TRANSFERING QUANTUM E-CHEQUES IN NONSECURED CHANNELS

DO NGOC DIEP[1,2]

Abstract. The problem of transfering e-cheques in absolutely secured channels was constructed in the first part. The construction guarantees that the participants could open the secret only if they cooperated toghether and the dishonest participants could not change the received informations. In practice the absolutely secured channels do not exist. In this second paper we produce quantum e-cheques, based on multiparty quantum telecommunication between customer and cooperated branches of bank and the channels are nonsecured: there could be some eavesdroppers.

AMS Mathematics Subject Classification: 15A06; 15A99
Keywords and Terms: quantum secret sharing scheme; quantum multivariate interpolation, quantum cheques, quantum e-cheques

1. Introduction

The problem of quantum cheques was initialized in [2] and [10] in 1969 as *quantum money*, and later it was retrieved by Aaronson [1] as *public key quantum money* in 2009. In 2010 it was studied again by Mosca and Stebila [8] under the name of *quantum coins* etc.... In the paper [9] S. R. Moulick and P.K. Panigrahi constructed a scheme for quantum cheques in 2017.

The problem of providing a quantum code of classical cheques is a central problem of the quantum money problem. The question is to provide a scheme of quantum code in such a way that it should be similar to the classical ones but with absolute high secrecy. In the work [9], the authors gave an adequate survey of development of the problem and constructed a scheme for quantum cheques. The scheme coveres the classical version of cheques: containing the ingredients like identtity, serial numbers, key, etc...... .The quantum cheque will use the schemes of the form $\Pi = (Gen, Sign, Vrfy)$.

Some customer Alice and bank make initialation by the *Gen scheme:* namely Alice came to some bank branch to open an account with *secret key* as a binary L-digit number $k \in \{0,1\}^L$ to provide an electronique *signature* in the future, by using some *secret key generation scheme* for Alice and bank. The bank later gives her a *cheque book serial number* s. For secrecy, Alice produces some *public key pk* and store a *secret* *key sk*. The bank produces 3 entangled qubits in Greenberger-Horne-Zeilinger (GHZ) states

$$|\phi^{(i}\rangle_{GHZ} = \frac{1}{\sqrt{2}}\left(|0^{(i)}\rangle_{A_1}|0^{(i)}\rangle_{A_2}|0^{(i)}\rangle_B + |1^{(i)}\rangle_{A_1}|1^{(i)}\rangle_{A_2}|1^{(i)}\rangle_B\right), 1 \leq i \leq n$$

and send two of them, namely $|\phi\rangle_{A_1}$ and $|\phi\rangle_{A_2}$ to Alice. Therefore Alice holds $(id, pk, sk, k, s, \{|\phi^{(i)}\rangle_{A_1}, \phi^{(i)}\rangle_{A_2}\})$ and the bank branch holds $(id, pk, sk, k, s, \{|\phi^{(i)}\rangle_B\})$.

The next step is the *Sign scheme:.* Alice chooses a random number r with using a random number generation procedure $r \leftarrow U_{\{0,1\}^L}$, a numeration $i = 1, \dots, n$ of orthogonal base $|\phi^{(i)}\rangle$ and certainly an amount M she likes to make some transaction with bank (debit or credit), and then evaluate the one-way funtion $f : \{0,1\}^* \times |0\rangle \to |\psi^{(i)}\rangle$ at the concatennation $x||y$ of the data as $k||id||r||M||i$ to providing a state $\psi^{(i)} = \alpha_i|0\rangle + \beta_i|1\rangle$. Alice encodes the data $|\psi^{(i)}\rangle$ with the $|\phi^{(i)}\rangle_{A_1}$, making them entangled and measuring the Bell states:

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

. The system is in the states of form $|\phi^{(i)}\rangle = |\psi^{(i)}\rangle \otimes |\phi\rangle_{GHZ} =$

$$\frac{1}{2}\left\{|\phi^+\rangle_{A_1}(\alpha_i|00\rangle_{A_2B} + \beta_i|11\rangle_{A_2B}) + |\phi^-\rangle_{A_1}(\alpha_i|00\rangle_{A_2B} - \beta_i|11\rangle_{A_2B})\right.$$

$$\left.+|\psi^+\rangle_{A_1}(\alpha_i|00\rangle_{A_2B} + \beta_i|11\rangle_{A_2B}) + |\psi^-\rangle_{A_1}(\alpha_i|00\rangle_{A_2B} - \beta_i|11\rangle_{A_2B})\right\}$$

Then Alice performs Pauli transforms

$$|\phi^+\rangle \to I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad |\phi^-\rangle \to \sigma_Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

$$|\psi^+\rangle \to \sigma_X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad |\psi^-\rangle \to \sigma_Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$

and make correction to $|\phi^{(i)}\rangle_{A_2}$ Alice makes signature by using the procedure $sign_{pk}(s)$ and produces the quantum cheque $\chi = (id, s, r, \sigma, M, \{|\phi^{(i)}_{A_2}\})$ then publicly send through Abby to an arbitrary of the valid branches of the bank.

The final step is the verification *Vrfy scheme:* A valid bank branch after received the cheque, informs to the main branch in order to check the signature $Vrfy(\sigma, s)$. For this one uses namely the well-known Fredkin gate ([9], Picture 1). If the (id, s) or σ is invalid, the bank destroy the cheque, otherwise the bank continue the measurement in Hadamard basis $|\phi\rangle_B$. If the result is $|\phi^+\rangle$ or $|\phi^-\rangle$ the main branch communicates to the acting banch to continue. The acting branch perform transformation $|\phi^+\rangle \to I$ and $|\phi^-\rangle \to \sigma_Z$. The bank accepts the cheque if it passes the swap test then destroy it.

We remark that the quantum cheque is produced and used quite similar to the classical one. We propose therefore to use the multipartite quantum key distribution to make quantum cheques become quantum e-cheques of high secrecy [4]. Our main result is Theorem 3.1 stating that the quantum cheques could be with high secrecy online transfered from Alice to the acting bank branches by a code of multiparty quantum telecommunication problem of secret sharing with quantum public key distribution in unsecured channels possibly with eavesdroppers.

The feature of our approach is that (i) Alice does not need to go to a bank branch to do a transaction, but divides her data to a disjoint union of parts and connects with acting branches to send to each one part of her data, (ii) the bank can record the Alice's data only if all acting branches cooperate together and therefore (iii) they defense the origin of data and Alice prevents some dishonest branches to change the data, (iv) the cheques transfering is absolutely secured in nonsecured channels with eavesdroppers.

The paper is organised as follows. In Section 2 we review the e-cheque transfering in absolutely secured channels. In Section 3 we show the scheme of quantum cheque transfering in nonsecured channels. The paper finishes with some conclusion in Section 4 and acknowledgments in Section 5.

We separately consider the problem of e-cheque transfering in the situation of absolute secured channel in order to point out the main idea of e-chequering. The more complicated problem of e-cheque transfering in presence of eavesdroppers in a nonserured channel or dishonest participants will be separately considered in a subsequent paper.

The paper is devoted to this construction in the next Section 2 for reviewing quantum e-cheques transfering in absolutely secured channels and in Section 3 is devoted for the problem of transfering e-cheques in nonsecured channels where possible appearin some eavesdroppers and we finish the paper with some conclusion.

2. Quantum e-cheques as multiparty quantum secrete sharing

Consider the following *modified problem* for the situation when Alice does not send the quantum cheques via Abby, but could online connect with acting branches of a bank. To prevent the fact that some distrusted branches could change the cheque. The bank could discover the informations from the quantum cheques only if all acting branches cooperate togheter and in that case the other branches prevent the some untrusted branches to change the contents of the cheque. The quantum cheques in that case are what we call **e-cheques**.

Solution to this problem is the following scheme of code.

After the first step *Gen scheme*, in the second step *Sign Scheme* one keeps the same as in the previous section, only now, Alice divides the provided concatened information $k||id||r||M||i$ into n parts,

$D_1^{(i)},\dots,D_n^{(i)}$, where n is an appropriate number of branches in action. Then she produces the corresponding states by using a one-way function f to have $f(D_j^{(i)}) = \psi_j^{(i)}$, for all $j = 1,\dots,n$. Following the multiparty secret sharing, when the branches cooperate together and inform to the main branch, one discover the states $|\phi_j^{(i)}\rangle$

The following solution to the problem was shown in [5] *Procedure*, which is similar to the one in the 3 persons case by Cabello [3], following which the system states are changing as follows.

$$|\psi_i\rangle \longrightarrow |\psi_{ii}\rangle \longrightarrow |\psi_{iii}\rangle \longrightarrow |\psi_{iv}\rangle$$

Let us consider it in more details.

Transfer Step 1. Initialization of 3n qubits. For a fixed i, Alice uses $n+2$ qubits, named: $1,2,3,D_1 = D_1^{(i)},\dots,D_{n-1} = D_{n-1}^{(i)}$: qubits 1 and 2 are entangled in Bell state, qubits $3,D_1,\dots,D_{n-1}$ are entangled in GHZ state with $n-1$ acting bank branches: Branch 1, Branch 2, ..., Branch n-1, each has 2 entangled qubits $i+3, C_i, i = 1\dots,n-1$ namely in null state. Alice produces a Bell state measurement on qubit 1 and 2 and a Fourier measurement $\boxed{F_n}$ on n qubits $3,D_1,\dots,D_{n-1}$. Each of acting branch makes a Bell state Fourier measurement $\boxed{F_2}$ of entangled $i+3, C_i, i = 1\dots n-1$. At the end of this step 1, the system is in the state

$$|\psi_i\rangle = |0\dots0\rangle_{3D_1\dots D_{n-1}} \otimes |00\rangle_{12} \otimes |00\rangle_{4C_1} \otimes\dots\otimes |00\rangle_{n+2,C_{n-1}}$$

Transfer Step 2. Entangled Bell-state measurements. Alice sends each qubit D_i of her GHZ state out to each i^{th} acting bank branch of the other $n-1$ branches. The system is in the state

$$|\psi_{ii}\rangle = |AP\rangle_{3D_1\dots D_{n-1}} \otimes |BP\rangle_{1C_1} \otimes |CP\rangle_{2C_2} \otimes\dots\otimes |NP\rangle_{n+2,C_{n-1}}$$

Transfer Step 3. Secret Bell-state measurement. Next, Alice and each user performs a Bell-state Fourier measurement $\boxed{F_2}$ on the received qubit and one of their qubits. After these measurements the state of the system becomes

$$|\psi_{iii}\rangle = |AP\rangle_{3D_1\dots D_{n-1}} \otimes |AS\rangle_{2,3} \otimes |BS\rangle_{4,D_1} \otimes\dots\otimes |NS\rangle_{n+2,D_{n-1}},$$

where $|AP\rangle$ is n-qubit GHZ state of the standard orthonormal basis.

Transfer Step 4. Secret sharing. The $n-1$ acting branches send a qubit (the one they have not used) to Alice, and she performs a Fourier measurement $\boxed{F_n}$ to discriminate between the 2^n GHZ states, and publicly announces the result $|AP\rangle_{1C_1\dots C_{n-1}}$. After these measurements the state of the system becomes

$$|\psi_{iv}\rangle = |AP\rangle_{1C_1\dots C_{n-1}} \otimes |AS\rangle_{2,3} \otimes |BS\rangle_{4,D_1} \otimes\dots\otimes |NS\rangle_{n+2,D_{n-1}},$$

The result AP, and the result of their own secret measurement allow each legitimate acting branch to infer the first bit of Alices secret result AS. To find out the second bit of Alice's secret AS, all users (except Alice) must cooperate.

The 4 steps scheme of public key secret sharing distribution can be generalized to the case of two levels groupped secret sharing as illustrated in the work of A. Jaffe, Z.-W. Liu, and A. Wozniakowsk[6] in Figure 3:

After discovered the e-cheque, bank continue to procede the same procedure *Vrfy Scheme* as in the quantum cheques scheme above to verify the validity of the e-cheque and accept of destroy it.

3. Transfering Quantum E-Cheques in Nonsecured Channels

In the previous part, we considered the scheme of transfering quantum e-cheques such that the bank branches should cooperate together in order to prevent the dishonest branches could change the information, but we supposed that we could transfer in the absolutely secured channels. Let us now consider the senario where the transfering channels are unsecured and there maybe appear some eavesdroppers. Therefore Alice should check the channels before sending informations of cheques.

Theorem 3.1. *The quantum cheques could be with high secrecy electronically transfered from Alice to the acting bank branches by a code of multiparty quantum telecommunication problem of secret sharing with quantum public key distribution in unsecured channels possibly with eavesdroppers.*

Proof. The theorem is proved by the following

Procedure

$$|\psi_i\rangle \longrightarrow |\psi_{ii}\rangle \longrightarrow |\psi_{iii}\rangle \longrightarrow |\psi_{iv}\rangle$$

Let us consider it in more details.

Transfer Step 1. Checking channels and Initialization

Before sending the informations, Alice should check security of the channels. She uses $2(n-1)L$ qubits $\{q_i^{A_1}, \dots q_i^{A_{n-1}}, p_i^{A_1}, \dots p_i^{A_{n-1}}\}, i = 1, ..., L$ to check the channels, where each $q_i^{A_j}$ is randomly in one of the four states $|0\rangle, |1\rangle, |\tilde{0}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), |\tilde{1}\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$ and each $p_i^{A_j}$ is randomly in one of the two states $|\tilde{0}\rangle, |\tilde{1}\rangle$. For each $j = 1, \dots, n-1$, Alice sends the qubits $A_j, q_i^{A_j}, p_i^{A_j}$ to bank branch A_j in a secretly random manner i.e. the order, that Alice should keep for later use.

After Branch 1, ..., Baranch (n-1) confirm that they have received the qubits, Alice reveals the position of the checking qubits $\{q_i^{A_j}\}$ and asks every participant Branch 1, ..., Branch (n-1) to measure them in the appropriate bases (i.e., in those they have been prepared by Alice) and then announce her their results. Through a careful statistical analysis of the measurement outcomes for the checking qubits $\{q_i^{A_j}\}$, Alice is able to assess the error rate of secure sharing of the quantum channel. If it exceeds a predetermined threshold, she decides to abort the scheme. Otherwise, she proceeds the next step, see [7] for more detailed.

For a fixed i, Alice uses $n+2$ qubits, named: $1, 2, 3, D_1 = D_1^{(i)}, \dots, D_{n-1} = D_{n-1}^{(i)}$: qubits 1 and 2 are entangled in Bell state, qubits $3, D_1, \dots, D_{n-1}$ are entangled in GHZ state with $n-1$ acting bank branches: Branch 1, Branch 2, ..., Branch n-1, each has 2 entangled qubits $i+3, C_i, i = 1 \dots, n-1$ namely in null state. Alice produces a Bell state measurement on qubit 1 and 2 and a Fourier measurement $\boxed{F_n}$ on n qubits $3, D_1, \dots, D_{n-1}$. Each of acting branch makes a Bell state Fourier measurement $\boxed{F_2}$ of entangled $i+3, C_i, i = 1 \dots n-1$. At the end of this step 1, the system is in the state

$$|\psi_i\rangle = |0\dots 0\rangle_{3D_1\dots D_{n-1}} \otimes |00\rangle_{12} \otimes |00\rangle_{4C_1} \otimes \dots \otimes |00\rangle_{n+2,C_{n-1}}$$

Transfer Step 2. Entangled Bell-state measurements. Alice sends each qubit D_i of her GHZ state out to each i^{th} acting bank branch of the other $n-1$ branches. The system is in the state

$$|\psi_{ii}\rangle = |AP\rangle_{3D_1\dots D_{n-1}} \otimes |BP\rangle_{1C_1} \otimes |CP\rangle_{2C_2} \otimes \dots \otimes |NP\rangle_{n+2,C_{n-1}}$$

Transfer Step 3. Secret Bell-state measurement. Next, Alice and each user performs a Bell-state Fourier measurement $\boxed{F_2}$ on the received qubit and one of their qubits. After these measurements the state of the system becomes

$$|\psi_{iii}\rangle = |AP\rangle_{3D_1\dots D_{n-1}} \otimes |AS\rangle_{2,3} \otimes |BS\rangle_{4,D_1} \otimes \dots \otimes |NS\rangle_{n+2,D_{n-1}},$$

where $|AP\rangle$ is n-qubit GHZ state of the standard orthonormal basis.

Transfer Step 4. Checking Security and Secret sharing. Alice appoint one of the branches, namely the Branch 1 as the leader branch and she reveals Branch 1 the position of C_1, C_2. Before the branches 1, ..., n-1 sending the qubits to Alice, she do again checking the channels. She asks branches to measure the remaining entangled qubits $3+j, p_i^{A_j}$ in Bell states and publish the results. If Alice discovers that the error rate exited a predetermined threshold, she discards the transfering cheque process. Otherwise, she knows that branches are not as cheated and then asks leader branch 1 to make the state

$$|\phi_{i_1,j_1,\dots,i_{n-1},j_{n-1}}\rangle_{C_1,C_2} = \xi_{i_1,j_1,\dots,i_{n-1},j_{n-1}}|00\rangle + \zeta_{i_1,j_1,\dots,i_{n-1},j_{n-1}}|01\rangle +$$

$$\eta_{i_1,j_1,\dots,i_{n-1},j_{n-1}}|10\rangle + \gamma_{i_1,j_1,\dots,i_{n-1},j_{n-1}}|11\rangle,$$

the coefficients are known from measurement public results, see [7] for more detailed.

The $n-1$ acting branches send a qubit (the one they have not used) to Alice, and she performs a Fourier measurement $\boxed{F_n}$ to discriminate between the 2^n GHZ states, and publicly announces the result

$|AP\rangle_{1C_1\ldots C_{n-1}}$. After these measurements the state of the system becomes

$$|\psi_{iv}\rangle = |AP\rangle_{1C_1\ldots C_{n-1}} \otimes |AS\rangle_{2,3} \otimes |BS\rangle_{4,D_1} \otimes \cdots \otimes |NS\rangle_{n+2,D_{n-1}},$$

The result AP, and the result of their own secret measurement allow each legitimate acting branch to infer the first bit of Alices secret result AS. To find out the second bit of Alice's secret AS, all users (except Alice) must cooperate.

The proof therefore is achieved. □

4. Conclusion

We show that the quantum cheques can be electronically transfered with high secrecy by a code of multiparty quantum telecommunication problem of secret sharing with quantum public key distribution in nonsecured channel.

5. Acknowledgments

We thank Prof. S. R. Moulick and Prof. P. K. Panigrahi for valuable comments and for reminding the authors about mediator.

References

[1] Aaronson, S.*Quantum copy-protection and quantum money.* In: Proceedings of 24th Annual IEEE Conference on Computational Complexity (CCC), 2009, pp. 229242. IEEE (2009)

[2] Bennett, C.H., Brassard, G., Breidbart, S., Wiesner, S., *Quantum cryptography, or unforgeable subway tokens.* In: Advances in Cryptology, pp. 267275. Springer (1983)

[3] A. Cabello, *Multiparty key distribution and secret sharing based on entanglement swapping*, arXiv:quant-ph/0009025v1, 2000.

[4] D. N. Diep, *Multiparty quantum telecommunication using quantum Fourier transforms*, arXiv: 1705.02608[quant-ph]

[5] D. N. Diep, Quantum E-cheques, arXiv:1705.10083 [quant-ph], 2017.

[6] A. Jaffe, Z.-W. Liu, and A. Wozniakowsk, *Holographic Software for Quantum Networks*, https://www.researchgate.net/publication/301818865

[7] Z.-X. Man, Y.-J. Xia, N. B. An, *Quantum state sharing of an arbitrary multiqubit state using nonmaximally entangled GHZ states*, Eur. Phys. J. D 42, 333340 (2007)

[8] Mosca, M., Stebila, D. Quantum coins. Error Correct. Codes Finite Geom. Cryptogr. 523, 3547 (2010)

[9] S. R. Moulick, P. K. Panigrahi, *Quantum cheques*, Quantum Inf Process **15**(2016), 2475-2486.

[10] Wiesner, S., *Conjugate coding.* ACM Sigact News 15(1), 7888 (1983)

[1] Instittute of Mathematics, Vietnam Academy of Science and Technology, 18 Hoang Quoc Viet road, 10307 Hanoi, Vietnam

E-mail address: dndiep@math.ac.vn

[2] Thang Long Institute of Mathematics and Applied Sciences, Thang Long University, Nghiem Xuan Yem road, Hoang Mai district, Ha Noi, Vietnam