Quantum Inf Process (2014) 13:2355–2374
DOI 10.1007/s11128-014-0767-1

A practical protocol for three-party authenticated quantum key distribution

D. J. Guan · Yuan-Jiun Wang · E. S. Zhuang

Received: 1 March 2012 / Accepted: 28 May 2014 / Published online: 19 June 2014

Abstract Recently, Hwang et al. proposed two three-party authenticated quantum key distribution protocols for two communicating parties to establish a session key via a trusted center. They also showed their protocols were secure by using random oracle model. However, their protocols were designed to run in an ideal world. In this paper, we present a more practical protocol by considering some issues, which have not been addressed in their protocols. These issues include (1) session key consistence, (2) online guessing attack, and (3) noise in quantum channels. To deal with these issues, we use error correction code and key evolution. We also give a formal proof for the security of our protocols by using standard reduction, instead of the random oracle model.

Keywords Quantum cryptography · Quantum key distribution · Three-party key distribution protocol · Provable security · Standard problem reduction

D. J. Guan · Y.-J. Wang (✉) · E. S. Zhuang
Department of Computer Science and Engineering, National Sun Yat-sen University,
Kaohsiung, Taiwan, ROC
e-mail: wangyj@isl.cse.nsysu.edu.tw

D. J. Guan
e-mail: guan@cse.nsysu.edu.tw

E. S. Zhuang
e-mail: zhuanges@isl.cse.nsysu.edu.tw

Present address
D. J. Guan
Department of Computer Science and Engineering, National Chung Hsing University,
Taichung, Taiwan, ROC

1 Introduction

1.1 Motivations

In 1984, Bennett et al. proposed quantum key distribution (QKD) protocols, which can be used by two authenticated parties to establish a random key without sharing a common secret [1–4]. These protocols have been proved to be unconditionally secure [2,5–12] under the assumption that the communication parties have been authenticated. Thus, the security of these QKD protocols are based on the properties of quantum physics, instead of the limitations of the computational power of the attacker.

User authentication is an important issue in secure communication. There exist information theoretically secure user authentication protocols, which can be used before applying the QKD [13]. However, in many applications, user authentication and key distribution can be integrated into one step.

Recently, Hwang et al. [14] proposed two three-party authenticated quantum key distribution protocols. The first one, which will be called 3AQKDP, can be used to establishes 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.

In this paper, we try to design a protocol, which can be run in a more practical environment under current technology. First, we briefly describe the issues that 3AQKDP has not addressed.

(1) The attacker can learn some information about the long-term key in each attack, and the information they learn can be accumulated. Thus, their protocols are vulnerable to online guessing attack.
(2) The attacker may alter some bits of the session key without being detected. Thus, the session key obtained by Alice and Bob may be inconsistent.
(3) The noise in the quantum channel was not considered in their protocols.

Note that the communicating parties must share a common secret to make authentication possible. User authentication can be done via a trusted authority (TA). In this case, each user and the TA need to share a common secret key. These secret keys are very important in the design of the protocols, and they are usually referred as the *long-term secret key*. Once the attacker learns the long-term secret key, the protocol cannot be secure anymore.

Many literature have shown the impossibility of perfect quantum secure authentication [15–17]. If legitimate users authenticate themselves by using the same secret key they shared, Eve can extract some information about the secret key from the protocol. Moreover, since the same key is used again and again, the information she learned can be accumulated. Thus, Eve can obtain the whole secret key after certain number of attacks.

In Sect. 3, we describe an attack on 3AQKDP. We show that there is a non-negligible probability that no eavesdropper can be detected, but the session key shared by Alice and Bob may be inconsistent. Furthermore, the information learned by the attacker can be accumulated. Therefore, the attacker can learn information about the long-term secret key after certain number of attacks. Therefore, their protocols are vulnerable to the online guessing attack. Note that this type of attack has been addressed by the authors themselves [14]. They suggested updating the secret key if the protocol has failed a certain number of times.

The third issue, the noise in quantum channel, is an important practical issue to implement a quantum cryptosystem by using current technology.

In addition to the above three issues, in Hwang et al.'s [14] paper, they proved the secrecy of the session key in 3AQKDP and 3QKDPMA by using the random oracle model. However, using random oracle in the proof of the security of a protocol is debatable. Canetti et al. have shown that there exist signature and encryption schemes that are proved to be secure in the random oracle model, but no secure implementation can exist [18,19].

1.2 Our main contributions

In this paper, we present a new three-party authenticated quantum key distribution protocol, N3AQKDP, to address some important issues in 3AQKDP. Our protocol can work in noisy quantum channels. This is closer to a real-world environment by using current technologies. Furthermore, we show that our protocol can resist the online guessing attack.

The main techniques used in our protocol against the online guessing attack are the following:

1. If Eve attacks a few qubits, the communicating parties can correct their session key by error correction codes and evolve the secret key efficiently. Hence, Eve obtains almost no information about the new secret key.
2. If Eve attacks many qubits to make our protocol abort, although the secret key cannot be updated, the information of the secret key obtained by Eve is negligible. Hence, Eve cannot obtain the secret key within a polynomial number of attacks.

We formally define the security of our N3AQKDP, which is similar to that of the BB84 protocol. We prove the security of our protocol N3AQKDP by standard reduction to the security of the BB84 protocol. This implies that any attacks to our protocol can also be used to attack BB84 protocol. Since BB84 protocol has been proven to be secure [11], our protocols are secure.

In the case that our protocol aborts, the same secret key will be used in the next run. We prove the following two facts to justify our claim that our protocol can resist the online guessing attack.

(1) The expected value of Eve's information gain about the shared secret key before our protocol succeeds is less than 0.6 bits in average.

(2) The probability that Eve can break the secret key is negligible. That is, the probability for Eve to break the secret key is less than $1/p(\lambda)$, for any polynomial p of the security parameter λ.

1.3 Main techniques used in our protocols

Classical error correction codes and key evolution [20] are the main techniques to make our protocol secure. Note that quantum error correction codes can also be used in the transmission of qubits to make quantum communication more reliable. Any quantum error correction code, such as the Calderbank-Shor-Steane (CSS) codes [21,22] can be used in our protocols. In this paper, we will omit these infrastructures for quantum communication.

One of the advantages of using qubits in communication, instead of using classical bits, is the attacker, Eve, can never learn all the information about the qubits. Furthermore, if Eve learns some information on the qubits, then she will also induce errors in the qubits with high probability. Therefore, if the *quantum bit error rate* is above a threshold, there is a high probability that there is an attacker who is trying to learn the information about the key or the message. By estimating quantum bit error rate, one can estimate the information leakage and thus to detect the adversary.

Our protocols use qubits to transmit the classical message. Each qubit is measured in a basis according to the shared secret key. The outcome of a qubit measured can be defined as 0 or 1 to represent a classical bit. Thus, the qubits are measured and decoded as a classical message by the receiver. We note that although a qubit can be disturbed by the noise of quantum channel and the attacker, in our protocol, the sender and the receiver are interested in classical messages. Any error, whether it is due to the attacker or the quantum system will be treated the same way.

We propose using key evolution [20] and error correction codes to deal with the online guessing attack. The key evolution is based on the principle of privacy amplification [23,24]. Since repeatedly using the same key may not be secure, the key evolution can be used to update the secret key so that a new key can be used in the next run. Furthermore, key evolution is more efficient than creating a new secret key.

1.4 Structure of this paper

The remaining sections of the paper are organized as follows. In Sect. 2, some techniques used in quantum cryptosystems are described. In Sect. 3, we briefly review Hwang et al.'s 3AQKDP and address some issues which have not considered by the authors on the design of 3AQKDP. The proposed protocol N3AQKDP is presented in Sect. 4. We also give some parameters to show that our protocol are practical. In Sect. 5, we prove and analyze the security of our protocol. We prove the security of our protocol N3AQKDP by standard reduction to the BB84 protocol if the secret key can be evolved in Sect. 5.1. We analyze the expected value of Eve's information gain and the probability of breaking our protocol to show that our protocol N3AQKDP can resist the online guessing attack in Sect. 5.2. Finally, we conclude and discuss our work in Sect. 6.

2 Quantum cryptosystem techniques

Many techniques, including *eavesdropper detection*, *error correction* and *privacy amplification*, can be used in the design of quantum cryptographic protocols. In this section, we briefly describe those techniques, which will be used in the design of our protocols.

A qubit can be described by a vector in two-dimensional Hilbert space. Let

$$\mathcal{R} = \{|0\rangle, |1\rangle\}$$

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

$$\mathcal{D} = \{|+\rangle, |-\rangle\}$$

be another basis. The bases $\mathcal{R}$ and $\mathcal{D}$ are mutually unbiased bases [25]. These two mutually unbiased bases are widely used in quantum cryptography, e. g., the BB84 protocol.

Assume that the state of a qubit $|q\rangle$ is in one of the four states $|0\rangle$, $|1\rangle$, $|+\rangle$,or $|-\rangle$. Note that these states are the union of $\mathcal{R}$ and $\mathcal{D}$. We call $\mathcal{R}$ and $\mathcal{D}$ the *bases* of $|q\rangle$. The outcome is 'random' if the qubit $|q\rangle$ is prepared in one basis and it is measured in the other basis. Let $|0\rangle$ and $|+\rangle$ correspond to 0 for a classical bit, and let $|1\rangle$ and $|-\rangle$ correspond to 1. We call 0 and 1 the *values* of $|q\rangle$.

Let $|q\rangle$ be a qubit defined as above. It is well known that without knowing the basis of a qubit, the attacker Eve will disturb its state with high probability if she measures the qubit with a randomly chosen basis $\mathcal{R}$ or $\mathcal{D}$.

Suppose that Alice and Bob communicate using the qubits. Assume that they know the bases of the qubits, then they can check the states of the qubits to detect whether Eve has eavesdropped in quantum channel or not. Combining this property with random sampling test, a quantum cryptosystem can estimate the error rate in quantum channel. This technique allows Alice and Bob to estimate Eve's information gain by the error rate. If the error rate is below the threshold, it means that not much information was leaked to Eve. Then they can correct errors in their communicating messages by using error correction code.

We also use the privacy amplification in our protocol. It is well known that Eve must be able to learn some information during the communication even if qubits are used. The technique of privacy amplification can be used to reduce Eve's mutual information on the secret key to a desired level of security if the information leakage is small. The idea is to shorten the length of the secret key to eliminate Eve's information.

A theorem of the privacy amplification [23] can be described as follows. Assume that Alice sends an n-bit secret to Bob, and Eve learns l bits of information about the secret in the transmission. Let $s > 0$ be a security parameter and let $m = n - l - s$. Alice and Bob can shorten the secret to m bits to reduce Eve's information about the shortened secret to be less than $2^{-s} / \ln 2$ bits. One can properly choose s such that Eve has almost no information about the m-bit secret if $n > l$. Furthermore, privacy amplification can be done efficiently by a universal hash function [13,26]. Alice chooses a hash function from a class of universal hash functions family and announces it publicly. It has been shown that only a little information is needed to identify the chosen hash function [23].

In order to overcome the noise and the attacker's disturbance in the qubits, we use classical error correction codes to correct the errors of the session key in our protocol. Since the session keys in our protocol are classical bits and our protocol uses single qubit to represent a classical bit, it is efficient to correct the errors of the session key using classical error correction codes.

3 Hwang et al.'s 3AQKDP

In this section, we briefly describe 3AQKDP [14] and address some issues, which have not been considered by the authors in the design of 3AQKDP.

3.1 A brief description of Hwang et al.'s protocol

Alice shares with the TC an n-bit secret key K_{TA}, and Bob shares with the TC another n-bit secret key K_{TB}. Alice and Bob would like to establish a u-bit session key K_s by the help of the trusted TC.

Let U_A be the identity of Alice. Let U_B be the identity of Bob. Both U_A and U_B are k-bit binary string. Let $\mathcal{R} = \{|0\rangle, |1\rangle\}$ and $\mathcal{D} = \{|+\rangle, |-\rangle\}$ be two bases. The 3AQKDP can be described as follows.

1. The TC randomly chooses a session key K_s.
2. The TC picks two random l-bit strings r_{TA} and r_{TB} for Alice and Bob, respectively, and then the TC computes $R_{TA} = h(K_{TA} \cdot r_{TA}) \oplus (K_s \cdot U_A \cdot U_B)$ for Alice and $R_{TB} = h(K_{TB} \cdot r_{TB}) \oplus (K_s \cdot U_B \cdot U_A)$ for Bob. Here h denotes the one-way hash function $\{0, 1\}^* \rightarrow \{0, 1\}^m$, $\oplus$ denotes modulo 2 addition or bit-wise exclusive-or operation and '$\cdot$' denotes string concatenation. Note that the lengths of R_{TA}, R_{TB}, $(K_s \cdot U_A \cdot U_B)$ and $(K_s \cdot U_B \cdot U_A)$ are all m bits and $m = u + 2k$.
3. Let $n = l + m$. Hence, the lengths of K_{TA} and $(r_{TA} \cdot R_{TA})$ are both equal to n. The TC creates n qubits Q_{TA} for Alice using K_{TA} and $(r_{TA} \cdot R_{TA})$. The structure of Q_{TA} is depicted in Fig. 1. For $(Q_{TA})_i$, if $(K_{TA})_i = 0$, the TC uses $\mathcal{R}$ as its basis, otherwise $\mathcal{D}$ is the chosen basis. $|0\rangle$ or $|+\rangle$ is created if $(r_{TA} \cdot R_{TA})_i = 0$; and $|1\rangle$ or $|-\rangle$ if $(r_{TA} \cdot R_{TA})_i = 1$. Table 1 lists the states to generate $(Q_{TA})_i$. Similarly, the TC creates Q_{TB} for Bob.

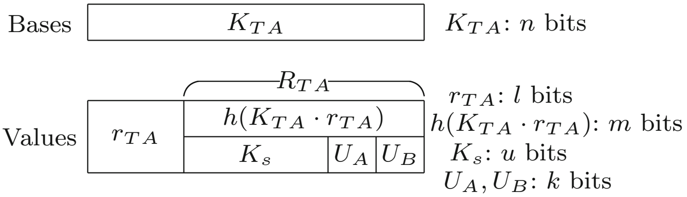

Fig. 1 Structure of Q_{TA} in 3AQKDP

Table 1 Qubit $(Q_{TA})_i$ generation

$(Q_{TA})_i$	$(r_{TA} \cdot R_{TA})_i = 0$	$(r_{TA} \cdot R_{TA})_i = 1$
$(K_{TA})_i = 0$	$\vert 0\rangle$	$\vert 1\rangle$
$(K_{TA})_i = 1$	$\vert +\rangle$	$\vert -\rangle$

4. The TC sends Q_{TA} and Q_{TB} to Alice and Bob, respectively.
5. Alice receives Q_{TA} and measures it according to K_{TA}. If $(K_{TA})_i = 0$, $\mathcal{R}$ is used to measure the $(Q_{TA})_i$; otherwise $\mathcal{D}$. Similarly, Bob measures Q_{TB} using $\mathcal{R}$ or $\mathcal{D}$ depending on K_{TB}.
6. The measuring outcomes are the values of $(r'_{TA} \cdot R'_{TA})$. Then Alice can compute $(K'_s \cdot U_A \cdot U_B) = h(K_{TA} \cdot r'_{TA}) \oplus R'_{TA}$. Similarly, Bob gets $(r'_{TB} \cdot R'_{TB})$ and computes $(K''_s \cdot U_B \cdot U_A) = h(K_{TB}, r'_{TB}) \oplus R'_{TB}$.
7. Alice and Bob verify the values of U_A and U_B. They accept the session key if the values of U_A and U_B are correct.

Hwang et al. [14] proved the security of 3AQKDP under the random oracle model and addressed that 3AQKDP suffers the online guessing attack. The security of 3AQKDP is defined as the amount of information leaked to the adversary attacking the session key K_s. Since $R_{TA} = h(K_{TA} \cdot r_{TA}) \oplus (K_s \cdot U_A \cdot U_B)$, Eve needs to call the hash function to get the value of $h(K_{TA} \cdot r_{TA})$ if she wants to break the K_s. They have shown the amount of information leaked to the adversary is negligible in 3AQKDP. However, the definition does not include the security of the shared secret key. When Eve attacks the secret key using the online guessing attack, she does not need to call the hash function. We show that Eve can attack the 3AQKDP without calling the hash function in the next subsection.

3.2 Security issues on 3AQKDP

In this subsection, we discuss three security issues on 3AQKDP mentioned in Sect. 1.

We first present an attack on 3AQKDP that the session keys obtained by Alice and Bob may not be consistent even if the values of U_A and U_B are correct. Assume that Eve attacks Q_{TA} sent to Alice. Recall that the values of Q_{TA} depend on $r_{TA} \cdot R_{TA} = r_{TA} \cdot (h(K_{TA} \cdot r_{TA}) \oplus (K_s \cdot U_A \cdot U_B))$. The Q_{TA} can be divided into three parts: r_{TA}, K_s and $U_A \cdot U_B$. If Eve only attacks the qubits in the K_s, i.e., from the $(l+1)$th to the $(l+u)$th qubits of Q_{TA}, the values of r_{TA}, $h(K_{TA} \cdot r_{TA})$, U_A and U_B remain intact. Therefore, U_A and U_B will always be correct when the users verify the identities. Alice thus believes there is no eavesdropper. However, if some values of the qubits in K_s are changed, the K'_s received by Alice may be different from the K_s generated by the TC. Therefore, the session key obtained by Alice and Bob may not be consistent even if U_A and U_B are intact. The authors of 3AQKDP only considered that Eve disturbs the qubits in r_{TA}. Moreover, 3AQKDP does not verify the correctness of the session keys or correct the errors of the session keys.

The second security issue of 3AQKDP is the online guessing attack that aims at the long-term secret key between the users, Alice or Bob, and the TC. The details of the attack can be described as follows. Eve intercepts the qubit sequence sent by the TC. Without loss of generality, assume that Eve attacks the qubits sent to Alice. She measures one qubit of the sequence by randomly choosing a basis from $\mathcal{R}$ and $\mathcal{D}$. After the qubit is measured, we call it the measured qubit. Then Eve places the measured qubit back to the original qubit sequence. She resends the new qubit sequence to Alice. The protocol can either finish successfully or fail. If the protocol fails, it indicates that Eve has measured the qubit in a wrong basis to make the identities incorrect. Therefore, Eve learns the correct basis of the qubit.

The following calculation shows that the long-term secret key in 3AQKDP suffers the online guessing attack. The protocol always succeeds if Eve used a correct basis to measure. However, the protocol succeeds with probability 0.5 even if Eve measured the qubit in a wrong basis. Alice's reaction is called *negative* if the protocol failed [14]. Eve learns the correct basis of the qubit if a negative reaction occurs. The probability is 0.25. On average she thus gets $0.25 \times 1 + 0.75 \times 0 = 0.25$ bits of information in each attack. Thus, Eve can get a some information about the shared secret key with a non-negligible probability.

The worst thing is that Eve's information about the long-term secret key can be accumulated. If the long-term secret key is not updated, it can be broken by Eve after about $4n$ attacks.

The third issue is the noise in quantum channel. The 3AQKDP is designed in a noiseless environment. In a noiseless environment, all qubits disturbances are induced by the attacker Eve. However, using current technology, a practical implementation is always in a noisy environment.

4 Our protocol

A new three-party authenticated quantum key distribution protocol, N3AQKDP, is presented in this section. Our protocol N3AQKDP can work in a noisy quantum channel and resist eavesdropping, replay attack, and the online guessing attack. Furthermore, both users can be sure that the session key obtained is consistent if the protocol succeed.

The main idea of our protocol N3AQKDP can be described briefly as follows. The TC encodes the session key into qubits sent to the two users according to the shared secret key with the user. Each user can obtain a binary string by measuring qubits and correct the errors to get the session key. The two users then verify whether their session keys are consistent or not. If their session keys are consistent, it represents that the users are legitimate and the information leaked to Eve is small. Then the users and the TC can evolve their secret keys for next round.

Assume that Alice and Bob are the two users who would like to establish a k-bit session key K_s via the TC. Let U_A and U_B be the identity of Alice and Bob, respectively. The TC shares n-bit secret keys K_{TA} and K_{TB} with Alice and Bob, respectively. They use the bases $\mathcal{R} = \{|0\rangle, |1\rangle\}$ and $\mathcal{D} = \{|+\rangle, |-\rangle\}$ to generate qubits. Some functions used in our protocol N3AQKDP are defined as follows.

- A linear $[n, k, e]$ code $\mathcal{C}_k^n$ to correct e errors is chosen to encode K_s into an n-bit code word C. The value of e will be determined later.
- Let e_K be an encryption algorithm agreed with Alice and Bob using a key K. Let d_K be a corresponding decryption algorithm agreed with Alice and Bob using K. For every plaintext P, $d_K(e_K(P)) = P$.

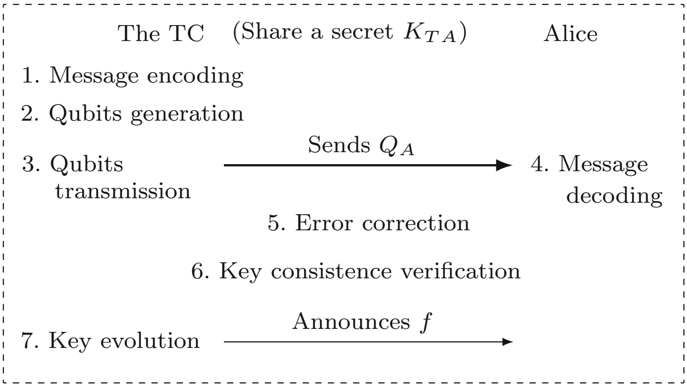

Fig. 2 The steps between Alice and the TC in our protocols

Table 2 Qubit $(q_A)_i$ generation

$(q_A)_i$	$(g_A)_i = 0$	$(g_A)_i = 1$
$(k_{TA})_i = 0$	$\|0\rangle$	$\|1\rangle$
$(k_{TA})_i = 1$	$\|+\rangle$	$\|-\rangle$

In our protocol, we use the uppercase symbols to denote sequences, sets and strings. The lowercase symbols denote values and elements in a set. The lowercase symbol with a subscript i indicates the ith bit of the string. For example, $(k_{TA})_i$ denotes the ith bit of the K_{TA}.

Our protocol can be divided into seven steps: (1) message encoding, (2) qubits generation, (3) qubits transmission, (4) message decoding, (5) error correction, (6) key consistence verification, and (7) key evolution. The steps between the TC and Alice are depicted in Fig. 2. The thick line in step 3 denotes the quantum channel. The thin lines in step 7 indicate the classical public channel.

4.1 Description of N3AQKDP

The detailed steps of our protocol N3AQKDP are described below.

1. (Message encoding) The TC randomly chooses a session key K_s and converts K_s into the code word C using error correction code $\mathcal{C}_k^n$.
2. (Qubits generation) Let $G_A = C \oplus K_{TA}$. The TC creates n qubits, Q_A, for Alice using K_{TA} and G_A. The $(q_A)_i$ denotes the ith qubit of the Q_A. Table 2 lists the states to generate $(q_A)_i$. Let $G_B = C \oplus K_{TB}$. The TC creates Q_B using K_{TB} and G_B for Bob in a similar way.
3. (Qubits transmission) The TC sends Q_A and Q_B to Alice and Bob, respectively.
4. (Message decoding) Alice receives Q_A and measures it according to K_{TA}. If $(k_{TA})_i = 0$, the $(q_A)_i$ is measured in basis $\mathcal{R}$; otherwise $\mathcal{D}$. Bob measures Q_B depending on K_{TB}. Alice gets the outcomes $H_A = (h_A)_1 \ldots (h_A)_n$ and Bob gets

H_B. Let $D_A = H_A \oplus K_{TA}$ be the binary string extracted from the Q_A by Alice. Similarly, Bob gets $D_B = H_B \oplus K_{TB}$ from the Q_B.

5. (Error correction) The TC notices Alice and Bob to correct D_A and D_B using error correction code $\mathcal{C}_k^n$. Alice and Bob get C_A and C_B, respectively. Hence, Alice and Bob can obtain the session key $(K_s)_A$ and $(K_s)_B$, respectively.
6. (Key consistence verification) Alice generate a time stamp, t. She computes $V_1 = e_{(K_s)_A}(U_A \cdot t)$ and sends V_1 to Bob. Here $e_{(K_s)_A}$ is an encryption algorithm using the session key $(K_s)_A$ and '$\cdot$' denotes string concatenation. Bob decrypts V_1 using $(K_s)_B$, obtaining t. Then, Bob computes $V_2 = e_{(K_s)_B}(t+1)$ and sends V_2 to Alice. Alice checks that $d_{(K_s)_A}(V_2) = t + 1$. Here $d_{(K_s)_A}$ is a corresponding decryption algorithm using the session key $(K_s)_A$. If this condition holds, it indicates that $C_A = C_B = C$. They go to step 7. Otherwise, Alice aborts the session.
7. (Key evolution) The TC chooses a hash function f from a class of $\{0, 1\}^{2n} \rightarrow \{0, 1\}^n$ universal hash functions and announces it. The TC and Alice compute

$$K'_{TA} = f(K_{TA} \cdot C_A)$$

as their new secret key. The TC and Bob compute their new secret key

$$K'_{TB} = f(K_{TB} \cdot C_B).$$

Alice verifies her session key with Bob's session key in step 6. The key consistence verification step ensures their session keys are consistent. This step is similar to the verification process in Kerberos-type session key distribution schemes. Since the $(K_s)_A$ and $(K_s)_B$ are used as a session key, this step dose not compromise the security of the session key.

We compare the amounts of qubits and classical bits needed in our protocol with those in 3AQKDP. In our protocol, the TC uses $2n$ qubits to establish a k-bit session key for Alice and Bob. The classical messages are transmitted in step 6 and 7. Alice and Bob use constant bits to verify the session key. The TC needs constant bits to announce hash function f. Our protocol N3AQKDP thus needs constant bits to transmit the session key. The 3AQKDP needs $2n$ qubits and no classical message to establish a k-bit session key. Although our protocol needs a few classical messages, it solves issues of 3AQKDP.

4.2 Session key consistency

We first note that both Alice and Bob obtain a consistent session key if the protocol succeed. If the session keys are found to be inconsistent in step 6, this session is aborted. When Alice and Bob require the TC to establish a session key for them next time, a new session key is generated. Therefore, our protocol do not suffer the replay attack. That is, either they establish a session key or none of them gets the session key in our protocol. The case which one of the communicating parties asks to retransmit a session key cannot occur. It implies that our protocol do not suffer the replay attack.

4.3 Selection of the value of e

The selection of the value of e depends on the noise of environment and the tolerance of the attack. We consider the errors caused by the quantum channel and the attacker in the same way. When the number of errors caused by the environment and Eve is below the threshold value e, Alice and Bob can obtain a consistent session key by error correction. A large e can thus tolerate more disturbances induced by the environment and the attacker Eve. However, for a fixed k, the length of the K_s, it needs more bits to correct more errors. Therefore, a larger n and more qubits are needed to send K_s if we expect the protocol to resist more disturbances.

We can set a proper error threshold e to let our protocol succeed with very high probability. As we described in Sect. 3.2, the probability is 0.25 if Eve attacks one qubit. If Eve attacks all n qubits, the number of errors she makes is $0.25n$ in average. By the Chernoff bound in probability theory, the probability that Eve makes more than $0.25n$ errors decreases exponentially. Hence, we can take $e = 0.25n + \lambda$ to let our protocol succeed with very high probability, here $\lambda > 0$ is a security parameter.

Error correction codes with high correction rates may not be very efficient in decoding. If error correction codes with less correction rates are used for efficient decoding, then the attacker Eve can make our protocol fail with non-negligible probability, and the information she learn can be accumulated. However, we show in Sect. 5 that, in this case, the attacker can learn a very small amount of information in each attack, and she cannot break our protocol with polynomial number of attacks.

We give examples for the selection of the value of e with small correction rates. Suppose that the binary Bose–Chaudhuri–Hocquenhem (BCH) codes of length 255 are used. Assume the error rate caused by the environment is 0.01. If the error rate caused by the adversary is 0.01, the total error rate is 0.02. Then the [255, 207] code to correct 6 errors can be used and $e = \lfloor \frac{n}{255} \times 6 \rfloor$ in our protocol. If the error rate induced by the adversary is 0.04, the total error rate is 0.05, then the [255, 155] code to correct 13 errors can be chosen and $e = \lfloor \frac{n}{255} \times 13 \rfloor$. The session key can be divided into many blocks. For a concrete example, let $n = 255$. The protocols can set $e = 6$ to transmit 207 bits/block of K_s using 255 qubits to endures an overall error rate of 0.02. If the overall error rate is 0.05, let $e = 13$, then 255 qubits can be used to transmit 155 bits/block of K_s.

Suppose the session key is used to encrypt messages by the Advanced Encryption Standard (AES). Table 3 shows the parameters to establish session keys of lengths of 128, 192 and 256 bits in our protocol N3AQKDP. In Table 3, the values of k, n and

Table 3 Parameters to establish session keys

k	r_e	BCH code	t	n	e
128	0.02	[127, 106]	3	154	4
192	0.02	[127, 106]	3	231	6
256	0.02	[255, 207]	6	316	8
128	0.05	[127, 78]	7	209	12
192	0.05	[255, 155]	13	316	17
256	0.05	[255, 155]	13	422	22

e are the length of K_s, the length of code word and the tolerable number of errors, respectively. The r_e denotes the total error rate. The third and fourth columns are the binary BCH codes to correct t errors which are chosen in our protocol N3AQKDP.

5 Security of our protocol

In this section, we analyze the security of our protocol. Our protocol do not reveal any information about the bases and measuring outcomes of the qubits. Hence, the attacker has no information about the transmitted session key. For the secret key shared between TC and user, we consider the following two cases:

1. Our protocol succeeds, or
2. Our protocol fails.

In the first case, the secret key is updated. By the privacy amplification, the secret key can be regarded as a random binary string to the attacker. We show that the security of the BB84 protocol can be reduced to the security of our protocol N3AQKDP. Thus, any attack to our protocol N3AQKDP can be used to attack BB84. The BB84 protocol has been proved to be secure [11], and consequently, our protocol N3AQKDP is secure. Furthermore, our protocol evolves the secret key using key evolution based on the principle of privacy amplification. Renner and König have shown that privacy amplification is universally composable [27]. Hence, key evolution can be done repeatedly.

If the error threshold e has set to a small number, our protocol may fail with a non-negligible probability. In this case, the same secret key will be used in subsequent runs. We assume that our protocol N3AQKDP works in a noiseless environment. Eve thus can apply the online guessing attack. We show that the expected value of Eve's information gain about the secret key before our protocol succeeds is less than 0.6 bits in average. Therefore, she cannot break our protocol. Suppose that Eve attacks many qubits to make the protocol fails with a high probability. Then we show that the information leaks to Eve is negligible. Thus, Eve cannot break our protocol with polynomial number of attacks.

Consider Eve performs the online guessing attack on our protocol in a noise quantum channel. If our protocol fails, she cannot know whether the errors come from her attack or from the noise. Moreover, some errors made by Eve may be corrected by noise, and vice versa. Noise increases the uncertainty of Eve's information gain. This implies that our protocol are more robust against the online guessing attack in a practical environment. This is a strong evidence that our protocol is secure under online guessing attack.

5.1 Case 1: The secret key is evolved

Theorem 1 *Assume that there exists an adversary Eve who can break our protocol N3AQKDP. Then there exists an adversary X who can break the BB84 protocol.*

Before we prove Theorem 1, the BB84 protocol is briefly described as follows.

The BB84 protocol can be described briefly as follows. Alice randomly chooses two $4n$-bit strings a and b. She creates $4n$ qubits using a and b: for qubit i, if $b_i = 0$, she chooses $\mathcal{R}$ as the basis, otherwise $\mathcal{D}$ is the chosen basis. $|0\rangle$ or $|+\rangle$ is created if $a_i = 0$; and $|1\rangle$ or $|-\rangle$ if $a_i = 1$. The $4n$ qubits are sent to Bob. Bob chooses a $4n$-bit string b' randomly and then measures the qubits according to b'. That is, he measures the ith qubit in $\mathcal{R}$ if $b'_i = 0$, otherwise in $\mathcal{D}$. Bob thus gets a $4n$-bit string a' of measuring outcomes. After Bob measured the qubits, Alice announces b and Bob announces b'. For qubit i, they discard a_i and a'_i if $b_i \neq b'_i$. If less than $2n$ bits of a (and a') are left, they abort and restart the protocol. Alice keeps $2n$ bits of a with $b_i = b'_i$ and Bob keeps the corresponding bits of a'. Let the $2n$ bits of a and a' be α and α', respectively. Alice randomly picks n bits from the α. Let T_1 denote the n picked bits. Alice tells Bob which bits she picked. Let T_2 denote the corresponding n bits of α'. They announce T_1 and T_2 and counts the number of errors of corresponding bits between T_1 and T_2. They aborts and restarts the protocol if the number of errors is more than the threshold of acceptance, otherwise each of them has n bits remained which are used as the sifted key. They employ the procedure of information reconciliation to reconcile their sifted keys and the procedure of privacy amplification to obtain a m-bit final secret key from the n-bit sifted key.

Let X be an adversary of the BB84 protocol. If X could break the BB84 protocol, he had to let the protocol succeed and get more information than Bob. Hence, X's information gain on the final key was not negligible after the privacy amplification. Definition 1 gives the definition of breaking the BB84 protocol.

Definition 1 Let the mutual information obtained by Bob and X from Alice on sifted key in the BB84 protocol be $I(A; B)$ and $I(A; X)$, respectively. The quantum bit error rate created by X is D. X breaks the BB84 protocol if $I(A; X) \geq I(A; B)$ and $D \leq 11\,\%$ [11,28].

Let Eve be an adversary of our protocol N3AQKDP. If Eve could break our protocol N3AQKDP, the protocol succeeded and she got enough information about the secret key and the code word that would not be completely eliminated after the key evolution. We note that both lengths of the secret key and the code word are n bits. In order to update the secret key, a key evolution procedure is performed in our protocol. Without loss of generality, assume that Eve attacks our protocol N3AQKDP running between the TC and Alice. Let l denote Eve's total information gain on the secret key K_{TA} and the code word C_A. Recall that the universal hash function f is chosen from $\{0, 1\}^{2n} \rightarrow \{0, 1\}^n$. By the theorem of the privacy amplification [23], the security parameter $s = n - l > 0$. Hence, the new key $K'_{TA} = f(K_{TA} \cdot C_A)$ is secure if $l < n$. Definition 2 gives the definition of breaking our protocol N3AQKDP.

Definition 2 Assume that Eve attacks the qubits Q_A sent from the TC to the user A. Eve breaks our protocol N3AQKDP if she creates less than e errors in the Q_A and gets at least n bits of information about the secret key K_{TA} and the code word C_A.

Theorem 1 is proved as follows.

Proof We first show that an instance of the BB84 protocol has a corresponding instance of our protocol as follows. Assume that Alice and Bob run the BB84 protocol to have

n qubits which Bob measures using the same bases that Alice creates the qubits. Let $\alpha = \alpha_1 \ldots \alpha_n$ and $\beta = \beta_1 \ldots \beta_n$ denote the values and the bases to create the qubits, respectively, here each $\alpha_i, \beta_i \in \{0, 1\}$. They picks $n/2$ qubits from the n qubits to test the quantum channel. Let the set of these $n/2$ picked qubits be $\mathcal{T}$. The outcomes of remaining $n/2$ qubits arranged in order are used as the sifted key (or called the raw key) K_r. Hence, $(\alpha, \beta, \mathcal{T}, K_r)$ can represent an instance of the BB84 protocol.

An instance of our protocol can be described as $(G_A, K_{TA}, \mathcal{T}_A, \mathcal{C}_k^n, K_s)$ for the TC and the user A. Here $\mathcal{T}_A$ is the set of qubits that be chosen to verify whether the session key is consistent or not. The TC uses α as the G_A in our protocol N3AQKDP. Let $K_{TA} = \beta$, i.e., the TC and the user A share a secret key β. Hence, the n qubits created in our protocol are the same as those in the BB84 protocol and $C_A = G_A \oplus K_{TA} = \alpha \oplus \beta$. The TC uses Q_A as the $\mathcal{T}_A$. The K_s can be converted from the value of C_A by using $\mathcal{C}_k^n$. Therefore, an instance $(\alpha, \beta, \mathcal{T}, K_r)$ of the BB84 protocol can be transferred to an instance $(G_A, K_{TA}, \mathcal{T}_A, \mathcal{C}_k^n, K_s)$ of our protocol N3AQKDP.

Assume that Eve has no information about the K_{TA} at the beginning. Let B_1 be the given instance of the BB84 protocol. Let N_1 be an instance of our protocol N3AQKDP. We now show that if Eve can break N_1, then we can construct X that can break B_1. The proof is as follows.

Suppose that X would like to break B_1. By the definition 1 and $I(A; X)+I(A; B) = 1$ described in Ref. [29], $I(A; X) \geq 0.5$ if X breaks B_1. That is, X has to get at least $(0.5 \times n/2)$ bits of information about the sifted key K_r and only induce the quantum bit error rate $D \leq 0.11$ in the qubits of $\mathcal{T}$. X can first transfer B_1 to N_1 as we described above. And then X chooses $e \leq 0.11n$ and calls Eve to break N_1. Therefore, Eve induces less than e errors in $\mathcal{T}_A = Q_A$ and learns at least n bits of information about K_{TA} and C_A. The following shows that if Eve can get at least n bits of information about K_{TA} and C_A in N_1, then X can get at least $(0.5 \times n/2)$ bits of information about the K_r in B_1. Thus, X breaks B_1.

We consider the information obtained by Eve in Q_A. Since neither the bases nor the values of Q_A is revealed, Eve can only manipulate the qubits to get information. She thus gets no information about the bases of Q_A, i.e., the values of K_{TA}. Hwang et al. [30] have shown the fact if Eve attacks the qubits individually. We argue that it is also correct even if Eve performs coherent attacks as follows. It cannot obtain more information to attach probes on the qubits because no information is revealed later. Eve can only measure the qubits to get information. Since the bases are chosen randomly, there is no correlation between them. The best measuring method to get the information about the bases is to measure each qubit individually. Therefore, Eve learns no information about the bases of Q_A, i.e., the values of K_{TA}, even if she performs coherent attacks.

We have shown that Eve gets no information on K_{TA}. Since Eve learns at least n bits of information about K_{TA} and C_A, she obtains at least n bits of information about the C_A. For X, the information about C_A in N_1 corresponds to the information about K_r in B_1. Therefore, X induces less than $D = e/v \leq 0.11$ error rate on $\mathcal{T}$ and gets at least $n > (0.5 \times n/2)$ bits of information about the sifted key K_r. X thus breaks B_1. □

5.2 Case 2: The secret key cannot be evolved

When Eve attacks our protocol by the online guessing attack, she can attack some qubits and observes whether the protocol aborts or not. Eve has to attack more than e qubits to make our protocols abort, because the code word C with no more than e errors can be corrected by error correction code. When Eve attacks many qubits, we can show that Eve's information gained is negligible. Hence, error correction codes in our protocols not only overcome the noise but also play an important role to resist the online guessing attack.

We now show that the expected value of Eve's information gain about the secret key is less than 0.6 bits in average before the secret key is evolved in our protocol N3AQKDP. Assume that Eve attacks α qubits when the TC sends Q_A to Alice. Let E_α be the event that Eve attacks α qubits in an attack. We define the notations as follows.

- Let $I(\alpha)$ be Eve's information gain in an attack if E_α occurs and our protocol N3AQKDP is aborted.
- Let $P(\alpha)$ be the probability that Eve makes our protocol N3AQKDP aborted when Eve attacks α qubits in an attack.
- Let $P_{KE}(\alpha)$ be the probability of performing key evolution when Eve attacks α qubits in an attack.
- Let $E(I_1^\alpha)$ be the expected value of Eve's information gain obtained in an attack of α qubits.
- Let $E(I^\alpha)$ be the expected value of Eve's information gain before our protocol N3AQKDP succeeds if Eve attacks α qubits.

Note that $P_{KE}(\alpha) = 1 - P(\alpha)$.

We derive $I(\alpha)$ as follows. Since Eve attacks α qubits, there are 2^α possible bases for these α qubits. If our protocol N3AQKDP aborts, it means that some of the basis of these α qubits were incorrect. For these α qubits, it needs at least $2^\alpha - 1$ trials to confirm the bases. Thus, the amount of information $I(\alpha)$ obtained by Eve can be computed as follows.

$$I(\alpha) = \frac{\alpha}{2^\alpha - 1}, \text{ for } \alpha \geq 1. \tag{1}$$

The value of $I(\alpha)$ decreases exponentially as the value of α increases.

The probability $P(\alpha)$ can be computed by

$$P(\alpha) = \frac{1}{2^\alpha}\left(\sum_{i=1}^{\alpha}\binom{\alpha}{i} \times \left(1 - \frac{1}{2^i}\right)\right). \tag{2}$$

Here i denotes the number of qubits that Eve measures in a wrong basis. In Eq. (2), $\binom{\alpha}{i}$ is the number of possible cases for i qubits chosen from α qubits, and $\left(1 - \frac{1}{2^i}\right)$ is the probability of making our protocol N3AQKDP aborted. We note that the probability of success of our protocol N3AQKDP is $1/2^i$ even if Eve measures these i qubits with wrong basis.

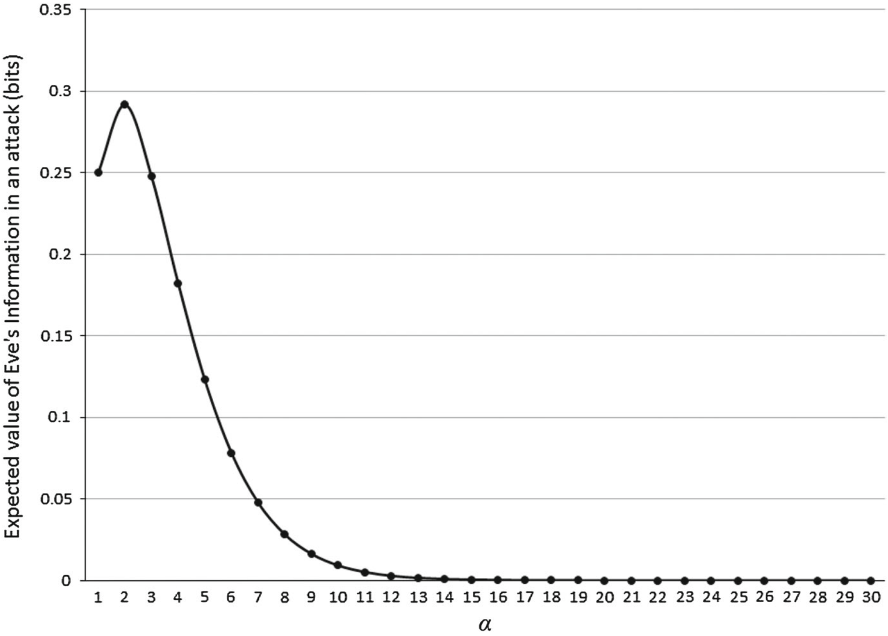

Fig. 3 The values of $E(I_1^\alpha)$ versus the values of α

Since

$$P_{KE}(\alpha) = 1 - P(\alpha). \tag{3}$$

We can obtain

$$P_{KE}(\alpha) \geq \left(\frac{3}{4}\right)^{\alpha}. \tag{4}$$

By Eq. (4), our protocol N3AQKDP has a high probability to evolve the secret key if α is small. On the other hand, if α is large, Eve's information is exponentially small. We show the fact as follows.

When Eve attacks α qubits in an attack, the expected value of information gain, $E(I_1^\alpha)$, is as follows.

$$\begin{aligned} E(I_1^\alpha) &= P(\alpha) \times I(\alpha) \\ &= \frac{1}{2^\alpha}\left(\sum_{i=1}^{\alpha}\binom{\alpha}{i} \times \left(1 - \frac{1}{2^i}\right)\right) \times \frac{\alpha}{2^\alpha - 1}. \end{aligned} \tag{5}$$

The values of $E(I_1^\alpha)$ versus the values of α are plotted in Fig. 3. The value of $E(I_1^\alpha)$ decreases exponentially as the value of α increases, for $\alpha \geq 2$. Thus, when Eve attacks many qubits in an attack, the expected value of information gain is negligible.

Table 4 Some examples of the values of $P_{KE}(\alpha)$, $E(I_1^\alpha)$ and $E(I^\alpha)$

α	$P_{KE}(\alpha)$	$E(I_1^\alpha)$	$E(I^\alpha)$
1	0.7500	0.2500	0.3333
2	0.5625	0.2917	0.5185
3	0.4219	0.2478	0.5873
4	0.3164	0.1823	0.5761
5	0.2373	0.1230	0.5184
6	0.1780	0.0783	0.4399
7	0.1335	0.0478	0.3578
8	0.1001	0.0282	0.2820
9	0.0751	0.0163	0.2170
10	0.0563	0.0092	0.1638
15	0.0134	0.0005	0.0338
20	0.0032	0.0000	0.0060
25	0.0008	0.0000	0.0010
30	0.0002	0.0000	0.0002

On the other hand, if $\alpha = 2$, Eve can obtain maximum expected value of information, which is less than 0.3 qubits. In this case, $P(\alpha = 2) = 0.4375$. Thus, our protocol N3AQKDP succeeds and the secret key is updated within 16 attacks with probability of $(1 - (1 - 0.4375)^{16}) = 0.9999$. Table 4 shows some examples to illustrate the values of $P_{KE}(\alpha)$ and $E(I_1^\alpha)$.

Consider that Eve attacks α qubits in a row. Before our protocol N3AQKDP succeeds, the expected value of Eve's information gain, $E(I^\alpha)$, can be computed as follows.

$$\begin{aligned} E(I^\alpha) &= (1 + P(\alpha) + (P(\alpha))^2 + \cdots) \times E(I_1^\alpha) \\ &= \frac{1}{1 - P(\alpha)} \times E(I_1^\alpha) \\ &= \frac{1}{P_{KE}(\alpha)} \times E(I_1^\alpha) \\ &= \left(\frac{4}{3}\right)^\alpha \times E(I_1^\alpha). \end{aligned} \tag{6}$$

The values of $E(I^\alpha)$ versus the values of α are plotted in Fig. 4. The maximum expected value of Eve's information before our protocol N3AQKDP succeeds is 0.5873 bits when $\alpha = 3$. This concludes that Eve's information about the secret key is very little before the secret key is updated.

Now, we show that the probability that Eve can break the secret key is exponentially small. By Eq. (1), $I(\beta) \leq 1$. That is, Eve can obtain at most 1 bit of information in an attack. In order to break the secret key, she has to abort our protocol N3AQKDP in succession at least n times. Since $P(\alpha) < 1$, the probability that Eve can break the secret key is $(P(\alpha))^n$. It is exponentially small if n is sufficiently large. This implies that the probability of breaking our protocol N3AQKDP by using online guessing

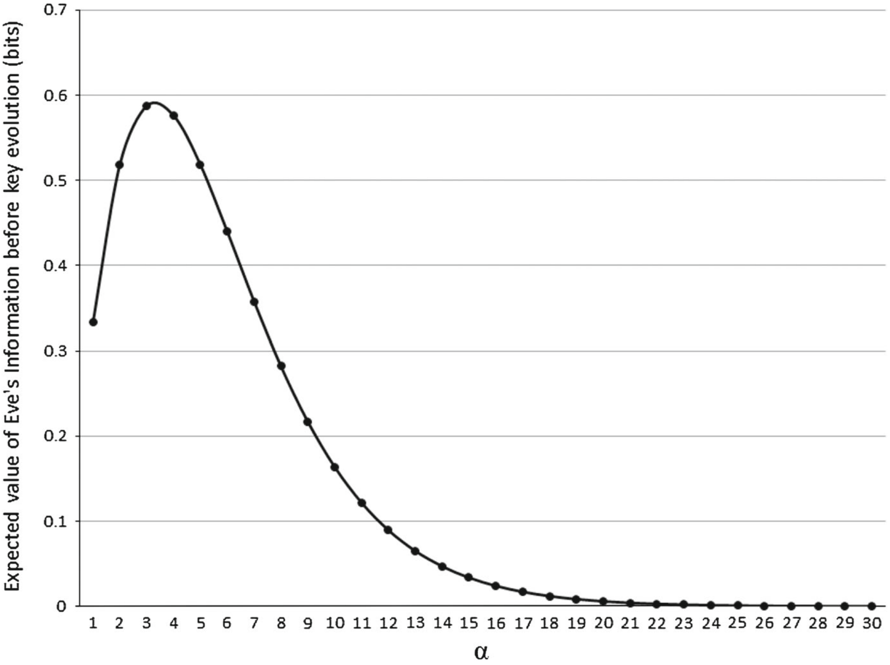

Fig. 4 The values of $E(I^{\alpha})$ versus the values of α

attack is negligible. In other words, our protocol N3AQKDP can resists the online guessing attack.

6 Conclusions and discussions

In this work, we present a practical protocol, N3AQKDP, to improve a three-party authenticated quantum key distribution protocol 3AQKDP proposed by Hwang et al. Our protocol can work in a noisy quantum channel.

The proposed protocol resolve some issues that the authors of 3AQKDP have not addressed, including the session key consistence, the online guessing attack, and the noise in quantum channel. We resolve these issues by using error correction codes and key evolution.

The security of our protocol N3AQKDP is proved by standard reduction to the BB84 protocol. Since the long-term secret key are evolved after each successful run and the message transmitted are unknown to the attacker, the new secret key can be regarded as a random number to the attacker. Therefore, our security proof implies that any attack to our protocol N3AQKDP can be used to attack the BB84 protocol. Since the BB84 protocol is proved to be secure, our proposed protocols are secure.

Our protocols assume that the user shares a secret key with the TC for identity authentication, and the session key distributed to the users is chosen by the TC. The TC knows all secret information in our protocols. Hence, our protocols require the center to be trusted. It is an interesting research topic to design an authenticated quantum key distribution protocols under the help of semi-honest TC.

Acknowledgments The authors would like to thank the anonymous reviewers for their valuable comments and suggestions to improve the quality of the paper. This work was supported in part by the National Science Council, Taiwan, under Contract NSC100-2219-E-110-004, NSC101-2219-E-110-004, and NSC102-2219-E-110-003.

References

1. Bennett, C.H.: Quantum cryptography using any two nonorthogonal states. Phys. Rev. Lett. **68**(21), 3121 (1992)
2. Bennett, C.H., Bessette, F., Brassard, G., Salvail, L., Smolin, J.: Experimental quantum cryptography. J. Cryptol. **5**(1), 3 (1992)
3. Bennett, C.H., Brassard, G.: Quantum cryptography: Public key distribution and coin tossing. In: Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, p. 175 (1984)
4. Ekert, A.K.: Quantum cryptography based on Bell's theorem. Phys. Rev. Lett. **67**(6), 661 (1991)
5. Biham, E., Boyer, M., Boykin, P.O., Mor, T., Roychowdhury, V.: A proof of the security of quantum key distribution. J. Cryptol. **19**(4), 318 (2006)
6. Biham, E., Boyer, M., Brassard, G., van de Graaf, J., Mor, T.: Security of quantum key distribution against all collective attacks. Algorithmica **34**(4), 372 (2002)
7. Biham, E., Mor, T.: Security of quantum cryptography against collective attacks. Phys. Rev. Lett. **78**(11), 2256 (1996)
8. Biham, E., Mor, T.: Bounds on information and the security of quantum cryptography. Phys. Rev. Lett. **79**(20), 4034 (1997)
9. Inamori, H., Lütkenhaus, N., Mayers, D.: Unconditional security of practical quantum key distribution. Eur. Phys. J. D Atom. Mol. Opt. Plasma Phys. **41**(3), 599 (2007)
10. Lo, H.K., Chau, H.F.: Unconditional security of quantum key distribution over arbitrarily long distances. Science **283**(5410), 2050 (1999). http://www.arxiv.org/abs/quant-ph/9803006
11. Mayers, D.: Unconditional security in quantum cryptography. J. ACM **48**(3), 351 (2001)
12. Shor, P.W., Preskill, J.: Simple proof of security of BB84 quantum key distribution protocol. Phys. Rev. Lett. **85**, 441 (2000). http://www.arxiv.org/abs/quant-ph/0003004
13. Wegman, M.N., Carter, J.L.: New hash functions and their use in authentication and set equality. J. Comput. Syst. Sci. **22**, 265 (1981)
14. Hwang, T., Lee, K.C., Li, C.M.: Provably secure three-party authenticated quantum key distribution protocols. IEEE Trans. Dependable Secure Comput. **4**(1), 71 (2007)
15. Colbeck, R.: The impossibility of secure two-party classical computation. Phys. Rev. A **76**(6), 062308 (2007)
16. Lo, H.K.: Insecurity of quantum secure computations. Phys. Rev. A **56**(2), 1154 (1997)
17. Salvail, L., Schaffner, C., Sotakova, M.: On the power of two-party quantum cryptography. In: Advances in Cryptology: Proceedings of Asiacrypt 2009, pp. 70–87. Springer, Berlin (2009)
18. Canetti, R., Goldreich, O., Halevi, S.: On the random-oracle methodology as applied to length-restricted signature schemes. In: Proceedings of the 1st Theory of Cryptography Conference (TCC'04), pp. 40–57. Springer, Berlin (2004)
19. Canetti, R., Goldreich, O., Halevi, S.: The random oracle methodology, revisited. J. ACM **51**(4), 557 (2004)
20. Guan, D.J., Wang, Y.J., Zhuang, E.S.: Quantum key evolution and its applications. Int. J. Quantum Inf. **10**(4), 1250044 (2012); 16 pp
21. Calderbank, A.R., Shor, P.W.: Good quantum error-correcting codes exist. Phys. Rev. A **54**, 1098 (1996). http://www.arxiv.org/abs/quant-ph/9512032
22. Steane, A.M.: Error correcting codes in quantum theory. Phys. Rev. Lett. **77**, 793 (1996)
23. Bennett, C.H., Brassard, G., Robert, J.M.: Privacy amplification by public discussion. SIAM J. Comput. **17**(2), 210 (1988)

24. Bennett, C.H., Brassard, G., Crépeau, C., Maurer, U.M.: Generalized privacy amplification. IEEE T. Inform. Theory **41**(6), 1915 (1995)
25. Schwinger, J.: Unitary operator bases. Proc. Natl. Acad. Sci. USA **46**(4), 570 (1960)
26. Carter, J.L., Wegman, M.N.: Universal classes of hash functions. J. Comput. Syst. Sci. **18**(2), 143 (1979)
27. Renner, R., König, R.: Universally composable privacy amplification against quantum adversaries. In: Kilian, J. (ed.) Theory of Cryptography. Lecture Notes in Computer Science, vol. 3378, pp. 407–425. Springer, Berlin (2005)
28. Gisin, N., Ribordy, G., Tittel, W., Zbinden, H.: Quantum cryptography. Rev. Mod. Phys. **74**(1), 145 (2002)
29. Hwang, W.Y., Ahn, D.D., Hwang, S.W.: Eavesdropper's optimal information in variations of Bennett-Brassard 1984 quantum key distribution in the coherent attacks. Phys. Lett. A **279**(3–4), 133 (2001)
30. Hwang, W.Y., Koh, I.G., Han, Y.D.: Quantum cryptography without public announcement of bases. Phys. Lett. A **244**(6), 489 (1998)