Journal of Information Hiding and Multimedia Signal Processing ©2018 ISSN 2073-4212
Ubiquitous International Volume **9**, Number **5**, September **2018**

Provably Secure and Distributed Authenticated Quantum Key Agreement Protocol with User-Privacy using Dynamic Basis

Hongfeng Zhu and Zixi Wang

Software College, Shenyang Normal University
No.253, HuangHe Bei Street, HuangGu District, Shenyang, P.C 110034 - China
zhuhongfeng1978@163.com;1041381713@qq.com

Received April, 2018; revised May, 2018

Abstract. *This paper presents a distributed password-authenticated quantum key agreement protocol (DPAQKAP) with user-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. And DPAQKAP will guide in new directions for biometric-based/smart card-based with quantum cryptography using distributed architecture. Compared with the former research AQKDPs (authenticated quantum key distribution protocols), DPAQKAP have five merits: (1) the basis is dynamic against the long shared key revealed, (2) key agreement replaces key distribution for eliminating the server get the session key of the two users, (3) the server 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 protection during the traditional channel in the first phase. Moreover, the distributed architecture can solve problems of single-point of security, single-point of efficiency and single-point of failure for the centralized server or registration center. 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 analysis and the comparison with the related works.*

Keywords: Quantum key agreement, Password, Dynamic basis, Privacy protection, Distributed architecture

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. In cryptography, a key agreement protocol is a protocol whereby N-party can agree on a key in such a way that both influence the outcome. If properly done, this precludes undesired third parties from forcing a key choice on the agreeing parties. Protocols that are useful in practice also do not reveal to any eavesdropping party what key has been agreed upon.

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.

With the coming of the quantum era, quantum cryptography must be adopted against quantum computer. 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) [4-7] adopt quantum techniques to distribute temporary session key for resisting eavesdroppers in public channel with mutual authentication and other security attributes.

Recently, Hwang et al. [6] proposed two kinds of three-party authenticated key distribution protocols with quantum techniques. The first one, which is called 3AQKDP, can be used to establish a session key in a noiseless quantum channel between two communicating parties, Alice and Bob, via a trusted center (TC). In their protocols, each communicating party shares a long-term secret key with the TC. User authentication is implicitly verified by quantum information without public discussion. The second one, which will be called 3QKDPMA, allows Alice and Bob to use the session key established by 3AQKDP to mutually authenticate each other and then create a novel session key for communication. Hwang et al. also proved the security of these two protocols under the random oracle model. Both of their protocols are designed to run in a noiseless environment. Next, the literature [7] pointed out that Hwang's protocol is vulnerable to online guessing attack and session key consistence problem, and then they presented a practical N3AQKDP which can work in a noisy quantum channel.

The distributed architecture password authenticated key exchange schemes [1, 19] are designed in classical channel, not quantum channel involved. In this paper, 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 user's 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 user-privacy protection during all the authenticated key agreement process.

(6) Our proposed protocol is designed in distributed architecture which can eliminate the problems of single-point of security, single-point of efficiency and single-point of failure in centralized architecture.

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 $(-\infty, +\infty)$. The enhanced Chebyshev polynomials are used in the proposed protocol:

$$T_n(x) = (2xT_{n-1}(x) - T_{n-2}(x))(modN)$$

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 1. *(Enhanced Chebyshev polynomials)* The enhanced Chebyshev maps of degree n $(n \in N)$ are defined as: $T_n(x) = (2xT_{n-1}(x) - T_{n-2}(x))(modp)$, 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. *(DLP, Discrete Logarithm Problem)* Given an integer a, find the integer r, such that $T_r(x) = a$.

Definition 3. *(CDH, Computational Diffie-Hellman 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 $\overline{R} = \{|+\rangle, |-\rangle\}$ be another basis. The bases R and $\overline{R}$ 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 [11-13].

2.3. **Threat Model.** The threat model should be adopted the widely accepted security assumptions about password based authentication schemes [16-18].

(1) A $user_i$ 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 $user_i$ by secure channel and the $user_i$ should keep the personalized security parameters safe.

(2) An attacker and a $user_i$ 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 $(\prod_U^i, \prod_S^j)$, Send $(\prod_U^i, m)$, Reveal $(\prod_U^i)$, Corrupt $(\prod_U^i, m)$ and Test $(\prod_U^i)$ can be found in Based on literatures [16-18], where $\prod$ 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 participant's interaction.

Consider an execution of the authentication protocol $\prod$ 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 $\prod$ is defined more precisely as follows:

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

The password authentication protocol is semantically secure if the advantage $Adv_{\prod,D}(A)$ 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 [6,10,18], 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. Notations.

The concrete notations used hereafter are shown in **Table 1**.

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
$a,b,s,r_a,r_a^{'}$	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 $\|1\rangle$
$\overline{R}$	The diagonal basis (two polarized orthogonal directions), $\frac{1}{\sqrt{2}}(\|0\rangle+\|1\rangle)$ and $\frac{1}{\sqrt{2}}(\|0\rangle-\|1\rangle)$

3.2. User registration phase.

Fig.1illustrates the user registration phase.

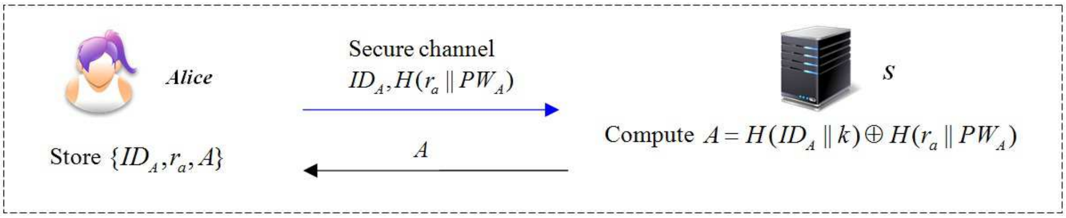


FIGURE 1. a premium user registration phase

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 $H(r_a \parallel PW_A)$. Then Alice submits $ID_A, H(r_a \parallel PW_A)$ to S by a secure channel.

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

3.3. Authenticated key agreement phase.

If Alice wishes to consult with S_K in a secure way, while she only registers at the server S_k. Alice need not register on S_K, and she can get the service of S_K by the helping of the S_k. **Fig.2** illustrates the process of authenticated key agreement phase.

Step 1. Alice inputs password and computes $A_A = A\bigoplus H(r_a \parallel PW_A)$, and then chooses two random integer numbers a, b and computes $T_a(x)$, $C_A = T_aT_k(x)(ID_A \parallel$

$ID_{S_k} \parallel b \cdot T_aT_K(x))$, $V_A = H(A_A \parallel C_A)$ and $SK = H(T_aT_b(x))$. After that, Alice sends $m_1 = \{T_a(x), C_A, V_A\}$ to the server S_k which she has registered, and sends $m_2 = \{ID_{S_k}, T_a(x)\}$ to the server S_K which she wants to get service.

Step 2. After receiving the message $m_1 = \{T_a(x), C_A, V_A\}$ from Alice, and S_k firstly uses the secret key k to decrypt $ID_A \parallel ID_{S_k} \parallel b \cdot T_aT_K(x) = C_A/T_kT_a(x)$, and checks if the identity is consistent or not. Then, S_k computes $A_A = H(ID_A \parallel k)$ and $V_A' = H(A_A \parallel C_A)$ based on ID_A. S_k compares $V_A' = V_A$?. If above equations hold, which means Alice is a legal user, otherwise S_k will abort this process. Next, S_k will build a basis to set up quantum channel: $Base = \dfrac{3H(T_kT_K(x) \parallel T_a(x))}{2}$.

Then S_k select a random number s and computes $Q = s \parallel (H(Base \parallel s) \bigoplus (b \cdot T_aT_K(x)) \parallel ID_A \parallel ID_{S_K})$. The structure of Q is depicted in **Fig.3**. For Alice, the quantum bit of $(Q_A)_i$,if $(Base)_i = 0$, the server S_k will use R as its basis, otherwise D is the chosen basis.

Finally the server S_k sends Q to S_K using quantum channel based on $Base$.

Step 3. S_K firstly receives the message $m_2 = \{ID_{S_k}, T_a(x)\}$ from Alice, and S_K knows Alice has already registered at S_k and the public key of S_k. Otherwise S_K can compute the $Base = \dfrac{3H(T_KT_k(x) \parallel T_a(x))}{2}$ locally using his secret key K and the public key of S_k. Then S_K receives Q and measures it based on **Base**. Next, S_K can get s from Q with the front $l/2$ bits, and then S_K will get $b \cdot T_aT_K(x) \parallel ID_A \parallel ID_{S_K} = (Q - s) \bigoplus H(Base \parallel s)$. Then, S_K checks ID_A, ID_{S_K}. If holds, S_K computes $b = b \cdot T_aT_K(x)/T_KT_a(x)$ and the session key $SK = H(T_bT_a(x))$.

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

Remark: $T_a(x)$ and $T_b(x)$ are the temporary authenticator which can be used for a certain time. So, Alice and Bob can use $T_a(x)$ and $T_b(x)$ to construct some other session keys, such as $SK = H(T_aT_b(x) \parallel ID_A \parallel ID_{S_K})$, $SK = H(T_aT_b(x) \parallel T_a(x) \parallel T_b(x))$ and so on, without the registation server S_k involved for saving time and quantum resources.

4. Security Analysis.

4.1. The provable security of the 3PAQKAP [6,16-18].

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,*

$$Adv_{\prod,D}(A) = Adv_{\prod,D}^{classical}(A) + Adv_{\prod,D}^{quantum}(A) \leq \frac{4q_h^2}{2^{l+1}} + 2q_hAdv_G^{dlp}(A)$$

$$+4q_hAdv_G^{cdh}(A) + \frac{2q_h}{p} + \frac{q_s}{D} + \frac{2\left(q_{ini} + q_s\right)^2}{q_{ini}} \cdot Adv_\psi^{UCB}(\Delta)$$

where $Adv_G^{cdh}(A)$ is the success probability of A of solving the chaotic maps-based computational Diffie-CHellman 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

Stage1: 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

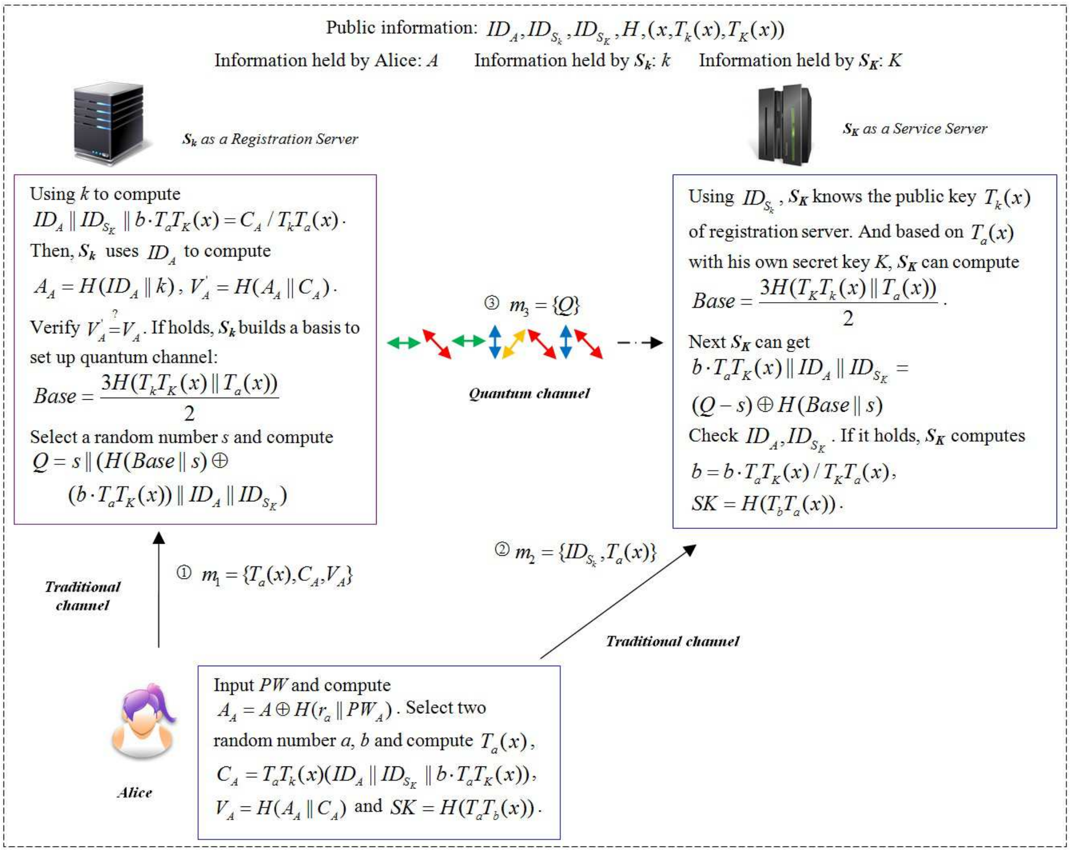

Public information: $ID_A, ID_{S_k}, ID_{S_K}, H, (x, T_k(x), T_K(x))$
Information held by Alice: A
Information held by S_k: k
Information held by S_K: K
S_k as a Registration Server
S_K as a Service Server
Using k to compute $ID_A \| ID_{S_K} \| b \cdot T_aT_K(x) = C_A / T_kT_a(x)$.
Then, S_k uses ID_A to compute $A_A = H(ID_A \| k)$, $V_A' = H(A_A \| C_A)$.
Verify $V_A' \overset{?}{=} V_A$. If holds, S_k builds a basis to set up quantum channel:
$Base = \frac{3H(T_kT_K(x) \| T_a(x))}{2}$
Select a random number s and compute $Q = s \| (H(Base \| s) \oplus (b \cdot T_aT_K(x)) \| ID_A \| ID_{S_K})$
③ $m_3 = \{Q\}$
Quantum channel
Using ID_{S_k}, S_K knows the public key $T_k(x)$ of registration server. And based on $T_a(x)$ with his own secret key K, S_K can compute
$Base = \frac{3H(T_KT_k(x) \| T_a(x))}{2}$.
Next S_K can get
$b \cdot T_aT_K(x) \| ID_A \| ID_{S_K} = (Q - s) \oplus H(Base \| s)$
Check ID_A, ID_{S_K}. If it holds, S_K computes
$b = b \cdot T_aT_K(x) / T_KT_a(x)$,
$SK = H(T_bT_a(x))$.
Traditional channel
① $m_1 = \{T_a(x), C_A, V_A\}$
② $m_2 = \{ID_{S_k}, T_a(x)\}$
Traditional channel
Alice
Input PW and compute $A_A = A \oplus H(r_a \| PW_A)$. Select two random number a, b and compute $T_a(x)$,
$C_A = T_aT_k(x)(ID_A \| ID_{S_K} \| b \cdot T_aT_K(x))$,
$V_A = H(A_A \| C_A)$ and $SK = H(T_aT_b(x))$.

FIGURE 2. Authenticated key agreement phase with quantum channel

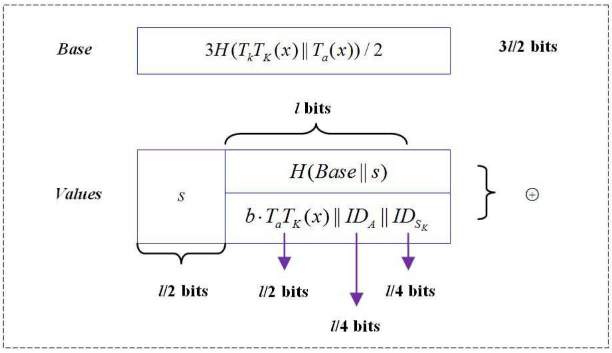


FIGURE 3. Structure of the quantum bits and the bases

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 corresponds 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 $Adv_{\prod,D}^{classical}(A) = 2|Pr[Succ_0] - \frac{1}{2}|$ (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 $Pr[Succ_1] = Pr[Succ_0]$ (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 $\{T_a(x), C_A, V_A\}$. According to the birthday paradox, the probability of collisions of the simulation of hash oracles is at most $q_h^2/2^{l+1}$. Since a, b were selected uniformly at random which are protected by the chaotic maps-based Discrete Logarithm problem. Thus, we have $Pr[Succ_2] - Pr[Succ_1] \leq q_h Adv_G^{dlp}(A) + q_h Adv_G^{cdh}(A) + \frac{q_h^2}{2^{l+1}}$ (3)

Game G_3 In this game, the session key is guessed without asking the corresponding oracle h so that it becomes independent of password and ephemeral keys a, b which are protected by the chaotic maps-based computational Diffie-Hellman problem. We change the way with earlier game unless A queries h on the common value $SK = H(T_a T_b(x))$. 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: $|Pr[Succ_3] - Pr[Succ_2]| \leq q_h Adv_G^{cdh}(A) + \frac{q_h}{p}$ (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 $SK = H(T_a T_b(x))$. 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 $|Pr[Succ_4] - Pr[Succ_3]| \leq \frac{q_h^2}{2^{l+1}}$ (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 $\prod$. 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:

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

Stage2: 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] uses the long shared key as the basis directly, while our related phase uses 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 ($SK = H(T_a T_b(x))$) 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:

$$Adv_{\prod,D}^{quantum}(A) \leq Adv_{3AQKDP}^{AQKD}(A) \leq \frac{2\left(q_{ini}+q_s\right)^2}{q_{ini}} \cdot Adv_{\psi}^{UCB}(\Delta)$$

4.2. **Further Security Discussion.**

(1) *The scheme could resist password guessing attack.*

Proof This attack means an adversary tries to guess a legal user's 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 online 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 server's 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 $A's$ request through validating the condition $V_A' \overset{?}{=} V_A$ during the proposed phase. To compute $A_A = A \oplus H(r_a \parallel PW_A)$, the attacker must have 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 S_K can compute the right basis: $Base = \frac{3H(T_k T_K(x) \parallel T_a(x))}{2}$, because they have the right secret key k or K.

For Alice authenticating S_k, she only need use SK to decrypt the encrypted message sent by S_K (Service Server). If the decrypted messages are plaintexts, which means that S_k is passed validation, or S_k fails the validation process.

For Alice authenticating S_K, she only need use SK to decrypt the encrypted message sent by S_K (Service Server). If the decrypted messages are plaintexts, which means that S_K is passed validation by S_k, or S_k cannot get b and S_k cannot compute SK.

(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 server's long-term secret key k because the session key is $SK = H(T_a T_b(x))$.

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

Proof There are no plaintext in the two messages of the proposed scheme. The message $\{T_a(x), C_A, V_A\}$ includes covered ciphertext $\{T_a(x), C_A\}$ which can transmit any important information to appointed node with the peer's public key, such as identity in the proposed scheme, and message $\{V_A\}$ is the verification ciphertext using one-way secure hash function. The other message $\{Q_A\}$ is transmitted using dynamic $Base_A$ by quantum channel which cannot be cloning **(No-cloning Theorem)**. Moreover, no message part is repeated in consecutive communications.

(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 out 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 $\{T_a(x), C_A, V_A\}$ which is protected by CDH problem in chaotic maps. Howerer, the adversary cannot compute $\{V_A\}$ as computation of $\{V_A\}$?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 $SK = H(T_aT_b(x))$ 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.*

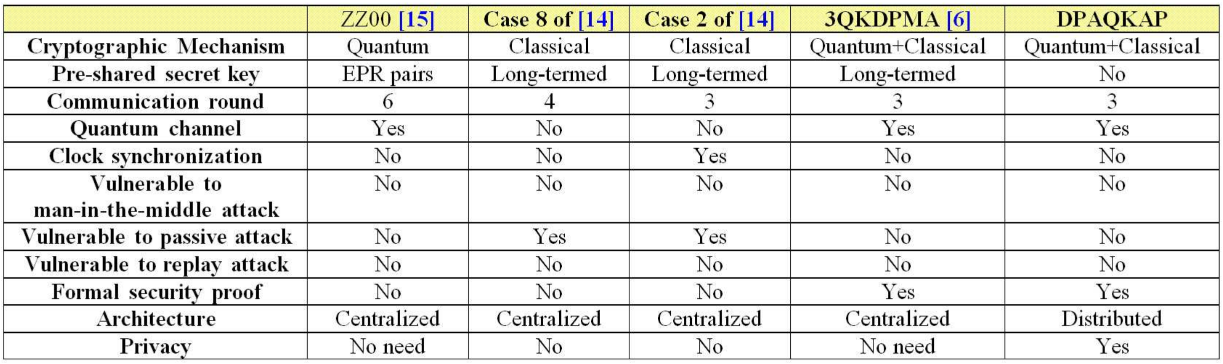
Proof Forward secrecy states that compromise of a legal user's long-term secret key does not become the reason to compromise of the established session keys. In our proposed scheme, the session key has not included the user's long-term secret key: Password. This shows that the forward secrecy property 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 dealt with the user's password which is stored in the user's 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 schemes.

Table 2. Comparison PAQKAPs among and Other Protocols



	ZZ00 [15]	Case 8 of [14]	Case 2 of [14]	3QKDPMA [6]	DPAQKAP
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	Distributed
Privacy	No need	No	No	No need	Yes

5. **Conclusion.** This work presents a distributed password-authenticated quantum key agreement protocol ($DPAQKAP$) which combines the advantages of classical cryptography and quantum cryptography in a universal way, and firstly introduces distributed architecture in classical cryptography into quantum cryptography. 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 user-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 quantum's feature. In the future, the features of different architecture and N-party will be considered, which will make the realm of classical cryptography with quantum cryptography more diversified to fit protean application scenarios.

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

REFERENCES

[1] H. F. Zhu, Y. F. Zhang, Y. Xia, and H. Y. Li, Password-Authenticated Key Exchange Scheme Using Chaotic Maps towards a New Architecture in Standard Model, *International Journal of Network Security*, vol. 18, no. 2, pp. 326-334, Mar. 2016.

[2] H. J. 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)*, 2013, v.31; no.101(03), pp. 397-400.

[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] D. Gottesman and H. K. Lo, Proof of Security of Quantum Key Distribution with Two-Way Classical Communications, *IEEE Trans. Information Theory*, vol. 49, p. 457, 2003.

[6] Hwang, T., Lee, K.C., Li, and C.M., Provably secure three-party authenticated quantum key distribution protocols, *IEEE Trans. Dependable Secure Comput*, vol. 4, no. 1, 71 (2007).

[7] D. J. Guan, Y. J. Wang, E. S. Zhuang, A practical protocol for three-party authenticated quantum key distribution, *Quantum Inf Process*,(2014), vol. 13, pp. 2355 - 2374.

[8] Zhang L, Cryptanalysis of the public key encryption based on multiple chaotic systems, *Chaos Solitons Fractals*, vol. 37, no. 3, pp. 669 - 674, 2008.

[9] Schwinger, J., Unitary operator bases, *Proc. Natl. Acad. Sci*, USA 46(4), 570 (1960).

[10] W. K. Wootters and W. H. Zurek, A Single Quantum Cannot Be Cloned, nature, vol. 299, pp. 802-803, 1992.

[11] M. N. Wegman, , J. L. Carter, New hash functions and their use in authentication and set equality, *Journal of Computer & System Sciences*, vol. 22, no. 265 (1981).

[12] C. H. Bennett, G. Brassard, and J. M. Robert, Privacy amplification by public discussion, SIAM *J. Comput.* vol. 17, no. 2, 210 (1988).

[13] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Quantum Cryptography, *Rev. of Modern Physics*, vol. 74, pp. 145-190, 2002.

[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] D. Dolev, A. C. Yao, On the security of public key protocols, *IEEE Transactions on Information Theory*, 29(2), 198-C208(1983).

[17] C. M. Chen, W. C. Fang, K. H. Wang, and T. Y. Wu, Comments on An improved secure and efficient password and chaos-based two-party key agreement protocol, *Nonlinear Dynamics*, vol. 87, issue 3, pp. 2073-2075, Feb. 2017.

[18] E. Bresson, O. Chevassut, D. Pointcheval, and J. J. Quisquater, Provably Authenticated Group Diffie-Hellman Key Exchange, *Proc. Eighth ACM Conf. Computer and Comm. Security*, pp. 255-264, 2001.

[19] H. F. Zhu, Flexible and Password-Authenticated Key Agreement Scheme Based on Chaotic Maps for Multiple Servers to Server Architecture, *Wireless Personal Communications*, 2015, 82(3):1697-1718.