A note on "SCPUAK: smart card-based secure protocol for remote user authentication and key agreement"

Zhengjun Cao[1], Lihua Liu[2]

Abstract. We show that the Cherbal-Benchetioui key agreement scheme [Comput. Electr. Eng., 109, 108759 (2023)] fails to keep user anonymity, not as claimed. The scheme simply thinks that user anonymity is equivalent to protecting the user's real identity. But the true anonymity means that the adversary cannot attribute different sessions to target entities, which relates to entity-distinguishable, not just identity-revealable.
Keywords: Authentication, Anonymity, Key agreement, Internet of Things

1 Introduction

The Internet of Things (IoT) is a network of physical devices, which uses a variety of technologies to connect the digital and physical worlds. These devices, such as smart home devices, personal medical devices, can transfer data to one another without human intervention. The core concept of IoT is communication among devices and users. Unique identifiers (UIDs) establish the context of a device within the larger network to enable this communication. Identifiers are patterns, like numeric or alphanumeric strings. One example of a UID that you might be familiar with is an internet protocol (IP) address. They can identify a single device (instance identifier) or the class to which that device belongs (type identifier).

The security of IoT has attracted much attention. In 2017, Lavanya and Natarajan [1] proposed a lightweight key agreement protocol for IoT based on IKEv2. After that, Parne et al. [2] presented a security enhanced authentication key agreement protocol for IoT enabled LTE/LTE-A networks. Garg and Lee [3] designed a secure key agreement for multi-device home IoT environment. Tedeschi et al. [4] discussed a lightweight certificateless key agreement for secure IoT communications. In 2021, Chen et al. [5] put forth a secure blockchain-based group key agreement protocol for IoT. Chatterjee, et al. [6] proposed a lightweight remote user authentication and key management scheme for IoT communication in context of fog computing. Mahmood, et al. [7] designed a seamless anonymous authentication protocol for mobile edge computing infrastructure. In 2023, Nikooghadam et al. [8] investigated a highly efficient authentication and key agreement scheme based on ECDH for RFID in IOT environment. Tomar et al. [9] presented a blockchain-assisted authenticated key agreement scheme for IoT-based healthcare system. Zahednejad et al. [10] presented a big data based authentication and key agreement scheme for IoT with revocability.

Recently, Cherbal and Benchetioui [11] have also presented a smart card-based protocol for remote user authentication and key agreement. In the considered scenario, there are two entities: user smart

[1]Department of Mathematics, Shanghai University, Shanghai, 200444, China
[2]Department of Mathematics, Shanghai Maritime University, Shanghai, 201306, China. liulh@shmtu.edu.cn

card and remote server. An end-user uses a smart card (SC) to connect to a remote server via a SC reader. Any user who can register to the server and has a SC can be part of the system. The user can have any type of an IoT device that can read SC information to connect to the IoT network. The scheme consists of Initialization, Registration, Login, and Authentication phases.

The scheme is designed to meet many security requirements, including mutual authentication, session-key establishment, user anonymity, and resistance to impersonation attack, reply attack, offline guessing attack, etc. In this note, we show that the scheme fails to keep anonymity, not as claimed.

2 Review of the Cherbal-Benchetioui scheme

Let E be an elliptic curve over a finite field of prime order p. G is a cyclic additive elliptic curve group with a generator g. $H : \{0,1\}^* \to \{0,1\}^l$ is a hash function. $PH(\cdot)$ is a perceptual hash function. Load the system parameters into each user's smart card. The scheme can be briefly depicted as follows (see Table 1).

3 The loss of user anonymity

Anonymity is a security requirement adopted by many protocols [12]. But we find its signification is often misunderstood. We want to stress that the true anonymity means that the adversary cannot attribute different sessions to entities. In other words, it relates to entity-distinguishable, not just identity-revealable. To illustrate the signification, we refer to Fig.1.

In Fig.a, the user's identity ID uniquely corresponds to the parameter A_4. Thus, different sessions launched by this user can be attributed to the entity by checking the consistency of A_4. In this case, *the parameter A_4 can be eventually used to recognize this entity.* But in Fig.b, ID only corresponds to different temporary identities $MID^1, \cdots, MID^n$. Therefore, the adversary cannot attribute different sessions to the entity, even though these sessions are launched by this entity.

As for the anonymity, the original argument says that (page 11, Ref.[11]):

> *Our proposed scheme grants the user anonymity. In all phases, the ID entered by the user is protected by a one-way hash function: $MID = H(ID)$ and is never sent directly to the server. Besides, to compute the parameter Y, ID is first wrapped with the hash function and XOR operation in $X = H(ID) \oplus MP$ and then wrapped with XOR and scalar multiplication of ECC in $Y = (X \oplus MB) \cdot g$. Thus, the adversary will not be able to guess the identity of the user even if he happens to know Y.*

We find the argument is not sound. It simply thinks that anonymity just equals to protecting the original identity.

As we see, the identity of a person or thing is the characteristics that distinguish it from others. In the scheme, the real identity ID could be a regular string of some meanings, while the parameters A_4 is a random string, i.e., $A_4 = k \cdot Y$, generated by the remote server for long-term use. Since a real identity uniquely corresponds to the parameter A_4, one should prevent both identifier ID and the parameter A_4 from exposure. But in the scheme the adversary can capture A_4 via the open channel and attribute sessions to the user by checking the consistency of A_4.

Table 1: The Cherbal-Benchetioui key agreement scheme

User smart card	Registration	Remote server
Input identity ID, password PW. Imprint the biometric B_i. The SC picks the timestamp T_1, computes $MID = H(ID)$, $MP = H(PW), MB = PH(B_i)$, $X = MID \oplus MP, Y = (X \oplus MB) \cdot g$	$\xrightarrow[\text{[secure channel]}]{MID,\ Y,\ T_1}$	Check the tiemstamp. If valid, pick the timestamp T_2, and a secret key k. Compute $MV = (MID \oplus k) \cdot g$.
Check the timestamp. If valid, store $\{MV, Y\}$.	$\xleftarrow{MV,\ T_2}$	Store $\{Y, MID, k\}$.
User smart card: $\{MV, Y\}$	Login & Authentication	Remote server: $\{Y, MID, k\}$
Input ID, PW, B_i. Compute $MID = H(ID), MP = H(PW)$, $MB = PH(B_i), X = MID \oplus MP$. Check $Y = (X \oplus MB) \cdot g$. If so, pick the timestamp T_3 and a nonce r_1. Compute $MID_1 = H(MID \oplus T_3)$, $A_1 = r_1 \cdot g, A_2 = r_1 \cdot MV$.	$\xrightarrow[\text{[open channel]}]{MID_1,\ A_1,\ A_2,\ T_3}$	Check the timestamp. If valid, check that $MID_1 = H(MID \oplus T_3)$ and $A_2 = (MID \oplus k) \cdot A_1$. If so, pick the timestamp T_4. Compute $A_3 = k \cdot g, A_4 = k \cdot Y$, $MID_2 = H(MID \oplus T_4)$.
Check the timestamp. If valid, check that $A_4 = (X \oplus MB) \cdot A_3$, and $MID_2 = H(MID \oplus T_4)$. If so, set $Skey = r_1 \cdot A_3$.	$\xleftarrow{MID_2,\ A_3,\ A_4,\ T_4}$	Set $Skey = k \cdot A_1$.

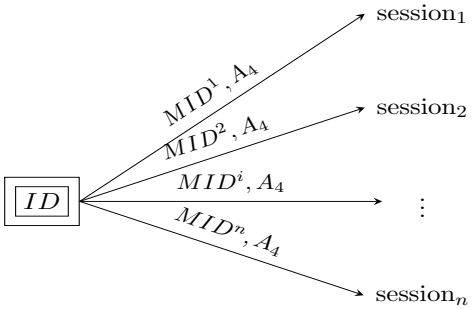

Fig.a: The false anonymity
(with the same identifier A_4)

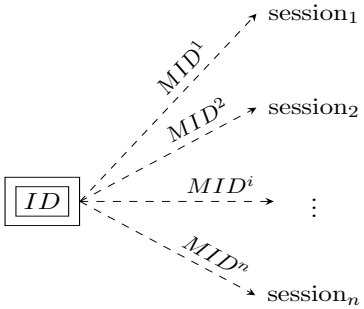

Fig.b: The true anonymity
(with different identifiers MID^i)

Figure 1: False anonymity versus true anonymity

4 Further discussions

It is worth noting that a member's identifier in the system is public and available. Otherwise, such an identifier loses its signification. Suppose Υ is the set of all identifiers in the system. The adversary who has captured $\{MID_1, T_3\}$ or $\{MID_2, T_4\}$ via open channels, can test

$$MID_1 = H(H(\chi) \oplus T_3), \quad \chi \in \Upsilon$$

or

$$MID_2 = H(H(\chi) \oplus T_4), \quad \chi \in \Upsilon$$

Once χ is searched out, the adversary can affirm that $\chi = ID$ due to the collision-free property of the hash function. Practically, the size of Υ is moderate and the success probability of above test is not negligible. That means the user's real identity ID can also be retrieved.

5 Conclusion

We show that the Cherbal-Benchetioui key agreement scheme is flawed. It seems difficult to revise the scheme because of its simple secret-key invoking mechanism. The findings in this note could be helpful for the future work on designing such schemes.

References

[1] M. Lavanya, V. Natarajan: Lightweight key agreement protocol for IoT based on IKEv2. *Comput. Electr. Eng.*, 64, 580-594 (2017)

[2] B. L. Parne, S. Gupta, N. S. Chaudhari: PSE-AKA: Performance and security enhanced authentication key agreement protocol for IoT enabled LTE/LTE-A networks. *Peer-to-Peer Netw. Appl.*, 12(5), 1156-1177 (2019)

[3] A. Garg, T. Lee: Secure key agreement for multi-device home IoT environment. *Internet Things*, 11, 100249 (2020)

[4] P. Tedeschi, S. Sciancalepore, A. Eliyan, R. D. Pietro: LiKe: Lightweight Certificateless Key Agreement for Secure IoT Communications. *IEEE Internet Things J.*, 7(1), 621-638 (2020)

[5] C. M. Chen, X. Deng, W. Gan, J. Chen, SK H. Islam: A secure blockchain-based group key agreement protocol for IoT. *J. Supercomput.*, 77(8), 9046-9068 (2021)

[6] U. Chatterjee, S. Ray, M. K. Khan, M. Dasgupta, C. M. Chen: An ECC-based lightweight remote user authentication and key management scheme for IoT communication in context of fog computing. *Computing*, 104(6), 1359-1395 (2022)

[7] K. Mahmood, M. F. Ayub, S. Z. Hassan, Z. Hassan, Z. Lv, S. A. Chaudhry: A seamless anonymous authentication protocol for mobile edge computing infrastructure. *Computer Communications*, 186, 12-21 (2022)

[8] M. Nikooghadam, H. R. Shahriari, S. T. Saeidi: HAKECC: Highly efficient authentication and key agreement scheme based on ECDH for RFID in IOT environment. *J. Inf. Secur. Appl.*, 76, 103523 (2023)

[9] A. Tomar, N. Gupta, D. Rani, S. Tripathi: Blockchain-assisted authenticated key agreement scheme for IoT-based healthcare system. *Internet Things*, 23, 100849 (2023)

[10] B. Zahednejad, T. Huang, S. Kosari, X. Ren: A Lightweight, Secure Big Data-Based Authentication and Key-Agreement Scheme for IoT with Revocability. *Int. J. Intell. Syst.*, 1-19 (2023)

[11] S. Cherbal, R. Benchetioui: ScPUAK: smart card-based secure protocol for remote user authentication and key agreement. *Comput. Electr. Eng.*, 109(Part B), 108759 (2023)

[12] A. Menezes, P. Oorschot, S. Vanstone: *Handbook of Applied Cryptography*, CRC Press, 1996.