Hindawi
Security and Communication Networks
Volume 2021, Article ID 6613392, 9 pages
https://doi.org/10.1155/2021/6613392

Research Article

A New Password- and Position-Based Authenticated Key Exchange

Jia Fan,[1] Lanfei Qiao ,[2,3] Yunfei Cao,[3] Shanglin Liu,[1] Wenke Zhang,[1] and Lin Tang[1]

[1]*Sichuan Innovation Center of Industrial Cyber Security, Chengdu 610000, China*
[2]*School of Information Science and Technology, Southwest Jiaotong University, Chengdu 610000, China*
[3]*Science and Technology on Communication Security Laboratory, Chengdu 610000, China*

Correspondence should be addressed to Lanfei Qiao; qiaolanfei@my.swjtu.edu.cn

Received 10 November 2020; Revised 14 January 2021; Accepted 9 February 2021; Published 24 February 2021

Academic Editor: Ximeng Liu

Password-based authenticated key exchange is a popular method for secure authentication and key exchange. With the wide application of unmanned aerial vehicles, position information has also become an important factor in authentication. In this paper, we present a new key exchange protocol, which firstly realizes dual authentication for both password and position, and we propose two applicable scenarios for the PPAKE mechanism: one is unmanned aerial vehicle authentication, and the other one is authentication in the military base. By adding position authentication, the reliability of authentication has improved, and the difficulty of adversarial attacks also increases. Any arbitrary adversary who can listen, tamper, and send messages can only perform an online attack for password guessing at a specified position. Finally, we provide security proofs under the defined model.

1. Introduction

Key exchange protocol is designed to allow two or more parties to negotiate and share session keys over insecure channels to establish an encrypted communication. To achieve secure communication in open and insecure communication channels, Diffie and Hellman [1] in 1976 introduced the concept of public key cryptography and the famous Diffie–Hellman key exchange protocol which establishes a shared session key between two communicating parties. However, the Diffie–Hellman protocol cannot resistant man-in-the-middle attacks or provide dual authentication.

A large number of authentication key exchange protocols have been proposed subsequently [2–5], as well as corresponding applications [6–10]. According to different application scenarios and assumptions, the authentication key exchange protocols are broadly divided into the following two categories: one assumes that each interacting party has a high-entropy private key which can be used to generate a high-entropy session key; the other one assumes that each interacting party only shares a weak password and generates a high-entropy session key through interaction.

Bellovin and Merritt [11] in 1992 first proposed the password-based authentication key exchange (PAKE) protocol, called the BM scheme. Subsequently, there were many improvements based on the BM scheme, but none of these had a security model. Until EUROCRYPT 2000, Boyko et al. [12] presented the first security model of PAKE. Under the random oracle model, the SPAKE scheme in [13] is an efficient provable secure scheme. Under the standard model, Goldreich and Lindell proposed a solution based on one-way functions and zero knowledge in EUROCRYPT 2001, but neither it nor the subsequent theoretical constructs based on it are practical. Katz et al. [14] proposed the first practical password-based solution for provable security with the help of public reference strings in EUROCRYPT 2001, called the KOY scheme. Gennaro and Lindell extended the KOY scheme to a general construction based on smooth projection hashing systems and the choice of secret security encryption schemes in EUROCRYPT 2003 [15]. There has have been much subsequent work based on this scheme [16–19], with [16, 17] being the most efficient.

Xue et al. [20] found that the scheme in [16], requiring six group elements and a random string, is more efficient than other current schemes in the BPR [21] model while

under the standard model. And they presented an improved PAKE protocol by replacing the CCA-secured encryption scheme in [16] with a CCA-secured key encapsulation mechanism (KEM). This protocol finally requires only 5 group elements and 2 short random strings. And the length of a random string is 1/3 log p bit (the size is equal to 1/6 of the length of a group element on an elliptic curve).

In previous proposals, the form of password-based key exchange needs to face the challenge of generating high-entropy session keys from low-entropy keys. The current password-based key exchange protocol is mainly used in the scenario of the server-client, and the mainstream technology adopts a CCA2 secure encryption scheme and a smooth projective hash function.

In many real applications, such as drone control stations and military base communications, the position information is also an important type of authentication information. The first position-based authentication protocol was presented by Chandran et al. [22], where a location can be verified in the 3D space using 4 verifiers. The protocol has many application scenarios, e.g., 4 aircrafts can verify the controller's position and communication between military bases. Followed by this work, a lot of schemes are proposed, such as blockchain-based positioning scheme [23], tracking cryptographic keys and encrypted data using position verification [24], and position-based encryption [25].

2. Motivation

Position and password are all important information in wireless communication. Our basic idea is to combine the result of PAKE in [20] with the secure position-based protocol in [22] to obtain a secure key exchange protocol for dual authentication of position and password (called PPAKE). Dual authentication based on the password and position can improve the reliability of authentication and increase the difficulty of adversarial attacks. To propose a secure PPAKE protocol, we solved the following issues:

(1) How do the four verifiers determine the position information of the participant and verify it simultaneously?

(2) How does the participant verify the password information of the four verifiers and generate a high-entropy session key at the same time?

(3) How do four verifiers generate the same high-entropy session key while verifying the position and password information of the participant?

By applying our PPAKE protocol, four verifiers use a common reference string to authenticate the participant and initiate encrypted communication by sharing the password and position information. The PPAKE protocol includes ElGamal ciphertext, universal projective hash function, key encapsulation mechanism, 4-wise independent hash function, and pseudo-random generator.

The proposed PPAKE protocol can realize the synchronization authentication of password and position information. The prior art authenticates participants unilaterally, but the present technique uses the password and position information to authenticate the joining party and negotiate a common session key to prepare for the next step of private communication. Specifically, the adversary cannot pretend to be the joining party to verify from a location that is inconsistent with its declared location. Any location and password forged by the adversary cannot be authenticated.

Our PPAKE can be widely applied in many scenarios, for example, (1) the communication base station that needs to verify the position and password of the user and authorizes networking and (2) real-life logistics distribution scenarios require password and location information verification to negotiate important content. Other applications, such as unmanned aerial vehicle authentication and military base authentication, will be described in the later section. From what has been discussed above, it is very meaningful to present a key exchange protocol for dual authentication of password and position.

3. Applications of PPAKE

Next, we propose two applicable scenarios for the PPAKE mechanism: one is unmanned aerial vehicle authentication, and the other one is authentication in military base.

3.1. Unmanned Aerial Vehicle Authentication. The unmanned aerial vehicle (UAV) is a kind of unmanned aircraft that uses wireless remote control or flight planning. Due to a series of advantages such as low cost, easy operation, fast image acquisition speed, high ground resolution, not restricted by a fixed environment, and no need to worry about accidental crashes that may cause casualties on board, UAVs have been widely used in map surveying and mapping update, geological survey, natural disaster monitoring, agricultural remote sensing monitoring, and other fields.

Control technology of the UAV refers to the technology of remote control, telemetry, tracking, positioning, and information transmission to the UAV. The corresponding technical facilities consist of a data chain and ground control station. The data chain realizes data transmission and delivery, tracking, and positioning between the ground control station and the UAV. The ground control station is used to realize such functions as mission planning, link control, flight control, load control, flight track display, and parameter and image display, as well as recording and distribution.

To ensure the authenticity of the information content and its source transmitted between the subjects, dual authentication and key exchange should be carried out before information exchange between the UAV and the ground control station. Our PPAKE adopts dual authentication based on the position and password to complete the identity authentication and key exchange between the two parties. When a UAV holding a legal identity and password granted by the ground control station sends a request to the ground control station for authentication and information transmission, it should also submit the encrypted identity, password, and position information.

Then, the ground control station authenticates the information separately. When the ground control station confirms the information, if it matches the prestored information, the session key is generated, and the message is transmitted; otherwise, the request for authentication and message transmission is aborted.

3.2. Military Base. In recent years, several local wars in the world have shown the wide application of information technology in the military field, which has brought about comprehensive and profound changes to the war pattern. With the increasing use of modern communication and computer network technology, the situation of military information carriers has undergone great changes. The hidden danger of information security also spreads from simple document management in the past to information systems, equipment, places, and various links in information operation.

Modern communication technology in the army can be divided into three categories, namely, wired communication, wireless communication, and network communication, which all exist in different ways and have different degrees of security risk. In the process of wireless communication, to remote access system resources or data transmission, the user must obtain appropriate permissions. Dual identity authentication gives a simple and effective security solution to the problem.

Specifically, the PPAKE adopts the form of dual authentication based on the password and position to authenticate a wireless user who has registered with the base and obtained his or her identity ID and password and generate a session key. For a user who holds an ID and password, when sending an access and authentication request to the base station, the user needs to submit the encrypted ID, password, and location information. Then, the base station will authenticate each message separately.

4. Security Model

In this model, we assume that (1) the clocks of all verifiers are synchronized. We require that the pace between verifiers and the participants be the same. (2) The protocol has a fixed set of protocol users. (3) Messages travel at a speed equal to that of radio waves. (4) Each principal can execute the protocol multiple times with different partners. As described above, the PPAKE protocol concludes two phases, namely, the initialization phase and the execution phase.

Initialization phase: in this phase, public parameters are established, each user's position is given, and the unique identifiers of all the verifiers are given to all protocol users. Each participant shares a password with all verifiers. Each password is uniformly chosen from the set $\{1, \ldots, D_n\}$ for some integer D_n depending on n.

Execution phase: in this phase, we separately define how the verifiers, participants, and adversaries execute in these following two security definitions according to [16, 22].

Position-based authentication [22]: in the execution phase, any verifier and adversary can send all the following three types of messages: broadcast messages, directional messages, and private multicast messages. Any participant can send broadcast messages and directional messages. The detailed description of all types of messages is as follows:

(1) Broadcast messages: a broadcast message travels with equal speed in all directions, in concentric hyperspheres centered at the sender's position P, which arrives at a position P' after time t (t is the time the radio waves travel from P to P')

(2) Directional messages: a directional message travels in a region of concentric hyperspheres centered at the sender's position P and arrives at position P' after time t (t is the time the radio waves travel from P to P')

(3) Private multicast messages: a verifier (or an adversary) talks to other verifiers (or other adversaries) via a private channel

A PPAKE protocol in the 3-dimensional space is described as a set of verifiers $\mathrm{Ver} = \{V_1, V_2, \ldots, V_n\}$ at positions $\mathrm{pos}_1, \mathrm{pos}_2, \ldots, \mathrm{pos}_n$, respectively, which take as input a claimed position P' of a participant at position P and jointly return "accept" after interacting with the honest participant (if $P' = P$) and in the absence of any adversarial parties.

Definition 1. A protocol PPAKE satisfies position-based authentication if for any position P (in the tetrahedron enclosed by $\mathrm{pos}_1, \mathrm{pos}_2, \ldots, \mathrm{pos}_n$) and for any adversary $\mathscr{A}_i$ at position $a\mathrm{pos}_i$ with $P \neq a\mathrm{pos}_i$, verifiers $\{V_1, V_2, \ldots, V_n\}$ at positions $\mathrm{pos}_1, \mathrm{pos}_2, \ldots, \mathrm{pos}_n$ jointly return "accept" with a negligible probability ε in the defined security parameter.

Password-based authenticated key exchange [16]: in the execution phase, the adversary is given oracle access to these different instances. All the oracles are described as follows:

(1) Send: this oracle sends message M to instance Π_U^i (denote instance i of user U as Π_U^i) and outputs the message sent by the instance of Π_U^i to the adversary

(2) Execute: if Π_U^i and $\Pi_{U'}^j$ have not yet been used, this oracle executes the protocol between these instances and outputs the resulting transcript to the adversary

(3) Reveal: this oracle outputs the session key sk_U^i to the adversary

Finally, adversary $\mathscr{A}$ makes a single query Test to a fresh instance Π_U^i and outputs a bit b'. In the Test oracle, a random bit b is chosen; if $b = 1$, the adversary is given sk_U^i, and if $b = 0$, the adversary is given a session key chosen uniformly from the appropriate space. $\mathscr{A}$ succeeds if either $b' = b$ or at the end of the experiment, there is an instance Π_U^i that accepts but is not semipartnered with any other instance (semipartnering is defined as follows: instances Π_U^i and $\Pi_{U'}^j$ are partners, or session ids sid_U^i and $\mathrm{sid}_{U'}^j$ agree, except possibly for the final message, and partner ids $\mathrm{pid}_U^i = U'$ and $\mathrm{pid}_{U'}^j = U$.)

Definition 2. A PPAKE protocol Π achieves password-based authenticated key exchange if for all dictionary sizes $\{D_n\}$ and for all PPT adversaries $\mathscr{A}$ making at most $Q(n)$ online

attacks, $\mathcal{A}$ succeeds with advantage $\mathrm{Adv}_{\mathcal{A},\Pi} \stackrel{\mathrm{def}}{=} 2 \cdot \Pr[\mathrm{Succ}] - 1 \le Q(n)/D_n + \varepsilon(n)$, where Succ is the event that the adversary succeeds and ε is negligible in the defined security parameter.

We claim that if protocol Π satisfies both position-based authentication and password-based authenticated key exchange, then protocol Π is a secure PPAKE protocol.

5. Description of PPAKE

In the PPAKE protocol, we assume that (1) all participants of the system have a synchronized clock, and all users have access to the public reference string CRS; (2) all verifiers share the private random number string VRS; (3) the calculation time is negligible relative to the transmission time of the information; and (4) computation for the Diffie–Hellman problem on a group with prime order p is difficult.

The main process of our PPAKE protocol is described in Figure 1, and the details are as follows.

5.1. Initialize Phase. In this phase, all users share a common reference string $\mathrm{CRS} = \{G, p, g, h, H, H_{cr}, \mathrm{PRG}, d, e\}$ and maintain a common clock. In CRS, G is a cyclic group of order p, and generally, the length of p is greater than 160 bits. g and h are random elements on group G. H is a 4-wise independent hash function. H_{cr} is a collision-resistant hash function. PRG is a pseudo-random generator. d and e are elements on group G; specifically, $d = g^{a_1}h^{b_1}$ and $e = g^{a_2}h^{b_2}$ are the public keys for the key encapsulation mechanism (KEM), where a_1, a_2, b_1, and b_2 are random numbers generated when the system is established.

Assume that all verifiers V_i $(i = 1, ..., 4)$ share a random number string $\mathrm{VRS} = (K_1, K_2, K_3, K_4, r)$ through a secure communication channel. Generally, the length of all K_1, K_2, K_3, and K_4 is greater than 80 bits. The length of r is greater than 160 bits, and $t_1, \ldots, t_4$, respectively, represent the time in which the radio waves were transmitted from the verifiers $V_1, \ldots, V_4$ to the position of the participant (write as P for short).

5.2. Execution Phase. Now, we introduce the execution phase, which is described from phase 1 to phase 4.

5.2.1. Phase 1. In this phase, all verifiers send authentication information to P, in which the content of the message sent by the prime verifier is slightly different from those sent by other nonprime verifiers. Figure 2 illustrates the calculation process of the prime verifier V_1. V_1 sends the calculated results, that is, encrypted password and position authentication information, to P. Figure 3 illustrates the calculation process of nonprime verifiers $V_i (i = 2, 3, 4)$. Nonprime verifiers calculate and send the position authentication information, which reaches P at the same time. The computation details are described as follows:

(1) V_1 selects r from VRS and calculates $A = g^r$ and $c' = h^r g^{\pi}$, where π represents the password previously shared between all verifiers and P. Then, V_1 broadcasts $(K_1, A \parallel c')$ at time $T - t_1$, as shown in Figures 1 and 2.

(2) V_2 randomly selects X_1, calculates $K_2' = \mathrm{PRG}(X_1, K_1) \oplus K_2$, and broadcasts (X_1, K_2') at time $T - t_2$, as shown in Figures 1 and 3.

(3) V_3 randomly selects X_2, calculates $K_3' = \mathrm{PRG}(X_2, K_2) \oplus K_3$, and broadcasts (X_2, K_3') at time $T - t_3$, as shown in Figures 1 and 3.

(4) V_4 randomly selects X_3, calculates $K_4' = \mathrm{PRG}(X_3, K_3) \oplus K_4$, and broadcasts $(X_3 K_4')$ at time $T - t_4$, as shown in Figures 1 and 3.

5.2.2. Phase 2. As shown in Figure 4, phase 2 can be divided into three steps, as detailed from Figures 5 to 7. The computation details are described as follows.

Figure 5 illustrates the process of calculating the password-based authentication information. When calculating the password information, P randomly calculates μ, the public key of the hash proof function, and the hash value σ, according to the password-encrypted ElGamal secret message. σ is divided into three parts, which can be written as $\tau_p \| \mathrm{sk}_p \| r_p \leftarrow \sigma$, where τ_p is used to verify the identity of the verifier, sk_p is used to generate the session key, and r_p is used to encapsulate the key and dissimulate the password and location information.

The specific calculation steps are as follows: P randomly selects λ_1 and λ_2 from $\mathbb{Z}q$ (the value of q is related to the safety parameters), computes $\mu = g^{\lambda_1}h^{\lambda_2}$, $c = c' g^{-\pi}$, and $\sigma = A^{\lambda_1}c^{\lambda_2}$, where σ is divided into three equal pieces by bit value $\tau_p \| \mathrm{sk}_p \| r_p \leftarrow \sigma$, then computes $c_{kem} = (g^{r_P}, h^{r_P})$ and $k_{\mathrm{kem}} = H(d^t e^{r_P})$, where $t = H_{cr}(g^{r_P}, h^{r_P}, A \| c', \mathrm{V}_1, \mathrm{P})$; and finally, it outputs $(\mu \| c_{\mathrm{kem}})$ and k_{kem} as $(2 - P - 1)$.

Figure 6 illustrates the process of calculating position-based authentication information K_4 by the information received in phase 1. P computes the position information $K_{i+1} = \mathrm{PRG}(X_i, K_i) \oplus K_{i+1}^{'} (i = 1, 2, 3)$ and outputs K_4 as $(2 - P - 2)$.

Figure 7 illustrates how to compute password and position authentication information $(2 - P - 3)$ from $(2 - P - 1)$ and $(2 - P - 2)$. P computes $\delta = k_{\mathrm{kem}}(\pi \| K_4)$ and broadcasts $(\mu \| c_{\mathrm{kem}} \| \delta)$ to V_i $(i = 1, 2, 3, \text{and } 4)$.

5.2.3. Phase 3. In this phase, all verifiers V_i $(i = 1, 2, 3, \text{and } 4)$ verify P's password and position authentication information, calculate the session key, and reply the authentication information to P.

As shown in Figure 8, all verifiers receive the information from P, calculate the hash value σ, verify the password, and check the consistency of the receiving time and location. After passing all the authentication checks, all verifiers send the first block of σ back to P. The detailed computation process is as follows: when V_i $(i = 1, 2, 3, \text{and } 4)$ receives $(\mu \| c_{\mathrm{kem}} \| \delta)$, it calculates the hash value $\sigma = \mu^r$ and sets $\tau_V \| \mathrm{sk}_v \| r_V \leftarrow \sigma$. Then, V_i verifies c_{kem}, δ, and the receiving time. Only if c_{kem} is equal to (g^{r_V}, h^{r_V}), δ is equal to $H(d^t e^{r_V}) \oplus (\pi \parallel K_4)$, where $t = H_{cr}(g^{r_V}, h^{r_V}, A \| c', V_1, P)$, and the receiving time is equal to $T + t_i$, then V_i sends τ_V as

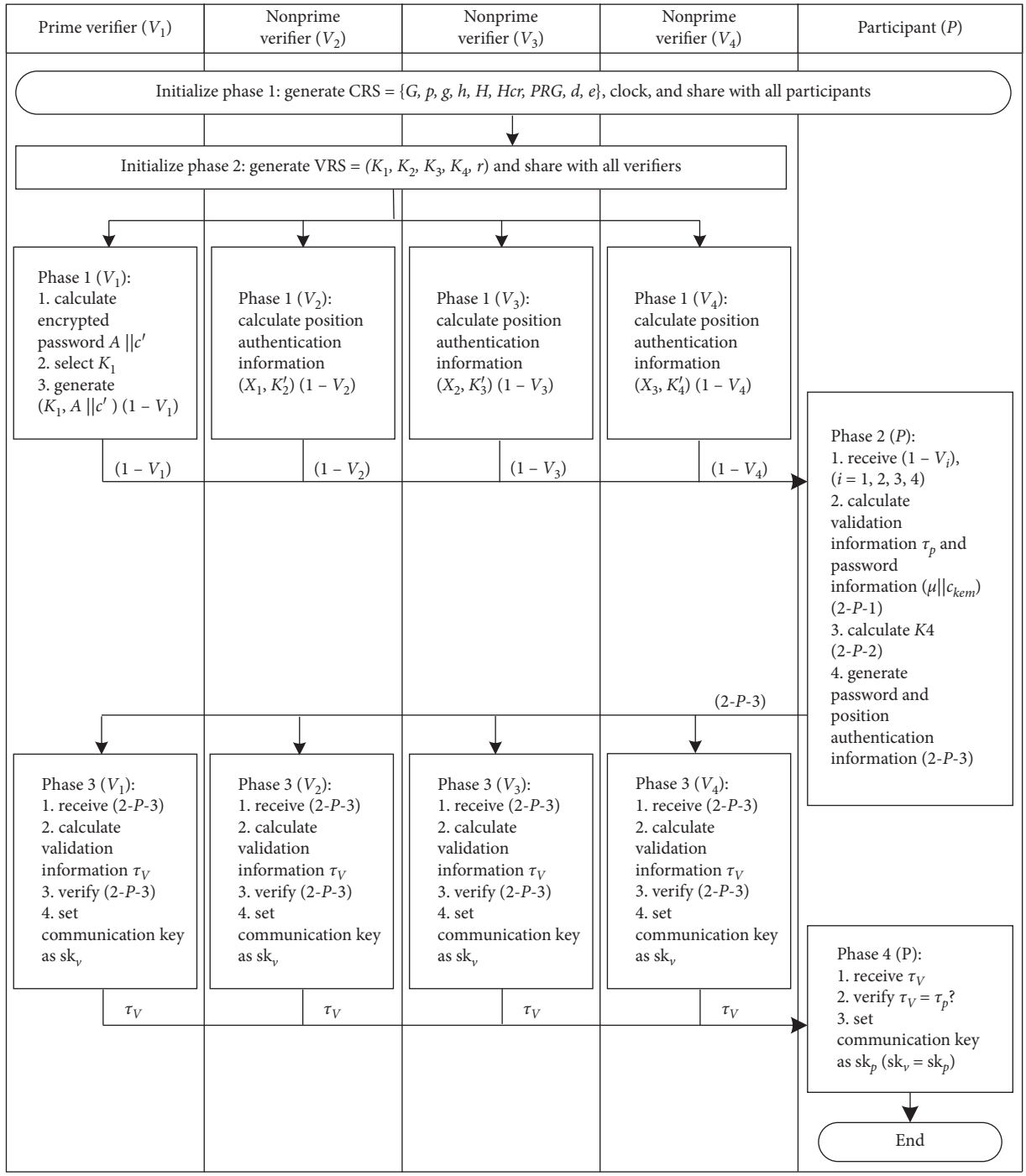

Figure 1: Main process of the PPAKE.

the message of (3–V_i) to P; otherwise, V_i aborts the progress of phase 3. At the end of this phase, V_i sets the negotiated session key as sk_v.

5.2.4. Phase 4. As shown in Figure 9, P determines whether the authentication message τ_V sent by V_i is equal to τ_p. If they are equal, P sets sk_p as the communication key with verifiers; otherwise, P aborts the progress of phase 4.

6. Security Analysis of PPAKE

Our PPAKE protocol dual authenticates the participant by password and position and negotiates a session key for the next step of private communication. In particular, the prime verifier V_1 is responsible for both password-based authenticated key exchange as well as position-based authentication with participant P, while V_2, V_3, and V_4 are mainly responsible for position-based authentication. Our protocol is

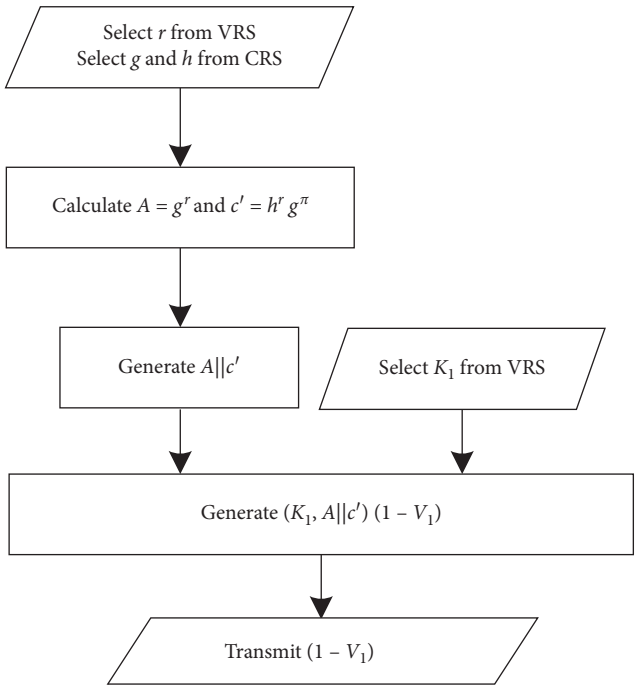

Figure 2: Prime verifier's algorithm for generating the sent message in phase 1.

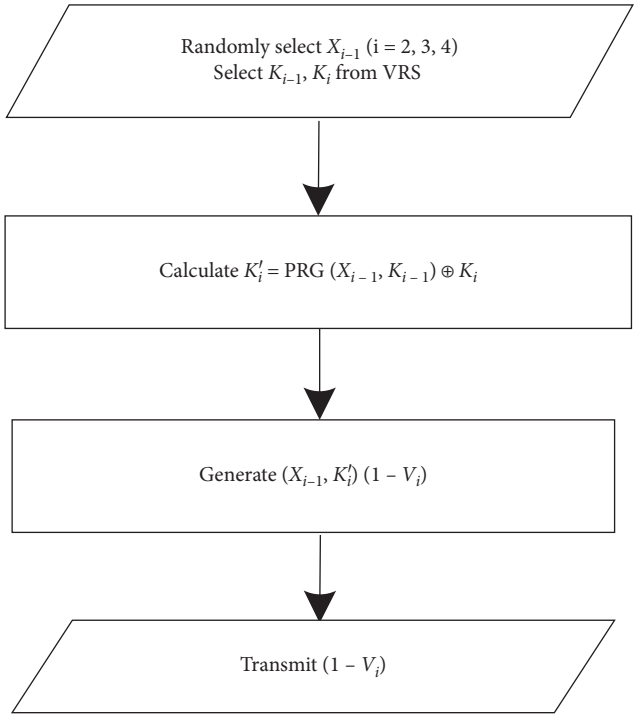

Figure 3: Nonprime verifier's algorithm for generating sent messages in phase 1.

resistant to an active adversary under the standard model. Firstly, we prove that our PPAKE protocol is secure on password-based authenticated key exchange.

Theorem 1. *Assume PKE in [16, 17] is an IND-CPA secure encryption scheme, SPHF (smooth projective hash function) is a ε-$_{smooth}$ SPHF over PKE, and KEM in [26] is an IND-PCA secure KEM, and the PPAKE is secure in the BPR model. In particular, let q_e be the number of execute queries, q_s be the number of send queries, and $q_e + q_s \leq t$; we have*

$$A\ dv_{A,\Pi}(n) \leq \frac{1}{D} + tA\ dv^{\mathrm{CPA}}_{B,\mathrm{Enc}} + t\epsilon_{\mathrm{smooth}} + tA\ dv^{\mathrm{kem-pca}}_{E}. \tag{1}$$

Proof of Theorem 1. In our PPAKE, we use a weak secure notion of KEM, namely, security against plaintext-checkable attack (PCA). Let PKE = (KGen, Enc, Dec) be an IND-CPA secure encryption. Let KEM = ($\mathrm{KGen_{kem}}$, $\mathrm{Enc_{kem}}$, $\mathrm{Dec_{kem}}$) be an IND-PCA secure KEM with KeySp = D. Let PRG be a pseudo-random generator.

We redescribe our PPAKE as follows, in which the position-based authentication part is omitted: in phase 1, V_1 sends $(A\|c')$ to P; in phase 2, P broadcasts $(\mu\|c_{\mathrm{kem}})$; in phase 3, every verifier computes the negotiated key as sk_v and sends τ_V to P; and finally, in phase 4, P checks the value of τ_V and computes similarly as in [20]. PAKE protocol assumes that, in phase 3, only V_1 will compute the negotiated key. In PPAKE, we assume that V_2, V_3, and V_4 can get the value of r from VRS, so they have the ability to compute the negotiated key. At the end of the protocol, all verifiers and the participant share the same session key. People without r cannot compute the shared key. Therefore, the security proof of our PPAKE can also follow the security proof in [20]. Xue et al. proved that their PAKE is secure in the BPR model; the security proof sketch is as follows.

The proof proceeds via a sequence of experiments. Let "G_i" denote the sequence of experiments and denote the advantage of adversary $\mathcal{A}$ in "G_i" as $\mathbf{A}\ \mathbf{dv}_{A,Gi(n)} = 2\Pr[A \text{ succeeds in } G_i] - 1$. Let G_0 be the experiment of BPR challenge. The proof is separated into two phases: the first phase (from G_1 to G_5) bounds out the advantage of execute queries, and the second phase (from G_6 to G_{10}) bounds out the advantage of send queries. The detailed descriptions of G_1 to G_{10} are the same as Theorem 2 in [20]. Finally, summing up all the gap advantages, we finally have $\mathbf{A}\ \mathbf{dv}_{A,\Pi}(n) \leq 1/D + t\mathbf{A}\ \mathbf{dv}^{\mathrm{CPA}}_{B,\mathrm{Enc}} + t\epsilon_{\mathrm{smooth}} + t\mathbf{A}\ \mathbf{dv}^{\mathrm{kem-pca}}_{E}$.

In the following, we analyze the security of position-based authentication. The completeness follows from the fact that verifiers can compute K_4 from the stored Xi values, and the participant can also compute K_4 since all the information required is gathered at time T at P. Now, we prove that our PPAKE protocol is secure on position-based authentication.

We redescribe the position-based authentication part in our PPAKE as follows: in phase 1, V_1 broadcasts $(A\|c', K_1)$ at time $T - t_1$, and V_i $(i = 2, 3, 4)$ broadcasts (X_{i-1}, K_i') at time $T - t_i$; in phase 2, P calculates $K_{i+1} = \mathrm{PRG}(X_i, K_i) \oplus K_{i+1}'$ $(i = 1, 2, 3)$ and broadcasts δ, where $\delta = k_{\mathrm{kem}} \oplus (\pi\|K_4)$, $k_{\mathrm{kem}} = H(d^t e^{r_P})$, and $t = H_{cr}(g^{r_P}, h^{r_P}, A\|c', \mathrm{V}_1, \mathrm{P})$; and in phase 3, all verifiers verify δ and the receiving time. If the verification passed,

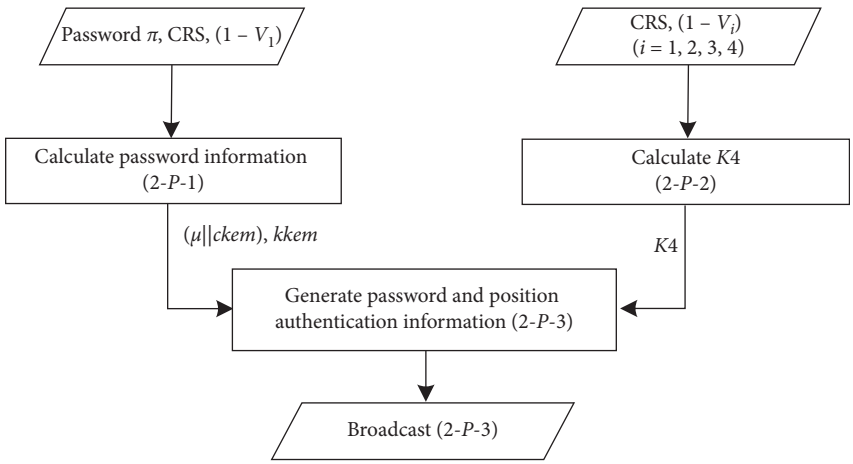

Figure 4: The participant's algorithm for generating the authentication information in phase 2.

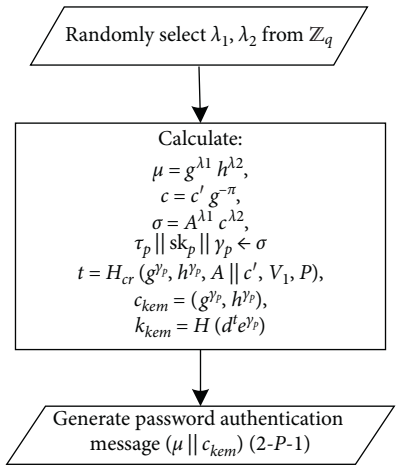

Figure 5: The participant's algorithm for calculating the password-based authentication information.

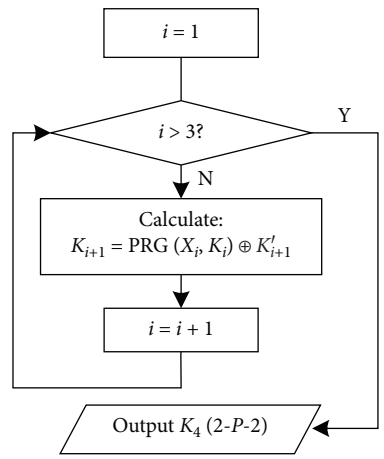

Figure 6: The participant's algorithm for calculating position-based authentication information.

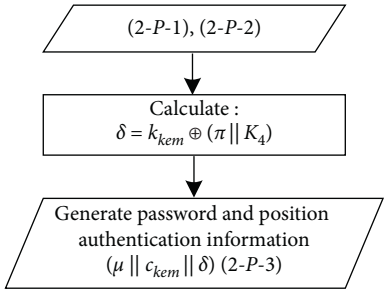

Figure 7: The participant's algorithm for generating password and position authentication information.

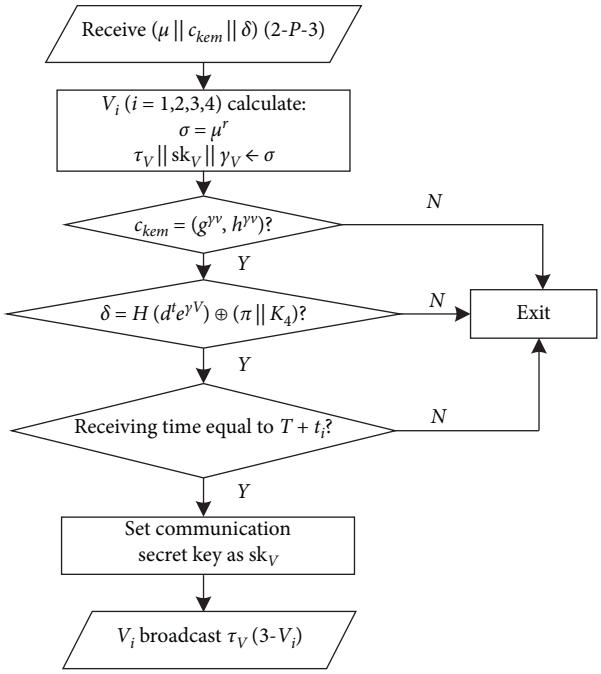

Figure 8: Verification algorithm of the verifiers in phase 3.

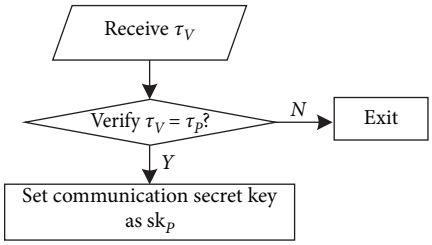

Figure 9: Protocol execution process of the participant in phase 4.

then V_i's authentication on P is successful. There are some differences between the secure positioning protocol proposed by Chandran et al. [22] and our PPAKE, that is, in phase 2, P broadcasts K_4, instead of δ.

In our protocol, to cooperate with password-based authenticated key exchange, we enhanced the protocol in [22] by encrypting K_4. We compute $\delta = k_{\mathrm{kem}} \oplus (\pi \| K_4)$, where $k_{\mathrm{kem}} = H(d^t e^{r_P})$, $t = H_{cr}(g^{r_P}, h^{r_P}, A \| c', \mathrm{V}_1, \mathrm{P})$. Therefore, our PPAKE protocol at least satisfies the security of position-based authentication in [22]. For more details of this proof, please refer to Section 7 in [22].

From the above analysis, we can claim that our proposed protocol is a secure authenticated key exchange, which provides both password- and position-based authentication.

7. Conclusion

In summary, the PPAKE protocol dual authenticates the participant through the password and position and negotiates a common session key to prepare for the next step of private communication. The proposed protocol can resist the attack of the active adversary under the standard model. Specifically, an arbitrary adversary who can listen, tamper, and send messages can only perform an online attack for password guessing at a specified position. The impersonation of any of the position and password by the adversary cannot be authenticated.

Data Availability

This is a pure theoretic research paper; therefore, it does not include any experimental data.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was supported by Sichuan Science and Technology Program (2020YFG0292).

References

[1] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, vol. 22, no. 6, pp. 644–654, 1976.

[2] Q. Jiang, N. Zhang, J. Ni, J. Ma, X. Ma, and K.-K. R. Choo, "Unified biometric privacy preserving three-factor Authentication and key agreement for cloud-assisted autonomous vehicles," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 9, pp. 9390–9401, 2020.

[3] Q. Jiang, Z. Chen, J. Ma, X. Ma, J. Shen, and D. Wu, "Optimized fuzzy commitment based key agreement protocol for wireless body area network," *IEEE Transactions on Emerging Topics in Computing*, vol. 1, 2019.

[4] D. Wang and P. Wang, "Two birds with one stone: two-factor Authentication with security beyond conventional bound," *IEEE Transactions on Dependable and Secure Computing*, vol. 15, no. 4, pp. 708–722, 2018.

[5] D. Wang, D. He, P. Wang, and C. Chu, "Anonymous two-factor Authentication in distributed systems: certain goals are beyond attainment," *IEEE Transactions on Dependable and Secure Computing*, vol. 12, no. 4, pp. 428–442, 2015.

[6] Y. Yang, X. Zheng, W. Guo, X. Liu, and V. Chang, "Privacy-preserving smart IoT-based healthcare big data storage and self-adaptive access control system," *Information Sciences*, vol. 479, pp. 567–592, 2019.

[7] Y. Yang, X. Zheng, W. Guo, X. Liu, and V. Chang, "Privacy-preserving fusion of IoT and big data for e-health," *Future Generation Computer Systems*, vol. 86, pp. 1437–1455, 2019.

[8] Y. Yang, X. Liu, and R. H. Deng, "Lightweight break-glass access control system for healthcare Internet-of-Things," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 8, pp. 3610–3617, 2017.

[9] Y. Yang, X. Zheng, X. Liu, S. Zhong, and V. Chang, "Cross-domain dynamic anonymous authenticated group key management with symptom-matching for e-health social system," *Future Generation Computer Systems*, vol. 84, pp. 160–176, 2018.

[10] Y. Yang, X. Liu, R. H. Deng, and Y. Li, "Lightweight sharable and traceable secure mobile health system," *IEEE Transactions on Dependable and Secure Computing*, vol. 17, no. 1, pp. 78–91, 2020.

[11] M. Bellovin and M. Merritt, "Encrypted key exchange: password-based protocols secure against dictionary attacks," in *Proceedings of the 1992 IEEE Symposium on Security and Privacy*, pp. 72–84, Oakland, CA, USA, May 1992.

[12] V. Boyko, P. MacKenzie, and S. Patel, "Provably secure password authenticated key exchange using DiffieHellman," in *Eurocrypt 2000. LNCS*, B. Preneel, Ed., pp. 156–171, Springer, Berlin, Germany, 2000.

[13] M. Abdalla and D. Pointcheval, "Simple password-based encrypted key exchange protocols," *Lecture Notes in Computer Science*, vol. 3376, pp. 191–208, 2005.

[14] J. Katz, R. Ostrovsky, and M. Yung, "Efficient password-authenticated key exchange using human-memorable passwords," in *Eurocrypt 2001. LNCS*, B. Pfitzmann, Ed., vol. 2045, pp. 475–494, Springer, Berlin, Germany, 2001.

[15] R. Gennaro and Y. Lindell, "A framework for password-based authenticated key exchange (extended abstract)," in *Eurocrypt 2003. LNCS*, E. Biham, Ed., vol. 2656, pp. 524–543, Springer, Berlin, Germany, 2003.

[16] A. Groce and J. Katz, "A new framework for efficient password-based authenticated key exchange," in *Proceedings of the 17th ACM Conference on Computer and Communications Security*, pp. 516–525, Chicago, IL, USA, October 2010.

[17] S. Jiang and G. Gong, "Password based key exchange with mutual authentication," in *SAC LNCS*, H. Handschuh and M. A. Hasan, Eds., vol. 3357, pp. 267–279, Springer, Berlin, Germany, 2004.

[18] J. Katz and V. Vaikuntanathan, "Smooth projective hashing and password-based authenticated key exchange from lattices," in *ASIACRYPT 2009. LNCS*, M. Matsui, Ed., vol. 5912, pp. 636–652, Springer, Berlin, Germany, 2009.

[19] J. Katz and V. Vaikuntanathan, "Round-optimal password-based authenticated key exchange," Edited by Y. Ishai, Ed., in *Proceedings of the 8th Theory of Cryptography Conference TCC 2011*, vol. 6597, pp. 293–310pp. 293–, Providence, RI, USA, March 2011.

[20] H. Xue, B. Li, and X. Lu, "IND-PCA secure KEM is enough for password-based authenticated key exchange (short paper)," in *Proceedings of the International Workshop on Security*, vol. 10418, pp. 231–241, Hiroshima, Japan, August 2017.

[21] M. Bellare, D. Pointcheval, and P. Rogaway, "Authenticated key exchange secure against dictionary attacks," in *EUROCRYPT 2000. LNCS*, B. Preneel, Ed., pp. 139–155, Springer, Berlin, Germany, 2000.

[22] N. Chandran, V. Goyal, R. Moriarty, and R. Ostrovsky, "Position based cryptography," *Advances in Cryptology-CRYPTO 2009*, vol. 5677, pp. 391–407, 2009.

[23] R. Singh and R. Selvakumar, "Designing a secure positioning system using blockchain technology," *International Journal of Security and Networks*, vol. 15, no. 2, pp. 78–84, 2020.

[24] M. Galambos and L. Bacsárdi, "Tracking cryptographic keys and encrypted data using position verification," *IET Quantum Communication*, vol. 1, no. 1, pp. 26–33, 2020.

[25] T. V. X. Phuong, W. Susilo, G. Yang, J. Yan, and D. Liu, "Location based encryption," in *Information Security and Privacy.ASISP 2019. LNCS*, J. Jang Jaccard and F. Guo, Eds., vol. 11547, pp. 21–38, Springer, Berlin, Germany, 2019.

[26] E. Kiltz, K. Pietrzak, M. Stam, and M. Yung, "A new randomness extraction paradigm for hybrid encryption," in *EUROCRYPT 2009. LNCS*, A. Joux, Ed., vol. 5479, pp. 590–609, Springer, Berlin, Germany, 2009.