# Modeling Elliptical Curve Cryptography Keys using Back Propagation Algorithm

**Ekta Narwal Sumeet Gill**

***ABSTRACT: Vehicular Ad Hoc Networks (VANETs) are the newest for of Ad Hoc Networks in which moving vehicles act as routers and nodes to form a network. VANETs use many cryptographic approaches like symmetric key approaches, public key approaches, certificate revocation, pseudonym based approaches, identity-based cryptography, identity-based signature, Elliptical Curve Cryptography (ECC) etc. for secure communication. These techniques use public and private keys for enhancing the security of messages and all these keys are stored on hardware devices like TPDs (Temper Proof Devices) in VANETs. TPDs are protected by the cryptographic algorithms. In this present era of technology these algorithms and their online simulators are freely available on internet and can be easily intruded. There is a potential need to enhance the security of these keys. In this paper we worked on enhancing the security of ECC keys stored in TPDs of VANETs using a specific network of Artificial Neural Networks.***

***KEYWORDS: VANETs (Vehicular Ad Hoc Networks), TPD (Temper Proof Devices), ECC (Elliptical Curve Cryptography), ANN (Artificial Neural Networks)***

## 1. INTRODUCTION

In recent years, many researchers are working on security of smart vehicles. They use an ad hoc environment which is called VANETs (Vehicular Ad Hoc Networks) for communication.

Many cryptographic algorithms are used in VANETs for secure communication. After deep investigation researchers find out that TPD (Temper Proof Device) which is used for securing keys obtained from the cryptography activities in smart vehicles are not at all safe. Many new attacks have been suggested on these devices for retrieving the secret information from their storage. There are many types of attacks like timing attacks, power attacks, side channel attacks, behavioral attacks etc. Here in this paper we will work on security of keys saved in TPD from intruders using ANN (Artificial Neural Networks).We will use private keys produced by ECC (Elliptical Curve Cryptography). ECC is the newest branch of cryptography used in VANETs for message security. [1]

## 1. TPD SECURITY THREATS AND CHALLENGES

Temper proof devices/ Temper resistance devices are secure computing platform consisting of tamper proof hardware and firmware having processing and storage facility. TPDs store private keys, perform cryptographic operations using these private keys and have a trusted clock. They have their own battery for maintaining trusted clock. The clock is used to match the timing with and to know that vehicle is not forced to produce false messages of wrong timing. Tamper proof hardware is for keeping the data secure because if the module is manipulated to extract security keys the hardware will delete the keys for keeping them away from unauthorized users.[2] The soft computing platform also performs cryptographic tasks inside the tamper proof device to ensure the safety of private keys produce during the operation. Implementation and maintenance of these devices are not cheap but for retrieving

Revised Manuscript Received on July 22, 2019

**EKTA NARWAL,** Department of Mathematics, M.D. University, Rohtak, Haryana, India
**SUMEET GILL,** Department of Mathematics, M.D.University, Rohtak, Haryana, India

*Retrieval Number: I33180789S319/2019©BEIESP*
*DOI: 10.35940/ijitee.I3318.0789S319*

*Published By:*
*Blue Eyes Intelligence Engineering*
*& Sciences Publication*

information from these devices by unauthorized users need very less expensive techniques. Realistic differential attack, attack on RSA, attacks on DES, reverse engineering on unknown block cipher, chip rewriting attacks, ROM overwrite attacks, EEPROM modification attacks, memory reminance attacks, protocol failure are some attacks which are explained by Anderson and their team. On the basis of cost and other factors these attacks can be divided into three parts:

- Invasive which are very expensive to perform and they uncover an integrated circuit completely. These attacks use microprobes to observe data on bus lines and for extracting secrets.
- Non-invasive which have low cost and they are mainly passive attacks. They records leaked information because they observe legal communication.
- Semi- invasive which are of low cost and do less damage to hardware modules. These attacks require partial uncovering of an integrated circuit and obtain results without full violation [3].

This lets us to conclude that all cryptographic approaches and protected hardware modules are not enough for security of data. Security system in VANETs should provide authentication, availability, access control, integrity, consistency, confidentiality, accountability, non-repudiation, data verification, privacy and obscurity. So we need some more advance techniques for security, and a bigger question is- Can techniques of soft computing be broken on the basis-encrypted key storage mechanism and encryption mechanism.

Here we are using neural network models for securing the cryptographic keys from unauthorized access. We will try to simulate the keys, which can then be replaced by network parameters and that network parameters cannot be cracked by anyone [4].

## 2. SECURITY PROTOCOLS BASED ON ECC

Protocols are necessary for data integrity, non-repudiation and reliability of messages. They can prevent the network or communication mechanism from various attacks and can guarantee the privacy and sender's identity of the message. Many security protocols are available for VANETs like secure VANET MAC protocols for DSRC applications; group based secure source authentication, protocols for security of vehicular distributed system etc. ECC (Elliptical Curve Cryptography) is commercially accepted and adopted by many standardizing bodies like ISO, IEEE, NIST and ANSI. There are many security protocols which uses ECC[6–8].

### 3.1 ECDH (Elliptical Curve Diffie Hellman)

ECDH is a key agreement protocol which uses shared secret key scheme. A shared key between sender and receiver produced only when they agree upon elliptic curve domain parameters. Public key of both sender and receiver are shared and then a shared key is produced by each using their own private key and other's public key[5].

### 3.2 ECDSA (Elliptical Curve Digital Signature Algorithm)

ECDSA is based on elliptic curve groups and a newer form of DSA (Digital Signature Algorithm). This protocol needs elliptical curve scalar multiplication, inverse operation, modular reduction operation and a hash function. In this algorithm sender produces a secret key and using this key produces digital signature. Receiver verifies the signature using public key of sender. Key generation, signature generation and signature verification are the three main steps involved in this model. ECDSA provide high security using very low bits keys and also reduces the cost of computation and communication [9].

S.S. Manvi et al. [10] proposed a protocol for authentication of messages in vehicles which is based on ECDSA protocol. Each vehicle who wants to communicate with other should have public and private key pairs and also have to agree upon domain parameters of elliptic curves. This protocol overcomes the drawbacks of communication cost, computational cost and speed, security of the message and storage space.

R. Singh et al. [11] proposed a protocol for efficient and secure communication in VANETs. The model has two phases one is for registration and the other is communication for transferring secure message. For registration phase ECC is used which provides public and private key for communication and in communication phase ECDH is used and shared secret key is generated. Both ECC and ECDH are used in this mechanism so better security is given by this protocol.

### 3.3 ECIES (Elliptical Curve Integrated Encryption Scheme)

In VANETs very high speed moving vehicles communicate with each other so they have very limited resources for communication. VANETs also do not fixed infrastructure for communication. Many attacks and threats can occur in this type of unsafe environment. These attacks and threats are detected by various cryptographic approaches. One of them is ECIES based on elliptical curves. ECIES is a hybrid approach. It uses key agreement (KA) for generating shared secret key by both parties, key derivation function (KDF) produces a set of keys for keying material and other parameters, Encryption (ENC) algorithm based on symmetric key algorithm, message authentication code (MAC) and hash digest function [12].

ECDH and ECDSA can use specifications from 112 to 384 and ECIES uses 128, 192, 256 and 512 bits keys. In our research we are focusing on domain specifications having key size 192 bits to 256 bits. In this paper, we will work on SECG (Standard for Efficient Cryptography group). SECG proposed many different specifications for different key sizes. Here we will use secp192r1, secp224r1 and secp256r1 [10]. Table-1 shows the specifications used in our research with their corresponding strengths and key sizes and their comparative key sizes used in RSA/DSA with same security strength.

*Table-1 Different Specifications used in our research with their Strength and Key Sizes*

| Parameters | Strength | Size | Value of P | RSA/DSA (Size) |
|---|---|---|---|---|
| Secp192r1 | 96 | 192 | $2^{192}-2^{64}-1$ | 1536 |
| Secp224r1 | 112 | 224 | $2^{224}-2^{96}-1$ | 2048 |
| Secp256r1 | 128 | 256 | $2^{224}(2^{32}-1)+2^{192}-2^{96}-1$ | 3072 |

## 3. THE GENERAL EXPERIMENT SETUP

i. Get Keys from Temper Proof/ Resistance Devices

Firstly keys are read from the TPD of vehicle and converted them into hexadecimal form as they are present in some specific format. Table-2 shows some private keys produced during cryptographic operations with different specifications of ECC.

*Table-2 ECC's Private Keys used in Network for Training*

| Specification | ECC 14 Standard Private Key |
|---|---|
| Secp192r1 | !_&>%%2hHO@]#@C$4ONgTMEI^^,a7% |
| Secp224r1 | &{N}lg5SEpkeLQkD#W&y3Y*UV>4vT2SRi<f |
| Secp256r1 | !G,C}NGZq%nRhNCV]T<C0pArfc17aUiKl9-1q%e^ |

ii. Network Training

Keys worked as input and target values. The network is then trained using feed forward back propagation model.

iii. Replacing keys with network parameters

The results obtained from the training of the network are saved in the hardware and the original alphanumeric keys are deleted from the memory.

## 4. RESULTS AND OBSERVATIONS

Network is trained using three different specifications with different input and output values using same number of neurons in input layer, hidden layer, output layer and with same network parameters. Two types of weights obtained after training. One is from input layer to hidden layer and other is from hidden layer to output layer. There are 16 neurons in input layer and 10 neurons in hidden layer so the first weight matrix should have 10X16 elements and second weight matrix should have 16X10 elements but our input and target matrices have first 12 elements of each row as 0 so the weight values have 10X4 and 4X10 elements respectively as first 10X12 values will remain 0 during training and also after training. Figures-2 to 4 show various performance graphs of training obtained during our experiment. In each graph variation of mse(mean squared error) w.r.t. the epochs of the network is drawn and also the best validation value is given at the top of the graph.

Regression plotting is also done which shows that the learning is successful or not. A straight line along diagonal shows that output values are equal to the target values. A little variation in the line shows a bit difference in values, as error rate is taken as 0.001 so a little variation in values is acceptable. Figures- 1 to 3 shows the final graphs of each experiment between target values and the output obtained from training.

Retrieval Number: I33180789S319/2019©BEIESP
DOI: 10.35940/ijitee.I3318.0789S319

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

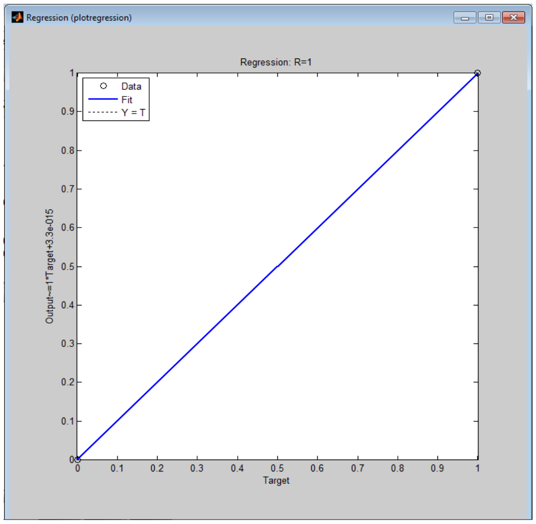

Figure-1 Regression Graph of secp192r1

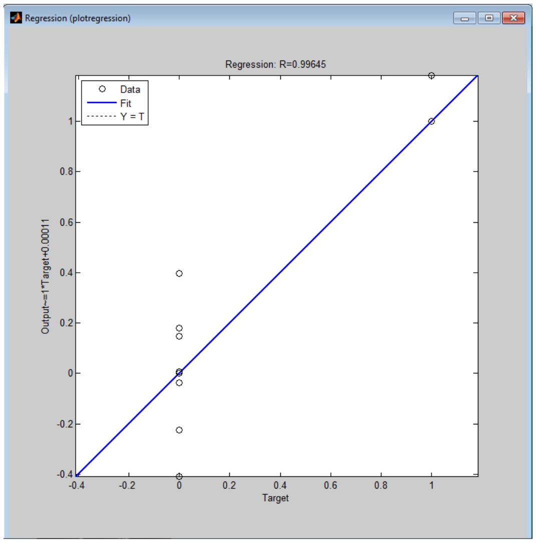

Figure-2 Regression Graph of secp224r1

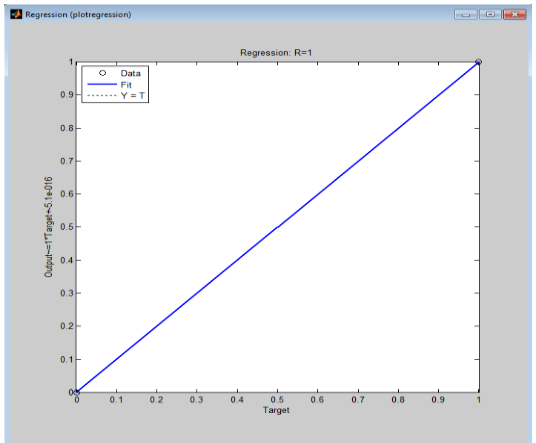

Figure-3 Regression Graph of secp256r1

Training of each network took nearly same time but number of epochs varies for learning. But from the epochs and time taken by the training shown in Table-3 we can conclude that secp256r1 is best among these three specifications when it trained with ANN. Table- 4 shows various training parameters (Bias Values) obtained during training.

*Table-3 Epochs and Time Taken by Different Specifications*

| Specification | Bits in Private Key (in binary form) | Epochs | Time |
|---|---|---|---|
| secp192r1 | 480 | 11 | 0.01 sec |
| secp224r1 | 640 | 8 | 0.01 sec |
| secp256r1 | 736 | 8 | 0.01 sec |

*Table-4 Training Parameters by the Network (Bias Values for Different Specifications)*

| secp192r1 | secp224r1 | secp256r1 |
|---|---|---|
| 1.593438 | 2.645164 | 2.880163 |
| 1.783756 | -1.68607 | -1.00328 |
| 0.90644 | 1.906623 | -1.63867 |
| 1.790482 | -0.70661 | -0.97771 |
| 0.354941 | 0.043884 | -0.61445 |
| -0.23242 | 0.212221 | 0.780252 |
| -2.00013 | 1.563556 | -0.41661 |
| 0.510379 | -1.84899 | 0.491122 |
| -1.23749 | -2.23069 | 1.864302 |
| -2.37971 | -2.01146 | -1.86053 |

## 5. CONCLUSION

In this paper neural network based security mechanism for keys generated during ECC in VANETs is described. Parameters obtained from the training using back propagation are saved in the EEPROM of TPDs in place of alphanumeric keys. Three different keys and specifications (secp192r1, secp224r1 and secp256r1) are used in our research and from results we find out that secp256r1 which produces security key of maximum size 256 bytes is the best among all because the training time taken by the network and performance of the network is best for this size of key.

## REFERENCES

[1] H. Handschuh, P. Paillier, and J. Stern, “Probing Attacks on Tamper-Resistant Devices,” Igarss 2014, vol. 1717, no. 1(2014) pp. 1–5.

[2] E. Narwal and S. Gill, “Secure and Faster Key Management of Elliptical Curve Cryptography in Vanets,” Int. J. Comput. Sci. Eng. Inf. Technol. Res., vol. 7, no. 4,( 2017) pp. 25–30.

[3] M. Aarts, “Hardware Attacks Tamper Resistance , Tamper Response and Tamper Evidence.”

[4] J. Domingo-Ferrer and Q. Wu, “Safety and privacy in vehicular communications,” CEUR Workshop Proc., vol. 397(2008) pp. 6–11.

[5] A. Naveena and K. R. Reddy, “A Review : Elliptical Curve Cryptography in Wireless Ad-hoc Networks,” (2016) pp. 1786–1789.

[6] J. Singh and G. Singh, “Clustering Based Routing Protocols in WSNs : A Review,” vol. 8491, no. 2 (2014) pp. 191–194.

[7] S. Gandhi and Shalini, “Routing Protocols for Vehicular Adhoc Networks (VANETs ): A Review,” Int. J. of Computer Science and Mobile Computing, vol. 5, no. 1 (2014) p. 948-953.

[8] Y. Liu, L. Wang, and H.-H. Chen, “Message Authentication Using Proxy Vehicles in Vehicular Ad Hoc Networks,” IEEE Trans. Veh. Technol., vol. 64, no. 8 (2015) pp. 3697–3710.

[9] H. A. Selma, “Elliptic Curve Cryptographic Processor Design using FPGAs,” pp. 1–6.

[10] S. S. Manvi, M. S. Kakkasageri, and D. G. Adiga, “Message Authentication in Vehicular Ad Hoc Networks: ECDSA Based Approach,” 2009 Int. Conf. Futur. Comput. Commun., 2009.

[11] R.Singh and S. Miglani, “Efficient and Secure Message Transfer in VANET,” no. June, 2016.

[12] Daniel R. L. Brown, “Standards for Efficient Cryptography 2 (SEC 2) : Recommended Elliptic Curve Domain Parameters,” Stand. Effic. Cryptogr., vol. 2, no. Sec 2 (2010) p. 37.

[13] G. Mart, “Encryption Scheme,” vol. 2, no. 2 (2010) pp. 7–13.

[14] E. Engineers, H. Networks, C. Networks, B. Propagation, and M. Tasks, “3 . The Back Propagation Algorithm,” Neural Networks, pp. 16–27.

[15] R.C. Chakraborty, “Back Propagation Network Soft Computing Back Propagation Network,” www.myreaders.info,(2010).

[16] I. C. Lin, H. H. Ou, and M. S. Hwang, “A user authentication system using back-propagation network,” Neural Comput. Appl., vol. 14, no. 3(2005) pp. 243–249.

[17] R. R. Al-nima, L. Muhanad, and S. Q. Hassan, “Data encryption Using Backpropagation Neural Network,” (2009).

[18] E. Narwal and S. Gill, “Perceptrons Helping to Secure VANETs,” Int. J. Adv. Res. Comput. Sci., vol. 8, no. 3(2017) pp. 3–6.

Retrieval Number: I33180789S319/2019©BEIESP
DOI: 10.35940/ijitee.I3318.0789S319

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication