vehicular networks. In addition, this paper uses Huffman codes in combination with authenticated dynamic hash k-ary trees to create a more efficient data structure. This structure allows using a tree where the most queried revoked pseudonyms correspond to the shortest paths in the tree. This provides a better model of the real behavior of vehicular networks, because some vehicles (such as public transport) are more common than others on the roads.

7. Acknowledgements

Research supported by the MINECO and the FEDER under Projects TIN2011- 25452 and IPT-2012-0585-370000, and the scholarship BES-2012-051817.

6. References

[1] G. Bertoni, J. Daemen, M. Peeters, G.V. Assche: "Keccak sponge function family main document", version 2.1, Updated submission to NIST (Round 2), 2010.

[2] S. Blake-Wilson: "Information security, mathematics, and public-key cryptography". Designs, Codes and Cryptography 19(2-3), pp. 77-99, 2000.

[3] D. Boneh, M. Franklin: "Identity-based encryption from the Weil pairing". Crypto. LNCS 2139, pp. 213-229, 2001.

[4] T. Cormen, C. Leiserson, R. Rivest: "Introduction to algorithms". MIT Press, 1990.

[5] ETSI: Intelligent Transport Systems. http://www.etsi.org/index.php/technologies-clusters/technologies/intelligent-transport, Access Date: 02 Dec 2014.

[6] C. Ganan, J. Munoz, O. Esparza, J. Mata-Diaz, J. Alins: "Toward Revocation Data Handling Efficiency in VANETs". Communication Technologies for Vehicles. LNCS 7266, pp. 80-90, 2012.

[7] M. Goodrich, M. Shin, R. Tamassia, W. Winsborough: "Authenticated dictionaries for fresh attribute credentials". Trust Management. LNCS 2692, pp. 332-347, 2003.

[8] M. Goodrich, R. Tamassia, N. Triandopoulos, R. Cohen: "Authenticated data structures for graph and geometric searching". CT-RSA. LNCS 2612, pp. 295-313, 2003.

[9] J.P. Hubaux, S. Capkun, J. Luo: "The security and privacy of smart vehicles". IEEE Security and Privacy 2(3), pp. 49-55, 2004.

[10] D. Huffman: "A Method for the Construction of Minimum-Redundancy Codes". Proceedings of IRE 40 (9), pp. 1098-1101, 1952.

[11] IEEE-1609: "Family of standards for Wireless Access in Vehicular Environments" (WAVE). U.S. Department of Transportation, 2006.

[12] M. Jakobsson, T. Leighton., S. Micali, M. Szydlo: "Fractal merkle tree representation and traversal". CT-RSA. LNCS 2612, pp.314-326, 2003.

[13] M. Jakobsson, S. Wetzel: "Efficient attribute authentication with applications to ad hoc networks". ACM workshop on vehicular ad hoc networks, pp. 38-46, 2004.

[14] A. Joux: "The weil and tate pairings as building blocks for public key cryptosystems". Algorithmic Number Theory Symposium. LNCS 2369, pp. 20-32, 2002.

[15] P. Kocher: "On certificate revocation and validation". FC'98. LNCS 1465, pp. 172-177, 1998.

[16] R. Merkle: "Protocols for public key cryptosystems". IEEE Security and privacy 1109, pp. 122-134, 1980.

[17] V. Miller: "Short programs for functions on curves". Unpublished manuscript, 97, pp. 101-102, 1986.

[18] J. Muñoz, J. Forne, O. Esparza, J. Manel: "Efficient Certificate Revocation System Implementation: Huffman Merkle Hash Tree (HuffMHT)." TrustBus, pp 119-127, 2005.

[19] M. Raya, J.P. Hubaux: "Securing vehicular ad hoc networks". Computer Security 15(1), pp. 39-68, 2007.

[20] A. Shamir: "Identity-based cryptosystems and signature schemes". Crypto. LNCS 196, pp. 47-53, 1985.