Quantum Inf Process (2017) 16:312
DOI 10.1007/s11128-017-1762-0

Experimental realization of quantum cheque using a five-qubit quantum computer

Bikash K. Behera[1] · Anindita Banerjee[2] · Prasanta K. Panigrahi[1]

Received: 9 July 2017 / Accepted: 1 November 2017

Abstract Quantum cheques could be a forgery-free way to make transaction in a quantum networked banking system with perfect security against any no-signalling adversary. Here, we demonstrate the implementation of quantum cheque, proposed by Moulick and Panigrahi (Quantum Inf Process 15:2475–2486, 2016), using the five-qubit IBM quantum computer. Appropriate single qubit, CNOT and Fredkin gates are used in an optimized configuration. The accuracy of implementation is checked and verified through *quantum state tomography* by comparing results from the theoretical and experimental density matrices.

Keywords IBM quantum experience · Quantum cheque · Quantum state tomography

1 Introduction

Currency bonds, when printed on textile or rag paper, can be counterfeited by any adversary party if it gets access to unlimited computational sources. The quantum analog of the same is physically impossible to copy due to the "No Cloning Theo-

✉ Bikash K. Behera
bkb13ms061@iiserkol.ac.in

Anindita Banerjee
aninditabanerjee.physics@gmail.com

Prasanta K. Panigrahi
pprasanta@iiserkol.ac.in

1 Department of Physical Sciences, Indian Institute of Science Education and Research Kolkata, Mohanpur, West Bengal 741246, India

2 Department of Physics and Center for Astroparticle Physics and Space Science, Bose Institute, Block EN, Sector V, Kolkata 700091, India

Published online: 12 November 2017

rem" [1]. Wiesner's quantum money [2,3] has led to development of a quantum key distribution scheme, known as BB84 protocol [4], to send messages with perfect security. Wiesner's original scheme was later broken [5–7]. However, Aaronson showed its existence by proposing a quantum copy protection scheme [8], which again was broken by Lutomirski et al. [9]. New versions were then introduced by Farhi et al. [10] and Aaronson et al. [11]. Subsequently, a scheme of quantum coins was developed by Mosca and Stebila [12], based on blind quantum computation requiring a communicating bank for verification purposes.

The idea of quantum cheques was put forward by Moulick and Panigrahi [13], which utilized quantum states to fabricate currency bonds. The proposed scheme was perfectly secure against any no-signalling adversary based on fundamental laws of quantum information. The quantum cheque involved a trusted bank providing every account holder with a valid quantum cheque book to issue cheques that can be verified by the main bank or any of its acting branches.

Establishing long distance quantum communication networks [14,15] is an active area of research, where a quantum cheque scheme can be potentially used as an alternate for *e-Payment Gateways* in the field of *e-commerce*. It can also be considered as the quantum analog of *Electronic Data Interchange* (EDI) [16]. In this scheme, efficient transactions can be performed by storing quantum states in computers or smart cards, equipped with quantum memories [17,18]. Without quantum memory, the transactions can be streamed over the quantum internet [19,20]. The protocol can run in real time, where the account holder physically goes to the Bank, collects a quantum cheque book and then prepares a quantum cheque and issues to a vendor. The vendor then communicates the quantum cheque to the Bank and withdraws money after a successful verification of the cheque. Recently, practical unforgeable quantum money has found experimental verification [21,22]. The experimental demonstration therefore paves the way for designing of physical devices for this purpose.

Here, we make use of the free web-based interface, *IBM Quantum Experience* (IBM QE) [23], to experimentally demonstrate the quantum cheque transaction [13]. The platform uses Python *Application Programming Interface* (API) and *Software Development Kit* (SDK) [24], which has enabled easy writing of codes and running them on quantum processors. With fast access to the results of an experiment, the IBM QE users can communicate and discuss results with IBM community. It permits a user easy connectivity to this cloud [25] based 5-qubit quantum computer, using which a number of quantum algorithms [26–29] and quantum computational tasks [30] have already been performed. Test of Leggett–Garg [31] and Mermin inequality [32], quantum teleportation of an unknown single qubit [33] and two-qubit state [34] have been reported. Entanglement-assisted invariance [35], non-Abelian braiding of surface code defects [36], and entropic uncertainty and measurement reversibility [37] have been illustrated. A comparison between two architectures for quantum computation [38] and nondestructive discrimination of Bell states [39] have also been experimentally performed. In this note, we explicate experimental realization of quantum cheque transaction by implementing the scheme on IBM interface and find the accuracy of quantum state preparation through quantum state tomography.

The paper is organized as follows. Section 2 describes the implementation of quantum gates, e.g. CNOT and Fredkin gates, in order to design quantum circuits for experimental realization of quantum cheque. Section 3 explicates the concept of a quantum cheque, following which the implementation is shown on IBM Interface. Section 5 reveals the accuracy of implementation by performing quantum state tomography. Finally, in Sect. 6, we conclude by summarizing and pointing out future directions of our work.

2 Designing gates and some protocols on IBM QE

For the implementation of a quantum cheque, one requires Hadamard (H), CNOT gate, the Pauli gates (X, Y and Z) and phase gates (S, $S^\dagger$, T and $T^\dagger$). Combining some of these gates, a fredkin gate can be constructed, which is used for the verification purposes of a quantum cheque. It is to be noted that CNOT gate is not accessible to all five qubits on the interface of IBM, because of certain restrictions on the qubits. Protocol I, depicted in Fig. 1, is used to construct CNOT gate in any order between two qubits. Similarly, Protocol II, depicted in Fig. 2, is used to swap any two qubits on IBM interface.

3 Quantum cheque

A quantum cheque scheme is composed of three algorithms, Gen, Sign and Verify. Gen algorithm produces a "cheque book" and a key for the customer, who issues a cheque. Sign algorithm creates a quantum cheque state, QC, and Verify algorithm checks the validity of a cheque. A quantum cheque has mainly three properties, Verifiability, i.e. it can be verified by a Bank's main branch or any of its acting branches, Nonrepudiation, i.e. after issuing a cheque, a customer must not be able to disclaim it, and Unforgeability, i.e. a quantum cheque can not be fabricated or it cannot be reused.

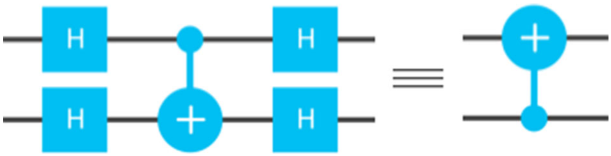


Fig. 1 **Protocol I**. Two equivalent quantum circuits showing implementation of CNOT gate in any order between two qubits on IBM interface

Fig. 2 **Protocol II**. Positioning of three CNOT gates for qubit swapping

3.1 The quantum cheque scheme

The quantum cheque scheme can be described by considering three parties, Alice, Bob and Bank. Here, the Bank is denoted as the main branch, which can have several branches securely connected by a classical channel. In this protocol, only Alice and Bank are considered to be trusted parties and not necessarily the branches. After a cheque is issued by Alice, Bob goes to Bank or any of its branches to withdraw money.

The following three schemes are followed for a successful quantum cheque transaction.

1. *Gen Algorithm* Initially, a shared key, k, is prepared by Alice and the Bank. Then, Alice gives her public key, pk, to the Bank and collects her Private Key, sk.

The Bank prepares a set of m number of GHZ states

$$\left|\phi^{(i)}\right\rangle_{\mathrm{GHZ}} = \frac{1}{\sqrt{2}}\left(\left|0^{(i)}\right\rangle_{A_1}\left|0^{(i)}\right\rangle_{A_2}\left|0^{(i)}\right\rangle_{B} + \left|1^{(i)}\right\rangle_{A_1}\left|1^{(i)}\right\rangle_{A_2}\left|1^{(i)}\right\rangle_{B}\right) \tag{1}$$

where $1 \leq i \leq m$, along with the respective unique serial number $s \in \{0, 1\}^n$. From every GHZ entangled state, the Bank gives two qubits, named $|\phi\rangle_{A_1}$ and $|\phi\rangle_{A_2}$, and the serial number to Alice, while keeping the third qubit, $|\phi\rangle_B$, and other information, secretly in a database.

Here, $\{|\phi^{(i)}\rangle_{\mathrm{GHZ}}\}_{i=1:m}$ stands for $\{|\phi^{(1)}\rangle_{\mathrm{GHZ}}, |\phi^{(2)}\rangle_{\mathrm{GHZ}}, \ldots, |\phi^{(m)}\rangle_{\mathrm{GHZ}}\}$.

At the end, Alice possesses $(id, pk, sk, k, s, \{|\phi^{(i)}\rangle_{A_1}, |\phi^{(i)}\rangle_{A_2}\}_{i=1:m})$, and the Bank carries $(id, pk, k, s, \{|\phi^{(i)}\rangle_B\}_{i=1:m})$.

2. *Sign Algorithm* Alice prepares a random number by using a random number generation procedure $r \leftarrow U_{\{0,1\}^L}$ to *sign* a cheque of amount M and creates a n-qubit state by using the following one-way function [40,41],

$$|\psi_{\mathrm{alice}}\rangle = f(k||id||r||M),$$

where k and id, are, respectively, the secret key and the identity of Alice. The symbol "||" concatenates two bit strings.

Alice also prepares m states $\{|\psi_M^{(i)}\rangle\}_{i=1:m}$ corresponding to the amount M, using the one-way function $g : \{0, 1\}^* \times |0\rangle \rightarrow |\psi\rangle$, as

$$|\psi_M^{(i)}\rangle = g(r||M||i).$$

Subsequently, Alice encodes [42] $|\psi_M^{(i)}\rangle$ with the entangled qubit, $|\phi^{(i)}\rangle_{A_1}$ after which she performs a Bell measurement on her first two qubits as shown in Fig. 3.

The state of the four qubit entangled system can be written in the following form

$$\begin{aligned}\left|\phi^{(i)}\right\rangle = & \left|\psi_M^{(i)}\right\rangle \otimes |\phi\rangle_{\mathrm{GHZ}} \\ = & \tfrac{1}{2}\Big\{\left|\Psi^+\right\rangle_{A_1}\left(\alpha_i\,|00\rangle_{A_2B} + \beta_i\,|11\rangle_{A_2B}\right) \\ & + \left|\Psi^-\right\rangle_{A_1}\left(\alpha_i\,|00\rangle_{A_2B} - \beta_i\,|11\rangle_{A_2B}\right)\end{aligned}$$

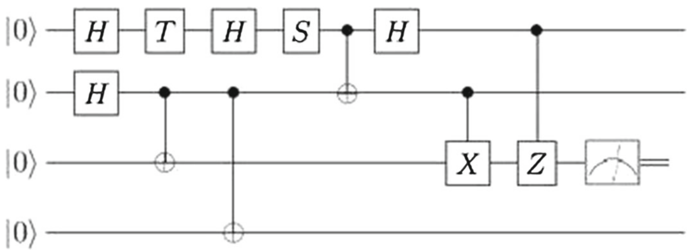
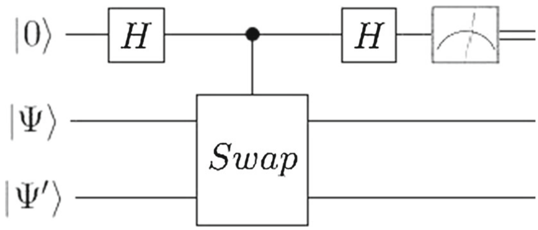


Fig. 3 Depicting the quantum circuit used to generate a quantum cheque state

Fig. 4 Quantum circuit for performing swap test on the two states $|\Psi\rangle$ and $|\Psi'\rangle$



$$+\left|\Phi^{+}\right\rangle_{A_1}\left(\beta_i\,|00\rangle_{A_2B}+\alpha_i\,|11\rangle_{A_2B}\right)$$
$$+\left|\Phi^{-}\right\rangle_{A_1}\left(\beta_i\,|00\rangle_{A_2B}-\alpha_i\,|11\rangle_{A_2B}\right)\Big\} \tag{2}$$

where $|\Psi^{+}\rangle$, $|\Psi^{-}\rangle$, $|\Phi^{+}\rangle$ and $|\Phi^{-}\rangle$ denote four Bell states.

Now, Alice applies an appropriate Pauli gate operation on her qubit $|\phi^{(i)}\rangle_{A_2}$, according to the Bell state measurement outcomes:

$$|\Psi^{+}\rangle \rightarrow I \qquad\qquad |\Psi^{-}\rangle \rightarrow Z$$
$$|\Phi^{+}\rangle \rightarrow X \qquad\qquad |\Phi^{-}\rangle \rightarrow Y$$

Figure 3 depicts the encoding procedure of quantum cheque, which is to be repeated m times.

Alice then uses sign algorithm to sign the serial number s as $\sigma \leftarrow \mathrm{Sign}_{sk}(s)$ and generates a quantum cheque

$$\mathrm{QC} = (id, s, r, \sigma, M, \{|\phi^{(i)}\rangle_{A_2}\}_{i=1:m}, |\psi_{\mathrm{alice}}\rangle)$$

for Bob to encash.

Swap Test The swap test is depicted in Fig. 4, where the measurement of ancilla (first qubit) on a computational basis yields zero if the two states $|\Psi\rangle$ and $|\Psi'\rangle$ are equal. In this case, swap test is said to be successful. However, if the two states are different, then the measurement of ancilla yields both $|0\rangle$ and $|1\rangle$ each associated with some probability. For $\langle\Psi|\Psi'\rangle \geq \lambda$, the swap test is successful with probability $\frac{1+\lambda^2}{2}$ and unsuccessful with probability $\frac{1-\lambda^2}{2}$. It is evident that, for the same input states, the swap test is successful with probability 1, and for different outputs, it is successful with probability less than 1. The efficiency of this test can be amplified by repeating it a large number of times.

3. *Verify algorithm* In the verification process, Bob produces the quantum cheque QC at any of the acting branches of the Bank. The branch communicates with the Bank (main branch) to check the validity of the (id, s) pair, and a verification is run by using $Vrfy_{pk}(\sigma, s)$. As described below, the Bank proceeds with the verification process if it finds (id, s) and σ to be valid, otherwise cancels the quantum cheque transaction.

The Bank then measures its qubit, $|\phi_B\rangle$ in Hadamard basis to get $|+\rangle$ or $|-\rangle$ as output and conveys the results to the acting branch. The branch applies the appropriate Pauli gate operation on $|\phi^{(i)}\rangle_{A_2}$ to retrieve the unknown state $|\psi_M^{(i)}\rangle$.

$$|+\rangle \rightarrow I \qquad\qquad |-\rangle \rightarrow Z$$

A similar procedure is followed m times to get m unknown states $\{|\psi_M^{(i)}\rangle\}_{i=1:m}$. The Bank generates $|\psi'_{\text{alice}}\rangle = f(k||id||r||M)$, and $\{|\psi_M^{;(i)}\rangle\}_{i=1:m} = \{g(r||M||i)\}_{i=1:m}$ by using these one-way functions and then performs a swap test on $m+1$ set of states, $\{|\psi_{\text{alice}}\rangle, |\psi'_{\text{alice}}\rangle\}$, and $\{|\psi_M^{(i)}\rangle, |\psi_M^{;(i)}\rangle\}_{i=1:m}$.

The cheque is accepted if the swap test is successful, i.e. if $\langle\psi_{\text{alice}}|\psi'_{\text{alice}}\rangle \geq \lambda_1$ and $\{\langle\psi_M^{(i)}|\psi_M^{;(i)}\rangle \geq \lambda_2\}_{i=1:m}$, where λ_1 and λ_2 are constants fixed by the Bank. Else, the branch terminates the transaction.

4 Implementation of quantum cheque at IBM QE

The IBM quantum circuit for generating a quantum cheque state is depicted in Fig. 5. It is equivalent to the quantum circuit shown in Fig. 3. Though these two figures appear to be different, their equivalency can be checked by using Protocol I, Protocol II and the concept of optimization of circuit. In Fig. 5, the first three qubits are in possession of Alice, the Bank contains the fifth qubit, and the fourth qubit remains unused. Alice uses one of her entangled qubit (second qubit), $|\phi^{(i)}\rangle_{A_1}$, provided by Bank, to encode the unknown state $|\psi_M^{(i)}\rangle$. Here, this unknown state cannot be generated by using the one-way function, "g" (Sect. 3), since we model only the quantum aspect, and for simplicity only assume the g spits out a description of the following state that is known to the preparation device, but unknown to anybody else as [33]

$$|\psi_M^{(i)}\rangle = \cos(\pi/8)|0\rangle + \sin(\pi/8)|1\rangle \tag{3}$$

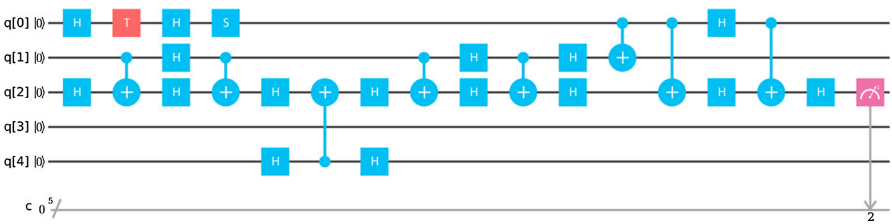


Fig. 5 IBM quantum circuit used to generate the quantum cheque state

Table 1 Results of the outcome of the quantum cheque state, depicted in Fig. 5, measured in computational basis

For quantum cheque generation		
Number of shots	Probability of $\|0\rangle$	Probability of $\|1\rangle$
Run 1 (1024)	0.741	0.249
Run 2 (4096)	0.766	0.234
Run 3 (8192)	0.755	0.245
Simulation 1 (1024)	0.848	0.152
Simulation 2 (4096)	0.856	0.144
Simulation 3 (8192)	0.856	0.144

The results are obtained by both running and simulating the experiment with 1024, 4096 and 8192 number of shots

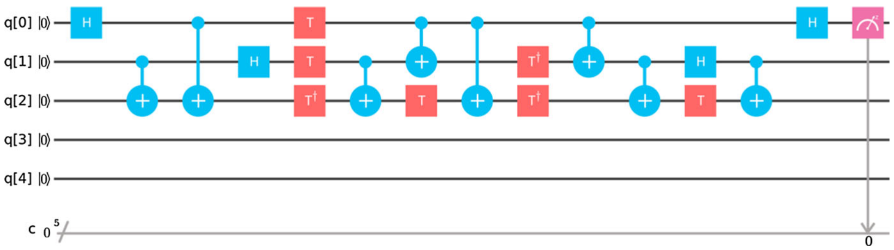


Fig. 6 IBM quantum circuit used to verify the quantum cheque. It is to be noted that a set of two states are to be taken on the second and the third qubit of the above circuit for checking swap test

It can be computed by operating H, T, H and S gates sequentially on $|0\rangle$. As this state is now split between Alice's qubit (third qubit) and Bank's qubit (fifth qubit), measuring the third qubit in computational basis, it is expected to have $|0\rangle$ with probability ≈ 0.85 and $|1\rangle$ with probability ≈ 0.15. The experimental results are tabulated in Table 1.

The encoding procedure (as described in Sect. 3) should be done m times by using m similar quantum circuits (Fig. 5). Through the IBM cloud, it is not possible to create n-qubit quantum state by using a one-way function, "f" (Sect. 3). So, we have taken two initial states $|0\rangle$ and $|0\rangle$ for comparison test.

The quantum circuits implemented on IBM interface, for quantum cheque verification, are illustrated in Fig. 6, which is equivalent to the circuit shown in Fig. 4. In this case, both the initial states (second qubit and third qubit) are taken as $|0\rangle$. (See Fig. 6.) It is expected to have $|0\rangle$ with probability 1, after measuring the ancilla qubit (first qubit) in computational basis. The experimental results are illustrated in Table 2.

Comparing run result and simulated result, shown in Tables 1 and 2, run result is found to be less accurate than the simulated result. It is evident that application of a large number of gates increases decoherence of a quantum state and produces more noise in the system. Decoherence and noise due to gates are the key disadvantages for realizing the implementation of a quantum cheque with exact accuracy.

Table 2 Information about the ancilla state, depicted in Fig. 6, when it is measured in computational basis

For quantum cheque verification		
Number of shots	Probability of $\|0\rangle$	Probability of $\|1\rangle$
Run 1 (1024)	0.813	0.188
Run 2 (4096)	0.839	0.161
Run 3 (8192)	0.846	0.154
Simulation 1 (1024)	1.000	0.000
Simulation 2 (4096)	1.000	0.000
Simulation 3 (8192)	1.000	0.000

The experiment has been performed with 1024, 4096 and 8192 number of shots. Both run and simulated results are illustrated

5 Quantum state tomography

We now proceed to carry out state tomography to check how well the quantum states are prepared in our experiment. We mainly consider two states, quantum cheque state ($|\phi^{(i)}\rangle_{A_2}$), which is to be stored in the quantum cheque, and ancilla state, used in swap test (See Sect. 3). In this process, by comparing both the theoretical and experimental density matrices of a quantum state, the accuracy of implementation can be tested.

State tomography can be explained through a single qubit quantum state, $|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$. The theoretical and experimental density matrices of the given state are given by equations 4 and 5, respectively.

$$\rho^T = |\Psi\rangle\langle\Psi|, \tag{4}$$

and

$$\rho^E = \frac{1}{2}(I + \langle X\rangle X + \langle Y\rangle Y + \langle Z\rangle Z) \tag{5}$$

Here, $\langle O\rangle = tr(|\Psi\rangle\langle\Psi|O)$, where $O = X, Y$, and Z. This expectation value can be obtained by rotating the quantum state along O axis and then measuring in computational basis. This can be evaluated as, $\langle O\rangle = P(0) - P(1)$, where $P(0)$ and $P(1)$ are the probabilities of outcomes 0 and 1, respectively.

The theoretical (ρ_x^T,) and experimental (ρ_x^{ER}, ρ_x^{ES}) density matrices (both for run result and simulated result) of quantum cheque state ($x = q$) (Fig. 7) and ancilla state ($x = a$) (Fig. 8) are given below.

$$\rho_q^T = \begin{bmatrix} 0.850 & 0.350 \\ 0.350 & 0.150 \end{bmatrix}$$
$$\rho_q^{ER} = \begin{bmatrix} 0.760 & 0.043 \\ 0.043 & 0.240 \end{bmatrix} + i \begin{bmatrix} 0.000 & -0.027 \\ 0.027 & 0.000 \end{bmatrix}$$
$$\rho_q^{ES} = \begin{bmatrix} 0.852 & 0.008 \\ 0.008 & 0.148 \end{bmatrix} + i \begin{bmatrix} 0.000 & -0.001 \\ 0.001 & 0.000 \end{bmatrix}$$

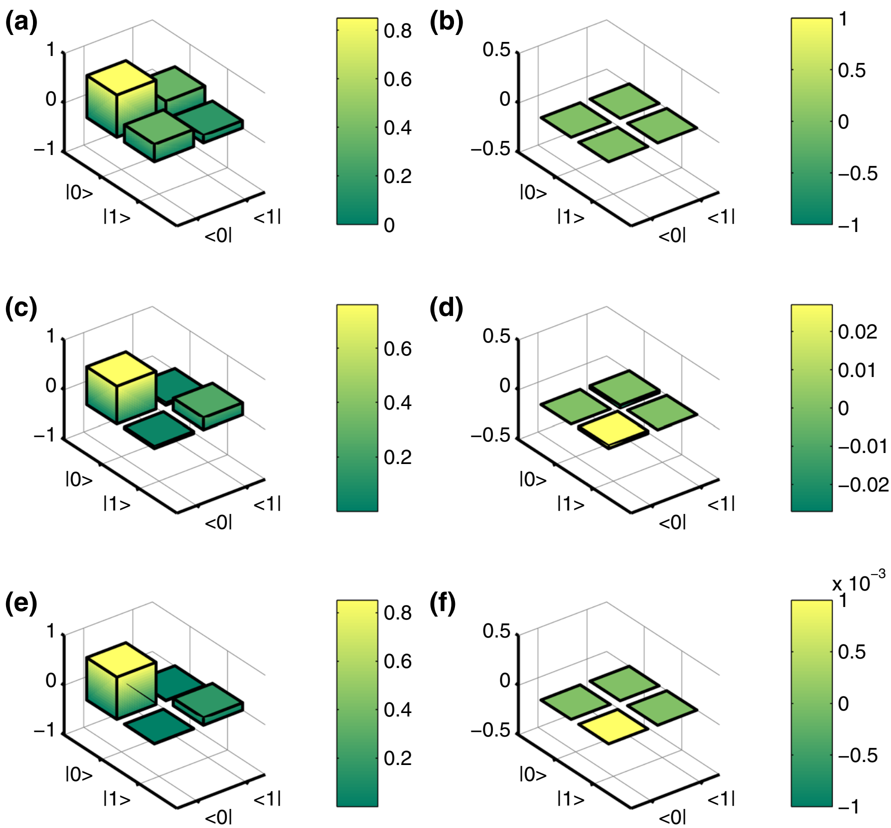


Fig. 7 **Quantum cheque generation**: Real (left) and imaginary (right) parts of the reconstructed theoretical (**a**, **b**), run (**c**, **d**) and simulated (**e**, **f**) density matrices for the quantum cheque state

$$\rho_a^T = \begin{bmatrix} 1.000 & 0.000 \\ 0.000 & 0.000 \end{bmatrix}$$

$$\rho_a^{ER} = \begin{bmatrix} 0.846 & 0.054 \\ 0.054 & 0.154 \end{bmatrix} + i \begin{bmatrix} 0.000 & 0.062 \\ -0.062 & 0.000 \end{bmatrix}$$

$$\rho_a^{ES} = \begin{bmatrix} 1.000 & 0.009 \\ 0.009 & 0.000 \end{bmatrix} + i \begin{bmatrix} 0.000 & -0.003 \\ 0.003 & 0.000 \end{bmatrix}$$

It is to be noted that the above experimental density matrices are calculated for running and simulating the experiment 8192 times. For other number of shots (1024 and 4096), similar procedure can be applied to obtain the corresponding density matrices. By comparing the run, simulated and theoretical density matrices, it can be concluded that the simulated result provides more accurate information, about the quantum state, as compared to the run results, which is already mentioned in Sect. 4.

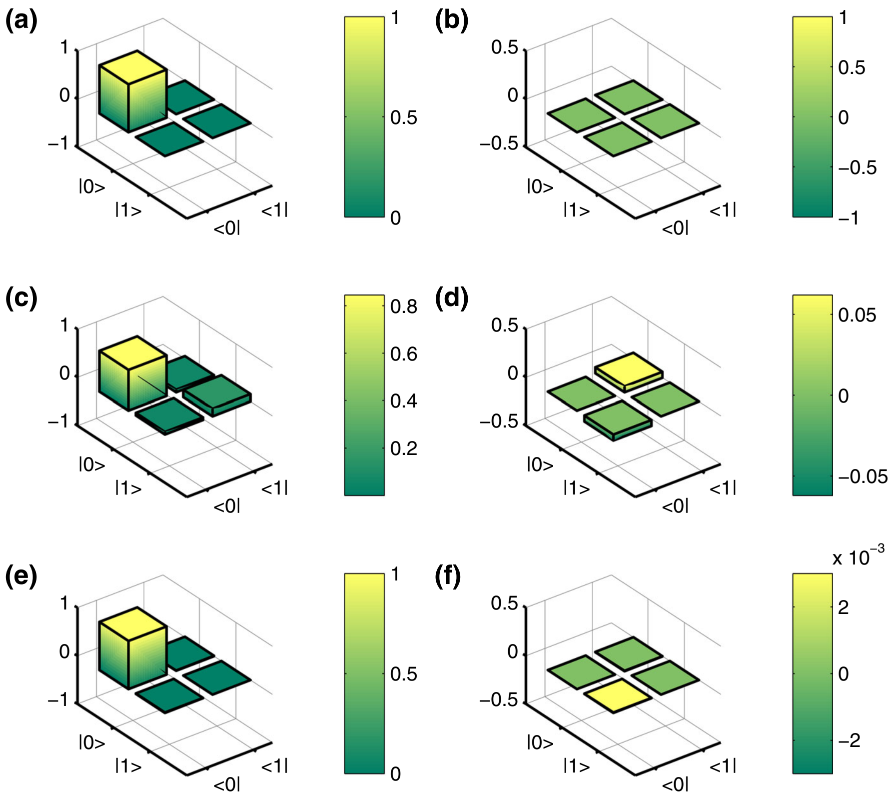


Fig. 8 **Quantum cheque verification**: Real (left) and imaginary (right) parts of the reconstructed theoretical (**a**, **b**), run (**c**, **d**) and simulated (**e**, **f**) density matrices for the ancilla state

6 Conclusion

To conclude, we have demonstrated here an experimental procedure of quantum cheque transaction in a quantum networked environment. Fredkin gate has been constructed, by using single qubit and CNOT gates, for verification of quantum cheque. The quantum state tomography has been performed to check the accuracy of the implementation. It is observed that the quantum cheque transaction has been carried out with a high fidelity.

Acknowledgements B.K.B. is financially supported by DST Inspire Fellowship. We thank Subhayan Roy Moulick (Oxford) for his original contribution to the concept of quantum cheque. We are extremely grateful to IBM team and IBM QE project. We thank IBM community for helpful suggestions regarding circuit construction. The discussions and opinions developed in this paper are only those of the authors and do not reflect the opinions of IBM or IBM QE team.

References

1. Wooters, W., Zurek, W.: Quantum no-cloning theorem. Nature **299**, 802 (1982)

2. Wiesner, S.: Conjugate coding. ACM Sigact News **15**(1), 78–88 (1983)
3. Bennett, C.H., Brassard, G., Breidbart, S., Wiesner, S.: Quantum cryptography, or unforgeable subway tokens. In: Chaum, D., Rivest, R.L., Sherman, A.T. (eds.) Advances in Cryptology, pp. 267–275. Springer (1983)
4. Bennett, C.H., Brassard, G.: Quantum cryptography: public key distribution and coin tossing. In: Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing, pp. 175–179. Bangalore, India (1984)
5. Lutomirski, A.: An online attack against Wiesner's quantum money. arXiv:1010.0256 (2010)
6. Molina, A., Vidick, T., Watrous, J.: Optimal counterfeiting attacks and generalizations for Wiesners quantum money. In: Theory of Quantum Computation, Communication, and Cryptography, 2012, pp. 45–64. Springer (2013)
7. Brodutch, A., Nagaj, D., Sattath, O., Unruh, D.: An adaptive attack on Wiesner's quantum money. arXiv:1404.1507 (2014)
8. Aaronson, S.: Quantum copy-protection and quantum money. In: Proceedings of 24th Annual IEEE Conference on Computational Complexity (CCC), 2009, pp. 229–242. IEEE (2009)
9. Lutomirski, A., Aaronson, S., Farhi, E., Gosset, D., Hassidim, A., Kelner, J., Shor, P.: Breaking and making quantum money: toward a new quantum cryptographic protocol. arXiv:0912.3825 (2009)
10. Farhi, E., Gosset, D., Hassidim, A., Lutomirski, A., Shor, P.: Quantum money from knots. In: Proceedings of the 3rd Innovations in Theoretical Computer Science Conference, pp. 276–289. ACM (2012)
11. Aaronson, S., Christiano, P.: Quantum money from hidden subspaces. In: Proceedings of the 44th Annual ACM Symposium on Theory of Computing, pp. 41–60. ACM (2012)
12. Mosca, M., Stebila, D.: Quantum coins. Error Correct. Codes Finite Geom. Cryptogr. **523**, 35–47 (2010)
13. Moulick, S.R., Panigrahi, P.K.: Quantum cheques. Quantum Inf. Process. **15**, 2475–2486 (2016)
14. Biham, E., Huttner, B., Mor, T.: Quantum cryptographic network based on quantum memories. Phys. Rev. A **54**, 2651 (1996)
15. Duan, L.M., Monroe, C.: Quantum networks with trapped ions. Rev. Mod. Phys. **82**, 1209 (2010)
16. Anderson, R.: Security Engineering. Wiley, New York (2008)
17. Trugenberger, C.A.: Probabilistic quantum memories. Phys. Rev. Lett. **87**, 067901 (2001)
18. Simon, C., Afzelius, M., Appel, J., Boyer de la Giroday, A., Dewhurst, S., Gisin, N., Hu, C., Jelezko, F., Kröll, S., Müller, J., et al.: Quantum memories. Eur. Phys. J. D **58**, 1–22 (2010)
19. Munro, W., Stephens, A., Devitt, S., Harrison, K., Nemoto, K.: Quantum communication without the necessity of quantum memories. Nat. Photonics **6**, 777–781 (2012)
20. Kimble, H.: The quantum internet. Nature **453**(7198), 1023–1030 (2008)
21. Bartkiewicz, K., Černoch, A., Chimczak, G., Lemr, K., Miranowicz, A., Nori, F.: Experimental quantum forgery of quantum optical money. npj Quantum Inf. **3**(1), 7 (2017)
22. Bozzio, M., Orieux, A., Vidarte, L.T., Zaquine, I., Kerenidis, I., Diamanti, E.: Experimental demonstration of practical unforgeable quantum money. arXiv:1705.01428 (2017)
23. IBM Quantum Experience. https://www.research.ibm.com/ibm-q/
24. Quantum computing gets an API and SDK. https://developer.ibm.com/dwblog/2017/quantum-computing-api-sdk-david-lubensky/
25. Castelvecchi, D.: IBM's quantum cloud computer goes commercial. Nat. News **543**, 159 (2017)
26. Shor, P.: Algorithms for quantum computation: discrete logarithms and factoring. In: Proceeding SFCS '94 Proceedings of the 35th Annual Symposium on Foundations of Computer Science, pp. 124–134. IEEE (1994)
27. Grover, L.K.: A fast quantum mechanical algorithm for database search. In: Proceeding STOC '96 Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing, pp. 212–219. ACM (1996)
28. Ambainis, A.: Quantum search algorithms. In: Fenner, S. (ed.) Newsletter ACM SIGACT News, vol. 35 (2), pp. 22–35. ACM (2004)
29. Mosca, M.: Quantum algorithms. In: Meyers, R.A. (ed.) Computational Complexity, pp. 2303–2333. Springer, New York (2012)
30. Devitt, S.J.: Performing quantum computing experiments in the cloud. Phys. Rev. A **94**(3), 032329 (2016)

31. Huffman, E., Mizel, A.: Violation of noninvasive macrorealism by a superconducting qubit: implementation of a Leggett–Garg test that addresses the clumsiness loophole. Phys. Rev. A **95**(3), 032131 (2017)
32. Alsina, D., Latorre, J.I.: Experimental test of Mermin inequalities on a five-qubit quantum computer. Phys. Rev. A **94**(1), 012314 (2016)
33. Fedortchenko, S.: A quantum teleportation experiment for undergraduate students. arXiv:1607.02398 (2016)
34. Sisodia, M., Shukla, A., Thapliyal, K., Pathak, A.: Design and experimental realization of an optimal scheme for teleportion of an n-qubit quantum state. arXiv:1704.05294 (2017)
35. Deffner, S.: Demonstration of entanglement assisted invariance on IBM's quantum experience. arXiv:1609.07459 (2017)
36. Wootton, J.R.: Demonstrating non-Abelian braiding of surface code defects in a five qubit experiment. Quantum Sci. Technol. **2**(1), 015006 (2017)
37. Berta, M., Wehner, S., Wilde, M.M.: Entropic uncertainty and measurement reversibility. New J. Phys. **18**(7), 073004 (2016)
38. Linke, N.M., Maslov, D., Roetteler, M., Debnath, S., Figgatt, C., Landsman, K.A., Wright, K., Monroe, C.: Experimental comparison of two quantum computing architectures. Proc. Natl. Acad. Sci. **114**(13), 3305–3310 (2017)
39. Sisodia, M., Shukla, A., Pathak, A.: Experimental realization of nondestructive discrimination of Bell states using a five-qubit quantum computer. arXiv:1705.00670 (2017)
40. Gottesman, D., Chuang, I.: Quantum digital signatures. arXiv:quant-ph/0105032 (2001)
41. Chuang, I., Gottesman, D.: Quantum digital signatures. US Patent 7,246,240, 17 July 2007
42. Hillery, M., Bužek, V., Berthiaume, A.: Quantum secret sharing. Phys. Rev. A **59**(3), 1829 (1999)