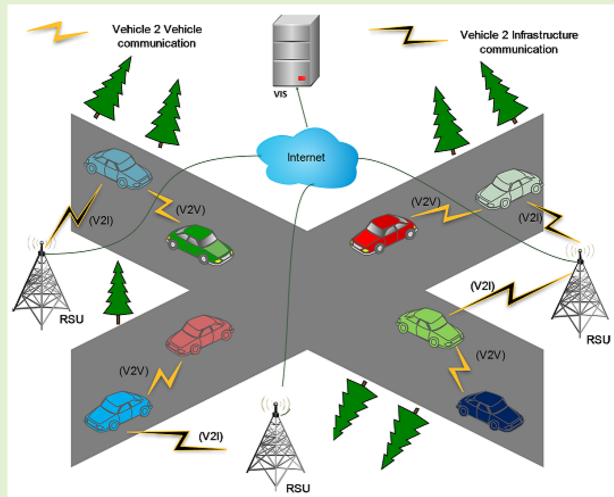
Comments and Corrections

Comments on “A Secure, Privacy-Preserving, and Lightweight Authentication Scheme for VANETs”

Shehzad Ashraf Chaudhry

***Abstract*—Very recently in 2021, Nandy *et al.* proposed an authentication scheme (IEEE Sensors Journal, 21(18), pp. 20998-21011, DOI: 10.1109/JSEN.2021.3097172, 2021) using elliptic curve cryptography and symmetric key-based hash functions and claimed it to provide privacy-preserving security for the VANETs. Nandy *et al.* further claimed that their designed method outperforms some of the existing schemes. Despite, the claim that their scheme can be deployed in real-world VANETs scenarios, this study mentions a critical design flaw in the computation of the key pair of each of the vehicles participating in the vehicular networks. Specifically, it is shown that a vehicle in Nandy *et al.*'s scheme cannot generate its private key. As a result, the public key of the vehicle is also void. Furthermore, it is also argued in this paper that Nandy *et al.*'s scheme does not provide vehicle privacy and during communication, two vehicles exchange useless pseudo numbers without any open or hidden identification information. Moreover, owing to the non-verification of the credentials of the process initiating vehicle, the scheme of Nandy *et al.* can become a prey to clogging attack.**



***Index Terms*—VANETs, public, private key pair, incorrectness, clogging attack, elliptic curve cryptography.**

I. Introduction

BEING adhoc and self-organized networks of vehicles and corresponding roadside units (RSU), the Vehicular adhoc networks (VANETs) are getting more and more attention and it can extend various advantages including the information exchange of traffic issues, road congestion, subsequent routes, parking vacancies and so on. The information exchange can be used to expedite the decision-making for the drivers [1], [2]. Moreover, autonomous vehicles and drones can use this information for to enhance route accuracy and vehicle safety using artificial intelligence techniques. However, the inter-vehicle and vehicle to RSU messaging within a VANET is carried on the public wireless channel and an adversary can exploit the public channel to fulfill his wicked intentions including vehicle tracking, which can be used for criminal purposes [3], [4]. Moreover, the listening of exchanged information and transmission of false/fake messages can be used for marketing, false traffic information, and for getting advantages on parking lots. Hence, the privacy of the vehicles and the security of message exchanges are the main concerns, and these can be accomplished through an authentication procedure. Recently, using elliptic curve cryptography (ECC), a VANETs authentication scheme was proposed by Nandy *et al.* [5]. Despite their claim to provide authentication between entities of a VANET, in this paper, we show that the Nandy *et al.*'s scheme used a faulty addition operation ECC point with a scalar number. Moreover, we also show that the scheme of Nandy *et al.* is prey to clogging attack [6] and it exchanges useless pseudo identities during an authentication round. The paper is further organized as follows: The notations used to describe Nandy *et al.*'s scheme are explained in Table I. In Section II, we briefly define ECC and operations defined over ECC points. The scheme of Nandy *et al.* is detailed in Section III. The pitfalls of the Nandy *et al.*'s scheme are argued in Section IV. Finally, concluding remarks are provided in Section V.

Manuscript received February 3, 2022; accepted April 14, 2022. Date of publication April 18, 2022; date of current version July 1, 2022. The associate editor coordinating the review of this article and approving it for publication was Prof. Zeynep Celik-Butler.
The author is with the Department of Computer Engineering, Faculty of Engineering and Architecture, Istanbul Gelisim University, 34310 Istanbul, Turkey (e-mail: ashraf.shehzad.ch@gmail.com).
Digital Object Identifier 10.1109/JSEN.2022.3168512

II. Elliptic Curve Cryptography: Preliminaries

This section briefly revisits the preliminaries related to ECC, and in comparison with traditional public key based cryptography including RSA, Diffie Hellman and DSA, the

TABLE I
NOTATIONS GUIDE

Symbols	Representations
VIS	Vehicle Information System
V_i	i^{th} Vehicle
$E_p(\alpha,\beta)$	Selected Elliptic Curve
G	Base point on $E_p(\alpha,\beta)$
SK_{vis}	Private key of VIS
$PK_{vis} = SK_{vis}.G$	Public key of VIS
SK_{vi}	Private key of vehicle V_i
PK_{vi}	Public key of vehicle V_i
$H_x(.) : \{x = 1, 2\}$	Two one way hash functions
$T^1_{vx}, T^1_{vy}, T^2_{vx}, T^2_{vy}$	Timestamps
PID_{vx}, PID_{vy}	Random pseduo identities of V_x and V_y
S_{yx}, S_{xy}	Computed session key

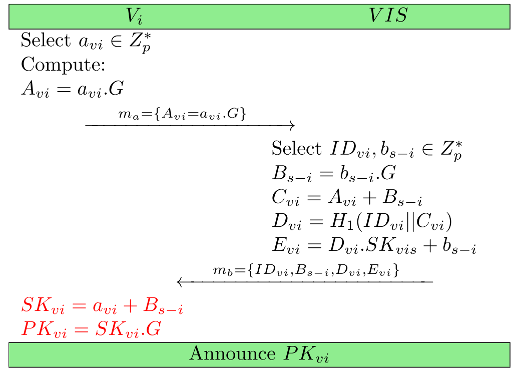


Fig. 1. Nandy *et al.*'s protocol: registration procedure.

ECC is more efficient. The ECC can be described by a curve $E_p(\alpha,\beta) : y^2 = x^3 + \alpha x + \beta \mod p$, such that the pair $\{\alpha,\beta\} \in Z^*_q$, where the scalars α and β are selected in order to satisfy $4\alpha^3 + 27\beta^2 \mod q \neq 0$. The p is chosen randomly and $|p| \geq 160\ bits$. The $E_p(\alpha,\beta)$ consists of numerous points of the form $(x_a, y_a) : \{a = 1, 2, \ldots .n\}$, where $|n| \leq p$. The $E_p(\alpha,\beta)$ also contains $\mathcal{O}$ as a point on infinity and it serves as the only identity element; whereas, $E_p(\alpha,\beta)$ forms an abelian group. The ECC can further be defined by only two following operations:

- **ECC Point addition:** Given $P = (x_p, y_p)$ and $Q = (x_q, y_q)$ be the two points, $P + Q$ results into another point $R = (x_r, y_r)$, where the $x_r = \lambda^2 - x_p - x_q \mod p$ and $y_r = (\lambda(x_p - x_r) - y_p) \mod p$, furthermore λ can be computed as follows:
$$\lambda = \begin{cases} \frac{3x_p^2+\alpha}{2y_p} \mod p & \text{if } P = Q, \\ \frac{y_q-y_p}{x_q-x_p} \mod p & \text{if } P \neq Q \end{cases}$$
- **ECC Point Scalar Multiplication:** Given $i \in Z^*_p$ be an integer and $P = (x_p, y_p)$ be a point over $E_p(\alpha,\beta)$. The $T = i.P$ can computed using the repeated addition i.e. $T = P + P + P + \ldots .P$ (i times) and the T is also another point over the same curve $E_p(\alpha,\beta)$ and can be represented by x and y coordinates i.e. $T = (x_t, y_t)$.

As explained above, the ECC operations could be comprehend by point addition and scalar multiplication operations. Precisely, ECC does not support any other operation. Specifically, the addition of a scalar with an ECC point is an illegal operation and has no defined result.

III. NANDY *et al.*'s PROTOCOL

The protocol of Nandy *et al.* [5] is briefly explained in following subsections:

A. Nandy et al.'s Protocol: Initialization

The Vehicle Information Server (VIS) administers the initialization and for this VIS chooses an elliptic curve on finite-field $E_p(\alpha,\beta) : y^2 = x^3 + \alpha x + \beta \mod p$. The $E_p(\alpha,\beta)$ satisfies $4\alpha^3 + 27\beta^2 \mod p \neq 0$. The p, which is a prime number and is selected carefully such that $|p| \geq 160 - bits$ The VIS marks G as a generate/base point out of the points over $E_p(\alpha,\beta)$. The VIS chooses/computes it's own private-public key pair $\{SK_{vis} \in Z^*_p, PK_{vis} = SK_{vis}.G\}$. The VIS then adopts two one-way and non-reversible hash functions $H_x : \{0,1\}^* \rightarrow Z^*_p$, where $x = 1, 2$ both hash functions take variable size inputs and produce fixed size outputs. The VIS secretly stores SK_{vis} and publicly distributes all other parameters, which are $\{E_p(\alpha,\beta), p, PK_{vis}, H_x\}$.

B. Nandy et al.'s Protocol: Vehicle Registration

In Nandy et al's scheme, the vehicle registration procedure is initiated by a vehicle which needs to be a part of the VIS network and it completes by the administration of the VIS. As depicted in Fig. 1, the vehicle V_i selects $a_{vi} \in Z^*_p$, computes and sends $A_{vi} = a_{vi}.G$ to the VIS and on receiving A_{vi}, the VIS selects $\{ID_{vi}, b_{s-i}\} \in Z^*_p$ and computes V_i related parameters $B_{s-i} = b_{s-i}.G$, $C_{vi} = A_{vi} + B_{s-i}$, $D_{vi} = H_1(ID_{vi}||C_{vi})$ and $E_{vi} = D_{vi}.SK_{vis} + b_{s-i}$. At end, the VIS sends $\{ID_{vi}, B_{s-i}, D_{vi}, E_{vi}\}$ to V_i. On receiving $\{ID_{vi}, B_{s-i}, D_{vi}, E_{vi}\}$, the V_i computes it's own private-public key pair $\{SK_{vi} = a_{vi} + B_{s-i}, PK_{vi} = SK_{vi}.G\}$. The public key PK_{vi} is distributed publicly and stores SK_{vi} secretly on OBU.

C. Nandy et al.'s Protocol: Mutual Authentication

This phase as depicted in Fig. 2 is further explained through following steps:

S- 1: To initiate an authentication round, a vehicle V_i generate a pseudo-identity PID_{vx}, along with a random number $c_{vx} \in Z^*_p$, and fresh timestamp T^1_{vx}. The V_i then computes $J_{vx} = c_{vx}.G$ and sends $m_a = \{PID_{vx}, J_{vx}, B_{s-x}, D_{vx}, T^1_{vx}\}$ to V_y.

S- 2: The V_y receives m_a, generates T^1_{vy} and checks the freshness of T^1_{vx}. The V_y aborts the session if $T^1_{vx} - T^1_{vy} \leq \Delta T$ does not hold. Now the V_y generates pseudo-identity PID_{vy}, along with a random number $c_{vy} \in Z^*_p$ and computes $J_{vy} = c_{vy}.G$, $K_{yx} = (c_{vy} + E_{vy}).(J_{vx} + B_{s-x} + D_{vx}.PK_{vis})$, $V_{yx} = H_2(PID_{vx}||K_{yx})$ and $S_{yx} = H_2(PID_{vx}||PID_{vy}||K_{yx})$. After this the V_y generates

V_x	V_y
Generate PID_{vx}, $c_{vx} \in Z_p^*$, T_{vx}^1 and Compute: $J_{vx} = c_{vx}.G$	
$\xrightarrow{m_a=\{PID_{vx}, J_{vx}, B_{s-x}, D_{vx}, T_{vx}^1\}}$	
	Generate T_{vy}^1 $T_{vx}^1 - T_{vy}^1 \leq \Delta T$, abort if not fresh Generate PID_{vy}, $c_{vy} \in Z_p^*$ $J_{vy} = c_{vy}.G$ $K_{yx} = (c_{vy} + E_{vy}).(J_{vx} + B_{s-x} + D_{vx}.PK_{vis})$ $V_{yx} = H_2(PID_{vx}\|\|K_{yx})$ $S_{yx} = H_2(PID_{vx}\|\|PID_{vy}\|\|K_{yx})$ Generate T_{vy}^2
$\xleftarrow{m_b=\{PID_{vy}, D_{vy}, B_{s-b}, D_{vy}, T_{vy}^2, V_{yx}\}}$	
Generate T_{vx}^2 $T_{vy}^2 - T_{vx}^2 \leq \Delta T$, abort if not fresh Generate PID_{vy}, $c_{vy} \in Z_p^*$ $K_{xy} = (c_{vx} + E_{vx}).(J_{vy} + B_{s-b} + D_{vy}.PK_{vis})$ $V_{xy} \stackrel{?}{=} H_2(PID_{vx}\|\|K_{xy})$ $S_{xy} = H_2(PID_{vx}\|\|PID_{vy}\|\|K_{xy})$	
$S_{xy} = H_2(PID_{vx}\|\|PID_{vy}\|\|K_{xy}) = S_{yx}$	

Fig. 2. Nandy *et al.*'s protocol: login and authentication procedure.

T_{vy}^2 and sends $m_b = \{PID_{vy}, D_{vy}, B_{s-b}, D_{vy}, T_{vy}^2, V_{yx}\}$ to V_x.

S- 3: The V_x receives m_b, generates fresh T_{vx}^2 and checks the freshness of T_{vx}^2. The V_x aborts the session if $T_{vy}^2 - T_{vx}^2 \leq \Delta T$, does not hold. Now, V_x generates pseudo-identity PID_{vy}, along with a random number $c_{vy} \in Z_p^*$ and computes $K_{xy} = (c_{vx} + E_{vx}).(J_{vy} + B_{s-b} + D_{vy}.PK_{vis})$, $V_{xy}=H_2(PID_{vx}||K_{xy})$ and $S_{xy} = H_2(PID_{vx}||PID_{vy}||K_{xy})$, where $S_{xy} = H_2(PID_{vx}||PID_{vy}||K_{xy}) = S_{yx}$ is the shared key among the two vehicles V_x and V_y.

D. Nandy et al.'s: Communication Phase

For sending a message M_{xy}, the V_x using the session key (S_{xy}) generated in the last session encrypts M_{xy} as $CM_{xy} = Enc_{S_{xy}}(M_{xy})$ and sends CM_{xy} along with current timestamp T_{vx}^3 to the V_y. On receiving $\{CM_{xy}, T_{vx}^3\}$, the V_y compares the T_{vx}^3 with current timestamp T_{vy}^3 and if it is within the legal range, the V_y decrypts CM_{xy} and gets $M_{xy} = Dec_{S_{xy}}(CM_{xy})$.

IV. Pitfalls of Nandy *et al.*'s Scheme

This section describes the pitfalls of Nandy *et al.*'s scheme. Specifically, it is proved in the proceeding subsections that Nandy *et al.*'s scheme cannot generate public/private key pair of a vehicle and the scheme is prone to clogging attack, in addition the vehicles send useless pseudo identities during authentication process.

A. Incorrect Public-Private Key Pair

In the scheme of Nandy *et al.*, the vehicle say V_i selects $a_{vi} \in Z_p^*$, computes and sends $A_{vi} = a_{vi}.G$ to VIS and the VIS on receiving A_{vi} selects $\{ID_{vi}, b_{s-i}\} \in Z_p^*$. Now, along with other parameters, the VIS computes $B_{s-i} = b_{s-i}.G$. At end, the VIS sends $\{ID_{vi}, B_{s-i}, D_{vi}, E_{vi}\}$ to V_i. The V_i on receiving $\{ID_{vi}, B_{s-i}, D_{vi}, E_{vi}\}$, computes it's private key as follows:

$$SK_{vi} = a_{vi} + B_{s-i} \tag{1}$$

In Eq. 1, the computation of private key SK_{vi} requires to add a_{vi} and B_{s-i}, where a_{vi} is a scalar number and $B_{s-i} = b_{s-i}.G$ is a point over the selected elliptic curve $E_p(\alpha, \beta)$ and no method exist, which can add a scalar with an ECC point [7]. Therefore, the computation of private key SK_{vi} is an operation without any result. The registration protocol enters into a halt state if it executes Eq. 1. Moreover, the computation of public key $PK_{si} = SK_{vi}.G$ is also an illegal operation. Hence, the registration phase of Nandy *et al.*'s scheme is faulty. Therefore, the scheme of Nandy *et al.* cannot register any vehicle.

B. Clogging Attack

During authentication, the initiating vehicle V_x sends $m_a = \{PID_{vx}, J_{vx}, B_{s-x}, D_{vx}, T_{vx}^1\}$ to the responding vehicle V_y. In return, the V_y after processing the request sends $m_b = \{PID_{vy}, D_{vy}, B_{s-b}, D_{vy}, T_{vy}^2, V_{yx}\}$ to V_x. Although, the V_x checks the authenticity of the V_y by verifying $V_{xy}=H_2(PID_{vx}||K_{xy})$, the V_y only checks the freshness of timestamp T_{vy}^1 by comparing it with the current timestamp T_{vy}^1 and if the comparisons yields a difference within specified range ΔT, the request is considered legitimate. There is no other verification furnished by V_y to check the legitimacy of the initiating vehicle V_x. Therefore, any adversary can generate a fresh timestamp and can send a forged message along with the fresh timestamp. This forged message will pass the legitimacy test. Although, the adversary may not be able to construct a valid and legitimate session key, the responding vehicle V_y processes the whole faked request, and it results into useless processing. In case, the adversary bombards the V_y with a large number of fake requests, the V_y may become unable to process the legitimate requests due to resource limitations. Therefore, the scheme of Nandy *et al.* is prone to clogging attack [6].

C. Useless Pseudo Identities

During authentication, the two communicating vehicles (V_x and V_y) sends some temporary identities PID_{vx}

and PID_{vy}. Both of these identities are generated randomly and have no hidden or otherwise identification information of the communicating vehicle. Therefore, these identities are sent over the communication network without any usage.

V. Conclusion

In this paper, we have analyzed and showed that a recent authentication scheme for VANETs entails a faulty design due to mistaken usage of an erroneous addition operation of an ECC point and a scalar. Moreover, it is also argued in this paper that the scheme of Nandy *et al.* is prone to clogging attacks in addition to the transmission of useless temporary identities over the public communication channel. Consequently, it is suggested that the scheme cannot be used in any real-time scenario without correcting the ECC-related erroneous operations.

References

[1] C.-M. Chen, B. Xiang, Y. Liu, and K.-H. Wang, "A secure authentication protocol for internet of vehicles," *IEEE Access*, vol. 7, pp. 12047–12057, 2019.

[2] S. A. Chaudhry, "Designing an efficient and secure message exchange protocol for internet of vehicles," *Secur. Commun. Netw.*, vol. 2021, pp. 1–9, May 2021.

[3] F. Qu, Z. Wu, F.-Y. Wang, and W. Cho, "A security and privacy review of VANETs," *IEEE Trans. Intell. Transp. Syst.*, vol. 16, no. 6, pp. 2985–2996, Dec. 2015.

[4] M. Kamal, G. Srivastava, and M. Tariq, "Blockchain-based lightweight and secured V2V communication in the internet of vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 7, pp. 3997–4004, Jul. 2021.

[5] T. Nandy *et al.*, "A secure, privacy-preserving, and lightweight authentication scheme for VANETs," *IEEE Sensors J.*, vol. 21, no. 18, pp. 20998–21011, Sep. 2021.

[6] Z. Ali, S. A. Chaudhry, K. Mahmood, S. Garg, Z. Lv, and Y. B. Zikria, "A clogging resistant secure authentication scheme for fog computing services," *Comput. Netw.*, vol. 185, Feb. 2021, Art. no. 107731.

[7] S. A. Chaudhry, "Correcting 'PALK: Password-based anonymous lightweight key agreement framework for smart grid,'" *Int. J. Electr. Power Energy Syst.*, vol. 125, Feb. 2021, Art. no. 106529.