A note on "a novel authentication and key agreement scheme for Internet of Vehicles"

Zhengjun Cao

Abstract. We show that the Yang et al.'s key agreement scheme [Future Gener. Comput. Syst., 145, 415-428 (2023)] is flawed. (1) There are some inconsistent computations, which should be corrected. (2) The planned route of a target vehicle is almost exposed. The scheme neglects the basic requirement for bit-wise XOR, and tries to encrypt the route by the operator. The negligence results in some trivial equalities. (3) The scheme is insecure against impersonation attack launched by the next roadside unit.

Keywords: Authentication, Anonymity, Impersonation attack, Key agreement, Internet of vehicles

1 Introduction

The internet of vehicles is a network of connected vehicles, which follows the same principles as other internet of things networks. In 2021, Bagga et al. [1] designed a mutual authentication and key agreement protocol in internet of vehicles-enabled intelligent transportation system. Chattaraj et al. [2] put forth a blockchain-assisted certificateless key agreement protocol for internet of vehicles in smart transportation. Kamil and Ogundoyin [3] proposed a certificateless authentication scheme and group key agreement with dynamic updating mechanism for internet of vehicles in smart cities. Wu et al. [4] presented a lightweight authenticated key agreement protocol using fog nodes in social internet of vehicles. In 2022, Wang et al. [5] discussed a multiserver authentication and key agreement protocol for internet of vehicles. Thapliyal et al. [6] proposed a robust authenticated key agreement protocol for internet of vehicles-envisioned intelligent transportation system. Xie et al. [7] investigated a blockchain-based efficient privacy-preserving handover authentication protocol with key agreement for internet of vehicles.

Recently, Yang et al. [8] have also presented a key agreement scheme for internet of vehicles. In the considered scenario, there are three entities: OBU, RSU, and TA. OBU is a hardware equipment installed on the vehicle. RSU (roadside unit) is a communication device arranged on both sides of the road or at a specific location. TA is a credible third party, responsible for the registration and management of vehicles in the whole system.

The scheme is designed to meet many security requirements, including authentication, session-key establishment, anonymity, traceability, and resistance to impersonation attack, reply attack, etc. In

Department of Mathematics, Shanghai University, Shanghai, 200444, China. Email: caozhj@shu.edu.cn

Table 1: The Yang et al.'s scheme for the first road section

$OBU_i : \{S\}$	The first $RSU_i : \{x_i\}$
Insert the smart card. Enter RID_i and RPW_i. Check RID_i and RPW_i. Pick $V_i \in Z_q^*$, compute the anonymous identity $PID_i = \{PID_{i,1}, PID_{i.2}\}$, where $PID_{i,1} = V_i \cdot P$, $PID_{i,2} = RID_i \oplus h(V_i \cdot Pub_{sys})$. Invoke the system key S to compute $Sig_i = S \cdot h(PID_i) + V_i \cdot h(m)$ where m is the vehicle's planned route. Pick $\alpha_i \in Z_q^*$ to compute $R_1 = h(V_i \cdot Pub^i_{RSU})$, $L_1 = R_1 \oplus \alpha_i$, $F_1 = h(\alpha_i) \oplus m$. Set the timestamp T^i_v and compute $Auth^i_{PID} = h(\alpha_I \\| m \\| L_1 \\| F_1 \\| T^i_V)$. Send $\{Sig_i, Auth^i_{PID}, T^i_V, PID_i, F_1, L_1\}$ to the first RSU_i. $\xrightarrow[\text{[open channel]}]{Sig_i,\ Auth^i_{PID},\ T^i_V,\ PID_i,\ F_1,\ L_1}$	
	Check the timestamp T^i_V. If so, compute $R_1^* = h(x_i \cdot PID_{i,1})$, $\alpha_i^* = R_1^* \oplus L_1$, $m^* = h(\alpha_i^*) \oplus F_1$, $Auth^{i*}_{PID} = h(\alpha_i^* \\| m^* \\| L_1 \\| F_1 \\| T^i_V)$. Check $Auth^{i*}_{PID} = Auth^i_{PID}$, and $Sig_i \cdot P = Pub_{sys} \cdot h(PID_i) + PID_{i,1} \cdot h(m^*)$. If so, select the next RSU_{i+1} and pick $\beta_i \in Z_q^*$, compute $Key = x_i \cdot Pub^{i+1}_{RSU}$, $W_1 = \alpha_i^* \oplus Key$, $Z_1 = R_1^* \oplus \beta_i$, $Session_{key} = h(\alpha_i^* \\| \beta_i)$. Set the timestamp T^i_R. Compute $Auth^i_{RSU} = h(W_1 \\| Z_1 \\| \beta_i \\| Key \\| T^i_R)$. $\xleftarrow{Auth^i_{RSU},\ T^i_R,\ W_1,\ Z_1}$
Check the timestamp T^i_R. Compute $Key^* = W_1 \oplus \alpha_i$, $\beta_i^* = R_1 \oplus Z_1$, $Auth^{i*}_{RSU} = h(W_1 \\| Z_1 \\| \beta_i^* \\| Key^* \\| T^i_R)$. Check $Auth^{i*}_{RSU} = Auth^i_{RSU}$. If so, compute $Session_{key} = h(\alpha_i \\| \beta_i^*)$.	

this note, we show that the scheme cannot be practically implemented due to some flaws.

2 Review of the Yang et al.'s scheme

Let $h() : \{0,1\}^* \to Z_q^*$ be a hash function. The authority TA picks two large primes P, q and defines an elliptic curve $E : y^2 = x^3 + ax + by \bmod q$. Pick $S \in Z_q^*$ as a private key and set the public key as $Pub_{sys} = S \cdot P$. The private key S is divided into two parts: S_1 and S_2. S_1 is stored in each vehicle's password device, and S_2 is stored in the smart card. Generate S using S_1 and S_2 when the vehicle wants to use the private key S. Select $x_i \in Z_q^*$ as RSU_i's private key and set the public key as $Pub_{RSU_i} = x_i \cdot P$. For each vehicle with the true identity RID_i and the password RPW_i, TA stores $\{RID_i, RPW_i, S_2\}$ into the smart card, and stores x_i into the device RSU_i. Publish the parameters

$\{P, q, a, b, Pub_{sys}, Pub_{RSU_i}, h\}$.

The initial authentication and key agreement phase can be depicted below (see Table 1). When a vehicle behaves maliciously, TA can compute $RID_i = h(S \cdot PID_{i,1}) \oplus PID_{i,2}$, to reveal the vehicle's identity.

3 Inconsistent computations

The scheme uses the basic operators over an elliptic curve. But we find there are some inconsistent computations. For example, it specifies that (see page 418, Ref.[8]):

> *1. TA randomly selects two large primes P, q, and finite fields Z_q^*, elliptic curve: $y^2 = x^3 + ax + by \bmod q$.*
> *2. TA randomly selects $S \in Z_q^*$ as a private key to the system and calculates the public key $Pub_{sys} = S \cdot P$.*

The specification is incorrect because it confuses the basic structure of an elliptic curve and associated elliptic curve groups. It is easy to see that P should be a point belonging to the underlying elliptic curve, *instead of a large prime*. Otherwise, any adversary can recover the master secret key S from the equation $Pub_{sys} = S \cdot P$, where both Pub_{sys} and P are public parameters. To revise, one can specify that:

> *TA randomly selects two large primes p, q, an elliptic curve $y^2 = x^3 + ax + by \bmod p$, and a cyclic additive elliptic curve group G_q of order q, with a generator P.*

In this case, the difficulty of retrieving secret key S from equation $Pub_{sys} = S \cdot P$ directly relies on that of elliptic curve discrete logarithm problem (ECDLP), which is a famous intractable problem in cryptography.

4 The exposure of planned route

The Boolean logic operation XOR, denoted by $\oplus$, is widely used in cryptography which compares two input bits and generates one output bit. If the bits are the same, the result is 0. If the bits are different, the result is 1. When the operator is performed on two strings, they must be of a same bit-length. Otherwise, the shorter string should be stretched by padding some 0s to its left side. In this case, the partial string corresponding to the padding bits is directly copied into the final string.

In the Yang et al.'s scheme, a target vehicle's planned route is expressed as m. To protect the route, the scheme adopts the below mechanism

$$R_1 = h(V_i \cdot Pub_{RSU}^i), \quad L_1 = R_1 \oplus \alpha_i, \quad \text{[Encryption]} \quad F_1 = h(\alpha_i) \oplus m,$$
$$R_1^* = h(x_i \cdot PID_{i,1}), \quad \alpha_i^* = R_1^* \oplus L_1, \quad \text{[Decryption]} \quad m^* = h(\alpha_i^*) \oplus F_1$$

due to that

$$V_i \cdot Pub^i_{RSU} = V_i(x_i \cdot P) = x_i(V_i \cdot P) = x_i \cdot PID_{i,1}$$

But we find the simple operation bit-wise XOR is insufficient to encrypt the route m, because the hash value $h(\alpha_i)$, practically 256 bits or 512 bits, is too short to mask the other operand m. Generally, the bit-length of route m is far greater than 512, i.e., BitLength(m)$>$ 512 (the route information contains more than 64 ASCII symbols). Hence, we have

$$F_1 = (00\cdots 0\| \underbrace{h(\alpha_i)}_{512-\text{bits}}) \oplus m$$

which means the route m is almost exposed, once the adversary captures the transferred parameter F_1 via the open channel. The scheme has neglected the basic requirement for bit-wise XOR operator and presented a trivial encryption. To revise, one should adopt other encryption mechanism such as block cipher, stream cipher, etc.

5 Insecure against impersonation attack

As we see, the agreed key is set as $Session_{key} = h(\alpha_i\|\beta_i)$, where α_i, β_i are picked by the OBU_i and the first RSU_i, respectively. To carry forward the planned route, the RSU_i should choose the next roadside unite RSU_{i+1} and invoke its public key Pub^{i+1}_{RSU}. But we find it adopts a very simple secret-key invoking mechanism, i.e.,

$$Key = x_i \cdot Pub^{i+1}_{RSU} = x_i(x_{i+1} \cdot P) = x_{i+1}(x_i \cdot P) = x_{i+1} Pub^i_{RSU}$$

which means the corrupted roadside unit RSU_{i+1} who knows the secret key x_{i+1}, can obtain the parameter Key by invoking the public key Pub^i_{RSU}. The corrupted unit then uses the captured data $\{Sig_i, Auth^i_{PID}, T^i_V, PID_i, F_1, L_1; Auth^i_{RSU},\ T^i_R,\ W_1,\ Z_1\}$ via open channels, to compute

$$\alpha_i = W_1 \oplus Key, \quad R_1 = \alpha_i \oplus L_1, \quad \beta_i = R_1 \oplus Z_1$$

With the retrieved nonce α_i and β_i, the corrupted roadside unit can compute the session key $Session_{key} = h(\alpha_i\|\beta_i)$. Using this key, the corrupted unit can impersonate the target unit in the upcoming session. Thus, the scheme is insecure against impersonation attack launched by the next roadside unit.

6 Conclusion

We show that the Yang et al.'s authentication and key agreement scheme is flawed. It seems difficult to revise the scheme because of its misused encryption and simple secret-key invoking mechanism. The findings in this note could be helpful for the future work on designing such schemes.

References

[1] P. Bagga, A. K. Das, M. Wazid, J. J. P. C. Rodrigues, K. R. Choo, Y. Park: On the design of mutual authentication and key agreement protocol in internet of vehicles-enabled intelligent transportation system. *IEEE Trans. Veh. Technol.*, 70(2), 1736-1751 (2021)

[2] D. Chattaraj, B. Bera, A. K. Das, S. Saha, P. Lorenz, Y. Park: Block-CLAP: blockchain-assisted certificateless key agreement protocol for internet of vehicles in smart transportation. *IEEE Trans. Veh. Technol.*, 70(8), 8092-8107 (2021)

[3] I. A. Kamil, S. O. Ogundoyin: A lightweight certificateless authentication scheme and group key agreement with dynamic updating mechanism for LTE-V-based internet of vehicles in smart cities. *J. Inf. Secur. Appl.*, 63, 102994 (2021)

[4] T. Y. Wu, X. Guo, L. Yang, Q. Meng, C. M. Chen: A lightweight authenticated key agreement protocol using fog nodes in social internet of vehicles. *Mob. Inf. Syst.*, 3277113, 1-14 (2021)

[5] J. Wang, L. Wu, H. Wang, K. R. Choo, L. Wang, D. He: A secure and efficient multiserver authentication and key agreement protocol for internet of vehicles. *IEEE Internet Things J.*, 9(23), 24398-24416 (2022)

[6] S. Thapliyal, M. Wazid, D. P. Singh, A. K. Das, S. H. Islam: Robust authenticated key agreement protocol for internet of vehicles-envisioned intelligent transportation system. *J. Syst. Archit.*, 142, 102937 (2023)

[7] X. Xie, B. Wu, B. Hou: BEPHAP: a blockchain-based efficient privacy-preserving handover authentication protocol with key agreement for internet of vehicles. *J. Syst. Archit.*, 138, 102869 (2023)

[8] Q. Yang, X. Zhu, X. Wang, J. Fu, J. Zheng, Y. Liu: A novel authentication and key agreement scheme for Internet of Vehicles. *Future Gener. Comput. Syst.*, 145, 415-428 (2023)