A PERFORMANCE IMPROVEMENT OF ANEL SCHEME THROUGH MESSAGE MAPPING AND ELLIPTIC CURVE CRYPTOGRAPHY

Benyamina Ahmed[1] and Benyamina Zakarya[2],
benyamina.ahmed@univ-bechar.dz benya.zakalg@gmail.com
[1]Department of Mathematics and Informatic, Tahri Mohamed University, Bechar, Algeria
[2]Department of Informatic, Aflou University, Laghouat, Algeria

Summary
The vehicular ad hoc network (VANET) is currently an important approach to improve personal safety and driving comfort. ANEL is a MAC-based authentication scheme that offers all the advantages of MAC-based authentication schemes and overcomes all their limitations at the same time. In addition, the given scheme, ANEL, can achieve the security objectives such as authentication, privacy preservation, non-repudiation, etc. In addition, our scheme provides effective bio-password login, system key update, bio-password update, and other security services. Additionally, in the proposed scheme, the Trusted Authority (TA) can disclose the source driver and vehicle of each malicious message. The heavy traffic congestion increases the number of messages transmitted, some of which need to be secretly transmitted between vehicles. Therefore, ANEL requires lightweight mechanisms to overcome security challenges. To ensure security in our ANEL scheme we can use cryptographic techniques such as elliptic curve technique, session key technique, shared key technique and message authentication code technique. This article proposes a new efficient and light authentication scheme (ANEL) which consists in the protection of texts transmitted between vehicles in order not to allow a third party to know the context of the information. A detail of the mapping from text passing to elliptic curve cryptography (ECC) to the inverse mapping operation is covered in detail. Finally, an example of application of the proposed steps with an illustration

Keywords:
VANET, ANEL scheme, message mapping, elliptic curve cryptography

1. Introduction

The vehicular ad hoc network (VANET) comprises of three significant segments to be specific:

- Trusted Authority (TA) is answerable for the enrollment of RSUs, vehicle OBUs and the vehicle users. What's more, it is likewise answerable for confirming the approval of the identity of OBUs, vehicles, or users so as to stay away from malicious vehicles [1] going into the VANET system, Figure 1. The TA aims for high computing power and adequate storage capacity. The TA can revoke the identity of OBUs because of broadcasting malicious messages or behavior.
- Fixed RSUs are commonly stationary gadgets that are fixed aside the streets or in committed places, for example, stopping spots or street crossing points. Like an OBU, an RSU likewise has a handset, reception apparatus, processor, and sensors. The RSUs are deliberately fixed along the streets to offer administrations to vehicles.
- The On-Board Units (OBUs) mounted on the moving vehicles [2], which are computational tool and transceiver installed on every vehicle to exchange data with RSUs and OBUs of different vehicles. The factors of an OBU are resource command processor (RCP) for computation functionality, examine/write garage for storing and retrieving records, a consumer interface and a DSRC radio primarily based on IEEE 802.11p radio generation to access the wireless channel [3]. OBUs get energy from the car battery. Every vehicle's OBU is associated with a gathering of sensors to accumulate the data, for example, speed, breaking data, and so on. These accumulated data are sent as messages to encompassing vehicles by means of the remote medium.

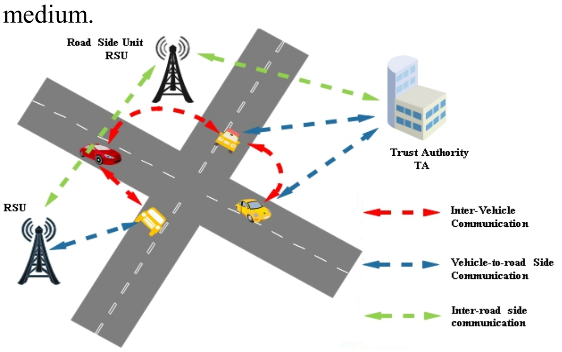

Fig. 1 Vehicular Ad hoc NETwork (VANET) system

All RSUs are interconnected with one another and are thus associated with the Trusted Authority (TA) through a wired connection. The TA has the obligation of keeping up the whole VANET system. Moreover, VANET system must guarantee the privacy of users and protect the communications from various attacks. Therefore, VANET requires security schemes with efficient computation and

Manuscript received March 5, 2023
Manuscript revised March 20, 2023
https://doi.org/10.22937/IJCSNS.2023.23.3.18

communication. However, several researches are proposed to secure the VANET system. One of the researches that play an important role in VANET information security is a novel efficient and lightweight authentication scheme for vehicular ad hoc networks (ANEL) [4].

ANEL consists of eight steps as follows: System Initialization Phase, Registration Phase, Driver Authentication Phase, Message Signing and Verification Phase, Biological Password Update Phase, system key update, vehicle revocation phase and message tracing phase. Initially, the TA computes the parameters that are required in the other phases. Then, all drivers can register themselves by providing their information (like biological password, vehicle identity, phone number, etc.) to the TA office directly. Subsequently, the TA uses this information to configure the TPDs, then sends the configured TPDs to the pilots. Even after the registration, the driver can update the biological password stored in his TPD without contacting the TA. When a driver wants to join VANET, then he first enters his vehicle identity and his biological password through a biometric technology. If the entered information matches the information that is already stored in the TPD, then the TPD allows this driver to join VANET by decrypting the group key that is already stored in it. If a driver dispatch a malicious message, the TA can trace the source biological driver and vehicle of this message, and then revokes them. Although an adversary cannot get the system key stored in TPD even if he steals the vehicle (as shown in security analysis), we perform two system key updating processes (PKU and SKU) to enhance the security of VANET.

In ANEL, the information sent is not encrypted. Then everyone can reveal these messages. Therefore, the disadvantage of ANEL is that it cannot be used on all models. Though, in this research, we improve the ANEL scheme by describing the messages using message mapping and ECC.

The remainder of this paper is organized as follows. Section 2 presents the threat model, then Section 3 contains our proposed scheme. In Section 4, we analyze the security strength of our proposed scheme. Section 5 an example is presented with illustration and Section 6 concludes the paper with future direction.

2. Threat model

We assume that the communication channel is insecure. Which means that a powerful attacker is able to listen and collect the information exchanged. We further assume that the adversary can compromise all RSUs and steal the on-board units of certain vehicles, and then obtain as much secret information from them as possible. We also consider the situation where an adversary with high computing power and communication capability can leak sensitive information using a brute force attack with the best case scenario for an attacker or by other means. We also summarize the most common attacks to decrypt a secret key in ECC under ANEL:

1- Message modification and generation attack

In this attack, an unauthorized user may generate fraudulently a valid message or modify the content of the exchanged message or some part of it to be transmitted and thus produce unauthorized effect [4].

2- known-plaintext attack (KPA)

Where the attacker has access to both the plaintext, and its encrypted version (ciphertext) [14,17].

3- Chosen-plaintext attack

Which presumes that the attacker can obtain the ciphertexts for arbitrary plaintexts [5,14,17].

4- Collision attack

A collision attack on a cryptographic hash tries to find two inputs producing the same hash value, i.e. a hash collision[14,17].

5- Man-in-the-middle attack

The attacker secretly relays and possibly alters the communications between two parties who believe that they are directly communicating with each other, as the attacker has inserted themselves between the two parties [14,17].

6- Chosen ciphertext attack

Is an attack which the cryptanalyst gathers information, by choosing a ciphertext and obtaining its corresponding plaintext [14,17].

3. The proposed scheme

The proposed encryption scheme is based on text mapping, elliptic curve cryptography (ECC) and the inverse mapping operations.

ECC was discovered in the year 1985 by Neal Koblitz and Victor Miller [6,17]. ECC schemes are shared-key mechanism similar to RSA and other primitive algorithms. ECC is an attractive shared key cryptosystem for resource-constrained devices because compared with traditional cryptosystems like RSA/DH, it offers equivalent security with smaller key sizes, faster computation, lower power consumption, and memory and bandwidth savings [7]. Cryptographic algorithms based on Diffie Helman [8,9,11] and ElGamal algorithm can be efficiently implemented using elliptic curves.

Unlike standard shared-key methods that operate over integer fields, the elliptic curve cryptosystems operate over points on an elliptic curve. Similar to other shared key cryptosystem, the security level of ECC also depends on the sizes of the keys used [10,17]

Before using ECC scheme in such a way that if one has to encrypt a message, then we attempt to map the message to some distinct point on the elliptic curve by modifying the message using a mapping algorithm [14,17,18]. Although the arithmetic involved in elliptic curve cryptography is computationally less complex than other cryptographic algorithms.

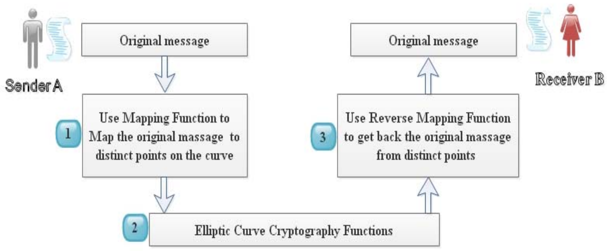

Fig. 2 Pictorial illustration of mapping and reverse mapping in elliptic curve cryptography (ECC).

3.1 Mapping and reverse mapping in Elliptic curve cryptography

The hassle with ECC is that it offers with (x, y) coordinates only, whereas messages that are despatched commonly consists of alphabets, numbers, and symbols. In ECC, a factor P_m is encrypted to a pair of factors $C_m(C_1, C_2)$ on the curve. But the vicinity of situation lies in the technology of factor P_m from plaintext message M [14,18,19].

The manner of technology of factor P_m from plaintext message M is acknowledged as mapping. Our center of attention ought to no longer solely be restricted to mapping the message however it ought to additionally make certain that after the receiver decrypts C_m, he can acquire again the unique message M from P_m. This system is recognized as reverse mapping. The total process is illustrated in Figure 2.

The scheme is primarily based on grouping the characters of the message and mapping it. We will take M characters at a time and map it.

3.1.1 Mapping algorithm

Algorithm 1: Mapping Algorithm [14,18,19]

Input: Message consisting of characters belonging to extend ASCII set.

Output: Distinct points *(X,Y)* on the Elliptic curve $E_p(a,b)$ to the Message.

Steps of the algorithm

Step 1: Begin

Step 2:

a: Consider *M* characters of the message at a time

b: Convert each character into 8-bits ASCII codes

c: Insert each 8-bits binary number into an array of length *M* + 8 bits

Step 3: Append N 0's at the end of array

Step 4: Extract the (*M* * 8 + *N*)-bits number from the array, convert it to a decimal number, and store it in *X*

Step 5:

a: Find Y from the equation Y2≡X3+aX+b mod p

b: If Y does not have a solution increment *X* by 1 and go to step 5a

Step 6: After obtaining Y use the distinct point *(X,Y)*for encryption using ECC ?

Step 7: Repeat step 2 to step 6 until the end of message

Step 8: End

3.1.2 Reverse mapping algorithm

Algorithm 5: Reverse Mapping Algorithm [14]

Intput: Distinct points *(X,Y)* on the Elliptic curve $E_p(a,b)$.

Output: Original message sent by sender. Steps of the algorithm

Step 1: Begin

Step 2: Ignore 'Y' coordinate

Step 3: Convert 'X' coordinate into binary number and ignore the last N bits

Step 4: Extract the rest of the bits and put it in a bit array

Step 5: Start from the right most bit. Consider 8 bits from the array at a time this 8- bit is nothing but the original alphanumeric ASCII character which formed the original plaintext. Repeat this step until M characters are retrieved item

Step 6: Repeat the earlier steps for each cipher point pair sent by the sender

Step 7: End

3.2 Elliptic Curve Cryptosystem

The Message Map that each elliptic curve is no longer beneficial in cryptography.

It is essential to comprehend what kind of elliptic curve is beneficial in Cryptography.

The elliptic curves that shape cyclic organizations and the elliptic curve factor that generates all the factors of the cyclic subgroup are beneficial in cryptography. Cryptography based totally on Elliptic curve is recognized as Elliptic curve cryptography (ECC) [16,17].

We all know that smaller key size, faster computational ability makes ECC too important to be ignored even in the era of transition from classical cryptography to quantum cryptography.

Table 1 shows recommended bit lengths for shared-key algorithms for the four security levels 80, 128, 192 and

256 bit. We see from the table that RSA-like schemes and discrete-logarithm schemes require very long operands and keys. The key length of elliptic curve schemes is significantly smaller, yet still twice as long as symmetric ciphers with the same cryptographic strength [17].

A 384-bit ECC key is roughly equal to a 7680-bit RSA, DSA, Diffie Helmann or Elgamal keys for example.

Table 1: Bit lengths of shared-key algorithms for different security levels [17]

Plaintext message	Cryptosystems	Security Level (bit)			
		80	128	192	256
Integer factorization	RSA	1024 bits	3072 bits	7680 bits	15360 bits
Discrete logarithm	DH, DSA, Elgamal	1024 bits	3072 bits	7680 bits	15360 bits
Elliptic curves	ECC (ECDH, ECDSA)	160 bits	256 bits	384 bits	512 bits

ECC states that if there exists an elliptic curve E defined over a finite field Fp, two point P,Q $\in$ E(p), then it is very difficult to find the integer k such that Q = kP. Elliptic curve cryptography consists of three distinct operations: key generation, encryption, and decryption [6,12,13,15]. These three operations are very much required to formulate a valid cryptosystem.

In ECC, the message is mapped to a valid point P_m on the curve. The message point P_m is then encrypted, and we obtain a pair of cipher points C_m. Subsequently, this C_m is decrypted to obtain back the original message point P_m. The total process is illustrated below in Figure 3.

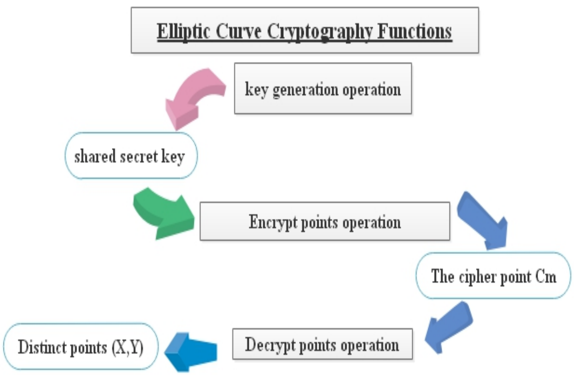

Fig. 3 Elliptic curve cryptography (ECC) functions

3.2.1 key generation operation

In this section, we will discuss the Diffie–Hellmann key generation operation on elliptic curves.

The Elliptic Curve Diffie- Hellmann (ECDH) [11] protocol is a secret key generation protocol between two distant parties Sender A and Receiver B and the secret key is one of the point on the elliptic curve. For the key generation operation, we need a point G, also called as the generator point. The order of G is always equal to the order of the elliptic curve group Ep(a, b) where a, b are elliptic curve parameters and p is a large prime integer. A large integer nB (nB < p) is kept as the Private Key, and the point PB = nB * G is declared as shared. It is to be noted that the information about the elliptic curve Ep (a, b) and the corresponding generator point G has to be made shared also. Otherwise, the encryption would not be possible [16,17].

Algorithm 2: key generation Algorithm

Intput: G point on the Elliptic curve $E_p(a,b)$.
Output: Shared P_A, P_B and Secret key K:
Step 1: Begin
Select Secret key n_A (n_A<n)
Calculate Shared key P_A: $P_A=n_A * G$
Select Secret key n_B (n_B<n)
Calculate Shared key P_B: $P_B=n_B * G$
Calculation of Secret key Sender A:
$K = n_A * P_B$
Calculation of Secret key Receiver B:
$K = n_B * P_A$
Step 2: End

3.2.2 Encryption operation

For encryption, the sender chooses a random positive integer k (k < p). He then uses the shared key P_B to generate the cipher point C_m that consists of two points [16,17].

The cipher point C_m is given by $C_m = [\{k * G\}, \{P_m +(k * P_B)\}]= [C_1,C_2]$.

The sender then sends the pair of cipher point C_1 and C_2 (both together C_m) to the receiver.

The receiver upon receiving the cipher point pair C_m multiplies the first point in the pair by its own secret or private key and subtracts the result from the second point as shown in the following.

Algorithm 3: Encrypt

Input: G point on the Elliptic curve $E_p(a,b)$ to the Message.
Output: The cipher point C_m
Step 1: Begin
Step 2: $C_1= k * G$
$C_2= P_m + (k * P_B)$
$C_m= [C_1, C_2]$.
Step 3 End

3.2.3 Decryption operation

The receiver upon receiving the cipher point pair C_m multiplies the first point in the pair by its own secret or private key and subtracts the result from the second point [16,17].

Algorithm 4: Decrypt

Input: The cipher point C_m.

Output: Distinct points *(X, Y)* on the Elliptic curve $E_p(a,b)$.
Step 1: Begin
Step 2: choose a random positive integer k (k<p)
$P1 = k * G * n_B$
$P2 = P_m + (k * P_B) - P1$
$P2 = P_m + K * P_B - (K * G * n_B)$.
//We know that: $P_B = n_B * G$
$P2 = P_m + K * n_B * G - (K * G * n_B)$
$P2 = P_m$
Step 3 End
The receiver gets the same point

3.2.4 Elliptic curve using proposed message mapping scheme

The total process of our proposed model consists of the following phases [14,19]:
- mapping,
- key exchange,
- elliptic curve encryption and decryption
- reverse mapping, takes place as described in the following:

- At the sender side:

Step 1: The value of N is taken as 8 bits.
Step 2: Select a value of M that satisfies equation $M \leq \left[\frac{p-8}{8}\right]$.
The value of M depends on the sender. In general, the sender must select large value of M as discussed in Section 4.
Step 3: Apply mapping algorithm for every M characters in the plaintext.
Step 4: After obtaining Pm for every M characters, apply ECC to obtain pair of cipher points C_m.
Step 5: Send C_m's to the receiver.

- At the Receiver side:

Step 1: Decrypt all pair of cipher points (C_m's) to obtain back the distinct points Pm.
Step 2: Consider each Pm = (x, y) at a time.
Step 3: Apply reverse mapping algorithm for each (x, y) coordinate.

4. Security analysis

The message mapping in ECC plays a significant role as it decides how vulnerable the encrypted message is to attacks. We know that the security of ECC depends on the hardness of ECC. But message mapping makes ECC vulnerable to many primitive security attacks. In this section, cryptanalysis based on the primitive cryptographic attacks are discussed [4,14,17].

The proposed ANEL scheme protects against all known cryptographic attacks and enables many security features as described in the following:

4.1 Resilience to message modification and generation attack

If an attacker wants to modify or forge messages in ANEL scheme, he needs to obtain the secret key of the sender, which is $K = n_A * P_B$, but it is infeasible to get it.

Which means ANEL is protected from message modification and generation attack.

4.2 known-plaintext attack (KPA)

The frequency of occurrence is taken into an account to exploit the encryption function. This scheme can map any string of characters belonging to 256 extended ASCII table to distinct points on the elliptic curve. Because we are mapping M characters at a time, we have 256^M pair of distinct cipher points and the chance of repetition of the same string of M characters in the future is $\frac{1}{256^M}$. As the value of M increases, the value of $\frac{1}{256^M}$ decreases.

4.3 Chosen-plaintext attacks

These attacks are effective if the relation between plaintext and ciphertext is one-to-one as this helps in frequency analysis [15]. Although our mapping is one-to-one, it still avoids frequency analysis. The main advantage of this mapping scheme is the difficulty in frequency analysis if M is greater than 4.

Researchers have found that a maximum up to four consecutive character analysis is possible. Unigram count frequency analysis, bigram count frequency analysis, trigram count frequency analysis, and four-gram count frequency analysis are possible but frequency analysis of M consecutive character ($M > 4$) count is practically impossible.

For example, in unigram analysis, the alphabet 'e' appears most frequently followed by the alphabet 't'. Similarly, in bigram analysis, the pair 'th' appears most frequently followed by the pair 'he'. These distributions remain more or less the same when any English phrase is considered. But when we analyze the frequency of M ($M>4$) consecutive characters, the distribution fluctuates and attack using frequency analysis becomes infeasible [15]. Then this attack is infeasible if M is sufficiently large.

4.4 Collision attack

Because hash functions have infinite input length and a predefined output length, there is a possibility of two different inputs that produce the same output hash. If any groups separate inputs produce the same hash output, it is called a collision.

This collision can then be applied by comparing two hashes together. The proposed scheme is a deterministic approach and does not use any hash function, and hence, collision attack will not be successful.

4.5 Man-in-the-middle attack

In the mapping scheme, there is no need to share any information prior to the mapping process. The value of p and N are public and the sender can determine the value of M from the equation $M \le \left\lfloor \frac{p-8}{8} \right\rfloor$. The receiver too does the same. No key or information is shared. Hence, a man in the middle attack would be useless in this case.

4.6 Chosen ciphertext attack

Similar to chosen plaintext attack, this attack is effective if the relation between plaintext and ciphertext is one- to-one. But as shown earlier, frequency analysis of M consecutive characters (M >4) is practically impossible. This kind of attack is also infeasible as frequency analysis is not possible in this method.

5. Example and illustration

In the example we will derive the shared secret key which is used for symmetric encoding with the help of same rule as in Elliptic Curve mentioned above with some modification.

The parameters are:

a = –3

b =
245515554600894381774029391519745178476910805816 1191238065

p =
627710173538668076383578942317605901376719477318 2842284081

we have taken 192-bit key size elliptic curve.

A plaintext message ‘A PERFORMANCE IMPROVEMENT OF ANEL SCHEME THROUGH MESSAGE MAPPING AND ELLIPTIC CURVE CRYPTOGRAPHY’ is taken as input.

In our proposed scheme we attempt to map the original message to some distinct point on the elliptic curve by modifying the message using a mapping algorithm.

Consequently, we apply the ECC until reaching the final phase which is reverse mapping.

5.1 Mapping algorithm:

The proposed mapping scheme discussed earlier produces a (M*8 +N)-bit decimal number after mapping that is later considered to be the x coordinate in E(p). The size of N should be equal to 8 bits and the value M should be less than or equal to |(p–8)/8| [14].

The elliptic curve taken in the example in the following is an NIST recommended curve [15] and abides by the rules of NIST curve.

At the sender side A, we apply the different steps mentioned above in the algorithm.

Step 1: The value of N is taken as 8 bits.

Step 2: We choose a value of M that satisfies the equation M <=|(192–8)/8|. We take M as 23. At a time, every consecutive 23 characters will be mapped to a point on the elliptic curve.

Step 3:

The first 23 characters:

TEXT 01: ‘A PERFORMANCE IMPROVEME’ is considered first.

Converted them to 8-bit ASCII values and put it in an array.

It produces the following bit string:

010000010010000001010000010001010101001001000110010011110101001001001101010000010100111001000011010001010010000001001001010011010101000001010100100100111101010110010001010100110101000101

N = 8, eight zeros are added at the end of this string.

01000001001000000101000001000101010100100100011001001111010100100100110101000001010011100100001101000101001000000100100101001101010100000101001001001111010101100100010101001101010001 01**00000000**

Assign the 192-bit string to an integer X.

The result is:

X =
159689038644910690838134809332258679853208748389 1840795904

Find Y from the equation $Y^2 = X^3 + aX + b \bmod p$. The first iteration will yield no solution of Y. Subsequently, X is incremented by one.

In the second iteration, Y will yield a nonzero value. Pm for the first 23 characters is:

$Y = \text{SQRT}(X^3 + aX + b)$

Calculation of Y with the following equation:

Y^2 = X^3 + aX + b mod p which is:

y^2 = X ^3 + -3 X +
245515554600894381774029391519745178476910805816 1191238065(mod
627710173538668076383578942317605901376719477318 2842284081)

Then :

Pm = (X1, Y1) =
(159689038644910690838134809332258679853208748389 1840795904,
165425439114248076478171068199955887912305227355 5838525895)

Repeat step 3 until all the characters are mapped. Because number of characters is 96, this mapping algorithm will produce three distinct points Pm.
TEXT 02: "NT OF ANEL SCHEME THROU"
Pm = (X2, Y2) =
(19206121250705662423723788072437332891275454590 51296937216,
14277464904362628163512324636982772299263048211 68773584780)
TEXT 03 = "GH MESSAGE MAPPING AND "
Pm = (X3, Y3) =
(17478232499103639097650686769309729213290346944 97331847168,
48932321601694624164050166507158849181212008908 73790304050)
TEXT 04 = "ELLIPTIC CURVE CRYPTOGR"
Pm = (X4, Y4) =
(16991829730591286132091671128802902468073484910 17127416320,
35258170641690463744922313212896752163350656565 10857700864)
TEXT 05 = "APHY"
Pm = (X5, Y5) = (280519792896,
10226921290961543008295035660617859953501826814 29428385746)
Step 4: All five distinct points must be encrypted using ECC to produce a pair of C_m encryption points.

After extracting the set of points from the message to be encrypted, we will move on to the use of the cryptographic elliptic curve algorithm.

Elliptic curve cryptography consists of three distinct operations: key generation, encryption, and decryption [6,12,13].

5.2 key generation Algorithm

Beginning with the first point:
Pm = (X1, Y1) = G =
(15968903864491069083813480933225867985320874838 91840795904,
16542543911424807647817106819995588791230522735 55838525895)
We will therefore convert all the numbers into hexadecimal to simplify the presentations.
Pm = (X1, Y1) =
(0x4120504552464f524d414e434520494d50524f56454d4 500,
0x437738c216d164e60f05511215fcfaec8bbd50910152e1c 7)
A shard key P_A:
0x9b3e91bbe1382011fd5a58dccff8366be85b57bcd6563b7 40
B shared key P_B:
0x87e5f4b46cab0e6a584d200ad7628b59bef710fac99597a 11

Now exchange the public keys (e.g. through ANEL)
A Secret key K:
0x8ab013e531079d8350a5e1c5195de99ebf7e0379e50ceac 30
B Secret key K:
0x8ab013e531079d8350a5e1c5195de99ebf7e0379e50ceac 30
Therefore, the shared keys are equal.

5.3 Encrypt Algorithm

Secret-key k:
0x5fda1afeac3adbb9730706fe48747ba27bdf93b636bf1ac8
Cipher point C1:
C10x9dc170eda3465637a37c6df105d5bd356b31d46532d b44230
Cipher point C2:
0x6e9e33537dfb6c98ce4e0bcd90cbdec02e9fbc581eb1e21 0
Cipher point C_m = (C1, C2)

5.4 Decrypt Algorithm

Cippher point = C_m = (C1, C2) =
(C10x9dc170eda3465637a37c6df105d5bd356b31d46532d b44230,
0x6e9e33537dfb6c98ce4e0bcd90cbdec02e9fbc581eb1e21 0)
Decryption key:
0xc1c14421e0f7331529b6910b237391250cdf5152543193 e70

5.5 Reverse Mapping algorithm:

Cippher point = C_m = (C1, C2) = (X , Y)
(C10x9dc170eda3465637a37c6df105d5bd356b31d46532d b44230,
0x6e9e33537dfb6c98ce4e0bcd90cbdec02e9fbc581eb1e21 0)
Convert to decimal :
(15968903864491069083813480933225867985320874838 891840795904,
11654254391142480764781710681999558879123052273 555838525895)
X =
15968903864491069083813480933225867985320874838 91840795904.
Ignore Y. It is of no use.
Convert X to binary number:
010000010010000001010000010001010101001001000110 01001111010100100100110101000001010011100100001 10100010100100000010010010100110101010000010100 1001001111010101100100010101001101010001 01
Bits are considered at a time from the right and converted

to characters.
The result is: A PERFORMANCE IMPROVEME
Repeat step 2 until all P_m's are reversed mapped and all characters are retrieved.
Note that the total number of characters in the plaintext message is 96 and the mapping algorithm only produces 5 mapped points.
Original plaintext: A PERFORMANCE IMPROVEMENT OF ANEL SCHEME THROUGH MESSAGE MAPPING AND ELLIPTIC CURVE CRYPTOGRAPHY

6. Conclusion

In this article, we have proposed an improvement of the ANEL scheme for security inside VANET. When using the scheme, messages sent between vehicles will go through a secure channel. Indeed, the use of text mapping, elliptic curves and reverse mapping allows the authentication of ANEL.
The example presented shows the simplicity of the proposed model and performs the security operation in an efficient way.

7. References

[1] Ghosh M, Varghese A, Kherani A, Gupta A. Distributed misbehavior detection in VANETs. IEEE Wireless Communications and Networking Conference. IEEE, 2009.
[2] Federal Communications Commission. Amendment of the commission's rules regarding dedicated short-range communication service in the 5.850-5.925 ghz band. https://www.fcc.gov/document/amendment-commissions-rules-regarding-dedicated-short-range accessed January 2022.
[3] Draft guide for Wireless Access in Vehicular Environment (WAVE) Architecture', https://ieeexplore.ieee.org/document/6531627/ accessed January 2022.
[4] Benyamina Z, Benahmed K, Bounaama F. ANEL: A novel efficient and lightweight authentication scheme for vehicular ad hoc networks. Computer Networks 164 (2019): 106899.
[5] Li B, Zhang D, Sun L, Chen C. Hunting or waiting? Discovering passenger-finding strategies from a large-scale real-world taxi dataset. 2011 IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops). IEEE, 2011.
[6] Koblitz N. Elliptic curve cryptosystems. Mathematics of Computation 1987; 48(177): 201–209.
[7] Barreto PSLM, Libert B, McCullagh N, Quisquater JJ. Efficient and provably-secure identity-based signatures and sign encryption from bilinear maps. In Advances in Cryptology – ASIACRYPT 2005, vol. 3788, Lecture Notes in Computer Science. Springer: Chennai, India; 515–532.
[8] Odlyzko AM. Discrete logarithms and their cryptographic significance. In Advances in Cryptology: Proceedings of Eurocrypt 84. Springer-Verlag: New York, 1985; 224–314.
[9] ElGamal T. A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE Transactions *on Information Theory* 1985; IT 31: 469–472.
[10] Pateriya RK, Vasudevan S. Elliptic curve cryptography in constrained environments: a review. *IEEE 2011 International Conference on Communication Systems and Network Technologies*, Bhopal,India, Sep-2011 ; 120–124.
[11] Diffie W, Hellman M. New directions in cryptography. IEEE Transactions on Information Theory 1976; 22: 644–654. DOI:10.1109/tit.1976.1055638.
[12] Hankerson D, Menezes A, Vanstone S. Guide to Elliptic Curve Cryptography. Springer: New York, 2004. ISBN 978-0-387-21846-5.
[13] Rosen K. Discrete Mathematics and Its Applications, 8th edition. McGraw Hill Higher Education: New York 2018. ISBN 10: 125967651X. ISBN 13: 9781259676512.
[14] Sengupta A, Kumar R U. Message mapping and reverse mapping in elliptic curve cryptosystem. Security and communication networks. Security Comm. Networks (2016)
[15] Lewand R. Cryptological mathematics. The Mathematical Association of America 2000, ISBN-13: 978-0883857199.
[16] Monika , Tomar T , Kumar V , Kumar Y . Implementation of Elliptic Curve Cryptography. International Journal of Electrical Engineering and Technology (IJEET), Volume 11, Issue 2, March-April 2020
[17] Christof P, Jan P. Understanding Cryptography: A textbook for Students and Practitioners. Springer-Verlag Berlin Heidelberg 2014. ISBN: 978-3642446498
[18] Muthukuru J, Sathyanarayana B. Fixed and variable size text based message mapping techniques using ECC. Global Journal of Computer Science and Technology 2012; 12(3): 12–18, Version 1.0.
[19] Laiphrakpam D S, Khumanthem M S. Implementation of Text Encryption using Elliptic Curve Cryptography. Procedia Computer Science 54 (2015) 73 – 82. Organizing committee of the Eleventh International Multi-Conference on Information Processing-2015.

Benyamina Ahmed Obtained an engineering degree in computer science from the Senia University of Oran (Algeria) in October 1992 and a Master's degree from the University of Bechar (Algeria) in May 2008. He obtained his doctorate in the field of artificial intelligence from the University of Science and Technology of Oran (Algeria) in April 2013. Currently, he teaches master students in the fields of data analysis and connectionist methods.

Benyamina Zakarya was born in Bechar city, Algeria, in 1991. He received his master degree in computer science from Tahri Mohamed University, Bechar, Algeria, in 2014. He has been a Ph.D. candidate in the field of information and communications technology (ICT) at Tahri Mohamed University, Bechar, Algeria, since 2016. His research interest includes the authentication and security issues in wireless networks and vehicular ad-hoc networks. He obtained his doctorate at Tahri Mohamed University, Bechar, Algeria since 2020.