

A Verification Algorithm and Its Application to Quantum Locker in IBM Quantum Computer

Avinash Dash^{*}

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

Sumit Rout[†]

*Integrated Science Education and Research Centre,
Visva Bharati University,
Santiniketan 731235, West Bengal, India*

Bikash K. Behera[‡] and Prasanta K. Panigrahi[§]

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

It is well known that Grover's algorithm asymptotically transforms an equal superposition state into an eigenstate (of a given basis). Here, we demonstrate a verification algorithm based on weak measurement which can achieve the same purpose even if the qubit is *not* in an equal superposition state. The proposed algorithm highlights the *distinguishability* between any arbitrary single qubit superposition state and an eigenstate. We apply this algorithm to propose the scheme of a Quantum Locker, a protocol in which any legitimate party can verify his/her authenticity by using a newly developed Quantum One-Time Password (OTP) and retrieve the necessary message from the locker. We formally explicate the working of Quantum Locker in association with the Quantum OTP, which theoretically offers a much higher security against any adversary, as compared to any classical security device.

Keywords: IBM Quantum Experience, Quantum Locker, Quantum OTP, Weak Measurement

I. INTRODUCTION

Before the advent of electronic information storage and transfer, a classical locker with a physical key was the only means available for secure storage of contents. The need to transmit information securely called for advanced methods of user authentication, *e.g.* passwords. The onset of the digital era has consequentially paved the way for highly secure means of information storage and retrieval such as e-lockers. However, the digitization era also brought with it increased vulnerability of static passwords to replay attacks. Recently, one-time passwords (OTPs) based on pseudo-random numbers have gained popularity, which are time-limited and suitable for highly confidential transactions.

In 1994, a quantum algorithm was introduced by Peter Shor which could efficiently prime-factorize any composite integer in polynomial time [1]. It is to be mentioned that one of the most extensively used and secure public-key cryptographic systems, the RSA protocol, relies on the fact that there is no existing

technology which can efficiently prime-factorize a very large integer in polynomial time [2]. The fascinating thing about a quantum computer is that the Shor's algorithm, if implemented on it, would break the RSA cryptosystem. A large-scale quantum computer once constructed, will render even some of the most secure classical cryptosystems futile. Over the past few years, the focus has shifted towards the development of security protocols which exploit some of the exclusive features of quantum mechanics, which may offer higher security than their classical counterparts. One such feature is the 'no-cloning theorem' [3], which forbids the construction of an exact replica of a generic/unknown quantum state. This property is greatly beneficial in quantum cryptosystems as it enables two communicating parties to detect whether or not an adversary has intercepted the transmitted message. Many quantum security schemes have been devised which have proved to be unconditionally secure protocols for safeguarding information [4–9]. Such protocols effectively use quantum phenomena like superposition and entanglement. Some of these information security techniques include a quantum key distribution scheme [4–12], quantum identification scheme [13–15], quantum digital signature scheme [16], quantum cheque scheme [17, 18], to name a few.

There have been many works in the past few years regarding the realization of OTPs in quantum format. A

^{*} ad16ms036@iiserkol.ac.in

[†] rsumitrou3@gmail.com

[‡] bkb13ms061@iiserkol.ac.in

[§] pprasanta@iiserkol.ac.in

quantum one-time password based on a set of n entanglements (Bell States) was proposed by Mihara [19]. Ioannou and Mosca presented an unconditionally secure quantum public-key identification protocol, in which the public keys were pure states [20]. Besides, recent works have led to the realization of robust authentication protocols based on quantum passwords [21, 22]. After then, encrypted data storage by the application of a disordered field on photonic quantum memories has been accomplished [23].

Some of the quantum security schemes mentioned above rely on the controlled Swap test for password verification, which indeed has some limitations. As in this case, an incorrect password gives the same outcome as a correct one with a considerably high probability, which is definitely undesirable. In our paper, we introduce a protocol based on weak measurement as a means of password verification. The advantage of our verification protocol is that the incorrect password can be distinguished from the correct one with a high probability, even for a single qubit one-time password. The accuracy of the protocol increases significantly if the OTP is composed of multiple qubits.

Some of the quantum security schemes, though deterministic, involve a system of qubits whose state is chosen from a finite set of distinguishable states. In such schemes, the OTP must consist of a very large number of such systems, to ensure that it becomes practically impossible for an adversary to guess the password. In contrast to this, the one-time password in our scheme comprises only a single qubit, prepared with the help of three parameters, each of which is an arbitrarily chosen real number lying in the interval $[-\pi, \pi]$, making it practically impossible for any adversary to guess the OTP.

The focus of our paper is the effective generation, communication and verification of a quantum One-Time Password. The OTP in our protocol constitutes a single qubit whose state is prepared by the designated party at will using parameter-based rotation matrices along the Bloch sphere axes, taking randomly generated values for parameters. The quantum teleportation protocol proposed by Bennett *et al.* [24] plays a key role for the secure conveyance of the OTP qubit to the receiving party. The receiver's qubit, now possessing the OTP state, is to be supplied to the locker for verification. The message is manifested in the form of a composite system of qubits. Using appropriate quantum gates, the information stored in message qubits is conveyed to corresponding qubits provided to the locker by the designated retriever.

The proposed quantum locker is one of many applications realizable in the future which will practically use quantum passwords. In our proposed scheme, the locker

does not involve any classical operations, nor does it require bits to store the output. In the course of our work, we hold the assumption that the sharing of entanglement between the two communicating parties considered is secure and can be preserved indefinitely without getting decohered or otherwise lost by other means [4, 25]. All quantum channels and gates used in our scheme are assumed to be free from decoherence and errors.

Recently, a series of quantum information processing tasks [26–40] have been run using IBM quantum computer. Hence, motivated by this fact, we have used “IBM 5 qubit transmon bowtie chip 3” named ibmqx4 to carry out the experimental procedure to explicitly show the working of our proposed verification algorithm and demonstrate the scheme of a Quantum Locker.

The paper is organized as follows. Section II provides the quantum gates used for the experimental purpose. Section III investigates the verification algorithm in detail, following which a comparison with Grover's search algorithm is shown. Section V & VII report the scheme of a Quantum Locker and its experimental demonstration respectively. Section VIII discusses about the security aspects of the proposed algorithm. Finally, we conclude in Section IX by stating an open problem to the scientific community.

II. PRELIMINARY GATES

Hadamard (H), Controlled-NOT ($CNOT$) and C^2NOT , Pauli gates (X , Y and Z), phase gate (S^\dagger), and rotation gates ($R_x(\theta_1)$, $R_y(\theta_2)$ and $R_z(\theta_3)$) are the key gates required for the experimental realization of the proposed protocol. Here, C^2NOT gate is a variant of the Toffoli gate which is explained in Section VID. $R_i(\theta)$ and $R_i(-\theta)$ denote rotation and inverse rotation gates respectively, along i direction by an angle θ , where $\theta \in [-\pi, \pi]$.

III. VERIFICATION ALGORITHM

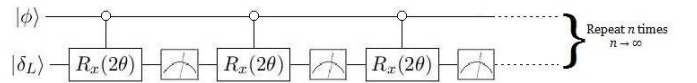


FIG. 1. Circuit illustrating the Verification Box V.

This algorithm uses a verification box V (Fig. 1) to discriminate two non-orthogonal states, i.e., $|0\rangle$, and a generic state $|\phi\rangle \equiv \alpha|0\rangle + \beta|1\rangle$. The proposed scheme is composed of several iterations of a weak measurement protocol, where an ancillary qubit $|\delta_L\rangle$ (in the state $|0\rangle$) is weakly coupled to the system. After each iteration, a projective measurement is performed on the ancilla, which slightly perturbs the state of the system ($|\phi\rangle$). The evolution of the coupled system ($|\phi\rangle \otimes |\delta_L\rangle$) after

each iteration is described by the following unitary operator U ,

$$U = [R_z(\theta) \otimes I_2][\cos\theta I_4 - i\sin\theta C^0 NOT_{12}] \quad (1)$$

where I_2 and I_4 denote identity matrices of order 2 and 4 respectively. Here, $C^0 NOT_{12}$ flips the target qubit only when the control qubit is in state $|0\rangle$. It is to be noted that the operator U describing the evolution of the coupled system is simply the $Controlled^0 - R_x(2\theta)$ operation, where the operator $R_x(2\theta)$ acts on the ancilla (target) qubit only if the system (control) qubit is in state $|0\rangle$. Here, θ is a parameter intrinsic to the locker, which is an arbitrarily small value ($\theta \rightarrow 0$). At the end of the first iteration, the operator U transforms the composite system $|\phi\rangle |\delta_L\rangle$ into the following state,

$$U |\phi\rangle |\delta_L\rangle \equiv (\alpha \cos\theta |0\rangle + \beta |1\rangle) |0\rangle - \alpha i \sin\theta |0\rangle |1\rangle \quad (2)$$

It can be verified that the operation $Controlled^0 - R_x(2\theta)$ can be implemented by using universal single qubit gates and $CNOT$ gate, as shown by the following circuit (Fig. 2).

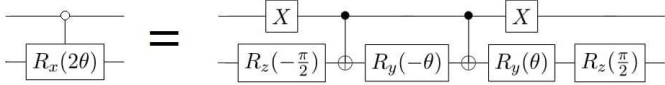


FIG. 2. Circuit depicting the implementation of $U \equiv Controlled^0 - R_x(2\theta)$.

After the execution of the unitary transformation U , a projective measurement (in z -basis) is performed on the ancillary qubit, resulting in outcomes $|0\rangle$ and $|1\rangle$ with probabilities p_0 and p_1 respectively.

$$p_0 = |\alpha|^2 \cos^2\theta + |\beta|^2 \approx 1 - |\alpha|^2 \theta^2 \quad (3)$$

$$p_1 = |\alpha|^2 \sin^2\theta \approx |\alpha|^2 \theta^2 \quad (4)$$

In the limit $\theta \rightarrow 0$, the probability of obtaining the state $|1\rangle$ on measurement of the ancilla is negligible. Hence, assuming the outcome of the ancilla state to be $|0\rangle$, the state of the system collapses to

$$\begin{aligned} |\phi\rangle &= \frac{\alpha \cos\theta |0\rangle + \beta |1\rangle}{\sqrt{|\alpha|^2 \cos^2\theta + |\beta|^2}} \\ &\approx (\alpha \cos\theta |0\rangle + \beta |1\rangle)(1 - |\alpha|^2 \theta^2)^{-\frac{1}{2}} \\ &\approx (\alpha(1 - \frac{\theta^2}{2}) |0\rangle + \beta |1\rangle)(1 + \frac{1}{2} |\alpha|^2 \theta^2) \\ &= \alpha(1 - \frac{|\beta|^2 \theta^2}{2}) |0\rangle + \beta(1 + \frac{|\alpha|^2 \theta^2}{2}) |1\rangle \end{aligned} \quad (5)$$

Evidently, after one iteration, the state of the system is perturbed. Denoting $\alpha' = \alpha(1 - \frac{|\beta|^2 \theta^2}{2})$ and $\beta' = \beta(1 + \frac{|\alpha|^2 \theta^2}{2})$, it is to be noted that $|\alpha'| < |\alpha|$, while $|\beta'| > |\beta|$, provided $\alpha \neq 0$ and $\beta \neq 0$. The state of the system is weakly perturbed towards the z -basis eigen state $|1\rangle$. If we repeat the unitary transformation U on the composite system, followed by a measurement on the ancillary qubit, the probability of obtaining the ancilla in the state $|1\rangle$, will be $p'_1 \approx |\alpha'|^2 \theta^2$, which is less than p_1 . Hence, the state of the ancilla collapses to the state $|0\rangle$ with an even higher probability than the previous one. In this case, the state of the system $|\phi\rangle$ is further perturbed towards the state $|1\rangle$. In other words, the co-efficient of the eigen state $|1\rangle$ in the superposition state of the system increases slightly in magnitude. If we repeat this protocol a large number of times, while assuming the state $|0\rangle$ is obtained in each measurement, we will obtain the final state $|\phi\rangle$ of the system (initially in the state $\alpha |0\rangle + \beta |1\rangle$) arbitrarily close to the z -basis eigen state $|1\rangle$. Our assumption, that the state $|0\rangle$ is obtained after every measurement of the ancilla, is justifiable since θ can take any arbitrary small value ($\theta \rightarrow 0$), such that the probability of getting $|1\rangle$ is also extremely small (having a θ^2 dependence). Additionally, our assumption is greatly aided by the fact that the probability of obtaining the state $|1\rangle$ decreases with each iteration, since it has a $|\alpha|^2$ dependence, and $|\alpha|$ decreases with each iteration.

It is evident that, after each iteration of the verification box, the state of the system does not change if it is initially in any of the z -basis eigenstates $\{|0\rangle, |1\rangle\}$. It can also be pointed out that the eigen states of the z -basis act as “fixed points” for the evolution protocol mentioned above, where $|0\rangle$ and $|1\rangle$ behave as unstable and stable fixed points respectively. However, if a generic superposition state $\alpha |0\rangle + \beta |1\rangle$ ($\alpha, \beta \neq 0$) is fed into our verification box, then the state of the system asymptotically approaches the stable fixed point $|1\rangle$. In this way, we can distinguish the eigenstate $|0\rangle$ from any arbitrary superposition state $\alpha |0\rangle + \beta |1\rangle$.

IV. COMPARISON WITH GROVER SEARCH ALGORITHM

Grover’s search algorithm is formulated to search a particular eigenstate by taking an equal superposition state, whereas our proposed algorithm can be used for the same purpose by considering an arbitrary superposition state. This is the distinguishing feature of our verification protocol from Grover’s algorithm.

Grover’s algorithm is based on rotation (more appropriately, reflection) matrices. A single iteration of Grover’s algorithm can be written as

$$G = DO \quad (6)$$

where D is the Grover diffusion operator and O is a unitary operator.

$$O = I - 2|\phi\rangle\langle\phi| \quad (7)$$

where $|\phi\rangle$ is the state to be “searched”.

The action of O on any generic state $|\psi\rangle$ can be imagined as a reflection operation on $|\psi\rangle$ about the hyperplane perpendicular to $|\phi\rangle$.

$$O|\psi\rangle \equiv R_{|\phi\rangle}|\psi\rangle \quad (8)$$

$$D = -(I - 2|\chi\rangle\langle\chi|) \quad (9)$$

$|\chi\rangle$ is the equal superposition state given by,

$$|\chi\rangle = \frac{1}{\sqrt{2^n}} \sum_{n=0}^{2^n-1} |x\rangle \quad (10)$$

D can also be imagined as a reflection operation.

$$D|\psi\rangle = -R_{|\chi\rangle}|\psi\rangle = R_{|\chi'\rangle}|\psi\rangle \quad (11)$$

If we consider a two-dimensional plane containing the unit vectors $|\phi\rangle$ and $|\chi\rangle$, then one may draw unit vectors perpendicular to these vectors, $|\phi'\rangle$ and $|\chi'\rangle$ respectively. Hence, O reflects any state about the $|\phi'\rangle$ axis, while D is equivalent to a reflection operation about the $|\chi\rangle$ axis.

Hence, the overall module of Grover’s algorithm is a series of two reflection operations. If

$$|\chi\rangle = \sin\theta|\phi\rangle + \cos\theta|\phi'\rangle \quad (12)$$

then the operation G performs an overall rotation of a generic state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ through an angle 2θ . $|\psi\rangle$ can be imagined as any unit vector lying in the two-dimensional plane.

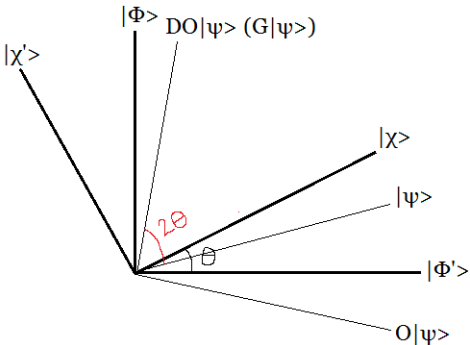


FIG. 3. Geometric visualization of Grover’s algorithm.

A single iteration of Grover’s algorithm rotates any arbitrary state $|\psi\rangle$, through an angle of $\frac{\pi}{2}$ about the z -axis, which can not be converted into an eigenstate asymptotically, as it transforms back to itself periodically after

4 iterations. Our verification algorithm uses an ancillary qubit, which is weakly coupled to the system qubit. It involves a repetitive series of coupling and decoupling of the ancilla (environment) with the system. Hence, some information about the state of the system is leaked to the environment. During the process, the coupling between the two qubits is followed by measurement of the ancilla in z -basis, which results in collapsing the state of the ancilla to a z -basis eigenstate ($|0\rangle$) with an extremely high probability. Correspondingly, the state of the system is only weakly perturbed, towards the other eigenstate ($|1\rangle$). This results in decoupling the system from the environment. The same procedure for coupling and decoupling is repeated a large number of times.

The coupling process takes place by means of the unitary transformation $U \equiv \text{Controlled}^0 - R_x(2\theta)$. To preserve the eigenstate $|0\rangle$ and transform any other arbitrary state to the eigenstate $|1\rangle$, the $\text{Controlled}^0 - R_x(2\theta)$ operation is used. In a way, it prevents any information about the state of the system related to the eigenstate $|0\rangle$ from passing to the environment (ancilla). The operation U is also equivalent to the operation $[R_z \otimes I]e^{-iC^0 \text{NOT}_{12}\theta}$, a *conditional* “decay” operation, which acts as an eigenstate amplifier, amplifying the eigenstate $|1\rangle$ in the superposition state $|\psi\rangle$.

V. QUANTUM LOCKER: BASED ON A QUANTUM OTP

A. Definition of a Quantum Locker and an OTP:

Informally, the proposed scheme of a quantum locker consists of three stages,

- **First stage**, where a message and certain parameters, required for the verification of One Time Password (OTP), are fed into the locker.
- **Second stage**, where a quantum OTP state is teleported to the intended receiver.
- **Third stage**, where a protocol is presented for the verification of the OTP and transfer of the message.

Ideally, an OTP is expected to have the following properties,

- **Verifiability**, i.e., it can be verified by the locker.
- **Unforgeability**, i.e., an OTP can neither be counterfeited nor can it be used more than once to access the message stored in the locker.

B. The Quantum Locker Scheme:

For the purpose of brevity, two parties, Alice and Bob, are introduced to describe the scheme. Initially,

they share a maximally entangled pair of qubits in the state, $\frac{|00\rangle + |11\rangle}{\sqrt{2}}$, which is to be used as the teleportation channel between the two. Alice stores a message along with an OTP in the locker, situated at a secure location accessible to both parties, so that Bob could access the message in the future. She then teleports the OTP to Bob, by using which he verifies his authenticity and retrieves the message from the locker.

Locker: It consists of m qubits which store the message (named as message qubits), and one ancillary qubit, which are inaccessible to any outside party. The message qubits can be either $|0\rangle$ or $|1\rangle$. The m qubit message is, therefore, an arbitrary string composed of $|0\rangle$ s and $|1\rangle$ s only. Let $|a_L^{(i)}\rangle$ and $|\delta_L\rangle$ denote the i^{th} message qubit and the ancillary qubit, in the locker respectively. Additionally, the locker has, an input slot for the password qubit through which any party may input the requisite qubit, as well as m other input slots into which the party may place m qubits in $|0\rangle$ state, meant for retrieving the message. In the whole scheme, it is assumed that Bob has the prior knowledge about the stored basis of all the message qubits.

VI. THE PROTOCOL

A. Storage of Message And Password

The m message qubits in the locker are initially prepared in $|0\rangle$ state. Now, Alice encodes her message in the locker by applying X gates on the requisite message qubits, in order to make a binary string of $|0\rangle$ s and $|1\rangle$ s. This feature is provided by the locker itself. For reasons that have been stated later, a string with all qubits in $|0\rangle$ state is not a valid message. Henceforth, for password purposes, Alice must randomly choose and input the values of θ_1 , θ_2 and θ_3 to the locker, where $\theta_1, \theta_2, \theta_3 \in [-\pi, \pi]$. These values act as parameters for the rotation operator denoted by, $R^{-1}(\theta_1, \theta_2, \theta_3)$, where $R^{-1}(\theta_1, \theta_2, \theta_3) = R_x(-\theta_1)R_y(-\theta_2)R_z(-\theta_3)$.

B. Generation of OTP State

Alice owns an ancilla qubit which is initially kept in $|0\rangle$ state. She is equipped with a portable device which can perform the operation, $R(\theta_1, \theta_2, \theta_3) = R_z(\theta_3)R_y(\theta_2)R_x(\theta_1)$, where θ_1, θ_2 and θ_3 are the same parameters previously used as inputs to the locker. Since this device is portable, she can perform this operation anytime and anywhere at her will. Alice generates the OTP state denoted by, $|\psi\rangle$ by performing the above operation on her ancilla qubit, and sends it to Bob through the teleportation channel.

C. Verification of OTP

For retrieving the message, Bob must store the teleported state, $|\psi\rangle$ in a qubit. The locker implements the operation $R^{-1}(\theta_1, \theta_2, \theta_3)$ on this qubit to create a new state, represented by $|\phi\rangle$. He also keeps m qubits (named as blank qubits) possessing $|0\rangle$ state in the specified slots of the locker. For the purpose of verification, a verification box V has been designed, the detailed working of which is discussed in Section III. The verification box V acts on $|\phi\rangle$ and produces two distinguishable results depending on whether the qubit entered by some party is in the state $|\psi\rangle$ (the state originally prepared by Alice) or not.

CASE I - Entering Correct Password: In this case, the password entered into the locker is in the state $|\psi\rangle$. The operation of $R^{-1}(\theta_1, \theta_2, \theta_3)$ on $|\psi\rangle$ yields $|\phi\rangle \equiv |0\rangle$. The state does not change by applying the verification box V on $|\phi\rangle$ a large number of times.

CASE II - Entering Wrong Password: In this case, the password entered into the locker is in a state $|\psi'\rangle$, which is different from the state $|\psi\rangle$. The operation of $R^{-1}(\theta_1, \theta_2, \theta_3)$ on $|\psi'\rangle$ yields $|\phi\rangle \equiv \alpha|0\rangle + \beta|1\rangle$, where α and β are arbitrary complex numbers. In this case, after the operation of the verification box V a large number of times, the state $|\phi\rangle$ is transformed into the state $|1\rangle$, which can be distinguished from the state $|0\rangle$.

D. Transfer of Message

After the operation of the verification box V on $|\phi\rangle$, a measurement is performed on this qubit (in z -basis). To transfer the i^{th} message qubit $|a_L^{(i)}\rangle$ to the i^{th} blank qubit $|b_L^{(i)}\rangle$, we use the circuit shown in Fig. 4.

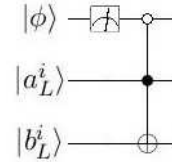


FIG. 4. A C^2 NOT gate is used for transferring information from the i^{th} message qubit $|a_L^{(i)}\rangle$ to the i^{th} blank qubit $|b_L^{(i)}\rangle$. This transfer of information takes place only if the qubit $|\phi\rangle$ is found to be in the state $|0\rangle$ after the measurement.

There are m such Toffoli gates as used in Fig. 4, where the first control qubit is in $|\phi\rangle$ state for all gates, the second control and the third target qubits are in $|a_L^{(i)}\rangle$

and $|b_L^{(i)}\rangle$ states respectively, for the i^{th} Toffoli gate. It is clear that the measurement of $|\phi\rangle$ gives the outcome $|0\rangle$ when the entered password is correct. Hence, $|b_L^{(i)}\rangle$ becomes $|1\rangle$ if $|a_L^{(i)}\rangle$ is in the state $|1\rangle$, otherwise it remains in the state $|0\rangle$. Thus, the information stored in the message qubits is transferred to the blank qubits entered into the locker by the party, which are now ready for retrieval.

For the case when the entered password is incorrect, measurement of $|\phi\rangle$ following the verification box gives the outcome $|1\rangle$ with an arbitrarily high probability. Hence, none of the $|b_L^{(i)}\rangle$ is flipped, resulting in no transfer of information. This explains why $|a_L^{(i)}\rangle = |0\rangle \forall i$ is not a valid message- we consider this case as “informationless”.

VII. IMPLEMENTATION IN IBM QUANTUM COMPUTER

A. Measurement of the ancillary qubit following each iteration

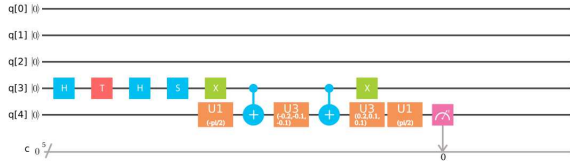


FIG. 5. IBM circuit illustrating a single iteration of the Verification Box V with an initial system state $|\phi\rangle \equiv \cos\frac{\pi}{8}|0\rangle + \sin\frac{\pi}{8}|1\rangle$ and ancilla state $|\delta\rangle \equiv |0\rangle$.

In the circuit shown in Fig. 5, measurement of the ancillary qubit is performed in z -basis. To obtain the experimental density matrix for state tomography, we must perform measurements on the ancilla in the x and y bases as well. By applying H or $S^\dagger H$ gate(s) before the measurement operation, the ancillary qubit can be measured in the x or y basis respectively. The experimental results are provided in Table I.

TABLE I. Table depicting the experimental results for the probability outcome of the ancilla state ($|\delta\rangle$).

Measurement of Ancilla State (For 8192 shots)		
Basis	Probability of $ 0\rangle$	Probability of $ 1\rangle$
x	0.498	0.502
y	0.710	0.290
z	0.938	0.063

To check the accuracy of our experimental results, quantum state tomography is performed. The theoretical density matrix of the ancilla is given by,

$$\rho^T = p_0 |0\rangle\langle 0| + p_1 |1\rangle\langle 1| \quad (13)$$

In the experiment, we have chosen $\theta = 0.2$ (Eq. (1)). Also, the initial state of the system (given by $|\phi\rangle$) is taken such that $\alpha = \cos\frac{\pi}{8}$ and $\beta = \sin\frac{\pi}{8}$. Putting the values of α , β and θ , and obtaining p_0 and p_1 (Eqs. (3),(4)), we evaluate ρ^T to be

$$\rho^T = \begin{bmatrix} 0.966 & 0.000 \\ 0.000 & 0.034 \end{bmatrix} \quad (14)$$

The following equation gives the experimental density matrix for a single qubit.

$$\rho^E = \frac{1}{2} [I + \langle x \rangle \sigma_x + \langle y \rangle \sigma_y + \langle z \rangle \sigma_z] \quad (15)$$

Here $\langle x \rangle$, $\langle y \rangle$ and $\langle z \rangle$ are related to the experimental outcomes of projective measurements in the x , y and z bases respectively, and are known as Stokes parameters. For a given basis j , its corresponding Stokes parameter is given by $\langle j \rangle = p_{|0_j\rangle} - p_{|1_j\rangle}$, where $|0_j\rangle$ and $|1_j\rangle$ are eigenstates of the given basis.

$$\rho_q^E = \begin{bmatrix} 0.937 & -0.002 \\ -0.002 & 0.063 \end{bmatrix} + i \begin{bmatrix} 0.000 & -0.210 \\ 0.210 & 0.000 \end{bmatrix} \quad (16)$$

Fig. 6 compares the theoretical and experimental density matrices of ancilla state. It is evident that the real part of the experimental density matrix is in good agreement with the theoretical one. Hence, it can be concluded that the ancilla state collapses to the eigenstate $|0\rangle$ with a high probability.

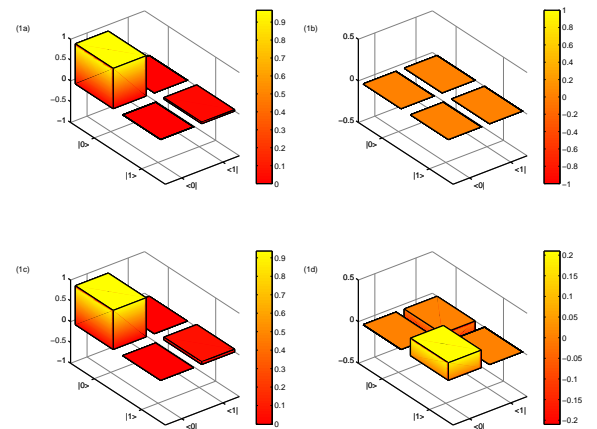


FIG. 6. Measurement of Ancillary Qubit: Real (left) and imaginary (right) parts of the reconstructed theoretical (1a,1b) and experimental (1c,1d) density matrices for the ancilla state.

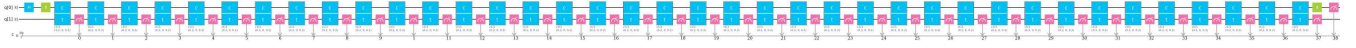


FIG. 7. Circuit clearly depicting the working of Verification Box V with an initial system state $|+\rangle$ and ancilla state $|0\rangle$.

B. Evolution of the system qubit after several iterations

We have used IBM's Custom Topology to simulate the working of our verification algorithm, where 38 iterations are taken into consideration. We use this model to examine the evolution of the system qubit $|\phi\rangle$ (initially in the state $|+\rangle$). In the above circuit (Fig. 7), $q[0]$ and $q[1]$ denote the system and the ancillary qubits respectively. The two qubit gates (c-t) represent the *Controlled* – $R_x(2\theta)$ operation, where $\theta = 0.1$. It is to be noted that, in our verification algorithm, we use the *Controlled*⁰ – $R_x(2\theta)$ operation, which can be equivalently produced by applying σ_x gates on system qubit ($q[0]$) before and after the *Controlled* – $R_x(2\theta)$ operation.

After simulating the above quantum circuit (Fig. 7) for 8192 shots, 248 different measurement outcomes are obtained, from which only two outcomes are found to occur a large number of times (6836 times). Specifically, each of these two outcomes are such that, all the 38 ancilla measurements (following every iteration) yield the state $|0\rangle$. Out of 6836 times, the system qubit measurement yields the state $|1\rangle$ 4116 times and the state $|0\rangle$ 2720 times. Hence, the system qubit is ultimately found to be in the eigenstate $|1\rangle$ with a high probability, even though it was initially prepared in the equal superposition state $|+\rangle$, as predicted by our proposed algorithm.

VIII. DISCUSSION

Here, we have discussed some significant features of the proposed quantum locker. It is also explained, how a quantum locker based on the principles of quantum mechanics offers significantly more security than a classical one which we use in our daily life.

A. Security Aspects

The security of the protocol is guaranteed by the secrecy of the parameters θ_1 , θ_2 and θ_3 , which are arbitrary real numbers chosen by the sender. It is in practice impossible to guess any arbitrarily chosen real number from a given interval $[a, b]$ which is dense in real numbers. Even for a single qubit OTP, like the case discussed so far in our paper, there are 3 real parameters, each one in the interval $[-\pi, \pi]$, which have to be guessed exactly in order to produce the correct password and retrieve the secured message. In a classical OTP, each

of its characters is chosen from a finite character set, for instance, the ASCII character set, which makes it, in practice, “crackable” with some finite probability. Thus, a classical OTP, even with multiple characters/digits, is no match for a quantum one consuming just a single qubit.

A profound feature of the protocol discussed here is the inability of a purported eavesdropper to steal the OTP, which Alice (the message encoder) teleports to Bob (the intended retriever). The members (qubits) of the EPR pair which serve as the teleportation channel is shared by the two parties only. Each operation required in the teleportation protocol is performed locally by either Alice or Bob. The only part of the protocol which is vulnerable to an eavesdropper is the series of classical channels used in the end. However, no productive information could possibly be obtained by stealing any data transmitted through these classical links. Unlike this, classical OTP must be communicated to the intended retriever through a classical link, which makes it vulnerable to outside party.

Another unique feature of the presented protocol is the intended retriever's ignorance of the OTP necessary for retrieval of the stored message. In our discussion, we have imagined that a person named Bob is the intended retriever of some message encoded by Alice. Bob receives the arbitrary state prepared by Alice by means of the teleportation protocol, which plays the role of the OTP. He has absolutely no idea as to which random values were chosen by Alice for the parameters θ_1 , θ_2 and θ_3 to prepare the OTP. In other words, no outside party—not even the one intended to retrieve the message—can forge the OTP. The necessary parameters for producing the correct password is known only to the encoder of the message.

In our protocol, the OTP is composed of a single qubit. The security can be further enhanced by the use of multiple qubits, say n , for the purpose of generating the OTP, where the values of the parameters (θ_1 , θ_2 and θ_3) are chosen independently for each qubit. We follow the same protocol as discussed here. All the n qubits are teleported to the intended retriever (say Bob) simultaneously. Bob places these qubits in their specified slots in the locker (along with the blank qubits for message retrieval). The verification protocol acts simultaneously on the OTP qubits (considering n in-built Verification

Boxes). The transfer of message takes place if and only if all the n qubits comprising the OTP collapse to the state $|0\rangle$ on measurement (similar to the case discussed earlier). In Section VID, the Toffoli gate, viz. the C^2NOT gate, the case in which $n = 1$, was used for message retrieval. In general, one may use a $C^{n+1}NOT$ gate for $n+1$ qubit system. Note that, a simple case of $n = 3$ has been shown in Fig. 8.

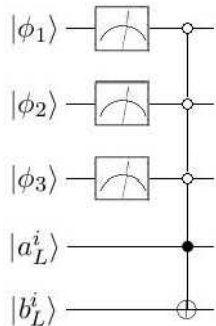


FIG. 8. A C^4NOT gate is used for transferring information from the i^{th} message qubit $|a_L^{(i)}\rangle$ to the i^{th} blank qubit $|b_L^{(i)}\rangle$, in case where the OTP comprises 3 qubits. Hence, the entered password must also consist of 3 qubits, whose states are transformed to the states $|\phi_1\rangle$, $|\phi_2\rangle$ and $|\phi_3\rangle$ respectively.

B. Limitations

The quantum locker scheme discussed here allows Bob to retrieve the message stored in the locker with certainty, viz. if the entered password is correct. When a wrong password is entered, then the protocol ensures that the message is not transferred to the blank qubits. However, the verification algorithm presented in Section III being probabilistic, there is always a minuscule possibility that the message is still transferred to the blank qubits. Consider the Case II stated earlier in Section VIC, namely the password entered into the locker is in a state $|\psi'\rangle$, implying that $|\phi\rangle \equiv \alpha|0\rangle + \beta|1\rangle$ ($\beta \neq 0$). When V operates on $|\phi\rangle$ there is an extremely slim chance of obtaining $|1\rangle$ whenever a projective measurement is performed on the ancillary $|\delta_L\rangle$ (Check Eq.(4)). In such a situation, the $|\phi\rangle$ collapses to the state $|0\rangle$, and remains in this state in subsequent iterations. Thus, the message will be transferred

to the blank qubits in such a scenario.

IX. CONCLUSION

To conclude, we have proposed here a verification algorithm, a novel version of Grover's algorithm, in a way that it takes an unequal superposition state and transforms it into an eigenstate. The algorithm also distinguishes any arbitrary superposition state from an eigenstate. Then we have introduced the concept of a locker based on the principles of quantum mechanics, which takes an arbitrarily generated quantum state as a password. The locker subsequently destroys the quantum information encoded in the password qubit(s) through the course of its operation. Hence, the password acts as a "One-Time Password". We have presented a password verification protocol based on the principles of weak measurement. The working of the verification algorithm has been experimentally realized with a high fidelity.

In our discussed protocol, we have imagined the contents of the locker to be some form of a message encoded by the sender, composed of a certain number of qubits. The basic principles of our quantum locker scheme could be extended to various other applications. Instead of storing a message, one may consider storing some physical entity, as one may wish, which could be accessible to the intended retriever once the entered password has been verified by the locker. Finally, we conclude our paper by inviting suggestions from the research community to tackle the limitations of our scheme to whatever possible extent. Is it possible to distinguish between an eigenstate and a generic superposition state deterministically? This is an open problem left for further discussion.

ACKNOWLEDGMENTS

AD would like to thank Kishore Vaigyanik Protsahan Yojana (KVPY) for providing financial support in the undertaking of this paper. BKB acknowledges the support of Inspire Fellowship awarded by DST, Government of India. SR would like to thank IISER Kolkata for providing hospitality during which this work has been done. The authors acknowledge the support of IBM Quantum Experience for producing experimental results. The views expressed are those of the authors and do not reflect the official policy or position of IBM or the IBM Quantum Experience team.

-
- [1] P. W. Shor, SIAM J. Comput. **26**, 1484 (1997).
 - [2] R. L. Rivest, A. Shamir, and L. Adleman, Mag. Commun. ACM **21**, 120 (1978).
 - [3] W. Wothers and W. Zurek, Nature **299**, 802 (1982).
 - [4] H. K. Lo and H. F. Chau, Science **283**, 2050 (1999).
 - [5] D. Mayers, eprint arXiv:quant-ph/9802025.

- [6] D. Mayers and A. Yao, Proc. 39th Annual Symp. Found. Comput. Sci. **IEEE**, 503 (1999).
- [7] E. Biham, M. Boyer, P. O. Boykin, T. Mor, and V. Roychowdhury, Proc. 32nd Annual ACM Symp. Theory Comput. **ACM**, 715 (2000).

- [8] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).
- [9] M. Fujiwara, A. Waseda, R. Nojima, S. Moriai, W. Ogata, and M. Sasaki, Sci. Rep. **6**, 28988 (2016).
- [10] C. H. Bennett and G. Brassard, Proc. IEEE Int. Conf. Comput. Syst. Signal Process. **IEEE**, 175 (1984).
- [11] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
- [12] C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).
- [13] M. L. Dušek, O. Haderka, M. Hendrych, and R. Myška, Phys. Rev. A **60**, 149 (1999).
- [14] H. N. Barnum, eprint arXiv:quant-ph/9910072.
- [15] J. G. Jensen and R. Schack, eprint arXiv:quant-ph/0003104.
- [16] D. Gottesman and I. Chuang, eprint arXiv:quant-ph/0105032.
- [17] S. R. Moulick and P. K. Panigrahi, Quantum Inf. Process. **15**, 2475 (2016).
- [18] B. K. Behera, A. Banerjee, and P. K. Panigrahi, eprint arXiv:1707.00182.
- [19] T. Mihara, Phys. Rev. A **65**, 052326 (2002).
- [20] L. M. Ioannou and M. Mosca, Theory Quantum Comput. Commun. Cryptogr. **6745**, 121 (2014).
- [21] M. Hotta and M. Ozawa, AIP Conf. Proc. **1110**, 388 (2009).
- [22] J. C. Garcia-Escartin and P. Chamorro-Posada, Phys. Rev. A **91**, 062310 (2015).
- [23] S-W. Su, S-C. Gou, L. Y. Chew, Y-Y. Chang, I. A. Yu, A. Kalachev, and W-T. Liao, Phys. Rev. A **95**, 061805 (2017).
- [24] C. H. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres, and W. K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993).
- [25] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, Phys. Rev. A **54**, 3824 (1996).
- [26] D. Alsina and J. I. Latorre, Phys. Rev. A **94**, 012314 (2016).
- [27] M. Berta, S. Wehner, and M. M. Wilde, New J. Phys. **18**, 073004 (2016).
- [28] J. R. Wootton, Quantum Sci. Technol. **2**, 015006 (2017).
- [29] A. R. Kalra, S. Prakash, B. K. Behera, and P. K. Panigrahi, eprint arXiv:1707.09462.
- [30] D. Ghosh, P. Agarwal, P. Pandey, and B. K. Behera, P. K. Panigrahi, eprint arXiv:1708.02297.
- [31] S. Gangopadhyay, Manabputra, B. K. Behera, and P. K. Panigrahi, eprint arXiv:1708.06375.
- [32] J. R. Wootton and D. Loss, eprint arXiv:1709.00990.
- [33] E. Huffman and A. Mizel, Phys. Rev. A **95**, 032131 (2017).
- [34] M. Sisodia, A. Shukla, and A. Pathak, eprint arXiv:1705.00670.
- [35] M. Schuld, M. Fingerhuth, and F. Petruccione, eprint arXiv:1703.10793.
- [36] A. Majumder, S. Mohapatra, and A. Kumar, eprint arXiv:1707.07460.
- [37] A. Kandala, A. Mezzacapo, K. Temme, M. Takita, M. Brink, J. M. Chow, and J. M. Gambetta, Nature **549**, 242 (2017).
- [38] R. Li, U. Alvarez-Rodriguez, L. Lamata, and E. Solano, eprint arXiv:1611.07851.
- [39] M. Sisodia, A. Shukla, K. Thapliyal, and A. Pathak, eprint arXiv:1704.05294.
- [40] Vishnu P. K., D. Joy, B. K. Behera, and P. K. Panigrahi, eprint arXiv:1709.05697.
- [41] İ. Yalçınkaya and Z. Gedik, eprint arXiv:1708.07900.