Archives of
Transport System
Telematics

Volume 7

Issue 2

May 2014

# Safety solutions for mobile nodes authentications in vehicular networks in applications of intelligent transportation systems

**M. FRANEKOVÁ[a], J. ĎURECH[a], P. LŰLEY[a]**

[a] UNIVERSITY OF ŽILINA, Department of Control and Information Systems, Faculty of Electrical Engineering, Univerzitná 8215/1, 010 26 Žilina, Slovakia

EMAIL: maria.franekova@fel.uniza.sk

## ABSTRACT

Applications of VANET (Vehicular ad hoc Networks) networks is focused on monitoring of the safety states of vehicles or roadway by exchanging messages between vehicles and infrastructure so that the applications will be able to help a driver to handle insecure situations. They are able to warn before possible risks which can occur during the process of transportation. Essential tool for assuring of safety communications within developed applications of intelligent transportations systems are cryptography constructions on the basis of digital signature schemes. In order to assuring safety and anonymity within vehicular communications are used pseudorandom authentications methods. The authors in the paper are focused on realization of mathematical model and description of modified cryptographic constructions which are suitable for sensor networks and applications orientated to memory and performance. In these systems it is very important to use signature scheme which do not have only computational safety but must also be effective from the view of performance and must generate short digital signatures in order to communications in real time conditions.

**KEYWORDS: intelligent transportation system, vehicular networks, applications focused on safety, mobile nodes, authentication, modified cryptography construction, mathematical model**

## 1. Introduction

In the question of communication safety for the network VANET (Vehicular Ad-hoc Networks) are applicable similar principles as for other wireless networks. The main safety requirements for communication between vehicles C2C and between vehicles and infrastructure C2I are [1]:

- Authentication of the message and its integrity – protection of the message in order not to allow its modification, possibility of identifying the sender.
- Non-repudiation of the message – the sender cannot deny that he sent the message.
- Timeliness of the message – the receiver can be sure that the message is actual and was generated within the specified interval.
- Access control – a decision which nodes in the network can perform them assigned actions.
- Confidentiality of the message – preservation of the message content from unauthorized parties.

Within the authorized communication between vehicles (Fig. 1) was established the technique of digital signatures based on asymmetric cryptography using PKI (Public Key Infrastructure)

which assumes the existence of a CA (Certificate Authorities). To fulfil the requirements of for a digital signature it is required in addition to the cryptographic solution of the schemes of digital signatures (selection of computationally secure cryptographic solutions) take into account also the implementation of the proposed schemes, the issues related to the keys management, the time stamps and similar issues.

In order to implement digital signatures for downloading of secure software to in-vehicle networks the issuer of the software signs the program code [2]. The control unit in the vehicle verifies the signature. It is suggested six steps from generating the code up to securely downloading it to the control unit. In the first step the code will be generated and then passed to a trust center in the second step. In the third step the code is signed by trust center's secret key, passed back and attached to the program object code. Afterwards, in the fourth step the code is stored in a database. The code can now be downloaded to the appropriate control unit. Finally ECUs can verify the authenticity of downloaded software by using their public keys which are stored in the ECUs (step 6). Fig. 1 shows the procedure in more detail.

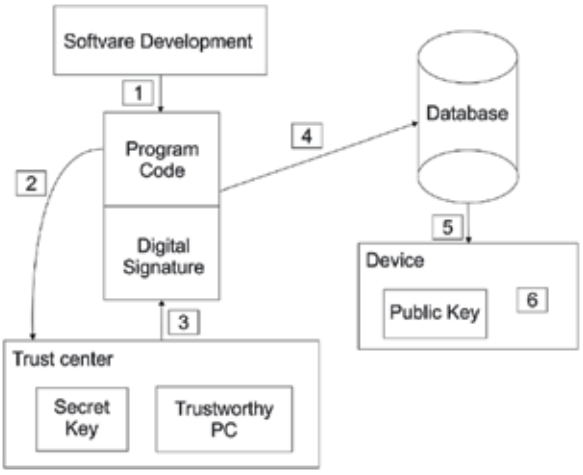


**Fig. 1. Implementation of digital signatures for downloading of secure software [own study]**

Signature verification can be realized in deterministic scheme (using RSA algorithm), respectively in non-deterministic schemes (with El Gamal or ECC algorithms). Cryptography based on elliptic curves ECC is a new promising direction in modern asymmetric cryptography. Its main advantage compared with existing cryptographic schemes and algorithms is the possibility to obtain the same security with shorter key length. Although RSA algorithm is still computationally secure cipher according to [3] the development in computing capabilities of modern information technology is resulting in the inevitable raise in the key length (N module) needed to maintain the required security. Current 1024 bit RSA key standard is according to GISA (German Information Security Agency) inadequate. Since 2006 is recommended to use 2048 bit key. The fact that most of the current chips do not handle keys longer than 1024 led to searching for alternative solutions in the field of cryptography with public key and EEC is such an alternative.

ECC system is based on algebraic structure of elliptic curves over finite fields and its security is based on the very difficult solvability of some mathematical problems. For protocol based on elliptic curves is assumed that finding the discrete logarithm of an element of elliptical curve is in real time practically impossible. The size of elliptical curves determines the difficulty of the problem. It is assumed that to obtain the same level of security as for RSA systems is possible to use smaller group. The use of small group reduces requirements for storage and transmission.

Currently the main problem of implementation of ECC is the lack of standardization. There exist only one way to implement RSA but many methods for ECC (as it will be seen from the description of ECC algorithm). This creates problems in the question of internal operability. While IEEE only described different implementation ANSI identified ten types of elliptic curves and recommended them to use.

## 2. Mathematical principles of computationally secure solutions of digital signature schemes

Digital signature is from the cryptographic perspective understood as a set of cryptographic functions that provide following features:

- Identification – signature must always be tied to particular person who created it.
- Authentication – the process of ensuring some degree of certainty that a given entity is actually that entity which it says it was.
- Integrity – the process by which is ensured that the message was not changed during the transmission from sender to recipient.
- Non-repudiation – signing entity cannot deny that it created the signature of the message.

From the perspective of the cryptography are the schemes of digital signatures in the practice almost exclusively realized using of asymmetric cryptography (public key system) and hash functions. Digital signature scheme consist of two parts: the signature generation and the signature verification. When generating keys in schemes of digital signature it is necessary to have a large amount of random numbers. For this purpose are used generators of pseudorandom numbers PRNG (Pseudorandom Noise Generator). Randomness of the PRGN outputs can be verified by various methods. Such methods are for example defined in American standard FIPS 140-2 [4].

In VANET type network was established for the signature verification ECDSA scheme which is still under development and is modified also with connection to effective implementation of ITS systems.

ECDSA is algorithm defining procedures and rules for creating of digital signature on the basis of ECC elliptic curves algorithm. It is analogous to the DSA algorithm, which means it uses a non-deterministic approach of digital signature creation as

shown in DSS standard. Security of ECDSA algorithm depends as well as encryption using elliptical curves on discrete logarithm problem solving. This problem is known as the ECDLP (Elliptic Curve Discrete Logarithm Problem).

## 2.1 Description of ECDLP problem

First let's explain what we understand by rank of elliptic curve and rank of point P. Rank of elliptic curve E is understood as the total number of points on this curve (referred to #*E*). Rank of point P is understood the smallest integer *n*, covered by *nP*=*O*, *where O* is the zero point.

The ECDLP problem is based on the following task:

- It is given elliptic curve *E* over finite field. Point *P* is an element of *E*.
- It is given such point *Q* for which applies $Q = xP$, where *x* is less than the rank of point *P* (applies $1< x < n-1$).
- The task is to determine (analogous to for DSA algorithm) the value of *x*, with the difference that the operation of exponentiation $g^x$ is changed to operation of multiplication $x.P = P+P+P+...+P$.

Analogy of operations in DSA algorithm and ECDSA algorithm is shown in Table 1.

**Table 1. Analogy of operations in DSA and ECDSA scheme of digital signature [own study]**

| Rank of group | DSA | ECDSA |
|---|---|---|
| Elements of rank of group | Whole numbers {0,1,2,...(p-1)} | Points x, y) of $E_p$(a, b) plus point O |
| Operation of group | Multiplication mod p | Addition of points |
| Entry | Elements g ,y<br>Multiplication g.y<br>Inversion $g^{-1}$<br>Dividing g/y<br>Exponentiation $g^x$ | Points P,Q<br>Addition P+Q<br>Opposite point –P<br>Subtract P-Q<br>Multiplication d.P |
| Problem of discrete algorithm | To find x for a given y, g $\in Z_p$ for which applies $y = g^x \bmod p$ | To find x for a given y, g $\in Z_p$ for which applies $y = g^x \bmod p$ |

## 2.2 Parameters of ECDSA scheme

Public parameters of ECDSA system may be disclosed and the safety is not compromised. The problem may occur if the same parameters are shared by several users together. In the event that these parameters are used to generate k different keys the difficulty of braking the keys decrease to the level of breaking k multiple the time necessary for braking a single key.

If is during the generation of random values used a pseudo-random generator PRNG it is possible to store the private key together with initialization value of PRNG generator (so called seed), due to later verification of generated parameters. For the protection of seed value applies the same rules as for the protection of the private key.

According to ANSI X9.62 standard it is allowed to choose ECDSA parameters for three kind of elliptic curves:

- elliptic curve over the finite field $F_p$, where *p* is an odd prime number,
- elliptic curve over the finite field $F_{2m}$,
- Koblitz curves.

Currently, in the field of automotive industry there are developed other effective solutions that are part of VPN networks, IPsec and TSL protocols. Some types of currently computationally secure elliptic curves are shown in Table 2 [5].

**Table 2. Examples of computationally secure elliptic curves [5]**

| Curve/Shape | Equation |
|---|---|
| Curve1174 Edwards | x^2+y^2 = 1-1174x^2y^2 |
| Curve25519 Montgomery | y^2 = x^3+486662x^2+x |
| BN(2,254) short Weierstrass | y^2 = x^3+0x+2 |
| NIST P-256 short Weierstrass | y^2 = x^3-3x+41058363725152142129326129780047268409114441015993725554835256314039467401291 |
| secp256k1 short Weierstrass | y^2 = x^3+0x+7 |
| E-382 Edwards | x^2+y^2 = 1-67254x^2y^2 |
| M-383 Montgomery | y^2 = x^3+2065150x^2+x |
| Curve383187 Montgomery | y^2 = x^3+229969x^2+x |
| brainpoolP384t1 short Weierstrass | y^2 = x^3-3x+19596161053329239268181228455226581162286252326261019516900162717091837027531392576647644262320816848087868142547438 |
| NIST P-384 short Weierstrass | y^2 = x^3-3x+27580193559959705877849011840389048093056905856361568521428707301988689241309860865136260764883745107765439761230575 |
| Curve41417 Edwards | x^2+y^2 = 0.1+3617x^2y^2 |
| Ed448-Goldilocks Edwards | x^2+y^2 = 1-39081x^2y^2 |
| M-511 Montgomery | y^2 = x^3+530438x^2+x |
| E-521 Edwards | x^2+y^2 = 1-376014x^2y^2 |

# 3. Simulation of ECDSA scheme in SW tools Cryptool

Elliptical curve under real numbers is described by:

$$y^2 = x^3 + ax + b. \quad (1)$$

Definition of elliptic curve contains special point *O*, which represents the point in infinity or null point. Set of points *E*(*a*, *b*) contains all points (*x*, *y*) which satisfy the equation (1) and element *O*. For graphical illustration of elliptic curve is necessary to calculate values according to

$$y = \sqrt{x^3 + ax + b}. \quad (2)$$

If we use different values of couple ($a$, $b$), then we keep different sets of $E(a, b)$, so different elliptic curves. For selected couple ($a$, $b$) graphical relation of elliptic curve contains positive and negative values of $y$ for every value $x$. It means that every elliptic curve is symmetrical to the x-axis. Example of elliptic curve with the parameters a = -1, b = 1, generated in software tool CrypTool [6] is shown in fig. 2.

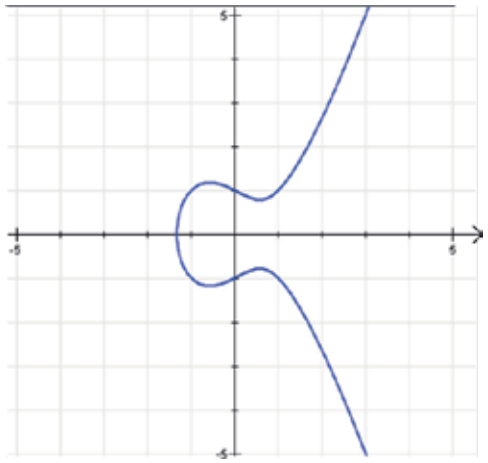


**Fig. 2. Example of elliptical curve $y^2 = x^3-x-1$ [own study]**

## 3.1 Selection of domain parameters

Suppose that all mobile nodes will have only one parameter setting of elliptic curves. This setting will be generated only once and only during the boot key managements KMS (Key Management System). For simulation example has been chosen the finite field GF ($2^m$) with length $m$= 409, which corresponds to the optimal security of 192 bit AES. Furthermore has been selected type of binary elliptic curves and at SW tools CrypTool were generated domain parameters (see fig. 3 and fig. 4) which are in VANET applications subsequently published.

K-409: $m = 409$, $f(z) = z^{409} + z^{87} + 1$, $a = 0$, $b = 1$, $h = 4$
$n$ = 0x 007FFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFE5F 83B2D4EA
20400EC4 557D5ED3 E3E7CA5B 4B5C83B8 B01E5FCF
$x$ = 0x 0060F05F 658F49C1 AD3AB189 0F718421 0EFD0987 E307C84C 27ACCFB8 F9F67CC2
C460189E B5AAAA62 EE222EB1 B35540CF E9023746
$y$ = 0x 01E36905 0B7C4E42 ACBA1DAC BF04299C 3460782F 918EA427 E6325165 E9EA10E3
DA5F6C42 E9C55215 AA9CA27A 5863BEC0 6B8D286B

**Fig. 3. Doman's parameters of Koblitz kurve [own study]**

B-409: $m = 409$, $f(z) = z^{409} + z^{87} + 1$, $a = 1$, $h = 2$
$S$ = 0x 4099B5A4 57F9D69F 79213D09 4C4BCD4D 4262210B
$b$ = 0x 0021A5C2 C8EE9FEB 5C4B9A75 3B7B476B 7FD6422E F1F3DD67 4761FA99 D6AC27C8
A9A197B2 72822F6C D57A55AA 4F50AE31 7B13545F
$n$ = 0x 01000000 00000000 00000000 00000000 00000000 000001E2 AAD6A612
F33307BE 5FA47C3C 9E052F83 8164CD37 D9A21173
$x$ = 0x 015D4860 D088DDB3 496B0C60 64756260 441CDE4A F1771D4D B01FFE5B 34E59703
DC255A86 8A118051 5603AEAB 60794E54 BB7996A7
$y$ = 0x 0061B1CF AB6BE5F3 2BEFA783 24ED106A 7636B9C5 A7BD198D 0158AA4F 5488D08F
38514F1F DF4B4F40 D2181B36 81C364BA 0273C706

**Fig. 4. Doman's parameters for randomly binary curve [own study]**

Where:
$m$ – integer (or prime) for the finite field GF($2^m$)
$f(z)$ – irreducible binary polynomial of degree m determinant representation of the field GF($2^m$)
$S$ – 160-bits input to set SHA-1
$a$, $b$ – two elements according to which is specified equation for the elliptic curve E over the field GF($2^m$)
$n$ – represents a series of curves (number of points on the curve)
$h$ – cofactor of curve (the largest prime number decomposition of points on the curve or its multiple)
$x$, $y$ – coordinates of basis points on the curve $G = (x_G, y_G)$
***Note*:** Domain parameters for elliptic curve we chose as recommended by FIPS 186-3.

## 3.3 Attacks to ECDSA scheme

VANETs are open networks and can be easily accessed by attackers. Due to the introduction and implementation of new technologies, attackers will be strongly motivated to exploit the vulnerabilities of VANETs.

Since the most efficient algorithm known to attack the cryptosystem of elliptic curves is time more demanding than the best algorithms for attacks on other cryptosystems can be simulated solution considered as for computationally secure. Known attacks include Shanks algorithm, Pollard p algorithm, Pohlig-Hellman algorithm, method of base the facts.

The most famous attack is the Pollard p algorithm that requires approximately

$$\sqrt{\frac{\pi n}{2}} \quad (3)$$

steps, where one step corresponds to one counting of points on elliptic curve. Tab. 3 shows the computational demands ECDLP by method Pollard *p*.

**Table 3. Computational demands ECDLP by method Pollard *p* [own study]**

| Size n in bits | $\sqrt{\frac{\pi n}{2}}$ | MIPS years |
|---|---|---|
| 160 | 280 | 9,6 x 1011 |
| 186 | 293 | 7,9 x 1015 |
| 234 | 2117 | 1,6 x 1023 |
| 354 | 2177 | 1,5 x 1041 |
| 426 | 2231 | 1,0 x 1052 |

# 4. Conclusion

In the present the brute force attack to ECC algorithm is computationally unreal (considering to recommended length of keys). But i tis needed regards that except of brute force attracts in the present there have been another attacks not only to key but to algorithm too. From the area of VANET networks there are e. g. Sybil attack, alteration attack, replay attack or Denial of Service (DoS) [2]. Since vehicular networks require real-time

responses, they are vulnerable to denial of service (DoS) attacks mainly. Security characteristic of VANET networks are necessary modelling for selected cryptograph construction scheme [7].

**Acknowledgement**

This work has been particularly supported by the Educational Grant Agency of the Slovak Republic (KEGA) Number: 024ŽU-4/2012: Modernization of technology and education methods orientated to area of cryptography for safety critical applications.

# Bibliography

[1] Car2Car Communication Consortium. In: http://www.car-2-car.org/ (accessed: 20.05.14)

[2] KASRA AMIRTAHMASEBI-SEYED REZA JALALINIA: Vehicular Networks – Security, Vulnerabilities and Countermeasures, University of Gothenburg, Sweden (2010)

[3] ENGE A.: Elliptic Curves and Their Applications to Cryptography – An Introduction. Kluwer Academic Publisher, Boston (2001)

[4] FIPS 140-2: Security Requirements for Cryptographic Modules (2002)

[5] GALLO, P.: Enhanced authentication algorithm based on elliptic curves. PhD thesis, TU Košice (2014)

[6] User guide Cryptool. In: www.cryptool.com (accessed: 20.05.14)

[7] ĎURECH, J., et. al.: Security analysis of cryptographic constructions used within communications in modern transportation systems on the base of modeling. ELEKTRO 2014, Rajecké Teplice, May (2014)