Security Analysis of One Anonymous Authentication and Dynamic Group Key Agreement Scheme for Industry 5.0

Kehui Song and Lihua Liu
(Corresponding author: Lihua Liu)

Department of Mathematics, Shanghai Maritime University
Haigang Ave 1550, Shanghai 201306, China
Email: liulh@shmtu.edu.cn

(Received May 1, 2024; Revised and Accepted June 4, 2024; First Online June 6, 2024)

Abstract

We show that Xu *et al.*'s authentication and key agreement scheme [IEEE Trans. Ind. Informatics, 18(10), 7118-7127, 2022] fails to realize its design targets. (1) It confused some operations for bilinear maps and presented some inconsistent computations. (2) The scheme cannot keep user anonymity as claimed. The adversary can use any device's public key stored in the blockchain to test some verification equations to reveal the identity of a target device. The analysis techniques developed in this paper could be helpful for future works on anonymous authentication and dynamic group key agreement.

Keywords: Anonymity; Authentication; Blockchain; Key Agreement

1 Introduction

Group key agreement plays a very important role in some group-based scenarios. In 2012, Chen *et al.* [5] presented a group-based authentication and key agreement scheme. Shimizu *et al.* [23] designed a group secret key agreement based on radio propagation characteristics in wireless relaying systems. Nicanfar and Leung [20] suggested a password-authenticated cluster-based group key agreement for smart grid communication. Naresh and Murthy [18] also presented an elliptic curve based dynamic contributory group key agreement protocol for secure group communication over ad-hoc networks. Ranjani *et al.* [21] proposed an extended identity based authenticated asymmetric group key agreement scheme. Tseng *et al.* [26] discussed the enhancement on one strongly secure group key agreement protocol.

In 2016, Kumar and Tripathi [11] investigated an anonymous ID-based group key agreement protocol without pairings. Naresh and Murthy [19] discussed a group key agreement protocol based on ECDH with integrated signature. Vijayakumar *et al.* [27] analysized an efficient group key agreement protocol for secure P2P communication. P. Hiranvanichakorn [9] presented a provably authenticated group key agreement based on braid groups for the dynamic case. H. Chien [7] suggested a group-oriented range-bound key agreement for Internet of Things scenarios. Lin and Hsu [13] proposed an anonymous group key agreement protocol for multi-server and mobile environments based on Chebyshev chaotic maps. Roychoudhury *et al.* [22] also proposed a group authentication and key agreement for machine

type communication using Chebyshev's polynomial. Xiong *et al.* [29] generated a survey of group key agreement protocols with constant rounds.

In 2020, Gharsallah *et al.* [8] presented an authentication and key agreement protocol for a group of vehicles devices in 5G cellular networks. Mandal *et al.* [14] discussed a certificateless authenticated group key agreement protocol for mobile networks. Chen *et al.* [3] proposed a blockchain-based group key agreement protocol for IoT. Chen and Lee [4] investigated an anonymous group-oriented time-bound key agreement for internet of medical things in telemonitoring using chaotic maps. In 2022, A. Braeken [2] suggested a pairing free asymmetric group key agreement protocol. Lee *et al.* [12] proposed an anonymous dynamic group authenticated key agreements using physical unclonable functions for internet of medical things. Naresh *et al.* [16] suggested a blockchain privacy-preserving smart contract centric dynamic group key agreement for large WSN. Naresh *et al.* [17] also discussed a provably secure sharding based blockchain smart contract centric hierarchical group key agreement for large wireless ad-hoc networks. Wang *et al.* [28] presented a lightweight certificateless group key agreement method without pairing based on blockchain for smart grid. Zhang *et al.* [31] designed a group key agreement protocol for intelligent internet of things system.

In 2023, Chhikara *et al.* [6] discussed a blockchain-based partial group key agreement protocol for intelligent transportation systems. Hsu *et al.* [10] proposed a lightweight authenticated group key agreement realizing privacy protection for resource-constrained IoMT. Nakkar *et al.* [15] investigated a lightweight group authentication scheme with key agreement for edge computing applications. G. Singh [24] designed a group-based efficient authentication and key agreement protocol for LPIoMT using 5G. Subrahmanyam *et al.* [25] presented a multi-group key agreement protocol using secret sharing scheme. Zhang *et al.* [32] presented a dynamic authenticated asymmetric group key agreement with sender non-repudiation and privacy for group-oriented applications.

Recently, Xu *et al.* [30] have also presented an anonymous authentication and dynamic group key agreement scheme for industry 5.0. It is designed to meet many security requirements, such as anonymity and untraceability, session key establishment, forward and backward secrecy, resistance to replay attack, impersonation attack, etc. In this paper, we show that the scheme has some inconsistent computations and fails to keep anonymity, not as claimed.

2 Review of Xu *et al.*'s Scheme

In the proposed scenario, there are two main kinds of entities, device (DE) and private key generator (PKG). The DEs are general nodes, and have mobile capabilities. Each PKG is similar to a group controller responsible for key generation, distribution, management, and group communication tasks. Each group is dynamic, which means that DE may join or leave a group at any time. The scheme consists of seven phases: initialization, registration, authentication without token, authentication with token, group key generation, DE join, and DE leave.

Initialization. The system administrator picks a cyclic additive group G_1 with a generator Q and a cyclic multiplicative group G_2. Both are of the prime order p. Select a bilinear map $e : G_1 \times G_1 \to G_2$ and a private key s, and set the public key as $P_{pub} = sQ$. Pick two random numbers n_{1_j}, n_{2_j}, and a unique identity IDP_j for each PKG_j. Store $\{s, n_{1_j}, n_{2_j}, IDP_j\}$ in the memory of PKG_j. Publish

$$\{p, G_1, G_2, Q, e, P_{pub}, h(\cdot), E_k, D_k\}$$

See Table 1 for descriptions of involved notations. For convenience, we now only depict the registration phase and authentication without token phase as follows (see Table 2).

Table 1: Notations and descriptions

Symbol	Description
TID_i	Temporary identity of the DE_i
IDD_i	The identity of DE_i
IDP_j	The identity of PKG_j
GID_k	The identity of kth group
s, P_{pub}	Private key and public key of all PKGs
S_i, a_i, b_i	The DE_i's private key
W_i, A_i, B_i	The DE_i's public key
ST_i, ET_i	The authorized time slot range $[ST_i, EY_i]$
E_k, D_k	Symmetric encryption/decryption with key k
$\oplus$	Bitwise XOR operation
(a, b)	Concatenation of data a and data b
$h(\cdot)$	A hash function $h(\cdot) : \{0,1\}^* \rightarrow \{0,1\}^l$
$h^a(b)$	Perform $a+1$ hash operations on b

3 Inconsistent Computations

Pairings in elliptic curve cryptography are functions which map a pair of elliptic curve points to an element of the multiplicative group of a finite field. Let n be a positive integer. Let G_1 and G_2 be Abelian groups written in additive notation. Suppose that G_1 and G_2 have exponent n (i.e., $[n]P = 0$ for all $P \in G_1, G_2$). Suppose G_3 is a cyclic group of order n written in multiplicative notation. A pairing is a function $\hat{e} : G_1 \times G_2 \rightarrow G_3$ satisfying:

> *Bilinearity.* For all $P, P' \in G_1$ and all $Q, Q' \in G_2$ we have $\hat{e}(P + P', Q) = \hat{e}(P, Q)\hat{e}(P', Q)$ and $\hat{e}(P, Q + Q') = \hat{e}(P, Q)e(P, Q')$.
>
> *Non-degeneracy.* For all $P \in G_1$, with $P \neq 0$, there is some $Q \in G_2$ such that $\hat{e}(P, Q) \neq 1$. For all $Q \in G_2$, with $Q \neq 0$, there is some $P \in G_1$ such that $\hat{e}(P, Q) \neq 1$.

To this day, the two practical examples of pairings are the Weil and Tate pairings on elliptic curves over finite fields [1]. Both use a non-rational homomorphism $\phi : G_2 \rightarrow G_1$ to construct the so-called self-pairing $e : G_1 \times G_1 \rightarrow G_3$. In view of this fact, we find the Xu *et al.*'s scheme have confused the basic operations for bilinear maps and presented some inconsistent computations. It wrongly specifies that

> *For points (x, y) belonging to G_1 or G_2, we only focus on x. For example, for $Q(x_Q, y_Q)$ and a private key s', we can obtain $(x_{s'Q}, y_{s'Q})$ by point multiplication operation $s'Q$, and the corresponding public key P'_{pub} is $x_{s'Q}$.*

It also wrongly formulates that

$$\begin{aligned} W_i &= h(IDD_i), \\ S_i &= sW_i, \\ DNT_4 &= h(DNT_3, T_2)S_i, \\ DNT_2 &= h(DNT_1, B_i, T_1, GID_k)S_i, \\ e(Q, DNT_2) &= e(P_{pub}, h(DNT_1, B_i, T_1, GID_k)W_i), \\ e(Q, DNT_4) &= e(P_{pub}, h(DNT_3, T_2)W_i). \end{aligned}$$

Table 2: The Xu *et al.*'s authentication and key agreement scheme

DE_i	Registration	PKG_j: $\{s, n_{1_j}, n_{2_j}, IDP_j\}$
Send the join request.	request ⟹	Pick a unique identity IDD_i.
Store $\{IDD_i, W_i, S_i\}$.	⟸ IDD_i, W_i, S_i [secure channel]	Compute $W_i = h(IDD_i), S_i = sW_i$.
		Create a new block containing $\{IDD_i, W_i\}$, and link it to the Blockchain.
DE_i: $\{IDD_i, W_i, S_i\}$	Authentication	PKG_j: $\{s, n_{1_j}, n_{2_j}, IDP_j\}$
Pick random a_i, b_i and group identity GID_k. Set a timestamp T_1 and time-slot $[ST_i, ET_i]$. Compute $A_i = a_iQ, B_i = b_iQ, TK = b_iP_{pub}$, $DNT_1 \leftarrow E_{TK}(IDD_i, ST_i, ET_i, A_i)$, $DNT_2 = h(DNT_1, B_i, T_1, GID_k)S_i$.		
	$DNT_1, DNT_2, B_i, GID_k, T_1$ ⟶ [open channel]	Check the timestamp T_1. Then compute $TK = sB_i$, $(IDD_i, ST_i, ET_i, A_i) \leftarrow D_{TK}(DNT_1)$. Retrieve (IDD_i, W_i) from the blockchain. Check $e(Q, DNT_2) = e(P_{pub}, h(DNT_1, B_i, T_1, GID_k)W_i)$.
		If so, generate TID_i and timestamp T_2. Compute $Seeda_i = h(IDP_j, date, ST_i, ET_i, n_{1_j})$, $Seedb_i = h(IDP_j, date, ST_i, ET_i, n_{2_j})$, $S_i = sW_i, SA_i = h(IDD_i, S_i, Seeda_i, Seedb_i)$, $TS_{a_i} = h^{ST_i - 1}(Seeda_i), TS_{b_i} = h^{z - ET_i}(Seedb_i)$,
	⟵ DNT_3, DNT_4, T_2	$DNT_3 \leftarrow E_{TK}(TID_i, SA_i, TS_{a_i}, TS_{b_i})$, $DNT_4 = h(DNT_3, T_2)S_i$. Insert $(IDD_i, TID_i, Seeda_i, Seedb_i, SA_i, ST_i, ET_i, A_i)$ into the list L, which containing the parameters required to verify each DE's token in each PKG.
Check the timestamp T_2. Then check $e(Q, DNT_4) = e(P_{pub}, h(DNT_3, T_2)W_i)$. If so, $(TID_i, SA_i, TS_{a_i}, TS_{b_i}) \leftarrow E_{TK}(DNT_3)$. Store $(TID_i, SA_i, TS_{a_i}, TS_{b_i}, A_i)$.		

Clearly, $W_i = h(IDD_i)$ is not a point over the underlying elliptic curve. So do DNT_2, DNT_4. Thus, the computations

$$e(Q, DNT_2) = e(P_{pub}, h(DNT_1, B_i, T_1, GID_k)W_i),$$
$$e(Q, DNT_4) = e(P_{pub}, h(DNT_3, T_2)W_i)$$

make no sense. Likewise, the following computations

$$e(x_Q, DNT_2) = e(x_{P_{pub}}, h(DNT_1, B_i, T_1, GID_k)W_i),$$
$$e(x_Q, DNT_4) = e(x_{P_{pub}}, h(DNT_3, T_2)W_i)$$

make no sense, too.

One should remove the above wrong specification and formulate that $W_i = h(IDD_i)Q$ i.e., converting W_i into a point over the underlying elliptic curve. In this case, all

$$DNT_2, h(DNT_1, B_i, T_1, GID_k)W_i, DNT_4, h(DNT_3, T_2)W_i$$

are compatible with the bilinear map.

4 The Loss of Anonymity

Anonymity is a security requirement adopted by many protocols. As for this property, it argues that (page 7124, [30]):

Among the messages sent during the authentication without token phase and authentication with token phase, only DNT_1, DWT_3, and HDE_i contain the IDD_i information. However, IDD_i in DWT_3 and HDE_i is protected by $h()$. In addition, if an adversary wants to get IDD_i from DNT_1, he/she must get the TK key. However, according to the computational Diffie-Hellman (CDH) problem, the adversary cannot obtain TK from P_{pub}, B_i, or Q in polynomial time.

The argument is not sound. In fact, the legitimate PKG_j needs to decrypt DNT_1 to retrieve the identity IDD_i, and then uses it to get the target public key W_i from the blockchain. Though an adversary cannot decrypt the ciphertext, he can access the set $\Upsilon = \{(IDD_i, W_i)\}_{1 \le i \le n}$, which is stored in the blockchain. The adversary who has captured $\{DNT_1, DNT_2, B_i, T_1, GID_k\}$ or $\{DNT_3, DNT_4, T_2\}$ via open channels, can test the equation

$$e(Q, DNT_2) = e(P_{pub}, h(DNT_1, B_i, T_1, GID_k)\chi),$$
$$\text{or} \quad e(Q, DNT_4) = e(P_{pub}, h(DNT_3, T_2)\chi), \ (\rho, \chi) \in \Upsilon$$

Practically, the size of Υ is moderate and the success probability of such testings is not negligible. Once such a public key χ is searched out, the adversary can reveal the target identity. To achieve true anonymity, we think, one should adopt other techniques.

5 Conclusion

We show that the Xu *et al.*'s key agreement scheme is flawed. We hope the findings in this paper could be helpful for the future work on designing such schemes.

Acknowledgements

We thank the National Natural Science Foundation of China (Project 61411146001). We are grateful to the reviewers for their valuable suggestions.

References

[1] I. Blake, G. Seroussi, and N. Smart (edited), *Advances in Elliptic Curve Cryptography.* UK: Cambridge University Press, 2005.

[2] A. Braeken, "Pairing free asymmetric group key agreement protocol," *Comput. Commun.*, vol. 181, pp. 267–273, 2022.

[3] C. Chen, X. Deng, W. Gan, J. Chen, and S. Islam, "A secure blockchain-based group key agreement protocol for iot," *J. Supercomput.*, vol. 77, no. 8, pp. 9046–9068, 2021.

[4] M. Chen and T. Lee, "Anonymous group-oriented time-bound key agreement for internet of medical things in telemonitoring using chaotic maps," *IEEE Internet Things J.*, vol. 8, no. 18, pp. 13939–13949, 2021.

[5] Y. Chen, J. Wang, K. Chi, and C. Tseng, "Group-based authentication and key agreement," *Wirel. Pers. Commun.*, vol. 62, no. 4, pp. 965–979, 2012.

[6] D. Chhikara and et al., "Blockchain-based partial group key agreement protocol for intelligent transportation systems," *IEEE Trans. Veh. Technol.*, vol. 72, no. 12, pp. 16701–16710, 2023.

[7] H. Chien, "Group-oriented range-bound key agreement for internet of things scenarios," *IEEE Internet Things J.*, vol. 5, no. 3, pp. 1890–1903, 2018.

[8] I. Gharsallah, S. Smaoui, and F. Zarai, "An efficient authentication and key agreement protocol for a group of vehicles devices in 5g cellular networks," *IET Inf. Secur.*, vol. 14, no. 1, pp. 21–29, 2020.
[9] P. Hiranvanichakorn, "Provably authenticated group key agreement based on braid groups - the dynamic case," *Int. J. Netw. Secur.*, vol. 19, no. 4, pp. 517–527, 2017.
[10] C. Hsu and et al., "Fast and lightweight authenticated group key agreement realizing privacy protection for resource-constrained iomt," *Wirel. Pers. Commun.*, vol. 129, no. 4, pp. 2403–2417, 2023.
[11] A. Kumar and S. Tripathi, "Anonymous id-based group key agreement protocol without pairing," *Int. J. Netw. Secur.*, vol. 18, no. 2, pp. 263–273, 2016.
[12] T. Lee, X. Ye, and S. Lin, "Anonymous dynamic group authenticated key agreements using physical unclonable functions for internet of medical things," *IEEE Internet Things J.*, vol. 9, no. 16, pp. 15336–15348, 2022.
[13] T. Lin and C. Hsu, "Anonymous group key agreement protocol for multi-server and mobile environments based on chebyshev chaotic maps," *J. Supercomput.*, vol. 74, no. 9, pp. 4521–4541, 2018.
[14] S. Mandal, S. Mohanty, and B. Majhi, "CL-AGKA: certificateless authenticated group key agreement protocol for mobile networks," *Wirel. Networks*, vol. 26, no. 4, pp. 3011–3031, 2020.
[15] M. Nakkar, R. AlTawy, and A. Youssef, "GASE: a lightweight group authentication scheme with key agreement for edge computing applications," *IEEE Internet Things J.*, vol. 10, no. 1, pp. 840–854, 2023.
[16] V. Naresh, V. Allavarpu, and S. Reddi, "Provably secure blockchain privacy-preserving smart contract centric dynamic group key agreement for large WSN," *J. Supercomput.*, vol. 78, no. 6, pp. 8708–8732, 2022.
[17] V. Naresh and et al., "A provably secure sharding based blockchain smart contract centric hierarchical group key agreement for large wireless ad-hoc networks," *Concurr. Comput. Pract. Exp.*, vol. 34, no. 3, 2022.
[18] V. Naresh and N. Murthy, "Elliptic curve based dynamic contributory group key agreement protocol for secure group communication over ad-hoc networks," *Int. J. Netw. Secur.*, vol. 17, no. 5, pp. 588–596, 2015.
[19] V. Naresh and N. Murthy, "Provably secure group key agreement protocol based on ECDH with integrated signature," *Secur. Commun. Networks*, vol. 9, no. 10, pp. 1085–1102, 2016.
[20] H. Nicanfar and V. Leung, "Password-authenticated cluster-based group key agreement for smart grid communication," *Secur. Commun. Networks*, vol. 7, no. 1, pp. 221–233, 2014.
[21] R. Ranjani, D. Bhaskari, and P. Avadhani, "An extended identity based authenticated asymmetric group key agreement protocol," *Int. J. Netw. Secur.*, vol. 17, no. 5, pp. 510–516, 2015.
[22] P. Roychoudhury, B. Roychoudhury, and D. Saikia, "Provably secure group authentication and key agreement for machine type communication using Chebyshev's polynomial," *Comput. Commun.*, vol. 127, pp. 146–157, 2018.
[23] T. Shimizu, H. Iwai, and H. Sasaoka, "Group secret key agreement based on radio propagation characteristics in wireless relaying systems," *IEICE Trans. Commun.*, vol. 95-B, no. 7, pp. 2266–2277, 2012.
[24] G. Singh, "GBEAKA: group-based efficient authentication and key agreement protocol for lpiomt using 5g," *Internet Things*, vol. 22, p. 100688, 2023.
[25] R. Subrahmanyam, N. Rekha, and Y. Rao, "Multi-group key agreement protocol using secret sharing scheme," *Int. J. Secur. Networks*, vol. 18, no. 3, pp. 143–152, 2023.
[26] Y. Tseng, T. Tsai, and S. Huang, "Enhancement on strongly secure group key agreement," *Secur. Commun. Networks*, vol. 8, no. 2, pp. 126–135, 2015.

[27] P. Vijayakumar, R. Naresh, L. Deborah, and S. Islam, "An efficient group key agreement protocol for secure P2P communication," *Secur. Commun. Networks*, vol. 9, no. 17, pp. 3952–3965, 2016.
[28] Z. Wang, R. Huo, and S. Wang, "A lightweight certificateless group key agreement method without pairing based on blockchain for smart grid," *Future Internet*, vol. 14, no. 4, p. 119, 2022.
[29] H. Xiong, Y. Wu, and Z. Lu, "A survey of group key agreement protocols with constant rounds," *ACM Comput. Surv.*, vol. 52, no. 3, pp. 57:1–57:32, 2019.
[30] Z. Xu and et al., "A time-sensitive token-based anonymous authentication and dynamic group key agreement scheme for industry 5.0," *IEEE Trans. Ind. Informatics*, vol. 18, no. 10, pp. 7118–7127, 2022.
[31] Q. Zhang and et al., "A group key agreement protocol for intelligent internet of things system," *Int. J. Intell. Syst.*, vol. 37, no. 1, pp. 699–722, 2022.
[32] R. Zhang, L. Zhang, K. Choo, and T. Chen, "Dynamic authenticated asymmetric group key agreement with sender non-repudiation and privacy for group-oriented applications," *IEEE Trans. Dependable Secur. Comput.*, vol. 20, no. 1, pp. 492–505, 2023.

Biography

Kehui Song is currently pursuing her bachelor degree from Department of Mathematics at Shanghai Maritime University. Her research interests include information security and applied mathematics.

Lihua Liu, associate professor with Department of Mathematics at Shanghai Maritime University, received her PhD degree in applied mathematics from Shanghai Jiao Tong University. Her research interests include combinatorics and cryptography. She has published over 50 academic papers in different journals and conference proceedings, including Information & Computation, Designs, Codes & Cryptography, IEEE Transactions on Cloud Computing, IEEE Transactions on Parallel & Distributed Systems, International Journal of Quantum Information, International Journal of Bifurcation & Chaos, International Journal of Information & Computer Security, International Journal of Network Security.