A Diffie-Hellman quantum session key establishment protocol without entanglement

Yalin Chen[1] and Chang Hsiang[2] and Liang-Chun Wang[3] and Yu-Yuan Chou[4] and Jue-Sam Chou[*5]

[1]Institute of information systems and applications, National Tsing Hua University
Yalin78900@gmail.com

[2,5] Department of Information Management, Nanhua University, Taiwan

*: corresponding author: jschou@nhu.edu.tw [1], jschou@mail.nhu.edu.tw[2]

Tel: 886+ (0)5+272-1001 ext.56536

[3]Department of Electrical Engineering, National Sun Yat-sen University , Taiwan
b053011015@student.nsysu.edu.tw

[4] The Affiliated Zhongli Senior High School of National Central University
amy53750@yahoo.com.tw

Abstract

In 2016 and 2017, Shi et al first proposed two protocols for the communication parties to establish a quantum session key. Both work by rotating the angle of one communicator's private key on the other party's quantum public key. In their approaches, the session key shared by each pair of communicators is fixed after the key generation phase. Thereafter, the key used in each communication does not change, but for security consideration, the session key should be changed in every time usage. In other words, those key agreement protocols do not satisfy the requirement of key security. In view of this, this paper develops a quantum session key establishment based on the Diffie-Hermann style key exchange to produce different quantum session keys in each communications. After analysis, we confirm that our method can resist various attacks and is therefore secure.

Keywords: Diffie-Hellman key agreement, session key, quantum asymmetric cryptography, man-in-the-middle attack

1.Introduction

In 2016 to 2017, Shi et al. proposed a series of quantum deniable identity authentication agreements [1-3], claiming that their agreements not only are unnecessary with a trusted third party, but also exempt both parties from communicating in the key generation phase. And can be applied to the electronic voting system. However, after looking at the agreements they proposed, the keys used by both communicating parties are fixed in the entire communication process after generation, this can lead to the risk that reduces the security level of the session key, because malicious attackers may take advantage of them to launch illegal actions.

In view of this, this study generates a quantum session key by referring to the traditional Diffie-Hellman key exchange method, to produce different keys whenever communicating parties need to change the session key. It is well known that Diffie-Hellman key exchange method generates a session key by using both the public key of the other party and its own secret. However, it can be attacked by a man-in-the-middle attack due to the lack of identity verification. In order to improve the security, we let the communicators generate the quantum session key by rotating the angles of both his quantum private key and a chosen random number on the quantum public key of the other party. In addition, our protocol embeds an identity verification process, to authenticate the other party's identity.

In summary, there are two purposes of this study. First, proposing a key generation agreement that is secure and can generate different session keys whenever needed. Secondly, proposing a session key agreement with an identity verification function to avoid the man-in-the-middle attack. In other words, our key generation protocol has a secure identity verification and thus can resist man-in-the-middle attacks.

The structure of this paper is organized as follows: In Section 2.1, we introduce the Diffie-Hellman key generation method, and introduce its man-in-the-middle attack problem in Section 2.2. In Section 2.3, we introduce Shi et al.s' three deniable quantum authentication protocols proposed in 2016 through 2017. Section 2.4 briefly introduces the cryptographic one-way hash function used in this study. In Section 3, we use the Diffie-Herman key exchange method to establish the quantum session key for the communicating parties. Section 4 proves why our protocol is secure. Section 5 discusses and compares this research with the state-of-the-art. Finally, a conclusion is given in Section 6.

2. Literature review

This section introduces the Diffie-Hellman key exchange method in Section 2.1, and explains why a malicious attatcker can launch the man-in-the-middle attack toward this method in Section 2.2. In Section 2.3, we review the session key generation agreements proposed by shi et al., and introduce the properties of one-way function in Section 2.4. Before that, we first introduce the used notations and their definitions, as listed in Table 1.

Table 1. The definitions of used notations

g	a generator in the field of mod p.
p	a large prime number which is the modulus of a finite field generated by g
$(S_j\theta_n)_i$	the first and second part of member i_s' private key
D_i	member i_s' private key, which equals $(S_j\theta_n)$ i
z	the canonical measurement basis $\{\|0\rangle, \|1\rangle\}$ in the Hilbert space

2.1. Diffie-Hellman Key exchange method

The Diffie-Hellman key generation protocol is based on the hard problem of solving discrete logarithms. In the public parameters, we assume that the modulus is p and the generator g. The operations are as follows.

Assume that the two communication parties are A and B. They select their own secret random numbers a and b as private keys, calculate $m = g^a \mod p$, $n = g^b \mod p$, and use them as their own public keys, respectively. A and B then send them to the other party. After that, they calculate $n^a \mod p$ and $m^b \mod p$, separately. Both will obtain the same result $W = g^{ab} \mod p$, which is then used as the session key for their communication, as shown in Figure 1. In the figure, it is assumed that the system parameters p and g are 19 and 7, and the private keys of A and B are a = 8 and b = 7, respectively. Accordingly, the session key generated is 11.

A selects a=8	B selects b=7
(1) A computes $7^8 mod\ 19 = 11$ —Sends 11→	B computes $11^7 mod\ 19 = 11$
(2) A computes $7^8 mod\ 19 = 11$ ←Sends 7—	B computes $7^7 mod\ 19 = 7$
A and B both get the session key 11	

Figure 1. Diffie-Hellman key agreement

2.2. The defect of Diffie-Hellman Key exchange method

With the current limitations of computer technology, there is no efficient way to solve the discrete logarithm problem, which thus ensures the security of the Diffie-Hellman key exchange protocol. However, the Diffie-Hellman key exchange method does not have identity verification, which makes it encounter the man-in-the-middle attack. We describe it as follows:

Assuming that attacker E launches a man-in-the-middle attack on the key exchange process for pretending A to B, and B to A, respectively. E will be able to disguise as A to B and vice versa, as shown in Fig. 2 and 3, separately. In the figures, we assume that the secrets of the communication parties A, B and attacker E are *a*, *b* and *e*, respectively.

Attacker E counterfeits, B to communicate with A		
A		E
	m(A send m to B)	
$(1) g^a mod\ p = m$	⟶	$(2) m^e mod\ p = g^{ea} mod\ p = K_{AE}$
	Intercepted by E	
$(4) o^a mod\ p = g^{ea} mod\ p = K_{AE}$	E send o to A ⟵	$(3) g^e\ mod\ p = o$
E and A share the common session key K_{AE}.		

Figure 2. E pretends B to communicate with A

Attacker E counterfeits A to communicate with B		
E		B
$(2) n^e mod\ p = K_{EB}$	⟵ (B send n to A)	$(1) g^b\ mod\ p = n$
	Intercepted by E	
$(3) g^e\ mod\ p = o$	⟶ E send o to AB	$(4) o^b mod\ p = K_{EB}$
Common session key of E and B K_{EB} ◦		

Figure 3. E pretends A to communicate with B

2.3.Review the schemes proposed by Shi et al.

Shi et al. proposed three deniable quantum signature schemes in 2016 through 2017 [1-3]. The following sections, Section 2.3.1 through 2.3.3, will briefly introduce the

key generation of these deniable quantum signature schemes. In Section 2.4, we will briefly introduce the properties of the cryptographic one-way hash function, which is used in our design.

2.3.1. An efficient quantum deniable authentication protocol without a trusted center [1]

In this scheme, Alice generates *n* EPR pairs and sends the second particles of all pairs to Bob, leaving the first particle of each EPR pair to form Alice's quantum state $|A\rangle = \{|A_1\rangle, |A_2\rangle \ldots |A_n\rangle\}$ and Bob has quantum state $|B\rangle = \{|B_1\rangle, |B_2\rangle \ldots |B_n\rangle\}$. Alice and Bob then generate random number strings r_A、$r_B \in \{0,1\}^{2n}$. According to their own random numbers r_A、r_B and their own quantum states $|A\rangle$ and $|B\rangle$, they perform unitary operations on the particle states and get $|K_A\rangle = \otimes_{i=1}^{n} \delta_{r_A^{2i-1} r_A^{2i}} |A_i\rangle$、$|K_B\rangle = \otimes_{i=1}^{n} \delta_{r_B^{2i-1} r_B^{2i}} |B_i\rangle$, under the definition that $\delta_{00}=I$、$\delta_{01}=\sigma_x$、$\delta_{10}= i\sigma_y$、$\delta_{11}=\sigma_z$. Then, Alice and Bob will send their $|K_A\rangle$ and $|K_B\rangle$ to each other through the quantum channel. After this, they convert the states $|K_B\rangle$、$|K_A\rangle$ according to their own r_{A} and r_{B} values in the way that $|K_{AB}\rangle = \otimes_{i=1}^{n} \delta_{r_A^{2i-1} r_A^{2i}} |K_B{}^i\rangle$ and $|K_{BA}\rangle = \otimes_{i=1}^{n} \delta_{r_B^{2i-1} r_B^{2i}} |K_A{}^i\rangle$.

That is, Alice uses r_A to perform unitary operations on $|K_B\rangle$, Bob uses r_B to perform unitary operations on $|K_A\rangle$, and obtains $|K_{AB}\rangle$ and $|K_{BA}\rangle$, respectively. After this, Alice and Bob use the same basis $Z = \{|0\rangle, |1\rangle\}$ for the measurements of $|K_{AB}\rangle$ and $|K_{BA}\rangle$. The measurement result will be the same session key *K*. In the scheme, Alice must generate an additional authentication signature $|S\rangle$ on message *M* and a time stamp *T*, and send $\{|S\rangle, M, T\}$ to Bob, so that Bob can confirm the identity of the signer Alice, and vice versa. Here, we only show the session key generated is fixed. The details can be referred to literature [1]. For simplicity, we omit it here.

2.3.2. A non-interactive quantum deniable authentication protocol [2]

In this scheme, the system generates the communication parties' , Alice and Bob, private keys (d_A、d_B) and public keys ($|\psi_{pkA}\rangle, |\psi_{pkB}\rangle$). Alice and Bob then each performs a rotation operation by the angle of his own private key on the other party's public key. As a result, they obtain $|K_{AB}\rangle$、$|K_{BA}\rangle$, respectively. Then, each transfers the traditional message *M* into a *n*-qubit long quantum state $|Q\rangle$. After generating the message authentication code *MAC* by compressing $|Q\rangle$ and $|K_{AB}\rangle$ through the quantum one-way hash function [4], Alice generates a time stamp *T*, and sends $\{M, MAC, T\}$ to Bob for signature confirmation and identity verification, as shown in Figure 4. The details can be referred to literature [2]. For simplicity, we omit it here.

Alice	Bob
Private key $d_A = \{s_A, n_A\}$ Public key $\|\psi_{pkA}\rangle = \otimes_{j=1}^{n} \hat{R}^{(j)}(s_j^A \theta_{nA})\|0_z\rangle$	Private key $d_B = \{s_B, n_B\}$ Public key $\|\psi_{pkB}\rangle = \otimes_{j=1}^{n} \hat{R}^{(j)}(s_j^B \theta_{nB})\|0_z\rangle$
Rotate $\|\psi_{pkB}\rangle$ by its own private key $s_j^A \theta_{nA}$. $\|K_{AB}\rangle = \otimes_{j=1}^{n} \hat{R}^{(j)}(s_j^A \theta_{nA})\|\psi_{pkB}\rangle$ transfers message *M* to *n*-qubit long quantum state Q:$\|Q\rangle = \{\|q_1\rangle, \|q_2\rangle, \|q_3\rangle, \dots, \|q_n\rangle\}$ Generate time stamp *T* Generate message authorization code: $MAC = \|f(Q\|K_{AB})\rangle$ where $f: \|Q\rangle \rightarrow \|f(Q)\rangle$ means quantum one-way hash function Transfer $\{M, MAC, T\}$ →	
	Rotate $\|\psi_{pkA}\rangle$ by its own private key $s_j^B \theta_{nB}$ $\|K_{BA}\rangle = \otimes_{j=1}^{n} \hat{R}^{(j)}(s_j^B \theta_{nB})\|\psi_{pkA}\rangle$ transfer message *M* to *n*-qubit long quantum state $\|Q\rangle = \{\|q_1\rangle, \|q_2\rangle, \|q_3\rangle, \dots, \|q_n\rangle\}$ And compute whether: $MAC' = MAC = \|f(Q\|\|K_{BA})\rangle$

Figure 4. A non-interactive quantum deny signature based on asymmetric cryptosystem

2.3.3. A restricted quantum deniable authentication protocol applied in an electronic voting system [3]

The identity verification and key exchange methods used in this scheme is the same as stated in Section 2.3.2. The meaning of restricted is that the person who takes part in the communication is traceable, but the digital signature is still deniable. In order to trace signatures, the signer has to generate two quantum states $U^{1,2}$ for identification purpose in the authorization phase. In that, U^1 is used as the input of the quantum one-way hash function to generate the *MAC*, and the time stamp in Section 2.3.2 is replaced with U^2, and both are sent to Bob to compute the MAC' for confirming the identity. However, the MAC' generated by Bob is the same as the *MAC* of Alice.

In other words, Bob can generate the same *MAC* as Alice. Therefore this scheme is deniable, as shown in Figure 5. The details can be referred to literature [3]. We omit it here.

Alice	Bob
Private key $d_A = \{s_A, n_A\}$ Public key $\|\psi_{pkA}\rangle = \otimes_{j=1}^{n} \hat{R}^{(j)}(s_j^A \theta_{nA})\|0_z\rangle$ Rotate $\|\psi_{pkB}\rangle$ by private key $s_j^A \theta_{nA}$ $\|K_{AB}\rangle = \otimes_{j=1}^{n} \hat{R}^{(j)}(s_j^A \theta_{nA})\|\psi_{pkB}\rangle$ Generate two quantum states: $U^{1,2} = \otimes_{j=1}^{n} \hat{R}^{(j)}(s_j^A \theta_{nA})\|0_z\rangle$ transfer message M to n-qubit long quantum state $\|Q\rangle$: $\|Q\rangle = \{\|q_1\rangle, \|q_2\rangle, \|q_3\rangle, \dots, \|q_n\rangle\}$ Generate message authorization code: MAC $= \|f(Q\|K_{AB}\|U^1)\rangle$ Where $f: \|Q\rangle \to \|f(Q)\rangle$ means quantum one-way hash function	Private key $d_B = \{s_B, n_B\}$ Public key $\|\psi_{pkB}\rangle = \otimes_{j=1}^{n} \hat{R}^{(j)}(s_j^B \theta_{nB})\|0_z\rangle$
$\{\|U^2\rangle, MAC, M\}$ →	Rotate $\|\psi_{pkA}\rangle$ by $s_j^B \theta_{nB}$ $\|K_{BA}\rangle = \otimes_{j=1}^{n} \hat{R}^{(j)}(s_j^B \theta_{nB})\|\psi_{pkA}\rangle$ transfer message M to n-qubit long quantum state$\|Q\rangle$ $\|Q\rangle = \{\|q_1\rangle, \|q_2\rangle, \|q_3\rangle, \dots, \|q_n\rangle\}$ And compute whether: MAC$' = MAC = \|f(Q\|K_{BA}\|U^2)\rangle$

Figure 5. Restricted Quantum Denied Signature Agreement applied to the electronic voting system

2.4. One-way function

The property of one-way function is that if a random value is given, it is easy to compute the function value; but if a function value is given, it is difficult to find the ramdom value. More formally, assum that a random value x is given, after the computation of hash function, the generated hash value y must satisfy the following: (1) it is difficult to trace back to the initial value, that is, when given y, it is impossible to know x, (2) slightly modify the ramdom value to x', the function value is greatly changed. That is, it has the avalanche effect; for example, if $|x - x'| < \varepsilon$, then $|f(x') - y| \gg \zeta$, where ε is a small number, and ζ is a large number, (3) no hash

collision will occur. That is if $f(x_1) = y = f(x_2)$, to find such x_1, x_2 is computationally impossible, (4) it is easy to calculate from the ramdom value to the function value. Equivalently, this means given *x*, it is easy to compute *y*.

3. Our scheme

After reveiwing sections 2.3.1 through 2.3.3, we found that the session keys generated by the schemes are fixed. All of them use the angle of their own private key to rotate on the other party's public key. As a result, it will reduce the session keys' security. In light of this, we propose a session key generation scheme, which can generate a different session key each time when required. Our scheme contains five phases: (0) public and private key generation phase, (1) Identity code generation phase, (2) parameters generation for the session key, (3) identity verification phase, (4) session key generation phase, as shown in Figure 6, and introduced as follows:

Phase 0: Public and private key generation phase

In this phase, the system generates each member's public key and private key. For example, it lets member Alice select $D_A = S_j\theta_n$ as her private key angle, and rotates angle D_A on $|0_Z\rangle$, to obtain her public key $|\psi_{pkA}\rangle$. Similarly, it does the same for the other members.

Phase 1: Identity code generation pahse

Alice generates three random numbers, r_1, r_2 and r_3, and computes $Y_{A1} = D_A + r_{A1}, Y_{A2} = D_A + r_{A2}$, and $Y_{A3} = D_A + r_{A3}$. Then, she computes $Y_{SA} = 3D_A + r_{A1} + r_{A2}$ and $S_A = D_A + Y_{SA} + Y_{A3} = 5D_A + r_{A1} + r_{A2} + r_{A3}$. After this, she performs a rotation operation using S_A on $|\psi_{pkB}\rangle$ and obtains $|IDC_A\rangle$. In a similar way, Bob also produces the relative parameters and performs a rotation operation using S_B on $|\psi_{pkA}\rangle$ to obtain $|IDC_B\rangle$

Phase 2: parameters generation for the session key

Alice randomly selects a rotation angle *a*. Similarly, Bob randomly selects a rotation angle *b*. Then, the two parties separately calculate the following terms.

Alice: $h_A = h(ID_A, a)$, $Y_A = D_A + h_A + a$, $W_A = 2D_A + h_A + 2a$;

Bob: $h_B = h(ID_B, b)$, $Y_B = D_B + h_B + b$, $W_B = 2D_B + h_B + 2b$

After completion, Alice uses Bob's public key to rotate angle W_A and outputs quantum state $|W_A\rangle$. Similarly, Bob rotates Alice's public key by using angle W_B and outputs state $|W_B\rangle$. Then, Alice sends $Y_{A3}, Y_{SA}, |IDC_A\rangle$, $|W_A\rangle$, Y_A, ID_A to Bob. Bob also does this in a similar way, as shown in Figure 7.

Phase 3: Identity verification phase

After receiveing $Y_{A3}, Y_{SA},$ and $|IDC_A\rangle$, Bob performs a rotation operation on $|\psi_{pkA}\rangle$ by degree $(D_B + Y_{SA})$, obtaining quantum state $|Z_A\rangle$. Then, he performs a reverse rotation on $|IDC_A\rangle$ by degree Y_{A3}, obtaining quantum state $|Z'_A\rangle$. After that, Bob measures and compares both measurement results of $|Z_A\rangle$ and $|Z'_A\rangle$ using the same basis *z*. If they are equal, Bob continues. Similarly, Alice will obtain $|Z_B\rangle$ and $|Z'_B\rangle$, and then measures and compares both results of $|Z_B\rangle$ and $|Z'_B\rangle$ by using the same basis. If they are equal, Alice continues, as shown in Figure 8.

Phase 4: Session key generation phase

Alice first performs a reverse rotation operation on $|W_B\rangle$ by angle Y_B, then rotates her secret angle a on the resultant quantum state. By the same way, Bob also preforms a reverse rotatation operation on $|W_A\rangle$ by angle Y_A, then rotates his secret angle b on the resultant state. As a result, A and B obtain the same communication session key $|K_{AB}\rangle = \otimes|0\rangle_{j=1}^{n} \hat{R}^{(j)}(D_A + D_B + b + a) = |K_{BA}\rangle = \otimes|0\rangle_{j=1}^{n} \hat{R}^{(j)}(D_B + D_A + a + b)$, as shown in Figure 9.

Alice	Bob
Phase 0 Public and private key generation phase	
private key D_A, secret angle a public key $\|\psi_{pkA}\rangle$= $\|\psi_{pkA}\rangle = \otimes_{j=1}^{n}\hat{R}^{(j)}(D_A)\|0_z\rangle$	private key D_B, secret angle b public key $\|\psi_{pkB}\rangle$= $\|\psi_{pkB}\rangle = \otimes_{j=1}^{n}\hat{R}^{(j)}(D_B)\|0_z\rangle$
Phase 1: Identity code generation pahse	
Alice generates three random number and computes: $Y_{A1} = D_A + r_{A1}$, $Y_{A2} = D_A + r_{A2}$, $Y_{A3} = D_A + r_{A3}$ then, she computes $Y_{SA} = 3D_A + r_{A1} + r_{A2}$, $S_A = D_A + Y_{SA} + Y_{A3}$ $= 5D_A + r_{A1} + r_{A2} + r_{A3}$ and rotates $\|\psi_{pkB}\rangle$ by S_A, obtaining $\|IDC_A\rangle = \otimes_{j=1}^{n}\hat{R}^{(j)}(S_A)\|\psi_{pkB}\rangle$	Bob generates three random number and computes: $Y_{B1} = D_B + r_{B1}$, $Y_{B2} = D_B + r_{B2}$, $Y_{B3} = D_B + r_{b3}$ then, he computes $Y_{SB} = 3D_B + r_{B1} + r_{B2}$, $S_B = D_B + Y_{SB} + Y_{B3}$ $= 5D_B + r_{B1} + r_{B2} + r_{B3}$ and rotates $\|\psi_{pkA}\rangle$ by S_B, obtaining $\|IDC_B\rangle = \otimes_{j=1}^{n}\hat{R}^{(j)}(S_B)\|\psi_{pkA}\rangle$
Phase 2: random numbers chosen for session key generation	

Calculates $h_A = (ID_A, a)$ $Y_A = D_A + h_A + a$ $\mathrm{W_A} = 2D_A + h_A + 2\mathrm{a}$ $\|W_A\rangle = \otimes_{j=1}^{n} \hat{R}^{(j)}(W_A)\|\psi_{pkB}\rangle$ sends $\|IDC_A\rangle, Y_{A3}, Y_{SA}, \|W_A\rangle, Y_A, ID_A$ to Bob →	Calculates $h_B = (ID_B, b)$ $Y_B = D_B + h_B + b$ $\mathrm{W}_B = 2D_B + h_B + 2\mathrm{b}$ $\|W_B\rangle = \otimes_{j=1}^{n} \hat{R}^{(j)}(W_B)\|\psi_{pkA}\rangle$ ← sends $\|IDC_B\rangle, Y_{B3}, Y_{SB}, \|W_B\rangle, Y_B, ID_B$ to Alice
Phase 3:Identity verification pahse	
Alice performs reverse rotation by degree Y_{B3} on $\|IDC_B\rangle$ to from $\|Z_B\rangle = \otimes_{j=1}^{n} \hat{R}^{J}(-Y_{B3})\ \|IDC_B\rangle$ and rotation $\|Z'_B\rangle = \otimes_{j=1}^{n} \hat{R}^{J}(Y_{SB} + D_A)\ \|\psi_{pkB}\rangle$ then compares and measures the result. If $\|Z_B\rangle = \|Z'_B\rangle$, Alice accepts. Otherwise, she stops the communication.	Bob performs reverse rotation by degree Y_{A3} on $\|IDC_A\rangle$ to from $\|Z_A\rangle = \otimes_{j=1}^{n} \hat{R}^{J}(-Y_{A3})\ \|IDC_A\rangle$ and rotation $\|Z'_A\rangle = \otimes_{j=1}^{n} \hat{R}^{J}(Y_{SA} + D_B)\ \|\psi_{pkA}\rangle$ then compares and measures the result. If $\|Z_A\rangle = \|Z'_A\rangle$, Bob accepts . Otherwise, he stops the communication.
Phase 4: Session key generation phase	
Alice reversely rotates by degree Y_B on $\|W_B\rangle$, to get: $\|K_B\rangle = \|\psi_{pkA}\rangle + D_B + b$ Then, Alice rotates his secret angle *a* on it to get: $\|K_{AB}\rangle = \|\psi_{pkA}\rangle + D_B + b + a.$ Let $K = D_A + D_B + b + a$, $\|K_{AB}\rangle = \otimes_{j=1}^{n} \hat{R}^{(j)}(K)\|0_z\rangle.$	Bob reversely rotates by degree Y_A on $\|W_A\rangle$, to get: $\|K_A\rangle = \|\psi_{pkB}\rangle + D_A + a$ Then, Bob rotates his secret angle *b* on it to get: $\|K_{BA}\rangle = \|\psi_{pkB}\rangle + D_B + a + b.$ Let $K = D_B + D_A + a + b$, $\|K_{BA}\rangle = \otimes_{j=1}^{n} \hat{R}^{(j)}(K)\|0_z\rangle.$

Figure 6. Our key generation scheme

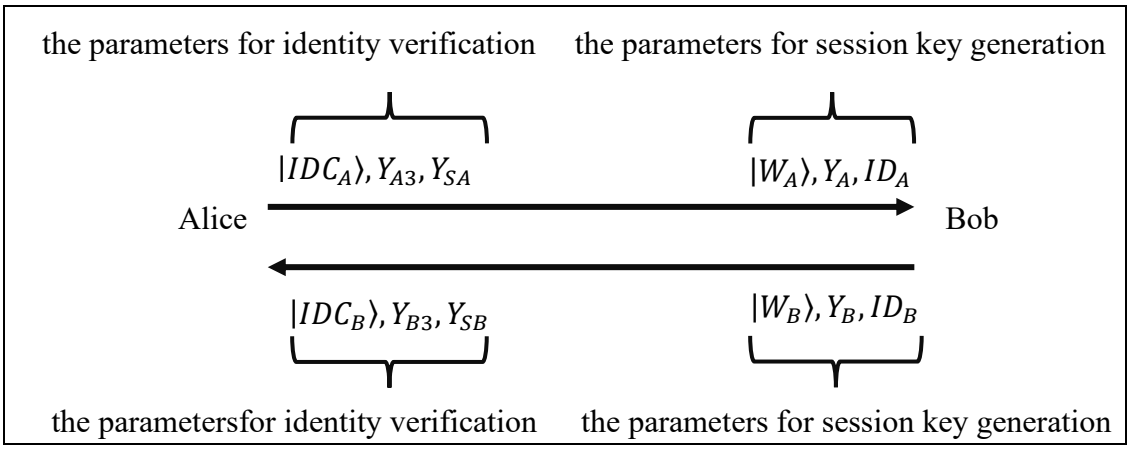

Figure 7. parameters transferred in our scheme

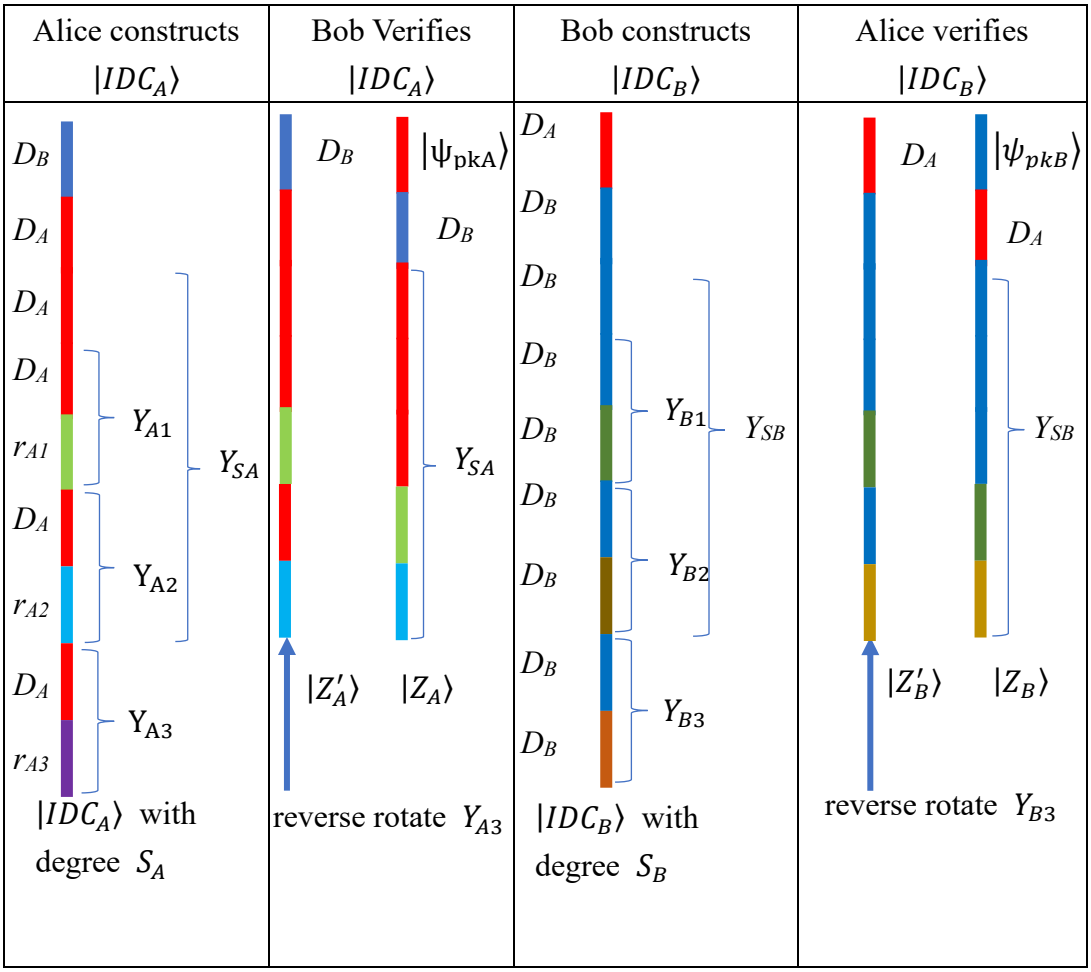

Figure 8. Quantum state rotation (identity verification)

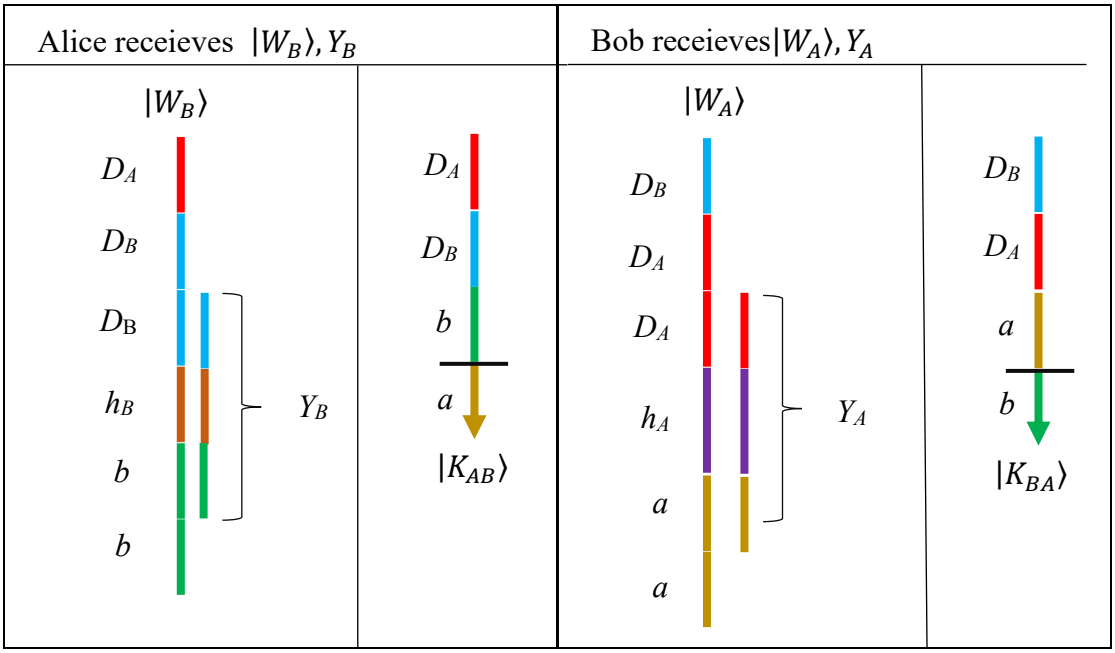

Figure 9. Quantum state rotation (session key)

4. Security analysis

In this section, we will make a series of security analyses on our protocol. In Section 4.1 we prove that attacker Eve cannot sucessfully forge Alice's identity, and in Section 4.2 we prove Eve cannot counterfeit Alice's session key $|K_{AB}\rangle(=|K_{BA}\rangle)$. In both sections, we only show the reasons why in one direction, the reverse one can be easily seen, therefore omitted. In addition, in Section 4.3, we also prove that this scheme can resist the man-in-the-middle attack.

4.1. Eve cannot forge A's identity successfully

In this section, we will analyze the reasons why Eve cannot forge Alice's identity by counterfeiting parameters $|IDC_A\rangle, Y_{A3}, Y_{SA}$. We will demonstrate this by using three cases: (1) E changes Y_{A3}, Y_{SA}, (2) Eve changes $|IDC_A\rangle$, and (3) Eve changes all identity verification parameters $|IDC_A\rangle, Y_{A3}, Y_{SA}$, as shown in the following.

(1) Eve changes Y_{A3}, Y_{SA}

We suppose that Eve changes Y_{A3}, Y_{SA} to $Y_{E3} = D_E + r_{E3}, Y_{SE} = 3D_E + r_{E1} + r_{E2}$, respectively. When Bob receieving Y_{E3}, Y_{SE} and $|IDC_A\rangle$, he performs a rotation on $|\psi_{pkA}\rangle$ by degree $(D_B + Y_{SE})$, and obtains $|Z_E\rangle$. Then, by reversely rotating Y_{E3} on $|IDC_A\rangle$, he gets $|Z'_E\rangle$.

After measuring and comparing both states $|Z_E\rangle$ and $|Z'_E\rangle$ in the same basis, Bob will find they are not equal, because the degrees of $|Z_E\rangle(= D_B + 4D_E + r_{E1} + r_{E2} + D_A)$ and $|Z'_E\rangle(= D_B + 5D_A + r_{A1} + r_{A2} + r_{A3} - D_E - r_{E3})$ are not equal. Therfore, Bob stops the communication.

(2) Eve changes $|IDC_A\rangle$

If attacker Eve changes $|IDC_A\rangle$ to $|IDC_E\rangle$ without changing anything else, because Eve does not know the values of D_B and D_A, he cannot counterfeit the correct quantum state to be verified by Bob. When Bob performs a rotation operation on $|\psi_{pkA}\rangle$ by degree $(D_B + Y_{SA})$, obtaining $|Z'_A\rangle$, and rotates reversely by degree Y_{A3} on $|IDC_E\rangle$, obtaining $|Z_E\rangle$. After that, when Bob measures and compares $|Z_E\rangle$ with $|Z'_A\rangle$ by using thee same basis, he will find that they are not equal, and stop this communication.

(3) Eve changes all identity verification parameters $Y_{A3}, Y_{SA}, |IDC_A\rangle$

We suppose Eve changes all parameters Y_{A3}, Y_{SA}, $|IDC_A\rangle$ to Y_{E3}, Y_{SE}, $|IDC_E\rangle$, with $Y_{E3} = D_E + r_{E3}$, $Y_{SE} = 3D_E + r_{E1} + r_{E2}$ and $|IDC_E\rangle = D_B + 4D_E + r_{E1} + r_{E2} + r_{E3}$. As for the modisfication of $|IDC_A\rangle$, we suppose that Eve performs a rotation on $|\psi_{pkB}\rangle$ by using his secret D_E and the three ramdoms r_{E1}, r_{E2} and r_{E3}, this is because Eve does not know D_A and three ramdoms r_{A1},

r_{A2} and r_{A3}. In this case, after receiving the parameters Bob rotates on $|\psi_{pkA}\rangle$ by D_B and Y_{SE}, he will obtain $|Z_E'\rangle$, whose degree now is $D_A + D_B + (3D_E + r_{E1} + r_{E2})$. In the second step, Bob performs a reverse rotation operation on $|IDC_E\rangle$ by Y_{E3} and obtains $|Z_E\rangle$, that is the degree of $|Z_E\rangle$ equals $D_B + 4D_E + r_{E1} + r_{E2}$. Obviously, the degrees of $|Z_E\rangle$ and $|Z_E'\rangle$ are not equal . Hence, Eve's attack fails.

4.2. Eve cannot forge the common session key

In this section, we will analyze several reasons why Eve cannot forge the session key. We will demonstrate this by using three cases. They are: (1) counterfeiting parameter Y_E as Y_A, (2) changing quantum state $|W_A\rangle$ to $|W_E\rangle$, (3) tampering with parameters W_A and Y_A.

(1) Counterfeiting parameter Y_E as Y_A

Suppose that Eve wants to get $|K_{BA}\rangle$. However, $|K_{BA}\rangle$ is made up from Bob by performing a reverse rotation on $|W_A\rangle$ by degree Y_A, and then rotating his secret angle b, as we mentioned above. We assume that Eve's $Y_E = D_E + h_A + e$, so the degree of $|K_{EA}\rangle = D_B + 2D_A + h_A + 2a - D_E - h_A - e + e$. Apparently, it is not equal to Alice's reverse rotatation Y_B on $|W_B\rangle$, and subsequently rotating her secret a on the resultant state, such that the degree of $|K_{AB}\rangle$ equals D_A+$D_B + b + a$. Therefore, the measurement results of both states $|K_{EA}\rangle \neq |K_{AB}\rangle$. Hence, Eve cannot successfully counterfeit $|K_{BA}\rangle$.

(2) Changing the quantum state $|W_A\rangle$ to $|W_E\rangle$

In order to obtain the session key $|K_{BA}\rangle$, we suppose that Eve changes $|W_A\rangle$ to $|W_E\rangle$, whose degree is $D_B + 2D_E + h_E + 2e$, and keeps Y_A unchanged, Then, sends them to Bob. After receiveing, Bob reversely rotates degree Y_A and then rotates his secret angle b on the recultant state. He obtains $|K_{BA}\rangle' = D_B + 2D_E + h_E + 2e - D_A - h_A - a + b$, which is not equal to the degree of Alice's session key $|K_{AB}\rangle = D_A + D_B + b + a$. Therefore, Eve's attack is not successful.

(3) Tampering with parameters W_A and Y_A

If attacker Eve tampers W_A and Y_A with the parameters $W_{\mathrm{E}}(= 2D_E + h_E + 2\mathrm{e})$ and $Y_E(= D_E + h_E + e)$, and performs a rotation on $|\psi_{pkB}\rangle$ by W_E, attacker Eve will get the quantum state $|W_E\rangle = D_B + 2D_E + h_E + 2e$. Then, sends $|W_E\rangle$ and Y_E to Bob, for Bob to obtain the session key $|K_{BA}\rangle$. However, when Bob receiving them, he first reversely rotates on $|W_E\rangle$ by degree Y_E and then adds its own secret b to obtain$|K_{BE}\rangle = D_B + D_E + e + b$. After receiving $|W_B\rangle$ and Y_B Eve first performs a reverse rotation on $|W_B\rangle$ by Y_B, and then rotates her secret angle e on the resultant state to get $|K_{EB}\rangle = D_A + D_B + b + e,$ which is not equal to $|K_{BE}\rangle$. So, Eve's attack fails.

4.3. Eve performs a man-in-the-middle attack by modifying bilateral parameters for impersonating A to communicate with B, and vice versa

Eve first reversely rotates on quantum state $|W_B\rangle$ by angel Y_B, obtaining quantum state whose degree is $|D_A{+}D_B + b\rangle$, and then reversely rotates on quantum state $|W_A\rangle$ by angle Y_A, obtaining quantum state whose degree is $|D_B{+}D_A + a\rangle$, but E cannot know D_A, D_B, a and b. Moreover, from the analyses shown in section 4.1 and 4.2, it can be easily seen that it is impossible for Eve to deduce $|K_{AB}\rangle$ and $|K_{BA}\rangle$, or equally forges $|K_{EB}\rangle = |K_{BE}\rangle$ and $|K_{EA}\rangle = |K_{AE}\rangle$. Therefore, the attack of Eve fails.

5. Comparisons and applications

In this section, in Section 5.1, we compare our proposed scheme with the literature. Section 5.2 explores the areas that our enhanced scheme can be practically applied.

5.1. Comparisons

The purpose of this protocol is to establish a quantum secret session key shared between both communicating parties in traditional Diffie-Herman way without entanglement. Compared with the methods in literature [1-3], the advantage of our method is that the session keys generated each time are different, which greatly enhances the security level of the communications. It thus outperforms the state-of-the-art in this aspect. The result is shown in Table 2.

Table 2: Comparison with methods in the literature

method / characteristic	Change the shared key every time
ours	✓
〔1〕	×
〔2〕	×
〔3〕	×

5.2. Applications

In the upcoming quantum computer era, the Diffie-Hellman type key exchange method and RSA encryption/signature method, which base on computational infeasibility, will encounter unprecedent challenges. Therefore, the use of quantum computing to establish a secure communication key becomes an unavoidable trend. Compared with the methods in the literature, our key agreement is more suitable to be applied in commercial applications, such as Fintech to ensure transaction security. Also, the security requirements in the fields, public documents, official information transmission, and voting accuracy in an election, can be guaranteed by our scheme.

6. Conclusion

This scheme is the first one to adapt a Diffie-Hellman key agreement by using quantum states without entanglement. It also embeds an identity verification phase to establish the shared quantum session key in the absence of a trusted third party, which thus can decrease the practical application limitations. Moreover, our method can create different session keys in each communications, hence greatly improves the security of both communicating parties. Therefore, our scheme is more suitable to be applied for the strict security requirements in our daily life for the upcoming quantum era.

7.Reference

1. Shi, W. M., Zhou, Y. H., Yang, Y. G., Zhang, X. L., & Zhang, J. B. (2016). An efficient quantum deniable authentication protocol without a trusted center. *Optik*, *127*(16), 6484-6489.
2. Shi, W. M., Zhang, J. B., Zhou, Y. H., Yang, Y. G., & Zhang, X. L. (2016). A non-interactive quantum deniable authentication protocol based on asymmetric quantum cryptography. *Optik*, *127*(20), 8693-8697.
3. Shi, W. M., Zhou, Y. H., Yang, Y. G., & Jiang, N. (2017). A restricted quantum deniable authentication protocol applied in electronic voting system. *Optik*, *142*, 9-12.
4. Gottesman, D., & Chuang, I. (2001). Quantum digital signatures. *arXiv preprint quant-ph/0105032*.
5. Chen, Y., Chou, J. S., Zhou, F.Q., Wang, C. L. (2019). A publicly verifiable quantum signature scheme based on asymmetric quantum cryptography.
6. Castelnovi, Laurent, Ange Martinelli, and Thomas Prest. "Grafting Trees: a Fault Attack against the SPHINCS framework." International Conference on Post-Quantum Cryptography. Springer, Cham, 2018.