Journal of Information Hiding and Multimedia Signal Processing ©2018 ISSN 2073-4212
Ubiquitous International Volume **9**, Number **4**, July **2018**

Provably Secure and Password-Authenticated Hybrid Key Agreement Protocol in Two-realm with Privacy-Protection

Dan Zhu

School of Foreign Languages
Shenyang Jianzhu University
No.9, HunNan East Street, HunNan District, Shenyang, P.C 110168 China
zhudan413@163.com

Hongfeng Zhu*,Shuai Geng and Rui Wang

Software College
Shenyang Normal University
No.253, HuangHe Bei Street, HuangGu District, Shenyang, P.C 110034 - China
1036103490@qq.com; 670322496@qq.com
*Corresponding author: zhuhongfeng1978@163.com

Received October, 2017; revised December, 2017

Abstract. *This paper presents a password-authenticated hybrid key agreement protocol (PAHKAP) with privacy-privacy to guard security for internet era, which can combine classical cryptography (Chaos Cryptography) and quantum cryptography in a universal way for the most common environment nowadays: Password with two users in two realms. Compared with the former research AQKDPs (authenticated quantum key distribution protocols), PAHKAP have five merits: (1) the basis is dynamic against the long shared key revealed, (2) key agreement replaces key distribution for eliminating the servers to get the session key of the two users, (3) the servers need not store the shared key with all the users, and the server only need keep its long secret key secret for saving storage space and avoiding verification table leakage, (4) any user need not store the shared key with the server, and s/he only keep the password in her/his brain, (5) the scheme can achieve privacy preserving for outsiders. Moreover, the two-realm architecture can permit any two users to negotiate a fresh session key even if they have registered at the different server. Compared with the related literatures recently, our proposed scheme can not only own high efficiency and unique functionality, but is also robust to various attacks and achieves perfect forward secrecy. Finally, we give the security proof and the comparison with the related works.*
Keywords: Quantum Channel, Key agreement, Password, Dynamic basis, Privacy protection

1. **Introduction.** Nowadays, more and more people want to enjoy surfing on Internet and meanwhile care about their security of information. The most popular technology is authenticated key agreement (AKA) [1,2] which can establish an authenticated and confidential communication channel. Many key distribution systems [3] have one party generate the key, and simply send that key to the other party that will lead to the other party has no influence on the key. And it can expand to N-party: one party choose a

session key and send the session key to all the other N-1 parties. Using a key agreement protocol avoids some of the key distribution problems associated with such systems.

Next stage, for achieving better adaptability, some researchers have introduced cross-domain or called two-realm in AKA protocols. Cross-domain password authentication key negotiation protocol is a user in a different security domain. Byun et al. [5] constructed the first direct communication cross-domain end-to-end authentication key agreement protocol in 2002. But the literature [18] found that their agreement cannot resist dictionary attacks. In the literature [17] of the agreement to other attacks, improve the agreement and improve the efficiency of the agreement. In the literature [12], a cross-domain end-to-end authentication and key agreement protocol with security proof is proposed. However, the literature [13] found that if the pre-shared symmetric key between domain servers is leaked, the protocol in the literature [12] cannot resist man-in-the-middle attacks. In addition, the literature [12] pointed out that the protocol in [12] cannot resist online undetectable dictionary attacks. On the basis of literature [12], the literature [12] improves the shortcomings of its security model, designs a new security model and proves the security of its own construction protocol. Furthermore, some others distributed architecture password authenticated key exchange schemes [1,19] are also designed with classical cryptography.

Nowadays, with the coming of the quantum era, quantum cryptography must be adopted against quantum computer. But owing to the low penetration of quantum device and the high price, that the trend for combining quantum cryptography and classical cryptography will be last for a long time. In cryptography with quantum realm, QKDPs (quantum key distribution protocols) [4,6,7] adopt quantum techniques to distribute temporary session key for resisting eavesdroppers in public channel with mutual authentication and other security attributes.

Combining the above-mentioned three areas: AKA, cross-domain and quantum cryptography, we try to design a new protocol, which can be set up in a more practical environment under current technology. We are inspired by the literature [6] and adopt the technology of literature [7] as a black box. So, the main contributions are shown as below:

(1) Our proposed protocol **improves** the security level. Because the basis is dynamic against the long shared key revealing, each session owns different basis which is constructed by users nonce with a long term key of the server.

(2) Our proposed protocol can **resist the curious server attack**. Because we use key agreement replace key distribution for eliminating the server get the session key of the two users.

(3) Our proposed protocol can **save storage space observably and avoid verification table leakage**. The server need not store the shared key with all the users, and the server only need keep its long secret key secretly. And more important thing is that the symmetric cryptosystem should not be used as key management scheme, because it will make the numbers of keys lead to exponential growth.

(4) Our proposed protocol has the **most prevalent method of login** (password) in classical cryptography. Any user need not store the shared key with the server, and s/he only keep the password in her/his brain.

(5) Our proposed protocol can provide Privacy-Protection, including **user-privacy** and **Server-privacy** during all the authenticated key agreement process.

(6) Our proposed protocol is designed in **different realms** which can adapt to the most application environment.

(7) Our proposed protocol can easily resist passive attacks between the servers owing to **quantum channel-based**.

The rest of the paper is organized as follows: Some preliminaries are given in Section 2. Next, a distributed privacy-protection scheme is described in Section 3. Then, the security proof with some discussions is given in Section 4. This paper is finally concluded in Section 5.

2. **Preliminaries.**

2.1. **Chebyshev chaotic maps.** Zhang [8] proved that semi-group property holds for Chebyshev polynomials defined on interval (-,+). The enhanced Chebyshev polynomials are used in the proposed protocol:

$$T_n(x) = (2xT_{n-1}(x) - T_{n-2}(x))(\mathrm{mod}N)$$

where $n \geq 2$,$x \in (-\infty, +\infty)$,and N is a large prime number. Obviously,

$$T_{rs}(x) = T_r(T_s(x)) = T_s(T_r(x))$$

Definition 2.1. *(Enhanced Chebyshev polynomials) The enhanced Chebyshev maps of degree n* ($n \in N$) *are defined as:* $T_n(x) = (2xT_{n-1}(x) - T_{n-2}(x))(\mathrm{mod}\, p)$,*where* $n \geq 2$,$x \in (-\infty, +\infty)$, *and p is a large prime number. Obviously,* $T_{rs}(x) = T_r(T_s(x)) = T_s(T_r(x))$.

Definition 2.2. *(DLP, Discrete Logarithm Problem) Given an integer a, find the integer r, such that* $T_r(x) = a$.

Definition 2.3. *(CDH, Computational DiffieHellman Problem) Given an integer x, and the values of* $T_r(x), T_s(x)$ *, what is the value of* $T_{rs}(x) = ?$.

It is widely believed that there is no polynomial time algorithm to solve DLP, CDH with a non-negligible probability.

2.2. **Quantum cryptosystem techniques.** A qubit can be described by a vector in two-dimensional Hilbert space. Let $R = \{|0\rangle, |1\rangle\}$ be the computational basis of a qubit $|q\rangle$. Here $|0\rangle$and$|1\rangle$ are two orthogonal qubit states. Define $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)and|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. The two vectors $|+\rangle$and$|-\rangle$ are also orthogonal. Let $D = \{|+\rangle, |-\rangle\}$ be another basis. The bases R and D are mutually unbiased bases [9]. These two mutually unbiased bases are widely used in quantum cryptography, e. g., the BB84 protocol. More details about Quantum cryptosystem techniques can be found in [11].

2.3. **Threat Model.** The threat model should be adopted the widely accepted security assumptions about password based authentication schemes [16].

(1) A useri remembers the low-entropy password from the small dictionary. A server stores the private key safely. In the stage of registration, the server transmits the customized security parameters to the useri by secure channel and the useri should keep the personalized security parameters safe.

(2) An attacker and a useri interplay through executing some oracle queries which enable an attacker to carry out various attacks on the authenticated protocol.

(3) The communication channel is controlled by an attacker who has the capacity to intercept, modify, delete, resend and reroute the eavesdropped messages.

The concrete **Definitions** of oracles Execute(Π_U^i, Π_S^j), Send(Π_U^i, m), R*eveal*(Π_U^i), Corr upt(Π_U^i, m) and Test(Π_U^i) can be found in Based on literatures [16], where Π means a password authenticated protocol, each participant is either a user $u_i \in U$ or a trusted server S interact number of times, and only polynomial number of queries occurs between adversary and the participants interaction.

Consider an execution of the authentication protocol Π by an adversary A, in which the latter is given access to the Execute, Send, and Test oracles and asks at most single Test query to a fresh instance of an honest client. Let b' be his output, if $b' = b$, where

b is the hidden bit selected by the Test oracle. Let D be user's password dictionary with size $|D|$. Then, the advantage of A in violating the semantic security of the protocol Π is defined more precisely as follows:

$$Adv_{\Pi,D}(A) = [2\Pr[b' = b] - 1]$$

The password authentication protocol is semantically secure if the advantage $Adv_{\Pi,D}(A)$ is only negligibly larger than $O(q_s)/|D|$, where q_S is the number of active sessions.

Some definitions of Security about quantum cryptography can be found in literatures [6,10], such as **No-cloning Theorem** (a user cannot copy a qubit if he/she does not know the polarization basis of the qubit), **Unbiased-Chosen Basis (UCB) Assumption, AQKD security** and so on.

3. The Proposed Privacy Protection Scheme with Dynamic Basis.

3.1. User registration phase.

Table 1. Notations

Symbol	Definition
ID_S	The l/4-bit identity of the server
ID_A	The l/4-bit identities of Alice
PW_A	Password of Alice
$a, b, s, S, r_a, r_a^{'}, r_b$	l/2 bits for each nonce
$(x, T_k(x))$	The public key based on Chebyshev chaotic maps of the server. And the length of $T_*(x)$ is l/2 bits
k	The secret key based on Chebyshev chaotic maps of the server
H	A secure hash function. $H: \{0,1\}^* \rightarrow \{0,1\}^l$ for any constant l
$\|\|$	concatenation operation
R	The rectilinear basis, polarized with two orthogonal directions, $\|0\rangle$ and $\|1\rangle$
D	The diagonal basis (two polarized orthogonal directions), $\frac{1}{\sqrt{2}}(\|0\rangle+\|1\rangle)$ and $\frac{1}{\sqrt{2}}(\|0\rangle-\|1\rangle)$

Step 1. When a user (Alice) wants to be a new legal user, she chooses her identity ID_A, a random number r_a, and computes $H(r_a||PW_A)$. Then Alice submits $ID_A, H(r_a||PW_A)$ to S by a secure channel.

Step 2. On getting $ID_A, H(r_a||PW)$ from Alice, the S computes $A = H(ID_A||k) \oplus H(r_a||PW_A)$, where k is the secret key of S. Then Alice stores $\{ID_A, r_a, A\}$ in a secure way.

3.2. Authenticated key agreement phase.

Fig.1 illustrates the process of authenticated key agreement phase.

Step 1. If Alice wishes to consult some personal issues establish with Bob in a secure way, but they are in different realm. Alice inputs *password* and compute $A_A = A \oplus H(r_a||PW_A)$, and then choose a random integer numbers a and compute $T_a(x)$, $C_A = T_aT_k(x)(ID_A||ID_B||ID_{S_K})$ and $V_A = H(A_A||C_A)$. After that, Alice sends $\{T_a(x), C_A, V_A\}$ to S_k where she registers on (The same way for Bob).

Step 2. After receiving the message $\{T_a(x), C_A, V_A\}$ from Alice, and S_k firstly uses the secret key k to decrypt $ID_A||ID_B||ID_{S_K} = C_A/T_kT_a(x)$, and checks the identity is consistent or not. Then, S_k computes $A_A = H(ID_A||k)$ and $V'_A = H(A_A||C_A)$ based on ID_A. S_k compares $V'_A = V_A$?. If above equations hold, which means Alice is a legal user, or S_k will abort this process. Next, S_k will Build a basis to set up quantum channel: $Base_A = \frac{3H(T_kT_K(x)||ID_A||ID_B||ID_{S_K})}{2}$.

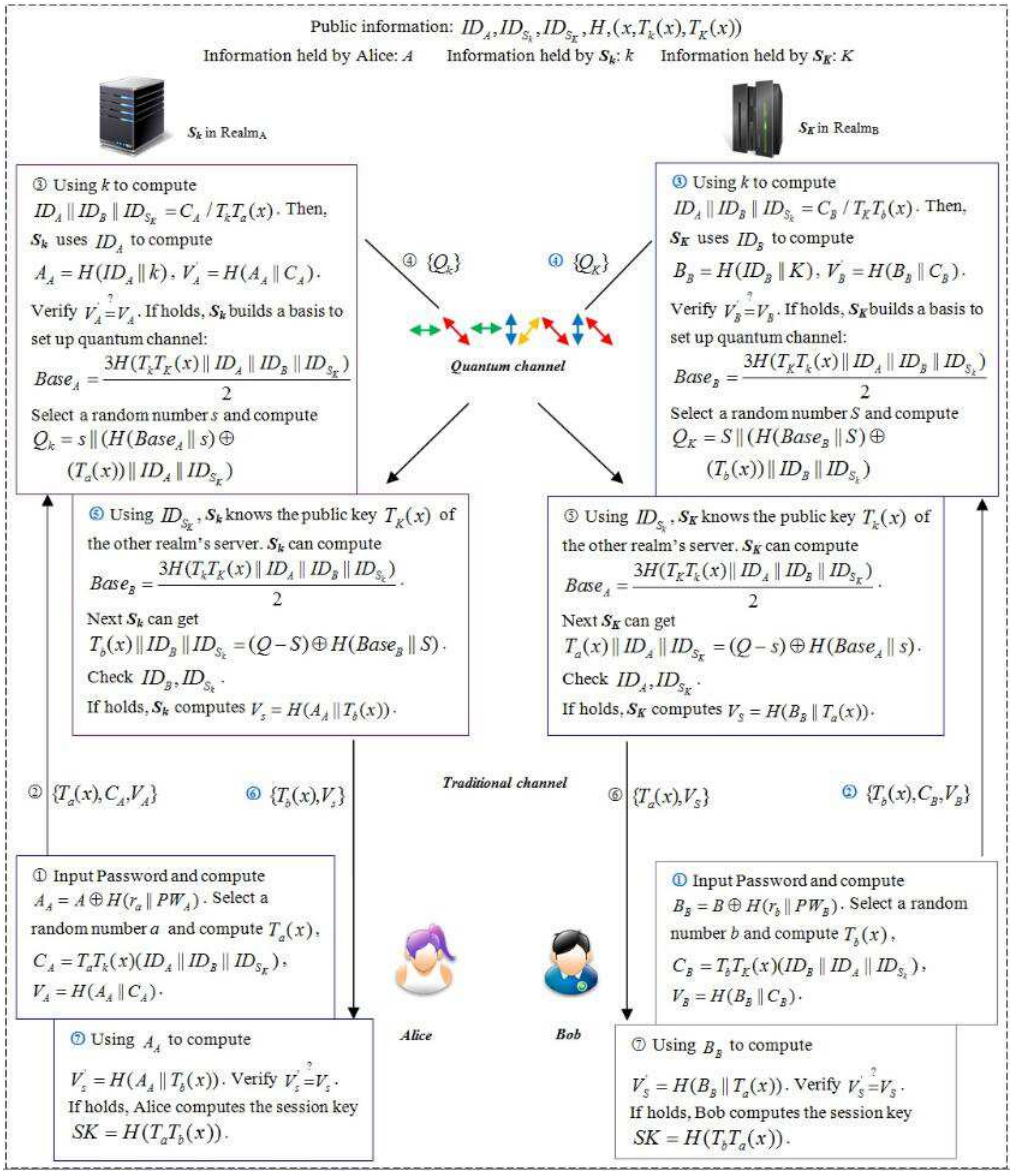

FIGURE 1. Authenticated key agreement phase with quantum channel

Then S_k select a random number s and computes $Q_k = s||(H(Base_A||s) \oplus (T_a(x))||ID_A||ID_{S_K})$. The structure of Q_k is depicted in **Fig.2 (a)**. For each quantum bit of $(Q_k)_i$, if $(Base)_i = 0$, the server Q_k will use R as its basis, otherwise D is the chosen basis.

Finally the server S_k sends Q_k to S_K using quantum channel based on $Base_A$ (The same way for S_K).

Step 3. S_K firstly receives the message $\{T_b(x), C_B, V_B\}$ from Bob, and S_K uses the secret key K to decrypt $ID_A||ID_B||ID_{S_k} = C_B/T_K T_b(x)$. Then S_K knows S_k will send messages to itself by quantum channel. So S_K can computes the $Base_A = \frac{3H(T_K T_k(x)||ID_A||ID_B||ID_{S_K})}{2}$ locally using his secret key K and the public key of S_k . Then S_K receives Q_A and measures it based on ***BaseA***. Next, S_K can get s from Q_A with the front $l/2$ bits, and then S_K will get $T_a(x)||ID_A||ID_{S_K} = (Q - s) \oplus H(Base_A||s)$. Then, S_K checks ID_A, ID_{S_K} . If holds, S_K computes $V_S = H(B_B||T_a(x))$ and sends the message $\{T_a(x), V_S\}$ to Bob (The same way for S_k).

Step 4. After receiving the message $\{T_a(x), V_S\}$ from S_K , Bob uses B_B to compute $V'_S = H(B_B||T_a(x))$ and compare $V'_S \stackrel{?}{=} V_S$. If above equations hold, which means S_K is the real S_K and S_K has already authenticated the message $T_a(x)$, or Bob will abort this process. Finally, Bob computes the session key $SK = H(T_bT_a(x))$ (The same way for Alice).

If any authenticated process does not pass, the protocol will be terminated immediately.

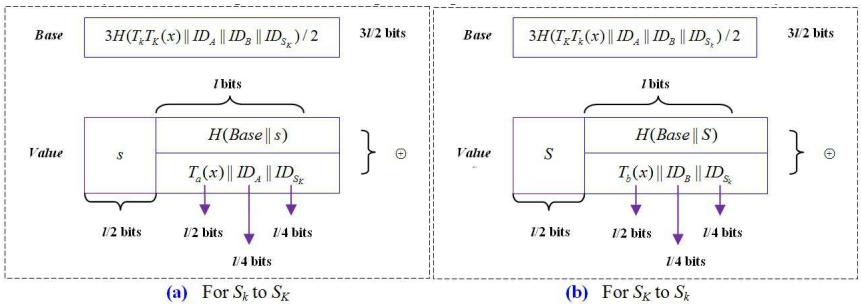

FIGURE 2. Authenticated key agreement phase with quantum channel

4. Security Analysis.

4.1. The provable security of the PAHKAP [6,16].

Theorem 4.1. *Let D be a uniformly distributed dictionary of possible passwords with size D, Let P be the improved authentication protocol described in Algorithm 1 and 2. Let A be an adversary against the semantic security within a time bound t. Suppose that CDH assumption and DLP assumption hold, then,* $Adv_{\Pi,D}(A) = Adv_{\Pi,D}^{\text{classical}}(A) + Adv_{\Pi,D}^{\text{quantum}}(A) \leq \frac{6q_h^2}{2^{l+1}} + 2q_h Adv_G^{dlp}(A) + 4q_h Adv_G^{cdh}(A) + \frac{2q_h}{p} + \frac{q_s}{D} + \frac{2(q_{ini}+q_s)^2}{q_{ini}} \cdot Adv_{\Psi}^{UCB}(\Delta)$, *where $Adv_G^{cdh}(A)$ is the success probability of A of solving the chaotic maps-based computational DiffieHellman problem, $Adv_G^{dlp}(A)$ is the success probability of A of solving the chaotic maps-based Discrete Logarithm problem, q_s is the number of Send queries, q_e is the number of Execute queries, q_h is the number of random oracle queries and q_ini is the initiate queries in quantum channel, an UCB assumption attacker Δ will have an advantage to break the UCB security of Ψ .*

Proof

Stage 1: This stage defines a sequence of hybrid games, simulating the classical cryptography and starting at the real attack and ending up in game where the adversary has no advantage. For each game $G_i (0 \leq i \leq 4)$, we define an event $Succ_i$ corresponding to the event in which the adversary correctly guesses the bit b in the test-query.

Game G_0 This game correspond to the real attack in the random oracle model. In this game, all the instances of U_A and U_B are modeled as the real execution in the random oracle. By definition of event $Succ_i$ in which the adversary correctly guesses the bit b involved in the Test-query, we have

$$Adv_{\Pi,D}^{\text{classical}}(A) = 2|\Pr[Succ_0] - \frac{1}{2}| \tag{1}$$

Game G_1 This game is identical to the game G_0, except that we simulate the hash oracles h by maintaining the hash lists $List_h$ with entries of the form (Inp, Out). On hash query for which there exists a record (Inp, Out) in the hash list, return Out. Otherwise, randomly choose $Out \in \{0, 1\}$, send it to A and store the new tuple (Inp, Out) into the

hash list. The Execute, Reveal, Send, Corrupt, and Test oracles are also simulated as in the real attack where the simulation of the different polynomial number of queries asked by A. From the viewpoint of A, we identify that the game is perfectly indistinguishable from the real attack. Thus, we have

$$\Pr[Succ_1] = \Pr[Succ_0] \tag{2}$$

Game G_2 In this game, the simulation of all the oracles is identical to game G_1 except that the game is terminated if the collision occurs in the simulation of the partial transcripts $\{T_a(x), C_A, V_A\}$ and $\{T_b(x), V_s\}$. According to the birthday paradox, the probability of collisions of the simulation of hash oracles is at most $2q_h^2/2^{l+1}$. Since a, b were selected uniformly at random which are protected by the chaotic maps-based Discrete Logarithm problem. Thus, we have

$$\Pr[Succ_2] - \Pr[Succ_1] \leq q_h Adv_G^{dlp}(A) + q_h Adv_G^{cdh}(A) + \frac{2q_h^2}{2^{l+1}} \tag{3}$$

Game G_3 In this game, the session key is guessed without asking the corresponding oracle h so that it become independent of password and ephemeral keys a, b which are protected by the chaotic maps-based computational DiffieHellman problem. We change the way with earlier game unless A queries h on the common value $SK = H(T_aT_b(x))$. Thus, $Adv_G^{cdh}(A) \geq \frac{1}{q_h}|\Pr[Succ_3] - \Pr[Succ_2]| - \frac{1}{p}$, that is, the difference between the game G_3 and the game G_2 is as follows:

$$|\Pr[Succ_3] - \Pr[Succ_2]| \leq q_h Adv_G^{cdh}(A) + \frac{q_h}{p} \tag{4}$$

Game G_4 This game is similar to the game G_3 except that in Test query, the game is aborted if A asks a hash function query with $SK = H(T_aT_b(x))$. According to the birthday paradox, A gets the session key SK by hash function query with probability at most $\frac{q_h^2}{2^{l+1}}$. Hence, we have

$$|\Pr[Succ_4] - \Pr[Succ_3]| \leq \frac{q_h^2}{2^{l+1}} \tag{5}$$

If A does not make any h query with the correct input, it will not have any advantage in distinguishing the real session key from the random once. Moreover, if the corrupt query $Corrupt(U, 2)$ is made that means the password-corrupt query $Corrupt(U, 1)$ is not made, and the password is used once in local computer to authenticate user for getting some important information and no more used in the process of the protocol Π. Thus, the probability of A made on-line password guessing attack is at most $\frac{q_s}{D}$, even A gets the secret information of Alice: $\{ID_A, r_a, A\}$. Furthermore, the probability of A made off-line password guessing attack is 0, because even if A gets the secret information $\{ID_A, r_a, A\}$, A has no any compared value to authenticate the guessing password is right or not. Combining the Eqs. 1-5 one gets the announced result as:

$$Adv_{\Pi,D}^{\text{classical}}(A) \leq \frac{6q_h^2}{2^{l+1}} + 2q_h Adv_G^{dlp}(A) + 4q_h Adv_G^{cdh}(A) + \frac{2q_h}{p} + \frac{q_s}{D} \tag{6}$$

Stage 2: This stage simulates the quantum cryptography. In order to make the security proof simple, we point out the differences between the literature [6] and our proposed protocol and use the result of it.

The only two differences between the $3AQKDP$ of the literature [6] and the quantum exchange in our proposed protocol are: 1) the literature [6] use the long shared key as the basis directly, while our related phase use dynamic basis which is agreed by the server and the user with their nonces and related secret information; 2) the literature [6] directly transfers the session key, while our scheme just transfers the agreement information about the session, and the two users must use it to compute the session key locally.

The above differences will lead to two results: 1) the security of extra computation ($SK = H(T_aT_b(x))$) will be considered in the stage1; 2) the advantage of the literature [6] is at least the upper bound of our corresponding phase(quantum section). So, the detailed descriptions of these games and lemmas are analogous to those in literature [6], with the differences discussed above, and therefore, they are omitted and the result as:

$$Adv_{\Pi,D}^{\text{quantum}}(A) \leq Adv_{3AQKDP}^{AQKD}(A) \leq \frac{2(q_{ini}+q_s)^2}{q_{ini}} \cdot Adv_{\Psi}^{UCB}(\Delta) \tag{7}$$

4.2. **Further Security Discussion.** (1) *The scheme could resist password guessing attack.*

Proof This attack means an adversary tries to guess a legal users password PW based on the transmitted information. Password guessing attack can only crack a function with one low entropy variable (password), so if we at least insert one large random variable which can resist this attack. In our protocol, the adversary only can launch the on-line password guessing attack, because there are no any of the transmitted messages including password as the input value. Even if the adversary gets the secret information $\{ID_A, r_a, A\}$, he has no any compared value to authenticate the guessing password is right or not without the servers help. In other words, the adversary cannot construct the form $function(*||PW') = y$, where * is any known message, and only the server can compute the value y. On the other side, about on-line password guessing attack, because the maximum number of allowed invalid attempts about guessing password is only a few times, then the account will be locked by the registration server.

(2) *The scheme could support mutual authentication.*

Proof The Registration Server S_k verifies the authenticity of user As request through validating the condition $V_A' \stackrel{?}{=} V_A$ during the proposed phase. To compute $A_A = A \oplus H(r_a||PW_A)$, the attacker must has the password. Furthermore, $\{T_a(x), C_A, V_A\}$ includes a large random nubmer a, the adversary cannot replay the old messages in the protocol.

For S_k and S_K authenticating each other, they only need compute the right basis for receiving message. Only S_k and SK can compute the right basis: $Base_A = \frac{3H(T_KT_k(x)||ID_A||ID_B||ID_{S_K})}{2}$ or $Base_B = \frac{3H(T_kT_K(x)||ID_A||ID_B||ID_{S_k})}{2}$, because they have the right secret key k or K.

For Alice authenticating S_k, she only need validate the condition $V_s' \stackrel{?}{=} V_s$ during the proposed phase. As for authenticating S_K and Bob, Alice just only trust S_k .

(3) *The perfect forward secrecy can be provided in the proposed scheme.*

Proof The perfect forward secrecy means if the adversary cannot compute the established session key by compromised secret key k of any server. The proposed scheme achieves perfect forward secrecy. In our proposed scheme, the session key has not included the servers long-term secret key k because the session key is $SK = H(T_aT_b(x))$.

(4) *The privacy-privacy protection can be provided in the proposed scheme.*

Proof There are no plaintext in the two messages of the proposed scheme. The message $\{T_a(x), C_A, V_A, T_b(x), C_B, V_B\}$ includes covered ciphertext $\{T_a(x), C_A, T_b(x), C_B\}$ which can transmit any important information to appointed node with the peers public key, such

as identity in the proposed scheme, and message $\{V_A, V_B\}$ is the verification ciphertext using one-way secure hash function. The other message $\{Q_k, Q_K\}$ is transmitted using dynamic $Base_A$ and $Base_B$ by quantum channel which cannot be cloning **(No-cloning Theorem)**. Moreover, no message part is repeated in consecutive communications. This shows that our scheme achieves the property of privacy-privacy.

(5) *Replay and man-in-the-middle attacks can be resisted in the proposed scheme.*

Proof The verification messages include the temporary random numbers a, b . More important thing is that all the temporary random numbers are protected by CDH problem in chaotic maps which only can be uncovered by the legal users (using secret keys or password).

(6) *Impersonation attack can be resisted in the proposed scheme.*

Proof For any adversary, there are two ways to carry this attack:

- The adversary may try to launching the replay attack. However, the proposed scheme resists the replay attack.
- The adversary may try to generate a valid authenticated message $\{T_a(x), C_A, T_b(x), C_B\}$ which is protected by CDH problem in chaotic maps. Howerer, the adversary cannot compute $\{V_A, V_B\}$ as computation of $\{V_A, V_B\}$ requires PW which is only known to legal users. Moreover, the proposed scheme has the feature of privacy protection, and the adversary has no idea about the identity of any user.

(7) *The key freshness property can be provided in the proposed scheme.*

Proof Each established session key $SK = H(T_a T_b(x))$ includes random values a and b. The unique key construction for each session shows that key freshness property can be provided in the proposed scheme.

(8) *The known key secrecy property can be provided in the proposed scheme.*

Proof Because each session key includes two nonces, which ensures different key for each session. So our proposed scheme achieves the known key secrecy property.

(9) *The forward secrecy can be provided in the proposed scheme.*

Proof Forward secrecy states that compromise of a legal users long-term secret key does not become the reason to compromise of the established session keys. In our proposed scheme, the session key has not included the users long-term secret key: Password. This shows that the forward secrecy property can be provided in the proposed scheme.

(10) *The stolen verifier attack can be resisted in the proposed scheme.*

Proof Any party stores nothing about the legal users information in the proposed scheme. All the en/decrypted messages can be deal with the users password which is stored in the users brain, or the secret keys which are covered strictly, so the proposed scheme withstands the stolen verifier attack.

From the **Table 2**, we can see that the proposed scheme is more secure and has much functionality compared with the recent related scheme.

Table 2. Comparison PAQKAPs among and Other Protocols

	ZZ00 [15]	Case 8 of [14]	Case 2 of [14]	3QKDPMA [6]	PAHKAP
Cryptographic Mechanism	Quantum	Classical	Classical	Quantum+Classical	Quantum+Classical
Pre-shared secret key	EPR pairs	Long-termed	Long-termed	Long-termed	No
Communication round	6	4	3	3	3
Quantum channel	Yes	No	No	Yes	Yes
Clock synchronization	No	No	Yes	No	No
Vulnerable to man-in-the-middle attack	No	No	No	No	No
Vulnerable to passive attack	No	Yes	Yes	No	No
Vulnerable to replay attack	No	No	No	No	No
Formal security proof	No	No	No	Yes	Yes
Architecture	Centralized	Centralized	Centralized	Centralized	Two realms
Privacy	Yes	No	No	Yes	Yes

5. **Conclusion.** This work presents a password-authenticated hybrid key agreement protocol (PAHKAP) . Compared with classical three-party key distribution protocols, the proposed protocol easily resists replay, man-in-the-middle attacks and passive attacks. Compared with other quantum key distribution protocols (QKDPs), the proposed scheme can achieve five advantages in distributed architecture at least: dynamic basis, key agreement, no verifiable table and no off-line password guessing attack and privacy-privacy. Additionally, the proposed scheme no need pre-shared secret key which can make the proposed protocol become more practical. Moreover, the proposed protocol has been shown secure under the random oracle model with UCB security of quantums feature.

Acknowledgment. This work is supported by the Liaoning Provincial Natural Science Foundation of China (Grant No. 201602680).

REFERENCES

[1] C. M. Chen, L. L. Xu, T, Y. Wu and C. R. Li,,em On the Security of a Chaotic Maps-based Three-Party Authenticated Key Agreement Protocol, *Journal of Network Intelligence*,Vol.1,No.2, 2016.
[2] H. Q. Wang, H. Zhang, J. X. Li and C. Xu, A(3,3) visual cryptography scheme for authentication, *Journal of Shenyang Normal University (Natural Science Edition)*, vol.31, no.101(03), pp.397–400, 2013.
[3] M. Bellare and P. Rogaway, Provably Secure Session Key Distribution: The Three Party Case, *Proc. 27th ACM Symp. Theory of Computing*, pp.57–66, 1995.
[4] G. Zeng and W. Zhang, Identity Verification in Quantum Key Distribution, *Physical Rev. A*, vol.61, 2000.
[5] J. W. Byun I. R. JeongD. H. Leeet al, Password-authenticated key exchange between clients with different passwordsC, */ / LNCS*, vol 2513, pp.134–146, 2002.
[6] T. Hwang, K. C. Lee, C. M. Li, Provably secure three-party authenticated quantum key distribution protocols, *IEEE Trans. Dependable Secure Comput*,2007.
[7] D. J. Guan, Y. J. Wang, E. S. Zhuang, A practical protocol for three-party authenticated quantum key distribution, *Quantum Inf Process* , pp.2355–2374, 2014.
[8] L. Zhang , Cryptanalysis of the public key encryption based on multiple chaotic systems, *Chaos Solitons Fractals*, vol.37, no.3, pp.669–674, 2008.
[9] J. Schwinger, , Unitary operator bases., *Proc. Natl. Acad. Sci.*, vol.46, no.4,1960.
[10] W. K. Wootters and W.H. Zurek, A Single Quantum Cannot Be Cloned, *nature*, vol.299,pp.802–803, 1992.
[11] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Quantum Cryptography, *Rev. of Modern Physics*, vol.74, pp.145–190, 2002.
[12] J. W. Byun D. H. LeeJ. I. Lim, EC2C-PAKA: an efficient client-to-client password-authenticated key agreement J , *Information Science*, vol.177,No.19, pp.3995–4013, 2007.
[13] F. J. Wang Y. Q. Zhang, Cryptanalysis of a client-to-client password-authenticated key agreement protocol, *http: / / eprint iacr org /*,2008.
[14] G. Li, Efficient Network Authentication Protocols: Lower Bounds and Optimal Implementations, *Distributed Computing*, vol.9,No.3, pp.131–145, 1995.
[15] G. Zeng and W. Zhang, Identity Verification in Quantum Key Distribution, *Physical Rev. A*, vol.61, 2000.
[16] S. H. Islam, Provably secure dynamic identity-based three-factor password authentication scheme using extended chaotic maps, *Nonlinear Dynamics*, vol.78, pp.2261–2276, 2014.
[17] J. Kim S. Kim J. Kwak, et al, Cryptanalysis and improvement of password-authenticated key exchange scheme between clients with different passwords, *LNCS*, vol.3043, pp.895–902, 2004.
[18] L. Chen, A weakness of the password-authenticated key agreement between clients with different passwords scheme, *ISO/IEC JTC 1 /SC27 N3716*,2003.
[19] Hongfeng Zhu, Flexible and Password-Authenticated Key Agreement Scheme Based on Chaotic Maps for Multiple Servers to Server Architecture, *Wireless Personal Communications*, vol.82,No.3, pp.1697–1718, 2015.