Journal of Information Hiding and Multimedia Signal Processing ©2018 ISSN 2073-4212
Ubiquitous International Volume **9**, Number **3**, May **2018**

Provably Secure and Password-Authenticated Quantum Key Agreement Protocol with Dynamic Basis

Tianhua Liu, Yanlin Meng and Hongfeng Zhu*

Software College, Shenyang Normal University
No.253, HuangHe Bei Street, HuangGu District, Shenyang, P.C 110034 - China
liutianhua@sina.com; 569072432@qq.com; zhuhongfeng1978@163.com

*Corresponding author: zhuhongfeng1978@163.com

Received November, 2017; revised December, 2017

Abstract. *This paper presents password-authenticated quantum key agreement protocols (PAQKAPs) to guard security for internet era, which can combine classical cryptography and quantum cryptography in a universal way for the most common environment nowadays: Password. And PAQKAPs will guide in new directions for biometric-based with quantum cryptography, smart card-based with quantum cryptography and so on. Compared with the former research AQKDPs (authenticated quantum key distribution protocols), PAQKAPs have four 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. 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 key agreement, Password, Chaotic maps, Dynamic basis

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 two or more parties 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. 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 quantum cryptography, quantum key distribution protocols (QKDPs) [4-7] employ quantum mechanisms to distribute session keys and public discussions to check for eavesdroppers and verify the correctness of a session key.

Recently, Hwang et al. [6] proposed two three-party authenticated quantum key distribution protocols. The first one, which will be 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 new 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 Hwangs 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.

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 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. 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:

$$T_n\left(x\right) = (2xT_{n-1}(x) - T_{n-2}(x))(\text{mod}N),$$

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: $T_n\left(x\right) = (2xT_{n-1}(x) - T_{n-2}(x))(\bmod p)$, 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 DiffieCHellman 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 [11-13].

2.3. **Threat Model of Classical Cryptography and Definitions of Quantum Security.** The threat model should be adopted the widely accepted security assumptions about password based authentication schemes. We omit the concrete definitions for brief and the detail can be found in literatures [16-18].

Definition 2.4. ***No-cloning Theorem:*** *In 1982, Wootters and Zurek [10] proved that one cannot duplicate an unknown quantum state; that is, a user cannot copy a qubit if he/she does not know the polarization basis of the qubit. Using this no-cloning theorem, and based on the UCB(Unbiased-Chosen Basis) assumption of the literature [6], in which one can identify the polarization basis of an unknown quantum state with a negligible probability to facilitate security proof of the proposed PAQKAPs.*

Definition 2.5. ***Unbiased-Chosen Basis (UCB) Assumption:*** *Let* $\Psi \in \{D, R\}$ *be the qubit generating algorithm. Moreover, we define* Δ *as an UCB distinguisher who receives a qubit q and two bases* $\{D, R\}$ *as the challenge.* Δ *knows the qubit q produced by* $\Psi \in \{D, R\}$ *with the probability* ε. *The advantage for the distinguisher* Δ *to break the UCB assumption is denoted as* $Adv_{\Psi}^{UCB}(\Delta) = \varepsilon - \frac{1}{2}$. *The qubit generating algorithm* Ψ *is called UCB secure if* $Adv_{\Psi}^{UCB}(\Delta)$ *is negligible, which means* $Adv_{\Psi}^{UCB}(\Delta) \to 0$.

Definition 2.6. ***AQKD security*** *[6,18]: When the adversary* A *sends a Test query to the Fresh instance* Π_U^i *in an execution of 3AQKDP,* Π_U^i *will toss an unbiased coin. If the tossing result* $b = 1, \Pi_U^i$ *returns the m-bit session key SK to the adversary* A *. Otherwise,* Π_U^i *returns a m-bit random string. After receiving the m-bit string, the adversary* A *output* b' *and wins if guessed correctly* ($b = b'$). *Moreover, we describe the AQKD advantage of the adversary* A *in 3PAQKP as* $Adv_{3PAQKAP}^{AQKD}(A) = \Pr[b = b'] - \frac{1}{2}$. *The proposed 3 PAQKP is called AQKD secure if* $Adv_{3PAQKAP}^{AQKD}(A)$ *is negligible.*

3. The Proposed Scheme with Dynamic Basis.

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

Table 1 Notations

3.2. **User registration phase.** FIGURE 1 illustrates the user registration phase

Step 1. When a user 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 the ***server S*** via a secure channel.

Symbol	Definition
ID_S	The l/4-bit identity of the server
ID_A, ID_B	The l/4-bit identities of Alice and Bob respectively
PW_A, PW_B	Password of Alice and Bob respectively
a, b, s, 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 one-way hash function. $H:\{0,1\}^* \to \{0,1\}^l$ for a constant l
$\|\|$	concatenation operation
R	The rectilinear basis, polarized with two orthogonal directions, $\|0\rangle$ and $\|1\rangle$
D	The diagonal basis, polarized with two orthogonal directions, $\frac{1}{\sqrt{2}}(\|0\rangle+\|1\rangle)$ and $\frac{1}{\sqrt{2}}(\|0\rangle-\|1\rangle)$

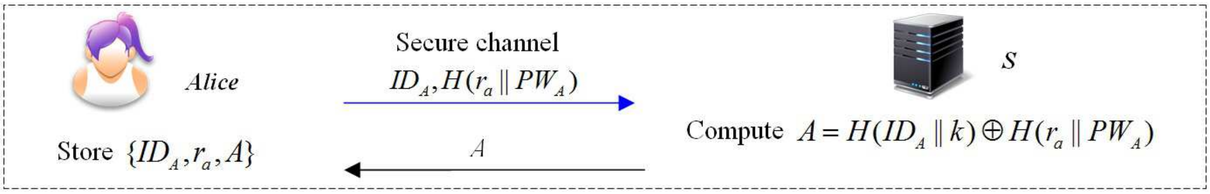


FIGURE 1. a premium user registration phase

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

The same way for Bob, and Bob stores $\{ID_B, r_b, B\}$ in a secure way.

3.3. **Authenticated key agreement phase.** FIGURE 2 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, she will input *password* and compute $A_A = A \oplus H(r_a||PW_A)$, and then choose a random integer number a and compute $T_a(x)$ and $V_A = H(A_A||ID_B||T_a(x))$. After that, Alice sends $m_1 = \{ID_A, ID_B, T_a(x), V_A\}$ to the server $\boldsymbol{S}$ which she has registered.

The same way for Bob, and Bob sends $m_2 = \{ID_A, ID_B, T_b(x), V_B\}$ to $\boldsymbol{S}$.

Step 2. After receiving the message
$m_1 = \{ID_A, ID_B, T_a(x), V_A\}$ and $m_2 = \{ID_A, ID_B, T_b(x), V_B\}$ from Alice/Bob, and $\boldsymbol{S}$ firstly computes $A_A = H(ID_A||k)$, $B_B = H(ID_B||k)$,
$V_A^{=}H(A_A||ID_B||T_a(x))$, $V_B^{=}H(B_B||ID_A||T_b(x))$ based on ID_A, ID_B. $\boldsymbol{S}$ compares $V_A^{=}V_A$? and $V_B^{=}V_B$?.
If above equations hold, which means Alice and Bob are legal users, or $\boldsymbol{S}$ will abort this process. Next, $\boldsymbol{S}$ will Build two bases to set up quantum channel: $Base_A = H(A_A||T_a(x))||(H(T_a(x))/2)$ and $Base_B = H(B_B||T_b(x))||(H(T_b(x))/2)$. Then $\boldsymbol{S}$ select a random number s and computes $Q_A = s||(H(Base_A||s) \oplus T_b(x)||ID_A||ID_B)$ and $Q_B = s||(H(Base_B||s) \oplus T_a(x)||ID_A||ID_B)$. The structure of Q_A and Q_B are depicted in FIGURE 3. For Alice, the quantum bit of $(Q_A)_i$, if $(Bases_A)_i = 0$, the server $\boldsymbol{S}$ will use R as its basis, otherwise D is the chosen basis. Similarly, $\boldsymbol{S}$ creates Q_B for Bob.

Finally the server $\boldsymbol{S}$ sends Q_A and Q_B to Alice and Bob using quantum channel based on $Base_A$ and $Base_B$ respectively.

Step 3. Alice has already computed the $Base_A = H(A_A||T_a(x))||(H(T_a(x))/2)$ locally. Then Alice receives Q_A and measures it based on $Base_A$. So, Alice can get s from Q_A with

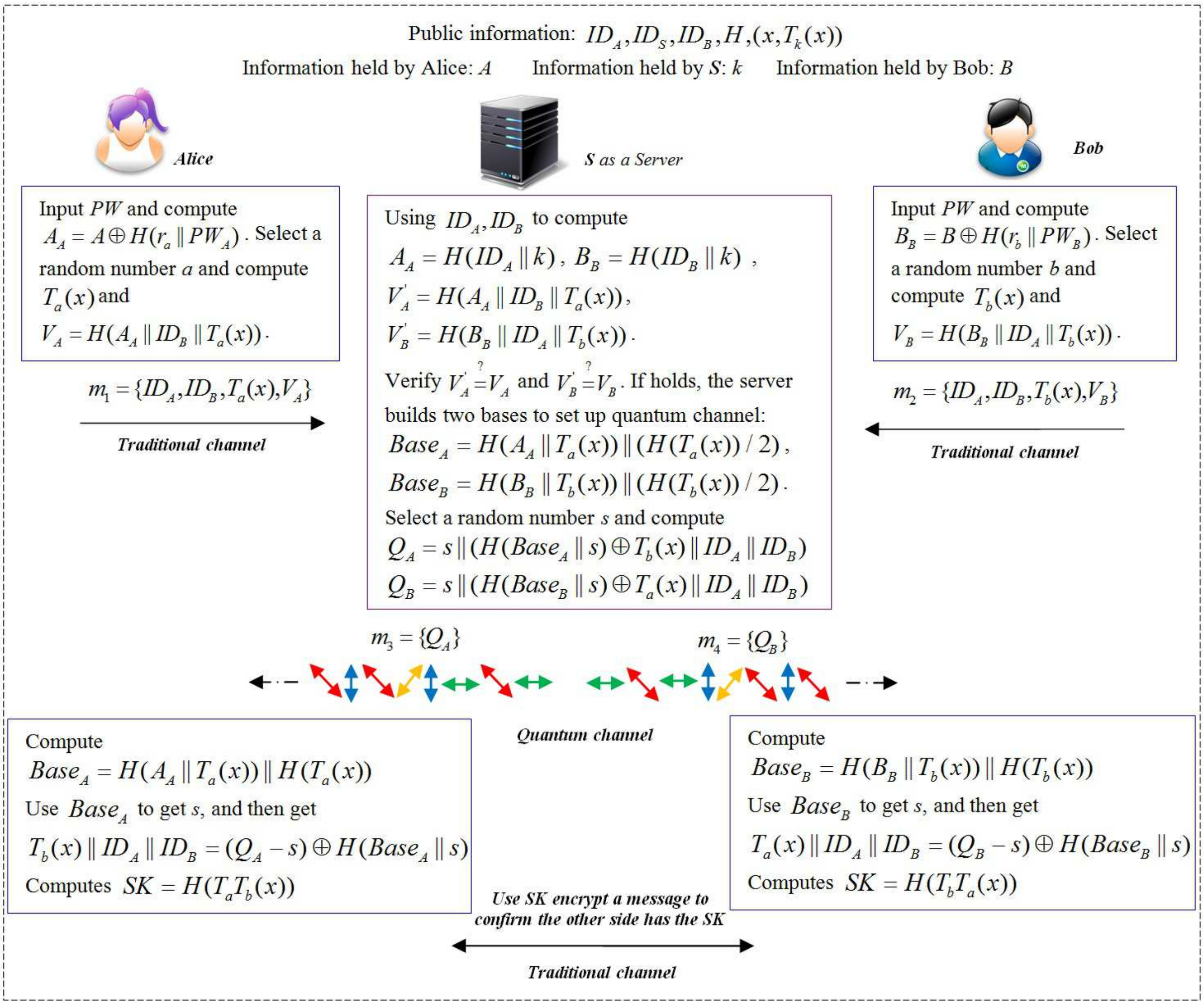

Public information: $ID_A, ID_S, ID_B, H, (x, T_k(x))$
Information held by Alice: A
Information held by S: k
Information held by Bob: B
Alice
S as a Server
Bob
Input PW and compute $A_A = A \oplus H(r_a \| PW_A)$. Select a random number a and compute $T_a(x)$ and $V_A = H(A_A \| ID_B \| T_a(x))$.
Using ID_A, ID_B to compute $A_A = H(ID_A \| k)$, $B_B = H(ID_B \| k)$, $V_A^{'} = H(A_A \| ID_B \| T_a(x))$, $V_B^{'} = H(B_B \| ID_A \| T_b(x))$.
Verify $V_A^{'} \overset{?}{=} V_A$ and $V_B^{'} \overset{?}{=} V_B$. If holds, the server builds two bases to set up quantum channel:
$Base_A = H(A_A \| T_a(x)) \| (H(T_a(x))/2)$,
$Base_B = H(B_B \| T_b(x)) \| (H(T_b(x))/2)$.
Select a random number s and compute
$Q_A = s \| (H(Base_A \| s) \oplus T_b(x) \| ID_A \| ID_B)$
$Q_B = s \| (H(Base_B \| s) \oplus T_a(x) \| ID_A \| ID_B)$
Input PW and compute $B_B = B \oplus H(r_b \| PW_B)$. Select a random number b and compute $T_b(x)$ and $V_B = H(B_B \| ID_A \| T_b(x))$.
$m_1 = \{ID_A, ID_B, T_a(x), V_A\}$
Traditional channel
$m_2 = \{ID_A, ID_B, T_b(x), V_B\}$
Traditional channel
$m_3 = \{Q_A\}$
$m_4 = \{Q_B\}$
Quantum channel
Compute $Base_A = H(A_A \| T_a(x)) \| H(T_a(x))$
Use $Base_A$ to get s, and then get $T_b(x) \| ID_A \| ID_B = (Q_A - s) \oplus H(Base_A \| s)$
Computes $SK = H(T_a T_b(x))$
Compute $Base_B = H(B_B \| T_b(x)) \| H(T_b(x))$
Use $Base_B$ to get s, and then get $T_a(x) \| ID_A \| ID_B = (Q_B - s) \oplus H(Base_B \| s)$
Computes $SK = H(T_b T_a(x))$
Use SK encrypt a message to confirm the other side has the SK
Traditional channel

FIGURE 2. Authenticated key agreement phase with quantum channel

the front l/2 bits, and next Alice will get $T_b(x)||ID_A||ID_B = (Q_A - s) \oplus H(Base_A||s)$. Alice verifies the identities of ID_AandID_B. If holds, based on $T_b(x)$ Alice can compute session key $SK = H(T_aT_b(x))$.

The same way for Bob. If any authenticated process does not pass, the protocol will be terminated immediately.

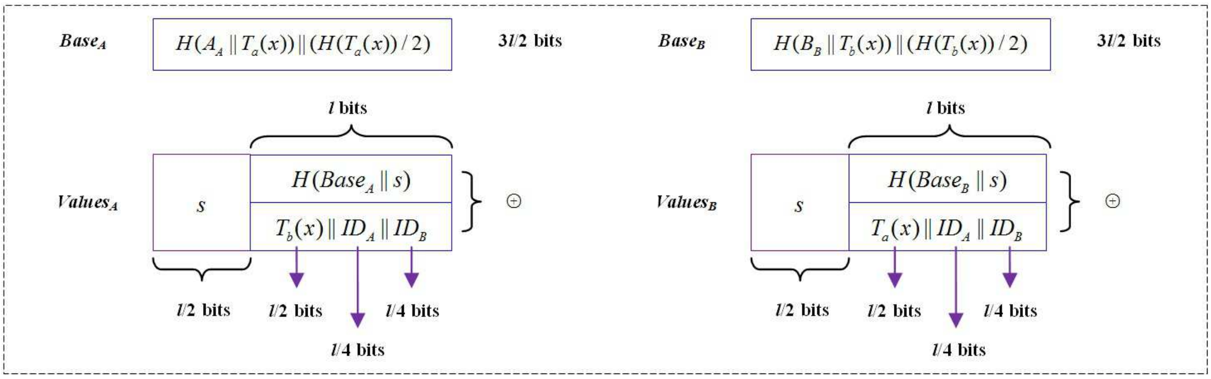


FIGURE 3. Structure of the quantum bits and the bases

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 $SK = H(T_aT_b(x)||ID_A||$
$ID_B)$, $SK = H(T_aT_b(x)||T_a(x)||T_b(x))$ and so on, without $\boldsymbol{S}$ involved for saving time and quantum resources.

3.4. **Password changing phase.** FIGURE 4 illustrates the password changing phase.

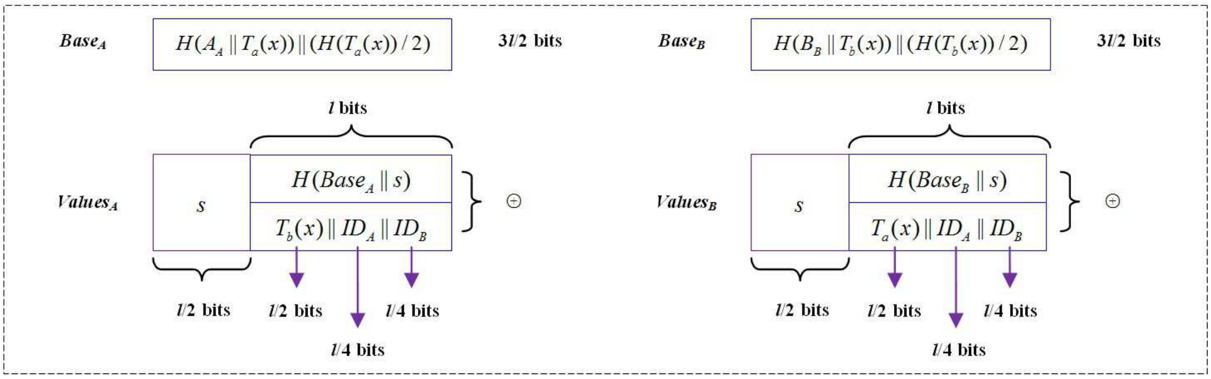


FIGURE 4. Password changing phase

Step 1. When a user wants to change her password, she chooses a new password PW', two random numbers r'_a, a, and computes $A_A = A \oplus H(r_a||PW)$, $T_a(x)$ and $V_A = H(A_A||ID_A||T_a(x))$. Then Alice sends $m_1 = \{ID_A, T_a(x), V_A\}$ to $\boldsymbol{S}$.

Step 2. After receiving the message $m_1 = \{ID_A, T_a(x), V_A\}$ from Alice, and $\boldsymbol{S}$ firstly computes $A_A = H(ID_A||k)$ and $V_A^{=}H(A_A||ID_A||T_a(x))$ based on ID_A. $\boldsymbol{S}$ compares $V_A^{=}V_A?$. If above equation holds, which means Alice is legal user, or $\boldsymbol{S}$ will abort this process. Next $\boldsymbol{S}$ will build a base to set up quantum channel $Base_A = H(A_A||T_a(x))||(H(T_a(x))/2)$. Then $\boldsymbol{S}$ select a random number s and computes $Q_A = s||(H(Base_A||s) \oplus T_sT_a(x)||ID_A||ID_S)$. The structure of Q_A is also depicted in FIGURE 3. For Alice, the quantum bit of $(Q_A)_i$, if $(Bases_A)_i = 0$, the server $\boldsymbol{S}$ will users R as its basis, otherwise D is the chosen basis.

Step 3. Alice has already computed the $Base_A = H(A_A||T_a(x))||(H(T_a(x))/2)$ locally. Then Alice receives Q_A and measures it based on $Base_a$. So, Alice can get s from Q_A with the front l/2 bits, and next Alice will get $T_sT_a(x)||ID_A||ID_S = (Q_A - s) \oplus H(Base_A||s)$. Alice computes $T_aT_s(x)$ verifies $T_aT_s(x) = T_sT_a(x)$ or not. If above equation holds, Alice computes $A' = A_A \oplus H(r'_a||PW')$ and stores $\{ID_A, r'_a, A'\}$ in a secure way.

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,*

$$Adv_{\Pi,D}(A) = Adv_{\Pi,D}^{\text{classical}}(A) + Adv_{\Pi,D}^{\text{quantum}}(A) \leq \frac{4q_h^2}{2^{l+1}} + 2q_hAdv_G^{dlp}(A) + 2q_hAdv_G^{cdh}(A) + \frac{2q_h}{p} + \frac{q_s}{D} + \frac{2(q_{ini}+q_s)^2}{q_{ini}} \cdot Adv_\Psi^{UCB}(\Delta)$$

where $Adv_G^{cdh}(A)$ is the success probability of A of solving the chaotic maps-based computational DiffieCHellman 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 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 $\{ID_A, ID_B, T_a(x), V_A\}$ or $\{ID_A, ID_B, T_b(x), V_B\}$. 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

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

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 DiffieCHellman 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 G3 and the game G2 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 $SK = H(T_a T_b(x))$. 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

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

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:

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

Stage2: This stage simulates the quantum cryptography. In order to make the security proof simple, we firstly 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:

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

4.2. **Further Security Discussion.** (1) *Resist password guessing attack.* 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) Mutual authentication. In our scheme, the Registration *Server* $\boldsymbol{S}$ verifies the authenticity of user $A's$ request by verifying the condition $V_A' \overset{?}{=} V_A$ during the proposed phase.To compute $A_A = A \oplus H(r_a||PW_A)$, the password is needed. Therefore, an adversary cannot forge the message. Additionally, $T_a(x), V_A$ includes a large random nubmer a, the adversary cannot replay the old message. This shows that $\boldsymbol{S}$ can correctly verify the message source. For Alice/Bob authenticating the server $\boldsymbol{S}$, s/he only computes $Base_A = H(A_A||T_a(x))||H(T_a(x))$ or $Base_B = H(B_B||T_b(x))||H(T_b(x))$ to receive the Q_A/Q_B. If the decrypted messages including $ID_A||ID_B$, which means that the server is passed validation, or the server fails the validation process.

(3)*Perfect forward secrecy.* A scheme is said to support perfect forward secrecy, if the adversary cannot compute the established session key, using 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 $SK = H(T_aT_b(x))$. This shows that our scheme provides the perfect forward secrecy property.

(4)*Resist stolen verifier attack.* In the proposed scheme, any party stores nothing about the legal users information. 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.

(5) *Withstand replay and man-in-the-middle attacks.* 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). So our proposed scheme resists the replay and man-in-the-middle attacks.

(6)*Resist user impersonation 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 $\{ID_A, ID_B, T_a(x)\}$ for a random value a. Howerer, the adversary cannot compute $\{V_A\}$ as computation of $\{V_A\}$ requires PW which is only known to legal users.

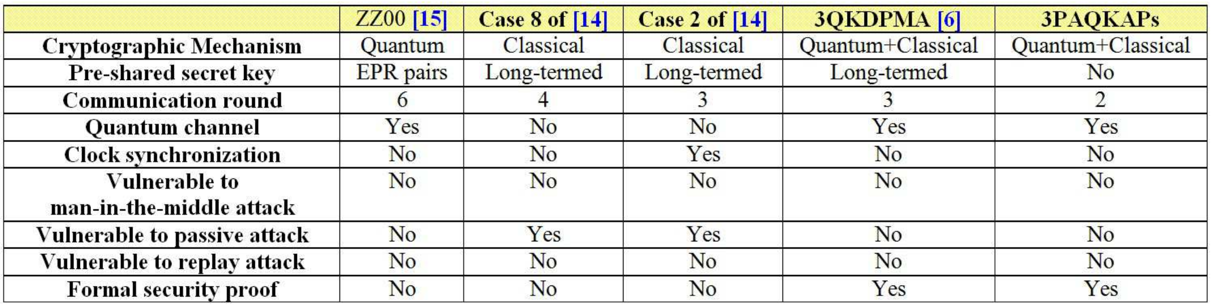
(7)*Key freshness property.* Note that in our scheme, each established session key $SK = H(T_aT_b(x))$ includes random values a and b. The unique key construction for each session shows that proposed scheme supports the key freshness property.

(8)*Have known key secrecy property.* Each session key is hashed with one-way hash function. Therefore, no information can be retrieved from the session key. Each session key includes two nonces, which ensures different key for each session. Since no information about other established group session keys from the compromised session key is extracted, our proposed scheme achieves the known key secrecy property.

(9)*Forward secrecy.* 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 our scheme preserves the forward secrecy property.

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]	3PAQKAPs
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	2
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

5. **Conclusions.** This work presents a three-party password-authenticated quantum key agreement protocol (3PAQKAP) which combines the advantages of classical cryptography and quantum cryptography in a universal way, and firstly introduces the most general authentication method–password 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 four advantages at least: dynamic basis, key agreement, no verifiable table and no off-line password guessing attack. Additionally, the proposed scheme has fewer communication rounds than other protocols and 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. By combining the advantages of password-authenticated in classical cryptography with quantum cryptography, this work presents a new direction from the user's perspective.

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

REFERENCES

[1] H. Zhu, Y. Zhang, Y. Xia, and H. 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. Wang, H. Zhang, J. Li and C. Xu, A(3,3) visual cryptography scheme for authentication, *Journal of Shenyang Normal University (Natural Science Edition)*, vo.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] 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] T. Hwang, K.C. Lee, C. M. Li, Provably secure three-party authenticated quantum key distribution protocols, *IEEE Trans. Dependable Secure Comput.* vol. 4, no. 1, pp. 71, 2007.

[7] D. J. Guan, Yuan-Jiun Wang, E. S. Zhuang, A practical protocol for three-party authenticated quantum key distribution, *Quantum Inf Process* vol. 13, 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*, 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, *J.Comput. Syst,* Sci. 22, 265, 1981.

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

[17] C. M. Chen, L. Xu, T. Y. Wu and C. R. Li, On the Security of a Chaotic Maps-based Three-Party Authenticated Key Agreement Protocol, *Journal Network Intelligence*, vol. 1, No 2, 2016.

[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.