Acronyms

CA	Certificate authority
CAM	Cooperative Awareness Message
CRL	Certificate revocation list
DENM	Decentralized Environmental Notification Message
FCD	Floating Car Data
GLOSA	Green Light Optimal Speed Advisory
HSM	Hardware security module
ICA	Intersection Collision Avoidance
IoT	Internet of Things
ITS	Intelligent Transport System
IVC	Inter-vehicular communication
LTCA	Long-Term Certificate Authority
OBU	On-board unit
OSR	Order for self-revocation
PCA	Pseudonym Certificate Authority
PUCA	Pseudonyms with User-Controlled Anonymity (pronounced *pooka*, Irish for spirit/ghost)
RA	Revocation Authority
REWIRE	REvocation Without REsolution
RSU	Road-side unit
TSN	Token serial number

D. Förster, *Verifiable Privacy Protection for Vehicular Communication Systems*, DOI 10.1007/978-3-658-18550-3

V2V Vehicle-to-vehicle (communication)

V2X Vehicle-to-X (communication)

VANET Vehicular Ad Hoc Network

Publications

[1] D. Förster, F. Kargl, and H. Löhr, "PUCA: A pseudonym scheme with user-controlled anonymity for vehicular ad-hoc networks (VANET)", in *Vehicular Networking Conference (VNC)*, IEEE, Dec. 2014, pp. 25–32.

[2] D. Förster, "Discussing different levels of privacy protection in vehicular ad-hoc networks", in *Proceeding of the 3rd GI/ITG KuVS Fachgespräch Inter-Vehicle Communication*, ser. Ulmer Informatik-Berichte, Ulm University, vol. 2015-03, Mar. 2015, pp. 29–30.

[3] D. Förster, F. Kargl, and H. Löhr, "A framework for evaluating pseudonym strategies in vehicular ad-hoc networks", in *Proceedings of the 8th ACM Conference on Security & Privacy in Wireless and Mobile Networks*, ACM, Jun. 2015, 19:1–19:6.

[4] D. Förster, H. Löhr, J. Zibuschka, and F. Kargl, "REWIRE – Revocation without resolution: A privacy-friendly revocation mechanism for vehicular ad-hoc networks", in *Trust and Trustworthy Computing*, ser. LNCS, vol. 9229, Springer, Aug. 2015, pp. 193–208.

[5] D. Förster, F. Kargl, and H. Löhr, "Datenschutzfreundliche Authentifizierung in der Car-to-X Kommunikation", in *31. VDI/VW Gemeinschaftstagung Automotive Security*, ser. VDI-Berichte, vol. 2263, VDI Wissensforum GmbH, Oct. 2015, pp. 129–134, (Best Paper Award).

[6] D. Förster, F. Kargl, and H. Löhr, "PUCA: A pseudonym scheme with strong privacy guarantees for vehicular ad-hoc networks", *Ad Hoc Networks*, vol. 37, Part 1, pp. 122–132, Feb. 2016, Special Issue on Advances in Vehicular Networks.

[7] D. Förster, H. Löhr, and F. Kargl, "Decentralized enforcement of k-anonymity for location privacy using secret sharing", in *Vehicular Networking Conference (VNC)*, IEEE, Dec. 2015, pp. 279–286.

[8] D. Förster, H. Löhr, A. Grätz, J. Petit, and F. Kargl, "An evaluation of pseudonym changes for vehicular networks in large-scale, realistic traffic scenarios", *IEEE Transactions on Intelligent Transportation Systems*, 2016, (submitted).

D. Förster, *Verifiable Privacy Protection for Vehicular Communication Systems*, DOI 10.1007/978-3-658-18550-3

References

[9] T. Acar, S. Chow, and L. Nguyen, "Accumulators and U-Prove revocation", in *Financial Cryptography and Data Security*, ser. LNCS, vol. 7859, Springer, 2013, pp. 189–196.

[10] D. Achenbach, D. Förster, C. Henrich, D. Kraschewski, and J. Müller-Quade, "Social key exchange network – from ad-hoc key exchanges to a dense key network", in *Tagungsband der INFORMATIK 2011, Lecture Notes in Informatics*, vol. P192, Oct. 2011.

[11] R. Anderson, *Security engineering*. John Wiley & Sons, 2008.

[12] D. Angermeier, A. Kiening, and F. Stumpf, "PAL – privacy augmented LTE: A privacy-preserving scheme for vehicular LTE communication", in *Proceeding of the tenth ACM international workshop on Vehicular inter-networking, systems, and applications*, ACM, 2013, pp. 1–10.

[13] H. Aniss, "Overview of an ITS Project: SCOOP@F", in *International Workshop on Communication Technologies for Vehicles*, ser. LNCS, Springer, vol. 9669, 2016, pp. 131–135.

[14] F. Armknecht, A. Festag, D. Westhoff, and K. Zeng, "Cross-layer privacy enhancement and non-repudiation in vehicular communication", in *ITG-GI Conference on Communication in Distributed Systems (KiVS)*, VDE, 2007, pp. 1–12.

[15] D. Banisar and S. G. Davies, "Global trends in privacy protection: An international survey of privacy, data protection, and surveillance laws and developments", *John Marshall Journal of Computer & Information Law*, vol. 18, no. 1, 1999.

[16] BBC, "The interview: A guide to the cyber attack on hollywood", Dec. 2014. [Online]. Available: `http://www.bbc.com/news/entertainment-arts-30512032` (Accessed: 08/31/2016).

[17] J. Benaloh and M. De Mare, "One-way accumulators: A decentralized alternative to digital signatures", in *Advances in Cryptology – EUROCRYPT '93*, ser. LNCS, Springer, vol. 765, 1994, pp. 274–285.

[18] S. Bera and K. Rao, "Estimation of origin-destination matrix from traffic counts: The state of the art", *European Transport / Trasporti Europei*, no. 49, pp. 2–23, 2011.

D. Förster, *Verifiable Privacy Protection for Vehicular Communication Systems*, DOI 10.1007/978-3-658-18550-3

[19] A. R. Beresford and F. Stajano, "Location privacy in pervasive computing", *IEEE Pervasive computing*, vol. 2, no. 1, pp. 46–55, 2003.

[20] A. R. Beresford and F. Stajano, "Mix zones: User privacy in location-aware services", in *Proceedings of the Second IEEE Annual Conference on Pervasive Computing and Communications Workshops*, IEEE, 2004, pp. 127–131.

[21] A. R. Beresford, "Location privacy in ubiquitous computing", Dissertation, University of Cambridge, Jan. 2005.

[22] D. Bezzina and J. Sayer, "Safety pilot model deployment: Test conductor team report", U.S. Department of Transportation, National Highway Traffic Safety Administration, Tech. Rep. DOT HS 812 171, Jun. 2015.

[23] N. Bißmeyer, "Misbehavior detection and attacker identification in vehicular ad-hoc networks", Dissertation, Technische Universität Darmstadt, Dec. 2014.

[24] N. Bißmeyer, H. Stübing, E. Schoch, S. Götz, J. P. Stotz, and B. Lonc, "A generic public key infrastructure for securing car-to-x communication", in *18th ITS World Congress*, Orlando, USA, 2011.

[25] A. Boualouache, S.-M. Senouci, and S. Moussaoui, "VLPZ: The vehicular location privacy zone", *Procedia Computer Science*, vol. 83, pp. 369–376, 2016, The 7th International Conference on Ambient Systems, Networks and Technologies (ANT).

[26] S. Boztas, "Your car spying on you: Warnings over how much personal information it may hold", *The Independent*, Dec. 2015.

[27] S. A. Brands, *Rethinking public key infrastructures and digital certificates: Building in privacy*. MIT Press, 2000.

[28] S. A. Brands, L. Demuynck, and B. De Decker, "A practical system for globally revoking the unlinkable pseudonyms of unknown users", in *Information Security and Privacy*, ser. LNCS, vol. 4586, Springer, 2007, pp. 400–415.

[29] E. F. Brickell, J. Camenisch, and L. Chen, "Direct anonymous attestation", in *Proceedings of the 11th ACM Conference on Computer and Communications Security*, Oct. 2004, pp. 132–145.

[30] V. Brik, S. Banerjee, M. Gruteser, and S. Oh, "Wireless device identification with radiometric signatures", in *Proceedings of the 14th ACM International Conference on Mobile Computing and Networking*, ACM, 2008, pp. 116–127.

[31] O. Bubeck, J. Gramm, M. Ihle, J. Shokrollahi, R. Szerwinski, and M. Emele, "A hardware security module for engine control units", in *Proceedings of the 10th ESCAR Conference*, 2011.

[32] T. Buburuzan, *V2X roadmaps beyond day-1*, Sep. 2015. [Online]. Available: `https://amsterdamgroup.mett.nl/Downloads/downloads_getfilem.aspx?id=506545` (Accessed: 08/31/2016).

[33] C. Büttner and S. A. Huss, "Path hiding for privacy enhancement in vehicular ad-hoc networks", in *82nd Vehicular Technology Conference (VTC Fall)*, IEEE, 2015, pp. 1–5.

[34] L. Buttyán, T. Holczer, and I. Vajda, "On the effectiveness of changing pseudonyms to provide location privacy in VANETs", in *Security and Privacy in Ad-hoc and Sensor Networks*, ser. LNCS, vol. 4572, Springer, 2007, pp. 129–141.

[35] L. Buttyán, T. Holczer, A. Weimerskirch, and W. Whyte, "SLOW: A practical pseudonym changing scheme for location privacy in VANETs", in *Vehicular Networking Conference (VNC)*, IEEE, Oct. 2009, pp. 1–8.

[36] N. Caceres, J. Wideberg, and F. Benitez, "Deriving origin destination data from a mobile phone network", *Intelligent Transport Systems, IET*, vol. 1, no. 1, pp. 15–26, Mar. 2007.

[37] G. Calandriello, P. Papadimitratos, J.-P. Hubaux, and A. Lioy, "Efficient and robust pseudonymous authentication in VANET", in *Proceedings of the fourth ACM international workshop on Vehicular ad hoc networks*, ACM, 2007, pp. 19–28.

[38] J. Camenisch, S. Hohenberger, M. Kohlweiss, A. Lysyanskaya, and M. Meyerovich, "How to win the clonewars: Efficient periodic n-times anonymous authentication", in *Proceedings of the 13th ACM conference on Computer and communications security*, ACM, 2006, pp. 201–210.

[39] J. Camenisch, M. Kohlweiss, and C. Soriente, "An accumulator based on bilinear maps and efficient revocation for anonymous credentials", in *Public Key Cryptography – PKC*, ser. LNCS, vol. 5443, Springer, 2009, pp. 481–500.

[40] J. Camenisch and A. Lysyanskaya, "A signature scheme with efficient protocols", in *Security in communication networks*, ser. LNCS, vol. 2576, Springer, 2003, pp. 268–289.

[41] J. Camenisch and A. Lysyanskaya, "An efficient system for non-transferable anonymous credentials with optional anonymity revocation", in *Advances in Cryptology – EUROCRYPT 2001*, ser. LNCS, vol. 2045, Springer, 2001, pp. 93–118.

[42] J. Camenisch and A. Lysyanskaya, "Dynamic accumulators and application to efficient revocation of anonymous credentials", in *Advances in Cryptology – CRYPTO 2002*, ser. LNCS, vol. 2442, Springer, 2002, pp. 61–76.

[43] J. Camenisch and A. Lysyanskaya, "Signature schemes and anonymous credentials from bilinear maps", in *Advances in Cryptology – CRYPTO 2004*, ser. LNCS, Springer, vol. 3152, 2004, pp. 56–72.

[44] CAR 2 CAR Communication Consortium, *European vehicle manufacturers work towards bringing vehicle-to-x communication onto european roads*, Oct. 2015. [Online]. Available: `https://www.car-2-car.org/` (Accessed: 08/31/2016).

[45] Centre for Economics and Business Research (CEBR), "The future economic and environmental costs of gridlock in 2030", Tech. Rep., Jul. 2014.

[46] D. Chaum, "Blind signatures for untraceable payments", in *Advances in Cryptology – CRYPTO '82*, Springer, 1983, pp. 199–203.

[47] D. Chaum, "Security without identification: Transaction systems to make big brother obsolete", *Communications of the ACM*, vol. 28, no. 10, pp. 1030–1044, 1985.

[48] D. Christin, J. Guillemet, A. Reinhardt, M. Hollick, and S. S. Kanhere, "Privacy-preserving collaborative path hiding for participatory sensing applications", in *Eighth International Conference on Mobile Ad-Hoc and Sensor Systems*, IEEE, 2011, pp. 341–350.

[49] L. Codeca, R. Frank, and T. Engel, "Luxembourg SUMO traffic (LuST) scenario: 24 hours of mobility for vehicular networking research", in *Vehicular Networking Conference (VNC)*, IEEE, Dec. 2015, pp. 1–8.

[50] CONVERGE, *Deliverable D4.3 "Architecture of the Car2X Systems Network", Section 4.1.2*, Jan. 2015.

[51] CONVERGE project partners, *CONVERGE – COmmunication Network VEhicle Road Global Extension*, 2012-2015. [Online]. Available: `http://converge-online.de/` (Accessed: 08/31/2016).

[52] L. Delgrossi and T. Zhang, *Vehicle safety communications: Protocols, security, and privacy*. John Wiley & Sons, 2012.

[53] C. Diaz, S. Seys, J. Claessens, and B. Preneel, "Towards measuring anonymity", in *Privacy Enhancing Technologies*, ser. LNCS, Springer, vol. 2482, 2003, pp. 54–68.

[54] S. Dietzel, L. Dölle, J. Freytag, C. Jouvray, F. Kargl, M. Kost, Z. Ma, F. Schaub, and B. Wiedersheim, *PRECIOSA – PRivacy Enabled Capability In Co-Operative Systems and Safety Applications, Deliverable 16*, 2010.

[55] R. Dingledine, N. Mathewson, and P. Syverson, "Tor: The second-generation onion router", in *Proceedings of the 13th USENIX Security Symposium*, Aug. 2004.

[56] J. R. Douceur, "The sybil attack", in *Peer-to-Peer Systems*, ser. LNCS, Springer, vol. 2429, 2002, pp. 251–260.

[57] F. Dressler, H. Hartenstein, O. Altintas, and O. Tonguz, "Inter-vehicle communication: Quo vadis", *Communications Magazine, IEEE*, vol. 52, no. 6, pp. 170–177, 2014.

[58] M. Duckham and L. Kulik, "A formal model of obfuscation and negotiation for location privacy", in *Pervasive computing*, ser. LNCS, vol. 3468, Springer, 2005, pp. 152–170.

[59] M. Duckham and L. Kulik, "Location privacy and location-aware computing", *Dynamic & mobile GIS: Investigating change in space and time*, vol. 3, pp. 35–51, 2006.

[60] P. Ducklin, "Anatomy of a 'goto fail' – Apple's SSL bug explained, plus an unofficial patch for OS X", Feb. 2014. [Online]. Available: `https://nakedsecurity.sophos.com/2014/02/24/anatomy-of-a-goto-fail-apples-ssl-bug-explained-plus-an-unofficial-patch/` (Accessed: 08/31/2016).

[61] C. Dwork, "Differential privacy", in *Automata, languages and programming*, ser. LNCS, vol. 4052, Springer, 2006, pp. 1–12.

[62] EC DG INFSO and USDOT RITA JPO, *Cooperative systems standards harmonization action plan (HAP)*, Jun. 2011.

[63] D. Eckhoff and C. Sommer, "Driving for big data? Privacy concerns in vehicular networking", *IEEE Security & Privacy*, vol. 1, no. 12, pp. 77–79, 2014.

[64] D. Eckhoff, C. Sommer, T. Gansen, R. German, and F. Dressler, "Strong and affordable location privacy in VANETs: Identity diffusion using time-slots and swapping", in *Vehicular Networking Conference (VNC)*, IEEE, 2010, pp. 174–181.

[65] J. Edmonds, "Paths, trees, and flowers", *Canadian Journal of mathematics*, vol. 17, no. 3, pp. 449–467, 1965.

[66] "Edward Snowden on why we must protect our privacy", *Literary Hub*, Apr. 2016. [Online]. Available: http://lithub.com/edward-snowden-on-why-we-must-protect-our-privacy/ (Accessed: 08/31/2016).

[67] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms", in *Advances in Cryptology – CRYPTO '84*, ser. LNCS, Springer, vol. 196, 1984, pp. 10–18.

[68] European Court of Human Rights, "European convention on human rights", 1950.

[69] European Telecommunications Standards Institute, "Intelligent transport systems (ITS); cooperative its (C-ITS); release 1", ETSI, TR 101 607 V1.1.1, May 2013.

[70] European Telecommunications Standards Institute, "Intelligent transport systems (ITS); european profile standard for the physical and medium access control layer of intelligent transport systems operating in the 5 ghz frequency band", ETSI, ES 202 663 V1.1.0, Nov. 2009.

[71] European Telecommunications Standards Institute, "Intelligent transport systems (ITS); security; trust and privacy management", ETSI, TS 102 941 V1.1.1, Jun. 2012.

[72] Federal Highway Research Institute (Germany), *Automated traffic counts on highways and national roads (Automatische Zählstellen auf Autobahnen und Bundesstraßen)*, 2013. [Online]. Available: http://www.bast.de/DE/Verkehrstechnik/Fachthemen/v2-verkehrszaehlung/Stundenwerte.html (Accessed: 08/31/2016).

[73] Federal Highway Research Institute (Germany), *Economic costs of accidents in Germany (Volkswirtschaftliche Kosten von Straßenverkehrsunfällen in Deutschland)*, Apr. 2015. [Online]. Available: http://www.bast.de/DE/Statistik/Unfaelle-Downloads/volkswirtschaftliche_kosten.pdf (Accessed: 08/31/2016).

[74] Federal Highway Research Institute (Germany), *International traffic and accident data*, Oct. 2015. [Online]. Available: http://www.bast.de/EN/Publications/Media/Unfallkarten-international-englisch.pdf (Accessed: 08/31/2016).

[75] Federal Highway Research Institute (Germany), *Traffic and accident data – summary statistics – Germany*, Sep. 2015. [Online]. Available: `http://www.bast.de/EN/Publications/Media/Unfallkarten-national-englisch.pdf` (Accessed: 08/31/2016).

[76] Fédération Internationale de l'Automobile, *What europeans think about connected cars*, Jan. 2016.

[77] A. Fiat and A. Shamir, "How to prove yourself: Practical solutions to identification and signature problems", in *Advances in Cryptology – CRYPTO '86*, ser. LNCS, Springer, vol. 263, 1986, pp. 186–194.

[78] J. Freudiger, M. Raya, M. Félegyházi, P. Papadimitratos, *et al.*, "Mix-zones for location privacy in vehicular networks", in *ACM Workshop on Wireless Networking for Intelligent Transportation Systems (ACM WiN-ITS)*, 2007.

[79] J. Freudiger, M. Raya, and J.-P. Hubaux, "Self-organized anonymous authentication in mobile ad hoc networks", in *International Conference on Security and Privacy in Communication Systems*, Springer, 2009, pp. 350–372.

[80] J. Freudiger, R. Shokri, and J.-P. Hubaux, "On the optimal placement of mix zones", in *International Symposium on Privacy Enhancing Technologies Symposium*, Springer, 2009, pp. 216–234.

[81] C. Gañán, J. L. Muñoz, O. Esparza, J. Mata-Díaz, and J. Alins, "PPREM: Privacy preserving revocation mechanism for vehicular ad hoc networks", *Computer Standards & Interfaces*, vol. 36, no. 3, pp. 513–523, Mar. 2014.

[82] General Motors, *Cadillac to introduce advanced "Intelligent and Connected" vehicle technologies on select 2017 models*, Sep. 2014. [Online]. Available: `http://media.gm.com/media/us/en/gm/news.detail.html/content/Pages/news/us/en/2014/Sep/0907-its-overview.html` (Accessed: 08/31/2016).

[83] M. Gerlach and F. Güttler, "Privacy in VANETs using changing pseudonyms - ideal and real", in *65th Vehicular Technology Conference (VTC Spring)*, IEEE, 2007, pp. 2521–2525.

[84] S. Goldwasser, S. Micali, and C. Rackoff, "The knowledge complexity of interactive proof systems", *SIAM Journal on computing*, vol. 18, no. 1, pp. 186–208, 1989.

[85] P. Golle and K. Partridge, "On the anonymity of home/work location pairs", in *Pervasive computing*, ser. LNCS, vol. 5538, Springer, 2009, pp. 390–397.

[86] A. Greenberg, "Apple's 'Differential Privacy' is about collecting your data–but not *your* data", *Wired*, Jun. 2016.

[87] A. Greenberg, "Cars that talk to each other are much easier to spy on", *Wired*, Oct. 2015.

[88] G. Greenwald, *No place to hide: Edward snowden, the NSA, and the US surveillance state*. Macmillan, May 2014.

[89] G. Greenwald, E. MacAskill, and L. Poitras, "Edward Snowden: The whistleblower behind the NSA surveillance revelations", *The Guardian*, Jun. 2013.

[90] A. Groll, J. Holle, C. Ruland, M. Wolf, T. Wollinger, and F. Zweers, "Oversee – A secure and open communication and runtime platform for innovative automotive applications", in *Proceedings of the 7th Embedded Security in Cars Conference (ESCAR)*, 2009.

[91] A. Groll, J. Holle, M. Wolf, and T. Wollinger, "Next generation of automotive security: Secure hardware and secure open platforms", in *17th ITS World Congress*, Busan, South Korea, 2010.

[92] M. Gruteser and D. Grunwald, "Anonymous usage of location-based services through spatial and temporal cloaking", in *Proceedings of the 1st international conference on Mobile systems, applications and services*, ACM, 2003, pp. 31–42.

[93] M. Gruteser and B. Hoh, "On the anonymity of periodic location samples", in *Security in Pervasive Computing*, ser. LNCS, vol. 3450, Springer, 2005, pp. 179–192.

[94] J. Guo, J. P. Baugh, and S. Wang, "A group signature based secure and privacy-preserving vehicular communication framework", in *Mobile Networking for Vehicular Environments*, IEEE, 2007, pp. 103–108.

[95] L. Hanzlik, K. Kluczniak, and M. Kutyłowski, "Attack on U-Prove revocation scheme from FC'13 - passing verification by revoked users", in *Financial Cryptography and Data Security*, ser. LNCS, vol. 8437, Springer, 2014, pp. 283–290.

[96] F. Harary, *Graph theory*. Addison-Wesley, 1969.

[97] M. Harrer, C. Lotz-Keens, H. Molin, F. op de Beek, G. Riegelhuth, K. Sauer, and F. Verweij, "Europe's C-ITS corridor paves the way for C2X", *ITS International*, pp. 29–30, May 2016.

[98] H. Hartenstein and K. P. Laberteaux, "A tutorial survey on vehicular ad hoc networks", *IEEE Communications Magazine*, vol. 46, no. 6, pp. 164–171, 2008.

[99] O. Henniger, A. Ruddle, H. Seudié, B. Weyl, M. Wolf, and T. Wollinger, "Securing vehicular on-board it systems: The EVITA project", in *VDI/VW Automotive Security Conference*, 2009.

[100] Herstellerinitiative Software (HIS), *SHE secure hardware extension version 1.1.* 2009.

[101] B. Hoh and M. Gruteser, "Protecting location privacy through path confusion", in *First International Conference on Security and Privacy for Emerging Areas in Communications Networks, SecureComm*, IEEE, 2005, pp. 194–205.

[102] B. Hoh, M. Gruteser, R. Herring, J. Ban, D. Work, J.-C. Herrera, A. M. Bayen, M. Annavaram, and Q. Jacobson, "Virtual trip lines for distributed privacy-preserving traffic monitoring", in *Proceedings of the 6th international conference on Mobile systems, applications, and services*, ACM, 2008, pp. 15–28.

[103] B. Hoh, M. Gruteser, H. Xiong, and A. Alrabady, "Enhancing security and privacy in traffic-monitoring systems", *Pervasive Computing, IEEE*, vol. 5, no. 4, pp. 38–46, 2006.

[104] L. Huang, K. Matsuura, H. Yamane, and K. Sezaki, "Enhancing wireless location privacy using silent period", in *Wireless Communications and Networking Conference*, IEEE, vol. 2, 2005, pp. 1187–1192.

[105] L. Huang, "Secure and privacy-preserving broadcast authentication for IVC", Master's thesis, University of Twente, Jul. 2012.

[106] IEEE, "Guide for wireless access in vehicular environments (WAVE) - architecture", IEEE, Std 1609.0, 2013.

[107] IEEE, "Standard for information technology–telecommunications and information exchange between systems–social and metropolitan area networks–specific requirements part 11: Wireless LAN medium access control (MAC) and physical layer (PHY) specifications", IEEE, Std 802.11, 2012.

[108] IEEE, "Standard for wireless access in vehicular environments – security services for applications and management messages", IEEE, Std 1609.2, 2013.

[109] Information is Beautiful, *World's biggest data breaches – selected losses greater than 30,000 records*, May 2016. [Online]. Available: `http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/` (Accessed: 08/31/2016).

[110] T. Jeske, "Floating car data from smartphones: What google and waze know about you and how hackers can control traffic", *Black Hat Europe*, 2013.

[111] F. Kargl, P. Papadimitratos, L. Buttyán, M. Muter, E. Schoch, B. Wiedersheim, T.-V. Thong, G. Calandriello, A. Held, and A. Kung, "Secure vehicular communication systems: Implementation, performance, and research challenges", *Communications Magazine, IEEE*, vol. 46, no. 11, pp. 110–118, 2008.

[112] M. Karppinen, *Data is not an asset, it's a liability*, Sep. 2015. [Online]. Available: `https://www.richie.fi/blog/data-is-a-liability.html` (Accessed: 08/31/2016).

[113] B. Könings and F. Schaub, "Territorial privacy in ubiquitous computing", in *Eighth International Conference on Wireless On-Demand Network Systems and Services (WONS)*, IEEE, 2011, pp. 104–108.

[114] D. Krajzewicz, J. Erdmann, M. Behrisch, and L. Bieker, "Recent development and applications of SUMO - Simulation of Urban MObility", *International Journal On Advances in Systems and Measurements*, vol. 5, no. 3&4, pp. 128–138, Dec. 2012.

[115] S. Krauß, "Microscopic modeling of traffic flow: Investigation of collision free vehicle", Dissertation, Universität zu Köln, 1998.

[116] I. Krstic, "Behind the scenes of iOS security", in *Black Hat*, Aug. 2016.

[117] J. Krumm, "A survey of computational location privacy", *Personal and Ubiquitous Computing*, vol. 13, no. 6, pp. 391–399, 2009.

[118] J. Krumm, "Inference attacks on location tracks", in *Pervasive Computing*, ser. LNCS, vol. 4480, Springer, 2007, pp. 127–143.

[119] H. W. Kuhn, "The hungarian method for the assignment problem", *Naval research logistics quarterly*, vol. 2, no. 1-2, pp. 83–97, 1955.

[120] K. P. Laberteaux, J. J. Haas, and Y.-C. Hu, "Security certificate revocation list distribution for VANET", in *Proceedings of the Fifth ACM International Workshop on Vehicular Inter-Networking (VANET)*, ACM, 2008, pp. 88–89.

[121] J. Lapon, M. Kohlweiss, B. De Decker, and V. Naessens, "Performance analysis of accumulator-based revocation mechanisms", in *Security and Privacy–Silver Linings in the Cloud*, ser. IFIP Advances in Information and Communication Technology, vol. 330, Springer, 2010, pp. 289–301.

[122] S. Lefèvre, J. Petit, R. Bajcsy, C. Laugier, and F. Kargl, "Impact of V2X privacy strategies on intersection collision avoidance systems", in *Vehicular Networking Conference (VNC)*, IEEE, 2013, pp. 71–78.

[123] T. Leinmüller, L. Buttyan, J.-P. Hubaux, F. Kargl, R. Kroh, P. Papadimitratos, M. Raya, and E. Schoch, "SEVECOM – Secure vehicle communication", in *IST Mobile and Wireless Communication Summit*, 2006.

[124] F. Li and Y. Wang, "Routing in vehicular ad hoc networks: A survey", *Vehicular Technology Magazine, IEEE*, vol. 2, no. 2, pp. 12–22, Jun. 2007.

[125] B. Lian, G. Chen, M. Ma, and J. Li, "Periodic k-times anonymous authentication with efficient revocation of violator's credential", *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 3, pp. 543–557, Mar. 2015.

[126] J. Liao and J. Li, "Effectively changing pseudonyms for privacy protection in VANETs", in *10th International Symposium on Pervasive Systems, Algorithms, and Networks (ISPAN)*, IEEE, 2009, pp. 648–652.

[127] X. Lin, X. Sun, P.-H. Ho, and X. Shen, "Gsis: A secure and privacy-preserving protocol for vehicular communications", *IEEE Transactions on Vehicular Technology*, vol. 56, no. 6, pp. 3442–3456, Nov. 2007.

[128] M. Lukuc, "V2V interoperability project", in *U.S. DOT ITS Connected Vehicle Workshop*, 2012.

[129] Z. Ma, "Location privacy in vehicular communication systems: A measurement approach", Dissertation, Ulm University, Jan. 2011.

[130] Z. Ma, F. Kargl, and M. Weber, "Measuring long-term location privacy in vehicular communication systems", *Computer Communications*, vol. 33, no. 12, pp. 1414–1427, 2010.

[131] S. Mansfield-Devine, "The Ashley Madison affair", *Network Security*, vol. 2015, no. 9, pp. 8–16, 2015.

[132] L. A. Martucci, M. Kohlweiss, C. Andersson, and A. Panchenko, "Self-certified sybil-free pseudonyms", in *Proceedings of the first ACM conference on Wireless network security*, ACM, 2008, pp. 154–159.

[133] J. Munkres, "Algorithms for the assignment and transportation problems", *Journal of the society for industrial and applied mathematics*, vol. 5, no. 1, pp. 32–38, 1957.

[134] S. Nakamoto, *Bitcoin: A peer-to-peer electronic cash system*, 2008.

[135] C. Nanthawichit, T. Nakatsuji, and H. Suzuki, "Application of probe-vehicle data for real-time traffic-state estimation and short-term travel-time prediction on a freeway", *Transportation Research Record: Journal of the Transportation Research Board*, no. 1855, pp. 49–59, 2003.

[136] L. Nguyen and C. Paquin, "U-Prove designated-verifier accumulator revocation extension", Microsoft Corporation, Tech. Rep. MSR-TR-2013-87, Sep. 2013.

[137] Oxford University Press, *Oxford dictionary*. Jun. 2016. [Online]. Available: `http://www.oxforddictionaries.com/definition/english/trust` (Accessed: 08/31/2016).

[138] M. Palmer, "Data is the new oil", *ANA Marketing Maestros blog*, Nov. 2006. [Online]. Available: `http://ana.blogs.com/maestros/2006/11/data_is_the_new.html` (Accessed: 08/31/2016).

[139] Y. Pan and J. Li, "Cooperative pseudonym change scheme based on the number of neighbors in VANETs", *Journal of Network and Computer Applications*, vol. 36, no. 6, pp. 1599–1609, 2013.

[140] P. Papadimitratos, L. Buttyán, T. Holczer, E. Schoch, J. Freudiger, M. Raya, Z. Ma, F. Kargl, A. Kung, and J.-P. Hubaux, "Secure vehicular communication systems: Design and architecture", *Communications Magazine, IEEE*, vol. 46, no. 11, pp. 100–109, 2008.

[141] P. Papadimitratos, L. Buttyán, J.-P. Hubaux, F. Kargl, A. Kung, and M. Raya, "Architecture for secure and private vehicular communications", in *7th International Conference on ITS Telecommunications (ITST)*, IEEE, 2007, pp. 1–6.

[142] "Report on the secure vehicular communications: Results and challenges ahead workshop", *ACM SIGMOBILE Mobile Computing and Communications Review*, vol. 12, no. 2, P. Papadimitratos and J.-P. Hubaux, Eds., pp. 53–64, 2008.

[143] P. Papadimitratos, G. Mezzour, and J.-P. Hubaux, "Certificate revocation list distribution in vehicular communication systems", in *Proceedings of the Fifth ACM International Workshop on Vehicular Inter-Networking (VANET)*, ACM, 2008, pp. 86–87.

[144] B. Parno and A. Perrig, "Challenges in securing vehicular networks", in *Workshop on hot topics in networks (HotNets-IV)*, 2005, pp. 1–6.

[145] J. Pei, J. Xu, Z. Wang, W. Wang, and K. Wang, "Maintaining k-anonymity against incremental updates", in *19th International Conference on Scientific and Statistical Database Management*, IEEE, 2007.

[146] J. Petit, F. Schaub, M. Feiri, and F. Kargl, "Pseudonym schemes in vehicular networks: A survey", *Communications Surveys Tutorials, IEEE*, vol. 17, no. 1, pp. 228–255, 2015.

[147] J. Petit, D. Broekhuis, M. Feiri, and F. Kargl, "Connected vehicles: Surveillance threat and mitigation", in *Black Hat Europe*, Nov. 2015.

[148] J. M. Porup, "How Hacking Team got hacked", *Ars Technica UK*, Apr. 2016.

[149] PRESERVE project partners, *PRESERVE – Preparing Secure Vehicle-to-X Communication Systems*, 2011-2015. [Online]. Available: `https://www.preserve-project.eu/` (Accessed: 08/31/2016).

[150] sim$^{\text{TD}}$ project partners, *Deliverable D5.5 – Final report*, Jun. 2013.

[151] sim$^{\text{TD}}$ project partners, *Sim^{TD} – Safe and Intelligent Mobility Test Field Germany*, 2009-2013. [Online]. Available: `http://www.simtd.de/` (Accessed: 08/31/2016).

[152] J.-J. Quisquater, M. Quisquater, M. Quisquater, M. Quisquater, L. Guillou, M. A. Guillou, G. Guillou, A. Guillou, G. Guillou, and S. Guillou, "How to explain zero-knowledge protocols to your children", in *Advances in Cryptology – CRYPTO '89*, ser. LNCS, Springer, vol. 435, 1989, pp. 628–631.

[153] S. Rass, S. Fuchs, M. Schaffer, and K. Kyamakya, "How to protect privacy in floating car data systems", in *Proceedings of the fifth ACM international workshop on Vehicular Inter-Networking (VANET)*, ACM, 2008, pp. 17–22.

[154] M. Raya and J.-P. Hubaux, "Securing vehicular ad hoc networks", *Journal of Computer Security*, vol. 15, no. 1, pp. 39–68, 2007.

[155] M. Raya, P. Papadimitratos, I. Aad, D. Jungels, and J.-P. Hubaux, "Eviction of misbehaving and faulty nodes in vehicular networks", *Selected Areas in Communications, IEEE Journal on*, vol. 25, no. 8, pp. 1557–1568, 2007.

[156] Road Traffic Center Baden-Württemberg, *Traffic monitoring 2013 on highways in Baden-Württemberg (Verkehrsmonitoring 2013: Fortschreibung für Bundesautobahnen in Baden-Württemberg)*, 2013. [Online]. Available: `http://www.svz-bw.de/info_vm.html` (Accessed: 08/31/2016).

[157] T. van Roermund, "Security and privacy standards are critical to the success of connected cars", *TechCrunch*, Jan. 2016.

[158] P. Rogaway, *The moral character of cryptographic work*, Dec. 2015.

[159] J. Rosevear, "Will your next new car report you for speeding?", *The Motley Fool*, Dec. 2014.

[160] I. Rouf, R. Miller, H. Mustafa, T. Taylor, S. Oh, W. Xu, M. Gruteser, W. Trappe, and I. Seskar, "Security and privacy vulnerabilities of in-car wireless networks: A tire pressure monitoring system case study", in *Proceedings of the 19th USENIX Security Symposium*, 2010, pp. 11–13.

[161] G. Sabidussi, "The centrality index of a graph", *Psychometrika*, vol. 31, no. 4, pp. 581–603, 1966.

[162] SAE International, "Dedicated short range communications (DSRC) message set dictionary", SAE, J 2735, 2016.

[163] SAE International, "On-board system requirements for V2V safety communications", SAE, J 2945/1, 2016.

[164] K. Sampigethaya, L. Huang, M. Li, R. Poovendran, K. Matsuura, and K. Sezaki, "CARAVAN: Providing location privacy for VANET", in *Embedded Security in Cars (ESCAR)*, 2005.

[165] K. Sampigethaya, M. Li, L. Huang, and R. Poovendran, "AMOEBA: Robust location privacy scheme for VANET", *IEEE Journal on Selected Areas in communications*, vol. 25, no. 8, pp. 1569–1589, Oct. 2007.

[166] J. Schaad and R. Housley, *Advanced Encryption Standard (AES) Key Wrap Algorithm*, RFC 3394, Internet Engineering Task Force, Sep. 2002.

[167] F. M. Schaub, "Dynamic privacy adaptation in ubiquitous computing", Dissertation, Ulm University, Apr. 2014.

[168] F. Schaub, F. Kargl, Z. Ma, and M. Weber, "V-tokens for conditional pseudonymity in VANETs", in *Wireless Communications and Networking Conference (WCNC)*, IEEE, 2010, pp. 1–6.

[169] F. Schaub, Z. Ma, and F. Kargl, "Privacy requirements in vehicular communication systems", in *International Conference on Computational Science and Engineering*, IEEE, 2009, pp. 139–145.

[170] E. Schoch, F. Kargl, T. Leinmüller, S. Schlott, and P. Papadimitratos, "Impact of pseudonym changes on geographic routing in VANETs", in *Security and Privacy in Ad-hoc and Sensor Networks*, ser. LNCS, Springer, vol. 4357, 2006, pp. 43–57.

[171] E. Schoch, F. Kargl, and M. Weber, "Communication patterns in VANETs", *IEEE Communications Magazine*, vol. 46, no. 11, pp. 119–125, 2008.

[172] A. Serjantov and G. Danezis, "Towards an information theoretic metric for anonymity", in *Privacy Enhancing Technologies*, ser. LNCS, Springer, vol. 2482, 2003, pp. 41–53.

[173] A. Shamir, "How to share a secret", *Communications of the ACM*, vol. 22, no. 11, pp. 612–613, 1979.

[174] R. Shokri, J. Freudiger, M. Jadliwala, and J.-P. Hubaux, "A distortion-based metric for location privacy", in *Proceedings of the 8th ACM workshop on Privacy in the electronic society*, ACM, 2009, pp. 21–30.

[175] R. Shokri, G. Theodorakopoulos, J.-Y. Le Boudec, and J.-P. Hubaux, "Quantifying location privacy", in *IEEE Symposium on Security and Privacy*, IEEE, 2011, pp. 247–262.

[176] A. Singh and H. C. S. Fhom, "Restricted usage of anonymous credentials in vehicular ad hoc networks for misbehavior detection", *International Journal of Information Security*, pp. 1–17, 2016.

[177] C. Sommer and F. Dressler, *Vehicular networking*. Cambridge University Press, 2014.

[178] C. Sommer, R. German, and F. Dressler, "Bidirectionally coupled network and road traffic simulation for improved IVC analysis", *IEEE Transactions on Mobile Computing*, vol. 10, no. 1, pp. 3–15, 2011.

[179] *Specification of the identity mixer cryptographic library – Version 2.3.40*, IBM Research – Zurich, Jan. 2013.

[180] R. Stahlmann, A. Festag, A. Tomatis, I. Radusch, and F. Fischer, "Starting european field tests for car-2-x communication: The DRIVE C2X framework", in *18th ITS World Congress*, Orlando, USA, 2011.

[181] "Status of the dedicated short-range communications technology and applications", U.S. Department of Transportation, Tech. Rep. FHWA-JPO-15-218, Jul. 2015.

[182] H. Stübing, M. Bechler, D. Heussner, T. May, I. Radusch, H. Rechner, and P. Vogel, "Sim^{TD}: A car-to-x system architecture for field operational tests", *Communications Magazine, IEEE*, vol. 48, no. 5, pp. 148–154, 2010.

[183] F. Stumpf, *CycurHSM – An automotive-qualified software stack for hardware security modules*. [Online]. Available: `https://www.escrypt.com/fileadmin/escrypt/pdf/CycurHSM-Whitepaper.pdf` (Accessed: 08/31/2016).

[184] F. Stumpf, L. Fischer, and C. Eckert, "Trust, security and privacy in VANETs – a multilayered security architecture for C2C-communication", *23. VDI/VW-Gemeinschaftstagung Automotive Security*, VDI-Berichte, vol. 2016, p. 55, Nov. 2007.

[185] L. Sustar, "RSA 2015: Tension continues to grow between govt, cryptographers", *SC Magazine*, Apr. 2015.

[186] L. Sweeney, "K-anonymity: A model for protecting privacy", *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, vol. 10, no. 05, pp. 557–570, 2002.

[187] The European Commission, *EU transport in figures – statistical pocketbook*, 2015.

[188] The European Commission, *G7 declaration on automated and connected driving*, Sep. 2015. [Online]. Available: `https://ec.europa.eu/commission/2014-2019/bulc/announcements/g7-declaration-automated-and-connected-driving_en` (Accessed: 08/31/2016).

[189] The Guardian, "Surveillance", Sep. 2015. [Online]. Available: `http://www.theguardian.com/world/surveillance` (Accessed: 08/31/2016).

[190] A. Tomandl, D. Herrmann, and H. Federrath, "PADAVAN: Privacy-aware data accumulation for vehicular ad-hoc networks", in *10th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, IEEE, 2014, pp. 487–493.

[191] A. Tomandl, F. Scheuer, and H. Federrath, "Simulation-based evaluation of techniques for privacy protection in VANETs", in *8th International Conference on Wireless and Mobile Computing, Networking and Communications*, IEEE, 2012, pp. 165–172.

[192] M. Torrent-Moreno, J. Mittag, P. Santi, and H. Hartenstein, "Vehicle-to-vehicle communication: Fair transmit power control for safety-critical information", *IEEE Transactions on Vehicular Technology*, vol. 58, no. 7, pp. 3684–3703, 2009.

[193] C. Troncoso, E. Costa-Montenegro, C. Diaz, and S. Schiffner, "On the difficulty of achieving anonymity for vehicle-2-x communication", *Computer Networks*, vol. 55, no. 14, pp. 3199–3210, 2011.

[194] Trusted Computing Group, *TCG TPM 2.0 Library profile for automotive thin specification, version 1.0*, TCG Specification, Mar. 2015.

[195] S. Turksma, "The various uses of floating car data", in *Proceedings of the 10th International Conference on Road Transport Information and Control*, Apr. 2000, pp. 51–55.

[196] UN General Assembly, "The universal declaration of human rights", *General Assembly Resolution 217 A (III)*, 1950.

[197] United States Department of Transportation, *U.S. department of transportation announces up to $42 million in next generation connected vehicle technologies*, Oct. 2015. [Online]. Available: `http://www.its.dot.gov/press/2015/ngv_tech_announcement.htm` (Accessed: 08/31/2016).

[198] U.S. Departement of Transportation – National Highway Traffic Safety Administration, "Federal motor vehicle safety standards: Vehicle-to-vehicle (V2V) communications; advance notice of proposed rulemaking (ANPRM); Docket No. NHTSA-2014-0022", *Federal Register*, vol. 79, no. 161, Aug. 2014.

[199] U.S. Environmental Protection Agency, "Inventory of U.S. greenhouse gas emissions and sinks: 1990 – 2014", Tech. Rep. EPA 430-R-16-002, Apr. 2016.

[200] I. Wagner and D. Eckhoff, "Privacy assessment in vehicular networks using simulation", in *Proceedings of the 2014 Winter Simulation Conference*, IEEE Press, 2014, pp. 3155–3166.

[201] M. Wall, "Is your connected car spying on you?", *BBC*, Nov. 2014.

[202] S. D. Warren and L. D. Brandeis, "The right to privacy", *Harvard Law Review*, vol. 4, no. 5, pp. 193–220, 1890.

[203] M. Weinstein, "Apple vs. Google: The privacy revolution rumble", *The Huffington Post*, Sep. 2014.

[204] M. Weiser, "The computer for the 21st century", *Scientific American*, vol. 265, no. 3, pp. 94–104, 1991.

[205] A. F. Westin, *Privacy and freedom*. Atheneum, 1967.

[206] S. Wheatley, T. Maillart, and D. Sornette, "The extreme risk of personal data breaches and the erosion of privacy", *The European Physical Journal B*, vol. 89, no. 1, pp. 1–12, 2016.

[207] J. White and I. Wells, "Extracting origin destination information from mobile phone data", in *Eleventh International Conference on Road Transport Information and Control*, IET, Mar. 2002, pp. 30–34.

[208] W. Whyte, A. Weimerskirch, V. Kumar, and T. Hehn, "A security credential management system for V2V communications", in *Vehicular Networking Conference (VNC)*, IEEE, 2013, pp. 1–8.

[209] B. Wiedersheim, Z. Ma, F. Kargl, and P. Papadimitratos, "Privacy in inter-vehicular networks: Why simple pseudonym change is not enough", in *Seventh International Conference on Wireless On-demand Network Systems and Services (WONS)*, IEEE, 2010, pp. 176–183.

[210] H. Wieker, K. Eckert, J. Vogt, and M. Fünfrocken, "CONVERGE – A german cooperative ITS architecture", in *21st ITS World Congress*, Orlando, USA, Sep. 2014.

[211] F.-L. Wong and F. Stajano, "Location privacy in bluetooth", in *European Workshop on Security in Ad-hoc and Sensor Networks*, ser. LNCS, Springer, vol. 3813, 2005, pp. 176–188.

[212] P. R. Zimmermann, "Why I wrote PGP", *PGP User's Guide*, 1991.