Analysis of One Certificateless Authentication and Key Agreement Scheme for Wireless Body Area Network

Zhengjun Cao, Lihua Liu

Abstract. We show that the certificateless authentication scheme [Mob. Networks Appl. 2022, 27, 346-356] fails to keep anonymity, not as claimed. The scheme neglects the basic requirement for bit-wise XOR, and tries to encrypt data by the operator. The negligence results in some trivial equalities. The adversary can retrieve the user's identity from one captured string via the open channel.
Keywords: Certificateless Authentication, Key Agreement, Anonymity, Wireless Body Area Network.

1 Introduction

Certificateless authentication has attracted much attention. In 2020, Hathal et al. [5] proposed a certificateless and lightweight authentication scheme for vehicular communication networks. Asari et al. [1] designed a hierarchical anonymous certificateless authentication protocol with aggregate verification. Gowri et al. [4] presented a certificateless aggregate signature-based authentication scheme for vehicular ad hoc networks. In 2022, Bouakkaz and Semchedine [2] put forth a certificateless scheme-based conditional privacy preservation authentication for applications in VANET. Imghoure et al. [6] introduced a certificateless conditional privacy-preserving authentication scheme in vehicular ad hoc network. Moni and Manivannan [7] presented a certificateless and reused-pseudonym based authentication scheme. Tomar and Tripathi [10] suggested a blockchain-based certificateless authentication system for vehicular network. Nkurunziza et al. [8] presented a certificateless anonymous authentication protocol for smart grid. Palaniswamy et al. [9] discussed a certificateless authentication protocol for the SAE J1939 commercial vehicles bus.

Recently, Cheng et al. [3] have presented a certificateless authentication and key agreement scheme for secure cloud-assisted wireless body area network. There are five entities: network manager (NM), leaf node (LN), root node (RN), target node (TN) and cloud server (CS). The NM acts as a trusted third party to provide registration and secret parameters generation. The scheme is designed to meet many security requirements, including user authentication, session-key establishment, user anonymity and untraceability, etc. In this note, we show that the scheme fails to keep user anonymity, not as claimed.

Z. Cao, Department of Mathematics, Shanghai University, Shanghai, 200444, China.
L. Liu, Department of Mathematics, Shanghai Maritime University, Shanghai, 201306, China.
Email: liulh@shmtu.edu.cn

Table 1: The Chen et al.'s authentication scheme

Leaf node (LN): ID_{LN}	Network manager (NM): $\{ x_0 \}$	Cloud server (CS): ID_{CS}
	Registration	
Select the identity $ID_{LN} \in \{0,1\}^*$.	Pick $r_{LN}, r_{CS} \in Z_q^*$, compute	Select the identity $ID_{CS} \in \{0,1\}^*$.
$\xrightarrow{ID_{LN}}$	$R_{LN} = r_{LN}P$, $R_{CS} = r_{CS}P$	$\xleftarrow{ID_{CS}}$
	$s_{LN} = r_{LN} + s_0 H_1(ID_{LN} \| R_{LN})$.	
	$s_{CS} = r_{CS} + s_0 H_1(ID_{CS} \| R_{CS})$.	
Store the private key (s_{LN}, R_{LN}).	$\xleftarrow[\text{[secure channel]}]{s_{LN},\ R_{LN}}$ $\xrightarrow[\text{[secure channel]}]{s_{CS},\ R_{CS}}$	Store the private key (s_{CS}, R_{CS}).
Leaf node (LN): (s_{LN}, R_{LN})	Authentication & key agreement	Cloud server (CS): (s_{CS}, R_{CS})
Pick $x \in Z_q^*$, timestamp T_{LN}, set $X = xP$,		Compute $g_{CS} = s_{CS} X_{LN}$,
$e = H_2(ID_{CS} \| X)$, $X_{LN} = (x + e s_{LN})P$,		$ID_{LN} \| R_{LN} \| T_{LN} \| h = H_3(g_{CS}) \oplus W$.
$g_{LN} = (x + e s_{LN})(R_{CS} + H_1(ID_{CS} \| R_{CS})P_0)$,	$\xrightarrow[\text{[open channel]}]{W,\ X_{LN}}$	Check the timestamp T_{LN}. If so, check
$h = s_{LN}(R_{CS} + H_1(ID_{CS} \| R_{CS})P_0)$,		$h = s_{CS}(R_{LN} + H_1(ID_{LN} \| R_{LN})P_0)$.
$W = H_3(g_{LN}) \oplus (ID_{LN} \| R_{LN} \| T_{LN} \| h)$.		If so, pick $y \in Z_q^*$ and timestamp T_{CS},
		compute $Y = yP$, $d = H_4(ID_{CS} \| ID_{LN} \| Y)$,
Check the timestamp. If so,		$Y_{CS} = (y + d s_{CS})P$, $key_{CS} = (y + d s_{CS}) X_{LN}$,
compute $key_{LN} = (x + e s_{LN}) Y_{CS}$,	$\xleftarrow{Y_{CS},\ T_{CS}}$	$SK_{CS} = H_5(key_{CS} \| ID_{LN} \| ID_{CS} \| Y_{CS} \| X_{LN})$.
$SK_{LN} = H_5(key_{LN} \| ID_{LN} \| ID_{CS} \| Y_{CS} \| X_{LN})$.		

2 Review of the scheme

The NM generates an additive cyclic elliptic curve group G_1 with a generator P, and a multiplicative cyclic group G_2 with the a prime order q. Pick $s_0 \in Z_q^*$ as the master private key, and set the public key $P_0 = s_0 P$. Choose five hash functions:

$$H_1 : \{0,1\}^* \times G_1 \to Z_q^*, \quad H_2 : \{0,1\}^* \times G_2 \to Z_q^*,$$
$$H_3 : G_2 \to \{0,1\}^* \times G_1 \times Z_q^*,$$
$$H_4 : \{0,1\}^* \times G_2^2 \to Z_q^*, \quad H_5 : \{0,1\}^* \times G_2^3 \to Z_q^*.$$

Publish $\{q, P, P_0, G_1, G_2, H_1, \cdots, H_5\}$ as the system parameters. The scheme can be restated as below (see Fig.1).

3 The loss of anonymity

Hashing is the one-way act of converting the data (called a message) into the output (called the hash). A hash function converts any digital data into an output string with a fixed number of characters. It is useful to ensure the authenticity of a piece of data and that it has not been tampered with, since even a small change in the message will create an entirely different hash. Hash functions can ensure data integrity. One can identify whether digital data has been tampered with after it's been created. Keyed hash functions can ensure data integrity and entity authenticity concurrently. Only the shared key owners can generate and verify the hash values.

The Boolean logic operation XOR, denoted by $\oplus$, is widely used in cryptography which compares two input bits and generates one output bit. 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 eventually exposed.

In the scheme the transfer of $ID_{LN}\|R_{LN}\|T_{LN}\|h$ from LN to CS depends on the below transformations

$$\begin{aligned}&\text{Encryption: } W = H_3(g_{LN}) \oplus (ID_{LN}\|R_{LN}\|T_{LN}\|h),\\ &\text{Decryption: } ID_{LN}\|R_{LN}\|T_{LN}\|h = H_3(g_{CS}) \oplus W,\end{aligned}$$

due to that

$$\begin{aligned}g_{CS} &= s_{CS}X_{LN} = s_{CS}(x + es_{LN})P\\ &= (x + es_{LN})(r_{CS} + s_0H_1(ID_{CS}\|R_{CS}))P\\ &= (x + es_{LN})(r_{CS}P + s_0H_1(ID_{CS}\|R_{CS})P)\\ &= (x + es_{LN})(R_{CS} + H_1(ID_{CS}\|R_{CS})P_0)\\ &= g_{LN}\end{aligned}$$

Note that the string $H_3(g_{LN})$ should be long enough to mask the other operand $ID_{LN}\|R_{LN}\|T_{LN}\|h$, which is the concatenation of $ID_{LN}, R_{LN}, T_{LN}, h$. Otherwise, such a lightweight encryption cannot be used to transfer data securely.

The hash function H_3 is inconsistently defined as

$$H_3 : G_2 \to \{0,1\}^* \times G_1 \times Z_q^*$$

which should be corrected as

$$H_3 : G_1 \to \{0,1\}^k \times G_1 \times Z_q^* \times G_1$$

where k is the security length for identifiers. This is because g_{LN} is a point over the underlying elliptic curve, and the last term h of the other operand belongs to G_1. Usually, the notation $\{0,1\}^*$ represents the set of all binary strings. That means the string length of output of H_3 is not fixed. It seems very difficult to construct such a hash function.

The output of any practical hash function is of 256 bits or 512 bits, like SHA-256, SHA-512. In view of this significant restriction, we find the effective string length of operand $ID_{LN}\|R_{LN}\|T_{LN}\|h$ is also of 256 bits or 512 bits. Hence, we have

$$W = (ID_{LN}\|R_{LN}\|T_{LN}\|h) \oplus (00\cdots0\|H_3(g_{LN}))$$

The substring $ID_{LN}\|R_{LN}\|T_{LN}$ or $ID_{LN}\|R_{LN}$ is almost copied into the string of W. Therefore, an adversary can retrieve the identity ID_{LN} by capturing W via the open channel. We want to stress that one needs to use other encryption mechanics (block cipher, stream cipher, etc.) to securely transfer such long target strings.

4 Further discussions

As we see, the leaf node LN needs to compute

$$g_{LN} = (x + es_{LN})(R_{CS} + H_1(ID_{CS} \| R_{CS})P_0)$$

where R_{CS} is specified as a private key of the target cloud server CS. That means the LN has to invoke the other party's private key. Clearly, the specification is not reasonable. In fact, it is better to specify R_{CS} as a public key of the cloud server CS. Since one cannot retrieve R_{CS} from the exchanged data $\{W, X_{LN}, Y_{CS}, T_{CS}\}$, the server anonymity is certainly reserved.

Notice that the hash functions H_1, H_2, H_4, H_5 have a common codomain Z_q^*. So, it is better to define a hash function $H : \{0,1\}^* \to Z_q^*$. All input strings are concatenated by the operator "$\|$". In the original computation for

$$H_5(key_{LN} \| ID_{LN} \| ID_{CS} \| Y_{CS} \| X_{LN})$$

(the definition $H_5 : \{0,1\}^* \times G_2^3 \to Z_q^*$ should be revised as $H_5 : G_1 \times \{0,1\}^k \times \{0,1\}^k \times G_1 \times G_1 \to Z_q^*$), one needs to check that the three points key_{LN}, Y_{CS}, Y_{CS} belong to the elliptic curve group G_1. But in the revision

$$H(key_{LN} \| ID_{LN} \| ID_{CS} \| Y_{CS} \| X_{LN})$$

the computational cost for this checking is exempted. The subtle difference between H_5 and H has often been ignored by some researchers.

5 Conclusion

In this note, we show that the Cheng *et al.*'s authentication scheme is flawed. It seems difficult to revise the scheme because the underlying encryption is misused. The findings could be helpful for the future work on designing such schemes.

References

[1] A. Asari, M. R. Alagheband, M. Bayat, and M. R. Asaar. A new provable hierarchical anonymous certificateless authentication protocol with aggregate verification in ADS-B systems. *Comput. Networks*, 185:107599, 2021.

[2] S. Bouakkaz and F. Semchedine. New efficient certificateless scheme-based conditional privacy preservation authentication for applications in VANET. *Veh. Commun.*, 34:100414, 2022.

[3] Q. Cheng, Y. Li, W. Shi, and X. Li. A certificateless authentication and key agreement scheme for secure cloud-assisted wireless body area network. *Mob. Networks Appl.*, 27(1):346–356, 2022.

[4] T. Gowri, G. S. Rao, P. V. Reddy, N. B. Gayathri, D. V. Reddy, and M. Padmavathamma. Efficient and secure certificateless aggregate signature-based authentication scheme for vehicular ad hoc networks. *IEEE Internet Things J.*, 8(3):1908–1920, 2021.

[5] W. Hathal, H. S. Cruickshank, Z. Sun, and C. Maple. Certificateless and lightweight authentication scheme for vehicular communication networks. *IEEE Trans. Veh. Technol.*, 69(12):16110–16125, 2020.

[6] A. Imghoure, A. El-Yahyaoui, and F. Omary. ECDSA-based certificateless conditional privacy-preserving authentication scheme in vehicular ad hoc network. *Veh. Commun.*, 37:100504, 2022.

[7] S. S. Moni and D. Manivannan. CREASE: certificateless and reused-pseudonym based authentication scheme for enabling security and privacy in VANETs. *Internet Things*, 20:100605, 2022.

[8] E. Nkurunziza, L. Tandoh, I. Elfadul, and F. Li. ECAAP-SG: efficient certificateless anonymous authentication protocol for SG. *Secur. Priv.*, 6(1), 2023.

[9] B. Palaniswamy, K. Ansari, A. G. Reddy, A. K. Das, and S. Shetty. Robust certificateless authentication protocol for the SAE J1939 commercial vehicles bus. *IEEE Trans. Veh. Technol.*, 72(4):4493–4509, 2023.

[10] A. Tomar and S. Tripathi. BCAV: blockchain-based certificateless authentication system for vehicular network. *Peer-to-Peer Netw. Appl.*, 15(3):1733–1756, 2022.