SCIENTIFIC REPORTS
nature research

OPEN

A Quantum secure sharing protocol for Cloud data based on proxy re-encryption

Yan Chang ✉, Shi-Bin Zhang, Li-Li Yan & Guo-gen Wan

A quantum scheme for cloud data sharing based on proxy re-encryption is proposed. The user Alice stores the cipher-text of her data on cloud data center. When Alice wants to share her data with another user Bob, Alice is called the delegator and Bob is called the delegatee. The cloud service provider (called the proxy) can convert the delegator's cipher-text into the delegatee's cipher-text without decrypting the former, so that the delegatee can get the plain-text of Alice's data with his private key. The proxy cannot obtain the plain-text of the user's data stored on cloud data center. Delegator in the protocol should have the ability of producing Bell states, performing Bell basis and Z-basis measurements, and storing qubits. The quantum requirements for the delegatee are reduced. The delegatee needs to have the ability of reflecting and performing Z-basis measurement. One secret at a time (one-time one-pad) is theoretically implemented, especially when the same data is shared multiple times. The anti-selection plain-text attack security and the anti-selective cipher-text attack security are realized. Fine-granularity secret data sharing is achieved flexibly.

Proxy re-encryption is a kind of secret sharing method, but it is different from secret sharing in common meaning. In general, secret sharing[1] refers to the split of secrets into several shares, and each share is managed by different participants. A single participant cannot recover secret information. Only a number of participants can work together to recover secret messages. Typical schemes are secret sharing schemes SSSs[2–4] and multi-secret sharing schemes (MSSSs)[5–7].

Proxy re-encryption is a new secret sharing method in cloud environment. The classical proxy re-encryption adds a proxy to the traditional public key encryption system. On the basis of the authorization of Alice (Alice give a conversion key to the proxy), the proxy can convert the cipher-text of Alice's data into the cipher-text of Bob without decryption, and the proxy cannot obtain the plain-text of Alice's data. This not only protects the key of Alice, but also ensures the security of Alice's data. The concept of proxy re-encryption is proposed by Blaze, Bleumer and Strauss[8] on Eurocrypt'98. In fact, proxy re-encryption does not need to re-encrypt, only the cipher-text is converted simply. Therefore, proxy re-encryptionis also called proxy conversion encryption. In 2005, on ACM CCS 2005, Ateniese, Fu, Green and Hohenberger gave the formal definition of their specification and proposed the first proxy re-encryption scheme[9]. This scheme is a two-way authorized proxy re-encryption scheme. That is, the proxy can transform not only the cipher-text of Alice's data into the cipher-text of Bob, but also the cipher-text of Bob's data into the cipher-text of Alice. Later, Ateniese, Fu, Green and Hohenberger proposed a one-way authorization proxy re-encryption scheme[10]. At the annual meeting of CCS 2007, Canetti and Hohenberger proposed a scheme of proxy re-encryption copywriting against selective cipher-text attack[11]. In 2008, Liber and Vergnaud proposed a one-way proxy re-encryption scheme against reproducing selected cipher-text attack[12]. In order to simplify the public key infrastructure in the proxy re-encryption scheme, Green and Ateniese proposed an identity-based proxy re-encryption scheme[13] on the basis of the identity-based public key encryption scheme of Boenh and Franklin[14]. This scheme is proved to be safe under the random prophet model. Then Chu and Tzeng proposed a secure identity-based proxy re-encryption scheme without random prophet model[15] based on identity-based public key encryption[16]. Weng, Deng and Chu put forward the concept of conditional proxy re-encryption[17]. In conditional proxy re-encryption scheme, only cipher-text that meets certain conditions can be re-encrypted by proxy. Subsequently, many conditional proxy re-encryption schemes[18–22] and identity-based conditional proxy re-encryption schemes[23] were proposed. In order to express the conditions and identities in conditional re-encryption more abundant, Liang, Cao, Lin and Shao proposed the

School of Cybersecurity, Chengdu University of Information Technology, Chengdu, 610225, China. ✉e-mail: cyttkl@cuit.edu.cn

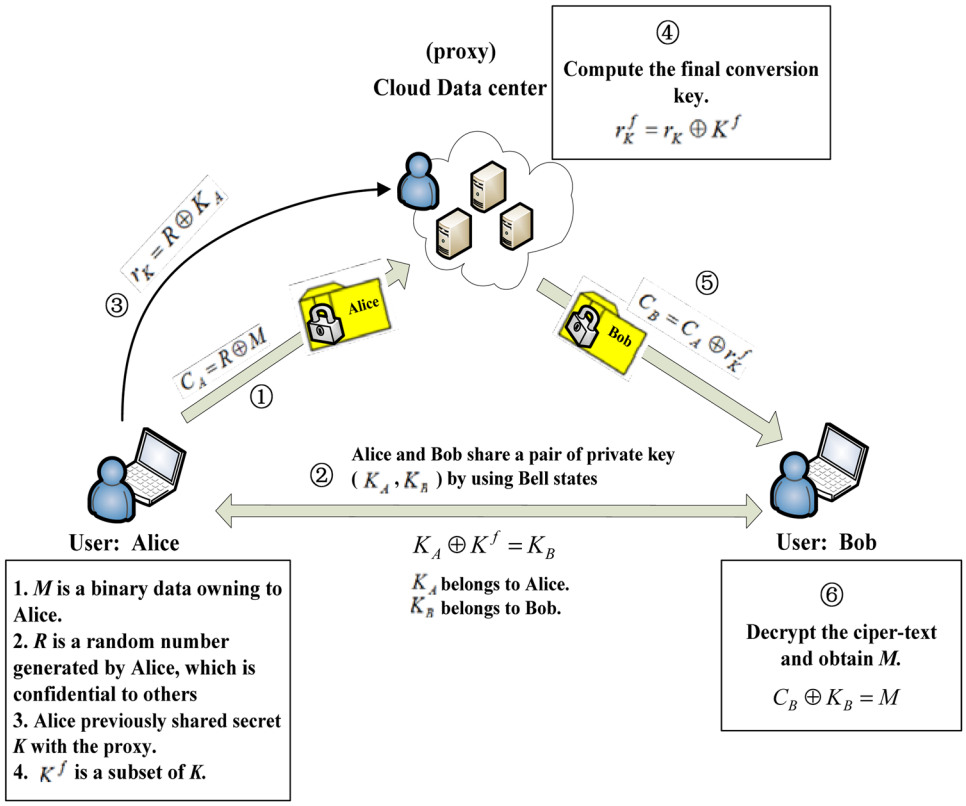

Figure 1. The structure of the protocol.

concept of attribute-based proxy re-encryption[24], and then many attribute-based conditional proxy re-encryption schemes[25–28] were proposed.

With the rapid development of quantum technology, the schemes of quantum encryption[29–34] and quantum secret sharing[35–41] are emerging. However, there is no quantum proxy re-encryption protocol yet. In this paper, a proxy re-encryption protocol based on quantum carriers and quantum principle is proposed. Delegator in the protocol should have the ability of producing Bell states, performing Bell basis and Z basis measurements and storing qubits. While the delegatee is only need to have the ability of performing Z basis measurement and reflecting[33,34,38–40], which reduces the quantum requirements for the delegatee, making it easier to implement. Proxy in the protocol can convert the cipher-text of the delegator (Alice) into the cipher-text of the delegatee (Bob) without decryption, and the proxy cannot obtain the corresponding plain-text information.

The Protocol

The goal of the protocol. Alice and Bob are both users of a cloud data center. $M \in \{0, 1\}^n$ is a binary data belonging to Alice. Alice stores the cipher-text of M on the cloud data center. The cloud service provider is called the proxy. The cipher-text of M is denoted as $C_A \in \{0, 1\}^n$, where $C_A = M \oplus R$. $R \in \{0, 1\}^n$ is a random number generated by Alice using quantum random number generator and is confidential to others. If Alice wants to share M with Bob, they can finish the task securely with the help of the proxy. The general process is as follows: Alice first sends a conversion key $r_K \in \{0, 1\}^n$ to the proxy to let him generate the final conversion key $r_K^f \in \{0, 1\}^n$. Then, the proxy uses r_K^f to change the cipher-text C_A to Bob's cipher-text $C_B \in \{0, 1\}^n$. Bob decrypts C_B to get the plain-text M by using his private key $K_B \in \{0, 1\}^n$. K_B can be obtained by executing the initial algorithm of the protocol, which will be described in the definition 3 of section 2.3. The proxy cannot know the plain-text M. The relation between K_B and other variables will be described in section 2.3. Figure 1 shows the whole structure of the protocol.

Preliminaries. **Definition 1**: Bell state is an important two-qubit state, which has four states:

$$\phi^{\pm} = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle), \quad \psi^{\pm} = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle) \tag{1}$$

The Bell states $\phi^{\pm} = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle)$ have the property that upon measuring the first qubit, one obtains two possible results: 0 with probability 1/2, leaving the post-measurement state $\phi^{\pm} = |00\rangle$, and 1 with probability 1/2,

leaving $\phi^{\pm} = |11\rangle$. As a result, a measurement of the second qubit always gives the same result as the measurement of the first qubit. That is, the measurement outcomes are correlated.

Similarly, the Bell states $\psi^{\pm} = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle)$ have the property that upon measuring the first qubit, one obtains two possible results: 0 with probability 1/2, leaving the post-measurement state $\psi^{\pm} = |01\rangle$, and 1 with probability 1/2, leaving $\psi^{\pm} = |10\rangle$. As a result, a measurement of the second qubit always gives the opposite result as the measurement of the first qubit. That is, the measurement outcomes are also correlated.

Definition 2: Z-basis $\{|0\rangle, |1\rangle\}$ measurement is the measurement of a qubit in the computational basis. This is a measurement on a single qubit with two outcomes defined by the two measurement operators $M_0 = |0\rangle\langle 0|$, $M_1 = |1\rangle\langle 1|$. The measurement operators satisfy the completeness. Suppose the state being measured is $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$. Then the probability of obtaining measurement outcome 0 is $p(0) = |\alpha|^2$. Similarly, the probability of obtaining the measurement outcome 1 is $p(1) = |\beta|^2$. The state after measurement in the two cases is therefore $|0\rangle$ or $|1\rangle$.

Algorithm definition. When Alice's data stored on cloud server is to be shared with Bob, Alice is the delegator, Bob is the delegatee, and the cloud server is the proxy. Alice previously shared $K \in \{0, 1\}^N$ with the proxy by executing quantum key distribution protocol.

Definition 3: The Initial Algorithm

Initial(K): On inputting the secret key $K \in \{0, 1\}^N$, this algorithm works as below:

1. Alice prepares N Bell states according to K. The preparation rule is: '0' to prepare state ϕ^+ and '1' to prepare state ψ^-.
2. Alice reserves one particle of each Bell state and sends the other particle to Bob.
3. Bob randomly performs Z-basis $\{|0\rangle, |1\rangle\}$ measurement or reflecting on each particle he received. Bob saves the measurement results as $K_B \in \{0, 1\}^n$, where '0' denotes result $|0\rangle$, and '1' denotes $|1\rangle$.
4. Alice performs joint Bell-basis measurements on reflected particles she received and the corresponding reserved particles. If each measurement result is consistent with the Bell state that originally prepared, or if the inconsistent ratio is below the predetermined threshold, the protocol will continue, otherwise the protocol will be terminated.
5. Alice records the positions as Q where she doesn't receive particles, and measures the corresponding reserved particles with Z-basis. She saves the measurement results as $K_A \in \{0, 1\}^n$, according to the rule: '0' for state $|0\rangle$ and '1' for state $|1\rangle$.

Definition 4: Key Generation Algorithm

KeyGen(K_A, R): On inputting Alice's secret key K_A and a random number R, this algorithm outputs key $r_K \in \{0, 1\}^n$, where $r_K = R \oplus K_A$.

Definition 5: Re-Encryption Key Generation Algorithm

ReKeyGen(r_K): On inputting the secret key r_K, this algorithm works as below:

1. Alice computes $r'_K = Encrypt_K(r_K, Q)$ and sends r'_K to the proxy (cloud server). Here $Encrypt_K()$ can be any symmetric encryption algorithm except for XOR.
2. The proxy decrypts r'_K with K to obtain r_K and Q.
3. According to Q, the proxy extracts the corresponding bits in K to get $K^f \in \{0, 1\}^n$.
4. The proxy computes $r_K^f = r_K \oplus K^f = R \oplus K_A \oplus K^f = R \oplus K_B$, and obtains the final conversion key $r_K^f \in \{0, 1\}^n$. Here, $K_A \oplus K^f = K_B$ is obtained according to the property of Bell states.

Definition 6: Encryption Algorithm

Encrypt(R, M): On inputting a random number R and plain-text M, this algorithm outputs the cipher-text $C_A \in \{0, 1\}^n$, where $C_A = R \oplus M$.

Definition 7: Re-Encryption Algorithm

ReEncrypt(r_K^f, C_A): On inputting the final conversion key r_K^f and cipher-text C_A, this algorithm outputs the re-encryption cipher-text $C_B \in \{0, 1\}^n$, where $C_B = C_A \oplus r_K^f$.

Definition 8: Decryption Algorithm

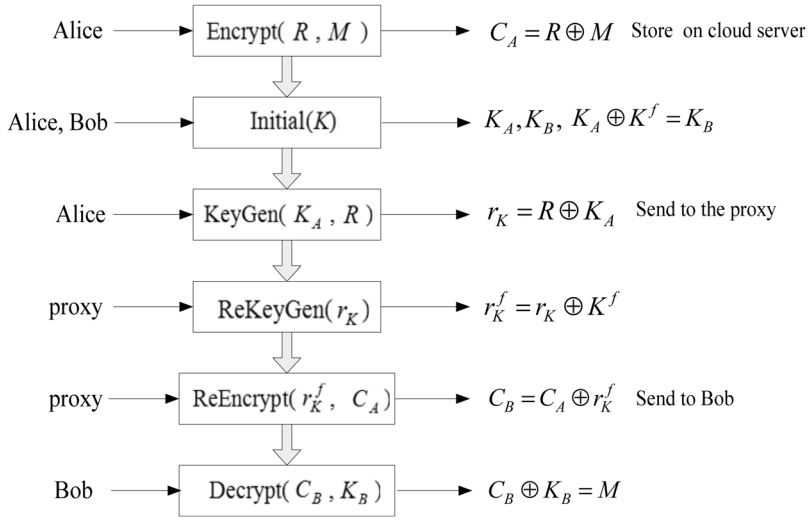

Figure 2. The process of algorithm execution.

Decrypt(C_B, K_B): On inputting Bob's secret key K_B and cipher-text C_B, this algorithm outputs the plain-text M.

Figure 2 shows the process of algorithm execution.

The Security Proof of the Protocol

We conclude that the protocol satisfies the consistency according to the following derivation: Alice-> the proxy:

$$Encrypt_K(r_K, Q)$$

$$C_A = R \oplus M$$

The proxy: $r_K,\ Q = Decrypt_K(Encrypt_K(r_K, Q))$

$$K^f = Extract(K, Q)$$

$$r_K^f = r_K \oplus K^f$$

The proxy –> Bob: $C_B = C_A \oplus r_K^f$

Bob: $C_B \oplus K_B = C_A \oplus r_K^f \oplus K_B = R \oplus M \oplus r_K^f \oplus K_B = R \oplus M \oplus R \oplus K_B \oplus K_B = M$

Generally speaking, in order to prove the security of a classical cryptography scheme, the security objectives are first determined. Then an attack model is constructed according to the ability of the attacker. Finally, the method specification for breaking the scheme is proposed to solve a difficult mathematical problem or difficult assumption.

In our scheme, Alice's data is encrypted with a random number R and stored on cloud server. Any user that Alice is willing to share data with can realize the sharing by executing the protocol. The principles of quantum non-cloning, uncertainty and entanglement ensure that the re-encryption cipher-text of the same shared data in each sharing process is different, which means that one secret at a time (one-time one-pad) is realized. Therefore, it can be proved that the protocol can resist anti-selective plain-text attack and anti-selective cipher-text attack without using the classical reduction method.

The principles of quantum non-cloning, uncertainty and entanglement work on the premise that the protocol has the ability to discover or prevent attackers from falsifying quantum carriers. Section 4.1 and 4.2 prove that if the eavesdropper intends to falsifying quantum carriers (replacing or destructing the Bell states), his behavior will be found with very high probability (almost 99.9%).

Furthermore, in the protocol, the proxy only knows K^f (the entanglement relationship between K_A and K_B), he cannot know the data stored on cloud server. Bob only know Q and K_B, he does not know the relationship between K_A and K_B, therefore he cannot know the data stored on cloud server without the re-encryption of cipher-text by the proxy.

Security Analysis

Intercept-resend attack. The external attacker Eve may intercept the particles that Alice sent to Bob, and measure them with Z-basis, then prepare some particles with the same state and send them back to Bob. Suppose that each particle reserved by Alice is expressed as particle 1, each particle sent to Bob is represented as particle 2, and each particle re-prepared by Eve is represented as particle e. Then, after Eve intercepting and measuring particles 2 with Z-basis, the state of particle 1 collapses to $\rho_1 = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1|$. The state of the particle reflected by Bob is $\rho_e = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1|$. The combined state of particle 1 and particle e is:

$$\rho_{1e} = \frac{1}{4}|00\rangle\langle 00| + \frac{1}{4}|11\rangle\langle 11| + \frac{1}{4}|01\rangle\langle 01| + \frac{1}{4}|10\rangle\langle 10| \tag{2}$$

If the initial combined state of particle 1 and 2 is ψ^-, after eavesdropping detection, the joint Bell-basis measurement result on particle 1 and e is as follows:

$$\rho'_{1e} = \frac{1}{2}|\psi^+\rangle\langle\psi^+| + \frac{1}{2}|\psi^-\rangle\langle\psi^-| \tag{3}$$

If the initial combined state of the particles 1 and 2 is ϕ^+, after eavesdropping detection, the joint Bell-basis measurement result on particle 1 and e is as follows:

$$\rho'_{1e} = \frac{1}{2}|\phi^+\rangle\langle\phi^+| + \frac{1}{2}|\phi^-\rangle\langle\phi^-| \tag{4}$$

Therefore, Alice can discover Eve's eavesdropping on each qubit with probability 1/2, and the total probability that Alice can detect Eve's eavesdropping is $1-(1/2)^n$. When $n=5$, the probability reaches 97%. The protocol will be terminated, and the eavesdropper will not obtain any data that Alice stored on the cloud server.

Source untrusted attack. The reflected particles are used for eavesdropping detection, not only detecting the intercept-resend attack, but also detecting the source untrusted attack[42–44]. Usually, in source untrusted attack, the eavesdroppers with super ability will control or provide devices used to prepare Bell states. Although Alice thinks a real Bell state is prepared, what she actually gets may be a different state because the preparing device is controlled or provided by Eve[42–44]. That is, the source is untrusted.

To steal secret message, Eve may control the device to prepare some non-entangled mixed states of $|00\rangle$, $|01\rangle$, $|10\rangle$, $|11\rangle$ or entangled states with higher dimensional such as GHZ states.

(1) Eve prepares state $\rho_{12} = \frac{1}{2}|00\rangle\langle 00| + \frac{1}{2}|11\rangle\langle 11|$ instead of ϕ^+ and prepares state $\rho_{12} = \frac{1}{2}|01\rangle\langle 01| + \frac{1}{2}|10\rangle\langle 10|$ instead of ψ^-. By doing so, Eve will know K_A and K_B before eavesdropping detection. However, during the eavesdropping detection, Alice performs the joint Bell-basis measurement on particles 1 and 2, and the following results will be obtained respectively:

$$\rho'_{12} = \frac{1}{2}|\phi^+\rangle\langle\phi^+| + \frac{1}{2}|\phi^-\rangle\langle\phi^-| \text{ or } \rho'_{12} = \frac{1}{2}|\psi^+\rangle\langle\psi^+| + \frac{1}{2}|\psi^-\rangle\langle\psi^-| \tag{5}$$

Obviously, Alice will discover Eve's eavesdropping on each qubit with probability 1/2, and the total probability that Alice finds Eve's eavesdropping is $1-(1/2)^n$. Thus, the protocol will be terminated, and the eavesdropper will not obtain any data that Alice stored on the cloud server.

(2) Eve prepares entangled state G_0, G_1 or $\rho_{123} = \frac{1}{2}|G_0\rangle\langle G_0| + \frac{1}{2}|G_1\rangle\langle G_1|$ instead of ϕ^+, and prepares entangled state G_2, G_3 or $\rho_{123} = \frac{1}{2}|G_2\rangle\langle G_2| + \frac{1}{2}|G_3\rangle\langle G_3|$ instead of ψ^-. Here,

$$\begin{aligned} G_0 &= \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{123}, \quad G_1 = \frac{1}{\sqrt{2}}(|001\rangle + |110\rangle)_{123} \\ G_2 &= \frac{1}{\sqrt{2}}(|010\rangle + |101\rangle)_{123}, \quad G_3 = \frac{1}{\sqrt{2}}(|100\rangle + |011\rangle)_{123} \end{aligned} \tag{6}$$

Eve sends particle 1 and 2 to Alice, and keeps particle 3 herself. When Bob measures the received particle 2 with Z-basis, the state of particle 1 and 3 collapse. Since Eve does not know on which positions Bob will measure and which positions to reflect, Eve will not measures those particles 3 on the un-reflected positions with Z-basis until she determines which positions are reflected. Although, by doing so, she will obtain K_A and K_B, but before that, to detect eavesdropping Alice performs joint Bell-basis measurement on particle 1 and 2. If Eve prepares entangled state G_0, G_1 or $\rho_{123} = \frac{1}{2}|G_0\rangle\langle G_0| + \frac{1}{2}|G_1\rangle\langle G_1|$ instead of ϕ^+, the measurement result is:

$$\rho'_{12} = \frac{1}{2}|\phi^+\rangle\langle\phi^+| + \frac{1}{2}|\phi^-\rangle\langle\phi^-| \tag{7}$$

If Eve prepares entangled state G_2, G_3 or $\rho_{123} = \frac{1}{2}|G_2\rangle\langle G_2| + \frac{1}{2}|G_3\rangle\langle G_3|$ instead of ψ^-, the measurement result is:

$$\rho_{12}{}' = \frac{1}{2}|\psi^+\rangle\langle\psi^+| + \frac{1}{2}|\psi^-\rangle\langle\psi^-| \tag{8}$$

Obviously, before Eve knows K_A and K_B, Alice will discover the eavesdropping behavior of Eve with probability $1-(1/2)^n$. Thus, the protocol will be terminated, and the eavesdropper will not obtain any data that Alice stored on the cloud server.

Proxy attack. In this protocol, an honest proxy knows only the correlation between K_A and K_B, but does not know exactly what K_A and K_B are. Therefore, the honest proxy cannot know M through $C_B = M \oplus K_B$. In addi-

tion, only the delegator knows the random number R which encrypted shared data M, so the proxy cannot know M through $C_A = R \oplus M$.

If the proxy is dishonest, assuming that he is the eavesdropper discussed in 4.1 and 4.2, besides having the power of eavesdroppers, he knows K. When the proxy performs intercept-resend attacks, having K will not help him with the success of his attack. Therefore, when Alice detects eavesdroppers, the attack will be found by Alice with probability $1 - (1/2)^n$. And the proxy cannot know the shared data that Alice stored on the cloud server.

For an honest proxy, although he has the conversion key r_k and the final conversion key r_K^f, he cannot obtain the plain-text of shared data stored on the cloud server. For a dishonest proxy, his bad behavior will be detected with probability closing to 100%. Therefore, neither honest proxy nor dishonest proxy have access to the plain-text of shared data stored on the cloud server.

The Comparisons with Previous Works

Compared with the previous classical proxy re-encryption protocols proposed in refs. [8–12], our protocol theoretically implements one secret at a time (one-time one-pad), especially when the same data is shared multiple times. In each data sharing process, K_A, K_B and r_K^f are random numbers with entanglement correlation, which is ensured by the principles of quantum non-cloning, uncertainty and entanglement. The second layer cipher-text (cipher-text of the delegatee) will not reappear. Therefore, the protocol realizes the anti-selection plain-text attack security and the anti-selective cipher-text attack security without basing on the difficult mathematical problem or difficulty assumption.

Compared with the protocols proposed in refs. [8–16], our protocol can flexibly achieve fine-granularity secret data sharing. Alice can control the sharing granularity to Bob by adjusting r_K and the starting location of shared data. However, the protocol cannot resist the conspiracy attack of the proxy and Bob.

Our protocol requires Alice have the ability of producing Bell states, performing Bell basis and Z basis measurements and storing qubits. The quantum ability of Bob is low; he is only need to have the ability of performing Z basis measurement and reflecting. Compared with QSS protocols proposed in refs. [37,39–41,45], our protocol reduces the difficulty of implementation. In refs. [39–41], multi-particle entanglement states need to be prepared, which is more difficult than preparing Bell states. In ref. [45], although both classical and quantum secret sharing are designed, however the quantum Fourier transform and d-level quantum system are needed, which are more complex and difficult to implement than our protocol.

Discussion

Smooth entropy and mutual information are usually used to analyse the security of quantum key distribution, i.e. secret key agreement by communication over a quantum channel[50–52]. In this section, we analyze the post-processing of the protocol from the perspective of mutual information.

In order to make the key shared by Alice and Bob logically consistent, and to reduce the amount of information Eve knows, the protocol has to carry out error reconciliation and privacy amplification. Eve may intercept the particle 2 sent by Alice to Bob, then measures it with the Z-basis and sends it back to Bob. Normally, Bob randomly chooses to reflect the particle or measure the particle with Z-basis. The results of the Z-basis measurement are taken as K_B. Eve's attack will not result in a bit error because the measurement basis is the same with Bob's.

Let the bit error rate be λ for the environmental factors[46,47] other than Eve's above attack. In order to correct errors, at least the extra information of $H_2(\lambda)$ needs to be transmitted for each bit. After privacy amplification, the security key rate is:

$$r \leq I(B\colon A) - I(B\colon E) = 1 - H_2(\lambda) - I(B\colon E) \tag{9}$$

Because the eavesdropping detection of the protocol is to detect whether the two parties share the entangled state ϕ^+ or ψ^-, once the shared entangled state is confirmed by the eavesdropping detection, Eve cannot obtain the information of K_B according to the monogamy of nonlocal correlations (entanglement). Therefore, in our protocol, $I(B\colon E) = 0$.

$$r \leq 1 - H_2(\lambda) \tag{10}$$

Assuming that the length of the secret data M is n, the length of r_K^f, K_A and K_B must be n bits in order to ensure that the secret data can be successfully shared. Therefore, the length of r_K^f, K_A and K_B before error reconciliation and privacy amplification which is denoted as m must satisfy the following inequality

$$m \geq \frac{n}{1 - H_2(\lambda)} \tag{11}$$

The number of Bell states prepared in the initial algorithm should satisfy:

$$N = 2m \geq \frac{2n}{1 - H_2(\lambda)} \tag{12}$$

Conclusion

The proposed quantum cryptography[48,49] protocol realizes secure data sharing on cloud server based on proxy conversion encryption. In the protocol, the intercept-resend attack, the source untrusted attack, and the proxy attack are analyzed. Delegator in the protocol should have the ability of producing Bell states, performing Bell basis and Z basis measurements and storing qubits. While the quantum requirements for the delegatee are

reduced. The delegatee is only need to have the ability to reflect and performing Z-basis measurement, which satisfies the semi-quantum condition. In data loss scenario, to ensure the normal keys sharing, after Alice sends particles to Bob, Bob should publish which particles are lost, and Alice discards the corresponding particles. Alice and the proxy should discard the corresponding bits of K before extracting K^f.

Received: 30 April 2019; Accepted: 27 March 2020;
Published online: 03 June 2020

References

1. Attasena, V., Darmont, J. & Harbi, N. Secret sharing for cloud data security: a survey. *The VLDB Journal.* **26**, 657–681 (2017).
2. Shamir, A. How to share a secret. *Commun. ACM.* **22**, 612–613 (1979).
3. Parakh, A. & Kak, S. Space efficient secret sharing for implicit datasecurity. *Inf. Sci.* **181**(2), 335341 (2011).
4. Liu, Y. X., Harn, L., Yang, C. N. & Zhang, Y. Q. Efficient (n, t, n)secret sharing schemes. *J. Syst. Softw.* **85**(6), 1325–1332 (2012).
5. Yang, C. C., Chang, T. Y. & Hwang, M. S. A (t, n) multi-secret sharing scheme. *Appl. Math. Comput.* **151**(2), 483–490 (2004).
6. Waseda, A. & Soshi, M. Consideration for multi-threshold multisecret sharing schemes. In: 2012 International Symposium onInformation Theory and its Applications (ISITA 2012), Honolulu, USA, pp. 265–269 (2012).
7. Takahashi, S. & Iwamura, K. Secret sharing scheme suitablefor cloud computing. In: 27th International Conference onAdvanced Information Networking and Applications (AINA2013), Barcelona, Spain, pp. 530–536 (2013).
8. Blaze, M., Bleumer, G. & Strauss, M. Divertible protocols and atomic proxy cryptography. International Conferenceon the Theory and Applications of Cryptographic Techniques EUROCRYPT 1998: Advances in Cryptology. pp 127–144 (1998).
9. Ateniese, G., Fu, K., Green, M. & Hohenberger, S. Improved proxy re-encryption schemes with applications to secure distributed storage. Proceedings of the 12th Annual Network and Distributed System Security Symposium. NewYork: ACM, pp.29–44 (2005).
10. Ateniese, G., Fu, K., Green, M. & Hohenberger, S. Improved proxy re-encryption schemes with applications to secure distributed storage. *NewYork: ACM* **90**(1), 1–30 (2009).
11. Canetti, R. & Hohenberger, S. Chosen-ciphertext secure proxy re-encryption. Proceedings of the14thACMconference on Computer and Comuniation, Security. NewYork: ACM, pp.185–194 (2007).
12. Libert, B. & Vergnaud, D. Unidirectional chosen-ciphertext secure proxy re-encryption. Proceedings of PKC 2008. Berlin: Springer-Verlag, Barcelona, pp.360–379 (2008).
13. Green, M. & Ateniese, G. Identity-based proxy re-encryption. Proceedings of ACNS 2007, Berlin:Springer-Verlag, pp.288–306 (2007).
14. Boneh, D. & Franklin, M., Identity-based encryption from theweil pairing. Proceedings of CRYPTO 2001, Berlin: Springer-Verlag, pp.231–229 (2001).
15. Chu, C. & Tzeng, W. Identity-based proxy re-encryption without random oracles. Proceedings of ISC 2007, Berlin:Springer-Verlag, pp.189–202 (2007).
16. Waters, B. Efficient identity-based encryption without random oracles. Proceedings of EUROCRYPT 2005, Berlin: Springer-Verlag, pp. 189–202 (2005).
17. Weng, J., Deng, R. H. & Chu, C. Conditional proxy re-encryption secure against chosen-ciphertext attack. Proceedings of the 4th International Symposium on ACM Symposium on Information, Computer and Communications Security 2009, NewYork: ACM, pp.322–332 (2009).
18. Weng, J., Yang, Y., Tang, Q., Deng, R. & Bao, F. Efficient conditional proxy re-encryption with chosen-ciphertext security. Proceedings of the 12th International Conference on Information Security 2009, Berlin:Springer-Verlag, pp.151–166 (2009).
19. Tang, Q. Type-based proxy re-encryption and its construction. Proceedings of INDOCRYPT 2008, Berlin:Springer-Verlag, pp.130–144 (2008).
20. Chu, C., Weng, J., Chow, S., Zhou, J. & Deng R. Conditional proxy broadcast re-encryption. Proceedings of ACISP 2009, Berlin:Springer-Verlag, pp.327–342 (2009).
21. Shao, J., Cao, Z. F., Liang, X. H. & Lin, H. Proxy re-encryption with keyword search. *Infromation Science.* **180**, 2576–2587 (2010).
22. Fang, L. M., Susilo, W., Ge, C. P. & Wang, J. D. Chosen-ciphertext secure anonymous conditional proxy re-encryption with keyword search. *Theoretical Computer Science.* **462**, 39–58 (2012).
23. Liang, K., Liu, Z., Tan, X., Wong, D. S. & Tang, C. A CCA-Secure Identity-Based Conditional Proxy Re-Encryption without Random Oracles. Proceedings ofICISC 2012, Berlin: Springer-Verlag, pp.189–202 (2012).
24. Liang, X., Cao, Z., Lin, H. & Shao, J. Attribute-Based Proxy Re-Encryption with Delegating Capabilities. Proceedings of ASIACCS 2009, NewYork: ACM, pp.276–286 (2009).
25. Liang, K., Fang, L., Wong, D. S. & Susilo W. A Ciphertext-Policy Attribute-Based Proxy Re-Encryption with Chosen-Ciphertext Security. Proceedings of the 5th International Conference onIntelligent Networking and Collaborative Systems 2013, USA: IEEE Computer Society, pp.552–559 (2013).
26. Liang, K. *et al*. An Adaptively CCA-Secure Ciphertext-Policy Attribute-Based Proxy Re- Encryption for Cloud Data Sharing. Proceedings of ispec 2014, Berlin: Springer-Verlag, pp.448–461 (2014).
27. Fang, L. M., Susilo, W., Ge, C. & Wang, J. D. Interactive conditional proxy re-encryption with fine grain policy. *Journal of Systerms and Software* **84**, 2293–2302 (2011).
28. Ge, C. G. *et al*. A Key-Policy Attribute-based Proxy Re-encryption without Random Oracles. *The Computer Journal.* **59**(7), 970–98 (2016).
29. Long, G. L. & Liu, X. S. Theoretically efficient high-capacity quantum-key-distribution scheme. *Phys Rev A.* **65**, 032302 (2002).
30. Deng, F. G., Long, G. L. & Liu, X. S. Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block. *Phys Rev A* **68** 042317(1-4) (2003).
31. Wang, C., Deng, F. G., Li, Y. S., Liu, X. S. & Long, G. L. Quantum secure directcommunicati -on with high-dimension quantum superdense coding. *Phys Rev A.* **71**, 044305 (2005).
32. Chang, Y., Xu, C. X., Zhang, S. B. & Yan, L. L. Quantum secure direct communication andauthentication protocol with single photons. *Chinese Science Bulletin.* **58**(36), 4571–4576 (2013).
33. Yu, K. F. *et al*. Authenticated semi-quantum key distribution protocol using Bell states. *Quantum Information Processing.* **13**(6), 1457–1465 (2014).
34. Zou, X. *et al*. Semiquantum-key distribution using less than four quantum states. *Phys Rev A.* **79**(5), 1744–1747 (2009).
35. Hillery, M., Buzek, V. & Berthiaume, A. Quantum secret sharing. *Phys Rev A* **59**, 1829–1834 (1999).
36. Gottesman, D. Theory of quantum secret sharing. *Phys. Rev. A* **61**, 042311 (2000).
37. Xiao, L., Long, G. L., Deng, F. G. & Pan, J. W. Efficient multiparty quantum-secret-sharing schemes. *Phys Rev A.* **69**: 052307(1-5) (2004).
38. Wang, J., Zhang, S., Zhang, Q. & Tang, C. J. Semiquantum secret sharing using two-particle entangled state. *Int. J. Quantum Inf.* **10**(5), 1250050 (2012).
39. Yang, C. W. & Hwang, T. Efficient key construction on semi-quantum secret sharing protocols. *Int. J. Quantum Inf.* **11**(05), 1350052 (2013).
40. Xie, C., Li, L. & Qiu, D. A novel semi-quantum secret sharing scheme of specific bits. *Int. J. Theor. Phys.* **54**(10), 3819–3824 (2015).

41. Gao, X., Zhang, S. B. & Chang, Y. Cryptanalysis and Improvement of the Semi-quantum Secret Sharing Protocol. *Int J Theor Phys.* **56**, 2512–2520 (2017).
42. Arnonfriedman, R. *et al*. Practical device-independent quantum cryptography via entropy accumulation. *Nature Communications.* **9**(1), 459 (2018).
43. Ribeiro, J., Murta, G. & Wehner, S. Fully device-independent conference key agreement. *Phys Rev A*. **97**(2), 022307 (2018).
44. Acín, A., Gisin, N. & Masanes, L. From Bell's.theorem to secure quantum key distribution. *Phys Rev Lett.* **97**(12), 120405 (2006).
45. Mashhadi, S. General secret sharing based on quantum Fourier transform. *Quantum Information Processing* **18**, 114 (2019).
46. Liu, W., Gao, P., Liu, Z., Chen, H., & Zhang, M. A quantum-based database query scheme for privacy preservation in cloud environment. *Security and Communication Networks*, https://doi.org/10.1155/2019/4923590 (2019).
47. Liu, W., Xu, Y., Zhang, M., Chen, J. & Yang, C. A novel quantum visual secret sharing scheme. *IEEE Access.* **7**, 114374–114384 (2019).
48. Qu, Z. G., Wu, S. Y., Wang, M. M., Sun, L. & Wang, X. J. Effect of quantum noise on deterministic remote state preparation of an arbitrary two-particle state via various quantum entangled channels. *Quantum Information Processing.* **16**(306), 1–25 (2017).
49. Qu, Z. G., Li, Z. Y., Xu, G., Wu, S. Y. & Wang, X. J. Quantum image steganography protocol based on quantum image expansion and grover search algorithm. *IEEE Access.* **7**, 50849–50857 (2019).
50. Renner, R. Security of quantum key distribution. Ph.D. dissertation, Dept. Phys., ETH Zurich, Zurich, Switzerland (2005).
51. Tomamichel, M., Schaffner, C., Smith, A. & Renner, R. Leftover hashing against quantum side information. *IEEE Transactions on Information Theory.* **57**(8), 5524–5535 (2011).
52. Hayashi, M. Large deviation analysis for quantum security via smoothing of Renyi entropy of order 2. *IEEE Transactions on Information Theory.* **60**(10), 6702–6732 (2014).

Acknowledgements

This work is supported by NSFC (Grant Nos. 61572086, 61402058), Sichuan Science and Technology Program (Grant Nos. 2017JY0168, 2018TJPT0012, 2018GZ0232, 2018CC0060, 2017GFW0119, 2017GZ0006, 2016GFW0127), the National Key Research and Development Program (No. 2017YFB0802302), Sichuan innovation team of quantum security communication (No. 17TD0009), Sichuan academic and technical leaders training funding support projects (No. 2016120080102643).

Author contributions

All authors designed the protocol. Yan Chang and Shibin Zhang analyzed its security. Lili Yan and Guogen Wan wrote the main manuscript text. All authors reviewed the manuscript.

Competing interests

The authors declare no competing interests.

Additional information

Correspondence and requests for materials should be addressed to Y.C.

Reprints and permissions information is available at www.nature.com/reprints.

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.