access* 7 (2019), pp. 12047–12057.

[178] Degan Zhang, Ting Zhang, and Xiaohuan Liu. "Novel self-adaptive routing service algorithm for application in VANET". In: *Applied Intelligence* 49 (2019), pp. 1866–1879.

[179] Trupil Limbasiya and Debasis Das. "Lightweight secure message broadcasting protocol for vehicle-to-vehicle communication". In: *IEEE Systems Journal* 14.1 (2019), pp. 520–529.

[180] Dingyi Pei, Arto Salomaa, and Cunsheng Ding. *Chinese remainder theorem: applications in computing, coding, cryptography*. World Scientific, 1996.

[181] Ran Canetti and Hugo Krawczyk. "Analysis of key-exchange protocols and their use for building secure channels". In: *International conference on the theory and applications of cryptographic techniques*. Springer. 2001, pp. 453–474.

[182] M Peters and P Rogaar. "A review of ProVerif as an automatic security protocol verifier". In: (2011).

[183] Ralf Küsters and Tomasz Truderung. "Using ProVerif to analyze protocols with Diffie-Hellman exponentiation". In: *2009 22nd IEEE Computer Security Foundations Symposium*. IEEE. 2009, pp. 157–171.

[184] Li-Minn Ang et al. "Deployment of IoV for Smart Cities: Applications, Architecture, and Challenges". In: *IEEE Access* 7 (2019), pp. 6473–6492. DOI: 10.1109/ACCESS.2018.2887076.

[185] Arooj Masood, Demeke Shumeye Lakew, and Sungrae Cho. "Security and privacy challenges in connected vehicular cloud computing". In: *IEEE Communications Surveys & Tutorials* 22.4 (2020), pp. 2725–2764.

[186] Prashant Rewagad and Yogita Pawar. "Use of digital signature with diffie hellman key exchange and AES encryption algorithm to enhance data security in cloud computing". In: *2013 International Conference on Communication Systems and Network Technologies*. IEEE. 2013, pp. 437–439.

[187] Jingwei Liu et al. "An efficient anonymous authentication scheme for internet of vehicles". In: *2018 IEEE International Conference on Communications (ICC)*. IEEE. 2018, pp. 1–6.

[188] Shancang Li, Li Da Xu, and Shanshan Zhao. "The internet of things: a survey". In: *Information systems frontiers* 17 (2015), pp. 243–259.

[189] Dan Boneh, Xavier Boyen, and Hovav Shacham. "Short group signatures". In: *Annual international cryptology conference*. Springer. 2004, pp. 41–55.

[190] Seyed Morteza Pournaghi et al. "NECPPA: A novel and efficient conditional privacy-preserving authentication scheme for VANET". In: *Computer Networks* 134 (2018), pp. 78–92.

[191] Dennis Meffert. "Bilinear pairings in cryptography". In: *Radboud Universiteit Nijmegen, Computing Science Department, the Netherlands* (2009), pp. 22–82.

[192] Reza R Farashahi et al. "Indifferentiable deterministic hashing to elliptic and hyperelliptic curves". In: *Mathematics of Computation* 82.281 (2013), pp. 491–512.

[193] JiuJun Cheng et al. “Routing in Internet of Vehicles: A Review”. In: *IEEE Transactions on Intelligent Transportation Systems* 16.5 (2015), pp. 2339–2352. DOI: 10.1109/TITS.2015.2423667.

[194] Tilmann Rabl et al. “Apache Flink in current research”. In: *it - Information Technology* 58.4 (2016), pp. 157–165.

[195] Dorian Amiet, Andreas Curiger, and Paul Zbinden. “FPGA-based accelerator for post-quantum signature scheme SPHINCS-256”. In: *IACR Transactions on Cryptographic Hardware and Embedded Systems* (2018), pp. 18–39.

[196] Tim Good and Mohammed Benaissa. “AES as stream cipher on a small FPGA”. In: *2006 IEEE International Symposium on Circuits and Systems*. IEEE. 2006, 4–pp.

[197] Ravi Shankar Dhakar, Amit Kumar Gupta, and Prashant Sharma. “Modified RSA encryption algorithm (MREA)”. In: *2012 second international conference on advanced computing & communication technologies*. IEEE. 2012, pp. 426–429.

[198] Jiun-Long Huang, Lo-Yao Yeh, and Hung-Yu Chien. “ABAKA: An anonymous batch authenticated and key agreement scheme for value-added services in vehicular ad hoc networks”. In: *IEEE Transactions on vehicular technology* 60.1 (2010), pp. 248–262.

[199] National Highway Traffic Safety Administration. *Vehicle Safety Research*. https://www.nhtsa.gov/vehicle-safety-research. Accessed: 2024-06-24.

[200] Zeeshan Hameed Mir et al. “Enabling DSRC and C-V2X integrated hybrid vehicular networks: Architecture and protocol”. In: *IEEE access* 8 (2020), pp. 180909–180927.

[201] Matteo Petracca et al. “On-board unit hardware and software design for vehicular ad-hoc networks”. In: *Roadside Networks for Vehicular Communications: Architectures, Applications, and Test Fields*. IGI Global, 2013, pp. 38–56.

[202] Andrés F Acosta, Jorge E Espinosa, and Jairo Espinosa. “TraCI4Matlab: Enabling the integration of the SUMO road traffic simulator and Matlab® through a software re-engineering process”. In: *Modeling Mobility with Open Data: 2nd SUMO Conference 2014 Berlin, Germany, May 15-16, 2014*. Springer. 2015, pp. 155–170.

[203] Shaik Ashfaq Hussain et al. “A review of quality of service issues in Internet of Vehicles (IoV)”. In: *2019 Amity International Conference on Artificial Intelligence (AICAI)*. IEEE. 2019, pp. 380–383.

[204] Ding Wang et al. “Zipf’s law in passwords”. In: *IEEE Transactions on Information Forensics and Security* 12.11 (2017), pp. 2776–2791.

[205] Mingyue Zhang et al. “EC-BAAS: Elliptic curve-based batch anonymous authentication scheme for Internet of Vehicles”. In: *Journal of Systems Architecture* 117 (2021), p. 102161.

[206] Yafang Yang et al. “Privacy-preserving aggregation-authentication scheme for safety warning system in fog-cloud based VANET”. In: *IEEE Transactions on Information Forensics and Security* 17 (2022), pp. 317–331.

[207] Seny Kamara and Tarik Moataz. “Boolean searchable symmetric encryption with worst-case sublinear complexity”. In: *Advances in Cryptology–EUROCRYPT 2017: 36th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Paris, France, April 30–May 4, 2017, Proceedings, Part III 36*. Springer. 2017, pp. 94–124.

[208] Weisen Shi et al. “Drone assisted vehicular networks: Architecture, challenges and opportunities”. In: *IEEE Network* 32.3 (2018), pp. 130–137.

[209] Alireza Shamsoshoara et al. “A survey on physical unclonable function (PUF)-based security solutions for Internet of Things”. In: *Computer Networks* 183 (2020), p. 107593.

[210] Blaise Gassend et al. “Silicon physical random functions”. In: *Proceedings of the 9th ACM Conference on Computer and Communications Security*. 2002, pp. 148–160.

[211] Blaise Gassend et al. “Controlled physical random functions”. In: *18th Annual Computer Security Applications Conference, 2002. Proceedings.* IEEE. 2002, pp. 149–160.

[212] Jorge Guajardo et al. “FPGA intrinsic PUFs and their use for IP protection”. In: *Cryptographic Hardware and Embedded Systems-CHES 2007: 9th International Workshop, Vienna, Austria, September 10-13, 2007. Proceedings 9*. Springer. 2007, pp. 63–80.

[213] Raphael Spreitzer et al. “Systematic classification of side-channel attacks: A case study for mobile devices”. In: *IEEE communications surveys & tutorials* 20.1 (2017), pp. 465–488.

[214] Iliano Cervesato. “The Dolev-Yao intruder is the most powerful attacker”. In: *16th Annual Symposium on Logic in Computer Science—LICS*. Vol. 1. Citeseer. 2001, pp. 1–2.

[215] Gregory H Shill. “Public Comment on Request for Comments on the National Highway Traffic Safety Administration’s New Car Assessment Program. Docket ID: NHTSA-2021-0002-0482”. In: *Docket ID: NHTSA-2021-0002-0482 (May 26, 2022). U Iowa Legal Studies Research Paper* 2022-11 (2022).

[216] Chao Lin et al. “Security and privacy for the internet of drones: Challenges and solutions”. In: *IEEE Communications Magazine* 56.1 (2018), pp. 64–69.

[217] Lav Gupta, Raj Jain, and Gabor Vaszkun. “Survey of important issues in UAV communication networks”. In: *IEEE communications surveys & tutorials* 18.2 (2015), pp. 1123–1152.

[218] Mahmoud Ammar, Giovanni Russello, and Bruno Crispo. “Internet of Things: A survey on the security of IoT frameworks”. In: *Journal of Information Security and Applications* 38 (2018), pp. 8–27.

[219] Teng Xu, James B Wendt, and Miodrag Potkonjak. “Security of IoT systems: Design challenges and opportunities”. In: *2014 IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*. IEEE. 2014, pp. 417–423.

[220] Ako Muhamad Abdullah et al. “Advanced encryption standard (AES) algorithm to encrypt and decrypt data”. In: *Cryptography and Network Security* 16.1 (2017), p. 11.

[221] Seung-Jo Han, Heang-Soo Oh, and Jongan Park. “The improved data encryption standard (DES) algorithm”. In: *Proceedings of ISSSTA’95 International Symposium on Spread Spectrum Techniques and Applications*. Vol. 3. IEEE. 1996, pp. 1310–1314.

[222] Rajdeep Bhanot and Rahul Hans. “A review and comparative analysis of various encryption algorithms”. In: *International Journal of Security and Its Applications* 9.4 (2015), pp. 289–306.

[223] Issam Damaj and Safaa Kasbah. “An analysis framework for hardware and software implementations with applications from cryptography”. In: *Computers & Electrical Engineering* 69 (2018), pp. 572–584.

[224] Sundararaman Rajagopalan et al. “Survey and analysis of hardware cryptographic and steganographic systems on FPGA”. In: *Journal of Applied Sciences(Faisalabad)* 12.3 (2012), pp. 201–210.

[225] Arvind Singh et al. “Energy efficient and side-channel secure cryptographic hardware for IoT-edge nodes”. In: *IEEE Internet of Things Journal* 6.1 (2018), pp. 421–434.

[226] Vishal A Thakor, Mohammad Abdur Razzaque, and Muhammad RA Khandaker. “Lightweight cryptography algorithms for resource-constrained IoT devices: A review, comparison and research opportunities”. In: *IEEE Access* 9 (2021), pp. 28177–28193.

[227] Zhe Liu et al. “Elliptic curve cryptography with efficiently computable endomorphisms and its hardware implementations for the internet of things”. In: *IEEE Transactions on Computers* 66.5 (2016), pp. 773–785.

[228] R Kousalya and GA Sathish Kumar. “A survey of light-weight cryptographic algorithm for information security and hardware efficiency in resource constrained devices”. In: *2019 International Conference on Vision Towards Emerging Trends in Communication and Networking (ViTECoN)*. IEEE. 2019, pp. 1–5.

[229] Kyungho Kim et al. “FACE–LIGHT: Fast AES–CTR mode encryption for low-end microcontrollers”. In: *Information Security and Cryptology–ICISC 2019: 22nd International Conference, Seoul, South Korea, December 4–6, 2019, Revised Selected Papers 22*. Springer. 2020, pp. 102–114.

[230] James M Turner. “The keyed-hash message authentication code (hmac)”. In: *Federal Information Processing Standards Publication* 198.1 (2008), pp. 1–13.