Use of a Duplex Construction of SHA-3 for Certificate Revocation in VANETs

F. Martín-Fernández, P. Caballero-Gil, and C. Caballero-Gil

Department of Statistics, Operations Research and Computing,
University of La Laguna, La Laguna, Spain

Abstract. This work describes the application of a version of the new standard SHA-3 to improve the performance of certificate revocation in Vehicular Ad-hoc NETworks (VANETs). In particular, it proposes the use of a duplex construction instead of the sponge one present in the SHA-3 version of the Keccak hash function, combined with a dynamic authenticated data structure based on k-ary trees that allows taking advantage of such a construction. Besides, a new scheme for authenticated encryption is also introduced to ensure integrity, authenticity and privacy of an auxiliary structure used to link the ordered identifier in the k-ary tree with the corresponding certificate serial number. This is an ongoing work, and the implementation of a prototype based on smartphones is being developed.

1 Introduction

Vehicular ad-hoc networks 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 a more efficient traffic management. Particularly, these networks are considered an emerging research area of mobile communications because they offer a wide variety of possible applications, ranging from 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, called On-Board Units (OBUs), but also static nodes, called Road-Side Units (RSUs).

Without security, all network nodes are potentially vulnerable to misbehavior of any dishonest user, what would make all services provided by the VANET untrustworthy. Therefore, it is absolutely necessary to have a secure procedure not only to identify misbehaving nodes, but also to exclude them from the network. One of the basic solutions to accomplish this task in networks where communications are based on a Public Key Infrastructure (PKI) is the use of certificate revocation. Thus, a critical part in such networks is the management of revoked certificates. Related to this issue, in the bibliography we can find two different types of solutions. On the one hand, a decentralized proposal enables revocation without the participation of any centralized infrastructure, based on trusting the criteria of honest network nodes. On the other hand, a centralized approach relies on the existence of a central trustful Certificate Authority (CA), which is the only entity responsible for deciding on the validity of each node certificate.

Martín-Fernández F., Caballero-Gil P. and Caballero-Gil C..
Use of a Duplex Construction of SHA-3 for Certificate Revocation in VANETs.
DOI: 10.5220/0004587300030011
In *Proceedings of the 10th International Workshop on Security in Information Systems* (WOSIS-2013), pages 3-11
ISBN: 978-989-8565-64-8

This second approach is usually based on the distribution of the so-called Certificate Revocation Lists (CRLs), which can be seen as blacklists of revoked certificates.

IEEE 1609 is a family of standards based on the IEEE 802.11p, which is an approved amendment to the IEEE 802.11 standard for vehicular communications [8]. Within such a family, 1609.2 deals with the issues related to security services for applications and management messages. In particular, the IEEE 1609.2 standard defines the use of PKIs, CAs and CRLs in VANETs, 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 the information to the OBUs. Thus, an efficient management of certificate revocation is crucial for the robust and reliable operation of VANETs.

Once VANETs are implemented in practice on a large scale, their size will grow and the use of multiple temporary certificates or pseudonyms will become necessary to protect the privacy of the users. Thus, it is foreseeable that CRLs will grow up to become very large. Moreover, in this context it is also expected a phenomena known as implosion request, consisting of several nodes who synchronously want to download the CRL at the time of its updating, producing serious congestion and overload of the network, what could ultimately lead to a longer latency in the process of validating a certificate. Consequently, since known naive approaches for the management of revoked certificates do not scale to large networks, the main motivation of this paper is to reduce the size of the part of the CRL that must be sent to the OBUs.

This proposal uses a k-ary tree as an Authenticated Data Structure (ADS), for the management of certificate revocation in VANETs. By using this ADS, the process of query on the validity of certificates will be more efficient because OBUs will send queries to RSUs, who will answer them on behalf of the CA. In this way, at the same time the CA will no longer be a bottleneck, and OBUs will not have to download the entire CRL. In particular, the used perfect k-ary trees are based on a version of the Secure Hash Algorithm SHA-3 that was recently chosen as standard [5].

Whereas the original SHA-3 uses the sponge construction [3], the proposal presented in this work applies a duplex construction of SHA-3 [4] because the combination of both structures allows improving the efficiency of updating and querying of revoked certificates. Besides, the proposal uses Authentication Encryption (AE) for providing confidentiality, integrity and authenticity during the transmission of information from the CA to the RSUs.

This paper is organized as follows. Section 2 addresses the general problem of the use of certificate revocation lists in VANETs, and provides a succinct revision of related works. Then, Section 3 focuses on the necessary preliminaries and a brief explanation of the tree-based module of the proposal. Afterwards, Section 4 introduces a novel authenticated encryption scheme proposed for transferring the CRL tree from the CA to the RSU. Finally, Section 5 discusses conclusions and possible future research lines.

2 Related Work

The general procedure when CRLs are used and a CA has to revoke a public-key certificate consists in including the corresponding certificate serial number in the CRL and distribute this CRL within the network in order to let users know which nodes are no

longer trustworthy [15]. It is important that the distribution of the CRL is done efficiently in order to allow that the knowledge about untrustworthy nodes can be spread quickly to the entire network.

In the particular case of VANETs, previous works assume that the entire CRL may be delivered by broadcasting it directly from RSUs to OBUs [10], and then distributed among OBUs cooperatively [14]. However, the large size of VANETs, and consequent large size of the CRLs, makes this approach infeasible due to the overhead it would cause to network communications. This issue is further increased with the use of multiple pseudonyms for the nodes, what has been suggested to protect privacy and anonymity of OBUs [16].

Since there are almost one thousand million cars in the world [11], considering the use of pseudonyms, a direct conclusion is that the number of revoked certificates might reach soon the same amount, one thousand million. On the other hand, assuming that each certificate takes at least 224 bits, in such a case the CRL size would be 224 Gbits, what means that its management following the traditional approach would not be efficient. Even though regional CAs were used and the CRLs could be reduced to 1 Gbit, by using the 802.11a protocol to communicate with RSUs in range, the maximum download speed of OBUs would be between 6 and 54 Mbit/s depending on vehicle speed and road congestion, so on average an OBU would need more than 30 seconds to download a regional CRL from an RSU.

A straight consequence of this size problem is that a new CRL cannot be issued very often, what would affect the freshness of revocation data. On the other hand, if a known technique for large data transfers were used for CRL distribution as solution for the size problem, it would result in higher latencies, what would also impact in the revocation data validity. Consequently, a solution not requiring the distribution of the full CRL from RSUs to OBUs, like the one proposed in this work, would be very helpful for the secure and efficient operation of VANETs.

In particular, to improve efficiency of communication and computation in the management of revoked public-key certificates in VANETs, some authors have proposed the use of particular ADSs such as Merkle trees [12] and skip lists [6] [9]. However, to the best of our knowledge no previous work has described in detail the use of k-ary trees in general as ADSs for the management of certificate revocation.

In general, a hash tree is a tree structure whose nodes contain digests that can be used to verify larger pieces of data [13]. The leaves 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. Hash trees usually require the use of a cryptographic hash function in order to prevent collisions. Most implementations of hash trees are binary, but this work proposes the use of the more general structure of k-ary trees because when combining it with a particular choice of cryptographic hash function, it is possible to optimize the update of the hash tree.

This paper proposes the use of a new version of Keccak as cryptographic hash function in the hash tree. Keccak is the cryptographic hash function used in the new SHA-3 standard [17]. The requirements set by NIST for SHA-3 candidates included classical security properties of hash functions, such as collision resistance, preimage resistance and second preimage resistance [1]. Different types of implementations of SHA-3 fi-

nalists have been evaluated in several works [7] [2], obtaining in most cases positive conclusions. The original SHA-3 uses a sponge construction [3], which in a cryptographic context is an operating mode on the base of a fixed length transformation and a padding rule. Instead of it, this paper proposes a duplex construction [4]. The main advantage of the duplex construction is that it provides digests on the input blocks received so far. This benefit is applied in the proposal here described so that the hash tree is constructed efficiently.

3 Tree-based Module of the Proposal

The scheme described in this paper is based on using as ADS a k-ary tree, which is a rooted tree where each node has no more than k children. The use of k-ary hash trees instead of binary trees allows increasing efficiency of the construction and update of hash trees, as we will see later. Specifically we propose the use of a perfect k-ary tree in which all leaf nodes are at the same depth. Thus, one of the major drawbacks of ordered tree structures, which is the necessary restructuring when there are changes in the tree, only occurs when the perfect k-ary tree requires a new level of depth, because otherwise the nodes simply are inserted from left to right to complete each level of depth. In this way, our proposal is based on a dynamic tree-based data structure that varies depending on the number of revoked certificates.

In the proposed scheme, the bandwidth cost of sending the new versions of the CRL tree from the CA to the OBUs is significantly reduced because only nodes in the tree that have changed need to be updated. This implies a significant improvement with respect to previous tree-based schemes for revoked certificate management because one of their main problems is the necessary update of the entire hash tree every time a new leaf node is added or an existing leaf node is deleted.

The authenticity of the used hash tree structure is guaranteed thanks to the CA signature of the root. The procedure to follow when the part of the CRL tree that is necessary for authenticity verification is pushed from an RSU to an OBU after this latter queries the first one about a certificate, is as follows. If the RSU finds the digest of the certificate among the leaves of the tree because it is a revoked certificate, then the RSU sends to the OBU the route from the root to the corresponding leaf, along with all the siblings of the nodes on this path. After checking all the digests corresponding to the received path and the CA signature of the root, the OBU gets convinced of the validity of the evidence on the revoked certificate received from the RSU.

The proposed model is based on the following notation:

- h: Cryptographic hash function used in the hash tree.
- D (≥ 1): Depth of the hash tree.
- d ($< D$): Depth of an internal node in the hash tree.
- s: Number of revoked certificates.
- RC_j ($j = 1, 2, ..., s$): Serial number of the $j - th$ Revoked Certificate.
- N_{ij} ($i = D - d$ and $j = 0, 1...$): Internal Node of the hash tree obtained by hashing the concatenation of all the digests contained in its children.
- N_{0j} ($j = 0, 1...$): Leaf node of the hash tree containing $h(RC_j)$, ordered according to revocation.

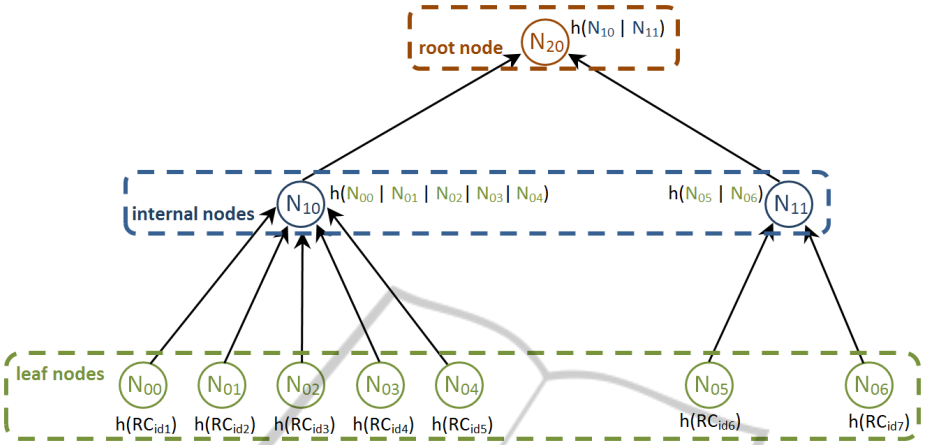

Fig. 1. Hash tree based on a perfect 5-ary tree.

- k: Maximum number of children for each internal node in the hash tree.
- f: Keccak function used in SHA-3.
- n: Bit size of the digest of h, which is here assumed to be the lowest possible size of SHA-3 digest, 224.
- b: Bit size of the input to f, which is here assumed to be one of the possible values of Keccak, 800.
- r: Bit size of input blocks after padding for h, which is here assumed to be 352.
- c: Difference between b and r, which is here assumed to be as in SHA-3, $2n$, that is 448.
- l: Bit size of output blocks for building the digest of h, which is here assumed to be lower than r.
- m: Bit size of input message blocks for the AE scheme.

Regarding the cryptographic hash function h used in the hash tree (see Figure 1), our proposal is based on the use of a new version of the Secure Hash Algorithm SHA-3. In SHA-3, the basic cryptographic hash function f called Keccak contains 24 rounds of a basic transformation and its input is represented by a 5×5 matrix of 64-bit lanes. In contrast, our proposal is based on 32-bit lanes. Another proposed variation of SHA-3 is the use of a duplex version of the sponge structure of SHA-3. 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 and data bit rate r. 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). Thus, the use of the duplex construction in the proposed hash tree allows the insertion of a new revoked certificate as new leaf of the tree by running a new iteration of the duplex construction only on the new revoked certificate. 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 one of those digests so that the total size of the resulting digest of all the children remains the same, n. This

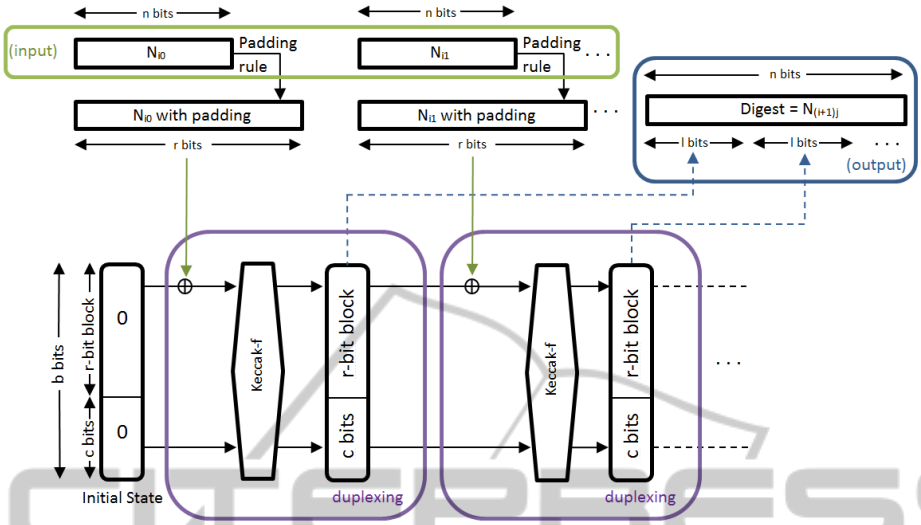

Fig. 2. Proposed duplex construction.

proposed procedure makes the hash tree construction more efficient than previous tree-based schemes when a new leaf corresponding to a new revoked certificate has to be added to the tree.

Note that, while the maximum number of children of an internal node has not been reached, the RSU has to store not only all the digests of the tree structure 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.

On the other hand, periodic delete operations of certificates that are in the tree and reach their expiration date, require rebuilding the part of the tree involving the path from those nodes to the root. Thus, in order to maximize our proposal, such tree rebuilding is proposed to be linked to the moment when all the sibling nodes of some internal node expire because this avoids unnecessary reductions of the system efficiency by having to rebuild the tree very often.

The choice of adequate values for the different parameters in our proposal must be done carefully, taking into account the relationships among them. In particular, since the maximum tree size:

$$n(1 + k + k^2 + k^3 + \cdots + k^D) = \frac{n(k^{(D+1)}-1)}{k-1}$$

is upperbounded by the size of available memory in the RSU, and the maximum number of leaves of the k-ary tree k^D is lowerbounded by the number of revoked certificates s, both conditions can be used to deduce the optimal value for k.

4 Authenticated Encryption Module of the Proposal

In our proposal, the used k-ary tree structure assigns a unique identifier to each revoked certificate to represent it in in order in each one of its leafs. Consequently, an auxiliary

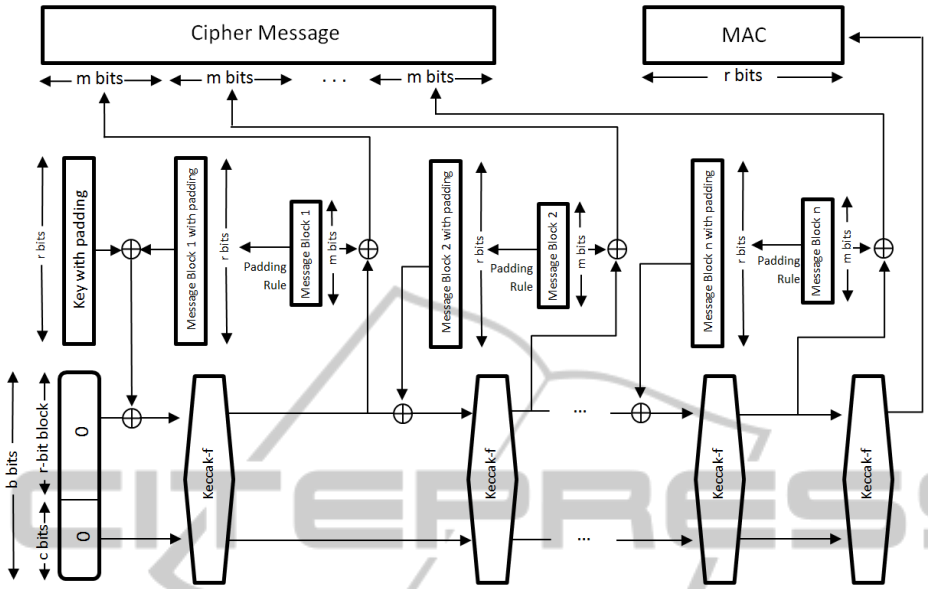

Fig. 3. Proposed authentication encryption.

structure linking such identifiers with the corresponding certificate serial number must be also stored in the RSU. Thus, when an OBU sends a request about a certificate, the RSU first gets from such structure the identifier generated by the k-ary tree structure by using the certificate serial number. Then it can proceed with the tree search.

In order to allow the ordered insertion of revoked certificates in the tree, the aforementioned auxiliary structure may be defined as a hash table (data structure used to implement an associative array mapping keys to values), or any other structure having a quick and efficient way to return the order value required for the search in the tree. This structure is first generated by the CA and then sent to all RSUs so that they can properly perform searches. Since the information contained in this structure is sensitive, it is necessary to ensure its authenticity, integrity and privacy along the communication between CA and RSUs. To achieve this, the use the authenticated encryption is here proposed. AE can be defined as an operation that simultaneously provides confidentiality, integrity and authenticity on the input data.

Many specialized authenticated encryptions have been proposed based on block ciphers. However, authenticated encryption can be generically constructed by combining an encryption scheme with a Message Authentication Code (MAC), provided that the encryption scheme is semantically secure under chosen plaintext attack and the MAC function is unforgeable under chosen message attack.

Here we propose the use of AE under the Output FeedBack (OFB) mode that applies a block cipher as a synchronous stream cipher. Specifically, we suggest an adaptation of the scheme proposed in [4], which combines a cipher-block chaining mode encryption with a duplex construction in a new mode of authenticated encryption (see Figure 3). The CA applies the proposed AE to encrypt and authenticate the auxiliary structure containing the unique identifiers of the revoked certificate and the corresponding tree

identifiers, when sending it to the RSUs in order to protect its integrity, authenticity and confidentiality.

5 Conclusions and Future Works

One of the most important security issues in VANETs is the problem of management of revoked certificates, because efficient verification of public-key certificates by OBUs is crucial in order to ensure the safe operation of the network. This paper proposes an alternative solution to CRL distribution, which uses authenticated data structures based on dynamic k-ary trees. In particular, the proposed mechanism applies the basic hash function of the new SHA-3 standard called Keccak combined with a duplex construction. Thanks to the structure of the used k-ary tree, the duplex construction allows taking advantage of the digests of previous revoked certificates for calculating the hash of every new revoked certificate, so that its inclusion in the tree can be performed by a single iteration of the hash function. Consequently, the whole process is more efficient. This work also includes the description of a new authenticated encryption scheme to ensure integrity, authenticity and privacy of the auxiliary structure linking the tree identifier with the corresponding certificate serial number, when such a structure is sent from the CA to the RSU. A complete analysis of optimal values for the parameters, a performance comparison with previous proposals, and the evaluation of practical and measurable outcomes obtained from the implementation of the proposal both on VANET devices and on Android and iOS smartphones are part of work in progress.

Acknowledgements

Research supported by the Spanish MINECO and the European FEDER Funds under projects TIN2011-25452 and IPT-2012-0585-370000, and the FPI scholarships BES-2009-016774 and BES-2012-051817.

References

1. E. Andreeva, B. Mennink, B. Preneel, M. Skrobot, Security analysis and comparison of the SHA-3 finalists BLAKE, Grostl, JH, Keccak, and Skein. Progress in Cryptology-AFRICACRYPT, pp. 287-305, 2012.
2. K. Aoki, K.Matusiewicz, G. Roland, Y. Sasaki, M. Schlffer, Byte Slicing Grstl: Improved Intel AES-NI and Vector-Permute Implementations of the SHA-3 Finalist Grstl, International Conference on E-Business and Telecommunications, pp. 281-295, 2012.
3. G. Bertoni, J. Daemen, M. Peeters, G. Van Assche, Keccak sponge function family main document version 2.1, Updated submission to NIST (Round 2), 2010.
4. G. Bertoni, J. Daemen, M. Peeters, G. Van Assche, Duplexing the Sponge: Single-Pass Authenticated Encryption and Other Applications, Selected Areas in Cryptography, pp. 320-337, 2011.
5. S. Chang, R. Perlner, W. Burr, M. Turan, J. Kelsey, S. Paul, L. Bassham, Third-Round Report of the SHA-3 Cryptographic Hash Algorithm Competition, http://nvlpubs.nist.gov/nistpubs/ir/2012/NIST.IR.7896.pdf, 2012.

6. C. Ganan, J. Munoz, O. Esparza, J. Mata-Diaz, J. Alins, Toward Revocation Data Handling Efficiency in VANETs, Communication Technologies for Vehicles, Lecture Notes in Computer Science 7266, pp. 80-90, 2012.
7. X. Guo, M. Srivastav, S. Huang, D. Ganta, M.B. Henry, L. Nazhandali, P. Schaumont, ASIC implementations of five SHA-3 finalists. IEEE Design, Automation and Test in Europe Conference and Exhibition, pp. 1006-1011, 2012.
8. IEEE 1609.3-2010 Standard for Wireless Access in Vehicular Environments (WAVE) - Networking Services. Amendment 1 to Version 2. http://www.standards.its.dot.gov/Standard/406, 2012.
9. M. Jakobsson, S. Wetzel, Efficient attribute authentication with applications to ad hoc networks, ACM international workshop on Vehicular ad hoc networks, pp. 38-46, 2004.
10. D. Jiang, L. Delgrossi, IEEE 802.11 p: Towards an international standard for wireless access in vehicular environments, IEEE Vehicular Technology Conference VTC Spring, pp. 2036-2040, 2008.
11. A. J. McMichael, The urban environment and health in a world of increasing globalization: issues for developing countries. Bulletin of the World Health Organization 78(9), pp. 1117-1126, 2000.
12. R. C. Merkle, Protocols for public key cryptosystems. IEEE Symposium on Security and privacy 1109, pp. 122-134, 1980.
13. R. C. Merkle, Method of providing digital signatures. U.S. Patent No. 4,309,569, 1982.
14. J. Molina-Gil, P. Caballero-Gil, C. Caballero-Gil, Enhancing Cooperation in Wireless Vehicular Networks, International Workshop on Security in Information Systems, pp. 91-102, 2011.
15. M. Naor, K. Nissim, Certificate revocation and certificate update. IEEE Journal on Selected Areas in Communications 18(4), pp. 561-570, 2000.
16. P. Papadimitratos, L. Buttyan, T. Holczer, E. Schoch, J. Freudiger, M. Raya, Z. Ma, F. Kargl, A. Kung, J.-P. Hubaux, Secure vehicular communications: Design and architecture. IEEE Communications Magazine 46(11), pp. 28, 2008.
17. V. Rijmen, Extracts from the SHA-3 Competition, Selected Areas in Cryptography, pp. 81-85, 2013.