On the Anonymity of One Authentication and Key Agreement Scheme for Peer-to-Peer Cloud

Zhengjun Cao, Lihua Liu

Abstract. Peer-to-peer communication systems can provide many functions, including anonymized routing of network traffic, massive parallel computing environments, and distributed storage. Anonymity refers to the state of being completely nameless, with no attached identifiers. Pseudonymity involves the use of a fictitious name that can be consistently linked to a particular user, though not necessarily to the real identity. Both provide a layer of privacy, shielding the user's true identity from public view. But we find their significations are often misunderstood. In this note, we clarify the differences between anonymity and pseudonymity. We also find the Zhong et al.'s key agreement scheme [IEEE TCC, 2022, 10(3), 1592-1603] fails to keep anonymity, not as claimed.
Keywords: Key agreement; Anonymity; Pseudonymity; Mutual authentication; Peer-to-peer cloud.

1 Introduction

In peer-to-peer (P2P) communication systems, each party has the same capabilities and either party can initiate a communication session. P2P systems can provide anonymized routing of network traffic, massive parallel computing environments, distributed storage, and so on. In 2018, Nguyen and Chang [8] designed a biometric-based three-party authenticated key exchange for dynamic P2P systems. Parne et al. [10] proposed a security enhanced authentication key agreement protocol for P2P networks. Tahavori et al. [2, 13–15] presentedd some authenticated key agreement schemes for smart grid. In 2023, Chen et al. [3, 9] discussed two provably-secure authenticated key agreement protocols for healthcare systems. Das et al. [4] presented a non-linear multi-objective technique for hybrid P2P communication. Khodoomi et al. [5, 7, 11, 12] discussed P2P energy trading case. Alfaverh et al. [1] investigated a dynamic P2P electricity market model.

In 2022, Zhong et al. [16] have also presented a mutual authentication and key agreement scheme based on elliptic curve certificate-free cryptography for peer-to-peer cloud. It is designed to meet many security requirements, such as mutual authentication, session key establishment, identity anonymity, identity traceability, perfect forward secrecy, resistance to replay attack, man-in-the-middle attack, impersonation attack, etc. In this note, we show that the scheme fails to keep anonymity, not as claimed. We also clarify the signification of true anonymity. To the best of our knowledge, it is the first time to clarify the explicit signification and the differences between anonymity and pseudonymity.

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

2 Review of the Zhong et al.'s scheme

In the proposed scenario, there are three entities: cell phone user U, request data cloud server C_i, and source data cloud server U_j. It consists of three phases: initialization, login, and cloud handshake.

Let $E(F_p)$ be an elliptic curve, G_q be an additive cyclic group over the curve with a base point P, where p, q are two large prime numbers. Let $E_k()$ be a symmetric key encryption with the key k. The user U picks $\omega \in Z_q^*$ and sets it as the private key, corresponding to the public key $P_{pub} = \omega P$. Choose four one-way secure hash functions:

$$H_1 : \{0,1\}^* \times G_q \to Z_q^*, \quad H_2 : \{0,1\}^* \times G_q \times G_q \times \{0,1\}^* \to Z_q^*$$
$$H_3 : \{0,1\}^* \times \{0,1\}^* \times G_q \times G_q \times \{0,1\}^* \times G_q \times G_q \to Z_q^*$$
$$H_4 : \{0,1\}^* \times \{0,1\}^* \times G_q \times G_q \times G_q \times G_q \times G_q \times \{0,1\}^* \to Z_q^*$$

Finally, the user U publishes system arguments as,

$$argums = \{E(F_p), p, q, P, P_{pub}, H_1, H_2, H_3, H_4\}$$

and saves ω secretly. The other phases can be depicted as follows (see Table 1).

3 Anonymity versus pseudonymity

Anonymity refers to the state of being completely nameless, with no attached identifiers. Pseudonymity involves the use of a fictitious name that can be consistently linked to a particular user, though not necessarily to the real identity [6]. Both provide a layer of privacy, shielding the user's true identity from public view. However, the key difference lies in traceability. While anonymous actions are designed to be unlinkable to any one individual, pseudonymous actions can be traced back to a certain entity.

We want to stress that the true anonymity means that the adversary cannot attribute different sessions to users. In other words, it relates to entity-distinguishable, not just identity-revealable. To illustrate the signification, we refer to Fig.1.

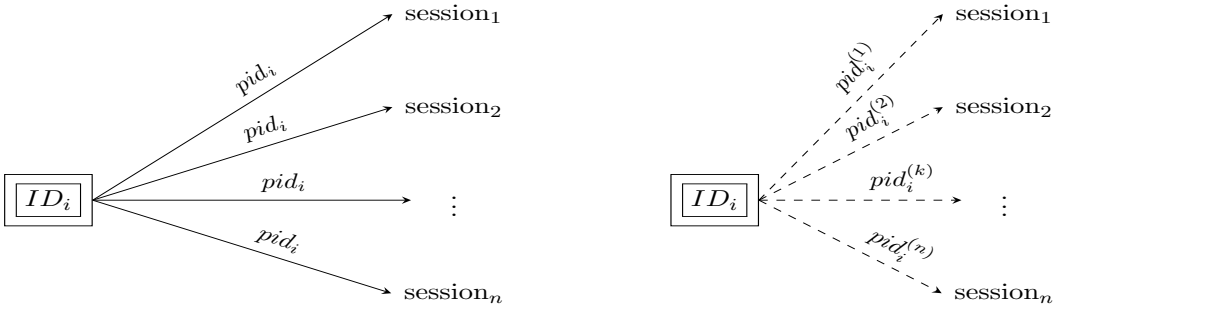

Fig.a: Pseudonymity
(with the same identifier pid_i)

Fig.b: Anonymity
(with different and irregular identifiers $pid_i^{(k)}$)

Figure 1: Pseudonymity versus anonymity

In Fig.a, the server's identity ID_i uniquely corresponds to the pseudo-identity pid_i. Thus, different sessions launched by this entity can be attributed to the entity by checking the consistency of pid_i.

Table 1: The Zhong *et al.*'s authentication and key agreement scheme

Cloud server: C_i	Cell phone user: U	Cloud server: C_j
Login phase		
Send the identity ID_i.	Pick $r_i, r_j \in Z_q^*$, compute	Send the identity ID_j.
$\xrightarrow{ID_i}$ [secure channel]	$R_i = r_i \cdot P, R_j = r_j \cdot P$	$\xleftarrow{ID_j}$
	$S_i = \omega^{-1} R_i, S_j = \omega^{-1} R_j$,	
	$pid_i = E_\omega(r_i, ID_i)$,	
	$pid_j = E_\omega(r_j, ID_j)$,	
	$\alpha_i = H_1(pid_i, R_i)$,	
Check $y_i \cdot P = S_i + \alpha_i \cdot P_{pub}$.	$\alpha_j = H_1(pid_j, R_j)$,	Check $y_j \cdot P = S_j + \alpha_j \cdot P_{pub}$.
If so, pick $x_i \in Z_q^*$. Set $X_i = x_i \cdot P$.	$y_i = \omega^{-1} \cdot r_i + \omega \cdot \alpha_i$,	If so, pick $x_j \in Z_q^*$. Set $X_j = x_j \cdot P$.
Save $\{x_i, y_i, pid_i, R_i, S_i, X_i\}$.	$y_j = \omega^{-1} \cdot r_j + \omega \cdot \alpha_j$.	Save $\{x_j, y_j, pid_j, R_j, S_j, X_j\}$.
Publish the public key $\{R_i, S_i, X_i\}$.	$\xleftarrow{pid_i, R_i, y_i, S_i}$ $\xrightarrow{pid_j, R_j, y_j, S_j}$	Publish the public key $\{R_j, S_j, X_j\}$.
Cloud server: C_i	**Cloud handshake phase**	Cloud server: C_j
Pick $a_i \in Z_q^*$. Set the timestamp T_i^1.	$\xleftarrow{pid_j}$ $\xrightarrow{pid_i}$ [open channel]	
Compute $A_i = a_i \cdot P$,		Set the timestamp T_j^1. Check the timestamp T_i^1.
$\beta_i = H_2(pid_i, A_i, S_i, T_i^1)$,	$\xrightarrow{\gamma_i,\ A_i,\ V_i,\ T_i^1}$	Compute $\alpha_i = H_1(pid_i, R_i)$,
$\gamma_i = x_i \cdot (a_i + x_i \cdot \beta_i + y_i)^{-1} \bmod q$,		$\beta_i = H_2(pid_i, A_i, S_i, T_i^1)$,
$V_i = H_3(pid_i, pid_j, R_i, R_j, \gamma_i, A_i, X_i)$.		$R_i' = A_i + \beta_i \cdot X_i + \alpha_i \cdot P_{pub} + S_i$, $X_i' = \gamma_i \cdot R_i'$.
		Check $V_i = H_3(pid_i, pid_j, R_i, R_j, \gamma_i, A_i, X_i')$.
		If so, pick $a_j \in Z_q^*$, compute
Check the timestamp T_j^1. Compute		$A_j = a_j \cdot P$, $\beta_j = H_2(pid_j, A_j, S_j, T_j^1)$,
$\alpha_j = H_1(pid_j, R_j)$, $\beta_j = h_2(pid_j, A_j, S_j, T_j^1)$,		$\gamma_j = x_j \cdot (a_j + x_j \cdot \beta_j + y_j)^{-1} \bmod q$,
$R_j' = A_j + \beta_j \cdot X_j + \alpha_j \cdot P_{pub} + S_j$, $X_j' = \gamma_j \cdot R_j'$.	$\xleftarrow{\gamma_j,\ A_j,\ V_j,\ T_j^1}$	$V_j = H_3(pid_i, pid_j, R_i, R_j, \gamma_j, A_j, X_j)$,
Check $V_j = H_3(pid_i, pid_j, R_i, R_j, \gamma_j, A_j, X_j')$.		$sk_j = H_4(pid_i, pid_j, R_i, R_j, V_i, V_j, x_j \cdot X_i', T_j^1)$.
If so, compute the session key		
$sk_i = H_4(pid_i, pid_j, R_i, R_j, V_i, V_j, x_i \cdot X_j', T_j^1)$.		

In this case, *the unique pseudo-identity pid_i can be eventually used to recognize this entity.* But in Fig.b, ID_i only corresponds to different temporary identities $pid_i^{(1)}, \cdots, pid_i^{(n)}$. Therefore, the adversary cannot attribute different sessions to the entity, even though these sessions are launched by this entity.

4 The Loss of anonymity in Zhong et al.'s scheme

The original argument says that (page 1599, Ref.[16]):

> *The two parties participating in the cloud handshakes and interacts with anonymous identities $pid_i = E_\omega(r_i, ID_i)$ and $pid_j = E_\omega(r_j, ID_j)$ in the PCAKA protocol. For them, anonymity protects the privacy of their identities when interacting with data on public channels. The adversary can not extract the $ID_i(ID_j)$ from the $pid_i(pid_j)$. Thus, the proposed PCAKA protocol supports cloud anonymity.*

We find the argument is not sound. It simply thinks that anonymity 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_i could be a regular string of some meanings, while the pseudo identity pid_i is a random string, i.e., $pid_i = E_\omega(r_i, ID_i)$, issued by the cell phone user U for long-term use. Since a real identity uniquely corresponds to a pseudo-identity, one should prevent both identifiers ID_i and pid_i from exposure. But in the scheme the adversary can capture pid_i via the open channel and attribute sessions to the entity by checking the consistency of the pseudo identifier.

The scheme simply thinks that anonymity is equivalent to protecting the 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.

5 Further discussions

The cloud server C_i needs to publish the public parameters R_i, S_i, X_i. These parameters will be invoked by other parties. For example, the cloud server C_j will invoke these public parameters to compute

$$\alpha_i = H_1(pid_i, R_i), \ \beta_i = H_2(pid_i, A_i, S_i, T_i^1)$$

The parameters are published for long-term use, not just for a single session. So, they can be used to recognize the target entity. To keep anonymity, these parameters should be updated in each session.

The scheme uses four hash functions H_1, H_2, H_3, H_4 with a same codomain Z_q^*. It suffices to specify a hash function $H : \{0,1\}^* \to Z_q^*$, in which all input strings are concatenated by the operator "$\|$". Hence, we have

$$\begin{aligned}
&\alpha_i = H(pid_i \| R_i), \quad \beta_i = H(pid_i \| A_i \| S_i \| T_i^1) \\
&V_i = H(pid_i \| pid_j \| R_i \| R_j \| \gamma_i \| A_i \| X_i) \\
&sk_i = H(pid_i \| pid_j \| R_i \| R_j \| V_i \| V_j \| x_i \cdot X_j' \| T_j^1) \\
&sk_j = H(pid_i \| pid_j \| R_i \| R_j \| V_i \| V_j \| x_j \cdot X_i' \| T_j^1)
\end{aligned}$$

The simplification can save much cost. Note that in the original computation of $\beta_i = H_2(pid_i, A_i, S_i, T_i^1)$, one needs to check $A_i \in G_q$ and $S_i \in G_q$, i.e., both two points belong to the elliptic curve group G_q. The subtle difference between H_2 and H is neglected by some researchers.

6 Conclusion

We show that the Zhong et al.'s key agreement scheme fails to keep anonymity. We also clarify the signification of anonymity and pseudonymity. The findings in this note could be helpful for the future work on designing such schemes.

References

[1] F. Alfaverh, M. Denai, and Y. Sun. A dynamic peer-to-peer electricity market model for a community microgrid with price-based demand response. *IEEE Trans. Smart Grid*, 14(5):3976–3991, 2023.

[2] C. M. Chen, L. Chen, Y. Huang, S. Kumar, and J. M. T. Wu. Lightweight authentication protocol in edge-based smart grid environment. *EURASIP J. Wirel. Commun. Netw.*, 2021(1):68, 2021.

[3] C. M. Chen, S. Liu, X. Li, SK H. Islam, and A. K. Das. A provably-secure authenticated key agreement protocol for remote patient monitoring iomt. *J. Syst. Archit.*, 136:102831, 2023.

[4] S. K. Das, N. Dey, R. G. Crespo, and E. H. Viedma. A non-linear multi-objective technique for hybrid peer-to-peer communication. *Inf. Sci.*, 629:413–439, 2023.

[5] M. R. Khodoomi and H. Sahebi. Robust optimization and pricing of peer-to-peer energy trading considering battery storage. *Comput. Ind. Eng.*, 179:109210, 2023.

[6] A. Menezes, P. Oorschot, and S. Vanstone. *Handbook of Applied Cryptography*. CRC Press, USA, 1996.

[7] M. Mishra, A. Singh, R. K. Misra, and D. Singh. Peer-to-peer energy trading with active participation of distributed generation. *IEEE Internet Things J.*, 10(23):21076–21088, 2023.

[8] N. T. Nguyen and C. C. Chang. Untraceable biometric-based three-party authenticated key exchange for dynamic systems. *Peer-to-Peer Netw. Appl.*, 11(3):644–663, 2018.

[9] V. Panchami, G. Rubell, M. Mahima, and J. Sharon. A provably secure,privacy-preserving lightweight authentication scheme for peer-to-peer communication in healthcare systems based on internet of medical things. *Comput. Commun.*, 212:284–297, 2023.

[10] B. L. Parne, S. Gupta, and 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.

[11] A. A. Raja and S. Grammatico. Bilateral peer-to-peer energy trading via coalitional games. *IEEE Trans. Ind. Informatics*, 19(5):6814–6824, 2023.

[12] A. M. Saatloo, M. A. Mirzaei, and B. M. Ivatloo. A robust decentralized peer-to-peer energy trading in community of flexible microgrids. *IEEE Syst. J.*, 17(1):640–651, 2023.

[13] M. Safkhani, S. Kumari, M. Shojafar, and S. Kumar. An authentication and key agreement scheme for smart grid. *Peer-to-Peer Netw. Appl.*, 15(3):1595–1616, 2022.

[14] V. Sureshkumar, S. Mugunthan, and R. Amin. An enhanced mutually authenticated security protocol with key establishment for cloud enabled smart vehicle to grid network. *Peer-to-Peer Netw. Appl.*, 15(5):2347–2363, 2022.

[15] M. Tahavori and F. Moazami. Lightweight and secure puf-based authenticated key agreement scheme for smart grid. *Peer-to-Peer Netw. Appl.*, 13(5):1616–1628, 2020.

[16] H. Zhong, C. Zhang, J. Cui, Y. Xu, and L. Liu. Authentication and key agreement based on anonymous identity for peer-to-peer cloud. *IEEE Transactions on Cloud Computing*, 10(3):1592–1603, 2022.