Journal of Computer and Communications, 2014, 2, 14-21
Published Online July 2014 in SciRes. http://www.scirp.org/journal/jcc
http://dx.doi.org/10.4236/jcc.2014.29003

Tree-Based Revocation for Certificateless Authentication in Vehicular Ad-Hoc Networks

Pino Caballero-Gil, Francisco Martín-Fernández, Cándido Caballero-Gil

Department of Computer Science, University of La Laguna, Tenerife, Spain
Email: pcaballe@ull.es, francisco.martin.07@edu.ull.es, ccabgil@ull.es

Received April 2014

Abstract

This work proposes authentication based on identity as a way to increase the efficiency and security of communications in vehicular ad-hoc networks. When using identity-based cryptography to achieve certificateless authentication, membership revocation is not a trivial problem. Thus, in order to improve the performance of revocation in such networks, the use of a dynamic authenticated data structure based on perfect k-ary hash trees combined with a duplex version of the new standard SHA-3 is here presented. Efficient algorithms in the used revocation trees allow reaching a refresh rate of at most simple updates per inserted node. Consequently, the proposal is especially useful for situations with frequent revocations, which are foreseeable when vehicular ad-hoc networks are widely deployed.

Keywords

K-Ary Tree, Identity-Based Cryptography, Revocation, Hash Function, Vehicular Ad-Hoc Network

1. Introduction

Authentication is a crucial requirement for any communication network. On the one hand, an efficient way to authenticate legitimate and honest nodes is necessary. On the other hand, being able to exclude compromised nodes is fundamental to guarantee trustworthiness of network.

When communication security is based on public-key cryptography, a central problem is to guarantee that a particular public key is authentic and valid. The traditional approach to this problem is through public-key certificates emitted by a Public-Key Infrastructure (PKI), in which a Certificate Authority (CA) certifies ownership and validity of public-key certificates. This solution presents many difficulties because the issues associated with certificate management are quite complicated and expensive. A different approach is the so-called Identity-Based Cryptography (IBC), where each user's public key is his/her public IDentity (ID) so that the need for public-key certificates is eliminated.

In order to use any public-key cryptosystem in practice, an efficient revocation mechanism is necessary because private keys may become compromised. Traditionally, this problem has been solved through a centralized approach based on the existence of a Trusted Third Party (TTP), which is usually a CA distributing the so-called Certificate Revocation Lists (CRLs) that can be seen as blacklists of revoked certificates. Alternatively, some

How to cite this paper: Caballero-Gil, P., Martín-Fernández, F. and Caballero-Gil, C. (2014) Tree-Based Revocation for Certificateless Authentication in Vehicular Ad-Hoc Networks. *Journal of Computer and Communications*, **2**, 14-21.
http://dx.doi.org/10.4236/jcc.2014.29003

authors have proposed an approach based on hash trees as Authenticated Data Structures (ADSs) for a more efficient management of certificate revocation.

Vehicular Ad-hoc NETworks (VANETs) are self-organizing networks built up from moving vehicles that communicate with each other mainly to prevent adverse circumstances on the roads, but also to achieve more efficient traffic management. In particular, these networks are considered an emerging research area of mobile communications because they offer a wide variety of possible applications, ranging from the aforementioned road safety and transport efficiency, to commercial services, passenger comfort, and infotainment delivery. Furthermore, VANETs can be seen as an extension of mobile ad-hoc networks where there are not only mobile nodes, named On-Board Units (OBUs), but also static nodes, named Road-Side Units (RSUs). The so-called Intelligent Transportation System (ITS) includes two types of communications: between OBUs and between OBUs and RSUs [1]. Both the European standard for ITS, named ITS-G5, and its American counterpart, named Wireless Access in Vehicular Environment (WAVE), are based on the IEEE 802.11p amendment to the IEEE 802.11 standard.

Security in VANETs faces many challenges due to the open broadcasting of wireless communications and the high-speed mobility of vehicles. In these networks, any malicious misbehaving user that can inject false information, or modify/replay any previously disseminated message, could be fatal to the others. Therefore, within the family of standards for vehicular communications IEEE 1609 based on the IEEE 802.11p, the standard 1609.2 deals in particular with the issues related to security services for applications and management messages. This standard describes the use of PKIs, CAs and CRLs, and implies that in order to revoke a vehicle, a CRL has to be issued by the CA to the RSUs, who are in charge of sending this information to the OBUs. In particular, the IEEE 1609.2 standard proposes both broadcast authentication and non-repudiation through the use of the elliptic curve digital signature algorithm.

Each vehicle is assumed to have a pair of keys: a private signing key and a public verification key certified by the CA; and any VANET message must contain: a timestamp with the creation time, the sender's signature, and the sender’s public-key certificate.

According to the so-called Dedicated Short-Range Communications (DSRC) channels specifically designed for automotive use, vehicles periodically exchange with nearby vehicles beacons containing sender's information such as location and speed because many VANET applications, such as the cooperative collision warning, rely on the information embedded in these beacons.

In order to protect privacy in VANETs, each OBU can obtain multiple certified key pairs and use different public keys each time. These public keys are linked to pseudonyms that allow preventing location tracking by eavesdroppers. Therefore, once VANETs are implemented in practice on a large scale, their size will grow rapidly due to the increasing number of OBUs and to the use of such multiple pseudonyms. Thus, it is foreseeable that if CRLs are used, they will grow up to become very large and unmanageable. Moreover, this context can bring a phenomenon known as implosion request, consisting of many nodes who synchronously try to download the CRL during its updating, producing serious congestion and overload of the network, which could lead to a longer latency in the process of validating a certificate.

The proposal described in this paper defines the use of IBC to achieve certificateless and cooperative authentication in VANETs. It also introduces a perfect k-ary hash tree as an ADS for the management of pseudonym revocation. By using this ADS, the process of query on the validity of public pseudonyms will be more efficient because OBUs will send queries to RSUs, who will answer them on behalf of the TTP. In this way, at the same time this TTP will no longer be a bottleneck and OBUs will not have to download any entire revocation list. Instead of that, they will have to manage hash trees where the leaf nodes contain revoked pseudonyms. In particular, the used k-ary trees are based on the application of a duplex construction of the Secure Hash Algorithm SHA-3 that was recently chosen as standard, because the combination of both structures allows improving efficiency of updating and querying revoked pseudonyms.

This paper is organized as follows. Section 2 presents a review of related work. Concepts and notation used in the proposed authentication scheme based on the combination of IBC, perfect k-ary hash trees and a duplex version of SHA-3 are introduced in Section 3. Section 4 summarizes the main ideas of the proposal. Finally, Section 5 discusses some conclusions and open problems.

2. Related Works

Under appropriate conditions and in certain circumstances, the use of public-key cryptography can be considered essential for information security [2].

For instance, the work [3] proposes the use of a PKI to protect messages and mutually authenticate entities in VANETs. [4] also defines a PKI-based security protocol where each vehicle pre-loads anonymous public/private keys and the TTP stores all the anonymous certificates of all the vehicles. Such a scheme produces inefficiency in the certificate management process.

Also based on a PKI, a well-known solution for strong authentication in VANETs is based on the signature of each message [5]. However, the use of a traditional approach to PKIs may fail to satisfy the real-time requirement in vehicular communications because according to the DSRC protocol, each OBU will periodically transmit beacons so even in a normal traffic scenario, it is a very rigorous requirement to deploy an authentication scheme that allows at the same time efficient revocation of invalid public keys, and efficient use of valid public keys. This is exactly the main goal of this work.

A revocation method called On-line Certificate Status Protocol (OCSP) involves a multitude of validation agents that respond to client queries with signed replies indicating the current status of a target certificate. This explicit revocation method has an unpleasant side-effect because it divulges too much information. Since validation agents constitute a global service, they must involve enough replication to handle the load of all validation queries, what means that the signature key must be replicated across many servers, which is either insecure or expensive. A solution called Certificate Revocation Tree (CRT) was proposed in [6] as an improvement for OCSP involving a single highly secure entity that periodically posts a signed CRL-like data structure to many insecure validation agents so that users query these agents. In CRTs the leaf nodes are statements concerning revoked certificates, and the CA signs the root. By using CRTs, the responder can prove the status of any certificate by showing the path from the root to the leaf node without signing the response, because the signatures of any leaf node are identical, and given by the signature contained in the root. Thus, no trust in the responder is necessary. The proposal here described is based on this idea, but does not use any certificate.

The basic ADS proposed in [6] is a Merkle hash tree [7] where the leaf nodes represent revoked certificates sorted by serial number. A client sends a query to the nearest agent, which produces a short proof that the target certificate is (or not) on the CRT. [8] introduces several methods to traverse Merkle trees allowing time-space trade-offs. Other ADSs based on multi-dimensional tree structures are studied in [9] to support efficient search queries, allowing the retrieval of authenticated certificates from an untrusted repository used for dissemination by various credential issuers. Besides, many tree-balancing algorithms have been proposed in the bibliography for hash trees [10]. For instance, AVL trees are balanced by applying rotation, B-trees are balanced by manipulating the degrees of the nodes, and 2 - 3 trees contain only nodes with at least 2 and at most 3 children. However, in the particular application of public-key revocation, balancing trees does not necessary minimize the overall communication.

Another interesting problem with CRTs appears each time a certificate is revoked as the whole tree must be recomputed and restructured. Skip-lists proposed in [11] can be seen as a natural and efficient structure for the purpose of reducing communication by balancing the CRT. However, they are not good solutions for other problems such as insertion of new leaf nodes.

Hash trees are usually based on widely used hash functions. This work uses a new version of SHA-3, which is a cryptographic hash function recently selected as the winner of the NIST hash function competition [12]. SHA-3 uses the Keccak function [13] and a sponge construction [14] in which message blocks are XORed into the initial bits of the state. However, the version of SHA-3 here used is based on a duplex construction [15], which allows a more efficient insertion of revoked nodes as leaf nodes of the revocation tree.

In order to solve the problem caused by the management of valid public-key certificates, [16] proposes the idea of an identity-based cryptosystem in which arbitrary strings can act as public keys so that there is no need for public-key certificates. The first practical identity-based encryption scheme was described in [17] using a bilinear map. Weil and Tate pairings on elliptic curves are the most efficient ways of constructing such bilinear maps [18]. The proposal here described was implemented using the Tate pairing for identity-based authentication.

3. Preliminaries

3.1. ID-Based Cryptography

The idea of IBC and, in particular, of Identity-Based Signature (IBS) is that the public identity ID of the signer can be used as verification key of a received signature, what avoids the need of any public-key certificate. In our scheme, such an identity is a public pseudonym P_j sent by the signer node together with the signed message. In the used ID-based system, each node has to receive all the signing private keys PrP_j linked to all its pseudonyms P_j from a TTP, because it cannot generate them by itself. In particular, a TTP, called in IBC the Private Key Generator (PKG), is in charge of computing and delivering to each node via a confidential channel, the signing private keys linked to each of its pseudonyms. On the other hand, the PKG publishes a master public key *MPu* and retains the corresponding master private key *MPr*. Thus, given the master public key *MPu*, any party will be able to compute the public key PuP_j corresponding to any pseudonym P_j by combining it with *MPu*. In order to use the corresponding private key, the node authorized to use a pseudonym must have received it from the PKG, which uses the master private key *MPr* to generate all the private keys corresponding to all the pseudonyms. Thus, the main algorithms in the proposed IBS are as follows:

- Setup: The PKG randomly picks its master private key *MPr*, and therefore computes and publishes its master public key *MPu*.
- Extraction: For each pseudonym *Pj*, the PKG uses its master private key *MPu* to compute the corresponding private key PrP_j and all pairs (P_j, PrP_j) are sent securely from the PKG to the corresponding owner.
- Signature: A signer node uses its private key PrP_j to compute the signature of a message *M*, and sends openly both the computed signature $PrP_j(M)$ and its pseudonym P_j.
- Verification: A node that receives a signed message and corresponding pseudonym ($PrP_j(M)$, P_j) uses *MPu* and P_j to compute PuP_j and verify the signature $PrP_j(M)$.

Note that no new ID-based cryptosystem is described in this paper because it is out of its scope. The ID-based system that has been implemented in the proof-of-concept prototype is the Boneh-Franklin scheme [17], which uses a bilinear pairing over elliptic curves and bases its security on the Bilinear Diffie-Hellman problem.

The used ID-based system is built from a bilinear map e: $G_1 \times G_1 \to G_2$ between two groups G_1 and G_2 so that according to the bilinearity of e: $e(aP, bQ) = e(P, Q)^{ab}$ for all P, $Q \in G_1$ and a, $b \in Z$. Specifically, an ID-based system can be built from a bilinear map e if and only if a variant of the Computational Diffie-Hellman problem in G_1 is hard. The considered Bilinear Diffie-Hellman problem in G_1 is defined as follows: Given P, aP, bP, cP, compute $e(P, P)^{abc}$, where $P \in G_1$ and a, b, $c \in Z$. In particular, the used bilinear pairing e is described for an elliptic curve E defined over some field K, so it maps a pair of points of E to an element of the multiplicative group of a finite extension of K.

The first satisfactory version of the Boneh-Franklin scheme was based on the Weil pairing [17]. However, the scheme implemented in this work uses the Tate pairing because this is considered the most convenient bilinear function for the Boneh-Franklin scheme in terms of computational cost. In particular, the implementation of the proposal includes the use of Miller's algorithm to compute the Tate pairing [19].

In IBC, just a few works exist on revocation mechanisms. Here we propose a scheme to manage revoked pseudonyms, built on the idea of revocation hash trees.

3.2. Tree Notation

The tree-based model described in this paper is based on the following notation:

- $h(\ldots)$: Hash function used to define the revocation tree.
- $h(A0 \mid A1 \mid \ldots)$: Digest obtained with the hash function h applied on the concatenation of the inputs Ai, $i = 0, 1\ldots$
- D (≥ 1): Depth of the hash tree.
- d_x ($< D$): depth of an internal node x in the tree.
- t: total number of revoked pseudonyms.
- RP_j ($j = 1, 2, \ldots, t$): *j-th* Revoked Pseudonym.
- N_{ij} ($i = D\text{-}d_{Nij}$ *and* $j = 0, 1\ldots$): Internal Node of the hash tree.
- N_{0j} ($j = 0, 1\ldots$): Leaf Node of the hash tree.
- k: Maximum number of children for each internal node in the hash tree.
- $f(\ldots)$: Keccak function used in SHA-3.
- n: Bit size of the digest of h.
- s: Bit size of the input to f.
- r: Bit size of the input blocks for h after padding.

- l: Bit size of the output blocks that build the digest of h, which is here assumed to be lower than r.

3.3. K-Ary Hash Tree

In order to improve efficiency of communication and computation in the management of revocations in VANETs, some authors have proposed the use of particular ADSs such as Merkle trees [7] and skip lists [20] [21]. However, to the best of our knowledge no previous work has described in detail the use of perfect k-ary trees as hash trees for revoked pseudonym management.

In general, a hash tree is a tree structure whose nodes contain digests that can be used to verify larger pieces of data. The leaf nodes in a hash tree are hashes of data blocks while nodes further up in the tree are the hashes of their respective children so that the root of the tree is the digest representing the whole structure. Most implemented hash trees require the use of a cryptographic hash function h in order to prevent collisions.

On the one hand, each leaf node N_{0j} of a hash tree is given by a hash value. On the other hand, for each internal node N_{ij}, i is defined by the distance from the node to a leaf node, or the depth of the node. Hence, a leaf node has $i = 0$ and the root has $i = D$. The subindices j of all nodes N_{ij} of each level are numbered from left to right, so that, for instance, N_{i0} is the leftmost node of level i.

Like most hash trees, the Merkle tree is a binary tree, so each internal node N_{ij} is the hash value of the concatenation of its two children: $N_{ij} = h(N_{i\text{-}1,0} \mid N_{i\text{-}1,1})$.

On the contrary, this work proposes the use of a more general structure known as k-ary tree, which is a rooted tree in which each node has no more than k children, and each internal node is obtained by hashing the concatenation of all the digests contained in its children. Specifically, we propose the use of a perfect k-ary tree in which all leaf nodes N_{0j} are at the same depth D (see **Figure 1**). In this way, one of the major drawbacks of ordered tree structures, which is the necessary restructuring when there are changes in the tree, only occurs in our proposal when the perfect k-ary tree requires the introduction of a new level of depth, because otherwise the nodes are simply inserted from left to right in order to complete each level of depth.

The authenticity of the used hash tree structure is guaranteed thanks to the TTP signature of the root N_{D0}. When a RSU answers to an OBU about a query on a pseudonym, it proceeds in the following way. If it finds the digest of the pseudonym among the leaf nodes of the tree, which means that it is a revoked pseudonym, the RSU sends to the OBU the route between the root and the corresponding leaf node, along with all the siblings of the nodes on this path. After checking all the digests corresponding to the received path, and the TTP signature of the root, the OBU gets convinced of the validity of the received evidence on the revoked pseudonym.

3.4. Duplex Version of SHA-3

Regarding the cryptographic hash function h used in the hash tree, the proposal is based on the use of a new version of the Secure Hash Algorithm SHA-3. In SHA-3, the padding of the input is a minimum 10*1 pattern that consists of a 1 bit, zero or more 0 bits (maximum r-1) and a final 1 bit, and the basic cryptographic hash function f called Keccak contains 24 rounds of a basic transformation that involves 5 steps. There the input is repre-

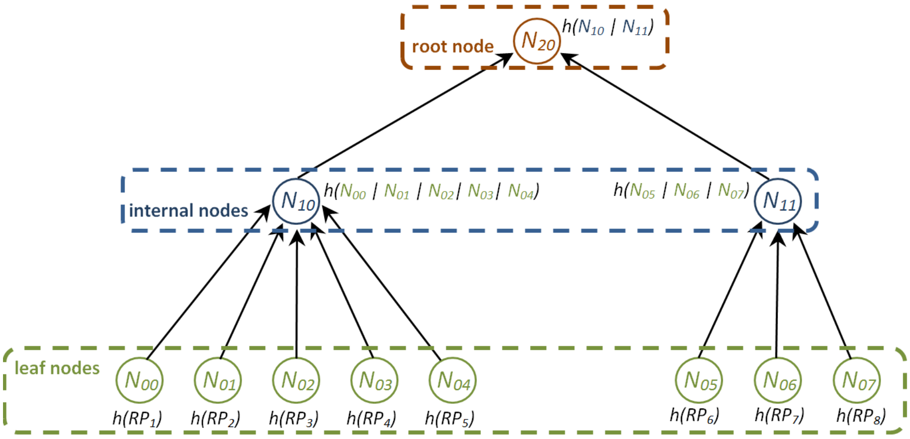

Figure 1. Hash tree based on a perfect 5-ary tree.

sented by a 5 × 5 matrix of 64-bit lanes. However, the proof-of-concept of our proposal has been implemented using 32-bit lanes in order to increase flexibility.

Another variation of SHA-3 is the combination of a duplex version of the sponge structure of SHA-3 [15] and a hash k-ary tree. On the one hand, like the sponge construction of SHA-3, our proposal based on a duplex construction also uses Keccak as fixed-length transformation *f*, the same padding rule based on the 10∗1 pattern, and data bit rate *r*, which is here assumed to be 352. On the other hand, unlike a sponge function, the duplex construction output corresponding to an input string might be obtained through the concatenation of the outputs resulting from successive input blocks (see **Figure 2**).

In this way, the use of the duplex construction in our proposed hash tree allows the insertion of a new revoked node as new leaf node of the tree by running a new iteration of the duplex construction only on the new revoked node. In particular, the RSU can take advantage of all the digests corresponding to the sibling nodes of the new node, which were computed in previous iterations, by simply discarding the same minimum number of the last bits of each of those digests so that the total size of the resulting digest of all the children remains the same, *n*, which is here assumed to be the lowest possible size of SHA-3 digest, 224. Thus, while the maximum number of children of an internal node has not been reached, the RSU stores not only all the digests of the tree but also the state resulting from the application of Keccak hash function *f* in the last iteration corresponding to such internal node, in order to use it as input in a next iteration.

4. Certificateless Authentication

In the scheme proposed in this work, a node does not need any certificate to prove the binding to its public key. Instead of that, an ID-based authentication scheme and revocation trees are used. We consider the following basic authentication architecture, which includes three main parties:

- TTP: This entity acts as key distribution centre because it is responsible for generating and assigning related parameters for VANET nodes, and for revoking pseudonyms of misbehaving OBUs and public keys of misbehaving RSUs.
- RSU: This entity serves as a gateway to provide OBUs within its transmission range with any requested information about revoked pseudonyms.
- OBU: Each vehicle is equipped with an OBU, which periodically broadcasts signed beacons that are received by neighbour OBUs and RSUs.

The proposed model is based on the use of a pseudonym P_j set by each OBU, so that for each one the TTP provides the OBU with a corresponding private key PrP_j. If any of those pseudonyms is revoked by the TTP, it inserts all the pseudonyms corresponding to the same OBU in the revocation tree. The TTP is also responsible for periodically updating the tree by deleting the expired pseudonyms, and for restructuring the tree when necessary. After each update, the TTP sends the corresponding modifications of the updated tree to all RSUs.

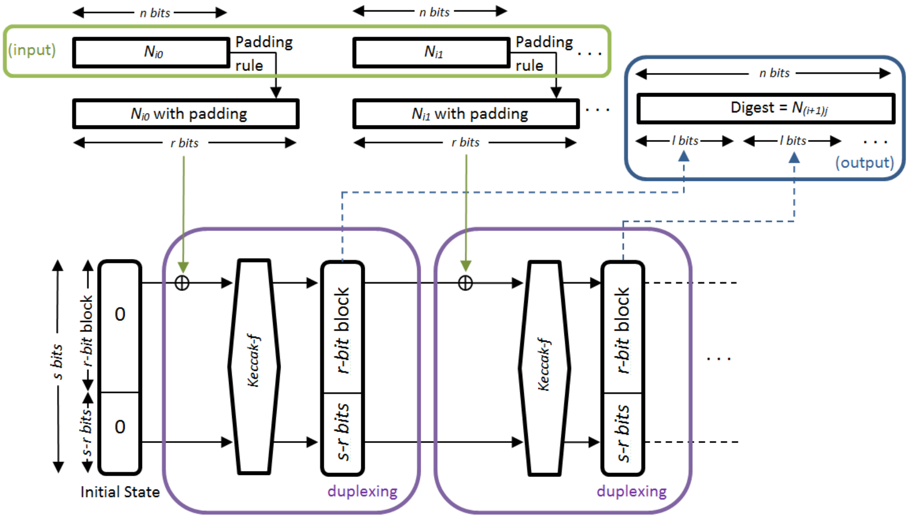

Figure 2. Proposed duplex construction.

The RSU has to search vehicle pseudonyms in the revocation tree each time an OBU requests it. The RSU must provide the requesting OBU either with a verifiable revocation proof of any revoked pseudonym or with a signed message indicating that the requested pseudonym has not been revoked and is labelled as "OK". In the first case, by using the answer data, the OBU can verify the TTP signature of the received signed root, recompute the root of the revocation tree, and check it by comparing it with the received signed root.

The proposed scheme is computationally efficient since it obviates the need to sign each RSU reply, as it removes most of the trust from it. The only case when the RSU's trust is questioned is when it provides an "OK" answer because that could be a fraud.

In this regard, when an OBU receives an "OK" message signed by a cheating RSU, it trusts it momentarily. However, when it contacts another RSU, it asks it again about the same pseudonym. If this RSU provides the OBU with a proof of revocation whose timestamp contradicts the "OK" answer signed by the questioned RSU, the OBU sends to the latter RSU an impeachment on the questioned RSU, so that the honest RSU can send it to the TTP who will revoke its public key by deleting it directly from the revoked RSU. Otherwise, if the second RSU also sends a signed "OK" message, the OBU goes on asking about the same pseudonym until it reaches either a contradiction or a prefixed trust threshold.

Thus, each OBU stores locally in two separate and complementary structures, the pseudonyms of those OBUs that it has previously checked as unreliable, and of those OBUs that have been reliable till then. Therefore, in the future, if it reconnects with any of these vehicles, it can use such information to decide how to proceed. If there is no RSU nearby, it uses these data to decide whether to establish the communication or not. Otherwise, even if there is an RSU nearby, there is no need to re-ask it about a checked revoked pseudonym.

5. Conclusion

One of the most important security issues in VANETs is authentication, involving an efficient management of both valid and invalid public keys. On the one hand, we have proposed identity-based cryptography to achieve certificateless authentication, what increases efficiency and security in vehicular communications. On the other hand, in order to deal with the problem of revocation management as VANETs grow, this paper has introduced the use of a dynamic authenticated data structure based on k-ary hash trees combined with a duplex version of the new standard SHA-3. Such a structure allows taking advantage of the digests of previous revoked pseudonyms for calculating the hash value corresponding to every new revoked pseudonym. Therefore, its insertion in the hash tree can be performed by a single iteration of the hash function. There are still some open questions such as the analysis of optimal values for the parameters and a comparison with previous proposals.

Acknowledgements

Research supported under TIN2011-25452, IPT-2012-0585-370000 and BES-2012-051817.

References

[1] ETSI (2012) Intelligent Transport Systems. http://http://www.etsi.org/index.php/technologies-clusters/technologies/intelligent-transport

[2] Blake-Wilson, S. (2000) Information Security, Mathematics, and Public-Key Cryptography. *Designs*, *Codes and Cryptography*, **19**, 77-99. http://dx.doi.org/10.1023/A:1008345904539

[3] Hubaux, J.P., Capkun, S. and Luo, J. (2004) The Security and Privacy of Smart Vehicles. *IEEE Security and Privacy*, **2**, 49-55. http://dx.doi.org/10.1109/MSP.2004.26

[4] Raya, M. and Hubaux, J.P. (2007) Securing Vehicular Ad Hoc Networks. *Computer Security*, **15**, 39-68.

[5] IEEE-1609 (2006) Family of Standards for Wireless Access in Vehicular Environments (WAVE). US Department of Transportation.

[6] Kocher, P. (1998) On Certificate Revocation and Validation. FC'98. LNCS 1465, 172-177.

[7] Merkle, R. (1980) Protocols for Public Key Cryptosystems. *IEEE Security and Privacy*, **1109**, 122-134.

[8] Jakobsson, M., Leighton, T., Micali, S. and Szydlo, M. (2003) Fractal Merkle Tree Representation and Traversal. CT-RSA. LNCS 2612, 314-326.

[9] Goodrich, M., Shin, M., Tamassia, R. and Winsborough, W. (2003) Authenticated Dictionaries for Fresh Attribute Credentials. *Trust Management*, LNCS 2692, 332-347.

[10] Cormen, T., Leiserson, C. and Rivest, R. (1990) Introduction to Algorithms. MIT Press.

[11] Goodrich, M., Tamassia, R., Triandopoulos, N. and Cohen, R. (2003) Authenticated Data Structures for Graph and Geometric Searching. CT-RSA. LNCS 2612, 295-313.

[12] Chang, S., Perlner, R., Burr, W., Turan, M., Kelsey, J., Paul, S. and Bassham, L. (2012) Third-Round Report of the Sha-3 Cryptographic Hash Algorithm Competition. NIST. nvlpubs.nist.gov/nistpubs/ir/2012/NIST.IR.7896.pdf

[13] Bertoni, G., Daemen, J., Peeters, M. and Assche, G.V. (2010) Keccak Sponge Function Family Main Document Version 2.1, Updated Submission to NIST (Round 2).

[14] Bertoni, G., Daemen, J., Peeters, M. and Assche, G.V. (2008) On the Indifferentiability of the Sponge Construction. *Eurocrypt*, LNCS 4965, 181-197.

[15] Bertoni, G., Daemen, J., Peeters, M. and Assche, G.V. (2012) Duplexing the Sponge: Single-Pass Authenticated Encryption and Other Applications. *Selected Areas in Cryptography*, LNCS 7118, 320-337.

[16] Shamir, A. (1985) Identity-Based Cryptosystems and Signature Schemes. *Crypto*, LNCS 196, 47-53.

[17] Boneh, D. and Franklin, M. (2001) Identity-Based Encryption from the Weil Pairing. *Crypto*, LNCS 2139, 213-229.

[18] Joux, A. (2002) The Weil and Tate Pairings as Building Blocks for Public Key Cryptosystems. *Algorithmic Number Theory Symposium*, LNCS 2369, 20-32.

[19] Miller, V. (1986) Short Programs for Functions on Curves. *Unpublished Manuscript*, **97**, 101-102.

[20] Ganan, C., Munoz, J., Esparza, O., Mata-Diaz, J. and Alins, J. (2012) Toward Revocation Data Handling Efficiency in VANETs. *Communication Technologies for Vehicles*, LNCS 7266, 80-90.

[21] Jakobsson, M. and Wetzel, S. (2004) Efficient Attribute Authentication with Applications to Ad Hoc Networks. *ACM Workshop on Vehicular Ad Hoc Networks*, 38-46.