Bibliography

[1] *6 firms that are testing driverless cars*. Accessed March 1, 2021. URL: https://ddswireless.com/blog/6-companies-leading-the-charge-in-self-driving-vehicles/.

[2] *Car to car communications a step closer*. 2012. URL: https://www.itsinternational.com/its10/feature/car-car-communications-step-closer.

[3] *U.S. Department of Transportation Announces Decision to Move Forward with Vehicle-to-Vehicle Communication Technology for Light Vehicles*. 2014. URL: https://mobility21.cmu.edu/u-s-department-of-transportation-announces-decision-to-move-forward-with-vehicle-to-vehicle-communication-technology-for-light-vehicles/.

[4] *Google Self-Driving Car Project*. Accessed March 1, 2021. URL: https://waymo.com/.

[5] IEEE-1609.2. "IEEE Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages". In: (2016). URL: https://standards.ieee.org/standard/1609_2-2016.html.

[6] ETSI. *ETSI TS 103 097 v1.2.1-Intelligent Transport Systems (ITS); Security; Security Header and Certificate Formats, Standard, TC ITS*. ETSI TS 103 097, 2015. URL: https://www.etsi.org/deliver/etsi_ts/103000_103099/103097/01.02.01_60/ts_103097v010201p.pdf.

[7] ETSI. *Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Definitions*. ETSI Tech. TR-102-638, 2009. URL: https://www.etsi.org/deliver/etsi_tr/102600_102699/102638/01.01.01_60/tr_102638v010101p.pdf.

[8] ETSI TR 102 731. *Intelligent Transport Systems (ITS); Security; Security Services and Architecture*. 2009. URL: https://www.etsi.org/deliver/etsi_ts/102700_102799/102731/01.01.01_60/ts_102731v010101p.pdf.

[9] ETSI TR 102 941. *Intelligent Transport Systems (ITS); Security; Trust and Privacy Management*. 2012. URL: https://www.etsi.org/deliver/etsi_ts/102900_102999/102941/01.01.01_60/ts_102941v010101p.pdf.

[10] *PKI Memo*. Tech. rep. C2C-CC, 2011. URL: http://www.car-2-car.org/.

[11] Panagiotis Papadimitratos, Virgil Gligor, and Jean-Pierre Hubaux. "Securing Vehicular Communications-Assumptions, Requirements, and Principles". In: *Workshop on Embedded Security in Cars (ESCAR)*. Berlin, Germany, 2006, pp. 5–14. URL: https://people.kth.se/~papadim/publications/fulltext/secure-vehicular-communication-requirements-fundamentals.pdf.

[12] Panagiotis Papadimitratos, Levente Buttyan, Tamas Holczer, Elmar Schoch, Julien Freudiger, Maxim Raya, Zhendong Ma, Frank Kargl, Antonio Kung, and J-P Hubaux. "Secure Vehicular Communication Systems: Design and Architecture". In: *IEEE Communications Magazine* 46.11 (2008), pp. 100–109. URL: https://ieeexplore.ieee.org/document/4689252.

[13] Frank Kargl, Panos Papadimitratos, Levente Buttyan, M Muter, Elmar Schoch, Bjoern Wiedersheim, Ta-Vinh Thong, Giorgio Calandriello, Albert Held, and Antonio Kung. "Secure Vehicular Communication Systems: Implementation, Performance, and Research Challenges". In: *IEEE Communications Magazine* 46.11 (2008), pp. 110–118. URL: https://ieeexplore.ieee.org/abstract/document/4689253.

[14] Panagiotis Papadimitratos, Levente Buttyan, J-P Hubaux, Frank Kargl, Antonio Kung, and Maxim Raya. "Architecture for Secure and Private Vehicular Communications". In: *IEEE International Conference on ITS Telecommunications (ITST)*. Sophia Antipolis, France, 2007, pp. 1–6. URL: https://ieeexplore.ieee.org/abstract/document/4295890.

[15] W. Whyte, A Weimerskirch, V. Kumar, and T. Hehn. “A Security Credential Management System for V2V Communications”. In: *IEEE Vehicular Networking Conference (VNC)*. Boston, MA, 2013, pp. 1–8. URL: https://ieeexplore.ieee.org/abstract/document/6737583.

[16] M. Khodaei, H. Jin, and P. Papadimitratos. “SECMACE: Scalable and Robust Identity and Credential Management Infrastructure in Vehicular Communication Systems”. In: *IEEE Transactions on Intelligent Transportation Systems* 19.5 (2018), pp. 1430–1444. URL: https://ieeexplore.ieee.org/abstract/document/8332521.

[17] Mohammad Khodaei, Hamid Noroozi, and Panos Papadimitratos. “Scaling Pseudonymous Authentication for Large Mobile Systems”. In: *Proceedings of the 12th ACM Conference on Security & Privacy in Wireless and Mobile Networks (ACM WiSec)*. Miami, FL, USA, 2019. URL: https://dl.acm.org/doi/10.1145/3317549.3323410.

[18] P. Papadimitratos, A La Fortelle, K. Evenssen, R. Brignolo, and S. Cosenza. “Vehicular Communication Systems: Enabling Technologies, Applications, and Future Outlook on Intelligent Transportation”. In: *IEEE Communications Magazine* 47.11 (2009), pp. 84–95. URL: https://ieeexplore.ieee.org/document/5307471.

[19] Reza Shokri, George Theodorakopoulos, Panos Papadimitratos, Ehsan Kazemi, and J-P Hubaux. “Hiding in the Mobile Crowd: Location Privacy through Collaboration”. In: *IEEE Transactions on Dependable and Secure Computing* 11.3 (2014), pp. 266–279. URL: https://ieeexplore.ieee.org/abstract/document/6682907.

[20] Hongyu Jin and Panos Papadimitratos. “Resilient Privacy Protection for Location-Based Services Through Decentralization”. In: *ACM Transactions on Privacy and Security (ACM TOPS)* 22.4 (2019), 21:1–36. URL: https://dl.acm.org/doi/abs/10.1145/3319401.

[21] Stylianos Gisdakis, Vasileios Manolopoulos, Sha Tao, Ana Rusu, and Panagiotis Papadimitratos. “Secure and Privacy-Preserving Smartphone-Based Traffic Information Systems”. In: *IEEE Transactions on Intelligent Transportation Systems (IEEE ITS)* 16.3 (2015), pp. 1428–1438.

[22] V. Manolopoulos, S. Tao, A. Rusu, and P. Papadimitratos. “HotMobile 2012 Demo: Smartphone-based Traffic Information System for Sustainable Cities”. In: *ACM Mobile Computing and Communications Review (ACM MC2R)* 16.4 (2012), pp. 30–31. ISSN: 1559-1662.

[23] V. Manolopoulos, Panos Papadimitratos, S. Tao, and A. Rusu. "Securing Smartphone based ITS". In: *IEEE International Conference on ITS Telecommunications (IEEE ITST)*. St. Petersburg, Russia, 2011, pp. 201–206.

[24] H. Jin, M. Khodaei, and P. Papadimitratos. "Security and Privacy in Vehicular Social Networks". In: *Vehicular Social Networks*. Taylor & Francis Group, 2016. URL: https://www.taylorfrancis.com/chapters/edit/10.1201/9781315368450-12/security-privacy-vehicular-social-networks-hongyu-jin-mohammad-khodaei-panos-papadimitratos.

[25] Virendra Kumar, Jonathan Petit, and William Whyte. "Binary Hash Tree based Certificate Access Management for Connected Vehicles". In: *Proceedings of the 10th ACM Conference on Security and Privacy in Wireless and Mobile Networks (ACM WiSec)*. Boston, USA, 2017. URL: https://dl.acm.org/doi/abs/10.1145/3098243.3098257.

[26] Patrick McDaniel and Aviel Rubin. "A Response to *"Can We Eliminate Certificate Revocation Lists?"*" In: *FC (Springer)*. Berlin, Heidelberg, 2000, pp. 245–258. URL: https://doi.org/10.1007/3-540-45472-1_17.

[27] Jeremy Clark and Paul C Van Oorschot. "SoK: SSL and HTTPS: Revisiting Past Challenges and Evaluating Certificate Trust Model Enhancements". In: *IEEE SnP*. Berkeley, USA, 2013. URL: https://ieeexplore.ieee.org/abstract/document/6547130.

[28] Mohammad Khodaei and Panos Papadimitratos. "Efficient, Scalable, and Resilient Vehicle-Centric Certificate Revocation List Distribution in VANETs". In: *Proceedings of the 11th ACM Conference on Security & Privacy in Wireless and Mobile Networks (ACM WiSec)*. Stockholm, Sweden, 2018. URL: https://dl.acm.org/doi/abs/10.1145/3212480.3212481.

[29] Marcos A Simplicio Jr, Eduardo Lopes Cominetti, Harsh Kupwade Patil, Jefferson E Ricardini, and Marcos Vinicius M Silva. "ACPC: Efficient Revocation of Pseudonym Certificates using Activation Codes". In: *Elsevier Ad Hoc Networks* (2018). URL: https://www.sciencedirect.com/science/article/pii/S1570870518304761.

[30] M. Khodaei, H. Jin, and P. Papadimitratos. "Towards Deploying a Scalable & Robust Vehicular Identity and Credential Management Infrastructure". In: *IEEE Vehicular Networking Conference (VNC)*. Paderborn, Germany, 2014. URL: https://ieeexplore.ieee.org/abstract/document/7013306.

[31] Ismail Ari, Bo Hong, Ethan L Miller, Scott A Brandt, and Darrell DE Long. "Managing Flash Crowds on the Internet". In: *IEEE/ACM MASCOTS*. Orlando, FL, USA, 2003, pp. 246–249. URL: https://ieeexplore.ieee.org/abstract/document/1240667.

[32] Stefan Santesson, Michael Myers, Rich Ankney, Ambarish Malpani, Slava Galperin, and Carlisle Adams. *X. 509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP*. Tech. rep. 2013. URL: https://www.hjp.at/doc/rfc/rfc6960.html.

[33] Giorgio Calandriello, Panos Papadimitratos, Jean-Pierre Hubaux, and Antonio Lioy. "Efficient and Robust Pseudonymous Authentication in VANET". In: *ACM VANET*. NY, USA, 2007, pp. 19–28. URL: https://dl.acm.org/doi/abs/10.1145/1287748.1287752.

[34] Panos Papadimitratos, Giorgio Calandriello, Jean-Pierre Hubaux, and Antonio Lioy. "Impact of Vehicular Communications Security on Transportation Safety". In: *IEEE INFOCOM Mobile Networking for Vehicular Environments (MOVE) Workshop (IEEE MOVE)*. Phoenix, AZ, USA, 2008, pp. 1–6. URL: https://ieeexplore.ieee.org/abstract/document/4544663.

[35] Giorgio Calandriello, Panos Papadimitratos, J-P Hubaux, and Antonio Lioy. "On the Performance of Secure Vehicular Communication Systems". In: *IEEE Transactions on Dependable and Secure Computing (TDSC)* 8.6 (2011), pp. 898–912. URL: https://ieeexplore.ieee.org/abstract/document/5611547.

[36] M. Khodaei, A. Messing, and P. Papadimitratos. "RHyTHM: A Randomized Hybrid Scheme To Hide in the Mobile Crowd". In: *IEEE Vehicular Networking Conference (VNC)*. Torino, Italy, 2017. URL: https://ieeexplore.ieee.org/abstract/document/8275642.

[37] Zhendong Ma, Frank Kargl, and Michael Weber. "Pseudonym-on-demand: A New Pseudonym Refill Strategy for Vehicular Communications". In: *IEEE VTC*. Calgary, BC, 2008, pp. 1–5. URL: https://doi.org/10.1109/VETECF.2008.455.

[38] Mohammad Khodaei and Panos Papadimitratos. “Evaluating On-demand Pseudonym Acquisition Policies in Vehicular Communication Systems”. In: *Proceedings of the First International Workshop on Internet of Vehicles and Vehicles of Internet (IoV/VoI)*. Paderborn, Germany, 2016. URL: https://dl.acm.org/doi/abs/10.1145/2938681.2938684.

[39] John R Douceur. “The Sybil Attack”. In: *ACM Peer-to-peer Systems*. London, UK, 2002. URL: https://link.springer.com/chapter/10.1007/3-540-45748-8_24.

[40] Hamid Noroozi, Mohammad Khodaei, and Panos Papadimitratos. “DEMO: VPKIaaS: A Highly-Available and Dynamically-Scalable Vehicular Public-Key Infrastructure”. In: *Proceedings of the 11th ACM Conference on Security & Privacy in Wireless and Mobile Networks (ACM WiSec)*. Stockholm, Sweden, 2018. URL: https://dl.acm.org/doi/abs/10.1145/3212480.3226100.

[41] Pierpaolo Cincilla, Omar Hicham, and Benoit Charles. “Vehicular PKI Scalability-Consistency Trade-Offs in Large Scale Distributed Scenarios”. In: *IEEE Vehicular Networking Conference (VNC)*. Columbus, Ohio, USA, 2016. URL: https://ieeexplore.ieee.org/abstract/document/7835970.

[42] Martin Fowler and Kent Beck. *Refactoring: Improving the design of existing code*. 2018. URL: https://martinfowler.com/books/refactoring.html.

[43] Mohammad Khodaei, Hamid Noroozi, and Panos Papadimitratos. “POSTER: Privacy Preservation through Uniformity”. In: *Proceedings of the 11th ACM Conference on Security & Privacy in Wireless and Mobile Networks (ACM WiSec)*. Stockholm, Sweden, 2018, pp. 279–280. URL: https://dl.acm.org/doi/abs/10.1145/3212480.3226101.

[44] *Redis, In-memory Data Structure Store, Used as a Database*. 2018. URL: https://redis.io/.

[45] *An Open Source Load Testing Tool*. 2019. URL: https://locust.io/.

[46] *What’s a Linux container?* 2021. URL: https://www.redhat.com/en/topics/containers/whats-a-linux-container.

[47] *What is a Container?A standardized unit of software*. 2021. URL: https://www.docker.com/resources/what-container.

[48] *Kubernetes: Production-Grade Container Orchestration*. 2019. URL: https://kubernetes.io/.

[49] *Google Kubernetes Engine Overview*. 2021. URL: https://cloud.google.com/kubernetes-engine/docs/concepts/kubernetes-engine-overview.

[50] *Kubernetes workloads, Pods*. 2021. URL: https://kubernetes.io/docs/concepts/workloads/pods/.

[51] *Kubernetes workloads, Deployments*. 2021. URL: https://kubernetes.io/docs/concepts/workloads/controllers/deployment/.

[52] *Kubernetes service*. 2021. URL: https://kubernetes.io/docs/concepts/services-networking/service/.

[53] *Kubernetes ingress*. 2021. URL: https://kubernetes.io/docs/concepts/services-networking/ingress/.

[54] *Kubelet*. 2021. URL: https://kubernetes.io/docs/reference/command-line-tools-reference/kubelet/.

[55] Martin Fowler. *Microservices, a definition of this new architectural term*. 2014. URL: https://martinfowler.com/articles/microservices.html.

[56] T. Leinmüller, L. Buttyan, J-P. Hubaux, F. Kargl, R. Kroh, P. Papadimitratos, M. Raya, and E. Schoch. "SEVECOM-Secure Vehicle Communication". In: *Proceedings of IST Mobile Summit*. 2006. URL: https://nss.proj.kth.se/publications/fulltext/sevecom-early-1.pdf.

[57] Antonio Kung. *Security Architecture and Mechanisms for V2V/V2I, SeVeCom - Deliverable 2.1*. Version 3.0. 2008. URL: https://sevecom.eu/Deliverables/Sevecom_Deliverable_D2.1_v3.0.pdf.

[58] PRESERVE-Project. 2015. URL: www.preserve-project.eu/.

[59] Stylianos Gisdakis, Marcello Laganà, Thanassis Giannetsos, and Panos Papadimitratos. "SEROSA: SERvice Oriented Security Architecture for Vehicular Communications". In: *IEEE Vehicular Networking Conference (VNC)*. Boston, MA, USA, 2013. URL: https://ieeexplore.ieee.org/abstract/document/6737597.

[60] Stylianos Gisdakis, Thanassis Giannetsos, and Panos Papadimitratos. "SPPEAR: Security and Privacy-preserving Architecture for Participatory-sensing Applications". In: *ACM Conference on Security & Privacy in Wireless and Mobile Networks (ACM WiSec)*. Oxford, United Kingdom, 2014, pp. 39–50. ISBN: 978-1-4503-2972-9.

[61] Stylianos Gisdakis, Thanassis Giannetsos, and Panagiotis Papadimitratos. "Security, Privacy, and Incentive Provision for Mobile Crowd Sensing Systems". In: *IEEE Internet of Things Journal (IEEE IoT)* 3.5 (2016), pp. 839–853.

[62] Thanassis Giannetsos, Stylianos Gisdakis, and Panos Papadimitratos. "Trustworthy People-Centric Sensing: Privacy, Security and User Incentives Road-Map". In: *IEEE IFIP Mediterranean Ad Hoc Networking Workshop (IEEE IFIP MedHocNet)*. Piran, Slovenia, 2014, pp. 39–46.

[63] M. Khodaei and P. Papadimitratos. "Scalable & Resilient Vehicle-Centric Certificate Revocation List Distribution in Vehicular Communication Systems". In: *IEEE Transactions on Mobile Computing (TMC)* (2021). URL: https://ieeexplore.ieee.org/abstract/document/9042314.

[64] Jason J Haas, Yih-Chun Hu, and Kenneth P Laberteaux. "Efficient Certificate Revocation List Organization and Distribution". In: *IEEE Journal on Selected Areas in Communications (JSAC)* 29.3 (2011), pp. 595–604. URL: https://ieeexplore.ieee.org/abstract/document/5719271.

[65] Kenneth P Laberteaux, Jason J Haas, and Yih-Chun Hu. "Security Certificate Revocation List Distribution for VANET". In: *Proceedings of the fifth ACM international workshop on VehiculAr Inter-NETworking*. New York, NY, USA, 2008. URL: https://dl.acm.org/doi/abs/10.1145/1410043.1410063.

[66] Jason J Haas, Yih-Chun Hu, and Kenneth P Laberteaux. "Design and Analysis of a Lightweight Certificate Revocation Mechanism for VANET". In: *Proceedings of the sixth ACM international workshop on VehiculAr InterNETworking*. New York, NY, USA, 2009. URL: https://dl.acm.org/doi/abs/10.1145/1614269.1614285.

[67] Julien Freudiger, Maxim Raya, Márk Félegyházi, Panos Papadimitratos, and Jean-Pierre Hubaux. "Mix-zones for Location Privacy in Vehicular Networks". In: *Win-ITS*. Vancouver, BC, Canada, 2007. URL: https:

//people.kth.se/~papadim/publications/fulltext/location-privacy-mix-zones-vanet.pdf.

[68] M. Khodaei and P. Papadimitratos. "Cooperative Location Privacy in Vehicular Networks: Why Simple Mix-zones are not Enough". In: *IEEE Internet Of Things Journal* (2021). URL: https://ieeexplore.ieee.org/document/9288855.

[69] Christian Vaas, Mohammad Khodaei, Panos Papadimitratos, and Ivan Martinovic. "Nowhere to hide? Mix-Zones for Private Pseudonym Change using Chaff Vehicles". In: *IEEE Vehicular Networking Conference (VNC)*. Taipei, Taiwan, 2018. URL: https://ieeexplore.ieee.org/abstract/document/8628449.

[70] Xiaodong Lin, Xiaoting Sun, Pin-Han Ho, and Xuemin Shen. "GSIS: A Secure and Privacy-preserving Protocol for Vehicular Communications". In: *IEEE Transactions on Vehicular Technology* (2007). URL: https://ieeexplore.ieee.org/abstract/document/4357367.

[71] Rongxing Lu, Xiaodong Lin, Haojin Zhu, Pin-Han Ho, and Xuemin Shen. "ECPP: Efficient Conditional Privacy Preservation Protocol for Secure Vehicular Communications". In: *IEEE Conference on Computer Communications (INFOCOM)*. Phoenix, AZ, USA, 2008. URL: https://ieeexplore.ieee.org/abstract/document/4509774.

[72] M. Khodaei and P. Papadimitratos. "The Key to Intelligent Transportation: Identity and Credential Management in Vehicular Communication Systems". In: *IEEE Vehicular Technology Magazine* 10.4 (2015), pp. 63–69. URL: https://ieeexplore.ieee.org/abstract/document/7317862.

[73] Dave Cooper. *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List Profile*. Tech. rep. RFC 5280, 2008. URL: https://tools.ietf.org/html/rfc5280.

[74] Maximiliano Contieri. *Singleton Pattern: The Root of All Evil*. 2020. URL: https://hackernoon.com/singleton-pattern-the-root-of-all-evil-e4r3up7.

[75] *Horizontal Pod Autoscaler*. 2019. URL: https://kubernetes.io/docs/tasks/run-application/horizontal-pod-autoscale/.

[76] *YAML API Reference*. 2018. URL: https://learn.getgrav.org/advanced/yaml.

[77] *Google Cloud HSM*. 2019. URL: https://cloud.google.com/hsm/.

[78] *FIPS 140-2 Level 3 Non-Proprietary Security Policy*. 2018. URL: https://csrc.nist.gov/csrc/media/projects/cryptographic-module-validation-program/documents/security-policies/140sp2850.pdf.

[79] *Redis Transactions*. 2021. URL: https://redis.io/topics/transactions.

[80] *Homomorphic Encryption Standard*. 2021. URL: https://homomorphicencryption.org/.

[81] *Bluemail app removed from Google play store without notice!* 2021. URL: https://www.androidheadlines.com/2020/07/bluemail-app-removed-from-play-store-without-notice-from-google.html.

[82] L. A. Martucci, A. Zuccato, B. Smeets, S. M. Habib, T. Johansson, and N. Shahmehri. "Privacy, Security and Trust in Cloud Computing: The Perspective of the Telecommunication Industry". In: *2012 9th International Conference on Ubiquitous Intelligence and Computing and 9th International Conference on Autonomic and Trusted Computing*. 2012, pp. 627–632. DOI: 10.1109/UIC-ATC.2012.166.

[83] *OpenStack by Open Infrastructure Foundation*. 2021. URL: https://www.openstack.org/.

[84] *Cloud Memorystore*. 2019. URL: https://cloud.google.com/memorystore/.

[85] Hsu-Chun Hsiao, Ahren Studer, Chen Chen, Adrian Perrig, Fan Bai, Bhargav Bellur, and Aravind Iyer. "Flooding-Resilient Broadcast Authentication for VANETs". In: *ACM Mobile Computing and Networking*. Las Vegas, Nevada, USA, 2011. URL: https://dl.acm.org/doi/abs/10.1145/2030613.2030635.

[86] *Cloud Armor*. 2021. URL: https://cloud.google.com/armor.

[87] Paul Heinlein. "FastCGI". In: *Linux journal* 1998.55es (1998), p. 1.

[88] *XML-RPC for C/C++*. Accessed March 1, 2021. 2021. URL: http://xmlrpc-c.sourceforge.net/.

[89] *Google Protocol Buffer*. Accessed March 1, 2021. 2021. URL: https://developers.google.com/protocol-buffers/.

[90] *Cloud SQL*. 2019. URL: https://cloud.google.com/sql.

[91] *Prometheus*. 2019. URL: https://prometheus.io/.

[92] *Grafana*. 2019. URL: https://grafana.com/.

[93] *Styx*. 2020. URL: https://github.com/go-pluto/styx.

[94] Sandesh Uppoor, Oscar Trullols-Cruces, Marco Fiore, and Jose M Barcelo-Ordinas. "Generation and Analysis of a Large-scale Urban Vehicular Mobility Dataset". In: *IEEE Transactions on Mobile Computing* 13.5 (2014), pp. 1061–1075. URL: https://ieeexplore.ieee.org/abstract/document/6468040.

[95] Lara Codeca, Raphaël Frank, and Thomas Engel. "Luxembourg SUMO Traffic (LuST) Scenario: 24 Hours of Mobility for Vehicular Networking Research". In: *IEEE Vehicular Networking Conference (VNC)*. Kyoto, Japan, 2015, pp. 1–8. URL: https://ieeexplore.ieee.org/abstract/document/7385539.

[96] John Harding, Gregory Powell, Rebecca Yoon, Joshua Fikentscher, Charlene Doyle, Dana Sade, Mike Lukuc, Jim Simons, and Jing Wang. *V2V Communications: Readiness of V2V Technology for Application*. Tech. rep. U.S. Department of Transportation - National Highway Traffic Safety Administration - DOT HS 812 014, 2014. URL: http://www.nhtsa.gov/staticfiles/rulemaking/pdf/V2V/Readiness-of-V2V-Technology-for-Application-812014.pdf.

[97] M. Abliz and T. Znati. "A Guided Tour Puzzle for Denial of Service Prevention". In: *IEEE ACSAC*. Honolulu, HI, 2009, pp. 279–288. URL: https://doi.org/10.1109/ACSAC.2009.33.

[98] Tuomas Aura, Pekka Nikander, and Jussipekka Leiwo. "DoS-Resistant Authentication with Client Puzzles". In: *Proceedings of Security Protocols Workshop*. New York, USA, 2001. URL: https://doi.org/10.1007/3-540-44810-1_22.

[99] *SOPS: Secrets OPerationS*. 2021. URL: https://github.com/mozilla/sops.